



Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.0.155.5

July 18, 2006

These release notes describe new features as well as open and resolved caveats for software release 4.0.155.5 for Cisco 2000 and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSM); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; and Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.



Note

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

Contents

These release notes contain the following sections.

- [Cisco Unified Wireless Network Solution Components, page 2](#)
- [Controller Requirements, page 2](#)
- [Software Release Information, page 3](#)
- [New Features, page 4](#)
- [Installation Notes, page 6](#)
- [Important Notes, page 8](#)
- [Caveats, page 18](#)
- [Troubleshooting, page 27](#)
- [Related Documentation, page 27](#)
- [Obtaining Documentation, page 27](#)



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 28](#)
- [Cisco Product Security Overview, page 28](#)
- [Obtaining Technical Assistance, page 29](#)
- [Obtaining Additional Publications and Information, page 31](#)

Cisco Unified Wireless Network Solution Components

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

- Software release 4.0.155.0 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 2.0
- Cisco Wireless Control System (WCS) software release 4.0
- Location appliance software release 2.1
- Cisco 2700 Series Location Appliances
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 Series Lightweight Access Points

Controller Requirements

The controller graphical user interface (GUI) requires the following operating system and web browser:

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

**Note**

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

Software Release Information

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



Note

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



Note

To use the controller in the Catalyst 3750G Wireless LAN Controller Switch, the switch must be running Cisco IOS Release 12.2.25.FZ or 12.2(25)SEE.

Finding the Software Release

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

Upgrading to a New Software Release

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



Caution

Do not power down the controller or any access point during this process; otherwise, you might corrupt the software image! Upgrading a controller with a large number of access points can take as long as 30 minutes. 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 4.0.155.5, following the instructions in the *Cisco Wireless LAN Controller Configuration Guide, Release 4.0*. Click this link to browse to that document:
http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html
4. Re-enable your 802.11a and 802.11b networks.



Note

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

New Features

The following new features are available in controller software release 4.0.155.0:

- Cisco Catalyst 3750G Integrated Wireless LAN Controller—Integrates controller functionality into stackable Catalyst 3750G Series Switches.
- Cisco unified intrusion detection system (IDS)/intrusion prevention system (IPS)
- IDS Event correlation—Automatically eliminates duplicate alerts for rogue access points, rogue clients, and IDS signatures when two or more access points detect the same attacker.
- Management frame protection—Provides for the authentication of 802.11 management frames by the wireless network infrastructure.
- DHCP server IP addresses for access points—Allows controllers to provide IP addresses to access points that are on the same subnet as the controller.
- EoIP ping support for mobility group members—May be used to validate connectivity between members of a mobility group, including guest controllers.
- DHCP relay option 82 support (access point MAC, SSID)
- Cisco Compatible Extensions (CCX) version 4—For more details, visit www.cisco.com/go/ciscocompatible/wireless
- Wi-Fi multimedia (WMM) call admission control (CAC)—Supports an optional element of WMM.
- Unscheduled automatic power save delivery—Extends the battery life of mobile clients and reduces the latency of traffic flow over the wireless media.
- VoWLAN metrics—Provide diagnostic information pertinent to VoIP performance on the wireless LAN and aids in determining whether problems are being introduced by the wireless LAN or the wired network.
- Guest access custom login screen—Permits administrators to upload an HTML image file to the controller that replaces the default web authentication page that guests traditionally see when logging into a controller-based guest network.
- Guest access lobby ambassador—Allows for the creation of local usernames and passwords and for local or RADIUS-based authentication of guest users.
- Access control list (ACL) enhancements
- Hybrid remote edge access point (REAP)—Allows the Cisco Aironet 1240AG and 1130AG Series Access Points to be deployed remotely from the controller.
- Unique device identifier (UDI) support—Provides the capability to uniquely identify controllers and lightweight access points.
- Regulatory domain updates—Expand the use of the Cisco UWN Solution in European Union countries and offer additional channel support in China, Singapore, Mexico, Australia, and Hong Kong.
- Wireless mesh user-configurable bridge distance—Bridge distance capabilities are expanded beyond 2 miles.
- Increased scalability of wireless mesh access points—Controllers now support a greater number of wireless mesh access points, simplifying management of large-scale mesh deployments.

