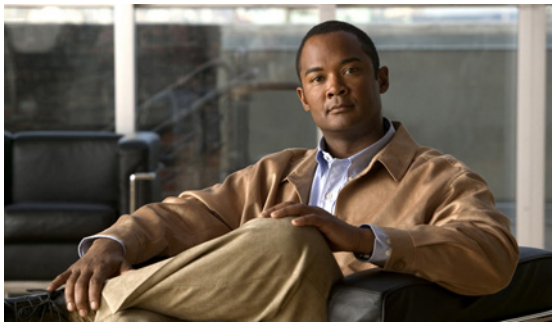

Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.2.205.0

May 13, 2009

These release notes describe open and resolved caveats for software release 4.2.205.0 for Cisco 2000, 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); and Cisco Aironet 1000, 1100, 1130, 1200, 1230AG, 1240, 1250, and 1300 Series Lightweight 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 4.2.205.0 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 4.2.128.0

Note Only Cisco WCS 4.2.128.0 supports controllers running software release 4.2.205.0.

- Cisco WCS Navigator 1.1.110.0
- Location appliance software release 3.1.43.0
- Cisco 2700 Series Location Appliances
- Cisco 2000 Series Wireless LAN Controllers
- 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
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1000, 1100, 1130, 1200, 1230AG, 1240, 1250, and 1300 Series Lightweight 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 series access point, and the 1140 series access point 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.

Special Notice for Mesh Networks

Note Do not upgrade to controller software release 4.2.205.0 if you have mesh access points in your network. If your network uses mesh access points, use only mesh-specific releases. These releases are labeled *MESH* in the Software Center.

Note Cisco WCS software release 4.2.128.0 may be used to manage both mesh and non-mesh controllers (such as controllers running software release 4.2.205.0 and 4.1.192.35M). You do not need different instances of WCS to manage mesh and non-mesh controllers.

Controller Requirements

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

- Windows XP SP1 or higher or Windows 2000 SP4 or higher
- Internet Explorer 6.0 SP1 or higher

Note Internet Explorer 6.0 SP1 or higher is the only browser supported for accessing the controller GUI and for using web authentication.

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 When you use the controller in the Catalyst 3750G Wireless LAN Controller Switch, the 3750 should not run Cisco IOS Releases 12.2(44)SE2 and 12.2(46)SE due to defect CSCsu02630.

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.

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.

Note When you downgrade from 4.2.205.0 to 4.2.178.0 or an earlier release, the LWAPP mode may or may not change from Layer 3 to Layer 2, depending on whether the configuration was saved in the earlier image. If the LWAPP mode changes, access points may not join the controller, and you must manually reset the controller to Layer 3 to resolve this issue.

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.

Special Rules for Upgrading to Controller Software Release 4.2.205.0

Caution Before upgrading your controller to software release 4.2.205.0, you must comply with the following rules.

- Make sure you have a TFTP server available for the software upgrade. Keep these guidelines in mind when setting up a TFTP server:
  - Controller software release 4.2.205.0 is larger 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 4.2.205.0 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 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 server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP server cannot run on the same computer as the WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.

- If your controller is running software release 4.0.206.0 (or a later 4.0 release), 4.1.171.0 (or a later 4.1 release), or 4.2.61.0, 4.2.99.0, 4.2.112.0, or 4.2.130.0, you can upgrade your controller directly to software release 4.2.205.0. If your controller is running a 3.2 release or a 4.0 release prior to 4.0.206.0, you must upgrade your controller to an intermediate release prior to upgrading to 4.2.205.0. Table 1 shows the upgrade path that you must follow before downloading software release 4.2.205.0.

Table 1 Upgrade Path to Controller Software Release 4.2.205.0

Current Software Release	Upgrade Path to 4.2.205.0 Software
3.2.78.0 or later 3.2 release	Upgrade to 4.0.206.0 (or a later 4.0 release) before upgrading to 4.2.205.0.
4.0.155.5	Upgrade to 4.0.206.0 (or a later 4.0 release) before upgrading to 4.2.205.0.
4.0.179.11	
4.0.206.0 or later 4.0 release	You can upgrade directly to 4.2.205.0.
4.1.171.0 or later 4.1 release	You can upgrade directly to 4.2.205.0.
4.2.61.0 or later 4.2 release	You can upgrade directly to 4.2.205.0.

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 4.2.205.0 software. In large networks, it can take some time to download the software on each access point.

- Cisco requires you to install the Cisco Unified Wireless Network Controller Boot Software 4.2.205.0 ER.aes file on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Wireless LAN Controller Switch. It is optional on other controller platforms. This file resolves CSCso00774 and is necessary to ensure proper operation of the controller. If you do not install the ER.aes file, your controller does not obtain the fix for this defect, and "Error" appears in the Bootloader Version field in the output of the **show sysinfo** command.

Note When you install the ER.aes file, a new bootloader file is also loaded. This is true for all controllers except the 2106 controller, for which the bootloader is not upgradable.

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 (4.2.205.0 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.

Note Do not install the 4.2.205.0 controller software file and the 4.2.205.0 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 4.2.205.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 4.2.205.0 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. to n. to download the remaining file (either the 4.2.205.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.2.205.0 ER.aes file).

Step 3 Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 4.2.205.0 ER.aes file to the default directory on your TFTP server.

Step 4 Click **Commands > Download File** to open the Download File to Controller page.

Step 5 From the File Type drop-down box, choose **Code**.

Step 6 In the IP Address field, enter the IP address of the TFTP server.

Step 7 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 8 In the File Path field, enter the directory path of the software.

Step 9 In the File Name field, enter the name of the software file (*filename*.aes).

Step 10 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Step 11 Repeat Step 4 to Step 10 to install the remaining file (either the 4.2.205.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.2.205.0 ER.aes file).

Step 12 After the download is complete, click **Reboot**.

Step 13 If prompted to save your changes, click **Save and Reboot**.

Step 14 Click **OK** to confirm your decision to reboot the controller.

Step 15 If desired, reload your latest configuration file to the controller.

Step 16 To verify that the 4.2.205.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 17 To verify that the Cisco Unified Wireless Network Controller Boot Software 4.2.205.0 ER.aes file is installed on your controller, enter the **show sysinfo** command on the controller CLI and look at the Bootloader Version field. “N/A” appears if the ER.aes file is installed successfully. “Error” appears if the ER.aes file is not installed.

Note You can use this command to verify the boot software version on all controllers except the 2106 because the bootloader is not upgradable on the 2106 controller.

New Features

The following new feature is available in this software release:

- Configurable Off-Channel Scanning to Improve Performance for Medical Devices—Using Radio Resource Management, lightweight access point radios can simultaneously scan all valid 802.11a/b/g channels for the country of operation as well as for channels available in other locations. The access point radios go “off-channel” for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points. In the presence of voice or video traffic in the last 100 ms, the access points defer off-channel measurements.

  Some devices, including some medical equipment, require a longer elapsed time without the appearance of a packet that defers off-channel scanning. Using two new CLI commands, you can configure, per WLAN, the minimum number of milliseconds that must elapse without the appearance of a specified packet before the access point radios begin an off-channel scan, and you can specify the priorities of packets that defer off-channel scans.

Note This feature affects the interaction of QoS and RRM. Refer to the "QoS Interaction with RRM in this Release" section on page 11 for additional information.

- Use this command to configure the priority of packets that defer an off-channel scan:

  config wlan channel-scan defer-priority [*packet priority value 0-7*] [**enable** | **disable**] [*WLAN ID*]

  For example, to configure defer priorities of 4 and 6 on WLAN 2, you enter these commands:

  ```
  config wlan channel-scan defer-priority 4 enable 2
  config wlan channel-scan defer-priority 6 enable 2
  ```

  The default setting for all new WLANs and upgrades from earlier software releases is priority 5 (video) and 6 (voice).

- Use this command to configure the minimum number of milliseconds that must elapse without the appearance of a specified packet before the access point radios begin an off-channel scan:

  config wlan channel-scan defer-time [*milliseconds 0-60,000*] [*WLAN ID*]

  For example, to configure a defer time of 500 ms on WLAN 2, you enter this command:

  ```
  config wlan channel-scan defer-time 500 2
  ```

  The default setting for all new WLANs and upgrades from earlier software releases is a defer-time of 100 ms.

