Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 5.0.148.2

July 18, 2008

These release notes describe open and resolved caveats for software release 5.0.148.2 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, 1240, 1250, and 1300 Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.

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

Contents

These release notes contain the following sections.

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

Cisco Unified Wireless Network Solution Components

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

- Software release 5.0.148.2 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 5.0.55.0
- Cisco WCS Navigator 1.2.55.0
- Location appliance software release 4.0.32.0
- Cisco 2700 Series Location Appliances
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers

Note The 5.0.148.2 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, 1240, 1250, and 1300 Series Lightweight Access Points

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 5.0.148.2 if you have mesh access points in your network. If your network uses mesh access points, use only mesh-specific releases such as 4.1.191.24M.

Note Cisco WCS software release 5.0.55.0 may be used to manage both mesh and non-mesh controllers (such as controllers running software release 5.0.148.2 and 4.1.191.24M). You do not need different instances of WCS to manage mesh and non-mesh controllers.

Controller Requirements

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

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

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

Software Release Information

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

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

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

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

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

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 Downgrading from this release to controller software release 4.2.130 sometimes corrupts the controller configuration. If you downgrade to software release 4.2.130, save the controller configuration before the downgrade and reload it after the downgrade.

Note When you upgrade the controller to software release 5.0.148.2, the binary configuration file might not migrate correctly. For details, see the "Software Upgrade Might Fail If Certain Characters Used in Previous Configuration" note in the "Important Notes" section on page 11.

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 5.0.148.2

Caution Before upgrading your controller to software release 5.0.148.2, you must comply with the following rules.

- Make sure you have a TFTP server available for the software upgrade. Keep these guidelines in mind when setting up a TFTP server:
  - Controller software release 5.0.148.2 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 tftpd32 and the TFTP server within the WCS. If you attempt to download the 5.0.148.2 controller software and your TFTP server does not support files of this size, the following error message appears: "TFTP failure while storing in flash."
  - If you are upgrading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are upgrading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP server cannot run on the same computer as the WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.

- 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 4.1 or 4.2 software release, you can upgrade your controller directly to software release 5.0.148.2. If your controller is running a 3.2 or 4.0 release, you must upgrade your controller to an intermediate release prior to upgrading to 5.0.148.2. Table 1 shows the upgrade path that you must follow before downloading software release 5.0.148.2.

Table 1 Upgrade Path to Controller Software Release 5.0.148.2

Current Software Release	Upgrade Path to 5.0.148.2 Software
3.2.78.0 or later 3.2 release	Upgrade to a 4.1 release before upgrading to 5.0.148.2.
4.0.155.5 or later 4.0 release	Upgrade to a 4.1 or 4.2 release before upgrading to 5.0.148.2
4.1.171.0 or later 4.1 release	You can upgrade directly to 5.0.148.2.
4.2.61.0 or later 4.2 release	You can upgrade directly to 5.0.148.2.

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

- Cisco recommends that you also install the Cisco Unified Wireless Network Controller Boot Software 5.0.148.2 ER.aes file on the controller. This file resolves defect CSCsd52483 and is necessary to ensure proper operation of the controller. The ER.aes file can be installed on all controller platforms. 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 Unlike previous ER images, a new bootloader file is not loaded when you install the 5.0.148.2 ER.aes file. This is true for all controllers. The 4.2.112.0 ER.aes file is the last ER file to contain a bootloader. If you want the latest bootloader, install the 4.2.112.0 ER.aes file. If you want to obtain the fix for CSCsd52483, also install the 5.0.148.2 ER.aes file.

Note The ER.aes files are independent from the controller software files. You can run any controller software file with any ER.aes file. However, installing the latest boot software file (5.0.148.2 ER.aes) ensures that the boot software modifications in all of the previous and current boot software ER.aes files are installed.

Caution If you require a downgrade from one release to another, you may lose the configuration from your current release. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.

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

Note Do not install the 5.0.148.2 controller software file and the 5.0.148.2 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 5.0.148.2 controller software and the Cisco Unified Wireless Network Controller Boot Software 5.0.148.2 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 5.0.148.2 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.0.148.2 ER.aes file).

Step 3 Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 5.0.148.2 ER.aes file to the default directory on your TFTP 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 In the IP Address field, enter the IP address of the TFTP server.

Step 9 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 10 In the File Path field, enter the directory path of the software.

Step 11 In the File Name field, enter the name of the software file (*filename*.aes).

Step 12 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Step 13 After the download is complete, click **Reboot**.

Step 14 If prompted to save your changes, click **Save and Reboot**.

Step 15 Click **OK** to confirm your decision to reboot the controller.

Step 16 After the controller reboots, repeat Step 6 to Step 15 to install the remaining file (either the 5.0.148.2 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.0.148.2 ER.aes file).

Step 17 Re-enable the WLANs.

Step 18 For Cisco WiSMs, re-enable the controller port channel on the Catalyst switch.

Step 19 Re-enable your 802.11a and 802.11b/g networks.

Step 20 If desired, reload your latest configuration file to the controller.

Step 21 To verify that the 5.0.148.2 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 22 To verify that the Cisco Unified Wireless Network Controller Boot Software 5.0.148.2 ER.aes file is installed on your controller, enter the **show sysinfo** command on the controller CLI and look at the Bootloader Version field. “N/A” appears if the ER.aes file is installed successfully. “Error” appears if the ER.aes file is not installed.

New Features

Software release 5.0.148.2 is a maintenance release and does not contain new features.

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.

Software Upgrade Might Fail If Certain Characters Used in Previous Configuration

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. However, the configuration file does not migrate correctly if it contains any of the following characters as part of a user configuration string: &, <, >, ', ". For example, a WLAN profile named *R&D* causes an XML parsing error after the second reboot, even though this profile name is valid in 4.1 and previous configurations.

Note You cannot download a binary configuration file onto a controller running software release 5.0.148.2. 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 5.0.148.2, the LWAPP mode changes to Layer 3 if it was previously configured for Layer 2.

If you downgrade from controller software release 5.0.148.2 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.

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.

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.

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.

