Release Notes for Cisco Wireless Controllers and Cisco Lightweight Access Points, Cisco Wireless Releases 8.0.150.0, and 8.0.152.0

First Published: August 31, 2017

This document describes what is new in 8.0.152.0 release, instructions to upgrade to this release, and information about the open and resolved caveats for this release. Unless otherwise noted, all Cisco Wireless Controllers are referred to as *Cisco WLCs*, and all Cisco lightweight access points are referred to as *access points* or *Cisco APs*.

Revision History

Table 1 Revision History

Modification Date	Modification Details
January 30, 2019	Added a note about issues related to Cisco Wave 1 AP flash and the solution to address them in the Upgrading Cisco Wireless Release section.
November 16, 2017	• Moved CSCvb77390 from Open Caveats list to Resolved Caveats list.
October 22, 2017	• Included Release 8.0.152.0 – Resolved caveats—CSCvf47808, CSCvg10793, CSCvg18366, CSCvg29019, and CSCvg42682
October 14, 2017	• Guidelines and Limitations, page 10 – Added note about reintroduction of support for Dynamic WEP in Cisco Wave1 APs.
October 10, 2017	• Features Not Supported on Cisco Virtual WLCs, page 23 – Added Wired Guest and FlexConnect central switching.

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

Cisco Wireless Controller and Cisco AP Platforms

The section contains the following subsections:

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

Supported Cisco Wireless Controller Platforms

The following Cisco WLC platforms are supported in this release:

- Cisco 2500 Series Wireless Controllers
- Cisco 5508 Wireless Controllers
- Cisco Flex 7500 Series Wireless Controllers
- Cisco 8510 Series Wireless Controllers
- Cisco Virtual Wireless Controllers (Cisco vWLC) on any one of the following systems:
  - Cisco Services-Ready Engine (SRE)
  - Cisco Wireless Controller Module for Integrated Services Routers G2 (UCS-E)
  - VMware vSphere Hypervisor (ESXi) version 5.x or 6.x
- 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 21.

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 24.

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

- AP860:

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

- AP880:

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

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

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

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

- AP890:

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

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

  Before you use an AP802 series lightweight access point with Cisco WLC software release 8.0.152.0, you must upgrade the software in the Next Generation Cisco 880 Series ISRs to Cisco IOS 15.1(4)M or later releases.

Unsupported Cisco Wireless Controller Platforms

The following Cisco WLC platforms are not supported:

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

What's New in Release 8.0.152.0

Release 8.0.152.0 is a repost of the Release 8.0.150.0 to address the caveats listed below. There are no other updates in this release, all resolved and open caveats in addition to the five resolved bugs apply to this release

Table 2 Resolved Caveats in Release 8.0.152.0

Caveat ID Number	Description
CSCvf47808	Cisco Wave1 APs: Key Reinstallation attacks against WPA protocol
CSCvg10793	Cisco Wave2 APs: Key Reinstallation attacks against WPA protocol

Table 2 Resolved Caveats in Release 8.0.152.0

Caveat ID Number	Description
CSCvg18366	hostapd deleting client entry when client goes to FWD state in WCPD
CSCvg29019	AP18xx : Bypassed scan in returning to DFS channel after blocked-list timeout
CSCvg42682	Cisco Wave 1 APs: Additional fix for Key Reinstallation attacks against WPA protocol

What's New in Release 8.0.150.0

There are no new features or enhancements in this release. This release addresses critical issues with the controller software. For more information, see the Caveats, page 25 section.

Software Release Support for Access Points

Table 3 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 3 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

Table 3 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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	—
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	—

Table 3 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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-1505	3.1.59.24	4.2.207.54M
	AIR-LAP-1510	3.1.59.24	4.2.207.54M

Table 3 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 3 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 version ID 01 (V01)	AIR-AP1572EAC-x-K9	8.0.110.0	—
	AIR-AP1572ICy[2]-x-K9	8.0.110.0	—
	AIR-AP1572ECy-x-K9	8.0.110.0	—
1570 version ID 02 (V02)[3]	AIR-AP1572EAC-B-K9	8.0.135.0	—
	AIR-AP1572EC1-B-K9	8.0.135.0	—
	AIR-AP1572EC2-B-K9	8.0.135.0	—
	AIR-AP1572IC1-B-K9	8.0.135.0	—
	AIR-AP1572IC2-B-K9	8.0.135.0	—
IW3700	IW3702-2E-UXK9	8.0.120.0	—
	IW3702-4E-UXK9	8.0.120.0	—

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

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

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

Software Release Types and Recommendations

This section contains the following topics:

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

Types of Releases

Table 4 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 5 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 Cisco Wireless Release

This section describes the guidelines and limitations that you must be aware of when you are upgrading the Cisco Wireless release and the procedure to upgrade.

