Release Notes for Cisco Wireless LAN Controllers and Mesh Access Points for Release 4.0.217.204

September 27, 2007

These release notes describe open and resolved caveats for software release 4.0.217.204 for Cisco 2000, 2100, and 4400 Series Wireless LAN Controllers; Cisco Wireless Services Modules (WiSM); Cisco Wireless LAN Controller Network Modules; Catalyst 3750G Integrated Wireless LAN Controller Switches; Cisco 3201 Wireless Mobile Interface Cards (WMIC); and Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 Series Lightweight Access Points (1505 and 1510), which are 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*.

Caution Please see the "Upgrading to a New Software Release" section on page 3 for important software upgrade and compatibility details prior to upgrading to this release.

Contents

These release notes contain the following sections.

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

Cisco Unified Wireless Network Solution Components

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

- Software release 4.0.217.204 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 4.0.96.0
- Location appliance software release 2.1.42.0
- Cisco 2700 Series Location Appliances
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 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 3201 Wireless Mobile Interface Card (WMIC)
- Cisco Aironet 1000, 1100, 1130, 1200, 1240, 1300, and 1500 (1505 and 1510) Series Lightweight Access Points

Controller Requirements

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

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

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

Software Release Information

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

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

Note The Cisco WiSM is supported on Cisco 7609 and 7613 series routers running only Cisco IOS release 12.2(18)SXF5 or higher.

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, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported in software release 4.0.217.204, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Cisco recommends the following sequence when performing an upgrade:

1. Upload your controller configuration files to a server to back them up.
2. Turn off the controller 802.11a and 802.11b networks.
3. Upgrade your controller to the latest software release, following the instructions in the *Cisco Wireless LAN Controller Configuration Guide, Release 4.0.* Click this link to browse to that document:

   http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html
4. Re-enable your 802.11a and 802.11b networks.

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

Upgrade Path to Release 4.0.217.204

Details for upgrading your network to release 4.0.217.204 from earlier releases of 3.1, 3.2 and 4.0 are described below:

- If your controller is installed with release 4.0.xx or 3.2.xx, you can upgrade directly to release 4.0.217.204.
- If your controller is installed with release 3.1.x, you must upgrade with one intermediate release prior to installing release 4.0.217.204.
  - First, upgrade to 3.2.195.10
  - Secondly, upgrade to 4.0.217.204.

Note

- If you are operating with indoor and outdoor access points in your network in Europe, Singapore and other countries requiring Dynamic Frequency Selection (DFS) functionality, you should install release 4.0.217.204.
- For the US and other countries that do not require DFS functionality:
  - Install 4.1.190.5 for outdoor mesh networks operating with Cisco Aironet 1500 (1505 and 1510) and 1520 series access points (1522).
  - If you are operating with indoor and outdoor access points (1505, 1510, and 1522), you will need to place all mesh traffic on a controller running release 4.1.190.5 and all indoor access points on a controller running release 4.1.185.0 or earlier 4.1.x version. Refer to the release notes for 4.1.190.5 and 4.1.185.0 at the following link for details on these releases: http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html
  - If you are operating with indoor and outdoor access points *excluding* 1522, you can operate with either release 4.1.185.0 or 4.1.190.5. (In the case of release 4.1.190.5, you must maintain separate controllers for indoor and outdoor access points as noted above.)
  - If you are operating with indoor access points only, you should install the latest non-mesh controller release such as 4.1.185.0.

Upgrade Compatibility Matrix

Table 1 outlines the upgrade compatibility of controller non-mesh releases and indicates the intermediate software releases required as part of the upgrade path. A summary of upgrade path requirements is noted in the "Upgrade Path to Release 4.0.217.204" section on page 4.

Table 1 Upgrade Compatibility Matrix for Controller Non-Mesh Releases

Upgrade from \ Upgrade to	4.0.217.204[1]	4.0.217.0	4.0.216.0	4.0.206.0	4.0.179.11	4.0.179.8	4.0.155.5	4.0.155.0	3.2.195.10	3.2.193.5	3.2.171.6	3.2.171.5	3.2.150.10	3.2.150.6	3.2.116.21	3.2.78.0	3.1.111.0	3.1.105.0	3.1.59.24
4.0.217.204[1]	–																		
4.0.217.0		–																	
4.0.216.0		Y	–																
4.0.206.0		Y		–															
4.0.179.11		Y		Y[2]	–														
4.0.179.8		Y		Y[2]	Y	–													
4.0.155.5		Y		Y[2]	Y	Y	–												
4.0.155.0		Y		Y[2]	Y	Y	Y	–											
3.2.195.10		Y		Y[2]	Y	Y	Y		–										
3.2.193.5		Y		Y[2]	Y	Y	Y		Y	–									
3.2.171.6		Y		Y[2]	Y	Y	Y		Y		–								
3.2.171.5		Y		Y[2]	Y	Y	Y		Y		Y	–							
3.2.150.10		Y		Y[2]	Y	Y	Y		Y		Y		–						
3.2.150.6		Y		Y[2]	Y	Y	Y		Y		Y		Y	–					
3.2.116.21		Y		Y[2]	Y	Y	Y		Y		Y		Y		–				
3.2.78.0		Y		Y[2]	Y	Y	Y		Y		Y		Y		Y	–			
3.1.111.0									Y		Y		Y		Y	Y	–		
3.1.105.0									Y		Y		Y		Y	Y	Y	–	
3.1.59.24									Y		Y		Y		Y	Y	Y	Y	–

