



Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.6.130.0

First Published: August 26, 2014

Last Updated: Jan 14, 2016

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

Contents

These release notes contain the following sections:

- [Cisco Wireless LAN Controller and Access Point Platforms, page 2](#)
- [What's New in This Release, page 3](#)
- [Software Release Support for Access Points, page 3](#)
- [Software Release Types and Recommendations, page 7](#)
- [Upgrading to Cisco WLC Software Release 7.6.130.0, page 8](#)
- [Special Notes for Licensed Data Payload Encryption on Cisco Wireless LAN Controllers, page 16](#)
- [Interoperability With Other Clients in Release 7.6.130.0, page 17](#)
- [Features Not Supported on Cisco WLC Platforms, page 19](#)
- [Caveats, page 22](#)
- [Installation Notes, page 44](#)
- [Service and Support, page 47](#)



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

Cisco Wireless LAN Controller and Access Point Platforms

The section contains the following subsections:

- [Supported Cisco Wireless LAN Controller Platforms, page 2](#)
- [Supported Access Point Platforms, page 2](#)
- [Unsupported Cisco Wireless LAN Controller Platforms, page 3](#)

Supported Cisco Wireless LAN Controller Platforms

The following Cisco WLC platforms are supported in this release:

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

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco Aironet 2700 and 700W Series Access Points.
- Cisco Aironet 3500p Access Point.
- Cisco 1040, 1130, 1140, 1240, 1250, 1260, 1600, 2600, 3500, 3600, 3700, Cisco 600 Series OfficeExtend Access Points, 700 Series, AP801, and AP802
- Cisco Aironet 1530 Series outdoor 802.11n mesh access points, Cisco Aironet 1550 (1552) Series outdoor 802.11n mesh access points, Cisco Aironet 1520 (1522, 1524) Series outdoor mesh access points
- AP801 and AP802 are integrated access points on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the access points and the ISRs, see the following data sheets:
 - AP860:
http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78_461543.html
 - AP880:
http://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.html
http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-613481.html

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

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

- AP890:

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



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



Note Before you use an AP802 series lightweight access point with Cisco WLC software release 7.6.130.0, you must upgrade the software in the Next Generation Cisco 880 Series ISRs to Cisco IOS 15.1(4)M or later releases.

Unsupported Cisco Wireless LAN Controller Platforms

The following Cisco WLC platforms are not supported:

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

What's New in This Release

There are no new features or enhancements in this release. For more information about updates in this release, see the [Caveats](#) section.

Software Release Support for Access Points

[Table 1](#) lists the Cisco WLC software releases that support specific Cisco access points. The First Support column lists the earliest Cisco WLC software release that supports the access point. For access points that are not supported in ongoing releases, the Last Support column lists the last release that supports the access point.



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

Table 1 **Software Support for Access Points**

Access Points		First Support	Last Support
700 Series	AIR-CAP702I-x-K9	7.5.102.0	—
	AIR-CAP702I-xK910	7.5.102.0	—
700W Series	AIR-CAP702W-x-K9	7.6.120.0	—
1000 Series	AIR-AP1010	3.0.100.0	4.2.209.0
	AIR-AP1020	3.0.100.0	4.2.209.0
	AIR-AP1030	3.0.100.0	4.2.209.0
	Airespace AS1200	—	4.0
	AIR-LAP1041N	7.0.98.0	—
	AIR-LAP1042N	7.0.98.0	—
1100 Series	AIR-LAP1121	4.0.155.0	7.0.x
1130 Series	AIR-LAP1131	3.1.59.24	—
1140 Series	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—
1220 Series	AIR-AP1220A	3.1.59.24	7.0.x
	AIR-AP1220B	3.1.59.24	7.0.x
1230 Series	AIR-AP1230A	3.1.59.24	7.0.x
	AIR-AP1230B	3.1.59.24	7.0.x
	AIR-LAP1231G	3.1.59.24	7.0.x
	AIR-LAP1232AG	3.1.59.24	7.0.x
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1260 Series	AIR-LAP1261N	7.0.116.0	—
	AIR-LAP1262N	7.0.98.0	—
1300 Series	AIR-BR1310G	4.0.155.0	7.0.x
1400 Series	Standalone Only	—	—
1600 Series	AIR-CAP1602I-x-K9	7.4.100.0	—
	AIR-SAP1602I-x-K9	7.4.100.0	—
	AIR-CAP1602E-x-K9	7.4.100.0	—
AP801	—	5.1.151.0	—
AP802	—	7.0.98.0	—
AP802H	—	7.3.101.0	—

Table 1 **Software Support for Access Points (continued)**

Access Points		First Support	Last Support
2600 Series	AIR-CAP2602I-x-K9	7.2.110.0	—
	AIR-SAP2602I-x-K9	7.2.110.0	—
	AIR-CAP2602E-x-K9	7.2.110.0	—
	AIR-SAP2602E-x-K9	7.2.110.0	—
2700 Series	AIR-CAP2702I-x-K9	7.6.120.0	—
	AIR-CAP2702E- x-K9	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 7.2.103.0 or a later release.			
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.207.54M
	AIR-LAP-1510	3.1.59.24	4.2.207.54M

Table 1 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later ¹	—
		All other reg. domains: 4.1.191.24M or 5.2 or later ¹	—
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later ¹	—
		All other reg. domains: 4.1.191.24M or 5.2 or later ¹	—
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later ¹	—
		All other reg. domains: 4.1.191.24M or 5.2 or later ¹	—
	AIR-LAP1522CM	7.0.116.0 or later.	—
	AIR-LAP1524SB	-A, C and N: 6.0 or later	—
		All other reg. domains: 7.0.116.0 or later.	—
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later ¹	—
1530	AIR-CAP1532I-x-K9	7.6	—
	AIR-CAP1532E-x-K9	7.6	—
1550	AIR-CAP1552I-x-K9	7.0.116.0	—
	AIR-CAP1552E-x-K9	7.0.116.0	—
	AIR-CAP1552C-x-K9	7.0.116.0	—
	AIR-CAP1552H-x-K9	7.0.116.0	—
	AIR-CAP1552CU-x-K9	7.3.101.0	—
	AIR-CAP1552EU-x-K9	7.3.101.0	—
1552S	AIR-CAP1552SA-x-K9	7.0.220.0	—
	AIR-CAP1552SD-x-K9	7.0.220.0	—

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



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

Software Release Types and Recommendations

This section contains the following topics:

- [Types of Releases, page 7](#)
- [Software Release Recommendations, page 8](#)
- [Solution Compatibility Matrix, page 8](#)

Types of Releases

Table 2 *Types of Releases*

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

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

Software Release Recommendations

Table 3 Software Release Recommendations

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

For detailed release recommendations, see the software release bulletin:

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

Solution Compatibility Matrix

Table 4 Solution Compatibility Matrix

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

For more information about the Cisco Wireless solution compatibility matrix, see

<http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html>.

Upgrading to Cisco WLC Software Release 7.6.130.0

Guidelines and Limitations

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

The workaround is as follows:

- a. Enter the following commands:

```
config boot backup
```



```
show boot
```

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

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

```
config boot primary
```



Note The pings are not available in Cisco 5500 Series WLC when New Mobility is enabled.



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

- If you have ACL configurations in the Cisco WLC and downgrade from a 7.4 or a later release to a 7.3 or an earlier release, you might experience XML errors on rebooting the Cisco WLC. However, these errors do not have any impact on any functionality or configurations.
- When FlexConnect access points (known as H-REAP access points in the 7.0.x releases) that are associated with a Cisco WLC that has all the 7.0.x software releases prior to Release 7.0.240.0 upgrade to Release 7.6.130.0, the access points lose the enabled VLAN support configuration. The VLAN mappings revert to the default values of the VLAN of the associated interface. The workaround is to upgrade from Release 7.0.240.0 or a later 7.0.x release to Release 7.6.130.0.
- When a client sends an HTTP request, the Cisco WLC intercepts it for redirection to the login page. If the HTTP request intercepted by the Cisco WLC is fragmented, the Cisco WLC drops the packet because the HTTP request does not contain enough information required for redirection.
- A client whose home page is an HTTPS (HTTP over SSL, port 443) one is not redirected by Web Auth to the web authentication dialog box. Therefore, it is not possible for such a client to get authenticated, and eventually, fails to connect to the network. The workaround is for the client to open an HTTP (port 80) web page.
- We recommend that you install Release 1.9.0.0 of Cisco Wireless LAN Controller Field Upgrade Software (FUS), which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA/MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. For more information, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_rn_OL-31390-01.html



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



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

- After you upgrade to Release 7.4, networks that were not affected by the existing preauthentication ACLs might not work because the rules are now enforced. That is, networks with clients configured with static DNS servers might not work unless the static server is defined in the preauthentication ACL.
- On Cisco Flex 7500 Series WLCs, if FIPS is enabled, the reduced boot options are displayed only after a bootloader upgrade.



