Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 5.2.178.0

February 10, 2009

Note Unlike controller software release 5.2.157.0, the 5.2.178.0 release is supported for use in Japan.

These release notes describe open and resolved caveats for software release 5.2.178.0 for Cisco 2100 and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSMs); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; Cisco 3201 Wireless Mobile Interface Cards (WMICs); Cisco Aironet 1100, 1130, 1140, 1200, 1230AG, 1240, 1250, 1300, and AP801 Series Lightweight Access Points; and Cisco Aironet 1130AG, 1240AG, 1522, and 1524 Mesh Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.

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

Contents

These release notes contain the following sections.

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

Cisco Unified Wireless Network Solution Components

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

- Software release 5.2.178.0 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 3.0
- Cisco Wireless Control System (WCS) software release 5.2.130.0
- Cisco WCS Navigator 1.4.130.0
- Location appliance software release 5.2.91.0
- Cisco 2700 Series Location Appliances
- Mobility services engine software release 5.2.91.0 and Context Aware Software

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

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

Note The 5.2.178.0 release does not support the NM-AIR-WLC6 platform.

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

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

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

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

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

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

Controller Requirements

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

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

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

MIB Files

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

Software Release Information

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

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

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

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

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

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

Finding the Software Release

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

Special Rules for Upgrading to Controller Software Release 5.2.178.0

Caution Before upgrading your controller to software release 5.2.178.0, you must comply with the following rules.

- Before you use an AP801 series lightweight access point with controller software release 5.2.178.0, you must upgrade the software in the Cisco 800 Series Integrated Services Router (ISR) to Cisco IOS Release 12.4(22)T.
- Make sure you have a TFTP or FTP server available for the software upgrade. Keep these guidelines in mind when setting up a TFTP or FTP server:
  - Controller software release 5.2.178.0 is larger than 32 MB; therefore, you must make sure that your TFTP server supports files that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd and the TFTP server within the WCS. If you attempt to download the 5.2.178.0 controller software and your TFTP server does not support files of this size, the following error message appears: “TFTP failure while storing in flash.”

  - If you are upgrading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.
- Cisco Controller 520 is a supported platform for Release 5.2.178.0. During upgrade from Release 4.1.154.22 to 5.2.178.0, the configuration is not retained. You can use 4.2.61 as a middle release to upgrade.
- You can upgrade or downgrade the controller software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to software release 5.2.178.0. Table 1 shows the upgrade path that you must follow before downloading software release 5.2.178.0.

Table 1 Upgrade Path to Controller Software Release 5.2.178.0

Current Software Release	Upgrade Path to 5.2.178.0 Software
3.2.78.0 or later 3.2 release	Upgrade to 4.0.206.0 or later 4.0 release, then upgrade to 4.2.176.0, before upgrading to 5.2.178.0.
4.0.155.5 or later 4.0 release	Upgrade to 4.2.176.0 before upgrading to 5.2.178.0.
4.1.171.0 or later 4.1 release	Upgrade to 4.2.176.0 before upgrading to 5.2.178.0.
4.1.191.xM or 4.1.192.xM	You can upgrade directly to 5.2.178.0.
4.2.61.0, 4.2.99.0, or 4.2.112.0	Upgrade to 4.2.176.0 or to a 5.1 release before upgrading to 5.2.178.0.
4.2.130.0	Upgrade to 4.2.176.0 before upgrading to 5.2.178.0.
4.2.173.0	You can upgrade directly to 5.2.178.0.
4.2.176.0 or later 4.2 release	You can upgrade directly to 5.2.178.0.
5.0.148.0 or later 5.0 release	You can upgrade directly to 5.2.178.0.
5.1.151.0 or later 5.1 release	You can upgrade directly to 5.2.178.0.
5.2.157.0	You can upgrade directly to 5.2.178.0.

Note When you upgrade the controller to an intermediate software release, wait until all of the access points joined to the controller are upgraded to the intermediate release before you install the 5.2.178.0 software. In large networks, it can take some time to download the software on each access point.

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

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

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

Special Rules for Upgrading to Controller Software 5.2.178.0 in Mesh Networks

Caution Before upgrading your controller to software release 5.2.178.0 in a mesh network, you must comply with the following rules.

Upgrade Compatibility Matrix

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

Software Upgrade Notes

- You can upgrade from all mesh releases to controller software release 5.2.178.0 without any configuration file loss.

  Note If you downgrade to a mesh release, you must then reconfigure the controller. Cisco recommends that you save the configuration from the mesh release before upgrading to release 5.2.178.0 for the first time. Then you can reapply the configuration if you need to downgrade.

- You cannot downgrade from controller software release 5.2.178.0 to a mesh release (4.1.190.5, 4.1.191.22M, or 4.1.192.xM) without losing your configuration settings.
- Configuration files are in the binary state immediately after upgrade from a mesh release to controller software release 5.2.178.0. After reset, the XML configuration file is selected.
- Do not edit XML files.
- Any field with an invalid value is filtered out and set to default by the XML validation engine. Validation occurs during bootup.
- If you upgrade the controller from software release 4.1.191.xM to 4.1.192.xM and then to software release 5.2.178.0, the controller might reboot without a crash file. To work around this problem, manually reset the controller without saving the configuration after you upgrade the controller to software release 5.2.178.0. Also, make sure to check the RRM configuration settings after the reset to verify that they are correct (CSCsv50357).

