



Release Notes for Cisco Aironet 1130AG, 1200, 1230AG, and 1240AG Series Access Points for Cisco IOS Release 12.3(7)JX

August 22, 2005

These release notes describe features, enhancements, and caveats for Cisco IOS Release 12.3(7)JX.



Note

This release must only be loaded onto access points at the factory or by using the Cisco IOS-TO-LWAPP upgrade tool. Your access point might become inoperable if you install this software without using the upgrade tool.

Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Features, page 4](#)
- [Installation Notes, page 4](#)
- [Important Notes, page 7](#)
- [Caveats, page 8](#)
- [Troubleshooting, page 9](#)
- [Related Documentation, page 10](#)
- [Obtaining Documentation and Submitting a Service Request, page 10](#)



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Introduction

Cisco IOS Release 12.3(7)JX provides support for the lightweight access point protocol (LWAPP) for 1130AG, 1200, 1230AG, and 1240AG series access points. When you use the Cisco IOS-TO-LWAPP upgrade tool to upgrade one of these access points to this release, the access point communicates with a Cisco 2006 series wireless LAN controller or a 4400 series controller and receives a full LWAPP configuration and software image from the controller. This release also functions as a recovery image if the access point fails to receive a full image from the controller.


Note

This release must only be loaded onto access points at the factory or by using the Cisco IOS-TO-LWAPP upgrade tool. Your access point might become inoperable if you install this software without using the upgrade tool.

System Requirements

You can use the Cisco IOS-TO-LWAPP upgrade tool to install Cisco IOS Release 12.3(7)JX on these access points:

- All 1130AG and 1240AG access points
- All modular 1200 series access points running Cisco IOS software and containing these supported radios:
 - 802.11g: MP21G, MP31G
 - 802.11a: AIR-RM21A-x-K9, AIR-RM22A-x-K9


Note

Access points must run Cisco IOS Release 12.3(7)JA or later before you use the upgrade tool to install this release.


Note

After you use the upgrade tool to install this release, the upgraded access point must connect to a wireless LAN controller to download a full LWAPP image and begin sending and receiving data.

Upgrading to this Software Release

For instructions on using the Cisco IOS-TO-LWAPP upgrade tool to install this software, refer to the *Application Note: Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* at this URL:

http://www.cisco.com/en/US/products/ps6108/prod_technical_reference_list.html

These are the main steps in the Cisco IOS-TO-LWAPP upgrade:

1. Prepare your network infrastructure so that converted access points can connect to a wireless LAN controller after the upgrade.
2. Find the Cisco IOS-TO-LWAPP upgrade tool and Cisco IOS release 12.3(7)JX at the Software Center on Cisco.com. Click this link to browse to the Cisco IOS Software Center:

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

In the menu on the left, click **Wireless Software** and log into Cisco.com to view the Cisco Wireless Software Display Tables.

3. Make sure that the access points that you want to upgrade to LWAPP mode are running Cisco IOS release 12.3(7)JA or later.
4. Prepare the wireless LAN controller for the upgrade.
5. Use the Cisco IOS-TO-LWAPP upgrade tool to upgrade the access points.

Refer to *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* for detailed instructions.

Reverting from LWAPP Mode to Autonomous Mode

After you use the Cisco IOS-TO-LWAPP upgrade tool to load Cisco IOS release 12.3(7)JX on an access point, you can convert the access point from an LWAPP unit back to an autonomous unit by loading a Cisco IOS release that supports autonomous mode (Cisco IOS release 12.3(7)JA or earlier). If the access point is associated to a controller, you can use the controller to load the Cisco IOS release. If the access point is not associated to a controller, you can load the Cisco IOS release using TFTP.

Using a Wireless LAN Controller to Return to a Previous Release

Follow these steps to revert from LWAPP mode to autonomous mode using a wireless LAN controller:

-
- Step 1** Log into the CLI on the controller to which the access point is associated.
- Step 2** Enter this command:
- ```
config ap tftp-downgrade tftp-server-ip-address filename access-point-name
```
- 

### Using a TFTP Server to Return to a Previous Release

Follow these steps to revert from LWAPP mode to autonomous mode by loading a Cisco IOS release using a TFTP server:

- 
- Step 1** The PC on which your TFTP server software runs must be configured with a static IP address in the range of 10.0.0.2 to 10.0.0.30.
- Step 2** Make sure that the PC contains the access point image file (such as *c1200-k9w7-tar.122-15.JA.tar* for a 1200 series access point) in the TFTP server folder and that the TFTP server is activated.
- Step 3** Rename the access point image file in the TFTP server folder to **c1200-k9w7-tar.default** for a 1200 series access point.
- Step 4** Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.
- Step 5** Disconnect power from the access point.
- Step 6** Press and hold the **MODE** button while you reconnect power to the access point.
- Step 7** Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the **MODE** button.
- Step 8** Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

**Step 9** After the access point reboots, reconfigure the access point using the GUI or the CLI.

---

## New Features

This section lists new features in Cisco IOS Release 12.3(7)JX. [Table 1](#) lists the features that are supported on the devices that support this release.