Note Bootloader upgrade is not required if FIPS is disabled.

- If you have to downgrade from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous Cisco WLC configuration files saved on the backup server, or to reconfigure the Cisco WLC.
- It is not possible to directly upgrade to Release 7.6.130.0 release from a release that is earlier than Release 7.0.98.0.
- You can upgrade or downgrade the Cisco WLC software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to Release 7.6.130.0. [Table 5](#) shows the upgrade path that you must follow before downloading Release 7.6.130.0.



Caution

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

Table 5 Upgrade Path to Cisco WLC Software Release 7.6.130.0

Current Software Release	Upgrade Path to 7.6.130.0 Software
7.0.x releases	You can upgrade directly to 7.6.130.0. Note If you have VLAN support and VLAN mappings defined on H-REAP access points and are currently using a 7.0.x Cisco WLC software release that is prior to 7.0.240.0, we recommend that you upgrade to the 7.0.240.0 release and then upgrade to 7.6.130.0 to avoid losing those VLAN settings.
7.1.91.0	You can upgrade directly to 7.6.130.0.

Table 5 Upgrade Path to Cisco WLC Software Release 7.6.130.0 (continued)

Current Software Release	Upgrade Path to 7.6.130.0 Software
7.2.x releases	<p>You can upgrade directly to 7.6.130.0.</p> <p>Note If you have an 802.11u HotSpot configuration on the WLANs, we recommend that you first upgrade to the 7.3.101.0 Cisco WLC software release and then upgrade to the 7.6.130.0 Cisco WLC software release.</p> <p>You must downgrade from the 7.6.130.0 Cisco WLC software release to a 7.2.x Cisco WLC software release if you have an 802.11u HotSpot configuration on the WLANs that is not supported.</p>
7.3.x releases	You can upgrade directly to 7.6.130.0.
7.4.x releases	You can upgrade directly to 7.6.130.0.
7.5.x releases	You can upgrade directly to 7.6.130.0.
7.6.100.0	You can upgrade directly to 7.6.130.0.
7.6.110.0	You can upgrade directly to 7.6.130.0.
7.6.120.0	You can upgrade directly to 7.6.130.0.

- When you upgrade the Cisco WLC to an intermediate software release, you must wait until all of the access points that are associated with the Cisco WLC are upgraded to the intermediate release before you install the latest Cisco WLC software. In large networks, it can take some time to download the software on each access point.
- Cisco Prime Infrastructure 1.4.1 is needed to manage Cisco WLC software Release 7.6.130.0.
- You can upgrade to a new release of the Cisco WLC software or downgrade to an earlier release even if Federal Information Processing Standard (FIPS) is enabled.
- When you upgrade to the latest software release, the software on the access points associated with the Cisco WLC is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.
- We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 9 or a later version or Mozilla Firefox 17 or a later version.

For the Cisco WLAN Express Setup for Cisco 2500 Series Wireless Controller feature, we recommend the following browsers:

- Microsoft Internet Explorer 10 or a later version
 - Mozilla Firefox 26 or a later version
 - Apple Safari 6 or a later version
- Cisco WLCs support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com.

- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the access points after a release upgrade and whenever an access point joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
 - Ensure that your TFTP server supports files that are larger than the size of Cisco WLC software Release 7.6.130.0. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the Prime Infrastructure. If you attempt to download the 7.6.130.0 Cisco WLC software and your TFTP server does not support files of this size, the following error message appears:

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

Bootloader menu for Cisco 5500 Series WLC:

```

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

Bootloader menu for other Cisco WLC platforms:

```

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

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



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

- The Cisco WLC bootloader stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the bootloader to boot with the backup image. With the backup image stored before rebooting, choose **Option 2: Run Backup Image** from the boot menu to boot from the backup image. Then, upgrade with a known working image and reboot the Cisco WLC.

- You can control the address(es) sent in the CAPWAP discovery responses when NAT is enabled on the Management Interface using the following command:

config network ap-discovery nat-ip-only {enable | disable}

Here:

- enable**— Enables use of NAT IP only in a discovery response. This is the default. Use this command if all the APs are outside the NAT gateway.
- disable**— Enables use of both NAT IP and non-NAT IP in a discovery response. Use this command if APs are on the inside and outside the NAT gateway; for example, Local Mode and OfficeExtend APs are on the same Cisco WLC.



Note

To avoid stranding APs, you must disable AP link latency (if enabled) before you use the disable option for the **config network ap-discovery nat-ip-only** command. To disable AP link latency, use the **config ap link-latency disable all** command.

- You can configure 802.1p tagging by using the **config qos dot1p-tag {bronze | silver | gold | platinum}** tag. For Release 7.2.103.0 and later releases, if you tag 802.1p packets, the tagging has impact only on wired packets. Wireless packets are impacted only by the maximum priority level set for QoS.
- You can reduce the network downtime using the following options:
 - You can predownload the AP image.
 - For FlexConnect access points, use the FlexConnect AP upgrade feature to reduce traffic between the Cisco WLC and the AP (main site and the branch). For more information about the FlexConnect AP upgrade feature, see the *Cisco Wireless LAN Controller FlexConnect Configuration Guide*.



Note

Predownloading Release 7.6.130.0 on a Cisco Aironet 1240 access point is not supported when upgrading from a previous Cisco WLC release. If predownloading is attempted on a Cisco Aironet 1240 access point, an AP disconnect will occur momentarily.

- Do not power down the Cisco WLC or any access point during the upgrade process; otherwise, you might corrupt the software image. Upgrading a Cisco WLC with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported, the upgrade time should be significantly reduced. The access points must remain powered, and the Cisco WLC must not be reset during this time.
- If you want to downgrade from Release 7.6.130.0 to Release 6.0 or an earlier release, perform either of these tasks:
 - Delete all the WLANs that are mapped to interface groups, and create new ones.
 - Ensure that all the WLANs are mapped to interfaces rather than interface groups.
- After you perform these functions on the Cisco WLC, you must reboot the Cisco WLC for the changes to take effect:
 - Enable or disable link aggregation (LAG)
 - Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
 - Add a new license or modify an existing license
 - Increase the priority for a license

- Enable the HA
- Install the SSL certificate
- Configure the database size
- Install the vendor-device certificate
- Download the CA certificate
- Upload the configuration file
- Install the Web Authentication certificate
- Make changes to the management interface or the virtual interface
- For TCP MSS to take effect

Upgrading to Cisco WLC Software Release 7.6.130.0 (GUI)

Step 1 Upload your Cisco WLC configuration files to a server to back them up.



Note We highly recommend that you back up your Cisco WLC configuration files prior to upgrading the Cisco WLC software.

Step 2 Follow these steps to obtain the 7.6.130.0 Cisco WLC software:

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

<https://software.cisco.com/download/navigator.html>

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

c. Click **Wireless LAN Controllers**.

The following options are available:

- Integrated Controllers and Controller Modules
- Standalone Controllers

d. Depending on your Cisco WLC platform, select one of these options.

e. Click the Cisco WLC model number or name.

The **Download Software** page is displayed.

f. Click a Cisco WLC software release number. The software releases are labeled as follows to help you determine which release to download:

- **Early Deployment (ED)**—These software releases provide new features and new hardware platform support as well as bug fixes.
- **Maintenance Deployment (MD)**—These software releases provide bug fixes and ongoing software maintenance.
- **Deferred (DF)**—These software releases have been deferred. We recommend that you migrate to an upgraded release.

g. Click a software release number.

h. Click the filename (*filename.aes*).

i. Click **Download**.

- j. Read the Cisco End User Software License Agreement and click **Agree**.
- k. Save the file to your hard drive.
- l. Repeat steps a. through k. to download the remaining file.

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

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



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

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

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

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

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

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

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

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

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

- a. In the **Server Login Username** text box, enter the username to log on to the FTP server.
- b. In the **Server Login Password** text box, enter the password to log on to the FTP server.
- c. In the **Server Port Number** text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

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

A message appears indicating the status of the download.

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

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

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

Step 17 Re-enable the WLANs.

Step 18 For Cisco WiSM2 on the Catalyst switch, check the port channel and re-enable the port channel if necessary.

Step 19 If you have disabled the 802.11a/n and 802.11b/g/n networks in [Step 4](#), re-enable them.

Step 20 To verify that the 7.6.130.0 Cisco WLC software is installed on your Cisco WLC, click **Monitor** on the Cisco WLC GUI and view the Software Version field under Controller Summary.