- Use the **show wlan** command to check your configuration:

  show wlan [*WLAN ID*]

  This example shows how the channel scan entries might appear in the command output:

  ```
  . . .
  Scan Defer Priority.............................. 4,6
  Scan Defer Time.................................. 500 milliseconds
  . . .
  ```

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

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

One-Time Password (OTP) Support

One Time Passwords (OTP) are supported on the Wireless Lan Controller (WLC) using TACACS and RADIUS. In this configuration, the controller acts as a transparent pass-thru device. The controller forwards all client requests to the TACACS/RADIUS server without inspecting the client behavior. When using OTP the client must only establish a single connection to the controller to function properly. The controller currently does not have any intelligence or checks to correct a client that is trying to establish multiple connections.

QoS Interaction with RRM in this Release

This release affects the way that QoS interacts with the RRM Scan Defer feature:

- When you configure a WLAN with a Bronze (Background Priority) QoS policy level, traffic with Scan Defer Priority 0 (UP=0) should be downgraded to UP=1 (UP 1,2 are the lowest priority; 0,3 are the next higher priority). Traffic to and from clients on this WLAN will compete with clients sending UP=0 traffic in Silver/Gold/Platinum policies.
- The QoS policy for the WLAN configuration overrides the traffic sent. In other words, if you have patient monitors, phones, or other client devices in a WLAN with a Silver QoS policy, the traffic is downgraded to a priority no higher than UP=3. If you attempt to defer off-channel scanning by configuring the WLAN for UP=5, the QoS policy overrides that configuration and off-channel scanning is not deferred.
- Traffic sent with UP=7 on a WLAN with a Platinum policy will be downgraded to UP=6; if you configure off-channel scanning for UP=7 only, scanning will not be deferred. You might not want to defer scanning for UP=7 traffic but you might for UP=6 traffic; in this case, the traffic sent with UP=7 will be downgraded and cause a deferral. Similarly, if you want to defer scanning for UP=7 traffic, you must set the scanning priority to UP=6 because the traffic will be downgraded.

If you completely disable off-channel scanning on your network, you should consider alternative ways to implement off-channel scanning: adding monitor-mode access points or creating AP groups where some access points in the area do not carry the configured WLANs for those devices.

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.

Crash Files for 1250 Series Access Points

The 1250 series access points may contain a bootloader older than version 12.4(10b)JA. Units with old bootloaders 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. Units with bootloader versions 12.4(10b)JA or later generate a crash log if the access point is associated to a controller software release 4.2.112.0 or later.

New 1250 series access points shipped from the factory contain new bootloader images, 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.

These examples show the output from the CLI commands (in bold) that you use to check the bootloader version on LWAPP and autonomous 1250 series access points:

LWAPP (commands entered on the controller CLI):

```
(wlc) >debug ap enable AP001b.d513.1754
(wlc) >debug ap command "show version | include BOOTLDR" AP001b.d513.1754
(wlc) >Thu Apr 23 09:31:38 2009: AP001b.d513.1754: BOOTLDR: C1250 Boot Loader
(C1250-BOOT-M) Version 12.4(10b)JA, RELEASE SOFTWARE (fc1)
```

Autonomous (command entered on the access point CLI):

```
ap# show version | include BOOTLDR
BOOTLDR: C1250 Boot Loader (C1250-BOOT-M) Version 12.4(10b)JA, RELEASE SOFTWARE (fc1)
```

Port Mirroring Not Supported on Some Controller Platforms

The controller Port Mirroring feature is not supported on 2100 series controllers, 4400 series controllers, Cisco WiSM controllers, and Wireless LAN Controller Network Modules.

RLDP Limitations in This Release

Rogue Location Discovery Protocol (RLDP) is a controller feature that detects the presence of rogue access points that are connected to your wired network. In this software release, RLDP operates with these limitations:

- RLDP detects rogue access points that are configured for open authentication.
- RLDP detects rogue AP which use a broadcast BSSID--that is, the access point broadcasts its SSID in beacons.
- RLDP detects only rogue AP that are on the same the network. In other words, if an access list in the network prevents the sending of RLDP traffic from the rogue AP to the controller, RLDP will not work.
- RLDP does not work on 5-GHz DFS channels.
- RLDP is a best-effort protocol. For each rogue, the controller initiates RLDP only once. If the controller does not detect a rogue (due to a noisy RF environment, for example), the controller does not retry. However, you can initiate RLDP manually on a rogue at any time.

Configuration File Stored in XML Format

In controller software 4.2, the controller's bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in binary format. Therefore, you cannot download a binary configuration file onto a controller running software release 4.2. However, when you upgrade a controller from a previous software release to 4.2, the configuration file is migrated and converted to XML.

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.

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.

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.

Multicast Limitations

Multicast is not supported on access points that are connected directly to the local port of a 2000 or 2100 series controller.

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).

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 4.2* 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).

Note Daylight Savings Time (DST) is not supported in controller software release 4.2.

UNII-2 Channels Disabled on New 1000 Series Access Points for United States, Canada, and Philippines

New Cisco 1000 series lightweight access points for the United States, Canada, and the Philippines do not support the UNII-2 band (5.25 to 5.35 GHz). These models are labeled AP10x0-B, where "B" represents a new regulatory domain that replaces the previous "A" domain.

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.
```

1000 Series Access Points and Radar Detection

The 1000 series access points perform radar detection on channels that do not require it (such as channel 36). If the access points detect radar on these channels, the controller captures it in log messages.

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:

- Switch between Layer 2 and Layer 3 LWAPP mode

- 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**}

Multicast Queue Depth

The multicast queue depth is 512 packets on all controller platforms. However, the following message might appear on 2006 and 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 2006 and 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.

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.

Resetting the Configuration on 2006 Controllers

If you wish to reset the configuration to factory defaults on a 2006 controller, perform one of the following:

- From the controller GUI, click **Commands > Reset to Factory Default > Reset**.
- From the controller CLI (after system bootup and login), enter **clear config**. Then after the configuration has been cleared, enter **reset system** without saving the current configuration.
- From the controller console (after system bootup), enter **Recover-Config** from the User Name prompt.

Caution Do not attempt to reset the controller's configuration by choosing Option 5, Clear Config, from the boot menu.

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 4.2.205.0 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 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.

Cisco 1000 Series Access Points and WMM

Cisco 1000 series access points in REAP mode do not support the Wi-Fi Multi-Media (WMM) protocol.

Cisco Aironet 1030 Remote Edge Lightweight Access Points and WPA2-PSK

Cisco Aironet 1030 Remote Edge Lightweight Access Points do not support WPA2-PSK in REAP standalone mode.

Lightweight Access Point Connection Limitations

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.

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 4.2* 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 4.2* 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 2000 and 2100 Series Controllers

These hardware features are not supported on 2000 and 2100 series controllers:

- Power over Ethernet (PoE) for 2000 series controllers only

Note Ports 7 and 8 on 2100 series controllers are PoE ports.

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

These software features are not supported on 2000 and 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
- Layer 2 LWAPP
- Spanning tree
- Port mirroring

Note Port mirroring is also not supported on 4400 series controllers.

- Cranite
- Fortress
- 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.

2006 Image Not Supported for 3504 Controllers

The 2006 controller image is supported for use with only 2000 series controllers. Do not install the 2006 image on a 3504 controller. Otherwise, errors may occur. Install only the 3504 image on a 3504 controller.

Running a 3504 Image on a 2000 Series Controller

It is possible to run a 3504 controller image on a 2000 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> </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    <input type="TEXT" name="username"
SIZE="25" MAXLENGTH="63" VALUE=""> </td> </tr> <tr align="center" > <td colspan="2">
Password      <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>
```

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 4.2.205.0.

- CSCsb57163—Controllers sometimes fail to boot using the backup image.

  Workaround: None.

- CSCsb77595—When logging out from Telnet/SSH sessions, the session always prompts the user to save changes, even when no changes have been made.