- Pre-stage configuration for LWAPP-enabled access points—Simplifies the deployment of LWAPP-enabled access points in remote locations by adding a new set of access point CLI commands to the recovery IOS image. The static IP address, netmask, default gateway, and primary controller IP address may now be configured on the IOS access point. Configuring the primary controller IP address helps the access point to discover and register a specific controller over the WAN links. In a deployment scenario where a DHCP server is not available in remote locations, the access point CLI commands may be used to configure the static IP address and the initial controller information.
- LWAPP for Cisco Aironet 1100 Series Access Points (802.11g radio only)—Allows the Cisco Aironet 1100 Series Access Point to be upgraded from autonomous access point mode to lightweight mode using the autonomous to lightweight mode upgrade tool.



Note You must install software release 4.0.155.0 on the controller before connecting 1100 series access points to the controller.

- LWAPP for Cisco Aironet 1300 Series Access Points (access point mode only)—Allows the Cisco Aironet 1300 Series Access Point to be upgraded from autonomous access point mode to lightweight mode using the autonomous to lightweight mode upgrade tool.



Note You must install software release 4.0.155.0 on the controller before connecting 1300 series access points to the controller.

- Autonomous to lightweight mode upgrade tool enhancements—Provide reliable upgrades on WAN links operating at 128 kbps or more and is capable of simultaneously upgrading four access points.
- 4.9-GHz support for wireless mesh—Available only to licensed public safety agencies in the U.S.
- Wireless mesh optimal parent selection—Enhances the Adaptive Wireless Path Protocol (AWPP) by enabling mesh access points to scan available backhaul channels to listen for the neighboring access point's path ease information and improves the automatic formation of the mesh network, helping to ensure optimal network capacity.
- Bridge group enhancements—Allow new wireless mesh access points to be introduced with zero-touch configuration into an existing wireless mesh network with a configured bridge group name, thereby simplifying deployment.
- Wireless mesh exclusion listing—Improves the convergence time of the mesh network.
- Cisco Aironet power-over-Ethernet (PoE) command enhancements—Provide support for enhanced PoE commands and the flashing LED command on access points.

Refer to the following location for more information:

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

Installation Notes

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

Warnings



Warning

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



Warning

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



Warning

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



Warning

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



Warning

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



Warning

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



Warning

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



Warning

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



Warning

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

**Warning**

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

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

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

7. If any part of an antenna system should come in contact with a power line, **do not touch it or try to remove it yourself. Call your local power company.** They will remove it safely.
8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

Refer to the appropriate Quick Start Guide or Hardware Installation Guide for instructions on installing controllers and access points.



Note

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

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

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

Important Notes

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

Connecting 1100 and 1300 Series Access Points

You must install software release 4.0.155.0 on the controller before connecting 1100 and 1300 series access points to the controller.

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

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

Preventing Clients from Accessing the Management Network on a Controller

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

Voice Wireless LAN Configuration

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

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.

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 they should associate with another access point. Use the following instructions 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.
- Both the 7920 phones and the controllers support Cisco Centralized Key Management (CCKM) fast roaming.
- When configuring WEP, there is a difference in nomenclature for the controller and the 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7920.

Changing the IOS LWAPP Access Point Password

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

```
config ap username user_id password password {AP_name | all}
```

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

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

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

```
“ERROR!!! Command is disabled.”
```

For more information, refer to [Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode](#).

Exclusion List (Blacklist) Client Feature

If a client is not able to connect to an access point and the security policy for the WLAN and/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.

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.

