Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.2.110.0

First Published: May 2012
OL-26578-02

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*.

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 12.4(25e)JA1
- Cisco Prime Network Control System (NCS) 1.1.1.24
- Mobility services engine software release 7.2.110.0 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 7.2.110.0*.

- Cisco 3350, 3310, 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 Wireless Services Module 2 (WiSM2) for Catalyst 6500 Series switches
- Cisco Wireless Controller on Cisco Services-Ready Engine (SRE) (WLCM2) running on ISM 300, SM 700, SM 710, SM 900, and SM 910
- 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, 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 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 Integrated Services Routers (ISRs).

Note Before you use an AP802 series lightweight access point with controller software release 7.2.110.0, you must upgrade the software in the Next Generation Cisco 880 Series Integrated Services Routers (ISRs) to Cisco IOS 151-4.M or later releases.

Controller Platforms Not Supported

The following controller platforms are not supported for the 7.2 and later releases:

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

What's New in This Release?

This section provides a brief description of what is new in this release. For more information about these features, see the *Cisco Wireless LAN Controller Configuration Guide*.

- The Cisco Wireless Controller on Service Ready Engine (WLCM2 on SRE) platform running on ISM 300, SM 700, SM 710, SM 900, and SM 910 is supported in this release. For more information, see http://www.cisco.com/en/US/products/ps11716/index.html.
- The Cisco Aironet 2600 Series Access Points are supported. For more information, see http://www.cisco.com/en/US/products/ps12534/index.html.
- Until the previous release, the Cisco Aironet 1520 and 1550 Series outdoor access points could work only in Bridge mode as RAP or mesh access points as MAP. With this release, these APs support the following two non-Bridge modes for both 2.4 GHz and 5 GHz:
  - Local mode
  - FlexConnect mode

Note Enhanced local mode (ELM) is not supported when the device is in Local mode.

- 802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP, which is called Fast Transition (FT). The initial handshake allows the client and APs to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and AP after the client does the reassociation request or response exchange with new target AP.

  802.11r provides two methods of roaming:
  - Over-the-Air

- Over-the-DS (Distributed System)

The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without the need to reauthenticate at every AP. WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

Note Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r enabled WLANs.

Another workaround is to have two SSIDs with the same name but with different security settings (FT and non-FT).

- Bring Your Own Device (BYOD) is a concept that allows users to connect, register, and provision their own personal devices onto the corporate network. With this release, the controller supports the following while working in conjunction with the Cisco Identity Services Engine (ISE) in either Local or FlexConnect Mode (both central and local switching with central authentication).
  - Device registration and supplicant provisioning
  - Onboarding personal devices (provisioning for iOS or Android devices)

  You can configure the following in the Advanced tab of the WLAN configuration page:
  - NAC State
  - DHCP Profiling under Client Profiling

Note RADIUS NAC with Layer3 web authentication security (local web authentication) is not supported.

Note Flex local switching with Radius NAC support is added in Release 7.2.110.0. It is not supported in 7.0 Releases and 7.2.103 Release. Downgrading 7.2.110.0 and later releases to either 7.2 or 7.0 releases will require you to reconfigure the WLAN for Radius NAC feature to work.

- When a client tries to associate with a WLAN, it is possible to determine the client type from the information received in the process. The controller acts as the collector of the information and sends the ISE with the required data in an optimal form.

  The controller can be configured to act as a collector for client profiling and interact with the DHCP thread along with the RADIUS accounting task that is running on the controller. The controller receives a copy of the DHCP request packet sent from the DHCP thread and parses the DHCP packet for two options:
  - Option 12—HostName of the client
  - Option 60—The Vendor Class Identifier

After this information is gathered from the DHCP_REQUEST packet, a message is formed by the controller with these option fields and is sent to the RADIUS accounting thread, which is in turn transmitted to the ISE in the form of an interim accounting message.

- External web authentication is supported on FlexConnect locally switched WLANs. Local switching is enabled for packets that are destined to the external server at the access point itself. FlexConnect ACLs need to be pushed to FlexConnect access points to match the traffic and allow it to be locally switched. When a client associates with a WebAuth-enabled locally switched WLAN, the AP searches the appropriate FlexConnect ACL and updates the client. The AP decides, on a per packet basis, whether the packet should be dropped or forwarded depending on the information specified in the ACL.
- You can now upgrade from an LDPE controller software to a non-LDPE controller software. For more information, see Special Notes for Licensed Data Payload Encryption on Cisco 5500 Series Wireless LAN Controllers, page 13.

Software Release Support for Access Points

Table 1-1 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 1-1 Software Support for Access Points

Access Points		First Support	Last Support
1000 Series	AIR-AP1010	3.0.100.0	4.2.209.0
	AIR-AP1020	3.0.100.0	4.2.209.0
	AIR-AP1030	3.0.100.0	4.2.209.0
	Airespace AS1200	—	4.0
	AIR-LAP1041N	7.0.98.0	—
	AIR-LAP1042N	7.0.98.0	—
1100 Series	AIR-LAP1121	4.0.155.0	7.0.x
1130 Series	AIR-LAP1131	3.1.59.24	—
1140 Series	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—
1220 Series	AIR-AP1220A	3.1.59.24	7.0.x
	AIR-AP1220B	3.1.59.24	7.0.x
1230 Series	AIR-AP1230A	3.1.59.24	7.0.x
	AIR-AP1230B	3.1.59.24	7.0.x
	AIR-LAP1231G	3.1.59.24	7.0.x
	AIR-LAP1232AG	3.1.59.24	7.0.x
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—

Table 1-1 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	
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	—	—
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	—
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 1-1 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-LAP1523CM	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	—
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.

Upgrading to Controller Software Release 7.2.110.0

Guidelines and Limitations

- 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.
- 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 7.2.110.0 release from a release that is older than 6.0.182.0.
- 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 7.2.110.0. Table 1-2 shows the upgrade path that you must follow before downloading software release 7.2.110.0.

Table 1-2 Upgrade Path to Controller Software Release 7.2.110.0

Current Software Release	Upgrade Path to 7.2.110.0 Software
6.0.182.0 or 6.0 releases	You can upgrade directly to 7.2.110.0
7.0.98.0 or later 7.0 releases	You can upgrade directly to 7.2.110.0
7.1.91.0	You can upgrade directly to 7.2.110.0
7.2.103.0	You can upgrade directly to 7.2.110.0

- 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 7.2.110.0 from an earlier release, you must also upgrade to NCS 1.1.1.24 and MSE 7.2.110.0.
- 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 later) or Mozilla Firefox 2.0.0.11 (or later).
- 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.
- 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/en/US/docs/wireless/controller/release/notes/fus_rn_1_7_0_0.html.
- Ensure that you have a TFTP or FTP server available for the software upgrade. Follow these guidelines when setting up a TFTP or FTP server:
  - Ensure that your TFTP server supports files that are larger than the size of the controller software release 7.2.110.0. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the NCS. If you attempt to download the 7.2.110.0 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.
  - A third-party TFTP or FTP server cannot run on the same computer as NCS because the NCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.
- 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 and Flex 7500 series controllers are different than for 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 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 discovery response. Use this command if APs are on the inside and outside of the NAT gateway; for example, Local Mode and OfficeExtend APs 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 Configuration Guide*.

Note Predownloading a 7.2.110.0 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.