Regulatory Changes

These regulatory changes apply to the following countries for controller software 4.2.61.0 and later:

- Argentina—802.11a support is removed
- Brazil—802.11a support is removed
- Canada—802.11a -N support is removed
- Philippines—802.11a -N support is removed
- Turkey—For 802.11a, -R is replaced by -I

Access points can no longer join the controller if you attempt to use the restricted 802.11 bands in these countries. For a complete list of the current regulatory rules, refer to the *Wireless LAN Compliance Status* document at this URL:

https://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps4555_Products_Data_Sheet.html

Supporting Oversized Access Point Images

Controller software release 4.2 or later allows you to upgrade to an oversized access point image by automatically 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 Limitations

Multicast applications have known performance limitations on the 2100 series controllers and the Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers. Cisco is working to address these limitations in a future production code release. In the meantime, Cisco recommends that you use the 4400 series or WiSM controllers for multicast intensive applications.

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

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.

Note For static devices behind the WGB, additional configuration may be needed. If the device does not send any packets, the WGB does not learn the MAC address. Therefore, you need to configure a static entry in the forwarding table as follows: **bridge 1 address xxxx.xxxx.xxxx forward FastEthernet0**.

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 5.0* 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 5.0.148.2 does not allow you to choose IPSec as a Layer 3 security option. None and VPN Passthrough are the only available options. If you upgrade to this release from a previous release that supported IPSec as a Layer 3 security option, any WLANs that are configured for this feature become disabled. If you want to configure IPSec, you must use a version of controller software prior to 4.0.

4400 Series Controllers Do Not Forward Subnet Broadcasts through Guest Tunnel

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

Re-enable Broadcast after Upgrading to Release 4.0.206.0

In software releases 4.0.179.0 and earlier, broadcast and multicast forwarding were both controlled with a single global flag that enabled multicast. Beginning with software release 4.0.206.0, these functions were broken into separate configuration flags: one that controls broadcast and one that controls non-broadcast multicast. If you have multicast enabled in software releases 4.0.179.0 and earlier, the broadcast flag is left disabled after upgrading to software release 4.0.206.0. As a result, some applications that rely on broadcast do not work after the upgrade.

After you upgrade to software release 4.0.206.0, use this CLI command to re-enable broadcast:

config network broadcast enable

When re-enabled, broadcast uses the multicast mode configured on the controller.

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.

Controllers Must Run Release 3.2.116.21 or Later to Support -P Regulatory Domain

To support access points configured for use in Japan, you must upgrade the controller software to release 3.2.116.21 or later. Earlier releases do not support access points configured for use in Japan (regulatory domain -P).

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 (ppcboot) 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 4: Change Active Boot Image** from the boot menu to set the backup image as the active boot image. Otherwise, when the controller resets, it again boots off the corrupted primary image.

After the controller boots, the active boot image can be changed to the backup image using the **config boot backup** command.

Home Page Retains Web Authentication Login with IE 5.x

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

Rogue Location Discovery Protocol (RLDP)

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

Ad-Hoc Rogue Containment

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

Changing the Default Values of SNMP Community Strings

The controller has commonly known default values of “public” and “private” for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.0* 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 5.0* 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

These hardware features are not supported on 2100 series controllers:

- Service port (separate out-of-band management 10/100-Mb/s 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
- Layer 2 LWAPP
- Spanning tree
- Port mirroring
- Cranite
- Fortress
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)
- Multicast unicast mode

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

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

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 Controller

It is possible to run a 3504 controller image on a 2106 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 5.0.148.2.

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

  Workaround: Ignore the prompt and exit as usual.

- CSCsd54928—The CPU ACL is unable to block LWAPP packets on the AP-manager 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 is expired, but it does not send the notice to the client.

  Workaround: None.

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

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

- CSCsf29783—The Cisco WiSM reboots after experiencing a software failure with the reaperWatcher mmMfpTask.

  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.

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

  Workaround: None.

- CSCsg59235—The controller CLI lacks commands for debugging activity at the IP, ICMP, TCP, UDP, Telnet, SSH, and HTTP layers.

  Workaround: Use an external packet capture device to collect packets to and from the controller. Send these packets to the Technical Assistance Center (TAC) for analysis.

- CSCsg66040—You might experience intermittent HTTPS access to the controller after a software upgrade.

  Workaround: Perform another software upgrade and downgrade.

- CSCsg87111—If you create a WLAN with WPA1+WPA2 and conditional web redirect enabled and then try to change it to 802.1X+conditional web redirect, the MIB browser shows a commit failed error.

  Workaround: Do not change from WPA1+WPA2+conditional web redirect to 8021.X+conditional web redirect in one step. Instead, do it in three steps: 1) Disable conditional web redirect and save. 2) Change Layer 2 to 802.1X and save. 3) Configure conditional web redirect and save.

- 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: None.

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

  Workaround: None.

- CSCsh31104—The word *channel* is misspelled in this message log:

  ```
  Jan 03 16:03:34.699 WPS-4-SIG_ALARM_OFF: AP 00:15:C7:81:24:60 : Alarm OFF, standard
  sig NULL probe resp 1, track=per-Mac preced=2 hits=1 slot=0 channle=1
  ```

  Workaround: None.

- CSCsh96186—When a 4400 series controller receives IP fragments with an IP payload that is greater than 32 bytes, it may fail to reassemble the large IP packets that have been split into multiple fragments.

  Workaround: Redesign the network or reconfigure the communications endpoints to eliminate any points in which such a small fragment would be generated.

- CSCsi06191—Customers who have large deployments use master controller mode to easily locate newly joined lightweight access points on the network so they can prime them and allow them to join their respective controller. However, when the controller is rebooted, this feature is disabled.

  Workaround: None.

- CSCsi15194—The controller might take a long time to respond to a message during a four-way handshake.

  Workaround: None.

- CSCsi15249—Hybrid-REAP access points perform an unnecessary channel scan when entering standalone mode.

  Workaround: None.

- CSCsi17242—The API osapiTimeMillisecondsGet() function returns a time value that wraps in less than 50 days.

  Workaround: None.

- CSCsi26248—You might lose connectivity when adding or recovering a second link aggregation (LAG) link.

  Workaround: None.

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

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

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

  Workaround: None.

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

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

- CSCsi72578—After you set up the mobility anchor feature between two controllers, the client does not successfully connect to the specified anchor controller if the WLAN QoS profile is set to Bronze.

  Workaround: Change the WLAN QoS profile on both the internal controller and the anchor controller to Silver.

