



Release Notes for Cisco Aironet 350, 1100, 1130AG, 1200, and 1230AG Series Access Points for Cisco IOS Release 12.3(2)JA

November 9, 2004

These release notes describe features, enhancements, and caveats for Cisco IOS Release 12.3(2)JA. They also provide important information about Cisco Aironet 350, 1100, 1130AG, 1200, and 1230AG series access points.

Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Updates to Existing Features, page 5](#)
- [New Features, page 6](#)
- [Installation Notes, page 8](#)
- [Important Notes, page 12](#)
- [Caveats, page 20](#)
- [Troubleshooting, page 26](#)
- [Related Documentation, page 26](#)
- [Obtaining Documentation and Submitting a Service Request, page 26](#)



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Introduction

The Cisco Aironet Access Point is a wireless LAN transceiver that acts as the connection point between wireless and wired networks or as the center point of a standalone wireless network. In large installations, the roaming functionality provided by multiple access points enables wireless users to move freely throughout the facility while maintaining uninterrupted access to the network.

You can configure and monitor 350, 1100, and 1200 series access points using the command-line interface (CLI), the web-browser interface, or Simple Network Management Protocol (SNMP).

System Requirements

You can install Cisco IOS Release 12.3(2)JA on all 1100 series access points, 1130AG access points, and on 1230AG access points.



Note

Software upgrades fail when you use the web-browser interface to install Cisco IOS Release 12.3(2)JA on 1200 series access points. The image size exceeds the access point's 4-MB restriction for software upgrades. Use TFTP to upgrade your 1200 series access point to this release. For complete instructions on using TFTP to upgrade access point software, see the "Working with Software Images" section in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*. Click this link to browse to that document:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/tsd_products_support_configure.html

You can also install this release on 350 and 1200 series access points that have been converted to run Cisco IOS software. You can tell whether an access point runs VxWorks or Cisco IOS software by looking at the GUI: the GUI on an access point running VxWorks has a yellow and red color scheme, and the GUI on an access point running Cisco IOS software has a green, light-green, and black color scheme.

Your 350 series access point must run one of these VxWorks versions before you can convert to IOS software: 12.03T, 12.02T1, 12.01T1, 11.23T, or 11.21. Your 1200 series access point must run one of these VxWorks versions before you can convert to IOS software: 12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, or 11.54T. If your access point runs version 12.04, you must downgrade to a supported VxWorks version before upgrading to IOS software.

The conversion upgrade image for 350 series access points installs Cisco IOS Release 12.2(13)JA1 on your 350 series access point. The conversion upgrade image for 1200 series access points installs Cisco IOS Release 12.2(13)JA2 on your 1200 series access point.



Note

Cisco Aironet 340 Series Access Points do not support IOS software. Do not attempt to load an IOS image on 340 series access points or on 350 and 1200 series access points that have not been converted.

Finding the IOS Software Version

To find the version of IOS software running on your access point, use a Telnet session to log into the access point and enter the **show version EXEC** command. This example shows command output from an access point running Cisco IOS Release 12.2(15)JA:

```
ap1200>show version
Cisco Internetwork Operating System Software
```

IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.2(15)JA
Copyright (c) 1986-2004 by Cisco Systems, Inc.

On access points running IOS software, you can also find the software version on the System Software Version page in the access point's web-browser interface. If your access point does not run IOS software, the software version appears at the top left of most pages in the web-browser interface.

Upgrading to a New Software Release

For instructions on installing access point software:

1. Follow this link to the Cisco Aironet Install and Upgrade page:
http://www.cisco.com/en/US/products/hw/wireless/ps430/tsd_products_support_install_and_upgrade.html
2. Click this link to browse to the Cisco IOS Software Center on Cisco.com:
<http://www.cisco.com/cisco/software/navigator.html>
Log into Cisco.com to use the Cisco IOS Upgrade Planner.

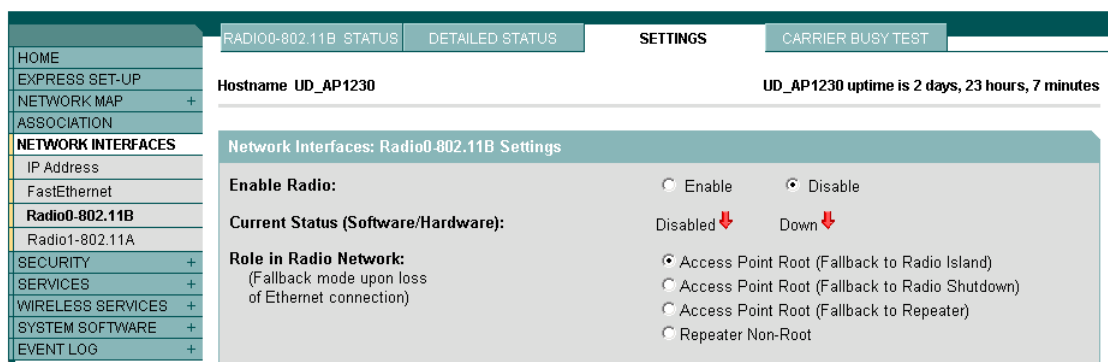
Disable Radios to Prevent Unexpected Reboot When Upgrading System Software

If your access point runs Cisco IOS Release 12.2(11)JA, 12.2(11)JA1, or 12.2(11)JA2, your access point might unexpectedly reboot after you upgrade to a later Cisco IOS Release. Because of a rare timing condition that affects the radios, the access point sometimes reboots immediately after the upgrade when the radios are enabled. However, after the access point reboots the upgrade is complete and the access point operates normally. To prevent the access point from rebooting unexpectedly, disable the radio interfaces before upgrading software.

Follow these steps to disable the radio interfaces using the web-browser interface:

- Step 1** Browse to the Network Interfaces: Radio Settings page. [Figure 1](#) shows the top portion of the Network Interfaces: Radio Settings page.

Figure 1 Network Interfaces: Radio Settings Page



- Step 2** Select **Disable** to disable the radio.

Step 3 Click **Apply** at the bottom of the page.

Step 4 If your access point has two radios, repeat these steps for the second radio.

