Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.4.110.0

First Published: August 2013
Last Updated: February 2014
OL-28134-03

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

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 Unified Wireless Network Solution Components

The following components are part of the Cisco UWN Solution and are compatible in this release:

Note For more information on the compatibility of wireless software components across releases, see the *Cisco Wireless Solutions Software Compatibility Matrix*.

- Cisco IOS Release 15.2(2)JB2
- Cisco Prime Infrastructure 1.3 and later releases
- Mobility Services Engine (MSE) 7.4.110.0 software release and context-aware software

Note Client and tag licenses are required to get contextual (such as location) information within the context-aware software. For more information, see the *Release Notes for Cisco 3350 Mobility Services Engine for Software Release 7.4.100.0*.

- Cisco 3355 Mobility Services Engine, Virtual Appliance
- 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 Virtual Wireless Controllers on Cisco Services-Ready Engine (SRE) or Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (UCS-E)
- Cisco Wireless Services Module 2 (WiSM2) for Catalyst 6500 Series switches
- Cisco Aironet 1550 (1552) series outdoor 802.11n mesh access points; Cisco Aironet 1520 (1522, 1524) series outdoor mesh access points
- Cisco 1040, 1130, 1140, 1240, 1250, 1260, 1600, 2600, 3500, 3500p, 3600, Cisco 600 Series OfficeExtend Access Points, AP801, and AP802

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 7.4.110.0, you must upgrade the software in the Next Generation Cisco 880 Series ISRs to Cisco IOS 151-4.M or later releases.

Controller Platforms Not Supported

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 Wireless LAN Controller software on Cisco Services-Ready Engine (SRE) running on ISM 300, SM 700, SM 710, SM 900, and SM 910
- 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	7.4.110.0	—
	AIR-CAP1602I-xK910	7.4.110.0	—
	AIR-SAP1602I-x-K9	7.4.110.0	—
	AIR-SAP1602I-xK9-5	7.4.110.0	—
	AIR-CAP1602E-x-K9	7.4.110.0	—
	AIR-SAP1602E-xK9-5	7.4.110.0	—
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 7.4.110.0

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 7.4.110.0 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 7.4.110.0 release.
- While a client sends an HTTP request, the Controller intercepts it for redirection to login page. If the HTTP request intercepted by Controller is fragmented, the Controller drops the packet as the HTTP request does not contain enough information required for redirection.
- 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 7.4.110.0 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 7.4.110.0. Table 2 shows the upgrade path that you must follow before downloading software release 7.4.110.0.

Table 2 Upgrade Path to Controller Software Release 7.4.110.0

Current Software Release	Upgrade Path to 7.4.110.0 Software
7.0.98.0 or later 7.0 releases	You can upgrade directly to 7.4.110.0 **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 7.4.110.0 to avoid losing those VLAN settings.
7.1.91.0	You can upgrade directly to 7.4.110.0
7.2. or later 7.2 releases	You can upgrade directly to 7.4.110.0 **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 7.4.110.0 controller software release. You must downgrade from the 7.4.110.0 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 7.4.110.0

- 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 7.4.110.0 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 7.4.110.0. 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 7.4.110.0 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 7.4.110.0 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 7.4.110.0 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 7.4.110.0 (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 7.4.110.0 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 Disable any WLANs on the controller.

Step 6 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 7 From the File Type drop-down list, choose **Code**.

Step 8 From the Transfer Mode drop-down list, choose **TFTP**, **FTP**, or **SFTP**.

Step 9 In the IP Address text box, enter the IP address of the TFTP, FTP, or SFTP server.

Step 10 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 11 In the File Path text box, enter the directory path of the software.

Step 12 In the File Name text box, enter the name of the software file (*filename*.aes).

Step 13 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 14 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Step 15 After the download is complete, click **Reboot**.

Step 16 If prompted to save your changes, click **Save and Reboot**.

Step 17 Click **OK** to confirm your decision to reboot the controller.

Step 18 Reenable the WLANs.

Step 19 For Cisco WiSM2 on the Catalyst switch, check the port channel and reenable the port channel if necessary.

Step 20 If you have disabled the 802.11a/n and 802.11b/g/n networks in Step 4, reenable them.

Step 21 To verify that the 7.4.110.0 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 21 detailed in the "Upgrading to Controller Software Release 7.4.110.0" section on page 7.

Interoperability With Other Clients in 7.4.110.0

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	7.4.110.0
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 7.4.110.0. 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.

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

https://tools.cisco.com/bugsearch/

To become a registered cisco.com user, go to the following website:

https://tools.cisco.com/IDREG/guestRegistration.do?locale=en_US

Open Caveats

Table 5 lists the open caveats in this release.

Table 5 Open Caveats

ID	Description
CSCud47264	**Symptom**: Controller web GUI displays duplicate domain IP names, but the controller CLI displays them correctly. Use CLI **Condition**: When the service provider domain name is more than 32 characters, the controller web GUI displays duplicate entries. This issue occurs in only the controller web GUI. **Workaround**: Use controller CLI.
CSCud48146	**Symptom**: On the controller, when limiting the "Max Concurrent Logins for a user name" to 1, for example to avoid using the same username more than once for web authentication, there is a possibility to ignore this setting for 802.1x authentication by setting "max-login-ignore-identity-response" to the enabled state. The "max-login-ignore-identity-response" feature does not work as expected and the global "Max Concurrent Logins for a user name" still takes precedence. **Condition**: Unknown. **Workaround**: Increase the global "Max Concurrent Logins for a user name" to a desired number.

Table 5 Open Caveats (continued)

ID	Description
CSCud48620	**Symptom**: On a channel with high utilization and interference numbers, the RRM DCA algorithm might not change the channel when it should. As a result, the channel assignment for a few access points may be suboptimal, which can negatively impact performance. **Condition**: If a channel change that is required to avoid the high utilization or interference has an adverse effect on the RF neighborhood, it might prevent the channel change. Release 6.0.182.0. **Workaround**: Configure DCA back to aggressive mode.
CSCud57238	**Symptom**: The Cisco 602 OEAP's Ethernet Counter stops incrementing after they reach the maximum value for a 32-bit signed integer (2147483647). **Note** This does not affect the operation of the AP or the Ethernet traffic. **Condition**: Unknown. **Workaround**: Reset the counters by rebooting the Cisco 602 OEAP.
CSCue50917	**Symptom**: When a RAP loses its wired connection, the RAP fails to restore connectivity as a MAP through the radio backhaul. The mesh adjacency is correctly built to a nearby MAP, and the RAP gets an IP address and can even join its controller, but shortly afterwards a radio reset is observed which causes the RAP to disconnect. The RAP goes into a loop till the wired connectivity is restored. Error messages similar to the following are displayed on the RAP console: `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` **Condition**: Mesh deployment on the following controller software releases: 7.0.230.0, 7.2.x, 7.3.112.0 **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCud64396	**Symptom**: The controller might stop working if a Syslog server entry is being removed from the GUI when the server is unreachable. **Condition**: Syslog server configured on the controller with TLS enabled. The Syslog server entry is removed using the controller GUI while it is unreachable, but the controller still considers it to be "connected", as per "TLS auth status" that can be seen by entering the **show logging** command on the controller CLI. **Workaround**: None.
CSCud80390	**Symptom**: MAC flap on Layer 2 switch connected to the remote LAN port of Cisco 600 Series OEAP. **Condition**: Wired computers plugged into the Layer 2 switch connected to the remote LAN port communicate with each other with only pings. **Workaround**: Configure static ARP entries to prevent the MAC flap.
CSCud86140	**Symptom**: AP intermittently does not send probe response when there are other APs in the neighborhood on the same channel. **Condition**: There need to be other APs or traffic on the same channel for this issue to occur. **Workaround**: If the client hears probes from other surrounding APs, the client should be able to join another AP. Some NICs might prefer to hear probes from a specific AP. Even with the AP having the issue, eventually, the probe response might be transmitted after a few attempts.
CSCud89654	**Symptom**: On a local-switching-enabled 802.1X WLAN, if the clients associate with a local AP (not FlexConnect AP), after successful authentication, only url-redirect attributed is accepted by the controller, not url-redirect-acl attribute, which causes failures on redirection thereafter. **Condition**: 802.1X WLAN with local switching enabled; Release 7.2 and later. **Workaround**: Disable local switching on the WLAN. You will have to segregate the local AP from FlexConnect APs on different controllers, making it an impossible solution to mix them together on a single controller.
CSCud97325	**Symptom**: Cisco AP3600 and Cisco AP2600 send invalid frames sourced with address 0000.0104.xxxx. This might result in security warnings on the switch, such as the following: `%AUTHMGR-5-SECURITY_VIOLATION: Security violation on the interface GigabitEthernet3/46, new MAC address (0000.0104.d634) is seen.` **Condition**: This issue occurs when the primary or secondary controller is changed in the AP High Availability tab. This issue is observed with only Cisco Aironet 2600 and 3600 Series access points. **Workaround**: None.
CSCue02826	**Symptom**: The 5-GHz radio on AIR-CAP1552E-N-K9 in the non-Bridge mode fails to enable if the controller is configured for Brazil (-T) Regulatory Domain. **Condition**: Release 7.3.101.0. **Workaround**: Use the Bridge mode in the AP.

Table 5 Open Caveats (continued)

ID	Description
CSCue09354	**Symptom**: Rogue AP does not get detected on the wired network when it is on non-native VLAN trunk to rogue detector AP. **Condition**: Release 7.4.x; Rogue detector mode AP; Rogue AP not on Rogue Detector native VLAN. **Workaround**: None.
CSCue18790	**Symptom**: Cisco AP1600, Cisco AP2600, and Cisco AP3600 might transmit management and control frames at maximum power, regardless of the configured power settings. **Condition**: Cisco AP1600, Cisco AP2600, and Cisco AP3600. **Workaround**: None.
CSCue32755	**Symptom**: Wireless clients are unable to associate with the mesh APs. **Condition**: When the wired clients are not operational; clients are connected to the mesh AP with Ethernet bridging enabled. **Workaround**: Reboot the mesh AP for the wired and wireless clients to associate.
CSCue42242	**Symptom**: When the controller detects more than 21 ad hoc rogues, the controller GUI shows only the first 20 entries (first page). **Condition**: More than 21 ad hoc rogues detected. On the controller GUI, choose **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**: On the controller CLI, enter the **show rogue adhoc summary** command.
CSCue55153	**Symptom**: Controller stops communicating with CAM with SNMPv3. **Condition**: 1. Enable HA. 2. Add controller to CAM with SNMPv3 (should have an authorization and authentication passwords) 3. Failover from primary to secondary controller. **Workaround**: Delete and add the controller in CAM again.
CSCuf35269	**Symptom**: The 802.11u domain is lost after a controller reboot. **Condition**: Same domain name is used on two different WLANs. This is allowed on CLI, but configuration validation fails on boot. **Workaround**: Reconfigure the domain, or use different domain names.

