Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.4.130.0

First Published: December 15, 2014
Last Updated: April 17, 2015

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

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

Contents

These release notes contain the following sections:

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

Cisco Wireless LAN Controller and Access Point Platforms

This section contains the following subsections:

Supported Cisco Wireless LAN Controller Platforms

The following Cisco WLC platforms are supported in this release:

- Cisco 2500 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Cisco Flex 7500 Series Wireless LAN Controllers
- Cisco 8500 Series Wireless LAN Controllers
- Cisco Virtual Wireless Controllers on Cisco Services-Ready Engine (SRE) or Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (UCS-E)
- Cisco Wireless Controllers for high availability (HA controllers) for 5500 series, WiSM2, Flex 7500 series, and 8500 series controllers
- Cisco Wireless Services Module 2 (WiSM2) for Catalyst 6500 Series switches
- Cisco Wireless Controller on Cisco Services-Ready Engine (SRE) (controllerM2) running on ISM 300, SM 700, SM 710, SM 900, and SM 910

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco 1040, 1130, 1140, 1240, 1250, 1260, 1600, 2600, 3500, 3500p, 3600, Cisco 600 Series OfficeExtend Access Points, AP801, and AP802
- Cisco Aironet 1550 (1552) series outdoor 802.11n mesh access points; Cisco Aironet 1520 (1522, 1524) series outdoor mesh access points
- The AP801 and AP802 are integrated access points on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the access points and the ISRs, see the following data sheets:
  - AP860:

    http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_461543.html
  - AP880:

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

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

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

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

– AP890:

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

Note The AP802 is an integrated access point on the Next Generation Cisco 880 Series ISRs.

Note Before you use an AP802 series lightweight access point with controller software release 7.4.130.0, you must upgrade the software in the Next Generation Cisco 880 Series ISRs to Cisco IOS 151-4.M or later releases.

Unsupported Cisco Wireless LAN Controller Platforms

The following controller platforms are not supported:

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

What's New in This Release

- Because of CSCur27551, Cisco WLC has a new behavior where SSLv3 is disabled by default. Older browsers, for example Microsoft Internet Explorer 8, might fail to connect over HTTPS because of compatibility issues. In such cases, you can explicitly enable SSLv3 by entering the **config network secureweb sslv3 enable** command.
- For other updates in this release, see the "Caveats" section on page 20.

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	7.4.130.0	—
	AIR-CAP1602I-xK910	7.4.130.0	—
	AIR-SAP1602I-x-K9	7.4.130.0	—
	AIR-SAP1602I-xK9-5	7.4.130.0	—
	AIR-CAP1602E-x-K9	7.4.130.0	—
	AIR-SAP1602E-xK9-5	7.4.130.0	—
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 7.4.130.0

Guidelines and Limitations

- WLAN-AP group association functionality:
  - Functionality prior to Release 7.4.130.0—If a WLAN was added to an AP group prior to Release 7.4.130.0, the RF radio policy is set to All after an XML upload/download. This is because the default value of RF policy was not added. This issue was addressed through CSCud37443. However, this corrects only the newly created WLAN-AP group associations and not the previous ones. Therefore, if you have configured a WLAN-AP group association prior to Release 7.4.130.0, you must remove the WLAN from the AP group and add it again in Release 7.4.130.0 or a later release.

    Also, the XML configuration for radio policy was not present in releases prior to 8.0. This issue is addressed through CSCul59089.
  - Change in functionality with Release 7.4.130.0—The RF radio policy is by default set to None for all WLAN-AP group associations created in Release 7.4.130.0. Any previous WLAN-AP group associations that are carried over will continue to be set to All unless a WLAN is removed from the AP group and added again.

    The XML upload/download for AP group RF radio policy is available only from Release 8.0.
- 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 7.4.130.0 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 7.4.130.0 release.
- We recommend that you install Wireless LAN Controller Field Upgrade Software for Release 1.7.0.0-FUS, which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA/MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. For more information, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_rn_1_7_0_0.html.
- If you are using a Cisco 2500 Series controller and you intend to use the Application Visibility and Control (AVC) and NetFlow protocol features, you must install Wireless LAN Controller Field Upgrade Software for Release 1.8.0.0-FUS. This is not required if you are using other controller hardware models. For more information, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_1_8_0_0.html

- When you enable LAG on a Cisco 2500 Series Controller with which a direct-connect access point is associated, the direct-connect access point dissociates with the controller. When LAG is in enabled state, the direct-connect access points are not supported. For direct-connect access points to be supported, you must disable LAG and reboot the controller.