Beginning in privileged EXEC mode, follow these steps to disable the access point radios using the CLI:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio {0 1}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	shutdown	Disable the radio port.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

If your access point has two radios, repeat these steps for the second radio. Use the **no** form of the **shutdown** command to enable the radio.

Converting to Cisco IOS Software

If your 350 or 1200 series access point does not run IOS software, you can use the conversion utility or the conversion upgrade image to convert the access point system to IOS software. Use the conversion utility to maintain the current configuration after the conversion, or load the upgrade image to convert to IOS software without saving the current configuration. Your access point must be running one of these VxWorks firmware versions before you can convert to IOS software:

- 350 series access points must be running VxWorks version 12.03T, 12.02T1, 12.01T1, 11.23T, or 11.21
- 1200 series access points must be running VxWorks version 12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, or 11.54T

The conversion upgrade image for 350 series access points installs Cisco IOS Release 12.2(13)JA1 on your 350 series access point. The conversion upgrade image for 1200 series access points installs Cisco IOS Release 12.2(13)JA2 on your 1200 series access point.



Note

The upgrade image and the conversion tool do not support VxWorks version 12.04. Access points running version 12.04 must be downgraded to a supported operating system version before you can use the upgrade image or the conversion tool.



Note

The upgrade to Cisco IOS software is permanent; you cannot revert to non-IOS software. Product warranties do not cover unintended upgrades.

For complete instructions on using the conversion utility, refer to the *Cisco Aironet Conversion Tool for Cisco IOS Software, 2.1 Administrator Guide for Windows*. Click this link to browse to the Administrator Guide:

http://www.cisco.com/en/US/docs/wireless/access_point/conversion/ios/administration/guide/tool3ios.html

To download the conversion utility or the upgrade image, click this link to browse to the Cisco IOS Software Center on Cisco.com:

<http://www.cisco.com/cisco/software/navigator.html>

On the Cisco IOS Software Center page, enter your Cisco.com username and password to use the Feature Navigator or the Cisco IOS Upgrade Planner, or click **Wireless Software** to go to the Wireless LAN Software page. Download the conversion utility or the upgrade image for 350 or 1200 series access points. You can also download instructions for using the utility and the image.

Some Fields Not Updated During Upgrade to IOS Software

When you upgrade an access point to run Cisco IOS software, some fields that are reported in the console messages during the upgrade are blank or are populated with zeros. However, blank or zero fields are normal after a successful upgrade, because 350 and 1200 series access points do not support that information. This example shows fields that might appear blank or populated with zeros:

```
32K bytes of flash-simulated non-volatile configuration memory.
Base Ethernet MAC Address: 00:05:9A:38:42:91
Part Number                : 0-0000-00
PCA Assembly Number        : 000-00000-00
PCA Revision Number        :
PCB Serial Number          :
Top Assembly Part Number   : 000-00000-00
Top Assembly Serial Number :
Top Revision Number        :
Product/Model Number       : AIR-AP352-IOS-UPGRD
```

Updates to Existing Features

Table 1 lists updates to existing features in Cisco IOS Release 12.2(15)XR and earlier. Cisco IOS Software Release 12.3(2)JA includes these updates for these features and platforms.

Table 1 Updates to Existing Features in Cisco IOS Release 12.3(2)JA

Existing Feature	1100 Series	1130AG Series	1230AG Series
IP-Based Wireless Domain Services (WDS)	x	x	x
Layer 3 Mobility Service via Fast Secure Roaming Tunnels	x	x	x
Work Group Bridge (WGB) Mode	x	—	—

New Features

This section lists new features in Cisco IOS Release 12.3(2)JA. [Table 2](#) lists the features that are supported on the devices that support this release.

Table 2 *New Features Introduced for Access Points in Cisco IOS Release 12.3(2)JA*

Feature	350 Series ¹	1100 Series	1130AG Series	1200 Series	1230AG Series
Support for Cisco Aironet IEEE 802.11a Radio Part Numbers AIR-RM21A and AIR-RM22A	–	–	x	x	x
Support for Cisco Aironet 1130AG and 1230AG Series Access Points	–	–	x	–	x
HTTPS - HTTP with SSL 3.0	x	x	x	x	x
AES-CCMP	–	x ²	x	x ³	x ⁴
IEEE 802.1X Local Authentication Service for EAP-FAST	x	x	x	x	x
Wi-Fi Multimedia (WMM) Required Elements	x	x	x	x	x
VLAN Assignment by Name	x	x	x	x	x
Microsoft WPS IE SSIDL ⁵	x	x	x	x	x
HTTP Web Server v1.1	x	x	x	x	x
IP-Redirect	–	x	x	x	x

1. Cisco Aironet 350 Series Access Points support the same feature set as an 1100 series access point, except that a 350 series access point cannot serve as a WDS access point.
2. IEEE 802.11g radio only
3. IEEE 802.11g and 802.11a radios only with the part numbers AIR-RM21A or AIR-RM22A
4. IEEE 802.11g and 802.11a radios only with the part numbers AIR-RM21A or AIR-RM22A
5. The ability to read SSIDL is planned for a future Microsoft service pack Windows XP release.

Support for Cisco Aironet 1230AG and 1130AG Series Access Points

Support for Cisco Aironet 1230AG series and Cisco Aironet 1130AG series access points is now available. These access points support all access point features introduced in Cisco IOS Software Release 12.3(2)JA, as well as all features supported by Cisco Aironet 1100 Series and 1200 Series access points in Cisco IOS Software Releases 12.2(15)JA, 12.2(15)XR, and earlier releases.

Support for Cisco Aironet IEEE 802.11a Radio Part Numbers AIR-RM21A and AIR-RM22A

Cisco IOS Software release 12.3(2)JA introduces support for the Cisco Aironet 1200 Series access point IEEE 802.11a radio part numbers AIR-RM21A and AIR-RM22A. These new IEEE 802.11a radios support all access point features introduced in Cisco IOS Software release 12.3(2)JA as well as all Cisco IOS Software access point features supported by Cisco Aironet 1200 Series access points in Cisco IOS Software release 12.2(15)XR and earlier releases.

