Release Notes for Cisco Aironet 1200 Series Access Points

July 3, 2002

These release notes describe caveats for Cisco Aironet 1200 Series Access Points running firmware version 11.42T. This firmware release resolves bug CSCdx79987.

Contents

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

Introduction

Cisco Aironet Access Points are wireless LAN transceivers that can act 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 allows wireless users to move freely throughout the facility while maintaining uninterrupted access to the network. The 1200 series access point allows you to add a 5-GHz radio module for dual-radio operation, and the 2.4-GHz internal radio is accessible and can be upgraded as new radios become available.

The access point uses a browser-based management system. The system settings are contained on web pages in the access point's firmware. You use your internet browser, a command-line interface, or SNMP commands to adjust access point settings.

Firmware version 11.42T resolves bug CSCdx79987.

New Features

Firmware version 11.42T resolves bug CSCdx79987 and does not include new software features.

Installation Notes

You can find the latest release of access point firmware at the following URL:

http://www.cisco.com/public/sw-center/sw-wireless.shtml

Installation in Environmental Air Space

Cisco Aironet 1200 Series Access Points are suitable for use in environmental air space in accordance with Section 300-22(c) of the *National Electrical Code*.

Note If you plan to mount the access point in an area subject to environmental air space with the intention of upgrading to a 5-GHz radio, Cisco recommends that you mount the access point horizontally so that its antennas point down. Doing so results in the access point complying with regulatory requirements for environmental air space after the 5-GHz radio is installed.

Caution The Cisco Aironet power injector has a smaller operating temperature range (32 to 104°F; 0 to 40°C) than the 1200 series access point. The power injector is not intended for use in extremely high or low temperatures or in environmental air spaces, such as above suspended ceilings.

Antenna Installation

For instructions on the proper installation and grounding of external antennas, 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.

Warning **Do not locate 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.**

Power Considerations

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

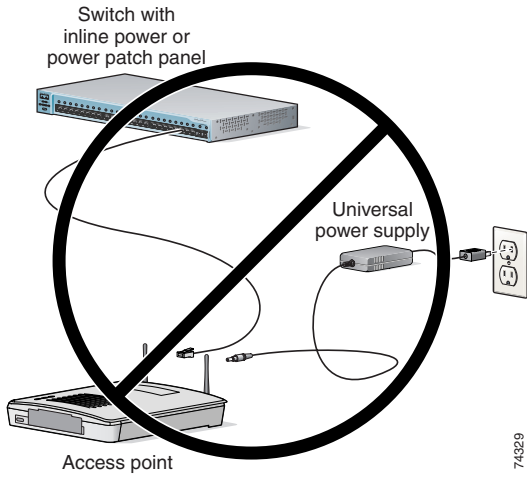
Caution The nominal voltage for 1200 series access points is 48VDC, and the access point is operational up to 60VDC. Voltage higher than 60VDC can damage the equipment.

Caution Cisco Aironet power injectors are designed for use with 1200 series access points 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 the access point 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



Access Point Requires 1200 Series Universal Power Supply and Power Injector

You must use a 1200 series universal power supply to power the access point. 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. The 350 series universal power supply and power injector are not compatible with the 1200 series access point.

System Requirements

You must have a 1200 series access point to install firmware version 11.42T.

Version Supported

Your access point must be running firmware version 11.40T or later to install firmware version 11.42T.

Upgrading to a New Firmware Release

Determining the Firmware Version

The firmware version number is in the upper-left corner of most management screens in the web-browser interface and at the top of the home (Summary Status) page in the command-line interface.

Upgrade Procedure

For instructions on installing access point firmware:

1. Follow this link to the Cisco Aironet documentation home page:

   http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm

2. Follow this path to the product, document, and chapter:
   Aironet 1200 Series Wireless LAN Products > Cisco Aironet 1200 Series Access Points > Cisco Aironet 1200 Series Access Point Software Configuration Guide > Managing Firmware and Configurations > Updating Firmware
3. Follow this link to the Software Center on Cisco.com and download firmware version 11.42T:

   http://www.cisco.com/public/sw-center/sw-wireless.shtml

Note To upgrade firmware from a file server, you must enter settings on the access point's FTP Server Setup page. Refer to the "Updating from a File Server" section on page 6-5 in the *Cisco Aironet 1200 Series Access Point Software Configuration Guide* for more information.

