



# Release Notes for Cisco Wireless LAN Controller and Cisco Lightweight Access Point for Software Release 3.1.59.24

---

**November 3, 2005**

These release notes describe open caveats for operating system release 3.1.59.24 for Cisco 2000 Series Wireless LAN Controllers, Cisco 4100 Series Wireless LAN Controllers, Cisco 4400 Series Wireless LAN Controllers, Cisco Aironet 1000 series lightweight access points, Cisco Aironet 1130 series lightweight access points, Cisco Aironet 1200 series lightweight access points, Cisco Aironet 1240 series lightweight access points, and Cisco Aironet 1500 series lightweight outdoor access points which comprise part of the Cisco Unified Wireless Network Solution (Cisco UWN).

The Cisco 2000 Series Wireless LAN Controllers, Cisco 4100 Series Wireless LAN Controllers, and Cisco 4400 Series Wireless LAN Controllers are hereafter collectively referred to as *Wireless LAN Controllers*, and the access points are hereafter collectively referred to as *Cisco lightweight access points*.

## Contents

These release notes contain the following sections.

- [Cisco Unified Wireless Network Solution Components, page 2](#)
- [Requirements for Cisco UWN Components, page 2](#)
- [Software Release Information, page 2](#)
- [New Features, page 3](#)
- [Installation Notes, page 3](#)
- [Important Notes, page 6](#)
- [Caveats, page 14](#)
- [Troubleshooting, page 18](#)
- [Related Documentation, page 18](#)
- [Obtaining Documentation, page 18](#)



---

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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

# Cisco Unified Wireless Network Solution Components

The following components are part of the Cisco Unified Wireless Network Solution (Cisco UWN):

- Operating System (Wireless LAN Controller and Cisco Lightweight Access Point) software 3.1.59.24
- Cisco Wireless Control System (Cisco WCS)
- Cisco 2700 Series Location Appliances
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 4100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco Aironet 1000 Series Lightweight Access Points
- Cisco Aironet 1130 Series Lightweight Access Points
- Cisco Aironet 1200 Series Lightweight Access Points
- Cisco Aironet 1240 Series Lightweight Access Points
- Cisco Aironet 1500 Series Lightweight Outdoor Access Points

## Requirements for Cisco UWN Components

- Requirements for Web user interface - Windows XP SP1 or Windows 2000 SP4 running Internet Explorer 6.0.2800.1106.xpsp2.130422-1633 or higher. You also need to load patch KB831167 from the following location:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=254eb128-5053-48a7-8526-bd38215c74b2&displaylang=en>

There are known issues with Opera, Mozilla and Netscape; these browsers are unsupported.

- Requirements for Web browser when using Web Authentication - Internet Explorer 6.0 with SP1 or Netscape 7.2. There are known problems with Opera.

## Software Release Information

Release 3.1.59.24 is factory installed on your Wireless LAN Controller and automatically downloaded to the Cisco lightweight access points after a release upgrade and whenever a Cisco lightweight access point associates with a Wireless LAN Controller. As new releases become available for the Wireless LAN Controllers and their associated Cisco lightweight access points, consider upgrading.

## Finding the Software Release

To find the software release running on your Wireless LAN Controller, refer to the instructions in the *Cisco Wireless LAN Solution Product Guide*.

## New Features

The following new features are available in the Wireless LAN Controller 3.1.59.24 release:

- 802.11h support
- Enhanced support for the Cisco Wireless IP Phone 7920
- Enhanced integration with Cisco Secure ACS
- Location services enhancements
- Regulatory domain updates
- New hardware platform support: Cisco Aironet 1130 series lightweight access points, Cisco Aironet 1200 series lightweight access points, Cisco Aironet 1240 series lightweight access points, and Cisco Aironet 1500 series lightweight outdoor access points

For more information, refer to the following location:

[http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_bulletins\\_list.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletins_list.html)

## Installation Notes

This section contains important information to keep in mind when installing your Wireless LAN Controllers and Cisco lightweight 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 Wireless LAN Controllers and Cisco lightweight 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

**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 an antenna, take extreme care not to come into 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.:NFPA 70, National Electrical Code, Article 810, in Canada: Canadian Electrical Code, Section 54).**

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 antenna you are about to install.
2. Select your installation site with safety, as well as performance in mind. Remember: 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, 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 complete 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.

## Cisco Lightweight Access Point Installation

Refer to the appropriate quick start guide or installation and configuration guide for instructions on how to install your Wireless LAN Controllers and Cisco lightweight access points.



