Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.2.61.0

October 26, 2007

These release notes describe open and resolved caveats for software release 4.2.61.0 for Cisco 2000, 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 1000, 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 4.2.61.0 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 4.2.62.0
- Cisco WCS Navigator 1.1.62.0
- Location appliance software release 3.1.35.0
- Cisco 2700 Series Location Appliances
- Cisco 2000 Series Wireless LAN Controllers
- 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
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1000, 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 4.2.61.0 if you have mesh access points in your network. If your network uses mesh access points, use only mesh-specific releases such as 4.1.190.5.

Note Cisco WCS software release 4.2.62.0 may be used to manage both mesh and non-mesh controllers (for example, controllers running software release 4.2.61.0 and 4.1.190.5). 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 4.2.61.0, 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 4.2.61.0

Caution Before upgrading your controller to software release 4.2.61.0, 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 4.2.61.0 is greater than 32 MB; therefore, you must make sure that your TFTP server supports files that are larger than 32 MB. Some TFTP servers that support files of this size are tftpd and the TFTP server within the WCS. If you attempt to download the 4.2 controller software and your TFTP server does not support files of this size, the following error message appears: "TFTP failure while storing in flash."
  - If you are upgrading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are upgrading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP server cannot run on the same computer as the WCS because the WCS built-in TFTP server and the third-party TFTP server require the same communication port.
- If your controller is running software release 3.2.195.10 (or a later 3.2 release), 4.0.206.0 (or a later 4.0 release), or 4.1.171.0 (or a later 4.1 release), you can upgrade your controller directly to software release 4.2.61.0. If your controller is running an earlier 3.2 or 4.0 release, you must upgrade your controller to an intermediate release prior to upgrading to 4.2.61.0. Table 1 shows the upgrade path that you must follow before downloading software release 4.2.61.0.

Table 1 Upgrade Path to Controller Software Release 4.2.61.0

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

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 4.2.61.0 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 4.2.61.0 ER.aes file on the controller. This file resolves bootloader defect CSCsh61233 and is necessary to ensure proper operation of the controller. The ER.aes file is required for 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 The bootloader is not upgradable on the 2106 controller.

Note The ER.aes files are independent from the controller software files. You can run any controller software file with any ER.aes file. However, installing the latest boot software file (4.2.61.0 ER.aes) ensures that the bootloader 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.

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

Step 3 Disable any WLANs on the controller.

Step 4 Follow these steps to obtain the 4.2.61.0 controller software and the Cisco Unified Wireless Network Controller Boot Software 4.2.61.0 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 4.2.61.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.2.61.0 ER.aes file).

Step 5 Copy the controller software file (*filename*.aes) and the Cisco Unified Wireless Network Controller Boot Software 4.2.61.0 ER.aes file to the default directory on your TFTP server.

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 Repeat Step 6 to Step 12 to install the remaining file (either the 4.2.61.0 controller software or the Cisco Unified Wireless Network Controller Boot Software 4.2.61.0 ER.aes file).

Step 14 After the download is complete, click **Reboot**.

Step 15 If prompted to save your changes, click **Save and Reboot**.

Step 16 Click **OK** to confirm your decision to reboot the controller.

Step 17 After the controller reboots, re-enable the WLANs.

Step 18 Re-enable your 802.11a and 802.11b/g networks.

Step 19 If desired, reload your latest configuration file to the controller.

Step 20 To verify that the 4.2.61.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

Step 21 To verify that the Cisco Unified Wireless Network Controller Boot Software 4.2.61.0 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.

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

Software Release Support for Access Points

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

Table 2 Software Support for Access Points

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

Table 2 Software Support for Access Points (Continued)

Access Points		First Support	Last Support
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 4.2.61.0.

Note Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 4.2* for details and configuration instructions for each of these features.

Controller Platform Changes

- The Catalyst 6500 series switch chassis can now support up to six Cisco WiSMs (rather than five) without any other service module installed. If one or more service modules are installed, the chassis can support up to a maximum of four service modules (WiSMs included).
- The Cisco 7600 series router can support up to six Cisco WiSMs without any other service module installed. The integrated Cisco 7600 router and two Cisco 4404 controllers support up to 300 lightweight access points.

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

New Controller Features

- **7920 and 7921 co-existence**—Because 7921 phones support WMM and 7920 phones do not, capacity and voice quality problems can arise if you do not properly configure both phones when they are used in a mixed environment. To enable both 7921 and 7920 phones to co-exist on the same network, make sure that load-based CAC and 7920 AP CAC are both enabled on the controller and the WMM Policy is set to Allowed.
- **802.11n support**—You can now configure the controller to manage 802.11n devices such as the Cisco Aironet 1250 Series Access Points. The 802.11n devices support the 2.4- and 5-GHz bands and offer high-throughput data rates. You can use the controller GUI or CLI to enable or disable 802.11n mode and to set the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. By default, 802.11n mode and all of the MCS data rates are enabled. You can also use the CLI to convert the channel bandwidth for 802.11n access points from 20 MHz to 40 MHz and to specify the aggregation method used for 802.11n packets.

Note The 802.11n high-throughput rates are available only on 1250 series access points for WLANs with no Layer 2 encryption or with WPA2/AES encryption enabled.

- **Access control list (ACL) counters**—ACL counters can assist in determining which ACLs were applied to packets transmitted through the controller. This feature is useful when troubleshooting your system.

Note ACL counters are available only on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

- **Access point join process**—To better troubleshoot issues with access points that fail to join a controller, you can now configure the access points to send all LWAPP-related errors to a syslog server. You can then view join-related information for all access points that have attempted to join the controller.
- **Backup controller support for access points to fail over to controllers outside the mobility group**—A single controller at a centralized location can act as a backup for access points when they lose the primary controller in the local region. Centralized and regional controllers need not be in the same mobility group. Using the controller CLI, you can specify a primary, secondary, and tertiary controller for your network's access points. In controller software release 4.2.61.0, you can

specify the IP address of the backup controller, which allows the access points to fail over to controllers outside of the mobility group. This feature is currently supported only through the controller CLI.

- **CCKM support for hybrid REAP**—Hybrid-REAP mode supports Layer 2 fast secure roaming using Cisco Centralized Key Management (CCKM). This feature prevents the need for full RADIUS EAP authentication as the client roams from one access point to another. To use CCKM fast roaming with hybrid-REAP access points, you need to configure hybrid-REAP groups.
- **Debug facility**—The debug facility enables you to display all packets going to and from the controller CPU. You can enable it for received packets, transmitted packets, or both. By default, all packets received by the debug facility are displayed. However, you can define access control lists (ACLs) to filter packets before they are displayed. Packets not passing the ACLs are discarded without being displayed.
- **DHCP proxy**—When DHCP proxy is disabled, the controller passes DHCP packets without any modification from the client to the upstream VLAN and vice versa. As a result, the internal DHCP server cannot be used when DHCP proxy is disabled. The ability to disable DHCP proxy allows organizations to use DHCP servers that do not support Cisco's native proxy mode of operation. It should be disabled only when required by the existing infrastructure.
- **EDCA support**—You can configure enhanced distributed channel access (EDCA) profiles per radio band to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic. The available options are WMM (the default value), Spectralink Voice Priority, Voice Optimized, and Voice & Video Optimized.

Note In controller software release 4.1, the EDCA profiles are not configurable per radio and do not offer four configuration options. Therefore, you might need to reconfigure the EDCA profiles after upgrading to 4.2.61.0.