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

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

1. You can upgrade directly from software release 4.1.190.5 to 4.1.192.35M; however, upgrading to 4.1.191.24M before upgrading to 4.1.192.35M is highly recommended.
2. CUSTOMERS WHO REQUIRE DYNAMIC FREQUENCY SELECTION (DFS) FUNCTIONALITY SHOULD NOT USE THIS RELEASE. This release does not provide DFS functionality fixes found in release 4.0.217.204. Additionally, this release is not supported in ETSI-compliant countries or Singapore.
3. Release 4.0.217.204 provides fixes for DFS on 1510 series access points. This functionality is needed only in countries where DFS rules apply.

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

Upgrading to a New Software Release

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

Caution Do not power down the controller or any access point during this process; otherwise, you might corrupt the software image. Upgrading a controller with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported in software release 4.0.206.0 and later, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Note In controller software release 5.2.178.0, the WLAN override feature has been removed from both the controller GUI and CLI. If your controller is configured for WLAN override and you upgrade to controller software release 5.2.178.0, the controller deletes the WLAN configuration and broadcasts all WLANs. You can specify that only certain WLANs be transmitted by configuring access point groups. Each access point advertises only the enabled WLANs that belong to its access point group. Access point groups do not enable WLANs to be transmitted on per-radio interface of AP.

Note Do not install the 5.2.178.0 controller software file and the 5.2.157.0 ER.aes boot software file at the same time. Install one file and reboot the controller; then install the other file and reboot the controller.

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

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

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

Step 2 Follow these steps to obtain the 5.2.178.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file from the Software Center on Cisco.com:

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

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

b. Click **Wireless Software**.

c. Click **Wireless LAN Controllers**.

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

e. Click a controller series.

f. If necessary, click a controller model.

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

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

i. Click a controller software release. The software releases are labeled as follows to help you determine which release to download:

- **Early Deployment (ED)**—These software releases provide new features and new hardware platform support as well as bug fixes.
- **Maintenance Deployment (MD)**—These software releases provide bug fixes and ongoing software maintenance.
- **Deferred (DF)**—These software releases have been deferred. Cisco recommends that you migrate to an upgraded release.

j. Click a software release number.

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

l. Click **Download**.

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

n. Save the file to your hard drive.

o. Repeat steps a. through n. to download the remaining file (either the 5.2.178.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

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

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

Step 5 Disable any WLANs on the controller.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 18 After the controller reboots, repeat Step 6 to Step 17 to install the remaining file (either the 5.2.178.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.2.157.0 ER.aes file).

Step 19 Re-enable the WLANs.

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

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

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

Step 23 To verify that the 5.2.178.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

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

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

Installation Notes

This section contains important information to keep in mind when installing controllers and access points.

Warnings

Warning **This warning means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.**

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

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

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

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground connector. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

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

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

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

Warning **In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft. (2 m) from your body or nearby persons.**

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

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the controllers and access points.

FCC Safety Compliance Statement

FCC Compliance with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

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

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

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.
2. Select your installation site with safety as well as performance in mind. Electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
3. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.
4. Plan your installation carefully and completely before you begin. Successfully raising a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
5. When installing an antenna, remember:
   a. **Do not** use a metal ladder.
   b. **Do not** work on a wet or windy day.
   c. **Do** dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.
6. If the assembly starts to drop, get away from it and let it fall. Remember that the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer: **you!**
7. If any part of an antenna system should come in contact with a power line, **do not touch it or try to remove it yourself. Call your local power company**. They will remove it safely.
8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

Refer to the appropriate quick start guide or hardware installation guide for instructions on installing controllers and access points.

Note To meet regulatory restrictions, all external antenna configurations must be professionally installed.

Personnel installing the controllers and access points must understand wireless techniques and grounding methods. Access points with internal antennas can be installed by an experienced IT professional.

The controller must be installed by a network administrator or qualified IT professional, and the proper country code must be selected. Following installation, access to the controller should be password protected by the installer to maintain compliance with regulatory requirements and ensure proper unit functionality.

Important Notes for Controllers and Non-Mesh Access Points

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

FIPS 140-2

The Cisco 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch have received NIST FIPS 140-2 Level 2 certification. Click this link to view the NIST Security Policies and compliant software versions:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

Internal DHCP Server

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

CAPWAP Problems with Firewalls and ACLs

If you have a firewall or access control list (ACL) between the controller and its access points that allows LWAPP traffic, before upgrading to software release 5.2 and CAPWAP, you should allow CAPWAP traffic from the access points to the controller by opening the following destination ports:

- UDP 5246
- UDP 5247

The access points use a random UDP source port to reach these destination ports on the controller. In controller software release 5.2, LWAPP was removed and replaced by CAPWAP, but if you have a new out-of-the-box access point, it could try to use LWAPP to contact the controller before downloading the CAPWAP image from the controller. Once the access point downloads the CAPWAP image from the controller, it uses only CAPWAP to communicate with the controller.

Note After 60 seconds of trying to join a controller with CAPWAP, the access point falls back to using LWAPP. If it cannot find a controller using LWAPP within 60 seconds, it tries again to join a controller using CAPWAP. The access point repeats this cycle of switching from CAPWAP to LWAPP and back again every 60 seconds until it joins a controller.

