Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 5.1.151.0

July 21, 2008

These release notes describe open and resolved caveats for software release 5.1.151.0 for Cisco 2100 and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSM); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; Cisco 3201 Wireless Mobile Interface Cards (WMICs); and Cisco Aironet 1100, 1130, 1200, 1230AG, 1240, 1250, 1300, and AP801 Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.

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

Contents

These release notes contain the following sections.

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

Cisco Unified Wireless Network Solution Components

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

- Software release 5.1.151.0 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 3.0
- Cisco Wireless Control System (WCS) software release 5.1.64.0
- Cisco WCS Navigator 1.3.64.0
- Location appliance software release 5.1.30.0
- Cisco 2700 Series Location Appliances
- Mobility service engine software release 5.1.30.0 and Context Aware Software

  Note Client and tag licenses are required to retrieve contextual (such as location) information within the Context Aware Software. See the *Release Notes for Cisco 3350 Mobility Services Engine for Software Release 5.1.30.0* for more information.

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

Note The 5.1.151.0 release does not support the NM-AIR-WLC6 platform.

- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1100, 1130, 1200, 1230AG, 1240, 1250, 1300, and AP801 Series Lightweight Access Points

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

Note Cisco Aironet 1000 series access points are not supported for use with controller software release 5.0.148.0 or later.

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

Special Notice for Mesh Networks

Note Do not upgrade to controller software release 5.1.151.0 if you have mesh access points in your network. If your network uses mesh access points, use only mesh-specific releases such as 4.1.192.22M.

Note Cisco WCS software release 5.1.64.0 may be used to manage both mesh and non-mesh controllers (for example, controllers running software release 5.1.151.0 and 4.1.192.22M). You do not need different instances of WCS to manage mesh and non-mesh controllers.

Controller Requirements

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

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

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

MIB Files

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

Software Release Information

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

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

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

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

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

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

Finding the Software Release

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

Upgrading to a New Software Release

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

Note When you downgrade from 5.1.151.0 to 4.2.61.0 or an earlier release, the LWAPP mode may or may not change from Layer 3 to Layer 2, depending on whether the configuration was saved in the earlier image. If the LWAPP mode changes, access points may not join the controller, and you must manually reset the controller to Layer 3 to resolve this problem.

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

Special Rules for Upgrading to Controller Software Release 5.1.151.0

Caution Before upgrading your controller to software release 5.1.151.0, you must comply with the following rules.

- Make sure you have a TFTP or FTP server available for the software upgrade. Keep these guidelines in mind when setting up a TFTP or FTP server:
  - Controller software release 5.1.151.0 is greater than 32 MB; therefore, you must make sure that your TFTP server supports files that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd and the TFTP server within the WCS. If you attempt to download the 5.1.151.0 controller software and your TFTP server does not support files of this size, the following error message appears: "TFTP failure while storing in flash."
  - If you are upgrading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as WCS because the WCS built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.
- You can upgrade or downgrade the controller software only between two releases. To upgrade or downgrade beyond two releases, you must first install an intermediate release. For example, if your controller is running a 4.2 or 5.0 release, you can upgrade your controller directly to software release 5.1.151.0. If your controller is running a 3.2, 4.0, or 4.1 release, you must upgrade your controller to an intermediate release prior to upgrading to 5.1.151.0. Table 1 shows the upgrade path that you must follow before downloading software release 5.1.151.0.

Table 1 Upgrade Path to Controller Software Release 5.1.151.0

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

Note When you upgrade the controller to an intermediate software release, wait until all of the access points joined to the controller are upgraded to the intermediate release before you install the 5.1.151.0 software. In large networks, it can take some time to download the software on each access point.

- Cisco requires you to install the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 ER.aes file on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Wireless LAN Controller Switch. It is optional on other controller platforms. This file resolves CSCso00774 and is necessary to ensure proper operation of the controller. If you do not install this ER.aes file, your controller does not obtain the fix for this defect, and "Error" appears in the Bootloader Version field in the output of the **show sysinfo** command.

  Note When you install the 4.2.112.0 ER.aes file, a new bootloader file is also loaded. This is true for all controllers except the 2106 controller, for which the bootloader is not upgradable.

  Note The ER .aes files are independent from the controller software files. You can run any controller software file with any ER.aes file. However, installing the latest boot software file (4.2.112.0 ER.aes) ensures that the boot software modifications in all of the previous and current boot software ER.aes files are installed.

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

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

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

Note Do not install the 5.1.151.0 controller software file and the 4.2.112.0 ER.aes boot software file at the same time. Install one file and reboot the controller; then install the other file and reboot the controller.

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

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

Step 2 Follow these steps to obtain the 5.1.151.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 ER.aes file from the Software Center on Cisco.com:

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

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

b. Click **Wireless Software**.

c. Click **Wireless LAN Controllers**.

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

e. Click a controller series.

f. If necessary, click a controller model.

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

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

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

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

j. Click a software release number.

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

l. Click **Download**.

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

n. Save the file to your hard drive.

o. Repeat steps a. through n. to download the remaining file (either the 5.1.151.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 ER.aes file).

Step 3 Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 ER.aes file to the default directory on your TFTP or FTP server.

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

Step 5 Disable any WLANs on the controller.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 18 After the controller reboots, repeat Step 6 to Step 17 to install the remaining file (either the 5.1.151.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 ER.aes file).

Step 19 Re-enable the WLANs.

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

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

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

Step 23 To verify that the 5.1.151.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 24 To verify that the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 ER.aes file is installed on your controller, enter the **show sysinfo** command on the controller CLI and look at the Bootloader Version field. "N/A" appears if the ER.aes file is installed successfully. "Error" appears if the 4.2.112.0 ER.aes file is not installed.

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

Software Release Support for Access Points

Table 2 lists the controller software releases that support specific Cisco access points. The First Support column lists the earliest controller software release that supports the access point. For access points that are not supported in ongoing releases, the Last Support column lists the last release that supports the access point.

Table 2 Software Support for Access Points

Access Points		First Support	Last Support
1000 Series	AIR-AP1010	3.0.100.0	4.2.207.0
	AIR-AP1020	3.0.100.0	4.2.207.0
	AIR-AP1030	3.0.100.0	4.2.207.0
	Airespace AS1200	—	4.1.171.0
1100 Series	AIR-LAP1121	4.0.155.0	—
	AIR-LAP1131	3.1.59.24	—
	AIR-LAP1141N	5.2.157.0	—
	AIR-LAP1142N	5.2.157.0	—
1200 Series	AIR-AP1220A	3.1.59.24	—
	AIR-AP1220B	3.1.59.24	—

Table 2 Software Support for Access Points (Continued)

Access Points		First Support	Last Support
1230 Series	AIR-AP1230A	3.1.59.24	—
	AIR-AP1230B	3.1.59.24	—
	AIR-LAP1231G	3.1.59.24	—
	AIR-LAP1232AG	3.1.59.24	—
1240 Series	AIR-LAP1242G	3.1.59.24	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1300 Series	AIR-BR1310G	4.0.155.0	—
1400 Series	Standalone Only	N/A	—
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.176.51M
	AIR-LAP-1510	3.1.59.24	4.2.176.51M
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1524SB	-A, C and N: 6.0 or later	—
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later[1]	—

[1] These access points are supported in the separate 4.1.19x.x Mesh Software Release train or with Release 5.2 or later. These access points are not supported in the 4.2, 5.0, or 5.1 Release trains.

New Features

The following new features are available in controller software release 5.1.151.0.

Note Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.1* for more details and configuration instructions.

Controller Platform Changes

- The 2100 series controllers can now support up to 6, 12, or 25 lightweight access points. Previously, these controllers could support a maximum of 6 access points.

  Note All client connections to the 2100 series controllers are limited to the 10/100 Ethernet uplink port connection between the switch and the controller, even though their connection speeds might be higher. The exception is for access points running in local hybrid-REAP mode because this traffic is switched at the access point level and not forwarded back to the controller.

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

- The controller network module within the Cisco 28/37/38xx Series Integrated Services Router can now support up to 6, 8, 12, or 25 access points (and up to 256, 256, 350, or 350 clients, respectively), depending on the version of the network module. The network module supports these access points through a Fast Ethernet distribution system port (on the NM-AIR-WLC6-K9 6-access-point version) or a Gigabit Ethernet distribution system port (on the 8-, 12-, and 25-access-point versions and on the NME-AIR-WLC6-K9 6-access-point version) that connects the router and the integrated controller. Previously, these modules could support a maximum of 12 access points, and only the NM-AIR-WLC6-K9 6-access-point Fast Ethernet version was available.

New Controller Features

- **40-MHz channelization—**In controller software releases prior to 5.1.151.0, only radios using 20-MHz channelization are supported by dynamic channel assignment (DCA). In controller software release 5.1.151.0, DCA is extended to support 802.11n 40-MHz channels in the 5-GHz band. 40-MHz channelization allows radios to achieve higher instantaneous data rates (potentially 2.25 times higher than 20-MHz channels).

  Note Radios using 40-MHz channelization in the 2.4-GHz band are not supported by DCA.

  You can override the globally configured DCA channel width setting by statically configuring an access point's radio for 20- or 40-MHz mode on the 802.11a/n Cisco APs > Configure page. If you ever then change the static RF channel assignment method to Global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

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

- **Access point failover priority**—Each controller has a defined number of communication ports for access points. When multiple controllers with unused access point ports are deployed on the same network and one controller fails, the dropped access points automatically poll for unused controller ports and associate with them. In controller software release 5.1.151.0, you can configure your wireless network so that the backup controller recognizes a join request from a higher-priority access point and if necessary disassociates a lower-priority access point as a means to provide an available port.