  Workaround: Ignore the prompt and exit as usual.

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

  Workaround: None.

- CSCsd77121—Only one CLI session is permitted from the router to the controller network module in a Cisco 28/37/38xx Series Integrated Services Router, even if multiple sessions are configured.

  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: None.

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

  Workaround: None.

- CSCse43488—The controller might not show the correct maximum output power configuration of a 1000 series access point 5-GHz radio in the -P domain.

  Workaround: None.

- CSCse75417—A 1000 series access point might report an 802.11b client transmitting at 12 Mbps.

  Workaround: None.

- CSCse87087—A controller with link aggregation (LAG) enabled fails Ethernet link redundancy. This problem occurs when the controller uses an Ethernet copper gigabit interface converter (GBIC) instead of a fiber GBIC and one of two Ethernet cables is pulled out of the GBIC.

  Workaround: Clear the configuration on the controller. Then reconfigure the controller and perform the redundancy test.

- CSCsg04831—There are not enough debugs to determine the packet flow in the controller for guest access.

  Workaround: Use a wireless sniffer trace.

- CSCsg32646—If link aggregation (LAG) is enabled on the controller and the port channel is configured on the infrastructure switch, the controller displays only a single entry for its neighbor when you enter the sh cdp neighbor CLI command. When you enter the same command on the switch, it displays two entries for the controller for two different ports that are part of LAG. The controller should display two entries when the command is entered on the controller because the switch sends the CDP message from two different ports that are part of the port channel.

  Workaround: None.

- CSCsg39910—The 1000 series access points should support direct Telnet to the controller CLI.

  Workaround: None.

- CSCsg39928—The 1000 series access points should support direct Secure Shell (SSH) to the controller CLI.

  Workaround: None.

- CSCsg45938—Devshell commands do not work on SSH or Telnet sessions.

  Workaround: Enter the devshell commands in a console session.

- CSCsg48089—If you lose your controller password and have not backed up the configuration, the recovery mechanism is to revert to the factory default settings.

  Workaround: None.

- CSCsg66040—After a software upgrade, controllers might experience intermittent access to the management interface through HTTPS.

  Workaround: Follow these steps to workaround the issue:

  a. Make sure HTTPS is enabled on the controller's management interface, reboot the controller from the CLI, and monitor the last service if error messages appear after the controller prompts you to enter a username and password to login.

  b. Login with the relevant credentials and reconfigure the virtual interface with this CLI command:

     config interface address virtual 1.1.1.1

  c. Reboot the controller and make sure the Secure Web service shows up as OK.

  d. Generate a certificate using this CLI command:

     config certificate generate webauth

  e. Click **Yes** when prompted and wait a few minutes for the certificate to generate.

  f. Reboot the controller.

- CSCsg68046—The complete reason for a TFTP download failure needs to appear on the controller GUI. If the controller cannot find the software file on the TFTP server during a software upgrade, it reports that the transfer failed rather than that the file is not present.

  Workaround: Make sure that the file and filename are entirely correct before upgrading, or upgrade using the CLI to receive a more accurate reason for the failure. Further details are available if you use the **debug transfer all enable** command prior to upgrade.

- CSCsg74578—If you change a controller's management IP address, it is not sent to the access point unless the access point is reset. As a result, multicasting does not work until the change is made on the access point.

  Workaround: Reset the access point so that it rejoins the controller and the controller updates the access point with the new configuration.

- CSCsg84209—The export foreign controller is not deleting the client device when it receives a HandoffEnd message.

  Workaround: None.

- CSCsg87111—While editing a WLAN configured for WPA1+WPA2 with a conditional web 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 Layer2 to 802.1X and save your change.
  c. Change Layer3 to conditional web redirect and save your change.

- 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."

  Workaround: Configure a larger value for the controller database, such as 2048.

- 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**.

- CSCsh15411—When an access point drops the IAPP packet from a CCX client just after association, the CCX Layer 2 roam history may not be available for CCX clients on the controller.

  Workaround: None.

- CSCsh31104—The word *channel* is misspelled in the message log.

  Workaround: None.

- CSCsh93279—The 1000 series access points do not consistently forward probe requests to the controller.

  Workaround: None.

- CSCsi13399—The Expiration Timeout for Rogue AP Entries parameter on the Rogue Policies page applies to both rogue access point entries and rogue client entries. The parameter name should be changed to reflect both types of entries.

  Workaround: None. This is a cosmetic issue.

- 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—You might lose connectivity when adding or recovering a second link aggregation (LAG) link.

  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.

- CSCsi54588—Some 802.1X error messages have inadequate descriptions or incorrect severity levels. For example, the following messages, which can be caused by an incorrectly configured client, have a severity level of 1 when they should have a severity level of 3. As a result, they are logged even when the logging level is set to Critical.

  –DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE

  –DOT1X-1-ABORT_AUTH

  Workaround: Make sure that clients are correctly configured to minimize error logging.

- 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.

- CSCsi72767—A script runs each time you generate a dependency file, which makes the build very slow.

  Workaround: None.

- 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.

- CSCsj14255—Sometimes the multicast stream to wireless clients stops, and the upstream router does not receive IGMP reports. This problem occurs when there are multiple IGMP requests on the same VLAN and the controller responds only to the last query or when simultaneous IGMP queries are sent from more than five VLANs and the controller responds to only the first five.

  Workaround: None.

- 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.

- CSCsj44861—An access point might transmit neighbor messages when it is not connected to a controller.

  Workaround: None.

- 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.

- CSCsj59237—The traffic stream metric (TSM) packet count is not reported correctly.

  Workaround: None.

- CSCsj59441—Channel information for a rogue access point does not appear on the rogue access point report.

  Workaround: Enable the rogue access point trap for the registered controllers or view the channel information on the controller.

- CSCsj61649—Whenever a log analysis report is generated on a CCXv5 client using WCS, the DHCP and AAA logs are swapped.

  Workaround: Use the controller CLI to view this information.

- CSCsj67447—When you use the controller GUI to modify an existing (or newly created) guest LAN and you choose an ingress interface that is already in use, no error appears. The error that appears on the CLI should also appear on the GUI: “Ingress interface is in use by some other guest lan.”

  Workaround: None.

- CSCsj85329—The controller GUI should explain how the password changes with RADIUS compatibility mode. The RADIUS server names help users match to their type of RADIUS server, but the server types should be explained:

  – Cisco ACS—In the RADIUS access-request packet, the username is the client MAC address, and the password is the client MAC address.

  - Free RADIUS—In the RADIUS access-request packet, the username is the client MAC address, and the password is the controller's shared secret with the RADIUS server.
  - Other—In the RADIUS access-request packet, the username is the client MAC address, and the password is not sent in the RADIUS access-request packet.

  Workaround: None.

- CSCsj87925—The controller GUI netmask for an ACL accepts arbitrary values.

  Workaround: Enter a valid netmask.

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

  Workaround: None.

- CSCsj88990—Rogue access point client information shown for the access point does not match the client information from the Rogue Client Details link.

  Workaround: View the current rogue client information from the controller.

- CSCsj96589—Using the MAC address from the label on an 1131 or 1242 access point in the **debug mac addr** command produces limited debug output.

  Workaround: None.

- CSCsj97900—The call admission control (CAC) TSPEC is not traffic shaping and allows a new call setup when the physical data rate is higher than one single data rate configured on the controller.

  Workaround: Follow the instructions in the VoWLAN deployment guide to enable a realistic higher data rate for the Cisco 7921 phone and turn on the supported rate as recommended.

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

  Workaround: None.

- CSCsk08401—The formatting for the **config paging** *?* CLI command needs to be corrected.

  Workaround: None.

- CSCsk08707—The 1250 series access points receive console error messages indicating that the primary discover decode failed.

  Workaround: None.

- CSCsk12420—Sometimes a 1000 series access point does not accept the DHCP offer from a Catalyst 3750 switch.

  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.

- CSCsk22861—An MGID entry is not cleared from the access point when IGMP snooping is disabled.

  Workaround: None.