Table 5 Open Caveats (continued)

ID	Description
CSCuf74326	**Symptom**: Cisco Virtual Wireless Controller is given a valid license with an AP count. Installation of the controller is successful, and the **show license summary** command shows the license in use with the correct count. However, the homepage of the controller GUI shows "0 access points supported" and APs are denied association with the controller. **Condition**: This issue occurs only when you provide a license file that contains only adder licenses and not the base feature. **Workaround**: Request for a correct base feature AP count license file.
CSCug08277	**Symptom**: Cisco AP1260 might stop working in the function mvl_transmit_recover. **Condition**: Cisco AP1260 using IOS version 12.4(23c)JA6 and controller version 7.0.235.3. **Workaround**: None.
CSCug14709	**Symptom**: Controller does not take into account anymore if "airespace wlan-identifier" attribute is sent back in access-accept by the RADIUS server. **Condition**: This issue occurs in Release 7.4, but was not present in Release 7.0.x. **Workaround**: Use another mechanism to restrict SSID access.
CSCug15064	**Symptom**: Controller goes into maintenance mode with HA in enabled state. **Condition**: HA in an enabled state; Cisco Flex 7500 and Cisco 8500 Series controllers in non-LAG scenario with backup port configured; primary port is not operational. **Workaround**: None.
CSCug27084	**Symptom**: The standby controller in an HA pair could reboot in a loop if the HA role negotiation succeeds, but the configuration synchronization fails. **Condition**: Low memory condition on the controller. **Workaround**: Reboot the primary controller.
CSCug46616	**Symptom**: RRM group leader is not operational and does not do channel or power update. **Condition**: This issue might occur if you have APs hearing each other when associated through a large set of controllers where RF group name is identical. **Workaround**: Options are as follows: • Limit the RF group size to 1000 APs. Place the APs accordingly and avoid salt and pepper deployment. • If you already are in this state, you can restart the group leader election by entering these commands: **config advanced 802.11a group-mode restart** (If RRM is in the 802.11a band) **config advanced 802.11b group-mode restart** (If RRM is in the 802.11b band)
CSCug49505	**Symptom**: Cisco AP3500 stops working. **Condition**: LWAPP Rogue Monitoring process is on. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCug53945	**Symptom**: After a Cisco AP reboot, the radio which was disabled before Cisco AP reboot is somehow reenabled automatically. This occurs when the Cisco AP belongs to an RF profile. **Condition**: Cisco AP joins nondefault AP group and the AP group has the RF profile. **Workaround**: Disable radio on AP again after the reboot.
CSCug59937	**Symptom**: Controller reboot with traceback tpcv2ConstructApProfile. **Condition**: TPCv2 in an enabled state. **Workaround**: None.
CSCug82976	**Symptom**: Cisco APs that are configured with submode PPPoE are losing the submode configuration (Submode = Unconfigured) after moving from one controller to another or after rebooting the Cisco AP when associating with the second controller. **Condition**: Reboot the PPPoE submode Cisco AP associated with the primary controller. **Workaround**: None.
CSCuh05276	**Symptom**: Controller might trigger a reaper reset crash at "apfFindRogueApEntry" while adding rogue rules on the controller, due to a deadlock condition. **Condition**: Adding rogue rules on the controller. **Workaround**: None.
CSCuh14797	**Symptom**: In Export Anchor-Foreign scenario, in both Foreign to Foreign as well as fresh association to a Foreign, if packets are not reaching to Export Anchor due to network issues, then after three retries, there will not be any further exchange. The request will go to Export Anchor and the client will stay in that state until it moves out. **Condition**: Network issues between mobility peers. **Workaround**: None. Instead, fix the underlying connectivity issues.
CSCuh16870	**Symptom**: Client with static IP loses connectivity on session timeout. **Condition**: This occurs only if the following set of conditions are met: 1. Interface that the client gets from the interface group does not match the interface corresponding to the static IP. 2. Client gets VLAN overridden with the following message: `apfReceiveTask: May 28 12:48:28.066: 00:1a:70:a5:2f:bd Overriding interface of client from 'vlan20' to 'vlan30' within interface group 'vlan20-30' *apfReceiveTask: May 28 12:48:28.066: 00:1a:70:a5:2f:bd Applying Interface policy on Mobile, role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 20` This overriding is lost when PMK expires, and a new authentication takes place. This occurs even if the client is continuously sending traffic. **Workaround**: Either disable interface groups or set to DHCP required state.

Table 5 Open Caveats (continued)

ID	Description
CSCuh26964	**Symptom**: During dynamic rf-group, an HA switchover controller stopped working. **Condition**: While running dynamic rf-group between an HA Cisco WiSM2 controller and Cisco 5500 Series standalone controller, enter the **show advanced 802.11a group** command in the standalone controller CLI. On a forced switchover, the standby controller stopped working. **Workaround**: None.
CSCuh35237	**Symptom**: Incorrect Data tracebacks and failure in response is observed in Cisco AP3600. **Condition**: 1. An HA Cisco Flex 7500 Series Controller using Build 7.4.100.105 and a Cisco AP3600 in FlexConnect mode associated with it. 2. Schedule a reset in the active controller using 'reset system in 00:03:00 image no-swap reset-aps save-config' 3. At the scheduled time, the Cisco AP3600 gets a reset push from the controller. While the AP reboots, incorrect data tracebacks are observed in the Cisco AP and the Cisco AP stops working. Later, the Cisco AP associates with the controller. **Workaround**: None.
CSCuh37728	**Symptom**: Cisco AP1600 prints tracebacks on the console at reboot after VLAN tagging is configured from the controller (using the **config ap ethernet tag id** *vlan-id cisco-ap-name* command). **Condition**: Cisco AP1600 with data encryption enabled. Traceback seen at the reboot following the VLAN tagging configuration from the controller. **Workaround**: None.
CSCuh44430	**Symptom**: SE-Connect mode APs show up as Local mode in GUI after fallback because after the fallback the CleanAir Admin and Oper Status becomes "NA" instead of UP. The Network Spectrum Key is not available and it shows up as Local Mode in GUI. Spectrum Analyzer is unable to connect to the SE-Connect mode APs. **Condition**: Reboot the controller and then let the SE-Connect APs associate with the controller. **Workaround**: 1. Reboot the Cisco AP. 2. After the reboot, the Cisco AP shows correct Mode of "SE-Connect" and also Network Spectrum Key is available.

Table 5 Open Caveats (continued)

ID	Description
CSCuh89626	**Symptom**: Client displays the following message: `"Ignoring 802.11 assoc request from mobile radio is NOT enabled"` **Condition**: Cisco AP is operational, but the controller shows the Cisco AP as nonoperational. **Workaround**: Disable the Cisco AP and then reenable it. **More Information**: This issue is only observed after three or more days of continuously disabling and then enabling the radio state every minute on internal testing.
CSCui25877	**Symptom**: Radio PCI resets are observed on Cisco AP1600. **Condition**: PCI resets on Cisco AP1600 with high load. **Workaround**: None.
CSCui32908	**Symptom**: A Cisco AP stopped working and then rebooted. **Condition**: Unknown. **Workaround**: Unknown. Check any CDP events on the connected switch.
CSCug90218	**Symptom**: In the controller GUI, access points appear in an unknown state. **Condition**: Unknown. **Workaround**: Reboot the controller.
CSCug92421	**Symptom**: Controller reports many stale client entries. **Condition**: Cisco Flex 7500 Series Wireless Controllers with Release 7.3.103.14 having many clients. **Workaround**: None.
CSCug98625	**Symptom**: WebAuth redirect fails when local switching is enabled on a WLAN. Manual redirect and redirect with central switching works. **Condition**: Local switching is enabled on a WLAN. **Workaround**: Add a dummy interface on the controller with the IP address of the VLAN that is locally switched for the client. The VLAN IDs need not be the same, however, the IP addresses must be same. The VLAN must be trunked to the controller.
CSCuh02340	**Symptom**: CleanAir status appears as N/A even when the access point supports and enables CleanAir. **Condition**: This issue occurs when the access points join a primary or secondary controller after the power goes down or a network problem arises. **Workaround**: Disable or reenable the access point radio to recover the CleanAir status on the controller.
CSCuh03648	**Symptom**: Controller sends accounting updates with different framed IP address for an endpoint. **Condition**: Central web authentication used with ISE and URL redirect is pushed. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCuh04548	**Symptom**: Client disconnects from its WLAN. **Condition**: When you change the parameters of a WLAN, a client disconnects from another WLAN. **Workaround**: None.
CSCuh10735	**Symptom**: RADIUS failover occurs when the controller sends RADIUS request packets with the same ID to the RADIUS server six times and receives no response from the RADIUS server. **Condition**: Release 7.3.112.0. **Workaround**: None.

CSCuh11730	**Symptom**: When a FlexConnect local switching access point roams using WGB, the following message appears on the access point console:
	`*May 22 11:24:34.559: capwap_ap_mgmt: delete mn 0d0d.0d0d.0d0d`
	`*May 22 11:24:34.559: capwap_ap_mgmt: Deleting PMK for 0d0d.0d0d.0d0d`
	`The station mac address is not present in the network neither as a wlan client, or wired WGB client.`
	Condition: This message appears on Release 7.4.x while using the **debug capwap client mgmt** command.
	Workaround: None.

CSCuh16539	**Symptom**: When you disable the radio of a Cisco AP2600, the radio gets enabled after the access point reloads. **Condition**: Release 7.4.x **Workaround**: None.
CSCuh16842	**Symptom**: Client gets IPv6 address from a different VLAN. A sample message is given below: `Overriding interface of client from 'vlan20' to 'vlan30' within interface group 'vlan20-30'` **Condition**: 1. VLAN is in an interface group. 2. Client sends traffic from either a static IP address or a previously allocated IP address. 3. Client traffic does not match the assigned VLAN. **Workaround**: Use DHCP required.
CSCuh17973	**Symptom**: When you start a calibration task using Prime Infrastructure 1.2 and 1.3, the task proceeds and at the end of the data collection the following message appears: `No data points collected when starting from location..` **Condition**: This message is displayed when there is no data in the controller calibration table. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCuh20357	**Symptom**: Cisco Services-Ready Engine (SRE) controller configured as a DHCP server shows reversed octet for the default gateway and DNS server values. For example, 4.3.2.1 instead of 1.2.3.4. **Condition**: Cisco Wireless Controller on Cisco SRE using Release 7.4.x. **Workaround**: Use an external DHCP server or downgrade the controller to a release that is earlier than Release 7.4.x.
CSCuh20385	**Symptom**: Unable to use the filter options for clients and access points when you use IE 10 to access the controller GUI. The filter popup box does not appear in the GUI. **Condition**: Microsoft Internet Explorer 10. **Workaround**: Switch the browser to compatibility view.
CSCuh20715	**Symptom**: Cisco 5508 controller with Release 7.3.101.0 stopped working on `Reaper Reset: Task "LDAP DB Task 2" missed software watchdog.` **Condition**: Unknown. **Workaround**: None.
CSCuh25790	**Symptom**: In an HA-enabled 5508 controller with 430 access points, when you perform predownload on all the access points, the controller does not reset. **Condition**: High AP count and failed predownlaod. **Workaround**: Reboot the controller using the **reset system forced** command.
CSCuh26716	**Symptom**: The **show redundancy summary** command shows the following output regardless of its real SKU. `Unit = Secondary - HA SKU` **Condition**: When you use the **show redundancy summary** command on: • Secondary machine which is converted from a primary machine • HA-SKU machine **Workaround**: None.
CSCuh28190	**Symptom**: AP stopped working once and the log was found on the controller and TFTP server. **Condition**: Unknown. **Workaround**: None. Access point resets on its own.
CSCuh31410	**Symptom**: Access point radio resets during the FlexConnect state change. **Condition**: Restore access point connectivity to controller. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description

