Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 5.0.148.0

February 13, 2008

These release notes describe open and resolved caveats for software release 5.0.148.0 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, and 1300 Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.

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

Contents

These release notes contain the following sections.

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

Cisco Unified Wireless Network Solution Components

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

- Software release 5.0.148.0 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 5.0.55.0
- Cisco WCS Navigator 1.2.55.0
- Location appliance software release 4.0.32.0
- Cisco 2700 Series Location Appliances
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers

Note The 5.0.148.0 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, and 1300 Series Lightweight Access Points

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

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

Special Notice for Mesh Networks

Note Do not upgrade to controller software release 5.0.148.0 if you have mesh access points in your network. If your network uses mesh access points, use only mesh-specific releases such as 4.1.191.24M.

Note Cisco WCS software release 5.0.55.0 may be used to manage both mesh and non-mesh controllers (such as controllers running software release 5.0.148.0 and 4.1.191.24M). You do not need different instances of WCS to manage mesh and non-mesh controllers.

Controller Requirements

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

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

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

Software Release Information

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

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

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

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

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

Finding the Software Release

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

Upgrading to a New Software Release

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

Note When you upgrade the controller to software release 5.0.148.0, the binary configuration file might not migrate correctly. For details, see the "Software Upgrade Might Fail If Certain Characters Used in Previous Configuration" note in the "Important Notes" section on page 18.

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

Special Rules for Upgrading to Controller Software Release 5.0.148.0

Caution Before upgrading your controller to software release 5.0.148.0, you must comply with the following rules.

- Make sure you have a TFTP server available for the software upgrade. Keep these guidelines in mind when setting up a TFTP server:
  - Controller software release 5.0.148.0 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 tftpd32 and the TFTP server within the WCS. If you attempt to download the 5.0.148.0 controller software and your TFTP server does not support files of this size, the following error message appears: "TFTP failure while storing in flash."
  - If you are upgrading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are upgrading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP server cannot run on the same computer as the WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.

- You can upgrade or downgrade the controller software only between two releases. To upgrade or downgrade beyond two releases, you must first install an intermediate release. For example, if your controller is running a 4.1 or 4.2 software release, you can upgrade your controller directly to software release 5.0.148.0. If your controller is running a 3.2 or 4.0 release, you must upgrade your controller to an intermediate release prior to upgrading to 5.0.148.0. Table 1 shows the upgrade path that you must follow before downloading software release 5.0.148.0.

Table 1 Upgrade Path to Controller Software Release 5.0.148.0

Current Software Release	Upgrade Path to 5.0.148.0 Software
3.2.78.0 or later 3.2 release	Upgrade to 4.0.206.0 (or a later 4.0 release) before upgrading to 5.0.148.0.
4.0.155.5	Upgrade to 4.0.206.0 (or a later 4.0 release) before upgrading to 5.0.148.0.
4.0.179.11	
4.0.206.0 or later 4.0 release	You can upgrade directly to 5.0.148.0.
4.1.171.0 or later 4.1 release	You can upgrade directly to 5.0.148.0.
4.2.61.0 or later 4.2 release	You can upgrade directly to 5.0.148.0.

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

- Cisco recommends that you also install the Cisco Unified Wireless Network Controller Boot Software 5.0.148.0 ER.aes file on the controller. This file resolves defect CSCsd52483 and is necessary to ensure proper operation of the controller. The ER.aes file can be installed on all controller platforms. If you do not install this ER.aes file, your controller does not obtain the fix for this defect, and "Error" appears in the Bootloader Version field in the output of the **show sysinfo** command.

Note Unlike previous ER images, a new bootloader file is not loaded when you install the 5.0.148.0 ER.aes file. This is true for all controllers. The 4.2.112.0 ER.aes file is the last ER file to contain a bootloader. If you want the latest bootloader, install the 4.2.112.0 ER.aes file. If you want to obtain the fix for CSCsd52483, also install the 5.0.148.0 ER.aes file.

Note The ER.aes files are independent from the controller software files. You can run any controller software file with any ER.aes file. However, installing the latest boot software file (5.0.148.0 ER.aes) ensures that the boot software modifications in all of the previous and current boot software ER.aes files are installed.

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

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

Note Do not install the 5.0.148.0 controller software file and the 5.0.148.0 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 5.0.148.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 5.0.148.0 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**, **Wireless Integrated Routers**, or **Wireless Integrated Switches**.

e. Click the name of a controller.

f. Click **Wireless LAN Controller Software**.

g. Click a controller software release.

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

i. Click **Download**.

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

k. Save the file to your hard drive.

l. Repeat steps a. to k. to download the remaining file (either the 5.0.148.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.0.148.0 ER.aes file).

Step 3 Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 5.0.148.0 ER.aes file to the default directory on your TFTP server.

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

Step 5 Disable any WLANs on the controller.

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

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

Step 8 In the IP Address field, enter the IP address of the TFTP server.

Step 9 The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work fine without any adjustment. However, you can change these values if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the software in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the software in the Timeout field.

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

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

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

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

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

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

Step 16 After the controller reboots, repeat Step 6 to Step 15 to install the remaining file (either the 5.0.148.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 5.0.148.0 ER.aes file).

Step 17 Re-enable the WLANs.

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

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

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

Step 21 To verify that the 5.0.148.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 22 To verify that the Cisco Unified Wireless Network Controller Boot Software 5.0.148.0 ER.aes file is installed on your controller, enter the **show sysinfo** command on the controller CLI and look at the Bootloader Version field. "N/A" appears if the ER.aes file is installed successfully. "Error" appears if the ER.aes file is not installed.

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 5.0.148.0.

Note Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.0* for details and configuration instructions for each of these features.

Controller Platform Changes

- Without any other service module installed, the Catalyst 6509 switch chassis can support up to seven Cisco WiSMs, the Catalyst 6506 with a Supervisor 720 can support up to four Cisco WiSMs, and any other Catalyst 6500 series switch chassis can support up to six Cisco WiSMs. If one or more service modules are installed, the chassis can support up to a maximum of four service modules (WiSMs included). Redundant supervisors cannot be used with these maximum configurations.
- Without any other service module installed, the Cisco 7609 router chassis can support up to seven Cisco WiSMs, and any other Cisco 7600 series router chassis can support up to six Cisco WiSMs. If one or more service modules are installed, the chassis can support up to a maximum of four service modules (WiSMs included). Redundant supervisors cannot be used with these maximum configurations.

  Note The WiSM is supported on Cisco 7600 series routers running only Cisco IOS Release 12.2(18)SXF5 or later.

- The 2000 series controllers are not supported for use with controller software release 5.0.148.0.