IPSec Not Supported

Software release 4.0.155.0 does not support IPSec. If you upgrade to this release from a previous release that supported IPSec, any WLANs that are configured for this feature become disabled. If you want to use IPSec, you must use a version of controller software prior to 3.2 or wait for a future release.

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

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

Lightweight Access Point Connection Limitations

Cisco Aironet lightweight access points do not connect to the 4400 series controller if the time is not set first. Set the time on the controller before allowing the access points to connect to it.

RADIUS Servers

This product has been tested with the following RADIUS servers:

- CiscoSecure ACS 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 Authentication 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.

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.

Ad-Hoc Rogue Containment

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

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.

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.



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

Using the GUI to Change the SNMP v3 User Default Values

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

- Step 1** Click **Management** and then **SNMP V3 Users** under **SNMP**.
- Step 2** If “default” appears in the User Name column, click **Remove** to delete this SNMP v3 user.
- Step 3** Click **New** to add a new SNMP v3 user.
- Step 4** When the SNMP V3 Users > New page appears, enter a unique name in the User Profile Name field. Do not enter “default.”
- Step 5** In the remaining fields, choose **Read Only** or **Read Write** to specify the access level for this user, choose the authentication and privacy protocols to be used, and enter a password for each.
- Step 6** Click **Apply** to commit your changes.
- Step 7** Click **Save Configuration** to save your settings.

Using the CLI to Change the SNMP v3 User Default Values

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

- Step 1** To see the current list of SNMP v3 users for this controller, enter this command:
show snmpv3user
- Step 2** If “default” appears in the SNMP v3 User Name column, enter this command to delete this user:
config snmp v3user delete *username*
The *username* parameter is the SNMP v3 username (in this case, “default”).

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

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

where

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

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

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

Web Authentication Limits on Hybrid-REAP Access Points

Access points in hybrid-REAP mode support web authentication with open authentication only if local switching is enabled on the WLAN.

Features Not Supported on 2000 Series Controllers

These hardware features are not supported on 2000 series controllers:

- Power over Ethernet (PoE)
- 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 a Network Device to a Controller Dynamic Interface

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

2006 Image Not Supported for 3504 Controllers

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

Running a 3504 Image on a 2000 Series Controller

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

Upgrading External Web Authentication

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

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

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



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

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

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

```
function submitAction(){
    var link = document.location.href;
    var searchString = "redirect=";
    var equalIndex = link.indexOf(searchString);
    var redirectUrl = "";
```

```

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

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

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

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

}

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

```

```

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

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

<tr align="center">

<td colspan="2"> User Name &nbsp;&nbsp;&nbsp;&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;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="Password" name="password"
SIZE="25" MAXLENGTH="24"> </td> </tr>

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

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

```

Caveats

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

Open Caveats in Software Release 4.0.155.5

- CSCse68633—Controllers in hybrid-REAP standalone mode support new WPA-PSK clients using only TKIP (not AES) and new WPA2-PSK clients using only AES (not TKIP).

Workaround: Be sure to use WPA-PSK TKIP clients and WPA2-PSK AES clients.

- CSCse73315—When the controller is upgraded from 3.2.150.10 to 4.0.155.5, any access point group VLAN configuration may be lost.

Workaround: Save your configuration before upgrading the controller software and restore it if you experience any configuration loss.

Open Caveats in Software Release 4.0.155.0

- 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.

