Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.4.121.0

First Published: December 2013
Last Updated: March 2014
OL-28134-04

These release notes describe what is new in this release, instructions to upgrade to this release, and open and resolved caveats for this release.

Note Unless otherwise noted, all of the Cisco Wireless LAN controllers are referred to as *controllers*, and all of the Cisco lightweight access points are referred to as *access points* or *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

This section contains the following subsections:

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 controllers) for 5500 series, WiSM2, Flex 7500 series, and 8500 series controllers
- Cisco Wireless Services Module 2 (WiSM2) for Catalyst 6500 Series switches
- Cisco Wireless Controller on Cisco Services-Ready Engine (SRE) (controllerM2) running on ISM 300, SM 700, SM 710, SM 900, and SM 910

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco 1040, 1130, 1140, 1240, 1250, 1260, 1600, 2600, 3500, 3500p, 3600, Cisco 600 Series OfficeExtend Access Points, AP801, and AP802
- Cisco Aironet 1550 (1552) series outdoor 802.11n mesh access points; Cisco Aironet 1520 (1522, 1524) series outdoor mesh access points
- The 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/en/US/prod/collateral/routers/ps380/data_sheet_c78_461543.html
  - AP880:

    http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_459542_ps380_Products_Data_Sheet.html

    http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78-613481.html

    http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps10082/data_sheet_c78_498096.html

http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps10082/data_sheet_c78-682548.html

– AP890:

http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78-519930.html

Note The 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 controller software release 7.4.121.0, you must upgrade the software in the Next Generation Cisco 880 Series ISRs to Cisco IOS 151-4.M or later releases.

Unsupported Cisco Wireless LAN Controller Platforms

The following controller platforms are not supported:

- Cisco 4400 Series Wireless LAN Controller
- Cisco 2100 Series Wireless LAN Controller
- Cisco Catalyst 3750G Integrated Wireless LAN Controller
- Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM)
- Cisco Wireless LAN Controller Module (NM/NME)

What's New in This Release

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

Software Release Support for Access Points

Table 1 lists the controller software releases that support specific Cisco access points. The First Support column lists the earliest controller 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.

Table 1 Software Support for Access Points

Access Points		First Support	Last Support
1000 Series	AIR-AP1010	3.0.100.0	4.2.209.0

Table 1 Software Support for Access Points (continued)

Access Points		First Support	Last Support
	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	7.4.121.0	—
	AIR-CAP1602I-xK910	7.4.121.0	—
	AIR-SAP1602I-x-K9	7.4.121.0	—
	AIR-SAP1602I-xK9-5	7.4.121.0	—
	AIR-CAP1602E-x-K9	7.4.121.0	—
	AIR-SAP1602E-xK9-5	7.4.121.0	—
AP801		5.1.151.0	
AP802		7.0.98.0	
AP802H		7.3.101.0	

Table 1 Software Support for Access Points (continued)

Access Points		First Support	Last Support
2600 Series	AIR-CAP2602I-x-K9	7.2.110.0	
	AIR-CAP2602I-xK910	7.2.110.0	
	AIR-SAP2602I-x-K9	7.2.110.0	
	AIR-SAP2602I-x-K95	7.2.110.0	
	AIR-CAP2602E-x-K9	7.2.110.0	
	AIR-CAP2602E-xK910	7.2.110.0	
	AIR-SAP2602E-x-K9	7.2.110.0	
	AIR-SAP2602E-x-K95	7.2.110.0	
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	—
600 Series	AIR-OEAP602I	7.0.116.0	
Note The Cisco 3600 Access Point was introduced in 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 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]	—
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 the separate 4.1.19x.x mesh software release or with release 5.2 or later releases. These access points are not supported in the 4.2, 5.0, or 5.1 releases.

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

Upgrading to Controller Software Release 7.4.121.0

Guidelines and Limitations

- Cisco WLCs validate client IP address at the time of learning, using the dynamic interface IP address as per the VLAN assigned to the client. Ensure that the clients and the dynamic interface VLAN of the clients are on the same subnet, even if DHCP proxy is disabled at the Cisco WLC.
- When H-REAP access points that are associated with a controller that has all the 7.0.x software releases that are prior to 7.0.240.0 upgrade to the 7.4.121.0 release, the access points lose their VLAN support configuration if it was enabled. The VLAN mappings revert to the default values of the VLAN of the associated interface. This issue does not occur if you upgrade from 7.0.240.0 or later 7.0.x release to the 7.4.121.0 release.
- We recommend that you install Wireless LAN Controller Field Upgrade Software for Release 1.7.0.0-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_1_7_0_0.html
- 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 Wireless LAN Controller Field Upgrade Software for Release 1.8.0.0-FUS. This is not required if you are using other controller hardware models. For more information, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_1_8_0_0.html
- When you enable LAG on a Cisco 2500 Series Controller with which a direct-connect access point is associated, the direct-connect access point dissociates with the controller. When LAG is in enabled state, the direct-connect access points are not supported. For direct-connect access points to be supported, you must disable LAG and reboot the controller.

  If LAG is enabled on the Cisco 2500 Series Controller and the controller is downgraded to a non-LAG aware release, the port information is lost and it requires manual recovery.
- After you upgrade to the 7.4 release, 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 7500 controllers 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 require a downgrade from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.
- It is not possible to directly upgrade to the 7.4.121.0 release from a release that is older than 7.0.98.0.
- You can upgrade or downgrade the controller software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to software release 7.4.121.0. Table 2 shows the upgrade path that you must follow before downloading software release 7.4.121.0.

Table 2 Upgrade Path to Controller Software Release 7.4.121.0

Current Software Release	Upgrade Path to 7.4.121.0 Software
7.0.98.0 or later 7.0 releases	You can upgrade directly to 7.4.121.0 **Note** If you have VLAN support and VLAN mappings defined on H-REAP access points and are currently using a 7.0.x controller 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 7.4.121.0 to avoid losing those VLAN settings.
7.1.91.0	You can upgrade directly to 7.4.121.0
7.2. or later 7.2 releases	You can upgrade directly to 7.4.121.0 **Note** If you have an 802.11u HotSpot configuration on the WLANs, we recommend that you first upgrade to the 7.3.101.0 controller software release and then upgrade to the 7.4.121.0 controller software release. You must downgrade from the 7.4.121.0 controller software release to a 7.2.x controller software release if you have an 802.11u HotSpot configuration on the WLANs that is not supported.
7.3 or later 7.3 releases	You can upgrade directly to 7.4.121.0
7.4 releases that are prior to this release	You can upgrade directly to 7.4.121.0

- When you upgrade the controller to an intermediate software release, you must wait until all of the access points that are associated with the controller are upgraded to the intermediate release before you install the latest controller software. In large networks, it can take some time to download the software on each access point.
- If you upgrade to the controller software release 7.4.121.0 from an earlier release, you must also upgrade to Cisco Prime Infrastructure 1.3 and MSE 7.4.
- You can upgrade to a new release of the controller software or downgrade to an older 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 controller is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.
- We recommend that you access the controller GUI using Microsoft Internet Explorer 6.0 SP1 (or a later release) or Mozilla Firefox 2.0.0.11 (or a later release).
- Cisco controllers support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com.
- The controller software is factory installed on your controller and automatically downloaded to the access points after a release upgrade and whenever an access point joins a controller. 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 the controller software release 7.4.121.0. 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 7.4.121.0 controller 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 or a different subnet because the distribution system port is routable.
- When you plug a controller into an AC power source, the bootup script and power-on self-test run to initialize the system. During this time, you can press **Esc** to display the bootloader Boot Options Menu. The menu options for the 5500 differ from the menu options for the other controller platforms.