- CSCsj03124—Rogue Location Detection Protocol (RLDP) behavior is inconsistent when initiated from a Cisco 1250 series access point.

  Workaround: None.

- 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—The controller generates a unicast query for 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 note that this action can interfere with the auto-RF functionality.

- CSCsj14304—The controller should not snoop reserved multicast addresses.

  Workaround: None.

- CSCsj17054—A misleading message appears on the controller GUI when you load certificates.

  Workaround: None.

- 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: None.

- CSCsj32243—All old multicast timer application program interfaces (APIs) need to be replaced with new APIs.

  Workaround: None.

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

  Workaround: None.

- CSCsj48872—The controller may reboot or lose network connectivity while running software release 4.1.185.0.

  Workaround: Reboot the controller.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Enter a valid netmask.

- CSCsj88889—Workgroup bridge (WGB) and wired WGB clients are shown using different radios.

  Workaround: None.

- CSCsj95069—The web authentication login page does not have the Cisco logo.

  Workaround: None.

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

  Workaround: None.

- CSCsk08360—Further clarification is needed on the following message log entry:

  ```
  APF-1-DISCONECT_MOBILE_DUE_TO_WLAN_SWITCH: Disconnecting mobile 00:16:6f:79:82:75 due
  to switch of WLANs from 2 to 1.
  ```

  Workaround: None.

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

  Workaround: None.

- CSCsk15603—On the controller GUI, a conditional web redirect configured with 802.1X security generates an error.

  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.

- CSCsk18471—When the controller supports a Layer 3 roam without symmetric tunneling, an ARP entry is required at the foreign controller to forward a packet from the client to the foreign VLAN. If the entry does not exist in the NPU when a packet arrives, the NPU sends an ARP resolution request to the CPU. The CPU then performs the ARP lookup and plumbs the entry to the NPU. However, the ARP entry is not being plumbed correctly to the NPU. As a result, each packet sent by the client results in a request to the NPU.

  Workaround: None.

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

  Workaround: None.

- CSCsk31842—The controller fails to join WCS when network address translation (NAT) or port address translation (PAT) is used.

  Workaround: Downgrade the controller software to the 3.2.195.13 release.

- CSCsk38779—The controller does not respond to a third-party SNMP manager's snmpbulkwalk request.

  Workaround: None.

- CSCsk42233—The controller reboots when you open the CDP AP Neighbors page.

  Workaround: Use the controller CLI to view this information.

- CSCsk44641—The controller needs to separate or prioritize ARP broadcast and multicast traffic types to avoid impacting access point communications.

  Workaround: None.

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

  Workaround: None.

- CSCsk54969—One of the controllers in the Cisco WiSM might stop providing web authentication login pages but continue to allow WPA2 RADIUS authentication to the same authentication server.

  Workaround: Reboot the controller.

- 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.

- CSCsk62403—A controller running software release 4.1.185.0 or 4.0.217.0 might reboot due to a software failure with the sshpmMainTask.

  Workaround: None.

- CSCsk63047—Dynamic transmit power control (DTPC) does not work on Cisco1240 series access points in WGB mode.

  Workaround: None.

- CSCsk67066—The proper error message is not displayed while removing the Radius server. The GUI error message is “Error in deleting auth server.” The correct error message displays in CLI: “Error: Server in use on a specific H-REAP group.”

  Workaround: None.

- CSCsk68619—When you use an Intel 4965 802.11n client with a 1250 series access point, the upstream throughput is higher than the downstream throughput.

  Workaround: None.

- CSCsk72885—The controller returns a 0 value instead of 1 or greater for the service port or virtual interface.

  Workaround: None.

- CSCsk76218—A configuration file encrypted with a key can be downloaded without a key.

  Workaround: None.

- CSCsk76973—When you upgrade a controller from software release 4.2.61.0 or earlier, access points immediately begin downloading the new software image from the controller instead of waiting until the controller is rebooted and the downloaded image is running on the controller.

  Workaround: Disconnect the access point-to-controller path before upgrading the controller from software release 4.2.61.0 or earlier.

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

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

- 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
  ```

  This condition was observed in a deployment containing a large number of access points belonging to the same mobility group within radio range of each other and transmitting on the same channel. It may also indicate a genuine spoofing attack.

  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.

- CSCsk87753—The 802.11n radio might experience low throughput.

  Workaround: None.

- CSCsk87972—DCA sensitivity settings and schedule configurations should be available on the controller GUI.

  Workaround: None.

- CSCsk93465—When the maximum number of hybrid-REAP access points is reached, the Remove button on the controller GUI becomes out of sync, making it impossible to remove an access point.

  Workaround: None.

- CSCsk93537—With four Intel 4965 clients simultaneously sending upstream TCP traffic, the aggregate throughput of an 802.11n 20-MHz radio drops to 25% of the traffic capacity of the radio.

  Workaround: None.

- CSCsk99318—When a workgroup bridge (WGB) roams between controllers, packets to the clients behind the WGB drop momentarily.

  Workaround: None.

- CSCsl01005—Sometimes bandwidth contracts do not take effect. If a user with bandwidth restrictions logs in and out and then another user without bandwidth restrictions logs in, the bandwidth restrictions are not removed immediately.

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

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

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

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

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

- CSCsl06484—When a 1250 series hybrid-REAP access point comes online, you might see the following traceback, which is harmless:

  ```
  Oct 25 22:21:10.747: WARNING: invalid slot ID (255) passed to REAP -Traceback=
  0x51F760 0x51F910 0x4CA740 0x4CDC60 0x4DAB20 0x4BCCBC 0x4BD5E8 0x1CC6DC 0x1CE454
  ```

  Workaround: None.

- CSCsl09066—A WCS access point group VLAN profile configuration does not match the actual controller configuration. This problem occurs when using 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 current console output does not indicate which controller the access point joins.

  Workaround: On the access point console, right after "Press Return to get started" appears, enter enable mode (the default password is "Cisco") and then enter the following debug command: **debug ip udp**. This command shows all UDP packets sent and received by the access point.

- CSCsl18161—The controller only supports TFTP transfer mode for upgrade, and sometimes TFTP fails over a slow WAN link.

  Workaround: To resolve this issue, TCP-based FTP transfer mode is added on the controller CLI. To get the best performance when you transfer an image over the management port, consider raising the CPU-NPU rate limit by issuing this command: **config advanced rate disable**.

- CSCsl21267—Too many retries causes a workgroup bridge (WGB) to continually disassociate.

  Workaround: None.

- CSCsl28130—A 4402 controller might reboot due to a software failure of the spamReceiveTask when accessed from the management interface through a NAT device on a firewall.

  Workaround: None.

- CSCsl29563—If you configure a syslog server on the controller GUI and then disable it, the controller CLI does not add the syslog server until "host 0.0.0.0" is deleted manually by the CLI.

  Workaround: Always use the controller GUI to configure syslog.

- CSCsl32786—Active guest user accounts are sometimes lost when a controller reboots.

  Workaround: None.

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

  Workaround: Use the controller CLI to change the syslog filter level.

- CSCsl34068—Guest roles for guest users configured on the controller should override the QoS parameters set for the WLAN. However, when a guest user is momentarily disconnected and reassociates, the WLAN parameters override the guest role.

  Workaround: None.

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

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

  Workaround: None.

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

  Workaround: None.

- CSCsl42843—You can assign an invalid value to the channel switch mode using this CLI command:

  config 802.11h channel switch enable *mode_value*

  The only valid values for the channel switch mode are 0 and 1.

  Workaround: None.

- CSCsl47720—The controller linktest results are sometimes inconsistent.

  Workaround: None.

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

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

- CSCsl50622—When a controller is configured with a WPA policy of WPA+TKIP or WPA+AES using either PSK or EAP, 802.11n client devices cannot connect at all data rates.

  Workaround: Change the WPA policy to include WPA2, or use only WPA2 with PSK or EAP.

- CSCsl51368—Some 802.11n client devices successfully connect to an access point but cannot pass traffic until they are rebooted.

  Workaround: None.

- CSCsl52445—The internal web authentication page on the controller accepts up to 2,047 characters, but the internal web authentication page in WCS accepts only130 characters.

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

- CSCsl52628—When you enable or disable SSH or Telnet on an access point, the SSH or Telnet state does not appear in the output of the **show ap config** CLI command.

  Workaround: None.

- CSCsl54491—Controllers sometimes report non-rogue access points as rogues when the 802.11a radios are disabled on the access points.

  Workaround: None. This issue is cosmetic.

- CSCsl55613—The controller GUI sometimes displays unavailable options when you attempt to delete more than one rule at a time.

  Workaround: Delete one rule at a time.

- CSCsl57356—Controllers sometimes display associated 802.11n client devices as 802.11a devices.

  Workaround: None.

- CSCsl57778—Cisco Aironet access point models 1100, 1200, and 1310 sometimes delete the recovery image when you upgrade them from software release 4.2.61.0.

  Workaround: None.

- CSCsl58122—You cannot configure access point credentials on the controller GUI until access points join the controller.

  Workaround: Use the controller CLI to configure the access point credentials.

- CSCsl59308—On networks that contain close to the maximum number of access points per controller, controllers sometimes generate spurious management frame protection (MFP) Anomaly Detected alarms. The alarms appear to originate from valid access points.

  Workaround: Disable infrastructure MFP on the controller GUI, or disable it on the controller CLI by entering **config wps mfp infrastructure disable**.

- CSCsl59466—When multicast is disabled, the controller still forwards DTP to the access point as a multicast packet. This traffic should be dropped by the NPU.

  Workaround: None.

- CSCsl60658—Some invalid values might appear while you perform a TFTP transfer from the controller GUI. These values do not affect functionality, but you might not receive an update regarding transfer status on the GUI.

  Workaround: Use the controller CLI for TFTP transfers.

- CSCsl61657—The Short Slot Time Capability Info bit is not cleared in association and reassociation responses when an 802.11b-only client associates to a lightweight access point.

  Workaround: None.

- CSCsl67177—You might lose connectivity from the Catalyst Express 500 (CE500) to the controller when one port of the port channel is shut down.

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

- CSCsl68867—One radio interface or both radio interfaces on a 1250 series access point might go down when there are many mixed radio clients associated to the same 1250 series access point and they are passing heavy unicast and multicast traffic.

  Workaround: Reboot the access point.

- CSCsl69160—If a client with 802.1X enabled connects to an access point, disconnects, and then reconnects, the client fails to connect to the access point again using 802.1X authentication.

  Workaround: Clear the client state by entering this command: **config client deauthenticate** *client_mac*.

- CSCsl70043—When a client connects to a secure EAP WLAN and immediately switches to an open WLAN, the client is denied by a Layer 2 association response, which is normal behavior. The issue is that the association response comes from the MAC address and BSSID of the EAP WLAN, even though the exchange to switch to the open WLAN was made with the MAC address and BSSID of the open WLAN.

  Workaround: Use the **config network fast-ssid-change enable** command to allow the client to connect.

- CSCsl71343—A Buffalo 802.11n client experiences very low TCP throughput on a 1250 series access point with a 5-GHz radio when tested with other clients (the Intel 4965AGN and the Intel 2915ABG).

  Workaround: None.

- CSCsl72335—If the access point mode is changed, the override global credentials configuration for that access point is enabled automatically.

  Workaround: None.

- CSCsl72538—After you set the session timeout on a WLAN to zero in the controller GUI, the WLAN does not show a value of zero. In the controller CLI, this same WLAN is set to zero or infinity.

  Workaround: None.

- CSCsl73635—802.11a uplink TSM aggregated reports do not arrive at the controller even though 802.11a TSM is enabled and a client is associated to the 802.11a network. The reports arrive only if 802.11b TSM is disabled.

  Workaround: Enable TSM on both 802.11a and 802.11b radios for uplink traffic stream metrics to operate correctly.

- 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.”

  Workaround: None.

