Release Notes for Cisco Access Points and Bridges for Cisco IOS Release 15.3(3)JPQ, 15.3(3)JPQ1, and 15.3(3)JPQ2

First Published: 2023-08-01

Last Modified: 2024-03-22

About the Release Notes

This document describes features, enhancements, and caveats for autonomous mode access points using the Cisco IOS Release software.

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:

- Support is reintroduced for the following APs from 17.9.3:
  - Cisco Aironet 1570 Series Access Points
  - Cisco Aironet 1700 Series Access Points
  - Cisco Aironet 2700 Series Access Points
  - Cisco Aironet 3700 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points

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.

What's New in Release

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

System Requirements

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

Software Upgrade

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:

Procedure

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.

What to do next

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: Image File Names, on page 3.

Table 1: Image File Names

Image File	Supported Access Points
Ap3g2	IW 3700

Supported Browsers

These browsers are supported:

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

Disabling Radios to Prevent Unexpected Reboots When Upgrading the System Software (GUI)

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:

Procedure

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.

What to do next

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

Disabling Radios to Prevent Unexpected Reboots When Upgrading the System Software (CLI)

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

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

Procedure

Step 1 configure terminal

Enters global configuration mode.

Step 2 interface dot11radio {0 | 1}

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 shutdown

Disables the radio port.

Step 4 **end**

Returns to privileged EXEC mode.

Step 5 **copy running-config startup-config**

(Optional) Saves your entries in the configuration file.

What to do next

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.

Caveats

Open Caveats

There are no open caveats in Cisco IOS Release 15.3(3)JPQ, 15.3(3)JPQ1, and 15.3(3)JPQ2.

Resolved Caveats

There are no resolved caveats in Cisco IOS Release 15.3(3)JPQ2.

Table 2: Resolved Caveats in 15.3(3)JPQ1

Identifier	Headline
CSCvz07719	Autonomous AP ends up in boot prompt when primary image in flash gets corrupted.
CSCwf28550	Both controller and Cisco Catalyst 9124 AP are unable to fetch wired client information from WGB.

Table 3: Resolved Caveats in 15.3(3)JPQ

Identifier	Headline
CSCwe87845	Cisco Industrial Wireless 3702 Series Access Points: WGB changes TID for EAP packets from TID 7 to TID 0.

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 DevNet.
- 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 gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.