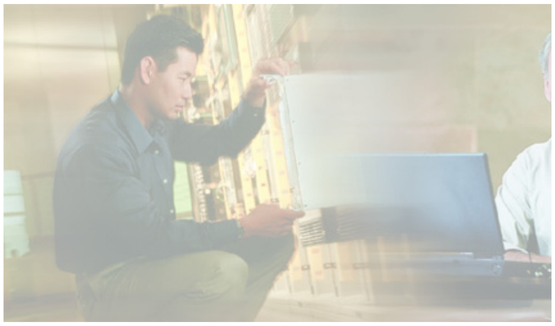


Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.0.206.0

January 9, 2006

These release notes describe open and resolved caveats for software release 4.0.206.0 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 (WMIC); and Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 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 4.0.206.0 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 2.01
- Cisco Wireless Control System (WCS) software release 4.0.96.0
- Location appliance software release 2.1.42.0
- 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, 1240, 1300, and 1500 Series Lightweight Access Points

Controller Requirements

The controller graphical user interface (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 WebAuth.

Software Release Information

Operating system software is factory installed on your controller and automatically downloaded to the access points after a release upgrade and whenever an access point associates to a controller. As new releases become available for the controllers and their associated 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 above, 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 The Cisco WiSM is supported on Cisco 7609 and 7613 Series Routers running only Cisco IOS Release 12.2(18)SXF5 or higher.

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 or 12.2(25)SEE.

Finding the Software Release

To find the software release running on your controller, look on the Monitor > Summary page of the controller GUI or enter **show sysinfo** on the controller command line interface (CLI).

Upgrading to a New Software Release

When a controller is upgraded, the code on its associated access points is also automatically upgraded. When an access point is loading code, each of its lights blinks in succession.

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, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Note You can upgrade to controller software release 4.0.206.0 from any previous controller software release.

Cisco recommends the following sequence when performing an upgrade:

1. Upload your controller configuration files to a server to back them up.
2. Turn off the controller 802.11a and 802.11b networks.

3. Upgrade your controller to the latest software release, following the instructions in the *Cisco Wireless LAN Controller Configuration Guide, Release 4.0*. Click this link to browse to that document:

   http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html

4. Re-enable your 802.11a and 802.11b networks.

Note Controllers can be upgraded from one release to another. However, should you require a downgrade from one release to another, you may be unable to use the higher release configuration. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.

New and Changed Information

Cisco 2106 Wireless LAN Controller

The Cisco 2106 Wireless LAN Controller works in conjunction with Cisco lightweight access points and the Cisco Wireless Control System (WCS) to provide system-wide wireless LAN functions. As a component of the Cisco Unified Wireless Network, the 2106 controller presents network administrators with the visibility and control necessary to effectively and securely manage business-class wireless LANs and mobility services, such as voice, guest access, and location services.

The 2106 controller supports up to six lightweight access points, making it a cost-effective solution for multi-controller architectures typical of enterprise branch deployments. It may also be used for single controller deployments for small and medium-sized business environments. The 2106 controller provides eight Ethernet ports, two of which can provide power directly to Cisco lightweight access points.

For additional information, refer to the quick start guide shipped with this controller and the "Features Not Supported on 2000 and 2100 Series Controllers" section on page 24.

Caution Do not connect a power-over-Ethernet (PoE) cable to the controller's console port. Doing so may damage the controller.

Note Wait at least 20 seconds before reconnecting an access point to the controller. Otherwise, the controller may fail to detect the device.

Multiple WLANs with the Same SSID

In controller software release 4.0.206.0, you can configure multiple WLANs with the same SSID. This feature enables you to assign different Layer 2 security policies within the same wireless LAN. To distinguish among WLANs with the same SSID, you need to create a unique profile name for each WLAN.

These restrictions apply when configuring multiple WLANs with the same SSID:

- WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in beacon and probe response. These are the available Layer 2 security policies:
  - None (open WLAN)
  - Static WEP or 802.1x

    Note Because static WEP and 802.1x are both advertised by the same bit in beacon and probe responses, they cannot be differentiated by clients. Therefore, they cannot both be used by multiple WLANs with the same SSID.

  - CKIP
  - WPA/WPA2

    Note Although WPA and WPA2 cannot both be used by multiple WLANs with the same SSID, two WLANs with the same SSID could be configured with WPA/TKIP with PSK and WPA/TKIP with 802.1x, respectively, or with WPA/TKIP with 802.1x or WPA/AES with 802.1x, respectively.

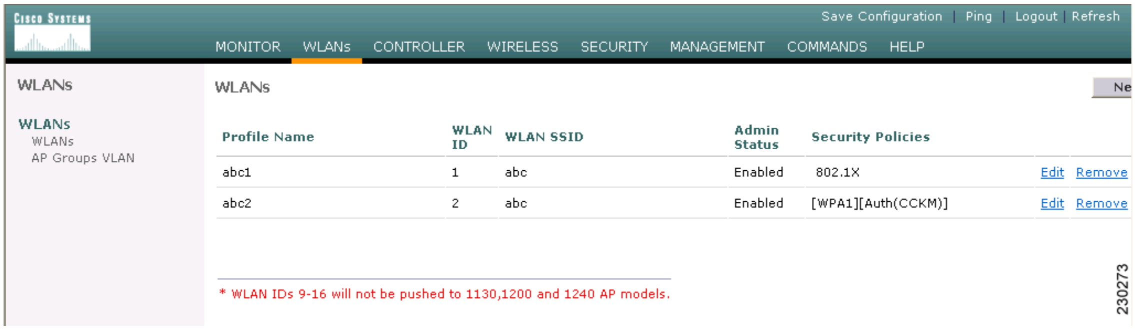
- Hybrid-REAP access points do not support multiple SSIDs.

Changes to the Controller GUI

The new Profile Name parameter appears on three controller GUI pages:

- The WLANs page, which lists all WLANs configured on the controller. Figure 1 shows two SSIDs named “abc” but with different profile names (abc1 and abc2). Notice that their security policies are also different.

Figure 1 WLANs Page



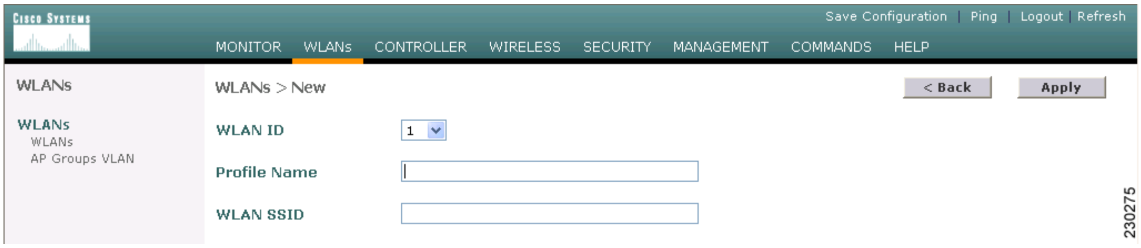
WLANs

Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies		
abc1	1	abc	Enabled	802.1X	Edit	Remove
abc2	2	abc	Enabled	[WPA1][Auth(CCKM)]	Edit	Remove

* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

- The WLANs > New page, which appears when you click **New** on the WLANs page to create a WLAN. Figure 2 shows the fields in which to enter the profile name and SSID for the WLAN.