Special Notes for Licensed Data Payload Encryption on Cisco Wireless LAN Controllers

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

Important Note for Customers in Russia

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



Note

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

Downloading and Installing a DTLS License for an LDPE Cisco WLC

-
- Step 1** Download the Cisco DTLS license.
- Go to the Cisco Software Center at this URL:
<https://tools.cisco.com/SWIFT/LicensingUI/Home>
 - On the Product License Registration page, choose **Get New > IPS, Crypto, Other Licenses**.
 - Under **Wireless**, choose **Cisco Wireless Controllers (2500/5500/7500/8500/WiSM2) DTLS License**.
 - 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:
- Go to the Cisco Software Center at this URL:
<http://www.cisco.com/cisco/software/navigator.html?mdfid=282585015&i=rm>
 - Choose the Cisco WLC model.
 - Click **Wireless LAN Controller Software**.
 - In the left navigation pane, click the software release number for which you want to install the non-LDPE software.
 - Choose the non-LDPE software release: AIR-X-K9-X-X.X.aes
 - Click **Download**.
 - Read the Cisco End User Software License Agreement and then click **Agree**.
 - 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 20](#) detailed in the “[Upgrading to Cisco WLC Software Release 7.6.130.0](#)” section on [page 8](#).
-

Interoperability With Other Clients in Release 7.6.130.0

This section describes the interoperability of Release 7.6.130.0 of the Cisco WLC software with other client devices.

[Table 6](#) describes the configuration used for testing the clients.

Table 6 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	7.6.130.0
Cisco WLC	Cisco 5500 Series Controller
Access points	1131, 1142, 1242, 1252, 3500e, 3500i, 3600, 3702, 2702, 702W
Radio	802.11ac, 802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 4.2, ACS 5.2
Types of tests	Connectivity, traffic, and roaming between two access points

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

Table 7 **Client Types**

Client Type and Name	Version
Laptop	
Intel 4965	v13.4
Intel 5100/5300/6200	v14.3.2.1
Intel 6300	V15.9.2.1
Intel 1000/1030/6205	v14.3.0.6
Intel 7260(11AC)	17.0.0.34, Windows 8.1
Broadcom 4360(11AC)	6.30.163.2005
Dell 1395/1397/Broadcom 4312HMG(L)	XP/Vista: 5.60.18.8 Win7: 5.30.21.0
Dell 1501 (Broadcom BCM4313)	v5.60.48.35/v5.60.350.11
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1515(Atheros)	8.0.0.239
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	v5.100.235.12
Cisco CB21	v1.3.0.532
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro	OSX10.9.2
MacBook Air	OSX 10.9.2, BCM43xx 1.0(6.30.223.154.45)
Macbook Pro with Retina Display 2013	OSX 10.9.2
Handheld Devices	
Apple iPad2	iOS 7.1(11D167)
Apple iPad3	iOS 7.1(11D167)
Apple iPad Mini with Retina display	iOS 7.1(11D167)
Asus Transformer	Android 4.0.3
Sony Tablet S	Android 3.2.1
Toshiba Thrive	Android 3.2.1
Samsung Galaxy Tab	Android 3.2
Motorola Xoom	Android 3.1
Nexus 7 2nd gen	Android 4.4.2
Intermec CK70	Windows Mobile 6.5 / 2.01.06.0355
Intermec CN50	Windows Mobile 6.1 / 2.01.06.0333
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R
Phones and Printers	

Table 7 *Client Types (continued)*

Client Type and Name	Version
Cisco 7921G	1.4.2.LOADS
Cisco 7925G	1.4.2.LOADS
Ascom i75	1.8.0
Spectralink 8030	119.081/131.030/132.030
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.345
Apple iPhone 4	iOS 7.1(11D167)
Apple iPhone 4S	iOS 7.1(11D167)
Apple iPhone 5	iOS 7.1(11D167)
Apple iPhone 5s	iOS 7.1(11D167)
Apple iPhone 5c	iOS 7.1(11D167)
Ascom i62	2.5.7
HTC One(11AC)	Android 4.3
Samsung Galaxy S4 - GT-I9500(11AC)	Android 4.3
Samsung Galaxy S4 - GT-I9500(11AC)	Android 4.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Samsung Galaxy Nexus GTI9200	Android 4.2.2
Samsung Galaxy SIII	Android 4.3
Sony Xperia Z ultra (11AC)	Android 4.3
Samsung Galaxy Mega SM900(11AC)	Android 4.4.2

Features Not Supported on Cisco WLC Platforms

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

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

Features Not Supported on Cisco 2500 Series WLCs

- Wired Guest Access
- Bandwidth Contract
- Service Port

- AppleTalk Bridging
- Right-to-Use licensing
- PMIPv6
- High Availability (1:1)
- Multicast-to-Unicast



Note

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



Note

Directly connected APs are supported only in the Local mode.

Features Not Supported on WiSM2 and Cisco 5500 Series WLCs

- Cisco WLAN Express Setup
- 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

- Cisco WLAN Express Setup
- Static AP-manager interface



Note

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

- L3 Roaming
- VideoStream
- TrustSec SXP
- IPv6/Dual Stack client visibility



Note IPv6 client bridging and Router Advertisement Guard are supported.

- Internal DHCP Server
- Access points in local mode



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

- Mesh
- Spanning Tree Protocol (STP)
- Cisco Flex 7500 Series WLC cannot be configured as a guest anchor Cisco WLC. However, it can be configured as a foreign Cisco WLC to tunnel guest traffic to a guest anchor Cisco WLC in a DMZ.
- Multicast



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

- PMIPv6
- New Mobility

Features Not Supported on Cisco 8500 WLCs

- Cisco WLAN Express Setup
- TrustSec SXP
- Internal DHCP Server

Features Not Supported on Cisco Virtual WLCs

- Cisco WLAN Express Setup
- Internal DHCP server
- TrustSec SXP
- Access points in local mode
- Mobility/Guest Anchor
- Multicast



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

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



Note Outdoor APs in the FlexConnect mode are supported.

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

Features Not Supported on Mesh Networks

- Multicountry support
- Load-based CAC (mesh networks support only bandwidth-based CAC or static CAC)
- High availability (fast heartbeat and primary discovery join timer)
- AP acting as supplicant with EAP-FASTv1 and 802.1X authentication
- Access point join priority (mesh access points have a fixed priority)
- Location-based services, which are deployed on outdoor mesh networks have a lesser degree of accuracy due to AP density

Caveats

The following sections lists [Open Caveats](#) and [Resolved Caveats](#) for Cisco WLCs and lightweight access points for Release 7.6.130.0. To enable you to locate caveats in the Cisco Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

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

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

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



Note

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

Open Caveats

Table 8 lists the open caveats in the 7.6.130.0 Cisco WLC software release.

Table 8 **Open Caveats**

ID	Description
CSCuo83747	<p>Symptom: DHCP RADIUS profiling fails for Windows XP and 7 workstations. ISE reports the client Endpoint Profile and Policy as Unknown.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • Controller with 7.6.100.0. • AP in FlexConnect mode. • Radius NAC and AAA override enabled. • DHCP required. <p>Workaround:</p> <ul style="list-style-type: none"> • Use central switching <p>Or</p> <ul style="list-style-type: none"> • For direct ISE profiling, send DHCP helper traffic to ISE.
CSCup47474	<p>Symptom: Controller has the following log message:</p> <pre>*apfRogueTask_2: <Date Timestamp>: #APF-1-ROGUE_AP_CONTAIN_FAILED: apf_rogue.c:5644 Unable to contain rogue <MAC address>. multicast bit set in BSSID.</pre> <p>Conditions: Controller tries to contain rogues.</p> <p>Workaround: None.</p>
CSCuo85511	<p>Symptom: WiSM2 appears as an unknown device type in PI.</p> <p>Conditions: Unknown</p> <p>Workaround: None</p>
CSCuh42398	<p>Symptom: Controller has the following message in log:</p> <pre>#NIM-3-CANT_DISABLE_MCAST: nim.c:4542 Cannot disable multicast state.</pre> <p>Conditions: Unknown</p> <p>Workaround: None</p>

Table 8 **Open Caveats (continued)**

ID	Description
CSCuo59440	<p>Symptom: Guest users continue to stay connected to the controller after the guest user account is suspended or expired on ISE.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • Controller with 7.6.100.16 and with guest anchor setup. • ISE 1.2 is used for central Webauth. • New mobility is enabled on the controller. <p>Workaround: Disable new mobility on the controller.</p>
CSCun40401	<p>Symptom: BV11 interface on the motherboard shows UP and Gig0 interface on the cable modem shows UP when AP 1552c reboots. AP does not use cable modem Ethernet and uses the radio interface.</p> <p>Conditions: Unknown</p> <p>Workaround: Reboot AP</p>
CSCup37463	<p>Symptom: AP 1552C cable modem Gig Ethernet link is marked down.</p> <p>Conditions: 1552C AP with cable modem.</p> <p>Workaround: Reset the AP.</p>
CSCui10087	<p>Symptom: 8500 controller does not send DNS IPv4 address in the DHCP offer received from PBA.</p> <p>Conditions: PMIPv6-enabled WLAN interfaces.</p> <p>Workaround: None.</p>
CSCul32444	<p>Symptom: Client does not get IP address from LMA.</p> <p>Conditions: Client is associated to a local mode AP.</p> <p>Workaround: None.</p>
CSCuo82771	<p>Symptom: Client does not get IP from LMA if the WLAN is a 802.1x WLAN.</p> <p>Conditions: WPA2-802.1x WLAN is configured.</p> <p>Workaround: Use open Auth WLAN.</p>
CSCup17073	<p>Symptom: Controller drops all PMIPv6 packets with UDP port 5436.</p> <p>Conditions: After controller gets a UDP packet with port 5436, which the MAG does not understand.</p> <p>Workaround: Reboot the controller.</p>
CSCup27028	<p>Symptom: Controller crashes.</p> <p>Conditions: PMIPV6_Thread_0 takes too much CPU.</p> <p>Workaround: None.</p>
CSCup13476	<p>Symptom: Mesh AP radio fails with missing radio power table file errors.</p> <p>Conditions: AP cannot find the power table for 802.11 radio1.</p> <p>Workaround: None.</p>