- The Cisco 5500 Series Controllers can download the 7.2.110.0 software to 500 access points simultaneously. The Cisco Flex 7500 Series Controllers can download the 7.2.110.0 software to 1500 access points simultaneously. The Cisco Wireless Services Module 2 (WiSM2) controller, The Cisco 2500 Series, and Cisco 8500 Series Controllers can download the software to 1500 access points simultaneously.
- 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 7.2.110.0 release to a previous 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

Upgrading to Controller Software Release 7.2.110.0 (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 7.2.110.0 controller software:

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

http://www.cisco.com/cisco/software/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 or FTP 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** or **FTP.**

Step 9 In the IP Address text box, enter the IP address of the TFTP or FTP 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 After the controller reboots, repeat Step 6 to Step 17 to install the remaining file.

Step 19 Reenable the WLANs.

Step 20 For Cisco WiSM2 on the Catalyst switch, check the port channel and reenable the port channel if necessary.

Step 21 If you have disabled the 802.11a/n and 802.11b/g/n networks in Step 4, reenable them.

Step 22 To verify that the 7.2.110.0 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 5500 Series 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 the Cisco 5500 Series Wireless LAN Controller 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 5500 Series 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.

The following table lists the Paper PAK licenses and their descriptions including their part numbers.

Table 1-3 Licensing for Cisco 5500 Series Wireless Controllers (PAKs)

Part Number	Description
LIC-CT5508-LPE-K9	Cisco 5508 Controller DTLS License (Paper Certificate - US Mail)
L-LIC-CT5508-LPE-K9	Cisco 5508 Controller DTLS License (electronic Certificate - must not be ordered by Russian Customers)

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

In 7.0.230.0 and 7.2.110.0 controller releases, you can upgrade from an LDPE controller software to a non-LDPE controller software. For all other releases, you must first upgrade to a release that supports LDPE before you upgrade to a non-LDPE controller software.

Note If you have a 7.2.103.0 release of the controller software, it is not possible to upgrade from an LDPE to a non-LDPE controller software.

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 **Cisco 5500 Series Controller** 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-CT5500-K9-X-XXX.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 22 detailed in the "Upgrading to Controller Software Release 7.2.110.0" section on page 8.

Interoperability With Other Clients in 7.2.110.0

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

Table 1-4 describes the configuration used for testing the clients.

Table 1-4 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	7.2.110.0
Controller	Cisco 5500 Series Controller
Access points	1131, 1142, 1242, 1252, 3500e, 3500i, and 3600

Table 1-4 Test Bed Configuration for Interoperability

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 1-5 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 1-5 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 5.0.1
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

Table 1-5 Client Types (continued)

Client Type and Name	Version
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R
Phones and Printers	
Cisco 7921G	1.4.2.LOADS
Cisco 7925G	1.4.2.LOADS
Ascom i75	1.8.0
Spectralink 8030	119.081/131.030/132.030
Vocera B1000A	4.1.0.2817
Vocera B2000	4.0.0.345
Apple iPhone4	iOS 5.0.1
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 platfroms:

- 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 Wireless Controller on Cisco Services-Ready Engine (SRE)
- Features Not Supported on Mesh Networks

Features Not Supported on Cisco 2500 Series Controllers

- Wired guest access
- Cisco 2500 Series Controller cannot be configured as an auto anchor controller. However, you can configure it as a foreign controller.

- Bandwidth contract
- Access points in direct connect mode
- Service port
- Apple Talk Bridging
- LAG

Note Directly connected APs are supported only in Local mode.

Features Not Supported on WiSM2 and Cisco 5500 Series Controllers

- Static AP-manager interface

  Note For Cisco 5500 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.

- Asymmetric mobility tunneling
- 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

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 Support

- WGB
- HotSpot2.0 (802.11u)
- Client rate limiting for centrally switched clients
- Internal DHCP server
- Access points in local mode

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
- LAG
- Spanning Tree Protocol (STP)
- Cisco Flex 7500 Controller as a guest anchor controller
- Multicast

Features Not Supported on Cisco Wireless Controller on Cisco Services-Ready Engine (SRE)

- Wired guest access
- Cannot be configured as an auto anchor controller. However, you can configure it as a foreign controller.
- Bandwidth Contract feature
- Access points in direct connect mode
- Service port support
- Apple Talk Bridging
- LAG
- IPv6

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)
- EAP-FASTv1 and 802.1X authentication
- Access point join priority (mesh access points have a fixed priority)
- Locally significant certificate
- Location-based services

Caveats

The following sections lists Open Caveats and Resolved Caveats for Cisco controllers and lightweight access points for version 7.2.110.0. 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:

http://tools.cisco.com/Support/BugToolKit/

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

http://tools.cisco.com/RPF/register/register.do

Open Caveats

Table 1-6 lists open caveats in controller software release 7.2.110.0.

Table 1-6 Open Caveats

ID	Description

CSCua43558	Controller does not respond during a task with IPv6 traffic.
	Symptom: Controller might unexpectedly reboot with crash information that is similar to the following:
	`Analysis of Failure:`
	`  Software was stopped for the following reason:`
	`  pmalloc detected memory corruption`
	`---`
	`pmalloc memory corruption type: ++PMALLOC_POISONED_AREA_CORRUPTION`
	`- Corruption detected at pmalloc entry address: (1cd15914)`
	`- Corrupt entry: entryMagic_0(0xbe90be90), entryMagic_1(0xbe91be91),`
	`trailer(0xead0ead0),poison(0xcc00ffed)`
	Conditions: Controller is handling IPv6 traffic.
	Workaround: None.

CSCtl95978	The controller does not respond to SNMP requests if the source address of the request comes from a subnet that is configured as a dynamic interface. **Symptom**: Unable to get an SNMP response from the WLC. **Workaround**: Remove the dynamic interface from the controller, or change the SNMP hosts source IP address to be in a different subnet.
CSCsq14833	Certain IP addresses used for management interfaces result in AP join issues. **Symptom**: When using VLSM, if the fourth octet of the management IP address is the same as the fourth octet of the broadcast address of another interface on the controller, the controller fails to respond to LAP discoveries. For example, if the management interface IP address is 10.10.10.15/25 and there is an another interface on the controller with a 172.16.10.9/29 address, 172.16.10.15 would be the broadcast address for the 172.16.10.x/29 subnet. **Workaround**: Change the IP address of the management interface.
CSCtz79377	Controller unresponsive on an SNMP task. **Symptom**: Controller unresponsive and reboots unexpectedly. **Conditions**: • Controller with multiple IPv6 clients • Stress testing of SNMP queries of IPv6 client addresses **Workaround**: None.

Table 1-6 Open Caveats (continued)

ID	Description
CSCsu54884	Ad hoc rogues are not shown in the controller after their status is changed to internal. **Symptom**: If the status of the detected ad hoc rogues is changed to internal, users cannot see the MAC address of the ad hoc rogues in the controller. **Workaround**: None. **Further Problem Description**: Unable to locate the MAC address of the ad hoc rogue using the **show run-config** command and in the configuration XML file of the controller.
CSCts32725	Controller AP list shows previously connected access points. **Symptom**: A Cisco 5508 Controller erroneously lists disconnected access points on the AP summary list. **Conditions**: Under normal operation, an access point previously registered on a Cisco 5508 Controller running 6.0.199.4 software is disconnected. However, the AP is still shown on the AP summary list. **Workaround**: None.

