Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 3.2.193.5

February 16, 2007

These release notes describe open and resolved caveats for operating system release 3.2.193.5 for Cisco 2000, 4100, and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSM); Cisco Wireless LAN Controller Network Modules; and Cisco Aironet 1000, 1130, 1200, 1240, and 1500 Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (Cisco 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:

- Operating system software release 3.2.193.5 for all Cisco controllers and lightweight access points
- Cisco Wireless Control System (WCS) software release 4.0.66.0, 4.0.81.0, 4.0.87.0, or 4.0.96.0
- Location appliance software release 2.1.34.0, 2.1.39.0, or 2.1.42.0
- Cisco 2700 Series Location Appliances
- Cisco 2000, 4100, and 4400 Series Wireless LAN Controllers
- Cisco Wireless Service Module (WiSM) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers
- Cisco Aironet 1000, 1130, 1200, 1240, and 1500 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 web authentication.

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.

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

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 latest version of the *Cisco Wireless LAN Controller Configuration Guide.* 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

Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain

The Japanese government has changed its 5-GHz radio spectrum regulations. These regulations allow a field upgrade of 802.11a 5-GHz radios. Japan allows three frequency sets:

- J52 = 34 (5170 MHz), 38 (5190 MHz), 42 (5210 MHz), 46 (5230 MHz)
- W52 = 36 (5180 MHz), 40 (5200 MHz), 44 (5220 MHz), 48 (5240 MHz)
- W53 = 52 (5260 MHz), 56 (5280 MHz), 60 (5300 MHz), 64 (5320 MHz)

Cisco has organized these frequency sets into the following regulatory domains:

- -J regulatory domain = J52
- -P regulatory domain = W52 + W53
- -U regulatory domain = W52

Regulatory domains are used by Cisco to organize the legal frequencies of the world into logical groups. For example, most of the European countries are included in the -E regulatory domain. Cisco access points are configured for a specific regulatory domain at the factory and, with the exception of this migration process, never change. The regulatory domain is assigned per radio, so an access point's 802.11a and 802.11b/g radios may be assigned to different domains.

Note Controllers and access points may not operate properly if they are not designed for use in your country of operation. For example, an access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Australia. Always be sure to purchase controllers and access points that match your country's regulatory domain.

The Japanese regulations allow the regulatory domain that is programmed into an access point's radio to be migrated from the -J domain to the -U domain. These regulations only affect the 802.11a 5-GHz radios. New access points for the Japanese market contain radios that are configured for the -P regulatory domain. -J radios are no longer being sold. In order to make sure that your existing -J radios work together with the new -P radios in one network, you need to migrate your -J radios to the -U domain.

Country codes, as explained in the previous section, define the channels that can be used legally in each country. These country codes are available for Japan:

- JP—Allows only -J 802.11a radios to join the controller
- J2—Allows only -P 802.11a radios to join the controller
- J3—Uses the -U frequencies but allows both -U and -P 802.11a radios to join the controller

  Note After migration, you need to use the J3 country code.

Refer to the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* document for the list of channels and power levels supported by access points in the Japanese regulatory domains.

Guidelines for Migration

Follow these guidelines before migrating your access points to the -U regulatory domain:

- Your controller and all access points must be running software release 3.2.193.5 or a later release of the 3.2 software.

  Note If you migrate your access points using software release 3.2.193.5, you cannot upgrade to software release 4.0. You can upgrade only to software release 4.1 or greater or to a later release of the 3.2 software.

- You must have had one of the Japan country codes (JP, J2, or J3) configured on your controller at the time you last booted your controller.

- Some access points were shipped with an “undefined” regulatory domain. These access points always act as a -J regulatory domain when in Japan. After they are migrated, they are assigned a -U regulatory domain.
- You must have at least one access point with a -J regulatory domain or an “undefined” regulatory doamin joined to your controller.
- You cannot migrate your access points from the -U regulatory domain back to the -J domain. The Japanese government has made reverse migration illegal.

Note You cannot undo an access point migration.

Migrating Access Points to the -U Regulatory Domain

Follow these steps to migrate your access points from the -J regulatory domain to the -U regulatory domain using the controller CLI. This process cannot be performed using the controller GUI.

