



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:

- [System Requirements, page 2](#)
[Important Information, page 6](#)
[New Features, page 7](#)
[Caveats, page 7](#)
[Related Documentation, page 8](#)
[Obtaining Documentation, Obtaining Support, and Security Guidelines, page 9](#)



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

© 2007 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, 1130, 1200, 1230, 1240 series access points and the 1300 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

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*

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/acsspts/i1232ja/i1232sc/index.htm>

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.



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

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.
```

Upgrading to a New Software Release

Obtaining the Software Image

Step 1

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

Step 2

Step 3

Step 4 **Download Software**

Step 5



Note

Step 6

IOS Software

Step 7

12.3(8)JEA2 > Wireless LAN Download

Step 8

Agree

Step 9

Configuration Guides

Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, Cisco IOS Release 12.3(8)JA

Disable Radios to Prevent Unexpected Reboot When Upgrading System Software

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

The screenshot displays the 'Network Interfaces: Radio Settings' page for Radio0-802.11B. The page has a navigation menu on the left with options like HOME, EXPRESS SET-UP, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, IP Address, FastEthernet, Radio0-802.11B, Radio1-802.11A, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area shows the following 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

103037

Disable

Apply

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

`shutdown`

`no`

Converting to Cisco IOS Software

-
-



Note



Note

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

Some Fields Not Updated During Upgrade to IOS Software

```

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 `authentication key-management wpa cckm admit-traffic` command in the access point SSID configuration as shown in the following example:

```

authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa cckm
admit-traffic
    
```

New Features

Caveats

Open Caveats

- 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)* 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 its 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.

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.

-

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

Related Documentation

-
- *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

What's New in Cisco Product Documentation

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

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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.

© 2007 Cisco Systems, Inc. All rights reserved.