New Controller Features

- **AutoInstall**—When a controller (without a configuration) boots up for the first time, it can use this feature to download a configuration file from a TFTP server automatically. Once the controller is configured by the auto-install (or auto-provisioning) process, it is automatically added to WCS.
- **Coverage hole detection**—In controller software release 5.0.148.0, if both the number and percentage of failed packets exceed the values configured for Failed Packet Count and Failed Packet Percentage (configurable through the controller CLI) for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the Min Failed Client Count per AP and Coverage Exception Level per AP fields over a 90-second period. The controller determines if the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.
- **Daylight Saving Time**—Daylight Saving Time (DST) is now supported on the controller. If you choose a timezone that uses DST when you configure the system date and time, the controller automatically sets its system clock to reflect the time change when DST occurs. To prevent DST from being set, you must manually set the timezone using the controller CLI.

- **DTIM per WLAN**—In 802.11a/n and 802.11b/g/n networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

  In controller software release 5.0.148.0, you can configure the DTIM period for the 802.11a/n and 802.11b/g/n radio networks on specific WLANs. In previous software releases, the DTIM period was configured per radio network only, not per WLAN. The benefit of this change is that now you can configure a different DTIM period for each WLAN. For example, you might want to set different DTIM values for voice and data WLANs.

  Note The **config** {**802.11a** | **802.11b**} **dtim** CLI command has been replaced by this new command: **config wlan dtim** {**802.11a** | **802.11b**} *dtim wlan_id*.

  Note When you upgrade the controller software to release 5.0.148.0, the DTIM period that was previously configured for a radio network is copied to all of the existing WLANs on the controller.

- **High availability**—The following features have been implemented on the controller CLI 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:
  - To reduce the controller failure detection time, you can configure the heartbeat interval (between the controller and access point) with a smaller timeout value.
  - The access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry on the list. You can now configure a primary discovery request timer to specify the amount of time that a controller has to respond to the access point's discovery request before the access point assumes that the controller cannot be joined and waits for a discovery response from the next controller in the list.
  - In addition to the option of configuring primary, secondary, and tertiary controllers for a specific access point, you can now also configure primary and secondary backup controllers for a specific controller. If the access point's local controller fails, it chooses an available controller from the backup controller list in this order: primary, secondary, tertiary, primary backup, secondary backup.
- **High-density networking for 802.11b/g**—High-density networking optimizes wireless LAN capacity and improves overall network performance in dense, multi-cell wireless networks. You can manually specify global values for receiver sensitivity threshold, clear channel assessment (CCA) sensitivity threshold, and transmit power values across all Cisco lightweight access points registered to a given controller. In controller software releases 4.2 and 4.1, you can configure these parameters only for 802.11a networks. In controller software release 5.0.148.0, you can configure them for both 802.11a and 802.11b/g networks. High-density networking is supported on all Cisco lightweight access points (except the wireless mesh access points) and on notebooks using the Intel PRO/Wireless 3945ABG and Intel Wireless WiFi Link 4965AG clients.
- **Hybrid-REAP Groups**—Controller software release 5.0.148.0 contains two new hybrid-REAP group features:
  - **Backup RADIUS server**—You can configure the controller to allow a hybrid-REAP access point in standalone mode to perform full 802.1X authentication to a backup RADIUS server. You can configure a primary RADIUS server or both a primary and secondary RADIUS server.

  - **Local authentication**—You can configure the controller to allow a hybrid-REAP access point in standalone mode to perform LEAP or EAP-FAST authentication for up to 20 statically configured users. The controller sends the static list of usernames and passwords to each hybrid-REAP access point when it joins the controller. Each access point in the group authenticates only its own associated clients. This feature is ideal for customers who are migrating from an autonomous access point network to an LWAPP hybrid-REAP access point network and are not interested in maintaining a large user database nor adding another hardware device to replace the RADIUS server functionality available in the autonomous access point.

    Note Local authentication can be used in conjunction with the hybrid-REAP backup RADIUS server feature. If a hybrid-REAP group is configured with both a backup RADIUS server and local authentication, the hybrid-REAP access point always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally the hybrid-REAP access point itself (if both the primary and secondary are not reachable).

- **IDS signature management**—In controller software release 5.0.148.0, you can configure signature IDs to uniquely identify signatures and modify the Signature Frequency, Signature Max Frequency, and Quiet Time parameters to reduce false positives.
- **Local EAP timers**—Additional timeout and retry parameters have been added for local EAP.
- **Mobility multicast messaging**—This feature enables the controller to use multicast mode to send Mobile Announce messages to the mobility members. If you do not enable this feature, the controller uses unicast mode to send the Mobile Announce messages.
- **RADIUS server fallback**—In controller software releases prior to 5.0.148.0, when a primary RADIUS server becomes unresponsive, the controller switches to the secondary RADIUS server and continues to use this server indefinitely, even if the primary server is available. In controller software release 5.0.148.0, you can configure the controller to fall back to the primary RADIUS server when it recovers or to a more preferable server.
- **Rogue management**—Controller software release 5.0.148.0 introduces the following rogue management features:
  - **Ignoring autonomous access points managed by WCS**—In previous releases, the controller regards autonomous access points as rogues even if WCS is managing them. In controller software release 5.0.148.0, the controller can now ignore these access points rather than treating them as rogues. The Rogue AP Ignore-List page shows the MAC addresses of any access points that are configured to be ignored.
  - **Rogue Location Detection Protocol (RLDP) on monitor mode access point**—The controller continuously monitors all nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses RLDP to determine if the rogue is attached to your network. In controller software release 5.0.148.0, you can configure the controller to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure the controller to use RLDP on all access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby.

    Note RLDP is not supported for use with Cisco autonomous rogue access points.

  - **Rule-based classification**—Controller software release 5.0.148.0 improves the classification and reporting of rogue access points through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states. In previous releases, the controller listed all rogue access points on one page sorted by MAC address or BSSID. Now you can create rules that enable the controller to organize and display rogue access points as Friendly, Malicious, or Unclassified.

- **Sending syslog events to multiple servers**—In controller software release 5.0.148.0, you can enable the controller to log system events to up to three remote syslog servers. The controller sends a copy of each syslog message as it is logged to each syslog server configured on the controller. Being able to send the syslog messages to multiple servers ensures that the messages are not lost due to the temporary unavailability of one syslog server.
- **Splash page web redirect**—This feature redirects a user to a particular web page after 802.1X authentication has completed successfully. After the redirect, the user has full access to the network. You can specify the redirect page on your RADIUS server. This feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security.
- **Telnet and SSH support**—The controller supports the use of Telnet or Secure Shell (SSH) protocols to troubleshoot lightweight access points. Using these protocols makes debugging easier, especially when the access point is unable to connect to the controller. You can configure Telnet and SSH support only through the controller CLI.
- **Wireshark sniffer support**—The controller enables you to configure an access point as a network "sniffer," which captures and forwards all the packets on a particular channel to a remote machine that runs packet analyzer software. These packets contain information on timestamp, signal strength, packet size, and so on. Sniffers allow you to monitor and record network activity and to detect problems. In previous controller software releases, only the following packet analyzers are supported: Wildpackets Omnipeek and Airopeek and the AirMagnet Enterprise Analyzer. In controller software release 5.0.148.0, the Wireshark packet analyzer is also supported.