Table 8 **Open Caveats (continued)**

ID	Description
CSCuo74117	<p>Symptom: Inconsistent results and channel do not change during interference for off-channel scan result of 20/40/80MHz channels.</p> <p>Conditions: AP 3702E in local mode with no clients.</p> <p>Workaround: None.</p>
CSCup72151	<p>Symptom: 802.11ac module does not power up and appears in reset state.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • AP3602i with 802.11ac module • Avaya ERS 4850GTS-PWR+ switch <p>Workaround: Use Cisco power injector or Cisco switch.</p>
CSCun23283	<p>Symptom: 5500 and 8500 controllers crashed when PMIPv6 clients connect.</p> <p>Conditions: Controller has HA setup.</p> <p>Workaround: None.</p>
CSCup72502	<p>Symptom: Cisco 5500 controller with 7.6.120.0 does not deauthenticate clients when FlexConnect ACL is not present on the AP.</p> <p>Conditions: FlexConnect ACL is pushed from AAA server but is not present on AP.</p> <p>Workaround: Apply the FlexConnect ACL on the AP.</p>
CSCuj17683	<p>Symptom: AP may send deauthentication with reason code 7 during 802.11r roaming.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • AP roam is in a bad RF environment. • Clients fail to hear ACK for reassociation request from AP and continue to send reassociation request. <p>Workaround: After deauthentication, roam is enabled and clients are able to join again.</p>
CSCun30047	<p>Symptom: The following message appears when clients with wrong credentials associate with WLAN and are kept in the same state for a few days:</p> <pre>ADD_TO_BLACKLIST_FAILED: Unable to create exclusion-list entry</pre> <p>Conditions: Unknown</p> <p>Workaround: None.</p>
CSCuj78942	<p>Symptom: Trunk VLAN ID is not in AP 1240.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCun20584	<p>Symptom: AP replicates broadcast packets to the default gateway.</p> <p>Conditions: Multiple IP subnetworks on the same VLAN that AP has its BVI.</p> <p>Workaround: None.</p>

Table 8 **Open Caveats (continued)**

ID	Description
CSCuj32257	<p>Symptom: AP secures CAC bandwidth for SIP phones during inter-controller roaming though the phone does not have any active SIP call.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • SIP phone is roaming with inter-controller • 32 byte call ID <p>Workaround: Use call ID less than 32 bytes.</p>
CSCum82560	<p>Symptom: AP2602 sends deauthentication frames to the new channel after channel change occurs due to radar detection.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • Controller with 7.6.100.0 • AP 3602E and AP 2602E • Channel change from DFS-enabled channel to another channel switch announcement is disabled. <p>Workaround: None.</p>
CSCun25987	<p>Symptom: AP stays in RLDP process for long time which results in beacon outage.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCun70043	<p>Symptom: AP 2600 crashes randomly and comes back automatically with the following trace decode:</p> <pre>Unexpected exception to CPU: vector 700, PC = 0x244ACD4 , LR = 0x244ACD4 Traceback= 0x244ACD4z 0x244ACD4z ap3g2-k9w8-tar.ap_n_esc.201310081058.symbols.gz read in Enter hex value: 0x244ACD4z 0x244ACD4z 0x244ACD4:soap_handle_isr_watchdog(0x244aca4)+0x30 0x244ACD4:soap_handle_isr_watchdog(0x244aca4)+0x30</pre> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCug38888	<p>Symptom: Disabled SSID is broadcast by 2.4-GHz radio.</p> <p>Conditions: SSID was created and disabled.</p> <p>Workaround: Reconfigure AP</p>
CSCuo57524	<p>Symptom: Unable to enable AVC with FUS older than 1.8.0.0.</p> <p>Conditions: FUS is older than 1.8.0.0.</p> <p>Workaround: Upgrade FUS version to 1.8.0.0 or above.</p>
CSCul44588	<p>Symptom: When a frame contains channel 0 in the radio header, at the AP, it appears as channel N/A for WIPS alarms, such as RTS and CTS.</p> <p>Conditions: The triggering frames are sent at 5 GHz.</p> <p>Workaround: None.</p>

Table 8 *Open Caveats (continued)*

ID	Description
CSCup21962	<p>Symptom: Client is unable to change SSIDs. When joining a second SSID, client data is not replicated to the anchor controller and the foreign controller updates the client details.</p> <p>Conditions: Fast SSID is enabled.</p> <p>Workaround: Disable fast SSID. However, Apple clients may fail for other reasons with this configuration.</p>
CSCud57046	<p>Symptom: Client entry is seen on multiple controllers even when it not anchored to the controller or its mobility group.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCun20768	<p>Symptom: Clients are unable to associate to flex mode local switching WLAN.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCuj48021	<p>Symptom: Client stays in WebAuth_REQD state after roaming from 7.4 MR to 7.6.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCuj28495	<p>Symptom: clmgmtLicenseUsageCountRemaining does not return Remaining AP Count.</p> <p>Conditions: 5500 controller with 7.3.103.15</p> <p>Workaround: None.</p>
CSCuh12796	<p>Symptom: Consecutive SNMP set commands for same MIB variable on controller fails. The following error appears in the packet:</p> <p>Reason: noCreation (That table does not support row creation or that object can not ever be created)</p> <p>Conditions: Unknown.</p> <p>Workaround: Perform SNMP get before doing set.</p>
CSCui99062	<p>Symptom: Controller accepts SysRq Magic key on the console. This action allows an unauthenticated user with access to the serial console to unconditionally reboot the controller from the SysRq menu.</p> <p>Following is the SysRq menu that appears when you enter the magic key:</p> <pre>SysRq : HELP : loglevel0-8 reBoot Crashdump tErm Full kIll Dump showMem Nice showPc show-all-timers(Q) Sync showTasks Unmount show-blocked-tasks</pre> <p>Conditions:</p> <ul style="list-style-type: none"> • All released images of the controller. • SysRq magic key given from the Serial console <p>Workaround: Return key exits from the SysRq menu and returns to the console. Controller functions normally while in the SysRq menu or even after exiting it.</p>

Table 8 **Open Caveats (continued)**

ID	Description
CSCuo19677	<p>Symptom: When you change the AP bandwidth setting from 20MHz to 40MHz, the configuration changes, but the HT_capability field is not updated.</p> <p>Conditions: Mesh configuration.</p> <p>Workaround:</p> <ul style="list-style-type: none"> • Manually reset the AP. <p style="text-align: center;">or</p> <ul style="list-style-type: none"> • Execute the test capwap restart command on the AP console to make the configuration change.
CSCun15820	<p>Symptom: 5508 controller reports its MAC address in duplicate IP address message:</p> <pre>#DTL-1-IP_CONFLICT_DETECTED: dt1_net.c:4857 Network device with mac addr <mac_address>:0f using IP address of local interface 'management'. <IP_address> - Received ARP Reply on interface 13 with vlan ID 189. IP conflict</pre> <p>Conditions: Problem continues after upgrading from 7.4.100.0 to 7.4.110.0 and occurs constantly.</p> <p>Workaround: None.</p>
CSCul72669	<p>Symptom: LWAP does not send out deauthentication messages to existing client before Dot11Radio interface is reset by RLDP. However, debug dot11 mgmt msg output indicates that the messages are sent out.</p> <p>Conditions: RLDP is enabled on the LWAP.</p> <p>Workaround: Disable RLDP.</p>
CSCup75446	<p>Symptom: Default interface takes precedence over foreign VLAN mapping in a guest anchor setup. If the AAA server does not send any interface details, the anchor controller uses the default interface configuration of the WLAN to assign IP address to the client.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • Configure Guest Anchor solution. • Enable foreign controller interface mapping in the anchor controller. • Enable AAA override in the WLAN and Radius NAC. <p>Workaround: None.</p>
CSCui22330	<p>Symptom: Default QoS DSCP and CoS (802.1p) value are not according to IEEE/IETF standards.</p> <p>Conditions: Unknown.</p> <p>Workaround: Map each priority on the switch/router between the controller and AP. In 7.5, default DSCP is 18 (010 010) which is IP Precedence 2 and it belongs to Class 2.</p>
CSCun19827	<p>Symptom: DHCP IPv6 address is detected as duplicate on MAC/linux.</p> <p>Conditions: Unknown.</p> <p>Workaround: Use SLAAC address on MAC. Ensure NS Multicast CacheMiss Forwarding option is disabled in the show ipv6 summary output.</p>