CSCuh39893	**Symptom**: Controller on Release 7.3 or 7.4 fails to authenticate the One Time Password (OTP) users authenticating with TACACS+. The following debug output is displayed when you use the **debug aaa tacacs enable** command:
	`TPLUS_AUTHEN_STATUS_GETPASS`
	`auth_cont get_pass reply: pkt_length=25`
	`processTplusAuthResponse: Continue auth transaction`
	`No auth response from: <SERVER IP>, retrying with next server`
	`Preparing message for retransmit. Decrypting first`
	`Forwarding request to <SERVER IP> port=4900`
	`AUTH Socket closed underneath`
	`No auth response from: <SERVER IP>, retrying with next server`
	`Preparing message for retransmit. Decrypting first`
	`Forwarding request to <SERVER IP> port=4900`
	`AUTH Socket closed underneath`
	`Exhausted all available servers for Auth/Author packet`
	
	Condition: This issue occurs in the following Condition:
	1. Controller uses Release 7.3 or 7.4.
	2. TACACS+ is used for management user authentication.
	3. OTP is used for TACACS+. Static passwords are not affected.
	Workaround:
	Extend the TACACS+ management server timeout value by using the following commands:
	config tacacs auth disable *server-index*
	config tacacs auth mgmt-server-timeout *server-index* 10
	config tacacs auth enable *server-index*

CSCuh41053	**Symptom**: When there is duplex mismatch between a Cisco Aironet 1140 Series Access Point port and an upper layer switch port, the following warning appears on the switch, controller, and access point: `duplex mismatch discovered` However, when the controller is upgraded to Release 7.4.x, the warning message is not logged to controller. **Condition**: Controller with Release 7.4.x. **Workaround**: None.
CSCuh44119	**Symptom**: Cisco 8510 controller does not update the config line after disabling DHCP proxy using the **config dhcp proxy disable bootp-broadcast disable** command. **Condition**: Release 7.4.100.60. **Workaround**: Manually enter the line in the config file or modify the configuration directly on the controller using the CLI or the GUI.

Table 5 Open Caveats (continued)

ID	Description
CSCuh45072	**Symptom**: Cisco 5508 controller in an HA configuration with two AAA servers sends TACACS+ authentication and authorization requests to different AAA servers. Users using TACACS+ account are unable to login to controller, as the controller sends authentication request to one AAA server, and authorization and accounting request is sent to another AAA server configured in the controller. **Condition**: This issue occurs in the following Condition: 1. HA configured on the controller. 2. Users log onto the controller using TACACS+. 3. Two or more AAA servers are defined in the controller TACACS+ authentication and authorization server list. **Workaround**: None.
CSCuh46996	**Symptom**: Wired clients behind a third party WGB device fail to get an IP address. **Condition**: • Third party bridge associates to an access point in H-REAP (FlexConnect) local switching mode. • Controller is using release higher than Release 7.0.116.0. **Workaround**: None.
CSCuh49135	**Symptom**: Beacon loss in Cisco AP1130. **Condition**: Cisco AP1130 in FlexConnect mode. **Workaround**: None.
CSCuh50219	**Symptom**: In a mesh topology, RAP-MAP1- MAP2 (all are 1522 access points using 5 GHz backhaul), when MAP1 does not have an Ethernet bridge client then MAP2 connects to MAP1 and joins the controller. However, when MAP1 has an Ethernet bridge client then MAP2 fails to connect to MAP1 to join the controller. The authentication process between MAP2 and MAP1 is never completed in this case. The issue also appears regardless of the radio used for backhaul (both 5 GHz and 2 GHz backhaul). **Condition**: Only on 1520 series access points. **Workaround**: None.
CSCuh51208	**Symptom**: On an HA pair, when the standby unit is active, the evaluation license remaining time warning is displayed. **Condition**: Unknown. **Workaround**: None. The HA controller continues to work as the local licenses are not used for access point join validation.
CSCue38133	**Symptom**: Controller sends a message that the APs should be moved to a primary controller, after 90 days of an AP joining the controller. **Condition:** This occurs when a HA-SKU controller is used as a secondary controller in a N1 configuration and an AP has joined the controller. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCue51838	**Symptom**: Flash is not accessible for Cisco AP1520 or Cisco AP1550. The APs will continuously write the following flash error to the console: `Write of the Private File nvram:/lwapp_ap.cfg Failed *Feb 8 15:10:34.947: %LWAPP-3-CLIENTERRORLOG: Save LWAPP Config: error saving config file *Feb 8 15:10:35.115: Write of the Private File nvram:/lwapp_ap.cfg Failed *Feb 8 15:10:35.119: %LWAPP-3-CLIENTERRORLOG: Save LWAPP Config: error saving config file *Feb 8 15:10:40.211: and can generate one of these two error messages, when a "dir" command is done: opening flash:/ (Invalid argument) opening flash:/ (Device or resource busy)` **Workaround**: Reboot the Cisco AP.
CSCuf03454	**Symptom**: Controller fails intermittently. **Condition:** Web pass through clients anchored from foreign controller to anchor controller. **Workaround**: Reboot the controller.
CSCuf08099	**Symptom**: New AP801 on C1941, cannot enable the radios. The radios gets reset continuously, and IOS shows 802.11 driver process using 99 percent CPU. Reloading the AP or router does not change. **Condition:** This occurs when AP801 joins controller using Release 7.4.x. **Workaround**: None.
CSCuf60628	**Symptom**: When AP which is in FlexConnect local switching mode, fails over from primary controller to secondary controller, the client protocol displays 802.11b, instead of 802.11g. **Condition:** This occurs in controller 7.3.112.0. **Workaround**: None.
CSCuf61599	**Symptom**: Clients are unable to join. **Condition:** This occurs in controller 7.3 5500 with FlexConnect and NAT/PAT AP IP. **Workaround**: Enable data encryption.

Table 5 Open Caveats (continued)

ID	Description

CSCuf77488	**Symptom**: The FT and LT detection time for an alarm is ahead/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.
	Condition: This occurs in controller 5508 7.0.235.3, AP3500 wIPS ELM mode, MSE 3350 on Release 7.0.201.204.
	Workaround: None.

CSCuf93093	**Symptom**: The "Central Dhcp" and "nat-pat Flag" are enabled on WLAN. With this configuration, when a wireless client tries to associate with an AP, the AP IP address is duplicated to default gateway. **Condition:** This occurs in controller 7.3.112.0. **Workaround**: Disable “nat-pat Flag”.
CSCug19563	**Symptom**: WiSM2 secondary controller DP stops responding due to deadlock in HA configuration while it gets booted and synchronizes with the primary controller. **Condition:** This occurs rarely when there are multiple reboot of controller in HA configuration. The controller recovers after reboot. **Workaround**: None.
CSCug27515	**Symptom**: Clients on 802.11n rates gets disconnected or experiences data transfer issues when certain segment number orders are used. **Condition:** When client leading segment number is lower than the window (lower order). **Workaround**: For Apple devices, disable AQM in the Apple wireless driver. Disable A-MPDU. Also refer CSCug65693 for workaround.
CSCug32970	**Symptom**: Memory leak in EAP. **Condition:** This issue occurs during excessive mesh AP Authentication. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCug34700	**Symptom**: Controller sends keep active alive as a wired packet instead of wireless. **Condition:** When the controller sends the keep alive as a wired packet the ISE drops it because of license. **Workaround**: Use passive keep alive instead of active.
CSCug38794	**Symptom**: WiSM2 stops responding and reboots (bcastReceiveTask 1332). **Condition:** Unknown. **Workaround**: None.
CSCug53680	**Symptom**: AP stops responding due to unexpected exception to CPUvector. **Condition:** There is no outstanding trigger. **Workaround**: None.
CSCug57216	**Symptom**: Ascom phone stops receiving voice packets. **Condition:** 11n in use Voice traffic QoS markings are lost on downstream direction. **Workaround**: Either fix QoS markings or disable 11n.
CSCug57545	**Symptom**: Clients are unable to connect to SNMP NAC SSID an displays the following error message: `Unable to process out-of-band login request from <MAC and IP Addr> [device-filter]. Cause: OOB client<MAC and IP Addr> not found.` **Condition:** This occurs after upgrade from controller 7.4. **Workaround**: Enable NAC Alert Client Trap.
CSCug73660	**Symptom**: As per the data sheet, the 1600 AP should have 17dbm of tx power on 1 antenna and up to 22 on 3 antennas. http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1600-series/data_sheet_c78-715702.html However, when you see the show controllers output, it shows that the power level 1 is 13dbm on 3 antennas (8dbm per antenna). Comparing show controllers output with 3600e, clearly shows that 1600AP has less tx power. Field tests also show it has a much smaller coverage area. This is on 2.4ghz. 5ghz power is meeting expectations. This was noted in -E reg domain. Also, on modifying the antenna gain has no effect at all on Tx power. **Condition:** This occurs in controller 7.4.100 code. European regulatory domain in countries where the expected power level is 17. **Workaround**: None.
CSCug74974	**Symptom**: Controller fails to redirect clients to the WebAuth/Passthrough page. **Condition:** This occurs in controller 7.4.x. When clients begins the WebAuth/Passthrough process by going to a web page that has cached their credentials in a cookie (such as “remember me” at www.yahoo.com). **Workaround**: Use a website that does not cache credentials in cookies. Clear the client's cookies for that particular website or all websites. Downgrade controller to controller 7.0/7.2/7.3.

