



Cisco Aironet Configuration Administration Tool (ACAT) 1.6 Administrator Guide for Windows

May 2005

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-3570-05



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0502R)

Cisco Aironet Configuration Administration Tool (ACAT) 1.6 Administrator Guide for Windows
© 2005 Cisco Systems, Inc. All rights reserved.



Preface vii

Audience	viii
Purpose	viii
Organization	viii
Conventions	viii
Related Publications	ix
Obtaining Documentation	ix
Cisco.com	ix
Documentation DVD	ix
Ordering Documentation	x
Documentation Feedback	x
Cisco Product Security Overview	x
Reporting Security Problems in Cisco Products	xi
Obtaining Technical Assistance	xi
Cisco Technical Support Website	xii
Submitting a Service Request	xii
Definitions of Service Request Severity	xiii
Obtaining Additional Publications and Information	xiii

CHAPTER 1

Overview 1-1

Introduction to ACAT	1-2
Obtaining ACAT Software	1-3
Activating ACAT	1-4
ACAT Configuration Tabs	1-5
File Menu	1-5
Help	1-5
Configuration File	1-6
Security Considerations	1-6
General Recommendations	1-6
Obtaining and Installing Client Adapter Software	1-7
Removing ACAT Software	1-7
Uninstalling Client Adapter Software	1-7

CHAPTER 2

Installed Components Tab 2-1

- Installed Components Tab Window 2-2
- Firmware 2-3
- Drivers 2-3
- ACU 2-4
- ACM 2-5
- Security Modules 2-7

CHAPTER 3

Global Override Settings Tab 3-1

- Overview 3-2
- Global Override Options 3-3

CHAPTER 4

Profile Settings Tab 4-1

- Adding Profiles 4-2
 - General Recommendations 4-2
 - Create/Manage Profile 4-2
 - Load From Registry 4-4
- Editing Profiles Using the Profile Settings Tab 4-4
 - Card Type 4-5
 - Profile 4-5
 - Connection Tab 4-6
 - Security Tab 4-10
 - Network Authentication 4-11
 - Data Encryption 4-13
 - Allow Association To Mixed Cells Parameter 4-14
 - Access Point Authentication 4-14
 - Entering a New Static WEP Key 4-15
 - Disabling Static WEP 4-16
 - Enabling LEAP 4-17
 - Enabling EAP-FAST 4-20
 - Enabling Host-Based EAP 4-24
 - RF Settings Tab 4-26
 - Infrastructure Tab 4-32
 - Ad Hoc Tab 4-35
 - Admin Override Tab 4-37
 - Auto Profile Selection 4-38
 - Profiles Tab 4-39

CHAPTER 5**Security Features 5-1**

Overview 5-2

Static WEP Keys 5-2

EAP (with Static or Dynamic WEP Keys) 5-3

Wi-Fi Protected Access (WPA) 5-6

Fast Roaming (CCKM) 5-7

Reporting Access Points that Fail LEAP or EAP-FAST Authentication 5-8

Additional WEP Key Security Features 5-8

Message Integrity Check (MIC) 5-8

Temporal Key Integrity Protocol (TKIP) 5-9

Broadcast Key Rotation 5-9

Synchronizing Security Features 5-9

APPENDIX A**Install Wizard Command Line Options A-1**

Command Line Options A-2

Sample Application A-3

GLOSSARY

INDEX



Preface

This section provides an overview of the *Cisco Aironet Configuration Administration Tool (ACAT) 1.6 Administrator Guide for Windows*, references related publications, and explains how to obtain other documentation and technical assistance.

The following topics are covered in this section:

- [Audience, page viii](#)
- [Organization, page viii](#)
- [Conventions, page viii](#)
- [Related Publications, page ix](#)
- [Obtaining Documentation, page ix](#)
- [Documentation Feedback, page x](#)
- [Cisco Product Security Overview, page x](#)
- [Obtaining Technical Assistance, page xi](#)
- [Obtaining Additional Publications and Information, page xiii](#)

Audience

This publication is for the administrator responsible for installing and configuring Cisco Aironet Wireless LAN Adapters (referred to as *client adapters*) and the Cisco Aironet Client Utility (ACU) in multiple PCs. The installer should be familiar with computing devices and with network structures, terms, and concepts.

Purpose

This publication describes the Cisco Aironet Configuration Administration Tool (hereafter referred to as *ACAT*) and provides instructions for installing it, configuring administrative overrides, and creating or importing profiles for the client adapter on PCs running a Windows operating system.



Note

This version of ACAT is compatible with Install Wizard 1.6.

Organization

This guide contains the following sections:

[Chapter 1, “Overview,”](#) provides an overview of the ACAT utility, describes how to obtain and activate the utility, and describes how to use the ACAT configuration file.

[Chapter 2, “Installed Components Tab,”](#) describes how to select the software components to be installed by the Cisco Aironet Client Adapter Installation Wizard (hereafter referred to as the *Install Wizard*).

[Chapter 3, “Global Override Settings Tab,”](#) describes the administrative override parameters that apply to all profiles being installed by the Install Wizard.

[Chapter 4, “Profile Settings Tab,”](#) describes the profile parameters supported by the ACAT utility.

[Chapter 5, “Security Features,”](#) provides an overview of the security features for the wireless LAN.

[Appendix A, “Install Wizard Command Line Options,”](#) describes the administrator command line options for Install Wizard 1.6.

The Glossary provides definitions for common wireless networking terms.

Conventions

This publication uses the following conventions to convey instructions and information:

- Commands and keywords are in **boldface** type.



Note

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Publications

For more information about wireless LAN adapters and related products, refer to the following publications:

- *Cisco Aironet 350 and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows*. provides instructions for using the Install Wizard to install and configure the wireless client adapter, the firmware, the driver, and the utilities.
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* provides software configuration information for access points running Cisco IOS software.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

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

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>



Overview

This chapter provides an overview of the Cisco Aironet Configuration Administration Tool (ACAT) for Windows utility used by administrators to create a configuration file to control the installation of the utilities, driver, firmware, and profiles for client adapters on PCs running a Windows operating system and using Cisco Aironet 2.4-GHz and 5-GHz client adapters.

The following topics are covered in this chapter:

- [Introduction to ACAT, page 1-2](#)
- [Obtaining ACAT Software, page 1-3](#)
- [Activating ACAT, page 1-4](#)
- [Obtaining and Installing Client Adapter Software, page 1-7](#)
- [Removing ACAT Software, page 1-7](#)
- [Uninstalling Client Adapter Software, page 1-7](#)

Introduction to ACAT

ACAT is a tool used by administrators to specify software installation options for client adapters in PCs running a Windows operating system. The specified options are placed in a configuration file used by the Cisco Aironet Wireless LAN Client Adapter Installation Wizard (hereafter referred to as the *Install Wizard*) to install the software components and a client adapter's configuration profiles.

**Note**

ACAT 1.6 supports only the Windows 2000 and XP operating systems.

Using ACAT, an administrator can specify the following installation options:

- Software components
 - Client adapter radio firmware
 - Driver for a client adapter
 - Cisco Aironet Client Utility (ACU)
 - Cisco Aironet Client Monitor (ACM)
 - Security Modules (LEAP, EAP-SIM, PEAP, and EAP-FAST)
- Administrator global override settings
- Client adapter configuration profiles
- Client adapter type
 - PCM-35x—Cisco Aironet 350 series PCMCIA card
 - MPI-35x—Cisco Aironet 350 series Mini-PCI card
 - PCI-35x—Cisco Aironet 350 series PCI card
 - CB20A—Cisco Aironet 5-GHz PC-Cardbus card

**Note**

ACAT 1.6 is compatible only with Install Wizard 1.6.

**Note**

ACAT 1.6 does not support the Cisco Aironet 340 and 4800 series client adapters or the Cisco Aironet IEEE 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG).

Obtaining ACAT Software

To obtain the latest ACAT software from the Cisco website, follow these steps:

-
- Step 1** Use your web browser to go to the Cisco Software Center at the following URL:
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
- Step 2** Choose **Option #2: Aironet Wireless Software Display Tables**.
- Step 3** Choose **Cisco Aironet Wireless LAN Client Adapters**.
- Step 4** Under Windows System Administration Tool, Choose **Aironet Configuration Administration Tool (ACAT)**.
- Step 5** Choose the ACAT file (**ACAT-v16.exe**) with the greatest version number, where *v16* is the version number.
- Step 6** Enter the requested information on the encryption authorization form and click **Submit**.
- Step 7** Read the terms and conditions of the Software License Agreement and click **Accept**.
- Step 8** Double-click the ACAT file to download it.
- Step 9** Save the file to your computer's hard drive then exit the web browser.
- Step 10** Find the downloaded ACAT-v16.exe file using Windows Explorer, double-click it, and extract the files into the same directory on your hard drive as the Install Wizard 1.6. The following files are extracted:
- ACAT.exe—ACAT executable file.
 - ACAT.HLP—ACAT help file used by the ACAT program.



Note If you do not place the ACAT files into the same directory as the Install Wizard 1.6, you must place a copy of the InstallData.txt file into your ACAT directory. The InstallData.txt file can be found in the Install Wizard directory.



Note InstallData.txt is an ASCII text installation file used by the ACAT program that cannot be edited. The file data is check-sum protected and if modified generates an error when ACAT is activated.

Activating ACAT

Follow the steps below to activate the ACAT program:

- Step 1** Click **Start > Run**.
- Step 2** Browse to the location of the extracted software, choose **ACAT.exe**, click **Open**, and click **OK**.

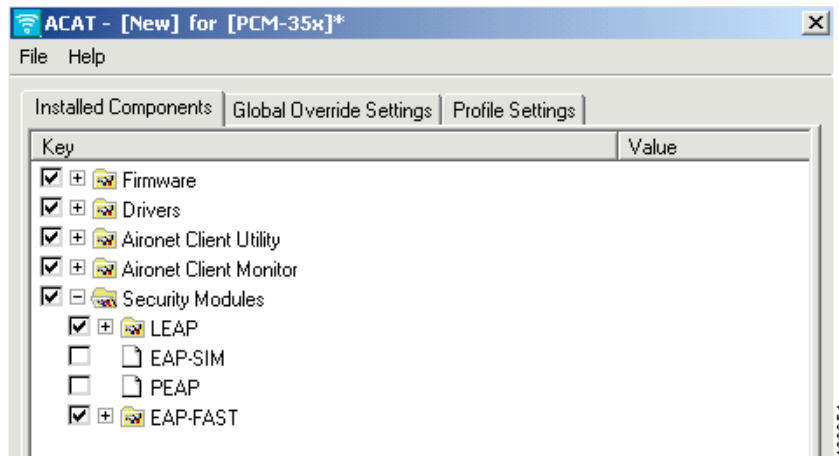


Note If the InstallData.txt file is not in the same folder as ACAT, an error message appears indicating that ACAT cannot find the InstallData.txt file. You must place a copy of the InstallData.txt file (located in the Install Wizard 1.6 directory) into the ACAT directory or place the ACAT (ACAT.EXE and ACAT.HLP) files into the Install Wizard directory.

When ACAT activates, a graphical user interface appears (see [Figure 1-1](#)) that allows the administrator to easily select and specify installation options. Typically, the administrator selects a client adapter type, software component installation options, global override options, and then creates client adapter profiles. To simplify the process, ACAT uses three major tabs and a drop-down menu.

The ACAT main window is shown in [Figure 1-1](#).

Figure 1-1 ACAT Main Window



ACAT Configuration Tabs

The main ACAT window provides three configuration tabs (see [Figure 1-1](#)):

- **Installed Components**—Allows you to specify the software components to be installed by the Install Wizard.
- **Global Override Settings**—Allows you to specify how to handle existing profiles and to enable or disable a user's ability to change the installed profiles using the ACU. These settings also allow you to specify that the Install Wizard uses a silent install without user interaction.
- **Profile Settings**—Allows you to specify configuration parameters for profiles to be installed by the Install Wizard.

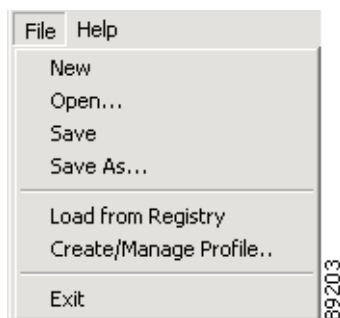
File Menu

The ACAT File menu provides the following selections (see [Figure 1-2](#)):

- **New**—Opens a new ACAT configuration file for a specified client adapter.
- **Open**—Locates and opens an existing ACAT configuration file.
- **Save**—Saves the ACAT configuration file to the ACAT directory and continues.
- **Save as**—Saves the ACAT configuration file to a desired location and continues.
- **Load from Registry**—Imports existing profiles from the Windows registry.
- **Create/Manage Profile**—Adds, deletes, or renames new profile names.
- **Exit**—Closes and exits the ACAT program.

The ACAT File menu is shown in [Figure 1-2](#).

Figure 1-2 ACAT File Menu



Help

The ACAT Help menu option provides the following selections:

- **Contents**—Provides help information on ACAT options and settings.
- **About**—Provides the ACAT version number.

Configuration File

ACAT creates a configuration file, *CiscoAdminConfig.dat*, using the specified installation options for a selected client adapter type. To operate, the ACAT configuration file must be in the Install Wizard folder. When you activate the Install Wizard by clicking **IWSetup.exe** in the Install Wizard folder, the Install Wizard program uses the ACAT configuration file to specify the installation options for a specific client adapter type.

**Note**

The ACAT configuration file uses the same filename as the Install Wizard configuration file. Prior to saving or placing the ACAT generated configuration file in the Install Wizard folder, you may want to copy the Install Wizard's original configuration file (*CiscoAdminConfig.dat*) into a backup folder for possible future use.

**Note**

Multiple invocations of the Install Wizard are required to configure multiple client adapter types.

Security Considerations

The ACAT configuration file is encrypted to protect sensitive security data such as SSID, WEP keys, and network security settings. Also, the client adapter profiles created by ACAT can be configured to support static WEP, LEAP, EAP-SIM, PEAP, or EAP-FAST network security options.

General Recommendations

When you need to install profiles for multiple client adapter types, you should consider the following recommendations:

- On a server accessible to all users, create and name a directory for each client adapter type.
- Place a copy of all the Install Wizard files and sub-directories into each of the client adapter directories.
- Create an ACAT configuration file with the needed profiles for each client adapter type. Save each ACAT configuration file into the appropriate client adapter directory with the Install Wizard files.

**Note**

All ACAT configuration files use the same filename (*CiscoAdminConfig.dat*) and therefore must be saved separately.

- To install profiles for a specific client adapter type, each user must execute the Install Wizard (**IWSetup.exe**) in the appropriate client adapter directory for their client adapter type.

Obtaining and Installing Client Adapter Software

The client adapter software (drivers, firmware, utilities, and the Install Wizard) are not part of the ACAT software package and must be obtained separately. Refer to the *Cisco Aironet 350 and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows* for instructions on obtaining and using the Install Wizard.

**Note**

This version of ACAT is compatible only with Install Wizard 1.6.

**Note**

The Install Wizard is automatically activated when you uncompress the Install Wizard software package. Click **Cancel** if you want only to uncompress the software and do not want to install the client adapter drivers, firmware, and utilities on your PC.

Removing ACAT Software

You can remove the ACAT software from your PC by deleting the following files:

- ACAT.exe
- ACAT.HLP
- ACAT.GID
- InstallData.txt (if not located in the Install Wizard directory)
- CiscoAdminConfig.dat (if not located in the Install Wizard directory)

Uninstalling Client Adapter Software

When you run the Install Wizard using an ACAT generated configuration file set for a silent install, the main Install Wizard window is not displayed. To uninstall the software components and profiles installed by the Install Wizard, follow these steps:

- Step 1** Click **Start > Settings > Control Panel > Add/Remove Programs**.
- Step 2** Choose **Cisco Aironet Installation Wizard**.
- Step 3** Click **Change/Remove**.
- Step 4** When the Install Wizard window appears, choose **Uninstall All Components** and click **Next**.

**Note**

Uninstall All Components removes all installed software components and all client adapter profiles in the PC registry.

**Note**

The Custom Installation/Upgrade selection on the Install Wizard window enables you to change the installation parameters and software components specified in the ACAT configuration file.

Step 5 The Install Wizard window indicates the uninstall progress. When a message appears that indicates the system is about to reboot, click **OK**.

When your PC reboots, the uninstall is complete.



Note If you uncompressed the Installation Wizard software package in a non-temporary folder, you must manually delete the Install Wizard installation files and directories.



