Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.6.120.0

First Published: May 2, 2014

Last Updated: July 16, 2014

OL-30342-03

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:

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 7.6.120.0, 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

This section provides a brief description of what is new in Release 7.6.120.0:

- Support for new access points:
  - Cisco Aironet 2700 Series Access Points. For more information see, http://www.cisco.com/c/en/us/products/wireless/aironet-2700-series-access-point/index.html.
  - Cisco Aironet 700W Series Access Point. For more information see, http://www.cisco.com/c/en/us/products/wireless/aironet-700w-series/index.html.

    Initially, the Ethernet ports of the 700W Series access points are disabled.

    Use the **config ap lan** <*port_id*> <*enable/disable*> <*AP_name*> command to enable the Ethernet ports.

    Use the **show ap lan** <*port_id*> <*AP_name*> and **show ap lan port-summary** <*AP_name*> commands to view the port details of the access point.
- Cisco WLAN Express Setup for Cisco 2500 Series Wireless Controller

Cisco WLAN Express Setup for Cisco 2500 Series Wireless Controller

7.6.120.0 introduces Cisco WLAN Express Setup on Cisco 2500 Series Wireless Controller. It includes easy to use GUI Configuration Wizard, an intuitive monitoring dashboard and several Cisco Wireless LAN best practices enabled by default.

Important Notes

- If you use the CLI configuration wizard or AutoInstall, Cisco WLAN Express Setup will be bypassed and associated features will not be enabled.
- If you upgrade to 7.6.120.0 and do not perform a new configuration of the controller using the GUI Configuration Wizard, Cisco WLAN Express Setup will not be enabled. You must use the GUI Configuration Wizard to enable Cisco WLAN Express Setup features.
- After you upgrade to 7.6.120.0, you can clear the controller configuration and then use the GUI Configuration Wizard to enable Cisco WLAN Express Setup features.
- If you downgrade from 7.6.120.0 to an older release, Cisco WLAN Express Setup features will be disabled. However, the configurations generated through Cisco WLAN Express Setup will not be removed.

Setting up Cisco 2500 Series Wireless Controller Using Cisco WLAN Express Setup

1. Connect and power on the controller.
2. Connect a computer to port 2 of the controller using an Ethernet cable. The controller uses auto-sense. You can use a straight-through Ethernet cable.

   Note AutoInstall starts on port 1. If port 1 is connected to network and if AutoInstall gets a configuration file from the TFTP server, it interrupts the configuration process and disables the GUI Configuration Wizard on port 2.

   a. The port LED will be green if both the machines are properly connected.

   b. The controller might take some time to be fully powered on and the GUI to be available on the computer. The LEDs on the front panel of the controller indicate the system status:

   – The controller is not ready if the LEDs are blinking or are amber in color.

   – The controller is ready if the SYS LED is green and ALM LED is off.

   – When you connect the computer to port 2, the machine gets an IP address 192.168.1.x (100 and above).
3. Open a client web browser at http://192.168.1.1 from the computer connected to port 2 to access the controller GUI configuration.

   Turn off the computer's other network connections (for examples, WiFi) if there is an IP conflict.
4. Create an admin account.
5. Click **Start**.
6. In Step 1—You setup your controller and configure the parameters.
7. In Step 2—You create your wireless network.

   By default, you must create your Employee network.

  - Security Method—The default security method is WPA2 Personal. If you choose WPA2 Personal, you must configure the passphrase. If you choose WPA2 Enterprise, you must configure the RADIUS IP address and shared secret.

  Guest network is optional.

  - Security Method—The default security method is Web Consent. Choose **Web Consent** if you do not want any preconfigured password. A guest user has to acknowledge an Accept Use Policy (AUP) policy. Select **WPA Personal** if you want guest users to be authenticated using a password to gain access to the guest network.

8. Verify the configured parameters and click **Apply** and **OK**. The controller reboots.
9. Disconnect the computer from port 2 of the controller.
10. Connect port 1 of the controller to the network switch trunk port.
11. Connect access points to the network switch.
12. Access points will join the controller and the configured wireless network is available.
13. Connect wireless clients to the wireless network.
14. Connect the computer to the network and access the controller GUI.
15. After you login, you can view the new dashboard. For more details, see New Dashboard of Cisco 2500 Series Wireless Controller Using Cisco WLAN Express Setup. Click **Advanced** to view the legacy Monitor Summary page. From the Monitor Summary page, click the **Home** icon to view the new dashboard.

New Dashboard of Cisco 2500 Series Wireless Controller Using Cisco WLAN Express Setup

The new dashboard of the Cisco 2500 Series Wireless Controller with Cisco WLAN Express Setup provides a summary of the configured wireless networks, access points, active client devices, rogues, and interferers. You can also view details of top access points, applications, operating systems, and clients as a table or as a pie chart.

When you click the elements that appear on top of the dashboard, you can view the details in the corresponding pages:

Element	Description	Corresponding Page
Wireless Networks	Displays the number of WLANs that are enabled and disabled.	WLANs and opens the WLANs page.
Access Points	Displays the number of access points that are in UP and REG states.	Wireless > Access Points > All APs
Active Client Devices	Displays the number of active client devices in the 2.4-GHz and 5-GHz bands.	Monitor > Clients

Element	Description	Corresponding Page
Rogues	Displays the number of rogue access points and rogue clients.	• Monitor > Rogues > Unclassified APs • Monitor > Rogues > Rogue Clients
Interferers	Displays the number of non-WiFi interferers in the 2.4-GHz and 5-GHz bands.	• Monitor > Cisco CleanAir > 802.11a/n/ac Cisco APs > Interference Devices • Monitor > Cisco CleanAir > 802.11b/g/n Cisco APs > Interference Devices

Click the Dashboard Settings icon on the top right corner of the GUI to configure the dashboard options. You can change the data format to rate or volume.

- If you choose volume, the cumulative data appears for Top Applications, Top Access Points, and Top Client Devices portlets.
- If you choose rate, the last 90 seconds data appears for the Top Applications, Top Access Points, and Top Client Devices portlets.
- There is no impact on the Top Operating Systems when you switch the data format between rate and volume.

You can also choose the default landing page of the controller GUI in the options page as the new dashboard or the legacy Monitor Summary page by changing the Landing Page option.

Default Configurations of Cisco 2500 Series Wireless Controller Using Cisco WLAN Express Setup

When you configure your Cisco 2500 Series Controller using the Cisco WLAN Express Setup, the following parameters are enabled or disabled. These settings are different from the default settings obtained when you configure the controller using the CLI wizard, and different from the default settings on other controller platforms.

