



# Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 4.0.179.8

---

**August 22, 2006**

These release notes describe new features as well as open and resolved caveats for software release 4.0.179.8 for Cisco 2000 and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSM); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; and Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (UWN) Solution.



**Note**

---

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

---

## Contents

These release notes contain the following sections.

- [Cisco Unified Wireless Network Solution Components, page 2](#)
- [Controller Requirements, page 2](#)
- [Software Release Information, page 3](#)
- [New Features, page 4](#)
- [Installation Notes, page 5](#)
- [Important Notes, page 7](#)
- [Caveats, page 17](#)
- [Troubleshooting, page 22](#)



---

**Corporate Headquarters:**

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

© 2006 Cisco Systems, Inc. All rights reserved.

- [Related Documentation, page 23](#)
- [Obtaining Documentation and Submitting a Service Request, page 23](#)

## Cisco Unified Wireless Network Solution Components

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

- Software release 4.0.179.8 for all Cisco controllers and lightweight access points
- Cisco autonomous to lightweight mode upgrade tool release 2.01
- Cisco Wireless Control System (WCS) software release 4.0.81.0
- Location appliance software release 2.1.39.0
- Cisco 2700 Series Location Appliances
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco Wireless Services Module (WiSM) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 Series Lightweight Access Points

## Controller Requirements

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

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

**Note**

---

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

---

# Software Release Information

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



## Note

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



## Note

The Cisco WiSM is supported on Cisco 7609 and 7613 Series Routers running only Cisco IOS Release 12.2(18)SXF5 or higher.



## Note

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

## Finding the Software Release

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

## Upgrading to a New Software Release

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



## Caution

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

Cisco recommends the following sequence when performing an upgrade:

1. Upload your controller configuration files to a server to back them up.
2. Turn off the controller 802.11a and 802.11b networks.
3. Upgrade your controller to software release 4.0.179.8, following the instructions in the *Cisco Wireless LAN Controller Configuration Guide, Release 4.0*. Click this link to browse to that document:  
[http://www.cisco.com/en/US/products/ps6366/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html)
4. Re-enable your 802.11a and 802.11b networks.

**Note**

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

## New Features

The following new features are supported in controller software release 4.0.179.8.

### Support for 1505 Access Points

The Cisco Aironet 1505 Lightweight Outdoor Mesh Access Point is a wireless device that together with the Cisco Aironet 1510 Lightweight Outdoor Mesh Access Point makes up the 1500 series. It is designed for wireless client access and point-to-point bridging, point-to-multipoint bridging, and point-to-multipoint mesh wireless connectivity. This access point is a standalone unit that can be mounted on a building wall or overhang, on a rooftop pole, or on a street light pole.

The 1505 model differs from the 1510 in that it has only one radio (IEEE 802.11b/g). The 1505 does not use an 802.11a radio, and its 5-GHz antenna connector is removed.

**Note**

At the present time, Cisco mesh networks can be built with either 1505 or 1510 mesh trees. A mesh tree consists of mesh access points connected to a wired rooftop access point (RAP). In a future software release, both models will be able to share a mesh tree.

### Support for Pango Tags

Controller software release 4.0.179.8 supports the use of Pango tags within a wireless network. These small wireless devices, created by PanGo Networks, are affixed to assets for real-time tracking. They operate by sending special radio frequency identification (RFID) packets, which are processed by access points and the controller.

To see a list of Pango tags currently connected to the controller, enter **show rfid summary** from the controller command line interface (CLI). Pango tags have an “unknown” designation, as shown in this example.

RFID ID	TYPE	Closest AP	RSSI	Time Since Last Heard
00:0c:cc:5b:e6:c7	unknown	AP1100	-60	9 seconds ago

### Support for Cisco WiSM on 7609 and 7613 Series Routers

The Cisco WiSM is supported on Cisco 7609 and 7613 Series Routers running only Cisco IOS Release 12.2(18)SXF5 or higher.