Step 1 To determine which access points in your network are eligible for migration, enter this command:

show ap migrate

Information similar to the following appears:

```
(Controller) >show ap migrate
AP Name AP Model Ethernet MAC Serial Num. RegDom
------------------ ------------------- ----------------- ----------- ------
ap1 AP1030 00:0b:85:5b:8e:c0 WCN093800CJ -J
ap2 AP1030 00:0b:85:5b:8e:c2 WCN093802CJ Undef.
ap3 AP1030 00:0b:85:5b:8e:c4 WCN093804CJ -U
ap4 AP1030 00:0b:85:5b:8e:c6 WCN093806CJ -P
```

Step 2 Enter these commands to disable the 802.11a and 802.11b/g networks:

config 802.11a disable network

config 802.11b disable network

Step 3 Enter this command to change the country code of the access points to be migrated to J3:

config country J3

Step 4 Enter this command to migrate the access points from the -J regulatory domain to the -U regulatory domain:

config ap migrate j52w52 {**all** | *ap_name*}

Information similar to the following appears:

```
(Controller) >config ap migrate j52W52 all
Migrate APs with 802.11A Radios in the "J" Regulatory Domain to the "U" Regulatory Domain.
The "J" domain allows J52 frequencies, the "U" domain allows W52 frequencies.
WARNING: This migration is permanent and is not reversible, as required by law.
WARNING: Once migrated the 802.11A radios will not operate with previous OS versions.
WARNING: All attached "J" radios will be migrated.
WARNING: All migrated APs will reboot.
WARNING: All migrated APs must be promptly reported to the manufacturer.
These APs are eligible for migration:
AP Name AP Model Ethernet MAC Serial Num. RegDom

------------------ ------------------- ----------------- ----------- ------

ap1 AP1030 00:0b:85:5b:8e:c0 WCN093800CJ -J
```

```
ap2 AP1030 00:0b:85:5b:8e:c2 WCN093802CJ Undef.
Begin to migrate Access Points from "J"(J52) to "U"(W52). Are you sure? (y/n) y
```

Step 5 Wait for completion, then use "show ap migrate" to verify migration for all APsEnter **Y** when prompted to confirm your decision to migrate.

Step 6 Wait for all access points to reboot and rejoin the controller. This process may take up to 15 minutes.

Step 7 Enter this command to verify migration for all access points:

show ap migrate

Information similar to the following appears:

```
(Controller) >show ap migrate
AP Name AP Model Ethernet MAC Serial Num. RegDom
------------------ ------------------- ----------------- ----------- ------
ap1 AP1030 00:0b:85:5b:8e:c0 WCN093800CJ -U
ap2 AP1030 00:0b:85:5b:8e:c2 WCN093802CJ -U
ap3 AP1030 00:0b:85:5b:8e:c4 WCN093804CJ -U
ap4 AP1030 00:0b:85:5b:8e:c6 WCN093806CJ -P
```

Step 8 Enter these commands to re-enable the 802.11a and 802.11b/g networks:

config 802.11a enable network

config 802.11b enable network

Step 9 Report the result of your migration to your manufacturer.

Installation Notes

This section contains important information to keep in mind when installing your 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 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 access 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, and a 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 your 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.

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, cchoose **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** at 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 19 for more details.

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).

Access Points Fail to Join Controllers If MTU Setting Is Less Than 1500

When the network path between access points and the controller is configured for an MTU size less than 1500, the controller does not receive join requests from access points in local mode. (MTU settings less than 1500 are common when you use tunneling protocols such as IPsec VPN, GRE, and MPLS.) The access point join request is larger than 1500 bytes, so the request is fragmented. The size of the first fragment is 1500 bytes (including IP and UDP header) and the second fragment is 54 bytes (including IP and UDP header).

Access points in REAP mode are not affected by this limitation, and the problem is resolved in the 4.0 release train because the LWAPP tunnel can reassemble up to 4 fragments. The problem occurs when all four of these conditions exist on your network:

- Your controller runs release 3.2 or earlier
- Your controller is configured for Layer 3 LWAPP
- The network path MTU between the access point and the controller is less than 1500 bytes
- The access point is in local access point (LAP) mode (not REAP mode)

Workarounds

Use one of these workarounds to resolve the problem on your network:

- Upgrade to controller software release 4.0 if the controller platform supports it.
- Use 1030 series access points in REAP mode for locations reachable through low-MTU paths.
- Increase the network path MTU to 1500 bytes.

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 commit 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.

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**.

FIPS 140-2

The Cisco 4400 Series Controllers are on the NIST FIPS 140-2 Pre-Validation List.

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).

Voice WLAN Configuration

Cisco recommends that load balancing always be turned off in any wireless LAN 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.

Inter-Subnet Roaming

Currently, multicast traffic cannot be passed during inter-subnet roaming.

Operating Mesh Networks Through Switches and Routers

In mesh networks that operate through low-speed switches and routers, access points can disconnect from the controller, causing the controller to generate alerts.

Heavily Loaded Controller CPU

When the controller CPU is heavily loaded (for example, when doing file copies or other tasks), it does not have time to process all of the ACKs that the NPU sends in response to configuration messages. When this happens, the CPU generates error messages. However, the error messages do not impact service or functionality.