Parameters in New Interface	Value
Aironet IE	Disabled
DHCP Address Assignment (Guest SSID)	Enabled
Client Band Select	Enabled
Local HTTP and DHCP Profiling	Enabled
Guest ACL	Applied **Note** Guest ACL denies traffic to the management subnet.
CleanAir	Enabled
EDRRM	Enabled
EDRRM Sensitivity Threshold	• Low sensitivity for 2.4 GHz • Medium sensitivity for 5 GHz
Channel Bonding (5 GHz)	Enabled
DCA Channel Width	40 MHz

Parameters in New Interface	Value
mDNS Global Snooping	Enabled
Default mDNS profile	Two new services added: • Better printer support • HTTP
AVC (only AV)	Enabled only with following prerequisites: • Bootloader version—1.0.18 Or • Field Upgradable Software version—1.8.0.0 and above **Note** If you upgrade the bootloader after you have setup the Cisco 2500 Series Controller using the GUI Wizard, you have to manually enable AVC on the previously created WLAN.
Management	• Via Wireless Clients—Enabled • HTTP/HTTPS Access—Enabled • WebAuth Secure Web—Enabled
Virtual IP Address	192.0.2.1
Multicast Address	Not configured
Mobility Domain Name	Name of employee SSID
RF Group Name	Default

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	—

Table 1 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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	—
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	—

Table 1 Software Support for Access Points (continued)

Access Points		First Support	Last Support
2700 Series	AIR-CAP2702I-x-K9	7.6.120.0	—
	AIR-CAP2702E- x-K9	7.6.120.0	—
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 11
- Software Release Recommendations, page 12
- Solution Compatibility Matrix, page 12

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 7.6.120.0

Guidelines and Limitations

- When you are upgrading from a release that is prior to Release 7.6.X, Cisco lightweight access point (LAP) is unable to set up DTLS with Cisco WLC when LAP tries to join Cisco WLC using ap3g1-k9w8-tar.152-4.JB4.tar image. The workaround is as follows:
  1. Downgrade the Cisco WLC to 7.4.121.0.

     LAP would still not join the Cisco WLC as it is running the 7.6 image in it, which it once downloaded.
  2. Delete the 7.6 image from LAP CLI, so it boots from the rcvk image.

Booting from the rcvk image lets it form DTLS with out-of-order packet situation.

The rcvk image should not be 7.6 image. If it fails on rcvk image too, then probably we have 7.6 based rcvk image in it.

3. Download the 7.4 rcvk image in the AP, via archive download-sw /force /overwrite commands.

   LAP downloads the 7.4 code and boots using it. Using 7.4 code on both the ends, will get the DTLS session up, with out-of-order packets.

   Key point is to not use 7.6 image at either ends, LAP or WLC.

   Further Problem Description: LAP with MTU 1400 is unable to set up DTLS with Cisco WLC. The cert present by the AP, arrive on the Cisco WLC properly fragmented but out of order. According to Cisco WLC debug dtls, it fails with the following "debug dtls all enable" logs on Cisco WLC:

```
*spamApTask4: Apr 17 16:54:15.551: b0:c6:9a:c5:74:01 record=Handshake epoch=1
seq=0
*spamApTask4: Apr 17 16:54:15.551: b0:c6:9a:c5:74:01 msg=Unknown or Encrypted
*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback: SSL state = 0x2181;
where = 0x2002; ret = 0x0
*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback:
ret_type_string=unknown
*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback:
ret_desc_string=close notify
*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback:
SSL_state_string=SSLv3 read client certificate B
*spamApTask4: Apr 17 16:54:15.551: b0:c6:9a:c5:74:01 SSL_do_handshake:
SSL_ERROR_SYSCALL while communicating with 164.154.94.8 : (null)
```

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

  The workaround is as follows:

  a. Enter the following commands:

```
config boot backup
show boot

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

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

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

