Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 5.2.157.0

November 21, 2008

Note Controller software release 5.2.157.0 is not supported for use in Japan.

These release notes describe open and resolved caveats for software release 5.2.157.0 for Cisco 2100 and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSM); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; Cisco 3201 Wireless Mobile Interface Cards (WMICs); Cisco Aironet 1100, 1130, 1140, 1200, 1230AG, 1240, 1250, 1300, and AP801 Series Lightweight Access Points; and Cisco Aironet 1130AG, 1240AG, 1522, and 1524 Mesh Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.

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

Contents

These release notes contain the following sections.

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

Cisco Unified Wireless Network Solution Components

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

- Software release 5.2.157.0 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 3.0
- Cisco Wireless Control System (WCS) software release 5.2.110.0
- Cisco WCS Navigator 1.4.110.0
- Location appliance software release 5.2.91.0
- Cisco 2700 Series Location Appliances
- Mobility service engine software release 5.2.91.0 and Context Aware Software

Note Client and tag licenses are required in order to retrieve contextual (such as location) information within the Context Aware Software. See the *Release Notes for Cisco 3350 Mobility Services Engine for Software Release 5.2* for more information.

- Cisco 3350 Mobility Services Engines
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers

Note The 5.2.157.0 release does not support the NM-AIR-WLC6 platform.

- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1130AG, 1240AG, 1522, and 1524 Mesh Access Points

Note This release does not support Cisco Aironet 1505 and 1510 access points.

- Cisco Aironet 1100, 1130, 1140, 1200, 1230AG, 1240, 1250, 1300, and AP801 Series Lightweight Access Points

Note Controller software release 5.0.148.0 or later is not compatible with Cisco Aironet 1000 series access points.

Note Only Cisco Aironet 1200 series access points that contain 802.11g (AIR-MP21G) or second-generation 802.11a radios (AIR-RM21A or AIR-RM22A) are supported for use with controller software releases. The AIR-RM20A radio, which was included in early 1200 series access point models, is not supported. To see the type of radio module installed in your access point, enter this command on the access point: **show controller dot11radio** *n*, where *n* is the number of the radio (0 or 1).

Note The 1250 and the 1140 series access points have a hardware limitation where beacons can only be output at intervals that are multiples of 17 milliseconds. When these APs are configured for a 100-millisecond beacon interval, they transmit beacons every 102 milliseconds. Similarly, when the beacon interval is configured for 20 milliseconds, these APs transmit beacons every 17 milliseconds.

Controller Requirements

The controller GUI requires the following operating system and web browser:

- Windows XP SP1 (or later) or Windows 2000 SP4 (or later)
- Internet Explorer 6.0 SP1 (or later) or Mozilla Firefox 2.0.0.11 (or later)

Note Internet Explorer 6.0 SP1 (or later) and Mozilla Firefox 2.0.0.11 (or later) are the only browsers supported for using the controller GUI and web authentication.

MIB Files

Cisco controllers support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com. Only one MIB is posted per major release (5.2, 5.1, and so on). If an updated MIB becomes available, the previous version is removed from the Software Center and replaced by the new version.

Software Release Information

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. As new releases become available for the controllers and their access points, consider upgrading.

Note The Cisco WiSM requires software release SWISMK9-32 or later. The Supervisor 720 12.2(18)SXF2 supports the Cisco WiSM software release 3.2.78.4 or later, and the Supervisor 720 12.2(18)SXF5 (Cisco IOS Software Modularity) supports the Cisco WiSM software release 4.0.155.5 (with Cisco IOS Software Modularity).

Note To use the Cisco WiSM in the Cisco 7609 and 7613 Series Routers, the routers must be running Cisco IOS Release 12.2(18)SXF5 or later.

Note The Cisco Wireless LAN Controller Network Module is supported on Cisco 28/37/38xx Series Integrated Services Routers running Cisco IOS Release 12.4(11)T2, 12.4(11)T3, and 12.5.

Note To use the controller in the Catalyst 3750G Wireless LAN Controller Switch, the switch must be running Cisco IOS Release 12.2(25)FZ, 12.2(35)SE or later, 12.2(37)SE or later, 12.2(44)SE or later, or 12.2(46)SE or later. The following Cisco IOS Releases and any variants are not supported: 12.2(25)SEC, 12.2(25)SED, 12.2(25)SEE, 12.2(25)SEF, and 12.2(25)SEG. All Catalyst 3750 software feature sets (IP Base, IP Service, and Advanced IP Services) are supported for use with the controller.

Note You can use the 2112 and 2125 controllers only with software release 5.1.151.0 or later.

Finding the Software Release

To find the software release running on your controller, click **Monitor** and look at the Software Version field under Controller Summary on the controller GUI or enter **show sysinfo** on the controller CLI.

Special Rules for Upgrading to Controller Software Release 5.2.157.0

Caution Before upgrading your controller to software release 5.2.157.0, you must comply with the following rules.

- Before you use an AP801 Series Lightweight Access Point with controller software release 5.2.157.0, you must upgrade the software in the Cisco 800 Series Integrated Services Router (ISR) to Cisco IOS Release 12.4(22)T.
- Make sure you have a TFTP or FTP server available for the software upgrade. Keep these guidelines in mind when setting up a TFTP or FTP server:
  - Controller software release 5.2.157.0 is greater than 32 MB; therefore, you must make sure that your TFTP server supports files that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd and the TFTP server within the WCS. If you attempt to download the 5.2.157.0 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 service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.
- 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 5.2.157.0. Table 1 shows the upgrade path that you must follow before downloading software release 5.2.157.0.

Table 1 Upgrade Path to Controller Software Release 5.2.157.0

Current Software Release	Upgrade Path to 5.2.157.0 Software
3.2.78.0 or later 3.2 release	Upgrade to 4.0.206.0 or later 4.0 release, then upgrade to 4.2.176.0, before upgrading to 5.2.157.0.
4.0.155.5 or later 4.0 release	Upgrade to 4.2.176.0 before upgrading to 5.2.157.0.
4.1.171.0 or later 4.1 release	Upgrade to 4.2.176.0 before upgrading to 5.2.157.0.
4.1.191.xM or 4.1.192.xM	You can upgrade directly to 5.2.157.0.
4.2.61.0, 4.2.99.0, or 4.2.112.0	Upgrade to 4.2.176.0 or to a 5.1 release before upgrading to 5.2.157.0.
4.2.130.0	Upgrade to 4.2.176.0 before upgrading to 5.2.157.0.
4.2.173.0 or 4.2.176.0	You can upgrade directly to 5.2.157.0.
5.0.148.0 or later 5.0 release	You can upgrade directly to 5.2.157.0.
5.1.151.0 or later 5.1 release	You can upgrade directly to 5.2.157.0.

Note When you upgrade the controller to an intermediate software release, wait until all of the access points joined to the controller are upgraded to the intermediate release before you install the 5.2.157.0 software. In large networks, it can take some time to download the software on each access point.

- Cisco recommends that you install the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file on all controller platforms. This file resolves CSCsm03461 and is necessary to view the version information for ER.aes files in the output of the **show sysinfo** CLI command. If you do not install this ER.aes file, your controller does not obtain the fix for this defect, and “N/A” appears in the Emergency Image Version field in the output of this command.

  Note The ER .aes files are independent from the controller software files. You can run any controller software file with any ER.aes file. However, installing the latest boot software file (5.2.157.0 ER.aes) ensures that the boot software modifications in all of the previous and current boot software ER.aes files are installed.

Caution If you require a downgrade from one release to another, you may 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.

Special Rules for Upgrading to Controller Software 5.2.157.0 in Mesh Networks

Caution Before upgrading your controller to software release 5.2.157.0 in a mesh network, you must comply with the following rules.

Upgrade Compatibility Matrix

Table 2 outlines the upgrade compatibility of controller mesh and non-mesh releases and indicates the intermediate software releases required as part of the upgrade path.

Software Upgrade Notes

- You can upgrade from all mesh releases to controller software release 5.2.157.0 without any configuration file loss.

  Note If you downgrade to a mesh release, you must then reconfigure the controller. Cisco recommends that you save the configuration from the mesh release before upgrading to release 5.2.157.0 for the first time. Then you can reapply the configuration if you need to downgrade.

- You cannot downgrade from controller software release 5.2.157.0 to a mesh release (4.1.190.5, 4.1.191.22M, or 4.1.192.xM) without experiencing a configuration loss.
- Configuration files are in the binary state immediately after upgrade from a mesh release to controller software release 5.2.157.0. After reset, the XML configuration file is selected.
- Do not edit XML files.
- Any field with an invalid value is filtered out and set to default by the XML validation engine. Validation occurs during bootup.
- If you upgrade the controller from software release 4.1.191.xM to 4.1.192.xM and then to software release 5.2.157.0, the controller might reboot without a crash file. To work around this issue, manually reset the controller without saving the configuration after you upgrade the controller to software release 5.2.157.0. Also, make sure to check the RRM configuration settings after the reset to verify that they are correct (CSCsv50357).

Table 2 Upgrade Compatibility Matrix for Controller Mesh and Non-Mesh Releases

Upgrade to	5.2	4.1.192.35M	4.1.191.24M	4.1.190.5	4.1.185.0	4.1.171.0	4.0.219.0	4.0.217.204	4.0.217.0	4.0.216.0	4.0.206.0	4.0.179.11	4.0.179.8	4.0.155.5	4.0.155.0	3.2.195.10	3.2.193.5	3.2.171.6	3.2.171.5	3.2.150.10	3.2.150.6	3.2.116.21	3.2.78.0	3.1.111.0	3.1.105.0
Upgrade from																									
4.1.192.35M	Y																								
4.1.192.22M	Y	Y																							
4.1.191.24M		Y	–																						
4.1.190.5		Y[1]	Y	–																					
4.1.185.0			Y	Y[2]	–																				
4.1.181.0				Y[2]	Y[2]																				
4.1.171.0				Y[2]	Y[2]	–																			
4.0.219.0					Y[2]	Y[2]	–																		
4.0.217.204			Y[2]		Y[2]	Y[2]	Y[2]	–																	
4.0.217.0					Y[2]	Y[2]	Y[2]	Y[3]	–																
4.0.216.0					Y[2]	Y[2]	Y[2]	Y[3]	Y	–															
4.0.206.0					Y[2]	Y[2]	Y[2]	Y[3]	Y		–														
4.0.179.11									Y		Y[4]	–													
4.0.179.8									Y		Y[4]	Y	–												
4.0.155.5									Y		Y[4]	Y	Y	–											
4.0.155.0									Y		Y[4]	Y	Y	Y	–										
3.2.195.10									Y		Y[4]	Y	Y	Y		–									
3.2.193.5									Y		Y[4]	Y	Y	Y		Y	–								
3.2.171.6									Y		Y[4]	Y	Y	Y		Y		–							
3.2.171.5									Y		Y[4]	Y	Y	Y		Y		Y	–						
3.2.150.10									Y		Y[4]	Y	Y	Y		Y		Y		–					
3.2.150.6									Y		Y[4]	Y	Y	Y		Y		Y		Y	–				
3.2.116.21									Y		Y[4]	Y	Y	Y		Y		Y		Y		–			
3.2.78.0									Y		Y[4]	Y	Y	Y		Y		Y		Y		Y	–		
3.1.111.0																Y		Y		Y		Y	Y	–	
3.1.105.0																Y		Y		Y		Y	Y	Y	–
3.1.59.24																Y		Y		Y		Y	Y	Y	Y

[1] You can upgrade directly from software release 4.1.190.5 to 4.1.192.35M; however, upgrading to 4.1.191.24M before upgrading to 4.1.192.35M is highly recommended.

[2] CUSTOMERS WHO REQUIRE DYNAMIC FREQUENCY SELECTION (DFS) FUNCTIONALITY SHOULD NOT USE THIS RELEASE. This release does not provide DFS functionality fixes found in release 4.0.217.204. Additionally, this release is not supported in ETSI-compliant countries or Singapore.

[3] Release 4.0.217.204 provides fixes for DFS on 1510 series access points. This functionality is needed only in countries where DFS rules apply.

4. An upgrade to 4.0.206.0 is not allowed in the following country codes when operating with the following access points: Australia (1505 and 1510), Brazil (1505 and 1510), Hong Kong (1505 and 1510), India (1505 and 1510), Japan (1510), Korea (1505 and 1510), Mexico (1505 and 1510), New Zealand (1505 and 1510), and Russia (1505 and 1510). Note: The 1505 mesh access point is not supported in release 5.0 and later. The 1510 mesh access point is supported only in mesh releases 4.1.190.5, 4.1.191.22M, and 4.1.192.xM.

Software Release Support for Access Points

Table 3 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 3 Software Support for Access Points

Access Points		First Support	Last Support
1000 Series	AIR-AP1010	3.0.100.0	4.2.207.0
	AIR-AP1020	3.0.100.0	4.2.207.0
	AIR-AP1030	3.0.100.0	4.2.207.0
	Airespace AS1200	—	4.1.171.0
1100 Series	AIR-LAP1121	4.0.155.0	—
	AIR-LAP1131	3.1.59.24	—
	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—
1200 Series	AIR-AP1220A	3.1.59.24	—
	AIR-AP1220B	3.1.59.24	—
1230 Series	AIR-AP1230A	3.1.59.24	—
	AIR-AP1230B	3.1.59.24	—
	AIR-LAP1231G	3.1.59.24	—
	AIR-LAP1232AG	3.1.59.24	—
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	—
1300 Series	AIR-BR1310G	4.0.155.0	—
1400 Series	Standalone Only	N/A	—
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.176.51M
	AIR-LAP-1510	3.1.59.24	4.2.176.51M

Table 3 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-LAP1524SB	-A, C and N: 6.0 or later	—
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later[1]	—

[1] These access points are supported in the separate 4.1.19x.x Mesh Software Release train or with Release 5.2 or later. These access points are not supported in the 4.2, 5.0, or 5.1 Release trains.

Upgrading to a New Software Release

When you upgrade the controller's software, the software on the controller's associated access points is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession. Up to 10 access points can be concurrently upgraded from the controller.

Caution Do not power down the controller or any access point during this 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 in software release 4.0.206.0 and later, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Note In controller software release 5.2.157.0, the WLAN override feature has been removed from both the controller GUI and CLI. If your controller is configured for WLAN override and you upgrade to controller software release 5.2.157.0, the controller deletes the WLAN configuration and broadcasts all WLANs. You can specify that only certain WLANs be transmitted by configuring access point groups. Each access point advertises only the enabled WLANs that belong to its access point group. Access point groups do not enable WLANs to be transmitted on per-radio interface of AP.

Note Do not install the 5.2.157.0 controller software file and the 5.2.157.0 ER.aes boot software file at the same time. Install one file and reboot the controller; then install the other file and reboot the controller.

Follow these steps to upgrade the controller software using the controller GUI.

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

Note Cisco highly recommends that you back up your controller's configuration files prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Follow these steps to obtain the 5.2.157.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file from the Software Center on Cisco.com:

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

   http://www.cisco.com/cisco/software/navigator.html

b. Click **Wireless Software**.

c. Click **Wireless LAN Controllers**.

d. Click **Standalone Controllers** or **Integrated Controllers and Controller Modules**.

e. Click a controller series.

f. If necessary, click a controller model.

g. If you chose Standalone Controllers in Step d., click **Wireless LAN Controller Software**.

h. If you chose Cisco Catalyst 6500 Series/7600 Series Wireless Services Module (WiSM) in Step e., click **Wireless Services Modules (WiSM) Software**.

i. 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. Cisco recommends that you migrate to an upgraded release.

j. Click a software release number.

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

l. Click **Download**.

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

n. Save the file to your hard drive.

o. Repeat steps a. through n. to download the remaining file (either the 5.2.157.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 3 Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file to the default directory on your TFTP or FTP server.

Step 4 Disable the controller 802.11a and 802.11b/g networks.

Step 5 Disable any WLANs on the controller.

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

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

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

Step 9 In the IP Address field, enter the IP address of the TFTP or FTP server.

Step 10 If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work fine 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 field and the amount of time (in seconds) that the TFTP server attempts to download the software in the Timeout field.

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

Step 12 In the File Name field, 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 field, enter the username to log into the FTP server.

b. In the Server Login Password field, enter the password to log into the FTP server.

c. In the Server Port Number field, 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 (either the 5.2.157.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 19 Re-enable the WLANs.

Step 20 For Cisco WiSMs, re-enable the controller port channel on the Catalyst switch.

Step 21 Re-enable your 802.11a and 802.11b/g networks.

Step 22 If desired, reload your latest configuration file to the controller.

Step 23 To verify that the 5.2.157.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 24 To verify that the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file is installed on your controller, enter the **show sysinfo** command on the controller CLI and look at the Emergency Image Version field.

Note If you do not install the 5.2.157.0 ER.aes file, the Emergency Image Version field shows “N/A.”

New Features

The following new features are available in controller software release 5.2.157.0.

Note Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* for more details and configuration instructions.

New Controller Features

- **100 clients on H-REAP**—You can now configure the controller to allow a hybrid-REAP access point in standalone mode to perform LEAP or EAP-FAST authentication for up to 100 statically configured clients. In previous releases, you could configure up to 20 clients.
- **512 WLANs**—The controller can now control up to 512 WLANs for lightweight access points. Each WLAN has a separate WLAN ID (1 through 512), a separate profile name, and a WLAN SSID and can be assigned unique security policies. The controller publishes up to 16 WLANs to each connected access point, but you can create up to 512 WLANs on the controller and then selectively publish these WLANs (using access point groups) to different access points to better manage your wireless network.

  Note Cisco 2106, 2112, and 2125 controllers support only up to 16 WLANs.

- **Automatically contain rogue access points**—When the controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network. If RLDP determines that the rogue is on your network, you can now choose to either manually or automatically contain the detected rogue. In controller software releases prior to 5.2.157.0, manual containment is the only option.

Caution When you enable any of the auto contain parameters, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party’s network could have legal consequences.

- **CAPWAP**—Control and Provisioning of Wireless Access Points protocol (CAPWAP), which is based on LWAPP, is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points. Cisco lightweight access points use CAPWAP to communicate between the controller and other lightweight access points on the network. Controller software releases prior to 5.2.157.0 use the Lightweight Access Point Protocol (LWAPP) for these communications.

LWAPP-enabled access points can discover and join a CAPWAP controller, and conversion to a CAPWAP controller is seamless. For example, the controller discovery process and the firmware downloading process when using CAPWAP are the same as when using LWAPP. The one exception is for Layer 2 deployments, which are not supported by CAPWAP.

Note Refer to the "CAPWAP Guidelines" section on page 27 for information on network changes that you might need to make to ensure that access points can join the controller.

Note If you inadvertently configure a controller that is running software release 5.2.157.0 with a failover controller that is running a different software release (such as 4.2, 5.0, or 5.1), the access point might take a long time to join the failover controller because the access point starts the discovery process in CAPWAP and then changes to LWAPP discovery.

- **Disabling client IP address checking**—When you enable hybrid-REAP local switching, the controller waits to learn the client IP address by default. You can now disable this option so the controller maintains the client connection without waiting to learn the client IP address. The ability to disable this option is supported only with hybrid-REAP local switching; it is not supported with hybrid-REAP central switching.
- **Disabling coverage hole detection per WLAN**—In controller software release 5.2.157.0, you can disable coverage hole detection on a per-WLAN basis. When you disable coverage hole detection on a WLAN, a coverage hole alert is still sent to the controller, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where guests are connected to your network for short periods of time and are likely to be highly mobile.
- **Forwarding plane for 2100-series-based controllers**—In controller software release 5.2.157.0, the software-based forwarding architecture for 2100-series-based controllers is being replaced with a new forwarding plane architecture. As a result, 2100 series controllers and the Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers bridge 802.3 packets by default. Therefore, 802.3 bridging can now be disabled only on 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch.

Note By default, 2100-series-based controllers that are running software release 5.2.157.0 bridge all non-IPv4 packets (such as Appletalk, IPv6, and so on).