Table 8 *Open Caveats (continued)*

ID	Description
CSCuc78713	<p>Symptom: Dynamic WEP client do not receive broadcast packets after broadcast key rotation.</p> <p>Conditions: Software: 7.0.235.0, 7.2.110.0, 7.3.101.0</p> <p>Workaround:</p> <ul style="list-style-type: none"> • Execute config advanced eap bcast-key-interval 86400 • Change security setting to WPA2
CSCul25617	<p>Symptom: A popup with the message, <code>Failed to Add MDNS profile</code> appears when you enable AP Management on dynamic interface.</p> <p>Conditions: When you enable AP Management on dynamic interface.</p> <p>Workaround: None.</p>
CSCum61068	<p>Symptom: <code>SNMP connection failure</code> error appears for controllers on PI 2.0. <code>ncs-0-0.log</code> on PI shows an exception in object <code>WlcScheduledReset</code>, error-</p> <pre>Failed to discovery class class com.cisco.server.managedobjects.bridge.WlcScheduledReset on device 10.3.252.22. Device is unreachable.</pre> <p>Conditions:</p> <ul style="list-style-type: none"> • Prime Infrastructure 2.0 • 5508 controller with 7.4.100.60 <p>Workaround: Configure a random future time for a scheduled reboot on the controller.</p>
CSCul82557	<p>Symptom: Flex group PMK cache causes <code>SpamReceieveTask 100%</code> and AP cannot join.</p> <p>Conditions: Flex APs using Flex groups join the controller at the same time and when the controller sends the PMK to the Flex APs.</p> <p>Workaround: Use the test pmk cache delete all command to delete the PMK, kill the queue and to join the APs.</p>
CSCui75794	<p>Symptom: Foreign controller does not respond to ARP from foreign export client to a local client being on the same VLAN.</p> <p>Conditions: Client performs L3 roaming.</p> <p>Workaround: Run an image that also has the fix for CSCug80814.</p>
CSCum73288	<p>Symptom: Friendly rogue AP disappears after 2 minutes.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCui26077	<p>Symptom: Fast transition roam fails between FlexConnect APs.</p> <p>Conditions: FT client and FlexConnect APs advertise 802.11r FT PSK WLAN.</p> <p>Workaround: None.</p> <p>Normal roam occurs when FT roam fails. Use FT-802.1x or use 802.11i fast roam methods like OKC.</p>

Table 8 **Open Caveats (continued)**

ID	Description
CSCup81511	<p>Symptom: Incorrect WMM UP to DSCP markings on AP1131 and AP1242.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • WISM2 • AP 1131 or AP 1242 • 7.6.120.0 <p>Workaround: None.</p>
CSCuj74920	<p>Symptom: Intermittent RADIUS assigned VLAN fails during inter-controller roam.</p> <p>Conditions: Client roams between two controllers.</p> <p>Workaround: None.</p>
CSCuj32157	<p>Symptom: iPad and iPhone cannot discover print services.</p> <p>Conditions: Unknown.</p> <p>Workaround: Remove the domain name setting in the DHCP and also on the clients (iPads, iPhones, etc.) from their server setting.</p>
CSCug91684	<p>Symptom: Layer 2 ACL does not work in virtual controller using central switching.</p> <p>Conditions: Virtual controller with central switching and Layer 2 ACL is applied.</p> <p>Workaround: Remove Layer 2 ACL.</p>
CSCuh46442	<p>Symptom: LWAP displays %CAPWAP-3-ERRORLOG messages when it joins a controller.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCuj58625	<p>Symptom: Controller with Local EAP-FAST crashes.</p> <p>Conditions: Unknown.</p> <p>Workaround: Use an external RADIUS server.</p>
CSCul75254	<p>Symptom: mDNS: memory leak observed when you create or delete service groups continuously.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCuj93777	<p>Symptom: Mesh AP does not block data packets before BPDU packets are handled.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • Mesh AP reboots. Movement between RAPs. • Intensive flooding of packets in the network causes packets to be sent before BPDUs are propagated. <p>Workaround: None.</p>
CSCtd34834	<p>Symptom: Unable to disable MFP traps.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>

Table 8 *Open Caveats (continued)*

ID	Description
CSCuj60088	<p>Symptom: The following error appears:</p> <pre>#MM-3-MEMORY_READ_ERROR: mm_mobile.c:1128 Error reading mobility memory, possible race condition. Encountered memory error, Please report the error if you experience a crash</pre> <p>Conditions: 5508 controller has mobility peers.</p> <p>Workaround: None.</p>
CSCun47705	<p>Symptom: Multicast traffic does not flow for some ranges of multicast addresses.</p> <p>Conditions: The failure of forwarding traffic happens under the following conditions</p> <ul style="list-style-type: none"> • 7500 controller, 8500 controller, vWLC • An address is searched within an address range. • Address is smaller than another address irrespective of the endianness on a byte comparison. <p>Workaround: None.</p>
CSCum77921	<p>Symptom: 5508 controller crashes at sshpmLscScepTask when you enable AP LSC provisioning.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCuo96442	<p>Symptom: Unable to join nor change the country code of an OEAP600 with -E regulatory domain when Israel (IL) country code is enabled.</p> <p>Conditions: OEAP600 with -E regulatory domain when Israel (IL) country code is enabled.</p> <p>Workaround: Depending on version of controller, disabling IL will allow the AP to join and also provide the ability to change the country code on a previously joined OEAP600.</p>
CSCuh16870	<p>Symptom: Client with static IP loses connectivity on session timeout.</p> <p>Conditions: This problem occurs when:</p> <ul style="list-style-type: none"> • Interface that the client gets from the interface group does not match the interface corresponding to the static IP. • Client gets VLAN overridden with this message: <pre>apfReceiveTask: May 28 12:48:28.066: 00:1a:70:a5:2f:bd Overriding interface of client from 'vlan20' to 'vlan30' within interface group 'vlan20-30' *apfReceiveTask: May 28 12:48:28.066: 00:1a:70:a5:2f:bd Applying Interface policy on Mobile, role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 20</pre> <p>Workaround: Either disable interface groups or set DHCP required.</p>

Table 8 **Open Caveats (continued)**

ID	Description
CSCuh16842	<p>Symptom: Client gets IPv6 address from different VLAN.</p> <p>Conditions: This problem occurs under the following conditions:</p> <ul style="list-style-type: none"> • Interface group • Client sends traffic from either static IP, or previously allocated IP. • Client traffic does not match the assigned VLAN received initially. <p>Workaround: Use DHCP required.</p>
CSCup60282	<p>Symptom: Ping generated from controller is of incorrect ICMP type.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCun18315	<p>Symptom: RADIUS server anomalies with controller.</p> <p>Conditions: When the primary RADIUS server fails, the secondary or tertiary controllers fail within 2 seconds.</p> <p>Workaround: None.</p>
CSCun99205	<p>Symptom: Rogue containment does not work on local mode AP 3600 with WSSI module.</p> <p>Conditions: Controller with Release 7.6.110.0.</p> <p>Workaround: None.</p>
CSCug34802	<p>Symptom: Rogue containment fails on 5-GHz radio.</p> <p>Conditions: Rogue AP on 5-GHz.</p> <p>Workaround: None.</p>
CSCun25338	<p>Symptom: Rogue state changed by field is missing after a config download.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCup49763	<p>Symptom: AP700 series cannot scan beyond the country channel that is determined by AP regulatory domain.</p> <p>Conditions: When the Channel List is “All Channels” (Wireless > 802.11a/b > RRM > General)</p> <p>Workaround: None.</p>
CSCul21877	<p>Symptom: RRM 2.4-GHz neighbor does not appear in the WSM wireless security module of AP in FlexConnect mode.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCul57266	<p>Symptom: Client details on controller is inaccurate compared to the FlexConnect AP details.</p> <p>Conditions: FlexConnect Local Auth is enabled.</p> <p>Workaround: Use the show capwap reap association command to check the correct status of the client.</p>