Limitations and Restrictions

This section describes limitations and restrictions for 1200 series access points.

Removing Power During Firmware Update Can Corrupt Radio Firmware

When you update the firmware on an access point, allow the unit to finish its start-up sequence before removing power. If you update the firmware and remove power before the unit finishes the start-up sequence, the radio firmware might be corrupted, making the unit inoperable. If the radio firmware is corrupted, the radio indicator (the bottom of the three indicators on top of the access point) is red continuously, and the following error message appears when the access point starts up:

```
Failed to start driver for port "awc0" (errno=0x006d0002)
```

If the radio firmware is corrupted, try resetting the unit to factory defaults using the **:resetall** command in the CLI; see the "Resetting to the Default Configuration" section on page 9-42 of the *Cisco Aironet 1200 Series Access Point Software Configuration Guide* for instructions on resetting the access point. If the unit cannot be reset to defaults, you must return the unit to Cisco for service.

Note The **resetall** command is valid for only 2 minutes immediately after the access point reboots.

You can safely remove power after a firmware update when the configuration management pages reappear in the command-line or web-browser interfaces, or when the three status indicators on top of the unit complete the following pattern:

1. All three indicators are steady green, meaning that the access point is beginning to update the firmware.
2. The middle indicator is steady green and the top and bottom indicators are off, indicating that the access point is updating the radio firmware.

When the middle indicator blinks or the top and bottom indicators blink, you can remove power.

EAP Authentication Requires Matching 802.1x Protocol Drafts

Note This section applies to wireless networks set up to use LEAP. If you do not use LEAP on your wireless network, you can skip this section.

Wireless client devices use Extensible Authentication Protocol (EAP) to log onto a network and generate a dynamic, client-specific WEP key for the current logon session. If your wireless network uses WEP without EAP, client devices use the static WEP keys entered in the Aironet Client Utilities.

If you use Network-EAP authentication on your wireless network, your client devices and access points must use the same 802.1x protocol draft. For example, if the radio firmware on the client devices that will associate with an access point is 4.16, the access point should be configured to use Draft 8 of the 802.1x protocol. Table 1 lists firmware versions for Cisco Aironet products and the draft with which they comply.

Table 1 802.1x Protocol Drafts and Compliant Client Firmware

Firmware Version	Draft 7	Draft 8	Draft 10[1]
PC/PCI cards 4.13	—	x	—
PC/PCI cards 4.16	—	x	—
PC/PCI cards 4.23	—	x	—
PC/PCI cards 4.25 and later	—	—	x
WGB34x/352 8.58	—	x	—
WGB34x/352 8.61 and later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later[2]	—	x	x
AP34x/35x 11.07 and later	—	x	x
AP12xx 11.40T and later	—	x	x

1. The functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1x standard.
2. The default draft setting in access point firmware version 11.06 and later is Draft 10.

Use the Authenticator Configuration page to select the draft of the 802.1x protocol the access point should use. Follow these steps to set the draft for your access point:

Step 1 Browse to the Authenticator Configuration page in the access point management system:

a. On the Summary Status page, click **Setup**.

b. On the Setup page, click **Security**.

c. On the Security Setup page, click **Authentication Server**.

Step 2 Use the 802.1x Protocol Version (for EAP authentication) pull-down menu to select the draft of the 802.1x protocol the access point radio should use. Menu options include:

- Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting.
- Draft 8—Select this option if LEAP-enabled client devices that associate with this access point use radio firmware versions 4.13, 4.16, or 4.23.
- Draft 10—This is the default setting. Select this option if client devices that associate with this access point use Microsoft Windows XP EAP authentication or if LEAP-enabled client devices that associate with this access point use radio firmware version 4.25 or later. The functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1x standard.

