Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.4.100.60

First Published: July 2013
OL-28134-02

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

The 7.4.100.60 controller software release is a maintenance release (Beta) based on the 7.4.100.0 release. The migration path is from 7.4.100.60 to the upcoming 7.4.x or later releases.

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

Contents

These release notes contain the following sections:

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

Cisco Unified Wireless Network Solution Components

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

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

- Cisco IOS Release 15.2(2)JB1
- Cisco Prime Infrastructure 1.3
- Mobility Services Engine (MSE) 7.4.100.0 software release and context-aware software

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

- Cisco 3355 Mobility Services Engine, Virtual Appliance
- Cisco 2500 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Cisco Flex 7500 Series Wireless LAN Controllers
- Cisco 8500 Series Wireless LAN Controllers
- Cisco Virtual Wireless Controllers on Cisco Services-Ready Engine (SRE) or Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (UCS-E)
- Cisco Wireless Controllers for high availability (HA controllers) for 5500 series, WiSM2, Flex 7500 series, and 8500 series controllers
- Cisco Virtual Wireless Controllers on Cisco Services-Ready Engine (SRE) or Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (UCS-E)
- Cisco Wireless Services Module 2 (WiSM2) for Catalyst 6500 Series switches
- Cisco Aironet 1550 (1552) series outdoor 802.11n mesh access points; Cisco Aironet 1520 (1522, 1524) series outdoor mesh access points
- Cisco 1040, 1130, 1140, 1240, 1250, 1260, 1600, 2600, 3500, 3500p, 3600, Cisco 600 Series OfficeExtend Access Points, AP801, and AP802

The AP801 and AP802 are integrated access points on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the access points and the ISRs, see the following data sheets:

- AP860:
  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_461543.html
- AP880:
  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78_459542_ps380_Products_Data_Sheet.html
  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/data_sheet_c78-613481.html
  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps10082/data_sheet_c78_498096.html

  - http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps10082/data_sheet_c78-682548.html
- AP890:

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

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

Note Before you use an AP802 series lightweight access point with controller software release 7.4.100.60, you must upgrade the software in the Next Generation Cisco 880 Series ISRs to Cisco IOS 151-4.M or later releases.

Controller Platforms Not Supported

The following controller platforms are not supported:

- Cisco 4400 Series Wireless LAN Controller
- Cisco 2100 Series Wireless LAN Controller
- Cisco Catalyst 3750G Integrated Wireless LAN Controller
- Cisco Wireless LAN Controller software on Cisco Services-Ready Engine (SRE) running on ISM 300, SM 700, SM 710, SM 900, and SM 910
- Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM)
- Cisco Wireless LAN Controller Module (NM/NME)

What's New in This Release?

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

Software Release Support for Access Points

Table 1 lists the controller software releases that support specific Cisco access points. The First Support column lists the earliest controller software release that supports the access point. For access points that are not supported in ongoing releases, the Last Support column lists the last release that supports the access point.

Table 1 Software Support for Access Points

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

Table 1 Software Support for Access Points (continued)

Access Points		First Support	Last Support
	AIR-AP1020	3.0.100.0	4.2.209.0
	AIR-AP1030	3.0.100.0	4.2.209.0
	Airespace AS1200	—	4.0
	AIR-LAP1041N	7.0.98.0	—
	AIR-LAP1042N	7.0.98.0	—
1100 Series	AIR-LAP1121	4.0.155.0	7.0.x
1130 Series	AIR-LAP1131	3.1.59.24	—
1140 Series	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—
1220 Series	AIR-AP1220A	3.1.59.24	7.0.x
	AIR-AP1220B	3.1.59.24	7.0.x
1230 Series	AIR-AP1230A	3.1.59.24	7.0.x
	AIR-AP1230B	3.1.59.24	7.0.x
	AIR-LAP1231G	3.1.59.24	7.0.x
	AIR-LAP1232AG	3.1.59.24	7.0.x
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1260 Series	AIR-LAP1261N	7.0.116.0	—
	AIR-LAP1262N	7.0.98.0	—
1300 Series	AIR-BR1310G	4.0.155.0	7.0.x
1400 Series	Standalone Only	—	—
1600 Series	AIR-CAP1602I-x-K9	7.4.100.60	—
	AIR-CAP1602I-xK910	7.4.100.60	—
	AIR-SAP1602I-x-K9	7.4.100.60	—
	AIR-SAP1602I-xK9-5	7.4.100.60	—
	AIR-CAP1602E-x-K9	7.4.100.60	—
	AIR-SAP1602E-xK9-5	7.4.100.60	—
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.

