



Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.2.173.0

October 31, 2008

Enhanced testing and intense focus on caveat resolution contribute to the quality of controller software release 4.2.173.0.

These release notes describe new and changed information as well as open and resolved caveats for software release 4.2.173.0 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.

- [Cisco Unified Wireless Network Solution Components, page 2](#)
- [Controller Requirements, page 3](#)
- [Software Release Information, page 3](#)
- [New and Changed Information, page 7](#)
- [Installation Notes, page 8](#)
- [Important Notes, page 11](#)
- [Caveats, page 23](#)
- [Troubleshooting, page 49](#)



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

© 2008 Cisco Systems, Inc. All rights reserved.

- [Documentation Updates, page 50](#)
- [Related Documentation, page 50](#)
- [Obtaining Documentation, Support, and Security Guidelines, page 50](#)

Cisco Unified Wireless Network Solution Components

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

- Software release 4.2.173.0 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 4.2.110.0



Note Only Cisco WCS 4.2.110.0 supports controllers running software release 4.2.173.0.

- Cisco WCS Navigator 1.1.110.0
- Location appliance software release 3.1.42.0
- 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 points have a hardware limitation where beacons can only be output at intervals that are multiples of 17 milliseconds. When these APs are configured for a 100-millisecond beacon interval, they transmit beacons every 102 milliseconds. Similarly, when the beacon interval is configured for 20 milliseconds, these APs transmit beacons every 17 milliseconds.

Special Notice for Mesh Networks


Note

Do not upgrade to controller software release 4.2.173.0 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 4.2.110.0 may be used to manage both mesh and non-mesh controllers (such as controllers running software release 4.2.173.0 and 4.1.192.22M). 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

To use the controller in the Catalyst 3750G Wireless LAN Controller Switch, the switch must be running Cisco IOS Release 12.2.25.FZ or 12.2(25)SEE.

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 4.2.173.0 to 4.2.61.0 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 4.2.173.0



Caution

Before upgrading your controller to software release 4.2.173.0, 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 4.2.173.0 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 4.2.173.0 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 4.2.173.0. 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 4.2.173.0. [Table 1](#) shows the upgrade path that you must follow before downloading software release 4.2.173.0.

Table 1 Upgrade Path to Controller Software Release 4.2.173.0

Current Software Release	Upgrade Path to 4.2.173.0 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 4.2.173.0.
4.0.155.5	Upgrade to 4.0.206.0 (or a later 4.0 release) before upgrading to 4.2.173.0.
4.0.179.11	
4.0.206.0 or later 4.0 release	You can upgrade directly to 4.2.173.0.
4.1.171.0 or later 4.1 release	You can upgrade directly to 4.2.173.0.
4.2.61.0	You can upgrade directly to 4.2.173.0.
4.2.99.0	You can upgrade directly to 4.2.173.0.
4.2.112.0	You can upgrade directly to 4.2.173.0.
4.2.130.0	You can upgrade directly to 4.2.173.0.



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 4.2.173.0 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 4.2.112.0 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 (4.2.112.0 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.

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 4.2.173.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 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 4.2.173.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 ER.aes file).

Step 3

Copy the controller software file (*filename.aes*) and the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 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 4.2.173.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 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 4.2.173.0 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 4.2.112.0 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 and Changed Information

The following changes are available in controller software release 4.2.173.0.

- Controller software release 4.2.173.0 and prior releases support both asymmetric and symmetric mobility tunneling. However, Cisco plans to deprecate asymmetric mobility tunneling in future controller software releases.

**Note**

Controllers within the same mobility group that run different software releases (such as 4.2, 5.0, and 5.1) can use guest tunneling, but they do not support normal client mobility.

- To help troubleshoot controller crashes, you can now configure the controller to automatically upload its core dump file to an FTP server after experiencing a crash using these CLI commands:
config coredump {enable | disable}
config coredump ftp server_ip_address filename
config coredump username ftp_username password ftp_password
show coredump summary
- To help troubleshoot hard-to-solve or hard-to-reproduce memory problems, you can configure the controller to monitor for memory leaks and to perform an auto-leak analysis between two memory thresholds. Refer to the “Monitoring Memory Leaks” section in the Troubleshooting appendix of the *Cisco Wireless LAN Controller Configuration Guide, Release 4.2* for information on these commands.
- You can now upload the console dump resulting from a software-watchdog-initiated reboot of the controller following a crash using the **transfer upload datatype watchdog-crash-file** controller CLI command. The software watchdog module periodically checks the integrity of the internal software and makes sure that the system does not stay in an inconsistent or non-operational state for a long period of time.
- You can upload the kernel panic information if a kernel panic occurs using the **transfer upload datatype panic-crash-file** controller CLI command.
- You can now disable Secure Socket Layer (SSL)v2 for web administration and web authentication. When SSLv2 is disabled, users cannot connect using a browser configured with SSLv2 only. They must use a browser that is configured to use a more secure protocol such as SSLv3 or later. The new CLI command to enable or disable SSLv2 is **config network secureweb cipher-option sslv2 {enable | disable}**. The default value is enabled.
- You can now use this CLI command to enable or disable client decrypt traps: **config trapflags 802.11-security wepDecryptError {enable | disable}**.
- For web authentication, you can now download device certificates as chained certificates (up to a level of two).