  Bootloader Menu for 5500 Series Controllers:

```
   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 Controller 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 controller), or enter **5** (on another controller platform) to run the current software and set the controller 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 for your controller for more details on running the bootup script and power-on self-test.

- The controller 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, be sure to 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 controller.

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

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

  where:

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

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 the 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 controller 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 a 7.4.121.0 version on a Cisco Aironet 1240 access point is not supported when upgrading from a previous controller release. If predownloading is attempted to a Cisco Aironet 1240 access point, an AP disconnect will occur momentarily.

- Do not power down the controller or any access point during the upgrade process; otherwise, you might corrupt the software image. Upgrading a controller 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 controller must not be reset during this time.
- If you want to downgrade from the 7.4.121.0 release to a 6.0 or an older release, do either of the following:
  - Delete all WLANs that are mapped to interface groups and create new ones.
  - Ensure that all WLANs are mapped to interfaces rather than interface groups.

- After you perform these functions on the controller, you must reboot the controller 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 SSL certificate
  - Configure the database size
  - Install vendor device certificate
  - Download CA certificate
  - Upload configuration file
  - Install Web Authentication certificate
  - Changes to management or virtual interface
  - TCP MSS

Upgrading to Controller Software Release 7.4.121.0 (GUI)

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

Note We highly recommend that you back up your controller's configuration files prior to upgrading the controller software.

Step 2 Follow these steps to obtain the 7.4.121.0 controller 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 controller platform, click one of the above options.

e. Click the controller model number or name. The **Download Software** page is displayed.

f. Click a controller software release. 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 Cisco's End User Software License Agreement and then 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 controller software file (*filename*.aes) to the default directory on your TFTP, FTP, or SFTP server.

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

Note For busy networks, controllers on high utilization, or small controller 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 controller. A message appears indicating the status of the download.

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

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

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

Step 17 For Cisco WiSM2 on the Catalyst switch, check the port channel and reenable the port channel if necessary.

Step 18 If you have disabled the 802.11a/n and 802.11b/g/n networks in Step 4, reenable them.

Step 19 To verify that the 7.4.121.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at 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 controller. 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 controller with DTLS that is disabled due to import restrictions but have authorization from local regulators to add DTLS support after the initial purchase. Consult your local government regulations to ensure that DTLS encryption is permitted.

Note Paper PAKs and electronic licenses available are outlined in the respective controller datasheets.

Downloading and Installing a DTLS License for an LDPE Controller

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 controller 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 Controller

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 controller model from the right selection box.

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

d. From 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 Cisco's End User Software License Agreement and then click **Agree**.

h. Save the file to your hard drive.

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

Step 3 Upgrade the controller with this version by following the instructions from Step 3 through Step 19 detailed in the "Upgrading to Controller Software Release 7.4.121.0" section on page 7.

Interoperability With Other Clients in 7.4.121.0

This section describes the interoperability of the version of controller software with other client devices.

Table 3 describes the configuration used for testing the clients.

Table 3 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	7.4.121.0
Controller	Cisco 5500 Series Controller
Access points	1131, 1142, 1242, 1252, 3500e, 3500i, and 3600
Radio	802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 4.2, ACS 5.2
Types of tests	Connectivity, traffic, and roaming between two access points

Table 4 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 4 Client Types

Client Type and Name	Version
Laptop	
Intel 3945/4965	11.5.1.15 or 12.4.4.5, v13.4
Intel 5100/5300/6200/6300	v14.3.0.6
Intel 1000/1030/6205	v14.3.0.6
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 (Broadcom)	5.10.91.26
Handheld Devices	
Apple iPad	iOS 5.0.1
Apple iPad2	iOS 6.0(10A403)
Apple iPad3	iOS 6.0(10A403)
Asus Slider	Android 3.2.1
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
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

Table 4 Client Types (continued)

Client Type and Name	Version
Vocera B2000	4.0.0.345
Apple iPhone 4	iOS 6.0(10A403)
Apple iPhone 4S	iOS 6.0(10A403)
Apple iPhone 5	iOS 6.0(10A405)
Ascom i62	2.5.7
HTC Legend	Android 2.2
HTC Sensation	Android 2.3.3
LG Optimus 2X	Android 2.2.2
Motorola Milestone	Android 2.2.1
RIM Blackberry Pearl 9100	WLAN version 4.0
RIM Blackberry Bold 9700	WLAN version 2.7
Samsung Galaxy S II	Android 2.3.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Samsung Galaxy Nexus	Android 4.0.2
Motorola Razr	Android 2.3.6

Features Not Supported on Controller Platforms

This section lists the features that are not supported in the following platforms:

- Features Not Supported on Cisco 2500 Series Controllers
- Features Not Supported on WiSM2 and Cisco 5500 Series Controllers
- Features Not Supported on Cisco Flex 7500 Controllers
- Features Not Supported on Cisco 8500 Controllers
- Features Not Supported on Cisco Wireless Controller on Cisco Services-Ready Engine
- Features Not Supported on Cisco Virtual Wireless Controllers
- Features Not Supported on Mesh Networks

Features Not Supported on Cisco 2500 Series Controllers

- Wired guest access
- Bandwidth contract
- Service port
- AppleTalk Bridging
- Right to Use licensing
- PMIPv6
- High Availability

- Multicast-to-unicast

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

Note Directly connected APs are supported only in Local mode.

Features Not Supported on WiSM2 and Cisco 5500 Series Controllers

- Spanning Tree Protocol (STP)
- Port mirroring
- Layer 2 access control list (ACL) support
- VPN termination (such as IPsec and L2TP)
- VPN passthrough option

  Note You can replicate this functionality on a 5500 series controller 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 Controllers

- Static AP-manager interface

  Note For Cisco 7500 Series controllers, 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 the following modes: Local, Rogue Detector, Sniffer, Bridge, and SE-Connect

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

- Mesh
- Spanning Tree Protocol (STP)
- Cisco Flex 7500 Series Controller cannot be configured as a guest anchor controller. However, it can be configured as a foreign controller to tunnel guest traffic to a guest anchor controller 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 that is based on IGMP or MLD snooping.

- PMIPv6
- 802.11w

Features Not Supported on Cisco 8500 Controllers

- Cisco 8500 Series Controller cannot be configured as a guest anchor controller. However, it can be configured as a foreign controller to tunnel guest traffic to a guest anchor controller in a DMZ.
- TrustSec SXP
- Internal DHCP server

Features Not Supported on Cisco Wireless Controller on Cisco Services-Ready Engine

- Wired guest access
- Cisco Wireless Controller on Cisco Services-Ready Engine (SRE) cannot be configured as a guest anchor controller. However, it can be configured as a foreign controller to tunnel guest traffic to a guest anchor controller in a DMZ.
- Bandwidth contract
- Access points in direct connect mode
- Service port support
- AppleTalk Bridging
- LAG
- Application Visibility and Control (AVC)

Features Not Supported on Cisco Virtual Wireless Controllers

- Data DTLS
- Cisco 600 Series OfficeExtend Access Points
- Wireless rate limiting (bandwidth contract)
- 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 that is based on IGMP or MLD snooping.

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

Note Outdoor AP in FlexConnect mode is supported.

- Indoor mesh access points
- 802.11w
- Application Visibility and Control (AVC)

Features Not Supported on Mesh Networks

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

Caveats

The following sections lists Open Caveats and Resolved Caveats for Cisco controllers and lightweight access points for version 7.4.121.0. For your convenience in locating caveats in Cisco's 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