# Installation Notes

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

## Warnings



**Warning**

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



**Warning**

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



**Warning**

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



**Warning**

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



**Warning**

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



**Warning**

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



**Warning**

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



**Warning**

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



**Warning**

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

**Warning**

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

## Safety Information

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

### FCC Safety Compliance Statement

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

### Safety Precautions

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

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

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

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

## Installation Instructions

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



### Note

---

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

---

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

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

## Important Notes

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

### Connecting 1100 and 1300 Series Access Points

You must install software release 4.0.179.8 on the controller before connecting 1100 and 1300 series access points to the controller.

### Association Delay for 1500 Series Access Points

The 1500 series access points may take up to 10 minutes to fully associate to the controller on initial startup.

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

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

## Preventing Clients from Accessing the Management Network on a Controller

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

## Voice Wireless LAN Configuration

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

## Inter-Subnet Roaming

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

## Operating Mesh Networks through Switches and Routers

In mesh networks that operate through switches and routers, network round-trip delays between access points and the controller must be less than 100 milliseconds (ms); otherwise, timing problems may occur during wireless client authentication. Also, network path outages of 7 seconds or longer between access points and the controller may cause the access points to lose connectivity.

## Cisco 7920 Wireless IP Phone Support

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

- Aggressive load balancing must be disabled on a per-controller basis. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.
- The QoS Basis Service Set (QBSS) information element (IE) must be enabled. The QBSS IE enables the access points to communicate their channel usage to wireless devices. Because access points with high channel usage might not be able to handle real-time traffic effectively, the 7920 phone uses the QBSS value to determine if they should associate with another access point. Use the following instructions to enable the QBSS IE:

– **sh wlan summary**



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

- **config wlan disable *wlan\_id\_number***
- **config wlan 7920-support ap-cac-limit enable *wlan\_id\_number***
- **config wlan enable *wlan\_id\_number***



- **sh wlan wlan\_id\_number**



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

- **save config**

- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the **config 802.11b dtpc enable** command. The DTPC IE is a beacon and probe information element that allows the access point to broadcast information on its transmit power. The Cisco 7920 Wireless IP Phone uses this information to automatically adjust its transmit power to the same level as the access point to which it is associated. In this manner, both devices are transmitting at the same level.
- Both the 7920 phones and the controllers support Cisco Centralized Key Management (CCKM) fast roaming.
- When configuring WEP, there is a difference in nomenclature for the controller and the 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7920.

## Changing the IOS LWAPP Access Point Password

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

**config ap username user\_id password password {AP\_name | all}**

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

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

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

“ERROR!!! Command is disabled.”

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

## Exclusion List (Blacklist) Client Feature

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

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

## RADIUS Servers and the Management VLAN

The RADIUS server can be on any subnet as long as it can be reached by the management VLAN subnet. The controllers can be managed via the management VLAN subnet from any other subnet that can reach the management VLAN subnet.

## IPSec Not Supported

Software release 4.0.179.8 does not support IPSec. If you upgrade to this release from a previous release that supported IPSec, any WLANs that are configured for this feature become disabled. If you want to use IPSec, you must use a version of controller software prior to 3.2 or wait for a future release.

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

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

## Lightweight Access Point Connection Limitations

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

## RADIUS Servers

This product has been tested with the following RADIUS servers:

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

## Management Usernames and Local Netuser Names

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

## 802.1x and Microsoft Wireless Configuration Manager

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

## Cisco Aironet 1030 Remote Edge Lightweight Access Point Default Operation

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

## Using the Backup Image

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

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

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

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

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

## Rogue Location Discovery Protocol (RLDP)

Enabling RLDP may cause access points connected to the controller to lose connectivity with their clients for up to 30 seconds.

