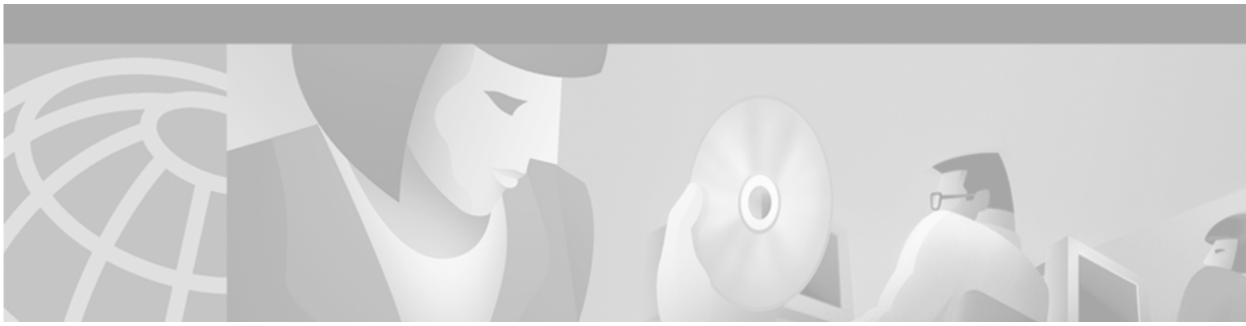

Release Notes for Cisco Aironet Mini PCI Client Adapter Firmware, Version 5.00.01

Contents

This document contains the following sections:

Introduction

This document describes system requirements, upgrade procedures, new features, and caveats for Cisco Aironet mini PCI client adapter firmware release 5.00.01.

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

System Requirements

You will need the following in order to install and use firmware version 5.00.01:

- A Cisco Aironet 350 series mini PCI card (MPI350)
- A computer running Windows 95, 98, NT, 2000, Me, or XP
- Windows Aironet Client Utility (ACU) version 5.01.001 or greater and Windows mini PCI card driver version 2.22 or greater

Note Mini PCI cards use different drivers and firmware than PC, LM, and PCI cards.

- To benefit from the latest security features, access point firmware version 11.10T or greater

Network-EAP Authentication Requires Matching 802.1X Protocol Drafts

In order to use Network-EAP authentication on your wireless network, your client devices and infrastructure devices (access points and bridges) must use the same 802.1X protocol draft. Mini PCI card firmware version 5.00.01 supports draft 10 of the 802.1X protocol standard. Therefore, if client devices use this version of firmware, an access point or bridge to which they associate must also be configured to use draft 10. The table below lists firmware versions for Cisco Aironet products and the drafts with which they comply.

Firmware Version	Draft 8	Draft 10[1]
Mini PCI card (MPI350)		
4.95.08 and later	—	x
Other client adapters (PCM34x/35x, LMC34x/35x, and PCI34x/35x)		
4.13	x	—
4.16	x	—
4.23	x	—
4.25 and later	—	x
Workgroup bridges (WGB34x/352)		
8.58	x	—
8.61 and later	—	x
Access points (AP34x/35x)		
11.05 and earlier	x	—
11.06 and later[2]	x	x
Bridges (BR352)		
11.06 and later[2]	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 and bridge firmware version 11.06 and later is draft 10.

If your client and infrastructure devices do not have matching 802.1X protocol drafts, upgrade the firmware in these devices to versions with the same draft number. However, if your access points or bridges are using firmware version 11.06 or later, you can use their Authenticator Configuration page to select the draft of the 802.1X protocol that they should use. To set the draft for your access points or bridges, follow the instructions in the *Release Notes for Cisco Aironet Access Points* for firmware version 11.06 or greater. You can access these Release Notes at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350rn/index.htm

Upgrading to a New Firmware Release

This section describes how to upgrade to mini PCI card firmware version 5.00.01.

Determining the Firmware Version

To determine the firmware version that your mini PCI card is currently using, open ACU. Then click the **Status** icon or select **Status** from the Commands drop-down menu. The firmware version is displayed in the Status screen.

Upgrade Procedure

To upgrade your mini PCI card's firmware to the 5.00.01 release, follow the steps below.