- CSCsl79069—When the AAA override is enabled for a WLAN and the AAA server is providing the session-timeout value, if a client 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.

  Workaround: None.

- CSCsl81514—The following error message appears when you create an untagged (Vlan ID = 0) dynamic interface: “First configure a valid non-zero vlan on this interface.”

  Workaround: None.

- CSCsl82329—A 4400 series controller might reboot when a CCXv5 client attempts to associate in 802.11g mode with CCKM+TKIP.

  Workaround: None.

- CSCsl83715—If you configure a controller with 802.11b/g data rates 11 Mb/s and higher enabled, anything below disabled, and 11 Mb/s configured for mandatory and then you change the WCS controller template so that 6 and 9 Mb/s are supported, thousands of msgQ messages appear after you apply the template.

  Workaround: None.

- CSCsl85298—The Redirect URL after Login option for customized web authentication is not available on a Cisco WiSM running controller software release 4.2.61.0.

  Workaround: None.

- CSCsl85407—A controller running software release 4.1.185 or 4.2.61 with PEAP authentication sometimes sends the MAC address of an Odyssey client as a username in the accounting record.

  Workaround: None.

- CSCsl86368—An error occurs when you try to configure an external web authentication URL on the GUI of a controller running software release 4.2.

  Workaround: None.

- CSCsl87036—The ifSpeed entry is missing for the interfaces on some controllers running software release 4.1.185.0 or 4.1.171.0.

  Workaround: None.

- CSCsl90630—Currently, dynamic channel assignment (DCA) requires at least one non-DFS channel. This requirement contradicts EU rules for outdoor WiFi deployment. Channels 52 through 140 require DFS checks, and these are the only channels available for outdoor deployment. This requirement forces customers with an outdoor deployment to add an indoor-only channel to the DCA list.

  Workaround: None.

- CSCsl90841—After you upgrade a controller to software release 4.2.61.0, any access point that does not have region coding (such as the Airespace 1250 access point) is unable to join the controller. An "Invalid country code" message with a country code of 0xFFFF appears in the output of the **debug lwapp events enable** command.

  Workaround: Downgrade the controller to software release 4.1.

- CSCsl92740—The driver transmit queue for a 1250 series access point might become stuck.

  Workaround: None.

- CSCsl94719—The Preview button on the controller GUI shows the internal default web page, even if you chose Customized for the Web Authentication Type.

  Workaround: None.

- 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: None.

- CSCsm05607—The controller ignores ICMP packet "too large" messages from the Microsoft ISA firewall when it forwards fragments to the firewall.

  Workaround: None.

- CSCsm08062—The controller might reboot due to a software failure in dtlDataLowTask.

  Workaround: None.

- CSCsm08623—When the controller has **config paging disabled** configured, the output of the **show msglog** command is periodically interrupted with the following prompt: "Would you like to display the next 15 entries?"

  Workaround: None.

- CSCsm08938—The channel width for an 802.11n access point shows an invalid type on the 802.11b/g/n Cisco APs > Configure page. It shows "802.11b/g/n" but should show "Below 40 MHz."

- CSCsm10213—In the debug lwapp events detail message, the Received LWAPP CHANGE_STATE_EVENT from the access point should also include the specific state event.

  Workaround: None.

- CSCsm12623—AAA override dynamic VLAN assignment fails with guest tunneling.

  Workaround: None.

- CSCsm13348—When running multiple multicast streams with IGMP snooping enabled on the controller, the 802.11 MAC counters do not increment properly on the Radio > Statistics page. Specifically, they do not show any multicast transmit traffic counts.

  Workaround: None.

- CSCsm15583—The output of the **show database summary** command exceeds the number of eligible entry types displayed by individual **show** commands. It also needs to be able to identify other entries and remove them so eligible entries configured on the controller can be entered up to the database maximum value.

  Workaround: None.

- CSCsm17459—Entering CLI commands in capital letters does not work or generates an error.

  Workaround: None.

- CSCsm18866—When you delete an access point from a hybrid-REAP group, the following error message appears: "Failed to add AP to the group."

  Workaround: None.

- CSCsm20279—An access point that has been converted to lightweight mode might intermittently enter a state where some (but not all) of its LWAPP packets that are addressed at the IP layer to the controller's AP-manager IP address are addressed at the MAC layer to the access point's default IP gateway, rather than to the AP-manager's MAC address.

  Workaround: Configure the access point's default gateway to forward the packets from the access point to the controller.

- CSCsm25127—When you use the controller CLI in controller software release 4.2.61.0 to add a custom logo to the internal web authentication page, a light green border appears above and to the right of the logo.

  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.

- CSCsm26793—A CCXv4 (or greater) link test initiated on a controller appears to incorrectly report signal-to-noise ratio (SNR) values for wireless clients.

  Workaround: None.

- 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.

- CSCsm36085—Poor IPTV multicast quality might occur on a controller running software release 4.2 with IGMP enabled.

  Workaround: None.

- CSCsm36798—An ACL that is created (but not applied) is not reflected in the controller's running configuration after you download the saved configuration from a TFTP server.

  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.

- CSCsm41794—Every two weeks or so the anchor controller stops serving web authentication pages to the wireless guest clients. The guest clients get an IP address, but they do not get an IP address for their default gateway.

  Workaround: Reboot the controller, and guest users should be able to work fine.

- CSCsm42172—1250 series access points sometimes fail to download an image from the controller when multiple controllers running different software releases are on the network.

  Workaround: On the controller CLI, enter **clear lwapp private-config** and reboot the controller. The access point then joins the controller, loads the image, and reboots.

- CSCsm45021—When low data rates (less than 2 Mbps) are used, the access point ACK is missing, which can result in sluggish voice calls.

  Workaround: None.

- CSCsm48076—Guest-related trap logs are not generated for a lifetime guest user.

  Workaround: Create a guest user account using the lobby ambassador feature on the controller. Then the controller shows a guest user with an unlimited time period.

- CSCsm50601—A Cisco WiSM controller might reboot due to a software failure at mmc_system.c:2089. After the primary WiSM controller reboots, one hundred to several hundred access points fail over to the backup WiSM controller.

  Workaround: None.

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

  Workaround: Create an access list with rules.

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

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

  Workaround: None.

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

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

  Workaround: None.

- CSCsm74430—5-GHz radios might stop working without showing that the radio interface is down.

  Workaround: Reboot the access point.

- 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.

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

  Workaround: None.

- 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.

- 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.
  ```