```
config boot primary
```

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

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

- If you 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 7.6.120.0, 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 7.6.120.0.
- 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 7.6.120.0 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 7.6.120.0. Table 5 shows the upgrade path that you must follow before downloading Release 7.6.120.0.

Table 5 Upgrade Path to Cisco WLC Software Release 7.6.120.0

Current Software Release	Upgrade Path to 7.6.120.0 Software
7.0.x releases	You can upgrade directly to 7.6.120.0. **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 7.6.120.0 to avoid losing those VLAN settings.
7.1.91.0	You can upgrade directly to 7.6.120.0.
7.2.x releases	You can upgrade directly to 7.6.120.0. **Note** If you have an 802.11u HotSpot configuration on the WLANs, we recommend that you first upgrade to the 7.3.101.0 Cisco WLC software release and then upgrade to the 7.6.120.0 Cisco WLC software release. You must downgrade from the 7.6.120.0 Cisco WLC software release to a 7.2.x Cisco WLC software release if you have an 802.11u HotSpot configuration on the WLANs that is not supported.
7.3.x releases	You can upgrade directly to 7.6.120.0.
7.4.x releases	You can upgrade directly to 7.6.120.0.
7.5.x releases	You can upgrade directly to 7.6.120.0.
7.6.100.0	You can upgrade directly to 7.6.120.0.

- 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 7.6.120.0.
- 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 7.6.120.0. 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 7.6.120.0 Cisco WLC software and your TFTP server does not support files of this size, the following error message appears:

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

  Bootloader menu for Cisco 5500 Series WLC:

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

  Bootloader menu for other Cisco WLC platforms:

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

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

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

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

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

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

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

  Here:

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

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

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

Note Predownloading Release 7.6.120.0 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 7.6.120.0 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 7.6.120.0 (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 7.6.120.0 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 7.6.120.0 Cisco WLC software is installed on your Cisco WLC, click **Monitor** on the Cisco WLC GUI and view the Software Version field under Controller Summary.

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

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

Important Note for Customers in Russia

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

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

Downloading and Installing a DTLS License for an LDPE Cisco WLC

Step 1 Download the Cisco DTLS license.

a. Go to the Cisco Software Center at this URL:

   https://tools.cisco.com/SWIFT/LicensingUI/Home

b. On the Product License Registration page, choose **Get New > IPS, Crypto, Other Licenses**.

c. Under **Wireless**, choose **Cisco Wireless Controllers (2500/5500/7500/8500/WiSM2) DTLS License**.

d. Complete the remaining steps to generate the license file. The license file information will be sent to you in an e-mail.

Step 2 Copy the license file to your TFTP server.

Step 3 Install the DTLS license. You can install the license either by using the Cisco WLC web GUI interface or the CLI:

- To install the license using the web GUI, choose:

  Management > **Software Activation** > **Commands** > **Action**: **Install License**

- To install the license using the CLI, enter this command:

  license install tftp:*//ipaddress /path /extracted-file*

After the installation of the DTLS license, reboot the system. Ensure that the DTLS license that is installed is active.

Upgrading from an LDPE to a Non-LDPE Cisco WLC

Step 1 Download the non-LDPE software release:

a. Go to the Cisco Software Center at this URL:

   http://www.cisco.com/cisco/software/navigator.html?mdfid=282585015&i=rm

b. Choose the Cisco WLC model.

c. Click **Wireless LAN Controller Software**.

d. In the left navigation pane, click the software release number for which you want to install the non-LDPE software.

e. Choose the non-LDPE software release: AIR-X-K9-X-X.X.aes

f. Click **Download**.

g. Read the Cisco End User Software License Agreement and then click **Agree**.

h. Save the file to your hard drive.

Step 2 Copy the Cisco WLC software file (*filename*.aes) to the default directory on your TFTP server or FTP server.

Step 3 Upgrade the Cisco WLC with this version by performing Step 3 through Step 20 detailed in the "Upgrading to Cisco WLC Software Release 7.6.120.0" section on page 12.

Interoperability With Other Clients in Release 7.6.120.0

This section describes the interoperability of Release 7.6.120.0 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	7.6.120.0
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)

Table 6 Test Bed Configuration for Interoperability

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

Table 7 Client Types (continued)

Client Type and Name	Version
Intermec CK70	Windows Mobile 6.5 / 2.01.06.0355
Intermec CN50	Windows Mobile 6.1 / 2.01.06.0333
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R
Phones and Printers	
Cisco 7921G	1.4.2.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 7.6.120.0. 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 7.6.120.0 Cisco WLC software release.

Table 8 Open Caveats

ID	Description

CSCuo35247	**Symptom**: Cisco lightweight access point (LAP) is unable to set up DTLS with Cisco WLC.
	Conditions: LAP trying to join Cisco WLC using ap3g1-k9w8-tar.152-4.JB4.tar image.
	Workaround:
	1. Downgrade the Cisco WLC to 7.4.121.0.
	LAP would still not join the Cisco WLC as it is running the 7.6 image in it, which it once downloaded.
	2. Delete the 7.6 image from LAP CLI, so it boots from the rcvk image.
	Booting from the rcvk image lets it form DTLS with out-of-order packet situation.
	The rcvk image should not be 7.6 image. If it fails on rcvk image too, then probably we have 7.6 based rcvk image in it.
	3. Download the 7.4 rcvk image in the AP, via archive download-sw /force /overwrite commands.
	LAP downloads the 7.4 code and boots using it. Using 7.4 code on both the ends, will get the DTLS session up, with out-of-order packets.
	Key point is to not use 7.6 image at either ends, LAP or WLC.
	Further Problem Description: LAP with MTU 1400 is unable to set up DTLS with Cisco WLC. The cert present by the AP, arrive on the Cisco WLC properly fragmented but out of order. According to Cisco WLC debug dtls, it fails with the following “debug dtls all enable” logs on Cisco WLC:
	`*spamApTask4: Apr 17 16:54:15.551: b0:c6:9a:c5:74:01 record=Handshake epoch=1 seq=0`
	`*spamApTask4: Apr 17 16:54:15.551: b0:c6:9a:c5:74:01   msg=Unknown or Encrypted`