New Guest Access Features

- **Customized web authentication pages**—In controller software release 5.0.148.0, you can configure the controller to display customized login, login failure, and logout web authentication pages per WLAN or guest LAN. In previous controller software releases, you can configure only customized web login pages.
- **LDAP support**—In controller software release 5.0.148.0, the controller supports web authentication using LDAP.

New Location Features

- **Location Optimized Monitor Mode (LOMM)**—To optimize the monitoring and location calculation of RFID tags, you can enable LOMM on up to four channels within the 2.4-GHz band of an 802.11b/g access point radio. This feature allows you to scan only the channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).
- **Location presence (S69)**—This feature enables a location server to provide a CCXv5 client with its location upon request. Location presence is enabled automatically on CCXv5 clients. The S69 Capability line in the output of the **show client detail** *client_mac* CLI command indicates whether a client supports location presence.

GUI Enhancements

- **RRM pages**—The RRM menu options have been divided among five new controller GUI pages to improve usability.

Access Point Changes

- **Cisco Aironet 1000 Series Access Points**—The 1000 series access points are not supported for use with controller software release 5.0.148.0 or later.
- **Global credentials**—In controller software releases prior to 5.0.148.0, you can set the access point enable password only for access points that are currently connected to the controller. In controller software release 5.0.148.0, you can set a global username, password, and enable password that all access points inherit as they join the controller. This includes all access points that are currently joined to the controller and any that join in the future. Also in controller software release 5.0.148.0, after an access point joins the controller, the access point enables console port security, and you are prompted for your username and password whenever you log into the access point's console port. When you log in, you are in non-privileged mode, and you must enter the enable password in order to use the privileged mode.

Note The global credentials feature in controller software release 5.0.148.0 is supported on all access points that have been converted to lightweight mode, except the 1100 series. VxWorks access points are not supported.

Note The following command is no longer valid: **config ap username** *user_id* **password** *passwd* {**all** | *ap_name*}.

Regulatory Updates

- **Japan update**—The Japanese government is formally permitting wireless LAN use of the frequencies in the W56 band for 802.11a radios. The W56 band includes the following channels, frequencies, and power levels (in dBm):

Channel	Frequency (MHz)	Maximum Power for AIR-LAP1132AG-Q-K9	Maximum Power for AIR-LAP1242AG-Q-K9
100	5500	17	15
104	5520	17	15
108	5540	17	15
112	5560	17	15
116	5580	17	15
120	5600	17	15
124	5620	17	15
128	5640	17	15
132	5660	17	15

Channel	Frequency (MHz)	Maximum Power for AIR-LAP1132AG-Q-K9	Maximum Power for AIR-LAP1242AG-Q-K9
136	5680	17	15
140	5700	17	15

All of the channels in the W56 band require dynamic frequency selection (DFS). In Japan, the W56 band is subject to Japan's DFS regulations. Currently, only the new 1130 and 1240 series access point SKUs (with the -Q product code) support this requirement: AIR-LAP1132AG-Q-K9 and AIR-LAP1242AG-Q-K9.

To set up a network consisting of only -P and -Q access points, configure the country code to J2. To set up a network consisting of -P, -Q, and -U access points, configure the country code to J3.

- **Additional country support**—Country codes have been added for these additional countries supported by the controller: Bahrain (BH), Costa Rica (CR), Dominican Republic (DO), Ecuador (EC), Kazahkstan (KZ), Kuwait (KW), Oman (OM), Pakistan (PK), Paraguay (PY), Puerto Rico (PR), Vietnam (VN).

Note For a complete list of country codes supported per product, refer to 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 5.0.148.0:

- You cannot configure the LWAPP mode from the controller configuration wizard, GUI, or CLI. Controller software release 5.0.148.0 supports only Layer 3 LWAPP mode.
- The **show msglog** CLI command will be discontinued. Please use the **show logging** command instead.
- The controller leverages actual PHY and Low Layer MAC measurements by the access point and client to better estimate Rx, Tx, and CCA loads.
- New messages appear on the controller CLI when you make a configuration change that requires a reboot. Here is an example: "Please save the configuration and reset the system ("reset system") for the change to take effect."

Installation Notes

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

Warnings

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

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

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

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

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

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

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

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

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

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

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

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

Installation Instructions

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

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

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

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

Important Notes

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

Software Upgrade Might Fail If Certain Characters Used in Previous Configuration

In controller software release 4.2.61.0 and later, the controller's bootup configuration file is stored in an Extensible Markup Language (XML) format rather than in binary format. When you upgrade a controller to 4.2.61.0 or a later software release, the binary configuration file is migrated and converted to XML. However, the configuration file does not migrate correctly if it contains any of the following characters as part of a user configuration string: &, <, >, ', ". For example, a WLAN profile named *R&D* causes an XML parsing error after the second reboot, even though this profile name is valid in 4.1 and previous configurations.

Note You cannot download a binary configuration file onto a controller running software release 5.0.148.0. 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, the LWAPP mode changes to Layer 3 if it was previously configured for Layer 2.

If you downgrade from controller software release 5.0.148.0 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.

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.

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.

Cisco 1250 Series Access Points and Cisco 7920 IP Phones

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

Disabling Radio Bands

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

40-MHz Channels in the 2.4-GHz Band

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

Impact of External Antenna Gain on Transmit Power

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

Regulatory Changes

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

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

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

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

Supporting Oversized Access Point Images

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

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

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

Follow these steps to perform the TFTP recovery procedure.

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

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

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

Multicast Limitations

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

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

Multicast Queue Depth

The multicast queue depth is 512 packets on all controller platforms. However, the following message might appear on 2106 controllers: "Rx Multicast Queue is full on Controller." This message does not appear on 4400 series controllers because the 4400 NPU filters ARP packets 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.

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

CKIP Not Supported with Dynamic WEP

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

Setting the Date and Time on the Controller

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

Synchronizing the Controller and Location Appliance

For controller software release 4.2 or later, if a location appliance (release 3.1 or later) is installed on your network, the time zone must be set on the controller to ensure proper synchronization between the two systems. Also, Cisco highly recommends that the time be set for networks that do not have location appliances. Refer to Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 5.0* for instructions for setting the time and date on the controller.