  Workaround: None.

- CSCsm86125—A controller running software release 5.0.148.0 might reboot while trying to authenticate an 802.1X client to an ACS RADIUS server.

  Workaround: None.

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

  Workaround: None.

- CSCsm95928—A 4400 series controller might reboot due to an NPU lockup.

  Workaround: None.

- CSCsm97258—An 1130 series access point might reboot with "%SYS-2-BADSHARE: Bad refcount in pool_getbuffer, ptr=CFFB."

  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.

- CSCso02773—The controller does not present the test result and the last test response after a DHCP test using the DC mode.

  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.

- CSCso04025—An SNMPwalk of the controller fails at ipAdEntAddr with the error message "OID not increasing."

  Workaround: Poll for individual objects instead of performing a complete SNMPwalk.

- CSCso05149—When you use mobility anchoring with wired guest access, the end controller set as "local" does not allow the WLAN to be enabled if the ingress interface is configured on the WLAN. An internal controller can be anchored to a remote controller, but the end controller (set as "local") fails when you configure an ingress interface and the WLAN is set to "local."

  Workaround: When you set up an anchor controller, do not configure an ingress interface because the clients are tunneled over from another controller, preventing selection of an ingress interface on the guest WLAN. Set the anchor for the guest WLAN to "local" and then enable the WLAN, leaving the ingress interface set to 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.

- CSCso08708—When the physical ports for the management and dynamic interfaces are changed on the controller, quarantine VLAN information is not pushed to the NPU, which prevents network admission control (NAC) out-of-band integration from working.

  Workaround: When physical ports are changed on the management and dynamic interfaces, set the quarantine VLAN to 0 and then reconfigure it to the previous value. The quarantine VLAN is then pushed to the NPU and NAC out-of-band integration works correctly.

- 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.

- CSCso13516—The controller sometimes crashes at random, and the crash file shows a signal 11. Signal 11 occurs when the program running on the controller accesses a part of memory that it does not have permission to access.

  Workaround: None.

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

  Workaround: Use the controller CLI to display users.

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

  Workaround: Use Omnipeek if possible.

- CSCso20452—When you enter **show wism status** on the Supervisor 720, the command output sometimes shows that the Cisco WiSM service port is down. The service port on the WiSM is not pingable from either the Supervisor 720 or the WiSM, and no traffic can pass to the service port on the WiSM.

  Workaround: Reset the Cisco WiSM.

- CSCso22875—During code download, some access points might disconnect and then reconnect to the controller.

  Workaround: None.

- CSCso23079—When a 7921 phone that is connected to a 1242 series access point using 802.11a receives multicast voice traffic, the audio is sometimes choppy and garbled.

  Workaround: Choose a lower mandatory basic data rate such as 12 Mbps and make sure that 24 Mbps is set to Supported, or use 1131 series access points.

- 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.

- CSCso26532—When you have multiple controllers in the same mobility group and Ascom phones on different controllers, only one-way audio is available for the Ascom phones.

  Workaround: None.

- 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.

- CSCso31244—2100 series controllers sometimes freeze randomly.

  Workaround: Manually reset the controllers.

- 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.

- 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."

  Workaround: None.

- 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.

- CSCso40371—The controller GUI does not allow spaces to be included in the primary, secondary, or tertiary controller name for an access point. However, the controller CLI permits spaces in the controller name.

  Workaround: Do not include spaces when configuring the primary, secondary, or tertiary controller for an access point from the controller GUI.

- CSCso46255—After you enable a few debugging commands, the 1250 series access point might reboot. All clients are dropped and have to reassociate.

  Workaround: Do not disable or enable radio interfaces while enabling debug commands.

- CSCso46517—If you try to change the access or quarantine VLAN to a VLAN that already exists on the controller, one of two error messages appears. The same error message should appear regardless of whether you are attempting to change the access or quarantine VLAN, and it should provide more detailed information.

  Workaround: None.

- CSCso47897—When the controller is connected to a switch, the MAC address table on the switch sometimes shows an invalid MAC address coming from the interfaces attached to the controller.

  Workaround: None.

- 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.

  Workaround: None.

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

  Workaround: Remove the PAC from the client.

- 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.

- 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.

  Workaround: Enable the management-over-dynamic interface or configure the SNMP station to use the dynamic interface instead of the management interface.

- CSCso52692—When NAC out-of-band mode is enabled and a client roams from quarantine to access on a foreign controller, it generates message logs with tracebacks, which can be confusing to an end user.

  Workaround: None.

- CSCso52700—In a guest anchor setup, roaming does not work for a workgroup bridge (WGB) access point, neither in the access state nor in the quarantine state. This problem occurs when the WGB access point associates to the anchor controller first and then roams to a foreign controller in the quarantine or access state.

  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.

- CSCso57867—When a client connected to a WLAN configured for mobility anchoring roams between two controllers, mobility anchoring fails on the controller to which the client roams. When you look at the client details on the controller where the client anchoring failed, it shows the anchor as the controller from which the client roamed, not the configured mobility anchor.

  Workaround: Join all access points that the client could roam between to the same controller.

- 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.

- CSCso60944—A controller running software release 5.0.148.0 might show an incorrect IP address in the Connection From field on the controller GUI and in the output of the **show loginsession** CLI command. This behavior is random, and the IP address shown is also random.

  Workaround: Reboot the controller and try multiple times until you see the correct IP address.

- 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.

  Workaround: Use the proper and complete **show hreap group detail** *groupname* CLI command.

- 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.

  Workaround: None.

- CSCso65170—The controller might reboot due to a software failure of the instruction located at 0x108d7c70 (ssh_pm_rule_set_ip+84).

  Workaround: None.

- CSCso65546—A controller running software release 4.1.185.0 might crash with different crash files.

  Workaround: None.

- 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.

- 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.

  Workaround: None.

- CSCso68457—Users are unable to configure an external web authentication server on a controller running software release 5.0 or 4.1 through the WCS template.

  Workaround: Manually configure the external web authentication server on the controller.

- 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.

- CSCso70770—If you downgrade the controller from software release 5.1 to 4.2, the hybrid-REAP group configuration is lost.

  Workaround: Remove all hybrid-REAP groups before downgrading the controller.

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

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

  Workaround: None.

- CSCso72588—When you use the wired guest feature, an accounting stop record is not sent after the timeouts expire.

  Workaround: None.

- CSCso74625—A 4400 series controller running software release 4.2.112.0 might reboot with task name dot11a.

  Workaround: None.

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

  Workaround: None.

- 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.

  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.

- CSCso86463—Some access points running software release 4.2.99.0 might crash if traffic stream metrics (TSM) is enabled.

  Workaround: Disable TSM for voice.

