Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 5.1.163.0

February 2, 2009

These release notes describe open and resolved caveats for software release 5.1.163.0 for Cisco 2100 and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSM); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; Cisco 3201 Wireless Mobile Interface Cards (WMICs); and Cisco Aironet 1100, 1130, 1200, 1230AG, 1240, 1250, 1300, and AP801 Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.

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

Contents

These release notes contain the following sections.

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

Cisco Unified Wireless Network Solution Components

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

- Software release 5.1.163.0 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 3.0
- Cisco Wireless Control System (WCS) software release 5.1.65.4
- Cisco WCS Navigator 1.3.65.4
- Location appliance software release 5.1.30.0
- Cisco 2700 Series Location Appliances
- Mobility service engine software release 5.1.35.0 and Context Aware Software

Note Client and tag licenses are required to retrieve contextual (such as location) information within the Context Aware Software. See the *Release Notes for Cisco 3350 Mobility Services Engine for Software Release 5.1.35.0* for more information.

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

Note The 5.2.163.0 release does not support the NM-AIR-WLC6 platform.

- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1100, 1130, 1200, 1230AG, 1240, 1250, 1300, and AP801 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 Cisco Aironet 1000 series access points are not supported for use with controller software release 5.0.148.0 or later.

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 5.1.163.0 if you have mesh access points in your network. If your network uses mesh access points, use only mesh-specific releases such as 4.1.192.22M.

Note Cisco WCS software release 5.1.64.0 may be used to manage both mesh and non-mesh controllers (for example, controllers running software release 5.1.163.0 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.

MIB Files

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

Software Release Information

Software is factory installed on your controller and automatically downloaded to the access points after a release upgrade and whenever an access point joins a controller. As new releases become available for the controllers and their access points, consider upgrading.

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

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

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

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

Note The 2112 and 2125 controllers are supported for use with only software release 5.1.151.0 or later.

Finding the Software Release

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

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 5.1.163.0 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 problem.

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 5.1.163.0

Caution Before upgrading your controller to software release 5.1.163.0, you must comply with the following rules.

- Make sure you have a TFTP or FTP server available for the software upgrade. Keep these guidelines in mind when setting up a TFTP or FTP server:
  - Controller software release 5.1.163.0 is greater than 32 MB; therefore, you must make sure that your TFTP server supports files that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd and the TFTP server within the WCS. If you attempt to download the 5.1.163.0 controller software and your TFTP server does not support files of this size, the following error message appears: "TFTP failure while storing in flash."
  - If you are upgrading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.
- You can upgrade or downgrade the controller software only between two releases. To upgrade or downgrade beyond two releases, you must first install an intermediate release. For example, if your controller is running a 4.2, 5.0, or 5.1 release, you can upgrade your controller directly to software release 5.1.163.0. If your controller is running a 3.2, 4.0, or 4.1 release, you must upgrade your controller to an intermediate release prior to upgrading to 5.1.163.0. Table 1 shows the upgrade path that you must follow before downloading software release 5.1.163.0.

Table 1 Upgrade Path to Controller Software Release 5.1.163.0

Current Software Release	Upgrade Path to 5.1.163.0 Software
3.2.78.0 or later 3.2 release	First upgrade to 4.0.155.5 and then upgrade to a 4.2 release before upgrading to 5.1.163.0.
4.0.155.5 or later 4.0 release	Upgrade to a 4.2 release before upgrading to 5.1.163.0.
4.1.171.0 or later 4.1 release	Upgrade to a 4.2 or 5.0 release before upgrading to 5.1.163.0.
4.2.61.0 or later 4.2 release	You can upgrade directly to 5.1.163.0.
5.0.148.0 or later 5.0 release	You can upgrade directly to 5.1.163.0.
5.1.151.0	You can upgrade directly to 5.1.163.0.

Note When you upgrade the controller to an intermediate software release, wait until all of the access points joined to the controller are upgraded to the intermediate release before you install the 5.1.163.0 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 this 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 4.2.112.0 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.

Note The 4.2.112.0 ER.aes file was released after the 5.0.148.0 ER.aes file, so the 4.2.112.0 ER.aes file is the latest boot software file and as such contains the CSCsd52483 fix included in the 5.0.148.0 ER.aes file.

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.

Note Do not install the 5.1.163.0 controller software file and the 4.2.112.0 ER.aes boot software file at the same time. Install one file and reboot the controller; then install the other file and reboot the controller.

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

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

Step 2 Follow these steps to obtain the 5.1.163.0 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. through n. to download the remaining file (either the 5.1.163.0 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 or FTP server.

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

Step 5 Disable any WLANs on the controller.

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

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

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

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

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

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

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

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

a. In the Server Login Username field, enter the username to log into the FTP server.

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

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

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

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

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

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

Step 18 After the controller reboots, repeat Step 6 to Step 17 to install the remaining file (either the 5.1.163.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 ER.aes file).

Step 19 Re-enable the WLANs.

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

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

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

Step 23 To verify that the 5.1.163.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 24 To verify that the Cisco Unified Wireless Network Controller Boot Software 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 4.2.112.0 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.

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.

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.

Messages Appearing Upon Controller Bootup

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

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

Web Authentication Redirects

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

Using WLAN Override with IPv6

At this time, the controller software does not provide full support of the IPv6 and DHCPv6 stack. If you enable WLAN override with IPv6, the clients move to the correct VLAN but do not obtain an IPv6 address using DHCP (CSCsv79914). However, static IPv6 addresses operate correctly with the WLAN override feature.

PLM Location Commands

The **config**, **show**, and **debug location plm** path loss measurement location commands are not supported in controller software release 5.1.163.0, although they appear in the CLI code.

Cisco 1250 Series Access Points and Cisco 7920 IP Phones

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

Crash Files for 1250 Series Access Points

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

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

Configuration File Stored in XML

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

Note You cannot download a binary configuration file onto a controller running software release 5.1.163.0. Also, do not attempt to make changes to the configuration file. If you do so and then download the file to a controller, the controller displays a cyclic redundancy checksum (CRC) error while it is rebooting and returns the configuration parameters to their default values.

LWAPP Mode Changes

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

If you downgrade from controller software release 5.1.163.0 or 5.0.148.0 to 4.2.61.0 or an earlier release, the LWAPP mode changes from Layer 3 to Layer 2. Access points may not join the controller, and you must manually reset the controller to Layer 3 to resolve this issue.

Access Points Send Multicast and Management Frames at Highest Basic Rate

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

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

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

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

Disabling Radio Bands

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

40-MHz Channels in the 2.4-GHz Band

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

Impact of External Antenna Gain on Transmit Power

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

Supporting Oversized Access Point Images

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

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

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

Follow these steps to perform the TFTP recovery procedure.

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

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

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

Multicast Queue Depth

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

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

MAC Filtering for WGB Wired Clients

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

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

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

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

CKIP Not Supported with Dynamic WEP

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

Setting the Date and Time on the Controller

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

Synchronizing the Controller and Location Appliance

For controller software release 4.2 or later, if a location appliance (release 3.1 or later) is installed on your network, the time zone must be set on the controller to ensure proper synchronization between the two systems. Also, Cisco highly recommends that the time be set for networks that do not have location appliances. Refer to Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 5.1* for instructions for setting the time and date on the controller.