- **IP-MAC address binding**—In controller software release 5.2.157.0, the controller enforces strict IP address-to-MAC address binding in client packets. The controller checks the IP address and MAC address in a packet, compares them to the addresses that are registered with the controller, and forwards the packet only if they both match. In previous releases, the controller checks only the MAC address of the client and ignores the IP address. To enable or disable this feature, enter this command: **config network ip-mac-binding** {**enable** | **disable**}. The default value is enabled. You can enter **show network summary** to see the current status.

Note You might want to disable this binding check if you have a routed network behind a workgroup bridge (WGB).

- **Local significant certificate**—In controller software releases prior to 5.2.157.0, the controller may either use self-signed certificates (SSCs) to authenticate access points or send the authorization information to a RADIUS server (if access points have manufacturing-installed certificates [MICs]).

In controller software release 5.2.157.0, you can configure the controller to use a local significant certificate (LSC). You can use an LSC if you want your own public key infrastructure (PKI) to provide better security; to have control of your certificate authority (CA); and to define policies, restrictions, and usages on the generated certificates.

Note LSCs are not supported on access points that are configured for bridge mode.

- **Probe request forwarding**—Probe requests are 802.11 management frames sent by clients to request information about the capabilities of SSIDs. You can configure access points to forward both acknowledged and unacknowledged probe requests to the controller. Acknowledged probe requests are probe requests for SSIDs that are supported by the access point. The controller can use the information from unacknowledged probe requests to improve location accuracy.
- **wIPS**—The Cisco Adaptive wireless intrusion prevention system (wIPS) is an advanced approach to wireless threat detection and performance management. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention. The Cisco Adaptive wIPS is enabled by the Cisco 3300 Series Mobility Services Engine (MSE), which is an appliance-based solution that centralizes the processing of intelligence collected by the continuous monitoring of Cisco Aironet access points. With Cisco Adaptive wIPS functionalities and WCS integration into the MSE, the wIPS service can configure, monitor, and report wIPS policies and alarms.
- **XML upload and validation**—When you save the controller's configuration, the controller stores it in XML format in flash memory. When you upload the configuration file to a TFTP or FTP server, the controller converts the configuration from XML to CLI. You can then read or edit the configuration file in CLI format on the server. When you are finished, you can download the file back to the controller, where it is reconverted to XML format and saved.

  Any CLI commands that have invalid values are replaced with default values. If the downloaded configuration contains a large number of invalid CLI commands, you can upload the invalid configuration to the TFTP or FTP server for analysis.

  Note You cannot modify the configuration files for 2000, 4000, and 4100 series controllers. The ability to modify configuration files is available in controller software release 5.2 or later, and these controllers support only earlier software releases (up to the 4.2 release for 2000 series controllers and up to the 3.2 release for 4000 and 4100 series controllers).

GUI Enhancements

- **802.11a > RRM > Dynamic Channel Assignment (DCA) page**—You can include or exclude the 4.9-GHz channels (1 through 26) in the channel list. These channels are supported on Cisco Aironet 1520 series mesh access points. The 4.9-GHz band is for public safety client access traffic only. You can include or exclude the extended UNII-2 channels (100, 104, 108, 112, 116, 132, 136, and 140) in the channel list.

  Note If you have Cisco Aironet 1520 series mesh access points in the –E domain, you must include these channels in the DCA channel list before you start operation. If you are upgrading from a previous release, verify that these channels are included in the DCA channel list.

- **802.11b/g/n Cisco APs > Configure page**—The "Location Optimized Monitor Mode (LOMM)" section has been renamed "Tracking Optimization," and the "LOMM Enabled" drop-down box has been renamed "Enable Tracking Optimization."
- **All APs > Details (Advanced) page**—The **Foreign** option has been removed from the Power Over Ethernet Settings section. If you want to configure the switch MAC address, enter the MAC address in the Injector Switch MAC Address field. If you want the access point to find the switch MAC address, leave the Injector Switch MAC Address field blank.
- **AP Groups page**—In previous releases, this page is titled AP Groups VLAN and can be used to create access point groups and assign each group to one or more WLANs. In controller software release 5.2.157.0, you can use this page to also assign access points to an access point group.
- **DHCP Allocated Lease page**—You can now use the controller GUI to view the MAC address, the IP address, and the remaining lease time for wireless clients.
- **DHCP Parameters page**—You can use the controller GUI to enable or disable DHCP proxy on a global basis rather than on a WLAN basis. DHCP proxy is enabled by default. When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself.
- **HREAP Groups > Edit (Local Users) page**—You can upload a comma-separated values (CSV) file with a list of up to 100 clients for LEAP or EAP-FAST authentication using the controller GUI.
- **HTTP Configuration page**—You can specify the amount of time (in minutes) before the web session times out due to inactivity in the Web Session Timeout field.
- **Local EAP > General page**—You can use the controller GUI to specify the amount of time (in seconds) and the maximum number of times that the controller attempts to send an EAP key over the LAN to wireless clients using local EAP. You can also use the controller GUI to limit the number of devices that can be connected to the controller with the same username. You can log in up to eight times from different devices (PDA, laptop, IP phone, and so on) on the same controller. Previously, these options could be configured only from the controller CLI.
- **Upload File from Controller page**—You can now upload the radio core dump file to a TFTP or FTP server using the controller GUI. Previously, radio core dump uploads could be configured only from the controller CLI.
- **WLANs page**—You can search the WLAN list so that only WLANs that meet certain criteria (such as profile name, SSID, or status) are displayed.

Access Point Additions and Changes

- **Cisco Aironet 1140 Series Access Point**—All controllers now support the Cisco Aironet 1140 Series Access Point. This indoor access point supports two draft IEEE 802.11n version 2.0 radio modules with integrated antennas: a 2.4-GHz radio and a 5-GHz radio. You can configure the radios separately, using different settings on each. This access point supports data rates of up to 300 Mbps per radio and can be used with hybrid-REAP. For more information, refer to the *Cisco Aironet 1140 Series Lightweight Access Point Getting Started Guide* and the *Cisco Aironet 1140 Series Access Point Data Sheet*.

Mesh Access Point Additions and Changes

- **Cisco Aironet mesh access points**—Access points within a mesh network operate as either a root access point (RAP) or a mesh access point (MAP). RAPs have wired connections to their controller, and MAPs have wireless connections to their controller. MAPs communicate among themselves and back to the RAP using wireless connections over the 802.11a radio backhaul. MAPs use the Cisco Adaptive Wireless Path Protocol (AWPP) to determine the best path through the other mesh access points to the controller. All the possible paths between the MAPs and RAPs form the wireless mesh network.

  Note Refer to Chapter 8 of the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* for information on the number of mesh access points supported per controller.

  Controller software release 5.2.157.0 supports the following Cisco Aironet mesh access points:

  - **Cisco Aironet 1522 and 1524 outdoor mesh access points**

    The 1522 access point has two simultaneously operating radios: a 2.4-GHz radio used for client access and a 5-GHz radio used for data backhaul.

    The 1524 access point has three radios: a 2.4-GHz, a 5.8-GHz, and a 4.9-GHz radio. The 2.4-GHz radio is for client access (non-public safety traffic), and the 4.9-GHz radio is for public safety client access traffic only. The 5.8-GHz radio is used as the backhaul for both public safety and non-public safety traffic.

    Note Those 1522 mesh access points with serial numbers prior to FTX1150XXXX do not support 5- and 10-MHz channels on the 4.9-GHz radio; however, they do support 20-MHz channels. Those 1522 mesh access points with serial numbers after FTX1150XXXX support 5-, 10-, and 20-MHz channels.

    Note For public safety only deployments, 1522 and 1524 access points must each be connected to their own separate RAP-based tree. For such deployments, 1522s must use the 4.9-GHz backhaul, and 1524s must be in their own RAP trees and use the 5.8-GHz backhaul.

    Note Refer to the *Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide* for details on the physical installation and initial configuration of the mesh access points at the following link: http://www.cisco.com/en/US/products/ps8368/tsd_products_support_series_home.html

  - **Cisco Aironet 1130AG and 1240AG indoor mesh access points**

    The 1130AG and 1240AG access points have two simultaneously operating radios: a 2.4-GHz radio used for client access and a 5-GHz radio used for data backhaul.

Note You must convert these access points in order for them to operate as indoor mesh access points. Refer to the "Converting Indoor Access Points to Mesh Access Points" section in Chapter 8 of the controller configuration guide.

- **4.9-GHz channel list**—If you are using Cisco Aironet 1520 series mesh access points in your network, you need to set the 4.9-GHz channels in the 802.11a band on which they are to operate on the 802.11a > RRM > Dynamic Channel Assignment (DCA) page. The 4.9-GHz band is for public safety client access traffic only.
- **16 SSIDs on mesh access points**—With controller software release 5.2.157.0, the 1130, 1240, 1522, and 1524 mesh access points support up to 16 SSIDs on each access radio. Software release 4.1.192.xxM supports only 8 SSIDs on these radios.
- **Backhaul client access (universal access)**—When you enable this feature, all mesh access points reboot and then allow wireless client association over the 802.11a radio. Universal access allows an access point to carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio. When you disable this feature, mesh access points transmit backhaul traffic over the 802.11a radio and allow client association only over the 802.11b/g radio.

  Note Universal access applies only to mesh access points with two radios (1130, 1240, and 1522). The 1524 access point does not support this feature.

- **Brown-out notification**—When a mesh access point experiences a reset, power outage, or drop in voltage below an acceptable threshold, it generates a brown-out trap and sends it to the controller to aid in troubleshooting.

  The following types of power outages at the mesh access point generate and send brown-out traps to the controller: external power loss, generic Power-over-Ethernet (PoE) loss, change of PoE source, power injector loss, AC power loss, cable power loss, and too high or too low power source.
- **Client roaming on 1522 and 1524 access points**—Outdoor mesh deployments of 1522 and 1524 mesh access points support high-speed roaming of Cisco Compatible Extension version 4 (v4) clients at speeds of up to 70 mph. An example application might be maintaining communication with a terminal in an emergency vehicle as it moves within a mesh public network. These mesh access points support three Cisco CX v4 Layer 2 client roaming enhancements: access point assisted roaming, enhanced neighbor list, and roam reason report.
- **Configuration database setting**—The configuration database total of 2048 is the new default setting. It includes MAC filter entries, access point MIC and SSC entries, dynamic interfaces, management users, and local net users. A larger configuration database setting is of value in large mesh deployments (CSCsg88704).
- **Ethernet bridging**—Ethernet bridging is used in two mesh network scenarios: point-to-point and point-to-multipoint bridging between MAPs (untagged packets). A typical trunking application might be bridging traffic between buildings within a campus.

  Note You do not need to configure VLAN tagging to use Ethernet bridging for point-to-point and point-to-multipoint bridging deployments.

- **Ethernet VLAN tagging**—Ethernet VLAN tagging allows specific application traffic to be segmented within a wireless mesh network and then forwarded (bridged) to a wired LAN (access mode) or bridged to another wireless mesh network (trunk mode).

A typical public safety access application using Ethernet VLAN tagging is placement of video surveillance cameras at various outdoor locations within a city. Each of these video cameras has a wired connection to a mesh access point. Then the video of all these cameras streams across the wireless backhaul to a central command station on a wired network.

- **Extended UNII-2 channels**—These extended UNII-2 channels no longer appear in the DCA channel list on the 802.11a > RRM > Dynamic Channel Assignment (DCA) page: 100, 104, 108, 112, 116, 132, 136, and 140. If you have Cisco Aironet 1520 series mesh access points in the -E regulatory domain, you must include these channels in the DCA channel list before you start operation. If you are upgrading from a previous release, verify that these channels are included in the DCA channel list. To include these channels in the channel list, check the **Extended UNII-2 Channels** check box.
- **External AAA (RADIUS) server for mesh access point**s—Controller software release 5.2.157.0 supports external authorization and authentication of mesh access points using a RADIUS server such as Cisco ACS (4.1 and later). The RADIUS server must support the client authentication type of EAP-FAST with certificates.
- **Interoperability with Cisco 3200 Series Wireless Mobile Access Routers**—Outdoor 1522 and 1524 mesh access points can interoperate with a Cisco 3200 Series Wireless Mobile Access Router (MAR) on the public safety channel (4.9-GHz) as well as on the 2.4-GHz access and 5.8-GHz backhaul channels.

  The Cisco 3200 MAR creates an in-vehicle network in which devices such as PCs, surveillance cameras, digital video recorders, printers, PDAs, and scanners can share wireless networks such as cellular- or WLAN-based services back to the main infrastructure. This functionality allows data collected from in-vehicle deployments such as a police cars to be integrated into the overall wireless infrastructure.
- **Mesh multicast containment for video**—You can use the controller CLI to configure three mesh multicast modes (in, in-out, and regular) to manage video camera broadcasts on all mesh access points. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

  Mesh multicast modes determine how bridging-enabled mesh access points and root access points send multicasts among Ethernet LANs within a mesh network. Mesh multicast modes manage non-CAPWAP multicast traffic only. A different mechanism governs CAPWAP multicast traffic.
- **Voice support**
  - **CAC**—Call admission control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN experiences congestion. All calls on a mesh access point use bandwidth-based CAC. They do not support load-based CAC.

    Bandwidth-based, or static, CAC enables the client to specify how much bandwidth or shared medium time the access point requires to accept a new call. Each access point determines whether it is capable of accommodating a particular call by looking at the bandwidth available and compares it against the bandwidth required for the call. If there is not enough bandwidth available to maintain the maximum allowed number of calls with acceptable quality, the access point rejects the call.
  - **QoS and DSCP marking**—The access and backhaul radios of mesh access points support QoS 802.11e. The access points can prioritize client traffic based on the QoS setting defined on the controller and implement CAC on the backhaul.

Mesh access points honor the DSCP marking received from video cameras to which they are connected. The originating Cisco 7920 voice handset (client) and the terminating voice handset or terminal perform DSCP. Neither the controller nor the mesh access points perform DSCP marking. The WLAN at the client access side of the mesh access point serves an independent function.

- **Workgroup bridge support**—A workgroup bridge (WGB) connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the 1522 or 1524 mesh access point using Internet Access Point Protocol (IAPP) messaging. The mesh access point treats the WGB as a wireless client.

  When configured as a WGB, the 1130, 1240, and 1310 autonomous access points as well as the 3200 series mobile access router (MAR) can associate with mesh access points. You can configure these access points as RAPs or MAPs. Both the 2.4-GHz (802.11b) and 5-GHz (802.11a) radio on the 1522 and both the 2.4-GHz (802.11b) and 4.9-GHz (public safety radio) on the 1524 support WGB association.

- **New and modified mesh CLI commands**
  - **config 802.11–a49** *?*—Configures the 4.9-GHz sub-band radio.

    where *?* is one of the following:

    antenna extAntGain *antenna_gain Cisco_MAP*: Configures the 802.11a 4.9-GHz antenna.

    channel {**ap** *Cisco_MAP channel_number* | **global**}: Configures either a single 802.11a 4.9-GHz channel (access point) or enables auto-RF (global).

    disable *Cisco_MAP*: Disables the 802.11a 4.9-GHz sub-band radio.

    enable *Cisco_MAP*: Enables the 802.11a 4.9-GHz sub-band radio.

    txPower *Cisco_MAP power_level*: Configures the transmit power level for the 802.11a 4.9-GHz sub-band radio.

  - **config 802.11–a58** *?*—Configures the 5.8-GHz sub-band radio.

    where *?* is one of the following:

    antenna extAntGain *antenna_gain Cisco_MAP*: Configures the 802.11a 5.8-GHz antenna.

    channel {**ap** *Cisco_MAP channel_number* | **global**}: Configures either a single 802.11a 5.8-GHz channel (access point) or enables auto-RF (global).

    disable *Cisco_MAP*: Disables the 802.11a 5.8-GHz sub-band radio.

    enable *Cisco_MAP*: Enables the 802.11a 5.8-GHz sub-band radio.

    txPower *Cisco_MAP power_level*: Configures the transmit power level for the 802.11a 5.8-GHz sub-band radio.

  - **config advanced 802.11–a49 profile** *?*—Configures the 4.9-GHz radio profile.

    where *?* is one of the following:

    coverage *Cisco_MAP threshold_value*: Configures the 802.11a coverage threshold. Values are 3 and 50 dB.

    customize *Cisco_MAP* {**on** | **off**}: Turns the performance profile either on or off.

    exception {**global** | *Cisco_MAP*} *percent*: Configures the 802.11a coverage exception level globally or for an individual access point. Values are 0 to 100.

    foreign {**global** | *Cisco_MAP*} *percent*: Configures the 802.11a interference threshold globally or for an individual access point. Values are 0 to 100.

level *Cisco_MAP clients*: Configures the 802.11a client minimum exception level. Values are 1 to 75 clients.

clients *Cisco_MAP clients*: Configures the 802.11a client threshold. Values are 1 to 75 clients.

noise {**global** | *Cisco_MAP*} *threshold*: Configures the 802.11a foreign noise threshold globally or for an individual access point. Values are –127 to 0 dBm.

throughput {**global** | *Cisco_MAP*} *threshold*: Configures the 802.11a throughput threshold globally or for an individual access point. Values are 1000 and 10000000 bytes per second.

utilization {**global** | *Cisco_MAP*} *percent*: Configures the 802.11a RF utilization threshold globally or for an individual access point. Values are 0 to 100.

- **config slot** *slot-ID ?*—Configures the access point slot.

  where *?* is one of the following:

  enable *Cisco_MAP:* Enables a slot for a particular mesh access point.

  disable *Cisco_MAP:* Disables a slot for a particular mesh access point.

  channel ap *Cisco_MAP* {*channel_number* | **global**}: Configures a single 802.11a 5.8-GHz channel for the slot or enables auto-RF (global).

  chan_width *Cisco_MAP channel_width*: Configures the channel width for a slot.

  txPower ap *Cisco_MAP* {*power_level* | **global**}: Configures the transmit power level for the slot.

- **show ap config** {**802.11–a49** | **802.11–a58**} {*Cisco_MAP* | **summary**}: Shows detailed or summary information for a 4.9-GHz or 5.8-GHz sub-band 802.11a radio.
- **show client ap 802.11–a49**: Shows client information for a 4.9-GHz sub-band radio.
- **show ap slots**: Shows slot information for mesh access points.
- **show mesh ap tree**: Shows mesh access points within a tree structure (hierarchy).
- **show mesh ap summary**: Revised to show the CERT MAC field, which shows a MAC address within an access point certificate that can be used to assign a username for external authentication.
- **show mesh cac access** *Cisco_AP*: Shows the mesh tree topology for the network and the number of voice calls that are in progress by access point radio.
- **show mesh cac bwused** {**voice** | **video**} *Cisco_AP*: Shows the voice or video bandwidth used on a particular mesh access point.
- **show mesh cac callpath** *Cisco_AP*: Shows the mesh tree topology for the network and the number of voice calls that are in progress.
- **show mesh cac rejected** *Cisco_AP*: Shows how many calls have been rejected on a particular mesh access point.
- **show mesh cac summary**: Shows a summary of voice calls across the mesh network.

Regulatory Updates

- **Regulatory domain encoding in SKUs**—These SKUs for the 1131AG, 1140AG, 1242AG, and 1250AG series lightweight access points are encoded with two regulatory domains to extend support to new bands:

Access Point SKU	2.4-GHz Regulatory Domain	5-GHz Regulatory Domain
L/AP-xxxx-I	-E	-I
L/AP-xxxx-S	-E	-S
L/AP-xxxx-T	-A	-T
L/AP-xxxx-N	-A	-N
L/AP-xxxx-C	-E	-C

- **Regulatory updates for existing countries**—The following regulatory domain updates have been implemented for these countries:

		2.4-GHz Regulatory Domain		5-GHz Regulatory Domain	
Country	Code	Old	New	Old	New
Brazil	BR	-A	-A	none	-T
Chile	CL	-A	-AE	none	-S[1]
Egypt	EG	-E	-E	none	-I

[1] To use the 5-GHz regulatory domain in Chile, the radio must use an external antenna with less than 3-dBi gain.