1. Only for mesh networks operating in countries outside the US that require DFS functionality.
2. An upgrade to 4.0.206.0 is not allowed in the following Country Codes when operating with the following access points: Australia (1505 and 1510), Brazil (1505 and 1510), Hong Kong (1505 and 1510), India (1505 and 1510), Japan (1510), Korea (1505 and 1510), Mexico (1505 and 1510), New Zealand (1505 and 1510), and Russia (1505 and 1510).

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 new features and operational notes about the controllers and access points.

NEW Features

Radar Detected by One Mesh Access Point is Forwarded to All in the Sector

When a mesh access point (MAP) detects radar in a sector, that information is forwarded to all mesh access points within that sector; and all MAPs and RAPs belonging to that sector will move to the new channel. This functionality lowers the probability of MAP strandings.

- To enable this functionality in a mesh network, enter the following CLI command:

  config mesh full-sector-dfs *enable*

- To prevent the RAP from moving its sector back to the previously configured channel, enter the following command:

  config advanced 802.11a channel delete *channel-number*

- To disable this functionality in a mesh network, enter the following CLI command:

  config mesh full-sector-dfs *disable*

Note

- While traffic is moved to a new channel, the MAPs remain connected to the controller but transmissions on the network are silent for one minute in keeping with the DFS standard. Transmission resumes after the minute silence on the new channel.
- If a MAP detects radar immediately after the first detection, the MAPs in the sector disconnect from the controller.
- If a MAP is connected to a RAP with a default bridge group name (BGN), the MAP does not relay the radar detection message to the RAP.

Dynamic Frequency Selection Added to Access Points in -A Regulatory Domain

In controller software release 4.0.217.204, dynamic frequency selection (DFS) is enabled automatically on the following Cisco lightweight access points that are configured for use in the -A regulatory domain (U.S., Canada, and Philippines): 1130, 1230, and 1240. DFS affects 8 channels (52 to 64) on the 802.11a radio within the 5.470 to 5.725 GHz frequency band. The access points use DFS to detect radar signals such as military and weather sources and then switch channels to avoid interfering with them.

DHCP Bridging

You can enable or disable the DHCP Proxy functionality on a controller. This feature is either enabled or disabled on a global basis rather than on a WLAN-by-WLAN basis using the following command:

config dhcp proxy {**enable** | **disable**}

Note DHCP Proxy is enabled by default. All controllers that will communicate must have the same DHCP Proxy setting.

When DHCP Proxy is enabled on a controller, the controller unicasts DHCP requests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself.

When DHCP Proxy is disabled on a controller, those DHCP packets transmitted to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are removed from the LWAPP tunnel and transmitted on the upstream VLAN. DHCP packets directed to the client are received on the upstream VLAN, converted to 802.11 packets and transmitted through an LWAPP tunnel toward the client. As a result, the internal DHCP server cannot be used when the DHCP Proxy is disabled.

Note In earlier releases, disabling DHCP Proxy only changed how the attributes were inserted and removed from the DHCP packets. Packets were still proxied by the controller to the configured DHCP servers.

Operational Notes

UNII-2 Channels Disabled for New 1000 Series Access Points

Newer versions of the Cisco 1000 series lightweight access points do not support the UNII-2 band (5.25 to 5.35 GHz). These models are labeled AP10x0-B, where "B" represents a new regulatory domain that replaces the previous "A" domain. In the B regulatory domain, all UNII-2 channels are disabled.

2106 Controller LEDs

The 2106 controller's Status LED and AP LED do not flash amber when software is being uploaded to the controller or downloaded to an access point, respectively.

Note Some versions of the *Cisco 2106 Wireless LAN Controller Quick Start Guide* may incorrectly state that these LEDs flash amber during a software upload or download.