  To configure this feature, you must enable failover priority on your network and assign priorities to the individual access points. By default, all access points are set to priority level 1, which is the lowest priority level.

  Note Failover priority takes effect only if there are more association requests after a controller failure than there are available backup controller ports.

- **Antenna selection**—Using the controller GUI or CLI, you can configure 1250 series access point radios to operate with only one or two antennas.
- **EAP-FAST/802.1X supplicant**—You can configure 802.1X authentication between a Cisco Aironet 1130, 1240, or 1250 series access point and a Cisco switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning.

  These switches and minimum software releases are currently supported for use with this feature:

  - Cisco Catalyst 3560 Series Switches with Cisco IOS Release 12.2(35)SE5
  - Cisco Catalyst 3750 Series Switches with Cisco IOS Release 12.2(40)SE
  - Cisco Catalyst 4500 Series Switches with Cisco IOS Release 12.2(40)SG
  - Cisco Catalyst 6500 Series Switches with Supervisor Engine 32 running Cisco IOS Release 12.2(33)SXH
- **NAC out-of-band integration**—The Cisco NAC Appliance, also known as Cisco Clean Access (CCA), is a network admission control (NAC) product that identifies whether machines are compliant with security policies and repairs vulnerabilities before permitting access to the network. In controller software releases prior to 5.1.151.0, the controller integrates with the NAC appliance only in in-band mode, where the NAC appliance must remain in the data path. For in-band mode, a NAC appliance is required at each authentication location (such as at each branch or for each controller), and all traffic must traverse the NAC enforcement point. In controller software release 5.1.151.0, the controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing.

  Note CCA software release 4.5 or later is required for NAC out-of-band integration.

  Note In controller software release 5.1.151.0, the Controller Network Module does not support NAC out-of-band integration.

- **WAN link latency**—You can configure link latency on the controller to monitor the round-trip time of the LWAPP heartbeat packets (echo request and response) from the access point to the controller and back. This time can vary due to network link speed and controller processing loads. This feature can be used with all access points joined to the controller but is especially useful for hybrid-REAP access points, for which the link could be a slow or unreliable WAN connection.

Note Link latency calculates the LWAPP response time between the access point and the controller. It does not measure network latency or ping responses.

New Location Features

- The Network Mobility Services Protocol (NMSP) manages communication between the location appliance and the controller for incoming and outgoing traffic. If your application requires more frequent location updates, you can modify the NMSP notification interval (to a value between 1 and 30 seconds) for clients, active RFID tags, and rogue access points and clients.
- You can use the controller CLI to view all mobility services active on the controller as well as detailed mobility services information for all connections or for a specific connection.

Multicast Enhancements

- Full multicast is now supported for use with the 2100 series controllers and the Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers. The previous performance limitations have been improved (CSCsd64081).
- The controller prioritizes ARP broadcast and multicast traffic types to avoid affecting access point communications (CSCsk44641). Access points can now survive in networks with a high rate of background broadcasts without affecting connectivity.

Note 2100 series controllers do not support multicast-unicast mode. They do, however, support multicast-multicast mode, except when access points are connected directly to the local port of a 2100 series controller.

GUI Enhancements

- **Dynamic channel assignment (DCA)**—You can now configure the interval, anchor time, and channel sensitivity level for DCA in the controller GUI on the 802.11a (and 802.11b) > RRM > Dynamic Channel Assignment (DCA) pages. Previously, these parameters could be configured only from the controller CLI.
- **High availability**—The high availability features that were implemented in the controller CLI in controller software release 5.0 are now also available in the controller GUI on the Global Credentials and All APs > Details pages. These features are designed to decrease the time that it takes for access points and their associated clients to move to a backup controller and for wireless service to resume after a controller goes down.
- **RRM**—The **On Demand** option for the Channel Assignment Method parameter on the 802.11a (and 802.11b) > RRM > Dynamic Channel Assignment (DCA) pages has been changed to **Freeze** to better reflect its actual function, which is to cause the controller to evaluate and update the channel

assignment for all joined access points, if necessary, but only when you click **Invoke Channel Update Once**. Also, the Noise Measurement and Load Measurement parameters have been removed from the Monitor Intervals section on the 802.11a (and 802.11b) > RRM > General pages.

Access Point Changes

- **AP801 support**—Controller software release 5.1.151.0 is supported for use with the AP801, the integrated access point in the Cisco 880 Series Integrated Services Routers (ISRs). This access point uses a software image separate from the router and can operate as an autonomous access point that is configured and managed locally or as a centrally managed access point utilizing LWAPP. The AP801 is preloaded with both an autonomous Cisco IOS release and an LWAPP recovery software image.

  The AP801 has a single 2.4-GHz 802.11b/g/n radio, which supports lower power levels than the 802.11b/g/n radio in the Cisco Aironet 1250 series access points. Also, the AP801 can be used in hybrid-REAP mode.

  Note Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.1* for information on enabling the LWAPP recovery image, upgrading the router to the Cisco Advanced IP Services IOS image to support LWAPP and meeting licensing requirements, and obtaining an IP address for the access point using DHCP.

  Note For more information on the AP801, refer to the documentation for the 800 series routers at this URL: http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html

- **Enhanced PoE switches—**Enhanced PoE switches (such as the Cisco Catalyst 3750-E Series Switches) can be used with 1250 series access points to auto-negotiate a power level in excess of 15.4 W per port.
- **Event logs**—Access points log all system messages (with a severity level greater than or equal to notifications) to the access point event log. The event log can contain up to 1024 lines of messages, with up to 128 characters per line. When the event log becomes filled, the oldest message is removed to accommodate a new event message. You can now view or clear the access point event log from the controller CLI.

Regulatory Updates

The 1131AG, 1232AG, and 1242AG lightweight access points are now supported for use in the Russian Federation -A and -E regulatory domains. At this time, the 1250 series access points are not certified for use in the Russian Federation -A and -E regulatory domains.

Note For a complete list of regulatory domains supported for each product, refer to this URL:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps6087_Products_Data_Sheet.html.

Other Changes

These additional changes are applicable to controller software release 5.1.151.0:

- The controller now supports traffic classification (TCLAS) coming from 7921 phones using firmware version 1.1.1. This feature ensures proper classification of voice streams to the 7921 phones.
- The default value for the RRM transmit power threshold has been changed from –65 dBm to –70 dBm.
- The **config network arpunicast** {**enable** | **disable**} command has been removed from the controller CLI, and the ARP Unicast Mode line has been removed from the output of the **show network summary** command (CSCsl72127).
- The **show run-config** command now includes access point group information (CSCsi22092).
- You can use these CLI commands to save debug messages to the controller buffer, the controller console, or an external syslog server (CSCsc33206):
  - **config logging debug buffered** {**enable** | **disable**}
  - **config logging debug console** {**enable** | **disable**}
  - **config logging debug syslog** {**enable** | **disable**}
- You can use these CLI commands to enable or disable timestamps in log messages and debug messages (CSCsk66663):
  - **config service timestamps log** {**datetime** | **disable**}
  - **config service timestamps debug** {**datetime** | **disable**}
- The LDAP SecureTLS mode feature, which is documented in previous releases, has been intentionally removed in controller software release 5.1.151.0 because it does not work properly (CSCso43490). On the controller GUI, the Server Mode field on the LDAP Servers pages has been removed. In the controller CLI, the **secure** option has been removed from the **config ldap add** *index server_ip_address port# user_dn password base_dn* {**secure**} command.

Installation Notes

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

Warnings

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

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

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

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

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

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

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

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

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

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

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

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

Installation Instructions

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

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

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

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

Important Notes

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

Internal DHCP Server

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

Messages Appearing Upon Controller Bootup

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

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

Web Authentication Redirects

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

Using WLAN Override with IPv6

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

PLM Location Commands

The **config**, **show**, and **debug location plm** path loss measurement location commands are not supported in controller software release 5.1.151.0, although they appear in the CLI code.

Cisco 1250 Series Access Points and Cisco 7920 IP Phones

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

Crash Files for 1250 Series Access Points

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

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

Configuration File Stored in XML

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

Note You cannot download a binary configuration file onto a controller running software release 5.1.151.0. Also, do not attempt to make changes to the configuration file. If you do so and then download the file to a controller, the controller displays a cyclic redundancy checksum (CRC) error while it is rebooting and returns the configuration parameters to their default values.

LWAPP Mode Changes

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

If you downgrade from controller software release 5.1.151.0 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 may not join the controller, and you must manually reset the controller to Layer 3 to resolve this issue.

Access Points Send Multicast and Management Frames at Highest Basic Rate

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

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

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

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

Disabling Radio Bands

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

40-MHz Channels in the 2.4-GHz Band

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

Impact of External Antenna Gain on Transmit Power

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

Supporting Oversized Access Point Images

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

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

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

Follow these steps to perform the TFTP recovery procedure.