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

FCC DFS Support on 1130 Series Access Points

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

Inaccurate Transmit Power Display

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

Setting the Retransmit Timeout Value for TACACS+ Servers

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

Configuring an Access Point's Prestandard Power Setting

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

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

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

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

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

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

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

Controller Functions that Require a Reboot

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

- 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**}

2106 Controller LEDs

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

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

Rate-Limiting on the Controller

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

Pings Supported to the Management Interface of the Controller

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

Pinging from a Network Device to a Controller Dynamic Interface

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

GLBP Not Supported

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

IPSec Not Supported

Software release 5.1.163.0 does not allow you to choose IPSec as a Layer 3 security option. None and VPN Passthrough are the only available options. If you upgrade to this release from a previous release that supported IPSec as a Layer 3 security option, any WLANs that are configured for this feature become disabled. If you want to configure IPSec, you must use a version of controller software prior to 4.0.

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

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

Connecting 1100 and 1300 Series Access Points

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

Preventing Clients from Accessing the Management Network on a Controller

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

Voice Wireless LAN Configuration

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

Changing the IOS LWAPP Access Point Password

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

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

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

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

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

“ERROR!!! Command is disabled.”

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

Exclusion List (Blacklist) Client Feature

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

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

RADIUS Servers and the Management VLAN

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

RADIUS Servers

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

Management Usernames and Local Netuser Names

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

802.1X and Microsoft Wireless Configuration Manager

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

Using the Backup Image

The controller bootloader stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the bootloader to boot with the backup image.

With the backup image stored before rebooting, be sure to choose **Option 2: Run Backup Image** from the boot menu to boot from the backup image. Then upgrade with a known working image and reboot the controller.

Home Page Retains Web Authentication Login with IE 5.x

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

Rogue Location Discovery Protocol (RLDP)

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

AdHoc Rogue Containment

Client card implementations may mitigate the effectiveness of adhoc containment.

Changing the Default Values of SNMP Community Strings

The controller has commonly known default values of "public" and "private" for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.1* for configuration instructions.

Changing the Default Values for SNMP v3 Users

The controller uses a default value of "default" for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.1* for configuration instructions.

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

Features Not Supported on 2100 Series Controllers

This hardware feature is not supported on 2100 series controllers:

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

These software features are not supported on 2100 series controllers:

- VPN termination (such as IPSec and L2TP)
- Termination of guest controller tunnels (origination of guest controller tunnels is supported)
- External web authentication web server list
- Spanning tree
- Port mirroring

- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)
- Multicast-unicast mode

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

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

2106 Image Not Supported for 3504 Controllers

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

Running a 3504 Image on a 2106 Series Controller

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

Upgrading External Web Authentication

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

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

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

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

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

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

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

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

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

function loadAction(){
     var url = window.location.href;
     var args = new Object();
     var query = location.search.substring(1);
     var pairs = query.split("&");
     for(var i=0;i<pairs.length;i++){
          var pos = pairs[i].indexOf('=');
          if(pos == -1) continue;
          var argname = pairs[i].substring(0,pos);
          var value = pairs[i].substring(pos+1);
          args[argname] = unescape(value);
     }
     //alert( "AP MAC Address is " + args.ap_mac);
     //alert( "The Switch URL is " + args.switch_url);
     document.forms[0].action = args.switch_url;

     // This is the status code returned from webauth login action
     // Any value of status code from 1 to 5 is error condition and user
     // should be shown error as below or modify the message as it suits
     // the customer
     if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your
part.");
     }
     else if(args.statusCode == 2){
        alert("You are not configured to authenticate against web portal. No further
action is required on your part.");
     }
     else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the user is
already logged into the system?");
     }
     else if(args.statusCode == 4){
        alert("Wrong username and password. Please try again.");
     }
     else if(args.statusCode == 5){
        alert("The User Name and Password combination you have entered is invalid.
Please try again.");
     }

}

</script>
```

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

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

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

<tr align="center">

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

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

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

Caveats

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

Open Caveats

These caveats are open in controller software release 5.1.163.0.

- CSCsb77595—When you log out from Telnet/SSH sessions, the session prompts you to save changes, even if you have made no changes.

  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.

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

  Workaround: Use a wireless sniffer trace.

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

  Workaround: Do not directly change from WPA1+WPA2+conditional web redirect to 802.1X+conditional web redirect. Instead, follow these steps:

  a. Remove conditional web redirect and save your change.
  b. Change 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**.

- 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.

- CSCsi17242—If a controller starts a timer (such as reauthentication or keylife time) after running for approximately 52 days, the timer might take a long time to fire (up to another 52 days).

  Workaround: Clean up the timers. If the problem is related to the client, deauthenticate the client to clean the timer. If the problem is related to the WLAN, such as a broadcast key update, disable and then re-enable the WLAN.

- CSCsi26248—After a failed link aggregation (LAG) link recovers, you might lose connectivity for approximately 30 seconds.

  Workaround: Recover the LAG link when service is not in use. You might also want to consider not using this type of configuration.

- CSCsi27596—The controller lacks a supported way to configure the broadcast key rotation interval. Instead, it is hardcoded to a group key rotation interval of 3600 seconds (1 hour).

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

  Example:

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

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

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

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

  Workaround: None.

- CSCsi54588—Some 802.1X controller error messages have inadequate descriptions or incorrect severities. In particular, the following messages, which can be caused by an incorrectly configured client, have a severity of 1 but should have a severity of 3. Because they are severity 1, they are logged even when the logging level is set to Critical. These messages can be generated repeatedly when clients are configured with incorrect credentials.

  ```
  DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE
  DOT1X-1-ABORT_AUTH
  ```

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

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

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

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

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

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

- CSCsi73129—You cannot upgrade a controller using TFTP through a client device that is associated to the controller.

  Workaround: The TFTP server must be located on a client that is not associated to the controller.

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

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

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

  Workaround: None.

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

  Workaround: None.

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

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

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

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

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

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

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Enter a valid netmask.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: None.

- 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
```

  Workaround: After you confirm that the cause is not a spoofing attack from a rogue access point, disable and then re-enable the access points identified in the messages. If the problem persists, disable MFP validation on some of the access points, or disable infrastructure MFP globally.

- 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.

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

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

- CSCsl33441—You cannot use the controller GUI to change the syslog filter level.

  Workaround: Use the controller CLI.

- 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.

- 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.

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

  Workaround: None. This issue appears to be cosmetic.

- 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: Make sure the client is using 802.11n rates.

- 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 fail to obtain an IP address if DHCP proxy is disabled.

  Workaround: Do not disable DHCP proxy.

- 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.

- CSCsm04752—The GUI of an anchor controller shows a wired client as mobile rather than as 802.3.

  Workaround: None.

- CSCsm05607—Large user packets may 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 there is an IOS router in the IP path used by the IP endpoints, use **ip tcp adjust-mss 1300** or a similar command to get the endpoints to 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 translations, 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.

- 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.

  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: Follow these steps:

  a. Determine whether you want to force your wireless clients to perform DHCP first, after associating, before they can send IP packets.
     - If you do, then disable DHCP Required, and you will not encounter this problem.
     - If you do not, then configure all clients to use DHCP.

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

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

  Workaround: None.

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

  Workaround: None.

- CSCsm40870—The following error message should be reworded:

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

  The message should read as follows:

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

  Workaround: None.

- CSCsm47699—The AP Manager Interface IP Address prompt in the configuration wizard generates an “Invalid Response” message instead of returning to the previous prompt as expected.

  Workaround: Finish the configuration and correct the DHCP server IP address during regular operation.

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

  Workaround: Create an access list with rules.

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

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

  Workaround: None.

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

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

  Workaround: None.

- CSCsm78257—Some workgroup bridge clients fail to associate if the WPA information element (IE) is different in the probe response and the associate response packets. This issue occurs only when WPA TKIP and AES and WPA2 TKIP and AES are all enabled.

  Workaround: If TKIP and AES are not both required for WPA and WPA2, then only enable them for the WPA version for which they are needed.

- 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.

