



Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 3.2.150.10

July 18, 2006

These release notes describe new and changed information as well as open and resolved caveats for operating system release 3.2.150.10 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:

- [Cisco Unified Wireless Network Solution Components, page 2](#)
- [Controller Requirements, page 2](#)
- [Software Release Information, page 2](#)
- [New and Changed Information, page 3](#)
- [Installation Notes, page 5](#)
- [Important Notes, page 8](#)
- [Caveats, page 18](#)
- [Troubleshooting, page 32](#)
- [Related Documentation, page 32](#)
- [Obtaining Documentation, page 32](#)



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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Documentation Feedback, page 33](#)
- [Cisco Product Security Overview, page 33](#)
- [Obtaining Technical Assistance, page 34](#)
- [Obtaining Additional Publications and Information, page 36](#)

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 3.2.150.6 for all Cisco controllers and lightweight access points
- Cisco Wireless Control System (WCS) software release 3.2.64.0
- Location appliance software release 2.0.48.0
- 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 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.

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 software release 3.2.150.6, following the instructions in the *Cisco Wireless LAN Controller Configuration Guide, Release 3.2*. 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

Image Load Protection

When you download a new controller image, a check is performed to ensure that the image being loaded is meant for the current controller. If you attempt to install an incorrect image, the install aborts, and an error message appears.

Support for Per-WLAN ACLs

Controller software release 3.2.150.6 enables you to apply access control lists (ACLs) to WLANs rather than to just interfaces. ACLs are applied in the following order:

- Interface ACLs
- WLAN ACLs
- Client ACLs (from the AAA server)

You can apply an ACL to a WLAN only through the controller CLI. To do so, enter this command:

```
config wlan acl
```

Support for Reusable Static WEP Key Indices

Controller software release 3.2.150.6 enables you to configure the same static WEP key index for multiple WLANs. However, access points can accept only up to four static WEP keys, which may vary by access point.

Support for Ad-Hoc Rogue Reporting

Controller software release 3.2.150.6 supports a new CLI command that enables you to enable or disable ad-hoc rogue reporting:

```
config wps rogue-ap adhoc {enable | disable}
```

Power-over-Ethernet Parameters Added to Controller GUI

Controller software release 3.2.150.6 supports new power-over-Ethernet (PoE), also known as *inline power*, parameters for the AP1131 and the AP1242 in the controller GUI. To access these parameters, click **Wireless** and then the **Detail** link of the desired access point. The new parameters appear on the All APs > Details page under Power Over Ethernet Settings.

These parameters enable you to configure inline power and power injector settings for an AP1131 or AP1242:

- **Pre-Standard State**—Check this check box if the access point is being powered by a high-power Cisco switch. These switches provide more than the traditional 6 Watts of power but do not support the intelligent power management (IPM) feature. These switches include:
 - WS-C3550, WS-C3560, WS-C3750,
 - C1880,
 - 2600, 2610, 2611, 2621, 2650, 2651,
 - 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691,
 - 2811, 2821, 2851,
 - 3620, 3631-telco, 3640, 3660,
 - 3725, 3745,
 - 3825, and 3845.

Do not check this check box if power is being provided by a power injector or by a switch not on this list.

- **Power Injector State**—Check this check box to enable the power injector state for an access point. This parameter is required if the attached switch does not support IPM and a power injector is being used. This parameter is not required if the attached switch supports IPM.
- **Power Injector Selection**—This parameter enables you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed. It appears if you check the Power Injector State check box above. Choose one of these options from the drop-down box to specify the desired level of protection:
 - **Installed**—This option examines and remembers the MAC address of the currently connected switch port and assumes that a power injector is connected. Choose this option if your network contains older Cisco 6-Watt switches and you want to avoid possible overloads by forcing a double-check of any relocated access points.

**Note**

Each time an access point is relocated, the MAC address of the new switch port will fail to match the remembered MAC address, and the access point will remain in low-power mode. You must then physically verify the existence of a power injector and reselect this option to cause the new MAC address to be remembered.