Note An access point with the LWAPP recovery image (an access point converted from autonomous mode or an out-of-the-box access point) uses only LWAPP to try to join a controller before downloading the CAPWAP image from the controller.

Messages Appearing Upon Controller Bootup

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

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

Web Authentication Redirects

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

PLM Location Commands

The **config**, **show**, and **debug location plm** path loss measurement location commands are not supported in controller software release 5.2.178.0, even though they appear in the CLI code.

Cisco 1250 Series Access Points and Cisco 7920 IP Phones

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

Crash Files for 1250 Series Access Points

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

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

Configuration File Stored in XML

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

Note You cannot download a binary configuration file onto a controller running software release 5.2.178.0. Also, do not attempt to make changes to the configuration file. If you do so and then download the file to a controller, the controller displays a cyclic redundancy checksum (CRC) error while it is rebooting and returns the configuration parameters to their default values.

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

LWAPP Mode Changes

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

If you downgrade from controller software release 5.2.178.0, 5.2.157.0, 5.1.151.0, or 5.0.148.0 to 4.2.61.0 or an earlier release, the LWAPP mode changes from Layer 3 to Layer 2. Access points might not join the controller, and you must manually reset the controller to Layer 3 to resolve this issue.

Access Points Send Multicast and Management Frames at Highest Basic Rate

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

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

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

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

Disabling Radio Bands

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

40-MHz Channels in the 2.4-GHz Band

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

Impact of External Antenna Gain on Transmit Power

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

Supporting Oversized Access Point Images

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

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

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

Follow these steps to recover the access point using the TFTP recovery procedure.

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

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

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

Multicast Queue Depth

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

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

MAC Filtering for WGB Wired Clients

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

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

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

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

CKIP Not Supported with Dynamic WEP

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

Setting the Date and Time on the Controller

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

Synchronizing the Controller and Location Appliance

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

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

FCC DFS Support on 1130 Series Access Points

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

Inaccurate Transmit Power Display

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

Setting the Retransmit Timeout Value for TACACS+ Servers

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

Configuring an Access Point's Prestandard Power Setting

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

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

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

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

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

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

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

Controller Functions that Require a Reboot

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

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

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

2106 Controller LEDs

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

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

Rate-Limiting on the Controller

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

Pings Supported to the Management Interface of the Controller

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

Pinging from a Network Device to a Controller Dynamic Interface

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

GLBP Not Supported

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

IPSec Not Supported

Software release 5.2.178.0 does not allow you to choose IPSec as a Layer 3 security option. None and VPN Passthrough are the only available options. If you upgrade to this release from a previous release that supported IPSec as a Layer 3 security option, any WLANs that are configured for this feature become disabled. If you want to configure IPSec, you must use a version of controller software prior to 4.0.

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

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

Connecting 1100 and 1300 Series Access Points

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

Preventing Clients from Accessing the Management Network on a Controller

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

Voice Wireless LAN Configuration

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

Changing the IOS LWAPP Access Point Password

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

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

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

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

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

“ERROR!!! Command is disabled.”

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

Exclusion List (Blacklist) Client Feature

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

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

RADIUS Servers and the Management VLAN

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

RADIUS Servers

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

Management Usernames and Local Netuser Names

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

802.1X and Microsoft Wireless Configuration Manager

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

Using the Backup Image

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

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

Home Page Retains Web Authentication Login with IE 5.x

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

Rogue Location Discovery Protocol (RLDP)

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

Ad-Hoc Rogue Containment

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

Changing the Default Values of SNMP Community Strings

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

Changing the Default Values for SNMP v3 Users

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

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

Features Not Supported on 2100 Series Controllers

This hardware feature is not supported on 2100 series controllers:

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

These software features are not supported on 2100 series controllers:

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

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

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

2106 Image Not Supported for 3504 Controllers

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

Running a 3504 Image on a 2106 Series Controller

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

Upgrading External Web Authentication

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

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

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

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

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

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

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

function submitAction(){
     var link = document.location.href;
     var searchString = "redirect=";
     var equalIndex = link.indexOf(searchString);
     var redirectUrl = "";
     var urlStr = "";
     if(equalIndex > 0) {
            equalIndex += searchString.length;
            urlStr = link.substring(equalIndex);
            if(urlStr.length > 0){
```

```
   redirectUrl += urlStr;
         if(redirectUrl.length > 255)
        redirectUrl = redirectUrl.substring(0,255);
       document.forms[0].redirect_url.value = redirectUrl;
  }
     }

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

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

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

}

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

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

Important Notes for Controllers and Mesh Access Points

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

Access Point Support Limit on Cisco WiSMs

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

Bridge MAC Filter Config Status Shown in Error

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

Limit Bridge Group Names to 11 Characters

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

Monitoring Port LED Status on a 1520 Series Access Point

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

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

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

Warning Message for Access Point Bridging Disable Requests

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

Warning Message for Antenna Gain Changes

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

Message for LinkTest Limitations

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

Features Not Supported on Mesh Networks

The following controller features are not supported on mesh networks:

- Multi-country support
- Load-based CAC (Mesh networks support only bandwidth-based, or static, CAC.)
- High availability (fast heartbeat and primary discovery join timer)
- EAP-FASTv1 and 802.1X authentication
- Access point join priority (Mesh access points have a fixed priority.)
- Locally significant certificate
- Location-based services

Caveats

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

Open Caveats

These caveats are open in controller software release 5.2.178.0.

