



# Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 3.2.210.0

---

May 2008

These release notes describe new and changed information as well as open and resolved caveats for operating system release 3.2.210.0 for Cisco 2000, 4100, and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSM); Cisco Wireless LAN Controller Network Modules; and Cisco Aironet 1000, 1130, 1200, 1240, and 1500 Series Lightweight Access Points, which comprise part of the Cisco Unified Wireless Network (Cisco UWN) Solution.



**Note**

---

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

---

## Contents

These release notes contain the following sections:

- [Cisco Unified Wireless Network Solution Components, page 2](#)
- [Controller Requirements, page 2](#)
- [Software Release Information, page 2](#)
- [New and Changed Information, page 3](#)
- [Installation Notes, page 5](#)
- [Important Notes, page 8](#)
- [Caveats, page 18](#)
- [Troubleshooting, page 19](#)
- [Related Documentation, page 19](#)
- [Obtaining Documentation, page 20](#)



---

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

- [Documentation Feedback, page 21](#)
- [Cisco Product Security Overview, page 21](#)
- [Obtaining Technical Assistance, page 22](#)
- [Obtaining Additional Publications and Information, page 23](#)

## 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 3.2.210.0 for all Cisco controllers and lightweight access points
- Cisco Wireless Control System (WCS) software release 3.2.68.0
- Location appliance software release 2.0.48.0
- Cisco 2700 Series Location Appliances
- Cisco 2000, 4100, and 4400 Series Wireless LAN Controllers
- Cisco Wireless Service Module (WiSM) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless LAN Controller Network Module for Cisco Integrated Services Routers
- Cisco Aironet 1000, 1130, 1200, 1240, and 1500 Lightweight Access Points



---

**Note** The 1130, 1200, and 1240 series access points are not supported on the 4100 and 3504 controllers.

---

## 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** Opera, Mozilla, and Netscape are not supported.

---

## Software Release Information

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



---

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

---

## Finding the Software Release

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

## Upgrading to a New Software Release

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

**Caution**

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

Cisco recommends the following sequence when performing an upgrade:

1. Upload your controller configuration files to a server to back them up.
2. Turn off the controller 802.11a and 802.11b networks.
3. Upgrade your controller to software release 3.2.210.0, following the instructions in the *Cisco Wireless LAN Controller Configuration Guide, Release 3.2*. Click this link to browse to that document:

[http://www.cisco.com/en/US/products/ps6366/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html)

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

**Note**

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

## New and Changed Information

### Image Load Protection

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

## Support for Per-WLAN ACLs

Access control lists (ACLs) can be applied to WLANs as well as interfaces. ACLs are applied in the following order:

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

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

```
config wlan acl
```

## Support for Reusable Static WEP Key Indices

The same static WEP key index can be configured for multiple WLANs.

## Power-over-Ethernet Parameters

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

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

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

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

- **Power Injector State**—Check this check box to enable the power injector state for an access point. This parameter is required if the attached switch does not support IPM and a power injector is being used. This parameter is not required if the attached switch supports IPM.

- **Power Injector Selection**—This parameter enables you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed. It appears if you check the Power Injector State check box above. Choose one of these options from the drop-down box to specify the desired level of protection:
  - **Installed**—This option examines and remembers the MAC address of the currently connected switch port and assumes that a power injector is connected. Choose this option if your network contains older Cisco 6-Watt switches and you want to avoid possible overloads by forcing a double-check of any relocated access points.




---

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

---

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

## Installation Notes

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

## Warnings



Warning

---

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

---



Warning

---

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

---

**Warning**

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

**Warning**

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

**Warning**

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

**Warning**

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

**Warning**

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

**Warning**

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

**Warning**

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

**Warning**

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

## Safety Information

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

## FCC Safety Compliance Statement

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

## Safety Precautions

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

For your safety, and to help you achieve a good installation, read and follow these safety precautions.

**They may save your life!**

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

## Installation Instructions

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



**Note**

---

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

---

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

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

## Important Notes

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

### 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.

## L2TP Not Supported

Software release 3.2.210.0 does not support L2TP. If you upgrade to this release from a previous release that supported L2TP, any WLANs that are configured for that feature become disabled. If you want to use L2TP you must use a version of controller software prior to 3.2 or wait for the next 3.2 release.

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

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

## Voice WLAN Configuration

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

## Inter-Subnet Roaming

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

## Operating Mesh Networks Through Switches and Routers

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

## Heavily Loaded Controller CPU

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

## RADIUS Servers and the Management VLAN

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

## Cisco 7920 Wireless IP Phone Support

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

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

– **sh wlan summary**



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

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




---

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

---

- **save config**
- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the **config 802.11a dtpc enable** command. The DTPC IE is a beacon and probe information element that allows the access point to broadcast information on its transmit power. The Cisco 7920 Wireless IP Phone uses this information to automatically adjust its transmit power to the same level as the access point to which it is associated. In this manner, both devices are transmitting at the same level.
- The 7920 phones and the controllers do not currently use compatible fast roaming mechanisms. The phone uses CCKM while the controllers use proactive key caching (PKC). To minimize roaming latency, static WEP is the recommended security mechanism.
- When configuring WEP, there is a difference in nomenclature for the controller and the 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7920.