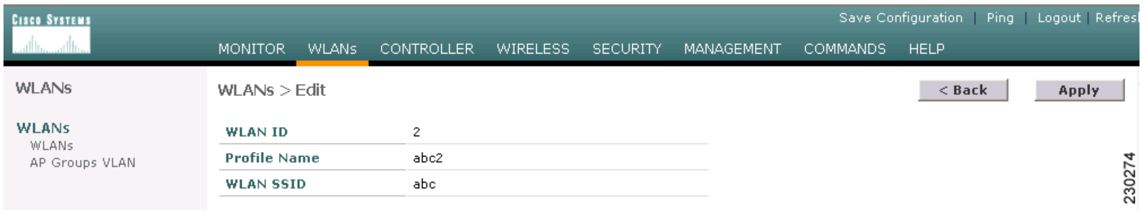
Figure 2 WLANs > New Page


Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > New
< Back
Apply
230275

WLAN ID 1
Profile Name
WLAN SSID

- The WLANs > Edit page, which appears when you click **Apply** on the WLANs > New page or when you choose to edit an existing WLAN. Figure 3 shows the ID, profile name, and SSID of the WLAN.

Figure 3 WLANs > Edit Page


Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > Edit
< Back
Apply
230274

WLAN ID	2
Profile Name	abc2
WLAN SSID	abc

Changes to the Controller CLI

The command for creating a WLAN has changed to enable you to specify a profile name.

From: **config wlan create** *wlan_id ssid*

To: **config wlan create** *wlan_id profile_name ssid*

Note If you do not specify an *ssid*, the *profile_name* parameter is used for both the profile name and the SSID.

Conditional Web Redirect with 802.1x Authentication

A new feature in controller software release 4.0.206.0 enables a user to be conditionally redirected to a particular web page after 802.1x authentication has completed successfully. Such conditions might include the user's password reaching expiration, the user needing to pay his or her bill for continued usage, and so on. You can specify the redirect page and the conditions under which the redirect occurs on your RADIUS server.

If the RADIUS server returns the Cisco AV-pair “url-redirect,” then the user is redirected to the specified URL upon opening a browser. If the server also returns the Cisco AV-pair “url-redirect-acl,” the specified access control list (ACL) is installed as a preauthentication ACL for this client. The client is not considered fully authorized at this point and is only allowed to pass traffic allowed by the preauthentication ACL.

After the client completes a particular operation at the specified URL (for example, changing a password or paying a bill), it must reauthenticate. When the RADIUS server does not return a “url-redirect,” the client is considered fully authorized and allowed to pass traffic.

The conditional web redirect feature is available only for WLANs that are configured for 802.1x or WPA1+WPA2 Layer 2 Security. You can configure this feature through the controller GUI or CLI.

Configuring the RADIUS Server

Follow these steps to configure your RADIUS server.

Note These instructions are specific to the CiscoSecure ACS; however, they should be similar to those for other RADIUS servers.

Step 1 From the CiscoSecure ACS main menu, click **Group Setup**.

Step 2 Click **Edit Settings**.

Step 3 From the Jump To drop-down menu, choose **RADIUS (Cisco IOS/PIX 6.0**). See Figure 4.

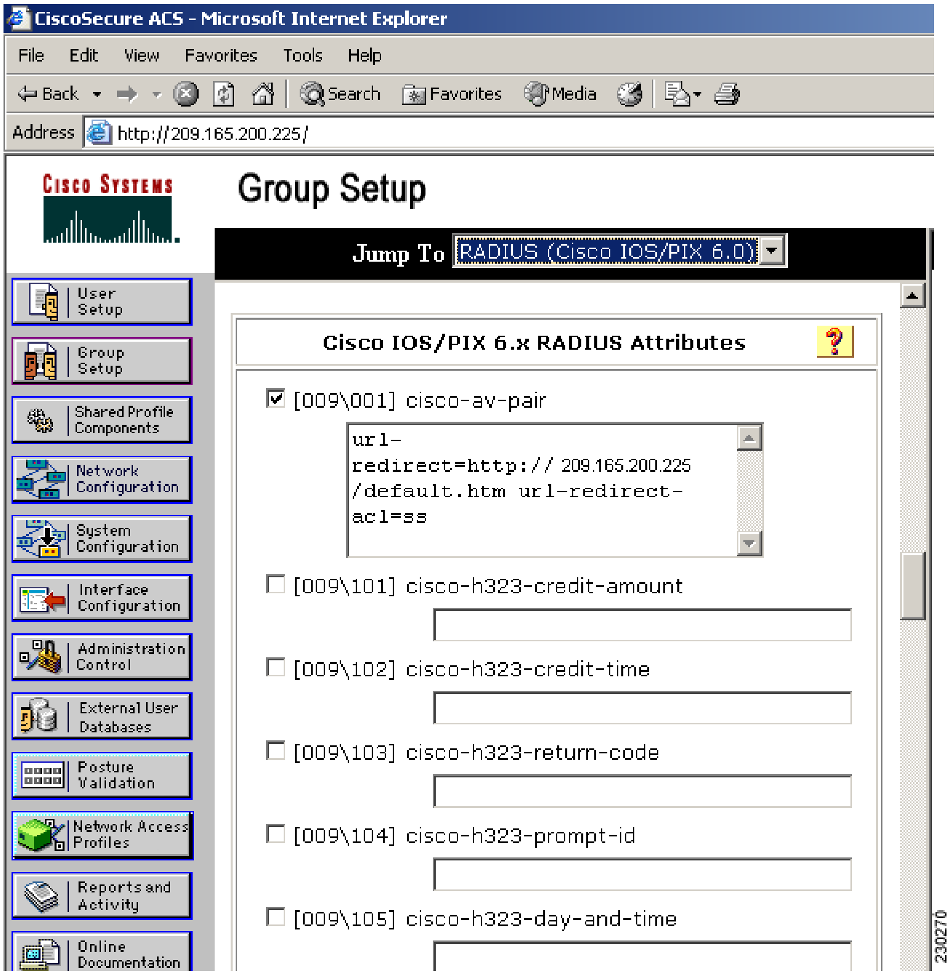
Step 4 Check the **[009\001] cisco-av-pair** check box.

Step 5 Enter the following Cisco AV-pairs in the [009\001] cisco-av-pair edit box to specify the URL to which the user is redirected and the conditions under which the redirect takes place, respectively:

url-redirect=http://*url*

url-redirect-acl=*acl_name*

Figure 4 ACS Server Configuration


CiscoSecure ACS - Microsoft Internet Explorer

Address http://209.165.200.225/

Group Setup

Jump To RADIUS (Cisco IOS/PIX 6.0)

Cisco IOS/PIX 6.x RADIUS Attributes

☑ [009\001] cisco-av-pair

```
url-
redirect=http:// 209.165.200.225
/default.htm url-redirect-
acl=ss
```

☐ [009\101] cisco-h323-credit-amount

☐ [009\102] cisco-h323-credit-time

☐ [009\103] cisco-h323-return-code

☐ [009\104] cisco-h323-prompt-id

☐ [009\105] cisco-h323-day-and-time

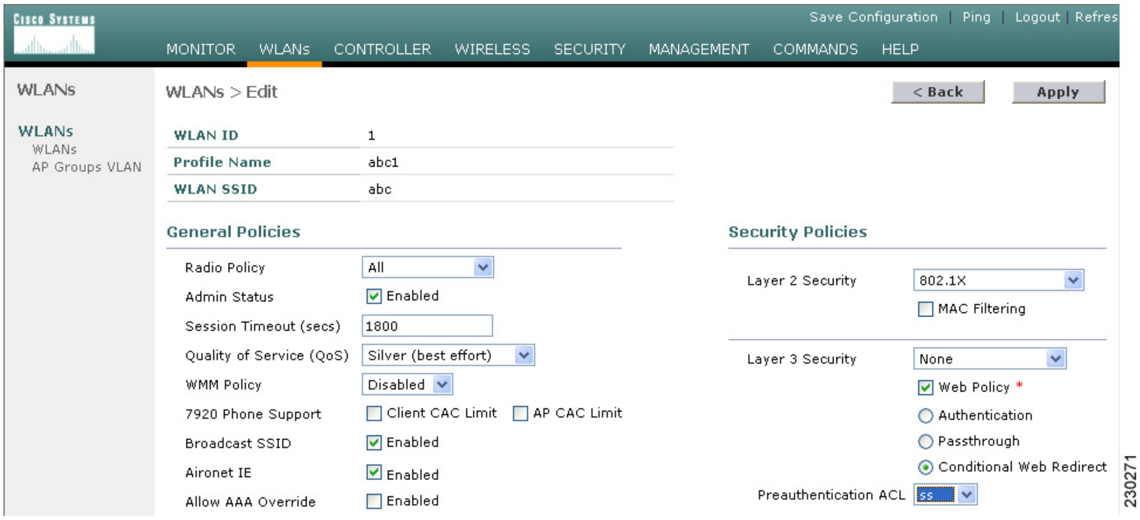
Using the Controller GUI to Configure Conditional Web Redirect

Follow these steps to configure conditional web redirect using the controller GUI.