- CSCsm83093—If client management frame protection (MFP) is disabled after a client successfully associates using WPA2 with AES-CCMP and client MFP, the client cannot reassociate.

  Workaround: Reboot the controller. It might also be possible to recover by disabling and then re-enabling the wireless interface (not just the radio) on the client.

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

  Workaround: None.

- 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.

- CSCso02714—The throughput is sometimes low for 4400 series anchor and foreign controllers using symmetric mobility tunneling and link aggregation (LAG).

  Workaround: None.

- CSCso03704—The Trap Receiver Name column on the SNMP Trap Receiver page of the controller GUI should be changed to "SNMP Community String" because the existing title does not adequately describe the field.

  Workaround: None.

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

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

- CSCso06889—The controller allows you to delete an LDAP server that is configured as a web authentication LDAP server on a WLAN.

  Workaround: Before you delete an LDAP server, make sure that it is not configured on any WLAN.

- 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.

- CSCso10043—When you add a RADIUS server on a controller, enable IPSec, apply the changes, then disable IPSec, apply the changes, and save the configuration, the controller sometimes indicates after a reboot that there are unsaved changes to the configuration.

  Workaround: None.

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

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

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

  Workaround: Use the controller CLI to display users.

- CSCso25781—IP connectivity is sometimes lost to a Cisco WiSM controller through either the service port or management interface. Console access continues to function, but no access point or user traffic can flow. This issue seems to be affected by the number of dynamic interfaces that have been created on the controller.

  Workaround: None. However, entering the **reset system** CLI command on the Cisco WiSM recovers IP traffic flow.

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

  Workaround: Connect to the access point locally.

- 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 or later, any hybrid-REAP groups configured on the controller are lost after the downgrade.

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

- CSCso33631—The Multicast Groups page on the controller GUI shows the correct multicast group IDs (MGIDs) for up to 20 client devices but shows incorrect MGIDs for any additional clients.

  Workaround: Use the **show network multicast mgid details** *mgid* CLI command to view MGIDs.

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

  Workaround: None.

- CSCso39413—Constant access control list (ACL) messages appear in the controller logs even though no ACLs are configured.

  Workaround: None.

- CSCso52140—If the controller is configured for WPA2, the RSN capability within the RSN information contains a PMK identifier (PMKID) count within all probe responses. However, the PMKID count should be used only in the RSN information element in re-association request frames to an access point.

  Workaround: Ignore the PMKID count within the RSN capability.

- CSCso52225—The output of the **show run-config** CLI command always shows the following parameters. It should show the parameters in use per queue based on the actual configuration.

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

  Workaround: None.

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

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

- CSCso59323—When you configure a WLAN with Layer 2 security WPA+WPA2 and PSK authentication with an ASCII key, the controller template in WCS shows the key as hexadecimal.

  Workaround: None.

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

  Workaround: None.