**Note**

---

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

---

Personnel installing the Wireless LAN Controllers and Cisco lightweight access points must understand wireless techniques and grounding methods. The internal-antenna Cisco lightweight access points can be installed by an experienced IT professional.

## Important Notes

This section describes important information about the Wireless LAN Controllers and Cisco lightweight access points.

## Important Regulatory Notice

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

## Voice Wireless LAN 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.

## Cisco 7920 Wireless IP Phone Support

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

- Aggressive Load Balancing on the Wireless LAN Controllers must be disabled on a per-Wireless LAN 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 Cisco lightweight access point to communicate its channel usage to wireless devices. Because Cisco lightweight 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 Cisco lightweight access point. Use the following instructions to enable the QBSS IE:
  - **>sh wlan summary**  
(use this to determine the wireless LAN ID No. of the wireless LAN to which you want to add QBSS support)
  - **>config wlan disable [Wireless LAN ID No.]**
  - **>config wlan dot11-phone compat [Wireless LAN ID No.]**
  - **>config wlan enable [Wireless LAN ID No.]**
  - **>sh wlan [Wireless LAN ID No.]**  
(use this command to verify that the wireless LAN is enabled and the field marked “Dot11-Phone Mode (7920)” is in the ‘compat’ mode)
  - **>save config**
- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled. The DTPC information element is a beacon and probe information element that allows the Cisco lightweight access point to broadcast information on its transmit power. The Cisco Wireless IP

Phone 7920 uses this information to automatically adjust its transmit power to the same level as the Cisco lightweight access point to which it is associated. In this manner, both devices are transmitting at the same level.

- The 7920 phones and the Wireless LAN Controllers do not currently use compatible fast roaming mechanisms. The phone uses CCKM while the Wireless LAN 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 the Wireless LAN Controller and the 7920 phone. Configure the Wireless LAN Controller for 104 bits when using 128-bit WEP for the 7920.

## The Upgrade Process

When a Wireless LAN Controller is upgraded, the code on the associated Cisco lightweight access points is also automatically upgraded. When a Cisco lightweight access point is loading code, its lights blink in succession.



### Caution

Do not power down the Wireless LAN Controller or any Cisco lightweight access point during this process, or you can corrupt the software image!

Upgrading a Wireless LAN Controller with a large number of Cisco lightweight access points can take as long as 30 minutes. The Cisco lightweight access points must remain powered on and the Wireless LAN Controller must not be reset during this time.

Cisco recommends the following sequence when performing an upgrade:

1. Upload your Wireless LAN Controller configuration files to a server to back them up.
2. Turn off the Wireless LAN Controller 802.11a and 802.11b networks.
3. Upgrade your Wireless LAN Controller.
4. Re-enable your 802.11a and 802.11b networks.



### Note

Wireless LAN Controllers can be upgraded from one release to another. However, if you require a downgrade from one release to another, you may be unable to use the higher release configuration (CSCsb79383). The workaround is to reload the previous Wireless LAN Controller configuration files saved on the backup server or to reconfigure the Wireless LAN Controller.

## Exclusion List (Blacklist) Client Feature

If a client is not able to connect, and the security policy for the wireless LAN and client are correct, the client has probably been disabled.

1. From the Web user interface, access the Monitor page under client summary, and you can see the client's status.
2. If the client is disabled you can just do a "Remove" operation to clear the client from the disabled list.
3. The client automatically restores its connection and, if necessary, reattempts authentication.

Automatic disabling happens as a result of too many failed authentications. Clients that are 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.

## IPSec Clients Supported in this Release

This operating system release has been tested with the following IPSec clients:

- NetScreen v8.0.0
- Cisco Unity v3.6.2
- SSH Sentinel v1.3.2(1)
- Movian v3.0

The Netscreen client does not handle fragmented ICMP packets, does not respond to large ping packets, and does not work with certificates. Other IP fragmented traffic should work correctly.

## Maximum MAC Filter Entries

The Wireless LAN Controller database can contain up to 2048 MAC filter entries for local netusers (CSCar12371).

## Client Channel Changes

Cisco lightweight access points are known to go off channel for up to 30 seconds (typically 1 to 2 seconds) while identifying rogue access point threats, when the Cisco lightweight access point has RLDP enabled. This can cause client connections to be dropped occasionally (CSCar10047).