- **Hybrid-REAP groups**—To better organize and manage your hybrid-REAP access points, you can create hybrid-REAP groups and assign specific access points to them. All of the hybrid-REAP access points in a group share the same CCKM, WLAN, and backup RADIUS server configuration information. This feature is helpful if you have multiple hybrid-REAP access points in a remote office or on the floor of a building and you want to configure them all at once. For example, you can configure a backup RADIUS server for a hybrid-REAP group rather than having to configure the same server on each access point. Per controller, you can configure up to 20 hybrid-REAP groups with up to 25 access points per group.
- **Hybrid-REAP 802.1X support**—Hybrid-REAP mode supports 802.1X authentication to a backup AAA server when the WAN link is down. To support 802.1X EAP authentication, hybrid-REAP access points in standalone mode need to have their own RADIUS servers to authenticate clients. You can configure a backup RADIUS server for individual hybrid-REAP access points by using the controller CLI or for hybrid-REAP groups by using either the GUI or CLI. A backup server configured for an individual access point overrides the RADIUS server configuration for a hybrid-REAP group.
- **IPv4 and IPv6 support on the same WLAN**—You can enable IPv6 bridging and IPv4 web authentication on the same WLAN. The controller bridges IPv6 traffic from all clients on the WLAN while IPv4 traffic goes through the normal web authentication process. The controller begins bridging IPv6 as soon as the client associates and even before web authentication for IPv4 clients is complete.

Note No other Layer 2 or Layer 3 security policy configuration is supported on the WLAN when IPv6 bridging and web authentication are enabled.

- **Local EAP support for PEAP**—Local EAP now supports PEAPv0/MSCHAPv2 and PEAPv1/GTC authentication (in addition to LEAP, EAP-FAST, EAP-TLS authentication) between the controller and wireless clients.
- **MAC enhancement**—A new parameter called **Enable Low Latency MAC** has been added to the 802.11a or 802.11b/g > EDCA Parameters page. This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, thereby improving the number of voice calls serviced per access point. You should enable low latency MAC only if the WLAN allows WMM clients.
- **Multicast enhancement**—In controller software release 4.2, Internet Group Management Protocol (IGMP) snooping is introduced to better direct multicast packets. When this feature is enabled, an access point transmits multicast packets only if a client associated to the access point is subscribed to the multicast group.

  Note IGMP snooping is not supported on the 2000 series controllers, the 2100 series controllers, and the Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers.

- **NAT mobility**—In controller software releases prior to 4.2.61.0, mobility between controllers in the same mobility group does not work if one of the controllers is behind a network address translation (NAT) device. This behavior creates a problem for the guest anchor feature where one controller is expected to be outside the firewall.

  Mobility message payloads carry IP address information about the source controller. This IP address is validated with the source IP address of the IP header. This behavior poses a problem when a NAT device is introduced in the network because it changes the source IP address in the IP header. Hence, in the guest WLAN feature, any mobility packet being routed through a NAT device is dropped because of the IP address mismatch.

  In controller software release 4.2.61.0, the mobility group lookup is changed to use the MAC address of the source controller. Because the source IP address is changed due to the mapping in the NAT device, the mobility group database is searched before a reply is sent to get the IP address of the requesting controller. This is done using the MAC address of the requesting controller.

  When configuring the mobility group in a network where NAT is enabled, enter the IP address sent to the controller from the NAT device rather than the controller's management interface IP address. Also, make sure that the following ports are open on the firewall if you are using a firewall such as pix:

  - UDP 16666 for tunnel control traffic
  - UDP 16667 for encrypted traffic
  - IP protocol 97 for user data traffic
  - UDP 161 and 162 for SNMP

  Note Client mobility among controllers works only if auto-anchor mobility (also called *guest tunneling*) or symmetric mobility tunneling is enabled. Asymmetric tunneling is not supported when mobility controllers are behind the NAT device.

- **Peer-to-peer blocking**—In controller software release 4.2, peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. You can configure client traffic on the same WLAN to be bridged locally within the controller, dropped by the controller, or forwarded to the upstream VLAN. This feature is not applicable to the wired guest access feature.

  Note The GUI option and CLI command to enable or disable peer-to-peer blocking globally have been removed from the software in favor of this new, more flexible feature.

- **QoS roles**—In order to prevent guest users from using the same level of bandwidth as regular users, you can create QoS roles with different (and presumably lower) bandwidth contracts and assign them to guest users.
- **Splash pages**—In controller software releases prior to 4.2, a default login page appears when a client associates to a WLAN using web authentication.This page, which is the same for every WLAN, allows users to enter their credentials. In controller software release 4.2, you can use the splash page feature to display different login pages for different WLANs. For example, different departments within an organization might want to display login pages with their own logo, message, and so on. When you enable web authentication for a wired or wireless guest access WLAN, you can choose to override the global authentication configuration set on the Web Login page (using the Override Global Config parameter) and choose one of the following web login pages for wired or wireless guest users: the default web login page for the controller, a custom web login page that is downloaded to the controller, or a web login page from an external server.
- **Syslog server**—You can configure the syslog facility for sending syslog messages to a remote host and set the severity level for filtering the syslog messages.
- **Wired guest access**—This feature enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or through specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature. Wired guest access can be configured in a standalone configuration or in a dual-controller configuration that uses both an anchor controller and a foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

  Note Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

  Note Wired guest access is supported only on the following controllers: 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Integrated Wireless LAN Controller Switch.

New CCXv5 Features

- **Diagnostic channel**—This feature enables you to troubleshoot problems regarding client communication with a WLAN. The client and access points can be put through a defined set of tests in an attempt to identify the cause of communication difficulties the client is experiencing and then allow corrective measures to be taken to make the client operational on the network.

- **Client reporting**—This protocol is used by CCXv5 clients and the access point to exchange client information. Client reports are collected automatically when the client associates. There are four types of client reports:
  - Client profile—Provides information about the configuration of the client.
  - Operating parameters—Provides the details of the client's current operational modes.
  - Manufacturers' information—Provides data about the wireless LAN client adapter in use.
  - Client capabilities—Provides information about the client's capabilities.
- **Roaming and real-time diagnostics**—You can use roaming and real-time logs and statistics to solve system problems. The event log enables you to identify and track the behavior of a client device. It provides a log of events and reports them to the access point. There are three categories of event logs:
  - Roaming log—Provides a historical view of the roaming events for a given client.
  - Robust Security Network Association (RSNA) log—Provides a historical view of the authentication events for a given client.
  - Syslog—Provides internal system information from the client. For example, it may indicate problems with 802.11 operation, system operation, and so on.

GUI Enhancements

- Monitor and Controller Menus—The options on these menus have been rearranged.
- All APs page— This page now shows the access point mode, and the layout has been changed to a tabbed format.
- AP Policies page—You can now search for an access point in the authorization list by MAC address.
- Clients page—You can filter clients so that only clients that meet certain criteria (such as MAC address, access point name, WLAN profile, status, radio type, and/or WGB status) are displayed on the Clients page.
- Summary page—You can view the default mobility group under Controller Summary.

Access Point Additions and Changes

- **Cisco Aironet 1250 Series Access Point**—All controllers now support the Cisco Aironet 1250 Series Access Point. This access point supports two (draft IEEE 802.11n version 2.0) radio modules: a 2.4-GHz radio and a 5-GHz radio. You can configure the radios separately, using different settings on each. For more information, refer to the Cisco Aironet 1250 Series Access Point Q&A at this URL: http://www.cisco.com/en/US/products/ps8382/index.html
- **Support for 16 BSSIDs**—All Cisco lightweight access points support 16 BSSIDs per radio and a total of 16 wireless LANs per access point. In previous releases, they supported only 8 BSSIDs per radio and a total of 8 wireless LANs per access point.

Other Changes

These additional changes are applicable to controller software release 4.2.61.0:

- The PMK cache lifetime timer, which is used to trigger reauthentication with the client when necessary, has been changed. It is now based on the timeout value received from the AAA server or the WLAN session timeout setting rather than on the default PMK cache lifetime default value of 12 hours.