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

  Workaround: None.

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

  Workaround: Use the controller CLI.

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

  Workaround: Users can interpret the **None** option as Static and a logical alternative to DHCP.

- CSCse06202—When a controller's IKE lifetime expires, a rekey is not offered.

  Workaround: Increase the length of the IKE timeout.

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

  Workaround: Increase the length of the IKE timeout.

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

  Workaround: Use a wireless sniffer trace.

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

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

  a. Remove **Conditional Web Redirect** and save your change.
  b. Change Layer 2 to **802.1X** and save your change.
  c. Change Layer 3 to **Conditional Web Redirect** and save your change.

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

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

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

  Workaround: None.

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

  Workaround: None. The master controller configuration is not persistent by design.

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

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

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

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

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

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

  Example:

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

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

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

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

  Workaround: None.

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

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

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

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

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

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

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

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

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

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

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

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

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

  Workaround: None.

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

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

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

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

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

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

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Enter a valid netmask.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

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

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

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

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

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

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

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

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

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

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

  Workaround: Disable the master controller mode.

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

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

  Workaround: Follow these steps:

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

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

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

  Workaround: None.

- CSCsm40870—The following error message should be reworded:

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

  The message should read as follows:

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

  Workaround: None.

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

  Workaround: Create an access list with rules.

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

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

  Workaround: None.

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

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

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

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

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

  Workaround: None.

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

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

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

  Workaround: Use the controller CLI to display users.

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

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

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

  Workaround: None.

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

  Workaround: Remove the PAC from the client.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

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

- CSCsq14030—With mesh software release 4.1.192.17M, you cannot configure a static IP address for an access point in local mode. The edit field does not appear.

  Workaround: Use the **config ap static-IP enable** controller CLI command to configure the IP address.

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

  Workaround: Change the IP address of the management interface.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Use the controller CLI.

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

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

  Workaround: None.

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

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

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

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

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

  Workaround: None.

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

  Workaround: Authenticate the clients using another WLAN.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: You can safely ignore this message.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- 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.

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

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

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

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

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

  Workaround: Clear rogue access points from your network.

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

  Workaround: None.

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

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

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

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

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

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

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

  Workaround: None.

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

  Workaround: Set a smaller value.

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: You can safely ignore this message.

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

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

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

  Workaround: None.

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

  Workaround: Re-enter the access point credentials.

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

  Workaround: None.

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

  Workaround: Configure the clients with a static IPv6 address.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

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

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

  Workaround: None.

- CSCsr49364—When a dynamic frequency selection (DFS) event occurs, the access point fails to populate the next 10 beacons with information element (IE) 37 (the channel switch announce IE). The access point also fails to send a broadcast channel switch announce action frame to alert associated 802.11h clients to move to the new channel.

  Workaround: None.

- CSCsr49559—The 802.11a radio in mesh access points sometimes adds an unnecessary extra byte in the country information element (IE 7) in the beacons.

  Workaround: None.

- CSCsr51667—When you use the GUI to refresh the message logs of a controller running software release 4.2.130.0, a "Connection interrupted/page load" error might appear, and the following message appears in the message logs:

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

  Workaround: Use the controller GUI to navigate to the **Message Logs** page or use the controller CLI to enter the **show msglog** command.

- CSCsr57256—A 1520 access point joined to a 4400 series controller running software release 4.1.192.22M reports an 802.11a radio operational state of UP when the radio is disabled after resetting the access point.

  Workaround: None.

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

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

- CSCsr61016—When you disable the 802.11a radio in a 1520 series access point in root access point (RAP) mode, the radio continues to send beacons, and client devices remain associated to it.

  Workaround: Disable 802.11a client access to force clients to disassociate. However, the radio remains enabled.

- CSCsr70862—A Cisco WiSM controller running software release 4.2.130.0 might reboot because of a software failure of the instruction located at 0x1038a140(ewsInternalAbort+348).

  Workaround: Set the session timeout to zero or remove Telnet access.

- CSCsr72091—The controller radio resource management (RRM) feature sometimes fails to adjust the transmit power on the radios in 1250 series access points.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Use the proper password recovery procedure. Follow the instructions in the "Restoring Passwords" section in Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2*.

- CSCsr83684—When you enable link aggregation (LAG), the source MAC address for dynamic interfaces might change during operation.

  Workaround: None.

- CSCsr85444—The link test does not work for non-Cisco Compatible Extension clients. The following error message appears on the access point CLI: "No response received."

  Workaround: None.

- CSCsr89399—Cisco 1131AG access points that are connected to Cisco WiSM controllers might reboot unexpectedly.

  Workaround: None.

- CSCsr89694—Cisco WiSM controllers running software release 4.2.130.0 generate trap logs indicating that the control path between two random mobility members is down. About 10 to 20 minutes later, the control path comes back up.

  Workaround: Disable guest tunneling.

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

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

- CSCsr91361—The Regulatory link returns a "Page not found" message on the controller GUI in software release 5.1.151.0.

  Workaround: None.

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

  Workaround: Use the controller CLI to classify rogue access points or disable TACACS+.