Open Caveats

Table 5 lists the open caveats in this release.

Table 5 Open Caveats

ID	Description
CSCud50209	**Symptom**: Controller fails when the management user form post is manipulated. **Conditions**: Management user fields are modified. **Workaround**: None.
CSCsz82878	**Symptom**: Controllers using Release 4.2.130.181M (Mesh) crash with Task Name: reaperWatcher. **Conditions**: Multiple WiSM controllers use Release 4.2.130.181M and have many Cisco Aironet 1510 Lightweight Outdoor Mesh Access Points associated to them. **Workaround**: 1. To disable the dynamic CAC tree updates, enter this command: **config mesh cac disable** 2. To enable the dynamic CAC tree updates, enter this command: **config mesh cac enable**

Table 5 Open Caveats (continued)

ID	Description

CSCtc16222	**Symptom**: The following messages appear on Cisco WiSM2s:
	`Message from syslogd@wism2-ms9-mgmt.it.osu at Sep 20 08:38:46 ... wism2-ms9-mgmt.it.osu wism2-ms9: *spamApTask7: Sep 20 08:38:42.434: #OSAPI-0-INVALID_TIMER_HANDLE: timerlib_mempool.c:241 Task is using invalid timer handle 15069/46996`
	`Message from syslogd@wism2-ms9-mgmt.it.osu at Sep 20 08:38:46 ... wism2-ms9-mgmt.it.osu wism2-ms9: -Traceback:  0x113b0060 0x10a26264 0x105c9810 0x105c2760 0x105c2b90 0x105c3094 0x105a19e0 0x10348180 0x103d88ec 0x103e4ac4 0x10e4c86c 0x10a22318 0x11d316a0 0x11d8ffcc`
	Conditions: Cisco WiSM2 using Release 7.3.101.0.
	Workaround: None.

CSCtn52995	**Symptom**: Mismatch between the association counters of controller and access point. **Conditions**: 802.11 authentication frames are sent sometimes on different WLANs and are not followed by association frames. 1. Client 1 associates to the controller with AID =1 on SSID x. 2. Client 1 sends 802.11 Auth frame on SSID y and AID = 1 is disassociated at the access point. Auth frames are not honored at the controller, so controller is not informed. 3. No association frame arrives from client 1 at ssid 2. 4. Client 2 associates to the access point and gets AID = 1. 5. Access point updates the controller about client 2 and AID =1. 6. Controller adds duplicate entries and increments the count (controller already has client 1 AID =1). 7. Counter gets incremented and reaches 256. **Workaround**: None.
CSCtq82437	**Symptom**: Unable to see CDP neighbor details of Cisco 1242, 1142 and 3500 series access points using the controller. **Conditions**: Controllers using Release 7.0.116.0. Access points are rebooted after a power outage, newly installed, or moved from one campus to another. **Workaround**: Reboot the access points.
CSCts20040	**Symptom**: Controller crashes when SXP parameters like default password are updated or SXP is disabled/enabled. **Conditions**: Reboot with a version 1 SXP connection. **Workaround**: Delete the version 1 SXP connection before you change any SXP settings.
CSCty84682	**Symptom**: Access point does not forward multicast data and IGMP query messages. **Conditions**: Reload of an access point. **Workaround**: Shutdown the interface to the WLAN and bring it up again.

Table 5 Open Caveats (continued)

ID	Description
CSCub63054	**Symptom**: VLAN transparency enabled on Release 7.2 does not pass VLAN tags. Span at endpoints shows all frames are placed on the native VLAN. **Conditions**: VLAN transparency is enabled. **Workaround**: Disable VLAN transparency and set the MAP Ethernet port as trunk.
CSCub96053	**Symptom**: Cisco Aironet 3500 Series Access Point gets DFS events when the DFS channel associates with a Cisco 7925 IP phone. Frequency of DFS events is higher on weekday and business hours. **Conditions**: Release 7.2.103.0. **Workaround**: None.
CSCuc32335	**Symptom**: Local mode access points associated to controller lose their configuration and get reset to factory defaults. **Conditions**: Cisco 3602 Access point and Cisco 5500 Series Wireless LAN Controller using Release 7.2.103.0. Local mode access point loses power. Shut or no shut is configured on the PoE port. **Workaround**: None.
CSCuc45005	**Symptom**: Controller stops working while using Release 7.3.101.0. **Conditions**: None. **Workaround**: None.
CSCuc68995	**Symptom**: Wireless WebAuth clients are unable to authenticate to the network. A blank window appears when the client opens a browser window. When you use the **debug web-auth redirect** command, the following messages appear: `*webauthRedirect: Oct 15 18:43:19.470: #EMWEB-6-REQUEST_IS_NOT_GET_ERROR: webauth_redirect.c:1055 Invalid request not GET on client socket 72` or `*webauthRedirect: Oct 10 16:36:30.715: %EMWEB-3-PARSE_ERROR: parse error after reading. bytes parsed = 0 and bytes read = 189` **Conditions**: HTTP GET from the client arrives at the controller in multiple TCP segments. **Workaround**: Reconfigure your network and the client's TCP/IP stack to ensure that the HTTP GET arrives in a single segment. An example of a client software that introduces TCP segmentation is AnyConnect Web Security 3.0.3054.
CSCuc69522	**Symptom**: Client sends TCP SYN to a multicast MAC for its gateway and the controller does not send a TCP SYN ACK back. As the TCP handshake is not complete, the client never generates HTTP traffic and is never redirected. Traffic arrives at foreign controller and goes to anchor controller. Anchor controller drops the TCP SYN messages. **Conditions**: Foreign and anchor controller perform Central Web Authentication (CWA). Client has multicast MAC address for its gateway. Gateway of the client has a load-balanced or clustered node. **Workaround**: Do not use multicast MAC address for gateway.

Table 5 Open Caveats (continued)

ID	Description
CSCuc70159	**Symptom**: Autonomous access point loses clock information after it reboots. **Conditions**: Autonomous access point using Release 15.2. **Workaround**: 1. Manually configure the clock after the access point reboots. 2. Configure SNTP in the access point for applications when the access point does not operate as a WGB with certificate based authentication using the command: **sntp server a.b.c.d version {1 | 2 | 3}**
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.
CSCuc81022	**Symptom**: Cisco Aironet 1520 Lightweight Outdoor Mesh Access Points get false DFS triggers when in-band or off-channel (ch 124) weather RADAR signals are present. These signals are received above -20 dBm and cause network instability. **Conditions**: AIR-LAP152x outdoor mesh AP is installed near a weather RADAR installation. **Workaround**: Use the **config 802.11a dfs-peakdetect disable** command.
CSCuc86805	**Symptom**: CLI debug outputs show the following message: `Association request from the P2P Client Process P2P Ie and Update CB` **Conditions**: None. **Workaround**: None.
CSCuc91441	**Symptom**: When multiple clients timeout at the same time, some clients are not removed from the controller's database after the user idle timer expires. **Conditions**: When around 100 clients expire their user idle timeout simultaneously, only 64 deauthentication messages are sent and 36 clients are not removed from the controller database. **Workaround**: Perform one of the following tasks: • Manually remove the stale clients. • Reboot the access point with these clients. • Reboot the controller. • Disable and enable the WLAN.
CSCuc93681	**Symptom**: Controller stops working intermittently and the crash log contains the following message: `Software Failed on instruction at : pc = 0x10a5fdfc (read_socket 492) ra = 0x10a5ff34 (read_socket 492)` **Conditions**: Controller using any Release from 7.0 to 7.4. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCuc98178	**Symptom**: When you change the HSRP configuration, CAPWAP access points send data to the old HSRP MAC address and control traffic to the new gateway. **Conditions**: Controller using Release 7.2 with Cisco Aironet 3500 Series Access Point and HSRP gateway. **Workaround**: Reboot the controller.
CSCud07983	**Symptom**: Local AAA sever of the controller shows the outer EAP username of wireless users who are authenticated using local EAP. **Conditions**: Local EAP is used on controller. **Workaround**: Disable identity protection on the wireless client to use the same username for inner and outer EAP usernames. For local EAP, inner username appears in the clients page or when you use the **show client detailed mac-addr** command.
CSCud12582	**Symptom**: Client RADIUS authentication fails. **debug client** command shows the following message: `*Dot1x_NW_MsgTask_7: Dec 17 11:43:36.983: 00:11:22:33:44:55 Entering Backend Auth Response state for mobile f0:d1:a9:24:d8:a7 *Dot1x_NW_MsgTask_7: Dec 17 11:43:36.985: 00:11:22:33:44:55 Processing AAA Error 'Out of Memory' (-2) for mobile f0:d1:a9:24:d8:a7 *Dot1x_NW_MsgTask_7: Dec 17 11:43:36.999: 00:11:22:33:44:55 Sent Deauthenticate to mobile on BSSID 20:37:06:00:11:22 slot 0(caller 1x_auth_pae.c:1394) at the same time the msglog shows a message similar to this: *Dot1x_NW_MsgTask_7: Dec 17 12:30:23.296: #DOT1X-3-ABORT_AUTH: 1x_bauth_sm.c:447 Authentication Aborted for client 00:11:22:33:44:55 and the traplog shows a message like this: 297 Mon Dec 17 12:36:29 2012 Client Deauthenticated: MACAddress:00:11:22:33:44:55` `Base Radio MAC:20:37:06:00:11:22 Slot: 1` `User Name: unknown Ip Address: unknown Reason:Unspecified ReasonCode: 1` **Conditions**: Large scale deployments with multiple clients. RADIUS queues fill up and fail under heavy authentication and accounting load. **Workaround**: Disable RADIUS accounting and authentication.
CSCud14147	**Symptom**: Controller calculates incorrect message authenticator value for RFC3576 CoA requests from some RADIUS servers such as PacketFence NAC. **Conditions**: Controller using Release 7.2.110.0 or Release 7.3.101.0. **Workaround**: None.