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

FCC DFS Support on 1130 Series Access Points

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

Inaccurate Transmit Power Display

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

Setting the Retransmit Timeout Value for TACACS+ Servers

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

Configuring an Access Point's Prestandard Power Setting

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

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

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

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

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

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

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

Controller Functions that Require a Reboot

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

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

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

2106 Controller LEDs

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

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

Rate-Limiting on the Controller

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

Pings Supported to the Management Interface of the Controller

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

Pinging from a Network Device to a Controller Dynamic Interface

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

GLBP Not Supported

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

IPSec Not Supported

Software release 5.0.148.0 does not allow you to choose IPSec as a Layer 3 security option. None and VPN Passthrough are the only available options. If you upgrade to this release from a previous release that supported IPSec as a Layer 3 security option, any WLANs that are configured for this feature become disabled. If you want to configure IPSec, you must use a version of controller software prior to 4.0.

4400 Series Controllers Do Not Forward Subnet Broadcasts through Guest Tunnel

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

Re-enable Broadcast after Upgrading to Release 4.0.206.0

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

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

config network broadcast enable

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

Connecting 1100 and 1300 Series Access Points

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

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

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

Preventing Clients from Accessing the Management Network on a Controller

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

Voice Wireless LAN Configuration

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

Changing the IOS LWAPP Access Point Password

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

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

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

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

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

"ERROR!!! Command is disabled."

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

Exclusion List (Blacklist) Client Feature

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

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

RADIUS Servers and the Management VLAN

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

RADIUS Servers

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

Management Usernames and Local Netuser Names

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

802.1X and Microsoft Wireless Configuration Manager

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

Using the Backup Image

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

With the backup image stored before rebooting, be sure to choose **Option 4: Change Active Boot Image** from the boot menu to set the backup image as the active boot image. Otherwise, when the controller resets, it again boots off the corrupted primary image.

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

Home Page Retains Web Authentication Login with IE 5.x

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

Rogue Location Discovery Protocol (RLDP)

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

Ad-Hoc Rogue Containment

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

Changing the Default Values of SNMP Community Strings

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

Changing the Default Values for SNMP v3 Users

The controller uses a default value of “default” for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 5.0* for configuration instructions.

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

Features Not Supported on 2100 Series Controllers

These hardware features are not supported on 2100 series controllers:

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

These software features are not supported on 2100 series controllers:

- VPN termination (such as IPSec and L2TP)
- Termination of guest controller tunnels (origination of guest controller tunnels is supported)
- External web authentication web server list
- Layer 2 LWAPP
- Spanning tree
- Port mirroring
- Cranite
- Fortress
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)
- Multicast unicast mode

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

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

2106 Image Not Supported for 3504 Controllers

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

Running a 3504 Image on a 2106 Controller

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

Upgrading External Web Authentication

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

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

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

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

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

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

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

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

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

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

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

}

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

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

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

<tr align="center">

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

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

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

Caveats

This section lists open, resolved, and closed caveats for Cisco controllers and lightweight access points.

Open Caveats

These caveats are open in controller software release 5.0.148.0.

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

  Workaround: Ignore the prompt and exit as usual.

- CSCsd54928—The CPU ACL is unable to block LWAPP packets on the AP-manager interface.

  Workaround: None.

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

  Workaround: Use the controller CLI.

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

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

- CSCsd96295—IPSec clients are not getting excluded. There is no trap or message log generated.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: Use a wireless sniffer trace.

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

  Workaround: None.

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

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

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

  Workaround: Perform another software upgrade and downgrade.

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

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

- CSCsg88704—When you use the default controller setting of 512 for the controller database size, the following problems may occur:

  - If you attempt to add a MAC address to a very long MAC filter list, the following error message appears: “Error in creating MAC filter.”
  - If you add a large number of users to the local database, some user entries might be silently ignored.
  - If you add SSCs for the access points, at some point no more entries can be added, and the following error message appears: “Authorization entry does not exist in Controller’s AP Authorization List.”

  Workaround: Configure a larger value for the controller database, such as 2048.

- CSCsg92043—The output of the **show running-config** CLI command cannot be pasted as is into a different controller because the MAC filters are shown without colons (for example, macfilter add 000b85626640 0). As a result, an incorrect input error message appears when the output is copied to another controller.

  Workaround: None.

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

  Workaround: Power cycle the 7921 phone.

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

  Workaround: None.

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

  Workaround: None.

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

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

  Workaround: None.

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

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

- CSCsi00003—If you enter the wrong username or password more than three times on the web login page, the client is blacklisted. The Client Excluded page, which instructs you to contact the administrator, does not appear, and the client disassociates from the network.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsi29262—The access point does not beacon an overridden WLAN with a 32-character SSID.

  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.

- CSCsi57300—A controller running software release 4.1.158.x might reboot when you execute the **show running-config** CLI command.

  Workaround: None.

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

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

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

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

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

  Workaround: None.

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

  Workaround: None.

- CSCsj10755—The controller generates a unicast query for each access point.

  Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsj39544—The console output takes precedence over the user configuration, Telnet, and HTTPS interfaces.

  Workaround: None.

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

  Workaround: None.

- CSCsj46537—When you are in config mode in the controller CLI and then enter the **exit** command, the controller prompt should appear, but instead the controller remains at the config prompt.

  Workaround: None.

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

  Workaround: Reboot the controller.

- CSCsj50364—Traps occur every 60 seconds when the channel assignment is set to off.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsj68456—Various access points on the controller report duplicate IP addresses detected and being used by an access point with a MAC address of 00:00:00:00:00:00.

  Workaround: None. This appears to be a cosmetic issue.

- CSCsj81768—Multicast performance on 802.11b/g radios is sometimes poor.

  Workaround: None.

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

  Workaround: Enter a valid netmask.

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

  Workaround: None.

- CSCsj92716—A workgroup bridge (WGB) device periodically loses connectivity with the controller.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsk04442—You are unable to configure the channel switch count and mode.

  Workaround: None.

- CSCsk08350—The “Not configured to accept self-signed access point certificates” message should be suppressed.

  Workaround: None.

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

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

  Workaround: None.

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

  Workaround: None.

- CSCsk08918—The RRM process occurs after changing an access point from monitor to local mode or from monitor to hybrid-REAP mode.

  Workaround: None.

- CSCsk09466—After you reboot the Cisco WiSM through the controller GUI, the controller becomes unresponsive.

  Workaround: To recover, pull out the Cisco WiSM module or power cycle the Catalyst 6500 switch.

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

Workaround: None.

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

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

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

  Workaround: None.

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

  Workaround: None.

- CSCsk25178—The web authentication type of the guest LAN does not configure nor display correctly for the override global configuration on the controller GUI.

  Workaround: Use the controller CLI to configure and view the results.

- CSCsk29034—CCA fails due to timing issues in accounting records when using web authentication, inter-controller roaming, and different VLANs.

  Workaround: Use PEAP, WPA-PSK, or something other than web authentication.

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

  Workaround: Downgrade the controller software to the 3.2.195.13 release.

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

  Workaround: None.

- CSCsk39361—An error appears when you check the **DHCP Addr. Assignment Required** check box.