Caution Before you upgrade to this release, we recommend that you go through the following documents to understand various issues related to Cisco Wave 1 AP flash and the solution to address them:

Field Notice: https://www.cisco.com/c/en/us/support/docs/field-notices/703/fn70330.html

Understanding Various AP-IOS Flash Corruption Issues: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/213317-understanding-various-ap-ios-flash-corru.html

Guidelines and Limitations

- Support for Dynamic WEP is reintroduced in Cisco Wave1 APs in this release.
- WLAN-AP group association functionality:
  - Functionality prior to Release 7.4.130.0—If a WLAN was added to an AP group prior to Release 7.4.130.0, the RF radio policy is set to All after an XML upload/download. This is because the default value of RF policy was not added. This issue was addressed through CSCud37443. However, this corrects only the newly created WLAN-AP group associations and not the previous ones. Therefore, if you have configured a WLAN-AP group association prior to Release 7.4.130.0, you must remove the WLAN from the AP group and add it again in Release 7.4.130.0 or a later release.
  - Change in functionality with Release 7.4.130.0—The RF radio policy is by default set to None for all WLAN-AP group associations created in Release 7.4.130.0. Any previous WLAN-AP group associations that are carried over will continue to be set to All unless a WLAN is removed from the AP group and added again.
  - If you have configured a WLAN radio policy for an AP group and are upgrading from Release 7.6 or an earlier release to an 8.0 release, the WLAN radio policy configuration is not retained. You will have to manually reconfigure the AP group WLAN radio policy. This issue is not encountered in any of the later releases. That is, if you are upgrading from a Release 8.0 to a later release, the WLAN radio policy configuration for an AP group is retained. This issue is addressed through CSCul59089.

Note The XML upload/download for AP group RF radio policy and WLAN radio are available only from Release 8.0.

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

  The workaround is as follows:

  a. Enter the following commands:

  ```
  config boot backup
  show boot

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

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

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