- CSCsk49157—When you change the session timeout of a WLAN that is using a backend RADIUS authentication server, any existing client that is using that WLAN shows its reauthentication timeout as infinite, even though there is a finite time after which reauthentication occurs.

  Workaround: None.

- CSCsk49200—The hybrid-REAP local switching option should be removed for wired guest LANs.

Workaround: None.

- CSCsk49282—The guest LAN and WLAN are not clearly differentiated.

  Workaround: None.

- CSCsk50477—The BCAST_Q_ADD_FAILED message contains typographical errors.

  Workaround: None.

- 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 Cisco1240 series access points in WGB mode.

  Workaround: None.

- CSCsk68117—U-APSD state changes on a client device are not updated on the controller.

  Workaround: Reboot the access point, or disassociate the client from the controller and then reassociate it.

- CSCsk74050— If you configure an ACL name with 32 characters, the ACL override fails during roaming.

  Workaround: Use ACL names with up to 31 characters.

- CSCsk78264—A change in the RF domain name takes effect only after a reboot.

  Workaround: Reboot the controller after changing the RF domain name.

- CSCsk79382—CCXv4 and CCXv5 clients receive an Adjacent Access Point Report from the controller even though this report should be sent only to CCXv2 and CCXv3 clients.

  Workaround: None.

- CSCsk83426—A hybrid-REAP access point does not reauthenticate after entering standalone mode.

  Workaround: None.

- CSCsk85091—If Rogue Location Detection Protocol (RLDP) is enabled on the controller, you may see radio reset messages on the access point console. There may also be a brief interruption in client traffic flow.

  Workaround: Disable RLDP.

- CSCsk86536—The wrong error message appears when you change country channels with the 802.11a radio enabled.

  Workaround: None.

- CSCsl01005—Sometimes bandwidth contracts do not take effect. If a user who has bandwidth restrictions logs in and logs out and then another user who does not have bandwidth restrictions logs in, the bandwidth restrictions are not removed immediately.

  Workaround: Reassociate the user between logout of the old user and login of the new user.

- 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.

- 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.

  Workaround: On the access point console, right after you see the "Press Return to get started" message, enter enable mode (the default password is *Cisco*), and enter this debug command:

  debug ip udp

  The output shows all UDP packets sent and received by the access point.

- CSCsl16445—When an access point radio status is down due to lack of CDP response from a neighboring switch, the controller reports Cause=Unknown. However, it should report Cause=Waiting for CDP response.

  Workaround: None; this issue is cosmetic.

- CSCsl24600—The 1000 series access points might experience multiple "Watch Exception" errors.

  Workaround: None.

- CSCsl40018—The hybrid-REAP design and deployment guide incorrectly implies that you can configure NAT on both the hybrid-REAP and controller sides of the network link. In reality, NAT is supported only on the access point side of the network link. The hybrid-REAP design and deployment guide is available at this URL:

  http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080736123.shtml

  Workaround: None.

- CSCsl41764—An access point should send a neighbor list to its clients as soon as it accepts the association.

  Workaround: None.

- 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.

- CSCsl48639—An IP address can be configured on a dynamic interface on a controller when that IP address has already been assigned to another device on the network.

  Workaround: Check the ARP table on the switch to see if the IP address is bound to a MAC address on the network that is not the controller MAC address.

- CSCsl48776—Controllers sometimes incorrectly forward SSC authentication requests to a RADIUS server.

  Workaround: None.

- 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.

Workaround: If you need to enter more than 130 characters on the internal web authentication page, use the controller interface instead of WCS.

- 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.

- CSCsl79765—When connected to a controller, 1230 series access points containing AIR-MP31G radios sometimes disable the radios and report that no channel is available.

  Workaround: Contact Cisco TAC for more information. A Cisco internal-only procedure can be used to update missing environment variables and burn them into a cookie.

- 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.

- 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.

- 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.

  Workaround: Install the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 ER.aes file, which contains a new bootloader. A successful transfer and upgrade of the ER file indicates that the ER file has been updated properly.

- 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.

  Workaround: None.

- 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: Perform the following 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.

- 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.

- CSCsm40903—Additional information is needed for the following message: "claspam_lrad.c:1626 LWAPP-6-PORTMAP_ERR: Failed to obtain multicast port map for interface 4, using default index (50)."

  Workaround: None.

- CSCsm40906—The following message appears on the 2106 controller when multicast is disabled: "claspam_lrad.c:1626 LWAPP-6-PORTMAP_ERR: Failed to obtain multicast port map for interface 4, using default index (50)." No multicast messages should appear when multicast is disabled.

  Workaround: None.

- CSCsm65043—1240 series access points might stop accepting new clients. In this case, the **show controller d1** command shows the following:

  ```
  Beacon Flags: 0; Beacons are disabled; Probes are disabled
  ```

  Workaround: Reboot the access point.

- 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.

- 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 Layer2 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.

- CSCsm84952—When you configure wired and wireless guest WLANs on two controllers, a wired guest user obtains an IP address but does not always receive the web authentication page or cannot login properly. Additionally, a reattempt by the wired client might result in obtaining an IP address from the other controller, causing the client to appear to have been handed an IP address from each controller.

  Workaround: Disable the wired guest WLAN on one of the controllers and enable it as needed. Using an external DHCP server might resolve this issue as well.

- CSCsm88913—Removing a mobile client on Anchor WLC GUI causes ARP look-up failure if the client associates with a dynamic interface.

  Workaround: None.

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

  Workaround: None.

- CSCsm94702—When the controller is configured through the service port, the VLAN ID and port information do not appear in the output of the **show int summary** CLI command.

  Workaround: None.

- 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.

  Workaround: None.

- CSCsm98659—The clcCdpGlobalEnable SNMP variable cannot be set on the controller unless there is at least one access point present on the controller. This creates problems when trying to add a new controller to WCS. When you create a new controller template on WCS and set the Global CDP on APs value to false, the template cannot be pushed out to any controller that does not have an access point associated to it.

  Workaround: Add an access point to the controller. Then you can add the controller to WCS or change the CDP parameter.

- CSCso02340—The controller might report a different power level than is actually used by the access point if you change the channel from one supporting one transmit power to another supporting a different transmit power.

  Workaround: Reapply the power configuration.

- 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—On rare occasions, a 4400 series controller might hang when you upgrade the software to a later release.

  Workaround: Reboot the controller or wait some time to clear this condition.

- CSCso28323—Clients might fail to associate to an 1130 series access point configured for WPA1 AES-CCMP and optional MFP.

  Workaround: None.

- CSCso31067—Some clients might experience failures during upstream-only prioritized traffic on 802.11a, despite radio resource management (RRM) features being disabled.

  Workaround: None.

- CSCso31640—When you downgrade a 2100 series controller from software release 5.1 to software release 4.2.112.0, 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.

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

  Workaround: Return the access point to local mode in order to modify the channel width settings. Then return it to sniffer mode. This process requires a minimum of two reboots of the access point.

- 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.

- CSCso79135—After an initial reboot of the Cisco WiSM or after the online insertion and removal (OIR) of the Cisco WiSM line card, the output of the **show wism status** CLI command on the Catalyst 6500 series switch shows that the service port is down, even if it is pingable. Wireless functionality is not impacted.

  Workaround: Follow these steps:

  a. Enter this CLI command on the Cisco WiSM to remove the service VLAN: **no wism service-vlan** *vlan_id*.

  b. Enter this command to OIR the Cisco WiSM: **hw-module module** *slot* **reset**.

  c. Enter this CLI command to add the service VLAN again: **wism service-vlan** *vlan_id*.

- CScsq06451—If you configure a guest LAN and map the ingress interface to a guest LAN interface, you cannot change the mapping to None using the controller GUI.

  Workaround: Use this CLI command to change the mapping to None: **config guest-lan ingress-interface 1 none**.

- 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.

- CSCsq14310—If the Allow AAA Override option is enabled for a WLAN, the guest role might not be applied for the local net user.

  Workaround: Disable the Allow AAA Override option.

- CSCsq14326—A 4400 series controller using a Cisco ACS as a TACACS+ server does not log these CLI commands into the ACS:

  - **config hreap group name add**
  - **config hreap group name ap add 00:1c:58:34:40:cc**
  - **config hreap group name ap add 00:1a:a1:3f:07:08**
  - **config hreap group name delete**

  Workaround: None.

