



Release Notes for Cisco Aironet Access Points for Firmware Release 11.03

Contents

- Introduction, page 1
- System Requirements, page 2
- Upgrading to a New Firmware Release, page 2
- Limitations and Restrictions, page 3
- Caveats, page 3
- Troubleshooting, page 5
- Related Documentation, page 5
- Obtaining Documentation, page 5
- Obtaining Technical Assistance, page 7

Introduction

This document describes requirements, installation procedures, and caveats for Cisco Aironet Access Point firmware version 11.03.

Firmware version 11.03 resolves sporadic lockup of 350 series Access Points when they are configured to use long headers and antenna diversity. Client adapter firmware release 4.16 is available for upgrading 350 series wireless LAN adapters. The 340 series does not have this problem, so upgrades to 11.03 and 4.16 do not provide any features or benefits for 340 series Access Points and wireless LAN adapters.



System Requirements

You must have a Cisco Aironet 340 or 350 series Access Point to install firmware version 11.03.

Version Supported

Your Access Point must be running firmware version 10.x or later to install firmware version 11.03.

Upgrading to a New Firmware Release

Determining the Firmware Version

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

Upgrade Procedure

For instructions on installing Access Point firmware:

1. Click on the following link to go to the Cisco Aironet documentation home page on CCO:
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm>
2. Use the following link path to go to the product, document and chapter:
Aironet 350 Series Wireless LAN Products > Cisco Aironet 350 Series Access Points > Cisco Aironet Access Point Software Configuration Guide > Maintaining Firmware > Updating Firmware

**Note**

Disable User Manager protection on your Access Point before upgrading from version 10.12 to 11.x. User Manager passwords created in version 10.12 are scrambled during the upgrade, and you need to recreate them in version 11.x. Passwords created in versions 10.13 or later are not affected.

**Note**

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

Limitations and Restrictions

MIB File Compatible with Firmware Version 11.0x

The Aironet Access Point MIB file (AWCVX-MIB) is supported by Access Point firmware versions 11.00 and later. Earlier versions of firmware do not support this MIB.

Aironet Extensions Required in Repeater Mode

You must enable Aironet extensions on the AP Radio Advanced page when you set up the Access Point as a repeater. If you disable Aironet extensions when in repeater mode, connect a serial cable to the Access Point and enable Aironet extensions with the console interface.

Caveats

Getting Bug Information on Cisco.com

If you are a Cisco registered 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 today at <http://www.cisco.com/support/bugtools/>.

Resolved Caveats

The following caveats have been resolved in firmware version 11.03:

- 350 series Access Points sometimes lock up when they are set to use long headers and antenna diversity and are associated to 350 series client devices using long headers.

The 340 series does not have this problem, so upgrades to 11.03 do not add any features or benefits for 340 series Access Points.

Open Caveats

The following caveats have not been resolved for firmware version 11.03:

- Difficult to end Telnet session (CSCav00156).

When you finish running a Telnet session to the Access Point you must close the Telnet window to end the session.

- Network response times might be slow on networks with thousands of client devices (CSCdr95686).

On large, flat networks with thousands of client devices, the Access Point might respond slowly to network traffic. Segmenting the network into subnets can improve Access Point performance.

- Must restart unit twice to enable standby mode (CSCds36123).

When you set up an Access Point as a standby unit, follow the instructions on page 7-5 in the *Cisco Aironet Access Point Software Configuration Guide*. When you complete the instruction steps, return to the Hot Standby page and click **Start Hot Standby Mode** again. When the unit restarts it is in standby mode.
- Corrupt characters sometimes appear in client names in the Association Table (CSCds56664).

Corrupt characters sometimes appear in the names of clients listed in the Access Point's Association Table.
- Access Point does not support client devices using LEAP with WEP keys of different lengths (CSCds61358).

The length of the transmit WEP key set on the Access Point determines the length of the session keys used by LEAP clients. For example, if the transmit key on the Access Point is a 128-bit key, all LEAP clients associated to the Access Point must use 128-bit WEP keys.
- Inoperable link in console and Telnet interfaces (CSCds71375 and CSCds71448).