CSCts50317	Idle status on **show client ap 802.11b** *ap-name* remains permanently.
	Symptom: When the **show client ap 802.11b** *ap-name* command is entered, the AP status is shown as 'Idle' and remains that way until the AP is rebooted.
	`(Cisco Controller) >show client ap 802.11b <AP Name>`
	
	`MAC Address  AP Id  Status  WLAN Id  Authenticated`
	`---  ---  ---  ---  ---`
	
	`xx:xx:xx:xx:xx:xx  XXX  Idle  N/A  No`
	`yy:yy:yy:yy:yy:yy  XXX  Idle  N/A  No`
	
	Also:
	• The **show client summary** command on the controller does not indicate the client entry.
	• The **show capwap client mn** and **show controllers d0/1** commands entered on the AP does not show the client association entry.
	Conditions: Unknown.
	Workaround: Reboot the AP.

Table 1-6 Open Caveats (continued)

ID	Description
CSCts69268	The **show run-config** command displays wrong command syntax. **Symptom**: The **show run-config** command displays commands that are no longer active and commands with incorrect syntax. **Conditions**: Controller software Release 7.0.116.0. • **conf 802.11a spectrum all enable** • **conf 802.11a spectrum device disable radar** • **conf 802.11b spectrum all enable** • **conf 802.11b 11nSupport a-msdu tx disable** • **conf advanced 802.11b group-mode STATIC** **Workaround**: The following options are available: • Replace **spectrum** with **cleanair** in the command syntax. • Enter the **config advanced 802.11b group-mode off** command.
CSCtt15179	Two clients unable to communicate after inter-AP group roam to the home VLAN. **Symptom**: When two wireless clients that are associated with APs on the same controller try to communicate, one client may not pass traffic to the other client. **Conditions**: L3 roam within controller. For example: 1. Associate client to an AP on controller1 in VLAN1. 2. Roam client to an AP in an AP group in VLAN2 on controller2 so that the client is anchored to WLC1. 3. Roam the client to an AP on controller2 but in an AP group in VLAN1. Even though the client is in VLAN1 and is on an AP on controller2 that is in VLAN1, the client will remain anchored to controller2. This will result in a failure of communication (ARP) between this client and another client that is in VLAN1 but that is local to controller2. **Workaround**: Do not use AP groups for this WLAN.
CSCtt32890	cckm timestamp-tolerance missing from the output of the **show run-config** command. **Symptom**: Although the **config wlan security wpa akm cckm timestamp-tolerance** *msec wlan-id* command is configured to a nondefault value, the information about the CCKM timestamp tolerance is not displayed in the output of the **show run-config** command. **Conditions**: A WLAN is configured with CCKM, and the CCKM timestamp tolerance has been configured to a nondefault value. **Workaround**: The following options are available: • Enter the **show wlan** *wlan-id* command. Information about the CCKM timestamp tolerance is displayed as follows: `CCKM tsf Tolerance..... 5000` • Transfer the configuration to a TFTP server.

Table 1-6 Open Caveats (continued)

ID	Description

CSCtt96265	Controller might fail to transfer or save configuration and then becomes unresponsive.
	
	Symptom: The controller might display the following errors when attempting to transfer or back up the configuration, and eventually reboots without storing a crash file:
	
	`(WiSM) >transfer upload start`
	`Transfer in progess by another user`
	
	`(WiSM) >save config`
	`Are you sure you want to save? (y/n) y`
	
	`Flash write in progress.  Cannot save configuration.`
	
	Conditions: Cisco WiSM running Controller software Release 7.0.116.0.
	
	Workaround: None.

CSCtu07081	Unable to reboot Cisco Flex 7500 Series Controller after predownloading the AP image. **Symptom**: The 'AP Software being upgraded, please try again later' message is displayed. After shutting down the controller ports, the same message is displayed even when there is no AP associated with the controller. **Conditions**: Unknown. **Workaround**: Unknown.
CSCtu19860	Cisco 5508 Controller does not set 802.1p marking for downstream CAPWAP packets. **Symptom**: Cisco 5508 Controller does not set the configured 802.1p marking for downstream CAPWAP to CAPWAP packets. The controller only sets the 802.1p marking for downstream wired to wireless packets to the AP. Downstream wireless to wireless traffic on the same controller (CAPWAP to CAPWAP) traffic has an 802.1p marking of 0. When trusting CoS on the controller port, this causes the switch CoS to DSCP map to remark the packet to 0. When the AP receives the packet and sends it over the air, the 802.11e UP value is 0 causing one-way QoS. **Conditions**: Configure WLAN for platinum QoS and configure the platinum QoS profile for an 802.1p value of 6. Wireless to wireless traffic on the same controller does not have a proper downstream marking. **Workaround**: Trust DSCP on the switchport connecting to the controller instead of trusting CoS.
CSCtu28535	APs unresponsive due to unexpected exception to CPUvector. **Symptom**: AP1142 on 12.4(23c)JA2 are randomly become unresponsive on a controller software Release 7.0.116.0. **Conditions**: Under heavy multicast traffic, the AP has this issue while trying to clean up multicast packet queue. Packet buffers are freed more than once to cause this issue. This can occur randomly with different APs at different times. **Workaround**: Avoid heavy multicast traffic.

Table 1-6 Open Caveats (continued)

ID	Description
CSCtu36088	MAP key error on failover recovery scenario between RAPs. **Symptom**: A MAP can be unresponsive on 'decrypt errors' for a long time and fail to recover when it joins from a secondary to the primary controller, after the primary controller has failed. The MAP might need reboot to recover. **Conditions**: The issue can be reproduced consistently in the lab in the following conditions: 1. Two controllers: one primary and one backup. 2. Two RAPs, two MAPs: All mesh APs are on the primary controller. 3. Mesh tree is R1-M1, R2-M2. 4. Primary controller is disconnected from the network. 5. All APs associate with the backup controller, with the same mesh tree. 6. After *n* minutes, the primary controller is brought back online, and fallback is enabled. 7. It is observed that APs move back to associate with the primary controller. 8. MAP1 tries to associate with RAP2, instead of RAP1. 9. MAP1 authenticates and starts join/discovery process, but a continuous set of decrypt errors at MAP is observed and reported in traps at the controller. **Workaround**: Disable AP fallback so that if there is a failure, recovery can be done in a controlled manner.

Table 1-6 Open Caveats (continued)

ID	Description

CSCtw55476	LWAPP Primary Discovery Request sent by newer AP.
	
	Symptom: On a controller software Release 7.0.116.0, APs send LWAPP Primary Discovery Request every AP Primary Discovery Timeout (120 seconds, which is the default value) when ap-fast-heartbeat is enabled.
	
	This results in the following message logged on the msglog:
	
	The newer AP platforms such as CAP3500 do not need to send LWAPP Primary Discovery Request because the AP does not associate with the controller which supports only LWAPP.
	