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

  Workaround: Change the IP address of the management interface.

- CSCsq19324—If you enter a long value for the access control list (ACL) name on the Access Control Lists page of the controller GUI and click **Apply**, the value appears in HTML text below the ACL Name field.

  Workaround: None.

- CSCsq19472—Cisco Compatible Extensions RM measurements are inaccurate if beacon, channel load, frame, and noise histograms are triggered together.

  Workaround: Trigger the RM measurements one at a time.

- CSCsq21956—An error occurs when you create a guest user and then try to edit the guest user's parameters such as lifetime, role, and so on through the controller GUI.

  Workaround: Use the controller CLI to edit the guest user's parameters.

- CSCsq23594—When a CCXv5 request is manually sent to a CCXv5 client, an emergency log message is written to the log and sent to any configured syslog servers.

  Workaround: None.

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

  Workaround: Stop the Nessus scan and reboot the controller.

- 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: Remove the console connection cable from the Cisco terminal server.

- CSCsq26491—The **show ap uptime** CLI command might contain some bogus values.

  Workaround: None.

- CSCsq29243—When you configure the 802.11h channel switch mode, you should be able to enter only 0 or 1, but you can enter any value.

Workaround: None.

- CSCsq30821—When a WLAN is configured on two controllers using web authentication and the WLAN is on a different VLAN on each controller, web authentication can be bypassed if a client roams from one controller to another controller and then back to the first controller.

  Workaround: Make sure that any WLAN spanning two controllers using web authentication is on the same VLAN on both controllers.

- CSCsq31622— An SNMP error occurs when you enable voice and video parameters on the controller using WCS.

  Workaround: Disable all WMM-enabled WLANs and enable voice and video parameters.

- CSCsq32038—The **config interface** CLI command allows up to 31 characters to be entered for the interface name. It should allow up to 32 characters.

  Workaround: None.

- CSCsq34262—A traceback might occur if you include three controllers in the same mobility group and enable a dynamic interface on all of them.

  Workaround: Reset the controller.

- CSCsq35402—After you upgrade the controller to software release 4.2.125.0, the following error message appears on the console of the Cisco WiSM controllers: "Mon May 19 12:56:44 2008: dtlARPProtoRecv: Invalid ARP packet!"

  Workaround: None.

- CSCsq35574—The Authorityid and the server key do not accept a value of 17 or greater.

  Workaround: None.

- CSCsq35590—If you change a 1240 series access point's country of operation from Spain to the U.S., tracebacks might occur while the access point joins the controller.

  Workaround: None; you can safely ignore the tracebacks.

- CSCsq37810—If you add a controller to WCS and later reboot the controller, WCS does not receive the trap for a cold start, which prevents it from pushing the configuration back to the controller.

  Workaround: Manually push the configuration from WCS.

- CSCsq38075—If you change a 1240 series access point's country of operation to Spain, tracebacks might appear on the access point console.

  Workaround: None; you can safely ignore the tracebacks.

- CSCsq38700—If you change the power level on an access point radio while clients are associated to the access point, the controller might display DOWN for the operational status of that radio. However, clients continue to pass traffic and function properly.

  Workaround: None.

- CSCsq47493—The cLReapApVlanId is not being updated on the controller, and the API is not throwing any exception to indicate that it has not been set.

  Workaround: First change the native VLAN ID. Then change the cLReapApVlanId.

- 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.

- CSCsq74144—The controller does not show the channel on which an access point in sniffer mode is 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.

- CSCsq83787—The port mirroring feature is not implemented on 4400 series controllers and should be removed. This is a legacy feature on 4000 series controllers and is no longer supported.

  Workaround: None.

- CSCsq83810—STP commands should be removed from the controller GUI and CLI. They are no longer supported and might cause undesired effects when interacting with PSVT.

  Workaround: None.

- CSCsr02316—Some SNMPSet operations show a successful status even though the controller is truncating the string.

  Workaround: Set a shorter value for the string.

- CSCsr44439—The web authentication page does not load on the browser when the client connects through a wired guest VLAN on a controller running software release 4.2.130.0.

  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.

- CSCsr53764—When workgroup bridges (WGBs) are installed on a train and clients joined to the WGBs are running some type of application, the WGBs roam very quickly between access points, and some wired clients might become stuck at a specific access point.

  Workaround: Reset the WGBs, enter the **clear bridge** command on the WGBs, or wait for the WGBs to roam back to the access point where the client is stuck.

- CSCsr58532—The following error message might appear on 2106 controllers: "sim_config.c:194 SIM-3-INTFGET_GIG_ETH_FAIL: Failed to get the interface number of the Gigabit Ethernet Port."

  Workaround: None.

- CSCsr63100—The controller's message log sometimes fills with "sysapi.c:160 SYSTEM-3-SYSAPI_ERR" messages after dump-low-level debugs are run.

  Workaround: None.

- CSCsr72091—The radio resource management (RRM) feature in controller software release 4.2.130.0 is not providing consistent results from coverage hole events and channel assignments.

  Workaround: None.

- CSCsr89694—On Cisco WiSM controllers running software release 4.2.130.0, trap logs are generated 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: None.

- CSCsu03464—The input radio statistics are incorrect on a 1250 series access point running software release 4.2.173.0.

  Workaround: None.

- CSCsu04143—The radio resource management (RRM) process on the controller can start allocating all available timers, until the controller is unable to register new timers for other processes.

  Workaround: Reset the controller.

- CSCsu07730—When you try to configure a network address for the AP-manager on a 4400 series controller, an "Invalid IP" error message sometimes appears.

  Workaround: None.

- CSCsu09424—A 2100 series controller might reboot when you attempt to upgrade the software from a 4.2 release to a 5.2 release.

  Workaround: None.

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

  Workaround: None.

- CSCsu31680—The AIRESPACE-SWITCHING-MIB contains a missing entry for 1.3.6.1.4.1.14179.1.1.4.5.

  Workaround: None.

- CSCsu40636—The access point sometimes violates the CTS duration when receiving a U-APSD trigger frame. Instead of waiting for a few milliseconds to protect an upcoming link exchange, it simply transmits the trigger frame.

  Workaround: Configure the client to carry through medium reservation time in subsequent frames.

- CSCsu40720—The following message might appear on the controller console without further explanation:

  ```
  Thu Sep  4 20:58:24 2008: mmMfpRequestedState: *** FIXME: Need to update BSSID state
  distributed to APs for 00:1E:4A:E0:00:A0 radio 1
  ```

  Workaround: None.

- CSCsu44722—The following invalid error message appears when you enable IPv6 for a mobility-anchor-enabled WLAN: "Cannot enable IPv6-bridging when DHCP Address Assignment is enabled for WLAN." You can safely ignore these messages.

- CSCsu47888—The crash file or controller console should show whether a core dump was generated following a crash and successfully uploaded to a TFTP server.

  Workaround: None.

- CSCsu50080—When you enable web authentication pass-through with email input selected, the controller allows any text to be entered rather than verifying that the email address has been entered in a valid address format.

  Workaround: None.

- CSCsu52837—Preauthenticated clients cannot reach web-authenticated clients on the same WLAN.

Workaround: None.

- CSCsu72717—The name is corrupted in the interrupt session of the Cisco WiSM controller's crash file.

  Workaround: None.

- CSCsu76295—If you try to manage a controller without web authentication by configuring the pre-authentication ACL to allow traffic in both directions, you cannot reach the management interface. You can access the management interface only after web authentication.

  Workaround: None.

- CSCsu80604—The memory monitor configuration returns to default values after the controller reboots.

  Workaround: None.

- CSCsu84498—The transmit diversity for multicast-broadcast packets is not alternating on the 1240 series access point's antenna ports.

  Workaround: None.

- CSCsu84629—The 1250 series access points change from maximum uniform transmit power back to maximum transmit power on neighbor discovery packets.

  Workaround: None.

