# Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(8)JEA2

**July 26, 2007**

This release is a maintenance release and contains no new features. These release notes list open and resolved caveats for Cisco IOS Release 12.3(8)JEA2. They also provide important information about the Cisco Aironet 1130 and 1240 Series Access Points and 1300 Series Outdoor Access Point/Bridges.

Cisco IOS Release 12.3(8)JEA2 supports autonomous 16 Mb platforms and platforms that were supported in Cisco IOS Release 12.3(8)JA and earlier. Autonomous 32 Mb platforms (1130 and 1240 series access points) are supported by Cisco IOS Release 12.3(11)JA.

## Contents

These release notes contain the following sections:

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

# 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, 1130, 1200, 1230, 1240 series access points and the1300 series outdoor access point/bridge using the command-line interface (CLI), the web-browser interface, or Simple Network Management Protocol (SNMP).

# System Requirements

Cisco IOS Release 12.3(8)JEA2 is a general maintenance release that concentrates on bug fixes. You can install Cisco IOS Release 12.3(8)JEA2 on all 350, 1100, 1130, 1200, 1230, 1240 series access points, and 1300 series outdoor access point/bridges.

**Note** Software upgrades fail when you use the web-browser interface to install Cisco IOS Release 12.3(8)JEA2 on 1200 series access points. The image size exceeds the access point's 4-MB restriction for software upgrades. Use TFTP to upgrade your 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/docs/wireless/access_point/12.3_2_JA/configuration/guide/i1232sc.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 12.3(8)JA:

```
ap1200>show version
Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.3(8)JA
Copyright (c) 1986-2006 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

## Obtaining the Software Image

To obtain the Cisco IOS software for your access point, follow these instructions to reach the Cisco IOS Software Center on Cisco.com:

**Step 1** Follow this link to the Cisco Software Center page:

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

**Step 2** Scroll down to the Access Point section.

**Step 3** Choose your access point from the displayed list. The access point introduction page appears.

**Step 4** Click **Download Software**. The Software Download page appears.

**Step 5** Click your highlighted access point and the software type page appears.

**Note** You must register or be a registered user to obtain the software image. Follow the registration instructions.

**Step 6** Click **IOS Software** and the software release page appears.

**Step 7** Click **12.3(8)JEA2** > **Wireless LAN** > **Download** and the Software License Agreement page appears.

**Step 8** Read the agreement, click **Agree**, and enter your username and password on the Log In screen.

**Step 9** Follow the prompts to save the software on your PC.

# Upgrading to a New Software Release

For instructions on installing new software for your bridge:

**Step 1** Follow this link to the Cisco Software Center page:

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

**Step 2** Scroll down to the Access point section.

**Step 3** Choose your access point from the displayed list. The Cisco Aironet 1400 Series Introduction page appears.

**Step 4** Under the Configure section, click **Configuration Guides**. A list of configuration documents appears.

**Step 5** Click **Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA**.

**Step 6** Navigate to the Managing Firmware and Configurations chapter.

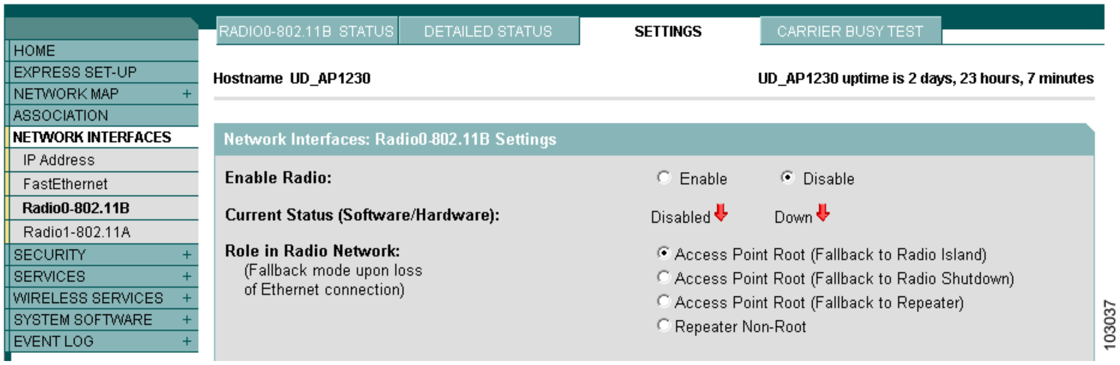
## Disable Radios to Prevent Unexpected Reboot When Upgrading System Software

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*



Hostname UD_AP1230

UD_AP1230 uptime is 2 days, 23 hours, 7 minutes

Network Interfaces: Radio0-802.11B Settings

Enable Radio: ○ Enable ● Disable

Current Status (Software/Hardware): Disabled ↓ Down ↓

Role in Radio Network:
(Fallback mode upon loss of Ethernet connection)

● Access Point Root (Fallback to Radio Island)
○ Access Point Root (Fallback to Radio Shutdown)
○ Access Point Root (Fallback to Repeater)
○ Repeater Non-Root

**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 upgrade 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
```