- CSCsu09424—Cisco 2100 series controllers sometimes reboot unexpectedly when you upgrade from software release 4.2.121.0 to 5.2.157.0.

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

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

  Workaround: Do not set the MTU below 800.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

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

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

  Workaround: Always map both the WLAN and the access point group to the same interface.

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

  Workaround: None.

- CSCsu42414—The controller CLI command **show client ccx rm** *mac_address* **pathloss** does not report correct information.

  Workaround: None.

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

  Workaround: None.

- CSCsu50275—When an1130 or 1240 series access point in bridge mode using mesh code attempts to join a non-mesh controller, the image transfer fails because non-mesh controllers do not contain mesh images.

  Workaround: Delete the *private-multiple-fs* file from the access point flash. After the access point joins a mesh controller, set the access point mode to local.

- CSCsu52247—Tracebacks sometimes appear on the anchor controller in Layer 3 mobility when a client roams from one controller to another.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

- CSCsu60683—Controllers sometimes report that a 1252 series access point in workgroup bridge mode is associated to an access point through the 802.11n radio when in fact it is associated through the 802.11g radio.

  Workaround: None.

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

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

- CSCsu62060—The 4400 series controller might reboot because of a software failure of the tplusTransportThread task.

  Workaround: None.

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

  Workaround: None.

- CSCsu69321—In controller software release 5.2.157.0, if you download a configuration with WPA + 802.1X and PSK security, no XML dependency errors appear.

  Workaround: While downloading the configuration, make sure that WPA + 802.1X and PSK are not both enabled. You should choose either WPA + 802.1X or WPA + PSK.

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

  Workaround: None.

- CSCsu72077—Debug commands sometimes become disabled on the controller several minutes after you enable them.

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

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

  Workaround: None.

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

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

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

  The correct output should be:

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

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

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

  The correct output should be:

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Disable the alarm notifications for ACS servers.

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

  Workaround: Reboot the access points.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

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

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

  Workaround: None.

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

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

  Workaround: None.

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

  Workaround: Clear the configuration and reconfigure the controller.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Clear the controller configuration and reconfigure the controller.

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

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

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

  Workaround: None.

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

  Workaround: Try the upgrade a second time.

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

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

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

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

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

  Workaround: Enable paging or use a Telnet session.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: Use the controller CLI to view the clients.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: Reapply the auto-RF settings.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

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

- CSCsv34136—When an RFC3576 message arrives, the controller enforces a source port check by searching for the server using the IP address and source port in the RFC3576 message rather than searching the configured RADIUS servers list using the same Find Server function as for any other RADIUS message.

  Workaround: Force a fixed source port to be used on the RADIUS server side.

- CSCsv34605—An access point using the Rogue Location Detection Protocol (RLDP) does not obtain a DHCP address if the DHCP server is on an autonomous access point. As a result, RLDP does not detect if a rogue access point is on the wire.

  Workaround: None.

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

  Workaround: None.

- CSCsv35162—One of the following messages appears when you try to designate a local controller as an anchor controller: “Request failed - Failed to add the IP into anchor list” (on the CLI) or “Failed to create anchor switch entry local” (on the GUI).

  Workaround: None. Mobility functionality is not broken.

- CSCsv39373—When you enable the access point fallback feature on the controller, the controller might not recognize client associations (even when clients are associated) because the controller sends a non-MFP protected disassociation message.

  Workaround: Disable MFP client protection.

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

  Workaround: None.

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

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

- CSCsv43156—The trap for an unsuccessful SSH login attempt sometimes shows the wrong IP address.

  Workaround: None.

- CSCsv44917—You can configure radio diversity for a 1250 series access point on the controller GUI, even though this configuration should not be allowed.

  Workaround: None.

- CSCsv47365—When you initiate a link test from the controller GUI or CLI, the controller's control plane (Telnet, SSH, and web sessions) might hang for approximately 1 minute.

  Workaround: Do not initiate a link test from the controller.

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

  Workaround: None.

- CSCsv54436—SSH is sometimes denied on the controller with the following message: "Sorry, telnet is not allowed on this port."

  Workaround: Retry the SSH connection.

- CSCsv56016—When a 2106 controller running software release 5.1.151.0 logs messages to the syslog server, the following error appears: "Invalid IP address, x.x.x.255, x.x.x.0, 127.x.x.x or Class D/E is not permitted."

  Workaround: None.

- CSCsv60932—If you use the GUI to set the RADIUS fallback mode to Active or Passive on a 2106 controller, the default value for the Interval parameter does not fall inside the allowable range.

  Workaround: Use the controller CLI to set the RADIUS fallback mode. The default value for the Interval parameter is 0 in the CLI.

- CSCsv62368—A CPU access control list (ACL) sometimes fails to block ICMP packets.

  Workaround: Wait for 30 seconds for the ACL rule to take effect.

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

  Workaround: None.

- CSCsv64590—After a reboot of the controller, SNMPv3 stops working. The controller running SNMPv3 shows as unreachable in WCS once the controller has been rebooted.

  Workaround: Delete and re-add the SNMPv3 users on the controller any time the controller reboots.

- CSCsv67671—If you configure an 1140 series access point for autonomous or hybrid-REAP mode and map SSIDs to VLANs that do not exist on the controller, the access point produces tracebacks and reboots continuously.

  Workaround: None.