**Table 1** *New Features Introduced for Access Points in Cisco IOS Release 12.3(7)JX*

| Feature                            | 1130AG Series | 1200 Series | 1230AG Series | 1240AG Series |
|------------------------------------|---------------|-------------|---------------|---------------|
| LWAPP Upgrade and Recovery Support | x             | x           | x             | x             |

## LWAPP Upgrade and Recovery Support

This feature allows an access point to communicate with a wireless LAN controller in order to receive the LWAPP image mandated by the controller. New LWAPP access points or access points being upgraded from autonomous to LWAPP mode use the LWAPP-recovery support feature to receive their LWAPP image from the controller. This release is also used as a recovery image in case the full LWAPP image becomes corrupted. The LWAPP-recovery support feature limits access point functionality to just that which is necessary to download a complete LWAPP image; for example, the radios are disabled on access points running the LWAPP-recovery support feature.

## Installation Notes

This section contains information you should keep in mind when installing access points.

### Installation in Environmental Air Space

This section provides information on installing 1200 series access points in environmental air space, such as above suspended ceilings.

Cisco Aironet 1130AG and 1200 Series Access Points provide adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(C) of the *National Electrical Code* (NEC) and Sections 2-128, 12-010(3) and 12-100 of the *Canadian Electrical Code*, Part 1, C22.1.



#### Caution

The power injector does not provide fire resistance and low smoke-producing characteristics and is not intended for use in extremely high or low temperatures or in environmental air spaces such as above suspended ceilings.

---

**Note**

If you plan to mount a 1200 series access point with a 5-GHz radio in an area subject to environmental air space, Cisco recommends that you mount the access point horizontally so that its antennas point down. Doing so ensures that the access point complies with regulatory requirements for environmental air space with the 5-GHz radio installed.

## Power Considerations

This section describes issues you should consider before applying power to an access point.

**Caution**

The nominal voltage for 1200 series access points is 48 VDC, and the access point is operational up to 60 VDC. Voltage higher than 60 VDC can damage the equipment.

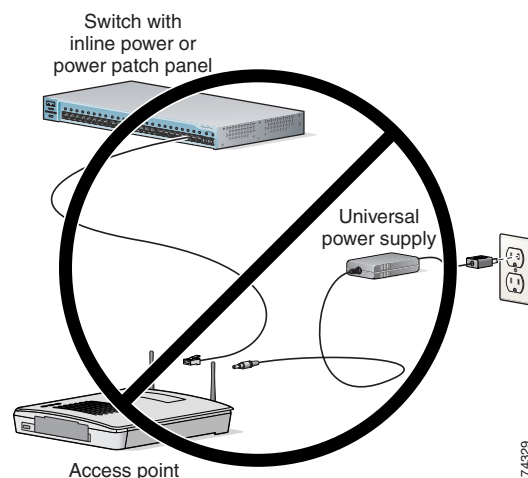
**Caution**

Cisco Aironet power injectors are designed for use with Cisco Aironet access points and bridges only. *Do not use the power injector with any other Ethernet-ready device.* Using the power injector with other Ethernet-ready devices can damage the equipment.

## Use Only One Power Option

You cannot provide redundant power to 1130AG and 1200 series access points with both DC power to its power port and inline power from a patch panel or powered switch to the access point's Ethernet port. If you apply power to the access point from both sources, the switch or power patch panel might shut down the port to which the access point is connected. [Figure 1](#) shows the power configuration that can shut down the port on the patch panel or powered switch.

**Figure 1** *Improper Power Configuration Using Two Power Sources*



## Configuring Power for 1130AG Access Points

The 1130AG access point disables the radio interfaces when the unit senses that the power source to which it is connected does not provide enough power. Depending on your power source, you might need to enter the power source type in the access point configuration. Use the System Software: System Configuration page on the web-browser interface to select a power option. Figure 2 shows the System Power Settings section of the System Configuration page.

**Figure 2** Power Options on the System Software: System Configuration Page

| System Power Settings                |                                                                                                                     |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Power State:                         | FULL POWER                                                                                                          |
| Power Source:                        | AC_ADAPTOR                                                                                                          |
| Power Settings:                      | <input type="radio"/> Power Negotiation <input checked="" type="radio"/> Pre-standard Compatibility                 |
| Power Injector:                      | <input type="checkbox"/> Installed on Port with MAC Address: <input type="text" value="DISABLED"/> (HHHH.HHHH.HHHH) |
| <input type="button" value="Apply"/> |                                                                                                                     |

### Using the AC Power Adapter

If you use the AC power adapter to provide power to the 1130AG access point, you do not need to adjust the access point configuration.

