Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 3.2.171.5

September 22, 2006

These release notes describe open and resolved caveats for operating system release 3.2.171.5 for Cisco 2000, 4100, and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSM); Cisco Wireless LAN Controller Network Modules; and Cisco Aironet 1000, 1130, 1200, 1240, and 1500 Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (Cisco UWN) Solution.

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

Contents

These release notes contain the following sections:

CISCO SYSTEMS

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

Cisco Unified Wireless Network Solution Components

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

- Operating system software release 3.2.171.5 for all Cisco controllers and lightweight access points
- Cisco Wireless Control System (WCS) software release 4.0.81.0 or 4.0.66.0
- Location appliance software release 2.1.39.0 or 2.1.34.0
- Cisco 2700 Series Location Appliances
- Cisco 2000, 4100, and 4400 Series Wireless LAN Controllers
- Cisco Wireless Service Module (WiSM) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers
- Cisco Aironet 1000, 1130, 1200, 1240, and 1500 Lightweight Access Points

Controller Requirements

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

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

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

Software Release Information

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

Note The Cisco WiSM requires software release SWISMK9-32 or later.

Finding the Software Release

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

Upgrading to a New Software Release

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

⚠️

Caution Do not power down the controller or any access point during this process; otherwise, you might corrupt the software image! Upgrading a controller with a large number of access points can take as long as 30 minutes. The access points must remain powered, and the controller must not be reset during this time.

Cisco recommends the following sequence when performing an upgrade:

1. Upload your controller configuration files to a server to back them up.

2. Turn off the controller 802.11a and 802.11b networks.

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

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

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

✏️

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

Installation Notes

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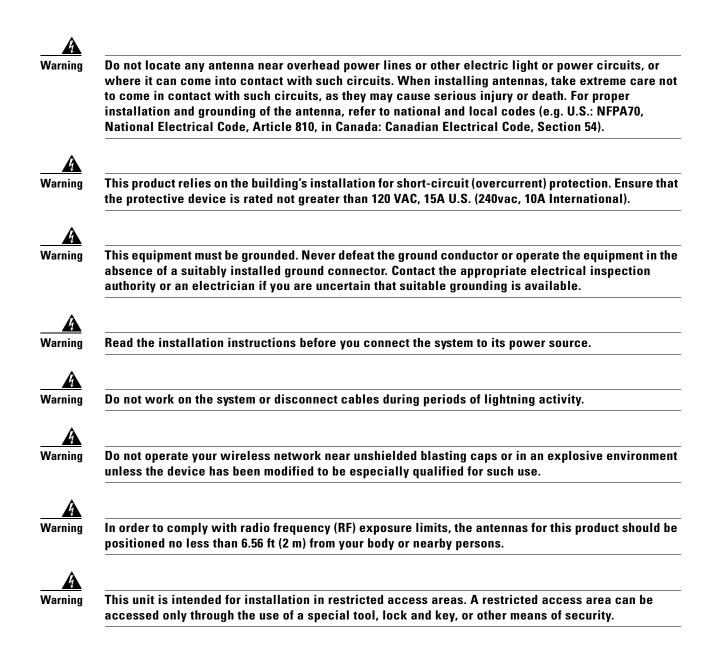
Warnings

⚠️

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

⚠️

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

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

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

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

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

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

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

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

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

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

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.

2. Select your installation site with safety as well as performance in mind. Electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.

3. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.

4. Plan your installation carefully and completely before you begin. Successfully raising a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.

5. When installing an antenna, remember:
   a. **Do not** use a metal ladder.
   b. **Do not** work on a wet or windy day.
   c. **Do** dress properly—shoes with rubber soles and heels, rubber gloves, and a long-sleeved shirt or jacket.

6. If the assembly starts to drop, get away from it and let it fall. Remember that the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer: **you!**

7. If any part of an antenna system should come in contact with a power line, **do not touch it or try to remove it yourself. Call your local power company**. They will remove it safely.

8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

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

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

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

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

Important Notes

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

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

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

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

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

Workarounds

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

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

Changing the Default Values of SNMP Community Strings

The controller has commonly known default values of "public" and "private" for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values.

Using the GUI to Change the SNMP Community String Default Values

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

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

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

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

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

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

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

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

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

Using the CLI to Change the SNMP Community String Default Values

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

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

show snmp community

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

config snmp community delete *name*

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

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

config snmp community create *name*

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

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

config snmp community ipaddr *ip_address ip_mask name*

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

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

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

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

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

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

Changing the Default Values for SNMP v3 Users

The controller uses a default value of "default" for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values.