- CSCsv70260—When a Cisco WiSM running software release 5.1.151.0 has TCLAS enabled and uses wireless phones that support TCLAS, the controller might experience up to a 20% downstream packet loss.

  Workaround: Disable TCLAS.

- CSCsv70556—When you create a new dynamic interface, assign a VLAN tag, and then apply the interface settings on the controller GUI, a message appears indicating that no netmask or IP address was added; however, the interface is created.

  Workaround: None.

- CSCsv73455—If you specify a value for the foreign 802.11a/b interference threshold percentage parameter on the controller, the uploaded configuration has a value that is 655 times the value that you entered. This value is incorrect and invalid because the percentage can be a maximum of 100.

  Workaround: None.

- CSCsv74342—Clients associated to a WLAN with the diagnostic channel enabled cannot reach the 2106 controller default gateway management interface.

  Workaround: None.

- CSCsv74572—In a non-link aggregation (non-LAG) setup with both ports plugged into a switch and the switch sending gratuitous ARPs on port 2 for the gateway when the dynamic interface is on port 1, the controller loses gateway access on a single VLAN, and off-subnet hosts (such as DHCP servers) cannot be reached for DHCP.

  Workaround: Enable LAG, or disconnect port 2 by shutting down the switch port.

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

  Workaround: None.

- CSCsv76635—When a controller running software release 4.2.130.0 generates either of the following traps, it sends an incorrect OID to the configured trap receiver: “All mobility anchors on wlan index 1 are down” or “Mobility anchoring is restored on wlan index 1.” As a result, the configured trap receiver does not receive the proper trap message, and you are not notified that the anchor controller went down.

  Workaround: None.

- CSCsv78027—When too many access points are close together, the controller might detect some of the access points as rogue and generate Honeypot traps against them. Normally, the controller generates a Honeypot trap alarm if a rogue access point is using WLANs that are configured on the controller.

  Workaround: Increase the distance between the access points.

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

  Workaround: None.

- CSCsv79601—When multiple SNMP walks or other SNMP activity occurs on the controller, the controller can become unresponsive until the SNMP traffic has completed.

  Workaround: Limit the number of SNMP devices monitoring the controller, or limit the number of SNMP requests sent to the controller.

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

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

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

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

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

  Workaround: None.

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

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

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

  Workaround: Reset the access point.

- CSCsv87385—The controller logs this message when the DHCP packet received on the interface does not contain any DHCP options: "dhcpd.c:206 DHCP-3-MSGTAG095: Bad DHCP packet from *DHCP Server*, dropping."

  Workaround: None.

- CSCsv91377—If you use the following CLI command to download a configuration, the controller returns to factory default settings:

  ```
  config country US,USX,CA,MX,FI,ES,EG,CO,CR,GB,HK,CH,IN,FR,IL,ILO,AU33333333333
  ```

  Workaround: Do not add extra characters with country codes.

- CSCsv91992—The controller does not remove DHCP option 82 in DHCP traffic from the server to the client.

  Workaround: None.

- CSCsv94993—When you enable DHCP Required on a WLAN, passive wired clients behind a workgroup bridge (WGB) might lose their connection to the wireless network.

  Workaround: Use a short DHCP lease, even though some traffic loss might still occur.

- CSCsw14316—The RADIUS accounting and RADIUS authentication server key format should return a default value other than ASCII or HEX.

  Workaround: None.

- CSCsw15327—When you configure rogue access point containment from WCS, the command appears to be accepted and processed. However, the controller does not contain the rogue access point because it is no longer available. WCS shows that the rogue access point is contained, but later the status returns to "Alert" without generating an error message.

  Workaround: None.

- CSCsw17659—A controller running software release 4.2.130.0 does not send an ARP reply to wireless clients and the default gateway. As a result, all wireless clients belonging to the controller fail to resolve ARP, even though they associate, authenticate, and obtain a DHCP IP address.

  Workaround: None.

- CSCsw20879—802.11a clients lose connectivity every 99 seconds when you enable All Channel Scanning for the 802.11a network.

  Workaround: None.

- CSCsw25388—When you change the antenna gain setting on a 1520 series mesh access point, the access point reloads, which might cause downstream mesh access points to go out of service.

  Workaround: Avoid making unnecessary changes to the antenna gain setting.

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

  Workaround: Use the controller CLI instead of the GUI.

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

  Workaround: Ensure that the hybrid-REAP access point can always receive DHCP services.

- CSCsw27841—A controller running software release 5.1.151.0 or 5.2.157.0 allows you to configure multiple untagged VLAN interfaces on the same physical port.

  Workaround: None.

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

  Workaround: None.

- CSCsw29731—A controller running software release 5.2.157.0 should (but does not) drop multicast traffic if the client has the same group address as the access point multicast group.

  Workaround: None.

- CSCsw29804—Lexmark printers that are used with 4400 series controllers running software release 4.2.130.0 or 4.2.176.0 cannot have apple ARP entries on a Layer 3 router and cannot join the Appletalk zone.

  Workaround: None.

- CSCsw34627—When you enter the **show dhcp lease** CLI command on a controller running software release 5.2.157.0, the hours and minutes are omitted in the output.

  Workaround: Use the controller GUI to view the hours and minutes.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Reboot the access point.