- **Override**—This option allows the access point to operate in high-power mode without first verifying a matching MAC address. It is acceptable to use this option if your network does not contain any older Cisco 6-Watt switches that could be overloaded if connected directly to a 12-Watt access point. The advantage of this option is that if you relocate the access point, it continues to operate in high-power mode without any further configuration. The disadvantage of this option is that if the access point is connected directly to a 6-Watt switch, an overload will occur.
- **Foreign**—This option causes the Injector Switch MAC Address parameter to appear. The Injector Switch MAC Address parameter allows the remembered MAC address to be modified by hand. Choose this option if you know the MAC address of the connected switch port and do not wish to automatically detect it using the Installed option.

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.

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.

IPSec and L2TP Not Supported

Software release 3.2.150.6 does not support IPSec or L2TP. If you upgrade to this release from a previous release that supported IPSec and L2TP, any WLANs that are configured for these features become disabled. If you want to use IPSec or L2TP, you must use a version of controller software prior to 3.2 or wait for a future release.

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 802.11 a/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)
```


WCP is the protocol running between the Cisco Catalyst 6500 Series Switch Supervisor and the WiSM. The supervisor uses WCP to monitor the health of the WiSM. If you enter the **show wism status** command or see a WiSM down trap on WCS, make sure that the WiSM service port and the supervisor are configured correctly. WCP can fail because of an incorrect configuration.

- CSCsb46260—A client connected to one of the controllers in a mobility group is shown as a rogue on the other controllers, but the access point is not shown in the rogue access point list. If a client is listed on the rogue client list, then the access point to which it is connected should be reported as a rogue access point.
- CSCsb53746—A 350 or CB20A client running ACU 6.5 or 6.4 and configured for LEAP authentication with WPA encryption can authenticate to a lightweight access point but does not receive an IP address. This problem does not affect clients running ACU 6.3, which does not use WMM data frames. To check for this problem, enter the following command on the controller:

debug dot1x events enable

In the body of the trace that follows authentication by an affected client, the following messages appear:

```
Fri Jun 3 07:29:59 2005: Received EAPOL-Key from mobile xx:xx:xx:xx:xx:xx
```

