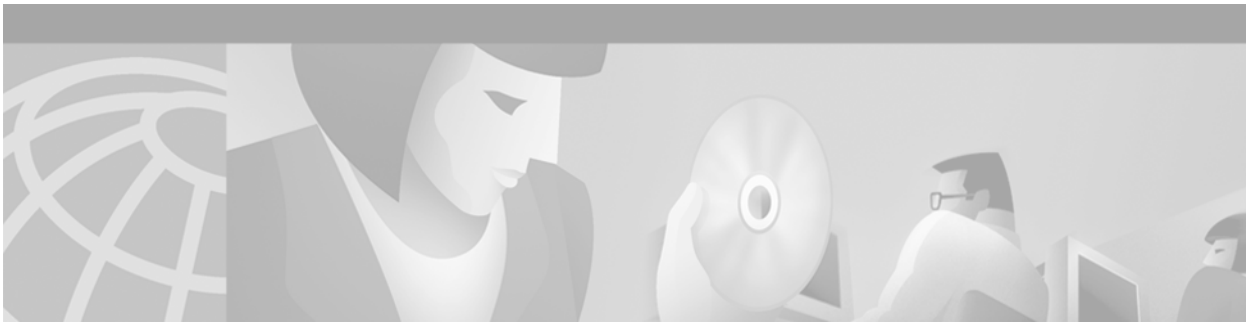

Release Notes for Cisco Aironet 340 and 350 Series Access Points Running Firmware Release 11.06a

Contents

Introduction

This document describes requirements, installation procedures, and caveats for Cisco Aironet access point firmware version 11.06a. This release resolves caveats CSCdw63011 and CSCdw63031.

CISCO SYSTEMS

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

System Requirements

You must have a Cisco Aironet 340 or 350 Series Access Point to install firmware version 11.06a.

Version Supported

Your access point must be running firmware version 10.x or later to install firmware version 11.06a.

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 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 link to the product, document and chapter:

   http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350ch5.htm

3. Follow this link to the Software Center on Cisco.com and download firmware version 11.06a:

   http://www.cisco.com/pcgi-bin/tablebuild.pl/aironet-350

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 of the *Cisco Aironet Access Point Software Configuration Guide* for more information.

Limitations and Restrictions

MIB File Compatible with Firmware Version 11.0x

The 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.

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, then 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
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 or later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later[1]	—	x	x
BR352 11.06 and later[1]	—	x	x

1. The default draft setting in access point and bridge firmware version 11.06 and later is Draft 10.

Note Draft standard 8 is the default setting in firmware version 11.05 and earlier, and it might remain in effect when you upgrade the firmware to version 11.06 or later. Check the setting on the Authenticator Configuration page in the management system to make sure the best draft standard for your network is selected.

Use the Authenticator Configuration page in access point firmware version 11.06a to select the draft of the 802.1x protocol the access point's radio 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's 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 in access point firmware versions 11.06 and later. 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.

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

Caveats

Resolved Caveats

The following caveats have been resolved in firmware version 11.06a:

- Resolved: CSCdw63011. An error can occur with management protocol processing. Please use this URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw63011

- Resolved: CSCdw63031. An error can occur with management protocol processing. Please use this URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw63031

The following caveats were resolved in firmware version 11.06 and are also resolved in version 11.06a:

- Resolved: 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 or bridge reports an error even when the distribution is successful.
- Resolved: Must restart unit twice to enable standby mode (CSCds36123).
- Resolved: Hot Standby feature does not function on 350 series access points (CSCdt44021).

- Resolved: 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.
- Resolved: Settings entered on the FTP Server Setup page are ignored when entered using the CLI (CSCds71448).
- Resolved: Access point or bridge reboots when you enter a fifth MAC address in the list of filtered MAC addresses using the CLI (CSCdt71588).

Open Caveats

The following caveats have not been resolved for firmware version 11.06a:

- Protocol filter settings sometimes revert to defaults during filter setup (CSCdu02040).

  When you add a new protocol filter set, you can set the filter's default disposition and time to live on the first filter configuration page. You add specific protocols to the filter set on subsequent pages. If you change the default disposition or default time to live values from the defaults, these values revert to default settings after you add specific protocols to complete the filter setup. Make sure the default disposition and time-to-live values are correct before you apply the filter set.

- IP Port filters do not block pings (CSCdu05324).

  Table B-3 in Appendix B of the *Cisco Aironet Access Point Software Configuration Guide* lists PING as the additional identifier for the echo IP Port filter entry. However, the echo entry does not block standard pings. To block standard pings, set up an IP Protocol filter to block ICMP.

- Access points lock up during firmware upgrade through Internet Explorer 2.0 (CSCdu05787).

  When you load new firmware into an access point using Microsoft Internet Explorer version 2.0, the access point stops functioning and must be rebooted. The access point management system is fully compatible with Microsoft Internet Explorer versions 4.0 or later and Netscape Communicator versions 4.0 or later. Earlier versions of these browsers cannot use all features of the management system.

- Cannot access workgroup bridges associated with access point (CSCdu10993).

  When a workgroup bridge (WGB34x or WGB352) is associated to an access point, you cannot access the WGB console menus or ping the WGB from a station on the wired LAN connected to the access point's Ethernet port. However, you can access the WGB from any client device connected to the WGB's Ethernet port and from any client device associated to the access point that is associated to the WGB. Radio traffic between the access point and the WGB is not affected.

- Access points ignore vendor specific options from DHCP servers (CSCdu19500).

  Access points ignore the vendor specific option (VSO) sent from DHCP servers inresponse to the access point's vendor class identifier, also called a DHCP identifier in the web browser interface and CLI.

- SNMP community name must include extra privelege to access all information (CSCdt31925).

  SNMP community names entered on the Express Setup page have limited access to the access point's configuration information. To provide full access to the SNMP community you specify on the Express Setup page, use the User Manager pages to assign firmware privelege to the community name. Refer to the "Setting Up Administrator Authorization" section of the *Cisco Aironet Access Point Software Configuration Guide* for complete instructions on using the User Manager.

- Filters can be disabled but not edited from the command-line interface (CSCdt34104).

  You cannot edit MAC address filters with the command-line interface. However, you can use the CLI's Ethernet Protocol Filters and Root Radio Protocol Filters pages to disable filters.

- Daylight Savings Time option displays time one hour behind (CSCdr55634).

  When the Use Daylight Savings Time setting on the Time Server Setup page in the configuration management system is enabled, the access point's time display is behind by one hour during Daylight Savings Time. Workaround: Choose a time zone from the GMT Offset pull-down menu that is one hour ahead of your current location. For example, if you would normally select GMT -5:00, select GMT -4:00 instead.

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 at http://www.cisco.com/support/bugtools/.

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.

Documentation Updates

This section describes errors, omissions, and changes in user documentation for Cisco Aironet Access Points.

Changes

The description of Admin capability in the access point's User Manager security feature that appears in the *Cisco Aironet Access Point Software Configuration Guide* now accurately describes the permission granted to a user with Admin capability:

- Admin—The user can view most system screens. To allow the user to view all system screens and make changes to the system, select Write capability.

Consult the "Setting Up Administrator Authorization" section of the *Cisco Aironet Access Point Software Configuration Guide* for more information on the User Manager feature.

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 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.

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.

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