Installed Components Tab

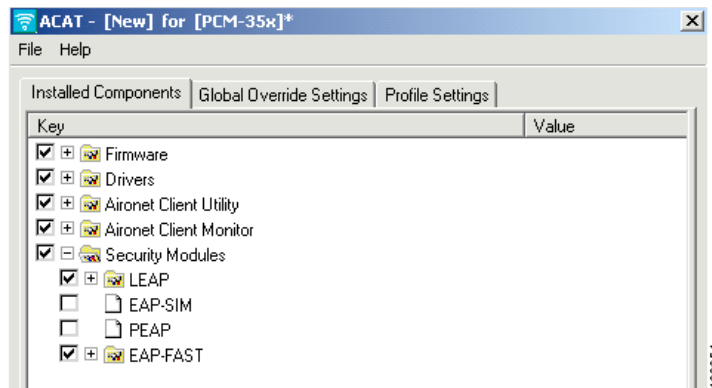
This chapter describes the Installed Components tab options. The following topics are covered in this section:

- [Installed Components Tab Window, page 2-2](#)
- [Firmware, page 2-3](#)
- [Drivers, page 2-3](#)
- [ACU, page 2-4](#)
- [ACM, page 2-5](#)
- [Security Modules, page 2-7](#)

Installed Components Tab Window

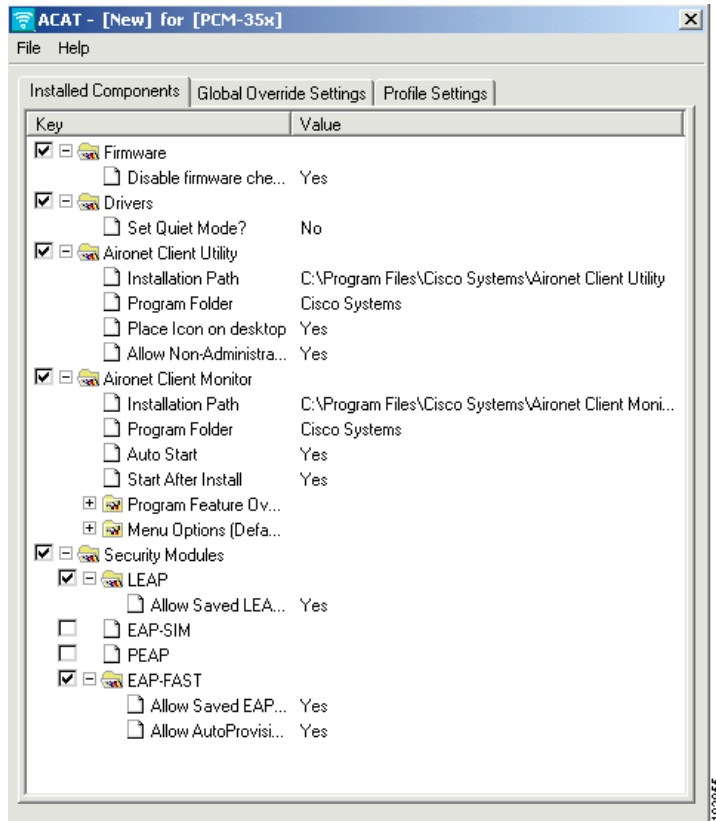
The Installed Components tab enables you to select the software components to be installed by the Install Wizard. All software components are bundled in the Install Wizard software package. [Figure 2-1](#) shows software components on the Installed Components tab.

Figure 2-1 *Installed Components Tab Window*



To view software component installation parameters, you must expand the selection by clicking the plus/minus box next to the component (see [Figure 2-2](#)).

Figure 2-2 *Software Component Installation Parameters*



The software component check box specifies whether or not the component is installed by the Install Wizard. A check indicates that the component is installed. Check the check box to change the selection.

**Note**

Some components cannot be installed separately. Therefore, when you select or deselect these components, the settings of other components may change. A Dependency Notice window appears when you select or deselect components that cannot be installed separately.

To view the entire component parameter line, use the scroll bar on the bottom of the window or resize the component and value fields.

To change the value of a component parameter, click the parameter value, such as *No*. An option value window appears that enables you to change the value using a drop-down menu. Click **OK** when you have completed your selection.

Firmware

The client adapter uses the installed firmware to control the radio. [Table 2-1](#) describes the firmware component installation parameters.

Table 2-1 *Firmware Parameters*

Parameter	Description
Disable firmware checking	Determines whether the currently installed firmware version is checked during the installation process. When the <i>yes</i> option is selected, firmware checking is disabled to prevent the overwriting of the currently installed firmware. When the <i>no</i> option is selected, the firmware version that is bundled with the Install Wizard is installed. Options: Yes or No Default: Yes

Drivers

The client adapter requires a specific driver that interfaces with the operating system and supports the radio firmware functionality. [Table 2-2](#) describes the driver installation parameter.

Table 2-2 *Driver Parameter*

Parameter	Description
Set Quiet Mode	Determines whether the client adapter automatically attempts to locate an available access point by transmitting beacon messages or transmits only in response to access point transmissions. Options: Yes or No Default: No

ACU

The ACU enables you to configure and change client adapter profile parameters. [Table 2-3](#) describes the ACU installation parameters.

Table 2-3 ACU Parameters

Parameter	Description
Installation Path	Determines the path in which the ACU software is installed. You can change the default by entering a new path. Default: C:\Program Files\Cisco Systems\Aironet Client Utility
Program Folder	Determines the program folder in which the ACU software is installed. You can change the default by entering a new folder name. Default: Cisco Systems
Place Icon on Desktop	Determines whether the ACU icon is placed on your computer's desktop to provide quick access to the utility. Options: Yes or No Default: Yes
Allow Non-Administrator Users to Save Settings to the Registry	Enables users without administrative rights to modify profiles in ACU and save them to the registry on computers running Windows 2000 or XP operating systems. Options: Yes or No Default: Yes Note To avoid conflicting settings, check the setting for Allow Non-Admin to Modify Profiles on the Global Override Settings tab.

ACM

The ACM operates as an icon in the Window's system tray to quickly monitor and control the client adapter's connection. [Table 2-4](#) describes the ACM parameters.

Table 2-4 ACM Parameters

Parameter	Description
Installation Path	Determines the path in which the ACM software is installed. You can change the default by entering a new path. Default: C:\Program Files\Cisco Systems\Aironet Client Monitor
Program Folder	Determines the program folder where the ACM software is installed. You can change the default by entering a new folder name. Default: Cisco Systems
Auto Start	Determines whether ACM starts automatically after Windows boots. Options: Yes or No Default: Yes
Start After Install	Determines whether ACM starts automatically after this application is installed. Options: Yes or No Default: Yes

Table 2-4 ACM Parameters (continued)

Parameter	Description																								
Program Feature Overrides	<p>Determines which ACM features are enabled and are available for use. If any features are not selected now and you later want to use them, you must run ACAT again, enable the features, create a new configuration file, and run the Install Wizard again.</p> <p>Note When disabled, the feature cannot be used and a user cannot enable the feature option by using Preferences from the ACM main menu.</p> <p>Features: About Box (Help), Exit Program, Launch Aironet Client Utility, Troubleshooting, Preferences, Turn Radio On/Off, Reauthenticate, Select Profile, Auto Profile Selection, Other Configuration Application, Show Connection Status</p> <p>Options per component: Enable or Disable</p> <p>Default per component: Enable</p>																								
	<table border="1"> <thead> <tr> <th>Feature</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>About Box (Help)</td> <td>Displays the ACM version number and enables you to access the online help.</td> </tr> <tr> <td>Exit Program</td> <td>Closes ACM for all client adapters.</td> </tr> <tr> <td>Launch Aironet Client Utility</td> <td>Activates ACU if it was installed.</td> </tr> <tr> <td>Troubleshooting</td> <td>Activates the troubleshooting utility, which enables you to identify and resolve configuration and association problems with your client adapter.</td> </tr> <tr> <td>Preferences</td> <td>Enables you to determine when ACM runs and to select the options that appear on the ACM pop-up menu.</td> </tr> <tr> <td>Turn Radio On/Off</td> <td>Turns the client adapter on or off.</td> </tr> <tr> <td>Reauthenticate</td> <td>Enables you to force your client adapter to try to reauthenticate using the existing name and password of the current profile.</td> </tr> <tr> <td>Select Profile</td> <td>Enables you to select the active profile for your client adapter.</td> </tr> <tr> <td>Auto Profile Selection</td> <td>Causes the client adapter's driver to automatically select a profile from the list of profiles that were set up in ACU to be included in auto profile selection.</td> </tr> <tr> <td>Other Configuration Application</td> <td>Enables an application other than ACU to configure the client adapter.</td> </tr> <tr> <td>Show Connection Status</td> <td>Provides information on the current status of your client adapter.</td> </tr> </tbody> </table>	Feature	Description	About Box (Help)	Displays the ACM version number and enables you to access the online help.	Exit Program	Closes ACM for all client adapters.	Launch Aironet Client Utility	Activates ACU if it was installed.	Troubleshooting	Activates the troubleshooting utility, which enables you to identify and resolve configuration and association problems with your client adapter.	Preferences	Enables you to determine when ACM runs and to select the options that appear on the ACM pop-up menu.	Turn Radio On/Off	Turns the client adapter on or off.	Reauthenticate	Enables you to force your client adapter to try to reauthenticate using the existing name and password of the current profile.	Select Profile	Enables you to select the active profile for your client adapter.	Auto Profile Selection	Causes the client adapter's driver to automatically select a profile from the list of profiles that were set up in ACU to be included in auto profile selection.	Other Configuration Application	Enables an application other than ACU to configure the client adapter.	Show Connection Status	Provides information on the current status of your client adapter.
Feature	Description																								
About Box (Help)	Displays the ACM version number and enables you to access the online help.																								
Exit Program	Closes ACM for all client adapters.																								
Launch Aironet Client Utility	Activates ACU if it was installed.																								
Troubleshooting	Activates the troubleshooting utility, which enables you to identify and resolve configuration and association problems with your client adapter.																								
Preferences	Enables you to determine when ACM runs and to select the options that appear on the ACM pop-up menu.																								
Turn Radio On/Off	Turns the client adapter on or off.																								
Reauthenticate	Enables you to force your client adapter to try to reauthenticate using the existing name and password of the current profile.																								
Select Profile	Enables you to select the active profile for your client adapter.																								
Auto Profile Selection	Causes the client adapter's driver to automatically select a profile from the list of profiles that were set up in ACU to be included in auto profile selection.																								
Other Configuration Application	Enables an application other than ACU to configure the client adapter.																								
Show Connection Status	Provides information on the current status of your client adapter.																								

Table 2-4 ACM Parameters (continued)

Parameter	Description
Menu Options (Defaults)	<p>Determines which menu options are displayed on the ACM pop-up menu. The menu feature must be enabled in Program Feature Overrides before they can be displayed.</p> <p>Menu options: About Box (w/Help), Exit Program, Launch Aironet Client Utility, Troubleshooting, Turn Radio On/Off, Reauthenticate, Select Profile, Show Connection Status</p> <p>Note You can change the default settings for the feature options by selecting Preferences from the ACM main menu.</p> <p>Note If the ACM was previously installed and you changed the menu options, subsequent reinstalls do not revise the menu options.</p> <p>Options per menu option: Show or Hide</p> <p>Default per menu option: Show</p>

Security Modules

The security module software components enable you to install special security modules to support LEAP, EAP-SIM, PEAP, and EAP-FAST with your client adapter. [Table 2-5](#) describes the security module parameters.

Table 2-5 Security Module Parameters

Parameter	Description
LEAP	<p>Enables you to create a profile that uses LEAP authentication. If this option is not selected now and you later want to use LEAP, you must run ACAT again, select this option, create a new configuration file, and run the Install Wizard again.</p> <p>Default: Selected</p> <p>Note Refer to Chapter 4 and Chapter 5 for information on LEAP.</p>
Allow Saved LEAP User Name and Password	<p>Enables you to create a profile in ACU that uses a saved (rather than temporary) username and password for LEAP authentication. When such a profile is used, the saved username and password are used to start the LEAP authentication process, and you are not prompted to enter them.</p> <p>Options: Yes or No</p> <p>Default: Yes</p>

Table 2-5 Security Module Parameters (continued)

Parameter	Description
EAP-SIM	<p>Installs the EAP-SIM supplicant, which enables the client adapter to support EAP-SIM authentication. If this option is not selected now and you later want to use EAP-SIM, you must run ACAT again, select this option, create a new configuration file, and run the Install Wizard again.</p> <p>Note This feature installs only on PCs running the Windows 2000 or XP operating systems. The Install Wizard does not provide an error message when a profile with EAP-FAST fails to install on a non-supported operating system.</p> <p>Default: Deselected</p> <p>Note Refer to Chapter 4 and Chapter 5 for information on EAP-SIM.</p>
PEAP	<p>Installs the PEAP supplicant, which enables the client to support PEAP authentication. If this option is not initially selected and you later want to use PEAP, you must run this installation program again and select this option.</p> <p>Note This feature installs only on PCs running the Windows 2000 or XP operating systems. The Install Wizard does not provide an error message when a profile with EAP-FAST fails to install on a non-supported operating system.</p> <p>Default: Deselected</p> <p>Note Refer to Chapter 4 and Chapter 5 for information on PEAP.</p>
EAP-FAST	<p>Installs the EAP-FAST supplicant, which enables the client to support EAP-FAST authentication. If this option is not initially selected and you later want to use EAP-FAST, you must run this installation program again and select this option.</p> <p>Note This feature requires a Cisco Aironet 350 Series or CB20A Client Adapter.</p> <p>Note This feature installs only on PCs running the Windows 2000 or XP operating systems. The Install Wizard does not provide an error message when a profile with EAP-FAST fails to install on a non-supported operating system.</p> <p>Default: Selected</p> <p>Refer to Chapter 4 and Chapter 5 for information on EAP-FAST.</p>

Table 2-5 Security Module Parameters (continued)

Parameter	Description
Allow Saved EAP-FAST User Name and Password	<p>Enables you to create a profile in ACU that uses a saved (rather than temporary) username and password for EAP-FAST authentication. When such a profile is used, the saved username and password are used to start the EAP-FAST authentication process, and you are not prompted to enter them.</p> <p>Note The ACU must be used to enter the saved EAP-FAST username and password.</p> <p>Options: Yes or No</p> <p>Default: Yes</p>
Allow Auto Provisioning	<p>Enables you to create a profile that automatically acquires a Protected Authentication Credential (PAC) from the EAP-FAST server by sending the username and password.</p> <p>Note When auto provisioning is not allowed, the ACU must be used to enter the provisioning information.</p> <p>Options: Yes or No</p> <p>Default: Yes</p>



Global Override Settings Tab

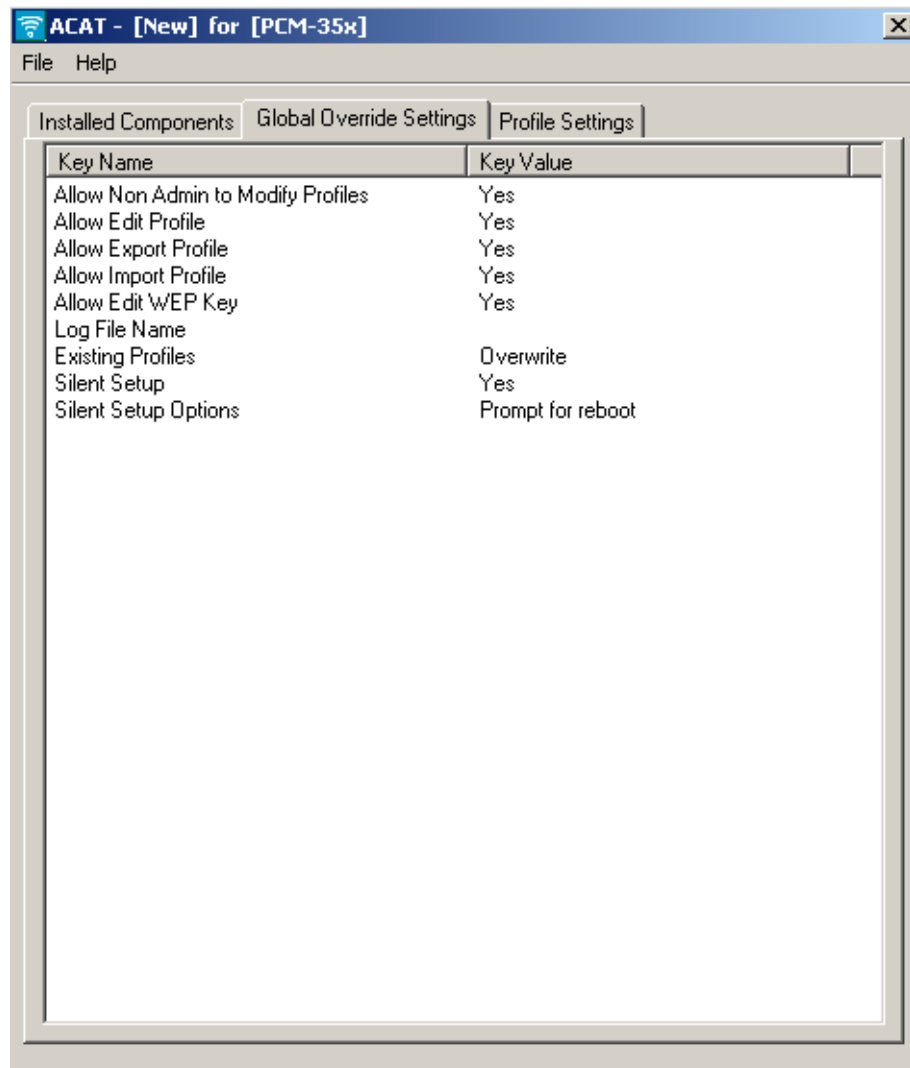
This chapter describes the Global Override Settings tab options. The following topics are covered in this section:

- [Overview, page 3-2](#)
- [Global Override Options, page 3-3](#)

Overview

The Global Override Settings tab enables you to select the override parameters used during the installation process by the Install Wizard. These settings apply to all client adapter profiles and override the settings in the individual profiles. [Figure 3-1](#) shows the override parameters.