Controller Functions that Require a Reboot

After you perform these functions on the controller, you must reboot the controller in order for them to take effect:

- Switch between Layer 2 and Layer 3 LWAPP mode
- Enable or disable link aggregation (LAG)
- Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
- Enable or disable the mobility protocol port using this CLI command:

  config mobility secure-mode {**enable** | **disable**}

Resetting the Configuration on 2006 Controllers

If you wish to reset the configuration to factory defaults on a 2006 controller, perform one of the following:

- From the controller GUI, click **Commands > Reset to Factory Default > Reset**.
- From the controller CLI (after system bootup and login), enter **clear config**. Then after the configuration has been cleared, enter **reset system** without saving the current configuration.
- From the controller console (after system bootup), enter **Recover-Config** from the User Name prompt.

Caution Do not attempt to reset the controller's configuration by choosing Option 5, Clear Config from the boot menu unless you have successfully upgraded to the _ER.aes image on Cisco.com. For more details see details for CSCsg18356 at the following link:
http://www.cisco.com/en/US/docs/wireless/controller/release/notes/cont402060rn.html

Rate-Limiting on the Controller

Cisco recommends that you always run the controller with the default **config advanced rate enable** command in effect in order to rate-limit traffic to the controller and protect against denial-of-service (DoS) attacks. You can use the **config advanced rate disable** command to stop rate-limiting of Internet Control Message Protocol (ICMP) echo responses for testing purposes. However, Cisco recommends that you reapply the **config advanced rate enable** command after testing is complete.

Re-enable Broadcast after Upgrading to Release 4.0.206 or Later

In software releases 4.0.179 and earlier, broadcast and multicast forwarding were both controlled with a single global flag that enabled multicast. In software release 4.0.206 these functions were broken into separate configuration flags: one that controls broadcast and one that controls non-broadcast multicast. If you have multicast enabled in software releases 4.0.179 and earlier, the broadcast flag is left disabled after upgrading to software release 4.0.206. As a result, some applications that rely on broadcast do not work after the upgrade.

After you upgrade to software release 4.0.206.0 or later, use this CLI command to re-enable broadcast:

config network broadcast enable

When re-enabled, broadcast uses the multicast mode configured on the controller. If you want to turn on broadcast only and set it to another multicast mode you must use the CLI because the GUI configuration forces multicast on.

Service Modules Supported in the Catalyst 6500 Series Switch

The Catalyst 6500 Series Switch chassis can support up to five Cisco WiSMs without any other service module installed. If one or more service modules are installed, the chassis can support up to a maximum of four service modules (WiSMs included).

Connecting 1100 and 1300 Series Access Points

You must install software release 4.0.179.8 or later 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.

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 for each controller. 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 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 802.11b 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 when the CLI commands are applied:

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 client are 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

If a RADIUS server is on a directly connected subnet (with respect to the controller), then that subnet must be the management VLAN subnet.

IPSec Not Supported

Software release 4.0.206.0 and later releases do not allow you to choose IPSec as a Layer 3 Security option. None and VPN Passthrough are the only available options. If you upgrade to this release from a previous release that supported IPSec as a Layer 3 Security option, any WLANs that are configured for this feature become disabled. If you want to configure IPSec, you must use a version of controller software prior to 4.0 or wait for a future release.

Cisco 1000 Series Access Points and WMM

- In order to use Layer 2 LWAPP mode and WMM with a 1000 series access point, you must make sure that WMM is disabled.
- Clients cannot associate to an AP1030 in REAP mode if WMM is enabled on the WLAN. Disable WMM to allow the clients to associate.

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 v4.0
- Funk Steel-Belted RADIUS release 4.4.137

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

Because of a caching problem in the Internet Explorer 5.x browser, the home page retains the web authentication login. To correct this problem, 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 apply 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 time zone 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**.

Features Not Supported on 2000 and 2100 Series Controllers

These hardware features are not supported on 2000 and 2100 series controllers:

- Power over Ethernet (PoE) for 2000 series controllers only

Note Ports 7 and 8 on 2100 series controllers are PoE ports.

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

These software features are not supported on 2000 and 2100 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
- Link aggregation (LAG)

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.

Ethernet Multicast Mode Required to Support IPv6

Ethernet Multicast Mode (EMM) is required to support IPv6. If you disable EMM, client devices using IPv6 lose connectivity.

Access Point LEDs Sometimes Require Extra Time to Display Status

Access point LEDs sometimes require extra time to display a change in status. For example, when an access point is searching for a controller, the search begins several seconds before the LEDs report that status.

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> </td></tr>

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

<tr align="center">

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

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

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

Caveats

This section lists Open Caveats and Resolved Caveats for Cisco controllers and lightweight access points in software release 4.0.217.204.

Open Caveats

The caveats listed below are open in controller software release 4.0.217.204.

- 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.

- 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: Save the controller configuration to a TFTP server or WCS; then reset the controller to restore the default configuration. After completing the setup wizard, reload the saved configuration from the TFTP server or WCS.