Step 1 Click **WLANs** to access the WLANs page.

Step 2 Click the **Edit** link for the desired WLAN. The WLANs > Edit page appears (see Figure 5).

Figure 5 WLANs > Edit Page



WLANs > Edit

WLAN ID 1
Profile Name abc1
WLAN SSID abc

General Policies

Radio Policy All
Admin Status ☑ Enabled
Session Timeout (secs) 1800
Quality of Service (QoS) Silver (best effort)
WMM Policy Disabled
7920 Phone Support □ Client CAC Limit □ AP CAC Limit
Broadcast SSID ☑ Enabled
Aironet IE ☑ Enabled
Allow AAA Override □ Enabled

Security Policies

Layer 2 Security 802.1X
□ MAC Filtering

Layer 3 Security None
☑ Web Policy *
○ Authentication
○ Passthrough
● Conditional Web Redirect

Preauthentication ACL ss

Step 3 Make sure that **802.1X** or **WPA1+WPA2** is selected for Layer 2 Security.

Step 4 Check the **Web Policy** check box under Layer 3 Security.

Step 5 Choose **Conditional Web Redirect** to enable this feature or leave it unselected to disable it. The default value is unselected.

Step 6 If the user is to be redirected to a site external to the controller, choose the ACL that was configured on your RADIUS server from the Preauthentication ACL drop-down list.

Step 7 Click **Apply** to commit your changes.

Step 8 Click **Save Configuration** to save your changes.

Using the Controller CLI to Configure Conditional Web Redirect

Follow these steps to configure conditional web redirect using the controller CLI.

Step 1 To enable or disable conditional web redirect, enter this command:

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

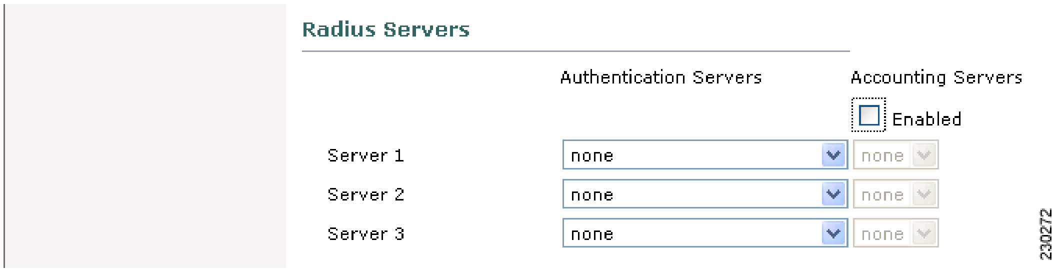
Step 2 To save your settings, enter this command:

save config

Ability to Disable Accounting Servers per WLAN

In controller software release 4.0.206.0, a new check box on the WLANs > Edit page allows you to disable all accounting servers for a WLAN. Simply uncheck the **Accounting Servers Enabled** check box (see Figure 6). Unchecking this box disables all accounting operations and prevents the controller from falling back to the default RADIUS server for the WLAN.

Figure 6 WLANs > Edit Page



Radius Servers

	Authentication Servers	Accounting Servers □ Enabled
Server 1	none	none
Server 2	none	none
Server 3	none	none

Dynamic Frequency Selection Added to Access Points in -N Regulatory Domain

In controller software release 4.0.206.0, dynamic frequency selection (DFS) is enabled automatically on Cisco lightweight access points that are configured for use in the -N regulatory domain (Mexico, Australia, Hong Kong, India, and New Zealand). The access points use DFS to detect radar signals such as military and weather sources and then switch channels to avoid interfering with them.

Mesh Security Timer

Currently, the only way to add an access point to a controller is by adding the MAC address of the access point to the controller's MAC filter. This functionality could allow a mesh access point (MAP) to join an adjacent Cisco mesh network as a result of someone adding the MAC address of the MAP on a foreign controller. If a MAP loses its root access point (RAP) with a configured bridge shared secret, it can join a foreign network by simply reverting back to its pair-wise master key (PMK).

To address this issue, controller software release 4.0.206.0 enables you to configure a security timer for the MAP in regard to the bridge shared secret. Once the timer is configured, the MAP only attempts to join a network with the same bridge shared secret for the specified period of time (for example, 10 hours). To eliminate access point stranding, the MAP starts to use the PMK after the timer expires. The timer gives the MAP enough buffered time (up to 24 hours) to rejoin the correct network in case of any scheduled or unscheduled network downtime.

Follow these steps to configure the mesh security timer using the controller CLI.

Step 1 To see your current network settings, enter this command:

show network

Step 2 Make sure that Allow Old Bridging APs to Authenticate is disabled.

Step 3 Make sure that the default bridge shared secret is not set to "youshouldsetme."

Step 4 To configure the mesh security timer, enter this command:

config mesh security-timer *timer*

where *timer* is a value between 0 and 24 hours.

After you enter this command, all of the MAPs reboot with the security timer set.

Step 5 To see the length of time set for the mesh security timer, enter this command:

show mesh security-timer

Information similar to the following appears:

```
Bridge Security Timer:    10 hour(s)
```

Note If you change the bridge shared secret, the MAPs do not re-join the network until the security timer expires. Setting the security timer to zero (0) allows the bridge shared secret to be changed without delay. However, changing the security timer on an operational system may cause the MAPs to reboot.

Lightweight Access Point Support for Cisco 3201 Wireless Mobile Interface Card (WMIC)

The Cisco 3200 Series is extending LWAPP and WCS support for the Cisco 3201 Wireless Mobile Interface Card (WMIC) configured as an access point only. With software release 4.0.206.0, controllers can manage a 2.4-GHz WMIC when deployed as a stationary access point.

The Cisco 3201 LWAPP WMIC is available for the North American and European markets. The SKUs can be ordered as a stand-alone WMIC or with select 3200 bundles. The table below lists the product names and part numbers for the LWAPP WMICs.

Product Name	Part Number
Cisco 3200 802.11g LWAPP WMIC Access Point for most of Europe AG 3200	C3201LAP-E-K9
Cisco 3200 802.11g LWAPP WMIC Access Point with thermal plates for Europe	C3201LAP-TPE-K9
Cisco 3200 802.11g LWAPP WMIC Access Point for North America	C3201LAP-A-K9
Cisco 3200 802.11g LWAPP WMIC Access Point with thermal plates for North America	C3201LAP-TPA-K9

For more information on feature support for the Cisco 3201WMIC LWAPP access point, please see the Product Bulletin for the Cisco Unified Wireless Network Software Release 4.0 at this URL:

http://www.cisco.com/en/US/products/ps7221/index.html

Other Changes

These additional changes are available in controller software release 4.0.206.0:

- Client roaming with multicast packets is now supported.
- Up to 10 access points can be concurrently upgraded from the controller.
- Hybrid REAP can now be used with up to eight access points.

  Note If the WAN link is not designed properly, the bandwidth between the access point and the controller and congestion may impact the operation of hybrid REAP.