HTTPS - HTTP with SSL 3.0

This feature supports a Secure Sockets Layer (SSL)/Secure Hypertext Transfer Protocol (HTTPS) method of managing Cisco Aironet access points via a Web browser using HTTP.

AES-CCMP

This feature supports Advanced Encryption Standard–Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). AES-CCMP is required for Wi-Fi Protected Access 2 (WPA2) and IEEE 802.11i wireless LAN security. This feature is not supported on 350 series access points.

This feature is supported on these devices:

- 1100 series access points (802.11g radio only)
- 1130AG series access points
- 1200 series access points (IEEE 802.11g and 802.11a radios only with the part numbers AIR-RM21A or AIR-RM22A)
- 1230AG series access points (IEEE 802.11g and 802.11a radios only with the part numbers AIR-RM21A or AIR-RM22A)

IEEE 802.1X Local Authentication Service for EAP-FAST

This feature expands wireless domain services (WDS) IEEE 802.1X local authentication to include support for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST). IEEE 802.1X local authentication was introduced in Cisco IOS Software release 12.2(11)JA.

Wi-Fi Multimedia (WMM) Required Elements

This feature supports the required elements of Wi-Fi Multimedia (WMM). WMM is designed to improve the user experience for audio, video and voice applications over a Wi-Fi wireless connection. WMM is a subset of the IEEE 802.11e Quality of Service (QoS) draft standard. WMM supports QoS prioritized media access via the Enhanced Distributed Channel Access (EDCA) method. Optional elements of the WMM specification including call admission control using traffic specifications (TSPEC) are not supported in this release.

VLAN Assignment By Name

This feature allows the Remote Authentication Dial-In User Service (RADIUS) server to assign a client to a virtual LAN (VLAN) identified by its VLAN name. In releases before Cisco IOS Software release 12.3(2)JA, the RADIUS server identified the VLAN by ID. This feature is important for deployments where VLAN IDs are not used consistently throughout the network.

Microsoft WPS IE SSIDL

This feature allows the Cisco Aironet access point to broadcast a list of configured SSIDs such as SSID Lists (SSIDL) in the Microsoft Wireless Provisioning Services Information Element (WPS IE). A client with the ability to read the SSIDL can alert the user to the availability of the SSIDs. This feature provides a bandwidth-efficient, software-upgradeable alternative to multiple broadcast SSIDs (MB/SSIDs).

HTTP Web Server v1.1

This feature provides a consistent interface for users and applications by implementing the HTTP 1.1 standard (see RFC 2616). In previous releases, Cisco software supported only a partial implementation of HTTP 1.0. The integrated HTTP Server API supports server application interfaces. When combined with the HTTPS and HTTP 1.1 Client features, provides a complete, secure solution for HTTP services to and from Cisco devices.

IP-Redirect

This feature provides the capability to redirect traffic intended for a particular destination to another IP address specified by the administrator.

This feature is not supported on 350 series access points.

Installation Notes

This section contains information you should keep in mind when installing 350, 1100, and 1200 series access points.

Installation in Environmental Air Space

This section provides information on installing 1100 and 1200 series access points in environmental air space, such as above suspended ceilings.

Cisco Aironet 1100, 1130, and 1200 Series Access Points provide adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(C) of the *National Electrical Code* (NEC) and Sections 2-128, 12-010(3) and 12-100 of the *Canadian Electrical Code*, Part 1, C22.1.

**Caution**

The power injector does not provide fire resistance and low smoke-producing characteristics and is not intended for use in extremely high or low temperatures or in environmental air spaces, such as above suspended ceilings.

**Note**

If you plan to mount a 1200 series access point with a 5-GHz radio in an area subject to environmental air space, Cisco recommends that you mount the access point horizontally so that its antennas point down. Doing so ensures that the access point complies with regulatory requirements for environmental air space with the 5-GHz radio installed.

Power Considerations

This section describes issues you should consider before applying power to an access point.

**Caution**

The operational voltage range for 1100 series access points is 24 to 60 VDC, and the nominal voltage is 48 VDC. Voltage higher than 60 VDC can damage the equipment.

**Caution**

The nominal voltage for 1200 series access points is 48 VDC, and the access point is operational up to 60 VDC. Voltage higher than 60 VDC can damage the equipment.

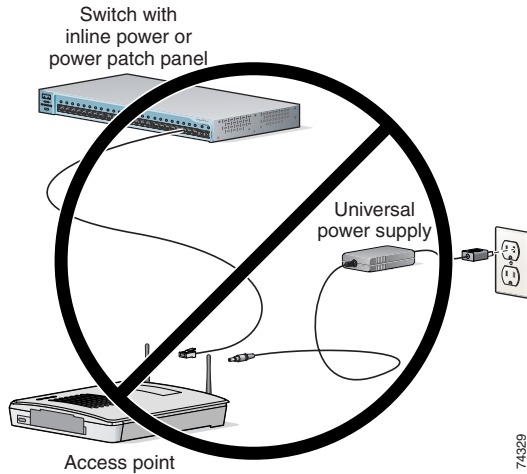
**Caution**

Cisco Aironet power injectors are designed for use with Cisco Aironet access points and bridges only. *Do not use the power injector with any other Ethernet-ready device.* Using the power injector with other Ethernet-ready devices can damage the equipment.

Use Only One Power Option

You cannot provide redundant power to 1100, 1130, and 1200 series access points with both DC power to its power port and inline power from a patch panel or powered switch to the access point's Ethernet port. If you apply power to the access point from both sources, the switch or power patch panel might shut down the port to which the access point is connected. [Figure 2](#) shows the power configuration that can shut down the port on the patch panel or powered switch.