Note 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 7.4.100.60

Guidelines and Limitations

- 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 7.4.100.60 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 7.4.100.60 release.
- While a client sends an HTTP request, the Controller intercepts it for redirection to login page. If the HTTP request intercepted by Controller is fragmented, the Controller drops the packet as the HTTP request does not contain enough information required for redirection.
- We recommend that you install Wireless LAN Controller Field Upgrade Software for Release 1.7.0.0-FUS, which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA/MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. For more information, see http://www.cisco.com/en/US/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/en/US/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 7.4.100.60 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 7.4.100.60. Table 2 shows the upgrade path that you must follow before downloading software release 7.4.100.60.

Table 2 Upgrade Path to Controller Software Release 7.4.100.60

Current Software Release	Upgrade Path to 7.4.100.60 Software
7.0.98.0 or later 7.0 releases	You can upgrade directly to 7.4.100.60 **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 7.4.100.60 to avoid losing those VLAN settings.
7.1.91.0	You can upgrade directly to 7.4.100.60
7.2. or later 7.2 releases	You can upgrade directly to 7.4.100.60 **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 7.4.100.60 controller software release. You must downgrade from the 7.4.100.60 controller software release to a 7.2.x controller software release if you have an 802.11u HotSpot configuration on the WLANs that is not supported.
7.3 or later 7.3 releases	You can upgrade directly to 7.4.100.60

- 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 7.4.100.60 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 7.4.100.60. 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 7.4.100.60 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 7.4.100.60 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 7.4.100.60 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 7.4.100.60 (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 7.4.100.60 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, FTP, or SFTP server.

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

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

Step 5 Disable any WLANs on the controller.

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

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

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

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

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

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

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

Step 13 If you are using an FTP server, follow these steps:

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

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

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

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

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

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

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

Step 18 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 7.4.100.60 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 22 detailed in the "Upgrading to Controller Software Release 7.4.100.60" section on page 7.

Interoperability With Other Clients in 7.4.100.60

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	7.4.100.60
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 5.0.1
Apple iPad3	iOS 5.1.1
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
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R
Phones and Printers	
Cisco 7921G	1.4.2.LOADS
Cisco 7925G	1.4.2.LOADS
Ascom i75	1.8.0
Spectralink 8030	119.081/131.030/132.030
Vocera B1000A	4.1.0.2817

Table 4 Client Types (continued)

Client Type and Name	Version
Vocera B2000	4.0.0.345
Apple iPhone 4	iOS 5.0.1
Apple iPhone 4S	iOS 5.1.1
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 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 LAN 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.
- LAG
- TrustSec SXP
- Local authentication (controller acting as authentication server)
- Internal DHCP server
- Wired guest access

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 LAN 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 7.4.100.60. 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 5 lists the open caveats in the 7.4.100.60 controller software release.

Table 5 Open Caveats

ID	Description
CSCto02968	**Symptom**: Slow memory leak observed on a controller doing web authentication. Also, custom web page changes every 20 minutes. Buffer allocation for 64 pool goes very high in a few days. Follow up for CSCtl71583, as at least one leak is not yet fixed. This affects the 7.2 and later controller software releases only for IPSec and some CPU ACL scenarios.‘ **Workaround**: Reboot the controller.