- You can now configure a username and password for an AP1000 from the controller. This new feature enables you to debug the access point through the controller's console port. Enter this command from the controller CLI:

  config ap username *username* **password** *password*

  Note This command is already available for Cisco IOS access points that have been migrated to LWAPP. See the "Changing the IOS LWAPP Access Point Password" section on page 19 for more information.

- The following CLI command has been added to enable you to configure 802.11 enhanced distributed channel access (EDCA) parameters to support SpectraLink phones:

  config advanced edca-parameters {**svp-voice** | **wmm-default**}

  where

  svp-voice enables SpectraLink voice priority (SVP) parameters and

  wmm-default enables wireless multimedia (WMM) default parameters.

  Note To propagate this command to all access points connected to the controller, make sure to disable and then re-enable the 802.11b/g network after entering this command.

- The following CLI command has been added to enable you to change the 4.9-GHz band on the -P regulatory domain if public-safety is disabled:

  config ap public-safety enable *Cisco_AP*

- The following CLI command has been added to allow you to enable or disable broadcasting without enabling or disabling multicasting as well. This command uses the multicast mode currently on the controller to operate.

  config network broadcast {**enable** | **disable**}

- The CLI commands used to enable or disable remote debugging of a Cisco lightweight access point or to remotely execute a command on a lightweight access point have changed as follows:

  From:

  config ap remote-debug enable *Cisco_AP*

  config ap remote-debug disable *Cisco_AP*

  config ap remote-debug exc-command *cmd Cisco_AP*

  To:

  debug ap enable *Cisco_AP*

  debug ap disable *Cisco_AP*

  debug ap command *cmd Cisco_AP*

- The following CLI commands have been added to allow devices that do not understand the controller's proxy Address Resolution Protocol (ARP) response without a minimum packet size of 60 bytes to communicate with the controller:
  - **config advanced arp padding** *bytes*—Allows the controller to pad ARP requests that it proxies or forwards to certain devices.
  - **show advanced arp**—Shows whether ARP padding is enabled.

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.

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* may incorrectly state that these LEDs flash amber during a software upload or download.

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)
- Enable or disable the mobility protocol port using this CLI command:

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

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 unless you have successfully upgraded to the _ER.aes image on Cisco.com. See CSCsg18356 in the "Resolved Caveats" section on page 33 for more details.

Rate-Limiting on the Controller

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.

Re-enable Broadcast after Upgrading to Release 4.0.206 or Later

In software releases 4.0.179 and earlier, broadcast and multicast forwarding were both controlled with a single global flag that enabled multicast. In software release 4.0.206 these functions were broken into separate configuration flags: one that contols broadcast and one that controls non-broadcast multicast. If you have multicast enabled in software releases 4.0.179 and earlier, the broadcast flag is left disabled after upgrading to software release 4.0.206. 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 or later, use this CLI command to re-enable broadcast:

config network broadcast enable

When re-enabled, broadcast uses the multicast mode configured on the controller. If you want to turn on broadcast only and set it to another multicast mode you must use the CLI because the GUI configuration forces multicast on.

Service Modules Supported in the Catalyst 6500 Series Switch

The Catalyst 6500 Series Switch chassis can support up to five Cisco WiSMs 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).

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.

Association Delay for 1500 Series Access Points

The 1500 series access points may take up to 10 minutes to fully associate to the controller on initial startup.

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

Operating Mesh Networks through Switches and Routers

In mesh networks that operate through switches and routers, network round-trip delays between access points and the controller must be less than 100 milliseconds (ms); otherwise, timing problems may occur during wireless client authentication. Also, network path outages of 7 seconds or longer between access points and the controller may cause the access points to lose connectivity.

Cisco 7920 Wireless IP Phone Support

When using Cisco 7920 Wireless IP Phones with controllers, make sure that the phones and controllers are configured as follows:

- Aggressive load balancing must be disabled for each controller. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.
- The QoS Basis Service Set (QBSS) information element (IE) must be enabled. The QBSS IE enables the access points to communicate their channel usage to wireless devices. Because access points with high channel usage might not be able to handle real-time traffic effectively, the 7920 phone uses the QBSS value to determine if they should associate with another access point. Use the following commands to enable the QBSS IE:
    - **sh wlan summary**

      Note Use this command to determine the WLAN ID number of the WLAN to which you want to add QBSS support.

    - **config wlan disable** *wlan_id_number*
    - **config wlan 7920-support ap-cac-limit enable** *wlan_id_number*
    - **config wlan enable** *wlan_id_number*

- **sh wlan** *wlan_id_number*

Note Use this command to verify that the WLAN is enabled and the Dot11-Phone Mode (7920) field is configured for compat mode.

- **save config**

- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the **config 802.11b dtpc enable** command. The DTPC IE is a beacon and probe information element that allows the access point to broadcast information on its transmit power. The Cisco 7920 Wireless IP Phone uses this information to automatically adjust its transmit power to the same level as the access point to which it is associated. In this manner, both devices are transmitting at the same level.
- Both the 7920 phones and the controllers support Cisco Centralized Key Management (CCKM) fast roaming.
- When configuring WEP, there is a difference in nomenclature for the controller and the 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7920.

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* {*AP_name* | **all**}

- The *AP_name* 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.

IPSec Not Supported

Software release 4.0.206.0 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 3.2 or wait for a future release.

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 time is not set first. Set the time on the controller before allowing the access points to connect to it.

RADIUS Servers

This product has been tested with the following RADIUS servers:

- CiscoSecure ACS v4.0
- Funk Steel-Belted RADIUS release 4.4.137

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.

Cisco Aironet 1030 Remote Edge Lightweight Access Point Default Operation

When a controller reboots, dropped Cisco Aironet 1030 Remote Edge Lightweight Access Points attempt to associate to any available controller. If the access points cannot contact a controller, they continue to offer 802.11a/b/g service on WLAN 1 only.

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.

Using the GUI to Change the SNMP Community String Default Values

Follow these steps to change the SNMP community string default values through the controller GUI.

Step 1 Click **Management** and then **Communities** under SNMP. The SNMP v1 / v2c Community page appears.

Step 2 If “public” or “private” appears in the Community Name column, click **Remove** to delete this community.

Step 3 Click **New** to create a new community.

Step 4 When the SNMP v1 / v2c Community > New page appears, enter a unique name containing up to 16 alphanumeric characters in the Community Name field. Do not enter "public" or "private."

Step 5 In the remaining fields, enter the IP address from which this device accepts SNMP packets with the associated community and the IP mask, choose **Read Only** or **Read/Write** to specify the access level for this community, and choose **Enable** or **Disable** to specify the status of this community.

Step 6 Click **Apply** to apply your changes.

Step 7 Click **Save Configuration** to save your settings.

Step 8 Repeat this procedure if a "public" or "private" community still appears on the SNMP v1 / v2c Community page.

Using the CLI to Change the SNMP Community String Default Values

Follow these steps to change the SNMP community string default values through the controller CLI.

Step 1 To see the current list of SNMP communities for this controller, enter this command:

show snmp community

Step 2 If "public" or "private" appears in the SNMP Community Name column, enter this command to delete this community:

config snmp community delete *name*

The *name* parameter is the community name (in this case, "public" or "private").

Step 3 To create a new community, enter this command:

config snmp community create *name*

Enter up to 16 alphanumeric characters for the *name* parameter. Do not enter "public" or "private."

Step 4 To enter the IP address from which this device accepts SNMP packets with the associated community, enter this command:

config snmp community ipaddr *ip_address ip_mask name*

Step 5 To specify the access level for this community, enter this command, where **ro** is read-only mode and **rw** is read/write mode:

config snmp community accessmode {**ro** | **rw**} *name*

Step 6 To enable or disable this SNMP community, enter this command:

config snmp community mode {**enable** | **disable**} *name*

Step 7 To save your changes, enter **save config**.