- The LDAP backend database now supports these local EAP methods: EAP-TLS, EAP-FAST/GTC, and PEAPv1/GTC. LEAP, EAP-FAST/MSCHAPv2, and PEAPv0/MSCHAPv2 are also supported but only if the LDAP server is set up to return a clear-text password. For example, Microsoft Active Directory is not supported because it does not return a clear-text password.
- You can configure the controller to allow users to access the controller GUI using browsers that support 128-bit (or larger) ciphers. This change provides increased security for secure web mode.
- CLI commands containing **locp** have been changed to **nmsp** for Network Mobility Services Protocol (NMSP).
- A new encryption option is available from the Privacy Protocol drop-down box on the SNMP V3 Users > New page called **CFB-AES-128** (Cipher Feedback Mode-Advanced Encryption Standard-128). This option is the default value.
- A trap is generated if a WPA or WPA2 client requests a security policy that is inconsistent with the approved security configuration.
- Over-the-air provisioning (OTAP) is now disabled by default on the controller.
- Load-based call admission control (CAC) is now supported on Cisco 1000 series access points.
- The controller's bootup configuration file is now stored in an Extensible Markup Language (XML) format rather than in binary format. Therefore, you cannot download a binary configuration file onto a controller running software release 4.2.61.0. However, when you upgrade a controller from a previous software release to 4.2.61.0, the configuration file is migrated and converted to XML.

Note 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.

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, 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 from a previous software release to 4.2.61.0, 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.

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.

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:

- 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:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps6087_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 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.

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.

Multicast Limitations

Multicast applications have known performance limitations on the 2000 series controllers, 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 2000 or 2100 series controller.

MAC Filtering for WGB Wired Clients

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

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

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

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

CKIP Not Supported with Dynamic WEP

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

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 4.2* for instructions for setting the time and date on the controller.

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

Note Daylight Savings Time (DST) is not supported in controller software release 4.2.

UNII-2 Channels Disabled on New 1000 Series Access Points for United States, Canada, and Philippines

New Cisco 1000 series lightweight access points for the United States, Canada, and the Philippines do not support the UNII-2 band (5.25 to 5.35 GHz). These models are labeled AP10x0-B, where "B" represents a new regulatory domain that replaces the previous "A" domain.

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.
```

1000 Series Access Points and Radar Detection

The 1000 series access points perform radar detection on channels that do not require it (such as channel 36). If the access points detect radar on these channels, the controller captures it in log messages.

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**}

Multicast Queue Depth

The multicast queue depth is 512 packets on all controller platforms. However, the following message might appear on 2006 and 2106 controllers: "Rx Multicast Queue is full on Controller." This message does not appear on 4400 series controllers because the 4400 NPU filters ARP packets, and all forwarding (multicast or otherwise) and multicast replication are done in the software on the 2006 and 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.

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.

Resetting the Configuration on 2006 Controllers

If you wish to reset the configuration to factory defaults on a 2006 controller, perform one of the following:

- From the controller GUI, click **Commands** > **Reset to Factory Default** > **Reset**.
- From the controller CLI (after system bootup and login), enter **clear config**. Then after the configuration has been cleared, enter **reset system** without saving the current configuration.
- From the controller console (after system bootup), enter **Recover-Config** from the User Name prompt.

Caution Do not attempt to reset the controller's configuration by choosing Option 5, Clear Config, from the boot menu.

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 4.2.61.0 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.

Cisco 1000 Series Access Points and WMM

Cisco 1000 series access points in REAP mode do not support the Wi-Fi Multi-Media (WMM) protocol.

Cisco Aironet 1030 Remote Edge Lightweight Access Points and WPA2-PSK

Cisco Aironet 1030 Remote Edge Lightweight Access Points do not support WPA2-PSK in REAP standalone mode.

Lightweight Access Point Connection Limitations

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.

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 4.2* for configuration instructions.

Changing the Default Values for SNMP v3 Users

The controller uses a default value of "default" for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values. Refer to the *Cisco Wireless LAN Controller Configuration Guide, Release 4.2* for configuration instructions.

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

Features Not Supported on 2000 and 2100 Series Controllers

These hardware features are not supported on 2000 and 2100 series controllers:

- Power over Ethernet (PoE) for 2000 series controllers only

  Note Ports 7 and 8 on 2100 series controllers are PoE ports.

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

These software features are not supported on 2000 and 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

Note Port mirroring is also not supported on 4400 series controllers.

- 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.

2006 Image Not Supported for 3504 Controllers

The 2006 controller image is supported for use with only 2000 series controllers. Do not install the 2006 image on a 3504 controller. Otherwise, errors may occur. Install only the 3504 image on a 3504 controller.

Running a 3504 Image on a 2000 Series Controller

It is possible to run a 3504 controller image on a 2000 series controller, but Cisco Aironet 1130, 1200, and 1240 series access points will not be able to connect to the controller.

Upgrading External Web Authentication

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

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

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

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

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

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

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

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

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

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

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

}

</script>
```

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

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

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

<tr align="center">

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

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

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

Caveats

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

Open Caveats

These caveats are open in controller software release 4.2.61.0.

- 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.

- CSCsb85113—When users download the software image to the controller using the CLI, access points are sometimes disconnected.

  Workaround: Download new code images to the WiSM at times when there are no clients to be affected.

- CSCsc03214—If a WLAN is configured to use web policy for Layer 3 security authentication and is also configured to use the controller's default authentication page, the client cannot access the authentication page using HTTPS.

  Workaround: Use HTTP (not HTTPS) to access the authentication page.

- CSCsd10643—The EAP timeout is too aggressive when using EAP-FAST.

  Workaround: Use the **config advanced eap request-timeout** *timeout* command to change the EAP timeout to 20 seconds or greater.

- CSCsd51193—The controller GUI displays only the first 80 blacklisted client devices.

  Workaround: Use the controller CLI to view the complete list of blacklisted clients.

- CSCsd52483—When you make changes in the bootloader of a 2006 controller or a Controller Network Module, the bootup process may halt, and the controller may stop responding. The controller also displays the "grub>" prompt on the console port.

  Workaround: Replace the controller.

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

  Workaround: None.

- CSCsd64081—Ethernet multicast mode is not passing multicast traffic on the 2006 controller.

  Workaround: None.

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

  Workaround: Use the controller CLI.

- CSCsd86375—HiFn sessions are being added and deleted with the session handles set to 0.

  Workaround: None.

- 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.

- CSCse01881—The following message might randomly appear in the controller's message logs: "[WARNING] dtl_arp.c 1656: Unable to delete ARP mapping."

  Workaround: None.

- CSCse11464—The Management Frame Protection Settings page on the controller GUI displays a maximum of 100 access points.

  Workaround: If there are more than 100 access points under MFP, use the controller CLI to view the list of access points.

- 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.

- CSCsf26609—The "cLCdpAllApStatus" MIB variable with *TruthValue* always returns a value of *false*. This problem affects WCS operations.

  Workaround: None.

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

  Workaround: None.

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

  Workaround: Use a wireless sniffer trace.

- CSCsg05789—The controller should send all crash information to WCS, and WCS should forward that information to Cisco.com.

  Workaround: None.

- CSCsg32646—If link aggregation (LAG) is enabled on the controller and the port channel is configured on the infrastructure switch, the controller displays only a single entry for its neighbor when you enter the **sh cdp neighbor** CLI command. When you enter the same command on the switch, it displays two entries for the controller for two different ports that are part of LAG. The controller should display two entries when the command is entered on the controller because the switch sends the CDP message from two different ports that are part of the port channel.

  Workaround: None.

- CSCsg39934—IOS LWAPP access points should support direct Telnet to the CLI.

  Workaround: None.

- CSCsg35690—The SNMP client troubleshooting buffer wraparound does not work in cases where the number of messages exceed 2,000.

  Workaround: Delete the client from the watchlist and then re-add it to the watchlist for the messages.

- 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.

- CSCsg54661—When you issue the **show run** CLI command on the controller, you do not get any information on the configured mobility anchors.

  Workaround: Issue the **show mobility anchor** command separately.

- 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.

- CSCsg68046—The complete reason for a TFTP download failure needs to appear on the controller GUI. If the controller cannot find the software file on the TFTP server during a software upgrade, it reports that the transfer failed rather than that the file is not present.

  Workaround: Make sure that the file and filename are entirely correct before upgrading, or upgrade using the CLI to receive a more accurate reason for the failure. Even further details are available if you use the **debug transfer all enable** command prior to upgrade.

- CSCsg74578—If you change a controller's management IP address, it is not sent to the access point unless the access point is reset. As a result, multicasting does not work until the change is made on the access point.