CSCug86566	**Symptom**: Upon downgrading from the 7.4.100.60 to the 7.3.112.0 controller software release, the following errors are observed on controller console:
	`readCPUConfigData: cardid 0x6070001`
	`xml_mask_and_compare_with_value failed for node ptr_aclCfgData.aclTable.list.bitmask, masked value = 8, value = 0`
	`Validation for node ptr_aclCfgData.aclTable.list.action failed, indices for node are 0 64`
	`xml_mask_and_compare_with_value failed for node ptr_aclCfgData.aclTable.list.bitmask, masked value = 8, value = 0`
	`Validation for node ptr_aclCfgData.aclTable.list.action failed, indices for node are 1 64`
	`Cisco is a trademark of Cisco Systems, Inc.`
	Conditions: Downgrade.
	Workaround: No functionality impact detected; configuration seems to be the same.

CSCub24389	**Symptom**: Cisco 5508 controller stops responding using LSC with multiple APs (AP3500 and AP1131)
	Conditions: Stack Trace:
	`[0x001A1A60] crashdump(0x1a18dc)+0x184 [0x001A19B0]`
	`crashdump(0x1a18dc)+0xd4 [0x001CB2F8] get_block(0x1cb130)+0x1c8`
	`[0x001BA118] malloc(0x1b9e9c)+0x27c [0x005AAA08]`
	`spamProcessCertPayload(0x5aa9e8)+0x20 [0x00585BAC]`
	`lwapp_client_process_q(0x5859c0)+0x1ec [0x00586BB4]`
	`lwapp_client_process(0x58679c)+0x418 [0x001A5AF0]`
	`process_execute(0x1a5964)+0x18c`
	Workaround: Disable LSC on the controller.

CSCub63054	**Symptom**: VLAN Transparent enabled on a 7.2 controller software release does not pass VLAN tags. Span at the end device shows all frames being placed on the native VLAN. **Conditions**: VLAN Transparent enabled. **Workaround**: Disable VLAN Transparent and set the MAP Ethernet port as trunk.

Table 5 Open Caveats

ID	Description
CSCuc02149	**Symptom**: A 3600 series AP in either autonomous IOS or FlexConnect local switching mode drops IP6to4 TCP SYN ACK packets that are received from its LAN port. A wired sniff at the AP port shows, when the wireless client attempts to establish a TCP connection over IPv6 in IPv4, that the AP transmits the TCP SYN (in IPv6 in IPv4) to the switch, and receives the SYN+ACK from the switch, but fails to forward the SYN+ACK packet to the wireless client. The first time that the AP, after a reload, drops the SYN+ACK packet, the following message is displayed on the AP console, or in its log file: `WARNING - Received pak from RXTX port - Check log for detailed info` At the same time, the wireless client can successfully ping the IPv6 address of its 6to4 gateway. **Conditions**: A 3600 or 2600 series AP, in autonomous or FlexConnect local switching mode. Wireless client is attempting to establish TCP connections over IPv6 in IPv4, that is IPv4 protocol type 41. **Workaround**s: • Use a AP1040, AP1140, AP1260, or AP3500 • Disable IPv6 support on the application server • If you are using lightweight mode, use a centrally switched WLAN rather than a locally switched one.
CSCuc06605	**Symptom**: AP1142 r0 core dump: incorrect rcv pak pointer **Workaround**: None.
CSCuc99675	**Symptom**: AP802 might fail to change to FlexConnect mode. **Conditions**: AP802 in local mode **Workaround**: None. **Note** This is random issue, under investigation.
CSCud16350	**Symptom**: Apple iPhone and Apple iPad have intermittent connectivity issues with WPA2 and Cisco OEAP **Conditions**: WPA2 **Workaround**: None.

