



# Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 15.2(2)JB3

---

These release notes describe features, enhancements, and caveats for Cisco Autonomous AP IOS Release 15.2(2)JB3. This release supports the following Cisco Aironet autonomous access points:

- AP 802
- AP1260
- AP 1040
- AP 1140
- AP 3500i
- AP 3500e
- AP 3600i
- AP 3600e
- AP 2600i
- AP 2600e
- AP 1600i
- AP 1600e
- AP 1550

Cisco IOS Release 15.2(2)JB3 does not support the following Cisco Aironet access points:

- AP 801
- AP 1130
- AP 1240
- AP 1250
- AP 1310



**Note**

You cannot use HTTPS file transfer to upgrade to Cisco IOS Release 15.2(2)JB from previous releases. Because of the image size for this release, you must use TFTP or FTP file transfer for the upgrade. Refer to the upgrade instructions at this URL:

[http://www.cisco.com/en/US/docs/wireless/access\\_point/12.4\\_10b\\_JA/configuration/guide/scg12410b-chap20-firmware.html#wp1035507](http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap20-firmware.html#wp1035507)

## Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Features and Important Installation Notes, page 5](#)
- [Caveats, page 5](#)
- [Troubleshooting, page 7](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 23](#)

## 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.

## System Requirements

You can install the 32 MB Cisco IOS Release 15.2(2)JB3 on all 1260, 1040, 1140, 3500i, 3500e, 3600i, 3600e, 2600i, 2600e, 1600i, 1600e, and 1550 series access points.

## Finding the Cisco IOS Software Release

To find the version of Cisco IOS software that is running on your access point, use a Telnet session to log into the access point, and enter the **show version EXEC** command.

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

## Upgrading to a New Software Release



### Note

You cannot use HTTPS file transfer to upgrade to Cisco IOS Release 15.2(2)JA from previous releases. Because of the image size for this release, you must use TFTP or FTP file transfer for the upgrade. Refer to the upgrade instructions at this URL:

[http://www.cisco.com/en/US/docs/wireless/access\\_point/12.4\\_10b\\_JA/configuration/guide/scg12410b-chap20-firmware.html#wp1035507](http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap20-firmware.html#wp1035507)

To upgrade your access point or bridge software, follow these steps:

- 
- Step 1** Follow this link to the Cisco home page:  
<http://www.cisco.com>
  - Step 2** Click **Support**. The Support and Documentation page appears.
  - Step 3** Under the Select a Product Name, click **Wireless**. The Product/Technology Support page appears.
  - Step 4** Under the Make a Selection to Continue section, click **Access Point**. Products and Access Point are highlighted.
  - Step 5** Select the access point model for which you need the information. For example, click the **Cisco Aironet 1260 series**. A list of documents appears.
  - Step 6** Click **Configure**. A list of configuration documents appears.
  - Step 7** Click **Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 15.2(2)JB3**.
  - Step 8** Navigate to the Managing Firmware and Software chapter.
- 

For information on Cisco IOS software, click this link to browse to the Cisco IOS Software Center on Cisco.com:

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

## Disabling Radios to Prevent Unexpected Reboots When Upgrading the 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 the software.

To disable the radio interfaces using the access point's web-browser interface, which you can access through the access point's Ethernet port, follow these steps:

- 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 Cisco Aironet 1260 Series Access Point web interface. The top navigation bar includes tabs for "RADIO0-802.11N2.4GHz STATUS", "DETAILED STATUS", "SETTINGS", and "CARRIER BUSY TEST". The "SETTINGS" tab is active. The main content area shows the "Network Interfaces: Radio0-802.11N2.4GHz Settings" page. The "Enable Radio" option is checked, and the "Current Status (Software/Hardware)" is "Enabled". The "Role in Radio Network" is set to "Non-Root Bridge". The "Data Rates" section shows "Require" selected for 1.0Mb/sec, 2.0Mb/sec, and 5.5Mb/sec. The "Operating Mode" is "Mixed".

- Step 2** Choose **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 access point CLI:

	<b>Command</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>interface dot11radio {0   1}</b>	Enters interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
<b>Step 3</b>	<b>shutdown</b>	Disables the radio port.
<b>Step 4</b>	<b>end</b>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>copy running-config startup-config</b>	(Optional) Saves 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.

## Supported Browsers

The following browsers are supported:

- Internet Explorer 8.x and later.
- Firefox 3.x and later.

## New Features and Important Installation Notes

No new features have been introduced in this release. Features introduced in Cisco IOS Release 15.2(2)JB2 continue to be supported.

For information on new features, and important notes on installing the software, see the release notes for Cisco IOS Release 15.2(2)JB2, at:

[http://www.cisco.com/c/en/us/td/docs/wireless/access\\_point/ios/release/notes/15-2\\_2\\_JB2.html](http://www.cisco.com/c/en/us/td/docs/wireless/access_point/ios/release/notes/15-2_2_JB2.html)

## Caveats

This section lists [Open Caveats](#) and [Resolved Caveats](#) for access points and bridges in Cisco IOS Release 15.2(2)JB3. For your convenience in locating caveats in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in boldface type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.

**Note**

If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:  
<http://tools.cisco.com/Support/BugToolKit/>

To become a registered cisco.com user, go to the following website:

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

## Open Caveats

The following table lists caveats that are open in Cisco IOS Release 15.2(2)JB3.

**Table 1**     *Open Caveats*

Identifier	Headline
CSCub96053	Cisco Aironet 3500 Series Access Points are getting DFS events due to radar signals on a DFS channel associated with a Cisco Unified Wireless IP Phone 7925.
CSCue90125	When monitoring the power on packets, it is seen that 40MHz block acknowledge packets are putting out maximum RF power on all antennas regardless of the configured power.
CSCuh52238	Client triggers false DFS detections due to Broadcom Radio Emissions.
CSCui25877	Radio PCI resets are seen on Cisco Aironet 1600 Series Access Points.
CSCui31945	A discrepancy is seen in the Txpower levels between SNMP and CLI.

## Resolved Caveats

The following table lists caveats that are resolved in Cisco IOS Release 15.2(2)JB3.

**Table 2**     *Resolved Caveats*

Identifier	Headline
CSCub58537	Traffic must not be allowed when the WEP40 and WEP128 key size do not match
CSCud00274	Non-native 802.11 frames incorrectly passed to the AP BVI1 interface
CSCud11674	Oxy: Enabling broad-key Multicast downstream fails on WGB wired client
CSCud44269	AP must not bridge ARP traffic for clients with DHCP required in WLAN
CSCuh46996	Clients behind 3rd party WGB fail DHCP post upgrade from 7.0.116.0
CSCui52567	GUI SSID manager page displays error and configuration is not reflected
CSCum26370	W56 Static TX power level changes to Max after AP reboot
CSCum85898	Autonomous AP crash at disc_vlan_find after association in 15.2(4)JB3a

## 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**.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

---

© 2013-2017 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://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. (1110R)