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.

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

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

Configuration File Stored in XML 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 4.2.173.0 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" cellpadding="0" cellspacing="0"> <tr> <td>&nbsp;</td></tr>

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

<tr align="center">

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

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

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

```

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 4.2.173.0.

- 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.

- 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.
- 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.
- 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.

- CSCsg95474—Lightweight access points do not queue disassociation messages, causing the Cisco 7921 phone to remain in a registering loop. This problem occurs when you change the data rate on the access point.

Workaround: Power cycle the 7921 phone.

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

Workaround: Do not stop the console using **Ctrl-S**.

- 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.

- CSCsi06191—After you reboot the controller, the master controller mode is disabled.

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.
- 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.
- 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.
- CSCsi72578—After you set up the mobility anchor feature between two controllers, the client does not successfully connect to the specified anchor controller when the WLAN QoS profile is set to bronze.
Workaround: Change the WLAN QoS profile on both the internal controller and the anchor controller to silver.
- 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.
- CSCsj10755—When multicast mode multicast and IGMP snooping are enabled, the controller periodically sends out IGMP query messages to the clients. This IGMP query is sent as individual queries to each access point.
Workaround: None.
- CSCsj10945—The controller does not factor in the antenna gain when reducing the output power.
Workaround: Manually adjust the antenna gain, but this action can interfere with auto RF.
- 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 Cisco 1240 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.
- CSCsl09066—The WCS access point group VLAN profile configuration does not match the actual WLC configuration when you use multiple interface mapping profiles under the same access point group VLAN where all of the SSIDs start with the same letters or numbers.
Workaround: None.
- 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.

- 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.

- CSCsl57356—When an 802.11n client is associated to a 1250 series access point, sometimes the client does not show up as 802.11n on the controller GUI and CLI. Instead, the controller shows the associated client using the 802.11a or 802.11b protocol if using the 2.4-GHz or 5-GHz band, respectively. However, the client software shows that the client is connected using the 802.11n protocol and at 802.11n data rates.

Workaround: None.

- 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.

- CSCsl79260—Wired guest LAN clients do not get an IP address if DHCP proxy is disabled.

Workaround: Do not disable DHCP proxy.

- 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.

- 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.

- CSCsm05607—Large user packets might fail to be successfully forwarded in an EoIP mobility/guest tunnel between controllers.

Workaround: Perform one of the following:

- Reconfigure the IP endpoints to use smaller MTUs.
- If an IOS router is in the IP path used by the IP endpoints, use **ip tcp adjust-mss 1300** (or a similar value) to have the endpoints reduce the size of the TCP/IP packets that they transmit.
- Redesign the network path between the EoIP tunnel endpoints to eliminate ICMP filters, tunnels, NAT translation, firewalls, and so on so that it can forward 1500-byte IP packets without fragmentation.

- 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.

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

Workaround: None.

- CSCsm40870—The following error message should be reworded:

```
Jan 24 15:20:55.374 apf_80211.c:2552 APF-4-ASSOCREQ_PROC_FAILED: Failed to process an
association request from 00:13: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.

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

Workaround: None.

- 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.

- 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.

- CSCsm95478—HT protection bits might incorrectly report the operating mode.

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 `clCdpGlobalEnable` 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.

- CSCso02467—When logging into a lobby ambassador account, you are able to create permanent guest user accounts by setting all parameters to “0.” After logging back into the account, you can verify that these permanent accounts were created under Security > Local Net Users.

Workaround: None.

- CSCso04989—The controller does not acknowledge video and voice streams from the client for about 60 ms. This problem occurs when WMM is used with Intel 4965 clients on Windows Vista.

Workaround: None.

- 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.

- 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.

- CSCso47897—The MAC address table on the switch might show an invalid MAC address coming from the interfaces attached to the controllers.

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.

- CSCso66183—Symbol Vocollect devices might disassociate from Cisco 1240 series access points and display the following error message:

```
"3/30/2008 04:42"      Error      " Mar 30 04:47:25.626 spam_api.c:816 WAPP-3-MAX_AID:
Reached max limit (200) on the association ID for AP 00:1d:a1:90:11:10"
"3/30/2008 04:42"      Error      " Mar 30 04:47:21.703 spam_api.c:816 WAPP-3-MAX_AID:
Reached max limit (200) on the association ID for AP 00:1d:a1:90:11:10"
```

Workaround: Manually power-cycle the access points.