	`(Cisco Controller) > show msglog`
	`Message Log Severity Level ..... VERBOSE`
	`*spamApTask0: Nov 24 17:26:17.051: %LWAPP-6-CAPWAP_SUPP_VER:`
	`spam_lrad.c:1821 Discarding Primary discovery request in LWAPP from AP`
	`cc:ef:48:xx:xx:xx supporting CAPWAP`
	`*spamApTask0: Nov 24 17:24:17.792: %LWAPP-6-CAPWAP_SUPP_VER:`
	`spam_lrad.c:1821 Discarding Primary discovery request in LWAPP from AP`
	`cc:ef:48:xx:xx:xx supporting CAPWAP`
	
	`/show run-config commands/`
	`advanced timers ap-fast-heartbeat local enable 1`
	
	Conditions:
	
	• Controller software Release 7.0.116.0.
	
	• APs: CAP3500, LAP1140, and so on.
	
	Workaround:
	
	• Ignore the messages.
	
	• Change msglog level.

CSCtw65316	Lag wih CDP does not show all the physical ports correctly. **Symptom**: CDP neighbors on the switch, where controller is connected to, does not display correct port information. **Conditions**: LAG is enabled on the controller and CDP is enabled on both sides and on the controller, number of ports connected are either 3, 5, 6 or 7. **Workaround**: None.

Table 1-6 Open Caveats (continued)

ID	Description

CSCtw67184	System losing RAID after the power was tripped.
	
	Symptom: While booting up, the following error message appears on the attached monitor or on a serial console as follows:
	
	`"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 does not boot from the disk.
	
	Conditions: Cisco Flex 7500 Series Controller, which went through an accidental power interruption, that is, the power plug was pulled while the system was operational. Upon reboot, the RAID card could not find its configuration in the flash memory and therefore it could not boot.
	
	Workaround: When this situation is encountered, the users must enter WebBIOS, which is a RAID management tool. There are two versions of this:
	
	• One that uses extensive menus and requires an attached monitor.
	• Another that is completely based on the command-line interface (CLI).
	
	The CLI version can be accessed from the serial console. A prompt is displayed for this on the serial console soon after the error message is displayed.
	
	Enter the CLI version of the WebBIOS utility by pressing the Ctrl-Y key and then entering the following command:
	
	`CfgForeign -Import -a0`
	
	Next, reboot the server.
	
	Further Problem Description: When the Space key is pressed, the system does not boot from the disk. During bootup, the LSI WebBIOS loads as expected and shows two physical disks but no virtual disks. It appears that it has lost the RAID configuration that was present in the system.
	
	The controller went through an accidental power interruption, that is the power plug was pulled while the system was operational. Upon reboot, the RAID card did not find its configuration in the flash memory and therefore it could not boot. The flash configuration was corrupted or erased due to the power interruption. The RAID card keeps a backup of the configuration on the hard drives. However, when the card loses the configuration information in the flash, it does not automatically pick up the backup configuration information from the hard drives. The information on the hard drives is considered a ‘foreign configuration’ that requires user intervention.
	
	At this time, the system waits for users to take action. All the data on the hard drives are still intact.

CSCtw70290	Inconsistent limitation of characters for guest username. **Symptom**: Guest username can be more than 24 characters when using R/W account. **Conditions**: When creating a guest username, logged on to the controller with read/write access, the username can be more than 24 characters. This, however, is stated as a limitation for guest account usernames in the configuration guide. **Workaround**: None

Table 1-6 Open Caveats (continued)

ID	Description
CSCtw74145	Creation of default SNMP entries with nondefault values is denied. **Symptom**: A controller configuration file that is uploaded loses '**config snmp community ipaddr** *ip-addr netmask* **********'. This symptom affects controller deployment. **Workaround**: Reconfigure the controller after restoring by entering this command: **config snmp community ipaddr** *ip-addr netmask community-name*
CSCtx17062	Controller client statistics are not displayed. **Symptom**: Clients connect to the guest SSID. However, when the clients want to check the traffic of clients, values are not displayed as expected on the accounting packets. When users enter the **show client detail** *mac_addr* command, the client statistics are not displayed. **Conditions**: • Cisco 5508 Controller (AIR-CT5508-K9) running controller software Release 7.0.116.0. • APs configured as H-REAP local switching, central authentication. • Guest SSID used. **Workaround**: None.
CSCtx56334	H-REAP client does not experience a successful intercontroller L2 roam. **Symptom**: After a web authenticated client roamed from LAP1 (associated with controller1) to LAP2 (associated with controller2), the client required web authentication again. This appears to be a regression of another caveat with ID CSCtj02816. **Conditions**: • Controller software releases 7.0.116.0 and 7.0.220.0 • LAP configuration: H-REAP local switching/central authentication • Controller software Release 7.0.98.0 was not affected • AP Local mode (no H-REAP) • H-REAP client roamed from a LAP associated with a controller to another LAP associated with the same controller (Intracontroller roaming) **Workaround**: Changing LAP mode as Local (not H-REAP) might resolve this issue.

Table 1-6 Open Caveats (continued)

ID	Description

CSCtx03556	TACACS user login failure on a Cisco 5508 Controller running controller software Release 7.0.116.0.
	
	Symptom: TACACS user login failure on a Cisco 5508 Controller running controller software Release 7.0.116.0.
	
	1. Enter the **debug aaa tacacs enable** command in the controller CLI while the TACACS user attempts to log on. The following is didsplayed:
	
	`(Cisco Controller) >*aaaQueueReader: Oct 11 20:14:45.909: TPLUS Transmission Queue Full -- dropping accounting packet`
	
	2. Enter the **show traplog** command. The following is displayed:
	
	`29 Tue Nov 29 09:52:16 2011 AAA Authentication Failure for UserName:zzzz User Type: WLAN USER`
	
	`30 Tue Nov 29 09:52:20 2011 AAA Authentication Failure for UserName:zzzz User Type: WLAN USER`
	
	`*aaaQueueReader: Nov 29 09:52:16.014: tplus_processAuthRequest: memory alloc failed for tplus message`
	`*aaaQueueReader: Nov 29 09:52:20.779: tplus_processAuthRequest: memory alloc failed for tplus message`
	`*aaaQueueReader: Nov 29 09:52:26.631: tplus_processAuthRequest: memory alloc failed for tplus message`
	
	3. Enter the **show msglog** command. The following is displayed;
	
	`*emWeb: Nov 29 09:52:16.335: %EMWEB-1-LOGIN_FAILED: ews_auth.c:2105 Login failed for the user:zzzz. Service-Type is not present or it doesn't allow READ/WRITE permission..`
	`*aaaQueueReader: Nov 29 09:52:28.335: %AAA-3-MEM_ALLOC_FAILED: tplus_db.c:511 Error allocating 4704 bytes on stack for message. Aborting..`
	`*emWeb: Nov 29 09:52:28.302: %EMWEB-1-LOGIN_FAILED: ews_auth.c:2105 Login failed for the user:zzzz. Service-Type is not present or it doesn't allow READ/WRITE permission..`
	`*aaaQueueReader: Nov 29 09:52:28.302: %AAA-3-MEM_ALLOC_FAILED: tplus_db.c:511 Error allocating 4704 bytes on stack for message. Aborting..`
	`*emWeb: Nov 29 09:52:28.298: %EMWEB-1-LOGIN_FAILED: ews_auth.c:2105 Login failed for the user:zzzz. Service-Type is not present or it doesn't allow READ/WRITE permission.`
	`*aaaQueueReader: Nov 29 09:52:28.298: %AAA-3-MEM_ALLOC_FAILED: tplus_db.c:511 Error allocating 4704 bytes on stack for message. Aborting..`
	
	Conditions: Cisco 5508 Controller running controller software Release 7.0.116.0.
	