```
Fri Jun 3 07:29:59 2005: Received EAPOL-key message with invalid version number from mobile
xx:xx:xx:xx:xx:xx
```

- CSCsb90622—AP impersonation alarms sometimes flood WCS.
- CSCsb91943—The web authentication login window does not appear when external web authentication has been configured on a 2000 series controller. This problem occurs because the controller forwards all http and https traffic to the CPU prior to authentication, thereby breaking the external web authentication mechanism.
- CSCsc12310—Aggressive load balancing is not performed for clients that do not send ACE information elements (IEs) if fast roaming is enabled.
- CSCsc17827—For Cisco Aironet 1500 Series Lightweight Outdoor Access Points and Cisco Aironet 1030 Remote Edge Lightweight Access Points, channel 165 for the 802.11a radio is only available for the -A SKU when the country code is set to USX. Channel 165 is not available for the -N SKU for any of the countries that use this SKU.
- CSCsc36050—A client associates to a controller running 802.1x + WEP on the first attempt. However, the client fails a second association attempt to this controller because the controller does not send an EAP request to the client. After removing the client information, the client is once again able to associate.
- CSCsc68105—Web authentication DNS queries are sent over the management interface instead of the dynamic interface to which the WLAN is assigned.
- CSCsc74740—A client fails to join a web-authentication WLAN with an anchor controller after a reboot.
- CSCsc76306—Access points running in REAP mode restart when their associated clients become disassociated.
- CSCsc80266—The controller may crash due to a problem with the radio resource management (RRM) logging function.
- CSCsc84681—SNMP version 1 and version 2 may stop responding.
- CSCsc84971—The access point sends two DHCP discover messages on bootup instead of a DHCP request.

- CSCsc86705—The controller may crash when configured for Cranite Layer 2 security. This problem occurs due to raw IP packets in a Cranite-passthrough-enabled WLAN.
- CSCsc96640—When a clustered firewall is used as the default gateway for wireless clients, web authentication does not work.
- CSCsd03934—When an access point uses a power injector to join the controller, the controller may log erroneous power injector errors after the access point reboots.
- CSCsd13731—The configuration wizard does not allow you to configure the AP-manager interface with a subnet of 192.168.1.x/24 if the same subnet is already configured on the management interface.
- CSCsd19752—If a controller is configured for Layer 3 mode and subsequently Layer 2 mode, a client that attempts to associate does not move to the Run state if its IP address is the same as that of the AP-manager interface. Although the IP address is not being configured correctly for the client, the controller sends a DHCP acknowledgment, so the client assumes that it has obtained an IP address. This problem has been resolved such that in Layer 2 mode the IP address comparison does not include the AP-manager interface, and the controller does not send a DHCP acknowledgment if the IP address configuration fails.
- CSCsd19776—When clients are MAC authenticated, the calling station ID changes to the access point's MAC address rather than the client's MAC address.
- CSCsd22087—Intel 2200 b/g clients cannot pass traffic with an AP1000 when connected in 802.11g mode. This condition lasts for 5 to 60 seconds and then recovers, but it can occur quite frequently.
- CSCsd26260—A 4100 controller configured for intrusion detection system (IDS) may crash when connected to access points in monitor mode.
- CSCsd29699—The NPU may occasionally have invalid crypto handles (set to 0), which causes the traffic to stop flowing for that client.
- CSCsd32317—Attempting to enter a long custom web message from the CLI on a 2006 or 4404 controller causes the controller to crash and reboot.
- CSCsd32384—Defining several DHCP servers may result in duplicate leases for a single client.
- CSCsd35492—The client exclusion feature does not operate correctly when aek keywrap is configured.
- CSCsd36689—Access points in monitor mode do not detect probing clients. These access points do not track the clients' RSSI values and do not contribute location information to the Location Appliance.
- CSCsd39937—An access point may crash due to an invalid cache index.
- CSCsd40065—If you set a certain time zone (such as JST) on your controller, you may notice that the real time shown on your controller jumps ahead after a reboot.
- CSCsd40853—The 2.4-GHz Singapore regulatory settings for the AP1000 are incorrect. The Allowed EIRP value should be 20 dBm (rather than 19 dBm), and channel 14 is not allowed to be used in Singapore.
- CSCsd41360—An 802.11g client cannot associate to a controller if 802.11g is disabled on the WLAN or globally.
- CSCsd41602—The controller software stops and is reset by the reaper if the Task "pemReceiveTask" misses the software watchdog.
- CSCsd43744—A deleted SNMP community string may intermittently reappear after the controller reboots.

- CSCsd45993—An access point may crash after running for some time due to an assertion failure at the MAC_RXDP register.
- CSCsd47454—If the 802.11b/g data rate settings on the controller are set to 11 Mbps mandatory; 6 and/or 9 Mbps mandatory; and 1, 2, and 5.5 Mbps disabled; then the 802.11b/g radio in the AP1240 fails with a traceback and ceases to transmit.
- CSCsd47657—Controllers running software release 3.2.78 may not display the entire output of the **show run-config** command in the controller CLI.
- CSCsd48466—Unless the WMM policy is set to Allowed or Required on the WLAN, the AP1200 does not set the DSCP value in the outer LWAPP header for packets that it forwards to the controller. As a result, the controller cannot set the 1p tag on upstream packets.