  Workaround: None.

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

  Workaround: Use the controller CLI to view this information.

- CSCsk42678—A universal workgroup bridge (WGB) client might have trouble getting a DHCP address. After configuring the WGB to connect to a controller running software release 5.0, the access point must disassociate and then reassociate in order to communicate with the DHCP server in order to get an IP address.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsk54910—For a 1250 series access point, the UDP throughput is lower than the TCP throughput.

  Workaround: None.

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

  Workaround: Reboot the controller.

- CSCsk56107— After you clear the configuration, any newly added SNMPv3 users are not recognized.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsk64674—The controller might become locked while the access point image is downloading.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

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

- CSCsk80312—If port 2, 3, or 4 is used for the management interface on a controller running software release 4.1.185.0, no management access is available after the controller reboots.

  Workaround: Use port 1 for the management interface, or assign a different port for the management interface and then change back to the original port using these CLI commands:

  - **config wlan disable** *wlan_id*
  - **config interface port management** *any_other_port#*
  - **config interface port management** *original_port#*
  - **config wlan enable** *wlan_id*

- CSCsk86992—Many instances of the following message appear in the controller or WCS trap logs:

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

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

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsk99556—The Cisco WiSM might reboot a few days after installation when it was up and running fine.

  Workaround: None.

- CSCsl00450—When ping sizes are forced to different platforms, different results display for MTU.

  Workaround: None.

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

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

- CSCsl02661—Access point group VLAN interface mapping is referenced even when the dynamic interface is deleted.

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

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

  Workaround: None.

- CSCsl09066—A WCS access point group VLAN profile configuration does not match the actual controller configuration. This problem occurs when using multiple interface mapping profiles under the same access point group VLAN where all of the SSIDs start with the same letters or numbers.

  Workaround: None.

- CSCsl10887—5-GHz clients are not able to associate to a 1250 series access point following a reboot.

  Workaround: None.

- CSCsl11352—The current console output does not indicate which controller the access point joins.

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

- CSCsl13487—Connectivity to the controller might be lost for about 5 minutes due to an NPU lockup. The controller's CPU remains up with console access but with no connectivity.

  Workaround: Use this command to enable RADIUS IPSec: **config radius auth ipsec enable** *index*. Loss of connectivity lasts for around 5 minutes. Afterwards, connectivity is re-established to the controller, and the controller functions normally.

- CSCsl13645—Controller changes to an access point radio might result in misconfigured radio power output unless the changes are applied twice.

  Workaround: None.

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

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

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

  Workaround: None.

- CSCsl24354—Data rate negotiation with select 802.11b and 802.11g rates results in poor performance.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Always use the controller GUI to configure syslog.

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

  Workaround: None.

- CSCsl32982—An access point in hybrid-REAP mode can fall into a state where it is in standalone mode but the radios are down for an indefinite amount of time. This behavior is not intended as hybrid REAP carries the promise of functionality even without WAN link availability.

  Workaround: Reboot the access point in hybrid-REAP mode to force it into functional standalone mode if the WAN link is down.

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

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

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

  Workaround: None.

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

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

  Workaround: None.

- CSCsl41757—If any WLAN profile names contain an ampersand (&) when you upgrade a controller to software release 4.2, the controller erases the current configuration and reboots into the setup wizard.

  Workaround: Remove any ampersands from WLAN names before you upgrade to software release 4.2.

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

  Workaround: None.

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

  config 802.11h channel switch enable *mode_value*

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

  Workaround: None.

- CSCsl46176—LDAP does not operate correctly on controllers.

  Workaround: None.

- CSCsl47720—The controller linktest results are sometimes inconsistent.

  Workaround: None.

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

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

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

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

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

  Workaround: None.

- 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 only130 characters.

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

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

  Workaround: None.

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

  Workaround: None. This issue is cosmetic.

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

  Workaround: Delete one rule at a time.

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

  Workaround: None.

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

  Workaround: None.

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

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

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

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

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

  Workaround: None.

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

  Workaround: Use the controller CLI for TFTP transfers.

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

  Workaround: None.

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

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

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

  Workaround: Reboot the access point.

- CSCsl69066—If a controller has 16 WLANs configured with 15 WLAN overrides on both radios, an 1130 access point and a 1250 access point join the controller with no problem. When both access points are reset, the 1130 access point has no issues, but a traceback is found on the 1250 access point, even though it still joins the controller.

  Workaround: None.

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

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

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

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

- CSCsl70838—In an environment with a lot of RF traffic, 802.11a radios go off channel frequently while scanning. This behavior causes clients to take a long time to authenticate (for example, when the clients connect using EAP-FAST, LEAP, or EAP-TLS).

  Workaround: Increase the values for the Noise Measurement and Channel Scan Duration intervals.

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

  Workaround: None.

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

  Workaround: None.

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

Workaround: None.

- CSCsl72849—A Cisco WiSM running controller software release 4.1.185.0 frequently reboots due to a software failure of the mmListen task.

  Workaround: None.

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

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

- CSCsl76700—A workgroup bridge (WGB) might time out while waiting for a reassociation response.

  Workaround: Increase the eapol-key-timeout value.

- CSCsl77058—The word “rogue” is misspelled in one of the WLAN message log statements. The correct statement should be “APF-1-UNABLE_TO_KEEP_ROGUE_CONTAIN.”

  Workaround: None.

- CSCsl79069—When the AAA override is enabled for a WLAN and the AAA server is providing the session-timeout value, if a client associated to that WLAN roams to another access point joined to the same controller and the session timeout has not expired, the session timeout for that client is reset to the initial value received from the AAA server.

  Workaround: None.

- CSCsl79623—When the WLAN session timeout is set to zero or is not selected at all, the user idle timeout is ignored.

  Workaround: Set a session timeout value.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsl85178—A bi-directional video conference call from an autonomous 1242 access point in WGB mode to a lightweight 1242 access point joined to a 4404 controller becomes overloaded after a few seconds, and data drops very rapidly.

  Workaround: Connect an autonomous 1242 bridge to an autonomous 1242 bridge using point-to-point communications.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Downgrade the controller to software release 4.1.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Disable the master controller mode.

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

  Workaround: None.

- CSCsm04265—Multiple 4402 controllers running software release 4.1.185.0 might hang with no console output. They cannot be accessed through the console or IP, and they do not reboot automatically.

  Workaround: Reboot the controllers.

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

  Workaround: None.

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

  Workaround: None.

- CSCsm08497—When a Cisco CB21AG client working as an 802.11a client is receiving downstream traffic from a 1250 series access point, it might become disconnected from the access point just prior to reaching an RSSI value of ~100 dB.

  Workaround: None.

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

  Workaround: None.

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

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsm13785—A controller running software release 4.2.61.0 can successfully transfer the upload "config" datatype but not the "binary-config" datatype.