## Client Channel Changes

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

## Exclusion List (Blacklist) Client Feature

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

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

## Maximum MAC Filter Entries

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

**config database size** *MAC\_filter\_entry*

where *MAC\_filter\_entry* is a value from 512 to 2048.

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

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

### RADIUS Servers

This product has been tested with the following RADIUS servers:

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

### Management Usernames and Local Netuser Names

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

### 802.1x and Microsoft Wireless Configuration Manager

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

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

When a controller reboots, dropped Cisco Aironet 1030 Remote Edge Lightweight Access Points attempt to associate to any available controller. If the access points cannot contact a controller, they continue to offer 802.11a/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){
```



# Caveats

This section lists resolved and closed caveats in operating system release 3.2.210.0 for Cisco controllers and lightweight access points.

## Resolved Caveats

These caveats are resolved in operating system release 3.2.210.0.

- 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.
- CSCsh97956—WLC cannot resolve ARP issue after software update.
- CSCsi41700—ARP does not work on WLC4000 R3.2 software.
- CSCsi67145—A 404 Not Found error displays when you click the GUI link to Preview your web auth login page. This is a result of the link sending you to [http://WLC-IP/login\\_preview.html](http://WLC-IP/login_preview.html) instead of [http://WLC-IP/screens/base/login\\_preview.html](http://WLC-IP/screens/base/login_preview.html). If you manually enter the correct path, the page displays properly.
- CSCsj97775—From the the monitor page of a controller running 3.2.195.10, when selecting Radio 802.11b/g and the details for one of the access points listed, a "Page not found" error displays.
- CSCsk18471—A wireless client associated to a wireless controller cannot communicate one direction to other clients from time to time, when they are roaming. Users of voice communication clients can experience one-way voice sessions.
- CSCsk23015—A REAP mode access point at times cannot join with the primary WLC when recovering the primary WLC.
- CSCsk97940—If rates 1.48 and 54 mbps are disabled, association responses include 24 M as supported rate and extended supported rate.
- CSCsl09407—A emWeb system crash occurs occasionally on the controller during telnetting to the controller.
- CSCsl41103—Beacon is not sent correctly when 11g is enabled.




---

**Note** If 11g is enabled while using 14ch, the channel 14ch changes to 1ch. However, the channel stays at 1ch if 11g is disabled after changing to 1ch. A warning message displays when the channel is changed.

---

- CSCsl61657—Wireless clients that only support long slot time (20 microseconds) have difficulties associating to access points.
- CSCsm11640—Wireless Controller (WLC4136) crashed at SNMPTask.
- CSCsm21340—WLC crashed at pemReceiveTask.
- CSCsm22946—WLC experiences an access point crash during network affection testing.
- CSCsm45577—One-way audio occurred after L3 hand-over.
- CSCsm52401—One-way audio occasionally occurs.
- CSCso54501—Access point crash occurred on L3 mode during switch-over testing.
- CSCso59867—Country code CY does not allow the user to configure 5GHz band channels in the 100 - 140 range.

## Closed Caveats

These caveats have been closed in operating system release 3.2.210.0

- CSCs109263—The controller occasionally crashes with no crash log.  
Workaround: None.
- CSCs111236—The configuration change on an individual controller's 802.11b/g parameter (Configure > Controllers > 802.11b/g > Parameters) throws the following exception: [ServletException in:/pages/configure/global/dot11bConfigDetail.jsp] No bean found under attribute key switchingForm.
- CSCs111361—The roaming candidate AP list sometimes contains incorrect parameters.
- CSCsm75468—AS-4024 crashed due to Deadlock.  
Workaround: None.
- CSCsm88913—Removing a mobile client on Anchor WLC GUI causes ARP look-up failure if the client associates with a dynamic interface.  
Workaround: None.
- CSCso26974—API000 experienced system restart due to "Assert in Software Task".  
Workaround: None.
- CSCsm23104—When the WLC is operating under low memory and stress conditions, it may display the invalid message "<BODY class="bodyattributes" when 802.11a Radios or 802.11b/g Radios is selected from the GUI. If the controller doesn't recover automatically, the controller may need a reboot to recover.  
Workaround: None.

## Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/en/US/support/index.html>

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

## Related Documentation

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

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

You can access these documents from this link:

[http://www.cisco.com/en/US/products/hw/wireless/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html)

## Obtaining Documentation

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

### Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

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

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

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

### Ordering Documentation

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

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

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

# Documentation Feedback

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

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

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

We appreciate your comments.

## Cisco Product Security Overview

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

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

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

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

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

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

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

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

- For Emergencies only—[security-alert@cisco.com](mailto:security-alert@cisco.com)

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

- For Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

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

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

**Tip**

---

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

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

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

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

---

## Obtaining Technical Assistance

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

## Cisco Technical Support & Documentation Website

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

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

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

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

**Note**

---

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

---

## Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

## Definitions of Service Request Severity

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

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

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

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

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

## Obtaining Additional Publications and Information

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

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

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:  
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:  
<http://www.cisco.com/go/iqmagazine>  
or view the digital edition at this URL:  
<http://cisoiq.texterity.com/cisoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:  
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:  
<http://www.cisco.com/en/US/learning/index.html>

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

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

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

© 2006 Cisco Systems, Inc. All rights reserved.