Step 8 Repeat this procedure if you still need to change the default values for a "public" or "private" community string.

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.

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

Using the GUI to Change the SNMP v3 User Default Values

Follow these steps to change the SNMP v3 user default values through the controller GUI.

Step 1 Click **Management** and then **SNMP V3 Users** under SNMP.

Step 2 If “default” appears in the User Name column, click **Remove** to delete this SNMP v3 user.

Step 3 Click **New** to add a new SNMP v3 user.

Step 4 When the SNMP V3 Users > New page appears, enter a unique name in the User Profile Name field. Do not enter “default.”

Step 5 In the remaining fields, choose **Read Only** or **Read Write** to specify the access level for this user, choose the authentication and privacy protocols to be used, and enter a password for each.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your settings.

Using the CLI to Change the SNMP v3 User Default Values

Follow these steps to change the SNMP v3 user default values through the controller CLI.

Step 1 To see the current list of SNMP v3 users for this controller, enter this command:

show snmpv3user

Step 2 If “default” appears in the SNMP v3 User Name column, enter this command to delete this user:

config snmp v3user delete *username*

The *username* parameter is the SNMP v3 username (in this case, “default”).

Step 3 To create a new SNMP v3 user, enter this command:

config snmp v3user create *username* {**ro** | **rw**} {**none** | **hmacmd5** | **hmacsha**} {**none** | **des**} *auth_password privacy_password*

where

- *username* is the SNMP v3 username,
- **ro** is read-only mode and **rw** is read/write mode,
- **none**, **hmacmd5**, and **hmacsha** are the authentication protocol options,
- **none** and **des** are the privacy protocol options,

- *auth_password* is the authentication password, and
- *privacy_password* is the privacy password.

Do not enter “default” for the *username* and *password* parameters.

Step 4 To save your changes, enter **save config**.

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
- Cranite
- Fortress
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through
- Link aggregation (LAG)

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.

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.

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:

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

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

```
     }

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

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

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

}

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

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

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

<tr align="center">
```

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

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

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

Caveats

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

Open Caveats

These caveats are open in controller software release 4.0.206.0.

- CSCsb01980—When the operator enters incorrect data for the management interface in the controller web configuration wizard, error messages are shown only at the end of the wizard, and the user must return to the Management Interface page for correction. The data entered on the Management Interface page, such as the port number, are not validated immediately but at the end of the wizard. As a result, any error messages are shown only at the end.

  Workaround: Use the CLI configuration wizard.

- CSCsb01983—The controller web configuration wizard is not reachable after making repeated invalid entries for the management interface port. If an operator connects to the wizard on address 192.168.1.1 and enters an invalid port number on the Management Interface page, the operator is redirected at the end of the wizard to the Management Interface page to correct the port. If the operator enters an incorrect port and submits, the wizard becomes inaccessible.

  Workaround: Reboot the controller through the CLI to access the wizard again.

- CSCsb20269—On the Cisco WiSM, when the service VLAN is configured as one of the VLANs on a data port, it does not operate correctly.

  Workaround: Do not configure the service VLAN as one of the VLANs on a data port.

- 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 code image to the Cisco WiSM using the CLI, associated access points are sometimes disconnected.

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

- CSCsb88588—Incorrect power levels are reported for access points when the controller is set to country code SG.

  Workaround: None at this time.

- CSCsc02860—When users download the code image to a Cisco WiSM for the first time, the WiSM fails to download the new image to flash memory.

  Workaround: Download new code images to the WiSM a second time.

- CSCsc04907—Resetting the access point to factory defaults does not clear the static IP address.

  Workaround: Clear the access point's static IP address by hand.

- CSCsc11660—The current country screen is not 100% accurate for all deployment scenarios, which may cause confusion in some instances.

  Workaround: None at this time.

- CSCsc68154—The controller's error log repeatedly displays the "Got an idle-timeout message from an unknown client" error message for some unknown reason.

  Workaround: None at this time.

- CSCsd52483—When you make changes in the boot loader of a 2006 controller or a Controller Network Module, the bootup process may halt, and the controller may stop responding.

  Workaround: None at this time. The controller must be returned for repair through the RMA process.

- CSCsd54171—After the controller configuration is modified, the changes may not take effect or function properly.

  Workaround: Save the controller configuration to a TFTP server or WCS; then reset the controller to restore the default configuration. After completing the setup wizard, reload the saved configuration from the TFTP server or WCS.

- CSCsd54750—The Cisco WiSM may display numerous timeout messages.

  Workaround: None at this time.

- CSCse04713—Rogue detection on the wired network may not operate properly.

  Workaround: None at this time.

- CSCse10109—For WMM clients without TSPEC support, ACM must be disabled for proper QoS mapping.

  Workaround: Disable ACM for WMM clients without TSPEC support.

- CSCse28941—AP1510 mesh access points (MAPs) using dynamic frequency selection (DFS) and deployed in the European Telecommunications Standards Institute (ETSI) domain may detect what they perceive to be radar signals, even if no radar is present.

  Workaround: To eliminate the risk of falsely detected radar, perform a site survey to ensure that no interference is detected in the 5.8-GHz band.

- CSCse42329—When the controller sends an IP packet to a node through its default gateway, it uses the MAC address of the interface where a packet was originated instead of the MAC address learned through the ARP process. This approach impacts failover performance, traffic profiles, and any network designs that rely on the standard behavior of an IP stack.

  Workaround: None at this time.

- CSCse65613—You cannot rate limit or block specific multicast or broadcast traffic from the wired network when broadcast/multicast is enabled on the controller. When you enable multicast, you also enable broadcast traffic. However, normal ACLs do not block certain multicast addresses or rate limit broadcasts coming from the wired network. A broadcast storm or large number of multicast packets generated on the wired network are transmitted on the wireless network.

  Workaround: None.

- CSCse66714—When you use the controller GUI to set a static IP address on a different subnet than the one the access point is on, the access point reboots, but the GUI page does not refresh. When the access point reboots, it sometimes uses a fallback address, and the display shows the static IP address configuration as well as the IP address it is using.

  Workaround: Check the configuration using the **show ap config** *name* CLI command, which shows the access point using a fallback address.

- CSCse72401—When you set a 1310 access point running software release 4.0.155.5 or 4.0.179.11 to the ETSI domain, the **show cont d0** CLI command displays the following for the carrier set: "Carrier Set: EMEA (EU) Japan."

  Workaround: None at this time.

- CSCse97007—If you disable management frame protection (MFP) on an AP1020 attached to the controller and save the configuration, MFP is enabled after a reboot.

  Workaround: None at this time.

- CSCsf09647—The AP1000 firmware may drop broadcast frames sent from rogue access points.

  Workaround: None at this time.

- CSCsf21931—The Cisco WiSM does not support Layer 2 LWAPP mode. However, the option to configure Layer 2 LWAPP mode is available through both the controller GUI and CLI.

  Workaround: None at this time.

- CSCsg12879—When you attempt to disable power-over-Ethernet (PoE) through the controller GUI, the following error message appears: "Error is setting Power Over Ethernet."

  Workaround: None at this time.

- CSCsg29291—If you change the name of an AP1010 that is connected to the 2106 controller, the AP Name field is not propagated correctly for the beacon within the Aironet information element (IE).

  Workaround: Reboot the controller.

- CSCsg30623—When a 2106 controller is connected to an AP1010 and AP1131, the CwMin and CwMax values in the Aironet IE are identical but are different for Platinum and Gold QoS.

  Workaround: None at this time.

- CSCsg36747—The **Clear Counters** button on the Controller Statistics page does not clear the controller's counters.

  Workaround: None at this time.

- CSCsg40594—If you connect an access point on a VLAN other than the management VLAN, multicast traffic is fragmented by the controller and sent to the access point with LWAPP encapsulated. Only the IP fragmented packet is received. The first packet is dropped due to the ACL applied, and the access point reboots after several minutes.