Table 5 Open Caveats

ID	Description
CSCud22588	**Symptom**: Traceback and message log flood with messages such as the following: `*mmListen: osapi_sem.c:1077 Failed to release a mutual exclusion object. mutex unlock failed, not owned by the calling thread.` **Conditions**: IPv6 enabled in the controller. You do not need IPv6 to be enabled on your wired network to see these error messages but this is coming from wireless clients that are IPv6 or IPv4 capable. These are cosmetic messages. **Workaround**: Disable IPv6 if IPv6 is not needed.
CSCud23648	**Symptom**: Controller with the 7.3.101.0 software release stops responding. **Conditions**: Task Name: osapiReaper User case: The system encountered a fatal condition at broffu_fp_dapi_cmd.c:3679 **Workaround**: None.
CSCud39329	**Symptom**: Controller 5500 on a 7.3 software release stopped working. **Conditions**: Task SXP SOCK **Workaround**: None.
CSCud41334	**Symptom**: Ethernet bridged client of a MAP does not work. **Conditions**: If the Ethernet bridged client has been plugged into the Ethernet port of a MAP before MAP joins the controller, the client will not work. The issue is seen on AP1140, AP3500, and AP3600 (all indoor MAPs). The issue is not seen on AP1552 (outdoor MAP). **Workaround**: Ensure that the bridged client is not plugged into the MAP Ethernet port and then reboot the MAP. Let MAP associate with the controller before plugging the client into the MAP Ethernet port. The client should get a valid IP address and should respond to pings.
CSCud41398	**Symptom**: With some specific clients (currently observed with only Android phones and Apple iPads), during downstream traffic, sometimes traffic flow is affected. The AP continuously transmits the same packets to the client even though the client has acknowledged. Only when the packet is transmitted as non-aggregate, the packet is successfully done from the AP end; all the aggregate packets are repeatedly transmitted. **Conditions**: This occurs only for downstream traffic with specific clients under BA exchange. **Workaround**: Disable aggregation.
CSCud63437	**Symptom**: Unplanned reboot on HA scenario after active reboot. **Conditions**: Network failover option is enabled. Low frequency issue. **Workaround**: None.

Table 5 Open Caveats

ID	Description
CSCud84135	**Symptom**: An access point upgraded to autonomous IOS 15.2(2)JB release has no IP connectivity to devices that are outside its local subnet. **Conditions**: Access point is using autonomous IOS 15.2(2)JB release, but does not have a default route configured. **Note** This is not an issue for lightweight IOS, which automatically install a default route to BVI1 if the default route is missing. **Workaround**: 1. Configure a default route. For example: ip route 0.0.0.0 0.0.0.0 <default-gateway-address> or ip route 0.0.0.0 0.0.0.0 BVI1 2. Disable IP routing. 3. If the AP gets its address from a DHCP server, configure a default gateway for the AP's scope in DHCP. **Further Problem Description**: In the 15.2(2)JA and earlier AP IOS software releases, 'no ip routing' was in effect. In this mode, the AP does ARP for all IP addresses if it does not have a default-gateway configured. In the 15.2(2)JB AP IOS release, 'ip routing' is enabled by default; in this mode if the AP does not have a default route, it drops traffic that is addressed to other networks.
CSCud97325	**Symptom**: AP3600 and AP2600 send invalid frames sourced with the 0000.0104.xxxx address. This might result in security warnings on the switch such as the following: `%AUTHMGR-5-SECURITY_VIOLATION: Security violation on the interface GigabitEthernet3/46, new MAC address (0000.0104.d634) is seen.` **Conditions**: This occurs when the primary or the secondary controller is changed in the AP High Availability tab. This issue is seen only with Cisco Aironet 2600 and 3600 Series Access Points. **Workaround**: None.
CSCue00164	**Symptom**: Standby unplanned reboot after mesh AP joins active controllers. **Conditions**: HA and mesh are in use. **Workaround**: Mesh APs are not supported on HA. **Further Problem Description**: Fix will prevent the incorrect handling of mesh AP information.
CSCue08874	**Symptom**: Tx power level is stored in the AP configuration file and has to be remembered after reboot. For AP1600, AP2600, AP3600, and the 802.11ac module, when the Tx power level is changed, say from level 1 to 4, then if AP is rebooted once or twice, the Tx power level goes back to 1. **Conditions**: STATIC Tx power level reset to 1 after several reboots of the AP. **Workaround**: Do not use STATIC Tx power for AP or do not reboot the AP. If changed, reconfigure the power.