	Workaround: Use local user account on the controller.

Table 1-6 Open Caveats (continued)

ID	Description

CSCtx52965	Cisco WiSM2 may reset under prolonged and very high client roaming conditions.
	Symptom: Crash file has an output similar to the following:
	`Analysis of Failure:`
	`Software Failed on instruction at :`
	`pc = 0x11301158 (eap_peer_receive_event+392), ra = 0x10bae188 (eap_peer_receive_event+392)`
	`Software Failed while accessing the data located at :0x6c6f62fd`
	Conditions: 1000 APs with 15000 clients associated to the Cisco WiSM2 with 1000 client roams per second on WLANs configured with 802.1X (WEP 104) and LEAP.
	Workaround: Avoid use of local authentication in large deployments. We recommend that you use external AAA server for large deployments.
	Further Problem Description: This condition occurred under prolonged, high client roaming conditions (approximately 25 to 30 minutes) with the maximum number of clients (15000) associated with the controller. This is not a supported deployment scenario in which local authentication is configured for use by 15000 clients and roaming is simulated at the rate of 1000 roams per second.

CSCtx60459	Retry count of 802.11 MAC counters display incorrect value in AP statistics. **Symptom**: After AP1142 is reset, connect one client and initiate constant ping to the gateway. The retry count of 802.11 MAC counter in test AP statistics is 21220 and it is nearly ten times larger than the Tx Frame count of 2279. This makes the statistics incorrect if users try to investigate retry percentage. The other counters might also be incorrect. It does not appear to be consistent with what is shown in the output of the **show controller do1** command if there is SSH into the AP. **Conditions**: Controller software Release 7.0.220.0. **Workaround**: None.
CSCtx69189	Cisco WiSM2 multicast IGMP proxy delay under load. **Symptom**: Wireless multicast message delivery delay of around 5 to 10 seconds. **Conditions**: Controller software Release 7.0.116.0 in multicast-multicast mode. **Workaround**: Unknown.

Table 1-6 Open Caveats (continued)

ID	Description
CSCtx91550	When `sh wlan apgroups` is generated, an error message is generated in syslog for all nondefault group APs. **Symptom**: 1. Error message is incorrect. This can be tested for any AP on the nondefault group. 2. Error message is sent to syslog, not to buffered logging (`sh msglog`), regardless of level, should be sent to both if using the same error level. 3. Error message does not show which is the wrong AP. Thus, it is difficult to determine the issue and correct because of incomplete data to troubleshoot. `*emWeb: Feb 08 18:00:08.328: %CLI-7-RAD_APGROUP_NOEXIST: cli_apf.c:35414 AP is moving from apgroup  AP Group to default-group.` **Conditions**: Command is entered. **Workaround**: None required. This issue has no effect on the AP group.
CSCtx92968	Controller SXP peering with ASA after long (random) delays. **Symptom**: SXP connection from controller to ASA is in 'Pending On' status. **Conditions**: Establishing SXP connection between controller and ASA. **Workaround**: Options include the following: • Wait for 5 to 8 minutes for the SXP connection to establish automatically. • Delete the connection from one end and reconfigure the connection.
CSCtx95544	Packets from H-REAP and locally switched WLAN should never egress the controller. **Symptom**: It is observed that the 6500 switch learns a lot of client MAC entries from the management interface of the controller. These correspond to MAC addresses of the locally switched H-REAP clients. **Conditions**: H-REAP locally switched clients send MDNS, TCP, and other traffic to the controller. This traffic sent between the time the controller moves the client into RUN state and the AP being informed of this causes the packets from the locally switched client to egress the controller. **Workaround**: Create a dummy interface and tie the WLAN to that interface with a dummy VLAN that does not exist on the switch. For MDNS traffic, enable IGMP snooping so that the controller sends only one report on behalf of all clients.

Table 1-6 Open Caveats (continued)

ID	Description

CSCtx94842	Client session stales on anchor controller.
	Symptom: Expired client sessions stales on the anchor controller.
	Conditions:
	1. Configure mobility between a Cisco 4404 Controller (AIR-WLC4404)and a Cisco 4402 Controller (AIR-WLC4402).
	2. Configure auto-anchor for WLAN.
	3. Connect the client to WLAN through the foreign controller.
	4. Wait till session timeout.
	Although anchor is notified about the expired session and deletes the entries based on debugs, for some client entries, the session stales on the anchor.
	Those entries cannot be cleared and results in increased current session time.
	For example:
	`<Cisco Controller> show client detail 00:26:c6:b6:cf:1e`
	`Client MAC Address..... 00:26:c6:b6:cf:1e`
	`Client Username ..... N/A`
	`AP MAC Address..... 00:00:00:00:00:00`
	`Client State..... Associated`
	`Client NAC OOB State..... Access`
	`Wireless LAN Id..... 1`
	`BSSID..... 00:00:00:00:00:ff`
	`Connected For ..... 121633 secs`
	`Channel..... N/A`
	`IP Address..... 192.168.87.190`
	`Association Id..... 0`
	`Authentication Algorithm..... Open System`
	`Reason Code..... 1`
	`Status Code..... 0`
	`Session Timeout..... 3600`
	Workaround: Reboot the controller to clear the 'stale' entries.

CSCtx98256	AP3502 connected to PoE-Out port of AP1522 loses power at random. **Symptom**: Mesh AP1522 at random stops providing power to AP3502e connected to PoE-Out port. **Conditions**: The mesh AP1522 is powered through AC power and the AP3502e is connected via PoE-Out port of mesh AP1522. The AP1522 is configured as a Root AP and has Ethernet connection to the controller. **Workaround**: Reboot the AP1522 as RAP.
CSCty28863	Client is deleted. **Symptom**: The client is deleted around 10 seconds after DHCP_REQD state even if it moved to RUN state in the meantime. It happens if the controller received a NAK from the DHCP server (even if ACK with valid IP is given later). **Conditions**: Controller software Release 7.2.103.0. **Workaround**: None.

Table 1-6 Open Caveats (continued)

ID	Description

CSCty29908	AP1252s in Local mode reboot; watchdog timer expired.
	Symptom: AP1252s restart and return with the following message:
	`------------------ show stacks ------------------`
	
	`Minimum process stacks:`
	`Free/Size Name`
	`4736/6000 soap_flash init`
	`5468/6000 Clock Update Proc`
	`5536/6000 dot11 platform init`
	`5904/12000 Init`
	`5360/6000 RADIUS INITCONFIG`
	`3728/6000 RAC I/F Conf.`
	`5480/6000 CDP Protocol`
	`2444/3000 Rom Random Update Process`
	`3892/6000 Hickory Sys Init`
	
	`Interrupt level stacks:`
	
	`Level Called Unused/Size Name`
	`4 22807426 7312/9000 SEC Interrupt`
	`5 0 9000/9000 M8349 GTM8 interrupt`
	`6 5395 8952/9000 NS16550 VECTOR`
	`7 27687684 8912/9000 M8349 PIT interrupt`
	
	`Spurious interrupts: 4788700`
	
	`System was restarted by watchdog timer expired`
	
	`System returned to ROM by watchdog timer expired`
	
	Conditions: Controller software Release 7.0.116.0.
	Workaround: None.