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

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

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

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

- CSCso66183—When more than 100 Symbol Vocollect devices are in a small area, they might disassociate from 1242 series access points with 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"
  ```

  Workaround: Manually power cycle the access points.

- CSCso66504—The controller and WCS both show management frame protection (MFP) for a wired LAN, even though MFP is not supported for use with wired LANs.

  Workaround: None.

- CSCso69005—After **config paging disable** is entered to disable page scrolling, the **show acl summary** and **show acl detailed** *acl_name* commands still show a "paging" prompt, which could break customer scripts.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCso79074—If a 1250 series access point receives a DHCP offer, the sniffer shows that the access point gets multiple DNS servers in the offer, but the access point broadcasts 255.255.255.255 when trying to resolve DNS.

  Workaround: Configure option 43 for the access point to join the controller.

- CSCso87175—SNMP support is needed to enable or disable DHCP proxy from WCS.

  Workaround: Configure DHCP proxy using the controller CLI command **config dhcp proxy** {**enable** | **disable**}.

- CSCso93918—NPU rate-limiting functions inconsistently because BSN_PKT_LEN is incorrect for certain types of packets.

  Workaround: Use ACL filtering to prohibit certain types of packets.

- CSCso98358—If you make an error when entering a command, the **config paging enable** CLI command is executed.

  Workaround: Disable paging again using the **config paging disable** CLI command.

- CSCsq01190—When the controller is running software release 5.0.148.0, the link test for the associated wireless client might fail on both the controller GUI and CLI.

  Workaround: Downgrade the controller to software release 4.2.

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

  Workaround: None.

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

  Workaround: None.

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

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

- CSCsq09933—After you use LWAPP conversion tool 3.2 to convert access points with a static IP address that have either SSCs or MICs, the access points seem to ignore the DNS resolution of cisco-lwapp-controller after already downloading the full image from the controller.

  Workaround: Let the access point use DHCP for its IP address. If you have other access points already joined, you can use over-the-air provisioning (OTAP) to prime the access point with static entries.

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

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

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

  Workaround: Change the IP address of the management interface.

- CSCsq14961—SNMP returns only one record for client roam reports whereas the controller CLI shows multiple records.

  Workaround: Use the controller CLI to view multiple entries.

- CSCsq15645—When you use the controller GUI to change DTPC support for a network, the access point radios are reset without any notification. If you use the controller CLI, you are prompted that the network has to be disabled before the change can be applied.

  Workaround: Use the controller CLI.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Use the controller CLI.

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

  Workaround: None.

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

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

  Workaround: None.

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

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

- CSCsq25029—A 2106 controller running software release 4.2.112.0 might reboot because of a software failure of the bcastReceiveTask.

  Workaround: None.

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

  Workaround: None.

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

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

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

- CSCsq25762—Currently the EAPOL-Key timeout can be configured only in seconds, but the capability to reduce this timeout is needed.

  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.

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

  Workaround: Authenticate the clients using another WLAN.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Reset the controller.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Use a Windows 2000 DHCP server.

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

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

- CSCsq49514—A duplex mismatch between the 2106 controller and the switch prevents the controller from connecting to the network.

  Workaround: Correct the duplex mismatch.

- CSCsq49831—A core dump should be created when the controller crashes to aid in debugging.

  Workaround: None.

- CSCsq55033—The AAA-1-INVALID_AUTHENTICATOR and other controller AAA messages are not documented or documented inadequately.

  Workaround: None.

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

  Workaround: None.

- CSCsq56139—If you configure the controller to send only access point register traps, the controller still sends client traps.

  Workaround: None.

- CSCsq58843—A 4400 series anchor controller cannot ping Ethernet-over-IP (EoIP) roamed clients.

  Workaround: None.

- 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.

  Workaround: None.

- CSCsq61533—SNMP can be used to set a blank access point username on a controller running software release 5.0.148.0.

  Workaround: None.

- CSCsq63937—When you enter the **transfer download mode ftp** CLI command, the value for the SNMP object agentTransferUploadMode is missing from snmpwalk.

  Workaround: Set the transfer download mode to TFTP using the **transfer download mode tftp** CLI command.

- CSCsq65563—A software watchdog needs to be implemented on the Controller Network Module in order to allow the controller to be rebooted in the event of a system freeze.

  Workaround: None.

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

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

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

  Workaround: None.

- CSCsq69712—A 2100 series controller might reboot while you are browsing the Monitor section of the controller GUI.

  Workaround: None.

- CSCsq73427—You cannot enable network admission control (NAC) on the management interface of a Controller Network Module using the controller GUI.

  Workaround: Use the controller CLI to enable NAC.

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

  Workaround: None.

- CSCsq74318—The controller GUI accepts more characters in web authentication messages than the controller CLI. If the web authentication message is longer than 130 characters, the following error message appears in the controller log when you enter the **show custom-web all** CLI command: "CLIWEB-3-BUFFER_TOO_SMALL: Buffer for Customization message too small."

  Workaround: Disregard the error, or use a custom web authentication bundle.

- CSCsq74459—Buffer corruption errors similar to the following might appear in the controller message log:

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

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

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

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

- CSCsr02316—Some SNMPSet operations appear to be successful even though the controller is truncating the string.

  Workaround: Set a shorter value for the SNMP string.

- CSCsr09192—The FTP username and password are limited to 24 characters each; however, the controller GUI and CLI state that up to 31 characters are allowed.

  Workaround: Do not enter more than 24 characters for the username and password.

- CSCsr12961—The controller CLI help syntax should specify the possible values for the *mode* parameter in the **config 802.11h channelswitch enable** *mode* CLI command.

  Workaround: None.

- CSCsr16752—The Controller Network Module NM-AIR-WLC6 might experience interface flapping after the interface is reset.

  Workaround: None.

- CSCsr18797—If you configure the controller for an external RADIUS server and create a WLAN with WPA2 and local authentication enabled, clients authenticate using local authentication. However, if you then switch the configuration to the RADIUS server, it might take several minutes for the client authentication to switch back to the external RADIUS server.

  Workaround: None.

- CSCsr20151—If you attempt to change the power level for the 5-GHz radio in a 1250 series access point, the change does not take effect.

  Workaround: Enable 802.11n for the 802.11a radio.

- CSCsr23785—When an access point joins a different controller in the same mobility group that has a different WLAN ID for the same WLAN profile and SSID, the information that appears in the access point WLAN override list is wrong.

  Workaround: None.

- CSCsr27851—If you add a controller to WCS and then create a diagnostic-channel WLAN on the controller, an SNMP error appears even though the template is pushed to the controller.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None. Re-enter the access point credentials.

- 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 a period equivalent to the configured user idle timeout. This problem occurs if you click **Edit All** on the controller GUI to update the mobility members.

  Workaround: Delete the mobility members and re-add them, or reboot all of the controllers after upgrading them to software release 4.2.112.0.

- CSCsr44439—The web authentication page does not load on the browser when a client connects through a wired guest VLAN on a controller running software release 4.2.130.0 or 5.0.148.2.

  Workaround: None.

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

  Workaround: Configure the clients with a static IPv6 address.

- CSCsr46119—The radio transmit queue buffer of a 1250 series access point locks up when transmitting with medium to heavy traffic.

  Workaround: None.

- CSCsr46256—If an association request contains TSPEC and SFA information elements (IEs), the access point sends an association response with only a TSPEC IE. The SFA IE is missing.

  Workaround: None.

- CSCsr46795—When MSE SSL verification fails on the controller, the RADIUS server log contains MSE authentication failures. The MAC address is inaccurately logged for the MSE instead of the controller.

  Workaround: None.

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

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

- CSCsr53764—Some wired workgroup bridge (WGB) clients might randomly become stuck at specific access points while roaming.

  Workaround: Reload the WGB, enter the **clear bridge** command on the WGB, or wait for the WGB to roam back to the old access point at which it is stuck.

- CSCsr58532—This message sometimes appears on 2106 controllers: "SIM-3-INTFGET_GIG_ETH_FAIL: Failed to get the interface number of the Gigabit Ethernet Port."

  Workaround: Cisco 2106 controllers do not contain a Gigabit Ethernet port, so you can safely ignore this message.

- CSCsr59986—Access points are able to serve clients on radar-detected channels even though the channels are in a radar non-occupancy period.

  Workaround: None.

- CSCsr72091—The radio resource management (RRM) feature on a controller running software release 4.1.130.0 does not provide consistent results from coverage hole events and channel assignment.

  Workaround: None.

- CSCsr78181—When a controller running software release 5.1 boots up, you can press **ESC** for more options. Password recovery should be an option, but it is not.

  Workaround: Use the proper password recovery procedure. Follow the instructions in the "Restoring Passwords" section in Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 5.1*.

- CSCsr83671—When radio resource management (RRM) is configured for medium or low sensitivity, the auto-RF dynamic channel assignment feature sometimes sets many access points to the same channel.

  Workaround: Change the RRM sensitivity level to high.

- CSCsr83684—When you enable link aggregation (LAG), 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—Cisco WiSM controllers running software release 4.2.130.0 generate trap logs indicating that the control path between two random mobility members is down. About 10 to 20 minutes later, the control path comes back up.

  Workaround: Disable guest tunneling.

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

  Workaround: Manually delete the client entry from the anchor controller.

- CSCsr91361—The List of Access Point Models and Protocols Supported Per Country and Regulatory Domain link on the Country GUI page of a controller running software release 5.1.151.0 is broken. Clicking this link returns a "Page not available" error.

  Workaround: None.

- CSCsr95295—The controller CLI allows you to disable all legacy data rates and with the network still enabled. This is an invalid configuration that disables the network.

  Workaround: Enable at least one legacy data rate.

- CSCsr97110—After you download an XML configuration file, a 4400 series controller running software release 5.1.151.0 might reboot continuously.

  Workaround: Clear the configuration and then reconfigure the controller.

- CSCsu04265—When you enter the **transfer download datatype eapcacert** controller CLI command, 2100 series controllers report that the data type is invalid, and 4400 series controllers report that the data type is unassociated.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

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

- CSCsu40636—The access point sometimes ignores the CTS duration when receiving U-APSD trigger frames and simply transmits.

  Workaround: None.

- CSCsu42414—The **show client ccx rm** *mac_address* **pathloss** CLI command does not provide information about the pathloss reports sent by the client.

  Workaround: None.

- CSCsu44722—If you try to enable IPv6 for a mobility-anchor-enabled WLAN, an invalid error message appears.

  Workaround: Do not attempt to enable IPv6 on a mobility-anchor-enabled WLAN.

- CSCsu46184—Snmpwalks fail to an SNMP v3 user configured on a 4.2.154.0 controller using MD5/DES or SHA/DES.

  Workaround: None.

- CSCsu50080—When you configure web authentication passthrough with email input on the controller, the controller allows any text to be entered. This feature implies that a client should have to enter an email address before proceeding. Although there is no way to verify that the email is valid, the controller should at least verify that it follows this format: *name@company.com*.

  Workaround: None.

- CSCsu52247—When a client roams from one controller to the other, tracebacks might appear on the anchor controller. This problem occurs for Cisco WiSM controllers running software release 5.1.151.0.

  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 problem can be serious when the access point is running a recovery image such as 12.3(11)JX1, which does not drop LWAPP data packets. If the number of data packets sent to the access point before it loads the full image is large enough, the access point locks up and fails to join the controller.

  Workaround: Change the multicast mode to multicast or disable multicast. For access point join issues, load recovery image 12.4(10b)JA3 on the access point, load the full LWAPP image on the access point, and disable multicast-unicast on the controller.

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

  Workaround: None.

- CSCsu54884—An ad-hoc rogue access point marked “Internal” on the controller is not trackable. You cannot see the rogue access point anywhere in the configuration of the controller.

  Workaround: None.

- CSCsu57111—The following tracebacks might appear in the controller message logs: “apf_foreignap.c:1292 APF-1-CHANGE_ORPHAN_PKT_IP: Changing orphan packet IP address for station00:11:22:33:44:55 from x.x.x.x --->y.y.y.y- Traceback: 100cd4c0 100cddd0 100e40a8 10409864 10c064cc 10d748d8.”

  Workaround: None.

- CSCsu57342—Join statistics for 1240 series access points are not available.

  Workaround: None.

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

  Workaround: Try to upload the logo, or try to unconfigure the custom logo.

- CSCsu61354—When you attempt to set MAC filters on the controller from WCS, an error message appears indicating that the MAC address cannot be set because it already exists in the database. The error message should indicate that the MAC address is already associated by Auth-list.

  Workaround: Enter **config auth-list delete** *mac_address* and **config macfilter** *mac_address* using the controller CLI. Then enter **show mac-filter** to see the newly created MAC address.

- CSCsu63676—An SNMP query on the agentInterfaceName SNMP variable sometimes creates a loop.

  Workaround: None.

- CSCsu68010—When you downgrade the controller from software release 5.1.151.0 to 4.2.130.0, the LWAPP mode automatically changes from Layer 3 to Layer 2, and the AP-manager disappears.

  Workaround: Configure Layer 3 mode on the downgraded controller and reboot the controller.

- CSCsu71747—On a Catalyst 3750G Wireless LAN Controller Switch running software release 5.1.151.0, the integer value returned by the SNMP object ifNumber is 2, but IfIndex actually returns three indexes.

  Workaround: None.

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

  Workaround: None.

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

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

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

  The correct output should be:

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

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

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

  The correct output should be:

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

  Workaround: None.

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

  Workaround: None.

- CSCsu84498—The transmit diversity for multicast or broadcast packets should alternate on a 1240 series access point’s antenna ports.

  Workaround: None.

- CSCsu84629—A 1250 series access point changes from maximum uniform transmit power back to maximum transmit power, resulting in a 3 to 6-dB error potential in transmit power control algorithms.

  Workaround: None.

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

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

- CSCsu88885—When **debug locp interface events** is enabled, the **debug disable** command does not disable the debug.

  Workaround: Use the **debug dot11 locp disable** command.

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

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

  Workaround: None.

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

  Workaround: Clear the configuration and reconfigure the controller.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Clear the controller configuration and reconfigure the controller.

- CSCsu92667—The controller might reboot after you make changes 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 this controller as an anchor for a WLAN that does not exist, create that WLAN and then overwrite the WLAN and remove its anchors. Then you can remove the controller from the mobility group.

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

  Workaround: Enable paging or use a Telnet session.

- CSCsv12308—Access points do not join the controller when there is a change in the MAC address of the default gateway but the IP address remains the same.

  Workaround: Change the default gateway on the AP-manager interface to some other IP address; then change the interface back to the correct IP address.

- CSCsv13068—The Authenticator field in an access-request sent from the controller to the RADIUS server is set to all zeros.

  Workaround: None.

- CSCsv14863—A controller running software release 4.2.130.0 might send a channel assignment of 0 and a power level of 0 to 1242 access points.

  Workaround: Reapply the auto-RF settings.

- CSCsv18730—The controller sends a unicast ARP to the default gateway every 5 to 7 seconds instead of using the configured ARP timeout value.

  Workaround: None.

- CSCsv19291—When you are configuring the controller, WCS reports in alarms that the access point interface is down. WCS does not sufficiently indicate that these alarms are meant to inform users of access point radio status and are caused by the user during configuration.

  Workaround: None.

- CSCsv21872—When a client associates to a WPA WLAN and does not have the correct security parameters (for example, the client is configured with the correct SSID but with static WEP instead of WPA-PSK or 802.1X), the controller generates this error message:

  ```
  %APF-1-PROC_RSN_WARP_IE_FAILED: apf_80211.c:2197 Could not process the RSN and WARP
  IEs. station not using RSN (WPA2) on WLAN requiring RSN.MobileStation:
  00:40:96:a1:4a:f6, SSID:RSN,AP: 00:1c:f9:05:92:80.
  ```

  The SSID: RSN incorrectly implies that WPA2 is being used when it is not.

  Workaround: None.

- CSCsv23643—When you configure a WLAN with WPA2+802.1X and an infinite session timeout, any client that connects to a 5.1.151.0 controller actually has a session timeout of approximately 11.6 hours.

  Workaround: Configure a manual session timeout of up to 1 day, or enable AAA override and set the timeout attribute to a large value from the RADIUS server.

- CSCsv35010—In 40-MHz mode, the controller GUI should not allow channel 11 to be set.

  Workaround: None.

- CSCsv35162—The controller displays “Request failed - Failed to add the IP into anchor list” on the CLI or “Failed to create anchor switch entry local” on the GUI when you try to configure a local controller as a mobility anchor controller.

  Workaround: None.

- CSCsv39373—When one access point takes over from another in fallback mode, client devices sometimes remain associated to the access point, but the controller does not recognize the association. The access point then sends a non-management frame protection (MFP) protected deauthentication or disassociation message.

  Workaround: Disable MFP client protection.

- CSCsv39950—Controllers running software release 4.2.130.0 sometimes reboot at apfMsCreateDeadlock+76 while configured for **debug pm ssh-engine enable**.

  Workaround: None.

- CSCsv43156—The trap for an unsuccessful login attempt contains the wrong IP address.

  Workaround: None.

- CSCsv47365—The controller control plane (Telnet, SSH, and GUI) sessions hang momentarily when you enter a link test command from the controller GUI or CLI.

  Workaround: Wait until the session is over before performing a link test.

- CSCsv49302—If the SSID interface is different from the management interface, the SSID interface changes to the management interface after the diagnostic channel is disabled.

  Workaround: None.

- CSCsv54436—When you use SSH to Telnet to a controller, the controller sometimes displays this message: "Sorry, telnet is not allowed on this port." However, if you retry the connection immediately, the controller accepts the connection. This defect sometimes affects monitoring tools that operate using SSH.

  Workaround: Retry the SSH connection when it fails.

- CSCsv56016—The 2106 controller sometimes incorrectly reports that the IP address of the syslog server is invalid.

  Workaround: None.

- CSCsv62706—When a client device performs a Layer 3 inter-controller roam, the client mobility state appears correctly as "foreign" but then changes incorrectly to "local." The client retains the IP address from the first controller and then is no longer able to pass traffic. If the client is rebooted, it authenticates and associates with no issue and obtains the correct IP address for a local mobility state.

  Workaround: Reboot the client device.

- CSCsv63732—Controllers sometimes display an error message in which the word "heartbeat" is misspelled.

  Workaround: None.

- CSCsv70556—On the controller GUI, you can create a new dynamic interface, assign a VLAN tag, and apply the interface settings. The controller warns that you also need to configure the netmask and IP address but still creates the interface, and it should not.

  Workaround: None.

- CSCsv74342—Clients associated to a diagnostic-channel WLAN cannot reach the default gateway management interface.

  Workaround: None.

- CSCsv74572—Controllers sometimes lose gateway access on a single VLAN. As a result, off-subnet hosts, such as DHCP servers, become unreachable for DHCP.

  Workaround: Configure link aggregation (LAG) or disconnect port 2 by shutting down its switch port.

- CSCsv76513—When you perform a wireless sniffer trace for a 2100 series controller, the same BSSID appears for the WLANs on both the 802.11a and 802.11b/g radios.

  Workaround: None.

- CSCsv79582—Controllers sometimes reboot because of a software failure of the SShpmMainTask task.

  Workaround: None.

- CSCsv79885—If you enter an incorrect mobility group name, you cannot use the Edit All feature to correct the group name for the members of the mobility group.

  Workaround: Delete the member and add it with the correct name.

- CSCsv84446—If you enter the **debug aaa all enable** CLI command during web authentication, the "Authentication failed for *user*" message appears even though the user was able to authenticate and pass traffic.

  Workaround: None.

- CSCsv84462—When you try to edit the parameters of a local network user from the controller GUI, the following error message appears: "Error in creating user."

  Workaround: Use the controller CLI to edit the local network user.

- CSCsv87385—The controller logs this message when the DHCP packet received on the interface does not contain any DHCP options:

  ```
  dhcpd.c:206 DHCP-3-MSGTAG095: Bad DHCP packet from <DHCP Server>, dropping
  ```

  Workaround: None.

- CSCsv91992—Controllers sometimes fail to remove DHCP option 82 from DHCP traffic sent from the server to the client.

  Workaround: None.

- CSCsv94146—Controllers sometimes reboot when external web authentication is used.

  Workaround: None.

- CSCsv94993—The static address learning capability sometimes fails when DHCP Required is configured for a WLAN.

  Workaround: Use a short DHCP lease. However, this approach sometimes results in some minutes of traffic loss.

- CSCsw17659—Controllers sometimes fail to reply to ARP requests.

  Workaround: None.

- CSCsw25810—When you attempt to configure a RADIUS server for a wired guest LAN using the controller GUI, a browser error might appear.

  Workaround: Use the controller CLI instead of the GUI.

- CSCsw26083—A hybrid-REAP access point should enter standalone mode immediately upon bootup. However, if the access point is configured for a DHCP IP address but the DHCP service is not available when the hybrid-REAP access point reloads, the access point never falls back to standalone mode.

  Workaround: None.

- CSCsw27841—Controllers sometimes allow you to configure multiple untagged VLAN interfaces on the same physical port, and they should not.

  Workaround: None.

- CSCsw28120—An access control list (ACL) fails to block traffic to the controller management IP address.

  Workaround: None.

- CSCsw29804—Frames from Lexmark printers come to the controller as DSAP: SNAP (0xaa), but the controller forwards them out the Ethernet port as DIX (Digital Intel Xerox). Because of this defect, Lexmark printers cannot have an apple ARP entry on Layer 3 routers and cannot join the Appletalk zone.

  Workaround: None.

- CSCsw30025—When you enter **show custom-web wlan** on the controller CLI, the controller sometimes reboots.

  Workaround: None.

- CSCsw35152—A Cisco WiSM running software release 4.2.176.0 might reboot because of a software failure of the osapiBsnTimer task.

  Workaround: None.

- CSCsw40239—Controllers sometimes disable the radio port on 1250 series access points.

  Workaround: Reboot the access point.

- CSCsw43518—When an access point is connected directly to a physical port on a controller and is using the controller's internal DHCP server, client devices associated to the access point sometimes fail to receive an IP address.

  Workaround: Connect the access point to a physical port on your network other than the ports on the controller.

- CSCsw44086—When the controller rotates the group key, client devices using static WEP are disconnected until they reboot or reassociate.

  Workaround: Increase the rotation interval for the group key from the default period, which is 63 minutes. Enter this command on the controller console (note that this command does not work when entered through a Telnet or SSH session):

  devshell dot1xUpdateBroadcastRekeyTimer *seconds*

  To set the interval to one day, enter 86400 seconds. This command does not become part of the configuration, so you must re-enter it if the controller reboots.

- CSCsw45913—The wrong access control list (ACL) is applied when the AAA override feature is enabled for ACLs.

  Workaround: Do not use the AAA override feature with ACLs.

- CSCsw46354—Tracebacks such as this one sometimes appear in the controller message log when you enable the Trace Info parameter:

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

  Workaround: Uncheck the **Trace Info** check box on the Syslog Configuration page of the controller GUI.

- CSCsw49530—If you misconfigure access point inline power settings (specifically configuring 802.3af negotiated connections on the controller as pre-standard), WCS can experience problems such as template apply failures and poor client tracking.

  Workaround: Change the configuration of the controllers to match the access points; then refresh the controller's configuration in WCS (with delete). Controller power settings for large numbers of access points can be corrected with these commands:

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

  config ap power injector {**disable** | **enable**} **all**

- CSCsw49636—Controllers sometimes reboot with nothing on the console. The crash file indicates that the reboot was caused by a software failure of the Reaper Watcher task.

  Workaround: None.

- CSCsw51183—When the WAN link to hybrid-REAP access points goes down, a 2106 controller might reboot because of a software failure of the spamReceiveTask task.

  Workaround: None.

- CSCsw51224—When the WAN link to hybrid-REAP access points goes down, a 2106 controller might reboot because of a software failure of the osapiBsnTimer task.

  Workaround: None.

- CSCsw51658—Cisco WiSM controllers with factory default settings sometimes fail to acquire an IP address.

  Workaround: None.

- CSCsw52884—Controllers sometimes reboot in the EAP framework.

  Workaround: None.

- CSCsw53035—When a controller sends a ping reply to a wireless client, the destination MAC address is the client MAC address. As a result, a Layer 3 switch cannot transfer the ping reply packet.

  Workaround: None.

- CSCsw59491—A controller might reboot on mobility anchor setup when link aggregation (LAG) is enabled.

  Workaround: None.

- CSCsw68923—HTTP requests sent by Cisco 7921 phones sometimes fail to access the Internet.

  Workaround: None.

- CSCsw75392—802.11n clients configured for WPA2-PSK (or WPA2-802.1X) can associate only at 802.11a/g data rates even though WPA2-AES was successfully negotiated by the client.

  Workaround: In the original WLAN profile, configure the security settings to use only WPA-TKIP and WPA-AES. Next, create a second WLAN profile. Using the same SSID, configure the security settings to use only WPA2-AES. Keep all other WLAN settings the same as the original WLAN profile. Both the legacy and the 802.11n clients should now be able to connect with the correct data rates and security profile.

- CSCsw79978—On the SNMP Trap Controls (Security) page on the controller GUI, the WEP Decrypt Error check box should be reworded because this setting also controls the SNMP decrypt error traps for WPA and WPA2. With the current wording, it is not clear whether this setting also disables the WPA decrypt traps.

  Workaround: None.

- CSCsw80153—When a RADIUS server is used for web authentication, the controller does not send RADIUS requests to any RADIUS server. The following message is logged from the **debug aaa all enable** command:

  ```
  Returning AAA Error 'No Server' (-7) for mobile
  ```

  Workaround: None.

- CSCsw83779—Symbol scanners (MC9090) fail to connect to a local EAP WLAN after an extended time. When this issue occurs, all clients are unable to successfully authenticate to the WLAN. Client IDs for the WLAN are created and deleted with authentication sessions, but not all IDs are deleted with failed authentications for Symbol scanners.

  Workaround: None.

- CSCsw84860—When you enter the **show 802.11b l2roam stat** CLI command in a Telnet or SSH session, the command output is improperly aligned and difficult to read.

  Workaround: Enter the command in a console session.

- CSCsw86749—When you upgrade a 4400 series controller to software release 5.1.151.0, irrelevant error messages like this one sometimes appear:

  ```
  Jan 06 08:35:08.785:%USMDB-4-MSGTAG027: usmdb_wcp.c:221 usmDbWcpGetParentRouterName():
  Non-Doberman platform.
  ```

  Workaround: None. You can safely ignore these messages.

- CSCsw87206—The service port interface must have an IP address on a different subnet from the management, AP-manager, and dynamic interfaces. The controller checks whether the IP address assigned to each interface is valid before the IP address setting is configured. However, this checking mechanism does not work when you change the subnet mask of each interface. As a result, the controller sometimes allows the service port interface to have an IP address on the same subnet as the other interface.

  Workaround: None.

- CSCsw88108—When you add a MAC address to the access point authentication list using SNMP, the controller allows uppercase characters. However, the controller should reject or convert addresses with uppercase letters as it cannot handle mixed case in the database.

  Workaround: Do not enter uppercase characters in the MAC address.

- CSCsw88545—The output of the **show client detail** *mac_address* CLI command is inconsistent for an EAP-FAST CCKM client. Sometimes the username is reported as "anonymous," and sometimes it shows the actual username configured on the device. If local authentication is used on the controller, the username is reported as "PEAP-*mac_address*."

  Workaround: None.

- CSCsw88727—When an unauthenticated wireless client changes IP addresses on a WLAN that has web authentication enabled, the controller sends level 1 syslog messages (immediate action required) to the syslog server. Here is a typical message:

  ```
  apf_foreignap.c:1285 Changing orphan packet IP address for station 00:23:32:xx:xx:xx
  from 192.168.X.Y --->192.168.X.Y
  ```

  Workaround: Change the open WLAN to WPA-PSK to prevent casual clients from trying a different IP address before obtaining an IP address on the open guest WLAN.

- CSCsw91395—"Trusted AP Missing or Failed" messages appear in the controller log even after you disable trusted access point alerts.

  Workaround: None.

- CSCsw92225—Controllers sometimes fail to forward broadcast traffic on UDP port 7013.

  Workaround: Enable multicast-multicast mode. Then change the setting back to multicast-unicast.

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

  Workaround: None.

- CSCsw97548—The controller might reboot because of a software failure of the osapiTimer task.

  Workaround: None.

- CSCsx04986—WCS might receive reports from the controller that a rogue access point is on the network, even though a rogue access point is not actually on the network.

  Workaround: None.

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

  Workaround: Reset the PC card on the client.

- CSCsx05975—When two wireless phones associate to the same access point and call each other, the controller does not allocate enough bandwidth in load-based call admission control (CAC).

  Workaround: None.

- CSCsx07480—A controller running software release 4.2.176.0 might experience a slow (1 MB per day) memory leak.

  Workaround: None.

- CSCsx07538—When a TCP connection is open to port 1000, the controller responds with a reset.

  Workaround: Create a CPU ACL to block TCP port 1000.

- CSCsx07878—Clients might be unable to log into a WLAN configured for web authentication.

  Workaround: Rebooting the controller might stop the problem temporarily.

- CSCsx08445—A Cisco WiSM running software release 4.2.130.0 or 4.2.176.0 and connected to a Catalyst switch running Cisco IOS Release 12.2(18)SXF12 might stop forwarding multicast packets to access points.

  Workaround: Try running the Catalyst switch with Cisco IOS Release 12.2(33)SXH3.

- CSCsx09827—In controller software release 4.2.176.0, the **config ap** *?* CLI command does not list the possible subcommands in alphabetic order.

  Workaround: None.

- CSCsx14840—The management interface source MAC address might change during operation.

  Workaround: None. This behavior is a problem only if a strict MAC-to-IP address rule is set.

- CSCsx18164—Undocumented "%DOT1X-4-INVALID_MSG_TYPE" messages appear when a client adapter experiences an EAP identity failure.

  Workaround: None.

- CSCsx21251—When a client successfully obtains a DHCP IP address with web authentication enabled on the WLAN and sends an orphan packet before authenticating, the controller marks the packet as an orphan and then sends out this erroneous debug message:

  ```
  Invalid MSCB state: ipAddr=X.Y.Z.A, regType=2, Dhcp required!
  ```

  Workaround: Ignore the erroneous debug message.

- CSCsx27145—The 802.11b radio beacons from a 1230 or 1310 series access point might toggle between enabled and disabled when a WPA2-AES client associates.

  Workaround: None.

Resolved Caveats

These caveats are resolved in controller software release 5.1.163.0.

- CSCsk08360—Further clarification is needed on the following message log entry: APF-1-DISCONECT_MOBILE_DUE_TO_WLAN_SWITCH: Disconnecting mobile 00:16:6f:79:82:75 due to switch of WLANs from 2 to 1.
- CSCsk47585—If you make WLAN changes on a controller running software release 4.1.185.0 and then save the configuration, a 1242 hybrid-REAP access point connected to the controller might crash.
- CSCsk54969—A controller might stop redirecting wireless clients to the Web Authentication login page on a WLAN that uses web authentication.
- CSCsk68619—When using an Intel 4965 802.11n client device with a 1250 series access point, the upstream throughput is higher than the downstream throughput.
- CSCsl10597—After a dynamic frequency selection (DFS) event, the 5-GHz radio in a 1250 series access point does not move to the new channel and start beaconing.
- 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."
- CSCsm04951—The number of entries in use appears with the local database size in the output of the **show database summary** CLI command:

  ```
  Current Max database entries..................... 512
  Max database entries on next reboot.............. 512
  Current number of entries used................... 3
  ```

  To aid in troubleshooting guest user account errors, more detailed information is necessary related to the type of entry in use, such as management user accounts, MAC filters, access point SSC or MIC information, excluded clients, and local net users.
- 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.
- CSCsm85717—The following error message needs to identify the root cause of the problem:

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

- CSCsm86125—When an 802.1X client attempts to authenticate to an ACS RADIUS server, a controller running software release 5.0.148.0 might reboot for an unknown reason.
- CSCsm91814—When clients associate and authenticate on the same SSID using a different username and password, a 4400 series controller configured for WPA2-AES and PEAP-MSCHAPv2 might cache AAA override values (such as the dynamic VLAN) and assign clients to the wrong VLAN. The clients might also obtain an IP address on the wrong VLAN.
- 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."
- 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.

- CSCso50723—When you use the controller's local RADIUS server for EAP-FAST authentications, authentication might fail if your client already has a protected access credentials (PAC) for the controller to which you are authenticating.
- 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.
- CSCso63232—The controller in the Catalyst 3750G Wireless LAN Controller Switch might reboot if you enter the **show hreap group detail** *groupname* CLI command without a group name or without a space between the **detail** parameter and the group name.
- CSCso65150—When AAA override is enabled for a WLAN and the AAA server is providing the session timeout value, if a client that is associated to that WLAN roams to another access point joined to the same controller and the session timeout has not expired, the session timeout for that client is reset to the initial value received from the AAA server.
- CSCso66778—The output of dump low-level debugs is not complete for several commands in controller software releases 5.0 and 4.2.112.0. This problem might affect proper troubleshooting for service port hangs, NPU issues, and so on.
- 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.
- 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."
- CSCso78437—After a client sends a reassociation request or response but before it has completed a four-way exchange, all of the packets coming to the client are dropped at the controller or forwarded to the wired side.
- CSCso86463—Some access points running software release 4.2.99.0 might crash if traffic stream metrics (TSM) is enabled.
- CSCso92229—The controller CLI accepts a CIDS SHA1 key with the correct number of hexadecimal digits but also accepts extra colons between the pairs of digits.
- CSCso92249—The controller sometimes reboots without a crash log when you run multiple Telnet sessions.
- CSCso92828—When an access point is running Rogue Location Discovery Protocol (RLDP), radio reset messages can be logged. However, the radio reset messages should be suppressed when caused by RLDP.
- CSCso97776—When management frame protection (MFP) and a guest LAN are configured, the controller might show unwanted logs.

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

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

- CSCsq07537—Clients continue to communicate with an access point that has its radio disabled by the controller. The controller shows that the access point radio is disabled when it is not.
- CSCsq11305—A 1250 series access point in monitor mode can transmit beacons.
- CSCsq12776—The controller might crash without generating a crash file.
- CSCsq14310—If the Allow AAA Override option is enabled for a WLAN, the guest role is not applied to the local net user.
- CSCsq23961—An orphan packet from the distribution system port might prevent DHCP from operating properly.
- CSCsq24255—When an access point is disabled or removed from the controller, a client entry is also cleared from the controller. However, the controller does not send an SNMP alert message to the NAC server that the client entry has been removed, so its entry remains on the server.
- CSCsq24256—The mobility anchor feature might not work properly for a controller running software release 4.2.121.0.
- CSCsq26901—A Cisco WiSM might reboot and not recover on its own. The following information appears in the controller's crash log:

```
Task Name:dot11a
Reason: System Crash
si_signo: 11
si_errno: 0
si_code:  196609
si_addr:  0x5e5e5e9e
timer tcb:  0xe1
timer cb:   0x10212aa0 ('rrmSendTimerMsg+284')
timer arg1: 0x14765390
timer arg2: 0x0
```

- CSCsq34216—The system logs on a controller running software release 5.0.148.0 might be filled with messages such as "apf_ms.c:4849 APF-1-USER_DEL_FAILED: Unable to delete user name **** for mobile **:**:**:**:**:**," where the first set of asterisks represents a username and the second set represents a MAC address. The username that is listed is not a username that is configured anywhere on the controller.
- CSCsq35662—More debug messages are needed when an access point fails to download the software image from the controller.
- CSCsq35990—The **config netuser lifetime** CLI command does not accept a zero (0) value for the *lifetime* parameter.

- CSCsq44516—Multiple vulnerabilities exist in the Cisco Wireless LAN Controllers (WLCs), Cisco Catalyst 6500 Wireless Services Modules (WiSMs), and Cisco Catalyst 3750 Integrated Wireless LAN Controllers. This security advisory outlines details of the following vulnerabilities:
  - Denial of Service Vulnerabilities (total of three)
  - Privilege Escalation Vulnerability

  These vulnerabilities are independent of each other. Cisco has released free software updates that address these vulnerabilities. There are no workarounds available for these vulnerabilities.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090204-wlc.
- CSCsq49329—The **show services mobility detail** *ip_addr* CLI command generates an error on the 2106 controller, even when you enter a valid IP address.
- CSCsq49975—When you enable ARP debugs and generate a gratuitous ARP, the gratuitous ARP does not come up to the dtl ARP module, and no debugs appear on the console.
- CSCsq50866—When you configure QoS data rates for a guest role using the controller CLI, you can set values greater than 60000.
- 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.
- CSCsq63106—The Cisco WiSM shows a memory leak of 1.8 MB every 2.5 hours. When the controller reaches a low-memory condition, it becomes unreachable, and the console might not be responsive.
- CSCsq81667—Large IP packets that have been fragmented into multiple fragments might fail to be reassembled by a 4400 series controller.
- CSCsq83843—The necessary components for the GARP declaration need to be clarified in the following message: “Jun 13 07:58:18.717 gid.c:506 DOT1D-6-PORT_FIND_FAIL: Port number 1 is not found for GARP Information Declaration (GID).”
- CSCsq83855—The following message requires further clarification: “Process: Name:fp_main_task, Id:11d92ca8.”
- CSCsq86975—The controller might reboot if you have global Cisco Discovery Protocol (CDP) and access point CDP disabled and then you click the Refresh button on the CDP Neighbors page.
- CSCsq87457—A Cisco WiSM might lock up or reboot due to a software failure of the NPUChecktask task.
- CSCsr03008—A 1252 access point delays packets to 7921 phones intermittently for up to 20 to 30 seconds. As a result, you might experience no rings, one-way audio, or no audio on the 7921 phones.
- CSCsr06596—After the controller has been up for days, it might reboot because of a software failure of the apfRogueTask task.
- CSCsr16689—Wired hosts cannot manage the 2106 controller through the dynamic interface.
- CSCsr17163—Under conditions of very high stress, the controller shows no joined access points and clients and no traffic to or from clients. The controller also generates a crash file and reboots automatically.
- CSCsr36756—After a controller running software release 5.1.151.0 contains a rogue access point, the state changes from “Contained” to “Alert.”

- CSCsr41231—The following error message might appear on a controller running software release 4.2.130.0: “sim.c:1061 SIM-3-MACADDR_GET_FAIL: Interface 1 source MAC address is not found.”
- CSCsr52442—Entering **show port summ** rather than **show port summary** generates the following error: “An invalid port has been used for this function.”
- CSCsr55816—After you upgrade the controller from software release 5.0.148.0 to 5.1.151.0, it might reboot because of a software failure of the emWeb task.
- CSCsr60506—The controller might unexpectedly reboot at spamReceiveTask with a signal 11 error (segmentation fault).
- CSCsr62942—A controller running software release 4.2.112.0 might reboot because of a software failure in the EAP framework. This problem occurs when 7921 phones are used as clients.
- CSCsr67250—A 1250 series access point does not adjust its power level correctly and always stays on either transmit power level 1 or 2.
- CSCsr67780—When you enable Rogue Location Detection Protocol (RLDP) on a 4400 series 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
  ```

- CSCsr68678—The following error appears to be a normal message and occurs after a reboot: “sim.c:309 SIM-3-INVALID_PORT: Using invalid port number. Port out of range. Port # 0.” However, the error does indicate a problem. If this message is valid, it needs to be reworded.
- CSCsr74113—After you create a user, you are no longer able to change the password for the user. You must delete the user and re-add the user with a new password.
- CSCsr74598—The RSSI value reported by a 1250 series access point’s 2.4-GHz radio might be 6 dB lower than the actual value.
- CSCsr75121—When clients are authenticating to WPA or WPA2 WLANs using both PSK and 802.1X, the following decrypt errors appear in the controller trap logs. The errors appear to result from the access point’s inability to decrypt client traffic when WPA- or WPA2-encrypted packets are sent to the access point before the access point receives the PMK from the controller. The errors do not affect client authentication or connection but generate a lot of messages in the trap logs.

  ```
  Decrypt errors occurred for client client_mac_address using WPA key on 802.11a
  interface of AP ap_mac_address

  Decrypt errors occurred for client client_mac_address using WPA2 key on 802.11b/g
  interface of AP ap_mac_address
  ```

- CSCsr97877—A 1250 series access point might transmit its neighbor discovery packets at the wrong power level. They should be transmitted at maximum power.
- CSCsu04447—If you enable TACACS+, you cannot classify rogue access points using the controller GUI.
- 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.
- CSCsu26961—The controller lets you configure WPA+WPA2 with 802.1X and PSK at the same time. This behavior can cause a security issue because the PSK user can still connect to the network.
- CSCsu27939—A controller running software release 4.2.130.0 might reboot because of a software failure of the usmWebRRMRadSlotNoiseChannelGetNext+64 task.

- CSCsu56269—A Cisco WiSM running software release 4.2.130.0 might reboot because of a software failure of the radiusTransportThread task.
- CSCsu62060—A 4400 series controller might reboot because of a software failure of the tplusTransportThread task.
- CSCsv00342—When you clear the Back-up Primary Controller and Back-up Secondary Controller parameters on the Global Configuration page and click **Apply**, the controller does not clear the parameters.
- CSCsv34136—When an RFC3576 message arrives, the controller enforces a source port check by searching for the server using the IP address and source port in the RFC3576 message rather than searching the configured RADIUS servers list using the same Find Server function as for any other RADIUS message.
- CSCsv34605—An access point using the Rogue Location Detection Protocol (RLDP) does not obtain a DHCP address if the DHCP server is on an autonomous access point. As a result, RLDP does not detect if a rogue access point is on the wire.
- CSCsw80627—Controllers running software release 5.1.151.0 sometimes reboot because of a software failure of the emWeb task.
- CSCsw92335—If you use WCS to set the session timeout for a WLAN with 802.1X, WPA, or WPA2 security, the timeout might not be set on the controller. The default value might be used instead.
- CSCsx29956—A 4400 series controller might reboot when it is configured to operate with an LDAP server because of a software failure of the LDAP DB Task 2 task.

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