## Cisco Aironet 1030 Remote Edge Lightweight Access Point WPA2-PSK in Standalone Mode

Cisco Aironet 1030 remote edge lightweight access points do not support WPA2-PSK in REAP standalone mode.

## XAuth Configuration with NetScreen

Do not enable XAuth on the NetScreen client. Configure XAuth on the Wireless LAN Controller. The Wireless LAN Controller initiates the XAuth session and the NetScreen client responds. Configure the NetScreen client with pre-shared keys only. You also need to set up a separate connection in the clear to your DHCP server.

## Rekeys Not Supported with Cisco VPN Client

If a rekey occurs clients must reauthenticate. To solve this problem, log into the Web user interface, navigate to the WLANs page, select **Edit** to display the WLANs > Edit page, choose **Advanced Configuration**, and change Lifetime (seconds) to a large value, such as 28800 seconds (this is the default), depending upon your security requirements.

## RADIUS Servers

This product has been tested with the following RADIUS servers:

- Odyssey Server and Odyssey Client v1.1 and 2.0 from Funk Software.
- Steel-Belted RADIUS from Funk Software release 4.40.337 Enterprise Edition.
- Microsoft Internet Authentication Service (IAS) release 5 on Windows 2000 Server/SP4; Microsoft Internet Authentication Service (IAS) release 5.2.3790.0 on Windows 2003 server.
- CiscoSecure ACS, v3.2.
- FreeRADIUS release 0.9.3, with OpenSSL 0.9.7B.

## 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 Windows Zero-Config Supplicant

Clients using Windows Zero-Config and 802.1x MUST use wireless LANs 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 Wireless LAN Controller reboots, dropped Cisco Aironet 1030 remote edge lightweight access points attempt to associate with any available Wireless LAN Controller. If the Cisco Aironet 1030 remote edge lightweight access points cannot contact a Wireless LAN Controller, they continue to offer 802.11a/b/g service on wireless LAN 1 only.

## WEP Keys

This release supports four separate WEP index keys. These keys cannot be duplicated between wireless LANs. At most four WEP wireless LANs can be configured on a Wireless LAN Controller. Each of these wireless LANs must use a different key index.

## Transmit Power Algorithms

Transmit power algorithms are designed to work with four or more Cisco lightweight access points. If there is a need to enable these algorithms for a smaller number of Cisco lightweight access points, contact Cisco Technical Assistance Center (TAC).

## Using the Backup Release

The Wireless LAN Controller Bootloader (ppcboot) stores a copy of the active primary and the backup release. If the primary release becomes corrupted, you can use the Bootloader to boot with the backup release.

After you have booted with the backup release, be sure to use Option 4: Change Active Boot Image on reboot to set the backup release as the active boot release. If you do not, then when the Wireless LAN Controller resets it again boots off the corrupted primary release.

## Home Page Retains Web Auth Login with IE 5.x

This is a caching problem in the Internet Explorer 5.x browser. Clearing the history file corrects it, or you can upgrade your operator workstation to Internet Explorer 6.x.

## RLDP Enable/Disable

RLDP Enable/Disable refers to the RLDP protocol which detects rogues on your wired network. Autocontainment enable/disable indicates whether you want the Wireless LAN Controller to automatically contain new rogues that it finds on the wire. Disabling RLDP or autocontainment does not disable containment for rogues that are being contained. When rogues are being contained, you must manually disable containment for each rogue individually.

## Ad-Hoc Rogue Containment

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

## Apple iBook

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

## Features Not Supported on Cisco 2000 Series Wireless LAN Controllers

Hardware Features:

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

#### Software Features:

- VPN Termination (such as IPSec and L2TP)
- Guest controller wireless LAN function
- External Web Authentication web server list
- Layer 2 LWAPP
- Spanning tree
- Port mirroring
- Cranite
- Fortress
- AppleTalk
- 802.1p tagging
- QoS per user bandwidth contracts
- IPv6 pass-through

## Some Clients Can 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 enforce RF policies in your buildings and campuses.

## Cisco 4400 Series Wireless LAN Controller Limitations

Cisco 4400 Series Wireless LAN Controllers have the following limitations:

- Data traffic that goes in Cisco 4400 Series Wireless LAN Controller port 1 or 2 and exits port 3 or 4 may experience a loss rate of less than 1%.
- Heavy multicast traffic may cause the Cisco 4400 Series Wireless LAN Controller to lose connection with Cisco lightweight access points.