Table 5 Open Caveats (continued)

ID	Description
CSCug80814	**Symptom**: The foreign controller does not respond to ARP from foreign export client to a local client being on the same VLAN. **Condition:** • Client1 associates with WLC1 (local) • Client1 performs Layer 3 roam to WLC2 (WLC2: foreign / WLC1: anchor) • Client2 associates with WLC2 (local) • Initiate traffic, that is ping from Client1 to Client2 **Workaround**: None.
CSCug86995	**Symptom**: SRE controller gives an option to configure the "External NAT IP State" and "External NAT IP Address" in the management interface. AP placed in the public domain will not be able to join the SRE. This is because the controller discovery response includes only the controller private IP address. Moreover, the option of enabling or disabling only the ap-discovery nat ip is not available in CLI. "config network ap-discovery nat-ip-only enable/disable". **Condition:** Unknown. **Workaround**: Do not place SRE-controller behind NAT even though the GUI allows you to configure it.
CSCug89084	**Symptom**: Clean Air sensor goes down and requires a reboot. **Condition:** First found on monitor mode APs. **Workaround**: Reboot the AP.
CSCub26289	**Symptom**: Controller changes the overlapping subnet interfaces IP addresses to all zeros without raising any visible alarm on GUI/CLI or any message on msglog/traplog or "show invalid-config". **Condition**: Controller had overlapping subnet interfaces prior to upgrade. **Workaround**: Ensure that controller does not have overlapping interfaces before an upgrade.
CSCub63054	**Symptom**: When VLAN transparent feature is enabled on controller version 7.2, it does not pass VLAN tags. Span at end device shows all frames being placed on the native VLAN. **Condition**: VLAN Transparent enabled. **Workaround**: Disable VLAN Transparent and set the MAP Ethernet port as trunk.
CSCub96053	**Symptom**: Cisco AP3500 gets DFS events because of radar on a DFS channel associated with an Cisco 7925 IP phone. The frequency of DFS events are higher on weekday and business hours. **Condition**: Controller Release 7.2.103.0. **Workaround**: None.
CSCuc02814	**Symptom**: When broadcast SSD is disabled, the client is unable to associate with the controller. **Condition**: Disable the broadcast SSID in controller. A client is unable to associate. **Workaround**: A non-Cisco client is able to associate.

Table 5 Open Caveats (continued)

ID	Description
CSCuc19950	**Symptom**: Anchored SSIDs on controller release 7.3.101.0 incorrectly shows recently configured peer controllers in its anchor list after a reboot. **Condition**: Controller Release 7.3.101.0 with existing anchored SSIDs. **Workaround**: Manually go to the anchored SSID and remove the recently added peer controllers from its anchor list.
CSCuc42026	**Symptom**: On FlexConnect (H-REAP) access points with a WLAN setup for local switching and local authentication, not all of the client detail fields are populated when a client connects to the WLAN. **Condition**: Unknown. **Workaround**: Switch the client authentication from local to central.
CSCuc45005	**Symptom**: Controller stops working while running controller release 7.3.101.0. **Condition**: Unknown. **Workaround**: None
CSCuc51315	**Symptom**: Controllers stops working if you clear the AP join statistics. **Condition**: This problem occurs only when you clear the AP join statistics (**Monitor > Statistics > AP join Statistics > Clear**) **Workaround**: None
CSCuc65606	**Symptom**: Cisco 4400 Controller stops working in spamreceive in release 7.0.235.3 **Condition**: None. **Workaround**: None.
CSCuc69522	**Symptom**: Client sending TCP SYN to a Multicast MAC for its gateway results in the controller not sending a TCP SYN ACK. TCP Handhsake does not complete and hence the client never generates HTTP traffic and is never redirected. Traffic is seen arriving at foreign and sending to anchor. The anchor ignores/drops the TCP SYN. **Condition**: Controller Foreign/Anchor doing Central Web Authentication. When a client has a Multicast MAC address for gateway, this issue occurs. This is usually the result of having a load-balance/clustered node for the gateway of a client. **Workaround**: Do not use Multicast MAC.
CSCuc70159	**Symptom**: Autonomous AP running software version 15.2 loses clock information after reboot. **Condition**: Autonomous AP running software version 15.2. Clock information is lost even when “clock save interval” is configured. This is important for WGB situations where the AP must use certificate-based authentication (EAP-TLS, PEAP), and the certificate validation fails the time check. **Workaround**: Perform the following: 1. Manually configure the clock after an AP reboot. 2. Configure SNTP for applications where AP is not operating as WGB with certificate-based authentication by entering this command on the AP console: `ap(config)#sntp server a.b.c.d {version 1|2|3}`

Table 5 Open Caveats (continued)

ID	Description
CSCuc81022	**Symptom**: The LAP1520 outdoor mesh APs gets false DFS triggers when in-band/off-channel (ch 124) weather RADAR signals are present and received above -20 dBm, causing network instability. A similar behavior was observed with off-band maritime radars operating in the 3.05 GHz band, but this can be addressed with Band-pass filters installed at the antenna port. **Condition**: AIR-LAP152x outdoor mesh AP installed near a weather RADAR installation. **Workaround**: New hidden CLI dfs-peakdetect added to address this issue.
CSCuc91441	**Symptom**: Some clients are not removed from the controller database after user idle timer is expired. **Condition**: When 100 clients expire simultaneously because of user idle timeout, only 64/65 deauths are sent and 36/37 clients are not removed from the controller database. **Workaround**: Manually remove the stale clients or reboot the AP that had these clients or reboot controller.
CSCuc93681	**Symptom**: Controller intermittently stops working. **Condition**: Any controller running software versions from 7.0 through 7.4. **Workaround**: None.
CSCuc98178	**Symptom**: If you remove the HSRP configuration, it leads the CAPWAP APs to keep sending data traffic to the old HSRP MAC while the control traffic is sent to the new correct gateway MAC. **Condition**: Cisco AP3500 and HSRP gateway. **Workaround**: Reboot AP.
CSCuc98518 $$IGNORE	**Symptom**: Guest LAN interface loses its guest LAN check box because of which the guest WLAN gets disabled. **Condition**: Guest LAN interface loses its guest lan check box. **Workaround**: Reenable the guest LAN check box on the guest LAN interface. Enable the guest WLAN and set the correct ingress interface.
CSCuc99675	**Symptom**: A Cisco AP802 may exhibit one of the following symptoms: • when configured for FlexConnect mode, it may come back up in local mode • the recovery (rcvk9w8) image attempts to download the full lightweight (k9w8) • image via CAPWAP, but the AP resets after 15 minutes and repeats the process **Condition**: Cisco AP802, lightweight IOS. **Workaround**: Disable RBCP heartbeat fail to detect default reset that occurs after 15 minutes by entering the “service-module wlan-ap0 heart-beat reset disable” command on the router.

Table 5 Open Caveats (continued)

ID	Description
CSCud07983	**Symptom**: The local AAA sever of the controller shows the outer username of wireless user who authenticates using local EAP. **Condition**: When using local EAP on the controller. **Workaround**: Disable identity protection on the wireless client to use the same username for the inner and outer EAP username. For local EAP, inner username will be shown in the clients page or in show client detailed mac-addr
CSCud10611	**Symptom**: High number of client exclusions can prevent configuration changes from being applied to Access Points. **Condition**: High number of client exclusions and access points joined the to controller. **Workaround**: Disable client exclusion.

CSCud12582	**Symptom**: Client RADIUS authentication fails. The **debug client** command shows a message similar to this:
	`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`
	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`
	Condition: Large scale deployments with multiple clients. RADIUS queues fill up and fail under heavy authentication/accounting load.
	Workaround: Disable RADIUS accounting and authentication.

CSCud16495	**Symptom**: Cisco Flex 7510 Series Wireless LAN Controller stops working when it is part of a HA pair. After this, the controller reloads and becomes active. **Condition**: Controller is part of an HA pair. **Workaround**: None.
CSCud23342	**Symptom**: When a Cisco 1142 lightweight access point joins to a 2504 controller, the access point name that appears in the Wireless page is different from the name that appears in the Monitor > Statistics > AP Join page. Some access point MAC address characters are appended to the access point name, or multiple entries are created with different base radio MAC addresses. **Condition**: Controller with 7.0.235.0 image. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCud26706	**Symptom**: After High Availability (HA) failover, the **show redundancy peer-route summary** command does not show any service port routes. This issue is applicable to Cisco 8500 Series Wireless LAN Controller. **Condition**: The service port routes doesn't exist after High Availability (HA) failover. **Workaround**: None.
CSCud33073	**Symptom**: mDNS snooping is enabled for FlexConnect local switching enabled WLAN after controller upgrade. **Condition**: When you use controller release 7.3 with FlexConnect local switching enabled WLAN and upgrade it to 7.4. **Workaround**: None.
CSCud34693	**Symptom**: LDAP Authentication occurs on a globally defined server listed outside the WLAN settings. **Condition**: When there is a timeout of LDAP authentication on the configured WLAN LDAP server. **Workaround**: Use 1 LDAP sever/OU for all users or use RADIUS authentication.
CSCud37443	**Symptom**: Clients are able to connect in b/g band even though Radio Policy for a SSID specifically set to “a only”. **Condition**: Create a WLAN with radio policy set to “a only” Configure the phones/clients in b/g mode and they successfully connect. **Workaround**: None.
CSCud41334	**Symptom**: The Ethernet bridged client of Mesh AP (MAP) does not work. **Condition**: If the Ethernet bridged client (for example, a PC) has been plugged into the Ethernet port of a MAP before MAP joins the controller, then the client will not work. The issue is seen on a AP1140, AP3500 and AP3600 (all indoor mesh APs). The issue is not seen on AP1552 (outdoor mesh AP). **Workaround**: Ensure that the bridged client is not plugged into the MAP Ethernet port, and then reload the MAP. Let MAP join the controller before plugging the client into the MAP Ethernet port. The client gets a valid IP address and should respond to pings.
CSCud44269	**Symptom**: AP sending ARP responses for a client in DHCP required state **Condition**: Flex mode AP on controller release 7.3.101.0. DHCP is enabled on the WLAN. Roaming breaks for clients on Flex mode APs. **Workaround**: Disable the DHCP REQD check box on the WLAN.
CSCuh52238	**Symptom**: Controller detects false positive Dynamic Frequency Selection Detections (DFS) owing to signals transmitted by Broadcom radios. **Condition**: Client hardware triggers DFS detections owing to signals transmitted by Broadcom radio. **Workaround**: Usage of non-DFS channels.

Table 5 Open Caveats (continued)

ID	Description
CSCuh53168	**Symptom**: While performing a device synchronization operation from Cisco NCS (SNMP query operation), Cisco controller returns a noSuchName value. **Condition**: Telnet is enabled (occasionally seen). **Workaround**: None.
CSCuh54815	**Symptom**: WPA2 with TKIP and WPA with AES is not supported in standalone mode, local-auth in connected mode, and CCKM fast-roaming in connected mode. **Condition**: Occurs only when the WLAN is configured as: – Flexconnect Local Switching and Local Authentication. – WPA-PSK with AES encryption. **Workaround**: Disable local authentication or use WPA2-PSK with AES or WPA-PKS with TKIP.
CSCuh55653	**Symptom**: AIR-CT5508-K9 unexpected reboot happens in Cisco controller 7.4.x software version with "apfMsConnTask_5" task suspended. **Condition**: Crash happens under normal condition without any changes in hardware or software configuration or network topology. **Workaround**: None.
CSCuh56264	**Symptom**: Client disassociated from fast transition roam due to key failure. This issue occurs only when both PMF and FT are supported. **Condition**: Client has negotiated both PMF and FT capabilities with the access point. **Workaround**: Disable PMF or FT.
CSCuh65005	**Symptom**: When the client is not authenticated by RSA/RADIUS server using webauth, Cisco controller places the client in RUN state. This issue is caused by the usage of two factor authentication. **Condition**: Unknown. **Workaround**: Non-usage of two factor authentication. Cisco controller does not support two factor authentication.
CSCuh69558	**Symptom**: While enabling a AAA over-ride in the WLAN during foreign controller-interface mapping on a guest access configuration, the anchor controller uses the default interface configuration to assign IP address to the client if the AAA server does not send any interface details. **Condition**: Unknown. **Workaround**: None.
CSCuh70825	**Symptom**: Cisco MAP gateway becomes unreachable using ICMP and displays memory allocation failures. **Condition**: 1552UE MAP with IP camera connected. **Workaround**: Reboot the access point.