  If LAG is enabled on the Cisco 2500 Series Controller and the controller is downgraded to a non-LAG aware release, the port information is lost and it requires manual recovery.
- After you upgrade to the 7.4 release, networks that were not affected by the existing preauthentication ACLs might not work because the rules are now enforced. That is, networks with clients configured with static DNS servers might not work unless the static server is defined in the preauthentication ACL.
- On 7500 controllers if FIPS is enabled, the reduced boot options are displayed only after a bootloader upgrade.

Note Bootloader upgrade is not required if FIPS is disabled.

- If you require a downgrade from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.
- It is not possible to directly upgrade to the 7.4.130.0 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 7.4.130.0. Table 2 shows the upgrade path that you must follow before downloading software release 7.4.130.0.

Table 2 Upgrade Path to Controller Software Release 7.4.130.0

Current Software Release	Upgrade Path to 7.4.130.0 Software
7.0.98.0 or later 7.0 releases	You can upgrade directly to 7.4.130.0 **Note** If you have VLAN support and VLAN mappings defined on H-REAP access points and are currently using a 7.0.x 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 7.4.130.0 to avoid losing those VLAN settings.
7.1.91.0	You can upgrade directly to 7.4.130.0
7.2. or later 7.2 releases	You can upgrade directly to 7.4.130.0 **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 7.4.130.0 controller software release. You must downgrade from the 7.4.130.0 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.

Table 2 Upgrade Path to Controller Software Release 7.4.130.0 (continued)

Current Software Release	Upgrade Path to 7.4.130.0 Software
7.3 or later 7.3 releases	You can upgrade directly to 7.4.130.0
7.4 releases that are prior to this release	You can upgrade directly to 7.4.130.0

- 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 7.4.130.0 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 7.4.130.0. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the Prime Infrastructure. If you attempt to download the 7.4.130.0 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 7.4.130.0 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 7.4.130.0 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 7.4.130.0 (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 7.4.130.0 controller software:

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

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

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

c. Click **Wireless LAN Controllers**.

The following options are available:

- Integrated Controllers and Controller Modules
- Standalone Controllers

d. Depending on your controller platform, click one of the above options.

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

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

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

g. Click a software release number.

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

i. Click **Download**.

j. Read Cisco's End User Software License Agreement and then click **Agree**.

k. Save the file to your hard drive.

l. Repeat steps a. through k. to download the remaining file.

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

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

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

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

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

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

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

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

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

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

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

a. In the Server Login Username text box, enter the username to log on to the FTP server.

b. In the Server Login Password text box, enter the password to log on to the FTP server.

c. In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

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

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

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

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

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

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

Step 19 To verify that the 7.4.130.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

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

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

Important Note for Customers in Russia

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

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

Downloading and Installing a DTLS License for an LDPE Controller

Step 1 Download the Cisco DTLS license.

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

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

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

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

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

Step 2 Copy the license file to your TFTP server.

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

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

  Management > Software Activation > Commands > Action: Install License

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

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

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

Upgrading from an LDPE to a Non-LDPE Controller

Step 1 Download the non-LDPE software release:

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

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

b. Choose the controller model from the right selection box.

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

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

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

f. Click **Download**.

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

h. Save the file to your hard drive.

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

Step 3 Upgrade the controller with this version by following the instructions from Step 3 through Step 19 detailed in the "Upgrading to Controller Software Release 7.4.130.0" section on page 7.

Interoperability With Other Clients in 7.4.130.0

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	7.4.130.0

Table 3 Test Bed Configuration for Interoperability

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

Table 4 Client Types (continued)

Client Type and Name	Version
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
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 7.4.130.0. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

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

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

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

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

Open Caveats

Table 5 lists the open caveats in this release.