Figure 3-1 Global Override Settings Tab Window



To change a parameter option value, you must click an option value such as *Yes*. An option value window appears that enables you to change the value.

Global Override Options

Table 3-1 describes the options for the global override settings tab.

Table 3-1 Options for Global Override Settings

Parameter	Description
Allow Non Admin to Modify Profiles	<p>Specifies whether a user without administrator privileges can change the profiles. Only the Windows NT, the Windows 2000, or the Windows XP operating system supports this option.</p> <p>Note To avoid conflicting settings, check Allow Non-Administrative Users to Save Settings to the Registry under the ACU on the Installed Components tab.</p> <p>Note This option is not available for Windows 95, 98, and Me because these versions of Windows do not support different classes of users.</p> <p>Range: yes or no Default: yes</p>
Allow Edit Profile	<p>Specifies whether or not the ACU can be used to edit a client adapter configuration profile.</p> <p>Note When this parameter is set to <i>no</i>, the ACU does not allow the user to edit, import, or export profiles and the ACAT's <i>Allow Export Profile</i> and <i>Allow Import Profile</i> settings are ignored by the ACU.</p> <p>Range: yes or no Default: yes</p>
Allow Export Profile	<p>Specifies whether or not the ACU can be used to export a client adapter configuration profile to a disk file.</p> <p>Range: yes or no Default: yes</p>
Allow Import Profile	<p>Specifies whether or not the ACU can be used to import a client adapter configuration profile from a disk.</p> <p>Range: yes or no Default: yes</p>
Allow Edit WEP	<p>Specifies whether or not the ACU can be used to edit the WEP security options in a client adapter configuration profile.</p> <p>Range: yes or no Default: yes</p>
Log File Name	<p>Specifies the location of an installation log file (drive, directory, and log filename).</p>

Table 3-1 Options for Global Override Settings (continued)

Parameter	Description
Existing Profiles	<p>Specifies how the existing profiles are handled on the PC during the installation process.</p> <p>Range: Delete, Overwrite, or Preserve</p> <ul style="list-style-type: none"> • Delete—All existing profiles are deleted prior to installing any new profiles. • Overwrite—Any existing profile with the same name as a new profile is overwritten. All other existing profiles are maintained and all new profiles are installed. • Preserve—All existing profiles are maintained. New profiles with the same name as existing profiles are not installed, but other new profiles are installed. <p>Default: Overwrite</p>
Silent Setup	<p>Specifies whether the Install Wizard installation process is silent without requiring user input.</p> <p>Range: yes or no</p> <p>Default: yes</p>
Silent Setup Options	<p>Specifies the options available when Silent Setup is selected. When <i>Prompt for reboot</i> is selected, the installation process displays a message indicating a reboot is necessary and asks if you want to reboot now. When <i>Reboot silently</i> is selected, the installation process automatically reboots the PC. When <i>Do not reboot</i> is selected, the installation process does not display a prompt message and waits for you to reboot the PC.</p> <p>Range: Prompt for reboot, Reboot silently, Do not reboot</p> <p>Default: Prompt for reboot</p>



Profile Settings Tab

This chapter describes ACAT profile options. The following topics are covered in this section:

- [Adding Profiles, page 4-2](#)
- [Editing Profiles Using the Profile Settings Tab, page 4-4](#)

Adding Profiles

ACAT enables you to import existing configuration profiles or create new profiles. The ACAT File menu contains two profile options:

- **Create/Manage Profile**—This option enables you to add, delete, or rename new profile names. When profile names are defined, you can use the ACAT Profile Settings tab to configure each of the profiles.
- **Load from Registry**—This option imports or loads existing profiles from your PC's registry into the ACAT configuration file.

The ACU enables you to create and verify profiles prior to distributing them to other users. The profiles created with the ACU are stored in your PC's registry. When you are satisfied that the profiles are correct and operational, you can use the ACAT Load from Registry option to import the profiles for a specific client adapter type into the ACAT configuration file.

Profiles are stored in the part of the registry reserved for the client adapter driver and therefore are tied to a specific radio type. Consequently, if you set up profiles for a 350 series PC card and the client adapter is later upgraded to a CB20A PC card, all of the profiles are not usable for the new client adapter.

General Recommendations

When you need to configure multiple client adapter types, you should consider the following recommendations:

- On a server accessible to all users, create and name a directory for each client adapter type.
- Place a copy of all the Install Wizard files and sub-directories into each of the client adapter directories.
- Create an ACAT configuration file with the needed profiles and configuration parameters for each client adapter type. Save each ACAT configuration file into the appropriate client adapter directory with the Install Wizard files.



Note All ACAT configuration files use the same filename (CiscoAdminConfig.dat) and therefore must be saved separately.

- To install profiles for a specific client adapter type, each user must execute the Install Wizard (IWSetup.exe) in the appropriate client adapter directory for their client adapter type.

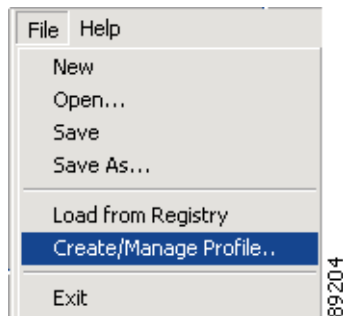
Create/Manage Profile

Prior to configuring a profile in ACAT, you must create a new profile name for each profile. The Create/Manage Profile option in the File menu enables you to add, delete, or rename new profile names. A maximum of 16 profiles can be created.

To create new profile names, follow these steps:

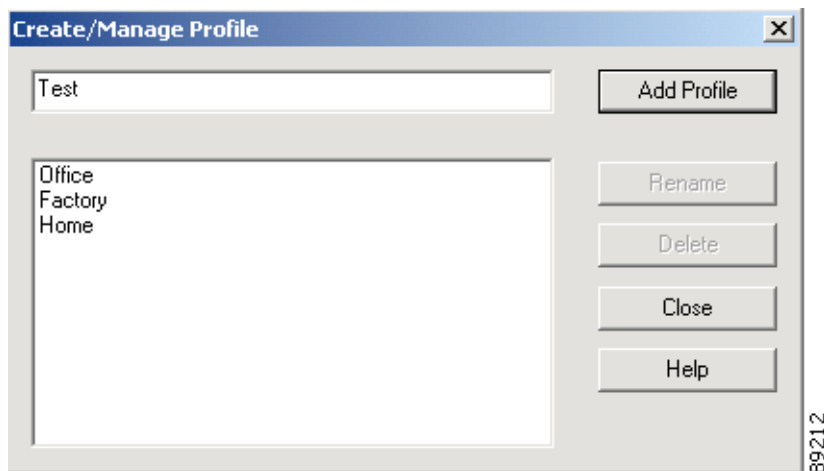
- Step 1** Choose **Create/Manage Profile** in the ACAT File menu (see [Figure 4-1](#)).

Figure 4-1 Create/Manage Profile Option



When you choose this option, the Create/Manage Profile window appears (see [Figure 4-2](#)).

Figure 4-2 Create/Manage Profile Window



- Step 2** Enter a new profile name (1 to 79 ASCII characters) in the entry field and click **Add Profile**.
- Step 3** To rename or delete a profile name, click the profile name and click **Rename** or **Delete**.
- Step 4** When you have completed the entry of new profile names, click **Close**.



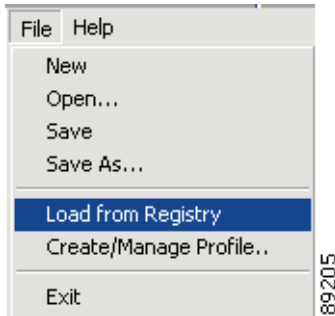
Note A maximum of 16 profiles can be created.

To enter profile configuration parameters, go to the [“Editing Profiles Using the Profile Settings Tab”](#) section on page 4-4.

Load From Registry

The ACAT utility enables you to import existing profiles from your PC's registry by using the Load from Registry option located in the File menu (see [Figure 4-3](#)).

Figure 4-3 Load from Registry Option



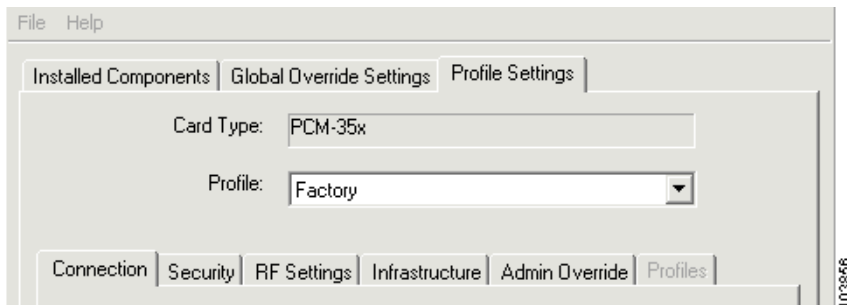
Prior to selecting this option, you must create new profiles using the ACU. These profiles are saved in your PC's registry.

To view or edit the imported profile parameters, go to the [“Editing Profiles Using the Profile Settings Tab”](#) section on page 4-4.

Editing Profiles Using the Profile Settings Tab

The ACAT Profile Settings tab enables you to edit existing profiles and new profiles being created (see [Figure 4-4](#)).

Figure 4-4 Profile Settings Tab Window



This section includes the following topics:

- [Card Type, page 4-5](#)
- [Profile, page 4-5](#)
- [Connection Tab, page 4-6](#)
- [Security Tab, page 4-10](#)
- [RF Settings Tab, page 4-26](#)
- [Infrastructure Tab, page 4-32](#)
- [Ad Hoc Tab, page 4-35](#)
- [Admin Override Tab, page 4-37](#)
- [Auto Profile Selection, page 4-38](#)

Card Type

The Card Type field specifies the client adapter card type being used in the profiles. You specify the card type when you select the New option in the File menu. ACAT defaults to the 350 series PCMCIA (PCM-35x) card type. The following card types are supported:

- PCM-35x—Cisco Aironet 350 series PCMCIA card
- MPI-35x—Cisco Aironet 350 series Mini-PCI card
- PCI-35x—Cisco Aironet 350 series PCI card
- CB20A—Cisco Aironet 5-GHz PC-Cardbus card

**Note**

ACAT 1.6 is compatible only with Install Wizard 1.6.

**Note**

ACAT 1.6 does not support the Cisco Aironet 340 and 4800 series client adapters or the Cisco Aironet IEEE 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG).

Profile

The Profile field enables you to select the profile to be configured. You can click the arrow on the right of the field to view the profile list.

Connection Tab

The Connection tab enables you to specify connection-specific parameters and the client adapter power save mode. The window is shown in [Figure 4-5](#).

Figure 4-5 Connection Tab Window

The screenshot shows the 'Connection Tab' window with the following settings:

- File Help
- Installed Components | Global Override Settings | Profile Settings
- Card Type: PCM-35x
- Profile: Factory
- Connection | Security | RF Settings | Infrastructure | Admin Override | Profiles
- SSID1: Test AP 1
- SSID2: (empty)
- SSID3: (empty)
- Network Type: Infrastructure
- Channel: 6 (2437 MHz)
- Power Save Mode: CAM (Constantly Awake Mode)

103852

Table 4-1 lists and describes the Connection tab parameters.

Table 4-1 Connection Tab Parameters

Parameter	Description						
SSID1	<p>The service set identifier (SSID) identifies the specific wireless network that you want to access.</p> <p>Range: You can enter up to 32 ASCII characters (case sensitive)</p> <p>Default: A blank field</p> <p>Note If you leave this parameter blank, your client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs (refer to your access point documentation). If the access point with which the client adapter is to communicate is not configured to allow broadcast SSIDs, the value of this parameter must match the SSID of the access point. Otherwise, the client adapter is unable to access the network.</p>						
SSID2	<p>An optional SSID that identifies a second distinct network and enables you to roam to that network without having to reconfigure your client adapter.</p> <p>Note A profile with multiple SSIDs cannot be used in auto profile switching.</p> <p>Range: You can enter up to 32 ASCII characters (case sensitive)</p> <p>Default: A blank field</p>						
SSID3	<p>An optional SSID that identifies a third distinct network and enables you to roam to that network without having to reconfigure your client adapter.</p> <p>Note A profile with multiple SSIDs cannot be used in auto profile switching.</p> <p>Range: You can enter up to 32 ASCII characters (case sensitive)</p> <p>Default: A blank field</p>						
Network Type	<p>Specifies the type of network in which your client adapter is installed.</p> <p>Options: Ad Hoc or Infrastructure</p> <p>Default: Infrastructure</p> <table border="1"> <thead> <tr> <th>Network Type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Ad Hoc</td> <td>Often referred to as <i>peer to peer</i>. Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point. For example, an ad hoc network could be set up between computers in a conference room so that users can share information in a meeting.</td> </tr> <tr> <td>Infrastructure</td> <td>Indicates that your wireless network is connected to a wired Ethernet network through an access point.</td> </tr> </tbody> </table>	Network Type	Description	Ad Hoc	Often referred to as <i>peer to peer</i> . Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point. For example, an ad hoc network could be set up between computers in a conference room so that users can share information in a meeting.	Infrastructure	Indicates that your wireless network is connected to a wired Ethernet network through an access point.
Network Type	Description						
Ad Hoc	Often referred to as <i>peer to peer</i> . Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point. For example, an ad hoc network could be set up between computers in a conference room so that users can share information in a meeting.						
Infrastructure	Indicates that your wireless network is connected to a wired Ethernet network through an access point.						