- **Additional country support**—Cisco controllers are now supported for use in these countries with the 1131G, 1131AG, 1140G, 1140AG, 1242G, 1242AG, 1250G, and 1250AG series lightweight access points:

Country	Code	Access Point SKU	2.4-GHz Regulatory Domain	5-GHz Regulatory Domain
Iraq	IQ	L/AP-xxxxG-E	-E	none
Macedonia	MK	L/AP-xxxxG-E	-E	none
		L/AP-xxxxAG-I	-E	-I
Montenegro	ME	L/AP-xxxxG-E	-E	none
		L/AP-xxxxAG-E	-E	-E
Qatar	QA	L/AP-xxxxG-E	-E	none
Serbia	RS	L/AP-xxxxG-E	-E	none
		L/AP-xxxxAG-E	-E	-E
Tunisia	TN	L/AP-xxxxG-E	-E	none
Uruguay	UY	L/AP-xxxxG-A	-A	none
		L/AP-xxxxAG-A	-A	-A

- **DFS support in the -T regulatory domain**—Taiwan does not require dynamic frequency selection (DFS) in the UNII-2 band, so until now the -T regulatory domain has not included support for it. However, Brazil (which now also uses the -T regulatory domain) does require DFS in the UNII-2 band. The -T regulatory domain is being modified so DFS is required on channels 56, 60, and 64 for indoor access points.

  Note Channel 52 is not available in the -T regulatory domain.

  The following DFS mechanisms, which already apply to channels 100 through 140 in the -T regulatory domain, also apply to UNII-2 channels 56 through 64:

  - The access point performs a 60-second scan for radar prior to initially sending any traffic on the channel. This scan may be bypassed if the controller detects a neighbor access point already operating on the same frequency.
  - Radar detection is constantly performed on the radio channel, as indicated in the output of the **show controller** CLI command for the access point radio.
  - If radar is detected on the channel, the access point moves to another channel.
  - The channel on which radar is detected is unavailable for 30 minutes.

Note For a complete list of regulatory domains supported for each product, refer to this URL:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps6087_Products_Data_Sheet.html.

Other Changes

These additional changes are applicable to controller software release 5.2.157.0:

- Controller software releases 4.1 through 5.1 support both asymmetric and symmetric mobility tunneling. Controller software release 5.2.157.0 supports only symmetric mobility tunneling, which is now always enabled by default.
- The WLAN override feature has been removed from both the controller GUI and CLI.

  Note In controller software release 5.2.157.0, the WLAN override feature has been removed from both the controller GUI and CLI. If your controller is configured for WLAN override and you upgrade to controller software release 5.2.157.0, the controller deletes the WLAN configuration and broadcasts all WLANs. You can specify that only certain WLANs be transmitted by configuring access point groups. Each access point advertises only the enabled WLANs that belong to its access point group.

- IGMP snooping can now be enabled on the 2100 series controllers and the Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers.
- The **show run-config** CLI command is replacing the **show running-config** command. Use **show run-config** to view the complete configuration of the controller or **show run-config commands** to view the list of user-configured commands on the controller.
- The **show ap cdp** CLI commands have been modified to include the **ap-name** parameter. The new commands are as follows:

  - **show ap cdp ap-name** *Cisco_AP*
  - **show ap cdp neighbors ap-name** *Cisco_AP*
- You can now disable Secure Socket Layer (SSL)v2 for web administration and web authentication. When SSLv2 is disabled, users cannot connect using a browser configured with SSLv2 only. They must use a browser that is configured to use a more secure protocol such as SSLv3 or later. The new CLI command to enable or disable SSLv2 is **config network secureweb cipher-option sslv2** {**enable** | **disable**}. The default value is enabled.
- To help troubleshoot controller crashes, you can now configure the controller to automatically upload its core dump file to an FTP server after experiencing a crash using these CLI commands:

  config coredump {**enable** | **disable**}

  config coredump ftp *server_ip_address filename*

  config coredump username *ftp_username* **password** *ftp_password*

  show coredump summary
- You can now upload the console dump resulting from a software-watchdog-initiated reboot of the controller following a crash using the **transfer upload datatype watchdog-crash-file** controller CLI command. The software watchdog module periodically checks the integrity of the internal software and makes sure that the system does not stay in an inconsistent or non-operational state for a long period of time.
- You can upload the kernel panic information if a kernel panic occurs using the **transfer upload datatype panic-crash-file** controller CLI command.
- To help troubleshoot hard-to-solve or hard-to-reproduce memory problems, you can configure the controller to monitor for memory leaks and to perform an auto-leak analysis between two memory thresholds. Refer to the “Monitoring Memory Leaks” section of the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* for information on these commands.
- The following CLI commands have been removed:
  - **config location 802.11b monitor enable** *Cisco_AP* **channel1 channel2 channel3 channel4**
  - **config location 802.11b monitor disable** *Cisco_AP*
  - **show location monitor summary**

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.**

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

Warning **Do not locate any antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing antennas, take extreme care not to come in contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, refer to national and local codes (e.g. U.S.: NFPA70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).**

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 120 VAC, 15A U.S. (240vac, 10A International)**

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.**

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

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

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

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.**

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

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

Each year hundreds of people are killed or injured when attempting to install an antenna. In many of these cases, the victim was aware of the danger of electrocution but did not take adequate steps to avoid the hazard.

For your safety, and to help you achieve a good installation, read and follow these safety precautions. **They may 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

Refer to 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 professionally installed.

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.

Important Notes for Controllers and Non-Mesh Access Points

This section describes important information about controllers and non-mesh lightweight access points.

FIPS 140-2

The Cisco 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch have received NIST FIPS 140-2 Level 2 certification. Click this link to view the NIST Security Policies and compliant software versions:
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

Internal DHCP Server

When clients use the controller's internal DHCP server, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one.

CAPWAP Guidelines

Follow these guidelines when using CAPWAP:

- If your firewall is currently configured to allow traffic only from access points using LWAPP, you must change the rules of the firewall to allow traffic from access points using CAPWAP.
- Make sure that the CAPWAP UDP ports 5246 and 5247 (similar to the LWAPP UDP ports 12222 and 12223) are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.
- If access control lists (ACLs) are in the control path between the controller and its access points, you need to open new protocol ports to prevent access points from being stranded.

Messages Appearing Upon Controller Bootup

Several messages might flood the message logs when the controller boots up. These messages appear because of a failure to read or delete several different configuration files. These are low-severity messages that can safely be ignored. They do not affect controller functionality. These are some examples:

```
Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file :
sshpmInitParms.cfg. file removal failed.
-Process: Name:fp_main_task, Id:11ca7618
Mar 18 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED: Failed to delete the file :
bcastInitParms.cfg. file removal failed.
-Process: Name:fp_main_task, Id:11ca7618
```

Web Authentication Redirects

The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.

PLM Location Commands

The **config**, **show**, and **debug location plm** path loss measurement location commands are not supported in controller software release 5.2.157.0, although they appear in the CLI code.

Cisco 1250 Series Access Points and Cisco 7920 IP Phones

Cisco 1250 series access points are not supported for use with the Cisco 7920 IP phone. They can, however, be used with the Cisco 7921 and 7925 IP phones.

Crash Files for 1250 Series Access Points

The 1250 series access points may contain either an old bootloader or a new bootloader. Those with an old bootloader do not generate a crash log when a crash occurs. The crash log is disabled so that a crash does not corrupt the flash file system. Those with a new bootloader generate a crash log if the access point is running controller software release 4.2.112.0 or later.

New 1250 series access points shipped from the factory contain the new bootloader image, which fixes the flash file system after it is corrupted during a crash (without losing files). This new bootloader automatically sets a new CRASH_LOG environment variable to "yes," which enables a crash log to be generated following a crash but only on controllers running software release 4.2.112.0 or later. Therefore, no user configuration is needed to enable a crash log on new 1250 series access points shipped from the factory.

Configuration File Stored in XML

In controller software release 4.2.61.0 and later, the controller's bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in binary format. When you upgrade a controller to 4.2.61.0 or a later software release, the binary configuration file is migrated and converted to XML.

Note You cannot download a binary configuration file onto a controller running software release 5.2.157.0. Also, do not attempt to make changes to the configuration file. If you do so and then download the file to a controller, the controller displays a cyclic redundancy checksum (CRC) error while it is rebooting and returns the configuration parameters to their default values.

Note You cannot modify the configuration files for 2000, 4000, and 4100 series controllers. The ability to modify configuration files is available in controller software release 5.2 or later, and these controllers support only earlier software releases (up to the 4.2 release for 2000 series controllers and up to the 3.2 release for 4000 and 4100 series controllers).

LWAPP Mode Changes

When you upgrade to controller software release 5.0.148.0 or later, the LWAPP mode changes to Layer 3 if it was previously configured for Layer 2.

If you downgrade from controller software release 5.2.157.0, 5.1.151.0, or 5.0.148.0 to 4.2.61.0 or an earlier release, the LWAPP mode changes from Layer 3 to Layer 2. Access points may not join the controller, and you must manually reset the controller to Layer 3 to resolve this issue.

Access Points Send Multicast and Management Frames at Highest Basic Rate

Access points running recent Cisco IOS versions transmit multicast and management frames at the highest configured basic rate, which could cause reliability problems. Access points running LWAPP or autonomous IOS should transmit multicast and management frames at the lowest configured basic rate. Such behavior is necessary to provide good coverage at the cell's edge, especially for unacknowledged multicast transmissions where multicast wireless transmissions may fail to be received.

Because multicast frames are not retransmitted at the MAC layer, clients at the edge of the cell may fail to receive them successfully. If reliable reception is a goal, then multicast frames should be transmitted at a low data rate. If support for high data rate multicast frames is required, then it may be useful to shrink the cell size and disable all lower data rates.

Depending on your specific requirements, you can take the following action:

- If you need to transmit multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, one that is low enough to reach the edges of the wireless cells.
- If you need to transmit multicast data at a certain data rate in order to achieve a certain throughput, then configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of non-multicast clients.

Disabling Radio Bands

The controller disables the radio bands that are not permitted by the configured country of operation (CSCsi48220).

40-MHz Channels in the 2.4-GHz Band

Cisco recommends that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe co-channel interference is likely to occur.

Impact of External Antenna Gain on Transmit Power

In controller software release 4.2 or later, external antenna gain is factored into the maximum transmit power of the access point. Therefore, when you upgrade from an earlier software release to 4.2 or later, you might see a decrease in transmit power output.

Supporting Oversized Access Point Images

Controller software release 4.2 or later allows you to upgrade to an oversized access point image by deleting the recovery image to create sufficient space. This feature affects only access points with 8 MB of flash (the 1100, 1200, and 1310 series access points). All newer access points have a larger flash size than 8 MB.

Note As of August 2007, there are no oversized access point images, but as new features are added, the access point image size will continue to grow.

The recovery image provides a backup image that can be used if an access point power-cycles during an image upgrade. The best way to avoid the need for access point recovery is to prevent an access point from power-cycling during a system upgrade. If a power-cycle occurs during an upgrade to an oversized access point image, you can recover the access point using the TFTP recovery procedure.

Follow these steps to perform the TFTP recovery procedure.

Step 1 Download the required recovery image from Cisco.com (c1100-rcvk9w8-mx, c1200-rcvk9w8-mx, or c1310-rcvk9w8-mx) and install it in the root directory of your TFTP server.

Step 2 Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the controller to download the oversized access point image and complete the upgrade procedure.

Step 3 After the access point has been recovered, you may remove the TFTP server.

Multicast Queue Depth

The multicast queue depth is 512 packets on all controller platforms. However, the following message might appear on 2106 controllers: “Rx Multicast Queue is full on Controller.” This message does not appear on 4400 series controllers because the 4400 NPU filters ARP packets, and all forwarding (multicast or otherwise) and multicast replication are done in the software on the 2106.

This message appears when too many multicast messages are sent to the CPU. In controller software releases prior to 5.1, multicast, CDP, and ARP packets share the same queue. However, in software releases 5.1 and later, these packets are separated into different queues. There are currently no controller commands that can be entered to determine if the multicast receive queue is full. When the queue is full, some packets are randomly discarded.

MAC Filtering for WGB Wired Clients

Controller software release 4.1.178.0 or later enables you to configure a MAC-filtering IP address for a workgroup bridge (WGB) wired client to allow passive WGB wired clients, such as terminal servers or printers with static IP addresses, to be added and remain in the controller’s client table while the WGB is associated to a controller in the mobility group. This feature, activated by the **config macfilter ipaddress** *MAC_address IP_address* CLI command, can be used with any passive device that does not initiate any traffic but waits for another device to start communication.

This feature allows the controller to learn the IP address of a passive WGB wired client when the WGB sends an IAPP message to the controller that contains only the WGB wired client’s MAC address. Upon receiving this message from the WGB, the controller checks the local MAC filter list (or the anchor controller’s MAC filter list if the WGB has roamed) for the client’s MAC address. If an entry is found and it contains an IP address for the client, the controller adds the client to the controller’s client table.

Note Unlike the existing MAC filtering feature for wireless clients, you are not required to enable MAC filtering on the WLAN for WGB wired clients.

Note WGB wired clients using MAC filtering do not need to obtain an IP address through DHCP to be added to the controller's client table.

CKIP Not Supported with Dynamic WEP

In controller software release 4.1.185.0 or later, CKIP is supported for use only with static WEP. It is not supported for use with dynamic WEP. Therefore, a wireless client that is configured to use CKIP with dynamic WEP is unable to associate to a wireless LAN that is configured for CKIP. Cisco recommends that you use either dynamic WEP without CKIP (which is less secure) or WPA/WPA2 with TKIP or AES (which are more secure).

Setting the Date and Time on the Controller

Cisco Aironet lightweight access points do not connect to the 4400 series controller if the date and time are not set properly. Set the current date and time on the controller before allowing the access points to connect to it.

Synchronizing the Controller and Location Appliance

For controller software release 4.2 or later, if a location appliance (release 3.1 or later) is installed on your network, the time zone must be set on the controller to ensure proper synchronization between the two systems. Also, Cisco highly recommends that the time be set for networks that do not have location appliances. Refer to Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* for instructions for setting the time and date on the controller.

Note The time zone can be different for the controller and the location appliance, but the time zone delta must be configured accordingly, based on Greenwich Mean Time (GMT).

FCC DFS Support on 1130 Series Access Points

Federal Communications Commission (FCC) dynamic frequency selection (DFS) is supported only on 1130 series access points in the United States, Canada, and the Philippines that have a new FCC ID. Access points use DFS to detect radar signals such as military and weather sources and then switch channels to avoid interfering with them. 1130 series access points with FCC DFS support have an FCC ID *LDK102054E* sticker. 1130 series access points without FCC DFS support have an *LDK102054* (no *E* suffix) sticker. 1130 series access points that are operating in the United States, Canada, or the Philippines; have an FCC ID *E* sticker; and are running the 4.1.171.0 software release or later can use channels 100 through 140 in the UNII-2 band.

Inaccurate Transmit Power Display

After you change the position of the 802.11a radio antenna for a lightweight 1200 or 1230 series access point, the power setting is not updated in the controller GUI and CLI. Regardless of the user display, the internal data is updated, and the transmit power output is changed accordingly. To see the correct transmit power display values, reboot the access point after changing the antenna's position. (CSCsf02280)

Setting the Retransmit Timeout Value for TACACS+ Servers

Cisco recommends that the retransmit timeout value for TACACS+ authentication, authorization, and accounting servers be increased if you experience repeated reauthentication attempts or the controller falls back to the backup server when the primary server is active and reachable. The default retransmit timeout value is 2 seconds and can be increased to a maximum of 30 seconds.

Configuring an Access Point's Prestandard Power Setting

An access point can be powered by a Cisco prestandard 15-watt switch with Power over Ethernet (PoE) by entering this command:

config ap power pre-standard {**enable** | **disable**} {**all** | *Cisco_AP*}

A Cisco prestandard 15-watt switch does not support intelligent power management (IPM) but does have sufficient power for a standard access point. The following Cisco prestandard 15-watt switches are available:

- AIR-WLC2106-K9
- WS-C3550, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

The **enable** version of this command is required for full functionality when the access point is powered by a Cisco prestandard 15-watt switch. It is safe to use if the access point is powered by either an IPM switch or a power injector or if the access point is not using one of the 15-watt switches listed above.

You might need this command if your radio operational status is "Down" when you expect it to be "Up." Enter the **show msglog** command to look for this error message, which indicates a PoE problem:

```
Apr 13 09:08:24.986 spam_lrad.c:2262 LWAPP-3-MSGTAG041: AP 00:14:f1:af:f3:40 is unable to
verify sufficient in-line power. Radio slot 0 disabled.
```

Controller Functions that Require a Reboot

After you perform these functions on the controller, you must reboot the controller in order for them to take effect:

- Enable or disable link aggregation (LAG)
- Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
- Add new or modify existing SNMP v3 users
- Enable or disable the mobility protocol port using this CLI command:

  config mobility secure-mode {**enable** | **disable**}

2106 Controller LEDs

The 2106 controller's Status LED and AP LED do not flash amber when software is being uploaded to the controller or downloaded to an access point, respectively.

Note Some versions of the *Cisco 2106 Wireless LAN Controller Quick Start Guide* might incorrectly state that these LEDs flash amber during a software upload or download.

Rate-Limiting on the Controller

Rate-limiting is applicable to all traffic destined to the CPU from either direction (wireless or wired). Cisco recommends that you always run the controller with the default **config advanced rate enable** command in effect in order to rate-limit traffic to the controller and protect against denial-of-service (DoS) attacks. You can use the **config advanced rate disable** command to stop rate-limiting of Internet Control Message Protocol (ICMP) echo responses for testing purposes. However, Cisco recommends that you reapply the **config advanced rate enable** command after testing is complete.

Pings Supported to the Management Interface of the Controller

Controller software release 4.1.185.0 or later is designed to support ICMP pings to the management interface either from a wireless client or a wired host. ICMP pings to other interfaces configured on the controller are not supported.

Pinging from a Network Device to a Controller Dynamic Interface

Pinging from a network device to a controller dynamic interface may not work in some configurations. When pinging does operate successfully, the controller places Internet Control Message Protocol (ICMP) traffic in a low-priority queue, and the reply to ping is on best effort. Pinging does not pose a security threat to the network. The controller rate limits any traffic to the CPU, and flooding the controller is prevented. Clients on the WLAN associated with the interface pass traffic normally.

GLBP Not Supported

Controller software release 4.2 or later is not compatible with the Gateway Load Balancing Protocol (GLBP). Make sure to configure the controller's default gateway to a fixed address and not to the GLBP virtual address.

IPSec Not Supported

Software release 5.2.157.0 does not allow you to choose IPSec as a Layer 3 security option. None and VPN Passthrough are the only available options. If you upgrade to this release from a previous release that supported IPSec as a Layer 3 security option, any WLANs that are configured for this feature become disabled. If you want to configure IPSec, you must use a version of controller software prior to 4.0.

4400 Series Controllers Do Not Forward Subnet Broadcasts through the Guest Tunnel

As designed, 4400 series controllers do not forward IP subnet broadcasts from the wired network to wireless clients across the EoIP guest tunnel.

Connecting 1100 and 1300 Series Access Points

You must install software release 4.0.179.8 or later on the controller before connecting 1100 and 1300 series access points to the controller.

Preventing Clients from Accessing the Management Network on a Controller

To prevent or block a wired or wireless client from accessing the management network on a controller (from the wireless client dynamic interface or VLAN), the network administrator should ensure that there is no route through which to reach the controller from the dynamic interface or use a firewall between the client dynamic interface and the management network.

Voice Wireless LAN Configuration

Cisco recommends that aggressive load balancing always be turned off either through the controller GUI or CLI in any wireless network that is supporting voice, regardless of vendor. When aggressive load balancing is turned on, voice clients can hear an audible artifact when roaming, and the handset is refused at its first reassociation attempt.

Changing the IOS LWAPP Access Point Password

Cisco IOS Lightweight Access Point Protocol (LWAPP) access points have a default password of *Cisco*, and the pre-stage configuration for LWAPP access points is disabled by default. To enable it, you must configure the access point with a new username and password when it joins the controller. Enter this command using the controller CLI to push a new username and password to the access point:

config ap username *user_id* **password** *password* {*Cisco_AP* | **all**}

- The *Cisco_AP* parameter configures the username and password on the specified access point.
- The **all** parameter configures the username and password on all the access points registered to the controller.