- CSCsu86627—The controller currently issues commands to transmit single neighbor discovery packets. However, the controller should issue bursts of neighbor discovery packets to access point radios in order to force radio transmit power control loops to settle at new power settings.

  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.

- CSCsu98641—The core-dump configuration does not show in the running configuration on the Cisco WiSM.

Workaround: None.

- 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.

- CSCsv76513—On a 2100 series controller, the WLANs for the 802.11a and 802.11b/g access point radios might show the same BSSID while the same access point on a 4400 series controller shows the correct BSSIDs.

  Workaround: None.

- CSCsv79885—If you initially enter an incorrect mobility group name, the Edit All feature does not save the new mobility group name.

  Workaround: Delete the mobility member and re-enter it with the correct name.

- CSCsw25810—When you use the GUI to configure a RADIUS server for a wired guest LAN on a controller running software release 4.2.176.0, a browser error might occur.

  Workaround: Use the controller CLI to configure the RADIUS server.

- CSCsw45913—The wrong access control list (ACL) might be applied when the AAA override option is enabled.

  Workaround: Disable the AAA override option.

- CSCsw53035—When a controller running software release 4.2.176.0 (with hybrid-REAP local switching and hybrid-REAP VLAN mode enabled) sends a ping reply to a wireless client, the destination MAC address is the client MAC address. As a result, the Layer 3 switch cannot transfer the ping reply packet.

  Workaround: None.

- CSCsw93671—Packets sourced from the service port are sent from the controller even when the service port is not connected to the network.

  Workaround: None.

- CSCsx05502—A guest-access anchor controller stops forwarding traffic to the wired clients.

  Workaround: Reset the PC card on the client.

- CSCsx07443—WCS traffic stream metrics reports sometimes show the packet loss ratio (PLR) at 100000%. It should be less than or equal to 100%.

  Workaround: None.

- CSCsx41062—Controllers sometimes reject valid NTP packets and label them spurious.

  Workaround: Use a Cisco router as your NTP server.

- CSCsx50408—LWAP DOS Attack trap messages sometimes fail to record the source MAC address.

  Workaround: None.

- CSCsx51635—On controllers, DHCP proxy is enabled by default, but it should be disabled by default.

  Workaround: Use the **config dhcp proxy disabled** command to disbale DHCP proxy on the controller.

- CSCsx53685—Output of the show run-config p config CLI command always displays default values for Power Type/Mode.

  Workaround: None.

- CSCsx60265—802.11b clients might experience poor performance with 1130 and 1240 series access points.

  Workaround: None.

- CSCsx64115—If you clear the configuration for a 4400 series controller and then reset the controller without saving the configuration, the following error log appears on the controller console: "dtlArpRequest: Cannot send an ARP reply to 00:0B:85:32:58:C0."

  Workaround: None.

- CSCsx67133—The 4.2 controller software includes some mesh configuration options in the GUI and CLI even though the 4.2 software does not support mesh access points.

  Workaround: Ignore the mesh options in 4.2.x software releases, or upgrade the controller software if you require mesh support.

- CSCsx70686—When you enable RLDP on the controller, the radio interfaces on 1250 series access points are sometimes disabled, and the radios stop sending beacons and probes.

  Workaround: Disable RLDP and reset the access point.

- CSCsx73649—1140 series access points join the controller, drop off, and then join again repeatedly, and appear on the controller GUI.

  Workaround: None.

- CSCsx75375—Controllers sometimes fail to display an error message when you save a configuration without entering a name for the configuration.

  Workaround: None.

- CSCsx75442—2106 controllers sometimes display this message during software upgrade:

  ```
  Routine system resource notification.
  ```

  You can safely ignore these messages.

- CSCsx75726—When DHCP proxy is enabled, controllers sometimes change the value in the siaddr field in the DHCP offer that is forwarded from the external DHCP server to the wireless client. Controllers change the value from the IP address of the external DHCP server to the virtual IP address of the controller. This change causes a delay when clients disassociate and then reassociate.

  Workaround: Use the **config dhcp proxy disabled** command to disbale DHCP proxy on the controller.

- CSCsx75745—When you enter show route ummary on the controller CLI, the controller displays Genmask instead of subnetmask.

  Workaround: On the controller GUI, click Controller > Network Routes to see the network route with subnetmask.

- CSCsx75872—When a client device connected to a workgroup bridge deauthenticates and then reauthenticates, it fails to receive an IP address through DHCP.

  Workaround: Force the workgroup bridge to reauthenticate to the wireless LAN; the client devices connected to the workgroup bridge then successfully receive IP addresses.

- CSCsx96204—Controllers fail to mark disabled client devices as excluded.

  Workaround: None.

- CSCsy03762—Local-Eap authentication fails the controller's issuer check when the controller and client certificates are from the same SubCA.

  Workaround: Disable these three controller settings:

  - Check against CA certificates
  - Verify certificate CN identity
  - Check certificate date validity
- CSCsy15449—When you enable Validate Rogue Clients against AAA and you configure multiple RADIUS servers on the controller, the controller uses the second RADIUS server to validate the rogues.

  Workaround: None.
- CSCsy15897—Off-channel scanning sometimes fails on 1232 series access points.

  Workaround: None.
- CSCsy19477—When a guest user is logged in and logged out using web auth, inccorrect messages appear on the controller console.

  Workaround: None.
- CSCsy30696—Wism controllers sometimes fail to receive an initial Service IP address through DHCP.

  Workaround: Toggle the **wism service-vlan** [*vlan_id*] command.
- CSCsy31678—When you use the controller CLI to enter a fingerprint SHA value for the CIDS sensor, the fingerprint value does not appear on the controller GUI.

  Workaround: None.
- CSCsy31942—4404 controllers add the incorrect 802.1p tag on uplink traffic sent with a bronze QoS profile.

  Workaround: None.
- CSCsy32145—You can only configure HTTP/HTTPS globally on the controller.

  Workaround: None.
- CSCsy37499—Controllers sometimes reboot unexpectedly at software task 0x10bb4ccc.

  Workaround: None.
- CSCsy50470—The **show wlan summary** command is case-sensitive, but it should not be.

  Workaround: Enter **show wlan summary** in lower-case letters on the CLI.
- CSCsy62007—Controllers sometimes drop the DHCP inform packet when a client device is in DHCP required state.

  Workaround: Use the **config dhcp proxy disabled** command to disbale DHCP proxy on the controller.
- CSCsy71541—Controllers sometimes fail to clear TSPEC statistics when phones are associated to 1010 series access points.

  Workaround: None.
- CSCsy79782—Controllers sometimes reset the uptime counter to zero when the uptime count reaches 497 days. When the counter resets to zero, client devices are disconnected.

  Workaround: Reset the controller.
- CSCsy82585—2106 controllers fail to detect that a rogue access point is connected to the wired infrastructure.

  Workaround: None.
- CSCsy83568—DHCP debug output does not contain mobility state information.

Workaround: None.

- CSCsy87329—When you enable WPA1 on the controller GUI, WPA2 is also sometimes enabled.

  Workaround: None.

- CSCsy92080—External Webauth pages sometimes do not appear if the URL for the external page contains more than 64 characters.

  Workaround: Use the controller CLI to configure Webauth and verify the configuration.

- CSCsy94826—The controller GUI limits your ability to change channel width on 1250 series access points. You must put Channel and Transmit Power into Custom mode, and the GUI allows you to change the channel width setting only to 40 MHz.

  Workaround: None.

- CSCsy94911—When you try to delete a guest WLAN, the controller sometimes displays this message: "Anchors configured on WLAN - unable to delete WLAN entry," even when no anchors are configured.

  Workaround: Add an anchor to the guest WLAN and then delete the anchor; you can then delete the WLAN.

- CSCsy96551—When a PC tries to renew an IP address it had before (for example from home network), the controller's internal DHCP server does not send an NAK frame. Instead the controller sends a DHCP ignore message and does not assign an IP address to the machine.

  Workaround: Manually release and renew the IP address on the PC.

- CSCsy99807—RLDP sometimes fails to detect that Linksys 802.11n access points are wired to the infrastructure.

  Workaround: None.

- CSCsy99905—RLDP consistently finds wired threats only when you use it manually.