  ```
  config boot primary
  ```

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

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

- If you downgrade from Release 8.0.152.0 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 8.0.152.0, 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 8.0.152.0.
- We recommend that you install Release 1.9.0.0 of Cisco Wireless Controller Field Upgrade Software (FUS), which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA/MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. For more information, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_rn_OL-31390-01.html.

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

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

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

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

Note Bootloader upgrade is not required if FIPS is disabled.

- If you have to downgrade from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous Cisco WLC configuration files saved on the backup server, or to reconfigure the Cisco WLC.
- It is not possible to directly upgrade to Release 8.0.152.0 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 8.0.152.0. Table 6 shows the upgrade path that you must follow before downloading Release 8.0.152.0.

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

Table 6 Upgrade Path to Cisco WLC Software Release 8.0.152.0

Current Software Release	Upgrade Path to 8.0.152.0 Software[1]
7.4.x releases	You can upgrade directly to 8.0.152.0.
7.6.x releases	You can upgrade directly to 8.0.152.0.
8.0.1x.0	You can upgrade directly to 8.0.152.0.

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

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

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

- Cisco WLCs support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com.
- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the access points after a release upgrade and whenever an access point joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
  - Ensure that your TFTP server supports files that are larger than the size of Cisco WLC software Release 8.0.152.0. 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 8.0.152.0 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 8.0.152.0 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 8.0.152.0 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 8.0.152.0 (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 8.0.152.0 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 8.0.152.0 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 Cisco Wireless Release" section on page 10.

Interoperability With Other Clients in Release 8.0.152.0

This section describes the interoperability of Release 8.0.152.0 of the Cisco WLC software with other client devices.

Table 7 describes the configuration used for testing the client devices.

Table 7 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 8 lists the laptop client types on which the tests were conducted.

Table 8 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
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 9 lists the tablet client types on which the tests were conducted.

Table 9 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 10 lists the phone client types on which the tests were conducted.

Table 10 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

Table 10 Phone Client Type List

Client Type and Name	Version
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 24
- Features Not Supported on 1520 and 1550 APs (with 64 MB memory), page 24

Features Not Supported on 1130 and 1240 APs

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

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

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

- PPPoE
- PMIPv6

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

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

Features Not Supported on Mesh Networks

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

Caveats

- Cisco Bug Search Tool, page 25
- Open Caveats, page 26
- Resolved Caveats, page 28

Cisco Bug Search Tool

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

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

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

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

Open Caveats

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 25

Table 11 Open Caveats for Release 8.0.150.0 and 8.0.152.0

Caveat ID Number	Description