Table 5 Open Caveats

ID	Description
CSCue09354	**Symptom**: Rogue AP does not get detected on wired when it is on a nonnative VLAN trunk to rogue detector AP. **Conditions**: 7.4.100.0 controller software release with rogue detector mode AP. Rogue AP not on rogue detector native VLAN. **Workaround**: None.
CSCue32755	**Symptom**: Wireless clients are unable to associate with mesh APs. **Conditions**: Wired clients go down, connected to the mesh AP that has Ethernet bridging enabled. **Workaround**: Reboot the mesh AP for the wired and wireless clients to associate.
CSCue34072	**Symptom**: Controller experiences leaking memory for task:mmlisten. **Conditions**: Unknown. **Workaround**: None.
CSCue51812	**Symptom**: Clients do not associate with the best serving AP; clients are observed to gain network access and roam relatively frequently. **Conditions**: Band Select enabled, default parameters or with less aggressive values (1 probe cycle, 100 ms suppression window). **Workaround**: Disable Band Select in high density environments.
CSCue55397	**Symptom**: Controller completes upgrade successfully, but the AP fails to do so. There are no errors except for APs failing to upgrade, and the corresponding syslog errors due to CAPWAP image request failure. This occurs on a high percentage of controllers. **Conditions**: Controller on a high load. **Workaround**: Reinstall controller software with no APs connected.
CSCue80531	dBm value is zero for AP802
CSCue97090	Standby controller reboots with GW not reachable with a backup port configured
CSCue99040	Cisco Flex 7500 and Cisco WiSM2 controllers have High Availability issues
CSCuf02268	HA controllers do not pair with 80ms RTT
CSCuf03309	**Symptom**: RDP sessions are timing out (no setup completed). Ping works. Moving client to another AP or VLAN solves the issue. **Conditions**: Cisco WiSM2 with DTLS enabled. **Workaround**: Disable DTLS.
CSCuf15633	**Symptom**: Unexpected controller reboot might happen when the **config wlan delete** command is entered. **Conditions**: The command is entered with multicast settings in place. **Workaround**: Use controller GUI to delete WLAN.

Table 5 Open Caveats

ID	Description
CSCuf35269	**Symptom**: 802.11u domain is lost after a controller reboot. **Conditions**: Same domain name is used on two different WLANs. This is allowed on controller CLI, but configuration validation fails on bootup. **Workaround**: Reconfigure the domain, or use different domain names.
CSCuf80340	**Symptom**: Internal web authentication is not working in virtual controller. **Conditions**: Cisco virtual controller. **Workaround**: None. **Further Problem Description**: Web authentication is a Layer 3 security feature that causes the controller to disallow IP traffic (except DHCP and DNS -related packets) from a particular client until that client has correctly supplied a valid username and password. It is an authentication method without the need for a supplicant or client utility. Web authentication is typically used by users who want to deploy a guest-access network. Typical deployments can include HotSpot locations such as T-Mobile or Starbucks.
CSCuf86303	**Symptom**: Controller stops responding with the following message displayed: `The system has encountered a fatal condition at broffu_fp_dapi_cmd.c:3820" and DP crashed with DP exception.` **Conditions**: This occurs when the controller is receiving multicast traffic at a very high rate. **Workaround**: None.
CSCuf93738	**Symptom**: It looks like the running configuration is correct as everything is working as expected and the **show run-config** command shows the correct configuration. However, if the configuration file .cfg is exported and opened, it is found that some AP groups reflect an old interface mapping that no longer exists, even if the configuration was saved. **Conditions**: Cisco 5508 controller using the 7.0.230.x software release. AP groups are in use with interface mappings. A WLAN to interface mapping is present and the interface is renamed using Cisco Prime Infrastructure. **Workaround**: Delete the AP group and create a new one.
CSCuf93777	**Symptom**: AP2600 and AP3600 fail with radio reset generating a core dump. **Conditions**: Monitor mode APs with active RLDP. **Workaround**: Disable RLDP.
CSCug04801	**Symptom**: After a couple of switchovers, none of the clients gets authenticated. **Conditions**: This is seen on doing a few failovers with 2000 802.1X authenticated clients with Cisco WiSM2 in an HA configuration. **Workaround**: None.
CSCug08318	**Symptom**: Controller stops responding in an HA scenario. **Conditions**: Very large user count; low frequency issue; under investigation. **Workaround**: None.