## Ad-Hoc Rogue Containment

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

## Changing the Default Values of SNMP Community Strings

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

### Using the GUI to Change the SNMP Community String Default Values

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

- 
- Step 1** Click **Management** and then **Communities** under SNMP. The SNMP v1 / v2c Community page appears.
  - Step 2** If “public” or “private” appears in the Community Name column, click **Remove** to delete this community.
  - Step 3** Click **New** to create a new community.

- Step 4** When the SNMP v1 / v2c Community > New page appears, enter a unique name containing up to 16 alphanumeric characters in the Community Name field. Do not enter “public” or “private.”
  - Step 5** In the remaining fields, enter the IP address from which this device accepts SNMP packets with the associated community and the IP mask, choose **Read Only** or **Read/Write** to specify the access level for this community, and choose **Enable** or **Disable** to specify the status of this community.
  - Step 6** Click **Apply** to commit your changes.
  - Step 7** Click **Save Configuration** to save your settings.
  - Step 8** Repeat this procedure if a “public” or “private” community still appears on the SNMP v1 / v2c Community page.
- 

## Using the CLI to Change the SNMP Community String Default Values

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

---

- Step 1** To see the current list of SNMP communities for this controller, enter this command:  
**show snmp community**
  - Step 2** If “public” or “private” appears in the SNMP Community Name column, enter this command to delete this community:  
**config snmp community delete *name***  
The *name* parameter is the community name (in this case, “public” or “private”).
  - Step 3** To create a new community, enter this command:  
**config snmp community create *name***  
Enter up to 16 alphanumeric characters for the *name* parameter. Do not enter “public” or “private.”
  - Step 4** To enter the IP address from which this device accepts SNMP packets with the associated community, enter this command:  
**config snmp community ipaddr *ip\_address ip\_mask name***
  - Step 5** To specify the access level for this community, enter this command, where **ro** is read-only mode and **rw** is read/write mode:  
**config snmp community accessmode {ro | rw} *name***
  - Step 6** To enable or disable this SNMP community, enter this command:  
**config snmp community mode {enable | disable} *name***
  - Step 7** To save your changes, enter **save config**.
  - Step 8** Repeat this procedure if you still need to change the default values for a “public” or “private” community string.
-

## Changing the Default Values for SNMP v3 Users

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



### Note

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

## Using the GUI to Change the SNMP v3 User Default Values

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

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

## Using the CLI to Change the SNMP v3 User Default Values

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

- 
- Step 1** To see the current list of SNMP v3 users for this controller, enter this command:  
**show snmpv3user**
  - Step 2** If “default” appears in the SNMP v3 User Name column, enter this command to delete this user:  
**config snmp v3user delete *username***  
The *username* parameter is the SNMP v3 username (in this case, “default”).
  - Step 3** To create a new SNMP v3 user, enter this command:  
**config snmp v3user create *username* {ro | rw} {none | hmacmd5 | hmacsha} {none | des} *auth\_password* *privacy\_password***  
where
    - *username* is the SNMP v3 username,
    - **ro** is read-only mode and **rw** is read/write mode,
    - **none**, **hmacmd5**, and **hmacsha** are the authentication protocol options,
    - **none** and **des** are the privacy protocol options,

- *auth\_password* is the authentication password, and
- *privacy\_password* is the privacy password.

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

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

---

## Web Authentication Limits on Hybrid-REAP Access Points

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

## Features Not Supported on 2000 Series Controllers

These hardware features are not supported on 2000 series controllers:

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

These software features are not supported on 2000 series controllers:

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

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

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

## Pinging from a Network Device to a Controller Dynamic Interface

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

## 2006 Image Not Supported for 3504 Controllers

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

## Running a 3504 Image on a 2000 Series Controller

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

## Upgrading External Web Authentication

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

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

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



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

2. The network manager must use the new login\_template shown here:

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

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

```

    }

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

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

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

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

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

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

<tr align="center">