Table 5 Open Caveats

ID	Headline
CSCts20040	Kernel oops when tried to disable SXP by configuration
CSCty84682	AP not forwarding mcast data and querier messages
CSCuc72713	WLC should not move the client to RUN state with LL IPv6 addr.
CSCuc78713	dWEP client cannot receive broadcast after broadcast key rotation
CSCuc98178	AP sends capwap data to wrong mac when hsrp is unconfigured

Table 5 Open Caveats (continued)

ID	Headline
CSCud07983	WLC not show inner username of Local EAP Transaction
CSCud26632	usmdb sync failure while changing channel width and channel number
CSCud69426	AAA Overridden ACL is not applied in WLAN Change
CSCue04517	Cannot disable 802.11 monitor measurements
CSCue44986	Client cannot detect SIP port while doing Face time call
CSCue56035	Various AP Predownload fixes
CSCue62171	HA: standby WLC forwards Multicast traffic on capwap tunnel
CSCue72667	8500 or vWLC doesn't include 4th SP data in response
CSCue86171	APs assigned power level is lower than min configured value.
CSCue88103	Traceback: #APF-3-VALIDATE_DOT11i_CIPHERS_FAILED
CSCue91034	Multicast: Handling link-local group addresses in CP/DP without L3 MGID
CSCue93501	Cannot select a-antenna option of AP by WLC's GUI
CSCue99208	Advance 802.11 monitor noise command is lost after reboot
CSCuf13997	Access vlan becomes -1 for web auth client when AAA is not configured
CSCuf56192	Unable to delete a mdns profile in a particular case
CSCuf57551	No need to validate name ACL on foreign WLC for auto-anchoring case
CSCuf93768	PI 1.3 displays incorrect POE status for AP
CSCug19228	SPWifi: config mesh linktest CLI broken
CSCug49148	Status LED on 1552 in local mode is blinking Green in Normal operation
CSCug73845	WLC NAS id override is taking system name
CSCug96865	Unexpected packet is send to RADIUS server periodically from standby WLC
CSCug97505	AP may send IAPP with DSCP different from 0
CSCuh16842	Override of assigned intf on intf group due to static IP breaks IPv6
CSCuh16870	Override assigned intf on intf group due to static IP removed on reauth
CSCuh20155	"2600/3600 AP gets into ""ap:"" mode after power cycle"
CSCuh46442	LAP displays %CAPWAP-3-ERRORLOG messages when AP join
CSCuh50505	WiSM2 or WLC crashed when enabling TPCv2 on 7.4.100.60
CSCuh94259	mDNS on Interface Group fails Active WLAN using interface group
CSCuh99194	Maximum number of Clients per AP Radio not working as expected
CSCui01912	AP1240 slave not predownloading image from primary AP.
CSCui23191	Release 7.4.110.0: 1242 AP predownload fails sometimes on upgrade
CSCui33284	Open SSID downstream packet loss due to Wireless Seq # Reset
CSCui55350	Continuous messages *dtlArpTask: osapi_sem.c:1179 Failed to acquire ..
CSCui65222	FlexConnect: VLAN-ACL at AP level does NOT work after HA - 7500 HA pair
CSCui65225	11k neighbor report response not sent when using AP-groups
CSCui73517	FlexConnect AP's radio interface reset on fault tolerance

Table 5 Open Caveats (continued)