RADIUS Servers and the Management VLAN

The RADIUS server can be on any subnet as long as it can be reached by the management VLAN subnet.

The controllers can be managed via the management VLAN subnet from any other subnet that can reach the management VLAN subnet.

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 on a per-controller basis. 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 it 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 802.11a 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.
- The 7920 phones and the controllers do not currently use compatible fast roaming mechanisms. The phone uses CCKM while the controllers use proactive key caching (PKC). To minimize roaming latency, static WEP is the recommended security mechanism.
- 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.

Client Channel Changes

Cisco access points are known to go off channel for up to 30 seconds while identifying rogue access point threats. This activity can cause occasional dropped client connections.

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/or client is 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.

Maximum MAC Filter Entries

The controller database can contain up to 2048 MAC filter entries for local netusers. The default value is 512. To support up to 2048 entries, you must enter this command in the controller CLI:

config database size *MAC_filter_entry*

where *MAC_filter_entry* is a value from 512 to 2048.

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.

RADIUS Servers

This product has been tested with the following RADIUS servers:

- CiscoSecure ACS v3.2
- Funk Odyssey Client v1.1 and 2.0
- Funk Steel-Belted RADIUS release 4.71.739 and 5.03 Enterprise Edition
- Microsoft Internet Authentication Service (IAS) release 5.2.3790.1830 on Windows 2003 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.

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 Auth Login with IE 5.x

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

Ad-Hoc Rogue Containment

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

RLDP Enable/Disable

The RLDP protocol detects rogues on your wired network. When RLDP is enabled, the controller reports a threat alarm for each rogue detected on the wired network. When RLDP is disabled, rogues detected on the wired network are shown in the Alert state.

Disabling RLDP stops the controller from detecting rogues on the wired network. Rogues can be manually contained by changing the status of the detected rogues. When rogues are being contained, you must manually disable containment for each rogue individually.

Apple iBook

Some Apple operating systems require shared key authentication for WEP. Other releases of the operating system do not work with shared key WEP unless the client saves the key in its key ring. How you should configure your controller is based on the client mix you expect to use. Cisco recommends testing these configurations before deployment.

Features Not Supported on 2000 Series Controllers

These hardware features are not supported on 2000 series controllers:

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

These software features are not supported on 2000 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

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 Any Network Device to a Dynamic Interface IP Address Is Not Supported

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.

Cisco Lightweight Access Points Fail to Join Cisco Controllers

When a Cisco lightweight access point is connected to a terminal server port and reboots because of a join failure or timeout, this sequence repeats until the access point returns to the boot prompt and remains there. This condition occurs when there is no telnet session to the access point’s console port and when the controller is not responding to the access point’s join response.

Workaround: Disconnect the access point’s console port from the terminal server. Reprogram the controller to have it respond to the access point’s join request. Power cycle the access point to force a restart.

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 resolved and open caveats for Cisco controllers and lightweight access points.

Resolved Caveats

These caveats are resolved in software release 3.2.193.5.

- CSCsc12222—The certificate presented for an HTTPS session should be unique with respect to the issuer and serial number.
- CSCsc14045—VPN passthrough should not be able to combine with web policy.
- CSCsc37945—Daylight savings checkbox removed.
- CSCsc92240—When you use WCS to create a VLAN, you must use lower-case letters to delete the interface.
- CSCsc98897—SecureCRT ends the SSHv2 session after accepting server certificate.
- CSCsd52292—NEC controller does not accept an upper-case MAC address from the WCS template.
- CSCsd65251—Session-timeout value for 802.1x corrected on GUI.
- CSCsd82363—WCS channel utilization incorrectly reported in radio utilization reports.
- CSCsd85126—Access point reboots at taskId = 0x80fb3a30.
- CSCse11202—WCS logs incorrect WEP key error when wireless clients run TKIP.
- CSCse14889—No Ad-Hoc rogue traps generated by controller.
- CSCse18855—RADIUS accounting cannot be disable on individual WLAN.
- CSCse30696—Controller sometimes shows both old and new IP addresses for an access point.