CSCud44269	**Symptom**: FlexConnect mode access point sends ARP responses for a client in DHCP-required state. Roaming breaks for clients associated to the access point. **Conditions**: • FlexConnect mode access point using Release 7.3.101.0. • DHCP required is enabled on the WLAN. **Workaround**: Disable the DHCP Required check box on the WLAN.

Table 5 Open Caveats (continued)

ID	Description
CSCud69426	**Symptom**: AAA Override ACL is not applied. **Conditions**: After a session timeout, the controller clears the AAA override cache and puts the wireless client in the default VLAN. **Workaround**: None.
CSCud89654	**Symptom**: When clients associate to a local access point after a successful authentication, only the URL redirect attribute is accepted by the controller and not the URL-redirect-ACL attribute. This causes failures on redirection thereafter. **Conditions**: Local switching-enabled 802.1x WLANs. Controller using Release 7.2. **Workaround**: Disable local switching on the WLAN. Segregate the local access point from FlexConnect access points on different controllers.
CSCue02826	**Symptom**: 5-GHz radio on AIR-CAP1552E-N-K9 in non-bridge mode fails to enable if the controller is configured for the Brazil (-T) regulatory domain. **Conditions**: Controller using Release 7.3.101.0. **Workaround**: Use access point in the bridge mode.
CSCue04517	**Symptom**: RRM cannot be disabled on the controller when the RF group DCA and TPC are disabled. Monitor mode command returns a message stating that DCA and TPC must be disabled even though they are already disabled. **Conditions**: Release 7.4.110.0. **Workaround**: Enter the following commands: • **config 802.11a txPower global** *1* • **config 802.11a channel global off** • **config advanced 802.11a group-mode leader** • **config advanced 802.11a monitor mode disable** • **config advanced 802.11a group-mode off**
CSCue09354	**Symptom**: Rogue access points are not detected when they are on a non-native VLAN trunk to a rogue detector access point. **Conditions**: Rogue detector mode access point using Release 7.4.100. Rogue access point is not on the rogue detector native VLAN. **Workaround**: None.
CSCue33057	**Symptom**: Reversed gateway address appears for CCXv5 diagnostics client. **Conditions**: Cisco 8500 Series WLC. **Workaround**: None.
CSCue38133	**Symptom**: Ninety days after an access point associates with a controller, the controller sends a message that the access point should be moved to the primary controller. **Conditions**: An HA-SKU controller is the secondary controller in a N+1 configuration and an access point joins the controller. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCue44986	**Symptom**: Facetime calls are not detected and proper bandwidth is not allocated. **Conditions**: Apple OS uses a different port to send SIP packets. **Workaround**: Reconnect the call.
CSCue46710	**Symptom**: Controller stops responding during scale stress tests. CPU utilization remains at around 26 percent. **Conditions**: Around 6000 APs and 64000 clients are associated with the controller. **Workaround**: None.
CSCue50917	**Symptom**: When an RAP loses its wired connection, it fails to restore connectivity as an MAP through the radio backhaul. Mesh adjacency is built to a nearby MAP and the RAP gets an IP address. RAP joins its controller and disconnects due to a radio reset. RAP keeps on looping till connectivity is restored. The following error messages appear on the RAP: `*Feb 8 19:37:54.919: %CAPWAP-3-ERRORLOG: Selected MWAR '5500-5'(index 0). *Feb 8 19:37:54.919: %CAPWAP-3-ERRORLOG: Go join a capwap controller ~ *Feb 8 19:37:45.139: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller 5500-5 ~ *Feb 8 19:37:45.183: %MESH-6-ADJ_VIDB_LINK: Mesh neighbor 0021.a1f9.fa0f VIDB Virtual-Dot11Radio0 forwarding ~ *Feb 8 19:37:46.075: %LINK-6-UPDOWN: Interface Dot11Radio1 changed state to down *Feb 8 19:37:46.083: %LINK-5-CHANGED: Interface Dot11Radio1 changed state to reset ~ *Feb 8 19:37:47.075: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1 changed state to down *Feb 8 19:37:47.099: %DOT11-6-DFS_SCAN_START: DFS: Scanning frequency 5700 MHz for 60 seconds. ~ *Feb 8 19:38:21.751: %MESH-4-NO_POTENTIAL_PARENT: There are no potential parents *Feb 8 19:38:24.751: %MESH-4-NO_POTENTIAL_PARENT: There are no potential parents *Feb 8 19:38:24.751: %MESH-6-LINK_UPDOWN: Mesh station 0021.a1f9.fa0f link Down *Feb 8 19:38:24.951: %MESH-6-ADJ_VIDB_LINK: Mesh neighbor 0021.a1f9.fa0f VIDB Virtual-Dot11Radio0 going down *Feb 8 19:38:24.955: %LINK-6-UPDOWN: Interface Virtual-Dot11Radio0 changed state to down10 *Feb 8 19:38:25.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Dot11Radio0 changed state to down` **Conditions**: Mesh deployment using Releases 7.0.230.0, 7.2.104.31, and 7.3.112.0. **Workaround**: None.
CSCue51812	**Symptom**: Clients do not associate with the access point, clients gain network access and roam frequently. **Conditions**: Band select is configured with default parameters or with low values. For example, probe cycle is 1 and suppression window is 100 ms. **Workaround**: Disable Band select when there are multiple clients.

Table 5 Open Caveats (continued)

ID	Description
CSCue88103	**Symptom**: Controller logs the following traceback message: `*apfMsConnTask_0: Feb 28 14:25:59.293: #APF-3-VALIDATE_DOT11i_CIPHERS_FAILED: apf_rsn_utils.c:841 Could not validate Dot11i security IE. Received an unsupported Multicast 802.11i OUI code from mobile.Mobile:00:11:22:33:44:55 -Traceback: 0x1019de50 0x1104434c 0x11049b30 0x10c12a28 0x12238810 0x122ab30` **Conditions**: Wireless client requests an invalid or unsupported encryption cipher during authentication. **Workaround**: None.
CSCue99208	**Symptom**: **config advance 802.11 {a | b} monitor noise** command configurations are lost after reboot. The following messages appear: `Node ptr_rrmCfgData.rrm.noiseInterferenceInterval value = xxx is out of range for min = 0 and max = 168 Validation for node ptr_rrmCfgData.rrm.noiseInterferenceInterval failed  indices for node are x` **Conditions**: Noise measurement interval is longer than 360 seconds. **Workaround**: Configure the noise measurement interval between 60 and 360 seconds.
CSCuf03454	**Symptom**: Controller stops responding. **Conditions**: Web pass-through clients are anchored from foreign controller to anchor controller. **Workaround**: Reboot the controller.
CSCuf52235	**Symptom**: After you upgrade to Release 7.4, global user idle timeout is not used and all WLANs have an individual default user idle timeout of 300 seconds. **Conditions**: Controllers using Release 7.4 **Workaround**: Configure the user idle timeout for each WLAN.
CSCuf54559	**Symptom**: Controller stops responding. **Conditions**: When you use the **show mdns profile detailed default-mdns-profile** command. **Workaround**: Do not use this command.

Table 5 Open Caveats (continued)

ID	Description
CSCui30568	**Symptom**: Cisco WiSM2 in HA pair on Release 7.4.100.60 consistently keeps getting this error message every minute. `415 Wed Jul 24 13:52:28 2013 RF failure notification ErrorType: 32 Reason :Error: Config Sync failed on Standby for the usmdb:HA_send_usmDbApfMsDelete 416 Wed Jul 24 13:52:27 2013 RF failure notification ErrorType: 32 Reason :Error: Config Sync failed on Standby for the usmdb:HA_send_usmDbApfMsDelete 417 Wed Jul 24 13:52:27 2013 RF failure notification ErrorType: 32 Reason :Error: Config Sync failed on Standby for the usmdb:HA_send_usmDbApfMsDelete 418 Wed Jul 24 13:52:27 2013 RF failure notification ErrorType: 32 Reason :Error: Config Sync failed on Standby for the usmdb:HA_send_usmDbApfMsDelete 419 Wed Jul 24 13:52:27 2013 RF failure notification ErrorType: 32 Reason :Error: Config Sync failed on Standby for the usmdb:HA_send_usmDbApfMsDelete 420 Wed Jul 24 13:52:27 2013 RF failure notification ErrorType: 32 Reason :Error: Config Sync failed on Standby for the usmdb:HA_send_usmDbApfMsDelete 421 Wed Jul 24 13:52:27 2013 RF failure notification ErrorType: 32 Reason :Error: Config Sync failed on Standby for the usmdb:HA_send_usmDbApfMsDelete 422 Wed Jul 24 13:52:27 2013 RF failure notification ErrorType: 32 Reason :Error: Config Sync failed on Standby for the usmdb:HA_send_usmDbApfMsDelete 423 Wed Jul 24 13:52:27 2013 RF failure notification ErrorType: 32 Reason :Error: Config Sync failed on Standby for the usmdb:HA_send_usmDbApfMsDelete` **Conditions**: Unknown. **Workaround**: None. **Further Problem Description**: At present, this issue does not impact normal services and an HA failover works as expected. There are a total of 820 Cisco APs in this deployment and there are a couple of interference and load profile failures.
CSCui33284	**Symptom**: Upon attempting to the Open Authentication SSID that has MAC Filtering enabled, substantial packet loss is observed at a mobile endpoint. This packet loss can result in no-redirect for a client and marginal connectivity issues for the mobile endpoint. **Conditions**: Open Authentication on the SSID with MAC Filtering enabled. **Workaround**: If a client disconnects and then reconnects to the SSID, this has proven to temporarily mitigate the issue.
CSCui45546	**Symptom**: DTIM count randomly sets to ‘zero’ for Cisco AP1140 and AP1040. **Conditions**: Random radio hardware issue mostly seen in dense RF environments. Easily seen for DTIM period configuration 180-255. **Workaround**: Use another Cisco AP platform.

Table 5 Open Caveats (continued)

ID	Description