Using the GUI to Change the SNMP v3 User Default Values

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

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

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

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

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

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

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

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

Using the CLI to Change the SNMP v3 User Default Values

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

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

show snmpv3user

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

config snmp v3user delete *username*

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

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

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

where

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

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

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

FIPS 140-2

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

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

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

Voice WLAN Configuration

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

Inter-Subnet Roaming

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

Operating Mesh Networks Through Switches and Routers

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

Heavily Loaded Controller CPU

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

RADIUS Servers and the Management VLAN

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

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

Cisco 7920 Wireless IP Phone Support

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

- Aggressive load balancing must be disabled on a per-controller basis. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.

- The QoS Basis Service Set (QBSS) information element (IE) must be enabled. The QBSS IE enables the access points to communicate their channel usage to wireless devices. Because access points with high channel usage might not be able to handle real-time traffic effectively, the 7920 phone uses the QBSS value to determine if it should associate with another access point. Use the following commands to enable the QBSS IE:

    - **sh wlan summary**

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

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

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

    - **save config**

- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the **config 802.11a dtpc enable** command. The DTPC IE is a beacon and probe information element that allows the access point to broadcast information on its transmit power. The Cisco 7920 Wireless IP Phone uses this information to automatically adjust its transmit power to the same level as the access point to which it is associated. In this manner, both devices are transmitting at the same level.

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

- When configuring WEP, there is a difference in nomenclature for the controller and the 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7920.

Client Channel Changes

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

Exclusion List (Blacklist) Client Feature

If a client is not able to connect to an access point and the security policy for the WLAN and/or client is correct, the client has probably been disabled. In the controller GUI, you can view the client's status on the Monitor > Summary page under Client Summary. If the client is disabled, click **Remove** to clear the disabled state for that client. The client automatically comes back and, if necessary, reattempts authentication.

Automatic disabling happens as a result of too many failed authentications. Clients disabled due to failed authorization do not appear on the permanent disable display. This display is only for those MACs that are set as permanently disabled by the administrator.

Maximum MAC Filter Entries

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

config database size *MAC_filter_entry*

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

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

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

RADIUS Servers

This product has been tested with the following RADIUS servers:

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

Management Usernames and Local Netuser Names

Management usernames and local netuser names must be unique because they are stored in the same database. That is, you cannot assign the same name to a management user and a local netuser.

802.1x and Microsoft Wireless Configuration Manager

Clients using the Microsoft Wireless Configuration Manager and 802.1x must use WLANs configured for 40- or 104-bit key length. Configuring for 128-bit key length results in clients that can associate but not authenticate.

Cisco Aironet 1030 Remote Edge Lightweight Access Point Default Operation

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

Using the Backup Image

The controller bootloader (ppcboot) stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the bootloader to boot with the backup image.

With the backup image stored before rebooting, be sure to choose **Option 4: Change Active Boot Image** from the boot menu to set the backup image as the active boot image. Otherwise, when the controller resets, it again boots off the corrupted primary image.

After the controller boots, the active boot image can be changed to the backup image using the **config boot backup** command.

Home Page Retains Web Auth Login with IE 5.x

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

Ad-Hoc Rogue Containment

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

RLDP Enable/Disable

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

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

Apple iBook

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

Features Not Supported on 2000 Series Controllers

These hardware features are not supported on 2000 series controllers:

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

These software features are not supported on 2000 series controllers:

- VPN termination (such as IPSec and L2TP)
- Termination of guest controller tunnels (Origination of guest controller tunnels is supported)
- External web authentication web server list
- Layer 2 LWAPP
- Spanning tree
- Port mirroring
- Cranite
- Fortress
- AppleTalk
- QoS per-user bandwidth contracts
- IPv6 pass-through

Some Clients See Only 64 Access Point MAC Addresses (BSSIDs) at a Time

In a crowded RF environment, clients may not be able to detect the desired SSID because of internal table limitations. Sometimes disabling and then enabling the client interface forces a rescan. Your RF environment needs to be controlled. Cisco UWN rogue access point detection and containment can help you to enforce RF policies in your buildings and campuses.

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

Clients on the WLAN associated with the interface pass traffic normally.

2006 Image Not Supported for 3504 Controllers

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

Running a 3504 Image on a 2000 Series Controller

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

Cisco Lightweight Access Points Fail to Join Cisco Controllers

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

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

Upgrading External Web Authentication

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

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

   config custom-web ext-webserver add *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> </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    <input type="TEXT" name="username"
SIZE="25" MAXLENGTH="63" VALUE=""> </td> </tr> <tr align="center" > <td colspan="2">
Password      <input type="Password" name="password"
SIZE="25" MAXLENGTH="24"> </td> </tr>

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

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

Caveats

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

Resolved Caveats

These caveats are resolved in software release 3.2.171.5.