- CSCse43755—Controller accepts client associations to access points even when the AP-manager interface is not configured on the controller.
- CSCse49339—A 1030 access point in bridge mode, set to regulatory domain KR, fails to join a 2000 series controller.
- CSCse50111—An active controller port sometimes fails when traffic is pumped from a wireless client to a wired client.
- CSCse52733—Controller reboots during code downloading.
- CSCse53024—Command *maxUserLogin* restricts all types of authenticated users.
- CSCse55173—Valid clients show up in rogue client list.
- CSCse56114—Controller forwards BPDU packets out the gigabit interface when it should not.
- CSCse68631—Unexpected channel is shown on Monitor with J2 domain.
- CSCse73897—Layer 3 Support for fortress required.
- CSCse74680—VLAN statistics are not always updated on the Monitor > Controller Statistics page.
- CSCse84310—Warning message misspelled when regenerating webauth.
- CSCse84334—Preview button for external webauth page shows internal page.
- CSCse87066—Access points on other controllers in same mobility group appear as rogues.
- CSCse87074—When you enter the show run-config command on the controller CLI, the output for the command is truncated.
- CSCse89257—Access point logs are generated but no logs there in some situation
- CSCse90361—During upgrade from version 2.2 to 3.2 the network user setting is not checked.
- CSCse90894—Internet Explorer redirects to login page with webauth due to cache.
- CSCse91470—Config option to pad ARP requests.
- CSCse96745—Bogus alert pops up when configuring macfilter with an address in AP policy.
- CSCse97036—User can log into one controller and get access to another controller’s management GUI.
- CSCse98609—A 1030 REAP access point can corrupt client certificate.
- CSCsf00511—All access points show 0 down even when an access point is set to disabled.
- CSCsf08091—You cannot create more than 64 interfaces through the controller GUI.
- CSCsf08102—WCS might not report WLAN Override correctly.
- CSCsf11493—WiSM reboots unexpectedly.
- CSCsf15084—Containment of rogue adhocs yields generation of more adhoc rogues track.
- CSCsf16082—The session timeout setting does not take effect when you apply a WCS template to a controller.
- CSCsf16100—Access points are unable to join the WiSM controller.
- CSCsf16129—Controllers sometimes fail to reply to ARP requests.
- CSCsf21919—Controllers sometimes discover client devices through either the backup or the primary port.
- CSCsf26567—Memory leaks no longer caused by EAPOL packets.
- CSCsf26863—Web Authentication sometimes inconsistent with proxy server.
- CSCsf27479—WiSM locks up and does not generate crash file after reboot.

- CSCsf28859—The AP-manager interface sometimes does not communicate through the HSRP virtual interface properly.
- CSCsf30757—WiSM reboots at task *radiusTransportThread*.
- CSCsf30777—ETSI parameter for 11a incorrect for GR country code.
- CSCsg03501—Access points sometimes reboot because of an Assert in Software Task.
- CSCsg11232—Unexpected layer 2 traffic causes an access point to disconnect from the controller.
- CSCsg17504—WiSM controllers sometimes run at high CPU levels.
- 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.

- CSCsg22555—Access points disconnect from the controller after 120 hours because of decryption failure.
- CSCsg22914—Controllers in Catalyst 3750 switches sometimes reboot at the software task *ewsStringCopyIn+188*.
- CSCsg29848—Controllers allow you to create overlapping interfaces.
- CSCsg32155—Access points detect duplicate IP with frequency as distributed by DHCP.
- CSCsg36361—Spectralink phone association sometimes causes NPU to lock up.
- CSCsg44506—Idle timeout clears the PS state on REAP access points.
- CSCsg56052—Controllers sometimes do not state whether a rogue access point is on the wired network.
- CSCsg59589—Controllers have been upgraded from OpenSSL 0.9.7i to 0.9.7l.
- CSCsg61582—Active port does not reply to ARP request after recovery.
- CSCsg64385—Controller sends disconnect for inactivity incorrectly.
- CSCsg66987—Controller sometimes sends three EAP requests, causing PEAP authentication to fail.
- CSCsg71469—RLDP does not work correctly if the association response contains certain information elements.
- CSCsg74074—Controller sometimes provides inconsistent information on rogue clients and access points.
- CSCsg74450—Clients sometimes cannot get an IP address after a controller port completes fail-over.
- CSCsg78411—Web authentication intercepts on port 80 but not on port 8080.
- CSCsg81385—The controller does not return a tagged ARP reply from AP-manager2 interface.

- CSCsg84515—1000 series access points sometimes reboot.
- CSCsh00092—AIR-LAP1510AG-N-K9 is not supported in Taiwan.
- CSCsh06513—During upgrade from version 2.2 to 3.2, the radius configuration sometimes changes.
- CSCsh10841—The NPU sometimes locks up on controllers.
- CSCsh18721—The aggressive-failover feature is disabled by default after upgrade.
- CSCsh24245—Unable to apply IP, MAC, gateway or VLAN to dynamic interface.
- CSCsh27334—802.1x Mode has been changed to normal.
- CSCsh35306—Unicast ARP fails for export-foreign clients.
- CSCsh40807—After you reset an access point from the controller, the LED behavior changes on the access point.
- CSCsh42178—Access point transmit power sometimes differs from expected output.
- CSCsh44465—Power levels on access points sometimes change after software upgrade.
- CSCsh44486—Access point sometimes reboot when a client device is associated to the radio interface that you're configuring.
- CSCsh44502—Client can associate even when the client and access point country codes are different.
- CSCsh48977—The controller IP stack becomes inoperable on a large Layer 2 subnet .
- CSCsh49310—Clearing the configuration on a 2000 series controller sometimes corrupts the image
- CSCsh50527—NPU truncates padding from unicast ARP frames.
- CSCsh52643—The 802.11b radio in 1200 series access points sometimes display only the P regulatory domain.
- CSCsh71613—Access points sometimes reboot when you enter *show ap migrate*.