Step 3 Click **Apply** or **OK** to apply the setting. The access point reboots.

Select WEP Key 1 as Transmit Key for EAP Authentication

If you use Network-EAP as the authentication type on your wireless network, you must select key 1 as the transmit key on the access point AP Radio Data Encryption page. The access point uses the WEP key you enter in key slot 1 to encrypt multicast and broadcast data signals that it sends to EAP-enabled client devices. Because the access point transmits the WEP key used for multicast messages to the EAP-enabled client device during the EAP authentication process, that key does not have to appear in the EAP-enabled device's WEP key list. The access point uses a dynamic WEP key to encrypt unicast messages to EAP-enabled clients. When you set up a repeater access point to authenticate as a LEAP client, the repeater derives a dynamic WEP key and uses it to communicate with the root access point. Repeaters not set up for LEAP authentication use static WEP keys when communicating with other access points.

Note If you do not use EAP authentication on your wireless network, you can select any WEP key as the transmit key. If you use EAP authentication and you enable broadcast key rotation, you can enable WEP without entering WEP keys.

MIB File Compatible with Firmware Version 11.00 and Later

The access point MIB file (AWCVX-MIB) is supported only by access point firmware version 11.00 and later. Earlier versions of firmware do not support this MIB. You can download the access point MIB at http://www.cisco.com/public/sw-center/sw-wireless.shtml.

Important Notes

This section lists important information about access points running firmware version 11.42T.

New Default Setting for Data Beacon Rate (DTIM)

In firmware version 11.42T, the default setting for Data Beacon Rate (DTIM) on the AP Radio Hardware page is 1. This setting determines how often the access point's beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them.

The new default setting causes client devices using power-save mode to wake up more often than the default setting in firmware version 11.40T, which was 2. To conserve battery power in client devices using power-save mode, increase the Data Beacon Rate (DTIM) setting.

See the "Data Beacon Rate (DTIM)" section on page 3-28 of the *Cisco Aironet 1200 Series Access Point Software Configuration Guide* for more information on this setting.

Set Flow Control to None or Xon/Xoff When Using Terminal Emulator

The terminal emulator flow control setting for 1200 series access points (**none** or **Xon/Xoff**) differs from the flow control setting for 340 and 350 series access points (**none**, **Xon/Xoff**, or **Hardware**).

To use a terminal emulator to open the 1200 series access point's command-line interface (CLI), use these settings for the terminal emulator connection:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit
- No flow control or Xon/Xoff

Reboot of Workgroup Bridges Required When Allowing More Than 20

With firmware version 11.42T, you can select **no** for the *Classify Workgroup Bridges as Network Infrastructure* setting on the AP/Root Radio Advanced page to allow up to 50 workgroup bridges to associate to the access point. When you select **no** for this setting, you must reboot workgroup bridges associated to the access point.

Cisco Discovery Protocol Re-Enabled for Individual Interfaces on Reboot

The Cisco Discovery Protocol (CDP) feature is enabled by default, and CDP is enabled for each of the access point's individual interfaces by default. However, if you disable CDP for one of the individual interfaces, the access point re-enables CDP for that interface when it reboots. If you disable CDP completely, the access point does not re-enable CDP on reboot.

Caveats

This section lists resolved and open software issues in firmware version 11.42T.

Getting Bug Information on Cisco.com

If you are a registered Cisco user, you can use the Cisco TAC Software Bug Toolkit, which consists of three tools (Bug Navigator, Bug Watcher, and Search by Bug ID Number) that help you identify existing bugs (or caveats) in Cisco software products.

Access the TAC Software Bug Toolkit at http://www.cisco.com/support/bugtools/.

Resolved Caveats

The following caveat has been resolved in firmware version 11.42T:

- Resolved: CSCdx79987—1200 series access points no longer hang under bursts of Ethernet traffic, such as Association Table updates from other access points.