# Important Information

## CCKM and Fast Roaming on Cisco 7921/7925 IP Phones

When a 7921 or 7925 wireless associates to an access point in a WDS with CCKM, it cannot fast roam because call admission control is not enabled. To work around this issue you must enable admission control by issuing the **admit-traffic** command in the access point SSID configuration as shown in the following example:

```
dot11 ssid voice
vlan 21
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-managemenet wpa cckm
admit-traffic
```

# New Features

No new features are introduced in Cisco IOS Release 12.3(8)JEA2.

# Caveats

This section lists open and resolved caveats.

## Open Caveats

These caveats are open in Cisco IOS Release 12.3(8)JEA2:

- CSCsc94510—GUI can set illegal combination of Low Latency Rates

  The GUI can set an illegal combination of low latency rates on the access point. Rates of 48 and 54Mbps set as both nominal and non-nominal can occur. Once the rates are set, you can not disable them and they stay set as non-nominal.
- CSCsc83206—A nested repeater access point fails to notify radar detection

  If radar is detected on a nested repeater in a nested repeater chain, no action is being taken by either the repeater or root/parent to notify the detection.
- CSCse34644—Shared authentication with a non-native vlan does not operate properly
- CSCsd69733—Hot standby access point cannot associate

  The hot standby access point almost always fails to authenticate with the error *cannot associate: Not standby parent (from incorrect mac address*. The incorrect mac address is the mac address of another access point on the same network but not its parent device's mac address. In other words, the hot standby unit attempts to authenticate with an access point that is not it's parent and fails.
- CSCsd62542—WPA(LEAP/EAP-FAST) reauthentication takes a long time and fails initially

  Reauthentication fails initially and takes more than 45 seconds with LEAP and EAP-FAST authentication with WPA key management configured.

## Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.3(8)JEA2:

- CSCse56501

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6 .

- CSCsj44081—Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures. This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  Details: The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp: May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error. The error message is then followed by a traceback.

## 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.)

# Related Documentation

This section lists documents related to Cisco IOS Release 12.3(8)JEA2 and to 350, 1100, 1130AG, 1200, 1240AG, 1250 series access points, and 1300 series outdoor access point/bridges.

- *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 1130AG Series Access Points*
- *Quick Start Guide: Cisco Aironet 1200 Series Access Points Running Cisco IOS Software*
- *Quick Start Guide: Cisco Aironet 1240AG Series Access Points*
- *Quick Start Guide: Cisco Aironet 1300 Series Outdoor Access Point/Bridge*
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *Hardware Installation Guide for Cisco Aironet 350 Series Access Points Running Cisco IOS Software*
- *Cisco Aironet 1100 Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1130AG Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1200 Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1300 Series Outdoor Access Point/Bridge Hardware Installation Guide*
- *Installation Instructions for Cisco Aironet Power Injectors*

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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