  Workaround: None.

- CSCsg84209—The export foreign controller is not deleting the client device when it receives a HandoffEnd message.

  Workaround: None.

- CSCsg87111—While editing a WLAN configured for WPA1+WPA2 with a conditional redirect to 802.1x, the MIB browser shows a commit failure error.

  Workaround: None.

- 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 log 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 may not be available for CCX clients on the controller.

  Workaround: None.
- CSCsh31104—The word *channel* is misspelled in the message log.

  Workaround: None.
- CSCsh35185—The packet loss for the 2106 controller varies between 4 and 12 percent for small packets (64 or 128 bytes) with a load between 5 and 50 Mbps.

  Workaround: None.
- CSCsh36770—The controller supports the sending of DHCP option 82 remote-id with the access point MAC and SSID. In larger deployments, users need to be able to enter on the controller a configurable text string to identify the access point.

  Workaround: None.
- CSCsh41819—When a WGB is associated to the WLAN, wired clients connected to the WGB are not receiving IP addresses from the controller using the internal DHCP server.

  Workaround: None.
- CSCsh50404—SSH needs to be implemented internally as a protocol to the switchdriver.

  Workaround: None.

- CSCsh71088—When you change the Layer 2 security setting for a WLAN from None to CKIP and apply the changes to the controller, the WLAN is disabled. This happens only the first time you change the Layer 2 security setting from None to CKIP. There are no problems in subsequent edits.

  Workaround: Change the Layer 2 security setting for the WLAN back to None and then to CKIP again.

- CSCsh83374—Web authentication stops working when the **debug client** *mac_address* CLI command is used.

  Workaround: Enter these commands to allow web authentication to work while using debug commands to troubleshoot: **debug dhcp packet disable** and **debug dot11 mobile disable**.

- CSCsh83698—The 2006 controller continuously displays the following error message when the lightweight access point is in direct mode (that is, the access point's Ethernet cable goes directly into the 2006 port): "bcastCPUMcastTx: Cannot send BCAST pkt to all DS ports."

  Workaround: None.

- CSCsh85227—You cannot use the GUI to clear the statistics on 2106 controllers.

  Workaround: Use the controller CLI to clear the statistics.

- CSCsh90338—The output of the **show run-config** and **show running-config** CLI commands is different, which might cause confusion.

  Workaround: None.

- CSCsh90499—Errors occur when performing failover testing on the Cisco WiSM.

  Workaround: None.

- CSCsh96186—Large IP packets that have been split into multiple fragments might fail to be reassembled by a 4400 series controller.

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

- CSCsh98559—CPU ACLs do not work for EoIP packets and DHCP received on the distribution system port.

  Workaround: None.

- CSCsi00003—If a user enters the wrong username or password more than three times on the Web Login page, the client is blacklisted, but the Client Excluded page, which tells the user to contact the administrator, does not appear, and the client disassociates from the network.

  Workaround: None.

- CSCsi05119—The 2106 controller reboots when you use the GUI to change the serial timeout value.

  Workaround: Use the controller CLI to set the serial timeout value.

- CSCsi05144—The CCX S60 path loss report displays the wrong access point MAC address.

  Workaround: None.

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

  Workaround: None.

- CSCsi09628—Controllers do not have an FTP, RCP, or SCP option for upgrading. If you have problems upgrading using TFTP over a WAN link, you must upgrade locally to the controller.

  Workaround: None.

- 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.

  Workaround: None. This is a cosmetic issue.

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

  Workaround: None.

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

  Workaround: None.

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

  Workaround: None.

- CSCsi23021—Having a Cisco WiSM installed in slot 13 of a Catalyst 6513 causes duplicate IP address errors and loss of access to the module that is reported as the duplicate.

  Workaround: Move the Cisco WiSM from slot 13 to another slot between 9 and 12.

- CSCsi25680—The broadcast enable and disable commands are not working properly on the 2106 controller.

  Workaround: None.

- CSCsi25756—The Clients > Detail page on the controller GUI does not refresh when you click **Refresh** on the top right corner of the page.

  Workaround: None.

- CSCsi26248—You might lose connectivity when adding or recovering a second 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.

- CSCsi32529—A 1200 series access point reboots randomly when running software release 4.0.179.11.

  Workaround: None.

- CSCsi34642—The external web server list in the output of the **show custom-web all** CLI command is misformatted and difficult to read.

  Workaround: None.

- CSCsi34673—The nearby access point statistics in the output of the **show client detail** *mac_address* CLI command is misformatted and difficult to read.

  Workaround: None.

- CSCsi35792—Controllers fail to establish a connection with open LDAP on a port other than 389.

  Workaround: Always use port number 389 with an LDAP server.

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

  Workaround: None.

- CSCsi53789—Autonomous access points that have been converted to lightweight mode sometimes do not forward controller-generated IGMP queries over the air. This issue occurs when no active clients are associated to the access point and the client roams to an access point on another controller.

  Workaround: Have at least one active client associated to the WLAN on that access point.

- CSCsi56797—When you attempt to change the default mobility group for the local controller in the Edit All field, the change is not applied.

  Workaround: None.

- CSCsi57300—The controller might reboot at emWeb when you execute the **show running-config** CLI command on a controller running software release 4.1.158.25, 4.1.158.32, or 4.1.158.33.

  Workaround: None.

- CSCsi60843—The ARP unicast setting on the controller, which disables proxy ARP, does not work for Layer 3 roaming.

  Workaround: None.

- CSCsi64422—The controller does not resend the ACK packet when TFTP times out.

  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 when the WLAN QoS profile is set to Bronze.

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

- CSCsi72767—A script runs each time you generate a dependency file, which makes the build very slow.

  Workaround: None.

- CSCsi74785—The syslog displays a traceback after you delete mobility members.

  Workaround: None.

- CSCsi76581—The WiSM controller reboots after running a ping test from the WCS map.

  Workaround: None.

- CSCsi78531—Port statistics values on the controller GUI do not match those on the controller CLI.

  Workaround: None.

- CSCsi86794—When auto channel selection is enabled on a controller running 4.1.171.0 or later and access points are set to channels 100, 104, 108, 112, 116, 132, 136, or 140, clients cannot associate.

  Workaround: Follow these steps to disable channels 100 to 140. Make sure to disable the radio network and then enable it after the channel change.

  a. On the controller GUI, click **Wireless > 802.11a/n**.
  b. Click **DCA** under RRM.
  c. Uncheck all of the channels between 100 to 140.
  d. Click **Apply** to commit your changes.

- CSCsi90344—When you use local EAP authentication to authenticate clients, the following message appears in the message log: "OSAPI-4-TIMERTCB_REALLOCATED: Timer 3607/1800205 (EAP Local Auth) found to be destroyed/reallocated."

  Workaround: None. This issue does not affect the clients' ability to authenticate. The message just unnecessarily fills the log.

- CSCsi94119—The WLAN template WPA1+WPA2 with the web policy conditional redirect fails when applied to the controller through WCS.

  Workaround: None.

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

  Workaround: None.

- CSCsj05699—An error might occur when setting web redirection on a WLAN with WPA1or WPA2 and PSK security.

  Workaround: None.

- CSCsj06015—When using rogue access point containment, intrusion detection system (IDS) broadcast deauthentication signature attack messages may be reported by a controller in the same mobility group as the controller that has initiated the containment.

  Workaround: None. The message is cosmetic only.

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

  Workaround: None.

- CSCsj07822—A more descriptive error message is needed when enabling web authentication on a WLAN with Layer 2 security and IPv6 enabled.

  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 this action can interfere with auto RF.

- CSCsj12086—Multicast IPTV traffic is very slow on the 2106 controller and the Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers.

  Workaround: None.

- CSCsj14255—The multicast feature needs to support IGMP queries on five VLANs simultaneously.

  Workaround: None.

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

  Workaround: None.

- CSCsj15970—The output of the **debug bcast igmp enable** CLI command does not display the MAC address of the client that sends the IGMPv3 reports.

  Workaround: None.

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

  Workaround: None.