Table 4-1 Connection Tab Parameters (continued)

Parameter	Description
Channel	<p>Specifies which frequency your client adapter uses as the channel for communications. These channels conform to the IEEE 802.11 standard for your regulatory domain.</p> <ul style="list-style-type: none"> • In infrastructure mode, this parameter is set automatically and cannot be changed. The client adapter listens to the entire spectrum, selects the best access point to associate to, and uses the same frequency as that access point. • In ad hoc mode, you must set the channel of the client adapter to match the channel used by the other clients in the wireless network. <p>Range: Dependent on client adapter radio and regulatory domain</p> <p>Example for 2.4-GHz client adapters:</p> <p style="padding-left: 40px;">1 to 11 (2412 to 2462 MHz) in North America</p> <p>Example for 5-GHz client adapters:</p> <p style="padding-left: 40px;">36, 40, 44, 48, 52, 56, 60, and 64 (5180, 5200, 5220, 5240, 5260, 5280, 5300, and 5320 MHz) in North America</p> <p>Default: Dependent on client adapter radio and regulatory domain</p> <p>Example for 2.4-GHz client adapters:</p> <p style="padding-left: 40px;">6 (2437 MHz) in North America</p> <p>Example for 5-GHz client adapters:</p> <p style="padding-left: 40px;">36 (5180 MHz) in North America</p>

Table 4-1 Connection Tab Parameters (continued)

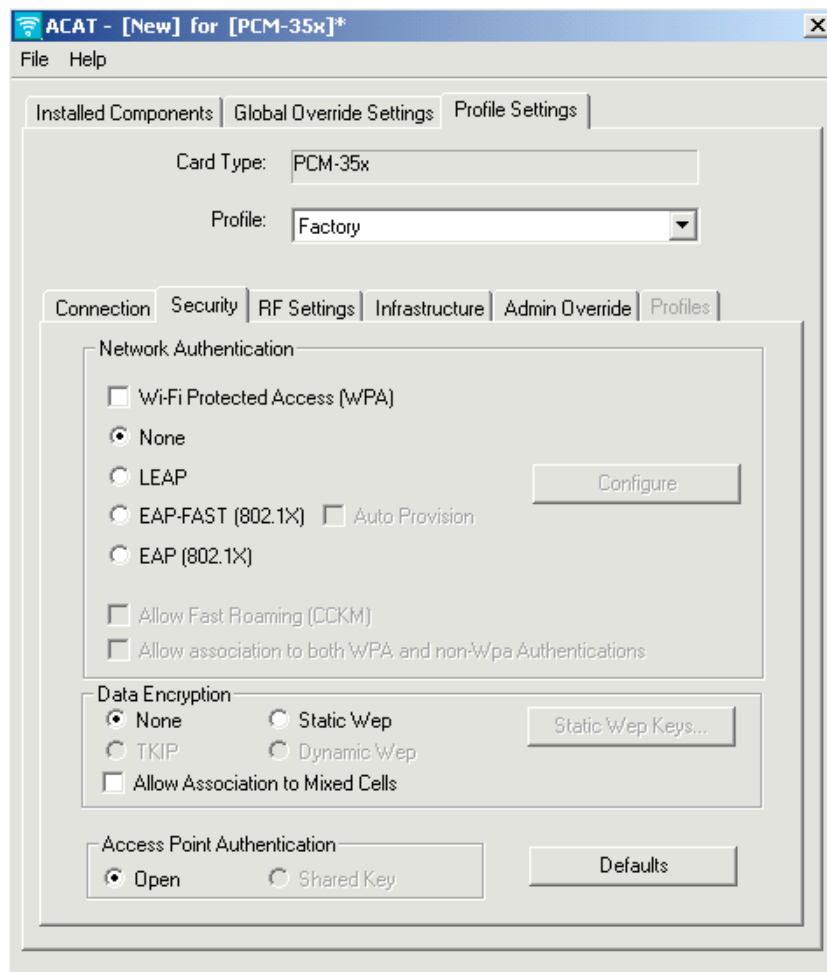
Parameter	Description								
Power Save Mode	<p>Sets your client adapter to its optimum power consumption setting.</p> <p>Options: CAM, Max PSP, or Fast PSP</p> <p>Default: CAM (Constantly Awake Mode)</p>								
	<table border="1"> <thead> <tr> <th>Power Save Mode</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CAM (Constantly Awake Mode)</td> <td> <p>Keeps the client adapter powered up continuously so that there is little lag in message response time.</p> <p>Consumes the most power but offers the highest throughput. This option is recommended for desktop computers and devices that use AC power.</p> </td> </tr> <tr> <td>Max PSP (Max Power Savings)</td> <td> <p>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.</p> <p>Conserves the most power but offers the lowest throughput. This option is recommended for devices for which power consumption is the ultimate concern (such as battery-powered devices).</p> <p>Note When you set Max PSP mode and close ACU, the following message appears the next time you open ACU: “Maximum Power Save mode is temporarily disabled while you are running this application.” While ACU is open, Fast PSP mode is active. When you close ACU, the card returns to Max PSP mode.</p> </td> </tr> <tr> <td>Fast PSP (Power Save Mode)</td> <td> <p>Switches between PSP mode and CAM mode, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets are retrieved.</p> <p>This option is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP.</p> </td> </tr> </tbody> </table>	Power Save Mode	Description	CAM (Constantly Awake Mode)	<p>Keeps the client adapter powered up continuously so that there is little lag in message response time.</p> <p>Consumes the most power but offers the highest throughput. This option is recommended for desktop computers and devices that use AC power.</p>	Max PSP (Max Power Savings)	<p>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.</p> <p>Conserves the most power but offers the lowest throughput. This option is recommended for devices for which power consumption is the ultimate concern (such as battery-powered devices).</p> <p>Note When you set Max PSP mode and close ACU, the following message appears the next time you open ACU: “Maximum Power Save mode is temporarily disabled while you are running this application.” While ACU is open, Fast PSP mode is active. When you close ACU, the card returns to Max PSP mode.</p>	Fast PSP (Power Save Mode)	<p>Switches between PSP mode and CAM mode, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets are retrieved.</p> <p>This option is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP.</p>
Power Save Mode	Description								
CAM (Constantly Awake Mode)	<p>Keeps the client adapter powered up continuously so that there is little lag in message response time.</p> <p>Consumes the most power but offers the highest throughput. This option is recommended for desktop computers and devices that use AC power.</p>								
Max PSP (Max Power Savings)	<p>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.</p> <p>Conserves the most power but offers the lowest throughput. This option is recommended for devices for which power consumption is the ultimate concern (such as battery-powered devices).</p> <p>Note When you set Max PSP mode and close ACU, the following message appears the next time you open ACU: “Maximum Power Save mode is temporarily disabled while you are running this application.” While ACU is open, Fast PSP mode is active. When you close ACU, the card returns to Max PSP mode.</p>								
Fast PSP (Power Save Mode)	<p>Switches between PSP mode and CAM mode, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets are retrieved.</p> <p>This option is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP.</p>								

Security Tab

The Security tab window (see [Figure 4-6](#)) enables you to set parameters that control how the client adapter associates to an access point, authenticates to the wireless network, and encrypts and decrypts data. The Security tab window is organized into three sections:

- Network Authentication—specifies network authentication options.
- Data Encryption—specifies data encryption options.
- Access Point Authentication—specifies access point authentication options.

Figure 4-6 Security Tab Window



This window presents several security features, each of which involves a number of steps. In addition, the security features themselves are complex and need to be understood before they are implemented. [Chapter 5, “Security Features,”](#) provides an overview of the security features.

Network Authentication

The network authentication section specifies the network authentication options available for your client adapter. [Table 4-2](#) describes the parameter options.

Table 4-2 Network Authentication Parameters

Parameter	Description
Wi-Fi Protected Access (WPA)	<p>Specifies whether WPA authentication is used by the client adapter.</p> <p>Note When WPA is selected, the TKIP data encryption parameter is automatically set. The other data encryption options are unavailable.</p> <p>Note When WPA is selected, you can also select LEAP (WPA), EAP-FAST (WPA), or EAP (WPA) authentication.</p> <p>Range: selected or not selected</p> <p>Default: not selected</p>
None	<p>When selected, specifies that network authentication is not used.</p> <p>Range: selected or not selected</p> <p>Default: selected</p>
LEAP	<p>Specifies whether LEAP authentication is used by the client adapter.</p> <p>Note When LEAP is selected, the Dynamic WEP data encryption option is automatically set. If WPA is selected also, the TKIP data encryption option is automatically set. The other data encryption options are unavailable and the Configure button is activated for entry of LEAP settings.</p> <p>Note When WPA is selected this parameter changes from LEAP to LEAP (WPA).</p> <p>Range: selected or not selected</p> <p>Default: not selected</p>

Table 4-2 Network Authentication Parameters (continued)

Parameter	Description
EAP-FAST (802.1X)	<p>Specifies whether EAP-FAST authentication is used by the client adapter.</p> <p>Note When EAP-FAST is selected, the Dynamic WEP data encryption option is automatically set and the Configure button is activated for entry of EAP-FAST settings. If WPA is selected also, the TKIP data encryption option is automatically set. The other data encryption options are unavailable.</p> <p>Note This feature is only available when using 350 series or CB20A cards and client adapters.</p> <p>Note When WPA is selected this parameter changes from EAP-FAST (802.1X) to EAP-FAST (WPA).</p> <p>Note This feature installs only on PCs running the Windows 2000 or XP operating systems. The Install Wizard does not provide an error message when a profile with EAP-FAST fails to install on a non-supported operating system.</p> <p>Range: selected or not selected Default: not selected</p>
Auto Provision	<p>Specifies whether EAP-FAST authentication uses automatically accessed or manually specified Protected Authentication Credentials (PAC) provisioning.</p> <p>Note Provisioning is the process of associating a PAC file with a specific user or group of users.</p> <p>Note When auto provisioning is not selected, the ACU must be used to enter the provisioning information.</p> <p>Range: selected or not selected Default: not selected</p>
EAP (802.1X)	<p>Specifies whether the client adapter uses an 802.1X authentication type supported by your PC operating system.</p> <p>Note When WPA is selected this parameter changes from EAP (802.1X) to EAP (WPA).</p> <p>Range: selected or not selected Default: not selected</p>

Table 4-2 Network Authentication Parameters (continued)

Parameter	Description
Allow Fast Roaming (CCKM)	<p>Specifies whether the client adapter can use the CCKM feature available in some access points.</p> <p>Note This option is available only when LEAP or EAP-FAST is selected.</p> <p>Note When this option is selected, the client adapter uses CCKM only with access points supporting the CCKM feature but the client adapter can associate with access points that do not support CCKM.</p> <p>Range: selected or not selected</p> <p>Default: not selected</p>
Allow association to both WPA and non-WPA Authentications	<p>Specifies whether the client adapter can associate to access points supporting or not supporting WPA.</p> <p>Note This option is only available when WPA is selected.</p> <p>Range: selected or not selected</p> <p>Default: not selected</p>

Data Encryption

The Data Encryption section specifies the encryption options (see [Table 4-3](#)) used by the client adapter.

Table 4-3 Data Encryption Options

Parameter	Description
None	<p>Specifies that data encryption is not used by the client adapter.</p> <p>Range: selected or unselected</p> <p>Default: selected</p>
Static WEP	<p>Specifies that static WEP encryption is used by the client adapter.</p> <p>Range: selected or unselected</p> <p>Default: unselected</p>
TKIP	<p>Specifies that Temporal Key Integrity Protocol (TKIP) is used by the client adapter.</p> <p>Note TKIP is automatically enabled when WPA is selected.</p> <p>Range: selected or unselected</p> <p>Default: unselected</p>

Table 4-3 Data Encryption Options (continued)

Parameter	Description
Dynamic WEP	<p>Specifies that dynamic WEP encryption is used by the client adapter.</p> <p>Note Dynamic WEP is automatically enabled when LEAP or EAP-FAST is selected.</p> <p>Range: selected or unselected</p> <p>Default: unselected</p>
Allow Association to Mixed Cells	<p>Indicates whether the client adapter can associate to an access point that enables both WEP and non-WEP associations.</p> <p>Range: selected or unselected</p> <p>Default: unselected</p>

Allow Association To Mixed Cells Parameter

The Allow Association To Mixed Cells parameter indicates whether the client adapter can associate to an access point that enables both WEP and non-WEP associations. Follow the guidelines below to set this parameter.

- Check the **Allow Association To Mixed Cells** check box if the access point with which the client adapter is to associate has WEP set to Optional and WEP is enabled on the client adapter. Otherwise, the client is unable to establish a connection with the access point.
- Uncheck the **Allow Association To Mixed Cells** check box if the access point with which the client adapter is to associate does not have WEP set to Optional.



Note For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP.



Note This parameter is not available in Ad Hoc mode.



Note This parameter is not available if WPA is selected unless the *Allow association to both WPA and non-WPA Authentications* parameter is also selected.

Access Point Authentication

The access point authentication section defines how your client adapter attempts to authenticate to an access point:

- **Open Authentication**—Enables your client adapter, regardless of its WEP settings, to associate and attempt to communicate with an access point. Open Authentication is the default setting.



Note The client adapter can successfully send data frames only when it has the same WEP key as the access point.

- **Shared Key Authentication**—Enables your client adapter to communicate only with access points that have the same WEP key.

In shared key authentication, the access point sends a known unencrypted challenge packet to the client adapter, which encrypts the packet and sends it back to the access point. The access point attempts to decrypt the encrypted packet and sends an authentication response packet indicating the success or failure of the decryption back to the client adapter. If the packet is successfully encrypted/decrypted, the user is considered to be authenticated.



Note Cisco does not recommend the use of shared key authentication because it is a security risk.



Note Shared key authentication is only available when Static WEP is selected as the data encryption method.

Entering a New Static WEP Key

Follow the steps below to enter a new static WEP key for this profile.

Step 1 Check **None** under the Network Associations section on the Security Tab Window.

Step 2 Check **Static WEP** under Data Encryption.



Note Selecting **LEAP** from the Network Authentication section on the Security tab window automatically disables static WEP and enables dynamic WEP.

Step 3 Click **Static WEP Keys** and the WEP Key Setting window appears.

Step 4 Choose one of the following WEP key entry methods using the drop-down menu:

- **Hexadecimal**—Specifies that the WEP key will be entered in hexadecimal characters, which include 0-9, A-F, and a-f.
- **ASCII Text**—Specifies that the WEP key will be entered in ASCII text, which includes alpha characters, numbers, and punctuation marks.



Note ASCII text WEP keys are not supported on Cisco Aironet 1200 Series Access Points (running VxWorks software), so you must select the Hexadecimal (0-9, A-F, a-f) option if you are planning to use your client adapter with these access points.

Step 5 For the static WEP key that you are entering (1, 2, 3, or 4), select a WEP key size of 40 or 128 using the drop-down menu. 128-bit client adapters can use 40- or 128-bit keys, but 40-bit adapters can use only 40-bit keys.

- Step 6** Obtain the static WEP key from your system administrator and enter it in the blank field for the key you are creating. Follow the guidelines below to enter a new static WEP key:
- WEP keys must contain the following number of characters:
 - 10 hexadecimal characters or 5 ASCII text characters for 40-bit keys
Example: 5A5A313859 (hexadecimal) or ZZ18Y (ASCII)
 - 26 hexadecimal characters or 13 ASCII text characters for 128-bit keys
Example: 5A583135333554595549333534 (hexadecimal) or ZX1535TYUI354 (ASCII)
 - Your client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.
 - When setting more than one WEP key, the keys must be assigned to the same WEP key numbers for all devices. For example, WEP key 2 must be WEP key number 2 on all devices. When multiple WEP keys are set, they must be in the same order on all devices.
- Step 7** Click the **Transmit Key** button to the left of the key you want to use to transmit packets. Only one WEP key can be selected as the transmit key.
- Step 8** Choose one of the following access point authentication options, which defines how your client adapter attempts to authenticate to an access point:
- **Open**—Enables your client adapter to authenticate and attempt to communicate with an access point, regardless of its WEP settings. Open Authentication is the default setting.
 - **Shared Key**—Enables your client adapter to communicate only with access points that have the same WEP key. This option is only available if Static WEP is selected.



Note Cisco recommends that shared key authentication not be used because it is a security risk.

- Step 9** Click **OK** to return to the Security tab window.



Note After a WEP key is configured, you can enter a new key value, but you cannot view the original key or delete it.

Disabling Static WEP

To disable static WEP for a particular profile, check **None** under Data Encryption on the Security Tab Window.



Note Selecting **LEAP** from the Network Authentication section on the Security tab window automatically disables static WEP and enables dynamic WEP.

Enabling LEAP

Before you can enable LEAP authentication, your network devices must meet the following requirements:

- Client adapters must support WEP and use the firmware, drivers, utilities, and security modules included in the Install Wizard file.
- To use WPA, 350 series and CB20A client adapters must use the software included in Install Wizard 1.2 or later on a computer running Windows 2000 or XP operating systems.
- To use the reporting access points that fail LEAP authentication and fast secure roaming features, client adapters must use the client adapter firmware included in Install Wizard 1.2 or later.
- Access points to which your client adapter may attempt to authenticate must use the following software releases or later: VxWorks release 11.23T (340 and 350 series access points), 11.54T (1200 series access points) or Cisco IOS Release 12.2(4)JA (1100 series access points).



Note To use WPA, access points must use Cisco IOS Release 12.2(11)JA or later. To use the reporting access points that fail LEAP authentication and fast secure roaming features, access points must use the VxWorks release 12.00T (340, 350, and 1200 series access points) or Cisco IOS Release 12.2(4)JA (1100 series access points).

- All necessary infrastructure devices (such as access points, servers, etc.) must be properly configured for LEAP authentication.

Follow these steps to enable LEAP authentication for the selected profile.

Step 1 If you want to enable WPA, check **Wi-Fi Protected Access (WPA)** on the Network Authentication section of the Security tab window. This parameter enables client adapters to associate to access points using WPA (for additional information refer to [“Wi-Fi Protected Access \(WPA\)” section on page 5-6](#)).