CSCui48291	**Symptom**: FlexConnect AP drops from the Cisco WLC and stops receiving traffic on GigabitEthernet0 interface until rebooted. At the time this issue is observed, the switchport connected to the Cisco AP remains operational and transmits and receives packets. The switch sees the Cisco AP as a CDP neighbor. When you access the Cisco AP console, the LAN interface is operational and transmits packets, but does not receive packets. **Conditions**: • Cisco AP3502 or AP1260 AP in FlexConnect mode. • Native VLAN ID does not match native VLAN on trunk to AP. • Cisco WLC using Release 7.3.112.0. **Workaround**: Reboot the affected Cisco AP.
CSCui55350	**Symptom**: The following messages are displayed continuously: `-Traceback: 0x10c31374 0x10c8a6a4 0x10c9ea08 0x10c94748 0x10c402d8 0x12283850 0x122f634c *rmgrMain: Aug 08 09:49:21.902: #OSAPI-5-MUTEX_UNLOCK_FAILED: osapi_sem.c:1036 Failed to release a mutual exclusion object. invalid(NULL) pointer passed. -Traceback: 0x10c30d9c 0x10c8a7f4 0x10c9ecf8 0x10c95d4c 0x10c402d8 0x12283850 0x122f634c *rmgrMain: Aug 08 09:49:21.902: #OSAPI-4-MUTEX_LOCK_FAILED: osapi_sem.c:1179 Failed to acquire a mutual exclusion object. invalid(NULL) pointer passed.` **Conditions**: • Cisco WLC Release 7.5 • AP SSO is in enabled state **Workaround**: Change the log level to filter out those messages—On the Cisco WLC GUI, choose **MANAGEMENT > Logs > Config > Msg Log Configuration**.
CSCui65225	**Symptom**: The 802.11k assisted roaming neighbor report is not returned upon a client request when the WLAN is mapped to an AP group. The following is the sample output of 802.11k debugs: `(""debug 11k all enable""): *apfMsConnTask_5: Aug 13 23:52:10.512: Received NEIGH_REQ from ms xx:xx:xx:xx:xx:xx d.token 14 *apfMsConnTask_5: Aug 13 23:52:10.512: Client WLAN 1 is not enabled for 802.11k neighbor list request request d.token 14 ignored` **Conditions**: • Cisco WLC using Release 7.4.110.0 or 7.5.102.0 • 802.11k neighbor list enabled on the WLAN (**config wlan assisted-roaming neighbor-list enable** *wlan-id* • AP groups are in use and the global WLAN ID does not match the position of the WLAN in the AP group configuration. **Workaround**: Use 802.11k on WLAN with an ID that is less than or equal to 16 either in the default group or where the AP group is configured to keep the WLAN in the same position as the global WLAN ID; for example, WLAN ID 2 is the second WLAN in the AP group.

Table 5 Open Caveats (continued)

ID	Description
CSCui65855	**Symptom**: Cisco WLC sends traffic from the virtual interface IP address onto the wired network outside of the CAPWAP tunnel. **Conditions**: • Clients connect to WLAN using an interface group • Cisco 5508 WLC with LAG in enabled state. **Workaround**: None.
CSCug04683	**Symptom**: Traceback appeared on the message log. **Conditions**: Unknown. **Workaround**: None.
CSCui73517	**Symptom**: Radio interface reset when the FlexConnect AP returns to the connected mode from the standalone mode. **Conditions**: This issue tends to occur if the Cisco AP moves to the secondary Cisco WLC from the primary Cisco WLC after AP continues to join to the primary one for a long time. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description

CSCui73764	**Symptom**: Cisco 1240 and 1130 Series APs—DHCP does not work with FlexConnect and VLAN Native 2.
	Conditions:
	• FlexConnect local switching
	• Cisco 1240 or 1130 Series APs
	• Cisco WLC Release 7.4.121.0 or earlier releases
	• VLAN Native 2
	• User unable to get IP address and to connect to the network
	Workaround: Change the native VLAN to an unexpectedly higher number, so no WLAN will ever get mapped to a bridge group number that high.
	Further Problem Description: Telnet to the FlexConnect mode AP. Example: VLAN3 is the native VLAN on the FlexConnect mode AP. The AP is correctly mapped to bridge group 1. The WLAN that does not work is the one that is mapped to VLAN2. VLAN2 is mapped to bridge group 3 (see below). This is the instance where the issues is encountered. It can be any WLAN-VLAN-Native VLAN combination.
	`interface FastEthernet0.1`
	`encapsulation dot1Q 3 native`
	`no ip route-cache`
	`bridge-group 1`
	`no bridge-group 1 source-learning`
	`bridge-group 1 spanning-disabled`
	`!`
	`interface FastEthernet0.2`
	`encapsulation dot1Q 1`
	`no ip route-cache`
	`bridge-group 2`
	`no bridge-group 2 source-learning`
	`bridge-group 2 spanning-disabled`
	`!`
	`interface FastEthernet0.3`
	`encapsulation dot1Q 2`
	`no ip route-cache`
	`bridge-group 3`
	`no bridge-group 3 source-learning`
	`bridge-group 3 spanning-disabled`

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 5 Open Caveats (continued)

ID	Description

CSCui77735	**Symptom**: Cisco 8510 WLC using Release 7.3.112.0 stopped working on taskname SNMPTask.
	Conditions: claPriorityOrder is set to 0 in SNMP set on Cisco Flex 7510 WLC, Cisco 8510 WLC, and Cisco vWLC.
	Example:
	`snmpset -v2c -c private 83.83.83.22 .1.3.6.1.4.1.9.9.598.1.1.1.1.2.1 u 0`
	`snmpset -v2c -c private 83.83.83.22 .1.3.6.1.4.1.9.9.598.1.1.1.1.2.2 u 0`
	`snmpset -v2c -c private 83.83.83.22 .1.3.6.1.4.1.9.9.598.1.1.1.1.2.3 u 0`
	`2.1 = Local 2.2 = Radius 2.3 = TACACS 0 1 2 = priority. 0 = None - where crash is happening. 1 2 = Either first or second (8510-2) >show aaa auth`
	`Management authentication server order:`
	`1..... local`
	`2..... radius On 5508 value of 0 will be taken. The box won't crash.`
	Workaround: Do not set claPriorityOrder to 0 when this MIB is used.

CSCui87160	**Symptom**: Cisco 5500 Series WLC stopped working due to an issue with the kernel. **Conditions**: Memory leak. **Workaround**: None.
CSCui94634	**Symptom**: Cisco APs in FlexConnect local switching mode with VLAN mapping dissociate from the 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 the Cisco WLC are not as per expectations with duplicate sequence number errors. Eventually, this state causes a DTLS timeout and the rejoin process on the Cisco AP fails over and over with same issue. It appears that the issue is related to incorrect CAPWAP private configuration as the actual content of the ACL does not matter. The issue occurs immediately at the point when the ACL is pushed. **Conditions**: • FlexConnect mode APs with VLAN mappings and FlexConnect ACL. • When AP is on low free flash space **Workaround**: Do not apply ACL to the Cisco AP. Use another enforcement point if required. A reimage of the Cisco AP with 15.2 recovery image.
CSCuj13054	**Symptom**: Cisco WiSM2 stopped working after an upgrade from Release 7.3.101.0 to 7.4.110.0. **Conditions**: Upgrade. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCuj15593	**Symptom**: Backed up Cisco WLC configuration with RF profile commands cannot be uploaded to another Cisco WLC. **Conditions**: Cisco WLC configuration with RF profile commands. **Workaround**: Open the configuration file in a text editor and find the commands related to RF profile This issue occurs when the commands for RF profile data rates, transmit power, and so on, occur before the command that actually creates the RF profile. For example, you may see something like this: **config rf-profile data-rates 802.11a mandatory 6 test** **config rf-profile data-rates 802.11a supported 9 test** **config rf-profile create 802.11a test**. Move the **create** command before any of the other commands related to the RF profile. Therefore, the above should be changed to the following: **config rf-profile create 802.11a test** **config rf-profile data-rates 802.11a mandatory 6 test** **config rf-profile data-rates 802.11a supported 9 test** Download the new configuration to the Cisco WLC. **Further Problem Description**: Cisco WLC Release 7.4.110.0. Create a configuration backup with RF profile configuration and then upload it to another Cisco WLC. The operation fails with the following message displayed: `*TransferTask: Sep 05 18:05:52.951: RESULT_STRING: Error: There cannot be multiple maps for the field 58.1.5.0 Config CLI:config rf-profile data-rates 802.11a disabled 6 test123”`
CSCuj26067	**Symptom**: Sporadically, RADIUS authentications to certain Cisco APs in FlexConnect mode fail while other authentication methods on the same Cisco AP are unaffected. **Conditions**: Cisco 8510 WLC using Release 7.4.110.0. Cisco AP3600 in FlexConnect mode configured in a FlexConnect group with a ‘backup RADIUS’ server pointing to a Microsoft NPS RADIUS server. **Workaround**: Reloading the Cisco AP corrects the issue for some time.
CSCuj35236	**Symptom**: Changing a parameter on an SSID causes issue in FlexConnect APs if another SSID exists with a different profile. **Conditions**: FlexConnect multiple WLANs with the same SSID. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
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.
CSCuj58556	**Symptom**: Cisco AP disconnects from the primary WLC and moves to the secondary WLC due to memory allocation. **Conditions**: Unknown. **Workaround**: Reboot AP.
CSCuj58625	**Symptom**: Cisco WLC unresponsive with local EAP-FAST in use. **Conditions**: Cisco WLC is performing local EAP-FAST. **Workaround**: Use an external RADIUS server.

Table 5 Open Caveats (continued)

ID	Description

CSCuj70166	**Symptom**: AP dissociates from Cisco WLC when %DOT11-2-NO_CHAN_AVAIL_CTR occurs.
	`Log details:`
	`DOT11-2-NO_CHAN_AVAIL_CTRL: Interface Dot11Radio1 no channel available.`
	`DTLS_CLIENT_EVENT: local_in_addr_comp: Client and server addresses of 2 nodes are AC190D09 BDAF AC190C01 147E : AC190D09 BDAF AC190C01 147E`
	`DTLS_CLIENT_EVENT: dtls_disconnect: Disconnecting DTLS connection 0x4369A0C`
	`DTLS_CLIENT_EVENT: dtls_connectionDB_del_connection: Connection deleted AC190D09 BDAF AC190C01 147E -----`
	Conditions: %DOT11-2-NO_CHAN_AVAIL_CTR occurs after DFS detects.
	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`
CSCuj84379	**Symptom**: Cisco WLC stops responding and then reboots. **Conditions**: When ad hoc rogue detection is enabled. **Workaround**: Disabling ad hoc rogue detection is a potential workaround.

Table 5 Open Caveats (continued)

ID	Description
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.