  Workaround: None.

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

  Workaround: None.

- CSCsm15608—The aggregate downstream UDP throughput with 20 802.11n clients might be lower than the throughput with one client. Typically, it is expected that additional clients yield higher throughput than with one client.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsm20234—The controller does not respond to discovery requests when the AP-manager interface is in a different VLAN than the management interface.

  Workaround: Move the AP-manager interface to the same VLAN as the management interface.

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

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

- CSCsm21360—When access point group VLANs are configured, client connectivity is interrupted after a roam between controllers.

  Workaround: Turn on symmetric mobility tunneling and reboot the controller.

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

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

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

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

Resolved Caveats

These caveats are resolved in controller software release 5.0.148.0.

- CSCsb81363—The bootloader version does not appear in the output of the **show sysinfo** command when the controller is booted up with a backup image.
- CSCsb85113—When you download the software image to the controller using the CLI, access points are sometimes disconnected.
- CSCsd52483—When you make changes to the bootloader of a 2106 controller or a Controller Network Module, the bootup process sometimes stops, and the controller stops responding. The controller also displays the "grub>" prompt on the console port.
- CSCsd92608—SntpServerNextGet() has an incorrect return type. The return type is L7_BOOL. However, the return values are: L7_FAILURE, L7_ERROR, and L7_SUCCESS.
- CSCse89587—The CPU ACL breaks when the LWAPP mode is Layer 2. The CPU ACL works in Layer 3 mode.
- CSCsf27201—The "Multicast Rx queue is full" message might appear in the system message log even when multicast is disabled and there is no multicast traffic.
- CSCsf99924—There is no way to automatically adjust the local time for Daylight Saving Time (DST).
- CSCsg05961—AppleTalk cannot see other clients or zones when access point group VLANs are configured.
- CSCsg26982—The 4402 controller does not respond properly to the SNMP server interface discovery.
- CSCsg45844—The **config port admin mode** {*port* | **all**} **disable** command does not bring the link status to the "DOWN" state.

- CSCsh18948—Some access points in monitor mode report RSSI and SNR values of –1. These values result in incorrect rogue detection and location tracking.
- CSCsh29597—When the OTP password is used to authenticate the web management interface of the controller, clicking any link on the controller GUI results in reauthentication.
- CSCsh54247—These changes need to be implemented in the controller logging functions:
  - Setting the syslog severity to filter out-going syslog messages
  - Setting the syslog facility
  - Configuring multiple syslog servers on the controller
- CSCsh58395—After successful web authentication, a gray web page appears with the words "Web Authentication." The web browser appears to be loading a page, but the original URL destination never loads.
- CSCsh61934—When a client authenticates to an LWAPP wireless infrastructure and sends a Reverse Address Resolution Protocol (RARP) packet to the RARP server, the client never receives a server response and cannot get a Layer 3 address.
- CSCsh67192—If link aggregation (LAG) is enabled but the controller was not rebooted, a new dynamic interface cannot be created. The controller displays the "Unable to create VLAN interface" message, but the message does not indicate why the interface cannot be created.
- CSCsh73488—When you apply a controller template for web authentication with the Web Auth Type set to external, an SNMP error occurs on WCS. The operation status is set to "Failure," and the reason is set to "SNMP operation to Device failed."
- CSCsh76257—When DHCP is enabled for both service ports on a Cisco WiSM, the two ports get different IP addresses from the DHCP server. Before the IP address leases expire, the two controllers try to renew the DHCP addresses, but this operation does not correctly renew the binding on the DHCP server. The DHCP server believes that these IP addresses are no longer in use and returns the addresses to the DHCP pool. The service ports still have the IP addresses previously requested. If one of the two controllers is restarted, this controller gets the first address in the pool that matches the address on the other service port.
- CSCsh78901—The controller displays the wrong bandwidth contract parameters for QoS levels.
- CSCsh79538—The **debug mac addr** command does not parse on a specific MAC address.
- CSCsh81184—A DHCP lease timeout is necessary for non-authenticated users that use web authentication. When DHCP addressing is limited, a timeout should occur on leased IP addresses for users that are not in the authenticated state.
- CSCsh83374—If you debug a client using the **debug client** command, web authentication stops working.
- CSCsh85278—The access point manager interface does not use the HSRP MAC address when replying to access points that are off the local subnet.
- CSCsh97400—When an out-of-the-box access point with a recovery image discovers, joins, and then tries to download an image from the controller, there are insufficient debug messages for troubleshooting purposes if the image does not download correctly.
- CSCsi13086—After third-party certificates are successfully installed and the controller is rebooted, the controller still shows a web authentication certificate that was generated locally on both the GUI and CLI.
- 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.

- CSCsi25491—When you choose the **Wireless** option from the CPU ACL Mode drop-down box on the CPU Access Control Lists page, the interface automatically chooses the Both option, not the Wireless option.
- CSCsi34642—The external web server list in the output of the **show custom-web all** CLI command is misformatted and difficult to read.
- CSCsi35427—The controller stops functioning due a software failure in the pemReceiveTask.
- CSCsi56611—The controller does not respond to a device with an x.x.x.255 address.
- CSCsi71840—When an invalid physical port number of 25 or less is configured on the access point manager and dynamic interface from the web console, the "Could not set the configuration" message appears, but an invalid physical port number is still set.
- CSCsi75400—DHCP leases for clients that have been disassociated for hours (or longer) still appear in the output of the **show dhcp lease** command. The controller does not expire or delete leases after clients drop or disassociate from the controller.
- CSCsi77945—Cisco 792x phones fail to join the network when using EAP-FAST with WPA+TKIP and local EAP authentication.
- CSCsi80732—When the 802.11b/g radio is configured with all rates disabled and only 24, 36, 48, and 54 Mb/s as mandatory, the controller does not associate wireless clients correctly.
- CSCsi81630—The controller might reboot with the apfProcessClientAssocResp process. This issue typically happens repeatedly about 5 minutes after system startup.
- CSCsi86800—After an upgrade to software release 4.1, the controller might start processing unicast traffic with a destination different from its MAC and IP address (in promiscuous mode). This issue can be aggravated by network topology issues (for example, traffic flooding).
- CSCsi90860—When local EAP is used to authenticate clients, the following message unnecessarily fills the system log:

  ```
  OSAPI-4-TIMERTCB_REALLOCATED: Timer 3607/1800205 ('EAP Local Auth') found to be
  destroyed/reallocated.
  ```

- CSCsi97452—When a Cisco 7921 phone associates to a WLAN that is configured on a 2106 controller, the controller becomes unresponsive and eventually reboots.
- CSCsi99388—The message log level for security errors cannot be configured correctly.
- CSCsi99569—The controller might report an incorrect number of rogue clients in the rogue access point summary.
- CSCsj00967—A wireless client cannot associate to an access point for 30 seconds after the SSID is changed on a hybrid-REAP access point.
- CSCsj12053—The controller cannot learn the IP address of wired clients such as terminal servers that do not initiate any traffic. The controller deletes these wired client records.
- CSCsj18577—After the controller is upgraded to software release 4.1.171.0 and configured with WPA1 or WPA2 using PSK, the syslog server logs the following message:

  ```
  AAA-5-RADSERVER_NOT_FOUND: Couldn't find appropriate Radius server for VAP 6. Reason :
  Radius accounting is disabled.
  ```

- CSCsj19875—The controller reports the following error:

  ```
  Client Association Failure: MACAddress:00:15:70:17:8f:69 Base Radio
  MAC:00:14:f2:7d:be:00 Slot: 0 Reason:Unspecified ReasonCode: 1
  ```

This error message does not contain the MAC address of the client. The MAC address in the message is for an access point that is associated to the controller. When this message is reported to WCS release 4.1.83.0, WCS reports the access point MAC address as the client MAC address.