CSCuc12395	Annoying continuous trap message from WLC Client with MAC address has joined profile
CSCur40006	WLC: Group size exceeded message is displayed while adding a member to the static RF Group
CSCur88123	Invalid PSK for layer 2 security after controller reboot
CSCus53495	Cisco 2700, 3700 APs: DFS detection due to Broadcom spurious emissions
CSCus79046	CAPWAP AP does NOT fallback to IPv6 if ACL blocks IPv4 CAPWAP packets
CSCus79791	Client connected to 802.11n AP shows as 802.11ac client on WLC
CSCus90178	AIR-OEAP602I has TCP port 5162 open
CSCut81253	Ethernet Bridging does not work on RAP with 5-GHz backhaul
CSCut83422	Cisco vWLC SN changed after management interface IP change
CSCut90276	AireOS Traceback: APF-4-PROC_ACTION_FAILED
CSCuu14124	RF-profile losing the channel and coverage values after downloading the config file
CSCuu71471	MTU value stacks in HA
CSCuv10692	AckFailureCount getting huge value in short period.
CSCuv79354	Cannot configure IP address x.x.x.255 or x.x.x.0 as gateway in GUI
CSCuw03323	Cisco AP 702w draws additional power (22.1 watts) when LAN port 4 is disabled
CSCuw09545	Incorrect DHCP "Pool Usage" on the WLC when queried via SNMP
CSCuw27160	RF Grouping Algorithm's update interval is not synchronized between the Cisco controllers
CSCuw70789	AP using a reserved port to join the WLC
CSCux01697	WLC negative SNR values reported
CSCux25323	Unable to configure the native VLAN on FlexConnect AP
CSCux40480	CDP/LLDP information is missing for external APs in monitoring screen
CSCux80925	Media Stream - is not grayed out on traffic profile violation
CSCux88967	Client associated to SSID on MAC filter failure, after the session timeout it cannot associate again
CSCux99806	WGB: Cisco 2602 AP goes for a sleep and end up not responding for 100ms
CSCuy63742	Account commands send inconsistently to TACACS+ server for rapid commands
CSCuy70124	WLC does not send trap for port down on HA standby WLC
CSCuy71261	VLAN mapping has incorrect VLAN number after AP moved to AP group
CSCuy91177	Client MSCB is removed during optimized roaming
CSCuz50774	WLC losing pings to itself Reaper cleaning up exited task osapi_ping_rx

Table 11 Open Caveats for Release 8.0.150.0 and 8.0.152.0

Caveat ID Number	Description
CSCuz59858	Cisco 3500AP (SC1), client association failure - R2H Buffer full
CSCuz90954	MAP not joining the WLC when invalid static IP is configured
CSCuz97296	Cisco 3500AP: Client pak stuck during Payload Encryption
CSCva13929	Flex Data DTLS enabled AP gets stranded with WAN link flap
CSCva47491	AP load information not clear nor reset after AP radios are disabled
CSCva66489	802.11r session timeout after reassociation causing deauth 17 mismatch FTIE
CSCva82261	Cisco 1532 AP uplink drops when sending heavy upstream traffic
CSCva85667	Clients get TKIP MIC from Cisco 2702AP due to receiving the broadcast IPX
CSCva90265	iPAD PRO with IOS10 is getting deauthenticated at times due to M3 timer
CSCvb02472	Cisco controller reloads unexpectedly on radiusTransportThread, memory corruption
CSCvb12565	Cisco WLC stops working when running 'show run-config' command with no APs
CSCvb13666	WiSM2 stopped working with Task Name 'IPv6_Msg_Task'
CSCvb16806	Cisco 5500 WLC acting as MC showing stale connections from MA clients
CSCvb44169	emWeb reaper reset after “clear mdns service-database all”
CSCvb44699	NMSP queue full due to Rouge AP task
CSCvb56598	Client associating to FlexConnect WLAN receive irrelevant VLAN's ARP
CSCvb64042	WLC HA transfer download failure with legitimate network latency
CSCvb79274	WGB wired client expiring periodically
CSCvb95147	Cisco AP 1572EAC unable to use 80MHz
CSCvb97383	Cisco WLC deauthenticating roaming client with idle timeout
CSCvc00358	Cisco WLC reloads unexpectedly on “apfRogueTask_0” missed software watchdog
CSCvc01761	Cisco WLC continuously probes active RADIUS server
CSCvc11630	Radio reset in switching to connected mode from standalone
CSCvc22121	Mobility tunnels not coming up with new mobility
CSCvc40564	TPC - maximum and minimum power level are not set as expected
CSCvc65568	Cisco Wireless IP Phone 8821 fails 802.11r FT roam with 'Invalid FTIE MIC'
CSCvc66547	CPU ACL configured to block access to Virtual IP does not work as expected
CSCvc78546	WLC sets value to zero for 802.11e QoS for downstream voice traffic when CAC is disabled
CSCvd06848	WLC stopped working on SNMPTask
CSCvd09240	Local-auth EAP-TLS Windows 10 not working
CSCvd16346	WLC memory corruption occurs when TACACS+ responds with unknown attributes
CSCvd20251	Data Plane stopped working on Cisco 5508 WLC running 8.0.140.0