Step 2 Check **LEAP** on the Network Authentication section of the Security tab window.



Note When you check this option, dynamic WEP is automatically enabled. If WPA is also selected, TKIP is enabled.

Step 3 Click **Configure** and the LEAP Settings window appears (see [Figure 4-7](#)).

Figure 4-7 LEAP Settings Window

Step 4 Choose one of the following LEAP username and password setting options:

- **Use Temporary User Name and Password**—Requires the entry of a LEAP username and password each time the computer reboots in order to authenticate and gain access to the network.
- **Use Saved User Name and Password**—Uses the LEAP username and password saved by the ACU in the computer’s registry each time the computer reboots. Authentication occurs automatically as needed using the saved username and password (which are registered with the RADIUS server).



Note When this option is selected, you must use the ACU on their PCs to configure LEAP by selecting the *Use Saved User Name and Password* option and entering the appropriate LEAP username and password. The option fields are unavailable in ACAT.



Note The Use Saved User Name and Password option is available only if the Allow Saved LEAP User Name and Password option is enabled on the Installed Components tab (refer to the [“Installed Components Tab Window”](#) section on page 2-2 for additional information).

- Step 5** If you selected Use Temporary User Name and Password in [Step 4](#), choose one of the following options using the drop-down menu:
- **Use Windows User Name and Password**—Causes your Windows username and password to also serve as your LEAP username and password, giving you only one set of credentials to remember. After you log in, the LEAP authentication process begins automatically. This option is the default setting.
 - **Automatically Prompt for LEAP User Name and Password**—Requires you to enter a separate LEAP username and password (which are registered with the RADIUS server) in addition to your regular Windows login in order to start the LEAP authentication process.
 - **Manually Prompt for LEAP User Name and Password**—Requires you to manually invoke the LEAP authentication process as needed using the Manual LEAP Login option from the ACU Commands drop-down menu. You are not prompted to enter a LEAP username and password during the Windows login. This option might be used to support a software token one-time password system or other systems that require additional software that is not available at login.
- Step 6** If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection without Login** check box. The default setting is not selected.
- Step 7** If you work in an environment with multiple domains and want your Windows login domain to be passed to the RADIUS server along with your username, check the **Include Windows Login Domain With User Name** check box. The default setting is not selected.
- Step 8** If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection without Login** check box. The default setting is checked.
- Step 9** In the LEAP Authentication Timeout Value field, enter the amount of time (in seconds) after which a LEAP authentication is considered a failure and an error message appears.
- Range:** 45 to 300 seconds
- Default:** 90 seconds
- Step 10** If you want to limit the amount of time that is spent finding a domain controller during the authentication process, follow these steps:
- a. Check **Restrict Time Finding the Domain Controller to (seconds)**.
Default: Unchecked
 - b. Enter the amount of time (in seconds) allowed in the authentication process to find the domain controller. Finding the domain controller is the last sequence of the authentication process.
Range: 0 to 300 seconds
Default: 0 seconds



Note Entering a value of zero causes the authentication process to skip the “Finding Domain Controller” step altogether.



Note The finding domain controller timeout value is included in the overall LEAP authentication timeout value. For example, if the authentication timeout value is 60 seconds, and the finding domain controller timeout value is 10 seconds, the client adapter has up to 60 seconds to complete the entire authentication process, up to 10 seconds of which is allocated for finding the domain controller.



Note If you require domain services such as login scripts and roaming desktops, Cisco recommends that you do not check the Restrict Time Finding Domain Controller to (seconds) check box.



Note Regardless of whether the check box is checked or unchecked, the “Finding Domain Controller” step is bypassed once you are logged into Windows or if you log into the local machine and not into a domain.

Step 11 Click **OK** to exit the LEAP Settings window and return to the Security tab window.

Step 12 If you want to enable fast roaming on your client adapter, check **Allow Fast Roaming (CCKM)** in the Network Authentication section of the Security tab window.

- Selecting this option enables the client adapter to use CCKM when associated to access points that are using CCKM. Using this option your client adapter can also associate to access points that are not using CCKM.
- Not selecting this option prevents your client adapter from using CCKM even with access points that use CCKM.

Default: Not selected



Note This option is available only when WPA is enabled.



Note If your computer uses the Microsoft 802.1X supplicant and you want to take advantage of the fast roaming feature, refer to the Microsoft documentation for instructions.

Step 13 If you want to associate to access points that support WPA and even those that do not support it, check **Allow Association to both WPA and non-WPA authentication**. If this option is not selected, your client adapter can associate only to access points that use WPA.

Default: Not selected

Enabling EAP-FAST

Before you can enable EAP-FAST authentication, your network devices must meet the following requirements:

- Client adapters must support WEP and use the firmware, drivers, utilities, and security modules included in the Install Wizard file.
- The 350 series and CB20A client adapters must use the software included in Install Wizard 1.3 or later on a computer running Windows 2000 or XP operating systems.
- To use the reporting access points that fail EAP-FAST authentication and fast secure roaming features, client adapters must use the client adapter firmware included in Install Wizard 1.3 or later.
- Access points to which your client adapter may attempt to authenticate must use the following software releases or later: VxWorks release 11.23T (340 and 350 series access points), 11.54T (1200 series access points) or Cisco IOS Release 12.2(4)JA (1100 series access points).



Note To use WPA, access points must use Cisco IOS Release 12.2(11)JA or later. To use the reporting access points that fail EAP-FAST authentication and fast secure roaming features, access points must use the VxWorks release 12.00T (340, 350, and 1200 series access points) or Cisco IOS Release 12.2(4)JA (1100 series access points).

- All necessary infrastructure devices (such as access points, servers, etc.) must be properly configured for EAP-FAST authentication.

Follow these steps to enable EAP-FAST authentication for the selected profile.

Step 1 If you want to enable WPA, check **Wi-Fi Protected Access (WPA)** on the Network Authentication section of the Security tab window. This parameter enables client adapters to associate to access points using WPA (for additional information refer to [“Wi-Fi Protected Access \(WPA\)” section on page 5-6](#)).

Step 2 Check **EAP-FAST** on the Network Authentication section of the Security tab window.



Note When you check this option, dynamic WEP is automatically enabled. If WPA is also selected, TKIP is enabled.

Step 3 Check **Auto Provision** to allow the EAP-FAST protocol to transmit the username and password to the EAP-FAST server to automatically obtain the PAC provisioning.



Note The Auto Provision option is available only if the Allow Auto Provisioning option is enabled on the Installed Components tab (refer to the [“Installed Components Tab Window” section on page 2-2](#) for additional information).



Note If Auto-Provision is not checked, the ACU must be used to manually configure the PAC settings for this profile.

Step 4 Click **Configure** and the EAP-FAST Settings window appears (see [Figure 4-8](#)).

Figure 4-8 EAP-FAST Settings Window

Step 5 Check one of the following EAP-FAST username and password setting options:

- **Use Temporary User Name and Password**—Requires the entry of an EAP-FAST username and password each time the computer reboots in order to authenticate and gain access to the network. This option is the default setting.
- **Use Saved User Name and Password**—Uses the EAP-FAST username and password saved by the ACU in the computer’s registry each time the computer reboots. Authentication occurs automatically as needed using the saved username and password (which are registered with the EAP-FAST server).



Note When this option is selected, you must use the ACU to configure EAP-FAST by selecting the *Use Saved User Name and Password* option and entering the appropriate EAP-FAST username and password. The option fields are unavailable in ACAT.



Note The Use Saved User Name and Password option is available only if the Allow Saved EAP-FAST User Name and Password option is enabled on the Installed Components tab (refer to the [“Installed Components Tab Window”](#) section on page 2-2 for additional information).

- Step 6** If you selected Use Temporary User Name and Password in [Step 4](#), choose one of the following options using the drop-down menu:
- **Use Windows User Name and Password**—Causes your Windows username and password to also serve as your EAP-FAST username and password, giving you only one set of credentials to remember. After you log in, the LEAP authentication process begins automatically. This option is the default setting.
 - **Automatically Prompt for User Name and Password**—Requires you to enter a separate EAP-FAST username and password (which are registered with the EAP-FAST server) in addition to your regular Windows login in order to start the EAP-FAST authentication process.
 - **Manually Prompt for User Name and Password**—Requires you to manually invoke the EAP-FAST authentication process as needed using the Manual EAP-FAST Login option from the ACU Commands drop-down menu. You are not prompted to enter a EAP-FAST username and password during the Windows login. This option might be used to support a software token one-time password system or other systems that require additional software that is not available at login.
- Step 7** If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection without Login** check box. The default setting is not selected.
- Step 8** If you work in an environment with multiple domains and want your Windows login domain to be passed to the EAP-FAST server along with your username, check the **Include Windows Login Domain With User Name** check box. The default setting is not selected.
- Step 9** If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection without Login** check box. The default setting is checked.
- Step 10** In the Authentication Timeout Value field, enter the amount of time (in seconds) before a EAP-FAST authentication is considered a failure and an error message appears.
- Range:** 45 to 300 seconds
- Default:** 90 seconds
- Step 11** If you want to limit the amount of time that is spent finding a domain controller during the authentication process, follow these steps:
- a. Check **Restrict Time Finding the Domain Controller to (seconds)**.
- Default:** Unchecked
- b. Enter the amount of time (in seconds) allowed in the authentication process to find the domain controller. Finding the domain controller is the last sequence of the authentication process.
- Range:** 0 to 300 seconds
- Default:** 0 seconds

**Note**

Entering a value of zero causes the authentication process to skip the “Finding Domain Controller” step altogether.

**Note**

The finding domain controller timeout value is included in the overall EAP-FAST authentication timeout value. For example, if the authentication timeout value is 60 seconds, and the finding domain controller timeout value is 10 seconds, the client adapter has up to 60 seconds to complete the entire authentication process, up to 10 seconds of which is allocated for finding the domain controller.



Note If you require domain services such as login scripts and roaming desktops, Cisco recommends that you do not check the Restrict Time Finding Domain Controller to (seconds) check box.



Note Regardless of whether the check box is checked or unchecked, the “Finding Domain Controller” step is bypassed once you are logged into Windows or if you log into the local machine and not into a domain.

Step 12 Click **OK** to exit the EAP-FAST Settings window and return to the Security tab window.

Step 13 If you want to enable fast roaming on your client adapter, check **Allow Fast Roaming (CCKM)** in the Network Authentication section of the Security tab window.

- Selecting this option enables the client adapter to use CCKM when associated to access points that are using CCKM. Using this option your client adapter can also associate to access points that are not using CCKM.
- Not selecting this option prevents your client adapter from using CCKM even with access points that use CCKM.

Default: Not selected



Note This option is available only when WPA is enabled.



Note If your computer uses the Microsoft 802.1X supplicant and you want to take advantage of the fast roaming feature, refer to the Microsoft documentation for instructions.

Step 14 If you want to associate to access points that support WPA and even those that do not support it, check **Allow Association to both WPA and non-WPA authentication**. If this option is not selected, your client adapter can associate only to access points that use WPA.

Default: Not selected

Enabling Host-Based EAP

Before you can enable host-based EAP authentication, your network devices must meet the following requirements:

- EAP authentication is supported only by 340 and 350 series access points running VxWorks release 11.06 (or later) or 1200 series access points running VxWorks release 11.40T (or later) or 1100 series access points.
- MIC, TKIP, PEAP, Broadcast Key Rotation, and EAP-SIM authentications are supported only by 340 and 350 series access points running VxWorks release 11.23T (or later), 1200 series access points running VxWorks release 11.54T (or later), or 1100 series access points.
- The Microsoft 802.1X supplicant must be installed on your user’s PCs running Windows.

- To use WPA or WPA-PSK, you must use a 350 series or CB20A client adapter with the software included in Install Wizard 1.2 or later on a computer running Windows 2000 or XP. Also one of the following host supplicants must be installed. You can download these supplicants from the URLs provided:
 - Funk Odyssey Client supplicant release 2.2 (for Windows 2000)
http://www.funk.com/radius/wlan/wlan_c_radius.asp
 - Windows XP Service Pack 1 and Microsoft supplicant Q815485 (for Windows XP)
<http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/default.asp>
<http://www.microsoft.com/downloads/details.aspx?FamilyID=009d8425-ce2b-47a4-abec-274845dc9e91&DisplayLang=en>



Note To use WPA, access points must use Cisco IOS Release 12.2(11)JA or later.



Note For additional information on configuring WPA or WPA-PSK on Microsoft Window PCs, refer to Microsoft documentation and the Cisco Aironet 350 and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows..

- All necessary infrastructure devices (for example, access points, servers, gateways, user databases, etc.) must be properly configured for the authentication type you plan to enable on the client.

Follow the steps below to enable host-based EAP authentication (EAP-TLS, PEAP, or EAP-SIM) for this profile.



Note Because EAP-TLS, PEAP, and EAP-SIM authentication are enabled in the operating system and not in ACU, you cannot switch between these authentication types simply by switching profiles in ACU. You can create a profile that uses host-based EAP, but you must enable the specific authentication type in Windows (provided Windows uses the Microsoft 802.1X supplicant). In addition, Windows can be set for only one authentication type at a time; therefore, if you have more than one profile that uses host-based EAP and you want to use another authentication type, you must change authentication types in Windows after switching profiles in ACU.

-
- Step 1** Check **Wi-Fi Protected Access (WPA)** under Network Authentication on the Security tab window if you want to enable WPA. This parameter enables the client adapter to associate to access points using WPA.
- Step 2** Check **Host Based EAP** from the Network Authentication on the Security tab window.
- Step 3** Dynamic WEP Keys are used if your access point is configured for EAP-TLS, PEAP, and EAP-SIM authentication. Click **Dynamic WEP** if WPA is not enabled.



Note For additional information on configuring a PC running Windows 2000 or XP, refer to Microsoft documentation or the *Cisco Aironet 350 and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows*.

RF Settings Tab

The RF Settings tab window (see [Figure 4-9](#)) enables you to set parameters that control how and when the client adapter transmits and receives data.

Figure 4-9 RF Settings Tab Window

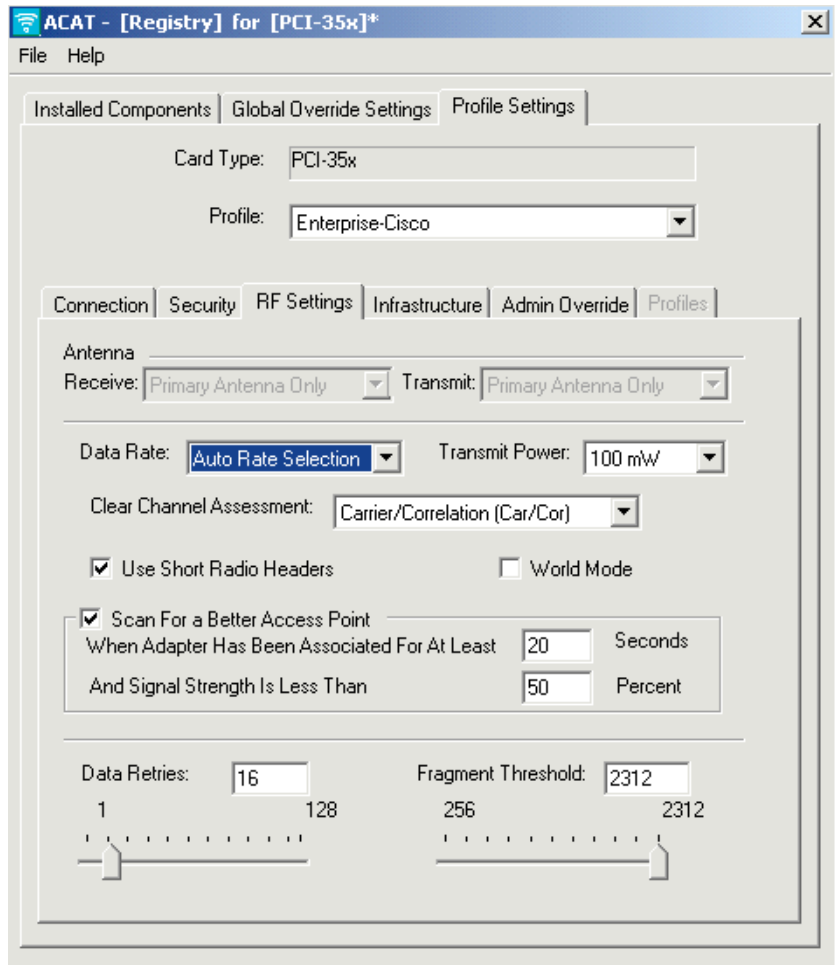


Table 4-4 lists and describes the client adapter's RF network parameters. Follow the instructions in the table to change any parameters.