Table 5 Open Caveats (continued)

ID	Description

CSCuh71233	**Symptom**: The 3600 AP running in FlexConnect mode stops working with the following decode:
	`Pid 65: Process "CAPWAP 802.11 MAC Management Reception "  stack 0x87AFC14 savedsp 0x5516CE4`
	`Flags: analyze prefers_new wakeup_posted`
	`Status  0x00000000 Orig_ra  0x00000000 Routine  0x0287B380`
	`Signal 0  Caller_pc  0x00000000 Callee_pc 0x00000000 Dbg_events 0x00000000`
	`State  0  Totmalloc  6733804  Totfree  2192816  Totgetbuf  119844`
	`Totretbuf  0  Edisms  0x0  Eparm 0x0  Elapsed 0x17598  Ncalls  0x5CD019  Ngiveups 0x0  Priority_q 4`
	`Ticks_5s  3  Cpu_5sec  0  Cpu_1min 6  Cpu_5min  0`
	`Stacksize 0xEA60  Lowstack 0xEA60  Ttyptr  0x54ED758`
	`Mem_holding 0x61E3C  Thrash_count 0  Wakeup_reasons  0x0FFFFFFF`
	`Default_wakeup_reasons 0x0FFFFFFF  Direct_wakeup_major 0x00000000`
	`Direct_wakeup_minor 0x00000000  Regs R14-R31, CR, PC, MSR at last suspend; R3 from proc creation, PC unused:  R3 : 00000000  R14: 05350000  R15: 05350000  R16: 05350000  R17: 04230000  R18: 04230000  R19: 04090000`
	`R20: 04DD0000  R21: 04DD0000  R22: 04DD0000  R23: 087BE138  R24: 087BE128  R25: 087BE130  R26: 087BE0B8  R27: 00029200  R28: 00000000`
	`R29: 00000000  R30: 04460000  R31: 00000005  CR: 28004042  PC : 022A04FC  MSR: 00029200`
	Condition: Unknown.
	Workaround: None.

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 some clients insist on requesting an IP unlisted in the connected interface range in a flood. The controller forwards the DHCP NAK responded by the DHCP server when a request is made. However, the interface will still be marked as dirty. **Condition**: Unknown. **Workaround**: None.
CSCuh76898	**Symptom**: When an access point is in FlexConnect Local Switching mode with disabled VLAN support, client communication is lost when access point switches over from one controller to another. **Condition**: Unknown. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description

CSCuh78753	**Symptom**: When an access point is in FlexConnect mode and has continuous association/re-association of clients with flapping WAN connection, access point may crash at the following decode:
	`Pid 120: Process "CAPWAP CLIENT " stack 0x8903104 savedsp 0x55F6604`
	`Flags: analyze prefers_new wakeup_posted Status 0x00000000`
	`Orig_ra 0x00000000 Routine 0x02863514 Signal 0 Caller_pc 0x00000000`
	`Callee_pc 0x00000000 Dbg_events 0x00000000 State 0`
	`Totmalloc 113928880 Totfree 111287540 Totgetbuf 287312 Totretbuf 0 Edisms 0x0 Eparm 0x0`
	`Elapsed 0x1239E4 Ncalls 0xC23E Ngiveups 0x4E7 Priority_q 4 Ticks_5s 65 Cpu_5sec 655`
	`Cpu_1min 1144 Cpu_5min 1561 Stacksize 0xEA60`
	`Lowstack 0xEA60 Ttyptr 0x55CD084 Mem_holding 0x141964`
	`Thrash_count 0 Wakeup_reasons 0x0FFFFFFF`
	`Default_wakeup_reasons 0x0FFFFFFF`
	`Direct_wakeup_major 0x00000000`
	`Direct_wakeup_minor 0x00000000`
	`Regs R14-R31, CR, PC, MSR at last suspend; R3 from proc creation,`
	`PC unused: R3 : 00000000 R14: 02863514 R15: 00000000`
	`R16: 00000000 R17: 00000000 R18: 00000000 R19: 00000000`
	`R20: 00000000 R21: 00000000 R22: 04DD0000 R23: 04DD0000`
	`R24: 00000000 R25: 88010C10 R26: 00000012 R27: 00000000`
	`R28: 00000000 R29: 08F24034 R30: 04470000 R31: 00000000`
	`CR: 28000028 PC : 022A0F04 MSR: 00029200`
	Condition: Access point is in FlexConnect mode and has continuous association/re-association of clients with flapping WAN connection.
	Workaround: None.

CSCuh86976	**Symptom**: Cisco NCS SNMP polling hangs as Cisco controller hangs while performing a SNMPwalk on the bsnMeshNeighsTable table for the Cisco controller 6.0.199.4. **Condition**: SNMPwalkon bsnMeshNeighsTable. **Workaround**: None.
CSCuh86993	**Symptom**: When an access point receives authentication request from a client that database is about to be freed/deleted, the access point should not respond with auth response for a disabled BSSID. **Condition**: Unknown. **Workaround**: None.
CSCuh87571	**Symptom**: Image upgrade fails in a high availability environment even when the standby is up and running. The standby HOT does not display any image download activity. **Condition**: Occurs on AP 5508/Wism2 high availability environment. **Workaround**: Reset the system and retry the image download.

Table 5 Open Caveats (continued)

ID	Description
CSCuh92835	**Symptom**: While trying to change Layer2 and Layer3 policies on any two similar WLAN, an error message "WLAN with duplicate SSID and Layer2 security policy found."is displayed. **Condition**: Occurs on AP 5508/WiSM2 high availability environment. **Workaround**: Perform the following workaround: 1. Change WLAN configuration from the CLI. You must disable both the WLANs from the GUI and enable the WLANs again after you complete the configuration again. 2. Delete the existing WLAN and re-create another WLAN using the GUI.
CSCuh93838	**Symptom**: WebAuth redirect fails when a FlexConnect access point joins the Cisco controller using the IP address from the DHCP server after a reload. A reload occurs when the FlexConnect AP with static IP address has lost connectivity to Cisco controller and the default gateway. **Condition**: Unknown. **Workaround**: Reload the FlexConnect access point.
CSCuh94259	**Symptom**: While enabling an mDNS profile on an interface group, an error "Active WLAN using interface group. Disable WLAN first" is displayed when an interface group is already mapped to a WLAN or an access point. **Condition**: Usage of mDNS gateway on interface group. **Workaround**: Ensure that you remove, add, and enable mDNS on the interface group before further use.
CSCuh94366	**Symptom**: Clients are unable to connect to receive DHCP information post upgrade. **Condition**: Usage of mDNS gateway on interface group. **Workaround**: Usage of other VLANs.
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. **Condition**: Change-of-authorization (CoA) on the controller. **Workaround**: When the three AVP pair attributes are sent, the controller accepts the disconnect request Calling-Station-ID MAC address of device (lower case works) Service-Type Login-user Called-Station-ID (upper case MAC of AP SSID separated by colons).
CSCuh99194	**Symptom**: Wireless Clients are not denied association when it re-associates. **Condition**: The maximum number of clients per access point radio is configured on each Cisco AP1142. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCui01948	**Symptom**: The "SNMP operation to Device failed. Table too large, possible agent loop." error message is displayed on monitoring access points on Cisco Prime Infrastructure 1.3. **Condition**: SSID is set to FlexConnect local switching and access point set to local AP mode. **Workaround**: None.
CSCui02779	**Symptom**: Cisco OEAP fails to connect when a failover occurs from LDPE to Non LDPE controller when in a high availability setup. **Condition**: Unknown. **Workaround**: None.
CSCui03652	**Symptom**: SIP client sometimes associate access points over CAC voice max-bandwidth. **Condition**: Unknown. **Workaround**: None.
CSCui05324	**Symptom**: Clients are unable to associate to the access point radio. The access point continues to beacon, but when the client sends an 802.11 authentication frame, the access point fails to respond with an authentication response. This issue occurs when the use of the current transmit queues is equal to the limit - the radio is unable to transmit. **Condition**: Unknown. **Workaround**: You must perform the following workaround: 1. Write a script that goes out to each access point and monitors the usage of the radio transmit queues. If a radio is found whose transmit queue utilization is nearing its limit, then issue the following command: `clear interface <interfacename>` 2. Manually reset the AP's impacted radio.
CSCui08633	**Symptom**: Access point information in an access point group does not match when verified in GUI and CLI. **Condition**: Unknown. **Workaround**: Perform an upgrade.
CSCui09037	**Symptom**: Client IP on controller does not get updated after executing the 7.3.101.0 upgrade. **Condition**: WLAN is used for mobile device, H-REAP local switching, but the DHCP server is central. **Workaround**: Synchronization will happen after some time.(20-30 minutes).
CSCui10841	**Symptom**: The access point arranges a bandwidth for SIP phone, though not on the phone. **Condition**: Unknown. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCsv54436	**Symptom**: While trying to connect Wireless LAN (WLAN) controller through SSH, the connection fails. If retried immediately from the same system to controller, the connection succeeds. **Condition**: The SSH connection is made from a different Layer 3 network. The issue is found in the Cisco 4400 and 2106 Series Controllers. **Workaround**: Retry SSH connection.
CSCsy66246	**Symptom**: An 802.11n AP does not downshift rates for retries when low latency MAC is enabled. The AP sends three retransmissions but the data rate for retransmissions is the same as the data rate at which the initial packet was sent. **Condition**: Using an 802.11n AP with low latency MAC enabled. **Workaround**: Do not enable low latency MAC.
CSCtn52995	**Symptom**: H-REAP reached a maximum limit on the association ID for AP. **Condition**: 1. Client 1 is associated to the controller with AID as 1 on SSID x. 2. Client 1 sends 802.11 auth frame on ssid y, at this point AID as 1 is freed at the AP. 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 AP and gets AID as 1. 5. AP updates the controller about client 2 and AID as 1, at this point the controller adds duplicate entries and increments the count (controller already has client 1 AID =1). 6. Counter is getting incremented and reaching 256. It is due to the network conditions in which the 802.11 authentication frames are sent (sometimes on a different WLAN) but is not followed by association frames. **Workaround**: None.
CSCtq32444	**Symptom**: When a port in a LAG goes down and then comes up, the controller does not send an UP trap through SNMP. **Condition**: Distribution ports are configured in a LAG and an SNMP trap receiver is configured. **Workaround**: Use the **show traplog** command to view traplog on controller for the UP trap.