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.

Table 5 Open Caveats (continued)

ID	Description
CSCuj93777	**Symptom**: In very rare situations, there is a racing condition that data packets are sent before switchport receiving BPDU packets from the wireless side cause MAC address flapping. **Conditions**: STP to break network loop mesh AP reboot or moving between RAPs intensive packets flooding in network to cause packets are sent before BPDUs are propagated. **Workaround**: None.
CSCuj91880	**Symptom**: Captive Portal pops up even when Captive Portal Bypass is enabled for certain clients such as Samsung Galaxy Note 3 (using JellyBean 4.3) or MS Surface Pro (Windows 8). **Conditions**: This issue occurs only for some client such as Surface Pro and Samsung Galaxy Note 3 when trying to provision the clients on a dual SSID BYOD Provisioning Setting. **Workaround**: None.
CSCuj97293	**Symptom**: Cisco WLC stops responding when the **show local-auth certificates** commands is entered. **Conditions**: Unknown. **Workaround**: None.
CSCul16796	**Symptom**: Client is using PEAP; the EAP handshake fails when the Cisco vWLC needs to send the server certificate. **Conditions**: Using a Cisco vWLC and an EAP method that requires certificates. The path MTU between the Cisco vWLC and the Cisco AP is 1200 bytes or less. **Workaround**: Increase the path MTU. **Further Problem Description**: This is a regression; the issue was not observed in Release 7.4.X.
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.
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.

Table 5 Open Caveats (continued)

ID	Description
CSCul43813	**Symptom**: Performing a filter using either "WLAN Profile" or "WLAN SSID," multiple clients and pages are displayed. The first page shows the maximum allowable information for that page. However, when you want to navigate to the subsequent pages, a "No clients found" message is displayed. **Conditions**: Include either "WLAN Profile" or "WLAN SSID" as the filter option. **Workaround**: None.
CSCuj89107	**Symptom**: Cisco WLC stopped working with the Task Name: spamApTask7 on Release 7.4.115.0. `********** * Start Cisco Crash Handler * ********** Sys Name: WLC-Campus-9 Model: AIR-CT5508-K9 Version: 7.4.115.0 Timestamp: Wed Oct 16 15:47:22 2013 SystemUpTime: 0 days 1 hrs 20 mins 41 secs signal: 10 pid: 1070 TID: 1030415184 Task Name: spamApTask7 Reason: System Crash si_signo: 10 si_errno: 0 si_code: 128 si_addr: 0x0 timer tcb: 0x845 timer cb: 0x10e76e80 ('alarmSendMsgToMsgTask 48') timer arg1: 0x0 timer arg2: 0x0 Long time taken timer call back inforamtion: Time Stamp: Wed Oct 16 14:45:33 2013 timer cb : 100ee078p('apfMsSessionExpireCallback 456') Duration : 745922 usecs cbCount= 5 ---------- Analysis of Failure: Software Failed on instruction at : pc = 0x102bd2f0 (usmDbSpamGetUpTime 72) ra = 0x10dd0d70 (usmDbSpamGetUpTime 72) Software Failed while accessing the data located at :0x0 ---------- System Stack Frame 0: 0x10012e90 create_crash_dump 7156 Frame 1: 0x10011c88 create_crash_dump 2540 Frame 2: 0x10007cfc sigsegv_handler 6168 Frame 3: 0x3d6acea0 license_xos_thread_create 730498928 Frame 4: 0x102bd2f0 spamGetUpTime 88 Frame 5: 0x10dd0d70 usmDbSpamGetUpTime 72 Frame 6: 0x10be4b9c trapMgrLwappApAssociatedTrapSend 372 Frame 7: 0x10452098 acPostDecodeConfigRequest 1816 Frame 8: 0x10459740 acCapwapSmInit 18536 Frame 9: 0x1045338c acPostDecodeConfigRequest 6668 Frame 10: 0x10460b3c capwapAcStatemachine 532 Frame 11: 0x10f86254 spamApReceiveTask 668 Frame 12: 0x10b07be8 osapiTaskAppKeySelfSet 304 Frame 13: 0x12020500 license_xos_thread_create 2211280 Frame 14: 0x12080eac license_xos_thread_create 2606972` **Conditions**: Unknown. **Workaround**: None.
CSCul72669	**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 msg** command outputs indicate the messages are sent out. **Conditions**: RLDP is enabled on a lightweight Cisco AP. **Workaround**: Disable RLDP.

Table 5 Open Caveats (continued)

ID	Description
CSCul78541	**Symptom**: AAA override client gets assigned to dynamic interface on roam. **Conditions**: As an extension to CSCui50515 on Release 7.4.X, WLAN using WPA2 AES, MAC Filter PSK, AAA override gets defaulted to dynamic interface on WLAN instead of AAA overridden VLAN value upon a roam. The Cisco APs are in local mode and associated with the same Cisco WLC. A new association to the Cisco AP or removing client entry from the Cisco WLC resolves the issue and the client gets AAA overridden VLAN again when fast-SSID change is disabled. **Workaround**: Enabling fast-SSID change resolves the issue and assigns the client the correct AAA-override VLAN on roam.
CSCuf74326	**Symptom:** On successful installation of Cisco WLC licenses access points are unable to join the controller as the web-user interface displays supported access points as none. However, when you execute the show license summary command using the CLI, the exact count of licenses in use is displayed. **Conditions:** Occurs when you install adder license file on the controller without installing the base licenses. **Workaround:** Contact Cisco Support for installing the base licenses of the controller.

CSCuf77488	**Symptom:** The FT and LT detection time for an alarm is ahead or later than the AP clock. This is causing a delay in 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 you will not see the alarm until the actual AP time matches the time reported in the FT.
	
	Conditions: This occurs in Cisco Wireless LAN Controller 5508 series with release 7.0.235.3, and Cisco Aironet 3500 series wIPS ELM mode, MSE 3350 on release 7.0.201.204.
	
	Workaround: None.

Table 5 Open Caveats (continued)

ID	Description
CSCuf77821	**Symptom:** A vulnerability in the web interface of the Cisco Wireless LAN Controller (WLC) could allow an unauthenticated remote attacker to execute a cross-frame scripting (XFS) attack. An attacker could exploit the vulnerability of insufficient HTML iframe protection and can direct users to an attacker-controlled web page with a malicious HTML iframe. The application allows users to perform certain actions via HTTP requests via iframes without performing any validity checks to verify the requests. **Conditions:** Device configured with default configuration. **Workaround:** None.
CSCug14709	**Symptom:** In Cisco WLC Release 7.4, the Cisco WLC does not respond when an "airespace wlan-identifier" attribute is sent back in an access-accept by the RADIUS server. **Conditions:** This issue exists in the Cisco WLC Release 7.4. **Workaround:** Use another mechanism to restrict SSID access.
CSCug14713	**Symptom:** RADIUS accounting update is seen twice from the controller when initial authentication occurs for RADIUS NAC-enabled WLAN. **Conditions:** This issue occurs when RADIUS NAC is enabled. **Workaround:** None.
CSCug19563	**Symptom:** Wism2 secondary controller DP crashed due to a deadlock in high availability configuration while boot and synchronization with the primary controller. **Conditions:** The secondary controller DP crash occurs only when there are multiple reboots of the controller in a high availability configuration. The controller recovers after the reboot. **Workaround:** None.
CSCug21736	**Symptom:** Cisco LAP1131 and LAP 1132 access points may experience a memory leak when a SIP phone roams from one access point to another while in an active call. This issue occurs when the handset sends multiple re-association messages when connecting to the new AP while in roaming. As a result of this bug, an authenticated adjacent attacker can trigger a memory loss and eventual cause the AP to reboot. **Conditions:** SIP Handsets that send multiple reassociation messages when roaming can trigger this issue. **Workaround:** None.
CSCug26521	**Symptom:** When using controller with Release 7.4 and DHCP proxy enabled, the packets were dropped during inspection because the option 255 is missing in the DHCP request packets sent out by the controller. **Conditions:** This issue occurs in the Cisco Wireless LAN Controller using release 7.4. **Workaround:** Convert the DHCP opt 82 format from binary to ASCII value using the **config dhcp opt-82 format ascii** command.

Table 5 Open Caveats (continued)

ID	Description
CSCug38794	**Symptom:** Cisco WiSM2 stops working and then reboots. **Conditions:** • Buffer corruption • Low frequency issue, under investigation **Workaround:** None.
CSCug40463	**Symptom:** A Cisco AP might stop transmitting traffic after several days with a switch port speed/duplex misconfiguration. **Conditions:** This issue exists on Cisco Aironet 2600 Series access points that are associated with a controller using software release 7.3.112.0 or with an autonomous Cisco IOS software release15.2(2)JA. The default Ethernet interface of the Cisco Aironet 2600 series access points is auto/auto; and switch port: duplex full/ speed 100. **Workaround:** Correct the speed/duplex misconfiguration in a manner that the configuration match the access point and the switch port.
CSCug57436	**Symptom:** In Cisco 3502 mesh access point the bridging does not exclude gig0 failing to join over radio. **Conditions:** Cisco 3502 Mesh when configured as a map with the bridging enabled connected behind a switch and a reboot on the map happens. **Workaround:** You must shut down the switch port so that the access points will join over the radio interface.
CSCug64950	**Symptom:** Modification of the access point group to a RAP which is currently connected through the radio backhaul interface—RAP in MAP mode as the wired uplink is down strands the RAP. **Conditions:** Occurs when a Cisco mesh access point such as 1552 or 1522 operates as an access point (root) without any wired backhaul interface available. This issue exists on the Cisco Wireless LAN Controller using release 7.0.x. **Workaround:** You must clear the CAPWAP private configuration using the **clear capwap private-config** command and reboot the access point.