Open Caveats

These caveats are open in software release 3.2.193.5.

- CSCar14535—When configuring a mobility group anchor that is not part of the mobility member list, the controller displays an "Invalid Parameter Provided" error message.

  Workaround: Make sure that the anchor controller is a mobility group member.
- CSCsa95763—The controller GUI cannot display more than 80 local net users on the Security > AAA > Local Net Users page.

  Workaround: Use the controller CLI to view all the Local Net User entries.
- 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: This problem can cause some inconvenience, and the user may prefer to use the CLI configuration wizard instead to avoid it.

- 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.
- CSCsb07168—The AP1000 802.11a radio experiences a very low receive packet count when the receive RSSI is –75 dBm.

  Workaround: None at this time.
- CSCsb20269—On the 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.
- CSCsb34149—Disabling or deleting a wireless LAN on which a large number of clients exists may not result in all clients being deleted. This generally occurs when several thousand clients are using the wireless LAN.

  Workaround: Make sure that wireless LANs with a large number of clients associated are not deleted or disabled.
- CSCsb38486—The Cisco Aironet 1500 Series Lightweight Outdoor Access Point Bridge CLI does not accept 10-character bridge group names.

  Workaround: Use 9-character bridge group names.
- CSCsb52557—Cisco access points do not connect to the 4400 series controller if the time is not set first.

  Workaround: Set the time on the controller before allowing the access points to connect to the controller.
- CSCsb55597—The access point’s output power may change after you modify a mandatory data rate.

  Workaround: None at this time.
- CSCsb55937—VLAN-tagged large ICMP packets that need to be fragmented are not sent by Cisco Aironet 1000 series access points in direct-connection mode. Ping replies never come back when the access point sends requests to a gateway from a wireless client using large 1500-byte packets and with RADIUS override configured with any 1p tag.

  Workaround: None at this time.
- CSCsb71060—Internal LAG errors occur when the management interface is changed from tagged to untagged.

  Workaround: Leave the WiSM management interface as tagged or untagged.
- 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 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 for this release.

- CSCsc01221—When downstream test data is sent from the wired endpoint to four wireless clients at different priority levels (voice, video, background, and best effort), the Cisco Aironet 1000 series access points crash.

  Workaround: None for this release.

- CSCsc02741—In the bootloader mode, users are unable to exit or return to the main prompt. If users make mistakes while entering values, they cannot quit the step and are unable to go back and change existing values.

  Workaround: Reset the system through IOS or power the device off and on if necessary.

- CSCsc02860—When users download the code image to a 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.

- CSCsc03072—Cisco lightweight access points do not always produce complete logs.

  Workaround: None for this release.

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

  Workaround: None for this release.

- CSCsc22084—Error messages and traps are not triggered when a PoE controller with CDP causes Cisco Aironet 1200 series access points to disable their radios.

  Workaround: Disabling CDP resolves this issue.

- CSCsc22663—Deleting a mobility member mapped to a controller as an anchor removes the anchor's entry as well, but the Auto Anchor knob remains enabled even though only the mobility anchor mapping is deleted.

  Workaround: Before deleting a mobility member, first delete the controller to which it is mapped from the WLAN.

- CSCsc35784—The transmit power control adjustment levels 3, 4, and 5 are not supported on Cisco Aironet 1500 Series Lightweight Outdoor Access Points in the 5745-to-5825-MHz band. The transmit power control adjustment levels 4 and 5 are not supported on Cisco Aironet 1500 series access points that operate in the 5500-to-5700-MHz band and at 2.4 GHz.

  These levels correspond to -6, -9, and (in the case of 5500 to 5700 MHz) -12 dB from the maximum power, respectively. Power levels 1, 2, and (in the case of 5500 to 5700 MHz) 3 are supported, which correspond to maximum power for the particular data rate and channel, and -3 dB relative to this maximum, at which these adjustment levels provide little or no further reduction in transmit power output.

  Workaround: Set the transmit power level to either 1 or 2 for 5745 to 5825 MHz. Set the transmit power level to either 1, 2, or 3 for all other bands.