## Cisco Lightweight Access Point Fails to Join Wireless LAN Controller When the Console Port is Connected Through a Terminal Server

The Cisco lightweight access point boots up Cisco IOS image and reboots due to join failure or timeout. This sequence repeats until the Cisco lightweight access point goes into boot prompt and stays there. This condition occurs when the Cisco lightweight access point console is connected to a terminal server port, when there is no Telnet session to the Cisco lightweight access point console port, and when the Wireless LAN Controller is not responding to the Cisco lightweight access point join response.

Workaround: Disconnect the Cisco lightweight access point console port from the terminal server. Reprogram the Wireless LAN Controller to have it respond to the Cisco lightweight access point join request. Restart the Cisco lightweight access point.

## Pinging from Any Network Device to a Dynamic Interface IP Address Not Supported

Clients on the wireless LAN associated with the interface pass traffic normally.

## Upgrading External Webauth

To upgrade External Webauth, do the following:

- When upgrading Wireless LAN Controllers from operating system release 2.0 or 2.2.127.4 to release 3.0, update the external webauth configuration as follows:
  - Instead of using a preauth ACL, the network manager must configure the external web server IP address using the CLI command:

```
config custom-web ext-webserver add <IP address>
```

(where <IP address> is the address of any web server that performs external web authentication.)

- Then, the network manager must use the new login\_template which is included below:

```
<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);
    }
}
```



# Caveats

This section lists open and closed caveats in operating system release 3.1.59.24 for Wireless LAN Controllers and associated Cisco lightweight access points.

## Open Caveats

These caveats are open in operating system release 3.1.59.24:

- CSCar13192—In Cisco 2000 Series Wireless LAN Controllers, the trap message for SNMP authentication failure contains a reversed IP address. If an SNMP query is made to a Cisco 2000 Series Wireless LAN Controller, and if the query results in an authentication failure, the IP address of the querying machine appears reversed on the trap log message.
- CSCar13259—Clients are not excluded on Cisco Aironet 1030 remote edge lightweight access points in REAP mode.
- CSCar13330—When using the web configuration wizard to complete the initial configuration on a Cisco 2000 Series Wireless LAN Controller, on the RADIUS configuration page, after enabling the server, an error message is returned saying “Error in enabling the server.”

Workaround: The RADIUS server may be enabled after the configuration wizard is complete and the Wireless LAN Controller UI is in regular mode. To go to the RADIUS server details, click the **Security** tab and then select **RADIUS Authentication** under the AAA menu. Then, click the edit link for the RADIUS server entry. On the RADIUS edit page, enable the server state and click **Apply**.

- CSCei65293—The 5-GHz, RM-21A radio module on Cisco Aironet 1200 series lightweight access points has an articulating antenna with a dual function: diversity omni or patch antenna. When the antenna is folded flat to the access point housing it is in 9-dBi patch mode, and when it is in any other position it is in 5-dBi omni mode. When you change the antenna position to switch antenna modes you must reset the Cisco Aironet 1200 series LWAPP-enabled access point to apply the change.
- CSCsa95763—The Wireless LAN Controller Web UI cannot display more than 80 local net users on the page **Security > AAA > Local Net Users**.

Workaround: Use the Wireless LAN Controller CLI to view all the Local Net User entries.

- CSCsb01980—When using the web configuration wizard on a Wireless LAN Controller, when the operator enters incorrect data for the management interface, error messages are shown only at the end of the wizard and therefore the user must return to the management interface page for correction. The data entered in the management interface page, such as the port number, is 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 Wireless LAN Controller Web Configuration wizard is not reachable after making repeated invalid entries for the management interface port. If an operator connects to the Wireless LAN Controller Web Configuration wizard on address 192.168.1.1 and enters an invalid port number on the Management Interface configuration 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 configuration wizard becomes inaccessible.

Workaround: Reboot the Wireless LAN Controller through the CLI to access the web wizard again.

- CSCsb09699—ACL rules with specified source or destination IP addresses are not working. For instance, if you create a permit ACL with source as 20.0.0.11/255.255.255.255 and all other parameters as any, the wireless client from this IP address cannot ping the server.
- CSCsb30211—Cisco lightweight access points continue rebooting when WMM mode is enabled. Cisco lightweight access points may not be able to join the Wireless LAN Controller if WMM is enabled on any of the wireless LANs.

Workaround: Make sure that the port to which the Cisco lightweight access point is connected is configured as trunk port and not an access port if any wireless LAN has WMM enabled.