- CSCso87099—Network access control (NAC) does not work when workgroup bridge (WGB) access points and wired clients roam in the quarantine state in the same subnet mobility setup.

  Workaround: Roam WGB access points only when wired clients have completed posture validation and moved from the quarantine to the access state.

- 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**}.

- CSCso89810—When you downgrade a controller from software release 5.0.148.*x* to 4.2.112.0, the LWAPP mode automatically changes from Layer 3 to Layer 2, and the AP-manager disappears and cannot be recreated.

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

- 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.

  Workaround: Re-enter the key with only one colon between each pair of digits. If you do enter extra colons with the correct number of hexadecimal digits, the correct key is set.

- CSCso92249—The controller sometimes reboots without a crash log when you run multiple Telnet sessions.

  Workaround: None.

- CSCso93216—When the controller is running software release 5.0.148.0, the associated access points might reboot many times a day.

  Workaround: Reboot each access point.

- 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.

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

  Workaround: None.

- 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.

- CSCsq01789—The access point continues to acknowledge unassociated clients without sending a deauthentication request.

  Workaround: None.

- 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
  ```

  Workaround: Reboot the controller.

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

  Workaround: None.

- 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.

  Workaround: Reset the access point from the controller to disable the radio. Then power cycle the access point and allow it to join with the radio disabled.

- 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.

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

  Workaround: None.

- CSCsq12776—The controller might crash without generating a crash file.

  Workaround: None.

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

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

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

  Workaround: None.

- CSCsq14833—When using VLSM, if the fourth octect of the management IP address is the same as the fourth octect 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.

- CSCsq15258—A controller running software release 4.2.61.0 might reboot due to a software failure of the instruction located at 0x46464644 (ber_int_sb_write+898372620).

  Workaround: None.

- 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.

- CSCsq15707—If you have twenty hybrid-REAP groups configured and delete them one by one on the controller GUI, the controller does not save the configuration.

  Workaround: Use the controller CLI to delete the hybrid-REAP groups one by one; then save the configuration using the 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.

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

  Workaround: None.

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

  Workaround: None.

- CSCsq20148—The apfRogueTask is leaking 316 bytes of memory periodically with only one access point connected.

  Workaround: Reboot the controller periodically, or reconfigure the controller.

- 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.

- CSCsq22805—The Cisco WiSM appears to be incorrectly sending all discovery replies to a single access point, regardless of which access point originated the request.

  Workaround: Downgrade to the previous controller release.

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

  Workaround: None.

- CSCsq23398—The 4404 controller might crash when 100 access points continuously download the controller software.

  Workaround: None.

- CSCsq23460—The sample time for client statistics is not accurate in WCS.

  Workaround: None.

- CSCsq23587—1250 series access points might show the incorrect UP time after running for a couple days in a mixed radio environment with heavy traffic.

  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.

- CSCsq23961—An orphan packet from the distribution system port might prevent DHCP from operating properly.

  Workaround: None.

- 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.

  Workaround: None.

- CSCsq24256—The mobility anchor feature might not work properly for a controller running software release 4.2.121.0.

  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.

- CSCsq25844—The 4400 series controller might crash due to a software failure of the NPUCheckTask.

  Workaround: Reboot the controller.

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

  Workaround: 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.

- CSCsq29950—The Controller Network Module and the 2100 series controllers sometimes report the following unknown syslog message: “Unable to find an ACL by name "".”

  Workaround: None.

- CSCsq30071—The Controller Network Module does not boot up normally after being downgraded from software release 4.1.185.0 to 4.0.219.0.

  Workaround: RMA the controller.

- CSCsq30276—A controller running software release 4.2.121.0 might crash when you apply a CPU ACL.

  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.

- CSCsq31294—After you downgrade the Controller Network Module to a software release prior to 4.1, the module ends up on the ServicesEngine boot-loader> prompt.

  Workaround: Do not downgrade the Controller Network Module to a software release prior to 4.1. This controller supports software release 4.1 or later.

- 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.

- CSCsq32279—An access point group VLAN can be mapped to a wired guest LAN interface.

  Workaround: None.

- CSCsq32721—After controller software release 5.1 is downloaded on a 3201 access point, the access point can join the controller and is configurable through the controller, but you no longer have access to the access point console.

  Workaround: None.

- 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.

  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.

- CSCsq34314—You can use the controller CLI to create a local guest user with a lifetime of 0 (no limit) for a WLAN that has web passthrough enabled. If you specify any finite value, the local netuser is not created.

  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.

- CSCsq35662—More debug messages are needed when an access point fails to download the software image from the controller.

  Workaround: None.

- CSCsq35990—The **config netuser lifetime** CLI command does not accept a zero (0) value for the *lifetime* parameter.

  Workaround: Delete the guest user and recreate it with a zero lifetime.

- 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.

- CSCsq40871—When a wireless client first boots up and joins the wireless network, it is moved from the untrusted to the trusted pool on the network access control (NAC) side while the authentication process takes place on the controller side. This process works correctly. However, if you introduce a second controller, when the client roams from an access point on controller 1 to an access point on controller 2, the client has to be moved from the trusted to the untrusted pool and back again to the trusted pool. This process takes some time, disrupting client connectivity.

  Workaround: Disable NAC.

- CSCsq41115—Hybrid-REAP access points do not show any nearby neighbor access points.

  Workaround: Change the access point mode to local.

- CSCsq41724—In an environment with mixed traffic and different radio clients, 2.4-GHz probes are disabled after the radios are reset a few times. Clients disassociate, reassociate, and pass traffic during the radio reset.

  Workaround: None.

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

  Workaround: None.

- CSCsq46045—1130 series access points joined to a controller running software release 5.0.148.0 might crash periodically and enter a continuous reboot cycle.

  Workaround: Physically reboot the access points.

- 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.

- CSCsq47516—If you downgrade a 2106 controller from software release 4.2.130.0 to 4.2.112.0 for a directly connected 1230 series access point, the access point joins but might not load the new image.

  Workaround: Connect the access point using Layer 3 (not a direct connection), or reset the controller and wait for the access point to join.

- 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.

  Workaround: Use the **show services mobility detail all** CLI command, which provides information for all the connections.

- 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.

- 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.

  Workaround: None.

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

  Workaround: Reboot the controller.

- CSCsq50866—When you configure QoS data rates for a guest role using the controller CLI, you can set values greater than 60000.

  Workaround: Use the controller GUI to set the guest role QoS data rate values.

- CSCsq51206—When you downgrade the controller from software release 4.2.130.0 to 4.1, the **show sysinfo** CLI command displays 4.2 as the RTOS version and "Error" as the bootloader version.

  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.

- CSCsq55117—The controller might reboot when multiple people are connected through Telnet at the same time.

  Workaround: None.

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

  Workaround: None.

- CSCsq57697—WPA2 PMK cache updates are not being sent across the mobility group.

  Workaround: Enable CCKM on the client and the WLAN.

- CSCsq58812—When you attempt to download a file from WCS to a controller running software release 5.1, the controller might reboot due to a failure of the spamReceiveTask.

  Workaround: None.

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

  Workaround: None.

- CSCsq58895—The following message appears in the log of a controller running software release 4.2 when a Cisco 7920 or 7921 phone roams: "APF-4-CREATE_PMK_CACHE_FAILED." This condition prevents fast roaming from working properly.

  Workaround: None.

- CSCsq59117—If an access point that is configured for WLAN override joins a new controller that is missing some of the WLANs that were configured to broadcast in WLAN override, the WLANs that were missing show up as unselected in WLAN override when the access point rejoins the original controller.

  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.

- CSCsq62347—A 1010 series access point running software release 4.1.185.0, 4.2.112.0, or 4.2.130.0 might reload or disconnect from the network after running for 70 to80 days. The amount of available memory on the access point also drops continuously as the uptime of the access point increases.

  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.

- CSCsq66390—The client statistics for excessive retries and the retries counter are always zero.

  Workaround: None.

- CSCsq67583—The controller sometimes generates unpredictable interference device IDs, which prevents you from being able to compare IDR messages and determine whether they indicate an update for an existing device or a new device notification.

  Workaround: None.

- 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.

- CSCsq69040—Traffic stream metrics (TMS) reports are not appearing on the controller GUI for a Cisco 7921 phone using WPA with a 1231 series access point on the 802.11b/g network.

  Workaround: Use the controller CLI to view TSM values.

- CSCsq69458—After you set 802.11b/g RRM transmit power control (TPC) or dynamic channel assignment (DCA) to On Demand on a controller running software release 5.0.148.0, the refresh page displays 802.11a information instead of 802.11b/g information.

  Workaround: Use the controller CLI.

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

  Workaround: None.

- CSCsq71302—Lock asserts might appear on the console of a Cisco WiSM.

  Workaround: None.

- CSCsq72954—When an 802.11n client connects to a 1252 access point using 40 MHz, the transmission speed shows 144 Mbps rather than 300 Mbps.

  Workaround: None.

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

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

- 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.

- CSCsq73939—When a client switches from a centrally switched WLAN to a locally switched WLAN on the same access point, it sometimes fails to obtain an IP address from the DHCP server.

  Workaround: Deactivate the radio from the client before switching, introducing a delay in the operation.

- 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.

- CSCsq74610—Clients fail to get a DHCP address from the external server on the initial attempt when running controller software release 4.2.130.0.

  Workaround: Perform a repair on the client, and it should get an IP address on the second attempt.

- CSCsq74644—The controller and access point sometimes accept invalid TSPECs.

  Workaround: None.

- CSCsq75541—If you create a permanent guest user and then change the lifetime to 800 seconds and change the WLAN to any WLAN, an incorrect error message appears.

  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.

- CSCsq78913—The console port on a Cisco WiSM controller might stop responding.

  Workaround: None.

- CSCsq82104—The controller might generate the following traceback messages. The traceback numbers vary from build to build, but the message text is consistent.