  Workaround: None at this time.

- CSCsg40655—The controller should not use two port numbers for different size packets. When the controller encapsulates the UDP payload from a multicast packet, it adds two different distribution ports for small and large packets.

  Workaround: None at this time.

- CSCsg44650—Cisco Discovery Protocol (CDP) does not operate correctly when a 2106 controller is connected to a 3750 switch. The controller sees the 3750 chassis as a CDP neighbor, but the 3750 does not recognize the 2106.

  Workaround: None at this time.
- CSCsg46430—Bridging information always shows the Hop Count as zero.

  Workaround: None at this time.
- CSCsg54850—During a stress test with 60-Mbps traffic, you may be unable to access the CLI through the Ethernet port or the GUI on a 2006 controller or the Wireless LAN Controller Network Module.

  Workaround: None at this time.
- CSCsg55649—Internet Group Management Protocol (IGMP) V3 join reports sent by the client upon starting a multicast application may be duplicated to one of the controller ports in the link aggregation (LAG) bundle.

  Workaround: None at this time.
- CSCsg58143—A frame marked with DSCP priority 7 may be downgraded to priority 6 and sent over the air.

  Workaround: None at this time.
- CSCsg64309—Roaming fails between hybrid-REAP access points using local switching and web authentication.

  Workaround: This behavior is as designed.
- CSCsg64815—The traplog for the 2006 controller and the Wireless LAN Controller Network Module has a very large port number.

  Workaround: None at this time.
- CSCsg65482—Controllers sometimes drop multicast packets in unicast or multicast mode.

  Workaround: None at this time.
- CSCsg66265—Client WMM states may not update properly. If a client associates to an access point as WMM capable, disconnects, is changed to non-WMM capable, and finally re-associates, the controller sends traffic to the client with a QoS header.

  Workaround: None at this time.
- CSCsg69021—Fast roaming with WPA2+CCKM on dynamic interfaces may not operate properly.

  Workaround: None at this time.
- CSCsg70979—When a mesh access point (MAP) joins the controller with the default bridge group name (BGN), the MAP BGN should appear as “DEFAULT.” However, the MAP BGN value is empty if the MAP does not have a BGN set or if the set value shows up on the controller even though the MAP joined the controller with the “DEFAULT” BGN string.

  Workaround: None at this time.
- CSCsg71039—When a mesh access point’s (MAP’s) root access point (RAP) goes down, the MAP falls back to the default bridge group name (BGN) and joins the controller through another RAP. When the first RAP comes back up, the MAP reverts back to the configured BGN and joins the first RAP. However, the first RAP declares the MAP as the default child, and the MAP declares the first RAP as the default parent, which is incorrect.

  Workaround: None at this time.

- CSCsg71421—The **show qos profile** command does not operate properly. The controller does not allow any further input after this command is entered.

  Workaround: None at this time.

- CSCsg72051—The Wi-Fi Multimedia (WMM) information element broadcast by 1000 series access points is not recognized by some wireless devices. The devices that do not recognize the WMM information element can associate to a 1000 series access point but cannot maintain WMM interoperability with the access point.

  Workaround: None at this time.

- 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 at this time.

- CSCsg78011—The controller fails to send an update about any access points in the mesh network that lose connectivity.

  Workaround: None at this time.

- CSCsg78130—The controller sometimes successfully loads a new controller software image but fails to load the accompanying access point images.

  Workaround: None at this time.

- CSCsg81953—Controllers sometimes report IDS Disassoc Flood attacks against valid clients in which the attacker’s MAC address is that of an access point joined to that controller.

  Workaround: None.

- CSCsg83671—There is no way to transfer a core-dump file from the controller to a TFTP server.

  Workaround: None at this time.

- CSCsg89311—The controller sometimes reboots when downloading a customized web authentication file.

  Workaround: None at this time.

- CSCsh04777—The AP1000 does not periodically send neighbor packets on the non-dynamic frequency selection (DFS) channels (36-48). As a result, the access point is hindered from properly forming a neighborhood with other access points in the same RF domain.

  Workaround: None at this time.

- CSCsh31384—When Ethernet broadcast and multicast are enabled on the controller and a wired host sends broadcast packets, the controller does not forward the packets to the access points.

  Workaround: None at this time.

- CSCsh35306—Unicast ARPs may drop from export-foreign clients because the IP address is not known at the foreign controller.

  Workaround: None at this time.

- CSCsh36213—If the controller is running a special engineering image with a version number higher than 4.0.179.102, the SSID information may not be migrated correctly when upgrading to software release 4.0.206.0 or greater. This issue only affects specific engineering builds. The problem does not occur when upgrading from released software images available from Cisco.com.

  Workaround: After the upgrade, remove the WLANs/SSIDs and recreate them. Then save the configuration.

- CSCsh44486—A 1200 series access point sometimes reboots when a client device is associated to the radio interface that you're configuring.

  Workaround: None.

- CSCsh47269—In software releases 4.0.179 and earlier, broadcast and multicast forwarding were both controlled with a single global flag that enabled multicast. In software release 4.0.206 these functions were broken into separate configuration flags: one that contols broadcast and one that controls non-broadcast multicast. If you have multicast enabled in software releases 4.0.179 and earlier, the broadcast flag is left disabled after upgrading to software release 4.0.206. As a result, some applications that rely on broadcast do not work after the upgrade.

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

  config network broadcast enable

  When re-enabled, broadcast uses the multicast mode configured on the controller. If you want to turn on broadcast only and set it to another multicast mode you must use the CLI because the GUI configuration forces multicast on.

- CSCsh47364—When access point debugging is enabled on a controller and you enter **debug lwapp ?** during a telnet or SSH session to the controller, the controller reboots.

  Workaround: None.

- CSCsh47906—Access points associated to a controller running software release 4.0.206 sometimes reboot when LWAPP traffic drops.

  Workaround: None.

- CSCsh48977—The controller IP stack becomes inoperable on a large Layer 2 subnet. The controller stops responding to pings, SNMP, and other management traffic, and RADIUS stops working. Access points stay connected but client devices are able to associate and pass traffic only on WLANs that do not require authentication.

  Workaround: None.

- CSCsh49310—Clearing the configuration on a 2000 series controller sometimes corrupts the image.

  Workaround: None.

- CSCsh50527—NPU truncates padding from unicast ARP frames. Access points now use the length field in the LWAPP header to determine the number of bytes to transmit over the air. As a result, padding is stripped from unicast ARP frames.

  Workaround: None.

- CSCsh50966—The controller sometimes fails to answer unicast ARP requests for the AP-manager interfaces. As a result, there might be sporadic interruptions in connectivity at ARP refresh time, resulting in the periodic loss of associations for access points associated through AP managers other than the first (ap-manager). This is especially likely if the default router is running an IOS version that is subject to CSCec40253.

  Workaround: On the system issuing the unicast ARP request, configure a static ARP entry for the AP-manager2 (and up) interface(s). For example, if the failing ARP unicasts are being issued by an IOS router, enter this command:

  ```
  router(config)#arp 10.1.1.1 0000.0102.abcd arpa
  ```

  where 10.1.1.1 is the AP-manager interface IP address, and 0000.0102.abcd is its MAC address.

- CSCsh61347—In some regulatory domains outside the US and Canada, MESH access points fail to join a controller after they are upgraded from software version 4.0.179.11 to 4.0.206.

  Workaround: None.

- CSCsh64994—RADIUS account records are not generated when an access point is configured in H-REAP mode with a locally switched SSID.

  Workaround: None.

- CSCsh67106—AAA interface override results in ACLs are sometimes not installed.

  Workaround: None.

- CSCsh68089—Access points connected directly to a port on 2000 or 4400 series controllers sometimes fail to receive an IP address through DHCP.