- CSCsb34149—Disabling or deleting a wireless LAN on which a large number of clients exists may not result in deletion of all of the clients. This occurs when a large number (several thousand) clients are using a wireless LAN when the wireless LAN is disabled or deleted.

Workaround: Make sure that wireless LANs with a large number of clients associated are not deleted or disabled.

- CSCsb37605—When the admin status of Cisco Aironet 1000 series lightweight access point radio A is disabled, toggling the 802.11a network status flag re-enables radio A; however, the admin status of radio A is still disabled.

Workaround: Disabling radio A and reapply.

- CSCsb42133—If you enter an invalid value for session timeout when editing a wireless LAN, an incorrect range is shown in an error message. This bug appears when you select the edit option for a wireless LAN on the Wireless LAN Controller user interface, set the wireless LAN for 802.1x security, and then enter an invalid value for session timeout. The error message shown when you click **Apply** incorrectly states that the correct range is 0 to 86400.

Workaround: The correct range for the wireless LAN session timeout is: 300-86400 for 802.1x and 0-65535 for all other security types.

- CSCsa47748—RLDP protocol is not supported in Cisco Aironet 1130 series lightweight access points, Cisco Aironet 1200 series lightweight access points, and Cisco Aironet 1240 series lightweight access points.

Workaround: Use **Rogue Detector AP** to detect rogue access points.

- CSCsb52557—Cisco lightweight access points do not connect to the Cisco 4400 Series Wireless LAN Controller if the time is not set first.

Workaround: Set the time on the Cisco 4400 Series Wireless LAN Controller before allowing the Cisco lightweight access points to connect.

- CSCsb53746—A 350 or CB20A client running ACU 6.4 or ACU 6.5 and configured for LEAP authentication with WPAv1 encryption can authenticate to a Cisco 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.

To check for this problem enter the following command on the Wireless LAN 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

Workaround: Configure WME policy to be allowed for the wireless LAN on the Wireless LAN Controller. To do this on the GUI, browse to the WLANs > Edit page for the appropriate WPAv1 wireless LAN, and in the drop-down menu next to WME policy, select **Allowed** or **Required**. The allowed option means that both WME and non-WME clients can authenticate and receive an IP address; for example, both Aironet ACU 6.4/6.5 and 6.3 clients could authenticate and receive an IP address. The required option means that only WME clients can authenticate; that is, only ACU 6.4/6.5 clients.

- CSCsb54444—RLDP does not work for regulatory domain -E. This condition applies only to countries which require DFS (radar detection) support.

Workaround: Do not enable RLDP in these countries.

- CSCsb55937—VLAN-tagged large ICMP packets that need to be fragmented are not sent by Cisco Aironet 1000 series lightweight access points in direct-connection mode. Ping replies never come back when the Cisco Aironet 1000 series lightweight access point is sending 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 Cisco 4400 Series Wireless LAN Controllers using direct-connect mode, with RADIUS override enabled, the override parameter set to 1p with any VLAN number, and Cisco Aironet 1000 series lightweight access points.
- CSCsb57305—Some Cisco lightweight access points transmit beacons after the associated wireless LAN is deleted from the Wireless LAN Controller. This happens only for wireless LANs with radio policy set to 802.11g only and when 802.11g support is globally disabled.

Workaround: If you have a wireless LAN with radio policy 802.11g only, do not disable 802.11g support.

- CSCsb62289—The displayed dBm for Cisco Aironet 1500 series lightweight outdoor access points appears lower than it actually is.

Workaround: In the CLI, the correct values can be up to 6 dBm higher for 2.4-GHz channels and up to 13 dBm higher for 802.11a channels 149 to 165.

- CSCsb63479—Clicking the Refresh link on the Cisco APs page sometimes results in a Page Not Found error. This generally occurs when there are more than 80 Cisco lightweight access points connected to the Wireless LAN Controller.

Workaround: Click the Wireless tab at the top of the page and click the Cisco APs link on the left. This causes Cisco WCS to list all the Cisco lightweight access points on the page.

- CSCsb65096—After changing the bridging shared secret key, the shared secret keys may not be uniformly distributed across the bridge or mesh network. This can cause some Cisco lightweight access points to fail to connect to the Wireless LAN Controller using LWAPP, and the Cisco lightweight access points to time out their connections.

Workaround: Upgrade to the latest code. Ensure that the Wireless LAN Controller is configured as follows: **config network allow-old-bridge-aps disable**.