Table 5 Open Caveats

ID	Description
CSCug10935	**Symptom**: Primary controller and secondary controller configured as HA SSO and ACL is configured for clients. When the primary controller is down, the ACL is not inherited to the secondary controller after the switchover so that the client can access the previously restricted information. **Condition**: Unknown. **Workaround**: None.
CSCug10985	**Symptom**: After a software release upgrade, the standby controller might reboot twice during configuration synchronization. **Conditions**: HA enabled. **Workaround**: None. Impact is limited, standby controller works after configuration synchronization.
CSCug14709	**Symptom**: In a 7.4 controller software release, the controller does not take into account anymore if 'airespace wlan-identifier' attribute is sent back in access-accept by the RADIUS server. **Conditions**: This used to work in the 7.0.x release but does not work in the 7.4 release. It is not known whether this issue affects the 7.2 and the 7.3 releases. **Workaround**: Use another mechanism to restrict SSID access.
CSCug15064	**Symptom**: Controller goes into maintenance mode with HA enabled, if primary port is down. **Conditions**: Cisco Flex 7500 and Cisco 8500 series controllers; non-LAG scenario; backup port is configured and primary port is down. **Workaround**: None.

CSCug16473	**Symptom**: Controller using the 7.4.100.0 software release stops responding. With the previous controller software releases, the controller works as expected.
	The messages on the console during this failure is similar to the following:
	`broffu broffu_fp_helpers.c:294 SIOCGIFINDEX failed`
	`broffu_dtl0_create: SYSTEM-REBOOTING:could not bring data plane 0`
	Conditions: Console cable is connected.
	Workaround: Remove the console connection during bootup.

CSCug21037	**Symptom**: Standby controller stops responding when active controller starts to upgrade to a new software release. **Conditions**: Upload the software release to the active controller. The software release is upgraded successfully on the standby controller. Upload another software release to the active controller and the standby controller might stop responding. **Workaround**: Do not perform two software release upgrades in a row to the active controller.
CSCug22648	**Symptom**: WSSI module might not come up on some AP regulatory domain types. **Conditions**: AP3600 using regulatory domain different from –A, –E. **Workaround**: None.

Table 5 Open Caveats

ID	Description
CSCug23395	**Symptom**: Active controller might stop responding during operation, passing the control to the standby controller. **Conditions**: MSE is in use; rogue location is enabled. **Workaround**: Disable location for rogues.
CSCug29258	**Symptom**: FlexConnect mode AP with ACL is no longer filtering traffic. **Conditions**: Apply ACL to the FlexConnect AP. If the AP reboots while it is in standalone mode, the ACL might no longer be applied. It works if AP is in connected mode. Workaround: Connect AP to the controller.
CSCug41333	**Symptom**: AP with DTLS encryption enabled is disconnecting every 73 seconds. **Conditions**: DTLS encryption; default gateway MAC address has changed. **Workaround**: Prevent change of router MAC address.
CSCug42330	**Symptom**: Interface ACL on the controller might incorrectly apply on all the interfaces even on the one it is not applied on. **Conditions**: Controller using 7.0 to 7.3 software releases. **Workaround**: None.
CSCug45057	**Symptom**: 2.4-GHz and 5-GHz radios are disabled due to “Radio disabled due to inline power” error. **Conditions**: Upgrade to 7.4.100.0 **Workaround**: None.
CSCug48432	**Symptom**: With HA configured and after the secondary controller reboots, the secondary controller goes into maintenance mode. The reason to go to maintenance mode is communication down. We see the interface configuration gets lost on the secondary controller after reboot and it is found that there is no connectivity. **Conditions**: HA configured. **Workaround**: None.
CSCug57216	**Symptom**: Ascom phone stops receiving voice packets. **Conditions**: 802.11n in use; voice traffic QoS markings are lost in downstream direction. **Workaround**: Either fix QoS markings or disable 802.11n.
CSCug64750	**Symptom**: Traffic disruption on some specific devices (Apple) while on L3 roaming state. **Conditions**: ARP unicast generated by client, dropped by foreign controller. Client on mobile state. **Workaround**: None.