- CSCso97776—If you enable MFP when a guest LAN is configured, the controller might show unwanted logs.

Workaround: None.

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

Workaround: None.

- 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**.

- CSCsq06690—The following log might appear unexpectedly on the controller: “Memory 0x3022c8e0 has been freed!”

Workaround: None.

- 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.

- 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.

- 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.

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

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.

- CSCsq22518—CCKM clients using WPA2 reauthenticate when moving between hybrid-REAP access points.

Workaround: None.

- CSCsq22827—The access point name sometimes disappears from the controller GUI and CLI.

Workaround: None.

- 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.

- CSCsq23806—Guest tunneling might not work if the WLAN on the foreign controller is created using the controller GUI and the WLAN on the anchor controller is created using WCS.
Workaround: Reboot the anchor controller or use the same method (either the controller GUI or WCS) to create the WLAN on both the anchor and foreign controllers.
- CSCsq25129—A controller software upgrade might fail with a Nessus scan running.
Workaround: None.
- CSCsq26051—When a Cisco terminal server connects to the controller but the user is not logged in through the console, the controller might hang after a reboot.
Workaround: None.
- 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: dtlARPPProtoRecv: 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.
- 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.

- 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.
- CSCsq67907—If a large number of rogue access points are present and there is a substantial amount of client activity, the apfRogueTask might report lock asserts.
Workaround: None.
- CSCsq73118—When a Cisco WiSM is used with multiple WLANs and the VLAN override feature, malformed packets might appear on the native VLAN associated to the link aggregation (LAG) trunk.
Workaround: Isolate the native VLAN on the switch so that it does not propagate malformed packets.
- CSCsq74144—The controller does not show the channel on which an access point in sniffer mode is sniffing. It shows only the last channel on which the access point was broadcasting in local mode.
Workaround: None.
- CSCsr01195—The controller drops a packet after a train of large packets.
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.
- CSCsr18694—After passing a substantial amount of traffic, the D0 interface might shut down on a controller running software release 4.2.173.0. Some packets might be stuck in the queue.
Workaround: None.
- CSCsr20434—Missing and invalid message integrity check (MIC) management frame protection (MFP) traps might be reported on 1250 series access points.
Workaround: None.
- CSCsr32354—When a 1250 series access point with an external power supply is connected to a 6548 FE blade inside a Cisco Catalyst 6500 switch, the line protocol does not come up after a reset. This problem also occurs intermittently when a power injector is used.
Workaround: None.
- 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.
- CSCsr55953—The controller might drop traffic to the CPU and log the following message:
“NP3400_interrupt.c:3766 Could not enqueue pkt_type 6 (proto 0x0000, len 108), return -12.(6 suppressed msgs).”
Workaround: None.
- 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.
- CSCsr63356—When a multicast application is in use, the multicast stream does not get the proper 802.1p QoS marking.
Workaround: None.
- CSCsr67250—1250 series access points do not adjust their power levels correctly and always stay on Tx Power Level 1 or 2.
Workaround: None.
- CSCsr70862—A Cisco WiSM controller running software release 4.2.130.0 might reboot due to a software failure of the instruction located at 0x1038a140(ewsInternalAbort+348).
Workaround: Set the session timeout to zero or remove Telnet access.
- CSCsr71245—A 4400 series controller without an embedded syslog manager (ESM) might reboot if you enable or disable encryption on the controller using WCS.
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.
- CSCsr75350—When a 1230 series access point is joined to a 4404 controller, the 2.4-GHz channel that the access point is on differs between the controller and the access point.
Workaround: None.
- CSCsr83307—A configuration file that is uploaded with an encryption key can be downloaded without the encryption key.
Workaround: None.
- CSCsr83671—The auto-RF feature on a Cisco WiSM or 4400 series controller sets 1130 and 1240 series access points to channel 36 for the 5-GHz band (802.11a).
Workaround: Follow these steps to work around the issue:
 - a. To change the sensitivity level, enter this command:
config advanced 802.11a channel dca sensitivity high

- b. To save your changes, enter this command:

save config

- c. To verify your changes, enter this command:

show advanced 802.11a channel

Information similar to the following appears:

DCA Sensitivity Level: HIGH (5 dB)