- CSCsj17665—QoS role configuration changes cause traffic to stop for 1 minute.

  Workaround: None.

- CSCsj18097—A CLI command is not available to check MGID counters.

  Workaround: None.

- CSCsj18325—Some packets that are forwarded over a wireless link are getting corrupted.

  Workaround: None.

- CSCsj22034—Duplicate packets are received when multicast and AAA override are configured.

  Workaround: None.

- CSCsj25653—The **show acl detailed** command might fail on the 2006 controller.

  Workaround: None.

- CSCsj25953—When 200 or more wireless clients try to associate to a controller at the same time, the clients become stuck in the DHCP_REQD state. The controller receives the DHCP offer from an external DHCP server but does not send the offer to the access point in LWAPP.

  Workaround: None.

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

  Workaround: None.

- CSCsj32097—The Clients > Detail page is not available in tab format.

  Workaround: None.

- CSCsj32112—A client search by access point name should return a proper message when the access point does not associate to the controller.

  Workaround: None.

- CSCsj33229—You might be unable to ping access points that are directly connected to the switch ports on a 2106 controller. The IP address of each access point does not appear in the ARP cache of the controller, but clients connected to the access points can browse the network.

  Workaround: Connect the access points to a different device such as a switch.

- CSCsj35540—There is no method to convert the Cisco 3201 Wireless Mobile Interface Cards (WMICs) from LWAPP to Cisco IOS.

  Workaround: None.

- CSCsi35682—The CPU ACL should skip the direction parameter. This parameter is fixed because the CPU ACL applies only to packets from the NPU to the CPU.

  Workaround: None.

- CSCsj35724—When the controller is running software release 4.1.171.0 or later, the syslog servers might stop adding an IP address to the front of syslog messages.

  Workaround: Change the syslog server to one that accepts the Cisco standard syslog format.

- CSCsj36772—Cisco CB21AG client adapters using WPA2 with AES fail to fast roam among hybrid-REAP access points.

  Workaround: None.

- CSCsj39337—Fragmentation issues with unicast traffic might occur on the WiSM controller.

  Workaround: None.

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

  Workaround: None.

- CSCsj43744—The controller ignores the default gateway MAC address learned 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.

  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.

- CSCsj47959—The access point neighbor list shows the wrong controller IP address.

  Workaround: None.

- 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.

- CSCsj54296—The Cisco 1000 series access points send ACK packets from non-associated clients.

  Workaround: None.

- CSCsj55397—1240 series access points might reboot due to a dot11_set_rate_lower failure.

  Workaround: None.

- CSCsj55664—You cannot use network access restrictions (NARs) to permit access to a web authentication WLAN.

  Workaround: Use only the deny portion of the NAR configuration.

- CSCsj57309—Nonsense characters appear on the controller CLI when you use the GUI to change the serial timeout value to zero. This problem occurs in software releases 4.1.176.2 and later.

  Workaround: Use the controller CLI to set the serial timeout value to zero.

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

  Workaround: None.

- CSCsj59441—Channel information for a rogue access point does not appear on the rogue access point report.

  Workaround: Enable the rogue access point trap for the registered controllers or view the channel information on the controller.

- CSCsj61649—The CCXv5 controller log analysis types are misaligned with results. The results for DHCP and AAA appear to be swapped.

  Workaround: None.

- CSCsj62010—The Cisco1000 series access points send beacons only at 802.11b data rates.

  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 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.

- CSCsj70062—Multicast throughput is low for the 2006 series controllers and the Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers.

  Workaround: None.

- CSCsj77847—The bidirectional voice stream throughput is low.

  Workaround: None.

- CSCsj79331—The controller fails to accept the original login and password after running for five days.

  Workaround: None.

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

  Workaround: None.

- CSCsj82877—The client filter on the controller should include wired guest clients.

  Workaround: None.

- CSCsj83509—The output for the **show mobility anchor** CLI command varies on different controllers.

  Workaround: None.

- CSCsj85329—The controller GUI should explain how the password changes with RADIUS compatibility mode. The RADIUS server names help users match to their type of RADIUS server, but the server types should be explained:

  - Cisco ACS—In the RADIUS access-request packet, the username is the client MAC address, and the password is the client MAC address.
  - Free RADIUS—In the RADIUS access-request packet, the username is the client MAC address, and the password is the controller’s shared secret with the RADIUS server.
  - Other—In the RADIUS access-request packet, the username is the client MAC address, and the password is not sent in the RADIUS access-request packet.

  Workaround: None.

- CSCsj86899—CPU usage can go up to 98% under a nessus attack, resulting in denial of service.

  Workaround: Configure CPU ACLs.

- CSCsj87201—When you try to change the DHCP server to a blank value, an error message appears on the controller GUI indicating that a gateway is mandatory even when a gateway is present.

  Workaround: None.

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

  Workaround: Enter a valid netmask.

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

  Workaround: None.

- CSCsj88990—Rogue access point client information shown for the access point does not match the client information from the Rogue Client Details link.

  Workaround: View the current rogue client information from the controller.

- CSCsj91851—When you issue the **show network multicast mgid detail** *mgid_value* CLI command for a non-existing Layer 3 multicast group ID (MGID), an incorrect message appears.

  Workaround: None.

- CSCsj92716—A WGB device periodically loses connectivity with the controller.

  Workaround: None.

- CSCsj94843—Lightweight access points might reboot with a console message indicating that the Interface Dot11Radio0 failed.

  Workaround: Reboot the access point.

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

  Workaround: None.

- CSCsj95227—The IGMP timeout should not be adjustable when IGMP snooping is disabled.

  Workaround: None.

- CSCsj96589—Using the MAC address from the label on an 1131 or 1242 access point in the **debug mac addr** command produces limited debug output.

  Workaround: None.

- CSCsj97631—The IGMP code uses the wrong timer library.

  Workaround: None.

- 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.

  Workaround: None.

- CSCsj97900—The call admission control (CAC) TSPEC is not traffic shaping and allows a new call setup when the physical data rate is higher than one single data rate configured on the controller.

  Workaround: Follow the instructions in the VoWLAN deployment guide to enable a realistic higher data rate for the Cisco 7921 phone and turn on the supported rate as recommended.

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

  Workaround: None.

- CSCsk01753—The Cisco WiSM might reboot due to a failure in the sshpmReceiveTask.

  Workaround: None.

- CSCsk02093—Wired guest traffic cannot be stopped.

  Workaround: None.

- CSCsk03591—A 45-second delay is observed when a client on a call is removed.

  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.

- CSCsk08401—The formatting for the **config paging** *?* CLI command needs to be corrected.

  Workaround: None.

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

  Workaround: None.

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

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

- CSCsk13707—Multicast does not work properly on an access point group VLAN with IGMP snooping disabled.

  Workaround: None.

- CSCsk14045—The voice TSPEC with TSRS is always rejected by the controller for the Cisco 1010 access point.

  Workaround: None.

- CSCsk14331—QoS profiles and QoS roles cannot be configured for clients that have been authenticated using TACACS+.

  Workaround: None.

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

  Workaround: None.

- CSCsk16196—A 1250 series access point does not send beacon packets on the 802.11a network.

  Workaround: None.

- CSCsk16314—Access points start downloading new software before the controller has been rebooted.

  Workaround: None.

- CSCsk16755—The Cisco 7921 phone cannot change to the 802.11a radio from the 802.11b/g radio when configured for shared WEP on the controller.

  Workaround: Uncheck the **Allow Shared Key Authentication** check box on the Layer 2 Security page and let the Cisco 7921 phone connect with the 802.11a radio. Then recheck the check box and click **Apply**.

- 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.

- CSCsk17110—A lightweight access point in hybrid-REAP mode fails when trying to reassociate to the primary controller from a secondary controller.

  Workaround: None.

- 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 performs the ARP lookup and plumbs the entry to the NPU. However, the ARP entry is not being plumbed correctly to the NPU, and as a result, each packet sent by the client results in a request to the NPU.

  Workaround: None.

- CSCsk19339—CCXv5 event logs (syslog, RSNA, and roam logs) are not displayed in the WCS Client Troubleshooting window.