The password pushed from the controller is configured as "enable password" on the access point.

There are some cases where the pre-stage configuration for LWAPP access points is disabled and the access point displays the following error message when the CLI commands are applied:

"ERROR!!! Command is disabled."

For more information, refer to *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode.*

Exclusion List (Blacklist) Client Feature

If a client is not able to connect to an access point, and the security policy for the WLAN and client are correct, the client has probably been disabled. In the controller GUI, you can view the client's status on the Monitor > Summary page under Client Summary. If the client is disabled, click **Remove** to clear the disabled state for that client. The client automatically comes back and, if necessary, reattempts authentication.

Automatic disabling happens as a result of too many failed authentications. Clients disabled due to failed authorization do not appear on the permanent disable display. This display is only for those MACs that are set as permanently disabled by the administrator.

RADIUS Servers and the Management VLAN

If a RADIUS server is on a directly connected subnet (with respect to the controller), then that subnet must be the management VLAN subnet.

RADIUS Servers

This product has been tested with CiscoSecure ACS 3.2 and later and works with any RFC-compliant RADIUS server.

Management Usernames and Local Netuser Names

Management usernames and local netuser names must be unique because they are stored in the same database. That is, you cannot assign the same name to a management user and a local netuser.

802.1X and Microsoft Wireless Configuration Manager

Clients using the Microsoft Wireless Configuration Manager and 802.1X must use WLANs configured for 40- or 104-bit key length. Configuring for 128-bit key length results in clients that can associate but not authenticate.

Using the Backup Image

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.

Home Page Retains Web Authentication Login with IE 5.x

Because of a caching problem in the Internet Explorer 5.x browser, the home page retains the web authentication login. To correct this problem, clear the history or upgrade your workstation to Internet Explorer 6.x.

Rogue Location Discovery Protocol (RLDP)

Enabling RLDP may cause access points connected to the controller to lose connectivity with their clients for up to 30 seconds.

Ad-Hoc Rogue Containment

Client card implementations may mitigate the effectiveness of ad-hoc containment.

Changing the Default Values of SNMP Community Strings

The controller has commonly known default values of “public” and “private” for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* for configuration instructions.

Changing the Default Values for SNMP v3 Users

The controller uses a default value of “default” for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* for configuration instructions.

Note SNMP v3 is time sensitive. Make sure that you have configured the correct time and time zone on your controller.

Features Not Supported on 2100 Series Controllers

This hardware feature is not supported on 2100 series controllers:

- Service port (separate out-of-band management 10/100-Mbps Ethernet interface)

These software features are not supported on 2100 series controllers:

- VPN termination (such as IPSec and L2TP)
- Termination of guest controller tunnels (origination of guest controller tunnels is supported)
- External web authentication web server list
- Spanning tree
- Port mirroring
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)
- Multicast-unicast mode

Some Clients See Only 64 Access Point MAC Addresses (BSSIDs) at a Time

In a crowded RF environment, clients may not be able to detect the desired SSID because of internal table limitations. Sometimes disabling and then enabling the client interface forces a rescan. Your RF environment needs to be controlled. Cisco UWN rogue access point detection and containment can help you to enforce RF policies in your buildings and campuses.

2106 Image Not Supported for 3504 Controllers

The 2106 controller image is supported for use with only 2100 series controllers. Do not install the 2106 image on a 3504 controller. Otherwise, errors may occur. Install only the 3504 image on a 3504 controller.

Running a 3504 Image on a 2106 Series Controller

It is possible to run a 3504 controller image on a 2106 series controller, but Cisco Aironet 1130, 1200, and 1240 series access points will not be able to connect to the controller.

Upgrading External Web Authentication

When upgrading a controller from operating system release 2.0 or 2.2.127.4 to release 3.2.116.21 or later, update the external web authentication configuration as follows:

1. Instead of using a preauthentication ACL, the network manager must configure the external web server IP address using this command:

   config custom-web ext-webserver add *index IP-address*

   Note *IP-address* is the address of any web server that performs external web authentication.

2. The network manager must use the new login_template shown here:

   Note Make sure to format the script to avoid any extra characters or spaces before using the web authentication template.

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache"> <meta HTTP-EQUIV=”Content-Type”
CONTENT="text/html; charset=iso-8859-1"> <title>Web Authentication</title> <script>

function submitAction(){
     var link = document.location.href;
     var searchString = "redirect=";
     var equalIndex = link.indexOf(searchString);
     var redirectUrl = "";
     var urlStr = "";
     if(equalIndex > 0) {
            equalIndex += searchString.length;
            urlStr = link.substring(equalIndex);
            if(urlStr.length > 0){
   redirectUrl += urlStr;
         if(redirectUrl.length > 255)
        redirectUrl = redirectUrl.substring(0,255);
       document.forms[0].redirect_url.value = redirectUrl;
  }
     }

     document.forms[0].buttonClicked.value = 4;
     document.forms[0].submit();
}

function loadAction(){
     var url = window.location.href;
     var args = new Object();
     var query = location.search.substring(1);
     var pairs = query.split("&");
     for(var i=0;i<pairs.length;i++){
          var pos = pairs[i].indexOf('=');
          if(pos == -1) continue;
          var argname = pairs[i].substring(0,pos);
          var value = pairs[i].substring(pos+1);
          args[argname] = unescape(value);
     }
     //alert( "AP MAC Address is " + args.ap_mac);
     //alert( "The Switch URL is " + args.switch_url);
     document.forms[0].action = args.switch_url;
     // This is the status code returned from webauth login action
     // Any value of status code from 1 to 5 is error condition and user
     // should be shown error as below or modify the message as it suits
     // the customer
     if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your
part.");
     }
     else if(args.statusCode == 2){
        alert("You are not configured to authenticate against web portal. No further
action is required on your part.");
     }
     else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the user is
already logged into the system?");
     }
     else if(args.statusCode == 4){
        alert("Wrong username and password. Please try again.");
     }
     else if(args.statusCode == 5){
        alert("The User Name and Password combination you have entered is invalid.
Please try again.");
     }

}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();"> <form method="post">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0"> <input
TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE=""> <input
TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0"> <tr> <td>&nbsp;</td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name &nbsp;&nbsp;&nbsp;<input type="TEXT" name="username"
SIZE="25" MAXLENGTH="63" VALUE=""> </td> </tr> <tr align="center" > <td colspan="2">
Password &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="Password" name="password"
SIZE="25" MAXLENGTH="24"> </td> </tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();"> </td> </tr> </table> </div>

</form>
</body>
</html>
```

Important Notes for Controllers and Mesh Access Points

This section describes important information about controllers and mesh access points.

Access Point Support Limit on Cisco WiSMs

The Cisco WiSM supports only up to 300 mesh access points reliably. Therefore, do not allow more than 300 mesh access points to associate to a Cisco WiSM.

Bridge MAC Filter Config Status Shown in Error

The **show network** command mistakenly shows a status for the Bridge MAC Filter Config parameter. This parameter is not a configurable option in software release 4.1.192.35M (CSCsk40572).

Limit Bridge Group Names to 11 Characters

Entering more than 11 characters into the bridge group name (BGN) field on the controller GUI mesh access point configuration page generates an error message. An error also appears when you configure this parameter through the **config ap bridgegroupname set groupname** *Cisco_MAP* CLI command or WCS (CSCsk64812).

Monitoring Port LED Status on a 1520 Series Access Point

When you disconnect a cable from a 1520 series access point, the port LED associated with that connection might remain lit for up to 3 seconds.

Data Rate Considerations in Short Link Deployments of 1520 Series Access Points

For dynamic frequency selection (DFS) bands, the current Hammer 5-GHz radio does not meet the receiver saturation specification of –30 dBm for some of the higher data rate modes due to a transceiver chipset optimization made to lower the DFS false detect probability. The typical receiver saturation input level is –37 dBm at 24 and 36 Mbps. The receiver saturation performance impact can be mitigated by reducing transmit power and antenna gain where possible. For typical deployments where radios are separated by reasonable distances, there is no impact to high data rate support.

Warning Message for Access Point Bridging Disable Requests

When you disable access point bridging using either the controller GUI (All APs > *AP_Name* > Mesh) or CLI (**config ap bridging disable**), the following message appears: “Disabling ethernet bridging will affect servicing of ethernet bridged clients. Are you sure you want to continue?” (CSCsi88127 and CSCsm16458).

Warning Message for Antenna Gain Changes

When you change the antenna gain on either the 1522 or 1524 access point radio using the controller GUI (Wireless > Access Points > Radios) or CLI (**config 802.11a antenna extAntGain**), the following message appears: "Changing antenna gain can make current channel unusable. The AP will be rebooted. A new channel must be chosen once the AP rejoins. If no channel is available with the new antenna gain, it will return back to the original value. Are you sure you want to continue?" (CSCsl75327).

Message for LinkTest Limitations

When you run a linktest that might oversubscribe the link using the controller GUI (Wireless > All APs > *Access_Point_Name* > *Neighbor_Info*) or CLI (**config mesh linktest**), the following message appears: "Warning! Data Rate (100 Mbps) is not enough to perform this link test on packet size (2000 bytes) and (1000) packets per second. This may cause AP to disconnect or reboot. Are you sure you want to continue?" (CSCsm11349).

Features Not Supported on Mesh Networks

The following controller features are not supported on mesh networks:

- Multi-country support
- Load-based CAC (Mesh networks support only bandwidth-based, or static, CAC.)
- High availability (fast heartbeat and primary discovery join timer)
- EAP-FASTv1 and 802.11x authentication
- Access point join priority (Mesh access points have a fixed priority.)
- Locally significant certificate
- Location-based services

Caveats

This section lists Open Caveats and Resolved Caveats for Cisco controllers and lightweight access points.

Open Caveats

These caveats are open in controller software release 5.2.157.0.

- CSCsd54928—The CPU ACL is unable to block LWAPP packets that are destined for the IP address of the dynamic interface.

  Workaround: None.

- CSCsd84706—Containment information for ad-hoc rogue access points is not shown on the controller GUI.

  Workaround: Use the controller CLI.

- CSCsd95723—Some users might be confused when presented with the **None** and **DHCP** options for configuring the service port interface in the initial controller setup wizard. These options are available for a controller that has no configuration and the setup wizard is being used to configure it.

  Workaround: Users can interpret the **None** option as Static and a logical alternative to DHCP.
- CSCse06202—When a controller's IKE lifetime expires, a rekey is not offered.

  Workaround: Increase the length of the IKE timeout.
- CSCse06206—The controller sends a DEL notification when the IKE lifetime expires, but it does not send the notice to the client.

  Workaround: Increase the length of the IKE timeout.
- CSCsg04831—There are not enough debugs to determine the packet flow in the controller for guest access.

  Workaround: Use a wireless sniffer trace.
- CSCsg87111—After you edit a WLAN configured for WPA1+WPA2 with a conditional redirect to 802.1X, the MIB browser shows a commit failure error.

  Workaround: Do not directly change from WPA1+WPA2+Conditional Web Redirect to 802.1X+Conditional Web Redirect. Instead, follow these steps:

  a. Remove **Conditional Web Redirect** and save your change.
  b. Change Layer 2 to **802.1X** and save your change.
  c. Change Layer 3 to **Conditional Web Redirect** and save your change.
- CSCsg95474—Lightweight access points do not queue disassociation messages, causing the Cisco 7921 phone to remain in a registering loop. This problem occurs when you change the data rate on the access point.

  Workaround: Power cycle the 7921 phone.
- CSCsh11086—If you press **Ctrl-S** and **Ctrl-Q** to pause and restart the output of a command such as **debug dot1x event enable**, the controller reboots.

  Workaround: Do not stop the console using **Ctrl-S**.
- CSCsh31104—The word *channel* is misspelled in the message log.

  Workaround: None.
- CSCsi06191—After you reboot the controller, the master controller mode is disabled.

  Workaround: None. The master controller configuration is not persistent by design.
- CSCsi17242—If a controller starts a timer (such as reauthentication or keylife time) after running for approximately 52 days, the timer might take a long time to fire (up to another 52 days).

  Workaround: Clean up the timers. If the problem is related to the client, deauthenticate the client to clean the timer. If the problem is related to the WLAN, such as a broadcast key update, disable and then re-enable the WLAN.
- CSCsi26248—After a failed link aggregation (LAG) link recovers, you might lose connectivity for approximately 30 seconds.

  Workaround: Recover the LAG link when service is not in use. You might also want to consider not using this type of configuration.
- CSCsi27596—The controller lacks a supported way to configure the broadcast key rotation interval. Instead, it is hardcoded to a group key rotation interval of 3600 seconds (1 hour).

Workaround: On the console, configure the hidden command **devshell dot1xUpdateBroadcastRekeyTimer**(*seconds*). This command does not work in an SSH or Telnet session and does not survive a reboot.

Example:

```
(Cisco Controller) >devshell dot1xUpdateBroadcastRekeyTimer(86400)
value = 0 = 0x0
```

- CSCsi30541—Loss of connectivity to the management interface occurs when you add a new dynamic interface and the configured DHCP server on all other interfaces is in the new dynamic interface subnet and the new interface has a shorter mask than the other interfaces.

  Workaround: Configure a 10/24 interface or a different 10/16 subnet such that the new dynamic interface does not contain the DHCP server IP address currently defined on all interfaces.

- CSCsi40354—Traffic stream metrics (TSM) information is not sorted chronologically on the controller GUI.

  Workaround: None.

- CSCsi62915—Static IP wireless devices are not shown on the controller until they send a packet. The IP address information should appear on the MAC Filtering > Details page of the controller GUI and in the output of the **show run-config** CLI command.

  Workaround: To see static IP wireless devices in the controller's local MAC filter list, enter a CLI command similar to the following:

  config macfilter add 00:01:02:03:04:05 3 200 "test prt" 192.168.200.10

- CSCsi72324—A service port with IP address 0.0.0.0 responds to an ARP for the AP-manager interface.

  Workaround: Unplug the service port and reconfigure it on the correct subnet.

- CSCsi73129—When you attempt to upgrade the controller using an associated wireless client as the TFTP or FTP server, the upgrade fails.

  Workaround: Place the server on a client that is not associated to the controller.

- CSCsj03124—RLDP behavior is inconsistent when initiated from a Cisco 1250 series access point.

  Workaround: Use access points other than the 1250 when RLDP needs to be used.

- CSCsj06245—Portions of the output of the **show tech-support** CLI command might be formatted incorrectly, making the information difficult to read.

  Workaround: None.

- CSCsj10755—When multicast mode multicast and IGMP snooping are enabled, the controller periodically sends out IGMP query messages to the clients. This IGMP query is sent as individual queries to each access point.

  Workaround: None.

- CSCsj10945—The controller does not factor in the antenna gain when reducing the output power.

  Workaround: Manually adjust the antenna gain, but this action can interfere with auto RF.

- CSCsj14304—With IGMP snooping enabled, MGIDs are assigned to reserved multicast addresses.

  Workaround: Use an upstream ACL if packets with reserved multicast addresses need to be blocked.

- CSCsj17054—A misleading message appears on the controller GUI when you upload software or certificates.

  Workaround: Ignore the message and choose the correct options to upload files on the controller.

- CSCsj29501—When the **session slot** or **telnet** command times out on the supervisor on the Cisco WiSM and you try to log in again, any character that you enter is duplicated.

  Workaround: Use a direct console connection to the Cisco WiSM.

- CSCsj54064—The downstream throughput is low when using a long packet size with ACLs on the 4400 series controller and the Catalyst 3750G Wireless LAN Controller Switch.

  Workaround: None.

- CSCsj62507—An access point in sniffer mode might report incorrect timestamps.

  Workaround: None.

- CSCsj87925—When you create a new rule for an access control list (ACL) using the controller GUI, the source and destination netmasks accept any value between 0 and 255, which are not actual netmask values.

  Workaround: Enter a valid netmask.

- CSCsj88889—WGB and wired WGB clients are shown using different radios.

  Workaround: None.

- CSCsk01633—The EAPOL key message is truncated with an invalid replay counter.

  Workaround: None.

- CSCsk08360—Further clarification is needed on the following message log entry: APF-1-DISCONECT_MOBILE_DUE_TO_WLAN_SWITCH: Disconnecting mobile 00:16:6f:79:82:75 due to switch of WLANs from 2 to 1.

  Workaround: None.

- CSCsk17001—When a guest LAN with a blank ingress interface name is added to the controller, the application fails with an SNMP exception message.

  Workaround: Use the controller CLI to configure a guest LAN. You might need to delete a previous guest LAN if it has a blank ingress interface configured on it and then recreate it. By default, the ingress interface is blank.

- CSCsk60655—The default frequency value in the intrusion detection system (IDS) file should be equal to or greater than the maximum deauthentication packets sent by an access point.

  Workaround: None.

- CSCsk63047—Dynamic transmit power control (DTPC) does not work on Cisco 1240 series access points in WGB mode.

  Workaround: None.

- CSCsl03097—When a hybrid-REAP access point in standalone mode is on the DFS channel, the access point’s radio goes down if a radar event occurs on its operating channel.

  Workaround: Wait until the access point’s connectivity to the controller recovers, or reboot the access point.

- CSCsl04281—The **show run-config** command might truncate access point neighbor information in a large environment.

  Workaround: To reduce the occurrence of this issue, disable paging using the **config paging disable** command.

- CSCsl09066—The WCS access point group VLAN profile configuration does not match the actual WLC configuration when you use multiple interface mapping profiles under the same access point group VLAN where all of the SSIDs start with the same letters or numbers.

  Workaround: None.

- CSCsl19319—If you create a local user profile on the GUI of a 2106 controller with the WLAN profile "any WLAN" and then edit the profile, the following error message appears: "Error in setting WLAN ID for user." However, your change is applied.

  Workaround: Delete the local user profile and create a new one with the updated password or description or define a WLAN profile for the user.

- CSCsl22707—A 1250 series access point using Power over Ethernet (PoE) continually resets when connected to a Catalyst 3550 series switch.

  Workaround: Use either a power injector or an AC power supply to provide power to the access point, or upgrade the switch to IOS Release 12.1(19)EA1 or later and enter this CLI command to configure the switch to continue providing power during initialization:

  power inline delay shutdown *seconds* **initial** *seconds*

  where **shutdown** *seconds* is the amount of time that the switch continues to provide power to the device after linkdown (between 0 and 20 seconds) and **initial** *seconds* is the initial time that the power shutdown delay is in effect (between 0 and 300 seconds).

  Without this command, the switch removes power immediately when a linkdown occurs on the connected device.

- CSCsl42328—The controller should not allow you to use the IP address of the gateway as the interface address.

  Workaround: Make sure that the interface IP address and gateway IP address are different.

- CSCsl47720—The link test report for a CCX client generated using the controller GUI does not provide enough information.

  Workaround: Use the controller CLI. It always provides the correct link test report, except in cases of a CCX client connected to a hybrid-HREAP access point broadcasting a centrally switched WLAN.

- CSCsl54491—When 802.11a radios are disabled globally on the controller but the individual radios of the access point are not disabled, WCS reports the known access point as a rogue. The alert is generated a few times but automatically cleared and not reported again for a couple of days.

  Workaround: None. This issue appears to be cosmetic.

- CSCsl67177—The Catalyst Express 500 (CE500) might lose connectivity to a 4400 series controller when one port of the portchannel is shut down.

  Workaround: Unplug and then plug in both Etherchannel links on the CE500 or the controller. Plug in or unplug any device on the CE500.

- CSCsl70043—When a client device connects to a secure EAP WLAN and immediately switches to an open WLAN, the access point sends a status 12 association response (which is normal) but sends it from the wrong MAC address and BSSID.

  Workaround: On the controller CLI, enter **config network fast-ssid-change** to allow the client devices to connect without incident.

- CSCsl95615—When a master controller exists on the network, an access point that is joined to a secondary or tertiary controller keeps going back to discovery.

  Workaround: Disable the master controller mode.

- CSCsm25943—The meaning of the following error message on the controller is not clear. This message does not necessarily imply that any actual “ARP poisoning” is occurring. Rather, this message appears when a WLAN is configured for DHCP Required and a client (after associating to this WLAN) transmits an ARP message without first using DHCP. The client is unable to send or receive any data traffic until it performs DHCP through the controller.