### Using a Switch Capable of IEEE 802.3af Power Negotiation

If you use a switch to provide Power over Ethernet (PoE) to the 1130AG access point and the switch supports the IEEE 802.3af power negotiation standard, select **Power Negotiation** on the System Software: System Configuration page.

### Using a Switch That Does Not Support IEEE 802.3af Power Negotiation

If you use a switch to provide Power over Ethernet (PoE) to the 1130AG access point and the switch does not support the IEEE 802.3af power negotiation standard, select **Pre-Standard Compatibility** on the System Software: System Configuration page.

### Using a Power Injector

If you use a power injector to provide power to the 1130AG access point, select **Power Injector** on the System Software: System Configuration page and enter the MAC address of the switch port to which the access point is connected.

## Operating 5-GHz Radio Requires Power Injector, Power Module, or Catalyst 3550-24 PWR Switch

The 1200 series power injector and the 1200 series power module support operation of the 5-GHz radio in the access point. Currently, the Catalyst 3550-24 PWR switch supports power for both the 2.4-GHz radio and the 5-GHz radio. Other switches and power patch panels might not provide enough power for the 5-GHz radio.

## Access Point Requires 1200 Series Universal Power Supply and Power Injector

The 350 series universal power supply and power injector are not compatible with the 1200 series access point. If you use a power injector or a power module to provide power to a 1200 series access point, you must use a 1200 series universal power supply. If you need to use a power injector to inject power into the access point's Ethernet port, you must use a 1200 series power injector.

## Antenna Installation

For instructions on the proper installation and grounding of external antennas for 1200 series access points, refer to the National Fire Protection Association's *NFPA 70, National Electrical Code*, Article 810, and the Canadian Standards Association's *Canadian Electrical Code*, Section 54.



---

**Do not install the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death.**

---

## Important Notes

This section describes important information about the access point.

### Default Username and Password Are *Cisco*

You must enter a username and password when you log into an access point interface. The default username for administrator login is *Cisco*, and the default password is *Cisco*. Both the username and password are case sensitive.

### Cisco IOS Release 12.3(7)JX Supports 2006 and 4400 Controllers Only

When you load this release on an access point, the access point can communicate with Cisco 2006 series wireless LAN controllers or 4400 series controllers only. Cisco 4100 series, Airespace 4012 series, and Airespace 4024 series controllers are not supported because lack the memory required to support access points running Cisco IOS software.

### Access Points Converted to LWAPP do not Support WDS

Access points converted to LWAPP mode communicate only with Cisco wireless LAN controllers and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.

## Access Points Converted to LWAPP Support 8 BSSIDs per Radio

Access points converted to LWAPP mode support 8 BSSIDs per radio and a total of 8 wireless LANs per access point. (Cisco 1000 series access points support 16 BSSIDs per radio and 16 wireless LANs per access point.) When a converted access point associates to a controller, only wireless LANs with IDs 1 through 8 are pushed to the access point.

## Access Points Converted to LWAPP do not Support Layer 2 LWAPP

Access Points converted to LWAPP must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.

## Access Points Converted to LWAPP Provide Read-Only Console Port

After you convert an access point to LWAPP mode, the console port provides read-only access to the unit.

## Caveats

This section lists open and resolved caveats in Cisco IOS Release 12.3(7)JX.

### Open Caveats

These caveats are open in Cisco IOS Release 12.3(7)JX:

- CSCsb47748—When the Rogue Location Discovery Protocol (RLDP) is enabled on a controller, associated access points converted to lightweight mode do not detect rogue access points as a threat.
- CSCei65293—The 5-GHz, RM-21A radio module on 1200 series access points has an articulating antenna with a dual function: diversity omni or patch antenna. When the antenna is folded flat to the access point housing it is in 9-dBi patch mode, and when it is in any other position it is in 5-dBi omni mode. When you change the antenna position to switch antenna modes you must reset the access point to apply the change.
- CSCsb68069—When all eight wireless LANS are defined on 1130AG and 1240AG access points converted to lightweight mode, and the radio environment is very busy, access point transmission attempts can be delayed. The 802.11g radios sometimes report this error:

```
%DOT11-2-RADIO_FAILED: Interface Dot11Radio0, failed - Radio command failed, cmd 121
(F80,0,0) status 7F21 (5,0,0)
```

When the failure occurs, the radio restarts, all clients are disassociated, the failure is logged, and normal operation resumes.

Workaround: Reduce the number of wireless LANs in use.

## Resolved Caveats

The following caveat is resolved in this release:

- CSCsb24007

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCei61732—

Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.

## 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**.

## Related Documentation

This section lists documents related to 1130AG, 1200 series, and 1240AG access points.

- *Cisco Aironet Conversion Tool for Cisco IOS Software, 2.0 Administrator Guide for Windows*
- *Quick Start Guide: Cisco Aironet 1200 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1240AG Access Points*
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *Installation Instructions for Cisco Aironet Power Injectors*

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

---

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [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. (1005R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.