- CSCsc40648—Rooftop access points are displayed in the web interface as poletop access points for more than four minutes, which prevents them from being configured.

  Workaround: Configure the access point as a rooftop access point using the controller CLI.

- CSCsc41313—The Cisco Aironet 1500 Series Lightweight Outdoor Access Points are configured by default to allow old bridges. When this configuration is enabled, the shared secret key set on the controller is not passed to the access points, so a few access points might be running on the old key. If these access points reset or new access points are waiting to join the running network, they may take a very long time to connect to the network or might not join at all. The default value has been changed to not allow old bridges to authenticate.

Workaround: Configure the controller using this command: **config network allow-old-bridge-aps disable**.

- 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.

- CSCsc70484—Most IPSec VPN clients start using the new security association (SA) immediately upon rekeying. However, the Cisco VPN Client continues to use the old SA for some time before switching to the new one, which results in packet loss until the client switches over.

  Workaround: Use these WLAN settings on the controller to ensure that the client controls when the rekey process takes effect and the controller responds to the client for the phase 1 SA rekey:

  - Session Timeout: 0 seconds
  - Layer 3 Security: IPsec
  - IPsec Authentication: HMAC SHA1
  - IPsec Encryption: AES (If you choose 3DES, configure the IPsec lifetime to a value greater than the expected duration of the client session.)
  - IKE Phase 1: Aggressive
  - Lifetime: 43200 to 57600 seconds (12 to 16 hours)
  - IKE Diffie Hellman Group: Group 2 (1024 bits)

- CSCsc75351—The controller CLI command **debug mac addr** *client_mac_address*, which is designed to limit debug output to the specified client, is not filtering client traffic.

  Workaround: None at this time.

- CSCsc77157—Multiple 4100 series controllers may simultaneously reset without crash files or message log entries being generated.

  Workaround: None at this time.

- CSCsc92354—The Security > MAC Filtering page on the controller GUI shows MAC address filters in this format: XX:XX:XX:XX:XX:XX, which differs from the Cisco standard format of XXXX:XXXX:XXXX.

  Workaround: None at this time.

- CSCse92865—The session timeout value is not modified when issuing a CLI or WEP+802.1x WLAN GUI selection. The default value of 1800 seconds is retained.

  Workaround: None at this time.

- CSCsd04684—The 4100 series controller ports do not work when the Gateway Load Balancing Protocol (GLBP) is configured on the management interface VLAN.

  Workaround: Do not configure GLBP on the management interface VLAN. For redundancy, Hot Standby Router Protocol (HSRP) can be used on the management interface VLAN.

- CSCsd18462—The **transfer download tftppktTimeout ?** command uses the wrong tag.

  Workaround: None at this time.

- CSCsd25491—The management IP address of a controller incorrectly sends an ARP request for a client IP address on a WLAN subnet over the wired interface. The ARP request is not answered because the management IP address and the client WLAN are on different subnets.

  Workaround: None at this time.

- CSCsd33178—Duplicate IP detection is not working. The controller does not detect duplicate IPs in its setup, so the http service to the controller stops working after some time.

  Workaround: None at this time.

- CSCsd34555—If the access point is not in protection mode, the PC350 client adapter is unable to pass traffic.

  Workaround: None at this time.

- CSCsd38979—When you set the QoS WLAN parameter to Platinum (voice), Internet Control Message Protocol (ICMP) requests from the client are not being marked for voice.

  Workaround: None at this time.

- CSCsd39873—The controller may report a WEP key encryption error for Intel 2200BG clients operating with OEM driver version 9.0.1.9, 9.0.2.5, or 9.0.3.9 and using some form of EAP authentication (PEAP, LEAP, EAP-FAST, or EAP-TLS).

  Workaround: None at this time. However, the client will attempt to reauthenticate and upon successful EAPOL key exchanges will communicate in a normal, encrypted fashion.

- CSCsd44612—Multicast is failing when traffic is passed between two wireless clients on access points directly connected to 2006.

  Workaround: None at this time.

- CSCsd50369—When radio resource management (RRM) is enabled on the controller, an access point in monitor mode may not send an acknowledge packet in response to a reassociation request.

  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. After completing the setup wizard, reload the saved configuration from the TFTP server or WCS.

- CSCsd65307—When radio resource management (RRM) is enabled on the controller, 1000 series access points sometimes fail to send an acknowledge packet (or send the packet after a delay) in response to a reassociation request. As a result, a wired IP phone cannot call an N900iL handset until the handset resends a reassociation request to the access point.

  Workaround: None at this time.

- CSCsd67332—If you have Telnet enabled and then disable it, the change does not take effect until you reboot the Cisco WiSM.

  Workaround: None at this time.

- CSCsd69158—After a RADIUS session timeout expires, the access point does not send a unicast key to the client.