```



```
<td colspan="2"> User Name &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="TEXT" name="username"
SIZE="25" MAXLENGTH="63" VALUE=""> </td> </tr> <tr align="center" > <td colspan="2">
Password &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="Password" name="password"
SIZE="25" MAXLENGTH="24"> </td> </tr>

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

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

## Caveats

This section lists [Open Caveats](#) and [Resolved Caveats](#) in operating system release 4.0.179.8 for Cisco controllers and lightweight access points.

## Open Caveats

These caveats are open in operating system release 4.0.179.8:

- CSCar14535—When configuring a mobility group anchor that is not part of the mobility member list, the controller displays an “Invalid Parameter Provided” error message.  
Workaround: Make sure that the anchor controller is a mobility group member.
- CSCsb01980—When the operator enters incorrect data for the management interface in the controller web configuration wizard, error messages are shown only at the end of the wizard, and the user must return to the Management Interface page for correction. The data entered on the Management Interface page, such as the port number, are not validated immediately but at the end of the wizard. As a result, any error messages are shown only at the end.  
Workaround: This problem can cause some inconvenience, and the user may prefer to use the CLI configuration wizard instead to avoid it.
- CSCsb01983—The controller web configuration wizard is not reachable after making repeated invalid entries for the management interface port. If an operator connects to the wizard on address 192.168.1.1 and enters an invalid port number on the Management Interface page, the operator is redirected at the end of the wizard to the Management Interface page to correct the port. If the operator enters an incorrect port and submits, the wizard becomes inaccessible.  
Workaround: Reboot the controller through the CLI to access the wizard again.
- CSCsb20269—On the Cisco WiSM, when the service VLAN is configured as one of the VLANs on a data port, it does not operate correctly.  
Workaround: Do not configure the service VLAN as one of the VLANs on a data port.
- CSCsb77595—When logging out from Telnet/SSH sessions, the session always prompts the user to save changes, even when no changes have been made.  
Workaround: Ignore the prompt and exit as usual.
- CSCsb85113—When users download the code image to the Cisco WiSM using the CLI, associated access points are sometimes disconnected.  
Workaround: Download new code images to the WiSM at times when there are no clients to be affected.

- CSCsb87264—If WLAN ID 1 is not configured on the controller, a REAP access point broadcasts the “Airespace” SSID after entering standalone mode. Clients can access this unsecured SSID and use the REAP access point to access the network.

Workaround: Be sure to properly configure WLAN ID 1.

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

Workaround: None for this release.

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

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

- CSCsc03644—Cisco lightweight access points do not retain location parameters after a reboot.

Workaround: None at this time.

- CSCsc04907—Resetting the access point to factory defaults does not clear the static IP address.

Workaround: Clear the access point’s static IP address by hand.

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

Workaround: Apply the Microsoft KB 883659 patch to IAS. The Microsoft patch may or may not work. There is no workaround on the controller.

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

Workaround: None at this time.

- CSCsc20416—ACU site survey disassociates other clients in the LWAPP environment.

Workaround: None at this time.

- CSCsc65354—IDS is unable to detect a deauthentication flood attack under certain conditions.

Workaround: None at this time.

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

Workaround: None at this time.

- CSCsd02837—The CB21AG client adapter may not send re-association requests with CCKM keys when roaming between controllers.

Workaround: Use a different client adapter.

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

Workaround: None at this time.

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

Workaround: None at this time.

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

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

- CSCsd54171—After the controller configuration is modified, the changes may not take effect or function properly.  
Workaround: Reset the controller to factory defaults and then reconfigure the controller exactly the same way.