  ```
  DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with
  invalid SPA 192.168.1.152/TPA 192.168.0.206
  ```

  Workaround: Follow these steps:

  a. Determine whether you want to force your wireless clients to perform DHCP first, after associating, before they can send IP packets.

     - If you do, then disable DHCP Required, and you will not encounter this problem.
     - If you do not, then configure all clients to use DHCP.

  b. If the client is configured for DHCP but sometimes still sends IP packets after associating without performing DHCP, then perform the following:

     - Verify that the client eventually does perform DHCP without undergoing an unacceptable outage. If the outage before performing DHCP is acceptable, then you can ignore this message.
     - If the client never does perform DHCP after associating, then it can never pass Layer 3 traffic. In this case, either determine how to change the client’s behavior so that it always performs DHCP after associating, or simply accept that this client does not work in this application or reconsider your decision to use DHCP Required.

- CSCsm32845—The Guest LAN parameter on the Interfaces > Edit page of the controller GUI might cause confusion for users because the guest LAN is used for interfaces involved in wired guest LANs, not for wireless guest WLANs.

  Workaround: None.

- CSCsm34676—Voice quality might be poor with multicast paging.

  Workaround: None.

- CSCsm40870—The following error message should be reworded:

  ```
  Jan 24 15:20:55.374 apf_80211.c:2552 APF-4-ASSOCREQ_PROC_FAILED: Failed to process an
  association request from00:13:ce:37:8b:ff. WLAN:2, SSID:TMDInternal-WPA. mobile in
  exclusion list or marked for deletion
  ```

  The message should read as follows:

  ```
  ASSOCREQ_PROC_FAILED: Failed to process an association request from 00:13:ce:37:8b:ff.
  WLAN:2, SSID:TMDInternal-WPA. Mobile excluded or marked for deletion.
  ```

  Workaround: None.

- CSCsm66780—Creating a WLAN with an access control list (ACL) that has no rules generates an SNMP error.

  Workaround: Create an access list with rules.

- CSCsm71573—When the following message appears, it fills up the entire message log:

  ```
  mm_listen.c:5078 MM-3-INVALID_PKT_RECVD: Received an invalid packet from 10.0.x.x.
  Source member:0.0.0.0. source member unknown.
  ```

  Workaround: None.

- CSCsm74060—The word "received" is misspelled in this log message:

  ```
  %APF-4-ASSOCREQ_PROC_FAILED: apf_80211.c:3121 Failed to process an association request
  from xx:xx:xx:xx:xx:xx. WLAN:Y, SSID:<SSID>. message received from disabled WLAN.
  ```

  Workaround: None.

- CSCsm79901—Wired clients attached to a workgroup bridge (WGB) are retaining the previous IP address after the WGB obtains a new IP address. As a result, the wired client stops sending traffic to the infrastructure network.

  Workaround: Release and renew the DHCP IP address manually on the WGB wired client.

- CSCsm80423—The controller cannot block Layer 2 multicast traffic.

  Workaround: None.

- CSCsm82725—Clients are able to connect to the Internet without authenticating when using web authentication and port 53 on a proxy server.

  Workaround: None.

- CSCsm82984—When a controller and an access point are brought up with factory default settings, you can Telnet to the access point (even though the **show ap config general** *Cisco_AP* CLI command shows the Telnet feature as disabled). Also, once Telnet and SSH are enabled, they are not disabled after you clear the controller's configuration (even though the output of the **show** command indicates that they have been disabled).

  Workaround: None.

- CSCsm89253—The controller should log a message if it sends "Telnet is not allowed on this port" to Telnet clients.

  Workaround: None.

- CSCso02714—Throughput sometimes drops when you configure two 4400 series controllers (one as an anchor and one foreign) with symmetric tunneling and link aggregation (LAG).

  Workaround: Dedicate a port to mobility tunneling if performance is not adequate.

- CSCso06740—When more than one controller belongs to an RF group, pressing the **Invoke Channel Update Once** button updates only the channels for the RF group leader but not the channels for the other RF group members.

  Workaround: Set the channel assignment method to Automatic mode on all controllers in the RF group and then switch back to Freeze (or On Demand) mode after 10 minutes.

- CSCso07457—When the controller downloads a file using FTP, WCS shows the previous transfer state as the intermediate state, which is different from the final transfer state.

  Workaround: None.

- CSCso10678—The controller might hang when you attempt to upgrade the controller software.

  Workaround: Upgrade to a more recent controller software release. Make sure to follow the upgrade instructions in the *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points* for that release.

- CSCso18251—When you log into the controller as a lobby ambassador and create a guest user with a lifetime of zero (infinite), the user information appears only on the controller CLI. It does not appear on the controller GUI.

  Workaround: Use the controller CLI to display users.

- CSCso20444—When a controller and a 1250 series access point operate together in sniffer mode, Wireshark sometimes shows incorrect data rates for 802.11n packets.

  Workaround: Use Omnipeek if possible.

- CSCso29405—When you are troubleshooting traffic on radio interfaces, remote debugs might fail for some radio debug commands.

  Workaround: Connect to the access point locally.

- CSCso31640—When you downgrade a 2100 series controller from software release 5.1 to software release 4.2.112.0 or later, any hybrid-REAP groups configured on the controller are lost after the downgrade.

  Workaround: None. You must reconfigure the hybrid-REAP groups.

- CSCso38808—When a CCXv5 client associates to a WLAN that has Aironet IE extensions enabled, the client information table contains no information.

  Workaround: None.

- CSCso50723—When you use the controller's local RADIUS server for EAP-FAST authentications, authentication might fail if your client already has a protected access credentials (PAC) for the controller to which you are authenticating.

  Workaround: Remove the PAC from the client.

- CSCso54794—If you disable the admin mode on all ports (using the **config port adminmode all disable** CLI command) after booting up the controller, the controller might crash without any logs or a crash file.

  Workaround: Shut down the port channel (40) on the switch.

- CSCso59323—The PSK ASCII key always displays "Hexadecimal" under controller WLAN and templates.

  Workaround: None.

- CSCso59528—When you try to change the access VLAN to any VLAN that exists on the controller (either access VLAN or quarantine VLAN) from the GUI, the following error message appears: "Port number is incompatible with VLAN configuration." Similarly, when you try to change the quarantine VLAN to any VLAN that exists on the controller (either access VLAN or quarantine VLAN), the following error message appears: "Error setting vlan." These error messages should be more explanatory.

  Workaround: None.

- CSCso60075—When you use the wireshark-setup-0.99.5-cscoairo.exe file to perform remote sniffer captures in controller software release 5.0, the destination PC sends a notification that an IP is unreachable for every packet it receives.

  Workaround: You can filter out the unreachable IPs using the Wireshark filter. However, the generation of the unreachable IPs causes unnecessary stress on the capture PC and causes the capture buffer to fill up quickly.

- CSCso60597—If a 1250 series access point is configured for the 20-MHz channel width and is then placed into sniffer mode, you cannot change the channel width to Above 40 MHz or Below 40 MHz. If the 1250 series access point was set to Above 40 MHz or Below 40 MHz before it was placed into sniffer mode, you can change it to 20 MHz but not to the other 40 MHz setting.

  Workaround: Configure the access point back to local mode in order to modify the channel width settings; then return it to sniffer mode. This sequence of actions requires a minimum of two access point reboots.

- CSCso69011—After **config paging disable** is entered to disable page scrolling, the **show interface summary** command still shows a “paging” prompt, which could break customer scripts.

  Workaround: None.

- CSCso69016—After **config paging disable** is entered to disable page scrolling, the **show traplog** command still shows a “paging” prompt, which could break customer scripts.

  Workaround: None.

- CSCso72229—After you upgrade the controller to software release 4.2.112.0, the following message might appear repeatedly:

  ```
  Mar 27 18:15:13.735 spam_join_debug.c:84 LWAPP-4-AP_JDBG_ADD_FAILED: Unable to create
  AP Join information entry for AP:00:0f:24:0e:34a0, Maximum number of AP join
  information entry supported already exists.
  ```

  Workaround: None.

- CSCso76131—The controller is not updating the MAC address in the ARP cache when receiving a gratuitous ARP. For example, in a redundant firewall setup, if the primary controller fails, the secondary controller sends out gratuitous ARPs to update the ARP cache of the devices on the network. The controller’s management interface mapping for the default gateway updates correctly, but the dynamic interface mappings are not updating the ARP table. The following message appears in the message log of the controller: “dtl_arp.c:1240 DTL-3-OSARP_DEL_FAILED: Unable to delete an ARP entry for <IP Addr> from the operating system. ioctl operation failed.”

  Workaround: None.

- CSCso97776—When management frame protection (MFP) and a guest LAN are configured, the controller might show unwanted logs.

  Workaround: None.

- CSCsq01766—When you change the radio configuration, the access point sends a deauthentication request using the wrong BSSID.

  Workaround: None.

- CSCsq06451—On the controller, you cannot change the mapping of the guest LAN ingress interface to None.

  Workaround: None.

- CSCsq06690—Controllers sometimes display a message similar to this one: “Memory 0x3022c8e0 has been freed!”

  Workaround: None. You can safely ignore this message.

- CSCsq09590—The client details on the controller GUI and CLI show a session timeout of 0 and a reauthentication timeout of infinite when you connect. However, after the client roams to another access point on the controller, the session timeout remains at 0, but the reauthentication timeout shows 1800 regardless of the timeout configured on the controller. This issue occurs when the controller is configured for WPA2+802.1X with no AAA override.

  Workaround: Use the **show pmk-cache** *mac_address* CLI command to see the timeout.

- CSCsq11933—The controller GUI should show additional client counters, such as device type, rates, current, supported rates, power save, connection-related statistics, and APSD-related information.

  Workaround: None.

- CSCsq13610—WCS allows special characters in the primary, secondary, and tertiary controller names and access point names, but the controller does not, making the overall behavior inconsistent.

  Workaround: Do not use special characters in the primary, secondary, and tertiary controller names and access point names when you configure them on the controller.

- CSCsq14833—When using VLSM, if the fourth octect of the management IP address is the same as the fourth octet of the broadcast address of another interface on the controller, the controller does not respond to access point discoveries.

  Workaround: Change the IP address of the management interface.

- CSCsq17074—If you use the controller GUI to access or modify an access point that is not longer reachable, the controller might generate a system crash on the emWeb task. No crash file is generated.

  Workaround: None.

- CSCsq19207—When DHCP option 82 is enabled on the controller, the debug commands do not show the wireless client payload information.

  Workaround: None.

- CSCsq19324—The long value of the access control list (ACL) name is shown in the HTML content.

  Workaround: None.

- CSCsq19430—The 2106 controller GUI shows a guest LAN interface, even though it is not supported.

  Workaround: None.

- CSCsq19472—CCX radio measurement reports are not accurate if you trigger beacon, channel load, noise histogram, and frame requests together.

  Workaround: None.

- CSCsq21956—An error might occur when you try to edit guest user values.

  Workaround: Use the controller CLI.

- CSCsq22518—When WPA2+CCKM is enabled on the WLAN and the client roams between access points in the hybrid-REAP group, the client reauthenticates.

  Workaround: None.

- CSCsq23594—If you send a CCXv5 request to a workgroup bridge (WGB) or client, the following emergency level log message is generated:

  ```
  May 13 00:22:45.795 timerlib_mempool.c:215 OSAPI-0-INVALID_TIMER_HANDLE: Task is using
  invalid timer handle 836008400/272443620
  - Traceback:  10786fc8 103da5d4 106d9c10 103d9b28 103d9da0 103d43cc 10b9585c 10d4ef2c
  -Process: Name:osapiBsnTimer, Id:11d94ba8
  ```

  Workaround: None.

- CSCsq23806—Guest tunneling does not work if the WLAN on the foreign controller is created by the controller GUI and the WLAN on the anchor controller is created by WCS.

  Workaround: Reboot the anchor controller or use the same method (either WCS or the controller GUI) to create the WLAN on both the anchor and foreign controllers.

- CSCsq25129—A controller software upgrade might fail with a Nessus scan running.

  Workaround: Stop the Nessus scan when upgrading the controller software.

- CSCsq25642—When an access point joins the controller or when WLANs are changed on the controller, the following invalid slot ID warning might appear on the access point console along with a traceback:

  ```
  WARNING: invalid slot ID (255) passed to REAP -Traceback= 0x4EF53C 0x4EF5AC 0x49BF74
  0x4953A4 0x4AE160 0x491118 0x4919B0 0x196D90
  ```

  Workaround: Disable either hybrid-REAP mode or the WLAN override feature on the access point or both.

- CSCsq26051—When a Cisco terminal server connects to the controller but the user is not logged in through the console, the controller might hang after a reboot.

  Workaround: None.

- CSCsq26420—The **show reader summary** and **show ap summary** CLI commands show the entries for both the reader and the access point. However, the **show reader summary** command should show only reader details, and the **show ap summary** command should show only access point details.

  Workaround: None.

- CSCsq26446—Clients using a WLAN with web authentication enabled might disconnect every 5 minutes. The "pem timed out" message appears in the controller logs.

  Workaround: Authenticate the clients using another WLAN.

- CSCsq29243—The 802.11h channel switch mode parameter accepts any value, even though only 0 or 1 should be accepted.

  Workaround: None.

- CSCsq30821—Web authentication is bypassed if a client associates to an access point on one controller, roams to an access point on another controller, and then roams back to the first controller. This behavior occurs if the WLAN is on different subnets on each controller, causing the client to be anchored to the first controller when roaming to the second.

  Workaround: None.

- CSCsq30980—When you upgrade a 4400 series controller to software release 5.1, no more than 48 access points are able to join if link aggregation (LAG) is disabled. The controller enters this state when all the ports on the controller are administratively disabled and the configuration is saved before the controller is reset.

  Workaround: Do not administratively disable link-aggregated ports on the controller. Use the shut on switch port instead.

- CSCsq31622—An SNMP error might occur when you enable voice and video parameters on a controller running software release 4.2.122.0.

  Workaround: None.

- CSCsq32038—The **config interface create** CLI command does not indicate the number of characters allowed for the interface name.

  Workaround: Do not enter an interface name containing more than 31 characters.

- CSCsq34262—When you add three controllers running software release 4.2.125.0 to the same mobility group and enable a dynamic interface on each, a traceback might appear on the controller console.

  Workaround: None.

- CSCsq35402—After you upgrade the controller to software release 4.2.125.0, the controller sometimes shows this message on the console: “dtlARPProtoRecv: Invalid ARP packet!”

  Workaround: You can safely ignore this message.

- CSCsq35574—The EAP-FAST parameters Authority ID and Server Key do not accept entries of 17 or more characters.

  Workaround: None.

- CSCsq35590—A traceback might appear on the access point console when you change the access point country from Spain to the US.

  Workaround: None.

- CSCsq37810—A controller running software release 4.2.124.0 does not send a ColdStart trap when you reboot it.

  Workaround: None.

- CSCsq38075—A traceback might appear on the access point console when you set the access point country to Spain.

  Workaround: None.

- CSCsq38700—After you change the power level of an access point radio, the controller shows the radio’s operational status as DOWN. However, clients continue to pass traffic and function properly.

  Workaround: None.

- CSCsq40265—The statistics of a second RADIUS server are never incremented and stay at 0 in the **show radius auth stats** command or display incorrect values. This behavior occurs when the first RADIUS server does not reply and the request falls back to the second RADIUS server.

  Workaround: None.

- CSCsq45912—The CPU access control list (ACL) is not blocking traffic from the RADIUS server.

  Workaround: None.

- CSCsq46220—The access point fails to get a DNS IP address and syslog facility IP address from a DHCP server hosted on an IOS router.

  Workaround: Use a Windows 2000 DHCP server.

- CSCsq47493—The hybrid-REAP access point VLAN ID is not being updated.

  Workaround: First change the native VLAN ID; then change the hybrid-REAP VLAN ID.

- CSCsq50649—The controller is slow to respond to SNMP set requests, which can cause the SNMP set request to time out.

  Workaround: Pace SNMP commands to the controller rather than flooding them.

- CSCsq55045—The IAPP-3-MSGTAG015 and other controller IAPP messages are not documented or documented inadequately.

  Workaround: None. The CAPWAP packet message format is documented in the IETF draft.

- CSCsq65895—If a DHCP server is not configured on a WLAN or interface, the **config dhcp proxy enable** CLI command returns the following message, even if all WLANs do not require DHCP: “Some WLAN configurations are inconsistent with the new configuration of the DHCP Proxy. Please check the message log ('show msglog') for details.”

  Workaround: Configure a valid (or dummy) DHCP address on the WLAN or interface.

- CSCsq67907—If too many rogue access points are present and there is a substantial client activity, the apfRogueTask reports lock asserts on a controller running software release 4.2.130.0.

  Workaround: Clear rogue access points from your network.

- CSCsq73118—On a Cisco WiSM using multiple WLANs with VLAN override in use, malformed packets might appear on the native VLAN associated to the link aggregation (LAG) trunk.

  Workaround: Isolate the native VLAN on the switch so that it does not propagate malformed packets.

- CSCsq74144—The controller does not show the channel on which an access point in sniffer mode is currently sniffing. It shows only the last channel on which the access point was broadcasting in local mode.

  Workaround: None.

- CSCsq78560—You can configure port mirroring on 4400 series controllers although this feature is not supported on those controllers.

  Workaround: Do not use port mirroring on 4400 series controllers.

- CSCsq88010—You cannot clear the controller crash logs even though controllers show crash log information from versions prior to the current release.

  Workaround: Reset the controller configuration and crash logs to default values.

- CSCsq92815—Throughput sometimes drops for large packets (1024 and 1280 bytes) sent from 4400 series controllers to the wired network.

  Workaround: None.

- CSCsq96655—The Controller Network Module in a Cisco Integrated Services Router (ISR) and clients associated to access points on this controller do not receive ARP replies from the gateway. As a result, NAC out-of-band integration does not work on this platform.

  Workaround: Configure the ISR so that ARPs are forwarded properly with the NAC setup.

- CSCsr02102—Non-mesh 4.2 software should not allow 1505 or 1510 mesh access points to join the controller and download software. The access points generally do not join, but they can become inoperable.

  Workaround: None.

- CSCsr02316—Some SNMPSet operations show successful despite the fact that the controller is truncating the string.

  Workaround: Set a smaller value.

- CSCsr08256—If you upgrade an access point from LWAPP to CAPWAP, it does not join an LWAPP controller after hearing a Discovery response from any CAPWAP controller.

  Workaround: Take all of the CAPWAP controllers off the network so they cannot send a Discovery response. Then the CAPWAP access point joins the primary LWAPP controller.

- CSCsr09192—The FTP username and password can contain no more than 24 characters; however, the controller indicates that it allows up to 31 characters.

  Workaround: Enter a username and password containing no more than 24 characters each.

- CSCsr12961—The CLI help syntax does not indicate the value you should enter for the *mode* option in the **config 802.11h** command.

  Workaround: None.

- CSCsr18797—After you switch from local authentication on the controller to using an external RADIUS server, clients continue to use local authentication for several minutes.

  Workaround: None.

- CSCsr24262—The controller reports invalid message integrity checks (MICs) on authentication management frames.

  Workaround: None.

- CSCsr27851—When you use WCS to create a diagnostic WLAN for a controller, the controller sometimes shows this error message even though the WLAN has been created: "SNMP operation to Device failed: Failed to create WLAN on device."

  Workaround: You can safely ignore this message.

- CSCsr31008—When you mark a rogue access point as a known access point in WCS, controllers sometimes continue to list the access point as a rogue.

  Workaround: On the controller GUI or CLI, manually remove the access point from the list of rogues.

- CSCsr32354—If a 1250 series access point is connected to the 6548 blade in a Cisco Catalyst switch using a power injector or external power supply, the access point's Ethernet port sometimes comes up in the Down state.

  Workaround: None.

- CSCsr39536—An error message appears if you make any changes on the AP Details page on the controller GUI and do not re-enter the access point credentials.

  Workaround: Re-enter the access point credentials.

- CSCsr44439—The Web Authentication page does not load on the controller GUI when a client connects through the wired guest VLAN on software releases 4.2.130.0 and 5.0.148.2.

  Workaround: None.

- CSCsr45163—When IPv6 clients move from an access point group or VLAN to a new access point group or VLAN, they lose connectivity because all traffic is forwarded to the old VLAN.

  Workaround: Configure the clients with a static IPv6 address.

- CSCsr46119—The transmit queue on 1250 series access points sometimes locks up under medium to heavy traffic.

  Workaround: None.

- CSCsr46256—If a Cisco Compatible Extensions v5 client associates and authenticates to a 1242 access point with management frame protection (MFP) enabled and then establishes a prioritized voice call, the client cannot perform a CCKM fast roam.

  Workaround: The Cisco Compatible Extensions v4 call admission control (CAC) feature and the Cisco Compatible Extensions v5 MFP feature do not work simultaneously. Disable one or the other.

- CSCsr46795—When MSE SSL verification fails on the controller, the MSE authentication failures in the RADIUS server logs show the MAC address for the MSE instead of the controller.

  Workaround: None.

- CSCsr49229—During very frequent upgrades between two controllers where the access points repeatedly join a controller and download code and then join another controller and download another version of code in a continuous cycle, the Cisco WiSM can lock up, making even the console port inaccessible.

  Workaround: Power the controller or reset the Cisco WiSM blade.

- CSCsr49318—When you configure the power constraint feature for the 802.11a/n network, the access point does not include information element (IE) 32 (the power constraint IE) in beacons.

  Workaround: None.
- CSCsr49364—When a dynamic frequency selection (DFS) event occurs, the access point fails to populate the next 10 beacons with information element (IE) 37 (the channel switch announce IE). The access point also fails to send a broadcast channel switch announce action frame to alert associated 802.11h clients to move to the new channel.

  Workaround: None.
- CSCsr49559—The 802.11a radio in mesh access points sometimes adds an unnecessary extra byte in the country information element (IE 7) in the beacons.

  Workaround: None.
- CSCsr51667—When you use the GUI to refresh the message logs of a controller running software release 4.2.130.0, a “Connection interrupted/page load” error might appear, and the following message appears in the message logs:

  ```
  EMWEB-1-BUFFER_TOO_MANY: Received too many Http buffers from a session. BufCount(xx) >
  Max (xx), BufLen= 16607. Aborting session
  ```

  Workaround: Use the controller GUI to navigate to the **Message Logs** page or use the controller CLI to enter the **show msglog** command.
- CSCsr55953—The controller might drop traffic to the CPU and log the following message: “NP3400_interrupt.c:3766 Could not enqueue pkt_type 6 (proto 0x0000, len 108), return -12.(6 suppressed msgs).”

  Workaround: None.
- CSCsr57256—A 1520 access point joined to a 4400 series controller running software release 4.1.192.22M reports an 802.11a radio operational state of UP when the radio is disabled after resetting the access point.

  Workaround: None.
- CSCsr58532—This message sometimes appears on 2106 controllers: “SIM-3-INTFGET_GIG_ ETH_FAIL: Failed to get the interface number of the Gigabit Ethernet Port.”

  Workaround: Cisco 2106 controllers do not contain a Gigabit Ethernet port, so you can safely ignore this message.
- CSCsr61016—When you disable the 802.11a radio in a 1520 series access point in root access point (RAP) mode, the radio continues to send beacons, and client devices remain associated to it.

  Workaround: Disable 802.11a client access to force clients to disassociate. However, the radio remains enabled.
- CSCsr70861—A controller running software release 5.0.148.0 does not display a reason when external web authentication fails.

  Workaround: None.
- CSCsr70862—A Cisco WiSM controller running software release 4.2.130.0 might reboot because of a software failure of the instruction located at 0x1038a140(ewsInternalAbort+348).

  Workaround: Set the session timeout to zero or remove Telnet access.
- CSCsr72091—The controller radio resource management (RRM) feature sometimes fails to adjust the transmit power on the radios in 1250 series access points.

  Workaround: None.

- CSCsr75350—When a 1230 series access point joins a 4404 controller, the 2.4-GHz channel on which the access point is operating differs between the controller and the access point.

  Workaround: None.
- CSCsr78181—When a controller running software release 5.1 boots up, you can press **ESC** for more options. Password recovery should be an option, but it is not.

  Workaround: Use the proper password recovery procedure. Follow the instructions in the “Restoring Passwords” section in Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2*.
- CSCsr83684—When you enable link aggregation (LAG), the source MAC address for dynamic interfaces might change during operation.

  Workaround: None.
- CSCsr85444—The link test does not work for non-Cisco Compatible Extension clients. The following error message appears on the access point CLI: “No response received.”

  Workaround: None.
- CSCsr86947—Under moderate traffic loads, 1310 series access points and bridges sometimes produce a core dump.

  Workaround: Reboot the access point.
- CSCsr89399—Cisco 1131AG access points that are connected to Cisco WiSM controllers might reboot unexpectedly.

  Workaround: None.
- CSCsr89694—Cisco WiSM controllers running software release 4.2.130.0 generate trap logs indicating that the control path between two random mobility members is down. About 10 to 20 minutes later, the control path comes back up.

  Workaround: Disable guest tunneling.
- CSCsr89894—If a client roams from one controller to another and then powers down or leaves the RF range, the client entry on the first (anchor) controller is not deleted even though the client entry on the second (foreign) controller is deleted correctly.

  Workaround: Manually delete the client entry from the anchor controller.
- CSCsr91361—The Regulatory link returns a “Page not found” message on the controller GUI in software release 5.1.151.0.

  Workaround: None.
- CSCsr94019—Under moderate traffic loads, 1100 and 1121 series access points sometimes generate a core dump.

  Workaround: Reboot the access point.
- CSCsu04447—If you enable TACACS+, you cannot classify rogue access points using the controller GUI.

  Workaround: Use the controller CLI to classify rogue access points or disable TACACS+.
- CSCsu09424—Cisco 2100 series controllers sometimes reboot unexpectedly when you upgrade from software release 4.2.121.0 to 5.2.157.0.

  Workaround: Upgrade to a more recent controller software release. Make sure to follow the upgrade instructions in the *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points* for that release.

- CSCsu11528—Very large (usually greater than 6000-byte) UDPs or pings sent from a wired node and originating at a 1-Gbps line rate might not be transmitted successfully downstream to a wireless client or even back onto the Ethernet or to the controller itself.

  Workaround: None.

- CSCsu21697—The following messages might appear for 1100 and 1200 series access points because of a script that periodically (every 30 minutes) uses Telnet or SSH to reach an access point to retrieve some information. The underlying problem is that these access points have low memory.

  ```
  *%AAA-3-ACCT_LOW_MEM_UID_FAIL: AAA unable to create UID for incoming calls due to
  insufficient processor memory
  *%DATACORRUPTION-1-DATAINCONSISTENCY: copy error,  -PC= 0x0
  0062AB8 -Traceback= 0x5E60C 0x7CFE4 0x9C754 0x62AB8 0x63698 0xBF8D8 0x19F0A0
  ```

  Workaround: Configure the following at the access point: **aaa memory threshold authentication reject 2**. This workaround reduces the requested memory during script operation.

- CSCsu24001—The controller does not fragment outgoing CAPWAP packets according to MTU value.

  Workaround: Do not set the MTU below 800.

- CSCsu24197—Users need the ability to limit the number of associations per access point or WLAN on the controller.

  Workaround: None.

- CSCsu25277—If you disable SSH and then try to use it, a Telnet error (rather than an SSH) error appears.

  Workaround: None.

- CSCsu27886—When you configure conditional web direct without first configuring 802.1X security, the controller shows this error message: “Invalid parameter specified.” The message should state that 802.1X is required when you configure conditional web direct.

  Workaround: None.

- CSCsu30254—When you configure an access point group VLAN for an old WLAN and then remove it, the access point group VLAN configuration does not remove the mapping accordingly.

  Workaround: Reconfigure the access point group VLAN to remove the unwanted VLAN mapping.

- CSCsu35798—The controller cannot send roam log requests to clients.

  Workaround: None.

- CSCsu37392—If you connect a 1250 series access point directly to a PC running Tftpd32 without a firewall and use a mode button reset, a timeout might occur during a TFTP transfer.

  Workaround: None.

- CSCsu37449—All of the access points joined to a controller running software release 4.2.112.0 might reboot at the same time.

  Workaround: None.

- CSCsu38925—After you upgrade a 2106 controller to software release 5.1, access points sometimes fail to join the controller automatically.

  Workaround: Downgrade the controller to a software release earlier than 5.1.

- CSCsu39716—When an access point in workgroup bridge mode associates in a NAC-enabled WLAN, it should receive an IP address from the interface that is mapped in the access point group. Instead, the workgroup bridge receives an IP address from the interface to which the WLAN is mapped.

  Workaround: Always map both the WLAN and the access point group to the same interface.
- CSCsu40636—The access point sometimes ignores the CTS duration when receiving U-APSD trigger frames and simply transmits.

  Workaround: None.
- CSCsu42414—The controller CLI command **show client ccx rm** *mac_address* **pathloss** does not report correct information.

  Workaround: None.
- CSCsu44516—A 4404 controller running software release 4.0.179.8 and connected to a Catalyst 3750 stack might sometimes show wireless clients stuck in the DHCP_REQD state and unable to pass traffic. This issue seems to occur for RF hand-held scanners.

  Workaround: Reset the controller to purge the client associations.
- CSCsu44722—When you enable a mobility anchor on a WLAN and then try to enable IPv6 support for the WLAN (which is not supported), the controller shows an invalid error message.

  Workaround: None.
- CSCsu50275—When an1130 or 1240 series access point in bridge mode using mesh code attempts to join a non-mesh controller, the image transfer fails because non-mesh controllers do not contain mesh images.

  Workaround: Delete the *private-multiple-fs* file from the access point flash. After the access point joins a mesh controller, set the access point mode to local.
- CSCsu52247—Tracebacks sometimes appear on the anchor controller in Layer 3 mobility when a client roams from one controller to another.

  Workaround: None.
- CSCsu52837—Pre-authenticated clients cannot reach web-authenticated clients on the same WLAN.

  Workaround: None.
- CSCsu52969—The controller's NPU table shows the static IP address for a client in reverse. For example, it shows the static IP address 12.34.56.78 as 78.56.34.12.

  Workaround: None.
- CSCsu54884—An ad-hoc rogue access point marked "Internal" on the controller is not trackable. You cannot see the rogue access point anywhere in the configuration of the controller.

  Workaround: None.
- CSCsu56269—The Cisco WiSM might reboot because of a software failure of the radiusTransportThread task on the instruction located at: 0x10c1a820 (ber_int_sb_write+361384).

  Workaround: None.
- CSCsu57111—The following tracebacks might appear in the controller message logs: "apf_foreignap.c:1292 APF-1-CHANGE_ORPHAN_PKT_IP: Changing orphan packet IP address for station00:11:22:33:44:55 from x.x.x.x --->y.y.y.y- Traceback: 100cd4c0 100cddd0 100e40a8 10409864 10c064cc 10d748d8."

  Workaround: None.

- CSCsu59410—If you upload a custom logo for web authentication, back up that configuration, and try to restore it on a controller that does not have this file uploaded, the controller reboots for every WCS audit. The controller might also reboot after you enter for a CLI command related to web authentication, such as **show custom web-auth**.

  Workaround: Try to upload the logo, or try to unconfigure the custom logo.
- CSCsu60683—Controllers sometimes report that a 1252 series access point in workgroup bridge mode is associated to an access point through the 802.11n radio when in fact it is associated through the 802.11g radio.

  Workaround: None.
- CSCsu61354—When you attempt to set MAC filters on the controller from WCS, an error message appears indicating that the MAC address cannot be set because it already exists in the database. The error message should indicate that the MAC address is already associated by Auth-list.

  Workaround: Enter **config auth-list delete** *mac_address* and **config macfilter** *mac_address* using the controller CLI. Then enter **show mac-filter** to see the newly created MAC address.
- CSCsu62060—The 4400 series controller might reboot because of a software failure of the tplusTransportThread task.

  Workaround: None.
- CSCsu63676—An SNMP query on the agentInterfaceName SNMP variable sometimes creates a loop.

  Workaround: None.
- CSCsu66305—When you enable link latency MAC on the controller GUI, the access point does not use voice data rates (24, 12, and 6 Mbps). Instead, the access point uses the regular rates defined for the radio.

  Workaround: Set the voice rates as the default data rates for the radios. However, this workaround might not be recommended if the network is being shared with data clients.
- CSCsu69321—In controller software release 5.2.157.0, if you download a configuration with WPA + 802.1X and PSK security, no XML dependency errors appear.

  Workaround: While downloading the configuration, make sure that WPA + 802.1X and PSK are not both enabled. You should choose either WPA + 802.1X or WPA + PSK.
- CSCsu71747—On a Catalyst 3750G Wireless LAN Controller Switch running software release 5.1.151.0, the integer value returned by the SNMP object ifNumber is 2, but IfIndex actually returns three indexes.

  Workaround: None.
- CSCsu72070—The following error message might appear in the message log of a 4402 controller running software release 4.1.192.22M:

  ```
  Sep 12 11:08:04.638 apf_policy.c:339 APF-3-CLEAR_TKN_TABLE_ENTRY_FAILED: Trying to
  clean an empty token entry 88!.
  ```

  Workaround: None.
- CSCsu72077—Debug commands sometimes become disabled on the controller several minutes after you enable them.

  Workaround: Enable **debug** commands on the controller console rather than through Telnet or SSH.

- CSCsu74008—On a Catalyst 3750G Wireless LAN Controller Switch running software release 5.1.151.0, the results of ipRouteIfIndex for some routes point to an interface with index 5. However, the results of IfIndex show only three interfaces with their corresponding indexes.

  Workaround: None.

- CSCsu74540—When intrusion attacks occur on access points, the controller does not generate expected IDS traps.

  Workaround: None.

- CSCsu75686—When you configure the DHCP Addr. Assignment option on a WLAN using the controller GUI, the controller CLI shows incorrect output in the **show running-config** command.

  When you use the controller GUI to enable the DHCP Server Override option and configure a DHCP address, and you do not enable the DHCP Addr. Assignment option, the **show running-config** command shows:

  ```
  wlan dhcp_server <wlan ID> x.x.x.x required
  ```

  The correct output should be:

  ```
  wlan dhcp_server <wlan ID> x.x.x.x
  ```

  When you use the controller GUI to enable the DHCP Server Override option, configure a DHCP address, and enable the DHCP Addr. Assignment option, the **show running-config** command shows:

  ```
  wlan dhcp_server <wlan ID> x.x.x.x required required
  ```

  The correct output should be:

  ```
  wlan dhcp_server <wlan ID> x.x.x.x required
  ```

  Workaround: None.

- CSCsu76295—When you configure a pre-authentication access control list (ACL) for a WLAN and allow traffic to and from the client to the management interface, the client cannot reach the management interface. Clients can access the management interface after web authentication.

  Workaround: None.

- CSCsu81856—A 4402 controller running software release 4.2.130.0 configured with an internal DHCP server might sometimes display DHCP leases for addresses that are statically assigned to various wireless clients.

  Workaround: Use an external DHCP server.

- CSCsu82045—On a controller running software release 5.1.151.0, clients that are redirected to an internal web authentication page receive a “Page not found” error. This error occurs using both HTTP and HTTPS.

  Workaround: None.

- CSCsu82097—When you configure the WCS server to monitor ACS servers, it might occasionally report false alarm notifications against the ACS servers. The alarm notification shows a deactivation followed almost immediately by an activation notice for the ACS servers.

  Workaround: Disable the alarm notifications for ACS servers.

- CSCsu84220—When a WAN outage occurs, the 1131AG and 1242AG access points joined to a controller running software release 4.2.130.0 come back online, but the radios remain in the “down” state, and the following message appears: “Unable to verify sufficient in-line power.”

  Workaround: Reboot the access points.

- CSCsu84498—The 1240 series access point transmit diversity for multicast and broadcast packets does not alternate on antenna ports. It should alternate on consecutive packets (from A to B and so on).

  Workaround: None.

- CSCsu84629—When 1250 series access points receive neighbor discovery packets (NDPs), they sometimes switch from maximum uniform transmit power to maximum transmit power.

  Workaround: None.

- CSCsu86627—Controllers sometimes fail to send burst neighbor discovery packets (NDPs) to correct radio power control loop errors.

  Workaround: None.

- CSCsu87249—When you use the controller as the local authenticator for PEAP, you cannot successfully authenticate a user account using the domain-username format.

  Workaround: When using PEAP, do not create user accounts with the domain credentials in front of the username.

- CSCsu88956—System messages with tracebacks sometimes appear in the message logs of Cisco WiSM controllers when you edit and save a WLAN with only the 802.11a radio enabled.

  Workaround: None.

- CSCsu89905—The following error message might appear on a controller running software release 4.2.130.0 during boot-up:

  ```
  dtl_cfg.c:714 DTL-3-CALLBACK_PROC_FAILED: Callback for command:26 failed for user
  port: 0/0/x
  ```

  Workaround: None.

- CSCsu90052—The following error message might appear on 4400 series controllers: “sim_config.c:194 SIM-3-INTFGET_GIG_ETH_FAIL: Failed to get the Interface number of the Gigabit Ethernet Port.”

  Workaround: Clear the configuration and reconfigure the controller.

- CSCsu90074—The following error message might appear on the controller at boot-up: “sim.c:272 SIM-3-INVALID_PORT: Using invalid port number. Port out of range. Port # 0.”

  Workaround: None.

- CSCsu90097—The following error message might appear on the controller: “spam.c:449 LWAPP-2-SEM_CREATE_ERR: Could not create semaphore for notifying AP registration.”

  Workaround: None.

- CSCsu90112—The following error message appears on the controller at boot-up, even though symmetric mobility tunneling is disabled: “dtl_ds.c:428 DTL-3-DSNET_CONF_FAILED: Unable to set symmetric mobility tunneling to enabled on Distribution Service interface.”

  Workaround: Clear the controller configuration and reconfigure the controller.

- CSCsu90335—Intel 4965 cards might experience connectivity problems when another client connects to the same 1250 series access point in hybrid-REAP mode on a controller running software release 4.2.130.0. The loss of connectivity can last up to 1 minute.

  Workaround: Disable local switching on the WLAN, use Intel 4965 driver version 11.1.1.11, or make sure the second client has an 802.11b radio and not an 802.11g radio.

- CSCsu92667—The controller might reboot after you make changes to the configuration.

  Workaround: None.

- CSCsu93474—Upgrading the controller from software release 4.2 to 5.2.157.0 sometimes fails.

  Workaround: Try the upgrade a second time.

- CSCsu93819—The LLM voice rate-shifting algorithm for voice packets does not work as expected with low-latency MAC enabled. The retransmission should occur with the rate shifted down for failed packets. However, the access point sends retransmissions at the same rate.

  Workaround: Do not enable low-latency MAC.

- CSCsu95855—After you change the mobility group name on some controllers, you cannot remove one of the controllers. An error appears stating that the controller is configured as an anchor for a WLAN, even though none of the existing WLANs has this controller configured as its anchor.

  Workaround: If the CLI shows this controller as an anchor for a WLAN that does not exist, create that WLAN and then overwrite the WLAN and remove its anchors. Then you can remove the controller from the mobility group.

- CSCsu96326—When you save the controller's map on WCS, all of the 1520 series access points that are joined to the controller suddenly disconnect.

  Workaround: Choose the correct antenna on WCS after initially placing the access points on the map. Your selection should correspond to the antenna gain configured on the controller. If this setting is the same for both radios and you save the map on WCS, the access point does not reboot.

- CSCsu96916—When you issue the **show run-config** CLI command using SSH on a 4400 series controller running software release 4.2.130.0 with paging disabled, the output locks up at a certain point, probably because the controller runs out of buffers.

  Workaround: Enable paging or use a Telnet session.

- CSCsv00108—The controller might report an invalid message integrity check (MIC) on beacon frames.

  Workaround: None.

- CSCsv00342—When you clear the Back-up Primary Controller and Back-up Secondary Controller parameters on the Global Configuration page and click **Apply**, the controller does not clear the parameters.

  Workaround: To clear the parameters, enter **0.0.0.0** in the Back-up Primary and Back-up Secondary Controller IP Address fields and enter an arbitrary name in the Back-up Primary and Back-up Secondary Controller Name fields and click **Apply**. The IP Address field changes to 0.0.0.0, and the Name field remains blank.

- CSCsv01840—During long-duration, dual-radio throughput to 802.11n clients, 1140 series access points sometimes show CAPWAP errors on the console. Traffic might be briefly interrupted but resumes at the same best rate.

  Workaround: None.

- CSCsv01844—When you filter clients using the controller GUI, the controller repeats the last two characters of the filter text, and the filter does not work.

  Workaround: Use the controller CLI to view the clients.

- CSCsv02613—The RxFragmentCount in the output of the **show ap stats** command shows an incorrect value. This issue seems to occur for 1100 and 1200 series access points and 1310 series bridges.

  Workaround: None.

- CSCsv11336—The web portal (portal_login.html, portal_logout.html, and offline.html) are not available in controller software release 4.2.

  Workaround: None.

- CSCsv12308—When the controller has to use its default gateway to talk to an access point, the access point never sees the join reply from the controller because the AP-manager uses the wrong MAC address for the default gateway.

  Workaround: Clear the default gateway on the AP-manager or reboot the controller.

- CSCsv12512—Cisco 1230 series access points might stop servicing clients. If this issue occurs while you are connecting a console cable, the following output appears:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 2396 bytes failed from 0x43C46C, alignment 0
  Pool: Processor  Free: 7332  Cause: Memory fragmentation
  Alternate Pool: None  Free: 0  Cause: No Alternate pool
   -Process= "LWAPP CLIENT", ipl= 0, pid= 36 -Traceback= 0x5DCB8 0x1A10C8 0x1A315C
   0x1A382C 0x43C470 0x448EBC 0x43F7B4 0x43F2F8 0x43DA04 0x193F50
  %LWAPP-3-CLIENTERRORLOG: Echo Request: could not allocate buffer
  %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 255.255.255.255 started - reconnection
  %% Low on memory; try again later
  ```

  Workaround: Reboot the access point.