Table 8 *Open Caveats (continued)*

ID	Description
CSCuh26716	<p>Symptom: <code>show redundancy summary</code> command shows HA SKU even if the controller is not a HA-SKU controller.</p> <p>Conditions: This problem occurs when you execute the command on:</p> <ul style="list-style-type: none"> • Secondary controller is converted from primary controller. • HA-SKU machine <p>Workaround: None.</p>
CSCui90481	<p>Symptom: <code>SnmpOperationException</code> Table is too large. Refresh configuration fails due to CDP SNMP looping.</p> <p>Conditions: Unknown.</p> <p>Workaround: Disable AP neighbor CDP on controller.</p>
CSCuf79553	<p>Symptom: SSH to controller works when <code>mgmt-via-dynamic-interface</code> is disabled.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCuo48442	<p>Symptom: Stale old data encryption session history appears when you do not have any APs associated to the controller.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • When you enable data encryption and disable it. • Controller with 7.5.102.0, 7.6.100.0, 7.6.110.0. • AP1600/2600/3600 series <p>Workaround: None.</p>
CSCuj95892	<p>Symptom: When a port in a LAG goes down and then comes up, the controller does not send syslog messages to the syslog server.</p> <p>Conditions: Distribution ports are configured in a LAG and syslog server is configured.</p> <p>Workaround: Check the message logs in the controller GUI.</p>
CSCuo20684	<p>Symptom: When you change the <code>timestamp-tolerance</code> value from 1000 to 0 after restoring, the value does not appear in <code>show guest-lan <wlan-id></code> command.</p> <p>Conditions: 7.4.110.0 , 7.4.121.0 and 7.6.</p> <p>Workaround: None.</p>
CSCun11108	<p>Symptom: Virtual controller serial number changes after three hardware or configuration changes.</p> <p>Conditions: The serial number is not valid after a certain number of changes.</p> <p>Workaround: Take a snapshot of the virtual machine and revert back.</p>
CSCuf77488	<p>Symptom: FT and LT detection time for an alarm is ahead or later than the AP clock and causes a delay in NCS to detect the alarm.</p> <p>Conditions: 5508 controller with 7.0.235.3 and AP3500 wIPS ELM mode</p> <p>Workaround: None.</p>

Table 8 **Open Caveats (continued)**

ID	Description
CSCun34295	<p>Symptom: WiSM2 crashes on radiusTransportThread task.</p> <p>Conditions: 7.4.121.5</p> <p>Workaround: To resolve the client connectivity or authentication problem, increase the RADIUS timeout.</p>
CSCuj66912	<p>Symptom: SNMP get for WiSM2 reports that WiSM2 has secondary power supply.</p> <p>Conditions: WiSM2 running 7.0.235.3.</p> <p>Workaround: None.</p>
CSCul04029	<p>Symptom: Controller crashes on emWeb task.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • 5508 controller with 7.3.112.0 with a mobility setup. • High Availability • Legacy Mobility in use (default) <p>Workaround: Do not change new mobility parameters while using legacy mobility and HA.</p>
CSCuh42665	<p>Symptom: Controller sends incorrect information about rogue AP detection using traps.</p> <p>Conditions: Controller with 7.4.110.</p> <p>Workaround: None.</p>
CSCuj60872	<p>Symptom: Controller crashes due to reaper reset for apfMsConnTask_6.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCuj97293	<p>Symptom: Controller crashes when you execute the show local-auth certificates command.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCuo36531	<p>Symptom: Controller crashes with task name: mmListen.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCup64468	<p>Symptom: Syslog messages with prefix # appears instead of %.</p> <p>Conditions: Syslog is enabled on controller.</p> <p>Workaround: None.</p>
CSCug74517	<p>Symptom: Controller shows wrong interface name for a client although the client is assigned to the right subnet.</p> <p>Conditions: This problem occurs when there are hundreds of dynamic interfaces on the controller. The display error appears also on Prime Infrastructure as it pulls the error from the controller.</p> <p>Workaround: None.</p>

Table 8 *Open Caveats (continued)*

ID	Description
CSCuj83637	<p>Symptom: After an HA failover, the service port on the active controller, configured to get its IP address via DHCP, loses connectivity after the DHCP lease expires.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • WLC or WiSM2 running 7.4.110.x or 7.5.102.x code in HA • Service port is configured for DHCP. • The problem is seen after the following events happen in the specified order: <ul style="list-style-type: none"> – HA failover – DHCP lease expiration of service port. <p>Workaround:</p> <p>Configure a static IP address for the service ports on both peers and then force a HA switchover.</p> <p>From the active controller, follow the steps below:</p> <ul style="list-style-type: none"> • config interface dhcp service-port disable • config interface address service-port <addr1> <netmask> • config redundancy interface address peer-service-port <addr2> <netmask> redundancy force-switchover <p>Note When you force a switchover, all the clients and any mesh APs are moved to 7.4. Cisco recommends that you perform the above steps during a maintenance window.</p>
CSCuh97457	<p>Symptom: Incompatibility behavior on CoA for RFC 3576 implementation.</p> <p>Conditions: COA on controller.</p> <p>Workaround: When the following three AVP pair attributes are sent, the controller accepts the disconnect request:</p> <ul style="list-style-type: none"> • Calling-Station-ID MAC address of device (lower case works) • Service-Type Login-user • Called-Station-ID (upper case MAC of AP+SSID separated by colons)
CSCud76513	<p>Symptom: Unable to view neighbor information.</p> <p>Conditions: Unknown.</p> <p>Workaround: Search individual AP for all missing ones</p>
CSCuh81923	<p>Symptom: Controller sends incorrect RADIUS accounting attributes.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • Controller with 7.2.111.3 • ACS Radius Server 5.4 • WLAN: L3 Web Auth <p>Workaround: None.</p>

Table 8 **Open Caveats (continued)**

ID	Description
CSCul34417	<p>Symptom: Active and standby controllers remain active with recovering when the network converges.</p> <p>Conditions: When both the controllers are booting, and RMI and RP are down.</p> <p>Workaround: Manually reboot one controller.</p>
CSCup57457	<p>Symptom: Unable to change rogue state of WS-SVC-WISM2-K9.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCuq32731	<p>Symptom: Cisco 2504 WLC stopped working while configuring New Mobility on Catalyst 3850 Switch side.</p> <p>Conditions: New mobility in use and mobility heartbeat transmitter list is empty.</p> <p>Workaround: Ensure that you have a mobility peer member in the WLC database (show mobility summary) whose IP address is less than the WLC's own management IP address. With this, the WLC would have non-empty transmitter list and not hitting the crash.</p>
CSCup59877	<p>Symptom: AP dissociate from the WLC when available 802.11a channels are exhausted after a DFS event, on dot11radio2.</p> <p><code>%DOT11-2-NO_CHAN_AVAIL_CTRL: Interface Dot11Radio2, no channel available.</code> <code>%DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to X.X.X.X:5246</code></p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p> <p>Further Problem Description: This issue is specific to DFS event on Dot11Radio2. This should not happen for DFS events on Dot11Radio1 as that has already been fixed.</p>
CSCup16770	<p>Symptom: WLC stops working while running PMIPv6 debugging commands.</p> <p>Conditions: Failure analysis of “Software was stopped by the reaper for the following reason: Reaper Reset: Task “emWeb” missed software watchdog”</p> <p>Workaround: Avoid disabling PMIPv6 debug commands.</p>
CSCuj73249	<p>Symptom: The AP's non-default credential is being shown as not-configured at WLC.</p> <p>Conditions: AP with specific credentials that moved to a WLC without credentials configured.</p> <p>Workaround: Fix is to do proper check at the WLC side.</p>

Table 8 **Open Caveats (continued)**

ID	Description
CSCu177390	<p>Symptom: On both 7.6 and 7.5 releases, VTH IE elements are sent when WMM is disabled on the WLAN.</p> <p>802.11n is correctly suppressed, but 802.11ac is still sent over the air.</p> <p>On Release 7.5, the IE elements contain 802.11n as well; on Release 7.6, only 802.11ac is present.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • WLAN with WMM disabled • RM3000AC module installed in a Cisco 3600 Series AP. <p>Workaround: Enable WMM.</p> <p>Further Problem Description: This bug fixes the problem with the RM3000AC module. For a similar bug on the Cisco 3700 Series AP, see CSCum68676.</p>
CSCum06146	<p>Symptom: Client is associated with a VLAN from the global WLAN interface group rather than the interface group assigned to the SSID in the AP group.</p> <p>Conditions: When an interface group is assigned to the WLAN globally and another interface group is assigned to the AP group WLAN.</p> <p>Workaround: None.</p>
CSCum17998	<p>Symptom: System stopped working when changing management IP address.</p> <p>Conditions: Cisco Flex 7500 Series and 8500 Series WLCs.</p> <p>Workaround: Clear the WLC configuration and change the management address.</p>
CSCum92822	<p>Symptom: AID leaks observed on Release 7.6; problem is not seen if AP is on Release 7.4.121.0.</p> <p>*apfMsConnTask_4: Jan 16 10:26:23.419: #LWAPP-3-INVALID_AID2: spam_api.c:1462 Association identifier 249 for client 60:6c:66:09:XX:XX is already in use by 50:32:75:2c:XX:XX</p> <p>*spamApTask6: Jan 16 10:25:39.315: 60:6c:66:09:XX:XX Association Failed on REAP AP BSSID 1c:aa:07:6f:XX:XX(slot 0), status 17 0 Max Client Reached, recieved an AID=0</p> <p>End users report connection errors after a while.</p> <p>Conditions: AP in FlexConnect mode, local switching.</p> <p>Workaround: None.</p>