- CSCsd48507—A Linksys WET54G Client Bridge cannot associate using WPA-PSK because the controller drops the association request from the bridge.
- CSCsd49026—The 2006 controller may stop responding unexpectedly. When this happens, the controller fails to answer https, console CLI, and ping requests.
- CSCsd50608—An access point may restart unexpectedly after associating to a different controller.
- CSCsd52888—An AP 10xx does not process gratuitous ARPs for the default gateway. The access point's LWAPP code caches the MAC address of the default router and uses this address when forwarding LWAPP control and data frames. It does not, however, update this address when receiving a gratuitous ARP from the default router. As a result, if the MAC address of the default router changes, the access point disconnects from its controller.
- CSCsd52912—UDP packets travel in only one direction during mobility. This problem occurs because the controller NPU is not correctly forwarding traffic between a foreign controller and an anchor controller.
- CSCsd54356—An LWAPP-enabled IOS access point does not process gratuitous ARPs for the default gateway. The LWAPP code caches the MAC address of the default router and uses this address when forwarding LWAPP control and data frames. It does not, however, update this address when receiving a gratuitous ARP from the default router. As a result, if the MAC address of the default router changes, the access point disconnects from its controller.
- CSCsd54797—The controller may fail to detect or prevent ARP attacks from clients.
- CSCsd56729—The 4402 controller drops out-of-order LWAPP fragments. When an EAP-TLS client sends packets to an access point, the access point produces LWAPP fragmented packets and sends them to the controller. The controller reassembles the packets if it receives them in order but drops out-of-order fragments.
- CSCsd60364—The AP1000 restarts after disconnecting from the controller and attempting to obtain a DHCP IP address. This issue has been resolved by preventing the AP1000 from restarting after reaching the maximum number of DHCP retries.
- CSCsd61943—When multiple RADIUS servers are configured for access point authorization and the first one is unreachable, the controller does not failover to the second RADIUS server.
- CSCsd67747—An access point that is associated to a controller may restart unexpectedly.
- CSCsd70230—The AP10xx flash may become corrupted due to a missing checksum error check in the LWAPP configuration.
- CSCsd76586—When the controller and the access point are on different subnets, the access point does not send an LWAPP discovery request to the first controller in the mobility group.
- CSCsd81238—The AP1000 drops packets due to a driver issue that controls antenna diversity.

- CSCsd94390—When two controllers with link aggregation (LAG) and multicast forwarding enabled share an interface on the same subnet, a multicast storm ensues that eventually takes down the network.
- CSCsd98255—After a Layer 3 roam from an anchor controller to a foreign controller, the client cannot renew its DHCP IP address. This problem occurs because the foreign controller is not receiving the DHCP information from the anchor controller.
- CSCsd99572—Capabilities are not validated consistently in association requests. As a result, some clients can communicate with access points in local mode but not in REAP mode.
- CSCse04508—External web authentication does not operate properly. A wireless client using web authentication with DHCP must do a release/renew to logon. This issue occurs if the user associates to the guest SSID, obtains a DHCP IP address, and fails to open the web browser for 15 minutes or more.
- CSCse13886—If you change an SSID from an authentication method that requires encryption to open authentication, unicast traffic is unencrypted, but multicast traffic from the access point remains encrypted.
- CSCse15233—LWAPP-enabled access points take a long time to fail over to a backup controller when the primary controller fails.
- CSCse15753—WCS may lock up when you add a controller with mobility anchors configured. This problem occurs because the controller returns mobility anchors in the order in which they were added rather than in numerical order. Eventually this problem can deplete java virtual memory, thereby leaving WCS unable to perform any functions.

Open Caveats

These caveats are open in software releases 3.2.150.10 and 3.2.150.6.

- 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.
- CSCsa89818—PDAs are unable to associate with Cisco Aironet 1030 Remote Edge Lightweight Access Points in REAP mode although local mode works correctly.
Workaround: None at this time.
- 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.
- CSCsb48197—Multiple authentication requests to the WCS server.
Workaround: None in this release.
- 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. This condition exists for 4400 series controllers using direct-connect mode, with RADIUS override enabled, the override parameter set to 1p with any VLAN number, and Cisco Aironet 1000 series access points.
Workaround: None at this time.
- CSCsb59898—Cisco Aironet 1030 Remote Edge Lightweight Access Points in REAP mode do not support roaming when configured with a WLAN that is set up for WPA security.
Workaround: None for this release.
- 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.
- CSCsb76389—Cannot failover to second instance IP address or port on a RADIUS server.
Workaround: None for this release.

- 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.
- CSCsb85582—Cisco 4100 series controllers crash at PES_rqst_exec_again.
Workaround: None for this release.
- 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.
Workaround: Be sure to properly configure WLAN ID 1.
- 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.