	`*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback: SSL state = 0x2181; where = 0x2002; ret = 0x0`
	`*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback: ret_type_string=unknown`
	`*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback: ret_desc_string=close notify`
	`*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback: SSL_state_string=SSLv3 read client certificate B`
	`*spamApTask4: Apr 17 16:54:15.551: b0:c6:9a:c5:74:01 SSL_do_handshake: SSL_ERROR_SYSCALL while communicating with 164.154.94.8 : (null)`

CSCuc78713	**Symptom**: Wireless clients cannot receive broadcast packets after broadcast key rotation. **Conditions**: Dynamic WEP; Release 7.0.235.0, 7.2.110.0, and 7.3.101.0. **Workaround**: Enter the **config advanced eap bcast-key-interval 86400** command in the middle of the night and then change security setting to WPA2.
CSCud57046	**Symptom**: Client entry is seen on multiple Cisco WLCs even when it is not anchored to a Cisco WLC or part of its mobility group. **Conditions**: Unknown. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description

CSCuf77488	**Symptom**: The FT and LT detection time for an alarm is ahead or later than the AP clock. This causes a delay in Cisco NCS to detect the alarm.
	`LCAVIAX014-2AD1#show capwap am alarm 54`
	`capwap_am_show_alarm = 54`
	
	`<A id='139266813'>`
	`<AT>54</AT>`
	`<FT>2013/03/12 23:37:44</FT>`
	`<LT>2013/03/12 23:38:07</LT>`
	`<DT>2013/03/01 21:59:47</DT>`
	`<SM>D0:57:4C:08:FB:B2-g</SM> <SNT>1</SNT>`
	` <CH>1</CH>`
	` <FID>0</FID>`
	` pAlarm.bPendingUpload = 0`
	`LCAVIAX014-2AD1#`
	`LCAVIAX014-2AD1#show clock`
	`*21:59:18.983 UTC Tue Mar 12 2013`
	In Cisco NCS, the alarm is not seen until the actual AP time matches the time reported in the FT.
	Conditions:
	• Cisco 5500 Series WLC using Release 7.0.235.3
	• Cisco AP3500 in wIPS ELM mode
	• MSE 3350 using Release 7.0.201.204
	Workaround: None.

CSCug34802	**Symptom**: Rogue containment fails on a 5-GHz radio. **Conditions**: Rogue on 5-GHz radio. **Workaround**: None.
CSCug38888	**Symptom**: Disabled SSID is broadcast by a 2.4-GHz radio. **Conditions**: SSID was created and disabled previously. This is a very rare occurrence, and only seen once; never reproduced in the lab, **Workaround**: Reconfigure the Cisco AP.

CSCuh12796	**Symptom**: Consecutive SNMP 'set' commands for same MIB variable on Cisco WLC fails.
	Conditions: When we set a MIB object on Cisco WLC using SNMP 'set' command, it works at the first attempt. However, if you repeat the same command, the following error message is displayed:
	`Error in packet.`
	`Reason: noCreation (That table does not support row creation or that`
	`object can not ever be created)`
	Workaround: Perform SNMP 'get' before doing 'set'.

Table 8 Open Caveats (continued)

ID	Description
CSCuh16842	**Symptom**: Client gets IPv6 address from a different VLAN. **Conditions**: This is a combination of the following factors: • Interface group • Client sends traffic from either a static IP address or a previously allocated IP address. • Client traffic does not match the assigned VLAN that was initially received. The following system message is displayed when this occurs: `Overriding interface of client from 'vlan20' to 'vlan30' within interface group 'vlan20-30'` **Workaround**: Use DHCP Required.

CSCuh16870	**Symptom**: Client with static IP address loses connectivity on session timeouts.
	Conditions: This occurs only if the following conditions are met:
	Interface that the client would get from an interface group does not match the interface corresponding to the static IP address.
	Client gets VLAN overridden and the following message is displayed:
	`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`
	This overriding is lost when PMK expires, and a new authentication occurs. This occurs even if the client continuously sends traffic.
	Workaround: Either disable interface groups or enable DHCP required.

CSCuh26716	**Symptom**: The **show redundancy summary** command shows the following line regardless of its real SKU: `Unit = Secondary - HA SKU` **Conditions**: Enter the **show redundancy summary** command on the following: Secondary Cisco WLC which is converted from the primary Cisco WLC. HA-SKU Cisco WLC. **Workaround**: None.
CSCuh42398	**Symptom**: Logs show the following: `#NIM-3-CANT_DISABLE_MCAST: nim.c:4542 Cannot disable multicast state` **Conditions**: Unknown. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCuh42665	**Symptom**: Cisco WLC sends incorrect information for Rogue AP detection through traps. **Conditions**: Only with Release 7.4. **Workaround**: None.

CSCuh46442	**Symptom**: Cisco lightweight access point displays %CAPWAP-3-ERRORLOG messages when AP associates with the Cisco WLC:
	`%CAPWAP-3-ERRORLOG: Invalid event 10 & state 5 combination.`
	`%CAPWAP-3-ERRORLOG: CAPWAP SM handler: Failed to process message type 10 state 5.`
	`%CAPWAP-3-ERRORLOG: Failed to handle capwap control message from controller`
	`%CAPWAP-3-ERRORLOG: Failed to process encrypted capwap packet from 172.22.170.1`
	Conditions: AP join process.
	Workaround: Unknown.

CSCui22330	**Symptom**: This issue is to track and discuss default QoS values for L2 and L3 QoS priority markings. **Conditions**: None. **Workaround**: You can map each priority on its switch/router between Cisco WLC and AP. In Release 7.5, the default value of DSCP is 18 (010 010), which is IP Precedence 2 and it belongs to Class 2.
CSCui26077	**Symptom**: FT roam fails between FlexConnect APs. **Conditions**: FT client and FlexConnect APs advertising 802.11r FT PSK WLAN. **Workaround**: Use FT-802.1x or use 11i fast roam methods like OKC because normal roam occurs because FT roam fails.
CSCui75794	**Symptom**: The foreign Cisco WLC does not respond to ARP from foreign export client to a local client being on the same VLAN. **Conditions**: • Client1 associates to Cisco WLC1 (local) • Client1 does an L3 roam to Cisco WLC2 (Cisco WLC2 is foreign and Cisco WLC1 is the anchor) • Client2 associates with Cisco WLC2 (local) • Initiate traffic, that is ping from Client1 to Client2 **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCui37300	**Symptom**: Cisco WLC uses 0.0.0.0 as source IP for mDNS query or response when Cisco WLC has untagged interface. **Conditions**: WLAN attached with untagged interface; mDNS client associated with this WLAN client request for service using mDNS; when Cisco WLC responds, it uses 0.0.0.0 as source IP address so the service provider might or might not be seen on the client device. **Workaround**: Use VLAN interfaces on mDNS WLAN.
CSCui90116	**Symptom**: 802.11r roaming failure. **Conditions**: Client sends retry packet for FT-AUTH request. Original packet and then following a retry, packet with same SN. **Workaround**: Use a non-802.11r SSID/clients. **Further Problem Description**: AP does not detect the second retry packet as a duplicate packet and forwards both packets to Cisco WLC. Therefore, there are two FT-Auth responses with different Announce numbers and (FT-AUTH responses from Cisco WLC). Client uses the Announce received in the first FT-AUTH but Cisco WLC has the last updated Announce (which is sent for retry packet). This results in MIC failure.