Table 8 **Open Caveats (continued)**

ID	Description
CSCun34295	<p>Symptom: After upgrade to BU esc image, a new crash was seen where task radiustransportthread failed.</p> <pre>Software Failed on instruction at : pc = 0x112e5b14 (makeOctetStringVarbind_real 688), ra = 0x112f1b18 (makeOctetStringVarbind_real 688) Software Failed while accessing the data located at :0xf8638 clients failed authentication after recovery from the crash</pre> <p>Conditions: Software code = 7.4.121.5</p> <p>Workaround: To resolve the client connectivity/authentication problem, increase the RADIUS timeout. None for the crash.</p> <p>Further Problem Description: Very low frequency issue (seen only twice).</p>
CSCun48116	<p>Symptom: Client traffic is blocked when local split ACL is applied on AP. Also, this message is displayed on the AP console, when encountering this issue:</p> <pre>"IP address conflicts with gateway ip address in static routing table"</pre> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>

Table 8 *Open Caveats (continued)*

ID	Description
CSCud70102	<p>Symptom: Intermittently, (once every several seconds), for a period of 70 to 80 milliseconds, an access point radio may fail to acknowledge any packets that are transmitted to it at this time.</p> <p>These periods correspond to the AP going off-channel for an RRM scan. The AP's RRM off-channel events can be seen with the following debugs:</p> <ul style="list-style-type: none"> • 7.4 and later releases: debug dot11 dot11Radio<n> trace print offc • Releases prior to 7.4: debug dot11 dot11Radio<n> trace print drvpsp <p>As a result, clients transmitting data to the AP will, during these brief, intermittent intervals, experience higher than usual latency or dropped packets.</p> <p>Conditions: Normal operation.</p> <p>Workaround: If this is an operational problem for the given clients in the given WLAN, configure the “channel-scan defer-priority” as needed. For example:</p> <pre>(Cisco Controller) >config wlan channel-scan defer-priority 0 enable 2 (Cisco Controller) >config wlan channel-scan defer-priority 1 enable 2 (Cisco Controller) >config wlan channel-scan defer-priority 2 enable 2 (Cisco Controller) >config wlan channel-scan defer-priority 3 enable 2 (Cisco Controller) >config wlan channel-scan defer-priority 4 enable 2 (Cisco Controller) >config wlan channel-scan defer-priority 5 enable 2 (Cisco Controller) >config wlan channel-scan defer-priority 6 enable 2 (Cisco Controller) >config wlan channel-scan defer-priority 7 enable 2 (Cisco Controller) >config wlan channel-scan defer-time 60000 2</pre> <p>This will make it such that, if there any traffic of any User Priority (0..7) in the preceding 60 seconds (60,000 milliseconds), in WLAN 2, the AP will skip going off-channel.</p> <p>Additionally, the interval at which RRM goes off-channel to scan can be increased—this is the “Channel Scan Interval.”</p> <p>Additional Information: It is normal for a lightweight access point to go off-channel to perform RRM scanning, for a period of 60 milliseconds, once every few seconds. During this period, the AP does not respond in any way to packets sent to it. This off-channel behavior does very slightly reduce client transmission performance (on the order of 1 percent.)</p> <p>This issue is fixed because the RRM off-channel duration was observed to be greater than the specified 60-millisecond period (70-millisecond or 80-millisecond). This issue is addressed by reducing the period that the AP monitors the off-channel, from 50 milliseconds to 40 milliseconds.</p>
CSCuo60416	<p>Symptom: Noise/interference information not showing for channels</p> <p>Conditions: FlexConnect mode with WSSI module.</p> <p>Workaround: None.</p>
CSCui57047	<p>Symptom: WLC stopped working.</p> <p>Conditions: While running automated regression testing for SXP feature.</p> <p>Workaround: None.</p>

Table 8 **Open Caveats (continued)**

ID	Description
CSCuo96366	<p>Symptom: Customer noticed that wireless clients sometimes are unable to connect to Dot1x SSID. And once the WLC is rebooted, this issue is resolved. But, after a couple of days, the issue recurs.</p> <p>Conditions: Dot1x SSID on Release 7.6.</p> <p>Workaround: Reboot the WLC.</p>
CSCup46302	<p>Symptom: vWLC: RSSI missing from Monitor mode AP.</p> <p>Conditions: vWLC cannot get the client RSSI information from Monitor mode AP. Back to work after changing AP to FlexConnect mode.</p> <p>Workaround: None.</p>
CSCup46986	<p>Symptom: Both clients have connectivity issue when duplicate IP occurs. Clients will not redo DHCP process until disassociation/roaming.</p> <p>Conditions: Two clients have the same IP address assigned by DHCP server.</p> <p>Workaround: Client may need to redo DHCP process.</p>
CSCuq00971	<p>Symptom: 7925 phones dropping from FlexConnect Local Switching APs every few seconds.</p> <p>WLC Debugs show:</p> <pre>*apfReceiveTask: Jun 27 02:42:06.878: 00:1b:d4:58:99:1c Freeing prev AID 9 on AP 34:db:fd:c3:0a:c0 slot 0 *apfReceiveTask: Jun 27 02:42:06.878: 00:1b:d4:58:99:1c apfHreapClientCreate (apf_80211.c:12306) Changing state for mobile 00:1b:d4:58:99:1c on AP 34:db:fd:c3:0a:c0 from Associated to Associated *apfReceiveTask: Jun 27 02:42:06.878: 00:1b:d4:58:99:1c 10.2.30.92 RUN (20) Change state to RUN (20) last state RUN (20)</pre> <p>AP debugs shows:</p> <pre>*Jul 16 08:10:24.039: A48B8A1C-0 Off Channel interrupt 1 0 0 0 *Jul 16 08:10:28.947: A4D72A74-0 31A84F - pak flags 0 *Jul 16 08:10:28.959: A4D75CF1-0 31A84F - pak flags 0 *Jul 16 08:10:28.959: A4D75FF2-0 31A84F - pak flags 0 *Jul 16 08:10:28.959: A4D762F9-0 31A84F - pak flags 0 *Jul 16 08:10:29.051: A4D8CE29-0 31A84F - pak flags 0 *Jul 16 08:10:29.055: A4D8D3D2-0 31A84F - pak flags 0 *Jul 16 08:10:29.055: A4D8D97A-0 31A84F - pak flags 0 *Jul 16 08:10:29.087: 31A84F - restart B0 300 *Jul 16 08:10:29.087: capwap_ap_mgmt: delete central info of mn 001d.a231.a84f</pre> <p>Conditions:</p> <ul style="list-style-type: none"> • Release 7.6.120.0, FlexConnect Local Switching • WLAN is configured for WPA2-PSK <p>Issue not seen on laptops</p> <p>Workaround: None.</p>

Table 8 **Open Caveats (continued)**

ID	Description
CSCuq11792	<p>Symptom: WLC 5508 experienced two crashes with message “pmalloc detected memory corruption.” Corrupted memory shows all zeros.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>
CSCuq14453	<p>Symptom: Memory leak on WLC when using PMIPv6 clients.</p> <p>Conditions:</p> <ul style="list-style-type: none"> • 8510 WLC with 500 APs, 7000 clients • OPEN SSID, PMIPv6 clients • Client join/disconnect on a scaled setup <p>Workaround: Reboot WLC when memory goes high.</p>
CSCuq33496	<p>Symptom: Interim accounting packets sporadically send huge amounts of data that are impossible for the interval of time that has elapsed.</p> <p>Conditions: Seen most often during times of high utilization.</p> <p>Workaround: None.</p>
CSCuq33765	<p>Symptom: Clients on FlexConnect SSID with tagged VLAN not getting IP.</p> <p>Conditions: 1600 AP with FlexConnect local switching.</p> <p>Workaround: Use Local mode.</p>
CSCul40203	<p>Symptom: Interface does not get marked as dirty because of dual stack clients.</p> <p>Conditions: VLAN pooling feature does not take care (marking interface dirty) of IPv6 clients. More than 3 clients do not get IPv4, but still moving to run state because it gets IPv6 address.</p> <p>Workaround: None.</p>
CSCuo05142	<p>Symptom: When EAP-AKA is used along with realm, fast re-authentication can only be supported when EAP server responds with AT_NEXT_REAUTH_ID attribute having both the username portion and realm portion.</p> <p>The purpose of the realm is received, WLC can pick up the right server for the subsequent fast re-authentication requests.</p> <p>For example, host APD server which supports EAP-AKA does not support realm portion. Therefore, Cisco WLC supports fast re-authentication only with those EAP servers that have this compatibility.</p> <p>This is as per the behavior described in RFC 4185.</p> <p>Conditions: Unknown.</p> <p>Workaround: None.</p>

Resolved Caveats

Table 9 lists the caveats that have been resolved in Release 7.6.130.0.