Table 5 Open Caveats

ID	Description
CSCue04528	**Symptom**: Controller stops responding on osapiBsnTimer task. **Conditions**: Cisco TrustSec SXP is enabled. HA is in use. **Workaround**: Either disable SXP or the HA features.
CSCug70229	**Symptom**: Web authentication fails for static IP client on export anchor or on foreign controller. **Conditions**: Unknown. **Workaround**: None.
CSCue91018	**Symptom**: SSID column in raw report from the controller shows incorrect data. **Conditions**: When netflow record is sent from the controller. **Workaround**: Use the same name for WLAN profile and WLAN SSID.
CSCug26521	**Symptom**: A controller using the 7.4 software release and option 82 with DHCP proxy enabled. It is found that the option 255 is missing in the DHCP request packets sent out by the controller thus resulting in packet being dropped during inspection. **Conditions**: 7.4 controller software release. **Workaround**: Set format to ASCII by entering this command: **config dhcp opt-82 format ascii** By default, the format is binary. Therefore, option 82 does not work.
CSCug73845	**Symptom**: Controller NAS ID override is taking system name instead of the NAS ID that is configured on the AP group/WLAN/Interface. **Conditions**: Configure AP group/WLAN/Interface NAS ID. **Workaround**: None.
CSCug18190	**Symptom**: After clearing configuration and rebooting the controller, if you configure HA again, the MAC address might be shown as different when you enter the **show mobility summary** command. **Conditions**: Configuration cleared. **Workaround**: This does not occur in a normal scenario, unless a full configuration wipe and reconfiguration process is done, and HA is reestablished.
CSCug65454	**Symptom**: Controller may stop responding with a reason of Reaper Reset: Task "dtlArpTask" missed software watchdog. **Workaround**: None.
CSCug54108	**Symptom**: AP memory leak causes SSH (to AP) to fail. **Conditions**: SSH to AP does not work. **Workaround**: Reboot the AP.
CSCuf30537	**Symptom**: RADIUS CalledStationID attribute is not consistent between web authentication and 802.1X authentication processes. **Conditions**: RADIUS server checking MAC address in CalledStation ID. **Workaround**: None.

Table 5 Open Caveats

ID	Description
CSCud72601	**Symptom**: Ascom i62 phones start to do full authentication while roaming when the WLAN session timeout expires. **Conditions**: WLAN session timeout is configured and it expires. The client does a reauthentication with a new PMK. **Workaround**: Disable session timeout on the WLAN.
CSCud33577	**Symptom**: FlexConnect AP does not work as expected. **Conditions**: When FlexConnect AP cannot renew DHCP lease, the BVI1 interface goes down. **Workaround**: Reboot the AP or increase lease time to a higher value. You can also use static IP addresses on the AP. Create a VLAN 1 from the FlexConnect group. **Further Problem Description**: This issue is not seen if the native VLAN on the FlexConnect AP is set to 1.

Resolved Caveats

Table 6 lists the caveats that are resolved in the 7.4.100.60 controller software release.

Table 6 Resolved Caveats

ID	Title
CSCty50404	Some of the RF profile configuration was not saved to uploaded configuration file
CSCub88183	Controller stopped responding at emWeb instruction: ewaFormSubmit_login_callback
CSCuc03576	ARP issues with MAPs
CSCuc07384	Web access issue on SRE in the 7.2 controller software release
CSCuc22875	Cisco Flex 7500 controller: HA Disabled CIDS query failed after changing the management IP address
CSCuc52952	75 DUP service IP address error messages seen on 6500 for WiSM2 in H setup
CSCuc84338	AP1550 appeared in local mode instead of MAP or RAP mode
CSCuc90398	RCB synchronization for the USMs which had radids as an argument
CSCuc95993	AP sent out ARP request for different subnet IP address
CSCud10200	AP1552 in local mode not obeying 30-minute channel blacklist after DFS event
CSCud16003	MSAP was unavailable after a certain period
CSCud28220	SFTP download failed on HA+LAG controller with high link delay
CSCud40050	Unable to find 802.1X interface; client was not authenticating after failover
CSCud62969	AP1600 was not deferring NDP and rogue containment with high traffic