CSCui94634	**Symptom**: Cisco APs in FlexConnect local switching mode with VLAN mappings dissociate from Cisco WLC when an ACL is applied to one of the VLANs. Once ACL is pushed, CAPWAP UDP processing become sluggish and retransmissions of packets from Cisco WLC result in errors with duplicate sequence number errors. Eventually, this state causes a DTLS timeout and reassociation process on the AP, which fails over and over with same issue. It appears that the issue is related to corruption of the CAPWAP private configuration because the actual content of the ACL does not matter. The issue occurs immediately at the point the ACL is pushed. **Conditions**: FlexConnect mode APs with VLAN mappings and FlexConnect ACL. **Workaround**: Do not apply ACL to the AP; use another enforcement point if required. Perform a reimage of the AP with 15.2 recovery image.
CSCui95938	**Symptom**: Apple devices such as iPad, iPhone, and iPod are unable to switch transparently from a 802.1X WLAN to a WPA-WPA2(PSK) WLAN. **Conditions**: Cisco AP1142 is used with Cisco WLC using Release 7.5.102.0; FlexConnect local switching is used; two SSIDs are created—one with 802.1X authentication and the other with WPA-PSK. Switching from the 802.1X WLAN to the PSK one does not happen smoothly **Workaround**: Use another AP (tested with AP1262 and AP3501); or use a Cisco WLC release other than 7.5.102.0.

Table 8 Open Caveats (continued)

ID	Description

CSCui99062	**Symptom**: Cisco WLC accepts the SysRq Magic key on the console. This allows even an unauthenticated user who has access to the serial console to unconditionally reboot the Cisco WLC from the SysRq menu.
	Following is the SysRq menu that pops up when you enter the magic key:
	`SysRq : HELP : loglevel0-8 reBoot Crashdump tErm Full kIll Dump showMem`
	`Nice showPc show-all-timers(Q) Sync showTasks Unmount shoW-blocked-tasks`
	Conditions:
	All released images
	SysRq magic key given from the serial console
	Workaround: Return key exits from the SysRq menu and returns to the console. Cisco WLC will still function normally while in the SysRq menu or even after exiting.

CSCuj05274	**Symptom**: Cisco WLC unresponsive. **Conditions**: Release 7.4.110.0. **Workaround**: None.
CSCuj17683	**Symptom**: 802.11r Roaming—AP might sometimes send deauthentication with reason code 7. **Conditions**: AP roam in a bad RF environment. Clients fail to hear ACK for reassociation request from AP and continues to send reassociation request and following a data packet. **Workaround**: After the deauthentication, complete roam occurs and the clients can join again. **Further Problem Description**: This issue is seen very rarely and only with Samsung I565 phones.
CSCuj28495	**Symptom**: clmgmtLicenseUsageCountRemaining task does not return the remaining AP count. **Conditions**: • Hardware: Cisco 5500 Series WLC • Software: Release 7.3.x **Workaround**: None.
CSCuj32157	**Symptom**: lb._dns-sd._udp.<domain-name> service is not supported by Cisco WLC. **Conditions**: When clients query for services of the nature mdns:lb._dns-sd._udp.<domain-name>, the Cisco WLC does not process the request because it is not listed in the master service database. Therefore, the service provider might or might not see the service provider. **Workaround**: Remove the domain name setting in the DHCP and on the clients (iPads, iPhones, and so on) from the server setting.

Table 8 Open Caveats (continued)

ID	Description
CSCuj32257	**Symptom**: AP secures CAC bandwidth for SIP phone in case of inter-Cisco WLC roaming even though the phone does not have any active SIP call. **Conditions**: SIP phone is roaming inter-Cisco WLC. Occurs only in case of a 32-byte call ID. **Workaround**: Use call ID, which is less than 32 bytes.
CSCuj36599	**Symptom**: On an 802.1X WLAN that has local switching in enabled state and where P2P blocking is in enabled state, if two clients are associated with the same AP, P2P blocking between them does not work as designed. However, for SSID with OPEN authentication, it works as expected. **Conditions**: • 802.1X WLAN with local switching enabled and P2P blocking enabled. • Release 7.4.110.0. **Workaround**: Remove VLAN override from AAA.
CSCuj45983	**Symptom**: When the Cisco WLC gets a CoA (Change of Authorization) RADIUS message, for example from ISE, the Cisco WLC sends a deauthentication to the client and move the client to DHCP_REQ state. Unless “DHCP Required” is disabled on the WLAN, this means that the client will then be disconnected unless it performs a new DHCP request. With “debug client” in effect on the Cisco WLC, the following message will be seen: `DHCP_REQD (7) DHCP Policy timeout. Number of DHCP request 0 from client` **Conditions**: Cisco WLC is using CoA from RADIUS and has DHCP Required on the WLAN. Client is one that does not reliably re-DHCP upon 802.11 deauthentication; some Windows 7 and Mac OS X systems have been seen to have this problem. **Workaround**: For a single VLAN system (same VLAN before and after CoA), disable DHCP Required. For some client types, you might be able to reconfigure them to make sure that they re-DHCP as needed. For example, on a Windows 7 system, perform the following: **1.** In the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces registry path, create a DWORD value named as ?UseNetworkHint? and set it to ?0?. **2.** Restart the DHCP client service by executing the following commands from elevated command prompt: **net stop dhcp** **net start dhcp** An alternative might be to use two VLANs, one a pre-CoA and the other a post-CoA. The DHCP leases for the pre-CoA scope might be set with very short lease durations such as 30 seconds. This should trigger a more timely DHCP lease renewal from the client so that it can regain access to the network after the CoA event.

Table 8 Open Caveats (continued)

ID	Description
CSCuj53861	**Symptom**: **config advanced statistics** command cannot be applied in Cisco WLC. **Conditions**: All Cisco WLC releases. **Workaround**: None.
CSCuj61455	**Symptom**: Clients get disconnected from FlexConnect AP. 802.11 deauthentication with Reason Code 1 (Unspecified) WLC "debug client" output shows "Sent Deauthenticate to mobile on BSSID 00:3a:98:8a:70:a0 slot 0 (caller 1x_bcastkey.c:951)". **Conditions**: Cisco Flex 7510 WLC using Release 7.4.110.0; Cisco AP 1602 in FlexConnect mode; WLAN = WPA2 AES PSK, Central Authentication, Local Switching. **Workaround**: None.
CSCuj66912	**Symptom**: SNMP get for Cisco WiSM2 reports that Cisco WiSM2 has secondary power supply. **Conditions**: Cisco WiSM2 using Release 7.0.235.3. **Workaround**: None.
CSCuj74920	**Symptom**: A client roam between two Cisco WLCs can fail intermittently making the client to be part of the VLAN originally mapped to the WLAN; for example two Cisco WLC serving clients, WLAN mapped to VLAN x, RADIUS assigned to VLAN y; intermittently, client can be put on VLAN x during roams between WLC1 to WLC2. **Conditions**: When a client roams between two Cisco WLCs. **Workaround**: None. **Further Problem Description**: Debug example: `pemReceiveTask: Oct 09 15:58:40.382: 60:fe:c5:69:ef:50 Set symmetric mobility tunnel for 60:fe:c5:69:ef:50 as in Foreign role *pemReceiveTask: Oct 09 15:58:40.382: 60:fe:c5:69:ef:50 167.73.161.198 Added NPU entry of type 1 dtlFlags 0x1 *pemReceiveTask: Oct 09 15:58:40.382: 60:fe:c5:69:ef:50 Skip Foreign / Export Foreign Client IP 167.73.161.198 plumbing in FP SCB *bcastReceiveTask: Oct 09 15:58:40.389: Sending MLD query First Time to 0C:85:25:C6:71:90 ap for mgid 15 *bcastReceiveTask: Oct 09 15:58:40.389: Entry for ap 0C:85:25:C6:71:90 MLD query packet not queued for mgid 15... Enquing the Query packet... *DHCP Socket Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50 DHCP received op BOOTREQUEST (1) (len 308 vlan 0 port 13 encap 0xec03) *DHCP Socket Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50 DHCP processing DHCP DISCOVER (1) *DHCP Socket Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50 DHCP op: BOOTREQUEST htype: Ethernet hlen: 6 hops: 0 *DHCP Socket Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50 DHCP xid: 0x75555ccb (1968528587) secs: 43 flags: 0 *DHCP Socket Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50 DHCP chaddr: 60:fe:c5:69:ef:50 *DHCP Socket Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50 DHCP ciaddr: 0.0.0.0 yiaddr: 0.0.0.0 *DHCP Socket Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50 DHCP siaddr: 0.0.0.0 giaddr: 0.0.0.0 *DHCP Socket Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50 DHCP successfully bridged packet to EoIP tunnel`