- CSCsj20381—In controller software release 4.1.171.0, the attributes sent to the RADIUS server in the AAA debugs are truncated. The debug output stops at between 48 and 64 bytes. When debug client functionality is enabled, no AAA attributes are displayed.
- CSCsj20565—When you access the CDP > Interface Neighbors page on the controller GUI from a 4402 or 4404 controller running software release 4.1.171.0, the controller might reboot.
- CSCsj21554—After logging into the controller, lobby ambassador users can gain read-only access to the controller configuration by using each section of any configuration URL.
- CSCsj24288—In controller software releases prior to 4.2, the **show running-config** CLI command shows the netuser password in clear text.
- CSCsj31387—The Cisco WiSM might reboot when the **show run-config** command is entered.
- CSCsj33740—A Location Protocol (LOCP) transmit crash might occur.
- CSCsj34491—Because the number of controller database entries in use is unknown, the "User cannot be created" messages might cause confusion when the maximum number of entries is reached.
- CSCsj40441—Manual PAC provisioning for Aironet Desktop Utility (ADU) release 3.6 fails with controller software release 4.1.171.0 when using a password to import the PAC.
- 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.
- CSCsj45526—Multiple syslog server hosts cannot be configured using SNMP.
- 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.
- CSCsj47539—The following message is logged in the controller message log when the rogue table in the controller is full:

  ```
  APF-1-ROGUE_AP_ADD_FAILED: Failed to add the rogue AP xx:xx:xx:xx:xx:xx. insertion
  failed.
  ```

- CSCsj47720—IP conflict detected messages on the 2106 controller for the management interface IP address might appear.
- CSCsj50374—After upgrading six WiSMs with ARP unicast enabled, broadcast loops (ARP requests) might be generated by the two controllers in slot 8. The transmit and receive rate on those two controllers could go up to ~1 Gb/s.
- CSCsj52661—Wireless multicast packets that exceed 1432 bytes are dropped after roaming.
- CSCsj54830—A message that warns users not to configure over the maximum number of access point groups on a VLAN is necessary.
- CSCsj55240—The Cisco IOS SSH client cannot establish a session with the controller SSH server. This issue is seen with Cisco IOS 12.3(8)JEB1 and controller software release 4.1.171.0.
- CSCsj56145—A controller running software release 4.1.171.0 reboots when managed by WCS release 4.1.83.
- CSCsj58351—A Windows PC sends an Address Resolution Protocol (ARP) request every 10 minutes, but the controller does not always respond to the ARP request. The client then resends the ARP request.

- CSCsj66345—Clients on a controller appear on the client exclusion list due to too many association failures. Although the exclusion timer is set to 60 seconds, the clients are not removed from the list after 60 seconds. Because they are not removed, clients cannot connect to the wireless network. These clients must be manually removed from the list.
- CSCsj67514—The virtual interface of a Cisco WiSM accepts connections on ports 22, 23, and 443. Access Control Lists (ACLs) cannot be used to block this traffic. This issue makes it possible for remote attackers to conduct brute force password cracking or denial-of-service attacks.
- CSCsj69233—A controller receives an Address Resolution Protocol (ARP) frame from a wireless client with the following attributes:
  - Layer 2: From a wireless client's MAC address
  - Layer 2: To a specific unicast MAC address (not seen in the infrastructure network)
  - Layer 3: From a unicast IP address (in a subnet not seen in the infrastructure network)
  - Layer 3: To a unicast IP address (in a subnet not seen in the infrastructure network)

  If DHCP_REQ is not set on the WLAN and there are other controllers in the mobility group, the ARP frame might be forwarded among the controllers at the wire rate.
- CSCsj72274—When CDP is disabled on the controller and you are using a third-party switch that floods CDP frames, these events are observed in message logs:

  ```
  Jul 19 12:26:19.681 osapi_msgq.c:463 OSAPI-4-MSGQ_SEND_FAILED: Failed to send a
  message to the message queue object: BCAST-Q . enqueue failed.
  -Process: Name:dtlDataLowTask, Id:11b55a98
  Jul 19 12:26:19.661 bcast_net.c:2614 BCAST-3-MSGTAG034: Multicast Rx queue is full
  ```

  As a result, high CPU utilization might occur, and the access point might disassociate.
- CSCsj73495—When the WLAN configurations do not match exactly on the foreign controller and the anchor controller, the debugs are misleading on the anchor controller and foreign controller.
- CSCsj76217—When a client performs a Layer 3 roam between two access points in different access point groups and on different controllers, the client is anchored correctly and keeps its original IP address. However, if the client is powered off or roams out of coverage and then returns to the foreign controller, the client sends out a DHCP discover message, which is correctly sent to the anchor controller. The anchor gets a DHCP offer and sends the offer to the foreign controller. The foreign controller drops the DHCP offer with this message:

  ```
  Dropping OFFER not from anchor: 10.62.112.12 client mac: 00:90:7a:07:0d:a8 offer ip:
  0.0.0.0
  ```

  The foreign controller thinks that the anchor is the dynamic interface of the access point group on the anchor instead of the management interface IP address of the anchor, but the DHCP offer goes to the foreign controller from the management interface of the anchor.
- CSCsj78813—A mobility anchor event occurs for an unauthenticated web authentication client when roaming between controllers that use the same WLAN. The VLAN that the WLAN is associated to is different on the controllers. After the client roams, a browser appears, but the client never receives a login prompt. The browser then times out.
- CSCsj83371—After upgrading to controller software release 4.1.181.0 or after resetting a controller that is running 4.1.181.0, the radio frequency signals in the coverage area appear to be unusually weak.
- CSCsj84923—The configuration refresh from the controller is successful, but some records are dropped because their key fields failed validations. This condition occurs because the controller returns extra interface entries that do not exist in the cLApDot11IfTable MIB table.