- CSCsb65731—Cisco Aironet 1500 series lightweight outdoor access points are sometimes slow to fail over to a new Wireless LAN Controller when the primary Wireless LAN Controller fails.

Workaround: Upgrade to the latest code.

- CSCsb68069—When all eight Wireless LANs are defined on 1130AG, 1200AG, and 1240AG access points converted to lightweight mode, and the radio environment is very busy, transmission attempts can be delayed. The 802.11g radios sometimes report this error:

```
%DOT11-2-RADIO_FAILED: Interface Dot11Radio0, failed - Radio command failed, cmd 121 (FF80,0,0) status 7F21 (5,0,0)
```

When the failure occurs, the radio restarts, all clients are disassociated, the failure is logged, and normal operation resumes.

Workaround: Reduce the number of Wireless LANs in use.

- CSCsb77161—Cisco Aironet 1500 series lightweight outdoor access points are out of compliance with the IEEE 802.11a requirement for maximum receive input level, that is receiver saturation, at data rates of 24, 36, 48, and 54 Mbps. Cisco lightweight access points can experience increased packet error rates when they are located too close to one another.

Workaround: Mount the Cisco Aironet 1500 series lightweight outdoor access points at least 50 feet (15 m) apart from one another. The software roadmap has a release planned that will enable a gain bypass feature which will correct this performance limitation.

- CSCsb98213—When Cisco Aironet 1030 remote edge lightweight access points and Cisco Aironet 1500 series lightweight outdoor access points in bridging mode are to be used as pole-top access points, they should be configured as pole-top access points before they are deployed in the network. Not configuring the Cisco lightweight access points as pole-top access points may result in a longer than normal loss of data connectivity if the roof-top access point loses connection to the Wireless LAN Controller.

Workaround: Use the CLI commands from a Wireless LAN Controller to configure the Cisco lightweight access points as pole-top access points before deploying them.

- CSCsc07129—Cisco Aironet 1500 series lightweight outdoor access points do not forward DHCP broadcast replies, such as those from Microsoft Windows DHCP servers. Pole-top access points do not obtain an IP address if the DHCP server sends the DHCP response to a broadcast address.

Workaround: Either configure the Cisco Aironet 1500 series lightweight outdoor access points with a static IP address or use a DHCP server that sends its response to a unicast address.

- 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.

Workaround: In order to set the 802.11a radio to channel 165 when using the -A SKU, set the country code of the Wireless LAN Controller to USX. For the -N SKU, please select one of the available channels.

- CSCsc35784—The transmit power control adjustment levels 3, 4 and 5 are not supported on Cisco Aironet 1500 series lightweight outdoor access points; these levels correspond to -6, -9, and -12 dB from the maximum power, respectively. Power levels 1 and 2 are supported, which correspond to maximum power for the particular data rate and channel, and -3 dB relative to this maximum. Both the 2.4- and 5.8-GHz bands are affected, 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.

- (NEW CAVEAT)—Over the temperature extremes of the product specification, primarily at the cold temperature extreme of -40 degrees Celsius, the Cisco Aironet 1500 series lightweight outdoor access point does not meet the IEEE 802.11a/b/g transmitter linearity parameter of error vector

magnitude (EVM) of the product specification. The software roadmap has a release planned that will enable temperature compensation of the transmit gain, which will address the EVM corner cases over the temperature range.

## Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following location:

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

Click **Technology Support**, select **Wireless** from the menu on the left, and click **Wireless LAN**.

## Related Documentation

For information on the Cisco Unified Wireless Network Solution and for instructions on how to configure and use the Cisco UWN, refer to the *Cisco Wireless LAN Solution Product Guide*.

## Obtaining Documentation

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

### Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

### Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

# Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.  
Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate and value your comments.

## Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

## Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: [www.cisco.com](http://www.cisco.com)
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to [cco-team@cisco.com](mailto:cco-team@cisco.com).

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use [www.cisco.com/techsupport](http://www.cisco.com/techsupport).

To contact TAC by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

## Obtaining Additional Publications and Information

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

- The Cisco Product Catalog describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at the following location:  
[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)
- Cisco Press publishes a wide range of general networking, training and certification titles. Both new and experienced user will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at the following location:  
<http://www.ciscopress.com>
- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at the following location:  
<http://www.cisco.com/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at the following location:  
<http://www.cisco.com/go/iqmagazine>
- 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 the following location:  
[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at the following location:  
<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.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.