Table 8 Open Caveats (continued)

ID	Description
CSCuj78942	**Symptom**: Trunk VLAN ID is not saved for Cisco AP1240. The VLAN ID is set in the **Advanced** tab. The Cisco AP reboots, but the VLAN ID is not displayed. **Conditions**: Not applicable. **Workaround**: None. **Further Problem Description**: http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01101110.html#task_43A307F686B3487F931FA496571987CA Issue is not seen on other AP platforms such as Cisco AP3600 or AP1140.
CSCuj83637	**Symptom**: Following an HA failover, the service port on the active Cisco WLC that is configured to get its IP address through DHCP loses connectivity after the DHCP lease expires (or the DHCP renew is forced through the **config interface dhcp service-port** {**enable** | **disable**} command). In case of Cisco WiSM2, this connectivity issue might cause the Cisco WLC and Catalyst 6000 to fail to exchange WCP keep-alives. Thus, the **show wism status** command shows the active module to be not operational. **Conditions**: • Cisco WLC or Cisco WiSM2 using Release 7.4.110.x or Release 7.5.102.0 in an HA environment • The service port is configured for DHCP • The issue is seen after the following events happen in the specified order: • HA failover • Service port DHCP lease expiry **Workaround**: Configure a static IP address for the service ports on both peers and force an HA switchover. From the active Cisco WLC, enter the following commands: **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** Forcing a switchover might disconnect all the clients and any mesh APs in Release 7.4.X. Therefore, we recommend that you perform this workaround during a maintenance window.
CSCuj95892	**Symptom**: When a port in a LAG goes down and then comes back up, the Cisco WLC does not send 'interface up' message to syslog server. **Conditions**: This issue is seen when distribution ports are configured in a LAG, and syslog server is configured. **Workaround**: Look in the message logs in the Cisco WLC GUI.

Table 8 Open Caveats (continued)

ID	Description
CSCuj97293	**Symptom**: Cisco WLC stops responding when the **show local-auth certificates** commands is entered. **Conditions**: Unknown. **Workaround**: None.
CSCul03672	**Symptom**: Cisco 5500 Series WLC lost some setting after restoring the configuration file. **Conditions**: AIR-CT5508-K9 using Release 7.5.102.0. **Workaround**: None.
CSCul04029	**Symptom**: Cisco WLC unresponsive on task name 'emWeb'. **Conditions**: Cisco 5508 WLC using Release 7.3.112.0 with a mobility setup. **Workaround**: None.
CSCul04090	**Symptom**: Cisco WLC unexpectedly reboots with Reaper Reset. System Stack indicates tsmClientStatsDataLock. **Conditions**: Unknown. **Workaround**: None.
CSCul15555	**Symptom**: A CCKM client associated with a FlexConnect AP using Cisco WLC Release 7.4.110.0 (local switching/central authentication) might lose IP connectivity soon after a successful CCKM roaming while remaining associated with the AP. On Cisco WLAN phone, the symptom is often seen as a two-way voice outage, phone stuck in "requesting DHCP" state. On the AP side, a radio level debugging shows decryption errors. **Conditions**: Cisco WLC/AP using Release 7.4.110.0; FlexConnect local switching and central authentication; frequent CCKM roaming events including interband roaming. **Workaround**: The issue recovers soon after the client roams to another AP. **Further Problem Description**: This is not a persistent issue; normally, the client can then roam back to the AP without any issues.
CSCul16911	**Symptom**: Cisco APs disconnect from the Cisco WLC due to DTLS errors. **Conditions**: Cisco AP disconnects. **Workaround**: None.
CSCul25617	**Symptom**: When you try to enable AP Management on dynamic interface, the "Failed to Add MDNS profile" message is displayed. **Conditions**: Not applicable. **Workaround**: None.
CSCul31732	**Symptom**: FlexConnect VLAN mode was changed to disabled after a power cycle. **Conditions**: Unknown. **Workaround**: Reconfigure the FlexConnect VLAN mode.

Table 8 Open Caveats (continued)

ID	Description
CSCun11124	**Symptom**: Serial number of virtual controller changes when using DRS or Vmotion. **Conditions**: When you use DRS or vMotion for high availability on VMware, the UUID changes and invalidates the AP licenses. **Workaround**: • Setup DRS rules • Do not use VMotion to keep virtual controller on a single host.
CSCun15820	**Symptom**: Controller reports its MAC address in the duplicate IP message. **Conditions**: When you upgrade from 7.4.100.0 to 7.4.110.0. **Workaround**: None.
CSCun18315	**Symptom**: Problems with RADIUS server of the controller: • RADIUS server liveness depends on response for every packet, within 5 retries every 2 seconds. There is a retry counter for each outstanding RADIUS message. • When you move from one RADIUS server to another, the retry counter is not reset to zero for all outstanding RADIUS packets. • If a client terminates and starts a fresh authentication, the packet for the previous authentication from the outstanding RADIUS messages is not cleared. • Stale association requests from apfMsConnTask queue are dropped based on a timer. **Conditions**: When the primary RADIUS server fails, the secondary and tertiary servers fails within two seconds. **Workaround**: None.
CSCun19827	**Symptom**: DHCP IPv6 address is detected as duplicate address on MAC and linux. **Conditions**: Unknown. **Workaround**: Use Stateless Address Autoconfiguration (SLAAC) address on MAC.
CSCun22507	**Symptom**: Running configuration uploaded to a TFTP/FTP server does not contain WLAN and Layer 2 ACL configurations. **Conditions**: When you upload the running configuration to a TFTP/FTP server. **Workaround**: • Use **show run-config** command to get the complete running configuration. • Use **show wlan** *wlan_id* to view the missing WLAN information. • Use **show acl layer2 summary** command and **show acl layer2 detailed** *acl_name* to view the missing Layer 2 ACL configuration.

Table 8 Open Caveats (continued)

ID	Description
CSCun34605	**Symptom**: RADIUS profiling fails for Windows XP and Windows 7 workstations. ISE reports the client endpoint profile endpoint policy as Unknown. **Conditions**: • Controller with 7.6.100.0. • AP is in FlexConnect mode. • WLAN is configured for RADIUS profiling, DHCP, HTTP, FlexConnect, local switching, Radius NAC, and AAA override is enabled, and DHCP required is enabled. • ISE has Release 1.2. Patch 5. **Workaround**: • Use central switching, if applicable. • For direct ISE profiling, send DHCP helper traffic to ISE. • Redirect client to ISE for HTTP user agent discovery.