- CSCsj85329—The controller GUI should explain how the password changes with the 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.
- CSCsj86603—An excessive number of clients are being blacklisted with the "Identity theft alert" message.
- CSCsj88990—Rogue access point client information shown for the access point does not match the client information from the Rogue Client Details link.
- CSCsj90453—After the controller has been running software release 4.1.181.0 successfully for several days, new clients cannot associate to any WLAN, including the guest WLAN. Clients that continue to be associated still work correctly.
- CSCsj93895—An access point sends QOS nulls with Blocked Acknowledge enabled. The access point sends multiple packets waiting for a response, but the access point should not expect to receive an acknowledgment.
- CSCsj96576—No discovery response output is generated when you execute the **debug mac addr** and **debug lwapp events enable** CLI commands.
- CSCsj97747—When using web authentication for guest user access, if the user enters an incorrect password and does not disconnect from the access point, the login attempt counts against the number allowed for that user ID.
- CSCsj98722—When MAC addresses for MAC filtering are added in the controller GUI, the "Error in setting WLAN ID for MAC Filter" message appears if you choose a specific WLAN to which the filtering policy applies from the drop-down box.
- CSCsj98808—If you upgrade the controller to software release 4.2 and then reset the controller, a checksum error might appear and the controller loses its configuration.
- CSCsj99816—Port management and LRAD table failures are reported on the controller console when controllers are repeatedly switched in the topology.
- CSCsk02562—The controller returns loops when performing an SNMPwalk on the TCP MIB.
- CSCsk03504—If SSH is disabled on the Cisco WiSM and the WiSM reboots, SSH becomes enabled. The output of the **show run-config** command still shows SSH as disabled, but users can SSH to the controller.
- CSCsk03709—The controller SNMPwalk returns loops on ipAdEntAddr.
- CSCsk08181—The following message is written to the syslog each time a user associates if there are no accounting servers configured and RADIUS accounting is not disabled on the WLAN:

  ```
  AAA-4-RADSERVER_NOT_FOUND: Could not find appropriate RADIUS server for WLAN 3 -
  reason unable to find a default server
  ```

- CSCsk14876—If you query the bsnMobileStationMobilityStatus MIB, it always returns a value of 5 (unknown).
- CSCsk21007—When you open a page or change a configuration setting on the controller GUI, the controller tries to perform TACACS+ authentication.

- CSCsk24403—When the controller is upgraded from software release 4.0.222.0 to 4.1.185.0, access points are misidentified by the controller as rogue access points when the access points are downloading software. This message is logged in the controller syslog and in the WCS trap log:

  ```
  Fake AP or other attack may be in progress. Rogue AP count on AP with Base Radio MAC
  00:1b:0d:d5:28:10 has exceeded the security warning threshold of (30).
  ```

- CSCsk26900—Wireless AppleTalk clients do not get information from existing wired AppleTalk network resources. AppleTalk frames are dropped.
- CSCsk41360—The controller processes an EAPOL LOGOFF request after receiving an EAPOL START request.
- 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
  ```

- CSCsk43155—Wireless IDS integration is not functioning properly with the guest network setup.
- CSCsk49157—When the session timeout of a WLAN that is using a backend RADIUS authentication server is changed, any existing client that is using that WLAN shows its reauthentication timeout as infinite.
- CSCsk51538—The controller might not form a single radio frequency group under certain conditions.
- CSCsk55844—The class attribute is not sent in an accounting request.
- CSCsk65659—Auto-anchor mobility is disabled when you apply a WLAN template from WCS to the 2106 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. The condition is simply reported.
- CSCsk70727—A Cisco 7921 IP phone in world mode might not connect to a 4400 series controller with the KE country code.
- CSCsk71405—The controller sets the DF bit when sending packets to WCS, which prevents WCS from adding the controller.
- 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—If you change the channel or power setting of an access point from the controller GUI, the controller might reboot due to a software failure of the tplusTransportThread task.
- CSCsk79865—The controller rejects an 11-Mb/s Phy rate in the TSPEC if a client associates with 802.11g rates.
- CSCsk82851—Debugs sometimes stop running under loaded conditions.
- CSCsk84846—Client devices are not able to pass traffic to or receive an IP address from an access point operating in hybrid-REAP mode.
- CSCsk85091—A controller running software release 4.2.61.0 might report bogus radio up or down messages when RLDP is enabled.
- CSCsk93726—The controller might reboot due to a software failure of the CrashdtlArpTask.
- CSCsk94804—Controllers sometimes reboot due to a software failure of the EAP Framework task at the instruction located at 0x108b10fc (pfree+56).

- CSCsk97359—When a tag has an expired access point as the last entry in the RFID table, the SNMP walk does not proceed.
- CSCsk97940—If rates 1, 48, and 54 Mb/s are disabled, association responses include 24 Mb/s as both a supported rate and as an extended supported rate. 24 Mb/s should be only a supported rate.
- CSCsl09218—A binary image cannot be uploaded with the controller CLI. Transfer of the image fails.
- CSCsl09856—After being upgraded to software release 4.2.61.0, the controller generates many of these messages:

  ```
  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 caused by a break in the APF rogue processing task between the last message type and the default error condition. The impact is harmless, but the issue generates hundreds of entries every day.
- CSCsl13335—The controller might reboot when you are removing a WLAN.
- CSCsl16445—The access point PoE status is incorrect. The TrapLog "Cause=Unknown" should say "Cause=Wait for CDP Power negotiation."
- CSCsl18523—For 2106 controllers, doing an SNMPwalk for a UDP object causes a loop. This issue affects interoperability with third-party management tools.
- CSCsl19025—The controller does not respond to a device with an x.x.x.0 address.
- 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.
- 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.
- 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.
- CSCsl34308—Controllers sometimes fail to deliver inter-NPU traffic from wired to wireless clients.
- CSCsl48726—The output of the **show run-config** command does not show the TACACS+ configuration.
- CSCsl48776—If a controller has an incorrect or missing value for an SSC access point hash, the controller incorrectly forwards the request to the configured RADIUS server.
- CSCsl52628—When you enable or disable SSH or Telnet on an access point, the SSH or Telnet state does not appear in the output of the **show ap config** CLI command.
- CSCsl53115—Clients that attempt to authenticate with EAP-TLS and LDAP sometimes fail.
- CSCsl55613—The controller GUI sometimes displays unavailable options when you attempt to delete more than one rule at a time.
- CSCsl56900—The controller sometimes fails to display the entire output of the **show run-config** command.
- CSCsl80208—When you run a mobility test with a large amount of clients roaming, the Cisco WiSM might reboot due to a software failure of the mmMobility task.

If You Need More Information

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

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

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

Troubleshooting

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

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

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

Documentation Updates

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

Omissions

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

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

Related Documentation

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

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

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

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

Obtaining Documentation, Support, and Security Guidelines

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

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