Open Caveats

The following caveats have not been resolved for firmware version 11.42T:

- CSCdx03420—Radio might shut down when downgrading firmware.

  When you downgrade access point firmware, the unit's radio might shut down. Workaround: Select **yes** for the *Require use of Radio Firmware X.XX* setting on the AP/Root Radio Advanced page and follow the firmware downgrade steps again.

- CSCdx07970—Cannot restore defaults on the CLI's Ethernet Protocol Filters and Root Radio Protocol Filters pages.

  The Restore Defaults feature does not work on the CLI's Ethernet Protocol Filters and Root Radio Protocol Filters. Workaround: Use the web-browser interface to restore defaults on the Ethernet Protocol Filters and Root Radio Protocol Filters pages.

- CSCdx11703—Hot standby packets can flood the network.

  Each time a standby access point checks the status of the access point it is monitoring, it sends 11 probe packets. If you have several access points on your network set up for hot standby, the probe packets can overload your network. Workaround: Enter a higher value for the *Polling Frequency* setting on the Hot Standby page. For example, instead of polling the monitored access point every few seconds, enter **600** in the Polling Frequency entry field to poll the monitored access point every ten minutes.

- CSCdw13878—Setting up hot standby when monitored access point's radio is disabled locks up standby access point.

  If the radio is disabled on the monitored access point when you set up the standby access point, the standby access point reports an initialization failure and must be rebooted. Workaround: Make sure the monitored access point's radio is working when you set up the standby access point.

- CSCdw16742—Broadcast key rotation does not work with repeater access points.

  When broadcast key rotation is enabled on a repeater access point that is authenticated to the network using LEAP, data cannot be passed between the repeater and the root access point. Workaround: Do not use broadcast key rotation on a repeater access point.

- CSCdx19068—Unlimited LEAP logins configuration on ACS server can lock out roamed clients.

  When the ACS server's session policy is configured for other than unlimited simultaneous LEAP logins and a LEAP-enabled client device roams away from the access point long enough for a STOP record to appear in the Radius Accounting log, the client cannot reauthenticate until it is purged from the list of logged-in users on the ACS server. Workaround: Set the server's IETF (028) idle timeout attribute to a low value so the server ends the roamed client's session and the client can start a new session when it returns.

- CSCdx19118—The access point reboots when more than 23 workgroup bridges are associated to it and you change one of these settings:
  - *SSID* on the Express Setup or AP/Root Radio Hardware pages
  - *Classify Workgroup Bridges as Network Infrastructure* on the AP/Root Radio Advanced page
  - *Requested Status* on the AP/Root Radio Advanced page from Up to Down and back to Up

- CSCdx19270—When the *Classify Workgroup Bridges as Network Infrastructure* setting is set to yes on an access point with more than 23 workgroup bridges associated, the access point reboots when the workgroup bridges send small amounts of data. Workaround: Reduce the number of workgroup bridges associated to the access point, or change the *Classify Workgroup Bridges as Network Infrastructure* setting to **no**.

- CSCdx87342—IP phones set to Max PSP do not respond to signals from a 1200 series access point when the Data Beacon Rate (DTIM) setting on the AP Radio Hardware page is set to 8 or higher. The Data Beacon Rate setting determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them. Workaround: Set IP phones associated to a 1200 series access point to CAM mode, or change the Data Beacon Rate setting on the 1200 series access point to 2, which is the default.
- CSCdx89832—When you access the management system on a 1200 series access point through the console port, the access point sometimes displays the prompt for a username but not a password when User Manager is enabled. Workaround: Use a Telnet session to access the management system.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at http://www.cisco.com/tac. Select **Wireless Technologies** under Top Issues.

Related Documentation

Use the following documents with this document:

- *Quick Start Guide: Cisco Aironet 1200 Series Access Points*
- *Quick Start Guide: 1200 Series Access Point 2.4-GHz Radio Installation Instructions*
- *Cisco Aironet 1200 Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1200 Series Access Point Software Configuration Guide*

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.