CSCun38541	**Symptom**: Controller does not include the virtual IP address in the redirect URL to the internal web engine. **Conditions**: Controller has 7.6.100.0 and WLAN is configured with 802.1X + conditional web redirect. **Workaround**: None. The configuration works on 7.0.240.0.
CSCun40401	**Symptom**: 1552c AP shows the BVI1 interface is up and Gig0 interface on the cable modem is also up. AP does not use the cable modem Ethernet and reverts to the radio interface. AP reboots and Gig0 interfaces are blocked. **Conditions**: When AP boots, BVI1 is created and cable modem's Gig0 interface comes up. Ethernet connection between motherboard bvi1 interface and cm gig0 port is not used. **Workaround**: None.
CSCun45503	**Symptom**: Connection of wired client breaks as it roams on a Flexconnect AP. The AP sends XID frames only to wired clients and not to the WGB to update the switch MAC address table. **Conditions**: • WGB with passive client with release 15.2(4)JA1. • FlexConnect APs • Local switching WLAN • Release 7.4.110.0 and 7.6.100.0 **Workaround**: Reduce the MAC address aging time for the WGB and wired client VLAN on the switches.

Table 8 Open Caveats (continued)

ID	Description
CSCun47705	**Symptom**: Some ranges of multicast addresses multicast traffic do not work on 7500, 8500, and virtual controllers. **Conditions**: • 7500, 8500, virtual controller on an Intel platform. • An address is searched within an address range. • Address is smaller than another irrespective of the endianess on a byte comparison. **Workaround**: None.
CSCun48405	**Symptom**: CAPWAP APs send deauthentication frames on new channel changed due to RRM DCA. **Conditions**: 5500 Series Controllers and all CAPWAP APs **Workaround**: None.
CSCun62368	**Symptom**: Wireless client connectivity problems on 802.1x-enabled SSIDs with release 7.6. **Conditions**: • Release 7.6 • Error: Dot1x_NW_MsgTask_4: <*date and time*> <*mac_address*> failure in apfMsUserNameSet, rc: 1. **Workaround**: Reboot the controller.
CSCun66868	**Symptom**: Controller crash at snmpApCurrChanChangedTrapSend. **Conditions**: None. **Workaround**: None. Controller crashes and recovers.
CSCun83393	**Symptom**: Unable to compile CISCO-LWAPP-DOT11-CLIENT-MIB by MG-Soft 6.0. The following error appears: `Error 43 : Cyclic reference to module "CISCO-LWAPP-DOT11-CLIENT-MIB` **Conditions**: None. **Workaround**: None.
CSCuo20684	**Symptom**: Timestamp tolerance value changes from 1000 to 0 after restoring. This tolerance value does not appear in the output of the **show guest-lan** <*wlan-id*> command. **Conditions**: Release 7.4.110.0 , 7.4.121.0 and 7.6. **Workaround**: None.
CSCun85954	**Symptom**: During high availability on 5508 controller, the active controller crashes with Task Name:rsyncmgrXferMain. **Conditions**: High availability on 5508 and release 7.6.101.7. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCuo57438	**Symptom**: Mismatch of application traffic statistics with the Top Access Points and Top Client Devices data in the new dashboard on a 2500 controller with Cisco WLAN Express Setup. **Conditions**: Only in some cases. **Workaround**: None.
CSCuo44427	**Symptom**: Small mismatch of application traffic statistics with the Top Access Points and Top Client Devices data in the new dashboard on a 2500 controller with Cisco WLAN Express Setup. **Conditions**: 2500 controller with Cisco WLAN Express Setup. **Workaround**: None.
CSCuo57524	**Symptom**: Unable to enable AVC with bootloader older than 1.8.0.0. **Conditions**: • 2500 controller with Cisco WLAN Express Setup. • Bootloader older than FUS version 1.8.0.0. **Workaround**: Upgrade FUS version to 1.8.0.0 or above.
CSCuo57544	**Symptom**: Login window pops up twice in some instances for 2500 controller with Cisco WLAN Express Setup. **Conditions**: • 2500 controller with Cisco WLAN Express Setup. • After the controller reboots. **Workaround**: None. Provide same login credentials for both login requests.
CSCsz82878	**Symptom**: Cisco WLCs using Release 4.2.130.181M (mesh) stop responding with Task Name: reaperWatcher. **Conditions**: Multiple Cisco WiSMs using Release 4.2.130.181M with numerous Cisco AP1510s associated. **Workaround**: If such a behavior and subsequent issue occurs in any deployment, use the following command to disable the dynamic CAC tree updates: **config mesh cac disable** To return the CAC tree to normal behavior, use the following command: **config mesh cac enable** **Further Problem Description**: At present, the issue appears to be due to a problem with the dynamic building of the mesh CAC tree. The issue is present even when CAC is not enabled for voice or video.

Table 8 Open Caveats (continued)

ID	Description
CSCum00101	**Symptom**: CAPWAP data tunnel gets stuck when DTLS encryption enabled in Cisco Aironet 2600/3600. **Conditions**: Occurs in the following scenario: • Cisco Aironet Access Points Series 2600 and 3600 with software release 7.5.102.11. • APs are in FlexConnect mode with data encryption enabled. • IP Addresses are mapped using NAT/PAT between access points and controller. **Workaround**: None. **Further Description**: Data encryption is enabled to leverage data keep-alive and re-establish the CAPWAP tunnel in case the NAT/PAT translation expires, but in some cases the keep-alives are lost and the tunnel stays down which means there is no self-recovery; while the controller displays the CAPWAP control tunnel and access points in UP state and access points are connected FlexConnect. However, when clients try to connect they are de-authenticated while re-association due to a timeout. This happens because the AP does not receive a reassociation response from the controller. The following error is displayed in the access point logs every minute: `%CAPWAP-3-ERRORLOG: Warning, data keep-alive failed, ignore data keep-alive timeout`
CSCum53429	**Symptom**: In Cisco Aironet Access Points 1130 series, FlexConnect VLAN mapping is corrupted when a change in VLAN mapping occurs. **Conditions**: This issue occurs when you use: • Cisco Aironet Access Points Series 1130 in FlexConnect with VLAN support • Multiple SSIDs in Local-switching **Workaround**: Reload the access points to reinstall the new VLAN mapping configuration.
CSCum63497	**Symptom**: Access to the controller CLI and Web UI is lost when service port is disconnected. However, the client authentication and DHCP still works and both clients and access points are connected to the controller. **Conditions**: This issue occurs on a virtual Cisco Wireless LAN Controller with software release 7.6.100.0. **Workaround**: None.
CSCum71699	**Symptom**: Flex AP bridge virtual interface (BVI) goes down while mapping to a VLAN. **Conditions**: This issue occurs because: • The controller tries to configure the WLAN-VLAN mapping on a newly joined AP. • The management interface of controller is untagged which means that the WLAN gets mapped to VLAN1 initially. **Workaround**: You can tag the management VLAN in the controller with the VLAN identifier.

Table 8 Open Caveats (continued)

ID	Description
CSCum82560	**Symptom**: Access point sends deauthentication frames to new-channel after a channel change occurs due to Radar detection. **Conditions**: This issue occurs in Cisco Aironet Access Points Series 5508 with a software release 7.6.100.0 when: • A channel change from a DFS-enabled channel to another occurs. • Channel switch announcement is disabled. **Workaround**: None.