  Workaround: None at this time.

- CSCsd75245—The management packet for the UserIdleTimer is incorrect on access points in REAP mode.

  Workaround: None at this time.

- CSCsd83743—Authentication fails if you enter a RADIUS-server key with more than 31 characters on the ACS server and a 4400 series controller.

Workaround: Do not enter more than 31 characters for the RADIUS-server key.

- CSCsd93784—Setting the Channel/Power Update (RRM) parameter on WCS does not change the channel or power settings on the controller.

  Workaround: None at this time.

- CSCse02235—Access points occasionally delay the transmission of beacons by 0.1 or 0.2 seconds. This condition occurs when the access points do not have any associated clients.

  Workaround: None at this time.

- CSCse04495—The Cisco WiSM controller may become stuck in a strange state after it is powered down and back up.

  Workaround: Reset the controller.

- CSCse04713—The controller detects a rogue access point, but it may not acknowledge it as a “Rogue on Wired Network” access point on WCS.

  Workaround: You can try to resolve this problem by downgrading your controller software to a release prior to 3.2.78.0.

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

  Workaround: None at this time.

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

  Workaround: None at this time.

- CSCse06509—The 4400 series controller sends out an undersized frame when it connects to certain Catalyst switches (2970, 3560, or 3750).

  Workaround: None at this time.

- CSCse07836—An access point may experience a system restart after a fail over.

  Workaround: None at this time.

- CSCse08725—A Vocera badge running MS-PEAP fails when trying to associate to an AP1010. This problem occurs because the controller is dropping the packets.

  Workaround: None at this time.

- CSCse09235—UDP traffic drops in both directions when per-user bandwidth is set for real-time traffic.

  Workaround: None at this time.

- CSCse15932—The 4404 controller may reboot if the TimerTickTask software fails.

  Workaround: None at this time.

- CSCse17260—WPA clients may receive an error message indicating that the WEP key is configured incorrectly on the client.

  Workaround: None at this time.

- CSCse30452—After the secondary DHCP server provides an IP address to an access point, the access point shows “(tNetTask): arpresolve” and then reboots.

  Workaround: None at this time.

- CSCse30514—When an LWAPP-enabled AP1100 or AP1200 first connects to a controller, the secondary controller name on the All APs > Details page in the controller GUI is not blank. The output of the **show ap config general** command also shows that the secondary controller name is not blank.

Workaround: None at this time.

- CSCse32656—The 4402 controller supports an enhanced security module (ESM) card only in slot 1, not in slot 2. Slot 2 is reserved for 4404 controllers.

  Workaround: Use slot 1, which is the slot closest to the power outlet, for an ESM card in the 4402 controller.
- CSCse34481—Numerous system event messages are received when trying a TFTP download.

  Workaround: None at this time.
- CSCse40636—The foreign controller incorrectly forwards multicast traffic onto the auto-anchor WLAN.

  Workaround: Configure the WLAN on the foreign controller to map to an invalid VLAN.
- CSCse42329—WLC managemend IP does not ARP to HSRP virtual MAC.

  Workaround: None at this time.
- CSCse52143—IPSec authentication with certificates may not always operate properly.

  Workaround: None at this time.
- CSCse60689—The controller may reboot due to a failure with the sshpmAddIPv4IpsecRules software.

  Workaround: None at this time.
- CSCse61840—The debug messages stop after some time even if the debugs are enabled to collect data.

  Workaround: Disable all debugs with the **debug disable-all** command and then re-enable them.
- CSCse72413—The controller may reboot due to a failure with the debugMaintask software.

  Workaround: None at this time.
- CSCse80636—Under heavy traffic conditions, the VPN module may reach capacity and fail to accept additional packets.

  Workaround: None at this time.
- CSCse88067—An “aborting SA dump due to timeout” error message is received when entering **show ipsec brief** command on the 4012 controller console.

  Workaround: None at this time.
- CSCse95768—When a controller is in the A regulatory domain with local power constraint enabled, beacons are sent out. This broadcast should only be present with an E regulatory domain.

  Workaround: None at this time.
- CSCsf02388—The WLC port did not link up following a repeated cable removal or connection.

  Workaround: Power cycle the WLC.
- CSCsf04684—On the 4400, the FPGA and VPN module are losing some packets. The packet loss is a small percentage of total throughput.

  Workaround: None at this time.
- CSCsf10167—The controller may reboot due to a failure with the pemReceiveTask software watchdog.

  Workaround: None at this time.
- CSCsf11862—Controllers sometimes reboot during a software upgrade.

Workaround: Download the software image twice. On the second try, the controller successfully loads the new image.

- CSCsf14716—On release 3.2, data rate shift from 11M to 5.5M does not occur.