- CSCsd54750—The Cisco WiSM may display numerous timeout messages.  
Workaround: None at this time.
- CSCsd59421—A wireless client fails to authenticate using 802.1X when the access point is on a different VLAN from the controller.  
Workaround: Configure the access point for the same VLAN as the controller.
- CSCsd69158—After a RADIUS session timeout expires, the access point does not send a unicast key to the client.  
Workaround: None at this time.
- CSCsd82363—Channel utilization is incorrectly reported in radio utilization reports on the controller and in WCS. Channel utilization may appear as zero when there is active client traffic or as an aggregate of client transmit and receive traffic.  
Workaround: None at this time.
- CSCsd85126—The access point may reboot unexpectedly after upgrading to software release 3.2.116.21.  
Workaround: None at this time.
- CSCsd87382—Bridging functionality for REAP devices is not available on OEM builds of controller software.  
Workaround: None at this time.
- CSCsd89139—Pocket PC devices may fail PEAP authentication through a 4400 series controller after resuming from standby.  
Workaround: None at this time.
- CSCsd91042—An access point may reboot when no clients are associated to it.  
Workaround: None at this time.
- CSCsd95992—When IGMPv3 is enabled on the controller, a significant amount of packet loss occurs. The packet loss is even greater when there is an active multicast stream.  
Workaround: None at this time.
- CSCsd96189—A CB21AG client adapter running on Windows XP SP2 experiences two ping timeouts when roaming from an AP1030 to an AP1242, when each is associated to a different 2006 controller.  
Workaround: None at this time.
- CSCse08725—A Vocera badge running MS-PEAP fails when trying to associate to an AP1010. This problem occurs because the controller is dropping the packets.  
Workaround: None at this time.

- CSCse08879—External web authentication fails to operate after upgrading the controller software from 2.2.127.9 to 3.1 or 3.2.

Workaround: Follow these guidelines:

- For 4xxx controllers, add the external web server to the list of external server IP addresses using this command: **config custom-web ext-webserver add server-ip-address**. Then remove the preauthentication ACL configuration for the web authentication WLAN.
- For 2006 controllers, make sure that the preauthentication ACL is configured properly.
- CSCse10109—For WMM clients without TSPEC support, ACM must be disabled for proper QoS mapping.

Workaround: Disable ACM for WMM clients without TSPEC support.

- CSCse10283—An error message may appear on the controller GUI when you try to assign a 4.9-GHz channel to an access point.

Workaround: Before you can assign a 4.9-GHz channel to an access point from the controller GUI, you must enable the 4.9-GHz backhaul feature. To do so, enter this command using the controller CLI: **config ap public-safety enable Cisco\_AP**.

- CSCse14889—The controller does not generate traps for ad-hoc rogues.

Workaround: None at this time.

- CSCse15326—Inconsistent file sizes may occur during configuration backups.

Workaround: None at this time.

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

Workaround: None at this time.

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

Workaround: None at this time.

- CSCse26358—The controller reboots if you enable local switching on any WLAN from 9 through 16.

Workaround: Enable local switching on a WLAN other than 9 through 16.

- CSCse28941—Cisco 1510 series mesh access points (MAPs) can become isolated when deployed in the ETSI (European Telecommunications Standards Institute) domain if the Dynamic Frequency Spectrum (DFS) feature detects what appear to be radar signals, even if no actual radar is present. Because the access point automatically stops using channels on which it detects radar, a MAP can quickly run out of usable channels and be unable to communicate with its rooftop access point (RAP). A MAP with no usable channels becomes isolated and even the lonely recovery mechanism cannot bring it back. You cannot reach or signal a MAP in this state from the controller (WLC) or from a RAP. MAPs in the US domain are not affected by this defect because radar detection is not used for the 5.8 GHz band.

Workaround: None at this time.

- CSCse31241—The backhaul transmit power level cannot be changed for a mesh access point.

Workaround: None at this time.

- CSCse31271—The 4.9-GHz band cannot be changed on the -P regulatory domain if public-safety is disabled.

Workaround: To change the 4.9-GHz band on the -P regulatory domain, enter this command using the controller CLI: **config ap public-safety enable Cisco\_AP**.