CSCty32663	**show run-config** commands: Invalid syntax for 802.11b rate disabled.
	Symptom: When disabling data rates or changing a rate to mandatory, the output keyword from the **show run-config** commands contains an upper case letter, which the CLI parser does not accept.
	Conditions: The following output is displayed:
	`802.11b rate Disabled 1`
	`802.11b rate Disabled 2`
	`802.11b rate Disabled 5.5`
	`802.11b rate Disabled 11`
	`802.11b rate Disabled 6`
	`802.11b rate Disabled 9`
	`802.11b rate Mandatory 12`
	
	`(wism2) config>802.11b rate Disabled 1`
	
	`Incorrect input! Use 'config 802.11b rate [disabled/mandatory/supported] <rate>'`
	Workaround: Use the command in the following manner:
	`(wism2) config>802.11b rate disabled 1`

Table 1-6 Open Caveats (continued)

ID	Description

CSCty32730	**show run-config** commands: Invalid syntax for 802.11b mandatory command.
	Symptom: On the output of the data rate commands, any changes in the mandatory rates should be output before disabled rates. If the disabled commands disable all the mandatory rates, the final disable command is rejected until the new mandatory rate is set.
	Conditions: The following output is displayed:
	`802.11b rate Disabled 1`
	`802.11b rate Disabled 2`
	`802.11b rate Disabled 5.5`
	`802.11b rate Disabled 11`
	`802.11b rate Disabled 6`
	`802.11b rate Disabled 9`
	`802.11b rate Mandatory 12`
	`input: (after correcting the issue with the upper case letters)`
	`(wism2) config> 802.11b rate disabled 1`
	`(wism2) config> 802.11b rate disabled 2`
	`(wism2) config> 802.11b rate disabled 5.5`
	`(wism2) config> 802.11b rate disabled 11`
	`Invalid parameter specified.`
	`(wism2) config> 802.11b rate disabled 6`
	`(wism2) config> 802.11b rate disabled 9`
	`(wism2) config> 802.11b rate mandatory 12`
	Workaround: Configure in the following order:
	`(wism2) config> 802.11b rate disabled 1`
	`(wism2) config> 802.11b rate disabled 2`
	`(wism2) config> 802.11b rate disabled 5.5`
	`(wism2) config> 802.11b rate mandatory 12`
	`(wism2) config> 802.11b rate disabled 11`

CSCty32835	**show run-config** commands: Missing DCA and band select commands. **Symptom**: Setting DCA and band select commands through CLI or GUI. **Conditions**: The DCA and band select commands are not displayed in the output of **show run-config** commands. **Workaround**: Use the TFTP backup.

Table 1-6 Open Caveats (continued)

ID	Description

CSCty32761	**show run-config** commands: Invalid index numbers for RADIUS servers.
	
	Symptom: If RADIUS servers are assigned nonsequential index numbers, some of the output in the **show run-config** commands have the wrong index numbers.
	
	Conditions:
	
	The following is the input:
	
	`config radius auth delete 1`
	`config radius auth delete 2`
	`config radius auth delete 3`
	`config radius auth delete 4`
	`config radius auth delete 5`
	`config radius auth add 3 10.10.10.64 1645 ascii 456fv3456jcy`
	`config radius auth add 4 10.10.10.65 1645 ascii 456fv3456jcy`
	`config radius auth add 5 10.10.10.66 1645 ascii 456fv3456jcy`
	`config radius auth disable 3`
	`config radius auth disable 4`
	`config radius auth disable 5`
	`config radius auth rfc3576 enable  3`
	`config radius auth rfc3576 enable  4`
	`config radius auth rfc3576 enable  5`
	`config radius auth management 3 disable`
	`config radius auth management 4 disable`
	`config radius auth management 5 disable`
	`config radius auth enable 3`
	`config radius auth enable 4`
	`config radius auth enable 5`
	`config wlan radius_server auth add 2 3`
	`config wlan radius_server auth add 2 4`
	`config wlan radius_server auth add 2 5`
	
	Output similar to the following is displayed:
	
	`radius auth add 3 10.10.10.64 1645 ascii ****`
	`radius auth add 4 10.10.10.65 1645 ascii ****`
	`radius auth add 5 10.10.10.66  1645 ascii ****`
	`radius auth rfc3576 enable 3`
	`radius auth rfc3576 enable 4`
	`radius auth rfc3576 enable 5`
	`radius auth management 3 disable`
	`radius auth management 4 disable`
	`radius auth management 5 disable`
	`wlan radius_server auth add 2 1`
	`wlan radius_server auth add 2 2`
	`wlan radius_server auth add 2 3`
	
	Note The index number used on the final 3 lines are 1, 2, and 3 instead of 3, 4, and 5.
	
	Workaround: Use the TFTP backup.

Table 1-6 Open Caveats (continued)

ID	Description

CSCty32823	**show run-config** commands: Missing quotes for names with spaces.
	Symptom: Some commands allow for imbedded spaces by including the parameter in quotes. The output from the CLI does not include the quotes. Therefore, the command is invalid. For example, **wlan create** and **wlan apgroup add** are such commands.
	Conditions: The following is the input:
	`(wism2) config>wlan create 22 "test WLAN name" testSSID`
	
	`(wism2) config>wlan apgroup add newAPgroup "MY NEW AP-GROUP"`
	
	`output`
	
	`  wlan create 22 test WLAN name testSSID`
	
	`  wlan apgroup add newAPgroup MY NEW AP-GROUP`
	
	`Input of these commands:`
	
	`(wism2) config> wlan create 22 test WLAN name testSSID`
	
	`Incorrect input! Use 'config wlan create <WLAN id> <profile name> [<ssid>]'`
	
	`(wism2) config> wlan apgroup add newAPgroup MY NEW AP-GROUP`
	
	`HELP:`
	`Special keys:`
	`   DEL, BS .... delete previous character`
	`   Ctrl-A  .... go to beginning of line`
	`   Ctrl-E  .... go to end of line`
	`   Ctrl-F  .... go forward one character`
	`   Ctrl-B  .... go backward one character`
	`   Ctrl-D  .... delete current character`
	`   Ctrl-U, X .. delete to beginning of line`
	`   Ctrl-K  .... delete to end of line`
	`   Ctrl-W  .... delete previous word`
	`   Ctrl-T  .... transpose previous character`
	`   Ctrl-P  .... go to previous line in history buffer`
	`   Ctrl-N  .... go to next line in history buffer`
	`   Ctrl-Z  .... return to root command prompt`
	`   Tab, <SPACE> command-line completion`
	`   Exit    .... go to next lower command prompt`
	`   ?       .... list choices`
	
	`(wism2) config>`
	
	Workaround: Manually add the quotes for names with spaces.

CSCty32853	**show run-config** commands: Commands are missing Y or N for confirmation. **Symptom**: Some commands need a confirmation of ‘Y’ or ‘N’ to continue. The output of the **show run-config** commands does not include this prompt. **Conditions**: For example, configuring an AP global syslog host. **Workaround**: Proceed without any confirmation.

Table 1-6 Open Caveats (continued)

ID	Description
CSCty32880	**show run-config** commands: Missing line-feeds on some lines. **Symptom**: Line-feeds are missing on some lines when you enter **show run-config** commands. **Workaround**: Use the TFTP backup.

CSCty36053	The **show client detail** *mac-addr* command does not display client statistics values.
	