Table 4-4 RF Network Parameters

Parameter	Description
Antenna (Receive)	<p>Specifies the antenna that your client adapter uses to receive data.</p> <ul style="list-style-type: none"> • PCM and CB20A cards—The integrated, permanently attached antennas operates best when used in diversity mode. Diversity mode enables the card to use the better signal from its two antenna ports. Options: Diversity (Both), Primary Antenna Only, Secondary Antenna Only Default: Diversity (Both) • PCI card—The PCI card must use the Primary Antenna Only option. Default: Primary Antenna Only • MPI card—The mini PCI card, which can be used with one or two antennas, operates best in diversity mode. Diversity mode enables the card to use the better signal from its two antenna connectors. Options: Diversity (Both), Primary Antenna Only, Secondary Antenna Only Default: Diversity (Both) <p>Note This parameter is available only for 2.4-GHz client adapters.</p>
Antenna (Transmit)	<p>Specifies the antenna that your client adapter uses to transmit data. See the Antenna (Receive) parameter above for information on the options available for your client adapter.</p> <p>Note This parameter is available only for 2.4-GHz client adapters.</p>

Table 4-4 RF Network Parameters (continued)

Parameter	Description		
Data Rate	<p>Specifies the rate at which your client adapter should transmit or receive packets to or from access points (in infrastructure mode) or other clients (in ad hoc mode).</p> <p>Auto Rate Selection is recommended for infrastructure mode; setting a specific data rate is recommended for ad hoc mode.</p> <p>Options: Auto Rate Selection, 1 Mbps Only, 2 Mbps Only, 5.5 Mbps Only, or 11 Mbps Only (2.4-GHz client adapters)</p> <p>Auto Rate Selection, 6 Mbps Only, 9 Mbps Only, 12 Mbps Only, 18 Mbps Only, 24 Mbps Only, 36 Mbps Only, 48 Mbps Only, or 54 Mbps Only (5-GHz client adapters)</p> <p>Default: Auto Rate Selection</p>		
	Data Rate		Description
	2.4-GHz Client Adapters	5-GHz Client Adapters	
	Auto Rate Selection	Auto Rate Selection	Uses the 11-Mbps (for 2.4-GHz client adapters) or 54-Mbps (for 5-GHz client adapters) data rate when possible but drops to lower rates when necessary.
	1 Mbps Only	6 Mbps Only	Offers the greatest range but the lowest throughput.
	2 Mbps Only and 5.5 Mbps Only	9 Mbps Only to 48 Mbps Only	Progressively offers less range but greater throughput than the 1 Mbps Only (for 2.4-GHz client adapters) or 6 Mbps Only (for 5-GHz client adapters) option.
	11 Mbps Only	54 Mbps Only	Offers the greatest throughput but the lowest range.
	<p>Note Your client adapter's data rate must be set to Auto Rate Selection or must match the data rate of the access point (in infrastructure mode) or the other clients (in ad hoc mode) with which it is to communicate. Otherwise, your client adapter may not be able to associate to them.</p>		

Table 4-4 RF Network Parameters (continued)

Parameter	Description						
Transmit Power	<p>Defines the power level at which your client adapter transmits. This value must not be higher than that allowed by your country's regulatory agency (FCC in the U.S., DOC in Canada, ETSI in Europe, MKK in Japan, etc.).</p> <p>Options: Dependent on the power table programmed into the client adapter; see the table below</p> <p>Default: The maximum level programmed into the client adapter and allowed by your country's regulatory agency</p> <table border="1"> <thead> <tr> <th>Possible Power Levels</th> <th>Client Adapter Type</th> </tr> </thead> <tbody> <tr> <td>100 mW, 50 mW, 30 mW, 20 mW, 5 mW, or 1 mW</td> <td>350 series client adapters</td> </tr> <tr> <td>20 mW, 10 mW, or 5 mW</td> <td>PC-Cardbus card (5-GHz client adapter)</td> </tr> </tbody> </table> <p>Note Reducing the transmit power level conserves battery power but decreases radio range.</p> <p>Note When World Mode is enabled, the client adapter is limited to the maximum transmit power level allowed by the country of operation's regulatory agency.</p> <p>Note If you are using an older version of a 350 series client adapter, your power level options may be different than those listed here.</p>	Possible Power Levels	Client Adapter Type	100 mW, 50 mW, 30 mW, 20 mW, 5 mW, or 1 mW	350 series client adapters	20 mW, 10 mW, or 5 mW	PC-Cardbus card (5-GHz client adapter)
Possible Power Levels	Client Adapter Type						
100 mW, 50 mW, 30 mW, 20 mW, 5 mW, or 1 mW	350 series client adapters						
20 mW, 10 mW, or 5 mW	PC-Cardbus card (5-GHz client adapter)						

Table 4-4 RF Network Parameters (continued)

Parameter	Description										
Clear Channel Assessment	Specifies the method that determines whether the channel on which your client adapter operates is clear prior to the transmission of data. Options: Firmware Default (<i>xxx</i>), Carrier/Correlation (Car/Cor), Energy Detect (ED), or ED or Car/Cor Default: Firmware Default (<i>xxx</i>)										
	<table border="1"> <thead> <tr> <th>Method</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Firmware Default (<i>xxx</i>)</td> <td>The Clear Channel Assessment (CCA) mechanism reports that the channel is busy based on the default value of the client adapter's firmware. The firmware's CCA default value is shown in parentheses. Note The CCA default <i>xxx</i> value for PCM/LMC/PCI card firmware is Car/Cor; the default value for mini PCI card firmware is ED.</td> </tr> <tr> <td>Carrier/Correlation (Car/Cor)</td> <td>The CCA mechanism reports that the channel is busy upon detection of a direct-sequence spread spectrum (DSSS) signal. This signal may be above or below the ED threshold.</td> </tr> <tr> <td>Energy Detect (ED)</td> <td>The CCA mechanism reports that the channel is busy upon detection of any energy above the ED threshold.</td> </tr> <tr> <td>ED or Car/Cor</td> <td>The CCA mechanism reports that the channel is busy upon detection of a DSSS signal or any energy above the ED threshold.</td> </tr> </tbody> </table>	Method	Description	Firmware Default (<i>xxx</i>)	The Clear Channel Assessment (CCA) mechanism reports that the channel is busy based on the default value of the client adapter's firmware. The firmware's CCA default value is shown in parentheses. Note The CCA default <i>xxx</i> value for PCM/LMC/PCI card firmware is Car/Cor; the default value for mini PCI card firmware is ED.	Carrier/Correlation (Car/Cor)	The CCA mechanism reports that the channel is busy upon detection of a direct-sequence spread spectrum (DSSS) signal. This signal may be above or below the ED threshold.	Energy Detect (ED)	The CCA mechanism reports that the channel is busy upon detection of any energy above the ED threshold.	ED or Car/Cor	The CCA mechanism reports that the channel is busy upon detection of a DSSS signal or any energy above the ED threshold.
	Method	Description									
	Firmware Default (<i>xxx</i>)	The Clear Channel Assessment (CCA) mechanism reports that the channel is busy based on the default value of the client adapter's firmware. The firmware's CCA default value is shown in parentheses. Note The CCA default <i>xxx</i> value for PCM/LMC/PCI card firmware is Car/Cor; the default value for mini PCI card firmware is ED.									
	Carrier/Correlation (Car/Cor)	The CCA mechanism reports that the channel is busy upon detection of a direct-sequence spread spectrum (DSSS) signal. This signal may be above or below the ED threshold.									
	Energy Detect (ED)	The CCA mechanism reports that the channel is busy upon detection of any energy above the ED threshold.									
ED or Car/Cor	The CCA mechanism reports that the channel is busy upon detection of a DSSS signal or any energy above the ED threshold.										
Note This parameter is available only for 2.4-GHz client adapters.											
Use Short Radio Headers	<p>Checking this check box sets your client adapter to use short radio headers. However, the adapter can use short radio headers only if the access point is also configured to support them and is using them. If any clients associated to an access point are using long headers, then <i>all</i> clients in that cell must also use long headers, even if both this client and the access point have short radio headers enabled.</p> <p>Short radio headers improve throughput performance; long radio headers ensure compatibility with clients and access points that do not support short radio headers.</p> <p>Default: Selected</p> <p>Note This parameter is available only for 2.4-GHz client adapters in Infrastructure mode.</p> <p>Note This parameter is referred to as <i>Preambles</i> on the access point windows.</p>										

Table 4-4 RF Network Parameters (continued)

Parameter	Description
World Mode	<p>Checking this check box enables the client adapter to adopt the maximum transmit power level and the frequency range of the access point to which it is associated, provided the access point is also configured for world mode. This parameter is available only in infrastructure mode and is designed for users who travel between countries and want their client adapters to associate to access points in different regulatory domains.</p> <p>Default: Deselected</p> <p>Note This parameter is available only for 2.4-GHz client adapters.</p> <p>Note When World Mode is enabled, the client adapter is limited to the maximum transmit power level allowed by the country of operation's regulatory agency.</p>
Periodically Scan For a Better Access Point	<p>Checking this check box causes the client adapter to look for a better access point if the signal strength of its associated access point is less than the specified value after the specified time and to switch associations if it finds one.</p> <p>Example: If the default values of 20 seconds and 50% are used, the client adapter begins monitoring the strength of the signal received from its associated access point 20 seconds after becoming associated. The monitoring continues once per second. If the client detects a signal strength reading below 50%, it scans for a better access point.</p> <p>Range: 5 to 255 seconds; 0 to 75% signal strength</p> <p>Defaults: Checked, 20 seconds, 50% signal strength</p>
Data Retries	<p>Defines the number of times a packet is resent if the initial transmission is unsuccessful.</p> <p>Range: 1 to 128</p> <p>Default: 16 (2.4-GHz client adapters) or 32 (5-GHz client adapters)</p> <p>Note If your network protocol performs its own retries, set this parameter to a smaller value than the default. This way, notification of a bad packet is sent up the protocol stack quickly so the application can retransmit the packet if necessary.</p>
Fragment Threshold	<p>Defines the threshold above which an RF data packet is split up or fragmented. If one of those fragmented packets experiences interference during transmission, only that specific packet would need to be resent.</p> <p>Throughput is generally lower for fragmented packets because the fixed packet overhead consumes a higher portion of the RF bandwidth.</p> <p>Range: 256 to 2312</p> <p>Default: 2312</p>

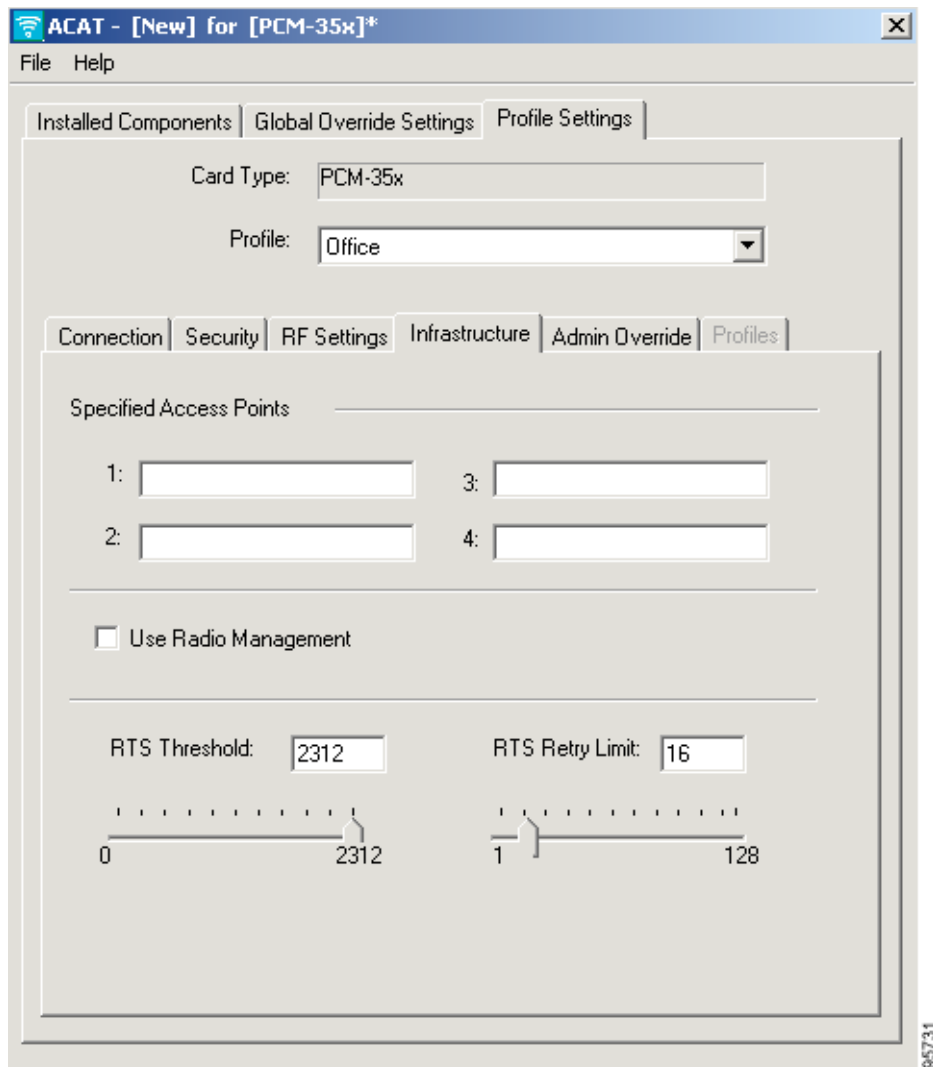
Infrastructure Tab

The Infrastructure tab window (see [Figure 4-10](#)) enables you to set parameters that control how the client adapter operates within an infrastructure network.


Note

You can set infrastructure parameters only if your client adapter is set to operate in an infrastructure network. See the Network Type parameter in [Table 4-1](#).

Figure 4-10 Infrastructure Tab Window



[Table 4-5](#) lists and describes the client adapter's infrastructure parameters. Follow the instructions in the table to change any parameters.

Table 4-5 Infrastructure Tab Parameters

Parameter	Description
Specified Access Points 1-4	<p>Specifies the MAC addresses of up to four preferred access points with which the client adapter can associate. If the specified access points are not found or the client adapter roams out of range, the adapter may associate to another access point.</p> <p>You can enter the MAC addresses of the access points in the edit boxes or choose not to specify access points by leaving the boxes blank.</p> <p>Default: Blank fields</p> <p>Note This parameter should be used only for access points that are in repeater mode. For normal operation, leave these fields blank because specifying an access point slows down the roaming process.</p>
Use Radio Management	<p>Selecting this parameter enables the access point to which the client adapter is associated to control the use of radio management (RM), provided RM is enabled on the access point. RM is a system-wide feature that involves multiple infrastructure nodes. The RM feature on the access point acts on radio measurement requests from other network devices to instruct the access point and/or its associated clients to perform required radio measurements and then report them.</p> <p>Note This parameter is available in Install Wizard version 1.2 or later and only for 350 series client adapters.</p> <p>Note Access points must use Cisco IOS Release 12.2(13)JA or later to enable RM. Refer to the documentation for your access point for instructions on enabling this feature.</p> <p>Range: Enable or disabled</p> <p>Default: Disabled</p>

Table 4-5 Infrastructure Tab Parameters (continued)

Parameter	Description
RTS Threshold	<p>Specifies the size of the data packet that the low-level RF protocol issues to a request-to-send (RTS) packet.</p> <p>Setting this parameter to a small value causes RTS packets to be sent more often. When this occurs, more of the available bandwidth is consumed and the throughput of other network packets is reduced. However, the system is able to recover faster from interference or collisions that may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p>Range: 0 to 2312</p> <p>Default: 2312</p> <p>Note Refer to the IEEE 802.11 standard for more information on the RTS/CTS mechanism.</p>
RTS Retry Limit	<p>Specifies the number of times the client adapter resends a request-to-send (RTS) packet if it does not receive a clear-to-send (CTS) packet from the previously sent RTS packet.</p> <p>Setting this parameter to a large value decreases the available bandwidth whenever interference is encountered. However, a large value makes the system more immune to interference and collisions that may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p>Range: 1 to 128</p> <p>Default: 16 (2.4-GHz client adapters) or 32 (5-GHz client adapters)</p> <p>Note Refer to the IEEE 802.11 standard for more information on the RTS/CTS mechanism.</p>

Ad Hoc Tab

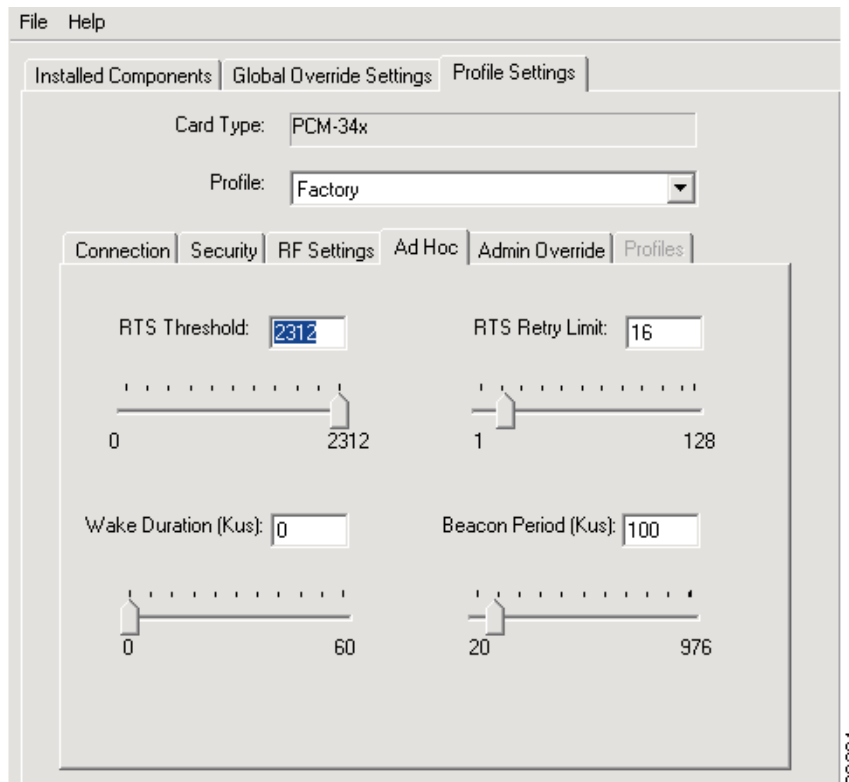
The Ad Hoc tab window (see [Figure 4-11](#)) enables you to set parameters that control how the client adapter operates within an ad hoc network.