Table 9 *Resolved Caveats*

ID	Description
CSCun26383	Memory corruption crashes in cac_parent_timer by rrm neigh tbl overwrite
CSCum26370	Static TX power level changes to Max after AP reboot
CSCuq36902	Memory Leak with Internal webauth in a loop for longer period
CSCuq16408	WISM2 multiple crashes on 7.6MR3 - Bonjour_Msg_Task
CSCuq18025	High CPU 99% on webauth Redirect Task 7.6.122.9
CSCuo69145	2504- Display new Dashboard after user login
CSCuo60383	AP3602 trying to contain its own RM3000AC module
CSCuo44048	AP3602 AP crashes in proc IPAM Manager
CSCup87612	Memory corruption on OpenSSL 7.6.122.7
CSCuq08015	WLC crash: spamGetRadGroupName
CSCul31732	FlexConnect VLAN mode was changed to Disabled after power cycle
CSCup55226	Apple client cannot authenticate on 1130 1240 running 7.6 code with FT
CSCup42789	AP3602 with RM3000AC module not able to pass traffic
CSCup60494	Gradual memory leak in 2048 byte chunks
CSCup40557	HIGH CPU (98%) on webauthRedirect
CSCup44648	PMIPv6: Add sshpm Rules for PMIPv6 Control only when MAG enabled
CSCuo69578	AP1532E/I bridge throughput is very low on 802.11n
CSCun15192	Radio Reset: (SC2) sensor crash due to dot11 driver off-channel timeout
CSCui90116	AP sends FT-auth original and retry packet to WLC causing MIC mismatch
CSCuo71809	CleanAir: Stale Bluetooth Device Entries in down state in AP with WSSI
CSCul42704	wIPS-Rogue APs are mistaken as infrastructure devices
CSCul16911	CAPWAP causing APs to disassociate due to DTLS errors
CSCuo74061	AP1600 intermittent low throughput (<1-2mpbs)
CSCum66202	FlexConnect: per-user ACL + WebAuth success/logout page not displayed
CSCuo97883	AP3700 AP 5ghz clients stop forwarding traffic under load with TKIP
CSCuo84219	Wi-Fi: AP1600 drops packets when a burst of A-MSDU data is received
CSCul04090	Reaper Reset: Task "SNMPTask" missed software watchdog
CSCul38572	CCKM roaming failing between a 7.0 WLC and a 7.4.
CSCul98577	Wired Guest can leak traffic out WLC Management Interface
CSCum86401	LAP in UNKNOWN_STATE on WLC
CSCun22507	transfer run-config lacks WLAN and L2ACL configuration information
CSCun38541	Conditional web redirect not working
CSCun69089	Vocera Badges Broadcast stops working randomly

Table 9 *Resolved Caveats (continued)*

ID	Description
CSCuo23909	FlexConnect Efficient Upgrade702W subordinate AP showing as invalid AP model
CSCuo63046	WLC crashes on task spamApTask6
CSCul78198	RAID Volume Status should show proper error codes instead of unknown.
CSCun48405	AP sent Death to wlan client after channel change by RRM DCA
CSCsz82878	4.2 Mesh controller crashing with Task Name: reaperWatcher
CSCui16915	Cisco IOS XE Release IRCM: Guest tunneling broken with Cisco 5760 WLC as GC and Cisco 5508 WLC as MC
CSCui37300	mDNS: WLC uses 0.0.0.0 as source IP for query/resp when use native VLAN
CSCui38822	OC: GUI won't allow change of HA 2ndary controller to primary controller
CSCui56456	RNG in Web Management Cookie is not cryptographically secure
CSCui94634	FlexConnect AP dissociates after ACL push CAPWAP processing hangs DTLS timeout
CSCui95938	Fast Switching SSDi and IPAD Issue
CSCuj04921	802.11ac: S4 Linksys 3x3 and Macbook Air clients not reach m8/m9 data rates
CSCuj05274	WLC Crash - Reaper Reset: Task ""loggerMainTask"" missed software watchdog
CSCuj61455	FlexConnect Clients are being Deauthenticated for an Unknown Reason
CSCul03672	Commands of backup-controller are lost after restoration on 7.5.102.0
CSCul15555	FlexConnect AP decrypt errors after CCKM roam phone stuck in DHCP req
CSCul91975	WGB may disconnect permanently after max retry of 802.11 probe
CSCum00101	AP 2600/3600 data tunnel stuck with DTLS encryption enable
CSCum15629	AP1140 in FlexConnect mode crash on 7.4.110.0 due to auth timer in loop
CSCum53429	AP1130 FlexConnect VLAN mapping corrupted after VLAN mapping change
CSCum63497	vWLC 7.6 Service port on distributed switch breaks communication
CSCum67742	RADIUS HTTP Profiling not working in latest Release 8.0 build
CSCum71699	FlexConnect AP BVI down on VLAN mapping push
CSCum87504	MFP Anomaly Detected messages continuously displayed
CSCun11124	vWLC serial number changes when using DRS or Vmotion
CSCun23679	WLC: protocol pack 6.3+ will not DP crash file
CSCun34605	RADIUS profiling failing for Windows XP and 7
CSCun52751	AP802 as MAP not falling back from invalid static IP
CSCun62368	RADIUS NAC Client auth issues for 7.6
CSCun66868	WLC crash at snmpApCurrChanChangedTrapSend
CSCun85954	Release 7.6: 5508 HA crash with Task Name: rsyncmgrXferMain
CSCuo18300	WLC: DNS based ACL feature is case sensitive and should not be
CSCuo20803	ACL rule direction is changed from any to out during backup
CSCuo35247	LAP unable to setup DTLS with WLC if packets arrive out of order
CSCuo37056	Rogue client and ad hoc rogue client containment failure in 7.6

Table 9 **Resolved Caveats (continued)**

ID	Description
CSCuo39416	AP1131/AP1242 not forwarding CWA redirects on 7.6
CSCuo62930	Unable to map ACL to wlan through GUI
CSCuo63103	Client local switching to central mode load aaa override RADIUS NAC
CSCuo68049	Not able to set client RSSI shows positive value
CSCuo71252	Express Setup WizardCountry and Timezone set to US regardless of config
CSCuo73572	Unable to add 8510/7510 Controller to Prime Infrastructure 2.1
CSCuo86478	WLC Set Wrong DHCP Relay Agent for Layer-2 Roaming
CSCuo86819	WLC crashes in 7.6.120.0 - memory corruption caused by Webauth
CSCup03264	Anchor WLC not appending client parameters for external webauth redirect
CSCup18354	Japanese DBCS characters is garbled in internal Webauth login.html page
CSCup22587	Multiple Vulnerabilities in OpenSSL - June 2014
CSCuj10329	FlexConnect AP crash in dot1q_vlan_exists() after IP addr change
CSCuj62550	Traceback observed when adding flex-ap to flex-group
CSCup24962	AP2700 crashed during scale MC2UC longevity
CSCuo44310	AP 3600 loses country code on reboot joins Disabled
CSCup59660	SYS-3-CPUHOG related traceback in 3600 AP
CSCup22590	Multiple Vulnerabilities in IOS/IOSd OpenSSL
CSCuo33271	WiSM2 crashed with DP watchdog on image 8.0.72.164
CSCum71927	AP1530: Handle all NF timeouts during hal reset
CSCui57980	WLC crash at task name 'aaaQueueReader' on Release 7.4.110.0
CSCuo21355	AP shows logs with 'Bad refcount in datagram_done' traceback
CSCup14580	Cisco 8500 WLC stopped working and the envMonitorStatus task missed software watchdog
CSCup75604	Cisco 5500 WLC/Cisco WiSM2 stopped working with task name "spamApTask1"

Installation Notes

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










Warnings



Warning

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

Statement 1071

-  **Warning** **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030
-  **Warning** **Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.: NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54).** Statement 280
-  **Warning** **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).** Statement 13
-  **Warning** **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground connector. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024
-  **Warning** **Read the installation instructions before you connect the system to its power source.** Statement 10
-  **Warning** **Do not work on the system or connect or disconnect any cables (Ethernet, cable, or power) during periods of lightning activity. The possibility of serious physical injury exists if lightning should strike and travel through those cables. In addition, the equipment could be damaged by the higher levels of static electricity present in the atmosphere.** Statement 276
-  **Warning** **Do not operate the unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 364
-  **Warning** **In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft. (2 m) from your body or nearby persons.** Statement 339
-  **Warning** **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

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

Installation Instructions

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

**Note**

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

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

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

Service and Support

Troubleshooting

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

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

Related Documentation

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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.

© 2015 Cisco Systems, Inc. All rights reserved.