CSCum86401	**Symptom**: Access points are unable to join the Cisco Wireless LAN Controller with software release 7.3 due to a stale entry on the controller. **Conditions**: Unknown. **Workaround**: Reboot the controller.
CSCum87504	**Symptom**: Controller continuously displays messages of detected MFP anomaly. **Conditions**: This issue occurs in Cisco Flex Access Points Series 7500 with software release 7.6 or 7.5 when: • Global Infrastructure MFP state is disabled. • Client MFP value set as either optional or disabled for all WLANs. **Workaround**: You must use a software release prior to 7.6 or 7.5.
CSCum92822	**Symptom**: FlexConnect AID leak **Conditions**: Unknown. **Workaround**: None.
CSCtd34834	**Symptom**: Unable to disable MFP traps when the clients are in power save mode or in busy environments. Hence, the logs are accumulated with trap entries. **Conditions**: Unknown Workaround: None
CSCuh81923	**Symptom**: After upgrade to controller software release 7.2.111.3, the accounting messages sent to the Radius server from the controller listed the clients as Remote, irrespective of where the clients were authenticated. **Conditions**: Unknown **Workaround**: None
CSCuh97457	**Symptom**: When a Change Of Authentication disconnect request is sent from the RADIUS server, the controller refuses to acknowledge attributes for user session disconnect request. **Conditions**: Unknown **Workaround**: None
CSCui16915	**Symptom**: Issues in guest tunneling while working with Cisco WLC controller 5508 as mobility controller and guest controller. **Conditions**: Unknown **Workaround**: None

Table 8 Open Caveats (continued)

ID	Description
CSCul38572	**Symptom**: CCKM roaming failing between a controller with software release 7.0 and a 7.4. **Conditions**: Unknown **Workaround**: None
CSCul42704	**Symptom**: Rogue APs are mistaken as infrastructure devices. Thus, the wIPS alarms such sa deauthentication spoofed MAC address are falsely triggered later. **Conditions**: Rogue devices that are not associated with Cisco AP send data packet such as data null to Cisco AP. This causes wIPS to falsely recognize rogue devices as part of infrastructure devices. **Workaround**: None.
CSCul44588	**Symptom**: Channel information is not displayed when the triggering frame contains channel 0 in radio header in access points for wIPS alarms. **Conditions**: The triggering frames are sent in 5GHz. **Workaround**: None.
CSCul57266	**Symptom**: Wireless clients on the controller (both in CLI and Web UI) interface indicates that the WMM is disabled and that no data rates are supported when Local Authentication is enabled. **Conditions**: FlexConnect Local Authentication is enabled. **Workaround**: Verify the actual client status using the **show capwap reap association** command.

Table 8 Open Caveats (continued)

<table>
<tr><th>ID</th><th>Description</th></tr>
<tr><td>CSCul72669</td><td>

Symptom: Lightweight Cisco AP might not send out deauthentication messages to an existing client before 802.11 radio interface reset by RLDP although **debug dot11 mgmt message** command outputs indicate the messages are sent out.

Conditions: RLDP is enabled on a lightweight Cisco AP.

Workaround: Disable RLDP.

</td></tr>
<tr><td>CSCuo86819</td><td>

Symptom: A Cisco WLC might stop working, displaying a variety of symptoms such as the following:

<pre>
Task Name: PMIPV6 Thread
Reason: System Crash
[...]
  Software Failed on instruction at:
 pc = 0x122e7cec (license_xos_thread_create+2139596), ra = 0x122f630c
(license_xos_thread_create+2139596)
  Software Failed while accessing the data located at :0x160c

or

  Software was stopped by the reaper for the following reason:
     Reaper Reset: Task "PMIPV6 Thread" taking too much cpu: 100%, (user
84%, system 15%) while SW Watchdog is disabled

or

Task Name: RRM-CLNT-2_4
Reason: System Crash
[...]
  Software was stopped for the following reason:
     pmalloc detected memory corruption
</pre>

Conditions: Cisco WLC is using Release 7.6.120.0; web-auth is in use.

Workaround: None, other than disabling web-auth or anchoring to Cisco WLC that does not use Release 7.6.120.0.

Further Problem Description: This issue is a regression caused by the commit of the fix for CSCuc68995 in Release 7.6.120.0.

</td></tr>
</table>

Resolved Caveats

Table 9 lists the caveats that have been resolved in Release 7.6.120.0.

Table 9 Resolved Caveats

ID	Title
CSCuf77821	A vulnerability in the Controller GUI allowed an unauthenticated, remote attacker to execute a cross-frame scripting (XFS) attack.
CSCul43158	Wireless devices were randomly disconnected every 5 to 10 minutes with unknown policy timeout message in debug client.
CSCun23245	Stateful DHCPv6 IP addressing work in release 7.6.100.0.
CSCun92928	In a HotSpot WLAN, APs did not advertise IE 107 (Interworking IE) until the config was saved and the controller rebooted.

Table 9 Resolved Caveats (continued)

ID	Title
CSCuh25790	Could not reload the HA-enabled controller even after predownload completed.
CSCun95013	Controller crashed with Task Name: Bonjour_Socket_Task after HA switchover.
CSCun71909	AP 700 series showed load profile as failed with only few clients or even no clients at all. The Tx and Rx utilization was 100%.
CSCun19267	Multicast failed on 1130 and 1240 APs.
CSCul55232	7500 controller crashed during validation of snmpv3user lifetime on HA.
CSCun95909	Could not enable or disable Telnet or SSH on 1240 and 1130 APs from controller.
CSCul82199	Controller crashed when interface group config was changed in 7.5.102.0.
CSCun79357	Daisy chain configuration did not exceed 90Mbps backhaul xfer rates beyond second MAP.
CSCul00381	WLAN clients did not get DHCP addresses.
CSCuh72474	Controller assigned an interface inside a group to dirty list.
CSCul45107	Controller with 7.5.102.0 crashed without any crash or core file in HA topology.
CSCui01948	`SNMP operation to Device failed Table too large` message appeared on PI 1.3
CSCuc68995	Webauth client was not authenticated to the network and HTTP GET from the client arrived at the controller in multiple TCP segments.
CSCun27153	ff02::2:ffxx:xxxx/104 taken as link local multicast.
CSCud50209	Controller crashed when management user form fields were updated.
CSCul30107	WiSM2 crashed due to DP failure on 7.5.102.0.
CSCul35980	WiSM2 crashed on 7.5.102.0.
CSCul78541	AAA override client got assigned to dynamic interface while roaming on controller with 7.4.111.9.
CSCul94534	WiSM2 did not process fragmented client certificate.
CSCum46098	False HA switch over occured due to keepalive loss in the kernel stack.
CSCum91313	WiSM2 crashed.
CSCun12965	AP sent CAPWAP packets with size larger than 1500 bytes.
CSCuh52238	False DFS related to client activity are detected.
CSCun20263	New association of 1530 root and non-root AP did not happen at low dBm.
CSCuj58556	3500 AP lost names and configurations.
CSCum68676	When 802.11ac was disabled, 3700 AP advertised VHT IEs with length 0.
CSCui73764	FlexConnect mode 1130 and 1240 series APs did not pass traffic on some WLANs.
CSCul16796	EAP certificate transmission failed on Virtual WLC running 7.5 and low PMTU.
CSCul33755	Controller did not respond to Apple clients that sent out unicast ARPs.

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.

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.