- CSCsv12525—The controller might freeze and then fail to respond to pings. The controller does not generate a crash log following a reboot.

  Workaround: None.

- CSCsv13068—An access request from the controller to the RADIUS server has the Authenticator field set to all zeros.

  Workaround: None.

- CSCsv14863—When access points that have been converted to lightweight mode join a 4.2.130.0 controller with a channel of 0 and a power level of 0, the controller does not send the correct RF settings to the access point.

  Workaround: Reapply the auto-RF settings.

- CSCsv16072—The controller might reboot multiple times.

  Workaround: Disable **debug** commands before transferring files or during normal operation. Also, make sure to install only valid software releases from the Software Center on Cisco.com.

- CSCsv18406—The help information for the controller CLI command **config ap led-state** {**enable** | **disable**} lists only *ap_name* as a configurable option. The **all** option is also available.

  Workaround: Use the **all** option even though it is not listed in the help.

- CSCsv18730—Controllers sometimes unicast an ARP check to the default gateway every 5 to 7 seconds rather than using the configured ARP timeout interval.

  Workaround: None.

- CSCsv34948—The following error message might appear after you upgrade from controller software release 4.1.192.35M to 5.2.157.0 on a Cisco WISM:

  ```
  Msg 'LRAD Entry set' of LRAD Table failed, Id = 0x0029b6b9 error value = 0xfffffffc
  Msg 'Set Multicast Params' of System Table failed, Id = 0x007fb6b9 error value =
  0xfffffffc
  ```

  Workaround: None.

- CSCsv41197—A new client can associate to a hybrid-REAP access point in standalone mode even though MAC filtering is enabled.

  Workaround: Do not use MAC filtering on a WLAN with hybrid-REAP access points in standalone mode.

- CSCsv50357—If you upgrade the controller from software release 4.1.191.xM to 4.1.192.xM and then to software release 5.2.157.0, the controller might reboot without a crash file.

  Workaround: After you upgrade the controller to software release 5.2.157.0, manually reset the controller without saving the configuration. You can ignore any XML validation errors that appear when the controller comes up after the manual reset. Make sure to check the RRM configuration settings after the reset to verify that they are correct.

- CSCsv83452—A 4400 series controller with link aggregation (LAG) disabled might reboot when a large number of access points attempt to join.

  Workaround: Reduce the number of access points trying to join the controller.

- CSCsv87375—The radios in an 1140 series access point might reset when operating in an environment with mixed clients and heavy traffic.

  Workaround: Reset the access point.

- CSCsv92640—When you use the **show ap eventlog** *Cisco_AP* controller CLI command to view the event log for mesh access points, the log might take some time to appear, or the access points might time out with an error.

  Workaround: None.

- CSCsv93998—In rare conditions when the network environment causes access points to quickly move back and forth between two controllers continually, the controller might reboot with a failure of the task “spamReceiveTask” and then resume normal operation.

  Workaround: In order to reduce the possibility of the task “spamReceiveTask” failing and the controller rebooting, adjust your network environment to prevent the access points from continually moving back and forth between controllers.

- CSCsv98057—If you try to upgrade a 2100 series controller from software release 4.2.130.0 to 5.2.157.0, the upgrade might fail, and the controller might reboot.

  Workaround: Upgrade to controller software release 4.2.176.0 before upgrading to 5.2.157.0. The controller might display the “Routine system resource notification” error message, as an indication of memory status. You can safely ignore this message.

Resolved Caveats

These caveats are resolved in controller software release 5.2.157.0.

- CSCsb77595—When you log out from Telnet/SSH sessions, the session prompts you to save changes, even if you have made no changes.
- CSCsg78333—When you define internal DHCP scopes on the controller, the current allocated lease information is not available on the controller GUI.

- CSCsg88704—When you use the default controller setting of 512 for the controller database size, the following problems may occur:
  - If you attempt to add a MAC address to a very long MAC filter list, the following error message appears: "Error in creating MAC filter."
  - If you add a large number of users to the local database, some user entries might be silently ignored.
  - If you add SSCs for the access points, at some point no more entries can be added, and the following error message appears: "Authorization entry does not exist in Controller's AP Authorization List."
- CSCsh34897—You cannot enable memory core dumps and upload them to a TFTP server on the controller GUI.
- CSCsh40424—You cannot configure Power over Ethernet (PoE) settings for access points using WCS.
- CSCsj47472—When refreshing the configuration from WCS on a 2106 controller with software release 4.1.171.0, the IP address and subnet mask are inverted in the SNMP community string template.
- CSCsj48872—After you upgrade the controllers in a Cisco WiSM from software release 4.0.206.0 to 4.1.171.0, both of the controllers may reboot repeatedly.
- CSCsk04796—You cannot upload the radio crash file using WCS or any other SNMP manager.
- CSCsk41197—When no RADIUS servers are configured and a 1510 series access point authenticates through the local database, the following message appears even though the access point joins: "bauth_sm.c:400DOT1X-1-MAXAAA_FAILURE_ON_MOBILE: Max AAA failure on mobile00:0b:85:xx:xx:xx."
- CSCsk44641—The "Multicast Rx queue is full" message might appear in the controller's message log even when multicast is disabled and no multicast traffic is present. The controller needs to separate or prioritize the incoming ARP broadcast and multicast traffic types so that they do not affect access point joining or LWAPP communications.
- CSCsk54969—One of the controllers in the Cisco WiSM might stop providing web authentication login pages but continue to allow WPA2 RADIUS authentication to the same authentication server.
- CSCsk68619—When using an Intel 4965 802.11n client device with a 1250 series access point, the upstream throughput is higher than the downstream throughput.
- CSCsk76537—4400 series controllers running software release 4.1.185.0 might lock up. They cannot be accessed through the console, and they do not reboot on their own.
- CSCsl11352—The console output in software release 4.2 does not indicate which controller an access point joins when you add it to your network.
- CSCsl24302—When a hybrid-REAP WLAN client acquires a DHCP address from a switch, it never encounters the DHCP timeout policy. The controller is able to see the IP address of the client. On the other hand, when the client does not have an IP address, the controller continuously runs the DHCP timeout every 2 minutes. The client disassociates after 2 minutes as the IP address is not seen, even while DHCP REQ has been disabled.
- CSCsl32786—Guest accounts might be lost after the controller reboots.
- CSCsl48417—The DTL-1-ARP_POISON_DETECTED, DTL-1-IP_CONFLICT_DETECTED, and other controller DTL messages need to be more descriptive.
- CSCsl52445—The internal web authentication page on the controller accepts up to 2,047 characters, but the internal web authentication page in WCS accepts only 130 characters.

- CSCsl57356—When an 802.11n client is associated to a 1250 series access point, sometimes the client does not show up as 802.11n on the controller GUI and CLI. Instead, the controller shows the associated client using the 802.11a or 802.11b protocol if using the 2.4-GHz or 5-GHz band, respectively. However, the client software shows that the client is connected using the 802.11n protocol and at 802.11n data rates.
- CSCsl59308—When you change the WLAN configuration, the controller might generate "MFP Anomaly Detected" alarms, which are reported on the WCS as "Invalid MIC" events. The alarms might originate from many different valid access points.
- CSCsl61657—When you enable the 802.11g network on the controller, wireless clients that support only long slot times (approximately 20 microseconds) have difficulties associating to the access points.
- CSCsl77058—The word "rogue" is misspelled in one of the WLAN message log statements. The correct statement should be "APF-1-UNABLE_TO_KEEP_ROGUE_CONTAIN."
- CSCsl79260—Wired guest LAN clients fail to obtain an IP address if DHCP proxy is disabled.
- CSCsl80225—The controller deletes the access point radio core dump file when the TFTP transfer is unsuccessful.
- CSCsl90630—Dynamic channel assignment (DCA) requires you to add at least one non-DFS channel to the list. However, non-DFS channels are not available for an access point deployed outdoors in the EU.
- CSCsl94719—The Preview button on the controller GUI shows the internal default web page, even if you chose Customized for the Web Authentication Type.
- CSCsm03461—A command is needed to show the ER image or bootloader version that is currently running as well as the one that will be installed on the next bootup. Currently, the bootloader is used to verify if an ER image or bootloader upgrade is successful. However, not all controllers include the bootloader in the ER image.
- CSCsm04622—The CPU ACL does not filter traffic to dynamic interface addresses.
- CSCsm04752—The GUI of an anchor controller shows a wired client as mobile rather than as 802.3.
- CSCsm05607—Large user packets may fail to be successfully forwarded in an EoIP mobility/guest tunnel between controllers.
- CSCsm08062—The controller might reboot due to failure in the dtlDataLowTask on the instruction located at 0x1042908c (hapiMmcReceiveDataLow+788).
- CSCsm08623—If the **config paging disabled** CLI command is entered on the controller, the output of the **show msglog** command is periodically interrupted with the "Would you like to display the next 15 entries?" prompt.
- CSCsm10852—If you disable client tracking on WCS under the Tracking parameters tab of the location server, a service change request is sent to the controller. The controller should not send client RSSI, INFO, and STATS notifications to the Location Appliance after receiving this message, but the Location Appliance still receives the notifications.
- CSCsm12623—The AAA override dynamic VLAN assignment fails with guest tunneling. Clients successfully authenticate, but the IP address is that of the interface the WLAN is associated to on the anchor controller.
- CSCsm15583—The **show database summary** output exceeds the number of eligible entry types displayed by individual **show** commands. This command needs to identify and remove "other" entries so eligible entries configured on the controller can be entered up to the maximum database value.

- CSCsm17459—Some CLI commands that are entered in capital letters (such as “EXIT”) do not work on the controller or generate an error.
- CSCsm25987—Users are unable to add a RADIUS server to a wired guest LAN using the controller GUI.
- CSCsm26312—The controller might reboot because of a software failure of the BsnMDAframeMonitorTask on the instruction located at 0x1040281c (BsnMDAFrameMonitor+1500).
- CSCsm27577—Local authentication EAP-TLS fails when CN Identity Check is enabled and the CN identity username contains spaces.
- CSCsm40866—The “ASSOCREQ_PROC_FAILED: Failed to process an association request” message should have some form of suppression. With a wireless network and a user base of approximately 10 users, this message fills up the logs, making them useless.
- CSCsm40899—The following message should include the MAC address or username of the aborted user and, if possible, the reason code: “1x_bauth_sm.c:443 DOT1X-3-ABORT_AUTH: Authentication Aborted.”
- CSCsm44025—The following unclear error message appears when you change the Web Authentication Type parameter from Internal (Default) to Customized (Downloaded) on the Web Login page without first disabling the WLAN: “Error! Please look up custom-web information and disable Web-Auth/Web-Passthrough WLAN's with Global Status set.”
- CSCsm44369—The following debug output does not indicate which stream could not be opened: “SshPmStAppgw/pm_st_appgw.c:681/ssh_pm_st_appgw_tcp_open_initiator_stream: Could not open initiator stream.”
- CSCsm44383—The following debug output does not indicate which instance was terminated: “SshPmStAppgw/pm_st_appgw.c:1094/ssh_pm_st_appgw_terminate: terminating appgw instance.”
- CSCsm45147—An error is not produced when you delete an interface mapped to an access point group VLAN. Instead, the access point group VLAN mapping retains the deleted interface in the configuration.
- CSCsm47699—The AP Manager Interface IP Address prompt in the configuration wizard generates an “Invalid Response” message instead of returning to the previous prompt as expected.
- CSCsm48076—Guest-related trap logs are not generated for a lifetime guest user.
- CSCsm50774—The controller might reboot due to a failure of the apfReceiveTask software watchdog.
- CSCsm58695—When an 802.3 raw broadcast packet is received from the wired network and 802.3 bridging is enabled, the packet is discarded rather than forwarded to the wireless network.
- CSCsm64359—If a WLAN uses LDAP as the back end for web authentication, any clients connected to the web-authentication-configured WLAN can become authenticated with the wrong username and password.
- CSCsm65113—Access points converted to lightweight mode do not retain the power injector state after a reboot.
- CSCsm71840—Mobile client handoff or client guest anchoring fails across mobility groups if the controller to which the client is associating has no other mobility member in its own mobility group but has all members in different groups.
- CSCsm72088—If you change the associated client filter on the controller GUI to filter on WLAN profiles that contain spaces, the controller reports that the profile name is wrong and shows no clients associated.

- CSCsm75593—When the AP-manager is untagged or configured for VLAN ID 0, the following error message appears: "First configure a valid non-zero VLAN on this interface."
- CSCsm78257—Some workgroup bridge clients fail to associate if the WPA information element (IE) is different in the probe response and the associate response packets. This issue occurs only when WPA TKIP and AES and WPA2 TKIP and AES are all enabled.
- CSCsm85717—The following error message needs to identify the root cause of the problem:

```
sntp_main.c:441 SNTP-4-PKT_REJECTED: Spurious.NTP packet rejected on socket.
```

- CSCsm88778—Cisco Aironet 1522 mesh access points use only clear channel assessment (CCA) and no virtual carrier sense mechanism to ensure the medium is free for a transmission. In environments where mesh access point children cannot hear each other but are all communicating with the same mesh access point parent, a "hidden node" issue could cause collisions at the parent's radio interface and with transmission retries on the access point children.
- CSCsm91814—When a client associates and authenticates on the same SSID using a different username and password, a 4400 series controller using WPA2-AES and PEAP-MSCHAPv2 might randomly cache the AAA override values such as dynamic VLAN and assign the client to the wrong VLAN. The client also obtains an IP address on the wrong VLAN.
- CSCsm95651—A controller running software release 4.1.185.0 might reboot spontaneously without generating a crash file.
- CSCsm96105—The controller does not pass traffic to a client device with a MAC address beginning with 00:00:00:00. This issue occurs with both WGB and wireless clients.
- CSCsm96307—A controller might reboot unexpectedly following a period of high CPU utilization charged to the SNMPtask. This condition triggers a Reaper Timeout and a system reset.
- CSCsm97315—While installing a web authentication certificate, the controller fails with an invalid password error. This problem occurs only on controllers that have been upgraded from software release 4.1.
- CSCsm98250—After you upgrade the controller to software release 5.0, web authentication stops working, and you can no longer access the controller through HTTP or a Telnet or SSH session.
- CSCsm99941—Controllers running software release 4.2 or 5.0 might reboot frequently if you enable rogue client and access point polling on the 2700 series Location Appliance, which is configured in WCS. If you enable the default polling interval for rogue clients and access points, the controller might reboot every 10 minutes.
- CSCso02467—When logging into a lobby ambassador account, you are able to create permanent guest user accounts by setting all parameters to "0." After logging back into the account, you can verify that these permanent accounts were created under Security > Local Net Users.
- CSCso03704—The Trap Receiver Name column on the SNMP Trap Receiver page of the controller GUI should be changed to "SNMP Community String" because the existing title does not adequately describe the field.
- CSCso06889—The controller allows you to delete an LDAP server that is configured as a web authentication LDAP server on a WLAN.
- CSCso07544—When mesh access points are on the same Layer 2 VLAN with autonomous access points, clients associated to mesh access points cannot ping or access network resources. Additionally, pings from the controller to the client often fail or intermittently return a third of the ping requests, and pings from the controller to mesh access points often fail as well.
- CSCso08708—When the physical ports for the management and dynamic interfaces are changed on the controller, quarantine VLAN information is not pushed to the NPU, which prevents network admission control (NAC) out-of-band integration from working.

- CSCso10043—When you add a RADIUS server on a controller, enable IPSec, apply the changes, then disable IPSec, apply the changes, and save the configuration, the controller sometimes indicates after a reboot that there are unsaved changes to the configuration.
- CSCso13516—The controller sometimes crashes at random, and the crash file shows a signal 11. Signal 11 occurs when the program running on the controller accesses a part of memory that it does not have permission to access.
- CSCso15640—The controllers in the Cisco WiSM might reboot due to a software failure of the instruction located at 0x1036f2ac (debugPrintMessage2+288).
- CSCso17430—Cisco 1510 access points show low throughput when joined to a workgroup bridge (WGB).
- CSCso17455—Controllers sometimes reboot when SSH is enabled.
- CSCso20018—If you configure wired guest access on a controller running software release 5.0, you cannot enable DHCP required on a guest LAN. The controller GUI becomes non-responsive and shows an error icon in the lower left-hand corner of the browser.
- CSCso23879—The coverage hold threshold values on the 802.11a (and 802.11b/g) > RRM > Coverage pages on the controller GUI cannot be changed when coverage hole detection is enabled. On the controller CLI, you can change the threshold values if the 802.11a or 80211b/g band is disabled globally. The controller GUI should operate the same way (as long as the 802.11a or 802.11b/g band is disabled globally, the threshold can be changed).
- CSCso27775—The controller logs on the CLI and the syslog server sometimes show several error messages on one line.
- CSCso30745—When a packet fails the admission control test, it is incorrectly forwarded to the CPU instead of being discarded.
- CSCso31067—Some clients might experience failures during upstream-only prioritized traffic on 802.11a, despite radio resource management (RRM) features being disabled.
- CSCso33631—The Multicast Groups page on the controller GUI shows the correct multicast group IDs (MGIDs) for up to 20 client devices but shows incorrect MGIDs for any additional clients.
- CSCso35129—If the controller is queried by SNMP for a virtual gateway interface address, it may generate messages such as “sim.c:1061 SIM-3-MACADDR_GET_FAIL: Interface 1 source MAC address is not found.”
- CSCso35517—The following error message appears continuously: “Potential Honeypot AP: 00:1a:a2:da:85:c0 detected on Base Radio MAC : 00:1a:e3:00:c0:90 Interface no:0(802.11b/g) with SSID: PrivateTH000A.”
- CSCso36248—The controller limits the LDAP username to 24 characters in software release 4.2.112.0.
- CSCso39413—Constant access control list (ACL) messages appear in the controller logs even though no ACLs are configured.
- CSCso40917—The FPGA link might stop working, causing the access points to disconnect from the controller and preventing the controller from being managed by any port other than the service port. The NPU Check Task or a similar task should monitor the status of the FPGA link.
- CSCso43490—The LDAP secure TLS feature does not work properly, so configuration and support for this feature needs to be removed from the controller GUI and CLI.
- CSCso43852—Controllers running software release 4.2.112.0 or controllers in the same mobility group that are running different versions of software might reboot unexpectedly.