- CSCsr83684—When link aggregation (LAG) is enabled, the source MAC address for dynamic interfaces might change during operation.
Workaround: None.
- CSCsr89399—Cisco 1131AG access points that are connected to Cisco WiSM controllers might reboot unexpectedly.
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.
- CSCsr89894—If a client roams from one controller to another and then powers down or leaves the RF range, the client entry on the first (anchor) controller is not deleted even though the client entry on the second (foreign) controller is deleted correctly.
Workaround: Manually delete the client entry from the anchor controller.
- CSCsr97377—Roaming latency might be high (around 300 ms) when 802.11n 5-GHz clients are using WPA2-PEAP with AES on the 40-MHz channel.
Workaround: None.
- CSCsu00583—Roaming latency might be high (around 200 ms) when 802.11n 2.4-GHz clients are using 802.11g default data rates.
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.
- CSCsu11528—The 4400 series controllers might drop very large (usually greater than 6000 bytes) UDP and ping frames sourced from a wired node on the Ethernet and originating at 1-Gbps line rate.
Workaround: Drop the line rate to 100 Mbps, decrease the size of UDP or ICMP frames, or use a different brand of wired client card.

- CSCsu12458—When a number of web-authentication users join the wireless network, the sshpmMainTask might spike above 90% on a 2106 controller running software release 4.2.130.0. Once sshpmMainTask spikes, the access points begin to drop off the controller, and access to the controller becomes very sluggish.

Workaround: Disable web authentication or web pass-through for the WLAN.

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

Workaround: None.

- 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: None.

- 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.

- CSCsu41774—All workgroup bridges (WGBs) joined to one controller might suddenly disconnect from the external network. However, when a WGB moves to a second controller, it regains connectivity.

Workaround: None.

- CSCsu44516—A 4404 controller running software release 4.0.179.8 and connected to a Catalyst 3750 stack might sometimes show wireless clients stuck in the DHCP_REQD state and unable to pass traffic. This issue seems to occur for RF hand-held scanners.

Workaround: Reset the controller to purge the client associations.

- CSCsu44722—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.”

Workaround: None.

- 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.

- CSCsu52812—When the controller is in multicast-unicast mode, it sends unicast traffic to an access point before that access point has fully joined the controller. This behavior can be a serious problem when the access point is running a recovery image like 12.3(11)JX1, which does not drop LWAPP data packets. If the number of data packets sent to the access point before it receives the full image is large enough, the access point locks up and cannot join the controller.

Workaround: To resolve access point join issues, follow these steps:

- a. Load recovery image 12.4(10b)JA3 on the access point.
- b. Load the full LWAPP image on the access point.

c. Disable multicast-unicast on the controller.

If the multicast mode multicast is supported, change the multicast mode to multicast, or disable multicast.

- CSCsu52837—Preauthenticated clients cannot reach web-authenticated clients on the same WLAN.
Workaround: None.
- CSCsu62060—A 4400 series controller might reboot due to a software failure of the `tplusTransportThread`.
Workaround: None.
- CSCsu67530—When more than six controllers are in a mobility group, client mobility can become sporadic.
Workaround: None.
- CSCsu72717—The name is corrupted in the interrupt session of the Cisco WiSM controller's crash file.
Workaround: None.
- CSCsu74487—Cisco 1131 access points attached to a controller running software release 4.2.130.0 might reboot unexpectedly. If you collect the core dumps to analyze the reason for the reboot, the core dump files produced are 0 bytes in size.
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.
- CSCsu81856—A 4402 controller running software release 4.2.130.0 and configured with an internal DHCP server might sometimes exhibit DHCP leases for addresses that are statically assigned to various wireless clients.
Workaround: None.
- 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, the access points come back up, but sometimes the radios do not.
Workaround: Reboot the access points.
- 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.

- CSCsu88532—When you download new software to the controller, a routine system resource notification appears on the controller console.
Workaround: None.
- CSCsu90335—Intel 4965 client cards might 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.
Workaround: Disable local switching on the SSID.
- CSCsu92667—The controller might reboot after you make a change to the configuration.
Workaround: None.
- CSCsu95855—After you change the mobility group name on some controllers, you cannot remove one of the controllers. An error appears stating that the controller is configured as an anchor for a WLAN, even though none of the existing WLANs has this controller configured as its anchor.
Workaround: If the CLI shows that this controller is configured as an anchor for a WLAN that does not exist, create that WLAN. Then overwrite the WLAN and remove its anchors. Then you can remove the controller from the mobility group.
- 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 locks up at a certain point, probably because the controller runs out of buffers.
Workaround: Enable paging or use a Telnet session.
- CSCsu98641—The core-dump configuration does not show in the running configuration on the Cisco WiSM.
Workaround: None.
- CSCsv00108—An invalid message integrity check (MIC) might be reported on beacon frames.
Workaround: None.
- CSCsv01484—The controller prepends UID usernames with “CN=,” which can cause problems for LDAP authenticated binds. The controller should check for usernames with “UID” but not prepend them with “CN=.”
Workaround: None.

Resolved Caveats

These caveats are resolved in controller software release 4.2.173.0.