Table 6 Resolved Caveats (continued)

ID	Title
CSCud67549	Cisco Flex 7500 controller stopped responding in task: emWeb
CSCud78560	Controller updated mDNS TTL with incorrect values when snooping is disabled or enabled
CSCud78928	Several client traps were disabled on controller reboot
CSCud83441	RADIUS callStationIdType was changed from radio to Ethernet MAC
CSCud93574	Memory leak was observed on the anchor controller for a client authentication trap
CSCud95613	Cisco WiSM2 stopped responding after upgrading to the 7.4.100.0 controller software release only when there was a high traffic load
CSCud97830	Telnet access to controller was lost
CSCud97983	AP1142 stopped responding after upgrading to the 7.4.100.0 controller software release
CSCud99466	Debug leaked due to lack of MAC address for APF
CSCue00375	System stopped responding in SNMP for AP CAPWAP retransmit change push
CSCue01983	AP3600 sent continuous corrupted deauthentication frames when in WIPS on the 7.4.100.0 controller software release
CSCue02707	HA redundancy did not fail over to the standby controller when powercycled
CSCue02718	HA redundancy did not fail over to the standby controller when the Ethernet cable was removed
CSCue04153	DP stopped responding because of DP exception
CSCue08313	AP stopped responding; client disconnected periodically
CSCue08660	High CPU stopped responding on mobility task mmlisten
CSCue13108	TPC reduced transmit power to lower than expected values
CSCue14501	WSSI interference forced DCA to change channels on serving radios
CSCue17421	RRM AP neighbor list was not synchronized to the HA standby controller after a switchover
CSCue19334	DHCP socket task nfaSyncMsgSendToTask dhcpSendRaw failed
CSCue26900	Controller stopped responding in ssh_x509_cert_decode
CSCue26907	Controller stopped responding in SrDoSnmp
CSCue26960	Pmalloc trailer issue - sshmp-integer-core.c
CSCue26968	Controller stopped responding in dtls1_buffer_message
CSCue27021	Memory leak observed with multicast DNS
CSCue30626	Insufficient output when the **show 802.11{a | b} cleanair air-quality summary** command was entered
CSCue32955	Wired guest did not get IP address on the controller
CSCue33125	Unable to enable bootp-broadcast with HA SSO configured

Table 6 Resolved Caveats (continued)

ID	Title
CSCue33222	Controller stopped responding on the 7.4.100.0 controller software release with mDNS service enabled
CSCue34763	Clients hit idle timeout after successful authentication
CSCue35315	Client traps were disabled when downgraded to prior releases
CSCue35344	DHCP scope was configurable in Cisco Flex 7500 controllers
CSCue53220	Controller dropped wireless to wireless client traffic with source UDP/16666
CSCue54977	RF profile configuration was not shown in the output of the **show run-config** commands
CSCue55191	Memory leak was observed in mm_listen.c line 8826
CSCue58727	Reaper reset controller due to mutex issue in spectrumRadSlotAQEnableGet
CSCue62388	AP rebooted with DOT11-3-NO_BEACONING “Not Beaconing for too long”
CSCue66112	HA link encryption was not established in some scenarios
CSCue71856	AP did not send traffic indication to client in power saving mode in time
CSCue83558	Cisco WiSM2 stopped responding due to Task Name: apfMsConnTask_6
CSCue87238	Cisco 5500 controller stopped responding on a 7.4 controller software release without any crashlogs
CSCue87884	AP1600 stopped forwarding DL traffic for 2 to 3 seconds occasionally
CSCue90110	Clients were not removed from AP after an HA failover
CSCue92521	Cisco 5500 controller stopped responding due to memory issue in task name spamApTask6

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, 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.