- 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.
- CSCsb20269—On the Cisco WiSM, when the service VLAN is configured as one of the VLANs on a data port, it does not operate correctly.
Workaround: Do not configure the service VLAN as one of the VLANs on a data port.
- CSCsb77595—When logging out from Telnet/SSH sessions, the session always prompts the user to save changes, even when no changes have been made.
Workaround: Ignore the prompt and exit as usual.
- CSCsb85113—When users download the code image to the Cisco WiSM using the CLI, associated access points are sometimes disconnected.
Workaround: Download new code images to the WiSM at times when there are no clients to be affected.
- 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.
- CSCsc02860—When users download the code image to a Cisco WiSM for the first time, the WiSM fails to download the new image to flash memory.
Workaround: Download new code images to the WiSM a second time.
- CSCsc03644—Cisco lightweight access points do not retain location parameters after a reboot.
Workaround: None at this time.
- CSCsc04907—Resetting the access point to factory defaults does not clear the static IP address.
Workaround: Clear the access point’s static IP address by hand.
- 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 at this time.
- CSCsc20416—ACU site survey disassociates other clients in the LWAPP environment.
Workaround: None at this time.
- CSCsc65354—IDS is unable to detect a deauthentication flood attack under certain conditions.
Workaround: None at this time.

- CSCsc68154—The controller’s error log repeatedly displays the “Got an idle-timeout message from an unknown client” error message for some unknown reason.
Workaround: None at this time.
- CSCsd02837—The CB21AG client adapter may not send re-association requests with CCKM keys when roaming between controllers.
Workaround: Use a different client adapter.
- 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.
- CSCsd47199—A session timeout of zero (infinity) may not operate as configured.
Workaround: Set the session timeout to 65535 seconds.
- 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: Reset the controller to factory defaults and then reconfigure the controller exactly the same way.
- CSCsd54750—The Cisco WiSM may display numerous timeout messages.
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.
- CSCsd69158—After a RADIUS session timeout expires, the access point does not send a unicast key to the client.
Workaround: None at this time.
- 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.
- CSCsd85126—The access point may reboot unexpectedly after upgrading to software release 3.2.116.21.
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.
- CSCsd89139—Pocket PC devices may fail PEAP authentication through a 4400 series controller after resuming from standby.
Workaround: None at this time.

- CSCsd91042—An access point may reboot when no clients are associated to it.
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.
- CSCsd96189—A CB21AG client adapter running on Windows XP SP2 experiences two ping timeouts when roaming from an AP1030 to an AP1242, when each is associated to a different 2006 controller.
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.
- CSCse10109—For WMM clients without TSPEC support, ACM must be disabled for proper QoS mapping.
Workaround: Disable ACM for WMM clients without TSPEC support.
- CSCse14889—The controller does not generate traps for ad-hoc rogues.
Workaround: None at this time.
- CSCse15326—Inconsistent file sizes may occur during configuration backups.
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 may be configured incorrectly on the client.
Workaround: None at this time.
- CSCse26358—The controller reboots if you enable local switching on any WLAN from 9 through 16.
Workaround: Enable local switching on a WLAN other than 9 through 16.
- CSCse31241—The backhaul transmit power level cannot be changed for a mesh access point.
Workaround: None at this time.
- CSCse31271—The 4.9-GHz band cannot be changed on the -P regulatory domain if public-safety is disabled.
Workaround: To change the 4.9-GHz band on the -P regulatory domain, enter this command using the controller CLI: **config ap public-safety enable *Cisco_AP***.

- CSCse34673—If you globally disable and then globally enable management frame protection (MFP) on a controller that is part of a mobility group and connected to LWAPP-enabled access points, the access points that are connected to the other controllers within the mobility group may report sequence number MFP anomalies.
Workaround: None at this time.
- CSCse48181—The stateless DHCP proxy on the controller does not properly support DHCP on centrally switched WLANs for access points in H-REAP mode.
Workaround: Use the default DHCP configuration on the controller. In the default configuration, the DHCP server address appears on client devices as 1.1.1.1.
- CSCse68633—Controllers in hybrid-REAP standalone mode support new WPA-PSK clients using only TKIP (not AES) and new WPA2-PSK clients using only AES (not TKIP).
Workaround: Be sure to use WPA-PSK TKIP clients and WPA2-PSK AES clients.