  Workaround: None.

- CSCsz03162—When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully associate to an access point but cannot pass traffic.

  Workaround: When you configure the controller for 802.11g traffic only, disable any channels (such as channel 14 in Japan) that allow associations from 802.11b client devices.

- CSCsz09498—When client devices trigger the auto-immune code on a controller, it can be difficult to determine how exactly the client device violated the auto-immune rules.

  Workaround: None.

Resolved Caveats

These caveats are resolved in controller software release 4.2.205.0.

- CSCsg00102—In Cisco IOS Release 12.4(9)T, the TCP no longer stops accepting new connections after a few days of SSLVPN running in the router.
- CSCsi51966—The ACL now appears in client details and in debug output.
- CSCsj25953—When 200 or more wireless clients try to associate to a controller at the same time, the clients no longer become stuck in the DHCP_REQD state when you use the **config advanced assoc-limit** command to limit association requests from access points.

  Use this CLI command to limit the rate at which access point radios send association and authentication requests to the controller:

config advanced assoc-limit [**enable** | **disable**] [*number of associations per interval*] [*interval in milliseconds*]

The valid range for number of associations per interval is 1 to 100; the valid range for interval in milliseconds is 100 to 10000. This command is disabled by default.

- CSCsl57356—When an 802.11n client is associated to a 1250 series access point, the client now shows up correctly as 802.11n on the controller GUI and CLI.
- CSCsl79260—Wired guest LAN clients now receive an IP address when DHCP proxy is disabled.
- CSCsm04951—Entries in the controller's local database are now listed by type.
- CSCsm05607— Large user packets are successfully forwarded in an EoIP mobility/guest tunnel between controllers.
- CSCsm25127—When you use the controller CLI to add a custom logo to the internal web authentication page, a light green border no longer appears above and to the right of the logo.
- CSCsm27071—A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS Software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:
  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available in the "workarounds" section of the advisory. The advisory is posted at this URL:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip
- CSCsm37204—Controller memory usage no longer grows to 44% after seven days of uptime.
- CSCso02467—When logging into a lobby ambassador account, you can no longer create permanent guest user accounts by setting all parameters to "0."
- CSCso04989—The controller no longer ignores video and voice streams from the client for about 60 ms when WMM is used with Intel 4965 clients on Windows Vista.
- 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 now appears on the controller CLI and on the controller GUI.
- CSCso20018—You can now enable DHCP Required on a guest LAN.
- CSCso29405—When you troubleshoot traffic on radio interfaces, remote debugs no longer fail for some radio debug commands.
- CSCso66830—Lightweight access points registered to a controller no longer show the domain name as cisco.com on the access point console.
- CSCso69005—After config paging disable is entered to disable page scrolling, the show acl summary and show acl detailed acl_name commands no longer show a "paging" prompt.
- CSCso97776—If you enable MFP when a guest LAN is configured, the controller no longer shows unwanted logs.
- CSCsq01766—When you change an access point's radio configuration, it no longer sends a deauthentication request using the wrong BSSID.

- CSCsq22518—CCKM clients using WPA2 no longer reauthenticate when moving between hybrid-REAP access points.
- CSCsq23806—Guest tunneling now works when the WLAN on the foreign controller is created using the controller GUI and the WLAN on the anchor controller is created using WCS.
- CSCsq34216—Controller system logs are no longer 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, and the username is not a username that is configured anywhere on the controller.
- CSCsq41190—The controller GUI now lists WEP settings in industry standard increments.
- CSCsq44516—Multiple vulnerabilities no longer exist in the Cisco Wireless LAN Controllers (WLCs), Cisco Catalyst 6500 Wireless Services Modules (WiSMs), and Cisco Catalyst 3750 Integrated Wireless LAN Controllers.
- CSCsq56139—When you configure the controller to send only access point register traps, the controller no longer continues to send client traps.
- CSCsr16689—Wired hosts cannot manage the 2106 controller through the dynamic interface.
- CSCsr22986—WCS now displays all access point groups even when the group names are consective.
- 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 now is able to perform a CCKM fast roam.
- CSCsr51667—When you click the **Refresh** button for the message logs on a controller running software release 4.2.130.0, the controller no longer generates a “Connection interrupted/Page load” error.
- CSCsr60506—The controller no longer unexpectedly reboots at spamReceiveTask with a signal 11 error (segmentation fault).
- CSCsr67250—1250 series access points now adjust their power levels correctly and no longer lock onto Tx Power Level 1 or 2.
- CSCsr63356—When a multicast application is in use, the multicast stream now receives the proper 802.1p QoS marking.
- CSCsr70862—A Cisco WiSM controller no longer reboots due to a software failure of the instruction located at 0x1038a140(ewsInternalAbort+348).
- CSCsr74362—Controllers no longer undergo memory leaks caused by saving the configuration.
- CSCsr75350—When a 1230 series access point is joined to a 4404 controller, the 2.4-GHz channel that the access point is on no longer differs between the controller and the access point.
- CSCsr83307—A configuration file that is uploaded with an encryption key can no longer be downloaded without the encryption key.
- CSCsr83671—The auto-RF feature on a Cisco WiSM or 4400 series controller no longer sets 1130 and 1240 series access points to channel 36 for the 5-GHz band (802.11a).
- CSCsr83684—When link aggregation (LAG) is enabled, the source MAC address for dynamic interfaces no longer changes during operation.
- CSCsr89399—Cisco 1131AG access points that are connected to Cisco WiSM controllers no longer reboot unexpectedly.
- CSCsu30254—When you configure an access point group VLAN for an old WLAN and then remove it, the access point group VLAN configuration now removes the mapping accordingly.

- CSCsu50080—When you configure web authentication passthrough with email input on the controller, the controller allows any text to be entered.
- CSCsu52812—When the controller is in multicast-unicast mode, it no longer sends unicast traffic to an access point before that access point has fully joined the controller.
- CSCsu57111—The following tracebacks no longer 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."
- CSCsu62060—A 4400 series controller no longer reboots due to a software failure of the tplusTransportThread.
- CSCsu74008—On a Catalyst 3750G Integrated Wireless LAN Controller Switch, the results of ipRouteIfIndex for some routes no longer point to an interface with index “5” when the results of IfIndex show only three interfaces with their corresponding indexes.
- CSCsu75686—When you configure the DHCP Addr. Assignment option on a WLAN using the controller GUI, the controller CLI now shows correct output in the show running-config command.
- CSCsu84220—When Cisco 1131 and 1242 access points are joined to a controller running software release 4.2.130.0 and a WAN outage occurs, both the the access points and the access point radios now come back up.
- CSCsu90335—Intel 4965 client cards no longer lose connectivity for up to 1 minute when another client connects to the same 1250 series hybrid-REAP access point on a controller running software release 4.2.130.0.
- CSCsu92667—The controller no longer reboots after you make a change to the configuration.
- CSCsu95855—After you change the mobility group name on some controllers, you can now remove one of the controllers.
- CSCsu96916—When you issue the **show run-config** CLI command via SSH on a 4400 series controller running software release 4.2.130.0 with paging disabled, the output no longer locks up.
- CSCsv00108—An invalid message integrity check (MIC) is no longer reported on beacon frames.
- CSCsv01484—The controller no longer prepends UID usernames with “CN=.”
- CSCsv01844—When you filter clients using the controller GUI, the controller no longer repeats the last two characters of the filter text.
- CSCsv12308—When the controller has to use its default gateway to talk to an access point, the access point now sees the join reply from the controller.
- CSCsv13068—An access request from the controller to the RADIUS server no longer has the Authenticator field set to all zeros.
- CSCsv23643—When you configure a WLAN with WPA2+802.1X and an infinite session timeout, any client that connects to a 5.1.151.0 controller no longer has a session timeout limited to approximately 11.6 hours.
- CSCsv34605—An access point using the Rogue Location Detection Protocol (RLDP) now receives a DHCP address even if the DHCP server is on an autonomous access point.
- CSCsv39950—Controllers running software release 4.2.130.0 no longer reboot at apfMsCreateDeadlock+76 while configured for debug pm ssh-engine enable.
- CSCsv40946—The FRAME-IP tag now appears in every RADIUS accounting message sent to the RADIUS server when a client uses WPA-PSK.
- CSCsv42697—The radio interface in an 1140 or 1250 series access point now reboots automatically after a radio failure.