- CSCsi86794—When auto-channel selection is enabled and access points use the following channels, clients are unable to associate: 100, 104, 108, 112, 116, 132, 136, 140, and 149.
- CSCsk08360—Further clarification is needed on the following message log entry:
APF-1-DISCONNECT_MOBILE_DUE_TO_WLAN_SWITCH: Disconnecting mobile 00:16:6f:79:82:75 due to switch of WLANs from 2 to 1.
- CSCsk15603—On the controller GUI, a conditional web-redirect configured with 802.1X security generates an error.
- CSCsk21007—The controller requires TACACS+ authentication when a configuration setting is changed on the controller GUI or a GUI page is opened.
- CSCsk47585—A 1242 hybrid-REAP access point reboots after you make a WLAN change from a 4.1.185.0 controller and then save the configuration on the controller.

- CSCsk54969—One of the controllers in the Cisco WiSM might stop providing web authentication login pages but continue to allow WPA2 RADIUS authentication to the same authentication server.
- CSCsk68619—A radio in a 1250 series access point might experience these problems:
 - A failure to pass traffic on the 2.4-GHz radio
When this problem occurs, the **show interface dot11radio0 dfs** command shows the Max Used Bins counter as greater than 254.
 - Poor performance when receiving data from the radio
When this problem occurs, the radio interface shows throttles.
 - 802.11n performance on the 5-GHz radio might be significantly lower in the access point's transmit path than in its receive path.
- CSCsk70727—A 7921 IP phone in world mode is not connecting to a 4400 series controller with country code KE.
- CSCsk86992—Many instances of the following message appear in the controller or WCS trap logs:


```
MFP Anomaly Detected - 1417 Missing MFP IE event(s) found as violated by the radio
xx:xx:xx:xx:xx:xx and detected by the dot11 interface at slot 0 of AP
xx:xx:xx:xx:xx:xx in 300 seconds when observing Probe responses, Beacon Frames.
Client's last source mac xx:xx:xx:xx:xx:xx
```
- CSCsk93026—A 1230 series access point might lose its certificate during a software upgrade. This issue occurs when the access point moves to another controller running a different software release.
- CSCsl09218—You cannot upload a binary backup from the CLI on controllers running software release 4.2.
- CSCsl10597—After dynamic frequency selection (DFS) chooses a new channel, the 5-GHz radio of a 1250 series access point does not move to the new channel and start beaconing.
- CSCsl19025—Controllers do not respond to a device with an IP address that ends in zero, as in x.x.x.0.
- CSCsl48417—The DTL-1-ARP_POISON_DETECTED, DTL-1-IP_CONFLICT_DETECTED, and other controller DTL messages need to be more descriptive.
- CSCsl77058—The word “rogue” is misspelled in one of the WLAN message log statements. The correct statement should be “APF-1-UNABLE_TO_KEEP_ROGUE_CONTAIN.”
- CSCsl90630—Dynamic channel assignment (DCA) requires you to add at least one non-DFS channel to the list. However, non-DFS channels are not available for an access point deployed outdoors in the EU.
- CSCsm12623—The AAA override dynamic VLAN assignment fails with guest tunneling. Clients successfully authenticate, but the IP address is that of the interface the WLAN is associated to on the anchor controller.
- CSCsm25127—When you use the controller CLI in controller software release 4.2.61.0 to add a custom logo to the internal web authentication page, a light green border appears above and to the right of the logo.
- CSCsm42355—The controller returns a signed 32-bit integer in the MIB object bsnAPIfSlotId although the published MIB module indicates that the controller should return an unsigned integer. This behavior may cause WCS to misinterpret incoming trap data that is eventually used in reports and graphs.
- CSCsm48076—Guest-related trap logs are not generated for a lifetime guest user.

- CSCsm65113—Access points converted to lightweight mode do not retain the power injector state on the controller after they are rebooted.
- CSCsm85717—To aid in troubleshooting, the following error message should identify the root cause of the problem:

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

- CSCsm91814—When a client associates and authenticates on the same SSID using a different username and password, a 4400 series controller using WPA2-AES and PEAP-MSCHAPv2 might randomly cache the AAA override values such as dynamic VLAN and assign the client to the wrong VLAN. The client also obtains an IP address on the wrong VLAN.
- CSCsm94067—1100 and 1200 series access points that have been converted to lightweight mode do not retain the power injector state after a reboot. This setting is enabled on the access point; however, when the access point reboots, it shows as not being enabled on the controller.
- CSCsm95677—When a WLAN is configured for WPA2-AES, the CB21AG client adapter is unable to send prioritized data.
- CSCsm98250—After you upgrade the controller to software release 5.0, web authentication stops working, and you can no longer access the controller through HTTP or a Telnet or SSH session.
- CSCso13516—The controller sometimes crashes at random, and the crash file shows a signal 11. Signal 11 occurs when the program running on the controller accesses a part of memory that it does not have permission to access.
- CSCso35129—If the controller is queried by SNMP for a virtual gateway interface address, it may generate messages such as “sim.c:1061 SIM-3-MACADDR_GET_FAIL: Interface 1 source MAC address is not found.”
- CSCso39413—Constant access control list (ACL) messages appear in the controller logs even though no ACLs are configured.
- CSCso48158—The tickle timer, which is used to update the watchdog timer, is not preserved correctly when the NPU-to-CPU interrupt handler becomes congested and overrun. This issue affects console output and serial port communications potentially used for low-level debug console output messages.
- CSCso52349—If SNMP is tested against the controller’s management IP address from a device on the same subnetwork as a dynamic interface, the controller fails to send SNMP responses.
- CSCso58919—When AAA override is disabled, the PMK CCKM lifetime value uses the attribute 27 setting from the AAA server instead of the WLAN session timeout.
- CSCso63232—The controller in the Catalyst 3750G Wireless LAN Controller Switch might reboot if you enter the **show hreap group detail groupname** CLI command without a group name or without a space between the **detail** parameter and the group name.
- CSCso65150—When AAA override is enabled for a WLAN and the AAA server provides the session timeout value, if a client that is associated to that WLAN roams to another access point joined to the same controller and the session timeout has not expired, the session timeout for that client is reset to the initial value received from the AAA server.
- CSCso66778—The output of dump low-level debugs is not complete for several commands in controller software releases 4.2 and 5.0. This problem might affect proper troubleshooting for service port hangs, NPU issues, and so on.

- CSCso69568—The RADIUS accounting setting does not appear in the output of the show wlan wlan_ID CLI command if the WLAN security policy is one of the following:
 - None
 - Static WEP
 - WPA-PSK
 - Web authentication
- CSCso71603—When a client moves from one controller to a 2106 controller on the same subnet, the client cannot pass traffic for 5 minutes.
- CSCso72229—After you upgrade the controller to software release 4.2.112.0, the following message might appear repeatedly:


```
Mar 27 18:15:13.735 spam_join_debug.c:84 LWAPP-4-AP_JDBG_ADD_FAILED: Unable to create
AP Join information entry for AP:00:0f:24:0e:34a0, Maximum number of AP join
information entry supported already exists.
```
- CSCso72588—When you use the wired guest feature, an accounting stop record is not sent after the timeouts expire.
- CSCso73635—During the LWAPP discovery process, 1000 series access points sometimes send Layer 2 discovery frames with Ethertype 0x88bb instead of 0xbbbb. As a result, the access points generate the following incorrect syslog message: “%LWAPP-ERRORLOG: Received unsupported message 0x1 from controller.”
- CSCso76131—The controller is not updating the MAC address in the ARP cache when receiving a gratuitous ARP. For example, in a redundant firewall setup, if the primary controller fails, the secondary controller sends out gratuitous ARPs to update the ARP cache of the devices on the network. The controller's management interface mapping for the default gateway updates correctly, but the dynamic interface mappings are not updating the ARP table. The following message appears in the message log of the controller: “dtl_arp.c:1240 DTL-3-OSARP_DEL_FAILED: Unable to delete an ARP entry for <IP Addr> from the operating system. ioctl operation failed.”
- CSCso76479—A CLI command is needed to disable SSLv2 for web administration and web authentication. When SSLv2 is disabled, users cannot connect using a browser configured with SSLv2 only. The new CLI command to enable or disable SSLv2 for web administration and web authentication is **config network secureweb cipher-option sslv2 {enable | disable}**.
- CSCso84256—During CCKM roaming, the following misleading debug message might appear: “Creating a new PMK Cache Entry for station.”
- CSCso86463—Lightweight access points running controller software release 4.2.99.0 might reboot if traffic stream metrics are enabled.
- CSCso87175—SNMP support is needed to enable or disable DHCP proxy from WCS.
- CSCso92229—The controller CLI accepts a CIDS SHA1 key with the correct number of hexadecimal digits but also accepts extra colons between the pairs of digits.
- CSCso92249—The controller sometimes reboots without a crash log when you run multiple Telnet sessions.
- CSCso92828—When an access point is running RLDP, radio reset messages caused by RLDP should be suppressed.
- CSCsq01201—Certain client applications might fail when the client is joined to a 1010 series access point running a 4.1 or 4.2 software release. The failure occurs when an application from a wireless client causes the access point to fragment packets, and the fragments reach the controller out of order.