  Workaround: Use the following commands from the controller CLI for the logs:

  - To send a log request, enter this command:

    config client ccx log-request *log_type client_mac_address*

    where *log_type* is roam, rsna, or syslog.

  - To view the log response, enter this command:

    show client ccx log-response *log_type client_mac_address*

- CSCsk19620—The access point console does not indicate that DHCP option 43 did not parse correctly.

  Workaround: Manually verify the DHCP option 43 syntax of “104xxxxxxx,” where “xxxxxxx” is the IP address in hexadecimal digits.

- CSCsk19896—The access point configuration page should differentiate between read-only and read-write data fields.

  Workaround: None.

- CSCsk20403—A web authentication client does not deauthenticate after the user closes all browser windows.

  Workaround: None.

- CSCsk21007—The controller requires TACACS+ authentication when a configuration setting is changed on the controller GUI or a GUI page is opened.

  Workaround: None.

- CSCsk21287—Wired guest access does not work when an ingress interface IP address is not configured.

  Workaround: None.

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

  Workaround: None.

- CSCsk24550—The controller drops the first UDP packet arriving very quickly after the association.

  Workaround: None.

- CSCsk24974—You cannot use the controller GUI to configure a hexadecimal password for a TACACS+ server. Only ASCII passwords are supported.

  Workaround: None.

- CSCsk25072—A client is able to associate when the username is disabled on the LDAP server.

  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.

- CSCsk25212—After the RADIUS server is disabled, PEAP-GTC clients cannot authenticate using the local LDAP database.

  Workaround: None.

- CSCsk26900—Wireless AppleTalk clients do not get information from wired AppleTalk network resources.

  Workaround: Use controller software release 4.0.

- CSCsk27673—A wired client de-authentication is not added to the controller log.

  Workaround: None.

- 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.

- CSCsk30032—On the controller GUI, if you create a VLAN interface, map it to a wireless WLAN, and then change it to “guest,” the WLAN is mapped automatically (and without warning) to the management interface.

  Workaround: Do not use an existing VLAN interface mapped to a wireless WLAN as the guest interface.

- CSCsk30151—The controller link is not restored after the controller is rebooted.

  Workaround: Reboot the controller.

- CSCsk31842—The controller fails to join the 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.

- CSCsk32911—Path loss measurement values are not updated properly.

  Workaround: None.

- CSCsk36683—The mobility control path is down when secure mode is enabled.

  Workaround: None.

- CSCsk36855—The controller should not display the IP address, netmask, default gateway, and DHCP addresses for guest LAN interfaces.

  Workaround: None.

- 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.

- CSCsk40623—SNMPwalk failed because the OID is not increasing.

  Workaround: None.

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

  Workaround: Use the controller CLI to view this information.

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

  Workaround: None.

- CSCsk45164—An 1130 series access point reboots when registered to a controller.

  Workaround: None.

- CSCsk47454—Guest users can access the controller GUI.

  Workaround: None.

- CSCsk49157—When you change the session timeout of a WLAN that is using a backend RADIUS authentication server, any existing client that is using that WLAN shows its reauthentication timeout as infinite, even though there is a finite time after which reauthentication occurs.

  Workaround: None.

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

  Workaround: None.

- CSCsk49282—The guest LAN and WLAN are not clearly differentiated.

  Workaround: None.

- CSCsk50477—The BCAST_Q_ADD_FAILED message contains typographical errors.

  Workaround: None.

- CSCsk51226—Wired devices on the same IP subnet as a dynamic interface have no IP connectivity to the management IP address of the controller.

  Workaround: Connect the access point to the controller through a different VLAN than the dynamic interface. After the access point is connected, statically reassign the access point's IP address and retag the switch port to the VLAN of the dynamic interface.

- CSCsk51608—When you refresh some controllers from WCS, a few controllers may fail to refresh.

  Workaround: None.

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

  Workaround: None.

- CSCsk55288—IPTV video problems might occur during wireless multicast transmissions.

  Workaround: None.

- CSCsk55844—The class attribute is not sent in an accounting request.

  Workaround: None.

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

  Workaround: None.

- CSCsk58185—You can enable DCA sensitivity using two different controller CLI commands: **config advanced 802.11a channel dca sensitivity** or **config advanced 802.11a channel sensitivity**.

  Workaround: None.

- CSCsk58561—A hybrid-REAP access point requires 802.11 authentication prior to association or reassociation.

  Workaround: None.

- CSCsk60182—The controller may reboot or lose network connectivity while running software release 4.1.185.0.

  Workaround: Reboot the controller.

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

  Workaround: None.

- CSCsk61063—A guest LAN with a VLAN interface as ingress can be enabled as an anchor.

  Workaround: None.

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

- CSCsk64844—System message logs indicate that an unknown access point is communicating with the controller.

  Workaround: None.

- CSCsk65659—Auto-anchor mobility is disabled when you apply a WLAN template from WCS to the 2006 or 2106 controller.

  Workaround: Reconfigure the anchor list manually on the 2006 or 2106 controller to re-enable auto-anchor mobility.

- CSCsk66965—Web authentication and CCKM are missing from the authentication column in the WLAN list.

  Workaround: None.

- CSCsk68117—U-APSD state changes on a client device are not updated on the controller.

  Workaround: Reboot the access point, or disassociate the client from the controller and then reassociate it.

- CSCsk68181—When the client is sending CCXv4 uplink measurements, the controller does not display traffic stream metrics (TSM) reports.

  Workaround: None.

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

  Workaround: None.

- CSCsk70265—The controller is sending the neighbor list to clients using the wrong information element (IE).

  Workaround: None.

- CSCsk70727—A 7921 IP phone in world mode is not connecting to a 4400 series controller with country code KE.

  Workaround: Use country code KR instead of KE. Note that this reduces the number of available channels on the 802.11a radio to 149, 153, 157, and 161.

- CSCsk71405—The controller should not set the DF bit when sending packets to WCS. This behavior prevents WCS from adding the controller.

  Workaround: There are two possible workaround procedures:

  - Limit the number of variables that WCS requests per SNMP packet. This workaround might not work in every situation.
  - Remove the DF bit in the packets that the controller sends to WCS.

  To limit the number of variables that WCS requests per SNMP packet, use the MaxVarBindsPerPDU setting. Also set the maximum number of repetitions to ensure that all responses come in under the specified number of varbinds.

  a. Stop WCS.
  b. Go to the \WCS4.0\webnms\classes\com\cisco\server\resources\SnmpParameters.properties folder.
  c. Open SnmpParameters.properties and edit the MaxVarBindsPerPDU to be 50 or lower.
  d. Start WCS.

  To remove the DF bit at the first hop router, use these CLI commands:

  ip policy route-map fragment
  route-map fragment permit 10
  match ip address 101 set ip df 0
  access-list 101 permit ip any any

  The **ip policy route-map fragment** command goes on the router interface. The rest of the commands are global commands. You might want to restrict the access list to the controller to WCS communications instead of all packets on the interface.

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

  Workaround: None.

- CSCsk73574—Directed roam frames might be sent with an incorrect BSSID list. The frames include only the base addresses when they should include all the VLANs on the destination access point.

  Workaround: None.

- CSCsk73928—On a 1250 series access point, the downstream throughput on channel 48 is lower than on the other 5-GHz 802.11n channels.

  Workaround: None.

- CSCsk74050— If you configure an ACL name with 32 characters, the ACL override fails during roaming.

  Workaround: Use ACL names with up to 31 characters.

- CSCsk76537—Multiple 4402 controllers running software release 4.1.185.0 lock up and cannot be accessed through the console port.

  Workaround: Reboot the controllers.

- 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.

- CSCsk77010—Although a customized web authentication login page is chosen for a guest WLAN, the internal default web authentication login page appears. This problem occurs only for a specific third-party PDA.

  Workaround: None.

- CSCsk77373—802.11n clients that are associated to 1250 series access points might lose packets while the radio is active.

  Workaround: None.