- CSCsb75736—The WLANs and the number of clients may not appear correctly in the Top WLANs list on the Monitor > Summary page of the controller GUI.

- 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.

- CSCsb88424—Access points in REAP mode may fail to join the controller due to a certificate-processing error in the Join request.

- CSCsc05495—Controllers intermittently send a state attribute 24 in an access-request packet.

- CSCsc34060—IPSec clients enter the run state but do not communicate.

- CSCsc44326—A 4400 series controller running software release 3.1.105.0 may fail to respond to ARP requests for the ap-manager2 interface's IP address when the ARP request is addressed at the MAC layer to the unicast MAC address of the interface rather than to the broadcast MAC address. As a result, there may be sporadic interruptions in connectivity at ARP refresh time, resulting in the periodic loss of associations for access points associated through the ap-manager2 interface.

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

- CSCsd18145—If you disable proxy ARP on the controller, the ARPs still go to the controller CPU.

- CSCsd19801—A 4000 series controller sometimes hangs while it is booting up.

- CSCsd27529—Static WEP does not operate properly for a REAP access point in standalone mode.

- CSCsd54712—An access point may reboot when it is connected to a 2000 series controller and an N900iL handset associated to the access point tries to place a call after the user idle timeout setting has expired.

- CSCsd55009—The access point may suddenly lose its connection to the controller. When this condition occurs, the access point periodically sends out DHCP requests, and the access point Alarm LED lights.

- CSCsd59700—The default AP1000/1200 settings for external antenna gain are incorrect. The 4000/4100 controller should show this value as "0" but instead shows it as "11."

- CSCsd65251—The Session Timeout parameter for WLANs on the controller GUI may not operate correctly. The value of this parameter appropriately changes to 1800 seconds when you choose the 802.1X option for Layer 2 security; however, it does not return to 0 seconds if you then choose a different Layer 2 security option.

- CSCsd76868—When you enable the Rogue Location Discovery Protocol (RLDP) to detect rogues but do not create WLAN ID 1, the controller reports minor alarms when critical alarms should be reported.

- CSCsd85859—The Refresh button does not operate properly on some of the controller GUI pages.

- CSCsd87382—Bridging functionality for REAP devices is not available on OEM builds of controller software.

- CSCsd90392—The idle timeout may not work correctly for an access point in REAP mode.
- CSCsd91051—An "Incorrect input!" message appears when you enter the **show wlan mobility** command in the controller CLI.
- 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.
- CSCsd99725—An access point restarts when you change its mode of operation from urgent mode to REAP mode.
- CSCse03869—When AP Authentication Policy is enabled on a 2006 controller, any connected access points may reboot when a client associates.
- CSCse11202—WCS logs an "Incorrect WEP Key" error for wireless clients running TKIP.
- CSCse14889—The controller does not generate traps for ad-hoc rogues.
- CSCse15889—The controller may reboot after running for many days due to a failure with the sshpmReceiveTask software watchdog.
- CSCse20190—When the controller is running software release 3.2.116.21, Spectralink phones fail shared key authentication.
- CSCse26437—After a communication breakdown occurs between a controller and an access point, the access point does not send a subsequent request to join the controller.
- CSCse27890—Access points in REAP mode send deauthentication frames to wireless clients without waiting for a PS poll.
- CSCse29193—The controller marks a RADIUS server as dead if a single request is not responded to after five retries and switches to a backup server.
- CSCse29686—After you upgrade from software release 3.2.78 to 3.2.116.21 or later, clients experience packet loss and a significant number of packet retransmissions on the AP1000. This condition is related to the antenna setting of the access point.
- CSCse30397—If you enter 24 characters for the username and password during the initial controller configuration, the "Routine system resource notification" error message may appear repeatedly.
- CSCse32639—Client exclusion may not operate properly when web authentication is enabled on the controller. If a wireless client becomes "excluded," it never disassociates from the access point and may be unable to log in again.
- CSCse33667—A controller running software release 3.2.116 with ssh disabled may crash without a crash dump.
- CSCse36426—Controllers with AP-group VLANs configured sometimes cause WCS to hang when the controllers are added to WCS.
- CSCse40350—During WPA2 client association, the access point sometimes sends a Reason 1 Deauthentication frame to the client, causing the client to disconnect and reassociate.
- CSCse43767—The **show client username** command shows only one client even when several clients are associated with the same username.
- CSCse46717—Access points sometimes reboot.
- CSCse47024—Clients sometimes lose their connection to the access point.
- CSCse47645—Controllers sometimes use an invalid IP address when sending pings.
- CSCse48743—When the idle timeout expires for a client, the controller sometimes displays this error message: "Got an idle-timeout message from an unknown client."