Note

You can set ad hoc parameters only if your client adapter is set to operate in an ad hoc network. See the network type parameter in [Table 4-1](#).

Figure 4-11 Ad Hoc Tab Window



[Table 4-6](#) lists and describes the client adapter's advanced ad hoc parameters. Follow the instructions in the table to change any parameter.

Table 4-6 Ad Hoc Tab Parameters

Parameter	Description
RTS Threshold	<p>Specifies the size of the data packet that the low-level RF protocol issues to a request-to-send (RTS) packet.</p> <p>Setting this parameter to a small value causes RTS packets to be sent more often. When this occurs, more of the available bandwidth is consumed and the throughput of other network packets is reduced. However, the system is able to recover faster from interference or collisions that may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p>Range: 0 to 2312</p> <p>Default: 2312</p> <p>Note Refer to the IEEE 802.11 standard for more information on the RTS/CTS mechanism.</p>
RTS Retry Limit	<p>Specifies the number of times the client adapter resends a request-to-send (RTS) packet if it does not receive a clear-to-send (CTS) packet from the previously sent RTS packet.</p> <p>Setting this parameter to a large value decreases the available bandwidth whenever interference is encountered. However, a large value makes the system more immune to interference and collisions that may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p>Range: 1 to 128</p> <p>Default: 16 (2.4-GHz client adapters) or 32 (5-GHz client adapters)</p> <p>Note Refer to the IEEE 802.11 standard for more information on the RTS/CTS mechanism.</p>
Wake Duration (K μ s)	<p>Specifies the amount of time following a beacon that the client adapter stays awake to receive announcement traffic indication message (ATIM) packets, which are sent to the adapter to keep it awake until the next beacon.</p> <p>Refer to the power save mode parameter in Table 4-1.</p> <p>Range: 0 Kμs (in CAM mode); 5 to 60 Kμs (in Max PSP or Fast PSP mode)</p> <p>Default: 0 Kμs</p> <p>Note If your client adapter is set to CAM mode, you must set the wake duration to 0 Kμs. If your client adapter is set to Max PSP or Fast PSP mode, you must set the wake duration to a minimum of 5 Kμs.</p> <p>Note Kμs is a unit of measurement in software terms. K = 1024, μ = 10⁻⁶, and s = seconds, so Kμs = .001024 seconds, 1.024 milliseconds, or 1024 microseconds.</p>

Table 4-6 Ad Hoc Tab Parameters (continued)

Parameter	Description
Beacon Period (Kμs)	Specifies the duration between beacon packets, which are used to help clients find each other in ad hoc mode. Range: 20 to 976 Kμs Default: 100 Kμs

Admin Override Tab

The Admin Override tab window (see [Figure 4-12](#)) enables you to specify administrator override settings for individual profiles. Each profile can have different settings.


Note

The settings on the Global Override Settings tab apply to all profiles and override these individual profile settings.

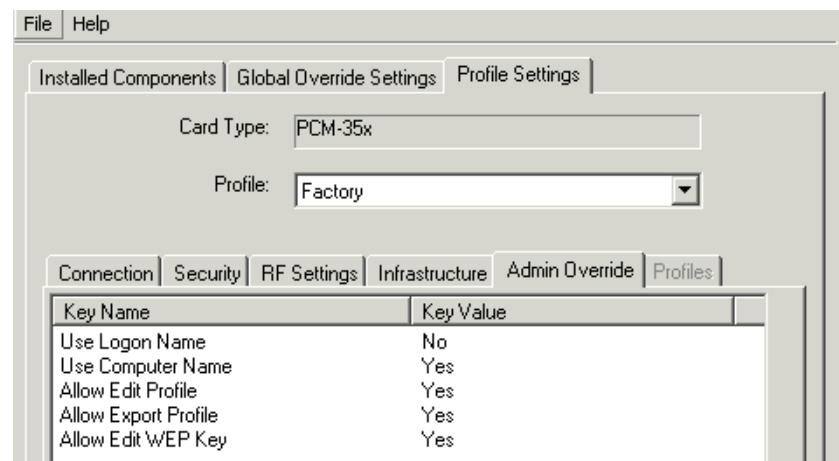
Figure 4-12 Admin Override Tab Window

Table 4-7 lists and describes the Admin Override tab parameters. Follow the instructions in the table to change any parameter.

Table 4-7 Admin Override Tab Parameters

Parameter	Description
Use Logon Name	Specifies whether the Window's logon name is used as the client's logon name. Range: yes or no Default: no Note When you select <i>Use Logon Name</i> , the Use Computer Name parameter is automatically deselected.
Use Computer Name	Specifies whether your computer's name is used as the client's logon name. Range: yes or no Default: no Note When you select <i>Use Computer Name</i> , the Use Logon Name parameter is automatically deselected.
Allow Edit Profile	Specifies whether the ACU can be used to edit the client adapter configuration profile. Range: yes or no Default: yes
Allow Export Profile	Specifies whether the ACU can be used to export the client adapter configuration profile to a disk file. Range: yes or no Default: yes
Allow Edit WEP	Specifies whether the ACU can be used to edit the WEP security options in the client adapter configuration profile. Range: yes or no Default: yes

Auto Profile Selection

When Auto Profile Selection is selected in the Profile field, you can manage up to 16 profiles (or saved configurations) for a client adapter. These profiles enable the client adapter to be used in different locations, each of which requires different configuration settings. For example, you may want to set up profiles for using the client adapter at the office, at home, and in public areas such as airports. After the profiles are created, they are automatically switched without requiring you to reconfigure the client adapter each time it is moved to a new location.



Note

Auto profile selection does not support profiles with multiple SSIDs, profiles with a null SSID (no value specified), or profiles with the same SSID.

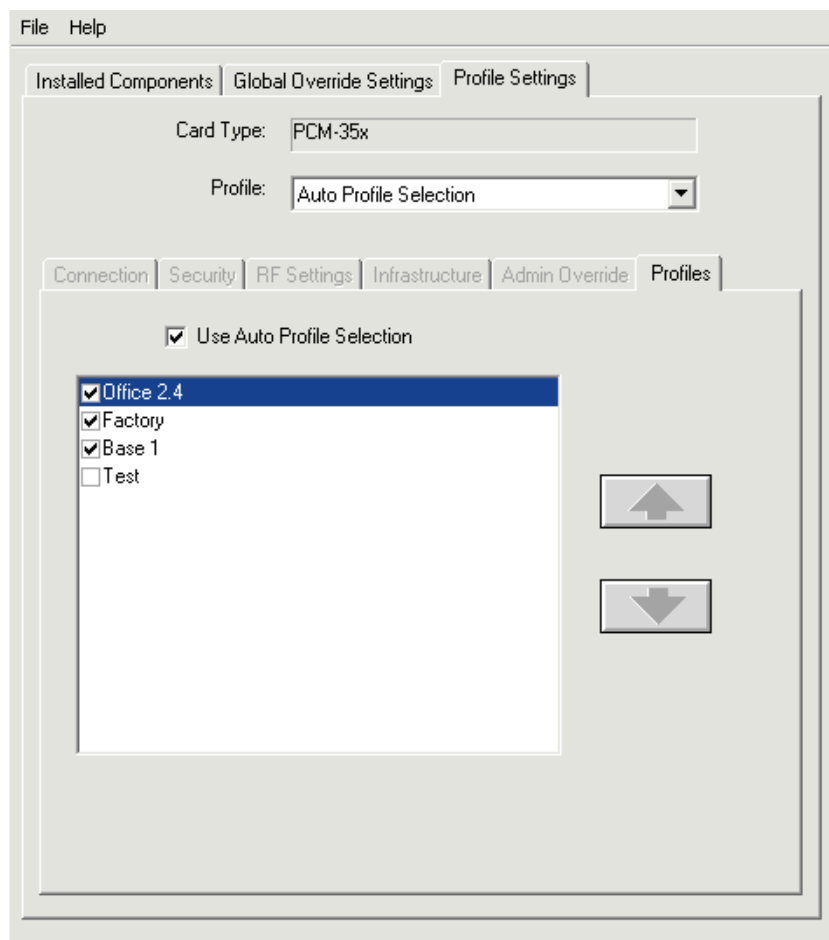
Profiles Tab

When you select Auto Profile Selection using the Profile drop-down menu, the Profiles tab window appears (see [Figure 4-13](#)). The window lists all available profiles and enables you to select and prioritize the profiles that are automatically switched. When you roam from one area to another, the SSIDs from the profiles are scanned by priority until a connection to an access point is established. When the client adapter's association to the access point is lost, the SSID scanning starts again from the highest priority profile in the list.

**Note**

Auto profile selection does not display profiles containing a null SSID (no value specified), a duplicate SSID, or multiple SSIDs. These types of profiles cannot be used in auto profile switching.

Figure 4-13 Profile Tab Window



Setting Priorities and Activating Auto Profile Selection

To set priorities and activate auto profile selection on the client adapter, follow these steps:

-
- Step 1** Check the profiles that you want to include in auto profile selection.
 - Step 2** Click each profile and use the up and down arrow keys to position the profile into the desired order, highest priority at top of the list and the lowest priority at the bottom of the list.
 - Step 3** Check the **Use Auto Profile Selection** check box.
-



Security Features

This chapter describes the security features. The following topics are covered in the chapter.

- [Overview, page 5-2](#)
- [Static WEP Keys, page 5-2](#)
- [EAP \(with Static or Dynamic WEP Keys\), page 5-3](#)
- [Additional WEP Key Security Features, page 5-8](#)
- [Synchronizing Security Features, page 5-9](#)

Overview

You can protect your data as it is transmitted through your wireless network by encrypting it with Wired Equivalent Privacy (WEP) encryption keys. With WEP encryption, the transmitting device encrypts each packet with a WEP key, and the receiving device uses that same key to decrypt each packet.

The WEP keys used to encrypt and decrypt transmitted data can be statically associated with your adapter or dynamically created as part of the EAP authentication process. The information in the [“Static WEP Keys”](#) and [“EAP \(with Static or Dynamic WEP Keys\)”](#) sections below can help you to decide which type of WEP keys to use. Dynamic WEP keys with EAP offer a higher degree of security than static WEP keys.

WEP keys, whether static or dynamic, are either 40 or 128 bits long. 128-bit WEP keys offer a greater level of security than 40-bit WEP keys.

**Note**

Refer to the [“Additional WEP Key Security Features”](#) section on page 5-8 for information on three security features that can make your WEP keys even more secure.

Static WEP Keys

Each device (or profile) within your wireless network can be assigned up to four static WEP keys. If a device receives a packet that is not encrypted with the appropriate key (as the WEP keys of all devices that are to communicate with each other must match), the device discards the packet and never delivers it to the intended receiver.

Static WEP keys are write-only and temporary; therefore, they cannot be read back from the client adapter, and they are lost when power to the adapter is removed or the Windows device is rebooted. Although the keys are temporary, you do not need to re-enter them each time the client adapter is inserted or the Windows device is rebooted because the keys are stored (in an encrypted format for security reasons) in the registry of the Windows device. When the driver loads and reads the client adapter's registry parameters, it also finds the static WEP keys, unencrypts them, and stores them in volatile memory on the adapter.

The Security Tab window enables you to view the current WEP key settings for the client adapter and then to assign new WEP keys or overwrite existing WEP keys as well as to enable or disable static WEP. Refer to the [“Entering a New Static WEP Key”](#) section on page 4-15 or [“Disabling Static WEP”](#) section on page 4-16 for instructions.

EAP (with Static or Dynamic WEP Keys)

The new standard for wireless LAN security, as defined by the IEEE, is called *802.1X for 802.11*, or simply *802.1X*. An access point that supports 802.1X and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server such as a RADIUS server, to which the access point communicates over the wired network.

Three 802.1X authentication types can be selected in ACAT for use with Windows operating systems:

- **LEAP**—This authentication type is available for Windows 95, 98, NT, 2000, Me, and XP, as well as non-Windows systems. Support for LEAP is provided not in the Windows operating system but in your client adapter's firmware and the Cisco software that supports it. RADIUS servers that support LEAP include Cisco Secure ACS release 2.6 and later, Cisco Access Registrar release 1.7 and later, and Funk Software's Steel-Belted RADIUS release 3.0 and later.

LEAP can be enabled or disabled for a specific profile through ACAT. When enabled, a variety of configuration options are available, including how and when a username and password are entered to begin the authentication process.

The username and password are used by the client adapter to perform mutual authentication with the RADIUS server through the access point. The username and password are stored in the client adapter's volatile memory; therefore, they are temporary and need to be re-entered whenever power is removed from the adapter, typically because of the client adapter being ejected or the system powering down.

- **EAP-FAST**—This authentication type (Flexible Authentication via Secure Tunneling) is available for Windows 2000 and XP systems. Support for EAP-FAST is provided not in the Windows operating system but in your client adapter's firmware and the Cisco software that supports it. RADIUS servers that support EAP-FAST include Cisco Secure ACS release 3.2.3 and later.



Note The Install Wizard does not provide an error indication when a profile with EAP-FAST fails to install on a non-supported operating system.

EAP-FAST can be enabled or disabled for a specific profile using ACAT, or the ACU can be used if the EAP-FAST security module was selected during installation. When EAP-FAST is enabled, a variety of configuration options are available, including how and when a username and password are entered to begin the authentication process and whether automatic or manual protected access credentials (PAC) provisioning is used.

The username, password, and PAC are used by the client adapter to perform mutual authentication with the RADIUS server through the access point. The username and password need to be re-entered each time the client adapter is inserted or the Windows device is rebooted, unless you configure your adapter to use saved EAP-FAST credentials.

PACs are created by Cisco Secure ACS and are identified by an ID. The user obtains his or her own copy of the PAC from the server, and the ID links the PAC to the profile created by ACAT or the ACU. When manual PAC provisioning is enabled, the PAC file is manually copied from the server and imported into the client device using the ACU. The following rules govern PAC storage:

- In most cases PACs are provisioned and stored separately for each Windows logon user. These per-user PACs are not viewable by other users.
- If a profile is configured to use manual provisioning, each user must manually provision his or her own PAC for that profile using the ACU.
- PAC files can be added or replaced using the ACU import feature, but they cannot be removed or exported.