- CSCsg12879—When you attempt to disable power-over-Ethernet (PoE) through the controller GUI, the following error message appears: “Error is setting Power Over Ethernet.”

  Workaround: None at this time.

- CSCsg36747—The **Clear Counters** button on the Controller Statistics page does not clear the controller’s counters.

  Workaround: None at this time.

- CSCsg44650—Cisco Discovery Protocol (CDP) does not operate correctly when a 2106 controller is connected to a 3750 switch. The controller sees the 3750 chassis as a CDP neighbor, but the 3750 does not recognize the 2106.

  Workaround: None at this time.

- CSCsg55649—Internet Group Management Protocol (IGMP) V3 join reports sent by the client upon starting a multicast application may be duplicated to one of the controller ports in the link aggregation (LAG) bundle.

  Workaround: None at this time.

- CSCsg65482—Controllers sometimes drop multicast packets in unicast or multicast mode.

  Workaround: None at this time.

- CSCsg71421—The **show qos profile** command does not operate properly. The controller does not allow any further input after this command is entered.
- CSCsg74578—If you change a controller's management IP address, it is not sent to the access point unless the access point is reset. As a result, multicasting does not work until the change is made on the access point.

  Workaround: None at this time.
- CSCsg78130—The controller sometimes successfully loads a new controller software image but fails to load the accompanying access point images.

  Workaround: None at this time.
- CSCsh13928—Access points sometimes disconnect from the controller intermittently in large deployments in busy radio environments.

  Workaround: Disable radio management (RM) and configure static settings for channels and power.
- CSCsh99970—The Country page on the controller GUI appears to limit the country code that you can enter to two characters.

  Workaround: Backspace to delete the characters in the code entry field and enter the three-character country code.
- CSCsi05119—Changing the Serial Port Login Timeout from the controller GUI makes the 2106 controller unreachable. However, you can still access the controller using the CLI.

  Workaround: Cold start the controller.
- CSCsi06504—When a Mesh access point is configured with the wrong static IP address, it never falls back to DHCP and fails to join the controller.

  Workaround: Log into the access point console and remove the static IP address in the boot prompt.
- CSCsi15249—Access points in HREAP mode sometimes repeat DFS scans at various times.

  Workaround: None.
- CSCsi23248—Neighboring access points sometimes fail to join the same RM group when they detect neighboring access points.

  Workaround: None.

Resolved Caveats

The caveats listed below represent those bugs resolved since controller software release 4.0.217.0.

- CSCsg83730—In some cases, some DHCP servers might not work with the controller's DHCP relay and proxy function. Issue was addressed by adoption of a new DHCP Bridging feature in 4.0.217.204. A summary of the feature is addressed in this release note.
- CSCsh12876—A high error rate was reported on a MAP due to acknowledgement delays between the RAP and the MAP.
- CSCsh12897—A MAP would not associate with a controller when there were fewer than two DFS channels available.
- CSCsh12911—Configurations for access points that were operating in MAP mode were sometimes corrupted after a software upgrade.
- CSCsh13158—When a bridged mesh access point could not access any non-DFS channels, it would reboot and sometimes would not join the controller upon reboot.

- CSCsh20492—Access points in MAP mode sometimes rebooted after they received a configuration request from the controller.
- CSCsi22591—Changing the 802.11a channel on the RAP access point turned off RRM channel assignment on the 802.11b radios for all the access points on the sector.
- CSCsi49767—When a WLAN was configured with an interface that had an ACL and an AP group had been applied on the access point that overrode the ACL, the controller sometimes crashed when a client associated to the access point.
- CSCsi68958—MAP reported radar events on the backhaul when radar was detected on another channel. The MAP would send radar detect messages to the controller and the controller would change the MAP's channel. This could cause a scanning MAP to become stranded.
- CSCsj69233, CSCsj70841—In certain configurations, controllers had problems handling Address Resolution Protocol (ARP) packets from wireless clients that could result in a denial of service (DoS) in certain environments.

Closed Caveats

- 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. The workaround is to use the CLI configuration wizard.
- 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. The workaround is to reboot the controller through the CLI to access the wizard again.
- CSCsh81683—The WiSM controller sometimes becomes unmanageable: it cannot be pinged or accessed through telnet or other protocols. Disabling Gigabit ports 3 and 4 on the Catalyst 6000 switch side of the port channel causes the WiSM to become fully operational. The workaround is to reboot the WiSM.
- CSCsi32464—The controller sometimes drops data traffic when the controller moves to the backup port on the same NPU. The workaround is to configure the backup port as port 3.

If You Need More Information

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

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

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

Troubleshooting

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

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

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

Documentation Updates

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

Omissions

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

- DB-9 to DB-9 null modem cable

Related Documentation

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

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

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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