- CSCse49083—Access points in REAP mode sometimes send a deauthentication packet at the end of phone calls on some handsets.

- CSCse50111—The controller's active port sometimes becomes disabled when traffic is pumped from a wireless client to a wired client.

- CSCse51940—WCS sometimes displays this error message when you change the WLAN encryption type from WPA-PSK to WEP: "SNMP operation to device failed."

- CSCse53252—Controllers sometimes reboot due to an issue with the time server.

- CSCse55473—The 5-GHz radios on access points sometimes remain enabled even when disabled on the controller.

- CSCse58258—Access points sometimes reboot during an Assert software task.

- CSCse59150—SVP packets through controllers have inconsistent timing, resulting in poor voice quality.

- CSCse64508—A controller running software release 3.2.116.21 does not allow a Nortel VPN client using Contivity to connect until the date on the controller is changed from 2006 to 2005.

- CSCse66940—When the primary port on a controller fails and the controller switches traffic to a backup port, all configured WLANs are deactivated.

- CSCse70081—An SNMP trap is required to alert users that either the RADIUS server is not responding to a specific client or that it is not responding at all and a failover is required.

- CSCse72853—Access points in REAP mode sometimes fail to act independently from the controller when the controller fails.

- CSCse78542—When the AutoRF feature causes the controller to select wrong channels for the country configured, the **show ap config 802.11a summary** command causes high CPU usage and eventual reboot of the controller.

- CSCse84879—When a primary, secondary, and tertiary controller are defined for an access point and the primary controller fails, the access point attempts to join the secondary controller even if that controller is carrying its maximum number of access point associations. The access point that needs to rejoin a controller never tries the tertiary controller; instead it reboots and attempts to join the secondary controller repeatedly.

- CSCse86585—Some controllers suffer a memory leak after 65 hours of operation.

- CSCse91528—Access points in REAP mode that have lost connection to a controller sometimes reboot when a client attempts to associate.

- CSCse93986—Pre-authentication ACLs sometime fail.

- CSCse99813—Some 1000 series access points use a transmit power level that is lower than normal.

- CSCsf01648—Web authentication sometimes fails for client devices using WPA-PSK.

- CSCsf01759—RADIUS class attributes are discarded after a stop record is sent.

Open Caveats

These caveats are open in software release 3.2.171.5.

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

  Workaround: Make sure that the anchor controller is a mobility group member.

- CSCsa95763—The controller GUI cannot display more than 80 local net users on the Security > AAA > Local Net Users page.

  Workaround: Use the controller CLI to view all the Local Net User entries.

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

  Workaround: This problem can cause some inconvenience, and the user may prefer to use the CLI configuration wizard instead to avoid it.

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

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

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

  Workaround: None at this time.

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

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

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

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

- CSCsb38486—The Cisco Aironet 1500 Series Lightweight Outdoor Access Point Bridge CLI does not accept 10-character bridge group names.

  Workaround: Use 9-character bridge group names.

- CSCsb52557—Cisco access points do not connect to the 4400 series controller if the time is not set first.

  Workaround: Set the time on the controller before allowing the access points to connect to the controller.

- CSCsb55597—The access point's output power may change after you modify a mandatory data rate.

  Workaround: None at this time.

- CSCsb55937—VLAN-tagged large ICMP packets that need to be fragmented are not sent by Cisco Aironet 1000 series access points in direct-connection mode. Ping replies never come back when the access point sends requests to a gateway from a wireless client using large 1500-byte packets and with RADIUS override configured with any 1p tag. This condition exists for 4400 series controllers using direct-connect mode, with RADIUS override enabled, the override parameter set to 1p with any VLAN number, and Cisco Aironet 1000 series access points.

  Workaround: None at this time.

- CSCsb71060—Internal LAG errors occur when the management interface is changed from tagged to untagged.

  Workaround: Leave the WiSM management interface as tagged or untagged.

- CSCsb77595—When logging out from Telnet/SSH sessions, the session always prompts the user to save changes, even when no changes have been made.

  Workaround: Ignore the prompt and exit as usual.

- CSCsb85113—When users download the code image to WiSM using the CLI, associated access points are sometimes disconnected.