ID	Headline
CSCui86670	DNS domain name not written to AP when configured w/ static IP from WLC
CSCuj05012	Radio reset: packets stuck in HW radio after channel change.
CSCuj07119	APgroup NASid override not honored when roaming between APs in dif group
CSCuj14843	vWLC: prevent service/data port confusion
CSCuj17683	802.11r Roaming: AP may sometimes send deauth with reason code 7
CSCuj29192	WLC: Traceback error seen with multiple instances
CSCuj32257	AP secures CAC bandwidth for SIP phone during inter WLC roaming w/o call
CSCuj36599	On the same Flex AP P2P blocking for 802.1x WLAN is broken
CSCuj60088	MM-3-MEMORY_READ_ERROR: msg logs on 5508
CSCuj66912	WiSM2 snmp get for secondary Power Supply is incorrect
CSCuj93777	Mesh AP should block data packets before BPDU packets are handled
CSCuj95892	Syslog Msg not generated when a port in a LAG comes back up
CSCuj96172	bsnDot11StationAssociate varbinds order is different than whats defined
CSCuj97293	wlc crashes at PKI_GetCertIssuerInfo w/ cmd show local-auth certificates
CSCul25617	Enabling AP Manager on WLC 2500 shows irrelevant mDNS profile popup
CSCul57266	Show client detail on WLC is inaccurate compared to the Flexconnect AP
CSCul72669	Deauth frame is not sent out before interface reset by RLDP
CSCul78198	RAID Volume Status should show proper error codes instead of unknown.
CSCul81000	Dirty interface logic broken for Interface Group override
CSCul87119	WLC log: ICMP dest unreachable reported as invalid ping response
CSCul99510	WGB client getting ip from different vlan
CSCum01621	FlexConnect local switching client VLAN shows N/A
CSCum21112	AP701E displays incorrect PoE status in WLC
CSCum50734	8510 crash when running show tech-support command
CSCum90765	WLC 5508 Drops fragmented packets
CSCun27153	Treat ff02::2:ffxx:xxxx/104 as link local multicast
CSCun36255	Configuring Bandwidth Parameters in QoS profile disables the WLAN status
CSCun45503	FlexConnect: wired client mac address table not updated on WGB roaming
CSCuo00381	FlexConnect group showing duplicate AP entry.
CSCuo20684	the value timestamp-tolerance is changed from 1000 to 0 after restoring
CSCuo44475	AP info file has wrong ws_management_version value
CSCup84060	Radio interface down with rcore on 1130 and 1240 APs
CSCup96353	HA enabled Controller crash Task: NFV9_Task
CSCuq09859	APs sending GARP and ARP requests aprox every 2 seconds.
CSCuq42751	WLC not sending all the Client attributes to PI
CSCuq88748	Rogue APs wrong classification from malicious to unclassified

Table 5 Open Caveats (continued)

ID	Headline
CSCur91010	“Failed backup “”config network multicast mode multicast {addr}”” on CT2504”
CSCuq86269	DFS detection due to broadcom spurious emissions
CSCuj65131	WiSM2: Webauth failing POST reply after 9990-10k clients
CSCun25338	rogue state changed by field is missing after config download.
CSCuo70899	traceback #APF-3-WLAN_OUT_OF_RANGE in HA 5500 standby controller
CSCup93935	RRM must not push DFS channel change to all of RF group

Resolved Caveats

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

Table 6 Resolved Caveats

ID	Headline
CSCsz82878	4.2 Mesh controller crashing with Task Name: reaperWatcher
CSCtc16222	FFT: %OSAPI-0-INVALID_TIMER_HANDLE: timerlib_mempool.c:240
CSCtj06944	Kernel panic - not syncing: Failed to allocate skb for hardware pool 0
CSCtn52995	AP association counter versus WLC association counter do not fit.
CSCtq32444	SNMP message port UP trap goes missing in LAG mode
CSCtx69300	CAPWAP-3-SEM_RELEASE_ERR errors in syslog
CSCuc32335	Access points lose config after power cycle
CSCuc41593	AP Flex Group and NAT parameters are not updated in Standby
CSCuc45005	RRM DCA task crash in Release 7.3.
CSCuc56829	Radio interface down with rcore
CSCuc65229	WLC crash if we clear the AP join statistics
CSCuc68995	Webauth fails on segmented HTTP GET
CSCuc69522	CWA anchor WLAN sends no TCP SYN ACK to client with IPV4Multicast GW MAC
CSCuc86805	Association request from the P2P Client Process P2P Ie and Update CB
CSCuc91441	not all clients purging from WLC client database once idle timer expired
CSCuc93681	5508 WLC (7.0.230.0) crashes in Task Name: sntpReceiveTask
CSCud09822	Called Station Id to be configurable in 802.1x Auth request
CSCud10632	Ignore MIC error reports from client for CCMP only BSSID
CSCud12582	Processing AAA Error ‘Out of Memory’
CSCud14147	WLC: RADIUS RFC3576 incorrect calculation of message authenticator
CSCud37443	“Clients connect in “”b/g”” even when ssid radio policy set explicitly “”a”””
CSCud50209	Crash on field manipulation for mgmtuser_create.html
CSCud57046	Client entry being seen on multiple controllers