- CSCsc03644—Cisco lightweight access points do not retain location parameters after a reboot.
Workaround: None for this release.
- CSCsc05495—Controllers intermittently send a state attribute 24 in an access-request packet.
Workaround: Apply the Microsoft KB 883659 patch to IAS. The Microsoft patch may or may not work. There is no workaround on the controller.
- 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.
- CSCsc14045—VPN passthrough should not be able to be combined with web policy.
Workaround: Do not assign VPN passthrough along with web policy.
- CSCsc15699—In Cisco Aironet 1000 series access points, the WMM IE (11) is correct, but the QBSS client cac limit (11) is still in its old place.
Workaround: None for this release.

- CSCsc20416—ACU site survey disassociates other clients in the LWAPP environment.
Workaround: Under investigation.
- CSCsc21196—Asymmetrical data rate with 802.11a radio on 4012 and 4024 controllers.
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.
- CSCsc26796—The WiSM web interface does not show the correct access point SNMP operator status (Registered versus Down).
Workaround: Use WCS to view the correct values.
- CSCsc28035—After three or four days, the Wireless Control Protocol (WCP) times out, and the state of the Cisco WiSM goes down and then up.
Workaround: None at this time.
- CSCsc28571—Task 181 (do_linktest) is taking 4265111% of the CPU.
Workaround: None for this release.
- CSCsc34060—IPSec clients enter the run state but do not communicate.
Workaround: None for this release.
- 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.
- CSCsc38093—Wireless clients experience poor performance when associated to a 4400 series controller.
Workaround: Under investigation.
- 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**.

- CSCsc44326—A 4400 series controller running software release 3.1.105.0 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.

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

router(config)#arp 10.1.1.1 0000.0102.abcd arpa

where 10.1.1.1 is the ap-manager<n> interface's IP address, and 0000.0102.abcd is its MAC address.

- CSCsc61004—Poletop access points (PAPs) may not be able to move from one rooftop access point (RAP) to another if the first RAP goes down. This problem usually occurs if the RAPs are configured statically at "rooftop" and the PAPs are configured at "poletop."

Workaround: Configure Auto mode on all RAPs and PAPs.

- 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.

- CSCsc72899—An access point in REAP mode crashes if packets are being processed in the access point by one task while discovery is occurring.

Workaround: None at this time.

- 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.

- CSCsc98897—The SecureCRT application cannot open an SSH session on the controller.

Workaround: Use PuTTY, the SSH client on Windows, or SSH in Linux.

- 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.

- CSCsd06075—A 4100 series controller may crash periodically for unknown reasons. After power cycling the system, some of the access points do not reassociate to the controller.
Workaround: Reboot the controller.
- CSCsd14546—A 4402 controller's link status indicators and port summary show the ports as being up and active even when an SFP gigabit interface converter (GBIC) is not installed.
Workaround: Maintain a text copy of the configuration and manually input the configuration in the event of an RMA or replacement.
- CSCsd18145—If you disable proxy ARP on the controller, the ARPs still go to the controller CPU.
Workaround: None at this time.
- CSCsd19781—If the AP manager interface is tagged, all multicast packets go out untagged. As a result, these packets may be dropped if the Layer 2 switch between the access point and the controller is configured to drop all untagged traffic.
Workaround: None at this time.
- CSCsd19801—A 4000 series controller sometimes hangs while it is booting up.
Workaround: Turn the controller off and on.
- 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.
- CSCsd27529—Static WEP does not operate properly for a REAP access point in standalone mode.
Workaround: None at this time.
- CSCsd34555—The PC350 client adapter is unable to pass traffic when the access point is not in protection mode.
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 exchange will communicate in a normal, encrypted fashion.
- CSCsd50227—When you enter **config voip 802.11bg dot11-retries all 0** on the controller CLI, the access point sends RTP retries three times.
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.
- CSCsd52292—The controller does not accept uppercase MAC addresses from the WCS templates.
Workaround: Do not use uppercase characters for MAC addresses in the WCS templates.

- 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.
- CSCsd54712—An access point may reboot when it is connected to a 2000 series controller and an N900iL handset associated to the access point tries to place a call after the user idle timeout setting has expired.
Workaround: None at this time.
- CSCsd55009—The access point may suddenly lose its connection to the controller. When this condition occurs, the access point periodically sends out DHCP requests, and the access point Alarm LED lights.
Workaround: Turn the access point off and back on.
- CSCsd56111—The 802.11 authentication response timeout uses the value configured by the **config advanced timers auth-timeout** command only when wireless clients first try to associate. After that, the controller always uses the default value of 10 seconds.
Workaround: None at this time.
- CSCsd59421—A wireless client fails to authenticate using 802.1x when the access point is on a different VLAN from the controller.
Workaround: Configure the access point for the same VLAN as the controller.
- CSCsd59700—The default AP1000/1200 settings for external antenna gain are incorrect. The 4000/4100 controller should show this value as “0” but instead shows it as “11.”