  Workaround: Create and enable a DHCP scope on the controller’s internal DHCP server. The scope, even a placeholder or non-functioning scope, is enough to disable the CHADDR filter and allow an access point to receive an IP address.

- CSCsh69985—When a Cisco 7920 phone is associated to a lightweight access point the controller sometimes fails to forward packets to the phone.

  Workaround: None.

Resolved Caveats

These caveats are resolved in controller software release 4.0.206.0.

- CSCsb87264—If WLAN ID 1 is not configured on the controller, a REAP access point broadcasts the “Airespace” SSID after entering standalone mode. Clients can access this unsecured SSID and use the REAP access point to access the network.
- CSCsc05495—Controllers intermittently send a state attribute 24 in an access-request packet.
- CSCsc14045—When you choose the VPN Passthrough Layer 3 security option on the WLANs > Edit page, you should not be able to enable the Web Policy feature on the same page.
- CSCsc44326—A 4400 series controller may fail to respond to ARP requests for the ap-manager2 interface’s IP address when the ARP request is addressed at the MAC layer to the unicast MAC address of the interface rather than to the broadcast MAC address. As a result, there may be sporadic interruptions in connectivity at ARP refresh time, resulting in the periodic loss of associations for access points associated through the ap-manager2 interface.
- CSCsd27529—Static WEP does not operate properly for a REAP access point in standalone mode.
- CSCsd82363—Channel utilization is incorrectly reported in radio utilization reports on the controller and in WCS. Channel utilization may appear as zero when there is active client traffic or as an aggregate of client transmit and receive traffic.
- CSCsd85126—The access point may reboot unexpectedly after upgrading to software release 3.2.116.21.
- CSCsd87382—Bridging functionality for REAP devices is not available on OEM builds of controller software.
- CSCsd95992—When IGMPv3 is enabled on the controller, a significant amount of packet loss occurs. The packet loss is even greater when there is an active multicast stream.
- CSCse11202—WPA clients may receive an error message indicating that the WEP key may be configured incorrectly on the client.

- CSCse14889—The controller does not generate traps for ad-hoc rogues.
- CSCse18855—RADIUS accounting cannot be disabled on an individual WLAN. Once a RADIUS accounting server is defined globally, WLANs fall back to the global RADIUS accounting server if no RADIUS accounting server is selected in the WLANs.
- CSCse21595—The state of the WMM admission control mandatory (ACM) bit is not updated in the access point beacons and probe responses immediately after you configure the Admission Control (ACM) parameter on the controller. Your change does not take effect until the next time the WLAN is enabled.
- CSCse29193—The controller marks a RADIUS server as dead if a single request receives no response after five retries.
- CSCse30891—Controllers have a limit of 8 access points for tracking a client or RFID tag element. When an element is observed by more than 8 access points, any extra access-point readings are discarded, and those signals are not used in the location calculation for that element. To resolve this issue, the access-point limit for tracking elements has been increased from 8 to 16 access points, and the ability to override the weakest RSSI value has been added.
- CSCse33667—A controller running software release 3.2.116 may reboot without providing an error log.
- CSCse34673—If you globally disable and then globally enable management frame protection (MFP) on a controller that is part of a mobility group and connected to LWAPP-enabled access points, the access points that are connected to the other controllers within the mobility group may report sequence number MFP anomalies.
- CSCse36426—Controllers with AP-group VLANs configured sometimes cause WCS to hang when the controllers are added to WCS.
- CSCse36920—The controller and access point software needs to support Pango's chirp tag packet format, which improves battery life.
- CSCse46717—An access point may reboot when connected to a 4404 controller running software release 3.2.150.06.
- CSCse50111—If port 1 is active and port 2 is the backup, the LED for port 2 flashes and web access becomes inaccessible after traffic is sent from a wireless PC to a wired PC.
- CSCse56114—Bridge protocol data unit (BPDU) packets are forwarded through the outbound gigabit interface regardless of how the interface is configured.
- CSCse63908—If DHCP Required is not configured on the controller, the access points should learn the IP address of wireless clients when the clients send out the first IP packet or ARP. However, if the wireless clients are passive devices (that is, devices that do not initiate communication such as wireless printers), the access points fail to learn the IP address of the wireless devices. As a result, the controller waits 10 seconds for the clients to send an IP packet. If the clients do not send a packet, the controller drops any packets to the passive wireless clients.
- CSCse66940—If you switch the management interface port on a 4404 controller with multiple AP-manager interfaces and WLAN interface redundancy, all WLANs become disabled.
- CSCse68462—The controller fails to restrict wireless clients from accessing the CLI management port through secure shell (SSH). With SSH enabled and management via wireless disabled, it is possible to get a login prompt by sending multiple SSH connections in rapid succession.
- CSCse75035—When IP packets are fragmented, access points cannot download the configuration from the controller. When IP fragmentation is removed, access points join the controller and download configurations normally.

- CSCse76633—Hybrid-REAP access points may not receive a configuration response from the controller and therefore experience continuous reboots.
- CSCse82841—You cannot configure multiple WLANs with the same SSID.
- CSCse82846—After a client authenticates using 802.1x, the controller cannot redirect that client to a specific web page.
- CSCse87066—Access points in the same mobility group are seen as rogue access points by another controller if either of the following is true:
  - An access point can see more than 24 neighbors. The neighbor list size is 24, so any additional access points are reported as rogues.
  - One access point can hear a client communicating to a another access point, but the second access point cannot be heard and, therefore, cannot be validated as a neighbor.
- CSCse87074—The controller does not show the entire output of the **show run-config** command on the CLI.
- CSCse90894—Microsoft Internet Explorer 6 sometimes redirects the controller home page back to the web authentication login page.
- CSCse91264—A WLAN using hybrid-REAP local switching and web authentication for Layer 3 WLANs does not forward users to the web authentication login page.
- CSCse93986—All HTTP and HTTPS traffic sent by the client is directed to the controller's CPU without regard to the preauthentication ACL.
- CSCse96745—When you add a MAC address to the MAC filter on the controller, the operation fails and an empty alert window appears if the same MAC address is configured in the access point authorization list.
- CSCsf00431—When you convert an autonomous access point to LWAPP mode, CDP is disabled on the access point when it joins the controller even though CDP is enabled in the default configuration that the controller sends to the access point.
- CSCsf00511—When you set an access point to administratively disabled, the controller Monitor page does not report that an access point is down.
- CSCsf01648—Clients that associate using web authentication with WPA-PSK cannot re-associate after the radio disconnects and then reconnects.
- CSCsf01759—The controller discards AAA attributes for a client when it sends a stop record, assuming that new attributes will be provided for the next session. This behavior, however, breaks single sign-on.
- CSCsf06007—Cisco WiSM controllers running software release 4.0.155.5 may experience counter errors for bytes sent and received.
- CSCsf06321—WPA2 with AES becomes disabled on hybrid-REAP access points after broadcast key rotation.
- CSCsf06408—When an ASCII PSK key is applied for WPA or WPA2 from WCS, the clients fail to join. The correct PSK key gets pushed from WCS, but the controller does not allow clients to associate.
- CSCsf08091—You can create a maximum of 64 interfaces using the controller GUI.
- CSCsf08102—WLAN override settings are not visible on the individual radio page.