- CSCsk78252—When the DCA channel list is changed, the neighbor packet interval for lightweight access points is 48 seconds when it should be 60 seconds. As a result, neighbor packets are not sent in channels other than those in the DCA list.

  Workaround: None.

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

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

- CSCsk78794—When you change the serial timeout using the controller GUI, the speed on the console port changes.

  Workaround: Delete the configuration and rebuild it, or change your terminal server speed to 19200 baud. The speed value is stored across reboots and saved in configurations. Note that before the bootloader update, the output is garbled because it is static at 9600 baud.

- CSCsk79089—1250 series access points might cause out-of-sequence management frame protection (MFP) events.

  Workaround: None.

- CSCsk79382—CCXv4 and CCXv5 clients receive an Adjacent Access Point Report from the controller even though this report should be sent only to CCXv2 and CCXv3 clients.

  Workaround: None.

- CSCsk79766—A mobility anchor controller for guest access reboots with the following error:

  ```
  Thu Oct  4 10:02:14 2007  [ERROR] sshglue.c 5731: SSHPM: failed to create Deny All
  rule.
  ```

  Workaround: None.

- CSCsk79865—The controller rejects an 11-Mbps Phy rate in the TSPEC if a client associates with 802.11g rates.

  Workaround: Send a 6-, 12-, or 24-Mbps minimum Phy rate in the TSPEC.

- CSCsk80227—Sometimes the lightweight access point does not respond properly to clear-to-send (CTS) packets from a client device.

  Workaround: None.

- CSCsk80312—If port 2, 3, or 4 is used for the management interface on a 2006 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*

- CSCsk80625—The controller is not able to see passive clients (such as cameras, programmable logic devices, and so on) behind a WGB. These clients do not initiate a traffic stream unless they are connected directly to an access point.

  Workaround: Follow these steps to work around this problem:

  a. Add a static MAC filter entry for the passive WGB device and a MAC filter entry for the devices that are behind it.

     Example: **config macfilter add** *client_mac wlan_id* [*interface*] [*description*] [*client_ip*]

  b. Enable MAC filtering on the WLAN along with AAA override.

  c. Add a static entry on the WGB IOS-based device and increase the dot11 activity timers.

     Example: bridge 1 addressxxxx.xxxx.xxxx forward FastEthernet0

  d. Add a static ARP entry on the Layer 3 router.

     Example: hostname(config)# **arp** *ip_addr mac_addr* **arpa**

- CSCsk82236—An access point join failure occurs on a 2106 controller if the access point is configured for EMEA (EU) Japan, and the controller is configured for the J, J2, or J3 domain.

  Workaround: None.

- CSCsk82851—Debugs sometimes stop running under loaded conditions.

  Workaround: Change the debug script to re-enable debugs frequently.

- CSCsk83040—An access point remote debug command is needed to show the client entry multicast tables. Such a command would provide visibility from the access point perspective to troubleshoot roaming events.

  Workaround: None.

- CSCsk83426—A hybrid-REAP access point does not reauthenticate after entering standalone mode.

  Workaround: None.

- CSCsk83477—4404 controllers running software release 4.1.171.0 or 4.1.181.0 might reboot repeatedly at a relatively high frequency.

  Workaround: None.

- CSCsk83868—Lightweight access points do not send a deauthentication request after sending request-to-send (RTS) packets to a non-responsive client device.

  Workaround: None.

- CSCsk84846—Client devices are not able to pass traffic or receive an IP address from an access point operating in hybrid-REAP mode.

  Workaround: Reboot the access point.

- CSCsk85091—If Rogue Location Detection Protocol (RLDP) is enabled on the controller, you may see radio reset messages on the access point console. There may also be a brief interruption in client traffic flow.

  Workaround: Disable RLDP.

- CSCsk85757—The Cisco WiSM reboots after operating for 32 days because the sshpmReceiveTask missed the software watchdog.

  Workaround: None.

- CSCsk86536—The wrong error message appears when you change country channels with the 802.11a radio enabled.

  Workaround: None.

- CSCsk86694—The Rogue Location Detection Protocol (RLDP) does not work on the 802.11a radio of access points that have been converted to lightweight mode.

  Workaround: None.

- CSCsk86952—The controller message logs are not cleared when you click **Clear** on the Message Logs page on the controller GUI.

  Workaround: None.

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

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

  Conditions: 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—Data throughput is lower than expected.

  Workaround: None.

- CSCsk89192—The controller allows two interfaces to have to same VLAN ID.

  Workaround: None.

- CSCsk91308—The 1250 series access points' transmit power calculation does not support OFDM duplicate mode.

  Workaround: None.

- CSCsk93026—A 1230 series access point that is converted to lightweight mode might lose the SSC during the conversion process.

  Workaround: Convert the access point to autonomous mode, and then convert it back to lightweight mode to regenerate the certificate.

- CSCsk93537—With four Intel 4965 clients simultaneously sending upstream TCP traffic using Chariot, the aggregate throughput drops to 25% of the traffic capacity of the radio.

  Workaround: None.

- CSCsk93726—The controller might reboot due to a failure with the Crash dtlArpTask.

  Workaround: None.

- CSCsk94804—Controllers sometimes reboot on the "EAP Framework" task, with the software failing on the instruction located at 0x108b10fc (pfree+56).

  Workaround: None.

- CSCsk96140—The upgrade might fail when you try to upgrade the bootloader from software release 4.0.191.0 to 4.1 using the 4.1.185.0-ER.aes image.

  Workaround: None.

- CSCsk96616—802.11n clients that are associated to 1250 series access points might drop traffic. This problem occurs when the clients are using 20-MHz channel width and the default A-MPDU settings.

  Workaround: None.

- CSCsk96636—The access points reboot after the controller is upgraded to 4.1.185.0.

  Workaround: None.

- CSCsk97014—When the 802.11g network is enabled on the controller, wireless clients that support only long slot time (20 microseconds) might have difficulties associating to access points.

  Workaround: Disable the 802.11g network for all WLANs and access points on the controller.

- CSCsk97359—When a tag has an expired access point as the last entry in the RFID table, the SNMP walk does not proceed after that.

  Workaround: None.

- CSCsk97362—Client devices sometimes fail to reauthenticate on a new channel when they disconnect from the diagnostic channel.

  Workaround: None.

- CSCsk97426—The controller GUI needs to provide external AAA support.

  Workaround: None.

- CSCsk97631—A 1250 series access point might reboot with a traceback when using traffic over a 40-MHz setup.

  Workaround: None.

- CSCsk97801—When clients are running IP/TV and FTP for 12 hours or more, the radio interface might go down due to a "driver transmit queue stuck" error.

  Workaround: None.

- CSCsk98015—The controller supports only RC4 ciphers for EAP-TLS in local authentication. FIPS certification requires AES ciphers.

  Workaround: None.

- CSCsk98326—Global configuration of the customized web-authentication page is not working. The client fails to display the customized web login page.

  Workaround: Configure the global override for the specific WLAN, choose **Customized** for the Web Authentication Type, and choose the appropriate login page. Then change the settings back to global. The page should now display properly.

- CSCsl01005—Sometimes bandwidth contracts do not take effect. If a user who has bandwidth restrictions logs in and logs out and then another user who does not have bandwidth restrictions logs in, the bandwidth restrictions are not removed immediately.

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

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

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

- CSCsl04945—If you manually change the channel for the 802.11b radio of a 1250 series access point, the controller GUI and CLI might show different values for the channel and radio status.

  Workaround: Reboot the access point.

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

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

  Workaround: None.

Resolved Caveats

These caveats are resolved in controller software release 4.2.61.0.