Table 5 Open Caveats (continued)

ID	Description

CSCtw67184	**Symptom**: While booting up the controller, you might view the following message on the attached monitor or on the serial console:
	`All the disks from your previous configuration are gone. If this is an unexpected message, then please power off your system and check your system and check your cables to ensure all disks are present.`
	`Press any key to continue or C to load the configuration utility.`
	When the **Space** key is pressed, the system could not boot from the disk.
	Condition: The controller might have passed through an accidental power interruption. Upon reboot, the RAID card could not find its configuration in the flash memory and therefore it could not boot.
	Workaround: When you encounter the situation, you must enter into the RAID management tool called WebBIOS. There are two versions of the tool available:
	• One that uses extensive menus and requires an attached monitor.
	• Another one that is completely based on the command-line interface (CLI). The CLI version can be accessed from the serial console. The prompt appears right after the message. Enter into the CLI version of the WebBIOS utility by pressing **Ctrl-Y** and then entering the following command: **-CfgForeign -Import -a0**.

CSCtx68850	**Symptom**: After upgrading to the controller (release 7.2), when trying to connect the controller through SSH, the connection fails randomly, the prompt for username is displayed, and then SSH session gets closed from the controller side. **Condition**: Unknown. **Workaround**: Try connecting several times.
CSCty84682	**Symptom**: AP is not forwarding Multicast data and IGMP querier messages. **Condition**: Upon fresh reload of an AP. **Workaround**: Perform shut or no shut on the WLAN.
CSCub14556	**Symptom**: If you use the **clear ap config** CLI command or the **clear all config** option under the **Set to Factory Defaults** page in the GUI on an indoor AP that has been configured for mesh (bridge) mode, the AP remains in bridge mode. **Condition**: An indoor AP that has been configured for mesh. **Workaround**: You can perform one of the following ways: • Remove the **IOS_STATIC_AP_MODE** environmental variable from the AP. This can be done on the console by reloading the AP, escaping into the bootloader, and entering the bootloader command: **ap: unset IOS_STATIC_AP_MODE**. • Copy **flash:env_vars** from the AP to a TFTP server, edit the file to remove the **IOS_STATIC_AP_MODE** line, and copy the file back. Then, clear the AP config. When the AP reboots, it should be back to factory defaults.
CSCub87374	**Symptom**: APs may not be able to join controller (with release 7.2 or 7.4) and the controller indicates the limit for maximum APs supported is reached. **Condition**: Controller indicates the limit for maximum APs supported is reached when it has not been reached as indicated in the **show license capacity** command. **Workaround**: Reboot the controller with evaluation license.

Table 5 Open Caveats (continued)

ID	Description

CSCuc68995	**Symptom**: A wireless webauth client is unable to authenticate to the network. When the client opens a browser window, the window is blank.
	Using the **debug web-auth redirect** command, the messages similar to the following appears:
	`*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`
	Condition: The HTTP GET from the client is arriving at the controller in multiple TCP segments.
	Workaround: Either reconfigure your network or the client's TCP/IP stack, or the both to ensure that the HTTP GET arrives in a single segment.

CSCuc80103	**Symptom**: WiSM2 is unreachable and unable to ping. All APs are dropped from the controller, and unable to ping the Management interface's gateway (through console) at the time of failure. Failure condition will recover on it's own typically within minutes.
	Condition: Cisco WiSM2 using Release 7.3.101.0.
	Buffer pool leak messages are printed within the msglog around the time of the failure:
	`*broffu_SocketReceive: Oct 20 07:31:15.291: #BROFFU-0-DP_BUFFER_POOL_LOW_DETECTED: broffu_fp_dapi_cmd.c:5060 Warning: DP Early PacketBuffer low detected. DP1 PacketBuffer=26105(<?26200) WQE=102318(<?26200)`
	`*broffu_SocketReceive: Oct 20 07:31:15.291: #BROFFU-0-DP_BUFFER_POOL_LOW_DETECTED: broffu_fp_dapi_cmd.c:5060 Warning: DP Early PacketBuffer low detected. DP0 PacketBuffer=26025(<?26200) WQE=102322(<?26200)`
	Workaround: Downgrade the controller to its prior release.

CSCuc94860	**Symptom**: If you configure the MAC filtering RADIUS compatibility mode from GUI choosing **Security > AAA > MAC Filtering > RADIUS Compatibility Mode** or using CLI with the **config macfilter radius-compat** command as **Cisco ACS** or **Free RADIUS**, the WLAN controller sends access-request packet with all bit zero Message Authenticator attribute. **Condition**: When configured the **MAC Filtering RADIUS Compatibility Mode** as **Cisco ACS** or **Free RADIUS**. **Workaround**: Choose **Other** (default value).
CSCud14147	**Symptom**: WLAN controller calculates an incorrect message authenticator value for RFC3576 CoA requests from some RADIUS servers such as PacketFence NAC. **Condition**: Controller with releases 7.2.110.0 or 7.3.101.0. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCud16984	**Symptom**: Access points are assigned to channels with lower maximum powers. **Condition**: Varying power levels in different channels of the new access points. The controller detects more neighbors with high RSSIs on channels with higher power. **Workaround**: None.
CSCud56753	**Symptom**: In a VMWare ESX cluster, when migrating a vWLAN controller from one host to another via vMotion, the vWLAN controller management may become unreachable for 15-30 seconds which may causes APs to transition to standalone mode temporarily and prevent centrally switched WLANs from communicating. **Condition**: A virtual controller's management interface is configured with a dot1q VLAN tag communicating through a virtual switch network configured with VLAN (4095 ALL) in promiscuous network. VMware network can be configured to "Notify Switches" causing RARP to be sent on VM's tagged interface for updating neighbors with CAM table seamlessly during vMotion transition. This is transparent to the VM. In the vWLAN controller deployment; hosts cannot know the vWLAN controller's management or other interface dot1q tags so RARP is delivered untagged. This prevents CAM tables from learning of MAC update on proper VLAN ID and therefore a loss of communication to the vWLAN controller. **Workaround**: Communication is established as soon as the vWLAN controller generates traffic through the new host after a vMotion event. No known workaround.
CSCud57046	**Symptom**: Client entry is seen on multiple controllers even when not anchored to the controller or part of its mobility group. **Condition**: Not known. **Workaround**: None.
CSCud57784	**Symptom**: In the Cisco 5508 Series Wireless Controller, when the MAC Filtering authentication is enabled from the GUI using the following procedure, client authentication fails. 1. Choose **Security > AAA > RADIUS > Authentication** to open the RADIUS Authentication page. Define more than one RADISU servers. 2. Choose **Security > AAA > MAC Filtering** and set the **RADIUS Compatibility Mode** as **Free RADIUS**. 3. In the **WLAN** setting, select the **MAC Filtering** check box, select the Authentication server that you have selected. The index number of the server is 1. 4. Choose **Security > AAA > RADIUS > Authentication**. Delete the Radius server which has index number 1. 5. In the **WLAN** setting, select Authentication server which has index number other than 1. **Condition**: None specified. **Workaround**: From the WLAN controller GUI, choose **Security > AAA > RADIUS > Authentication**, and define a dummy radius server which has index 1.

Table 5 Open Caveats (continued)

ID	Description
CSCud68413	**Symptom**: A Cisco controller functioning as a DHCP server with large DHCP scopes may stop servicing DHCP client requests. **Condition**: WLAN controller with release 7.2.110.0. **Workaround**: Reload the WLAN controller.
CSCud84109	**Symptom**: When adding a new 3600 AP to the WLAN controller with multiple countries, the AP may select a country in a different regulatory domain than that of the AP. **Condition**: With a AIR-CAP3602I-A-K9 joining a controller with countries in regulatory domains for -A and -N. The AP selects the country in the -N regulatory domain. **Workaround**: Select the correct country and enable the AP admin state.
CSCui12365	**Symptom**: The Cisco 5508 Wireless LAN Controller fails to respond when a client moves from PMIP enabled wireless controller to non PMIP enabled wireless controller if fast SSID is enabled. **Condition**: Fast SSID is enabled. The controller is deployed with a with mix of PMIP and normal WLANs in use. **Workaround**: Disable Fast SSID.
CSCui13401	**Symptom**: After multiple 802.1x failures, the client is never excluded when the controller uses the 7.2.115.2 software version. **Condition**: Client repeatedly fails when 802.1x authentication is used. **Workaround**: None
CSCui15077	**Symptom**: The controller fails to respond when the AAA server pushes the Cisco AV pair when the url-redirect-acl is longer than 32 characters. **Condition**: The error occurs when the url-redirect-acl name is longer than 32 characters. **Workaround**: Use url-redirect-acl names of less than 32 characters.
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 flex mode. **Condition**: WLAN is disabled before being added to the AP group. **Workaround**: Perform the following steps: 1. Enable the WLAN before adding to AP group. 2. Add another enabled WLAN. 3. Reload AP.
CSCui16011	**Symptom**: Configuration import of ASCII and HEX commands for PSK do not work as expected. Clients fail to authenticate. **Condition**: This happens when the configuration contains ASCII and HEX commands in un-encrypted format for PSK. **Workaround**: Use an encrypted format when you upload the configuration for PSK.

Table 5 Open Caveats (continued)

ID	Description
CSCui18377	**Symptom**: Cisco Aironet 1242 Access Point generates tracebacks and coredump after the controller upgrades to 7.4.100.60. Additionally, the radios also reset as shown in the log below: `Jul 10 06:02:54.569: %SYS-2-BADSHARE: Bad refcount in datagram_done, > ptr=125F318, count=0 -Traceback= <HEX Tracebacks>` **Condition:** The Cisco Aironet 1242 Access Point generates tracebacks and coredumps when upgraded to the Cisco WLC software version 7.4.100.60 **Workaround**: None.
CSCui19817	**Symptom**: Cisco Aironet 2600 Access Points fail to perform location calibration when using either the linear or by data points methods. Location calibration works for other models of access points. **Condition:** When location calibration is performed when there are Cisco Aironet 2600 Series Access Points as part of the deployment. **Workaround**: None.
CSCui20773	**Symptom**: BCAST queue is filled up displaying the following error: `Traplog indicates : "RX Multicast Queue Full"` **Condition**: Wireless clients send the IGMP report as soon as the query is sent by the Cisco WLC causing a Spike in Bcast queue. The spike is for very brief moment to cause queue to go full. Ideally for each query, clients should send report within 10 seconds. So throttling would happen. But in some cases, if the application does not do backoff (it sends as soon as query is received) a Bcast queue full message is displayed. **Workaround**: Increase IGMP query interval and timeout. If the queue is full and the IGMP query is not processed on first try, the stream will still not be affected until no report is received over the timeout value.
CSCui22463	**Symptom**: Cisco WLC fails to respond when software version 7.4.103.6 is used. **Condition:** The Cisco WLC fails to respond when mDNS snooping enabled on software version 7.4.103.6. **Workaround**: Disable mDNS snooping.
CSCui22736	**Symptom**: Unable to use **debug pm pmk** command. **Condition:** Unable to use the debug pm pmk **Workaround**: None
CSCui23134	Cisco WLC fails to respond with the task **spamPacketDumpHandleIntraRoamCase** **Symptom**: Cisco WLC fails to respond with the task **spamPacketDumpHandleIntraRoamCase** **Condition:** The Cisco WLC fails to respond when the **ap packet-dump** command is used. **Workaround**: Do not use ap packet-dump feature.