- CSCsv43156—The trap for an unsuccessful SSH login attempt no longer shows the wrong IP address.
- CSCsv44917—You can no longer configure radio diversity for a 1250 series access point on the controller GUI.
- CSCsv52889—Controllers no longer reboot due to Reaper Reset.
- CSCsv69899—Controllers no longer randomly reboot and generate a crash file due to a software failure of the spamReceiveTask or pemReceiveTask task.
- CSCsv70556—When you create a new dynamic interface, assign a VLAN tag, and then apply the interface settings on the controller GUI, a message no longer appears indicating that no netmask or IP address was added.
- CSCsv74572—In a non-link aggregation (non-LAG) setup with both ports plugged into a switch and the switch sending gratuitous ARPs on port 2 for the gateway when the dynamic interface is on port 1, the controller no longer loses gateway access on a single VLAN, and off-subnet hosts (such as DHCP servers) can now be reached for DHCP.
- CSCsv77075—HTTPS now works on 4400 series controllers after you upgrade from software release 4.1.185.0.
- CSCsv79582—Controllers no longer reboot because of a software failure of the SShpmMainTask task.
- CSCsv91992—The controller now removes DHCP option 82 in DHCP traffic from the server to the client.
- CSCsv94993—When you enable DHCP Required on a WLAN, passive wired clients behind a workgroup bridge no longer lose their connection to the wireless network.
- CSCsw14316—The RADIUS accounting and RADIUS authentication server key format now return a default value other than ASCII or HEX.
- CSCsw15327—When you configure rogue access point containment from WCS, the controller now correctly contains the rogue access point.
- CSCsw19963—An SNMP trap message stating that the controller is out of sync with the central timebase no longer appears when the controller reboots.
- CSCsw20879—802.11a clients no longer lose connectivity every 99 seconds when you enable All Channel Scanning for the 802.11a network.
- CSCsw24700—Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:
  - Crafted HTTPS packet will crash device—Cisco Bug ID CSCsk62253.
  - SSLVPN sessions cause a memory leak in the device—Cisco Bug ID CSCsw24700.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities. This advisory is posted at the following link:

  http://www.cisco.com/en/US/products/csa/cisco-sa-20090325-webvpn.html
- CSCsw29804—Lexmark printers that are used with 4400 series controllers can now have apple ARP entries on a Layer 3 router and can now join the Appletalk zone.
- CSCsw30025—When you enter show custom-web wlan on the controller CLI, the controller no longer reboots.

- CSCsw34627—When you enter the show dhcp lease CLI command, the hours and minutes are now included in the output.
- CSCsw37323—The show sntp CLI command no longer prints an extra line when you enter it from HTTP.
- CSCsw41668—The Cisco WiSM no longer reboots and displays the following error message on the console: "** LOCK ASSERT ** (pemReceiveTask) !! prio=332 root=400 word=1000."
- CSCsw46354—The following traceback no longer appears in the controller message log:

```
Dec 12 08:48:16.957 apf_80211.c:3942 APF-1-SEND_ASSOC_RESP_FAILED: Could not send a
Client Association response to XX:XX:XX:XX:XX:XX. Suspected Auto-Immune attack Not
sending Assoc Response.
 - Traceback:  1051b51c 1051f7a0 100eaedc 100eb0a4 103e582c 10bb1168 10d6baac
```

- CSCsw49097—FCC DFS test no longer fails at certain off-center frequencies.
- CSCsw49636—A Cisco WiSM no longer reboots because of a software failure of the Reaper Watcher.
- CSCsw51658—A Cisco WISM with factory default settings now acquires an IP address during auto configuration when the Catalyst 6500 switch is running Cisco IOS Release 12.2(33)SXI.
- CSCsw63365—Autonomous access points with a static IP address that have either SSCs or MICs and that have been converted to LWAPP (using the 3.2 LWAPP conversion tool) no longer ignore the DNS resolution of CISCO-LWAPP-CONTROLLER.
- CSCsw71172—Controllers no longer crash when some VLANs are configured to use the controller as a local authenticator.
- CSCsw75392—If you configure a WLAN to simultaneously support WPA+TKIP, WPA+AES, and WPA2+AES, 802.11n clients that are configured for WPA2+PSK or WPA2+802.1X can now associate at 802.n data rates.
- CSCsw75514—When you connect a 1250 series access point to a computer with a straight-through cable and set up the computer with a 10 Mb half duplex link, link protocol on the GigabitEthernet interface on the access point now comes up correctly.
- CSCsw80092—Upstream TCP throughput is now normal between access points with antenna diversity and 802.11a or 802.11g clients.
- CSCsw86749—Irrelevant error messages no longer appear on 4400 series controllers.
- CSCsw87206—Because the service port interface must have an IP address on a different subnet from the Management, AP Manager, and any dynamic interfaces, the controller checks whether the IP address that you assign to each interface is valid. This check mechanism now works when you change the subnet mask of each interface.
- CSCsw83779—Symbol scanners (MC9090) no longer fail to connect to a local EAP WLAN after an extended time.
- CSCsw88108—When you add a MAC address to the access point authentication list using SNMP, the controller no longer allows uppercase characters.
- CSCsw89469—The transmit datarate on 1000 series access points is no longer limited to 1M when you disable 24M.
- CSCsw91505—Log messages from Mesh access points now provide timestamps.
- CSCsw92225—Controllers no longer fail to forward broadcast traffic on UDP port 7013.
- CSCsw92335—If you use WCS to set the session timeout for a WLAN with 802.1X, WPA, or WPA2 security, the timeout is now set on the controller.

- CSCsw97548—The controller no longer reboots because of a software failure of the osapiTimer task.
- CSCsw97549—Browsing to the client page in WCS no longer crashes the controller.
- CSCsw39752—802.1X authentication no longer fails during client reassociation.
- CSCsx04986—WCS no longer receives reports from the controller that a rogue access point is on the network when a rogue access point is not actually on the network.
- CSCsx07538—When a TCP connection is open to port 1000, the controller no longer responds with a reset.
- CSCsx07878—Client devices no longer intermittently fail to log into a WLAN with web authentication (webauth).
- CSCsx14840—The management interface source MAC address no longer changes during operation.
- CSCsx29956—A 4400 series controller no longer reboots when it is configured to operate with an LDAP server because of a software failure of the LDAP DB Task 2 task.
- CSCsx49984—Client devices now progress from Probing status.
- CSCsx44137—Controllers no longer reboot while sending message logs to FTP.
- CSCsx49415—1230 series access points no longer stop servicing clients while displaying messages stating that the access point is running out of memory.
- CSCsx74494—The controller GUI now displays the status of mobility members.
- CSCsx77035—The description field for disabled clients is no longer limited to three characters.
- CSCsx80743—Enabling, disabling, and then re-enabling LAG without rebooting the controller no longer causes loss of communication to the controller.
- CSCsy15893—You can now disable world-mode on lightweight access points.
- CSCsy18634—The controller no longer reboots in task apfOpenDtlSocket function apfProcessAuthReq.
- CSCsy20914—Controllers no longer send multiple client association traps.
- CSCsy24245—The show run-config command output now includes information on WLAN AP groups.
- CSCsy27502—The system message “Mobility Response: code 1, reason 5” now includes an explanation of the conditions that triggered the message.
- CSCsy33571—Client devices can now send upstream traffic which has an actual packet length different from the indicated length.
- CSCsy40666—Controllers no longer silently drop malformed UDP control packets.
- CSCsy50654—Controllers no longer undergo memory leaks caused by incrementing of the mmlisten process.
- CSCsy57573—Controllers no longer reboot at software task spamReceiveTask.
- CSCsy83600—Downgrading from controller software release 5.2.x to 4.2.x no longer causes the configuration wizard to fail.
- CSCsy80680—Client devices no longer fail to obtain an IP address after roaming.

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