CSCvd44909	Client traffic dropped in Anchor foreign AireOS setup with new-mobility if foreign client behind NAT

Table 11 Open Caveats for Release 8.0.150.0 and 8.0.152.0

Caveat ID Number	Description
CSCvd53205	DCA lists in RF profiles are broken in the WLC configuration after the backup and restore is done
CSCvd72131	Cisco 7500 WLC in flex-mode stopped working after the SNMPTask Reaper reset
CSCve02612	HA-Config sync fails on standby when flex AP configurations are modified
CSCve02689	Silent reboot is observed after the memory usage goes up to 85%
CSCve68039	Some APs cannot join the WLC because the WLC misrecognizes the number of APs
CSCve75022	Cisco WLC does not apply QoS tag upstream from foreign to anchor
CSCve90085	Active WLC in HA pair crashes with task apfRogueTask_0
CSCvf55741	Cisco 1532 AP cannot use static IP address when configured as mesh AP (MAP)

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 25

Table 12 Resolved Caveats for Release 8.0.150.0 and 8.0.152.0

Caveat ID Number	Description
CSCuc78713	WEP client cannot receive broadcast after broadcast key rotation
CSCuq28038	Hop2- multiple attempts to rejoin WLC in very-fast convergence
CSCuq86263	False DFS detection on Cisco 1600AP
CSCur37829	AP management through non native VLAN - WGB clients does not join the AP
CSCur63031	AP error: %ENTROPY-0-ENTROPY_ERROR: Unable to collect sufficient entropy
CSCur68316	802AP-891 in FlexConnect mode are losing VLAN mapping after power cycle
CSCus83638	5-GHz radio on Cisco AP beaconing but not accepting client associations
CSCuu08012	Cisco 2700 AP CleanAir sensor died (src/dspm_main.c:389) - slot 0
CSCuu98142	Cisco 1130, 1240 Series APs do not work as root AP after software upgrade to 8.0.140.0 release
CSCuv33255	AP CDP neighbor information is missing or outdated
CSCuw29539	AP running lightweight IOS will not discover WLC using DNS
CSCux90031	Intermittent multiple packet or ping drop between RAP and Cisco 1572 Mesh AP
CSCux92335	Cisco 3602 APs running on Cisco 8.0.120.0 release is losing MAC address
CSCuy13829	AIR-CAP2602I reloads unexpectedly on dot11_pmkid_timeout
CSCuy32349	NDP timer change for 7.6 parity

Table 12 Resolved Caveats for Release 8.0.150.0 and 8.0.152.0

Caveat ID Number	Description
CSCuy53596	CleanAir fatal error and radio reset on Flex+Bridge AP
CSCuy61155	802.11b inconsistent probe response - band select enabled - 2.4GHz
CSCuy63094	Cisco 1572CM AP is not sending Option60
CSCuy93000	SC2 radio randomly sending corrupted timestamp BCN on hidden SSID
CSCuy94534	Cisco 3700, 2700APs on DFS do not see 3700, 2700 APs as neighbor when RxSOP is set to High/Med/Low
CSCuz20714	Cisco WLC reloads unexpectedly on emWeb with Reaper Reset
CSCuz22367	Cisco 3502 AP reloads unexpectedly on “LWAPP RM Receive process”
CSCuz47559	Error saving configuration file happens on Cisco Wave1 APs
CSCuz49804	Fix AID leak problems
CSCuz72994	FT clients reassociation denied leading to full association
CSCuz79051	WiSM2 8.1.131.0 reloads unexpectedly on ewaFormServe_multicast_detail
CSCva03376	UX-AP3702i After primed carrier set 5-GHz only allowing four UNII3 ch
CSCva27711	FlexConnect: AP radio reset during FT when Central DHCP is enabled WLAN
CSCva28211	AireOS UX AP: 'JP' should be used as world mode in Beacon and Probe Res
CSCva36161	Cisco 1600 AP reloads unexpectedly while 802.11w client connects or disconnects
CSCva41482	Autonomous AP does not forward ARP requests to client on tag VLAN
CSCva50180	AIR-CAP1602I-E-K9 stopped working
CSCva50196	Memory corruption EAP for Cisco Mesh AP
CSCva54211	IPsec tunnel of WLC with Linux Peer fails for AES128
CSCva56521	Cisco 1600 AP running 8.0 MR4 release - False DFS detection
CSCva65826	Wireless LAN Controller reboots unexpectedly
CSCva72044	Cisco 1572 Mesh AP with no distance command implementation
CSCva77451	AireOS WLC Local Auth EAP handler leak
CSCva83884	WLC System reloads unexpectedly on aaaQueueReader
CSCva87295	Flex AP radio reset during FT with Central DHCP and Nat-PAT is enabled
CSCva92615	Access Point antenna gain changes to 0dBi randomly
CSCva98597	Emweb task stuck at 100% CPU usage
CSCvb18339	DTLS connection failed because max control DTLS connections reached
CSCvb18427	DNS ACL allowing more URLS than the ones defined on 8.0.140.0
CSCvb19729	Cisco WLC reloads unexpectedly on task name EAP_Framework_0
CSCvb20553	CoA for session timeout not working using free RADIUS server
CSCvb21254	80MR4:AAA override VLAN lost on inter-controller roaming
CSCvb33101	Cisco AP 702w Ethernet stop passing traffic
CSCvb35018	Cisco WiSM2 reloads unexpectedly on task mdnsHATask

Table 12 Resolved Caveats for Release 8.0.150.0 and 8.0.152.0