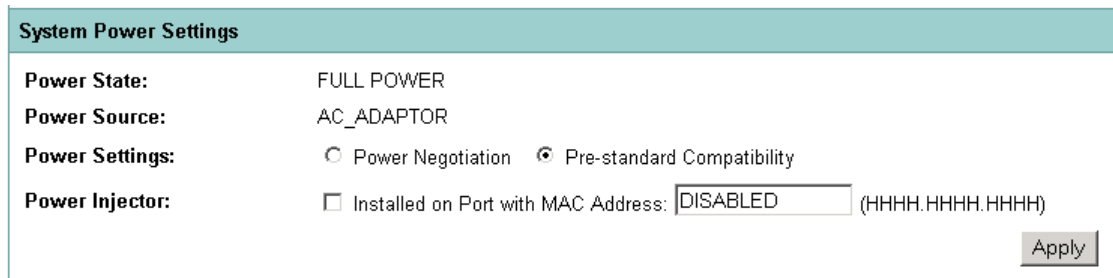
Figure 2 *Improper Power Configuration Using Two Power Sources*



Configuring Power for 1130AG Access Points

The 1130AG access point disables the radio interfaces when the unit senses that the power source to which it is connected does not provide enough power. Depending on your power source, you might need to enter the power source type in the access point configuration. Use the System Software: System Configuration page on the web-browser interface to select a power option. Figure 3 shows the System Power Settings section of the System Configuration page.

Figure 3 *Power Options on the System Software: System Configuration Page*



Using the AC Power Adapter

If you use the AC power adapter to provide power to the 1130AG access point, you do not need to adjust the access point configuration.

Using a Switch Capable of IEEE 802.3af Power Negotiation

If you use a switch to provide Power over Ethernet (PoE) to the 1130AG access point and the switch supports the IEEE 802.3af power negotiation standard, select **Power Negotiation** on the System Software: System Configuration page.

Using a Switch That Does Not Support IEEE 802.3af Power Negotiation

If you use a switch to provide Power over Ethernet (PoE) to the 1130AG access point and the switch does not support the IEEE 802.3af power negotiation standard, select **Pre-Standard Compatibility** on the System Software: System Configuration page.

Using a Power Injector

If you use a power injector to provide power to the 1130AG access point, select **Power Injector** on the System Software: System Configuration page and enter the MAC address of the switch port to which the access point is connected.

Operating 5-GHz Radio Requires Power Injector, Power Module, or Catalyst 3550-24 PWR Switch

The 1200 series power injector and the 1200 series power module support operation of the 5-GHz radio in the access point. Currently, the Catalyst 3550-24 PWR switch supports power for both the 2.4-GHz radio and the 5-GHz radio. Other switches and power patch panels might not provide enough power for the 5-GHz radio.

Access Point Requires 1200 Series Universal Power Supply and Power Injector

The 350 series universal power supply and power injector are not compatible with the 1200 series access point. If you use a power injector or a power module to provide power to a 1200 series access point, you must use a 1200 series universal power supply. If you need to use a power injector to inject power into the access point's Ethernet port, you must use a 1200 series power injector.

Unpowered 1100 Series Access Points Cause Loopback When Connected to Switches Without Loopback Detection

When you connect an unpowered 1100 series access point to a switch without loopback detection, the access point causes a loopback. To avoid this problem, make sure loopback detection is enabled on the switch to which the access point is connected. If your switch does not have loopback detection, disconnect the access point from the switch when the access point power is off.

Antenna Installation

For instructions on the proper installation and grounding of external antennas for 1200 series access points, refer to the National Fire Protection Association's *NFPA 70, National Electrical Code*, Article 810, and the Canadian Standards Association's *Canadian Electrical Code*, Section 54.



Warning

Do not install the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death.

Important Notes

This section describes important information about the access point.

Default Username and Password Are *Cisco*

When you open the access point interface, you must enter a username and password. The default username for administrator login is *Cisco*, and the default password is *Cisco*. Both the username and password are case sensitive.

Proxy Mobile-IP Feature Removed From This Release

The proxy Mobile-IP feature is not supported in Cisco IOS Release 12.3(2)JA.

AIR-RM21A/AIR-RM22A Radio Modules Usually Set to Max Transmit Power

AIR-RM21A and AIR-RM22A radio modules measure transmit power in decibels per milliwatt (dBm), but earlier versions of 802.11a radios in Cisco Aironet access points measure power in milliwatts (mW). Because power settings in mW do not translate directly to settings in dBm, the access point usually uses the default power setting of maximum when you install a new AIR-RM21A or AIR-RM22A radio module.

[Table 3](#) lists 802.11a transmit power settings in mW and the power settings that the access point assigns to a new radio module.

Table 3 Transmit Power Settings Assigned to New Radio Modules

Power Settings in mW	Power Setting Assigned to New Radio Module
5	5 dBm (approximately 3 mW)
10	maximum (17 dBm)
20	maximum
40	maximum

New Express Security Page Simplifies Security Setup

The new Express Security page in the access point web-browser interface makes it easier to create SSIDs and assign security settings to them. [Figure 4](#) shows the Express Security page.

Limitations of the Express Security page include:

- You cannot edit SSIDs. However, you can delete SSIDs and re-create them.
- You cannot assign SSIDs to specific radio interfaces. The SSIDs that you create are enabled on all radio interfaces. To assign SSIDs to specific radio interfaces, use the Security SSID Manager page.
- You cannot configure multiple authentication servers. To configure multiple authentication servers, use the Security Server Manager page.

- You cannot configure multiple WEP keys. To configure multiple WEP keys, use the Security Encryption Manager page.
- You cannot assign an SSID to a VLAN that is already configured on the access point. To assign an SSID to an existing VLAN, use the Security SSID Manager page.
- You cannot configure combinations of authentication types on the same SSID (such as MAC address authentication and EAP authentication). To configure combinations of authentication types, use the Security SSID Manager page.

For complete instructions on using the Express Security page, see the “Configuring Basic Security Settings” section on page 2-11 in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*. Click this URL to browse to that document:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/acsspts/i12215ja/i12215sc/index.htm>

Figure 4 Express Security Page

Express Security Set-Up

SSID Configuration

1. SSID Broadcast SSID in Beacon

2. VLAN

No VLAN Enable VLAN ID: (1-4095) Native VLAN

3. Security

No Security

Static WEP Key

Key 1 128 bit

EAP Authentication

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

WPA

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

Apply Cancel

SSID Table

Delete	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
<input checked="" type="radio"/>	tsunami	none	none	open	none		<input checked="" type="checkbox"/>

111856

GRE Tunnelling Through WLSM Sometimes Requires MTU Setting Adjustments

If client devices on your wireless LAN cannot use certain network applications or cannot browse to Internet sites, you might need to adjust the MTU setting on the client devices or other network devices. For more information, refer to the Tech Note at this URL:

http://www.cisco.com/en/US/tech/tk827/tk369/technologies_tech_note09186a0080093f1f.shtml

TACACS+ and DHCP IP Address Sometimes Locks Out Administrators

When you configure an access point for TACACS+ administration and to receive an IP address from the DHCP server, administrators might be locked out of the access point after it reboots if the administrator does not have a local username and password configured on the access point. This issue does not affect access points configured with a static IP address. Administrators who have been locked out must regain access by using the mode button to reset the unit to default settings.