Step 1 Use your computer's web browser to access the following URL: http://www.cisco.com/public/sw-center/sw-wireless.shtml

Step 2 Locate the section for client adapter firmware.

Step 3 Click the link for your client adapter's series (for example, 350 series).

Step 4 Click the latest radio firmware file for mini PCI cards.

Note If your wireless network uses LEAP authentication, remember to select a radio firmware file of the same draft standard as the access points to which your client adapter will be authenticating.

Note If your wireless network uses EAP-TLS or EAP-MD5 authentication, you must select draft 10 of the radio firmware.

Step 5 Read and accept the terms and conditions of the Software License Agreement.

Step 6 Select the firmware file to download it.

Step 7 Save the file to a floppy disk or to your computer's hard drive.

Step 8 Locate the file on your floppy disk or on your computer's hard drive and use an unzip program to extract the image file to a folder.

Step 9 Open ACU; then click the **Load Firmware** icon or select **Load New Firmware** from the Commands drop-down menu.

Step 10 Find the location of the new firmware in the Open Window's Look in box. The default location is *InstallPath*\Firmware, where *InstallPath* is the directory that ACU was installed in.

Step 11 Click the firmware image file (*.img) so that it appears in the File name box at the bottom of the Open window.

Step 12 Click the **Open** button. A progress bar displays while the selected image is loaded into the mini PCI card's Flash memory.

Step 13 Click **OK** when the "Firmware Upgrade Complete!" message appears. The OK button cannot be selected until the process is complete or an error occurs.

New Features

This section describes new features for mini PCI card firmware release 5.00.01.

Support for Enhanced Security

Mini PCI card firmware release 5.00.01 supports two new security features designed to prevent sophisticated attacks on your wireless network's Wired Equivalent Privacy (WEP) keys. These features do not need to be enabled on the client adapter; they are supported automatically in the firmware version listed above. However, they must be enabled on the access point. Access point firmware version 11.10T or greater is required to enable these security features. Refer to the *Cisco Aironet Access Point Software Configuration Guide* for instructions on enabling these security features on the access point.

- Temporal Key Integrity Protocol (TKIP) – This feature, also referred to as *WEP key hashin*g, defends against an attack on WEP in which the intruder uses an unencrypted segment, called the *initialization vector (IV),* in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. TKIP protects both unicast and broadcast WEP keys.

  Note If you enable TKIP on the access point, your client adapter's firmware must support TKIP; otherwise, the client cannot associate.

  Note When you enable TKIP, you do not need to enable broadcast key rotation. TKIP prevents intruders from calculating the static broadcast key, so you do not need to rotate the broadcast key.

- Broadcast key rotation – EAP authentication provides dynamic unicast WEP keys for client devices but uses static broadcast, or multicast, keys. When you enable broadcast WEP key rotation, the access point provides a dynamic broadcast WEP key and changes it at the interval you select.

  Note When you enable broadcast key rotation on the access point, only wireless client devices using LEAP or EAP-TLS authentication can associate to the access point. Client devices using static WEP (with open, shared key, or EAP-MD5 authentication) cannot associate.

Open Caveats

This section describes known problems for mini PCI card firmware version 5.00.01.

Mini PCI Card Does Not Recover from Standby in Max PSP Mode

On Windows Me, the mini PCI card does not reassociate when recovering from standby if the power-saving mode is set to Max PSP (CSCdv89345).

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 to identify existing bugs (or caveats) in Cisco software products.

Access the TAC Software Bug Toolkit today at the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Troubleshooting

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

Related Documentation

For more information about 350 series client adapters, refer to the *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows*.

Obtaining Documentation

The following 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 the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package shipped separately from the Cisco Aironet Wireless LAN Client Adapters CD that shipped 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.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 corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click the **Fax** or **Email** option under the “Leave Feedback” at the bottom of the Cisco Documentation home page.

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:

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 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 to

- 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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

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

Inquiries to Cisco TAC 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.

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

Cisco TAC Web Site

The Cisco TAC Web Site allows you 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 the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services 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 the following URL to register:

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

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

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; 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 will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following 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). In addition, 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.