Table 6 Resolved Caveats (continued)

ID	Headline
CSCud84109	Dual-Band AP may select the wrong country on the controller
CSCud89654	url-redirect-acl not working on local-switching enabled 802.1x WLAN
CSCud90600	Sanity check always reboots the primary WLC
CSCud97325	3600 AP sends invalid frames (0000.0104.xxxx) when changing primary WLC
CSCue02826	5ghz Fails on 1552-N in non-bridge mode joined to WLC with Brazil (-T)
CSCue17689	Unwanted message is seen in WLC after creating 512 wlan
CSCue33057	8500:Gateway address shown as reversed for ccxv5 diagnostics client
CSCue37691	Dot1x+Radius NAC : Client not authenticated with FlexConnect AP
CSCue38133	Need to reset 90 day license timer on secondary controller
CSCue50917	Root AP failing association as MAP when wired backhaul is lost
CSCuf01491	Local auth Local switching client is getting deleted after fast roam
CSCuf03454	Anchor Controller Hangs intermittently
CSCuf52235	per-WLAN user idle timeout breaks global timeout after upgrade
CSCuf54559	“WLC Crash when execute “”show mdns profile detailed”””
CSCuf74326	Valid vWLC license misinterpreted by vWLC : no AP count
CSCuf77821	Cisco Wireless LAN Controller Cross-Frame Scripting Vulnerability
CSCug14709	WLC doesn’t care about airespace wlan-id attr in access-accept
CSCug14713	WLC sends acct-update twice in the same millisecond
CSCug15064	7500 HA WLC always goes to MTC mode when MGMT/RMI is mapped to Port 2
CSCug19563	MMR1: Wism2 secondary crashes while boot due to deadlock
CSCug26521	WLC 7.4 in DHCP Proxy mode: option 255 missing in DHCP request packet
CSCug46616	RRM grouping state stuck in computation state.
CSCug51714	Clean up Error Messages about IPV6-3-INVALID_ADDR_ORPHAN
CSCug64950	AP group change to RAP in MAP mode results in stranded RAP
CSCug66306	WLC may deauthenticate a client before EAP-Identity-Request Timeout
CSCug73371	HA WLC reboots with: panic: System lockup - Watchdog Timeout
CSCug74517	WLC displays wrong interface name when having hundreds of interfaces
CSCug82805	RRM Group leader not getting formed for 2.4 GHz
CSCug83271	cpu ACL does not block ssh to virtual ip however telnet does
CSCug92421	WLC is reporting a large number of stale client entries
CSCuh09591	msglog: Service specific query: Sending serice specific query failed
CSCuh14797	Client not authenticating due to wrong mobility peer detail in Anchor
CSCuh25790	MMR1:Can’t reload the HA enabled WLC even after prednload completes
CSCuh26964	Crash observed during dynamic rf-group while HA switchover
CSCuh39893	WLC Login Fails When Using TACACS OTP Login Authentication
CSCuh42398	#NIM-3-CANT_DISABLE_MCAST: nim.c:4542 Cannot disable multicast state

Table 6 Resolved Caveats (continued)