Access Points Do Not Support Loopback Interface

You must not configure a loopback interface on the access point.



Configuring a loopback interface might generate an IAPP GENINFO storm on your network and disrupt network traffic.

Non-Cisco Aironet 802.11g Clients Might Require Firmware Upgrade

Some non-Cisco Aironet 802.11g client devices require a firmware upgrade before they can associate to the 802.11g radio in the access point. If your non-Cisco Aironet 802.11g client device does not associate to the access point, download and install the latest client firmware from the manufacturer's website.

Throughput Option for 802.11g Radio Blocks Association by 802.11b Clients

When you configure the 802.11g access point radio for **best throughput**, the access point sets all data rates to basic (required). This setting blocks association from 802.11b client devices. The **best throughput** option appears on the web-browser interface Express Setup and Radio Settings pages and in the **speed** CLI configuration interface command.

Transmit Power Set to Maximum When You Install 802.11g Radio

When you replace the 802.11b radio in a 1200 series access point with an 802.11g radio, the 802.11g radio is set to the maximum transmit power allowed in your regulatory domain regardless of the power setting configured on the 802.11b radio. After you install the 802.11g radio and the access point reboots, configure the 802.11g radio to the preferred transmit power.

Use Auto for Ethernet Duplex and Speed Settings

Cisco recommends that you use **auto**, the default setting, for both the speed and duplex settings on the access point Ethernet port. When your access point receives inline power from a switch, any change in the speed or duplex settings that resets the Ethernet link reboots the access point. If the switch port to which the access point is connected is not set to **auto**, you can change the access point port to **half** or **full** to correct a duplex mismatch and the Ethernet link is not reset. However, if you change from **half** or **full** back to **auto**, the link is reset and, if your access point receives inline power from a switch, the access point reboots.

**Note**

The speed and duplex settings on the access point Ethernet port must match the Ethernet settings on the port to which the access point is connected. If you change the settings on the port to which the access point is connected, change the settings on the access point Ethernet port to match.

Use force-reload Option with archive download-sw Command

When you upgrade access point or bridge system software by entering the **archive download-sw** command on the CLI, you must use the **force-reload** option. If the access point or bridge does not reload the Flash after the upgrade, the pages in the web-browser interface might not reflect the upgrade. This example shows how to upgrade system software successfully using the **archive download-sw** command:

```
AP# archive download-sw /force-reload /overwrite tftp://10.0.0.1/image-name
```

Radio MAC Address Appears in ACU

When a Cisco Aironet client device associates to an access point running IOS software, the access point MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the access point radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Radio MAC Address Appears in Access Point Event Log

When a client device roams from an access point (such as access point *alpha*) to another access point (access point *bravo*), a message appears in the event log on access point alpha stating that the client roamed to access point bravo. The MAC address that appears in the event message is the MAC address for the radio in access point bravo. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Mask Field on IP Filters Page Behaves the Same As in CLI

In Cisco IOS Release 12.2(8)JA and later, the mask that you enter in the Mask field on the IP Filters page in the access point GUI behaves the same way as a mask that you enter in the CLI. If you enter 255.255.255.255 as the mask, the access point accepts any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address that you entered in the IP Address field.

Repeater Access Points Running IOS Software Cannot Associate to Parent Access Points Running VxWorks

Repeater access points running Cisco IOS software cannot associate to parent access points that do not run IOS software (all 340 series access points, and 350 and 1200 series access points that have not been converted to run IOS software).

Repeater Access Points Cannot Be Configured as WDS Access Points

Repeater access points do not support WDS. You cannot configure a repeater access point as a WDS access point, and if a root access point becomes a repeater in fallback mode, it cannot provide WDS.

Crossover Cable Sometimes Needed When Ethernet Speed and Duplex Set to Fixed on 1100 Series Access Points

If you change the speed and duplex settings from auto to fixed on an 1100 series access point's Ethernet port, the auto-MDIX feature on the port is disabled. When auto-MDIX is disabled, you must determine whether to use a straight-through or a crossover cable to connect the access point Ethernet port to another device. If the Ethernet link goes down after you set the speed and duplex to fixed, try changing the Ethernet cable from crossover to straight-through or from straight-through to crossover.

Cannot Perform Link Tests on Non-Cisco Aironet Client Devices and on Cisco Aironet 802.11g Client Devices

The link test feature on the web-browser interface does not support non-Cisco Aironet client devices nor Cisco Aironet 802.11g client devices.

System Software Upgrade Sometimes Fails Using Microsoft Internet Explorer 5.01 SP2

A system software upgrade sometimes fails when you use Microsoft Internet Explorer version 5.01 SP2 to upgrade system software using the HTTP Upgrade page in the web-browser interface. Use a later version of Microsoft Internet Explorer to perform HTTP system software upgrades, or use TFTP to upgrade system software. Click this URL to browse to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for complete instructions on performing software upgrades:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/tsd_products_support_configure.html

1100 Series Access Points with Boot Loader Version 12.2(4)JA Boot into Monitor Mode

When the Ethernet port is disabled on an 1100 series access point running boot loader version 12.2(4)JA, the access point boots into monitor mode when it reboots. To avoid this problem, connect the access point Ethernet port to one of the following:

- a wired LAN
- the Ethernet port on a PC

Remove power from the access point and reapply power to reboot the unit. When the access point senses an Ethernet connection, it boots normally.