CSCug73845	**Symptom:** Cisco Wireless LAN Controller NAS-identifier override is taking system name instead the NAS-identifier configured on an access point group, WLAN, or interface. **Conditions:** Configure an AP group, WLAN, or interface NAS-ID. **Workaround:** None.

Table 5 Open Caveats (continued)

ID	Description

CSCug88172	**Symptom:** Cisco Aironet 1600 series access points transmits TKIP packets with MIC errors. The errors are reported and traffic disrupted. The following message log is displayed:
	`*Dot1x_NW_MsgTask_7: Oct 11 06:17:21.387:`
	`#DOT1X-3-WPA_KEY_MIC_ERR: 1x_eapkey.c: 618`
	`TKIP MIC errors reported in EAPOL key msg from client 00:11:22:33:44:55`
	Conditions: This issue exists on Cisco Aironet 600 series access points that use TKIP encryption method.
	Workaround: You must ensure sage of AES encryption methods instead of TKIP encryption methods.

CSCug92421	**Symptom:** Controller reports stale client entries in large numbers. **Conditions:** This issue exists on Cisco Wireless LAN Controller when numerous clients use FlexConnect access point local authentication while in connected mode. **Workaround:** Do not use FlexConnect local authentication while in connected mode.
CSCug73660	**Symptom:** Cisco Aironet 1600 series access points should have 17dbm of transmission power on one antenna and transmission power up to 22dbm with three antennas. However the **show controllers** command output displays that power level 1 is 13dbm on 3 antennas (8dbm per antenna). The output displayed is correct for the given AP/domain/radio/channel. However, modifying the antenna gain has no effect on the transmission power. **Conditions:** This issue exists in the Cisco Wireless LAN Controller release 7.4.100. European regulatory domain in countries where the expected power level is 17. **Workaround:** You must configure the radio to reduce its power as required if the configured antenna gain would cause the EIRP to exceed regulatory limits. The maximum power allowed is dependent upon: 1. The AP model 2. The AP domain 3. The radio 4. The specific channel in use 5. The number of antennas in use 6. The configured antenna gain To find the specific allowed power levels of interest, see the Channels and Maximum Power Settings document for the selected AP. On verification for the document, you will find that the maximum power settings are correct—except that the configured gain does not limit the allowed power. This bug is thus fixed by having the configured antenna gain limit the transmit power."

Table 5 Open Caveats (continued)

ID	Description
CSCug83271	**Symptom:** Cisco Virtual Wireless LAN Controllers fail to properly implement virtual CPU access control lists that have been configured to restrict access to the private virtual management address. **Conditions:** This issue exists on Cisco Virtual Wireless LAN Controllers with controller software release 7.4. **Workaround:** None. **Further Problem Description:** This issue does not allow an intruder to bypass any forms of authentication. However, if an attacker accesses the private virtual management interface, the controller prompts them to provide valid credentials to gain access.
CSCug86995	**Symptom:** Configuration of an external NAT IP state and address in management interface using the Cisco WLC GUI is available in SRE controller. However, access points in public domains cannot join the controller as the discovery response of the controller includes only the private address of the controller. To enable or disable NAT IP address for access point discovery, you must use the **config network ap-discovery nat-ip-only {enable | disable}** command in the command line interface of the controller. **Conditions:** None. **Workaround:** Refrain from placing the SRE-WLC behind NAT even though the controller web UI allows you the configuration. This configuration is currently unsupported in the controller.
CSCuh11409	**Symptom:** A RAP connected through radio backhaul interface while the wired backhaul interface is down can be stranded by manually disabling the 11a backhaul interface. The controller should prevent this configuration to be pushed as in Mesh APs (role MAP). **Conditions:** This issue exists on Cisco Wireless LAN Controller using release 7.0.240.4 with Mesh AP (tested with 1552 and 1522 models) in role Root AP with no wired backhaul interface available. **Workaround:** Use the **clear capwap private-config reload** command to clear the CAPWAP private configuration using the command line interface.
CSCuh16842	**Symptom:** Client gets IPv6 address from different VLAN. **Conditions:** This issue occurs due simultaneous occurrence of the following: 1. Interface group 2. Client sends traffic from either the static IP address or a previously allocated IP address. 3. Client traffic does not matching the traffic received by the assigned VLAN initially. The following message will be displayed when this occurs “Overriding interface of client from ‘vlan20’ to ‘vlan30’ within interface group ‘vlan20-30’”. **Workaround:** Use DHCP required to join a VLAN.

Table 5 Open Caveats (continued)

ID	Description
CSCuh20155	**Symptom:** A Cisco Aironet 3600 or 2600 series access points fail to boot the Cisco IOS software and the access point stays at the boot loader prompt —the ap prompt. **Conditions:** The Cisco AP moves to standalone mode and is power cycled. **Workaround:** Perform the following steps: 1. Initialize the Cisco AP, to do this enter the **ap: flash_init** command at the ap prompt. 2. Reboot the access point to load a new image, to do this enter the **ap: boot** command at the ap prompt. 3. Upgrade the bootloader of the access point to the Autonomous AP IOS Software release15.2(4)JA1 or later. To upgrade the bootloader: Copy the bootloader image onto AP flash. To do this, execute the **copy flash:/BOOTLOADERFILENAME bs:** command at the ap prompt.
CSCuh42665	**Symptom:** Cisco Wireless LAN Controller sends incorrect information while detecting rogue access points using traps. **Conditions:** This issue exists only in the Cisco Wireless LAN Controller using Release 7.4. **Workaround:** None.
CSCuh46355	**Symptom:** Cisco Wireless LAN Controllers that have been configured for high availability may crash when a second node is added to the HA cluster. The error message displayed indicates a crash in SNMPTask. **Conditions:** This issue exists for Cisco Wireless LAN Controllers that use an affected version of controller software release is configured for high availability. **Workaround:** None.
CSCuh46996	**Symptom:** Wired device such as scale behind a third party bridge device fails to get an IP address. **Conditions:** This issue occurs when third party bridge is associating to an access point in the HREAP/FlexConnect local switching mode and controller uses a software release later than the release 7.0.116.0. **Workaround:** None.

CSCuh47502	**Symptom:** Controller displays non-valid scrolling messages.
	`*DHCP Server: Jun 12 12:59:29.966: adding option 0x35`
	`*DHCP Server: Jun 12 12:59:29.966: adding option 0x36`
	Conditions: This issue occurs when the debug of DHCP messages that are exchanged to and from the DHCP server is enabled.
	Workaround: Disable the debug of DHCP messages that are exchanged to and from the DHCP server using the **debug dhcp message disable** command in the controller command line interface.

Table 5 Open Caveats (continued)

ID	Description
CSCuh50505	**Symptom:** WiSM2 controller crashes and reboots. **Conditions:** This issue occurs when TPCv2 is enabled in the WiSM2 controller. **Workaround:** You must disable TPCv2.
CSCuh52238	**Symptom:** Controller detects false positive Dynamic Frequency Selection Detections (DFS) owing to signals transmitted by Broadcom radios. **Conditions:** Clients trigger DFS detections due to spurious emissions. This commit tracks additional filtering Cisco can do from their side to help with DFS falsifying. The commit as per customer site information helps with DFS falsifying about 30% of the time. Broadcom is also working on a fix from their side as well to fix the root issue. **Workaround:** You must use non-DFS channels for transmission.
CSCuh56733	**Symptom:** Cisco Aironet 1550 series access points are unable to configure transmit power greater than 20dbm while in autonomous mode. **Conditions:** Unknown. **Workaround:** None.
CSCuh68059	**Symptom:** Cisco Aironet 1300 and 1400 series Access Points crashes after some period of operation. The crash file reports an error in the REAP process and occurs when a heavily loaded access point performs a cleanup of the time-out sessions. **Conditions:** Cisco Aironet 1300 and 1400 series APs connected to a Cisco Wireless LAN controller using an affected version of controller software release. **Workaround:** None. **Further Problem Description:** This issue is specific to the affected access points and is not triggered by any external means. The crash occurs on APs that are heavily loaded and experience a significant number of connections which are timed-out.
CSCuh72474	**Symptom:** Controller marks an interface in a group as dirty even when a response is received from the DHCP server. This issue is observed when clients insist on requesting an IP outside of their connected interface range in a flood (more than 100 DHCP request in the same second). The DHCP server start slowing down the responses as a result of this flood. The interface gets marked as Dirty as the dirty marking is based on requests without responses. **Conditions:** Clients insist on requesting an IP address outside their range using flood way. **Workaround:** None