ID	Headline
CSCuh42665	WLC 7.4 code sending invalid trap notification
CSCuh46355	Controller crashed with SNMPTask
CSCuh46996	Clients behind 3rd party WGB fail DHCP post upgrade from 7.0.116.0
CSCuh47502	crazy annoying dhcp server message scrolls when dhcp debug enabled
CSCuh65653	”Error “”standby booting”” while downloading config even if standby is up”
CSCuh66635	Maintenance mode auto recovery
CSCuh69558	Default intf takes precedence over foreign VLAN mapping w/ AAA override
CSCuh72474	Interface inside a group gets Dirty due to DHCP flood by client and NAK
CSCuh81923	WLC sends incorrect Radius accounting attributes
CSCuh92835	Cannot edit/change wlan config that has similar name and L2/L3 security
CSCuh97457	WLC incompatibility behavior on CoA for RFC 3576 implementation
CSCui01948	PI:SNMP operation to Device failed Table too large possible agent loop
CSCui09037	Hreap Client IP address didn’t get updated on WLC sometimes
CSCui09901	Controller crashed since user credentials sent as NULL.
CSCui15077	WLC crashes with cisco-av-pair url-redirect-acl is greater than 32 chars
CSCui23134	Controller crash spamPacketDumpHandleIntraRoamCase
CSCui23580	RAP loses static 5GHz channel 2.4GHz channel gets set to static
CSCui30568	WLC-HA RF Config Sync failed on Standby
CSCui35807	WLC: Crash with Task: nmspRxServerTask
CSCui48291	FlexConnect AP May Fail to Receive Input Traffic on Ethernet Interface
CSCui56456	RNG in Web Management Cookie is not cryptographically secure
CSCui56460	Insufficient entropy in RNG for RADIUS Authenticator
CSCui65855	WLC sending traffic from the virtual interface IP address on the wire.
CSCui70321	client not redirected to URL in web-passthru WLAN
CSCui72240	Active WLC crashes while transfer download and RP down
CSCui73764	Flex mode APs 1130 & 1240 series will not pass traffic on some wlans
CSCui75509	crash on wism2 running 7.5.102.0
CSCui75794	Foreign WLC doesn’t respond to ARP which is from foreign client -> local
CSCui77735	wlc 8510 7.3.112.0 crashed on taskname SNMPTask
CSCui82573	Double AID allocation in OKC Fast Roaming in FlexConnect
CSCui90116	AP sends FT-auth original and retry packet to WLC causing MIC mismatch
CSCui90233	Band-select feature not working with 8500/7500
CSCui94634	Flex AP disjoins after ACL push CAPWAP processing hangs DTLS timeout
CSCui95938	fast Switching SSDi and IPAD Issue
CSCui99062	Console gets to be unavailable after Ctrl+Shift+6 executed
CSCuj05274	”WLC Crash - Reaper Reset: Task “”loggerMainTask”” missed software watchdog”

Table 6 Resolved Caveats (continued)

ID	Headline
CSCuj07410	Clients on Flex AP Unable to Reauth on WPA2-PSK WLANs After Switchover
CSCuj13054	wism2 crashed after code update to 7.4.110.0 from 7.3.101
CSCuj15593	configuration with rf-profile commands cant be uploaded
CSCuj28495	clmgmtLicenseUsageCountRemaining does not reteun Remaining AP Count
CSCuj33535	Controller shows wrong client summary
CSCuj55832	client is able to associate acl is not present on wlc in aaa override
CSCuj58556	ap3500 lose names & configs w/ failover malloc failure in NSI
CSCuj58625	Local EAP FAST crashes WLC
CSCuj61455	FlexConnect Clients are being Deauthenticated for an Unknown Reason
CSCuj67203	show mesh neigh summary all showing non Mesh APs
CSCuj74920	Intermittent radius assigned vlan fails during inter-controller roam
CSCuj83637	WLC HA: service port with DHCP address loses connectivity after failover
CSCuj84379	“wlc crash - Reaper Reset: Task “”emWeb”” missed software watchdog”
CSCuj89107	WLC Crash with Task Name: spamApTask7 on 7.4.115.0
CSCul00381	WLC: DHCP w/VLAN pooling takes too long to switch vlans
CSCul04090	“Reaper Reset: Task “”SNMPTask”” missed software watchdog”
CSCul09432	7500 crashes with Task Name: osapiReaper
CSCul15555	FlexConnect AP decrypt errors after CCKM roam phone stuck in DHCP req
CSCul16796	EAP certificate transmission fails with vWLC running 7.5 with low PMTU
CSCul30107	WiSM2 crash due to DP failure on 7.5.102.0
CSCul33755	WLC’s not responding back to Apple clients that send out Unicast ARP’s
CSCul34417	WLCs stay in Active-Active without auto-recovery while network converges
CSCul35980	WISM2 silent crash on 7.5.102.0 code
CSCul38572	CCKM roaming failing between a 7.0 WLC and a 7.4.
CSCul42393	SNMP trap support for HA switchover
CSCul42704	WIPS-Rogue APs are mistaken as infrastructure devices
CSCul43158	Random mobile disassociation with PEM unknown timeout
CSCul44588	Channel N/A was shown in WIPS alarms
CSCul45107	WLC silent crash - Kernel Dump - 7.5.102.0
CSCul51785	Controller Crash on WiSM2
CSCul57988	Controller crashed Task Name: EAP Framework
CSCul64523	Flex Module sending new encryption keys when AP sends reass to same AP
CSCul72415	HA: need to handle almost concurrent Sanity Check & Heartbeat timeout
CSCul78541	AAA override client gets assigned to dynamic interface on roam on 7.4mr2
CSCul82199	WLC Crash when changing interface group config on 7.5.102.0
CSCul85903	Alpha: WLC Crash Bonjour_Process_Task