Corrupt EAP Packet Sometimes Causes Error Message

During client authentication, the access point sometimes receives a corrupt EAP packet and displays this error message:

```
Oct 1 09:00:51.642 R: %SYS-2-GETBUF: Bad getbuffer, bytes= 28165
-Process= "Dot11 Dot1x process", ipl= 0, pid= 32
-Traceback= A2F98 3C441C 3C7184 3C604C 3C5E14 3C5430 124DDC
```

You can ignore these messages.

When Cipher is TKIP Only, Key Management Must Be Enabled

When you configure **TKIP-only** cipher encryption (not **TKIP + WEP 128** or **TKIP + WEP 40**) on any radio interface or VLAN, every SSID on that radio or VLAN must be set to use WPA or CCKM key management. If you configure TKIP on a radio or VLAN but you do not configure key management on the SSIDs, client authentication fails on the SSIDs.

Cisco CKM Supports Spectralink Phones

Cisco CKM (CCKM) key management is designed to support voice clients that require minimal roaming times. To date, CCKM supports only Spectralink Wireless Phones. Other voice clients have not been tested with CCKM and are not supported.

Non-Cisco Aironet Clients Sometimes Fail 802.1x Authentication

Some non-Cisco Aironet client adapters do not perform 802.1x authentication to the access point unless you configure **Open authentication with EAP**. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.

Microsoft Patch Fixes WPA Authentication Delay

When the access point is configured for optional or mandatory WPA authentication, client adapters in Windows XP platforms sometimes experience a delay when initially authenticating to the access point immediately after it starts up. A patch from Microsoft resolves this issue. The patch is described in Microsoft Knowledge Base Article 826942.

Linksys Driver Fixes Bug CSCed60301

When you enable shared key authentication and TKIP on an SSID on a 1200 series access point, some Linksys client devices cannot associate using the SSID. However, a Linksys driver update fixes the problem.

Pings and Link Tests Sometimes Fail to Clients with both Wired and Wireless Network Connections

When you ping or run a link test from an access point to a client device installed in a PC running Microsoft Windows 2000, the ping or link test sometimes fails when the client has both wired and wireless connections to the LAN. Microsoft does not recommend this configuration. For more information, refer to Microsoft Knowledge Base article 157025 at this URL:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;157025&Product=win2000>

Layer 3 Mobility Not Supported on Repeaters and Workgroup Bridges

Repeater access points and workgroup bridges cannot associate to an SSID configured for Layer 3 mobility. Layer 3 mobility is not supported on repeaters and workgroup bridges.

WLSM Required for Layer 3 Mobility

You must use a Wireless LAN Services Module (WLSM) as your WDS device in order to properly configure Layer 3 mobility. If you enable Layer 3 mobility for an SSID and your WDS device does not support Layer 3 mobility, client devices cannot associate using that SSID.

Change to Default IP Address Behavior

Cisco IOS Release 12.3(2)JA changes the default behavior of access points requesting an IP address from a DHCP server:

- When you connect a 350, 1130AG, or 1200 series access point with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an address, continues to send requests indefinitely.
- When you connect an 1100 series access point with a default configuration to your LAN, the 1100 series access point makes several attempts to get an IP address from the DHCP server. If it does not receive an address, it assigns itself the IP address 10.0.0.1 for five minutes. During this five-minute window, you can browse to the default IP address and configure a static address. If after five minutes the access point is not reconfigured, it discards the 10.0.0.1 address and reverts to requesting an address from the DHCP server. If it does not receive an address, it sends requests indefinitely. If you miss the five-minute window for browsing to the access point at 10.0.0.1, you can power-cycle the access point to repeat the process.

Caveats

This section lists [Open Caveats](#) and [Resolved Caveats](#) in Cisco IOS Release 12.3(2)JA.

Open Caveats

These caveats are open in Cisco IOS Release 12.3(2)JA:

- CSCeb50727—Unpowered 1100 series access points sometimes cause a loopback when connected to switches without loopback detection. When you connect an unpowered 1100 series access point to some switches without loopback detection, the access point sometimes causes a loopback. To avoid this problem, make sure loopback detection is enabled on the switch to which the access point is connected. If your switch does not have loopback detection, disconnect the access point from the switch when the access point power is off.
- CSCeb52431—When logging into a TACACS+ server, 1100 series access points sometimes send hundreds of additional authentication requests to the server after a successful authentication.
- CSCee90230—When the access point is configured for TACACS+ administrator authentication and uses an IP address from the DHCP server, this traceback occurs sometimes when the access point reboots:

```
Traceback= 2C120 2C150 2EFC4 2BE34 2BD50 330724 3EBD44 19C888 19E5B0 2A3FC0 3AAA04
1337F8
```

The traceback does not appear on access points using a static IP address.

- CSCef11167—The access point sometimes returns an inaccurate value when you poll cDot11ActiveWirelessClients through SNMP.
- CSCef65076—The access point GUI sometimes reports this error when you a RADIUS server hostname to the access point:

```
HTTP 400 - Bad Request
```

Workaround: Enter the server IP address instead of the hostname.

- CSCef67806—When you enter the show cdp traffic command on a repeater access point or the parent to which the repeater is associated, the access point reports an inaccurate total of CDP packets.
- CSCef70234—When the access point is configured to select the least-congested channel at start-up, the access point sometimes selects a channel which is not the least congested.
- CSCef71351—When CDP is enabled on a radio interface with VLANs configured, the radio output drop counter sometimes increments when the access point sends a CDP packet.
- CSCef71825—When a memory allocation failure occurs on the access point, it sometimes fails to respond to authentication requests from client devices running Microsoft Windows CE. The access point again responds to client requests after you reboot it.
- CSCef75032—When you disable the 802.11g radio on the access point GUI, the radio is disabled but the Settings page and the Network Interfaces page sometimes indicate that the radio is still enabled.
- CSCef78627—The access point sometimes reports an incorrect transmit power value for the 802.11a radio when you change the external antenna position from high-gain to low-gain or from low-gain to high-gain while the access point is on.

Workaround: Change the antenna position on the 802.11a radio only when the unit is off.