CSCuh76898	**Symptom:** Client communication fails when access point joins a controller and then tries to join another controller while in FlexConnect local switching mode with disabled VLAN support. **Conditions:** None. **Workaround:** Turn on/off the radio of the client adapter.

Table 5 Open Caveats (continued)

ID	Description
CSCuh97457	**Symptom:** Controller displays incompatibility behavior on Cisco controller incompatibility behavior on Change-of-authorization (CoA) for RFC 3576 implementation and shows the debug output error 'RFC-3576 Disconnect-Request' which indicates that session identification attributes are invalid. The following error message is displayed: `Error cause 402 generated for 'RFC-3576 Disconnect-Request' from 192.168.1.5 (Session Identification attributes not valid)` **Conditions:** Change-of-authorization (CoA) on the controller. **Workaround:** The controller accepts the disconnect request when the three AVP pair attributes are sent— Calling-Station-ID MAC address of device (lower case works), Service-Type Login-user, and the Called-Station-ID (upper case MAC of AP SSID separated by colons).
CSCuh99194	**Symptom:** A client's first attempt to associate is unsuccessful; the second attempt is successful. **Conditions:** This issue occurs when the maximum number of clients per AP radio is configured on each Cisco Aironet 1142 series Access Point. **Workaround:** None.
CSCui09037	**Symptom:** Update for Client IP on controller does not happen after the 7.3.101.0 software release upgrade. **Conditions:** This issue exists in Cisco Wireless LAN Controller release 7.3.101.0 when WLAN is used for a locally switched H-REAP RADIUS authentication of mobile device when the DHCP server is central. **Workaround:** You must wait for 20 to 30 minutes for synchronization to complete.
CSCui15110	**Symptom:** After adding a WLAN to an AP group, the WLAN properties cannot be edited on the AP VLAN mapping page when the AP is in FlexConnect mode. **Conditions:** This issue occurs when you disable WLAN before adding it to the AP group. **Workaround:** 1. Enable the WLAN before adding to AP group. 2. Add another enabled WLAN. 3. Reboot the Cisco AP.

CSCui18377	**Symptom:** Crash errors, traceback conditions, and radio reset errors displayed in Cisco Aironet 1240AG series after the controller upgrades to software release 7.4.100.60.
	`log Jul 10 06:02:54.569:`
	`%SYS-2-BADSHARE: Bad refcount in datagram_done  > ptr=125F318  count=0`
	`-Traceback= <HEX Tracebacks>`
	Conditions: This issue exists on Cisco Wireless LAN Controller while upgrading to the 7.4.100.60 software release.
	Workaround: None.

Table 5 Open Caveats (continued)

ID	Description
CSCue42242	**Symptom**: When the Cisco WLC detects more than 21 ad hoc rogues, the web GUI shows only the first 20 entries (first page). **Conditions**: Path on the web GUI: Monitor > Rogue > Adhoc Rogues and click on "Unclassified Adhoc" or "Custom Adhoc". The first page shows correctly, but it is not possible to browse to the subsequent pages. **Workaround**: Use the **show rogue adhoc summary** command on the CLI.
CSCuf56192	**Symptom**: Unable to delete an mDNS profile. **Conditions**: When the mDNS profile is mapped to an interface and the interface is deleted. **Workaround**: Before deleting the interface, detach the profile and then delete the interface.
CSCuc72713	**Symptom**: Static IP on clients working with interface group VLAN select feature gets assigned to an incorrect interface. **Conditions**: Though the static IP subnet exists as a valid interface, it does not get overridden to the correct subnet interface and gets marked into mac-hash interface and the client is unable to pass traffic. **Workaround**: Enter the **config ipv6 disable** command.

Resolved Caveats

Table 6 lists the caveats that are resolved in this release.

Table 6 Resolved Caveats

ID	Title
CSCuj12935	Cisco WiSM2 stopped working on Release 7.4.110.0 with memory allocation issues at load
CSCuh81880	A vulnerability in the CAPWAP protocol of the Cisco Wireless LAN Controller Series of products could have allowed an unauthenticated remote attacker to cause a denial of service condition (DoS).
CSCul65002	Cisco WLC frequently stopped working silently @ewaFormSubmit_exp_list with Release 7.4.110.0
CSCul68057	CF driver change for Cisco 5500 Series WLC and Cisco WiSM2
CSCuh71233	FlexConnect Stress Test: SYS-2-INTSCHED - all interrupts disabled
CSCul50441	Cisco AP stopped working
CSCui11302	Write the image directly into flash
CSCuj88982	Multicast failed sometimes
CSCuj99846	Cisco WLC HA: Incorrect mesh AP count after an HA failover
CSCul20597	Local EAP stopped working after FTP configuration upload
CSCul55930	Cisco 8500 Series WLC stopped working

Table 6 Resolved Caveats (continued)

ID	Title
CSCud10611	Client exclusion notifications should have been sent only to Cisco APs in the group
CSCul25937	Trap Scale improvements required for client association
CSCul63384	Cisco WLC stopped working on Bonjour_Process_Task
CSCuj64462	Cisco AP radio flapping with CleanAir not in operational state
CSCue20209	CleanAir was unable to report interference
CSCue88466	SC2 radio firmware download failed CRC check cmd for certain image sizes
CSCui84582	Bcast queue was full when IGMP was in disabled state. “RX Multicast Queue Full”
CSCul30051	Clients failed authentication (PSK/802.1X) due to uncreated 802.1X interface for Cisco AP
CSCud69687	Cisco 5500 Series WLC: AP count was not reflected correctly in the output of the **show ap summary** command.
CSCul22530	Reaper unresponsive on Bonjour_Msg_Task
CSCui36121	Cisco AP stopped working in dot11_driver_timer_expiry() after AES-CCMP TSC replays
CSCui82573	Double AID allocation in OKC Fast Roaming in FlexConnect
CSCud09069	Unable to add IP mask with 0.0.0.0
CSCue49527	Cisco WLC should have deleted the session ID from PMK cache when a client was removed
CSCui50515	DHCP proxy selected an incorrect IP address after using cached AAA override values
CSCul16913	Massive AP radio’s transmission power changed when the system was overheated
CSCul26859	Cannot disable RADIUS authentication and accounting for WLAN using Cisco WLC GUI
CSCul27717	Cisco APs dissociated in a large scale setup when debug commands were used
CSCui66891	Marvell-based radio stopped working due to issues with multicast packets in driver
CSCuj36260	Could not disable mDNS snooping on WLAN with local switching after upgrade
CSCuj87123	Cisco WLC stopped working when license was being installed
CSCuf16416	802.11h client was deauthenticated in a non-DFS channel after a DFS simulation
CSCue59791	VPN performance on Cisco AP3600s was not as per expectations
CSCuj12898	Cisco WiSM2 stopped working on Bonjour_Msg_Task
CSCuh25556	Incorrect Fix Aggr Sched AVL tree stops working with design change to doubly-LL
CSCui26351	Default route to BVI1 might have stayed on routing table
CSCui43621	Cisco 1552E AP: FlexConnect gig fiber port did not pass DHCP to wireless client
CSCue25685	Wi-Fi Direct did not authenticate with Cisco 8500 Series WLC
CSCui25170	Cisco APs were unable to associate with the new Cisco WLC. The Management interface was not reachable (BUFFER_POOL_LOW_DETECTED).
CSCui55610	Incorrect status code returned for invalid FT IE MIC
CSCui58670	Cisco WLC sends M5 key with protected flag = 0 for an 802.11r SSID after a roam
CSCuj21417	AID leak caused stale client entries on Cisco WLC

Table 6 Resolved Caveats (continued)

ID	Title
CSCuj25911	Cisco WLC Release 7.4.110.0: RRM queue was full
CSCuj28718	Cisco WiSM2 using Release 7.4.110.0 stopped working with “osapiReaper” task suspended.
CSCud41334	MAP Ethernet bridged client did not work
CSCuj46010	DTLS connections were dropped regularly that caused APs to dissociate from Cisco WLC
CSCuj17884	Memory leak was observed on HA AP SSO
CSCuj18674	Captive Portal/WISPr support for Apple iOS7
CSCuc65606	Cisco WLC stopped working in spamreceive on Release 7.0.235.3
CSCud26706	HA: Peer service port routes were not shown after a switchover on Cisco 8510 WLC
CSCue34115	Cisco 1552C cable modem AP’s Gig Ethernet Link became nonoperational
CSCug53945	Disabled radio was enabled after AP reload when AP group used RF profile
CSCug97769	Device behind MAP was unreachable after a high AP uptime. Rebooting the AP fixed the issue.
CSCuh08009	WPA2-PSK MAC Filter assign interface was incorrect after a client roaming
CSCui05324	Cisco AP1242 AP radio stopped transmitting (Transmit Queues Are Full)
CSCui20773	Bcast queue was full (“RX Multicast Queue Full”)
CSCui25877	Cisco AP1600: Radio reset due to ‘AMPDU attempt without BA setup from host’
CSCui41685	Required show command support in Cisco WLC CLI for Reap Payload
CSCui59553	Required command to disable or customize dead GW detection for HA
CSCui60915	Mesh APs caused MAC flapping and loop on the switch
CSCul94742	Cisco WLC stopped working because of incorrect memory
CSCul58609	With AVC enabled, a dataplane exception issue was observed.

Installation Notes

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

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

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

The controller must be installed by a network administrator or qualified IT professional, and the proper country code must be selected. Following installation, access to the controller 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 additional information about the Cisco controllers and lightweight access points, see these documents:

- The quick start guide or installation guide for your particular controller or access point
- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless LAN Controller System Message 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, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

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