In the console and Telnet (CLI) interfaces the link to the FTP Server Setup page is inoperable on the Update All Firmware From File Server and Selectively Update Firmware From File Server pages.
- No address filtering pages in console and Telnet interfaces (CSCdt02327).

You cannot set up MAC address filters through the console and Telnet interfaces. Use the browser interface to create and enable MAC address filters.
- User management passwords corrupted when updating firmware from version 10.12 to 11.0x (CSCdt07632).

When upgrading Access Point firmware from version 10.12 to 11.0x with user information in the user manager database, the user passwords are corrupted during the upgrade. This problem also occurs if the users are added to the user manager database in version 10.12, the firmware is upgraded to version 10.13, and then upgraded to version 11.0x. If the users and passwords are created in version 10.13, the passwords are not corrupted during the upgrade. To avoid being locked out of the Access Point, disable the user manager before upgrading from version 10.12 to 11.0x. After the upgrade, re-enter the user passwords and enable user manager.
- Broken help links on Access Point and Bridge CD (CSCdt12716).

If you change the default help root URL on a 350 series Access Point's Web Server Setup page to use the help files on the Cisco Aironet Access Point and Bridge CD, the help buttons on the AP Radio Port, AP Radio Advanced, AP Radio Hardware, and AP Radio Identification pages will not work. To use the most up-to-date online help, leave the default help root URL at its default setting.
- Successful firmware distribution reports error (CSCdt31501).

When distributing firmware to an Access Point running firmware version 11.01 or later, the distribute status on the distributing Access Point reports an error even when the distribution is successful. To verify that the distribution was successful, browse to the Access Point to which you sent the firmware and check that the firmware has been loaded.
- Repeater 340 series Access Points using 128-bit WEP do not pass client traffic (CSCdt15869).

Client devices can associate to 340 series Access Points set up as repeaters but cannot communicate when WEP is enabled.
- SNMP sysObjectID is identical for both 340 and 350 series Access Points (CSCdt21451).

Because both 340 and 350 series Access Points have the same SNMP sysObjectID, the devices are both perceived as 340 series Access Points by a network management platform such as HP OpenView.

- Client devices sometimes remain associated to disabled Access Point instead of switching to standby Access Point (CSCdt44184).

When the primary Access Point loses Ethernet connectivity, the standby Access Point tells the primary Access Point to shut off its radio so that clients associated to it will associate with the standby Access Point instead. However, sometimes the primary Access Point does not shut off its radio and does not disassociate its clients. Workaround: Power cycle both APs and set up Hot Standby again.

- Unauthorized reset of Access Point possible through Telnet (CSCdt47758).

Unauthorized users can reset the Access Point by opening a Telnet session and pressing **Ctrl-x** even when the Access Point's User Manager is enabled.

Troubleshooting

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

Related Documentation

Use the following documents in conjunction with this document.

- *Quick Start Guide: Cisco Aironet Access Points*
- *Cisco Aironet Access Point Hardware Installation Guide*
- *Cisco Aironet Access Point Software Configuration Guide*

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. 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 as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered 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 corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. You can also e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Software Configuration Tips on the Cisco TAC Home Page

Visit these Cisco TAC pages for more information on upgrading software. These pages require you to log in as a Cisco registered user.

Aironet Product	Path from www.cisco.com	Hyperlink
Cisco Aironet 340 Access Points	Cisco > Service & Support > Technical Assistance Center > Products > Cisco Aironet 340 Access Points	Go to TAC web page
Cisco Aironet 340 Client Adapter	Cisco > Service & Support > Technical Assistance Center > Products > Cisco Aironet 340 Client Adapters	Go to TAC web page
Cisco Aironet Ethernet Bridges	Cisco > Service & Support > Technical Assistance Center > Products > Cisco Aironet 340 Ethernet Bridges	Go to TAC web page

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

AccessPath, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Discover All That's Possible, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Voice LAN, Wavelength Router, WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site 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. (0101R)

Copyright © 2001, Cisco Systems, Inc.
All rights reserved.