Resolved Caveats in Software Release 4.0.155.5

- CSCsd23638—LWAPP-enabled access points are able to join a controller running software release 4.0.155.0 but are unable to download the image.
- CSCsd34445—An AP1230 joined to a controller may show periodic trace backs, indicating a leak in IO memory.
- CSCse58195—When you upgrade from controller software release 3.0.x.x to 3.2.x.x or 4.0.x.x, any access control lists (ACLs) that were previously configured or applied to interfaces are removed or disabled.
- CSCse60203—Cisco Aironet 1100 and 1200 series access points sometimes fail to upgrade from release 3.2.150.6 to release 4.0.
- CSCse64027—LWAPP-enabled IOS access points joined to a controller running software release 3.2.150.6 or 4.0.155.0 may disconnect and reconnect every 120 hours when the access point's heartbeat timer is set to the default value of 30 seconds. When the heartbeat timer is set to a smaller value (such as 10 seconds), the disconnect occurs more frequently (such as every 40 hours). While the access point is disconnected from the controller, clients are unable to associate to this access point.
- CSCse77682—The controller may reboot if an Inter-Access Point Protocol (IAPP) packet with a corrupted SSID field is sent to an access point joined to the controller.

Resolved Caveats in Software Release 4.0.155.0

- CSCar10047—Access point channel surfing causes repeated client disconnects.
- CSCar12371—The controller database can contain up to 2048 MAC filter entries for local netusers.
- CSCar15063—In the same mobility group, access points appear as rogues.
- CSCeh68636—802.3af power management with a legacy Ethernet switch needs to be improved.
- CSCek16101—The Controller Network Module does not get the correct time from the NTP server for 1 hour if it fails initially.
- CSCsa95763—The controller GUI is limited to displaying only 80 local net users on the Security > AAA > Local Net Users page.
- CSCsb13548—Cisco lightweight access points may frequently reset.

- CSCsb38486—The Cisco Aironet 1500 Series Lightweight Outdoor Access Point Bridge CLI does not accept 10-character bridge group names.
- CSCsb39522—When a user changes the setting from a static IP address to DHCP and the DHCP IP address is not available, the supervisor loses keepalive, and the Cisco WiSM sends a WCP going down trap. Similarly, when a user changes a static IP address and enters an incorrect subnet on the service port, the supervisor detects a loss of WCP keepalive, and the WiSM sends a WCP going down trap.
- CSCsb43906—When the backhaul is overloaded with 18-Mbps downstream data, the PAP resets.
- CSCsb48765—When the controller CPU is heavily loaded (for example, when doing file copies or other tasks), it does not have time to process all the ACKs that the NPU sends in response to configuration messages. When this happens, the CPU generates error messages.
- CSCsb53746—A 350 or CB20A client running ACU 6.4 or 6.5 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 WME data frames.
- 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.
- CSCsb63749—A client on the anchor controller cannot ping a client on the foreign controller.
- CSCsb76419—The client state appears on two switches in a Layer 2 roaming environment. Fixes include 1) a memory leak fix when an associated response deliver failure notification is received from the access point and 2) the access point no longer measuring other access points as interference.
- CSCsb78835—The controllers are not sending all rogue trap information to the WCS.
- CSCsb88424—Cisco Aironet 1030 Remote Edge Lightweight Access Points in REAP mode may reboot continuously.
- CSCsb90622—AP impersonation alarms sometimes flood the 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.
- CSCsb97559—The candidate list returned by the controller in association/reassociation responses may have an access point that the client cannot reach as the top-most entry.
- CSCsc06090—Some systems with a large number of access points and controllers may experience slow performance when rogue access point policy is enabled.
- CSCsc12222—Controller HTTPS certificates should be unique with respect to the issuer and serial number.
- CSCsc15385—CCX-compliant clients may lose connectivity while roaming.
- 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.
- CSCsc22084—No error message or trap is triggered when a PoE controller with CDP causes Cisco Aironet 1200 Series Lightweight Access Points to disable their radios.