- CSCsf09997—It may take a minute or more for a wireless client to receive a new IP address when switched to a new VLAN. When the controller switches the wireless client to a new VLAN, the controller sends the DHCP request for the client with the wrong network information, so the client does not receive an IP address until the DHCP retries expire and the controller resets the client information.
- CSCsf11493—The Cisco WiSM sometimes stops functioning and reboots when its gigabit ports are disabled.
- CSCsf12843—Access points in hybrid-REAP mode sometimes reboot but do not allow clients to associate. This condition occurs when multiple WLANs are defined on the controller (for example, WLANs 1, 2, 3, 4, and 5) but only a few are enabled on the access point (for example, WLANs 1, 3, and 5).
- CSCsf15084—Containing rogue ad-hoc devices sometimes generates more ad-hoc entries.
- CSCsf23000—When you use the controller GUI to change the antenna type from internal to external on the 802.11a radio in a 1000 series access point or in a 1500 series access point, the operation sometimes fails, and the GUI displays an error message.
- CSCsf23095—The controller GUI does not indicate that the AES Key Wrap setting is designed for FIPS customers and requires a key-wrap compliant RADIUS server.
- CSCsf24925—The **config ap remote-debug exc-command** *exec_command ap_name* controller CLI command can be used to send an access point an arbitrary exec command to be executed. This command, however, has several usability restrictions:
  - If the *exec_command* contains embedded white space, it should be contained within double quotes.
  - The output of the exec command is written to the controller console, regardless of whether the **config ap remote-debug exc-command command** was issued within a console CLI session or within a Telnet/SSH session. Therefore, to validate the command's syntax or to view the command output, the command should be issued from the controller console.
- CSCsf26863—When you use web authentication with a proxy server, you are redirected to an invalid URL such as "http://http://***."
- CSCsf27479—The Cisco WiSM may stop functioning and become inaccessible from the console. Error messages may or may not appear.
- CSCsf28852—AP1510 mesh access points (MAPs) may become isolated when deployed in the European Telecommunications Standards Institute (ETSI) domain if the dynamic frequency selection (DFS) feature detects what it perceives to be radar signals, even if no radar is present. The MAPs stop using channels in which radar is thought to have been detected, quickly run out of usable channels, and are rendered unable to communicate with their root access point (RAP) and the controller.
- CSCsf28859—In a Hot Standby Routing Protocol (HSRP)/link aggregation (LAG) setup, the ap-manager communicates with the access point through the physical interface of the primary device to which the access point is connected. When the access point loses connectivity, the ap-manager attempts to reach the access point over the primary route, instead of the secondary route. Eventually, the access point re-registers with the controller over the secondary path.
- CSCsg00178—When peer-to-peer blocking is enabled, traffic from one client to another client is forwarded on the controller DS port. However, the controller still performs proxy ARP for the client, and packets from the first client to the second client are addressed to the second client's MAC address, which prevents client-to-client communication.
- CSCsg01470—Access point impersonation traps do not include the source MAC address.

- CSCsg10170—A controller using link aggregation (LAG) may reboot after you delete an untagged interface.
- CSCsg11232—Unexpected Layer 2 traffic causes the access point to stop accepting incoming packets. As a result, the access point and controller cannot exchange LWAPP echo traffic, and the access point disconnects.
- CSCsg11758—Canadian 1510 mesh access points with an -N domain setting do not enable 802.11b/g radios with a CA country code in release 4.0.179.8.
- CSCsg14327—When a 1000 series access point is connected to a power-over-Ethernet switch that supports Cisco Discovery Protocol (CDP), such as a 3560 Catalyst switch, it draws 8 watts of power rather than the 10 watts that the access point is documented as requiring or the 15.4 watts that it negotiates when using the 802.3af standard.
- CSCsg15901—4400 series controllers may lock up, causing them to disconnect from the network.
- CSCsg18356—The image becomes corrupted when you clear the configuration (using Option 5, Clear Config from the boot menu) on 2006 controllers running software release 3.2.78.0, 3.2.116.21, 3.2.150.6, 3.2.150.10, 3.2.171.5, 3.2.171.6, 4.0.155.5, 4.0.179.8, 4.0.179.11, 4.0.206.0, or later. When you clear the configuration, the eeprom.dat file (which holds the serial number, MAC address, and other manufacturing information) does not get backed up and is deleted. Without this file, the controller cannot boot up and must be returned to Cisco through the RMA process. To prevent this from occurring, download the _ER.aes image that is posted on the Software Download page of Cisco.com to your 2006 controller, using the same procedure that you would to download a controller software release image.

Caution Do not choose Option 5 from the boot menu unless you have successfully upgraded to the _ER.aes image on Cisco.com.

- CSCsg18453—When you apply changes on the 802.11b > Client Roaming page, the changes appear on the 802.11a pages although they have been correctly applied to the 802.11b parameters.
- CSCsg21262—When a mesh access point (MAP) has a wired Ethernet connection to the controller, a data path loop is created for backhaul traffic, which ultimately causes all MAP traffic to drop.
- CSCsg22915—When the Ethernet Multicast Mode parameter is set to Multicast, the multicast address configured on the controller (which is the IP address of the group that the access points will join) is also used for the multicast stream address. As a result, multicast packets from mobile clients with this group address are not dropped at the controller. Therefore, the configured multicast address and the address used by multicast streams should be different, and the controller will drop any packets matching the configured address to prevent them from being encapsulated within LWAPP.
- CSCsg29848—The controller allows you to create interfaces with overlapping IP address ranges.
- CSCsg36361—Controllers sometimes lock up when a SpectraLink phone associates to an access point.
- CSCsg44506—When an idle-timeout event occurs on an access point in REAP mode, the client's PS state is cleared before a deauthentication or disassociation message is sent. As a result, clients in sleep mode are not aware that they have been deleted by the controller and access point.
- CSCsg45847—A customized web logo fails to appear on the Preview Page for internal web authentication/passthrough after the logo has been transferred to the controller using TFTP.
- CSCsg48059—The client counts may be inaccurate after you enable hybrid REAP on the controller.

- CSCsg50343—Access points with management frame protection (MFP) enabled may send management frames either without an MFP information element (IE) or with an IE that has a corrupted signature. As a result, MFP alerts are generated on other controllers in the mobility group.
- CSCsg50596—Conditional web redirect does not work with external web authentication.
- CSCsg83671—Controllers sometimes fail to transfer a crash file from an access point to a TFTP server.
- CSCsg54483—When an AP1510 mesh access point (MAP) loses its connection to the root access point (RAP), the MAP may join another MAP or RAP without the same shared secret key.
- CSCsg59589—This caveat is included in Cisco Security Response "Multiple vulnerabilities in OpenSSL library" published at http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20061108-openssl.
- CSCsg67615—Although the 3750G Integrated Wireless LAN Controller does not support Cisco Discovery Protocol (CDP), CDP CLI commands are available for this controller.
- CSCsg71469—When the AP1210 is in the Alert state, it may send deauthentication frames to rogue access points.
- CSCsg71919—The controller was accepting invalid RSSI values. With the resolution in software release 4.0.206.0, the controller now rejects any RSSI values greater than 0.
- CSCsg72758—The AP1010 may generate a reboot if the tNetTask software fails.
- CSCsg82854—The heatmap client count may show an incorrect number of clients when the access point is using hybrid REAP.
- CSCsg89868—The controller GUI displays incorrect web pages for lobby ambassador users when the username is stored in a RADIUS server database. The GUI shows the read-only interface instead of the lobby ambassador interface.
- CSCsg90140—The controller reboots unexpectedly when you perform these steps:
  1. Under Wireless, click **Detail** on an access point in H-REAP mode.
  2. Select **VLAN Support** under H-REAP Configuration.
  3. Click **Apply**.
  4. When the access point rejoins the controller, click **Detail** for the access point.
  5. Click **VLAN Mappings** under H-REAP Configuration. The controller reboots.
- CSCsh04731—If you attempt to switch SSIDs by choosing a new SSID and clicking **Connect** from the Microsoft Wireless Configuration Manager, the client becomes stuck trying to connect to the new SSID.
- CSCsh12897—Mesh access points (MAPs) process radar events on all channels, which results in a repeated error message from the stranded MAP and prevents the MAP from joining the controller.
- CSCsh13158—Mesh access points (MAPs) fail to join the controller when dynamic frequency selection (DFS) events are set manually on all channels.

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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

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

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.