- CSCsw40946—The controller might act as an ARP proxy for a locally switched hybrid-REAP client, which might cause problems with the MAC forwarding table of some switches and prevent client traffic from passing properly. This problem occurs only when all devices are on the same subnet and connected to a single switch.

  Workaround: Deploy the hybrid-REAP access point over the WAN or make sure that the addressing between the remote location (where the access point is) and the central location is different.

- CSCsw41668—The Cisco WiSM might reboot and display the following error message on the console: "** LOCK ASSERT ** (pemReceiveTask) !! prio=332 root=400 word=1000."

  Workaround: None.

- CSCsw43518—When an access point is connected directly to a port (such as the Power-over-Ethernet port) on a 2100 series controller and is using the internal DHCP server on the controller, users might not be able to obtain an IP address.

  Workaround: Move the access point to a port that is not on the controller such as another switch.

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

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

- CSCsw46354—The following traceback might appear in the controller message log:

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

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

- CSCsw49530—When the inline power configuration on the controller does not match the physical configuration of the access points, WCS problems (such as template apply failures and poor client tracking) can occur.

  Workaround: Correct the configuration of the controller to match the access points; then refresh the controller's configuration in WCS. You can use these CLI commands to correct the controller power settings for large numbers of access points:

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

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

- CSCsw49636—A Cisco WiSM might reboot because of a software failure of the Reaper Watcher.

  Workaround: None.

- CSCsw50747—The controller GUI should show the emergency/boot image on the controller.

  Workaround: None.

- CSCsw51183—A 2100 series controller running software release 5.2 might reboot because of a software failure of the spamReceiveTask task. This problem occurs when the WAN link to a hybrid-REAP access point fails.

  Workaround: None.

- CSCsw51224—A 2100 series controller running software release 5.2 might reboot because of a software failure of the osapiBsnTimer task. This problem occurs when the WAN link to a hybrid-REAP access point fails.

  Workaround: None.

- CSCsw51658—A Cisco WISM with factory default settings does not acquire an IP address during auto configuration. The behavior occurs only when the Catalyst 6500 switch is running Cisco IOS Release 12.2(33)SXI.

  Workaround: None.

- CSCsw52367—The controller CLI command **debug client** *mac_address* incorrectly shows the following error message when shared authentication is not enabled or shared authentication is failing: "*Dec 05 11:12:52.550: 00:1f:5b:c2:07:a4 Suspected Auto-Immune attack: Not Sending Assoc Response to station on BSSID 00:21:d8:93:cb:00 (status 13)." The message should be changed to reflect the actual problem.

  Workaround: None.

- CSCsw52884—A controller running software release 4.2.176.0 might reboot because of a software failure in the EAP framework.

  Workaround: None.

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

  Workaround: None.

- CSCsw53454—A 4400 series controller reboots if you enable and disable link aggregation (LAG) when an access point tries to join the controller.

  Workaround: None.

- CSCsw65287—You cannot configure a login banner on the controller.

  Workaround: None.

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

  Workaround: None.

- CSCsw73514—The backup controller configuration file does not properly reflect security and radio settings. All WLAN security settings are lost and reset to None. When you disable 802.11g rates, this change is not reflected in the uploaded configuration file. When the file is downloaded, the 802.11g rates are enabled and no security settings are enabled on the WLANs.

  Workaround: Enter these controller CLI commands after you download the configuration file:

  config wlan disable 1

  config wlan security wpa wpa1 enable 1

  config wlan security wpa wpa2 disable 1

  config wlan security wpa wpa1 ciphers tkip enable 1

  config wlan security wpa enable 2

  config wlan security wpa enable 3

  config 802.11b 11gSupport disable

- CSCsw75392—If you configure a WLAN to simultaneously support WPA+TKIP, WPA+AES, and WPA2+AES, 802.11n clients that are configured for WPA2+PSK or WPA2+802.1X can associate only at 802.11a/g data rates even if WPA2+AES is successfully negotiated by the client.

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

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

  Workaround: None.

- CSCsw80153—When a RADIUS server is used for web authentication, a controller running software release 5.1.151.0 might not send any RADIUS requests to the server. This problem pertains only to a specific configuration.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Enter the command in a console session.

- CSCsw85672—When you attempt to change the hybrid-REAP VLAN mapping through the controller GUI, the change appears to be made, but the VLAN tag reverts back to its original setting.

  Workaround: Configure hybrid-REAP VLAN mapping using the controller CLI.

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

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

  Workaround: None. You can safely ignore these messages.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

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

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

- CSCsw90266—For 2100 series controllers and controller network modules, clients associated to a WLAN pointing to a dynamic interface can access the HTTPS, Telnet, and SSH services of the management IP address, regardless of the state of the Management over Wireless setting.

  Workaround: Create a CPU access control list (ACL), denying all traffic from the dynamic interface subnetwork toward the management IP address. Allow all other traffic, or adjust as needed by your security policy. Then apply the ACL as a CPU ACL with Both as the direction setting.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Reset the PC card on the client.

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

  Workaround: None.

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

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

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

  Workaround: Rebooting the controller might stop the problem temporarily.

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

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

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

  Workaround: None.

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

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

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

  Workaround: None.

- CSCsx20559—Point-to-Point Tunneling Protocol (PPTP) connections might fail to be established through a wireless connection with a 2106 controller running software release 5.2.