Table 5 Open Caveats (continued)

ID	Description
CSCui23580	**Symptom**: RAP loses static Channel on 5 GHZ and 2.4GHZ channel get set to static when configured for auto. **Condition:** When the RAP is configured with the following values: RAP-1 - Set to Channel 100. 2.4 GHZ = Auto RAP-2 - Set to Channel 161. 2.4 GHZ = Auto Both RAPs are initially joined with wired connection to the Cisco WLC. When RAP-1 eth link is lost/goes down, it joins over wireless backhaul through RAP-2. When eth connection is available RAP-1 joins over eth and gets set to channel 161 (remembers previous parents channel info) and 2.4 GHZ gets set to static channel 11. **Workaround**: RAP eth connection is never lost. If eth connection is lost, RAP should not join another RAP.

Table 5 Open Caveats (continued)

ID	Description

cscue50917	**Symptom**: When a RAP loses its wired connection it fails to restore connectivity as a MAP through the radio backhaul.
	The mesh adjacency is correctly build to a nearby MAP and the RAP gets an IP address and can even join its WLC, but shortly afterwards a radio reset is observed which causes the RAP to disconnect.
	The RAP never settles down (it keeps on looping) till the wired connectivity is restored.
	Sample error messages on RAP console:
	`*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`
	Condition: Mesh deployment on the following software versions: 7.0.230.0 / 7.2.104.31 / 7.3.112.0
	Workaround: None.

CSCug23281	**Symptom**: 802.11 statistics do not update in Cisco AP1600 in Monitor mode. **Condition:** On the AP console, enter the **show int dx statistics** command. The statistics are not updated. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description
CSCug18190	**Symptom**:After clearing and reloading the configuration, if HA is configured, the MAC addresses differ on the active and standby mobility controllers when the show mobility summary command is executed. **Condition:** Configuration clear. **Workaround**: This does not happen on normal operation, unless a full configuration wiped and reconfiguration process is done, and HA is reestablished.
CSCue26844	**Symptom**: Cisco WLC controller fails to respond and resets the **spectrumNMSPTask** **Condition:** Cisco WLC fails to respond under normal conditions. Conditions unknown. **Workaround**: None.
CSCug26521	**Symptom**: Cisco WLC running the software version 7.4 in DHCP Proxy mode misses the option 255 in DHCP request packet, resulting in packets being dropped during inspection. **Condition:** Release 7.4. **Workaround**: Set format to ASCII by running the following command: `config dhcp opt-82 format ascii`
CSCtw92430	**Symptom**: In an HA scenario, when the default management gateway is broken, the standby or active controller goes into maintenance mode and never comes out of that mode even after the connection is restored. **Condition**: 1. Configure an HA pair and configure a standby and active controller. 2. Shut down the management default gateway and ensure that one controller goes into maintenance mode after a reboot. 3. After some time, restore the management gateway connection and try to make the controller in maintenance mode come back to the corresponding mode after the connection is restored. 4. The controller always remains in the maintenance mode until a manual reboot is performed and the status is shown to be in negotiation. **Workaround**: Perform a manual reboot of the controller.
CSCuc72493	**Symptom**: The APs disjoin after the switchover if the Cisco 8500 WLC has 6000 APs and 64000 clients on the full load. **Condition:** This happens when the Cisco 8500 controller is fully loaded. **Workaround**: None.

Table 5 Open Caveats (continued)

ID	Description

CSCtc16222	**Symptom**: The following messages are displayed on Cisco WiSM2:
	`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`
	Condition: The error message is displayed when using WiSM2 using 7.3.101.0 wireless controller software version.
	Workaround: None.

CSCuj13054	**Symptom**: Cisco WiSM2 stopped working after an upgrade from Release 7.3.101.0 to 7.4.110.0 **Condition:** Cisco WiSM2; upgrade. **Workaround**: None.
CSCuh50505	**Symptom**: Cisco WiSM2 stopped working and rebooted. **Condition:** TPCv2 is in enabled state. **Workaround**: Disable TPCv2.
CSCug83271	**Symptom**: Cisco Virtual Wireless LAN Controllers fail to correctly implement Virtual CPU Access Control Lists that have been configured to restrict access to the private virtual management address. **Condition:** Cisco Virtual Wireless LAN Controllers running WLC Release 7.4 are affected. **Workaround**: None. **Further Problem Description**: This issue does not allow an attacker to bypass any forms of authentication. An attacker that did access the private virtual management interface would need to provide valid credentials to gain access to the device.

Table 5 Open Caveats (continued)

ID	Description

CSCuj64462	**Symptom**: On the WLC or PI GUI, CleanAir operational status for one or more Cisco Aironet series access points shows 'Down' as operational status with reason 'CleanAir internal error [5]'. On the console log for the access point, there are messages such as the following:
	`%CLEANAIR-3-ERROR: Slot 0 could not connect to spectrum FW`
	`*Oct 2 13:30:07.327: NCI-I1: openSensor(slot=1)`
	`*Oct 2 13:30:37.315: NCI-E1: Sensor Connect failure, 260`
	`*Oct 2 13:30:37.315: CleanAir: **** Slot 1: Failed to start, err=5`
	`*Oct 2 13:30:37.315: NCI-I1: shutdownNci`
	`*Oct 2 13:29:57.327: CleanAir: **** Slot 1: Failed to start, err=5`
	The event log shows repeated radio resets with reason code 37 (Radio IDB Reset):
	`Sep 26 22:32:53.579: %EVT-5-NTC: Radio d0 RST 37 Flags 60109 BCN 0`
	`Sep 26 22:32:53.579: %EVT-5-NTC: Radio d0 RST 37 Flags 60109 BCN 0`
	`Sep 26 22:32:53.579: %EVT-5-NTC: Radio d0 RST 37 Flags 60109 BCN 0`
	Condition: Occurs only with CleanAir capable Cisco Aironet Access Points such as the 3500, 2600, and 3600 series APs.
	Workaround: None.

CSCuj84379	**Symptom**: Controller stops working and then reboots. **Condition:** Ad hoc rogue detection is in enabled state. **Workaround**: Disabling ad hoc rogue detection is a potential workaround. On the controller GUI, choose **Security > Wireless Protection Policies > Rogue Policies > General**, and set **Detect and report Ad-Hoc Networks** to disabled state.

CSCuj25911	**Symptom**: Messages similar to the following may be seen in the msglog:
	`#OSAPI-4-MSGQ_SEND_FAILED: osapi_msgq.c:520 Failed to send a message to the message queue object: RRM-DCLNT-2_4-Q. enqueue failed.`
	`*iappSocketTask: Sep 10 14:33:26.160: #RRM-3-MSGTAG021: rrmClient.c:1279 Airewave Director: Unable to queue enchanced coverage data from AP 00:25:84:00:11:22(1) on 802.11a`
	`*iappSocketTask: Sep 10 14:33:26.165: #RRM-3-MSGTAG021: rrmClient.c:1279 Airewave Director: Unable to queue enchanced coverage data from AP 00:25:84:00:11:22(0) on 802.11bg`
	`#RRM-3-RRM_LOGMSG: rrmClient.c:1885 RRM LOG: Airewave Director: Unable to queue load data from AP 00:27:0D:00:11:22(1) on 802.11a`
	Another symptom is that the WLC might stop working when the RRM profile is changed:
	`Reaper Reset: Task "emWeb" missed software watchdog`
	Condition: Unknown.
	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.
CSCub89883	**Symptom**: System is unresponsive in different tasks after guest LAN is enabled. **Conditions**: • Guest LAN • Cisco 5500 Series WLC using 7.2 or later releases • IPv6 traffic from clients **Workaround**: Disable guest LAN or disable IPv6.
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.
CSCuj58556	**Symptom**: Cisco AP disconnects from primary and moves to secondary WLC because of memory allocation. **Conditions**: Unknown. **Workaround**: Reboot the Cisco AP.

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`

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.

Resolved Caveats

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

Table 6 Resolved Caveats

ID	Title
CSCtk58442	LC needs force reset option to recover if stuck in sw download state.
CSCto02968	“New Memory leak sshpm, on sshencode. line 252”
CSCtt47397	Cisco AP3500 watchdog crashes at random with CPU Hog while under light load.
CSCtx61744	OEAP600 low TCP throughput less than 50Mbps for personal SSID
CSCua97184	Aggr Sched Cat 1: AP crashes due to function pointer corruption
CSCub24389	AP crash in spamProcessCertPayload
CSCub26654	AP3600/3500 DFS false detect
CSCub88183	Controller stopped working at emWeb instruction: ewaFormSubmit_login_callback
CSCub89883	Controller stopped working on multiple tasks, high CPU, after enabling guest-lan
CSCuc02149	Local switching 3600 drops IP6to4 TCP SYN ACK packets received from LAN
CSCuc03576	ARP problems with MAPs
CSCuc06605	Radio reset: SF3 radio 'tx jammed'[BZ 809]
CSCuc07384	Web access issue on SRE with 7.2 code
CSCuc32120	"AP: %SYS-2-INTSCHED: 'idle' at level 0 , interrupts -Process: CAPWAP CL"
CSCuc52952	75Dup service ip add error messages on 6500 for WiSM2 in HA setup
CSCuc84338	1550 AP showing up in Local mode instead of MAP or RAP mode
CSCuc95993	AP send out ARP request for different subnet IP address
CSCuc99037	RRM queues running full on 7.3
CSCud04882	LAP1142's display of Active Power levels is incorrect
CSCud04901	LAP1550 excessive DFS detection for in-band/off-channel weather radar
CSCud10200	CAP1552 local mode not obeying 30 min channel blacklist after DFS event
CSCud12437	DHCPv6 sollicits are sent over the air while they shouldn't
CSCud16350	"OEAP WPA2 issue, stuck at - wpaState to HANDSHAKE_AT_AP"
CSCud22588	Cleanup : mmListen:Failed to release a mutual exclusion object
CSCud23648	Controller stopped working on Release 7.3.101.0
CSCud33577	FlexConnect APs stuck in limbo when DHCP server is unreachable
CSCud39329	Load 7.3.50.17 - Controller 5500 stopped working --Task SXP SOCK
CSCud41398	"AP sometimes fails to hear BA from clients, causing BA timeouts [BZ 786]"
CSCud58247	License storage issues
CSCud62969	AP1600 not deferring NDP and Rogue containment with high traffic
CSCud63437	HA controller stopped working on reboot
CSCud65237	Encryption key corruption on BA ack with wrong ID
CSCud70484	Updating NB/WB spur suppression for 2600/3600 AP
CSCud83441	7.4 changes radius callStationIdType from radio to eth mac
CSCud84135	AP without default route lacks IP connectivity to other subnets
CSCud87439	AP1242 in H-REAP mode crashed with traceback pointing to CAPWAP bindings