- CSCsq02092—1100 and 1200 series access points and 1310 series bridges fail to download image code from a 4400 series controller running software release 4.2. The following error message is logged:

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

- CSCsq07537—Clients continue to communicate with an access point that has its radio disabled by the controller. The controller shows that the access point radio is disabled when it is not.
- CSCsq08062—A TACACS+ connection initiated from the controller to the TACACS+ server sometimes times out in 0.5 seconds.
- CSCsq12626—The following error message appears on the controller's syslog server when the controller is in a network with HSRP nodes:

```
Message=<131> Apr 30 08:20:53.174 ccx_rm.c:2771 CCX-3-AP_NOT_FOUND: AP
00:00:0c:07:ac:00 does not exist.
```

- CSCsq12776—The controller might crash without generating a crash file.
- CSCsq13174—Web authentication device certificates cannot contain the Certificate Authority (CA) roots chained to the device certificate. However, device certificates should be able to be downloaded as chained certificates (up to a level of two).
- CSCsq14961—SNMP returns only one record for client roam reports whereas the controller CLI shows multiple records.
- CSCsq23961—An orphan packet from the distribution system port might prevent DHCP from operating properly.
- CSCsq25029—A 2106 controller running software release 4.2.112.0 might reboot due to a software failure of the bcastReceiveTask.
- CSCsq25642—When an access point joins the controller or when WLANs are changed on the controller, the following invalid slot ID warning might appear on the access point console along with a traceback:

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

- CSCsq26901—Cisco WiSMs running controller software release 4.1.186.2 sometimes crash due to a software failure on the instruction located at: 0x1020387c (rrmLradSetTxPower+676).
- CSCsq31662—The controller reboots after you upgrade from software release 4.2.61.0 to 4.2.112.0.
- CSCsq35662—More debug messages are needed when an access point fails to download the software image from the controller.
- CSCsq35990—The **config netuser lifetime** CLI command does not accept a zero (0) value for the *lifetime* parameter.
- CSCsq41327—Under certain circumstances, the network processing unit (NPU) of a 4400 series controller or Cisco WiSM might lock up, causing a system restart, or the NPU Check Task might invoke a software crash. The resolution of this bug adds additional error and integrity checking in the NPU code path logic to ensure that the NPU Check Task does not branch to an invalid address.
- CSCsq49831—The controller should generate a core dump when it crashes to aid in debugging.
- CSCsq49975—When you enable ARP debugs and generate a gratuitous ARP, the gratuitous ARP does not come up to the dtl ARP module, and no debugs appear on the console.
- CSCsq51733—The controller sometimes drops BOOTP packets from wireless clients.

- CSCsq55117—The controller might reboot when multiple people are connected through Telnet at the same time.
- CSCsq57697—WPA2 PMK cache updates are not being sent across the mobility group.
- CSCsq58843—A 4400 series anchor controller cannot ping Ethernet-over-IP (EoIP) roamed clients.
- CSCsq59283—You cannot set the WLAN override group name or description to a length of 32 characters using SNMP.
- CSCsq59896—A 4400 series controller might reboot after you upgrade the controller software from the 4.2.112.0 release to the 4.2.130.0 release.
- CSCsq63106—The controller shows a memory leak of 1.8 MB every 2.5 hours. When the controller enters a low-memory condition, it becomes unreachable and requires a reboot.
- CSCsq63937—When you enter the **transfer download mode ftp** CLI command, the value for the SNMP object agentTransferUploadMode is missing from snmpwalk.
- CSCsq65563—The Controller Network Module needs a software watchdog in order to allow the controller to be rebooted in the event of a system freeze.
- CSCsq69712—A 2100 series controller might reboot while you are browsing the Monitor section of the controller GUI.
- CSCsq81667—Large IP packets that have been fragmented into multiple fragments might not be reassembled by a 4400 series controller.
- CSCsq83843—The following error message requires more information:
“DOT1D-6-PORT_FIND_FAIL: Port number 1 is not found for GARP Information Declaration (GID).”
- CSCsq83855—The following error message requires more explanation: “Process:
Name:fp_main_task, Id:11d92ca8.”
- CSCsq84257—If you configure an SNMP trap receiver, the controller sends an SNMP decrypt traps event when all of the client traps are disabled. A CLI command is needed to enable or disable client decrypt traps. To resolve this issue, the **config trapflags 802.11-security wepDecryptError {enable | disable}** command has been added.
- CSCsq86975—The controller might crash under the following conditions:
 - If global CDP and access point CDP are disabled and you click the **Refresh** button on the CDP > AP Neighbors page.
 - If global CDP and access point CDP are enabled, the access points are connected to a non-Cisco switch and no CDP information is provided, and you click the **Refresh** button on the CDP > AP Neighbors page.
- CSCsq87457—The Cisco WiSM might experience an NPU lockup or reboot on the NPUChecktask.
- CSCsr02760—When you configure a 1250 series access point with MFP validation, the access point triggers an MFP out-of-sequence alarm. For example:

```
31 Thu Jun 26 16:17:40 2008 MFP Anomaly Detected - 1 Out of sequence event(s) found as
violated by the radio XX:XX:XX:XX:XX and detected by the dot11 interface at slot 1 of
AP YY:YY:YY:YY:YY in 300 seconds when observing Beacon Frames. Client's last source
mac XX:XX:XX:XX:XX
```
- CSCsr03008—A Cisco 1250 series access point intermittently delays packets to Cisco 7921 phones for up to 20 to 30 seconds. As a result, the 7921 phones experience no rings, one-way audio, or no audio.
- CSCsr06596—After the controller has been up for several days, it might crash if the apfRogueTask fails.