- CSCef87205—There are problems with the following SNMP MIB object identifiers in the CISCO-DOT11-SSID-SECURITY-MIB:
 - cdot11SecAuxSsidVlanName is not writable unless the value corresponds to the same VLAN as the cdot11SecAuxSsidVlan already set for the SSID. The same cdot11SecAuxSsidVlanName and cdot11SecAuxSsidVlan must correspond to an existing entry in the cdot11SecVlanNameTable.
 - cdot11SecSsidInformationElement value cannot be modified after it has been set.
 - cdot11SecSsidRedirectFilter allows you to set an ACL number that is outside the valid range.
 - cdot11SecAuxSsidWirelessNetId allows you to set a value only from 0 to 4095.
 - Setting cdot11SecAuxSsidAuthKeyMgmtOpt value to true without also configuring key management creates an invalid configuration.
 - You can set cdot11SecAuxSsidLoginUsername without configuring the required corresponding authentication type for the SSID.
 - cdot11SecAuxSsidInfraStruct is not of the TruthValue type as described in some object descriptions, and only infraStructure(1) and nonInfraStructure(2) are supported.
 - The default address for cdot11SecSsidRedirectDestAddr should be 0.0.0.0 but is " ".
 - cdot11SecAuxSsid does not allow you to enter non-hexadecimal characters such as + or /.
 - cdot11SecAuxSsidWpaPsk is implemented with a maximum length of 32 characters instead of the 128 characters indicated in the MIB.
 - cdot11SecVlanName does not allow you to enter a number greater than 4095 as the VLAN name. It only allows alphabetic characters to be used as VLAN names.
 - You cannot use this MIB to configure shared and network-EAP authentication.

Workaround: Use the OIDs in the CISCO-DOT11-IF-MIB.

- CSCef95164—When ARP chaching is enabled on the access point, Cisco 7920 IP phones sometimes cannot communicate with other 7920 phones and with Cisco 7960 IP phones.

Workaround: Disable ARP chaching, or enable ARP caching and select the check box labeled **Forward ARP Requests To Radio Interfaces When Not All Client IP Addresses Are Known**.
- CSCef95410—When an access point is configured to interact with a WDS device, the WLCCP packets that it receives from the WDS device sometimes cause the radio interface output drop counter to increment when it should not.
- CSCef95472—After operating for several weeks, some Symbol client devices cannot communicate with the 802.11b radio in an access point even though they are associated. The clients can communicate again after you reboot the access point.
- CSCeg15035—The **drop-packets** option in the **packet retries** configuration interface command is not supported in this release. The **drop-packets** option sometimes causes the access point to stop transmitting packets, and the access point must be rebooted.

Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.3(2)JA:

- CSCeb40058—This release includes the **logging snmp-trap** global configuration command to specify syslog severity levels that are sent as SNMP traps. This example shows how to configure the access point to send all severity levels as traps:

```
AP1100#config term
Enter configuration commands, one per line. End with CNTL/Z.
AP1100(config)#logging snmp-trap 0 7
AP1100(config)#exit
```

- CSCec25430—Access points no longer reload when they receive a corrupt CDP packet.
- CSCec55763, CSCec57354—When both the 802.11g and 802.11a radios in a 1200 series access point simultaneously operate under extremely high data loads for an extended period, the 802.11a radio no longer freezes and the access point no longer reboots.
- CSCec74066—The access point GUI now includes a **Restart** button to reset a standby access point that has taken the place of the monitored unit. When the monitored access point comes back online, browse to the Services: Hot Standby page on the standby access point and click **Restart** to put the standby unit back into standby mode.
- CSCed03154—The access point no longer indicates that a client device is associated when the client is not associated.
- CSCed25530—The Ethernet interface input queue on a 350 series access point running Cisco IOS software no longer hangs after a period of operation.
- CSCed57726—An access point configured as the WDS device no longer displays tracebacks when under a heavy load of client reauthentications.
- CSCed62173—The access point now sends the list of adjacent access points to qualified client devices when they associate to the access point and when the list of adjacent access points is updated.
- CSCed63953—The access point information element now transmits the value that you enter for default QoS CWMin value for best effort regardless of the value that you enter for that setting.
- CSCed75292—The access point radio no longer reboots when a client device attempts to authenticate at the same time that you enter this command on the access point CLI:


```
show aaa user all
```
- CSCed82111—An access point configured as a WDS device now authenticates successfully with a Funk RADIUS server.
- CSCed84527—The access point no longer deauthenticates roaming client devices when the 1 and 2 Mbps datarates are disabled on the access point.
- CSCed86456—TKIP/WPA now has replay detection for bridge links with concatenation enabled.
- CSCed87329—Access points now use only one DHCP client identifier when they boot.
- CSCed90455—Client devices no longer reauthenticate unexpectedly when WDS is configured on your network.
- CSCed91130—When an 802.11g radio in an access point configured for use in Japan is set to channel 14, you can no longer select **Best Throughput** for the data rate setting on the access point GUI.
- CSCed92054—The access point now uses the same MAC address format for both authentication and accounting when sending MAC addresses to the RADIUS server.

- CSCee05762, CSCed21433—Entry fields on the access point GUI now accept all characters except the following:
 - “
 -]
 - +
 - /
- **Tab**
- **Trailing space**
- CSCee09515—The Associations page on the access point GUI now includes all associated client devices in its count of associated clients.
- CSCee09624—The transmitted fragment counter on the access point now counts all transmitted fragments.
- CSCee12053—Access points do not support the **service compress-config** command, and the command has no effect on access points when you enter it.
- CSCee14096—If the access point is not configured as a local authenticator, the access point no longer reboots when you enter the **clear radius local-server user user** command.
- CSCee14599—Access points in standby mode no longer allow client associations when the Ethernet port is disabled.
- CSCee22037—When you convert an access point from VxWorks to Cisco IOS software and you have SNMP traps enabled before the conversion, the access point GUI now indicates as enabled only the SNMP traps that are enabled after the conversion.
- CSCee24611—After several days of connectivity, access points no longer fail to communicate with workgroup bridges that are LEAP authenticated.
- CSCee26301—SSH now operates correctly when you change the access point host name.
- CSCee29096—Access point error messages now comply with ISO standards.
- CSCee29948—The access point now correctly assigns the **ntp broadcast client** command to the `bvi1` interface.
- CSCee30632—Access points now support SNTP.
- CSCee30896—Access points configured as local authenticators no longer unnecessarily authenticate clients twice.
- CSCee32246—The **rts retries** command now works as expected.
- CSCee35686—When you set an 802.11g-only data rate to **required** on the access point 802.11g radio, the access point GUI now displays a reminder that the setting prevents associations from 802.11b client radios.
- CSCee38517—The access point now sends an EAP-FAILURE message to a client device that fails authentication when the ACS server sends an ACCESS-REJECT message.
- CSCee39180—The default link to online help files is now automatically updated when you upgrade the access point software.
- CSCee39809—Access points configured for LEAP no longer randomly reboot.
- CSCee44666—Software upgrade no longer disables TACACS+.
- CSCee45192—You can now enable both debugging notifications and Syslog messages on the access point GUI.
- CSCee50581—SSIDs that contain spaces are no longer truncated in the Adjacent Nodes list on the Network Map page on the access point GUI.