	Symptom: Only 6 Mbps rate is configured as mandatory on 802.11a radio.
	
	`(Cisco Controller) >show client detail xx:xx:xx:xx:xx:xx`
	`Client MAC Address..... xx:xx:xx:xx:xx:xx`
	`Client Username ..... test`
	`Client Statistics:`
	`Number of Bytes Received..... 0`
	`Number of Bytes Sent..... 0`
	`Number of Packets Received..... 0`
	`Number of Packets Sent..... 0`
	`Number of EAP Id Request Msg Timeouts..... 0`
	`Number of EAP Request Msg Timeouts..... 0`
	`Number of EAP Key Msg Timeouts..... 0`
	`Number of Data Retries..... 0`
	`Number of RTS Retries..... 0`
	`Number of Duplicate Received Packets..... 0`
	`Number of Decrypt Failed Packets..... 0`
	`Number of Mic Failured Packets..... 0`
	`Number of Mic Missing Packets..... 0`
	`Number of Policy Errors..... 0`
	`Radio Signal Strength Indicator..... Unavailable`
	`Signal to Noise Ratio..... Unavailable`
	
	Conditions: Unknown.
	
	Workaround: Unknown,

CSCty45920	Controller allows creation of dynamic interfaces with overlapping subnet.
	
	Conditions: This is usually seen when users create two dynamic interfaces with different VLAN IDs, but the subnets overlap. In the following example, the VLAN IDs are different but they have overlapping subnets:
	
	`vlan 10 IP address 172.16.5.1 255.255.0.0 Gateway 172.16.1.1`
	`vlan 12 IP address 172.16.25.25 255.255.224.0 Gateway 172.16.25.1`
	
	Workaround: Users must create dynamic interfaces with unique VLAN IDs and subnets to have a correct flow of traffic for the clients. Users must ensure that there are no multiple VLANs with overlapping subnets, which might cause issues with Layer 3 roaming of clients.

CSCty47582	Controller unresponsive when executing the **show ap eventlog** *ap-name* command. **Symptom**: Controller reboots with crash file created while executing the **show ap eventlog** *ap-name* command. **Workaround**: None.

Table 1-6 Open Caveats (continued)

ID	Description
CSCty55275	Controller responds to ARP REQ for clients on a different VLAN rather than the source VLAN. **Symptom**: Wired clients are unable to reach wireless clients due to receiving incorrect MAC information from the controller. **Conditions**: This occurs when using proxy ARP and a /16 network with multiple /24 networks. For example, 10.0.0.0/16 on the wired side and 10.0.1.0/24 on the wireless side. **Workaround**: Disable the VLAN from getting the ARP request that comes into the controller. This can be seen by entering the **show arp switch** command where the IP address of the wired client and VLAN are displayed.
CSCty64490	Controller GUI displays information about an AP even when the AP is not in the controller database. **Symptom**: Controller GUI displays information about an AP even when the AP is not in the controller database. **Conditions**: Controller software release 7.2.103.0. **Workaround**: Reboot the controller.
CSCty91749	High parallel QoS traffic streams cause radio transmission watchdog resets and radio coredumps. **Symptom**: High parallel QoS traffic streams cause radio transmission watchdog resets and radio coredumps. **Workaround**: None.
CSCtz05016	Problem receiving multicast on wireless clients on WiSM2. **Symptom**: Multicast and unicast traffic between controller and AP fails. **Conditions**: When the ‘Recover-config’ command is entered to download the config file from the TFTP server there is likely race condition that does not occur always and when it does happen the "replication group tunnels" are not getting plumbed to the DP and hence the communication between the WLC and AP is lost. This issue is only observed during ‘Recover-config’ and not always. **Workaround**: Changing the mode to "multicast-multicast" mode resolves the issue and further reverting to "multicast-unicast" mode also resolves the issue because this explicitly cleans the replication group tunnels to the DP.
CSCtz07676	Controller failed to bring up SXP connection with N7k. **Symptom**: SXP connection from controller to N7k report "On" on the controller side while N7k reports “Waiting for response.” **Conditions**: Establishing SXP connection between controller and ASA. **Workaround**: Add an intermediate device that supports SXP v2 between controller and N7k.

Table 1-6 Open Caveats (continued)

ID	Description

CSCtz13525	Controller secure password policies enforced for local net users on CLI.
	Symptom: Secure password policies, which are available for the management users, are invoked when changing the password for a local net user on the controller CLI. A local net user can be created with any username and password. Issue only occurs when you change the password.
	`(Cisco Controller) >show switchconfig`
	
	`802.3x Flow Control Mode..... Disable`
	`FIPS prerequisite features..... Disabled`
	`secret obfuscation..... Enabled`
	`Strong Password Check Features:`
	
	`case-check ...Enabled`
	`consecutive-check ....Enabled`
	`default-check .....Enabled`
	`username-check ......Enabled`
	
	`(Cisco Controller) >config netuser add test test wlan 0 userType permanent`
	
	`(Cisco Controller) >config netuser password test abcd`
	
	Use at least three of the following four classes in the password:
	• Lowercase letters
	• Uppercase letters
	• Digits
	• Special characters.
	Conditions: When changing the local net user password through the CLI. This issue is observed on all controller platforms running controller software releases 7.0.230.0 and 7.2.103.0.
	Workaround: Use the controller GUI to change the passwords for local net users.

CSCtz13994	Cisco 5500 Series Controller unresponsive and then reboots after a successful upgrade from a 7.0 to 7.2 release. **Conditions**: Upgrade from a 7.0 release to 7.2. The controller became unresponsive after a client tried to associate with the controller and tried to do web authentication. **Workaround**: This issue is not reproducible.
CSCtz24275	FlexConnect AP with VLAN support: enabling SSH causes the radios to reset. **Symptom**: Radios reset on AP after enabling SSH. **Conditions**: Troubleshooting connectivity issues for clients. **Workaround**: Enable SSH and telnet during a maintenance window on all FlexConnect locally switched APs to avoid bouncing the radios causing connectivity issues during business hours.

Table 1-6 Open Caveats (continued)

ID	Description
CSCtz28357	Accounting traffic statistics counters are unreliable with web authentication. **Symptom**: The RADIUS accounting "bytes sent/received" information sent at the end of a wireless client session might not be reliable because of the following reasons: • They are not real-time. Therefore, the traffic right before disconnection is not accounted for. • The traffic sent and received even before the client was logged on through web authentication was also accounted for (portal page counts as traffic). **Conditions**: Controller software releases 7.0.x and 7.2.103.0. **Workaround**: None.
CSCtz31572	H-REAP local switching: ARP issues and wrong VLAN seen in NCS. **Symptom**: NCS may report clients in the controller management VLAN, which is not configured for the SSIDs. These clients are not reachable. **Conditions**: H-REAP with local switching. Controller software Release 7.0.220.0. **Workaround**: None.
CSCtz35153	Multicast packets from the H-REAP local switching clients egress the controller. **Symptom**: Any multicast packets from the H-REAP local switching clients sent to the controller, egress the controller when clients are in the ‘web authentication required’ state. **Conditions**: This is not reproducible and is observed only on the customer site deployment. **Workaround**: Unless IGMP snooping is on.
CSCtz41068	Web authentication on MAC filter failure; authentication sporadically fails when using a freely available RADIUS server. **Symptom**: Web authentication on MAC filter failure; authentication sporadically fails. **Conditions**: • Controller software Release 7.0.116.0 or 7.0.230.0. • Free RADIUS Server authentication for MAC authentication. • Default 1 second access-reject timer. • Clients may fail to get redirected to the web authentication splash page for authentication attempt, and remain in the 'DHCP required' state. **Workaround**: Configure the RADIUS server’s access-reject response timer to zero.
CSCtz43631	Controller keeps the ghost client entry. **Conditions**: Network between the controller and H-REAP is unstable. **Workaround**: To delete the ghost entry, the following options are available: • Disable the WLAN and then enable the WLAN. • Configure session timeout.