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

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

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

Multicast Queue Depth

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

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

MAC Filtering for WGB Wired Clients

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

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

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

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

CKIP Not Supported with Dynamic WEP

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

Setting the Date and Time on the Controller

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

Synchronizing the Controller and Location Appliance

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

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

FCC DFS Support on 1130 Series Access Points

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

Inaccurate Transmit Power Display

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

Setting the Retransmit Timeout Value for TACACS+ Servers

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

Configuring an Access Point's Prestandard Power Setting

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

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

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

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

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

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

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

Controller Functions that Require a Reboot

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

- Switch between Layer 2 and Layer 3 LWAPP mode
- Enable or disable link aggregation (LAG)
- Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
- Add new or modify existing SNMP v3 users
- Enable or disable the mobility protocol port using this CLI command:

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

2106 Controller LEDs

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

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

Rate-Limiting on the Controller

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

Pings Supported to the Management Interface of the Controller

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

Pinging from a Network Device to a Controller Dynamic Interface

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

GLBP Not Supported

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

IPSec Not Supported

Software release 5.1.151.0 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 5.1* for configuration instructions.

Changing the Default Values for SNMP v3 Users

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

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

Features Not Supported on 2100 Series Controllers

This hardware feature is not supported on 2100 series controllers:

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

These software features are not supported on 2100 series controllers:

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

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

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

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

2106 Image Not Supported for 3504 Controllers

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

Running a 3504 Image on a 2106 Series Controller

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

Upgrading External Web Authentication

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

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

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

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

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

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

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

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

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

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

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

}

</script>
```

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

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

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

<tr align="center">

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

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

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

Caveats

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

Open Caveats

These caveats are open in controller software release 5.1.151.0.

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

  Workaround: Ignore the prompt and exit as usual.

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

  Workaround: None.

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

  Workaround: Use the controller CLI.

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

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

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

  Workaround: None.

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

  Workaround: None.
- CSCsf29783—The Cisco WiSM reboots after experiencing a failure with the reaperWatcher mmMfpTask.

  Workaround: None.
- CSCsg04831—There are not enough debugs to determine the packet flow in the controller for guest access.

  Workaround: Use a wireless sniffer trace.
- CSCsg59235—The controller CLI lacks commands for debugging activity at the IP, ICMP, TCP, UDP, TELNET, SSH, and HTTP layers.

  Workaround: Use an external packet capture device to collect packets to and from the controller. Send these packets to the Technical Assistance Center (TAC) for analysis.
- CSCsg87111—After you edit a WLAN configured for WPA1+WPA2 with a conditional redirect to 802.1X, the MIB browser shows a commit failure error.

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

  a. Remove conditional web redirect and save your change.

  b. Change Layer2 to 802.1X and save your change.

  c. Change Layer3 to conditional web redirect and save your change.
- CSCsg88704—When you use the default controller setting of 512 for the controller database size, the following problems may occur:
  - If you attempt to add a MAC address to a very long MAC filter list, the following error message appears: “Error in creating MAC filter.”
  - If you add a large number of users to the local database, some user entries might be silently ignored.
  - If you add SSCs for the access points, at some point no more entries can be added, and the following error message appears: “Authorization entry does not exist in Controller’s AP Authorization List.”

  Workaround: Configure a larger value for the controller database, such as 2048.
- CSCsg95474—Lightweight access points do not queue disassociation messages, causing the Cisco 7921 phone to remain in a registering loop. This problem occurs when you change the data rate on the access point.

  Workaround: Power cycle the 7921 phone.
- CSCsh11086—If you press **Ctrl-S** and **Ctrl-Q** to pause and restart the output of a command such as **debug dot1x event enable**, the controller reboots.

  Workaround: Do not stop the console using **Ctrl-S**.
- CSCsh31104—The word *channel* is misspelled in the message log.

  Workaround: None.
- CSCsh96186—Large IP packets that have been split into multiple fragments might fail to be reassembled by a 4400 series controller.

  Workaround: Redesign the network and reconfigure the communication endpoints to eliminate any points where such a small fragment could be generated.

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

  Workaround: None.

- CSCsi15194—The controller takes a long time to respond to the second message of a four-way handshake.

  Workaround: None.

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

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

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

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

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

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

  Example:

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

- CSCsi29262—When an access point radio is configured to override a WLAN of 32 characters, the access point radio stops beaconing the WLAN.

  Workaround: None.

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

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

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

  Workaround: None.

- 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.

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

  Workaround: Change the WLAN QoS profile on both the internal controller and the anchor controller to silver.
- CSCsj03124—RLDP behavior is inconsistent when initiated from a Cisco 1250 series access point.

  Workaround: Use access points other than the 1250 when RLDP needs to be used.
- CSCsj06245—Portions of the output of the **show tech-support** CLI command might be formatted incorrectly, making the information difficult to read.

  Workaround: None.
- CSCsj10755—When multicast mode multicast and IGMP snooping are enabled, the controller periodically sends out IGMP query messages to the clients. This IGMP query is sent as individual queries to each access point.

  Workaround: None.
- CSCsj10945—The controller does not factor in the antenna gain when reducing the output power.

  Workaround: Manually adjust the antenna gain, but this action can interfere with auto RF.
- CSCsj14304—With IGMP snooping enabled, MGIDs are assigned to reserved multicast addresses.

  Workaround: Use an upstream ACL if packets with reserved multicast addresses need to be blocked.
- CSCsj17054—A misleading message appears on the controller GUI when you upload software or certificates.

  Workaround: Ignore the message and choose the correct options to upload files on the controller.
- CSCsj29501—When the **session slot** or **telnet** command times out on the supervisor on the Cisco WiSM and you try to log in again, any character that you enter is duplicated.

  Workaround: Use a direct console connection to the Cisco WiSM.
- CSCsj54064—The downstream throughput is low when using a long packet size with ACLs on the 4400 series controller and the Catalyst 3750G Wireless LAN Controller Switch.

  Workaround: None.
- 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.

- CSCsk28639—If you add a controller to WCS, clear the configuration of the controller, and then try to restore the configuration, the WLAN gets restored but with the default security setting and in the disabled state, the ACL is not applied to the interface, and TACACS+ is not restored.

  Workaround: Restore the template individually or access the controller through the GUI and make the changes.
- 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.
- CSCsk68619—When using an Intel 4965 802.11n client device with a 1250 series access point, the upstream throughput is higher than the downstream throughput.

  Workaround: None.
- CSCsk76973—When you upgrade a controller from software release 4.2.61.0 or earlier, access points immediately begin downloading the new software image from the controller instead of waiting until the controller is rebooted and the downloaded image is running on the controller.

  Workaround: Disconnect the access point-to-controller path before upgrading the controller from software release 4.2.61.0 or earlier.
- CSCsk86992—Many instances of the following message appear in the controller or WCS trap logs:

  ```
  MFP Anomaly Detected - 1417 Missing MFP IE event(s) found as violated by the radio
  xx:xx:xx:xx:xx:xx and detected by the dot11 interface at slot 0 of AP
  xx:xx:xx:xx:xx:xx in 300 seconds when observing Probe responses, Beacon Frames.
  Client's last source mac xx:xx:xx:xx:xx:xx
  ```

  Workaround: After you confirm that the cause is not a spoofing attack from a rogue access point, disable and then re-enable the access points identified in the messages. If the problem persists, disable MFP validation on some of the access points, or disable infrastructure MFP globally.
- CSCsk99318—Controllers sometimes drop packets for client devices attached to a workgroup bridge when the workgroup bridge roams from one access point to another.

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

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

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

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

  Workaround: None.
- CSCsl09066—The WCS access point group VLAN profile configuration does not match the actual WLC configuration when you use multiple interface mapping profiles under the same access point group VLAN where all of the SSIDs start with the same letters or numbers.

  Workaround: None.
- CSCsl11352—The console output in software release 4.2 does not indicate which controller an access point joins when you add it to your network.

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

  debug ip udp

  The output shows all UDP packets sent and received by the access point.
- CSCsl19319—If you create a local user profile on the GUI of a 2106 controller with the WLAN profile "any WLAN" and then edit the profile, the following error message appears: "Error in setting WLAN ID for user." However, your change is applied.

  Workaround: Delete the local user profile and create a new one with the updated password or description or define a WLAN profile for the user.
- 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.
- CSCsl48417—The DTL-1-ARP_POISON_DETECTED, DTL-1-IP_CONFLICT_DETECTED, and other controller DTL messages need to be more descriptive.

  Workaround: None.
- CSCsl52203—When you use the controller CLI to create a guest user account, the controller fails to generate a trap log.

  Workaround: Use the controller GUI to create guest user accounts.
- CSCsl52445—The internal web authentication page on the controller accepts up to 2,047 characters, but the internal web authentication page in WCS accepts only 130 characters.

  Workaround: If you need to enter more than 130 characters on the internal web authentication page, use the controller interface instead of WCS.
- CSCsl54491—When 802.11a radios are disabled globally on the controller but the individual radios of the access point are not disabled, WCS reports the known access point as a rogue. The alert is generated a few times but automatically cleared and not reported again for a couple of days.

  Workaround: None. This issue appears to be cosmetic.

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

  Workaround: Make sure the client is using 802.11n rates.
- CSCsl67177—The Catalyst Express 500 (CE500) might lose connectivity to a 4400 series controller when one port of the portchannel is shut down.

  Workaround: Unplug and then plug in both Etherchannel links on the CE500 or the controller. Plug in or unplug any device on the CE500.
- CSCsl70043—When a client device connects to a secure EAP WLAN and immediately switches to an open WLAN, the access point sends a status 12 association response (which is normal) but sends it from the wrong MAC address and BSSID.

  Workaround: On the controller CLI, enter **config network fast-ssid-change** to allow the client devices to connect without incident.
- CSCsl70587—CB21AG client adapters using 802.11b mode might experience low throughput with 802.11n clients. Throughput can be affected by a number of factors. For example, high throughput devices can consume more of the bandwidth than older clients.

  Workaround: None.
- CSCsl71343—Client throughput can be affected by a number of factors. Another client's traffic on the same access point can cause throughput degradation.

  Workaround: None.
- CSCsl77058—The word "rogue" is misspelled in one of the WLAN message log statements. The correct statement should be "APF-1-UNABLE_TO_KEEP_ROGUE_CONTAIN."

  Workaround: None.
- CSCsl79260—Wired guest LAN clients fail to obtain an IP address if DHCP proxy is disabled.

  Workaround: Do not disable DHCP proxy.
- CSCsl95615—When a master controller exists on the network, an access point that is joined to a secondary or tertiary controller keeps going back to discovery.

  Workaround: Disable the master controller mode.
- CSCsm03461—A command is needed to show the ER image or bootloader version that is currently running as well as the one that will be installed on the next bootup. Currently, the bootloader is used to verify if an ER image or bootloader upgrade is successful. However, not all controllers include the bootloader in the ER image.

  Workaround: Install the Cisco Unified Wireless Network Controller Boot Software 4.2.112.0 ER.aes file, which contains a new bootloader. A successful transfer and upgrade of the ER file indicates that the ER file has been updated properly.
- CSCsm04752—The GUI of an anchor controller shows a wired client as mobile rather than as 802.3.

  Workaround: None.
- CSCsm05607—Large user packets may fail to be successfully forwarded in an EoIP mobility/guest tunnel between controllers.

  Workaround: Perform one of the following:

  - Reconfigure the IP endpoints to use smaller MTUs.

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

- CSCsm08623—If the **config paging disabled** CLI command is entered on the controller, the output of the **show msglog** command is periodically interrupted with the "Would you like to display the next 15 entries?" prompt.

  Workaround: None.

- CSCsm12623—The AAA override dynamic VLAN assignment fails with guest tunneling. Clients successfully authenticate, but the IP address is that of the interface the WLAN is associated to on the anchor controller.

  Workaround: None.

- CSCsm19182—When an 802.11n radio is operating on channel 52 through 140, the channel width is configured for 40 MHz, and a radar event is detected, it is possible for the radio interface to become disabled instead of moving to another channel. This problem occurs when the access point is operating in the vicinity of radar operations or under extreme traffic conditions (when a false radar detection may occur).

  Workaround: Disable and re-enable the radio interface.

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

  Workaround: None.

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

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

  Workaround: Follow these steps:

  a. Determine whether you want to force your wireless clients to perform DHCP first, after associating, before they can send IP packets.

    - If you do, then disable DHCP Required, and you will not encounter this problem.
    - If you do not, then configure all clients to use DHCP.

  b. If the client is configured for DHCP but sometimes still sends IP packets after associating without performing DHCP, then perform the following:

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsm40870—The following error message should be reworded:

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

  The message should read as follows:

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

  Workaround: None.

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

  Workaround: None.

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

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

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

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

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

  Workaround: None.

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

  Workaround: Create an access list with rules.

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

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

Workaround: None.

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

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

  Workaround: None.

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

  Workaround: Reboot the access point.

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

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

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

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

- CSCsm80423—The controller cannot block Layer2 multicast traffic.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

- CSCsm85717—The following error message needs to identify the root cause of the problem:

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: When you set up an anchor controller, do not configure an ingress interface because the clients are tunneled over from another controller, preventing selection of an ingress interface on the guest WLAN. Set the anchor for the guest WLAN to “local” and then enable the WLAN, leaving the ingress interface set to None.

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

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

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

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

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

  Workaround: None.

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

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

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

  Workaround: None.
- CSCso10678—The controller might hang when you attempt to upgrade the controller software.

  Workaround: Reboot the controller or wait for some time to clear this condition.
- CSCso13516—The controller sometimes crashes at random, and the crash file shows a signal 11. Signal 11 occurs when the program running on the controller accesses a part of memory that it does not have permission to access.

  Workaround: None.
- CSCso18251—When you log into the controller as a lobby ambassador and create a guest user with a lifetime of zero (infinite), the user information appears only on the controller CLI. It does not appear on the controller GUI.

  Workaround: Use the controller CLI to display users.
- CSCso20444—When a controller and a 1250 series access point operate together in sniffer mode, Wireshark sometimes shows incorrect data rates for 802.11n packets.

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

  Workaround: Reset the Cisco WiSM.
- CSCso22875—During code download, some access points might disconnect and then reconnect to the controller.

  Workaround: None.
- CSCso23079—When a 7921 phone that is connected to a 1242 series access point using 802.11a receives multicast voice traffic, the audio is sometimes choppy and garbled.

  Workaround: Choose a lower mandatory basic data rate such as 12 Mbps and make sure that 24 Mbps is set to Supported, or use 1131 series access points.
- CSCso25781—IP connectivity is sometimes lost to a Cisco WiSM controller through either the service port or management interface. Console access continues to function, but no access point or user traffic can flow. This issue seems to be affected by the number of dynamic interfaces that have been created on the controller.

  Workaround: None. However, entering the **reset system** CLI command on the Cisco WiSM recovers IP traffic flow.
- CSCso26532—When you have multiple controllers in the same mobility group and Ascom phones on different controllers, only one-way audio is available for the Ascom phones.

  Workaround: None.
- CSCso29405—When you are troubleshooting traffic on radio interfaces, remote debugs might fail for some radio debug commands.

  Workaround: Connect to the access point locally.
- CSCso31067—Some clients might experience failures during upstream-only prioritized traffic on 802.11a, despite radio resource management (RRM) features being disabled.

Workaround: None.

- CSCso31244—2100 series controllers sometimes freeze randomly.

  Workaround: Manually reset the controllers.

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

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

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

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

- CSCso35129—If the controller is queried by SNMP for a virtual gateway interface address, it may generate messages such as "sim.c:1061 SIM-3-MACADDR_GET_FAIL: Interface 1 source MAC address is not found."

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

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

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

  Workaround: None.

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

  Workaround: None.

- CSCso48158—The tickle timer, which is used to update the watchdog timer, is not preserved correctly when the NPU-to-CPU interrupt handler becomes congested and overrun. This issue affects console output and serial port communications, potentially used for low-level debug console output messages.

  Workaround: None.

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

  Workaround: Remove the PAC from the client.

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

  Workaround: Ignore the PMKID count within the RSN capability.

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

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

  Workaround: None.

- CSCso52349—If SNMP is tested against the controller's management IP address from a device on the same subnetwork as a dynamic interface, the controller fails to send SNMP responses.

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

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

  Workaround: None.

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

  Workaround: None.

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

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

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