- CSCsc22663—Deleting a mobility member mapped to a controller as an anchor removes the anchor's entry as well, but the auto-anchor feature remains enabled even though only the mobility anchor mapping is deleted.
- CSCsc33769—Radio resource management (RRM) does not correctly set the transmit power on Cisco Aironet 1000 Series Lightweight Access Points.
- CSCsc34060—IPSec clients enter the run state but do not communicate.
- CSCsc35784—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. Transmit power control adjustment levels 4 and 5 are not supported on 1500 series access points that operate in the 5500-to-5700-MHz band and at 2.4 GHz. These issues were resolved by removing unsupported power adjustment levels.
- CSCsc40648—Rooftop access points are displayed in the GUI as pole-top access points for more than 4 minutes, which does not allow them to be configured.
- 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.
- CSCsc42773—LWAPP-enabled AP1130s and AP1200s may shut down their radio interfaces due to insufficient power from the power over Ethernet (PoE).
- CSCsc42923—A 32-character SSID does not allow lightweight access points to join controllers.
- CSCsc43587—The controllers crash in the apfReceiveTask software.
- CSCsc44897—The WCS shows an incorrect antenna orientation while viewing an object.
- CSCsc46598—When performing a lightweight access point placement preplanning site survey, some items may show up in the wrong position in the placement diagram, and various items in the printed site survey document may be incorrect.
- CSCsc47951—The controller reboots because the mmListen task missed the software watchdog.
- CSCsc49148—The 2006 controller reboots because of a stack corruption of the apfRogueTask.
- CSCsc51291—An EAP ID request is sent to a client even when it is not connected on a WLAN with WEP or WPA security.
- CSCsc53452—When a WCS user attempts to retrieve the association history of a client that was formerly associated to a replaced lightweight access point, the association history cannot be retrieved. The WCS shows an error message with the MAC address of the replaced access point indicating that it cannot be located.
- CSCsc54020—Two new guest access features need to be added: web authentication customization with page and image downloads to the controller and guest access accounts with a lifetime associated to them.
- CSCsc59377—Access points fail to join the controller with sustained high CPU utilization (~97%).
- CSCsc63217—AP1000 LEDs are disabled by default.
- CSCsc68105—On the 4400 series controllers, web authentication DNS queries are sent from the management interface instead of the dynamic interface to which the WLAN is assigned.
- CSCsc70407—The controller stops accepting new IPSec authentications.
- CSCsc72027—Radios remain in reset due to insufficient power over Ethernet (PoE), even if a power injector is being used.

