



Release Notes for Cisco Aironet Access Points for Cisco IOS Release 15.3(3)JPK2, 15.3(3)JPK3, 15.3(3)JPK4, and 15.3(3)JPK6

This document describes features, enhancements, and caveats for autonomous mode access points using Cisco IOS Release 15.3(3)JPK2, 15.3(3)JPK3, 15.3(3)JPK4, and 15.3(3)JPK6.

The release notes for lightweight Cisco Aironet Access Points are included in the *Release Notes for Cisco Wireless Controllers and Lightweight Access Points*, at the following URL:

<https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html>

Supported Cisco Aironet Access Points

This release supports the following Cisco Aironet access points in autonomous mode:

- Cisco Industrial Wireless 3700 Series Access Points



Contents

These release notes contain these sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Updates and Features in this Release, page 4](#)
- [Important Notes, page 6](#)
- [Caveats, page 4](#)
- [Troubleshooting, page 5](#)

Introduction

The Cisco Industrial Wireless 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

Cisco Industrial Wireless 3700 Series Access Point supports 64 MB minimum flash.

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

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 and Learn**.
The Support and Learn page appears.
 - Step 3** Under Find Product and Downloads section, enter the product name.
For example, enter 3702 in the search field. The Product Support page and Downloads options appear.
 - Step 4** Click **Downloads**.

- Step 5** Click **Autonomous AP IOS Software**.
List of supported release software download options appear.
- Step 6** Download the selected software release.

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

<https://software.cisco.com/download/home>

Converting a Lightweight Access Point Back to Autonomous Mode

You can convert an access point from lightweight mode back to autonomous mode by loading a Cisco IOS Release that supports autonomous mode. If the access point is associated with a controller, you can use the controller to load the Cisco IOS release. If the access point is not associated with a controller, you can load the Cisco IOS release using TFTP. The image files and their supported access points are listed in [Table 1](#).

Table 1 *Image File Names*

Image File	Supported Access Points
Ap3g2	IW 3700

Disabling Radios to Prevent Unexpected Reboots When Upgrading the System Software

It is recommended to disable the radio interfaces before upgrading the software to prevent the access point from rebooting unexpectedly.

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.
- 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:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>interface dot11radio {0 1}</code>	Enters 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	<code>shutdown</code>	Disables the radio port.
Step 4	<code>end</code>	Returns to privileged EXEC mode.
Step 5	<code>copy running-config startup-config</code>	(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

These browsers are supported:

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

New Updates and Features in this Release

There are no new features or updates introduced in this release.

Caveats

This section lists the [Open Caveats](#) and [Resolved Caveats](#) for access points and bridges in Cisco IOS Release .

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat listed in this document:

1. Access the BST (use your Cisco user ID and password) at <https://tools.cisco.com/bugsearch/>.
2. Enter the bug ID in the **Search For:** field.



Note

To have a Cisco User ID and password, you need to be a registered cisco.com user, To become a registered cisco.com user, go to the following website:
<https://tools.cisco.com/RPF/register/register.do>

Open Caveats

There are no open caveats in Cisco IOS Release 15.3(3)JPK2, 15.3(3)JPK3, 15.3(3)JPK4, and 15.3(3)JPK6.

Resolved Caveats

There are no resolved caveats in Cisco IOS Release 15.3(3)JPK3 and 15.3(3)JPK4.

Table 3 lists caveats that have been resolved in Cisco IOS Release 15.3(3)JPK6.

Table 2 Resolved Caveats in 15.3(3)JPK6

Identifier	Headline
CSCwd11897	Power parameter for AP803 under the radio interface shows ambiguous

Table 3 lists caveats that have been resolved in Cisco IOS Release 15.3(3)JPK2.

Table 3 Resolved Caveats in 15.3(3)JPK2

Identifier	Headline
CSCvw88392	Factory Reset on IW3702 via RESET/MODE button not enforced
CSCvw90523	IW3702 in WGB takes too much time to authenticate when Radio 1 is bounced on WGB AP
CSCvx32096	Removing 3DES cipher for Cisco Wave 1 AP's
CSCvx71577	Controller sends MDIE to IOS APS when WLAN is configured for adaptive FT enabled Flex Local Auth/SW
CSCvx84524	Cisco Aironet 1570 AP does not display the RRM neighbors
CSCvy32680	Multiple Vulnerabilities in Frame Aggregation and Fragmentation Implementation of 802.11
CSCvy32690	Multiple Vulnerabilities in Frame Aggregation and Fragmentation Implementation of 802.11-1532

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**.

Important Notes

This section describes important information about access points and bridges.

Point-to-Point and Point-to-Multipoint Bridging Support for 802.11n Platforms

The point-to-point and point-to-multipoint bridging is supported on the 802.11n Cisco Aironet series access points. The 5-GHz bands support 20 and 40-MHz channel widths, and the 2.4-GHz bands support only a 20-MHz channel width.

The following items are supported on the 802.11n platforms for bridging:

- MIMO, short-range bridging (on campus or inter-building bridge deployments), with dipole and MIMO antennas (line of sight and short range) under 1 km.
- 20-MHz and 40-MHz 802.11n support.
- Workgroup bridge (WGB) short-range support.
- SISO (single-in, single-out), MCS 0-7 and legacy bridge rates (802.11 a/b/g and 802.11n) using one outdoor antenna.

**Note**

This is only supported using short range links and is not a replacement for the 1530 and 1570 series access points which support bridging.

The following are not supported on AP 702 for bridging:

- The distance CLI command: long-range links over 1 km currently are not supported; therefore, the distance command is not supported.
- Outdoor MIMO bridging using external antennas has not been fully tested and is not fully supported with this release.

Low Throughput Seen on Access Points with 16 BSSIDs Configured

If your network uses 16 BSSIDs with 1 and 2-Mbps data rates, access points might experience very low throughput due to high management traffic.

802.11n HT Rates Apply Only to No Encryption or WPA2/AES Encryption

As per the 802.11n amendment, the 802.11n HT rates apply only to no encryption or WPA2/AES encryption. They do not apply to WEP or WPA encryption. If WEP or TKIP encryption is used, the access point and any 802.11n clients will not transmit at HT rates. Legacy rates (802.11a/b/g) will be used for any clients using WEP or TKIP encryption.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).

- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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. 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. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.