- CSCee51677—When you configure a time zone on the access point GUI, the access point configuration viewed on the CLI matches the GUI setting.
- CSCee56830—The hot standby access point no longer shuts down the radio of the primary access point when the standby access point radio is disabled.
- CSCee61010—The access point now requires 63 hexadecimal characters for the WPA pre-shared key.
- CSCee62247—Client devices in power-save mode no longer generate tracebacks when associated to 350 series access points.
- CSCee62546—The access point GUI now warns users that Aironet extensions must be enabled when you configure MIC or per-packet keying on the access point.
- CSCee63284—1200 series access points no longer reboot intermittently while displaying this error:

```
LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset.
```
- CSCee63875—The createAndWait option in the CISCO-FLASH-MIB now operates correctly on access points.
- CSCee64873—The password hash function of WLCCP no longer changes the resulting hash with every execution.
- CSCee66841—When VLANs are enabled and WEP encryption is added to the infrastructure SSID, an access point in fallback repeater mode can now associate to a root access point and successfully pass traffic.
- CSCee70832—When the primary ACS server fails, the access point now switches to the next ACS server in the access point's server priority list.
- CSCee73172—Access points configured as the WDS device no longer have memory leaks that generate MALLOCFAIL errors.
- CSCee76716—When WDS is enabled, the access point now sends the client's user ID in accounting requests instead of the client's MAC address.
- CSCee77277—Access points now correctly send these RADIUS accounting attributes: Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets, and Acct-Output-Packets.
- CSCee78082—Throughput is now the same for unicast and multicast packets sent by the access point.
- CSCee78757—Non-Cisco client adapters now are able to associate to the 802.11g radio in an access point when OFDM data rates (6, 9, 12, 18, 24, 36, 48, and 54 Mbps) are enabled.
- CSCee87254—You can now use the access point GUI to disable SSH.
- CSCee90065—An access point with a default configuration no longer sends a DHCP request when you click the **Network Interfaces: IP Address** link on the access point GUI.
- CSCef01790—When access point interfaces are configured to allow unicast-flooding and the configuration is saved, the unicast-flooding command is now applied after the unit reboots.
- CSCef02795—Access points no longer allow you to configure both MAC-address authentication and WPA-PSK for the same SSID.
- CSCef06846—The access point no longer has a memory leak.
- CSCef06976—Applying a service policy to input traffic on the access point radio interface to classify traffic now carries through to the 802.1d marking on the Ethernet trunk.
- CSCef14899—The drop-down menu on online help pages now operates correctly.

- CSCef18797—The WDS device now sends the class attribute to participating access points so that the access points can include the attribute in RADIUS accounting messages.
- CSCef23452—The access point data packet counter now increments correctly.
- CSCef24269—The Time Server entry field now allows more than 15 characters on the Services: NTP page on the access point GUI.
- CSCef41592—After booting from factory defaults, an access point now automatically sets its hostname to the name returned in the DNS PTR record corresponding to any of the access point's IP addresses.
- CSCef45558—When configured as root access points through the GUI, 1310 series access points now contain essential access point configuration elements.
- CSCef46191—A specifically crafted TCP connection to a telnet or reverse telnet port of an access point running Cisco IOS software no longer blocks further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and HTTP access to the access point.
- CSCef47638—The configuration on 350 series access points no longer contain random characters.
- CSCef49603—The Cisco IOS Software Configuration Guide for Cisco Aironet Access Points now contains a description for the RADSRV-4-NAS_UNKNOWN error message.
- CSCef53367—Access points no longer display runtime errors when you browse to the Express Setup page on the GUI.
- CSCef53401—Client devices associated to an access point no longer fail to receive IP addresses from the DHCP server.
- CSCef55725—Transmit power no longer drops on channel 14 on access points configured for use in Japan.
- CSCef59317—When a failed authentication holdoff time is configured on the access point, the access point now allows three authentication failures before it invokes the holdoff time for the failed user.
- CSCef62562—Access points no longer reboot after displaying this traceback:


```
"SNMP ENGINE", ipl= 6, pid= 69
-Traceback= B5E18 2E9C94 2E9EF0 13C6BC 140910
```
- CSCef62817—User passwords configured on a local authenticator access point now appear as either clear text or nhash.
- CSCef66214—Uninitialized message structures no longer cause the access point to reboot.
- CSCef83419—Non-root bridges and repeater access points now report associations to parent access points and bridges in response to these SNMP queries: cDot11ClientStatisticTable, cDot11ClientConfigInfoTable, and cDot11ActiveDevicesTable.
- CSCin74956—Client devices that associate to the access point using an SSID with CKIP+CMIC encryption now receive IP addresses from the DHCP server.
- CSCsa32966—Access points no longer send randomly corrupted beacons that cause them to appear as rogue devices on the WLSE.

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 select 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/cisco/web/support/index.html>. Click **Technology Support**, choose **Wireless** from the menu on the left, and click **Wireless LAN**.

Related Documentation

This section lists documents related to Cisco IOS Release 12.2(15)JA and to 350, 1100, and 1200 series access points.

- *Cisco Aironet Conversion Tool for Cisco IOS Software, 2.0 Administrator Guide for Windows*
- *Quick Start Guide: Cisco Aironet 350 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1100 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1200 Series Access Points*
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *Installation Instructions for Cisco Aironet Power Injectors*

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.