- CSCsr10990—1010 series access points constantly reset when a third-party IP management tool is enabled on the VLAN on which the access points are installed.
- CSCsr16752—The Controller Network Module NM-AIR-WLC6 might experience interface flapping after the interface is reset.
- CSCsr20151—If you change the power level of a 1252 series access point 5-GHz radio, the change does not take effect.
- CSCsr31687—When two Spectralink phones are used with a 1250 series access point, the uplink from one phone might collide with the downlink of the other phone, resulting in a high number of retries.
- CSCsr40109— When a client roams from an access point joined to one controller to an access point joined to another controller, the client might lose connectivity for as long as the configured user idle timeout.
- CSCsr43364—The controller sometimes reboots after you click the WLANs tab on the controller GUI.
- CSCsr46718—When connectivity is lost between a foreign controller and an anchor controller for an auto-anchoring WLAN, wireless clients that are able to successfully associate and authenticate fall back to the foreign controller's WLAN interface VLAN instead of anchoring to the external controller or failing connectivity.
- CSCsr52442—Auto completion does not work for the **show port summary** CLI command. If you enter **show port summ** rather than the complete command, an error message appears.
- CSCsr53347—You cannot add a CIDS sensor using the controller GUI.
- CSCsr53558—Guest user creation allows the user to select any WLAN.
- CSCsr55816—The controller might reboot due to a software failure of emWeb timer cb: 0x102265dc ('mmMipResendTimeout+476') on the instruction located at: 0x3 (Unknown).
- CSCsr62942—Controllers running software release 4.2.112.0 might reboot due to a problem with the EAP framework.
- CSCsr67780—When RLDP is enabled on a 4402 controller running software release 4.2.130.0, the following error message appears with tracebacks:


```
apf_rogue_detect.c:593 APF-1-AUTHMOBILE_SEND_FAILED: Could not send
the LWAPP Authenticate Mobile command to rogue AP xx:xx:xx:xx:xx:xx for mobile
xx:xx:xx:xx:xx:xx. Unable to find rogue client.
- Traceback: 100f342c 100f4f94 103d409c 10b955a8 10d4ec6c
```
- CSCsr74598—6 dB should be added to RSSI reports for 1250 series access points using 2.4 GHz.
- CSCsr86536—After a random period of operation, a 1000 series access point stops accepting new clients.
- CSCsr94483—The controller GUI allows you to add a mobility group member with a blank group name. It shows the name as “local” when it should show the local mobility group name instead.
- CSCsr97220—Different error messages appear on the controller GUI and CLI while a configuration file is being downloaded. The GUI shows “Error while downloading the configuration file. Hint: Please specify the encryption key if the file was encrypted” while the CLI shows “File is not intended for this product!”
- CSCsr97877—If the configured power for the interface on a 1250 series access point is low, then the power settings used to send the maximum power neighbor discovery packet are likely to be incorrect.

- CSCsu02354—A 4400 series controller might crash when it attempts to authenticate a client using EAP-TLS.
- CSCsu04193—The subnet mask for the IP address in the SNMP community is inverted in the value for the controller while the one in the WCS database for the controller is correct.
- CSCsu05190—The AP-manager does not reply with the correct destination MAC address with GARP. As a result, access points cannot join the controller after a failover from the primary firewall to the secondary firewall.
- CSCsu08222—The WLAN override configuration should list the WLAN profile on the controller GUI.
- CSCsu27939—Controllers running software release 4.2.130.0 might reboot because of a software failure of usmWebRRMRadSlotNoiseChannelGetNext+64.
- CSCsu44970—A 1230 series access point might stop accepting clients. After some hours of operation, the access point can beacon and answer probe requests, but it does not transmit unicast traffic to the client, so the client becomes stuck in the 802.11 authentication state and never proceeds to the association state.
- CSCsu56269—A Cisco WiSM running software release 4.2.130.0 might reboot because of a software failure of the radiusTransportThread task on the instruction located at 0x10c1a820 (ber_int_sb_write+361384).

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>

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2008 Cisco Systems, Inc. All rights reserved.