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

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

  Workaround: None for this release.

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

  Workaround: None for this release.

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

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

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

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

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

  Workaround: None for this release.

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

  Workaround: None for this release.

- CSCsc14045—VPN passthrough should not be able to be combined with web policy.

  Workaround: Do not assign VPN passthrough along with web policy.

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

  Workaround: Disabling CDP resolves this issue.

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

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

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

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

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

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

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

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

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

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

  Workaround: None at this time.

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

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

  – Session Timeout: 0 seconds

  – Layer 3 Security: IPsec

  – IPsec Authentication: HMAC SHA1

  – IPsec Encryption: AES (If you choose 3DES, configure the IPsec lifetime to a value greater than the expected duration of the client session.)

  – IKE Phase 1: Aggressive

  – Lifetime: 43200 to 57600 seconds (12 to 16 hours)

  – IKE Diffie Hellman Group: Group 2 (1024 bits)

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

  Workaround: None at this time.

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

  Workaround: None at this time.

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

  Workaround: None at this time.

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

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

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

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

- 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.

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

  Workaround: None at this time.

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

  Workaround: None at this time.

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

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

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

  Workaround: None at this time.

- CSCsd52292—The controller does not accept uppercase MAC addresses from the WCS templates.

  Workaround: Do not use uppercase characters for MAC addresses in the WCS templates.

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

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

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

  Workaround: None at this time.

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

  Workaround: None at this time.

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

  Workaround: None at this time.

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

  Workaround: None at this time.

- CSCsd82363—Channel utilization is incorrectly reported in radio utilization reports on the controller and in WCS. Channel utilization may appear as zero when there is active client traffic or as an aggregate of client transmit and receive traffic.

  Workaround: None at this time.

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

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

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

  Workaround: None at this time.

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

  Workaround: None at this time.

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

  Workaround: Reset the controller.

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

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

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

  Workaround: None at this time.

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

  Workaround: None at this time.

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

  Workaround: None at this time.

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

  Workaround: None at this time.

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

  Workaround: None at this time.

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

  Workaround: None at this time.

- CSCse18855—RADIUS accounting cannot be disabled on an individual WLAN. Once a RADIUS accounting server is defined globally, WLANs fall back to the global RADIUS accounting server if no RADIUS accounting server is selected in the WLANs.

  Workaround: Create a fictitious RADIUS accounting server and assign it to the WLAN for which RADIUS accounting is not required.

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

  Workaround: None at this time.

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

  Workaround: None at this time.

- CSCse30696—The controller does not refresh the access point's IP address correctly when the admin status for that access point is disabled.

  Workaround: None at this time.

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

  Workaround: Use slot 1, which is the slot closest to the power outlet, for an ESM card in the 4402 controller.

- CSCse40636—The foreign controller incorrectly forwards multicast traffic onto the auto-anchor WLAN.

  Workaround: Configure the WLAN on the foreign controller to map to an invalid VLAN.

- CSCse52143—IPSec authentication with certificates may not always operate properly.

  Workaround: None at this time.

- CSCse60689—The controller may reboot due to a failure with the sshpmAddIPv4IpsecRules software.

  Workaround: None at this time.

- CSCse72413—The controller may reboot due to a failure with the debugMaintask software.

  Workaround: None at this time.

- CSCse80636—Under heavy traffic conditions, the VPN module may reach capacity and fail to accept additional packets.

  Workaround: None at this time.

- CSCsf10167—The controller may reboot due to a failure with the pemReceiveTask software watchdog.

  Workaround: None at this time.

- CSCsf11862—Controllers sometimes reboot during a software upgrade.

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

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

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

If You Need More Information

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

Troubleshooting

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

http://www.cisco.com/en/US/support/index.html

Click **Product Support** > **Wireless**. Then choose your product and **Troubleshooting** to find information on the problem you are experiencing.

Documentation Updates

This section lists updates to user documentation that has not yet been added to either printed or online documents.

Omissions

The Package Contents section in the *Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers* should be updated to include this item, which is included with the 4400 series controller:

- DB-9 to DB-9 null modem cable

Related Documentation

For additional information on the Cisco controllers and lightweight access points, refer to these documents:

- The Quick Start Guide for your particular controller or access point
- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Wireless LAN Controller Online Help*
- *Cisco Wireless Control System Configuration Guide*
- *Cisco Wireless Control System Online Help*

Click this link to browse to the Cisco Support and Documentation page:

http://www.cisco.com/cisco/web/support/index.html

Obtaining Documentation and Submitting a Service Request

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

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

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