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

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

Workaround: None.

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

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

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

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

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

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

- CSCso63232—The controller in the Catalyst 3750G Wireless LAN Controller Switch might reboot if you enter the **show hreap group detail** *groupname* CLI command without a group name or without a space between the **detail** parameter and the group name.

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

- CSCso65150—When AAA override is enabled for a WLAN and the AAA server is providing the session timeout value, if a client that is associated to that WLAN roams to another access point joined to the same controller and the session timeout has not expired, the session timeout for that client is reset to the initial value received from the AAA server.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCso66183—When more than 100 Symbol Vocollect devices are in a small area, they might disassociate from 1242 series access points with the following error message:

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

  Workaround: Manually power cycle the access points.

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

  Workaround: None.

- CSCso66778—The output of dump low-level debugs is not complete for several commands in controller software releases 5.0 and 4.2.112.0. This problem might affect proper troubleshooting for service port hangs, NPU issues, and so on.

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCso78437—After a client sends a reassociation request or response but before it has completed a four-way exchange, all of the packets coming to the client are dropped at the controller or forwarded to the wired side.

  Workaround: None.

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

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

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

  Workaround: Disable TSM for voice.

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

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

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

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

- CSCso92229—The controller CLI accepts a CIDS SHA1 key with the correct number of hexadecimal digits but also accepts extra colons between the pairs of digits.

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

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

  Workaround: None.

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

  Workaround: Reboot each access point.

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

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

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

  Workaround: None.

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

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

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

  Workaround: Downgrade the controller to software release 4.2.

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

  Workaround: None.

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

  Workaround: None.

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

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

  Workaround: Reboot the controller.

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

  Workaround: None.

- CSCsq07537—Clients continue to communicate with an access point that has its radio disabled by the controller. The controller shows that the access point radio is disabled when it is not.

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

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

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

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

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

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: Change the IP address of the management interface.

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

  Workaround: Use the controller CLI to view multiple entries.

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

  Workaround: None.

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

  Workaround: Use the controller CLI.

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: Use the controller CLI.

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

  Workaround: None.

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

  Workaround: Downgrade to the previous controller release.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

  Workaround: None.

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

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

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

  Workaround: None.

- CSCsq24255—When an access point is disabled or removed from the controller, a client entry is also cleared from the controller. However, the controller does not send an SNMP alert message to the NAC server that the client entry has been removed, so its entry remains on the server.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

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

  Workaround: Reboot the controller.

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

  Workaround: None.
- CSCsq26446—Clients using a WLAN with web authentication enabled might disconnect every 5 minutes. The “pem timed out” message appears in the controller logs.

  Workaround: Authenticate the clients using another WLAN.
- CSCsq29243—The 802.11h channel switch mode parameter accepts any value, even though only 0 or 1 should be accepted.

  Workaround: None.
- CSCsq29950—The Controller Network Module and the 2100 series controllers sometimes report the following unknown syslog message: “Unable to find an ACL by name "".”

  Workaround: None.
- CSCsq30071—The Controller Network Module does not boot up normally after being downgraded from software release 4.1.185.0 to 4.0.219.0.

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

  Workaround: None.
- CSCsq30821—Web authentication is bypassed if a client associates to an access point on one controller, roams to an access point on another controller, and then roams back to the first controller. This behavior occurs if the WLAN is on different subnets on each controller, causing the client to be anchored to the first controller when roaming to the second.

  Workaround: None.
- CSCsq30980—When you upgrade a 4400 series controller to software release 5.1, no more than 48 access points are able to join if link aggregation (LAG) is disabled. The controller enters this state when all the ports on the controller are administratively disabled and the configuration is saved before the controller is reset.

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

  Workaround: Do not downgrade the Controller Network Module to a software release prior to 4.1. This controller supports software release 4.1 or later.
- CSCsq31622—An SNMP error might occur when you enable voice and video parameters on a controller running software release 4.2.122.0.

  Workaround: None.
- CSCsq32038—The **config interface create** CLI command does not indicate the number of characters allowed for the interface name.

  Workaround: None.
- CSCsq32279—An access point group VLAN can be mapped to a wired guest LAN interface.

  Workaround: None.

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

  Workaround: None.
- CSCsq34216—The system logs on a controller running software release 5.0.148.0 might be filled with messages such as "apf_ms.c:4849 APF-1-USER_DEL_FAILED: Unable to delete user name **** for mobile **:**:**:**:**:**," where the first set of asterisks represents a username and the second set represents a MAC address. The username that is listed is not a username that is configured anywhere on the controller.

  Workaround: None.
- CSCsq34262—When you add three controllers running software release 4.2.125.0 to the same mobility group and enable a dynamic interface on each, a traceback might appear on the controller console.

  Workaround: None.
- CSCsq34314—You can use the controller CLI to create a local guest user with a lifetime of 0 (no limit) for a WLAN that has web passthrough enabled. If you specify any finite value, the local netuser is not created.

  Workaround: None.
- CSCsq35574—The EAP-FAST parameters Authority ID and Server Key do not accept entries of 17 or more characters.

  Workaround: None.
- CSCsq35590—A traceback might appear on the access point console when you change the access point country from Spain to the US.

  Workaround: None.
- CSCsq35662—More debug messages are needed when an access point fails to download the software image from the controller.

  Workaround: None.
- CSCsq35990—The **config netuser lifetime** CLI command does not accept a zero (0) value for the *lifetime* parameter.

  Workaround: Delete the guest user and recreate it with a zero lifetime.
- CSCsq37810—A controller running software release 4.2.124.0 does not send a ColdStart trap when you reboot it.

  Workaround: None.
- CSCsq38075—A traceback might appear on the access point console when you set the access point country to Spain.

  Workaround: None.
- CSCsq38700—After you change the power level of an access point radio, the controller shows the radio's operational status as DOWN. However, clients continue to pass traffic and function properly.

  Workaround: None.
- CSCsq40265—The statistics of a second RADIUS server are never incremented and stay at 0 in the **show radius auth stats** command or display incorrect values. This behavior occurs when the first RADIUS server does not reply and the request falls back to the second RADIUS server.

  Workaround: None.

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

  Workaround: Disable NAC.
- CSCsq41115—Hybrid-REAP access points do not show any nearby neighbor access points.

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

  Workaround: None.
- CSCsq45912—The CPU access control list (ACL) is not blocking traffic from the RADIUS server.

  Workaround: None.
- CSCsq46045—1130 series access points joined to a controller running software release 5.0.148.0 might crash periodically and enter a continuous reboot cycle.

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

  Workaround: Use a Windows 2000 DHCP server.
- CSCsq47493—The hybrid-REAP access point VLAN ID is not being updated.

  Workaround: First change the native VLAN ID; then change the hybrid-REAP VLAN ID.
- CSCsq47516—If you downgrade a 2106 controller from software release 4.2.130.0 to 4.2.112.0 for a directly connected 1230 series access point, the access point joins but might not load the new image.

  Workaround: Connect the access point using Layer 3 (not a direct connection), or reset the controller and wait for the access point to join.
- CSCsq49329—The **show services mobility detail** *ip_addr* CLI command generates an error on the 2106 controller, even when you enter a valid IP address.

  Workaround: Use the **show services mobility detail all** CLI command, which provides information for all the connections.
- CSCsq49514—A duplex mismatch between the 2106 controller and the switch prevents the controller from connecting to the network.

  Workaround: Correct the duplex mismatch.
- CSCsq49831—A core dump should be created when the controller crashes to aid in debugging.

  Workaround: None.
- CSCsq49975—When you enable ARP debugs and generate a gratuitous ARP, the gratuitous ARP does not come up to the dtl ARP module, and no debugs appear on the console.

  Workaround: None.
- CSCsq50649—The controller is slow to respond to SNMP set requests, which can cause the SNMP set request to time out.

  Workaround: Reboot the controller.

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Enable CCKM on the client and the WLAN.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsq59896—A 4400 series controller might reboot after you upgrade the controller software from the 4.2.112.0 release to the 4.2.130.0 release.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Use the controller CLI to view TSM values.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: Use the controller CLI to enable NAC.

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

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

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

  Workaround: None.

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

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

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

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

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

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

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

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

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

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

  Workaround: None.

- CSCsr00444—The controller might intermittently become inaccessible.

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

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

- CSCsr17163—Under conditions of very high stress, the controller shows no joined access points and clients and no traffic to or from clients. The controller also generates a crash file and reboots automatically.

  Workaround: None.

- CSCsr18679—Some Intel 802.11n clients might be unable to pass FTP streams or might experience rate fluctations as low as 6 Mbps.

  Workaround: None.

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

  Workaround: None.

- CSCsr26228—The radio in a 1250 series access point sometimes locks up with used in an environment with mixed clients and mixed traffic.

  Workaround: None.

- CSCsr29994—The Cisco WiSM might reboot without generating a crash file. The following error message appears on the console:

  ```
  16Memory 0x40e1e07c has been freed (osapi_task.c:613)!
  Memory Entry 0x40e1e07c: Magic 0xdeadf00d, Size 16, len 0,thread (nil)
  file free_lib.c, line 71, ts 0
  Resetting system ...
  ```

  Workaround: None.

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

  Workaround: None.

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

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

- CSCsr43364—The controller sometimes reboots after you click the WLANs tab on the controller GUI.

  Workaround: None.

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

  Workaround: None.

- CSCsr48006—A 1250 series access point might crash during Layer 2 roaming with 50 clients.

  Workaround: None.

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

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

Resolved Caveats

These caveats are resolved in controller software release 5.1.151.0.

- CSCsb85113—When you download the software image to the controller using the CLI, access points are sometimes disconnected.
- CSCsc33206—The current software for wireless controllers does not allow you to save debug messages in the controller log or on a syslog server. This issue creates serviceability problems when trying to enable debugs for a long period of time.
- CSCsc36000—The **show running-config** CLI command includes all associated access point details, which makes the output very lengthy. The access point information should be removed from the output of this command.
- CSCsd10643—The default EAP timeout value of 1 second is too aggressive for some clients. The default value should be changed to 30 seconds.
- CSCsd29484—The access point log shows the reason for the last access point restart. However, under certain conditions, the restart reason does not provide enough useful information. For example, if an access point disconnects from a controller because the controller is running at a high CPU speed, the access point sends an LWAPP discovery packet to the controller, and the controller replies with an LWAPP discovery response. When the access point requests the MAC address of the AP-manager, the controller drops the ARP packet from the access point. The AP log shows "Could not resolve switch ARP in Join" as the restart reason.

This problem is resolved in controller software release 5.1 so that the access point log shows the restart reason for all failures, including the initial failure. In the example above, the access point log would show the initial failure (losing the heartbeat) and the subsequent failures (cannot resolve the switch ARP in join). To view the access point log, enter this controller CLI command: **show ap eventlog** *Cisco_AP*.

- CSCsd64081—When a 2000 series controller, 2100 series controller, or Wireless LAN Controller Network Module attempts to forward multicast traffic to wireless clients at a rate greater than 50 packets per second, the message log might show many "Multicast Rx queue is full" entries, the controller might be unable to pass user data, and the access points might be unable to join the controller.
- CSCse87087—A controller with link aggregation (LAG) enabled fails Ethernet link redundancy. This problem occurs when the controller uses an Ethernet copper gigabit interface converter (GBIC) instead of a fiber GBIC and one of two Ethernet cables is pulled out of the GBIC.
- CSCsf23288—Some clients that are configured for WPA2 might send encrypted data immediately after the four-way handshake. If this occurs before the encryption key gets plumbed on the access point, a WEP decryption error might result.
- CSCsg48089—If you lose your controller password and have not backed up the configuration, the recovery mechanism is to revert to the factory default settings.
- CSCsg66040—After a software upgrade, controllers might experience intermittent access to the management interface through HTTPS.
- CSCsg68046—The complete reason for a TFTP download failure needs to appear on the controller GUI. If the controller cannot find the software file on the TFTP server during a software upgrade, it reports that the transfer failed rather than that the file is not present.
- CSCsg74578—If you change a controller's management IP address, it is not sent to the access point unless the access point is reset. As a result, multicasting does not work until the change is made on the access point.
- CSCsg84209—The export foreign controller is not deleting the client device when it receives a HandoffEnd message.
- CSCsh78901—The controller displays the wrong bandwidth contract parameters for QoS levels.
- CSCsh97904—During web authentication, the **show msglog** command might show an authentication failure although the user can successfully authenticate and pass traffic.
- CSCsi13399—The Expiration Timeout for Rogue AP Entries parameter on the Rogue Policies page applies to both rogue access point entries and rogue client entries. The parameter name should be changed to reflect both types of entries.
- CSCsi34642—The external web server list in the output of the **show custom-web all** CLI command is misformatted and difficult to read.
- CSCsi72767—A script runs each time you generate a dependency file, which makes the build very slow.
- CSCsj14255—Sometimes the multicast stream to wireless clients stops, and the upstream router does not receive IGMP reports. This problem occurs when there are multiple IGMP requests on the same VLAN and the controller responds only to the last query or when simultaneous IGMP queries are sent from more than five VLANs and the controller responds to only the first five.
- CSCsj32243—All old multicast timer application program interfaces (APIs) need to be replaced with new APIs.
- CSCsj36298—When you edit the session timeout for a WLAN on the controller GUI, the session timeout shows "0" regardless of the value. This issue is cosmetic because the change is applied.

- CSCsj43744—The controller ignores the default gateway MAC address that is learned by using ARP and uses the source MAC address of the packet to send the traffic back to the destination when the traffic should be sent to a different subnet.
- CSCsj44861—An access point might transmit neighbor messages when it is not connected to a controller.
- CSCsj47472—When refreshing the configuration from WCS on a 2106 controller with software release 4.1.171.0, the IP address and subnet mask are inverted in the SNMP community string template.
- CSCsj48872—After you upgrade the controllers in a Cisco WiSM from software release 4.0.206.0 to 4.1.171.0, both of the controllers may reboot repeatedly.
- CSCsj56899—The controller does not send the hostname or IP address in the syslog message header, making it difficult to determine which controller sent the message.
- CSCsj59237—The traffic stream metric (TSM) does not show the correct packet count for downlink packets.
- CSCsj59441—Channel information for a rogue access point does not appear on the rogue access point report.
- CSCsj61649—Whenever a log analysis report is generated on a CCXv5 client using WCS, the DHCP and AAA logs are swapped.
- CSCsj67447—When you use the controller GUI to modify an existing (or newly created) guest LAN and you choose an ingress interface that is already in use, no error appears. The error that appears on the CLI should also appear on the GUI: “Ingress interface is in use by some other guest lan.”
- CSCsj85329—The controller GUI should explain how the password changes with RADIUS compatibility mode. The RADIUS server names help users match to their type of RADIUS server, but the server types should be explained:
  - Cisco ACS—In the RADIUS access-request packet, the username is the client MAC address, and the password is the client MAC address.
  - Free RADIUS—In the RADIUS access-request packet, the username is the client MAC address, and the password is the controller’s shared secret with the RADIUS server.
  - Other—In the RADIUS access-request packet, the username is the client MAC address, and the password is not sent in the RADIUS access-request packet.
- CSCsj95069—The web authentication login page does not show the Cisco logo.
- CSCsj96589—Using the MAC address from the label on an 1131 or 1242 access point in the **debug mac addr** command produces limited debug output.
- CSCsj97900—The call admission control (CAC) TSPEC is not traffic shaping and allows a new call setup when the physical data rate is higher than one single data rate configured on the controller.
- CSCsk00963—If you make multiple configuration changes on the All APs > Details page on the controller GUI and click **Apply**, the changes are not committed, and the access point fails to join the controller.
- CSCsk03370—The controller needs to have millisecond timestamps in its debug messages in order to align captures from multiple devices.
- CSCsk08401—The formatting for the **config paging** *?* CLI command needs to be corrected as it displays line breaks between the options.

- CSCsk18471—When the controller supports a Layer 3 roam without symmetric tunneling, an ARP entry is required at the foreign controller to forward a packet from the client to the foreign VLAN. If the entry does not exist in the NPU when a packet arrives, the NPU sends an ARP resolution request to the CPU. The CPU then performs the ARP lookup and plumbs the entry to the NPU. However, the ARP entry is not being plumbed correctly to the NPU. As a result, each packet sent by the client results in a request to the NPU.
- CSCsk21007—The controller requires TACACS+ authentication when a configuration setting is changed on the controller GUI or a GUI page is opened.
- CSCsk22861—An MGID entry is not cleared from the access point when IGMP snooping is disabled.
- CSCsk26900—Wireless AppleTalk clients do not get information from existing wired AppleTalk network resources. AppleTalk frames are dropped.
- CSCsk38779—The controller does not respond to a third-party SNMP manager's snmpbulkwalk request. This behavior typically occurs when the number of maximum repeaters is greater than 10.
- CSCsk41891—After the controller is upgraded to software release 4.1.171.0 or later, the controller logs this message because it cannot find the access point to which the client is associated:

  ```
  CCX-4-MSGTAG012: Mobile xx:xx:xx:xx:xx:xx has unsupported CCXversion
  ```

- CSCsk44641—The controller should prioritize ARP broadcast and multicast traffic types to avoid impacting access point communications.
- CSCsk49157—When you change the session timeout of a WLAN that is using a backend RADIUS authentication server, any existing client that is using that WLAN shows its reauthentication timeout as infinite, even though there is a finite time after which reauthentication occurs.
- CSCsk49200—The hybrid-REAP local switching option should be removed for wired guest LANs.
- CSCsk49282—The guest LAN and WLAN are not clearly differentiated.
- CSCsk50477—The BCAST_Q_ADD_FAILED message contains typographical errors.
- CSCsk55844—When you log into the wireless network on a Cisco WiSM with a back-end RADIUS authentication server, the class attribute returned in the Access-Accept is not forwarded in the Accounting-Request.
- CSCsk62403—A controller running software release 4.1.185.0 or 4.0.217.0 might reboot due to a software failure with the sshpmMainTask.
- CSCsk65659—Auto-anchor mobility is disabled when you apply a WLAN template from WCS to the 2106 controller.
- CSCsk67066—The proper error message is not displayed while removing the Radius server. The GUI error message is "Error in deleting auth server." The correct error message displays in CLI: "Error: Server in use on a specific H-REAP group."
- CSCsk68117—U-APSD state changes on a client device are not updated on the controller.
- CSCsk70071—The BIG NAV trap (bsnwras.my, bsnApBigNavDosAttack) states that traffic on a specified channel is suspended. The trap message is incorrect because traffic is not suspended.
- CSCsk70727—A 7921 IP phone in world mode is not connecting to a 4400 series controller with country code KE.
- CSCsk71405—The controller should not set the DF bit when sending packets to WCS. This behavior prevents WCS from adding the controller.

- CSCsk72885—The controller returns a 0 value instead of 1 or greater for the service port or virtual interface.
- CSCsk74050—If you configure an ACL name with 32 characters, the ACL name is overwritten during roaming.
- CSCsk76218—A configuration file encrypted with a key can be downloaded without a key.
- CSCsk76537—Additional troubleshooting information is needed in low-level debugs to investigate controller issues.
- CSCsk76973—Access points immediately begin downloading a new software image when it is placed on the controller instead of waiting until the controller is rebooted and the downloaded image is running on the controller.
- CSCsk78212—The controller might reboot due to a failure with the tplusTransportThread task. The reboot usually occurs after you change the channel or power setting of an access point from the controller GUI.
- CSCsk78264—A change in the RF domain name takes effect only after you reboot the controller.
- CSCsk79382—CCXv4 and CCXv5 clients receive an Adjacent Access Point report from the controller after associating successfully.
- CSCsk79766—The controller might reboot after numerous guest user attempts are made to resources that are denied by configured rules. The following error message might appear in the controller logs: "[ERROR] sshglue.c 5731: SSHPM: failed to create Deny All rule."
- CSCsk79865—The controller rejects an 11-Mbps Phy rate in the TSPEC if the client associates with 802.11g rates.
- CSCsk82851—Debugs sometimes stop running under heavy loads.
- CSCsk83426—When a hybrid-REAP access point is in standalone mode and a session timeout is configured for the WLAN, the client does not timeout when the session expires.
- CSCsk84846—Sometimes hybrid-REAP access points start placing clients onto the wrong VLAN.
- CSCsk86536—The wrong error message appears when you change country channels with the 802.11a radio enabled.
- CSCsk93026—A 1230 series access point might lose its certificate during a software upgrade. This issue occurs when the access point moves to another controller running a different software release.
- CSCsk93726—The controller might reboot due to a software failure of the CrashdtlArpTask.
- CSCsk94804—The controller might reboot due to a failure with the EAP framework task and software filing on the instruction located at 0x108b10fc (pfree+56).
- CSCsk97359—The SNMP table containing RSSIs sometimes breaks, so the Location Appliance does not get all of the RSSIs for a tag. If the Location Appliance receives no RSSIs, it uses any RSSI it can find.
- CSCsk97940—If you disable the 1, 48, and 54 Mbps data rates, association responses include 24 Mbps as a supported rate and an extended supported rate.
- CSCsk98326—If you globally configure customized web authentication, the client might not be able to access the custom web page.
- CSCsl01005—Sometimes bandwidth contracts do not take effect. If a user who has bandwidth restrictions logs in and logs out and then another user who does not have bandwidth restrictions logs in, the bandwidth restrictions are not removed immediately.
- CSCsl09218—You cannot upload a binary backup from the CLI on controllers running software release 4.2.

- CSCsl09856—After you upgrade to software release 4.2.61.0, the controller sometimes generates these messages when a location appliance is part of the system and rogue access points are detected:

  ```
  Oct 30 07:46:38.739 apf_rogue.c:193 APF-3-RCV_UNSUPP_MSG: Rogue Task: Received
  unsupported message 34.
  Oct 30 07:46:29.709 apf_rogue.c:193 APF-3-RCV_UNSUPP_MSG: Rogue Task: Received
  unsupported message 34.
  ```

  This issue is cosmetic, but a large number of messages are generated.
- CSCsl13335—The controller might reboot when you are removing a WLAN.
- CSCsl16445—When an access point radio status is down due to lack of CDP response from a neighboring switch, the controller reports Cause=Unknown. However, it should report Cause=Waiting for CDP response.
- CSCsl18161—Controller software upgrades often fail when you use TFTP transfer mode across a slow WAN link.
- CSCsl18523—For 2106 controllers, doing an SNMPwalk for a UDP object causes a loop. This issue affects interoperability with third-party management tools.
- CSCsl19025—Controllers do not respond to a device with an IP address that ends in zero, as in x.x.x.0.
- CSCsl20584—When the **show ap config** command is entered, the controller sometimes reboots.
- CSCsl21545—The object identifier (OID) is not increasing in the controller's IP address table.
- CSCsl27682—In an inter-controller mobility environment, a controller might reboot due to a failure of the spamReceiveTask on the instruction located at 0xc5f6726 (Unknown).
- CSCsl28130—The 4402 controller might reboot due to a failure of the spamReceiveTask when the device is accessed through the management interface using NAT translation on a firewall.
- CSCsl28216—Continuous ACL messages might fill the controller log when no ACLs are configured.
- CSCsl30758—Clients reauthenticate several times with the RADIUS server, and some clients drop after 30 minutes. These reauthentications and drops occur with WPA enabled, with no CCKM, and with the WLAN session timeout disabled.
- CSCsl31372—The controller might reboot if it receives a data packet without a SNAP header from an associated client.
- CSCsl32263—If the dynamic interface tied to an access point group VLAN does not exist when access point group VLANs are configured, the controller might reboot when you enable the WLAN.
- CSCsl32786—Guest accounts might be lost after the controller reboots.
- CSCsl41757—When you upgrade a controller to 4.2.61.0 or a later software release, the controller's binary configuration file does not migrate correctly to XML if it contains any of the following characters as part of a user configuration string: &, <, >, ', ". For example, a WLAN profile named R&D causes an XML parsing error after the second reboot, even though this profile name is valid in 4.1 and previous configurations.
- CSCsl47575—When DHCP proxy is disabled and guest networking is enabled, the DHCP offer is tunneled to the export foreign controller, where it is sent to the CPU and then dropped.
- CSCsl48639—An IP address can be configured on a dynamic interface on a controller when that IP address has already been assigned to another device on the network.

- CSCsl48726—The **show run-config** CLI command does not show the TACACS+ configuration on the controller.
- CSCsl48776—Controllers sometimes incorrectly forward SSC authentication requests to a RADIUS server.
- CSCsl51368—Some 802.11n client devices successfully connect to an access point but cannot pass traffic until they are rebooted.
- CSCsl53115—Clients that attempt to authenticate with EAP-TLS and LDAP sometimes fail.
- CSCsl56900—Controllers sometimes fail to display the entire output of the **show run-config** CLI command.
- CSCsl58122—Access point credentials cannot be set when no access points are joined to the controller.
- CSCsl61596—The controller might reboot due to a failure of the iappSocketTask.
- CSCsl61657—When the 802.11g network is enabled on the controller, wireless clients that support only long slot time (20 microseconds) have difficulties associating to access points.
- CSCsl67263—If you try to enable both IPv6 and DHCP Addr. Assignment Required from the controller GUI or CLI, an error message appears, and the WLAN becomes disabled.
- CSCsl72127—The ARP unicast feature should be removed from the controller GUI and CLI and on upgrade from prior releases.
- CSCsl79069—When the AAA override is enabled for a WLAN and the AAA server is providing the session-timeout value, if a client associated to that WLAN roams to another access point joined to the same controller and the session timeout has not expired, the session timeout for that client is reset to the initial value received from the AAA server.
- CSCsl80225—The controller deletes the access point radio core-dump file when a TFTP transfer is unsuccessful.
- CSCsl85407—When a client associates to the WLAN and uses PMKID to bypass full authentication with the RADIUS server again, the controller might be unable to populate the username field associated with this authentication and therefore resort to using the MAC address in accounting requests.
- CSCsl90630—The dynamic channel allocation (DCA) function on the controller requires that one non-DFS channel be enabled on a controller. However, there are no non-DFS channels in the EU for outdoor deployment.
- CSCsl94719—The Preview button on the controller GUI shows the internal default web page, even if you chose Customized for the Web Authentication Type.
- CSCsl97666—If you make any change to an access point in the controller GUI, the following error message appears: “Error: Enter password and enable password to update with new credentials.” This message is cosmetic.
- CSCsm04622—The CPU ACL does not filter traffic to dynamic interface addresses.
- CSCsm08062—The controller might reboot due to failure in the dtlDataLowTask on the instruction located at 0x1042908c (hapiMmcReceiveDataLow+788).
- CSCsm10213—In the **debug lwapp detail** CLI command, the “Received LWAPP CHANGE_STATE_EVENT” message from the access point should include the specific state event, such as downloading.

- CSCsm10852—If you disable client tracking on WCS under the Tracking parameters tab of the location server, a service change request is sent to the controller. The controller should not send client RSSI, INFO, and STATS notifications to the Location Appliance after receiving this message, but the Location Appliance still receives the notifications.
- CSCsm11640—The controller might reboot due to a software failure of the SNMPTask at the instruction located at 0x10582794 (CmpOIDWithLen+128).
- CSCsm15583—The **show database summary** output exceeds the number of eligible entry types displayed by individual **show** commands. This command needs to identify and remove "other" entries so eligible entries configured on the controller can be entered up to the maximum database value.
- CSCsm17459—Some CLI commands that are entered in capital letters (such as "EXIT") do not work on the controller or generate an error.
- CSCsm18363—Local authentication bind support to an LDAP server needs to be available using either the anonymous method, which is the default value, or the authenticated method. The anonymous method allows anonymous access to the LDAP server whereas the authenticated method requires that a username and password be entered to secure access. In controller software release 5.1, the following CLI command has been added for this purpose: **config ldap simple-bind** {**anonymous** *index* | **authenticated** *index* **username** *username* **password** *password*}.
- CSCsm20278—The **show wlan summary** CLI command does not allow a condensed command. For instance, the **show ap summ** command can be used instead of **show ap summary**. However, **show wlan summ** cannot be used for **show wlan summary**.
- CSCsm20279—When an access point that has been converted to lightweight mode is on the same subnet as its controller's AP-manager interface, it intermittently enters a state where some (but not all) of its LWAPP packets that are addressed at the IP layer to the AP-manager IP address are instead addressed at the MAC layer to the access point's default IP gateway.
- CSCsm21340—The controller might reboot due to a failure of the pemReceiveTask software on the instruction located at 0x100bb080 (PES_rqst_exec_again+264).
- CSCsm25963—The radio in a 1240 series access point might report +127 for noise across all channels.
- CSCsm25987—Users are unable to add a RADIUS server to a wired guest LAN using the controller GUI.
- CSCsm26312—The controller might reboot due to a software failure with the BsnMDAframeMonitorTask.
- CSCsm27577—EAP-TLS local authentication fails when CN Identity Check is enabled and the username or CN identity contains spaces.
- CSCsm28852—In controller software release 4.2, the controller GUI does not allow spaces in WLAN profiles, but the controller CLI does allow spaces.
- CSCsm30414—If a controller tries unsuccessfully to add a rogue entry to its internal data structure, it might reset while trying to generate an error message.
- CSCsm31814—A global configuration of custom web authentication using the controller CLI might be disabled after a WLAN is deleted and then recreated.
- CSCsm40866—The "ASSOCREQ_PROC_FAILED: Failed to process an association request" message should have some form of suppression. With a wireless network and a user base of approximately 10 users, this message fills up the logs, making them useless.

- CSCsm40899—The following message should include the MAC address or username of the aborted user and, if possible, the reason code: "1x_bauth_sm.c:443 DOT1X-3-ABORT_AUTH: Authentication Aborted."
- CSCsm42355—The controller returns a signed 32-bit integer in the MIB object bsnAPIfSlotId although the published MIB module indicates that the controller should return an unsigned integer. This behavior may cause WCS to misinterpret incoming trap data that is eventually used in reports and graphs.
- CSCsm44025—The following unclear error message appears when you change the Web Authentication Type parameter from Internal (Default) to Customized (Downloaded) on the Web Login page without first disabling the WLAN: "Error! Please look up custom-web information and disable Web-Auth/Web-Passthrough WLAN's with Global Status set."
- CSCsm44369—The following debug output does not indicate which stream could not be opened: "SshPmStAppgw/pm_st_appgw.c:681/ssh_pm_st_appgw_tcp_open_initiator_stream: Could not open initiator stream."
- CSCsm44383—The following debug output does not indicate which instance was terminated: "SshPmStAppgw/pm_st_appgw.c:1094/ssh_pm_st_appgw_terminate: terminating appgw instance."
- CSCsm45147—An error is not produced when you delete an interface mapped to an access point group VLAN. Instead, the access point group VLAN mapping retains the deleted interface in the configuration.
- CSCsm50322—The controller GUI and WCS do not indicate when the database has reached the maximum number of local net users.
- CSCsm50774—The controller might reboot due to a failure of the apfReceiveTask software watchdog.
- CSCsm56708—For some rogue clients, the "First Heard" time is after the "Last Heard" time, and the rogue access point MAC address is set to all zeros.
- CSCsm58695—When an 802.3 raw broadcast packet is received from the wired network and 802.3 bridging is enabled, the packet is discarded rather than forwarded to the wireless network.
- CSCsm65113—Access points converted to lightweight mode do not retain the power injector state on the controller after they are rebooted.
- CSCsm70189—An 1130 series access point sometimes crashes before the "Press RETURN to get started" prompt appears on the console.
- CSCsm71840—Mobile client handoff or client guest anchoring fails across mobility groups if the controller to which the client is associating has no other mobility member in its own mobility group but has all members in different groups.
- CSCsm72088—When you change the associated client filter in the controller GUI to filter on specific WLAN profiles that have spaces in them, the controller reports the wrong profile name and shows that no clients are associated. In controller software releases 4.2.61 and 4.2.99, you cannot create a WLAN with a profile name that contains spaces.
- CSCsm75593—When the AP-manager interface is untagged or configured for VLAN ID 0, the following error message appears: "First configure a valid non-zero vlan on this interface."
- CSCsm75708—If you save a controller configuration with five WLANs using different security methods, upload it to a server, and then delete it from the controller, when you try to download the configuration from the server, it downloads without displaying any error messages, but it returns the controller to factory default settings.

- CSCsm80066—When a controller receives an ARP request with its own IP address as the source, it stops responding to Telnet and GUI connections.
- CSCsm80555—On the controller GUI, an incorrect DTIM value appears for the access point configuration. This field should either be removed from the GUI or modified to show the DTIM value for each WLAN on which the access point broadcasts.
- CSCsm85862—You cannot access a 1250 series access point after it is unable to join the controller for several hours.
- CSCsm94067—1100 and 1200 series access points that have been converted to lightweight mode do not retain the power injector state after a reboot. This setting is enabled on the access point; however, when the access point reboots, it shows as not being enabled on the controller.
- CSCsm95651—A controller running software release 4.1.185.0 might reboot spontaneously without generating a crash file.
- CSCsm96105—The controller does not pass traffic to a client device with a MAC address beginning with 00:00:00:00. This issue occurs with both WGB and wireless clients.
- CSCsm96305—After you change the session timeout value of a WLAN, the client reauthentication timeout is not updated.
- CSCsm96307—A controller might reboot unexpectedly following a period of high CPU utilization charged to the SNMPtask. This condition triggers a Reaper Timeout and a system reset.
- CSCsm97315—While installing a web authentication certificate, the controller fails with an invalid password error. This problem occurs only on controllers that have been upgraded from software release 4.1.
- CSCsm98250—After you upgrade the controller to software release 5.0, web authentication stops working, and you can no longer access the controller through HTTP or a Telnet or SSH session.
- CSCsm98659—You cannot change the CDP state in WCS or effectively use the **config ap cdp** {**enable** | **disable**} **all** controller CLI command unless there is at least one access point present on the controller.
- CSCsm99941—Controllers running software release 4.2 or 5.0 might reboot and create a crash log. This behavior occurs frequently if rogue client and access point polling is enabled through WCS on the Location Appliance. If the default polling interval for rogue clients and access points is used, the controller might reboot every 10 minutes.
- CSCso02340—The controller might report a different power level than is actually used by the access point if you change the channel from one supporting one transmit power to another supporting a different transmit power.
- CSCso15640—The controllers in the Cisco WiSM might reboot due to a software failure of the instruction located at 0x1036f2ac (debugPrintMessage2+288).
- CSCso17455—Controllers sometimes reboot when SSH is enabled.
- CSCso20018—In controller software release 5.0, you cannot enable DHCP Required on a guest LAN. In the controller GUI, an error icon appears in the lower left-hand side of the browser.
- CSCso23879—The coverage hold threshold values on the 802.11a (and 802.11b/g) > RRM > Coverage pages on the controller GUI cannot be changed when coverage hole detection is enabled. On the controller CLI, you can change the threshold values if the 802.11a or 80211b/g band is disabled globally. The controller GUI should operate the same way (as long as the 802.11a or 802.11b/g band is disabled globally, the threshold can be changed).

- CSCso27775—The controller logs show several error messages on one line only (both on the CLI and on the syslog server). The error message is truncated, so it does not reach the carriage return in the end. This error message appears when several access points are trying to join a controller that is already at full access point capacity.
- CSCso30745—When a packet fails the admission control test because the switch fabric cell buffers corresponding to its stream are full, it is incorrectly forwarded to the CPU instead of being discarded. This incorrect forwarding of many such packets could cause an overload of the CPU and a Reaper reset.
- CSCso33532—The controller fails to notify WCS when you configure an extension channel for 40-MHz channel width on the controller.
- CSCso36248—The LDAP username is limited to 24 characters in controller software release 4.2.112.0.
- CSCso40917—The FPGA link might stop working, causing the access points to disconnect from the controller and preventing the controller from being managed by any port other than the service port. The NPU Check Task or a similar task should monitor the status of the FPGA link.
- CSCso43852—A controller running software release 4.2.112.0 might reboot due to a software failure of the apfReceiveTask at mmParsePayload.
- CSCso44508—When link aggregation (LAG) is enabled on the controller, the ipAdEntIfIndex value is not listed in the ifIndex.
- CSCso58911—After a controller is upgraded to software release 4.2.112.0, it no longer executes the Java pop-up window on the custom web authentication bundle login page.
- CSCso58919—When AAA override is disabled, the PMK CCKM lifetime value uses the attribute 27 setting from the AAA server instead of the WLAN session timeout.
- CSCso61281—If you enter an invalid username or password on the web authentication page in controller software release 5.0.148.0, an error message does not appear indicating that the username and password combination is invalid and to try again.
- CSCso62862—You cannot edit the TACACS+ priority using SNMP on a 4400 series controller running software release 4.2.112.0.
- CSCso62922—EAP authentication fails for clients when the controller is under high load. In the 802.1X debugs, the client responds to the identity request, but the controller does not seem to process it and times out the authentication.
- CSCso62975—The following error message might appear for Vista clients using an external DHCP server to obtain an IP address after going through the anchor controller: "DHCP dropping REPLY to STA with invalid mobility state 'Export Foreign' (5) on foreign controller."
- CSCso66819—The service port on a Cisco WiSM running software release 5.0.148.0 might become unreachable after some time. The WiSM remains reachable from the management interface, and the access point and client connection is not affected.
- CSCso66889—The @ character cannot be used when configuring access point credentials on a controller running software release 5.0.
- CSCso69568—The RADIUS accounting setting does not appear in the output of the **show wlan** *wlan_ID* CLI command if the WLAN security policy is one of the following:
  - None
  - Static WEP
  - WPA-PSK
  - Web authentication

- CSCso71603—When a client moves from one controller to a 2106 controller on the same subnet, the client cannot pass traffic for 5 minutes.
- CSCso81687—A forwarding failure occurs when an orphan packet is sent to the CPU using the slow path. The following message appears on the console: "NP3400_interrupt.c 3663: In 'NP3400_BSN_process_frame_rx' Unknown packet type 0."
- CSCso81725—The controller's broadcast module is replicating CDP packets to all connected access points even if multicast is disabled. In addition, the controller is replicating broadcast orphan packets from a client even when multicast and broadcast are disabled.
- CSCso84256—During CCKM roaming, the following misleading debug message might appear: "Creating a new PMK Cache Entry for station."
- CSCso89810—When you downgrade a controller from software release 5.0.148.*x* to 4.2.112.0, the LWAPP mode automatically changes from Layer 3 to Layer 2, and the AP-manager disappears and cannot be recreated. This problem is resolved in controller software release 4.2.130.0, so you can successfully downgrade from software release 5.0.148.*x* to 4.2.130.0.
- CSCso90721—When the controllers in a Cisco WiSM are running software release 4.1.112.0, they might reboot three times due to a software failure of the dtlArpTask software watchdog.
- CSCso95257—Clients might time out during WPA2-PSK roaming.
- CSCso97157—A memory leak might occur in the mobility code of controller software release 4.2.
- CSCso98021—The software watchdog needs to be implemented in the 2106 controller.
- CSCso98915—A controller running software release 4.0.219.0 or 4.2.112.0 might reboot during the emweb process.
- CSCsq08062—A TACACS+ connection initiated from the controller to the TACACS+ server sometimes times out in 0.5 seconds.
- CSCsq13407—The dot1x tree might become corrupted as the tree lock is not being acquired prior to entries being deleted from the tree.
- CSCsq31662—The controller reboots after you upgrade from software release 4.2.61.0 to 4.2.112.0.
- CSCsq51733—The controller drops BOOTP packets from the wireless client.
- CSCsq59283—The controller SNMP does not allow an access point group name or description of 32 characters.

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