  Workaround: Downgrade the controller to software release 5.1.

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

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

  Workaround: Ignore the erroneous debug message.

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

  Workaround: None.

- CSCsx29427—The controller might reboot because of a memory corruption error such as "(pmallocProcessMemoryCorruption): pmallocGenericCrashInfo=(++PMALLOC_POISONED_AREA_CORRUPTION)." This corruption occurs on rare occasions and only during heavy loads with a large number of access points.

  Workaround: None.

Resolved Caveats

These caveats are resolved in controller software release 5.2.178.0.

- CSCsg00102—In Cisco IOS Release 12.4(9)T, the TCP stops accepting new connections after a few days of SSLVPN running in the router. The **debug ip tcp transaction** command shows the error with the connection queue limit reached. When the problem happens, the **show tcp bri all** command shows five connections in the Closed state.
- CSCsj25953—When 200 or more wireless clients try to associate to a controller at the same time, the controller might experience these problems: scanners become stuck in the DHCP_REQD state, the CPU runs above 70%, and this message appears: "apf_policy.c:258 APF-1-MOBSTA_ADD_FAILED: Unable to add mobile xx:xx:xx:xx:xx:x to PEM module."
- CSCsl22707—A 1250 series access point using Power over Ethernet (PoE) continually resets when connected to a Catalyst 3550 series switch. This problem is resolved by a new bootloader. New 1250 series access points shipped from the factory contain the new bootloader image [12.4(18a)JA1]. Do not, however, attempt to replace the bootloader in 1250 series access points in the field. Instead, follow the instructions in the workaround below.

  Workaround: For 1250 series access points in the field, use either a power injector or an AC power supply to provide power to the access point, or upgrade the switch to IOS Release 12.1(19)EA1 or later and enter this CLI command to configure the switch to continue providing power during initialization:

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

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

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

- CSCso66778—The output of the **dump-low-level-debugs** command is incomplete for several commands (such as dmesg and ifconfig) in controller software release 5.0 and 4.2.112.0.
- CSCsq35662—More debug messages are needed when access points fail to download the software image from the controller.

- CSCsv42697—The radio interface in an 1140 or 1250 series access point should reboot automatically after experiencing a radio failure.
- CSCsv69899—A controller running software release 5.2.157.0 or earlier randomly reboots and generates a crash file due to a software failure of the spamReceiveTask or pemReceiveTask task.
- CSCsv94146—A 4400 series controller might reboot while using web authentication.
- CSCsw36743—If you create an access point group to associate a WLAN with a dynamic interface, SNMP-get always returns the interface as "management." This problem occurs only when setting the mapping for the first time.
- CSCsw37377—An 1140 series access point shows a low power warning LED sequence (the Status LED cycles through blue, green, red, and off), the radios are held in reset, and the following messages appear on the access point console:

```
*Mar  1 01:22:17.451: %CDP_PD-2-POWER_LOW: All radios disabled -
    LOW_POWER_CLASSIC_NO_INJECTOR_CONFIGURED WS-C2950G-24-EI (0009.e8b3.6010)
*Mar  1 01:22:17.451:  -Verify the required power-injector is installed on this port:
    WS-C2950G-24-EI(Fas 0/16).
*Mar  1 01:22:17.451:  -If a power-injector is installed, issue the command:"power
    inline negotiation injector installed"
```

  This condition occurs when the access point is powered from a power injector but is connected to a switch that supports CDP but cannot provide the full 15.4-W Power over Ethernet (PoE).
- CSCsw38078—An anchor controller running software release 5.2.157.0 might reboot when you view DHCP leases using the GUI.
- CSCsw40474—If you create a WLAN with WPA security using the controller GUI and then change the session timeout value using WCS, the security setting changes to WPA2.
- CSCsw63365—Autonomous access points with a static IP address that have either SSCs or MICs and that have been converted to LWAPP (using the 3.2 LWAPP conversion tool) ignore the DNS resolution of CISCO-LWAPP-CONTROLLER even though they have downloaded the full 5.2.157.0 image from the controller.
- CSCsw68975—SNMP-get shows incorrect values for hybrid-REAP access point VLAN mapping.
- CSCsw73028—After you downgrade a 2106 controller from software release 5.2.178.0 to 4.2.163.0, a 1230 series access point is unable to join the controller.
- CSCsw80042—When you use an 1140 series access point with a controller running software release 5.2, the access point does not use DNS resolution to join the controller.
- CSCsw92335—If you use WCS to set the session timeout for a WLAN with 802.1X, WPA, or WPA2 security, the timeout might not be set on the controller. The default value might be used instead.
- CSCsx19599—A controller running software release 5.2 might reboot because of a software failure of the spamReceiveTask task.
- CSCsx29643—Cisco 802.11n access points that are joined to a controller running software release 5.2 might experience frequent channel changes, which causes a disruption in service.
- CSCsx29956—A 4400 series controller might reboot when it is configured to operate with an LDAP server because of a software failure of the LDAP DB Task 2 task.

If You Need More Information

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at

http://www.cisco.com/en/US/support/index.html

Click **Product Support > Wireless**. Then choose your product and **Troubleshooting** to find information on the problem you are experiencing.

Documentation Updates

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

Omissions

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

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

Related Documentation

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

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

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

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

Obtaining Documentation, Support, and Security Guidelines

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

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