Workaround: None at this time.
- CSCsd63888—When access points migrate from a failed 2000 series controller configured as the primary controller to a 2000 series controller configured as the secondary controller, the secondary controller sometimes restarts unexpectedly.
Workaround: None at this time.
- 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.
- CSCsd76868—When you enable the Rogue Location Discovery Protocol (RLDP) to detect rogues but do not create WLAN ID 1, the controller reports minor alarms when critical alarms should be reported.
Workaround: Configure WLAN ID 1 on your controller when you enable RLDP.

- 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.
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.
- CSCsd85859—The Refresh button does not operate properly on some of the controller GUI pages.
Workaround: None at this time.
- CSCsd87382—Bridging functionality for REAP devices is not available on OEM builds of controller software.
Workaround: None at this time.
- CSCsd88939—When you enter the **config 802.11b fast-roaming** command, a REAP access point in standalone mode fails to send “Subelement: 4 WLAN Capabilities” in beacon and probe responses.
Workaround: None at this time.
- CSCsd90392—The idle timeout may not work correctly for an access point in REAP mode.
Workaround: None at this time.
- CSCsd90994—Some configuration settings may be lost after upgrading the controller.
Workaround: None at this time.
- CSCsd91042—An access point may experience a crash when no clients are associated to it.
Workaround: None at this time.
- CSCsd93784—Setting the Channel/Power Update (RRM) parameter on the WCS does not change the channel or power settings on the controller.
Workaround: None at this time.
- 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.
Workaround: None at this time.
- CSCsd99725—An access point restarts when you change its mode of operation from urgent mode to REAP mode.
Workaround: None at this time.
- CSCse01133—IPSec clients using XAuth authentication do not pass traffic.
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.
- CSCse06339—The **show inventory** command may display an incorrect machine model for the 4402 controller.
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.
- CSCse08879—External web authentication fails to operate after upgrading the controller software from 2.2.127.9 to 3.1 or 3.2.
Workaround: Follow these guidelines:
 - For 4xxx controllers, add the external web server to the list of external server IP addresses using this command: **config custom-web ext-webserver add *server-ip-address***. Then remove the preauthentication ACL configuration for the web authentication WLAN.
 - For 2006 controllers, make sure that the preauthentication ACL is configured properly.
- CSCse09235—UDP traffic drops in both directions when per-user bandwidth is set for real-time traffic.
Workaround: None at this time.
- CSCse14889—The controller does not generate traps for ad-hoc rogues.
Workaround: None at this time.
- CSCse15889—The controller may reboot after running for many days due to a failure with the sshpmReceiveTask software watchdog.
Workaround: None at this time.
- CSCse15932—The 4404 controller may crash if the TimerTickTask software fails.
Workaround: None at this time.
- CSCse17260—WPA clients may receive an error message indicating that the WEP key may be configured incorrectly on the client.
Workaround: None at this time.
- 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.
Workaround: Create a fictitious RADIUS accounting server and assign it to the WLAN for which RADIUS accounting is not required.

- CSCse25208—If you are running software release 2.2.162.x on the controller and enter the **clear config** command for access points, all LEDs on the access points turn off.
Workaround: None at this time.
- CSCse26437—After a communication breakdown occurs between a controller and an access point, the access point does not send a subsequent request to join the controller.
Workaround: None at this time.
- CSCse28278—When the client occasionally sends a reassociation request to the access point during roaming, the access point acknowledges the request but fails to send a reassociation response.
Workaround: None at this time.
- CSCse29193—The controller marks a RADIUS server as dead if a single request is not responded to after five retries and switches to a backup server.
Workaround: None at this time.
- CSCse29686—After you upgrade from software release 3.2.78 to 3.2.116.21 or later, clients experience packet loss and a significant number of packet retransmissions on the AP1000. This condition is related to the antenna setting of the access point.
Workaround: Set the antenna to “external” to restore performance.
- CSCse30397—If you enter 24 characters for the username and password during the initial controller configuration, the “Routine system resource notification” error message may appear repeatedly.
Workaround: Reboot the controller and do not enter 24 characters for the username and password.
- 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.
- CSCse30696—The controller does not refresh the access point’s IP address correctly when the admin status for that access point is disabled.
Workaround: None at this time.
- CSCse31547—The wrong WEP key may be used when a client attempts to associate to a particular WLAN in a multi-WLAN environment.
Workaround: None at this time.
- CSCse33667—A controller running software release 3.2.116 with ssh disabled may crash without a crash dump.
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.

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.

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*

You can access these documents from this link:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006 Cisco Systems, Inc. All rights reserved.