- CSCsc72479—The access point configuration cannot be cleared if the access point's name contains spaces.
- CSCsc72899—An access point in REAP mode reboots if packets are being processed in the access point by one task while discovery is occurring.
- CSCsc76782—The access point cannot properly handle frames on the power-save queue.
- CSCsc80754—The Location field on the All APs > Details page defaults to default_location after the access point reboots.
- CSCsc82863—HP laptops with Intel embedded client adapters may reboot when connecting to an LWAPP-enabled AP1230 or AP1130 using PEAP authentication.
- CSCsc85671—The MAC filter on the controller GUI does not change after clicking the Apply button.
- CSCsc85775—Changing the management IP address on a 4404 controller causes the controller to reload.
- CSCsc86705—The controller may reboot while using Cranite security.
- CSCsc86727—Setting any access point parameter using WCS causes an SNMP exception error.
- CSCsc87698—The access point reboots when multiple clients are connected on a WLAN with any encryption other than TKIP.
- CSCsc91461—The controller cannot bring up the 802.11g radio interface.
- CSCsc93617—The lack of a MAC address during SSH delete leads to an eventual crash.
- CSCsc94879—A 1200 series access point continues to send RTP packets to the CP-7920 after the CP-7920 sends a deauthentication packet to the access point.
- CSCsc96640—Web authentication does not operate properly with a clustered firewall as the client's default gateway.
- CSCsc97687—Slow roam times may occur due to WPA-PSK failures.
- CSCsc98586—Backup port functionality does not operate properly when configured for management and dynamic ports.
- CSCsd01495—CKIP support is needed on the controller for LWAPP-enabled access points.
- CSCsd02525—With the 802.11a network disabled, if the access point is reset, it comes back up and sends a change state event to the controller indicating that its 802.11a radio is operational, if the PoE power detection takes some time to complete.
- CSCsd02579—The RRM transmit power control threshold needs to be configurable.
- CSCsd02586—The client pem policy rule ID initializes incorrectly.
- CSCsd03083—Association request processing generates excess logs when the SSID is invalid.
- CSCsd03939—Enabling or disabling the 802.11g network may cause a lightweight access point to reboot.
- CSCsd04657—The primary controller sends an LWAPP discovery response even when it is maxed out.
- CSCsd09768—An AP1000 gets stuck in DHCP discovery after a link failure.
- CSCsd09898—Sometimes the NPU has crypto handles that are invalid.
- CSCsd11774—LWAPP-enabled access points do not send the second fragment of a large packet.
- CSCsd14113—The controller sends delayed access requests to the RADIUS server.
- CSCsd18195—After an access point falls back to the original controller, the client traffic fails.

- CSCsd21147—NPU ARP filters are not being properly deleted.
- CSCsd21248—A memory leak occurs in hapi buffer pool 0.
- CSCsd22087—The Intel 2200 b/g client cannot pass traffic with an AP1000 using 802.11g.
- CSCsd30983—Support needs to be added for per-WLAN ACLs.
- CSCsd32317—Entering custom web messages from the controller CLI causes the controller to reboot.
- CSCsd32642—The maximum retry count from the controller is misinterpreted.
- CSCsd37198—Support needs to be added for reusable static-WEP key indices.
- CSCsd40853—The AP1000 2.4-GHz Singapore regulatory settings are incorrect.
- CSCsd41360—The controller does not pass traffic to 802.11g clients if 802.11g is disabled.
- CSCsd41602—The controller reboots due to a pemReceiveTask missed software watchdog.
- CSCsd43744—A deleted SNMP community string reappears after the controller reboots.
- CSCsd44941—The 802.11g radio in an AP1130 or AP1240 loses connectivity with clients.
- CSCsd47657—An incomplete output displays when the **show run-config** command is entered using the controller CLI.
- CSCsd48507—A Linksys WET54G client bridge cannot associate using WPA/PSK.
- CSCsd52888—When an access point's default gateway changes, the access point disconnects from the controller.
- CSCsd52912—UDP packets travel in only one direction during mobility.
- CSCsd54797—The controller needs to drop invalid ARPs from STAs.
- CSCsd62518—SNMP v1/v2 is not accessible after a controller's configuration is cleared.
- CSCsd72556—The controller does not retain a newly created admin username and password.
- CSCsd73855—A contained rogue access point is reported as a missing trusted access point.
- CSCsd80877—Image load protection needs to be implemented on the controller.
- CSCsd85326—The 2000 series controllers do not track the latest Aeroscout tags.
- CSCsd94967—Access points fail to join a controller when the network path MTU setting is configured for less than 1500 bytes.
- CSCsd98255—Clients connected to a 4400 series controller cannot renew their DHCP IP address after a Layer 3 roam.
- CSCsd99572—Some hand-held clients are unable to connect to a secure WLAN advertised by REAP access points.
- 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.
- CSCse15753—WCS hangs when adding a controller or refreshing a controller configuration when mobility anchors for a WLAN are added in non-numerical order, such as 1.1.1.2 and then 1.1.1.1.
- CSCse23197—A client fails to get a DHCP IP address and the controller GUI becomes unresponsive when the client attempts to connect to a WLAN with web policy authentication.

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.