- CSCar09153—After downgrading or upgrading the controller from one software release to another, the controller's configuration might be partially or entirely destroyed.
- CSCsc04907—Resetting the access point to factory defaults does not clear the static IP address.
- CSCse02006—If duplicate IP addresses exist on the network, the access point keeps power cycling and is unable to join the controller.
- CSCse36574—There is no way to view how many times a packet has hit an ACL, which would help in troubleshooting ACLs. ACL counters have been implemented in controller software release 4.2.
- CSCsf27201—The "Multicast Rx queue is full" message might appear in the system message log even when multicast is disabled and no multicast traffic exists.
- CSCsg22915—Multicast packets from mobile clients with the access point group multicast address are not dropped at the controller when multicast mode is set to mcast.
- CSCsg26982—The 4400 series controller does not respond properly to the SNMP server interface discovery.
- CSCsg47218—The controller is accessible through the console or service port, but it does not pass traffic through the management interface or any dynamic interface.
- CSCsh06518—The size of the SNMP community string in the controller is limited to 16 characters. In controller software release 4.2.61.0, the size has been increased to 32 characters.
- CSCsh13494 and CSCsg80237—If you set the session timeout for an 802.1X WLAN to some value and then check the session timeout through the controller CLI, the timeout always shows as infinity. However, the controller GUI displays the correct value.
- CSCsh29597—Reauthentication occurs if you click any link on the controller GUI after using a one-time password to authenticate management users.

- CSCsh54247—You cannot perform the following logging functions on the controller:
  - Setting the system logging severity to filter out-going syslog messages
  - Setting the syslog facility
  - Configuring multiple syslog servers on the controller
- CSCsh61934—A client connecting to the LWAPP architecture using reverse-ARP may fail to obtain an IP address.
- CSCsh67192—If the controller is not rebooted after LAG is enabled, a new dynamic interface cannot be created and produces the following error message: "Unable to create VLAN interface." This message does not indicate why the interface cannot be created.
- CSCsh73171—When you enable CCKM on the controller for use with CB21AG client adapters, some CCKM configuration settings cause the client to send an association request in the middle of CCKM, thereby resulting in full authentication rather than CCKM.
- CSCsh80130—If you use auto LAG to configure the port channel for the Cisco WiSM and then manually edit the ports, you might be unable to access the controller.
- CSCsi03423—During web authentication, the HTTPS SSL server might be forced to use a weak cipher in the SSL hello handshake.

  Note For SSLv3, the client (not the server) chooses the cipher to use for the connection. Make sure your browser runs SSLv3 or TLS.

- CSCsi05147—Path loss reports are not appearing on the controller.
- CSCsi06037—You can configure peer-to-peer blocking mode only globally. You cannot configure it on a per-WLAN basis. In addition, this feature does not block ARP packets between wireless clients on the same WLAN, only IP packets.
- CSCsi06849—When the available bandwidth becomes a negative number and the corresponding voice bandwidth in use is above 100%, roam calls [with 7921 traffic specifications (TSPECs) sent as part of the re-association packets] are accepted even when the roam bandwidth is exhausted.
- CSCsi15588 and CSCsj05914—Wireless-to-wireless calls made using a 7921 phone may become disconnected after a few minutes. This issue occurs when bidirectional traffic specifications (TSPECs) are present and the inactivity timer becomes activated due to inactivity in any one direction.
- CSCsi18966—When the multiple-country feature is used, dynamic frequency selection (DFS) does not operate properly if a DFS channel that is not common among the configured countries is assigned manually. As a result, the access point does not scan for 60 seconds when changed to a DFS channel. If radar is detected, then the 802.11a radio is shut down until manually reset.
- CSCsi25491—If you choose **Wireless** from the CPU ACL Mode drop-down box on the CPU Access Control Lists page after selecting an ACL from the ACL Name drop-down box, the controller automatically defaults to the Both option instead of the Wireless option.
- CSCsi56611—Client and rogue access point detection might not function properly, and the controller might not respond to SNMP requests.
- CSCsi64689—If the existing power level is lower than power level 5 and you disable and then re-enable the WLAN, the transmit power for LWAPP-enabled access points changes to power level 1.

- CSCsi78368—The client packet dot1p check, which performs the client's tos-to-DSCP translation, is not supported in controller software release 4.2 for packets from wireless clients to the network. The priority is always mapped to 0 (null). This problem occurs when you configure the "qos profile" for platinum, gold, silver, or bronze and the "wired qos protocol" for type = 802.1p and tag = N. This issue affects the priority field in the dot1p vlan header tag for the 4.2 release, so clients on VLANs are affected.
- CSCsi80732—When you configure the b/g radio with all the data rates disabled except for 24, 36, 48, and 54 Mbps, which are configured as mandatory, the controller refuses the association of a wireless client that correctly provides the four supported rates.
- CSCsi81630—The controller might reboot repeatedly around 5 minutes after startup. This condition usually occurs when the controller, acting as a client station, attempts to associate with a rogue access point.
- CSCsi90962—When an access point tries to join a controller but fails AAA authorization, an SNMP trap is not generated to show the failure.
- CSCsi91600—The user's home page leads back to the reauthentication page if a redirect URL is populated.
- CSCsj02690—For 1000 series access points, beacons come at irregular intervals on the 2.4-GHz band.
- CSCsj10736—The controller sends query packets at the wrong interval.
- CSCsj18577—After you upgrade to controller software release 4.1.171.0 or later and configure WPA1 or WPA2 with PSK, the syslog server might display the following message: "AAA-5-RADSERVER_NOT_FOUND: Couldn't find appropriate Radius server for VAP 6. Reason: Radius accounting is disabled."
- CSCsj19875—When the controller reports the following error, it fails to include the MAC address of the client. Instead, it reports the MAC address of one of its own access points.

  Thu Jun 7 12:25:19 2007 Client Association Failure: MAC Address:00:15:70:17:8f:69 Base Radio MAC:00:14:f2:7d:be:00 Slot: 0 Reason:Unspecified ReasonCode: 1
- CSCsj20565—A 4400 series controller might reboot when you click **Monitor > CDP > Interface Neighbors** on the controller GUI in software release 4.1.171.0 or later.
- CSCsj35158—You cannot make changes to the User Base DN, User Attributes, and User Object Type parameters on an existing LDAP server configuration on the 2006 controller. After making changes and choosing **Apply**, the page shows the server index as zero and blank entries. Also, the changes are not saved after you re-edit the parameters.
- CSCsj35964 and CSCsi97060—A hybrid-REAP access point might reboot under the following conditions:
  - The WLAN has WMM allowed.
  - The radio policies are set to something other than *All*, such as *802.11b/g Only.*
  - The 802.11a network is disabled.
  - Changes are made to the WLAN configuration (such as enabling or disabling the SSID).

  The hybrid-REAP configuration (VLAN mappings) might also become lost, requiring a manual reconfiguration to enable them.
- CSCsj40291 and CSCsg05961—Controller software release 4.1.171.0 or later does not encapsulate broadcast traffic in the LWAPP tunnel. As a result, broadcast traffic is not sent from a server application to the wireless clients.

- CSCsj47472—When you refresh the configuration from WCS on a 2006 or 2106 controller running software release 4.1.171.0, the controller inverts the IP address and subnet mask for the SNMP community string template.
- CSCsj55240—An IOS SSH client cannot establish a session with the controller's SSH server.
- CSCsj58351—The controller sometimes does not respond to an ARP request, causing the client to resend it.
- CSCsj61739—The CCXv5 controller event log is parsing errors.
- CSCsj71552—In controller software release 4.1, the location-based RSSI timer for access points may expire the rogue access point entries.
- CSCsj76217—The controller drops a DHCP offer from another controller after a client device performs a Layer 3 roam across multiple controllers and different access point groups.
- CSCsj77612 and CSCsj82564—The 7921 phone may drop calls if the controller is running software.
- CSCsj83597—If you choose the Any WLAN option on the controller GUI, you might be unable to add local net users.
- CSCsj98722—You cannot add a MAC address for MAC filtering through the controller GUI.
- CSCsk03709—On the 2006 controller, SNMP walk returns loops on ipAdEntAddr.
- CSCsk37047—The controller displays a numeric value for a CCXv5 security status request. The controller should display the cipher suite description, such as WPA with TKIP.
- CSCsk50653—When a user is logged in with a lobby ambassador account, no WLAN SSIDs appear in the drop-down box.
- CSCsk97299—Newly manufactured 2106 controllers log a temperature sensor failure message. This message is cosmetic in nature.

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