Table 6 Resolved Caveats (continued)

ID	Headline
CSCul94534	WiSM2 does not process fragmented client certificate
CSCul96254	Processing AAA Error 'Out of Memory'
CSCum05034	Debug client output clean up
CSCum06146	When using AP groups with interface groups clients get wrong VLAN
CSCum15629	1140 AP in Flexconnect Mode crash on 7.4.110.0 due to auth timer in loop
CSCum17998	8500wlc crashes when changing mgmt address w/ specfic downloaded config
CSCum26370	Static TX power level changes to Max after AP reboot
CSCum46098	HA false switch over due to keepalives loss possibly in the kernel stack
CSCum48150	PI reports client bandwidth utilization above 100%
CSCum48825	unable to ping from/to the management interface of wlc from same subnet
CSCum52951	Sanity: Client not getting ip after reauth in standalone mode
CSCum53429	AP1130/1240 FlexConnect VLAN mapping corrupted after VLAN mapping change
CSCum67742	RADIUS HTTP Profiling not working in latest pineridge build
CSCum71699	flex ap BVI down on vlan mapping push
CSCum73288	Friendly rogue AP disappears after 2 minutes.
CSCum86401	LAP in UNKNOWN_STATE on WLC
CSCum91313	WiSM2 Crash
CSCum92822	AID leak on 7.6.100.0 FlexConnect local sw scenario
CSCun18315	Radius server anomalies with WLC
CSCun32237	Wlan AVC stats code corrupts stack causing crash - Stack corruption
CSCun47705	Multicast direct (MC2UC) doesn't work on 8500 controller
CSCun69089	Vocera Badges Broadcast stops working randomly
CSCun87349	TACACS wireless role insufficient to modify Flexconnect VLAN mappings.
CSCuo20803	ACL rule direction is changed from any to out during backup
CSCuo21472	Wired Guest User configuration is not saved in backup config
CSCuo33271	WiSM2 crashed with DP watchdog on image 8.0.72.164
CSCuo38797	Frequent RRM TX power changes after upgrade from 7.3
CSCuo63103	Client local switching to central mode load aaa override radius nac
CSCuo78598	Direct AP not reaching its gateway after fallbacking from static IP.
CSCuo83496	WiSM2 HA - transfer download image getting failed
CSCuo86819	WLC crashes in 7.6.120.0 - memory corruption caused by Webauth
CSCup02770	WLC: SNMPTask process is growing at an alarming rate
CSCup18354	Japanese DBCS characters is garbled in internal Webauth login.html page
CSCup22587	Multiple Vulnerabilities in OpenSSL - June 2014
CSCup40557	HIGH CPU (98%) on webauthRedirect
CSCuq04522	OEAP access points lose config after power cycle

Table 6 Resolved Caveats (continued)