Table 6 Resolved Caveats (continued)

ID	Title
CSCud89663	Some WLANs disabled after reboot
CSCud93574	Memory Leak on Anchor controller for client auth trap.
CSCud95613	Cisco WiSM2 stopped working after upgrading to 7.4.x only when high traffic load
CSCud97830	Telnet Access to controller lost
CSCud97983	AP1142 crashing after upgrading to 7.4.x
CSCud99466	Debug leaking due to lack of mac address for APF
CSCue00164	Standby controller continuous crash when a mesh joined to Active
CSCue00375	Failure observed in SNMP for AP CAPWAP retransmit change push
CSCue01983	3600 sends continuous corrupted deauth frames when in WIPS + 7.4
CSCue02475	Failure observed during Web-auth rediect
CSCue02707	HA redundancy does not failover to standby when powercycled
CSCue02718	HA redundancy does not failover to standby when removing ETH cable
CSCue03301	Power level:2 in 2.4GHz on 3602I/2602I APs is stated invalid
CSCue04153	DP failure because of DP Exception on 7.4.110.0
CSCue04528	Controller failure task: osapiBsnTimer SNMPTask
CSCue08313	AP failure due to chunk corruption; periodic client disconnects
CSCue08660	"High CPU on mobility task, crash on mmlisten"
CSCue08874	TX power level changes are reset after AP reboot (11nAP)
CSCue13108	TPC in 7.4 reduces transmit power to lower than expected values
CSCue14501	WSSI interference triggers DCA to change channels on serving radios
CSCue17421	RRM AP Neighbor list is not synced to HA Standby after switchover
CSCue19334	Failure in DHCP Socket Task nfaSyncMsgSendToTask dhcpSendRaw
CSCue26907	Controller failure in SrDoSnmp
CSCue26960	Pmalloc trailer failure - sshmp-integer-core.c
CSCue30626	Insufficient output by 'show 802.11a/b cleanair air-quality summary'
CSCue32955	Wired guest not getting IP address on controller
CSCue33125	"Unable to enable ""bootp-broadcast"" with HA SSO configured"
CSCue33222	Controller failure on 7.4.110.0 with mDNS service enabled
CSCue34072	Controller leaking memory for task:mmlisten
CSCue34763	Clients hit Idle timeout after successful authentication
CSCue49141	Controller: Failure with w/iappSocketTask reason
CSCue53220	Controller drops wireless to wireless client traffic with source UDP/16666
CSCue54977	rf-profile configuration not shown in show run-config commands
CSCue55191	"Memory leak in mm_listen.c, line 8826"
CSCue55397	Failure to create AP bundle during controller upgrade
CSCue56731	RF group state is HA standby on the active after failover

Table 6 Resolved Caveats (continued)

ID	Title
CSCue58727	Reaper reset controller due to mutex issue in spectrumRadSlotAQEnableGet
CSCue62225	HA: IGMP/MLD join goes out of standby controller
CSCue62388	"AP reloads with DOT11-3-NO_BEACONING ""Not Beaconing for too long"""
CSCue66168	Sanity check is not performed and both controllers stay Active
CSCue67286	"MSE: Need auto archive log feature, log full brings down MSE services"
CSCue68272	Standby does not take over when active is powered down
CSCue71856	AP not send traffic indication to client in power saving mode in time
CSCue75015	TPC on demand functionality not working with HA.
CSCue77449	MSE out of memory while adding APs to floor.
CSCue80531	dBm value is zero for AP802
CSCue83558	WiSM2 crash due to Task Name: apfMsConnTask_6
CSCue84694	AP does not clear L2 MGID info after Dynamic Interface Change
CSCue87238	Controller failure: Silent crash on 5508 running 7.4.103.4 without any crashlogs
CSCue87961	Unable to access controller GUI using management via wireless on 7.4
CSCue89182	Unable to upgrade from previous cco to phos via GUI
CSCue90110	Clients not removed from AP after HA failover
CSCue91018	SSID column in raw report from controller shows wrong data
CSCue92521	Controller 5508 crash due to memory corruption in task name spamApTask6
CSCue92971	"fixes for: reporting times, location corner cases and analytic services"
CSCue93244	HA 5500 controller stopped working due to memory corruption during AAA initialization
CSCue99040	7500 and WiSM2 High Availablity issue
CSCuf02268	HA will not even pair with 80ms RTT
CSCuf03309	Small packet drop on wism2 + DTLS scenario
CSCuf15633	"emWEB task controller Crash observed when execute ""config wlan delete"""
CSCuf20330	Mobility control path is down between 8500(HA)-8500
CSCuf21360	A-Pair stuck in image download state
CSCuf30537	CalledStation Id should use MAC Address per CalledStationID change
CSCuf38824	1552E: Flash fills up and cannot join as flash cannot be written to...
CSCuf43147	All ap clears the L2 MGID when wlan intf mapping deleted frm 1 apg.
CSCuf48138	getTagLocationlistfortelemetry api returns null
CSCuf61780	"1600, 2600, 2600 aIOS permits only 7 dBm power setting"
CSCuf65468	RRM misbehaving on BGL Alpha HA OEAP controller
CSCuf80340	Virtual controller: Web authentication feature is broken in virtual controller
CSCuf86303	"DP heartbeat lost, crash at longevity testbed"
CSCuf93738	Save config is not updating startup config with new AP group int mapping

Table 6 Resolved Caveats (continued)

ID	Title
CSCuf93777	AP radio Core dump: Transmitter seems to have stopped
CSCug04801	After a few Failover None of the Clients get authenticated
CSCug06084	Controller crashed - Task Name: SNMPTask
CSCug08318	"New 7500 M3 Hardware Version, unable to scale to 6000 APs "
CSCug10935	ACL is not inherited when controller switched over
CSCug10985	HA - Standby ctrl reboots twice due to mobility related XML mis-match
CSCug16101	CAPWAP background config save fixes/optimization
CSCug16473	HA Standby controller 7.4.110.0 FUS 1.7.0.0 DP failure crash loop
CSCug20166	'Network interrupt loop detected'; does not show AP traceback
CSCug21037	Standby Crashing when Active tries to transfer images in a particular sc
CSCug21715	AP is not able to boot with recovery image
CSCug22648	"WSSI not supported in -S, -N reglatory Domains (possibly more)"
CSCug23395	Secondary 5500 controller has went to hung up state
CSCug25517	L2roam entry not initialized in HA standby controller
CSCug27985	5500 controller failure during upgrade after kitchen sink stress with mem @ 79%util
CSCug28397	No beacon is sent from AP1600 for bake-off image
CSCug29258	FlexConnect ACL is not retaining after AP reboot in standalone
CSCug37360	"back out CSCuc3599, devshell over telnet"
CSCug41333	AP 1142 DATA_KEEPALIVE_ERR When DTLS Enabled - Not Staying Connected
CSCug42677	Controller crashes when applying CPU ACL in HA
CSCug45057	Radio disabled due to inline power on 7.4.100.6
CSCug46718	New client 802.11 auth fails 3600 or 2600 AP on 2.4GHz band after time
CSCug50611	Central DHCP Processing WLAN not getting added to Flexconnect AP
CSCug52338	2504 Traceback errors after image upgrade
CSCug54108	AP memory leak - %SYS-2-MALLOCFAIL: Memory allocation failed
CSCug57376	WISM2 : HA : - AP disconnects the Active and rejoins post switchover
CSCug59452	AP 1524PS/AG crashing while doing clear config
CSCug64750	ARP request unicast is dropped on anchor scenario
CSCug65454	WiSM2 crashes Reason: Reaper Reset Task:dtlArpTask
CSCug65693	Macbook client disconnect on alpha_ac
CSCug66578	Crashinfo files continue to grow on AP without being cleaned
CSCug69212	HA pair broken & config disappeared for WiSM2 running version 7.4.100.9
CSCug70229	Web-authentication with static ip client fails in Export Anchor
CSCug73771	All the rogue config params are lost on the AP in the following scenario
CSCug74738	Controller-GUI Radius Response Time shows Centi-Seconds when it's really msecs
CSCug75833	Crash of SXP core when trying to delete configured SXP connection

Table 6 Resolved Caveats (continued)

ID	Title
CSCug81582	WiSM-2 crash Task Name: apfMsConnTask_7 Reason: System Crash
CSCug86804	Controller 7.4 crash on tplusTransportThread
CSCug89547	Controller console hung after serial timeout if any show cli output in buffer
CSCug90440	Controller: Observing double 'client authenticated' Trap logs
CSCug91572	FlexConnect AID leak
CSCug93826	Instrumentation for reaper task
CSCug94941	7500 primary controller crashed while start image transfer
CSCug96183	Controller Crash Task Name: emWeb Reason: System Crash (HA)
CSCug97390	L2 mgids are getting deleted in APs after HA switchover
CSCug99623	APs disconnect on software download in a HA Pair
CSCuh01030	Aggr_Sched Stack Corruption (infinite loop in timer_send path)
CSCuh01250	7500 controller crash at task emweb
CSCuh01980	HTTPS to HA controller fails after reload as it misses Web Admin key
CSCuh02439	Missing reset interrupt level for flex ext. webauth
CSCuh03740	Rogue transient threshold computation is wrong in AP
CSCuh11295	HA messages showing in console during boot
CSCuh12262	Wired Client behind Universal WGB does not get an ip
CSCuh12457	HA Primary controller (Cisco Flex 7500 controller) reboots with gateway reachability issue
CSCuh15491	Aggr_Sched_Stack Corruption
CSCuh19146	AP SSO active controller crash at emWeb Task
CSCuh23819	ipv6 webauth not working if wlan is mapped to dynamic interface
CSCuh29693	Controller crash on 7.3.112.0 if you make any config change
CSCuh29695	Sys Crash seen on New Act on S/Wover at acDtlsPlumbDataPlaneKeys
CSCuh33173	APs are not properly detecting RRM measurements
CSCuh41842	Intra controller roaming with Webauth broken
CSCuh44600	RRM changing txpower when interval timer not expired
CSCuh47735	Aggr_Scheduler_Crash - FWD_TRACE_L function (freed dtx in cpq)
CSCuh48729	3600 AP hang on network interrupt loop
CSCuh52660	AP602 OEAP using invalid channels for E domain
CSCuh54131	Stand-by controller Reloading when power down the Active controller
CSCuh55612	OEAP: Evora WLAN client can't connect since client database is full
CSCuh55895	Controller: WiSM2 crashed when CNA began device discovery
CSCuh63491	"With RF profile created, certain clients are not able to join "
CSCuh67141	OEAP600 frequently disconnecting when joined to controller with HA pair
CSCuh81757	ap3500 crash with TLB Miss in sig_channel_stats()

Table 6 Resolved Caveats (continued)

ID	Title
CSCuh87654	AP 3600 fails to generate coredump
CSCuh98417	One-way audio issue seen on spectralink 8400

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

Information About Caveats

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/

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

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.