Table 1-6 Open Caveats (continued)

ID	Description
CSCtz48004	APs seen to dissociate from the controller when sysname is 31 characters long. **Conditions**: • AP1261 and AP1142 • Cisco 5508 Controller • Controller software Release 7.2.103.0 **Workaround**: Restrict the controller system name length to 30 characters.
CSCtz55837	Mesh AP unable to associate using mesh security EAP. **Symptom**: Mesh AP unable to associate using mesh security EAP. **Workaround**: Use mesh security 'PSK'.
CSCtz50719	Cisco WiSM unresponsive due to out of memory. **Symptom**: Controller unresponsive due to out of memory issue with logs such as the following: `Out of Memory: Killed process 1044 (switchdrvr)` **Conditions**: Very high CPU utilization. **Workaround**: None.
CSCtz07676	Controller cannot establish SXP connection with a Cisco Nexus 7000 Series switch. **Symptom**: An SXP connection from the controller to the Cisco Nexus 7000 Series switch reports the On state on the controller side while the switch reports the Waiting for Response state. **Conditions**: Establishing SXP connection between the controller and ASA. **Workaround**: Add an intermediate device that supports SXPv2 between the controller and the Cisco Nexus 7000 Series switch.

Resolved Caveats

Table 1-7 lists caveats resolved in controller software release 7.2.110.0.

Table 1-7 Resolved Caveats

ID	Title
CSCtx64420	Error message appears when Cisco 2500 Wireless Controller and Cisco Flex 7500 Controller are unconfigured for the first time.
CSCtz48004	APs seen to dissociate from the controller when sysname is 31 characters long.
CSCtr70376	Access Point Group Profile when uploaded using the TFTP does not contain the RF Profile information.
CSCtz49941	Cisco 5508 Controller unresponsive due to memory corruption.
CSCtx17373	Lightweight Access Point syslog level setting cannot be saved.
CSCts52226	Controller refuses the EAP-ID response from the client.

Table 1-7 Resolved Caveats (continued)

ID	Title
CSCtt19986	Cisco 5508 Controller repeatedly unresponsive due to being out of memory.
CSCth19326	cldCountryTable is not lexicographically ordered.
CSCtw50829	AP goes to DISCOVERY state after %DOT11-2-NO_CHAN_AVAIL_CTRL by DFS.
CSCtw69980	DCA 802.11b invalid channel 17 & 21 on certain country code configuration.
CSCtx02515	A library used for controller web pages, may cause high CPU if CPU ACL allows traffic to TCP port 4242, which is blocked by default.
CSCtx08257	DHCP address assignment required is not retained after a reboot.
CSCtx14684	SNMP response delays and ICMP port unreachable.
CSCtx17650	The Cisco Wireless LAN Controllers may experience a partial denial of service condition when receiving certain malformed HTTP/HTTPS packets.
CSCtx27358	WLC does not respond to SNMP after some time.
CSCtx43418	AP-manager replies to ping on port1 when connected to port2.
CSCtx43436	1522CM RAP is blacklisting the Ethernet/Cable interface.
CSCtx49189	Preauthentication ACL is removed from web authentication WLAN.
CSCtx52191	Web GUI fails when the ‘<‘ (less than symbol) is used in WLAN profile or SSID.
CSCtx60002	1522: Errant Regulatory Domain check failure for country code Panama.
CSCtx61062	Duplicate client entries are present in the ARP table of the controller.
CSCtx61744	Cisco 600 Series OEAP has a low TCP throughput for its personal SSID.
CSCtx67950	RRM queue unresponsive.
CSCtx68753	HTTP parser errors.
CSCtx72143	WCS/MSE 7.0.220.0 raises a WIPS alert for ChopChop attack even though WEP is not being used.
CSCtx80300	CVE-2008-5161 is not patched into the controller SSH code.
CSCtx80961	Controller stops accepting any new client associations (or reassociations), due to depletion of timers.
CSCtx95858	WLANs are appended when nonalphanumeric symbols are used in WLAN SSID.
CSCty04385	AP3600: DSCP value 46 (EF) is not forwarded from UP5 to UP6.
CSCty05792	Wireless clients receive GARP from different a VLAN.
CSCty07036	CCKM EAPOL broadcast key rotation break at M5 exchange.
CSCty07426	Controller shows 500 AP support for Evaluation License with 7.2.103.0.
CSCty15308	CAP3502P-Q reboots every 15 minutes with 7.0.230.0.
CSCty17976	High latency with wireless N clients on a Cisco Flex 7500 Series Controller running the controller software 7.2.103.0.
CSCty27692	ClientLink was disabled by default in the 7.2 release.
CSCty35602	Interface group use count error.
CSCty37471	A Cisco 5500 Series Controller unresponsive when a client with WPA2 PSK roams to another other Cisco 5500 Series Controller.
CSCty37818	H-REAP LocalSwitching client not counted on Attached Clients field.

Table 1-7 Resolved Caveats (continued)

ID	Title
CSCty38823	Controller Memory Leak in EAP Framework Task.
CSCty44701	Broken dynamic VLAN assignment when WLAN has FlexConnect Local Switching.
CSCty47430	Controller configuration with AE country code has channels not legal for 36 to 64.
CSCty49012	Controller sends RADIUS accounting retries faster than the configured timeout.
CSCty52472	H-REAP/FlexConnect clients may not report IP address correctly on the controller.
CSCty61970	AP group Radio policy changed to 'ALL' after upgrade.
CSCty71853	APs going off channel frequently causing clients to drop packets.
CSCty77318	CDP stops working after VLAN mapping is enabled.
CSCty82919	AP does not send deauthentication to nonexisting client on receipt of data frame.
CSCty84002	RADIUS calling-station-id is not preserved after upgrade to the 7.2 release.
CSCty89630	Controller does not convert sgt value from hexadecimal to decimal.
CSCty96959	Add back support for spaces in SSID.
CSCtz05201	Cisco 5508 Controller unresponsive on LDAP DP Task 2.
CSCtz07332	Deadlock on association processing in apfFindSiteTableEntry.
CSCtz13182	Mobility group stops working when management interface fails over to backup port.
CSCtz17758	Wireless client unable to manage anchor controller through HTTPS.
CSCtz18666	AP1520 generates unwanted DHCP discovers during the boot process.
CSCtz24594	Issues with controller deauthenticating EAP client on credential change.
CSCtz38309	Controller unresponsive at an SNMP task.
CSCtz48398	AP1552e cannot associate with a Cisco 2500 Series Controller join 2500 using country code Croatia.
CSCtz54101	Controller unresponsive during an initial IPv6 client association.

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:

http://tools.cisco.com/Support/BugToolKit/

(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/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/cisco/web/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/en/US/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.