ID	Headline
CSCuq18025	High CPU 99% on webauth Redirect Task 7.6.122.9
CSCuq50181	OpenSSL issues August 2014 - WLC
CSCuq82202	WLC hung - No free Mbufs (ARP Fllod) available
CSCur27551	SSLv3 Poodle attack against https in wlc CVE-2014--3566
CSCul16911	CAPWAP causing APs to disassociate due to DTLS errors
CSCup22590	Multiple Vulnerabilities in IOS/IOSd OpenSSL - June 2014
CSCun94615	flood of DEBUG-4-INVALID_MODULE: [PA] debug. Unhandled debug module 191
CSCur66908	WLC Crashes on Bonjour_Process_Task
CSCtl96208	"""capwap ap hostname"" CLI returns ""ERROR!!! Command is disabled.""""
CSCtq82437	No CDP Neighbor details for LAP
CSCub96053	CAP3500 False radar detection by CP7925 phone
CSCub58537	Traffic must not be allowed when theWEP40 and WEP128 key size donot match
CSCuc81022	LAP1520 excessive DFS detection for in-band/off-channel weather radar
CSCud00274	N: non-native 802.11 frames incorrectly passed to the AP BVI1 interface
CSCud11674	Enabling broad-key Multicast downstream fails on wgb wired client.
CSCue04497	Radio reset: SC2 radio 'unresponsive thread' [BZ 804]
CSCue32755	Wireless client not able to associate to map with ethenet bridged client
CSCuf77488	wips alarm detection time stamp is ahead of AP clock
CSCuf89817	Unable to configure Network interface & Management page on 1550
CSCug21736	Memory leak at dot11_driver_cal_update_call_params (MallocLite)
CSCug40463	2600/3600 AP stops tx traffic after days with speed/duplex mismatch
CSCug57436	3502-Mesh eth bridging does not exclude gig0 failing to join over radio
CSCug73660	1602e AP has insufficient TxPower on 2.4ghz (13dbm)
CSCug88172	1600 series AP transmits small TKIP packets with MIC errors
CSCuh41274	Configuration vanishes from AP802 in standalone mode.
CSCuh52238	DFS Falsing from Broadcom Radio Emissions
CSCuh56733	Unable to configure power listed on show cont do1
CSCuh68059	1130s and 1140s keep crashing on REAP process
CSCuh76898	Client connection fails after WLC failover
CSCuh93838	Web Auth fails in FlexConnect AP in bootup standalone mode case
CSCui18377	ap1240 BADSHARE freeing packet in dot11_mgmt_sta_del() w/ FlexConnect AP
CSCui45546	Incorrect DTIM count field in AP beacons (1140/1040)
CSCui86001	Mesh AP does not retain its power level after restart
CSCuj70166	After DFS scan AP disassociates due to DOT11-2-NO_CHAN_AVAIL_CTRL
CSCul31732	FlexConnect Vlan mode was changed to Disabled after power cycle

Table 6 Resolved Caveats (continued)

ID	Headline
CSCum57455	dot11_rm_offchan tracebacks RADIO_INVALID_FREQ_FOR_CHAN
CSCuq04247	Flex/local-sw/central-auth/dhcp-required: psk 4-way handshake fail

Installation Notes

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

Warnings

Warning **This warning means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.** Statement 1071

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.: NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54).** Statement 280

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).** Statement 13

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground connector. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Read the installation instructions before you connect the system to its power source.** Statement 10

Warning **Do not work on the system or connect or disconnect any cables (Ethernet, cable, or power) during periods of lightning activity. The possibility of serious physical injury exists if lightning should strike and travel through those cables. In addition, the equipment could be damaged by the higher levels of static electricity present in the atmosphere.** Statement 276

Warning **Do not operate the unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 364

Warning **In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft. (2 m) from your body or nearby persons.** Statement 339

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.
2. Select your installation site with safety as well as performance in mind. Electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
3. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.
4. Plan your installation carefully and completely before you begin. Successfully raising a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.

5. When installing an antenna, remember:
   a. Do not use a metal ladder.
   b. Do not work on a wet or windy day.
   c. Do dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.
6. If the assembly starts to drop, get away from it and let it fall. Remember that the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer: **you!**
7. If any part of an antenna system should come in contact with a power line, do not touch it or try to remove it yourself. Call your local power company. They will remove it safely.
8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

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

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

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

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

Service and Support

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:

http://www.cisco.com/c/en/us/support/index.html

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

Related Documentation

For additional information about the Cisco controllers and lightweight access points, see these documents:

- The quick start guide or installation guide for your particular controller or access point

- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless LAN Controller System Message Guide*

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

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