Caveat ID Number	Description
CSCvb44979	WLC Local EAP with Cisco Unified Wireless IP Phone 7925 IP Phone Handshake Failure
CSCvb48354	RRM Not updating as per configured on WLC
CSCvb48603	Evaluation of WLC for OpenSSL September 2016
CSCvb67724	Cisco 5508 WLC is going out of memory
CSCvb69962	Client traps not showing session IDs
CSCvb77390	Cisco WLC stopped working while accessing MAC Address Database
CSCvb73104	Cisco 1600AP: radio d1 reset: FW: irq/mac stat=40000/10000000 command timeout
CSCvb76654	Clients not getting excluded on max EAPid timeouts; reassoc rejected with reason 12
CSCvb77649	PI 3.1.3 DP4 Identifies Cisco IW3700 as Cisco 1850E AP
CSCvb80511	CWA is not working for flex-bridge APs pointing ACL Rx from RADIUS that does not exist
CSCvb92562	Evaluation of all for OpenSSL 1.0.1 September 2016
CSCvb93189	AP drops retransmitted M3 from WLC
CSCvb94716	Cisco WLC reloads unexpectedly on task:spamReceiveTask running 8.0.140.3
CSCvb97456	80MR4: SSH on FIPS 140-1 is not compatible with older clients, SSH high disable does not work
CSCvb99468	AirOS WLC reloads unexpectedly in emWeb when serving an EmWebForm exclusion-list
CSCvc04089	Cisco 2700 series AP radio resets reason code 71 RADIO_RC_NO_REPORT
CSCvc08052	DFS false detection on Cisco 2700APs
CSCvc23658	Clients not removed from FlexConnect and CAPWAP in APs FlexConnect central-sw
CSCvc24485	#APF-3-UNKNOWN_RADIO_TYPE: [SS] apf_utils.c:571 Unknown Radio Type 0 from Standby flooding syslog
CSCvc33258	WLC: Unable to config RX-SOP threshold for Cisco IW3702 AP
CSCvc33793	Cisco WLC and connected AP get disconnected due to unequal load balance between SPAM queues high load
CSCvc40267	WLC sends wrong VLAN for AAA overridden client re-associating to AP belonging to FlexConnect Group
CSCvc45620	Cisco WLC reloads unexpectedly in SNMPTask due to missed software watchdog
CSCvc50436	WGB wired client randomly stuck in the DHCP_REQD state after layer 2 roaming between the controllers
CSCvc52093	Cisco WLC sends deauth 17 to phone in 4-way handshake
CSCvc52619	Local EAP do not support any of ciphers, used by Cisco Wireless IP Phone 8821
CSCvc62481	WLC 7500 HA stopped working on upgrade to 8.0.140.0 with Task Name: spamApTask
CSCvc65675	Cisco WLC: constantly increasing memory consumption by SNMPTask
CSCvc74507	Fix incorrect commit of CSCuu59589 in 8.0-mr

Table 12 Resolved Caveats for Release 8.0.150.0 and 8.0.152.0

Caveat ID Number	Description
CSCvc75625	PAosapi_msgq.c:926 Message queue RFID Queue is nearing full. Capacity 1024 Messages 973
CSCvc82053	The NMSP info and probe notification queue is saturating
CSCvc82559	Cisco WLC 5508 reaper rest stopped working on several tasks
CSCvc94648	Evaluation of WLC for OpenSSL Jan 2017
CSCvc99928	AP changing UP marking from 6 to 0 for downlink traffic after 802.11r roam with 8821 phones
CSCvd06463	AMSDU packets Tx cause 5 sec gap of packet Tx to Cisco Wireless IP Phone 8821 from Cisco Wave1 APs
CSCvd15742	Cisco AP reloads unexpectedly with %ENTROPY-0-ENTROPY_ERROR: Unable to collect sufficient entropy
CSCvd18025	Anchor1 WLC does not free client sessions after client roaming to Anchor2 WLC-client entries stale
CSCvd21155	WLC stopped working when multicasting traffic and accessing WLC GUI
CSCvd22535	Transfer upload support bundle support on GUI
CSCvd27398	WLC management access stops working while WLAN services are still up
CSCvd28374	Cisco 802AP incorrect base radio MAC assigned not ending with zero results in only one BSSID support
CSCvd31160	Cisco WLC shows cleared NAC clients with quarantine IP addresses
CSCvd44446	Retried EAP response dropped as a duplicate while First EAP Response was not even received on the AP
CSCvd50044	System stopped working multiple times on ping Rx task
CSCvd67178	Anchor not deleting webauth req client beyond webauth timeout
CSCve02679	VMs with Bridged Mode NIC on wireless client fails to get IP address
CSCve36706	AP cannot clear the client exclusion list after an exclusion timeout
CSCve55604	Cisco 3702 APs fail to download their image after joining Cisco 8510 WLC
CSCve76202	WLC IPv4 CPU ACL is applied as IPv6 CPU ACL during backup recovery or SSO failover
CSCvf47808	Cisco Wave 1 APs: Key Reinstallation attacks against WPA protocol
CSCvg10793	Cisco Wave 2 APs: Key Reinstallation attacks against WPA protocol
CSCvg18366	hostapd deleting client entry when client goes to FWD state in WCPD
CSCvg29019	AP18xx : Bypassed scan in returning to DFS channel after blocked-list timeout
CSCvg42682	Cisco Wave 1 APs: Additional fix for Key Reinstallation attacks against WPA protocol

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.