- CSCso44508—When link aggregation (LAG) is enabled on the controller, the ipAdEntIfIndex value is not listed in the ifIndex.
- CSCso46517—If you try to change the access or quarantine VLAN to a VLAN that already exists on the controller, one of two error messages appears. The same error message should appear regardless of whether you are attempting to change the access or quarantine VLAN, and it should provide more detailed information.
- CSCso48158—The tickle timer, which is used to update the watchdog timer, is not preserved correctly when the NPU-to-CPU interrupt handler becomes congested and overrun. This issue affects console output and serial port communications, potentially used for low-level debug console output messages.
- CSCso52140—If the controller is configured for WPA2, the RSN capability within the RSN information contains a PMK identifier (PMKID) count within all probe responses. However, the PMKID count should be used only in the RSN information element in re-association request frames to an access point.
- CSCso52225—The output of the **show run-config** CLI command always shows the following parameters. It should show the parameters in use per queue based on the actual configuration.

```
MAC Operation Parameters
      Configuration ............................ AUTOMATIC
      RTS Threshold ............................ 2347
      Short Retry Limit ........................ 7
      Long Retry Limit ......................... 4
      Fragmentation Threshold .................. 2346
      Maximum Tx MSDU Life Time ................ 512
      Maximum Rx Life Time .................. 512
```

- CSCso52349—If SNMP is tested against the controller’s management IP address from a device on the same subnetwork as a dynamic interface, the controller fails to send SNMP responses.
- CSCso52692—When NAC out-of-band mode is enabled and a client roams from quarantine to access on a foreign controller, it generates message logs with tracebacks, which can be confusing to an end user.
- CSCso58911—After a controller is upgraded to software release 4.2.112.0, it no longer executes the Java pop-up window on the custom web authentication bundle login page.
- CSCso58919—When AAA override is disabled, the PMK CCKM lifetime value uses the attribute 27 setting from the AAA server instead of the WLAN session timeout.
- CSCso61281—If you enter an invalid username or password on the web authentication page in controller software release 5.0.148.0, an error message does not appear indicating that the username and password combination is invalid and to try again.
- CSCso62862—You cannot edit the TACACS+ priority using SNMP on a 4400 series controller running software release 4.2.112.0.
- CSCso62922—EAP authentication fails for clients when the controller is under high load. In the 802.1X debugs, the client responds to the identity request, but the controller does not seem to process it and times out the authentication.
- CSCso62975—The following error message might appear for Vista clients using an external DHCP server to obtain an IP address after going through the anchor controller: “DHCP dropping REPLY to STA with invalid mobility state `Export Foreign' (5) on foreign controller.”
- CSCso63232—The controller in the Catalyst 3750G Wireless LAN Controller Switch might reboot if you enter the **show hreap group detail** *groupname* CLI command without a group name or without a space between the **detail** parameter and the group name.

- CSCso65150—When AAA override is enabled for a WLAN and the AAA server is providing the session timeout value, if a client that is associated to that WLAN roams to another access point joined to the same controller and the session timeout has not expired, the session timeout for that client is reset to the initial value received from the AAA server.
- CSCso66504—The controller and WCS both show management frame protection (MFP) for a wired LAN, even though MFP is not supported for use with wired LANs.
- CSCso66778—The output of dump low-level debugs is not complete for several commands in controller software releases 5.0 and 4.2.112.0. This problem might affect proper troubleshooting for service port hangs, NPU issues, and so on.
- CSCso66819—The service port on the Cisco WiSM might become unreachable after some time.
- CSCso66889—When you configure access point credentials using software release 5.0, you cannot use the @ character.
- CSCso69005—After **config paging disable** is entered to disable page scrolling, the **show acl summary** and **show acl detailed** *acl_name* commands still show a "paging" prompt, which could break customer scripts.
- CSCso69568—The RADIUS accounting setting does not appear in the output of the show wlan wlan_ID CLI command if the WLAN security policy is one of the following:
  - None
  - Static WEP
  - WPA-PSK
  - Web authentication
- CSCso71603—When a client moves from one controller to a 2106 controller on the same subnet, the client cannot pass traffic for 5 minutes.
- CSCso72588—When you use the wired guest feature, an accounting stop record is not sent after the timeouts expire.
- CSCso76479—A CLI command is needed to disable SSLv2 for web administration and web authentication. When SSLv2 is disabled, users cannot connect using a browser configured with SSLv2 only. The new CLI command to enable or disable SSLv2 for web administration and web authentication is config network secureweb cipher-option sslv2 {enable | disable}.
- CSCso78437—After a client sends a reassociation request or response but before it has completed a four-way exchange, all of the packets coming to the client are dropped at the controller or forwarded to the wired side.
- CSCso81687—A forwarding failure occurs when an orphan packet is sent to the CPU using the slow path. The following message appears on the console: "NP3400_interrupt.c 3663: In `NP3400_BSN_process_frame_rx' Unknown packet type 0."
- CSCso81725—The controller's broadcast module is replicating CDP packets to all connected access points even if multicast is disabled. In addition, the controller is replicating broadcast orphan packets from a client even when multicast and broadcast are disabled.
- CSCso81845—The encryption requirements for 802.11n are either no encryption or AES. If WEP or TKIP is enabled on the WLAN, wireless clients cannot associate to the controller at 802.11n rates. The controller GUI should include a footnote specifying the requirements for 802.11n.
- CSCso83894—The output of the **show ap cdp neighbors** CLI command shows an incorrect message.
- CSCso84256—During CCKM roaming, the following misleading debug message might appear: "Creating a new PMK Cache Entry for station."

- CSCso84303—To aid in troubleshooting, the following error message should include the From and To MAC addresses: “apf_utils.c:2035 APF-3-VALIDATE_CCKM_REASS_REQ_ELEMENT_ FAILED: Could not validate the CCKM Reassociation request element.Received Timestamp deviation > 1sec in CCKM Info Element from mobile. Mobile:00:1d:a2:31:c9:0d.”
- CSCso86463—Some access points running software release 4.2.99.0 might crash if traffic stream metrics (TSM) is enabled.
- CSCso87099—Network access control (NAC) does not work when workgroup bridge (WGB) access points and wired clients roam in the quarantine state in the same subnet mobility setup.
- CSCso87175—SNMP support is needed to enable or disable DHCP proxy from WCS.
- CSCso89810—When you downgrade a controller from software release 5.0.148.x to 4.2.112.0, the LWAPP mode automatically changes from Layer 3 to Layer 2, and the AP-manager disappears and cannot be recreated. This problem is resolved in controller software release 4.2.130.0, so you can successfully downgrade from software release 5.0.148.x to 4.2.130.0.
- CSCso92229—The controller CLI accepts a CIDS SHA1 key with the correct number of hexadecimal digits but also accepts extra colons between the pairs of digits.
- CSCso92249—The controller sometimes reboots without a crash log when you run multiple Telnet sessions.
- CSCso92828—When an access point is running Rogue Location Discovery Protocol (RLDP), radio reset messages can be logged. However, the radio reset messages should be suppressed when caused by RLDP.
- CSCso93918—NPU rate-limiting functions inconsistently because BSN_PKT_LEN is incorrect for certain types of packets.
- CSCso98021—The software watchdog needs to be implemented in the 2106 controller.
- CSCso98358—If you make an error when entering a command, the **config paging enable** CLI command is executed.
- CSCso98702—The CCKM old access point MAC address never shows because the data structure is not updated.
- CSCso98915—A controller running software release 4.0.219.0 or 4.2.112.0 might reboot during the emweb process.
- CSCsq02092—1100 and 1200 series access points and 1310 series bridges fail to download image code from a 4400 series controller running software release 4.2. The following error message is logged:

```
Refusing image download to AP xx:xx:xx:xx:xx: - unable to open image file
/bsn/ap//c1yyy
xx:xx:xx:xx:xx:xx is the MAC address of the AP and c1yyy is the AP model number
```

- CSCsq07537—Clients continue to communicate with an access point that has its radio disabled by the controller. The controller shows that the access point radio is disabled when it is not.
- CSCsq08062—A TACACS+ connection initiated from the controller to the TACACS+ server sometimes times out in 0.5 seconds.
- CSCsq09933—After you use LWAPP conversion tool 3.2 to convert access points with a static IP address that have either SSCs or MICs, the access points seem to ignore the DNS resolution of cisco-lwapp-controller after already downloading the full image from the controller.
- CSCsq12776—The controller might crash without generating a crash file.

- CSCsq13174—Web authentication certificates have to be device certificates and should not contain the CA roots chained to the device certificate. This bug is resolved to now allow the device certificate to be downloaded as chained certificates (up to a level of 2).
- CSCsq13407—The dot1xTree might become corrupted if the tree lock is not acquired before entries are deleted from the tree.
- CSCsq14310—If the Allow AAA Override option is enabled for a WLAN, the guest role is not applied to the local net user.
- CSCsq14961—SNMP returns only one record for client roam reports whereas the controller CLI shows multiple records.
- CSCsq15645—When you use the controller GUI to change DTPC support for a network, the access point radios are reset without any notification. If you use the controller CLI, you are prompted that the network has to be disabled before the change can be applied.
- CSCsq23961—An orphan packet from the distribution system port might prevent DHCP from operating properly.
- CSCsq24255—When an access point is disabled or removed from the controller, a client entry is also cleared from the controller. However, the controller does not send an SNMP alert message to the NAC server that the client entry has been removed, so its entry remains on the server.
- CSCsq24256—The mobility anchor feature might not work properly for a controller running software release 4.2.121.0.
- CSCsq25029—A 2106 controller running software release 4.2.112.0 might reboot because of a software failure of the bcastReceiveTask.
- CSCsq26901—Cisco WiSMs running controller software release 4.1.186.2 sometimes crash due to a software failure on the instruction located at: 0x1020387c (rrmLradSetTxPower+676).
- CSCsq31662—The controller reboots after you upgrade from software release 4.2.61.0 to 4.2.112.0.
- CSCsq34216—The system logs on a controller running software release 5.0.148.0 might be filled with messages such as “apf_ms.c:4849 APF-1-USER_DEL_FAILED: Unable to delete user name **** for mobile **:**:**:**:**:**,” where the first set of asterisks represents a username and the second set represents a MAC address. The username that is listed is not a username that is configured anywhere on the controller.
- CSCsq35662—More debug messages are needed when an access point fails to download the software image from the controller.
- CSCsq35990—The **config netuser lifetime** CLI command does not accept a zero (0) value for the *lifetime* parameter.
- CSCsq41327—Under certain circumstances, the network processing unit (NPU) of a 4400 series controller or Cisco WiSM might lock up, causing a system restart, or the NPU Check Task might invoke a software crash. The resolution of this bug adds additional error and integrity checking in the NPU code path logic to ensure that the NPU Check Task does not branch to an invalid address.
- CSCsq49329—The **show services mobility detail** *ip_addr* CLI command generates an error on the 2106 controller, even when you enter a valid IP address.
- CSCsq49831—A core dump should be created when the controller crashes to aid in debugging.
- CSCsq49975—When you enable ARP debugs and generate a gratuitous ARP, the gratuitous ARP does not come up to the dtl ARP module, and no debugs appear on the console.
- CSCsq50866—When you configure QoS data rates for a guest role using the controller CLI, you can set values greater than 60000.
- CSCsq51733—The controller sometimes drops BOOTP packets from wireless clients.

- CSCsq55033—The AAA-1-INVALID_AUTHENTICATOR and other controller AAA messages are not documented or documented inadequately.
- CSCsq55117—The controller might reboot when multiple people are connected through Telnet at the same time.
- CSCsq56139—If you configure the controller to send only access point register traps, the controller still sends client traps.
- CSCsq57697—WPA2 PMK cache updates are not being sent across the mobility group.
- CSCsq59283—You cannot set the WLAN override group name or description to a length of 32 characters using SNMP.
- CSCsq61533—SNMP can be used to set a blank access point username on a controller running software release 5.0.148.0.
- CSCsq64862—Wired clients behind a non-root MAP cannot communicate with a GLBP or HSRP router through a mesh bridge link. Changes were made in the software to make the default multicast mode in-out to eliminate this communication problem.
- CSCsq65563—A software watchdog needs to be implemented on the Controller Network Module in order to allow the controller to be rebooted in the event of a system freeze.
- CSCsq73427—You cannot enable network admission control (NAC) on the management interface of a Controller Network Module using the controller GUI.
- CSCsq74318—The controller GUI accepts more characters in web authentication messages than the controller CLI. If the web authentication message is longer than 130 characters, the following error message appears in the controller log when you enter the **show custom-web all** CLI command: "CLIWEB-3-BUFFER_TOO_SMALL: Buffer for Customization message too small."
- CSCsq74459—Buffer corruption errors similar to the following might appear in the controller message log:

```
Message from syslogd@192.168.200.15 at Wed Jun 11 15:50:40 2008 ...
192.168.200.15 cntl4404_1: -Traceback:  10486788 10256018 1025731c 10257504 1062dd7c
1062eec0 1025b520 1044e158 10c710d4 10f1674c

Message from syslogd@192.168.200.15 at Wed Jun 11 15:50:40 2008 ...
192.168.200.15 cntl4404_1: -Process: Name:dot11a, Id:11fced78

Message from syslogd@192.168.200.15 at Wed Jun 11 15:50:50 2008 ...
192.168.200.15 cntl4404_1: *Jun 11 15:50:49.994: %BUFF-0-BUFFER_CORRUPT: buff.c:380
Buffer Pool id 5 ptr 0x3d2c532c, packet is printed on console.
```

- CSCsq74965—When you enter certain mesh CLI commands on the controller, the controller sometimes reboots, and you might see a traceback in the logs or a crash file indicating an EmWeb Reaper Reset.
- CSCsq81667—Large IP packets that have been fragmented into multiple fragments might not be reassembled by a 4400 series controller.
- CSCsq82061—The 2100 series controllers might reboot repeatedly because of a missed software watchdog in the SNMPTask.
- CSCsq83843—The following error message requires more information: "DOT1D-6-PORT_FIND_FAIL: Port number 1 is not found for GARP Information Declaration (GID)."
- CSCsq83855—More explanation is required for the following error message: "Process: Name:fp_main_task, Id:11d92ca8."

- CSCsq84257—If you configure an SNMP trap receiver, the controller sends an SNMP decrypt traps event when all of the client traps are disabled. A CLI command is needed to enable or disable client decrypt traps. To resolve this issue, the config trapflags 802.11-security wepDecryptError {enable | disable} command has been added.
- CSCsq87457—The Cisco WiSM might experience an NPU lockup or reboot on the NPUChecktask.
- CSCsr02760—When you configure a 1250 series access point with MFP validation, the access point triggers an MFP out-of-sequence alarm. For example:

```
31 Thu Jun 26 16:17:40 2008 MFP Anomaly Detected - 1 Out of sequence event(s) found as
violated by the radio XX:XX:XX:XX:XX and detected by the dot11 interface at slot 1 of
AP YY:YY:YY:YY:YY:YY in 300 seconds when observing Beacon Frames. Client's last source
mac XX:XX:XX:XX:XX
```

- CSCsr06596—After the controller has been up for several days, it might crash due to a failure of the apfRogueTask.
- CSCsr16752—The Controller Network Module NM-AIR-WLC6 might experience interface flapping after the interface is reset.
- CSCsr17163—Under conditions of very high stress, the controller shows no joined access points and clients and no traffic to or from clients. The controller also generates a crash file and reboots automatically.
- CSCsr20151—If you change the power level of a 1252 access point 5-GHz radio, the change does not take effect.
- CSCsr36756—When a controller running software release 5.1.151.0 tries to contain a rogue access point, the access point state changes from Contained to Alert.
- CSCsr41231—The following error message might appear on a controller running software release 4.2.130.0: “sim.c:1061 SIM-3-MACADDR_GET_FAIL: Interface 1 source MAC address is not found.”
- CSCsr52442—Auto completion does not work for the show port summary CLI command. If you enter show port summ rather than the complete command, an error message appears.
- CSCsr60506—The controller might unexpectedly reboot at spamReceiveTask with a signal 11 error (segmentation fault).
- CSCsr62942—Controllers running software release 4.2.112.0 might reboot due to a problem with the EAP framework.
- CSCsr63100—The controller’s message log sometimes fills with “sysapi.c:160 SYSTEM-3-SYSAPI_ERR” messages after you run dump-low-level debugs.
- CSCsr63356—Multicast does not get marked with the proper DSCP marking.
- CSCsr67780—When you enable RLDP on a 4402 controller running software release 4.2.130.0, the following error message appears:

```
apf_rogue_detect.c:593 APF-1-AUTHMOBILE_SEND_FAILED: Could not send the LWAPP
Authenticate Mobile command to rogue AP xx:xx::xx:xx:xx:xx  for mobile
xx:xx:xx:xx:xx:xx. Unable to find rogue client.
- Traceback:  100f342c 100f4f94 103d409c 10b955a8 10d4ec6c
```

- CSCsr68678—The following error message might appear following a reboot of the controller: “sim.c:309 SIM-3-INVALID_PORT: Using invalid port number. Port out of range. Port # 0.”
- CSCsr74598—6 dB should be added to RSSI reports for 1250 series access points using 2.4 GHz.

- CSCsr75121—The following decrypt errors might appear in the controller trap logs:

```
Decrypt errors occurred for client <client mac address> using WPA key on 802.11a
interface of AP <ap mac address>
Decrypt errors occurred for client <client mac address> using WPA2 key on 802.11b/g
interface of AP <ap mac address>
```

- CSCsr83671—The controller's dynamic channel assignment (DCA) feature sets access points to channel 36 for the 5-GHz band (802.11a).
- CSCsr89403—Diversity is disabled on 2.4-GHz access point radios.
- CSCsr95295—The controller CLI allows you to disable all legacy data rates with the network enabled. However, this invalid configuration disables the network.
- CSCsr97110—After you download an XML configuration file, a 4400 series controller running software release 5.1.151.0 might reboot continuously.
- CSCsu05190—The AP-manager does not reply with the correct destination MAC address with GARP. As a result, access points cannot join the controller after a failover from the primary firewall to the secondary firewall.
- CSCsu22727—After WCS pushes an access point template to the controller, the controller might reboot.
- CSCsu26961—Using WCS or the controller CLI, you can configure the controller for WPA+WPA2 with 802.1x/CCKM and PSK. To see whether 802.1x/CCKM is configured at the same time with PSK, run the **show wlan 1** or **show run-config** command and look at the output.
- CSCsu27939—Controllers running software release 4.2.130.0 might reboot because of a software failure of usmWebRRMRadSlotNoiseChannelGetNext+64.
- CSCsu50080—When you configure web authentication passthrough with email input on the controller, the controller allows any text to be entered. This feature implies that a client should have to enter an email address before proceeding. Although there is no way to verify that the email is valid, the controller should at least check that it follows this format: *name@company.com*.
- CSCsu52812—When the controller is in multicast-unicast mode, it sends unicast traffic to an access point before that access point fully joins the controller. This problem is serious when the access point is running a recovery image that does not drop LWAPP data packets, such as 12.3(11)JX1. If the number of data packets sent to the access point before it gets the full image is large enough, the access point locks up and cannot join the controller.
- CSCsv01484—The controller prepends UID usernames with "CN=," which can cause problems for LDAP authenticated binds. The controller should check for usernames with "UID" but not prepend them with "CN=."
- CSCsv65475—Noise measurements for some access points might vary greatly over small intervals. This variation occurs with no noise source present around the access point.

If You Need More Information

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, refer to the Cisco TAC website at

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.

Documentation Updates

This section lists updates to user documentation that has not yet been added to either printed or online documents.

Omissions

The Package Contents section in the *Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers* should be updated to include this item, which is included with the 4400 series controller:

- DB-9-to-DB-9 null modem cable

Related Documentation

For additional information on the Cisco controllers and lightweight access points, refer to these documents:

- The quick start guide for your particular controller or access point
- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless Control System Configuration Guide*

Click this link to browse to the Cisco Support and Documentation page:

http://www.cisco.com/cisco/web/support/index.html

Obtaining Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html