```
Jun 18 14:07:28 192.168.200.15 cntl4404_1: *Jun 18 14:07:28.240:
%APF-1-AUTHMOBILE_SEND_FAILED: apf_rogue_detect.c:683 Could not send the LWAPP
Authenticate Mobile command to rogue AP 00:17:0f:d8:e6:e0  for mobile
00:17:0f:d8:e6:e1. Unable to find rogue client. 10105244 1044e158 10c710ac 10f1672c -
this is due to the failure of an AP to associate to a rogue AP when RLDP is enabled.
Jun 18 14:15:02 192.168.200.15 cntl4404_1: *Jun 18 14:14:12.574:
%DOT1X-3-INVALID_CLIENT_DOT1X_CB: dot1x_api.c:48 Missing 802.1X control block for
client 00:01:6c:2d:89:8d10163c48 10621154 101ab490 101dc56c 106237e8 1044e158 10c710ac
10f1672c - this indicates a client is failing to associate with WPA authentication.
```

  Workaround: None. These messages do not affect system operation.

- 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.

- CSCsr00444—The controller might intermittently become inaccessible.

  Workaround: Follow these steps to clear the configuration using the Boot ROM menu:

  1. Reboot the controller.
  2. Press **ESC** when prompted.
  3. Choose **Option 5** to clear the configuration.

- CSCsr44439—When you downgrade from software release 5.0.148.2 to controller software release 4.2.130, client devices sometimes fail WebAuth when they authenticate to the controller using Wired Guest Access.

  Workaround: If you downgrade to software release 4.2.130, save the controller configuration before the downgrade and reload it after the downgrade.

Resolved Caveats

These caveats are resolved in controller software release 5.0.148.2:

- CSCsl41757—Special characters no longer cause an XML parsing error.
- CSCsm71840—Mobile client handoff or client guest anchoring no longer fails across mobility groups if the controller to which the client is associating has no other mobility member in its own mobility group but has all members in different groups.
- CSCsm86125—Controllers running software release 5.0.148.0 sometimes crash when authenticating clients using 802.1x.
- CSCsm98250—Webauth stops working after you upgrade the controller to software release 5.0.148.0.
- CSCsm99941—Controllers no longer crash, reboot, and create crash logs when rogue client and access point polling is enabled on location appliances.

- CSCso66819—The service port becomes unreachable on WiSM controllers running software release 5.0.148.0.
- CSCso97157—Mobility code no longer contains a memory leak.

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 LAN Controller Online Help*
- *Cisco Wireless Control System Configuration Guide*
- *Cisco Wireless Control System Online Help*

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 this URL:

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