  Workaround: None at this time.

- CSCsf17520—With REAP AP connected to the controller, the first WLAN with WMM enabled on the controller does not get a client DHCP IP address.

  Workaround: You can disable the WMM from which the client gets the IP address.

- CSCsf17618—The reason and status code of the client is always zero whether the client is in probing, associated, or excluded state.

  Workaround: None at this time.

- CSCsf21931—The Cisco WiSM does not support Layer 2 LWAPP mode.

  Workaround: The option to configure Layer 2 LWAPP mode is available through both the controller GUI and CLI.

- CSCsf26816—A WLC crash occurred in NEC WL3036 while running the nPCSL_timer task.

  Workaround: None at this time.

- CSCsf27061—If you are configuring the AP group VLAN, all controller interfaces (CLI, web, and WCS) show the dynamic ap-manager interface in the interface-mapping-to-the-WLAN list. Because dynamic AP manager is not supposed to be mapped to a WLAN, it should not appear in the list.

  Workaround: None at this time.

- CSCsf27201—You may receive a “Multicast Rx queue is full” message in your msglog even if multicast is disabled and no multicast traffic exists.

  Workaround: None at this time.

- CSCsf28181—When two ct4400s are connected and security mobility is enabled, the client loses the current IP address from the dynamic interface during the handoff and gets a new IP address from the new controller.

  Workaround: None at this time.

- CSCsf28446—WLCs running 3.2.151.4 experience a system crash at pemReceiveTask.

  Workaround: None at this time.

- CSCsg09867—A WLC crash occurred in an NEC WL3036 due to TaskName:pemReceiveTask.

  Workaround: None at this time.

- CSCsg10391—When you use the **remote-debug enable** command on the controller CLI to enable remote debugging on an access point, debugging stops when your CLI session times out.

  Workaround: Open a new CLI session, disable remote debugging (enter **remote-debug disable**), and re-enable remote debugging.

- CSCsg13067—An access point loses association with the controller with repeated associations or when free system memory is decreased to 4MB or less. Log information is recorded.

  Workaround: None at this time.

- CSCsg32267—Even if you disable 1M and 2M 802.11b operational rates, data is transmitted from the access point at that rate.

  Workaround: None at this time.

- CSCsg45166—The voice quality is less than desirable when six FOMA clients are associated to an AP125x (NECl UNIVERGE WL2024/3006/3025). If the access point is in PEAP or LOCAL mode, the voice quality is poor, but if short preamble is disabled, the quality improves.

  Workaround: Disable short preamble.
- CSCsg56010—Some unnecessary access point images are not removed after an upgrade.

  Workaround: None at this time.
- CSCsg93477—On an AP1000, the username and password may be lost when upgrading 4.0.

  Workaround: None at this time.
- CSCsh05353—An error is returned when you attempt to display the Internal Webauth window. This error occurs when you go to Management > Web Login Page, ensure external webauth is not selected, and click **Preview**.

  Workaround: None at this time.
- CSCsh41347—The following warning appears when you enter dynamic interface details and click **Apply**:

  ```
  Changing the Interface parameters causes the WLANs to be temporarily disabled and thus
  may result in loss of connectivity for some clients.
  ```

  After accepting the warning message, the GUI does not apply the interface configuration. This warning occurs only on a ct4000 and ct2006.

  Workaround: None at this time.
- CSCsh44942—When an ipsec client roams from a 4400 to a 4000 controller, a crash occurs in apfReceiveTask, and a “crypto card not responding” message occurs.

  Workaround: None at this time.
- CSCsh45097—When associating a client to an ipsec WLAN on a 4000 locally, a “crypto card not responding” error message appears.

  Workaround: None at this time.
- CSCsh47792—With a Ct3500 and AP1200 in local mode, the AP1200 crashes within 10 to 15 minutes after RLDP is enabled on the controller.

  Workaround: None at this time.
- CSCsh47973—When the client idle timeout is expired and the client disassociates, the same disassociation packet sent by the access point to the client is repeated numerous times.

  Workaround: None at this time.
- CSCsh53198—When sending upstream traffic from the wireless client to the wired client, DSCP mapping is not working on an AP1130.

  Workaround: None at this time.
- CSCsh54674—The wrong default WLAN.1p value on platinum QoS profile displays.

  Workaround: None at this time.
- CSCsh55290—A foreign WLC sends an XID for STAs on the foreign controller when an STA in the foreign state does a DHCP release.

  Workaround: None at this time.
- CSCsh68089—Access points directly connected to the 2006 or 4000 WLC are unable to perform DHCP.

Workaround: Create and enable a DHCP scope on the internal DHCP server. The DHCP does not need to be legitimate.

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, at:

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.