- CSCse34673—If you globally disable and then globally enable management frame protection (MFP) on a controller that is part of a mobility group and connected to LWAPP-enabled access points, the access points that are connected to the other controllers within the mobility group may report sequence number MFP anomalies.

Workaround: None at this time.

- CSCse48181—The stateless DHCP proxy on the controller does not properly support DHCP on centrally switched WLANs for access points in H-REAP mode.

Workaround: Use the default DHCP configuration on the controller. In the default configuration, the DHCP server address appears on client devices as 1.1.1.1.

- CSCse56114—Bridge protocol data unit (BPDU) packets are forwarded through the outbound gigabit interface regardless of how the interface is configured.

Workaround: None at this time.

- CSCse63449—The state of the WMM admission control mandatory (ACM) bit is not updated in the access point beacons and probe responses immediately after you configure the Admission Control (ACM) parameter on the controller. Your change does not take effect until the next time the WLAN is enabled.

Workaround: After you change the ACM configuration, disable and then re-enable all of the WLANs with WMM enabled.

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

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

- CSCse76547—Mesh access points (MAPs) fail to join the controller when Ethernet bridging is enabled.

Workaround: Before making any global changes to the access point settings on the controller, disable Ethernet bridging on all access points, make any relevant changes, wait for the access points to rejoin the controller, and then reenable Ethernet bridging on the access points.

- CSCse76633—Hybrid-REAP access points may not receive a configuration response from the controller and therefore experience continuous reboots.

Workaround: None at this time.

- CSCse80234—After you upgrade the controller to a new software release but before the controller is rebooted, access points that join the controller for the first time may become stuck in an image download loop.

Workaround: Reboot the controller to synchronize the primary access point image on the controller and the controller's running code.

- CSCsf06007—Cisco WiSM controllers running software release 4.0.155.5 may experience counter errors for bytes sent and received.

Workaround: None at this time.

- CSCsf06321—WPA2 with AES becomes disabled on hybrid-REAP access points after broadcast key rotation.

Workaround: Use only TKIP with WPA or WPA2.

- 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.

## Resolved Caveats

These caveats are resolved in operating system release 4.0.179.8:

- CSCsd18145—Unicast ARP handling is not optimized.
- CSCsd39873—Controller reports WEP key decryption error with Intel 2200BG clients.
- CSCsd55009—If an AP1200 is rebooted through a software command while a transaction is taking place to control the LEDs, the access point may suddenly lose its connection to the controller. When this occurs, the access point periodically sends out DHCP requests, and its Alarm LED lights.
- CSCsd94967—Access points fail to join a controller when the network path MTU setting is configured for less than 1500 bytes.
- CSCse15233—Access point models other than the 1000 series take longer than expected to fail over to a backup controller when the primary controller fails.
- CSCse30891—Controllers keep a limit of 8 access point tracking entries for a given client or RFID tag.
- CSCse52733—Controllers sometimes reboot when debugs are enabled on the controller and an access point downloads an image from the controller.
- CSCse73315—When the controller is upgraded from software release 3.2.150.10 to 4.0.155.5, any access point group VLAN configuration may be lost.
- CSCse76478—Controllers sometimes fail to join WCS if the length of the shared secret of the AAA server is longer than 32 hexadecimal digits.
- CSCse78916—Guest users can be created on controllers with no timeout.

## Closed Caveats

This caveat has been closed in operating system release 4.0.179.8.

- CSCsf03352—When you change the 802.11a channel on the root access point (RAP), the channel changes on the RAP but may not be propagated to the mesh access points (MAPs). As a result, the MAPs lose connectivity with the controller and never reconnect. This issue may occur if you upgrade your controller from software release 3.2.x.x to 4.0.155.5 or 4.0.179.8.

Workaround: If you encounter this issue, perform one of the following:

- Erase the controller's configuration, reconfigure the controller, and allow the MAPs to rejoin the controller.
- Power-cycle the RAP and MAPs.

## 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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

---

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1005R)

© 2006 Cisco Systems, Inc. All rights reserved.