- For profiles configured with saved EAP-FAST usernames and passwords, the PACs are not stored per user but in a global PAC area shared by all users. Global PACs are also enabled when the No Network Connection Unless User Is Logged In checkbox is unchecked on the ACU. These global PACs can be imported using the ACU and used by all users.



Note Checking the Use Saved Username and Password check box in ACAT enables the option on the ACU. You must use the ACU to enter the EAP-FAST username and password parameters.



Note PACs are also stored globally on computers that use the Novell Network login prompt or any other third-party login application that does not share its credentials with the EAP-FAST supplicant.

EAP-FAST authentication is designed to support the following user databases over a wireless LAN:

- Cisco Secure ACS internal user database
- Cisco Secure ACS ODBC user database
- Windows NT/2000/2003 domain user database
- LDAP user database

LDAP user databases (such as NDS) support only manual PAC provisioning while the other three user databases support both automatic and manual PAC provisioning.



Note If the EAP-FAST security module was not selected during installation, the EAP-FAST option is unavailable in the ACU. To enable and disable EAP-FAST, you must run ACAT or the Install Wizard again and select EAP-FAST. EAP-FAST is supported in ACAT and Install Wizard versions 1.3 and later.

- **EAP**—Selecting this option enables you to use any 802.1X authentication type for which your operating system has support. For example, if your operating system uses the 802.1X supplicant, it provides native support for EAP-TLS authentication and general support for PEAP and EAP-SIM authentication.



Note To use EAP-TLS, PEAP, or EAP-SIM you must install the Microsoft 802.1X supplicant and the PEAP or EAP-SIM security module; configure your client adapter using ACAT or the ACU; enable the authentication type in Windows; and enable Network-EAP on the access point.

- **EAP-TLS**—EAP-TLS is enabled or disabled through the operating system and uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. Once enabled, a few configuration parameters must be set within the operating system.

RADIUS servers that support EAP-TLS include Cisco Secure ACS release 3.0 or later and Cisco Access Registrar release 1.8 or later.



Note EAP-TLS requires the use of a certificate. Refer to Microsoft's documentation for information on downloading and installing the certificate.

- **Protected EAP (or PEAP)**—PEAP authentication is designed to support One-Time Password (OTP), Windows NT or 2000 domain, and LDAP user databases over a wireless LAN. It is based on EAP-TLS authentication but uses a password or PIN instead of a client certificate for authentication. PEAP is enabled or disabled through the operating system and uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. If your network uses an OTP user database, PEAP requires you to enter either a hardware token password or a software token PIN to start the EAP authentication process and gain access to the network. If your network uses a Windows NT or 2000 domain user database or an LDAP user database (such as NDS), PEAP requires you to enter your username, password, and domain name in order to start the authentication process.

RADIUS servers that support PEAP authentication include Cisco Secure ACS release 3.1 or later and Cisco Access registrar release 3.5 or later.



Note Service Pack 1 for Windows XP and the Microsoft 802.1X supplicant for Windows 2000 include Microsoft's PEAP supplicant, which supports a Windows username and password only and does not operate with Cisco's PEAP supplicant. To use Cisco's PEAP supplicant, install the Install Wizard file after Service Pack 1 for Windows XP or the Microsoft's 802.1X supplicant for Windows 2000. Otherwise, Cisco's PEAP is overwritten by Microsoft's PEAP supplicant.

- **EAP-SIM**—EAP-SIM authentication is designed for use in public wireless LANs and requires clients equipped with PCSC-compliant smartcard readers. The EAP-SIM supplicant included in the Install Wizard file supports only Gemplus SIM+ cards; however, an updated supplicant is available that supports standard GSM-SIM cards as well as more recent versions of the EAP-SIM protocol. The new supplicant is available for download from the ftpeng FTP server at the following URL:

<ftp://ftpeng.cisco.com/ftp/pwlan/eapsim/CiscoEapSim.dll>

Please note that the above requirements are necessary but not sufficient to successfully perform EAP-SIM authentication. Typically, you are also required to enter into a service contract with a WLAN service provider, who must support EAP-SIM authentication in its network. Also, while your PCSC smartcard reader may be able to read standard GSM-SIM cards or chips, EAP-SIM authentication usually requires your GSM cell phone account to be provisioned for WLAN service by your service provider.

EAP-SIM is enabled or disabled through the operating system and uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data.

EAP-SIM requires you to enter a user verification code, or PIN, for communication with the SIM card. You can choose to have the PIN stored in your computer or to be prompted to enter it after a reboot or prior to every authentication attempt.

RADIUS servers that support EAP-SIM include Cisco Access Registrar release 3.0 or later.



Note Because EAP-TLS, PEAP, and EAP-SIM authentication are enabled in the operating system and not in ACU, you cannot switch between these authentication types simply by switching profiles in ACU. You can create a profile in ACU that uses host-based EAP, but you must enable the specific authentication type in Windows (provided Windows uses the Microsoft 802.1X supplicant). In addition, Windows can be set for only one authentication type at a time; therefore, if you have more than one profile in ACU that uses host-based EAP and you want to use another authentication type, you must change authentication types in Windows after switching profiles in ACU.

When you enable Network-EAP or Require EAP on your access point and configure your client adapter for LEAP, EAP-FAST, EAP-TLS, PEAP, or EAP-SIM, authentication to the network occurs in the following sequence:

1. The client associates to an access point and begins the authentication process.



Note The client does not gain full access to the network until authentication between the client and the RADIUS server is successful.

2. Communicating through the access point, the client and RADIUS server complete the authentication process, with the password (LEAP, EAP-FAST, and PEAP), certificate (EAP-TLS), or internal key stored on the SIM card and in the service provider's Authentication Center (EAP-SIM) being the shared secret for authentication. The password, certificate, or internal key is never transmitted during the process.
3. If authentication is successful, the client and RADIUS server derive a dynamic, session-based WEP key that is unique to the client.
4. The RADIUS server transmits the key to the access point using a secure channel on the wired LAN.
5. For the length of a session, or time period, the access point and the client use this key to encrypt or decrypt all unicast packets (and broadcast packets if the access point is set up to do so) that travel between them.

Refer to the “[Enabling LEAP](#)” section on page 4-17 for instructions on enabling LEAP, or to the “[Enabling EAP-FAST](#)” section on page 4-20 for instructions on enabling EAP-FAST, or to the “[Enabling Host-Based EAP](#)” section on page 4-24 for instructions on enabling EAP-TLS, PEAP, or EAP-SIM.

Refer to the IEEE 802.11 standard for more information on 802.1X authentication and to the following URL for additional information on RADIUS servers:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgr/secur_c/scprt2/scrad.htm

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages Temporal Key Integrity Protocol (TKIP) for data protection and 802.1X for authenticated key management.

WPA supports two mutually exclusive key management types: WPA and WPA-Pre-shared key (WPA-PSK). Using WPA key management, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the access point. Using WPA-PSK, however, you configure a pre-shared key on both the client and the access point, and that pre-shared key is used as the PMK.



Note

Only 350 series and CB20A cards that are installed on computers running Windows 2000 or XP and running LEAP, EAP-FAST, or host-based EAP authentication can be used with WPA.

Support for WPA is available in Install Wizard version 1.2 or later. However, if you want to use host-based EAP authentication with WPA, you must also install a host supplicant with WPA support. The following host supplicants are recommended for use with Cisco Aironet client adapters:

- Funk Odyssey Client supplicant release 2.2 (for Windows 2000)
- Windows XP Service Pack 1 and Microsoft supplicant Q815485 (for Windows XP)

Refer to the “[Enabling LEAP](#)” section on page 4-17 for instructions on enabling LEAP with WPA or to the “[Enabling Host-Based EAP](#)” section on page 4-24 for instructions on enabling EAP-TLS, PEAP, or EAP-SIM with WPA.

WPA must also be enabled on the access point. Access points must use Cisco IOS Release 12.2(11)JA or later to enable WPA. Refer to the documentation for your access point for instructions on enabling this feature.

Fast Roaming (CCKM)

Some applications that run on a client device may require fast roaming between access points. For example, voice applications require seamless roaming to prevent delays and gaps in conversation. Support for fast roaming is available for LEAP-enabled clients in Install Wizard version 1.1 or later or for EAP-FAST-enabled clients in Install Wizard 1.6 or later.

During normal operation, LEAP or EAP-FAST-enabled clients mutually authenticate with a new access point by performing a complete LEAP or EAP-FAST authentication, including communication with the main RADIUS server. However, when you configure your wireless LAN for fast roaming, LEAP or EAP-FAST-enabled clients securely roam from one access point to another without the need to reauthenticate with the RADIUS server. Using Cisco Centralized Key Management (CCKM), an access point that is configured for wireless domain services (WDS) uses a fast rekeying technique that enables client devices to roam from one access point to another in under 150 milliseconds (ms). Fast roaming ensures that there is no perceptible delay in time-sensitive applications such as wireless Voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions.

The fast roaming feature is enabled on the client adapter in two different ways, depending on the software installed:

- If you are using client adapter firmware version 5.40.xx (which is included in Install Wizard 1.3), you need to enable fast roaming in ACAT or Aironet Client Utility (ACU) 6.3. For additional details, refer to [Step 12](#) in the “[Enabling LEAP](#)” section on page 4-17 or to [Step 13](#) in the “[Enabling EAP-FAST](#)” section on page 4-20.
- If you are using client adapter firmware version 5.20.17 (which is included in Install Wizard 1.1), fast roaming is supported automatically.

Regardless of how fast roaming is enabled on the client adapter, it must also be enabled on the access point.

**Note**

Access points must use Cisco IOS Release 12.2(11)JA or later to enable fast roaming. Refer to the documentation for your access point for instructions on enabling this feature.

**Note**

If the Microsoft 802.1X supplicant is installed on your computer, you must disable one or two Windows parameters in order for this feature to operate correctly. Refer to [Step 13](#) in the “[Enabling LEAP](#)” section for details.

Reporting Access Points that Fail LEAP or EAP-FAST Authentication

Client adapter firmware version 5.02.20 or later and the following access point software releases support a feature that is designed to detect access points that fail LEAP authentication:

- VxWorks release 12.00T or later (340, 350, and 1200 series access points)
- Cisco IOS Release 12.2(4)JA or later (1100 series access points)

An access point running one of these software releases records a message in the system log when a client running firmware version 5.02.20 or later discovers and reports another access point in the wireless network that has failed LEAP or EAP-FAST authentication.

The process takes place as follows:

1. A client with a LEAP or EAP-FAST profile attempts to associate to access point A.
2. Access point A does not handle the LEAP or EAP-FAST authentication successfully, perhaps because the access point does not understand LEAP or EAP-FAST or cannot communicate to a trusted LEAP or EAP-FAST authentication server.
3. The client records the MAC address for access point A and the reason why the association failed.
4. The client associates successfully to access point B.
5. The client sends the MAC address of access point A and the reason code for the failure to access point B.
6. Access point B logs the failure in the system log.



Note

This feature does not need to be enabled on the client adapter or access point; it is supported automatically in both devices. However, the client adapters and access points must use the firmware versions or software releases shown above (or later).

Additional WEP Key Security Features

The three security features discussed in this section (MIC, TKIP, and broadcast key rotation) are designed to prevent sophisticated attacks on your wireless network's WEP keys. These features do not need to be enabled on the client adapter; they are supported automatically in the firmware and driver versions included in the Install Wizard file. However, they must be enabled on the access point.

For instructions on enabling these security features on your access point, refer to the corresponding software configuration guide or the installation and configuration guide available at the following URL:

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



Note

The 340 and 350 series access points require VxWorks 11.10T or later to enable these security features. Refer to the documentation for your access point for instructions on enabling these security features.

Message Integrity Check (MIC)

MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The MIC adds a few bytes to each packet to make the packets tamper-proof.

The Status window indicates if MIC is being used, and the Statistics window provides MIC statistics.

**Note**

If you enable MIC on the access point, your client adapter's driver must support these features; otherwise, the client cannot associate.

Temporal Key Integrity Protocol (TKIP)

This feature, also referred to as *WEP key hashing*, defends against an attack on WEP in which the intruder uses 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. It protects both unicast and broadcast WEP keys.

**Note**

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

**Note**

TKIP is automatically enabled whenever WPA is enabled and disabled whenever WPA is disabled.

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. When you enable this feature, only wireless client devices using LEAP, EAP-TLS, PEAP, or EAP-SIM authentication can associate to the access point. Client devices using static WEP (with open or shared key authentication) cannot associate.

Synchronizing Security Features

In order to use any of the security features discussed in this section, both your client adapter and the access point to which it associates must be set appropriately. [Table 5-1](#) indicates the client and access point settings required for each security feature. Refer to [Chapter 2, "Installed Components Tab Window,"](#) and the ["Security Tab" section on page 4-10](#) for installation and configuration instructions for your client adapter's security features. Refer to the documentation for your access point for instructions on enabling any of these features for your access point.

Table 5-1 Client and Access Point Security Settings

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Enable Static WEP and Open Access Point Authentication and create a WEP key.	Set up and enable WEP and enable Open Authentication for the SSID.
Static WEP with shared key authentication	Enable Static WEP and Shared Key Access Point Authentication and create a WEP key.	Set up and enable WEP and enable Shared Key Authentication for the SSID.

Table 5-1 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
LEAP authentication	Install LEAP security module and enable LEAP.	Set up and enable WEP and enable EAP for the SSID.
LEAP authentication with WPA	Install LEAP security module. Enable WPA and LEAP. Note To enable the client adapter to associate to both WPA and non-WPA access points, enable Allow Association to both WPA and non-WPA authenticators.	Select a cipher suite, set up; and enable WEP, and enable EAP and WPA for the SSID. Note To enable both WPA and non-WPA client adapters to use the SSID, enable optional WPA.
EAP-FAST authentication	Install EAP-FAST security module and enable EAP-FAST.	Set up and enable WEP and enable EAP for the SSID.
EAP-FAST authentication with WPA	Install EAP-FAST security module. Enable WPA and EAP-FAST. Note To enable the client adapter to associate to both WPA and non-WPA access points, enable Allow Association to both WPA and non-WPA authenticators.	Select a cipher suite, set up; and enable WEP, and enable EAP and WPA for the SSID. Note To enable both WPA and non-WPA client adapters to use the SSID, enable optional WPA.
EAP-TLS authentication		
If using ACAT or ACU to configure client adapter	Enable Host Based EAP and Dynamic WEP in ACAT or ACU and in Windows, select Enable network access control using IEEE 802.1X and Certificates (or Smart Card or other Certificate) as the EAP Type.	Set up and enable WEP and enable EAP and Open Authentication for the SSID.
If using Windows XP to configure client adapter	In Windows, select Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP Type.	Set up and enable WEP and enable EAP and Open Authentication for the SSID.

Table 5-1 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
EAP-TLS authentication with WPA		
If using ACAT or ACU to configure client adapter	Enable WPA, Host Based EAP and Dynamic WEP in ACAT or ACU and in Windows, enable WPA or WPA-PSK and select Enable network access control using IEEE 802.1X and Certificates (or Smart Card or other Certificate) as the EAP Type.	Select a cipher suite; set up and enable WEP; and enable EAP, Open Authentication, and WPA for the SSID. Note To enable both WPA and non-WPA client adapters to use the SSID, enable optional WPA.
If using Windows XP to configure client adapter	In Windows, enable WPA or WPA-PSK and select Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP Type.	Select a cipher suite; set up and enable WEP; and enable EAP, Open Authentication, and WPA for the SSID. Note To enable both WPA and non-WPA client adapters to use the SSID, enable optional WPA.
PEAP authentication		
If using ACAT or ACU to configure client adapter	Install PEAP security module. Enable Host Based EAP and Dynamic WEP in ACAT or ACU and in Windows, select Enable network access control using IEEE 802.1X and PEAP as the EAP Type.	Set up and enable WEP and enable EAP and Open Authentication for the SSID.
If using Windows XP to configure client adapter	In Windows, select Enable network access control using IEEE 802.1X and PEAP as the EAP Type.	Set up and enable WEP and enable EAP and Open Authentication for the SSID.
PEAP authentication with WPA		
If using ACAT or ACU to configure client adapter	Enable WPA, Host Based EAP and Dynamic WEP in ACAT or ACU and in Windows, enable WPA or WPA-PSK and select Enable network access control using IEEE 802.1X and PEAP as the EAP Type.	Select a cipher suite; set up and enable WEP; and enable EAP and Open Authentication, and WPA for the SSID. Note To enable both WPA and non-WPA client adapters to use the SSID, enable optional WPA.

Table 5-1 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
If using Windows XP to configure client adapter	In Windows, enable WPA or WPA-PSK and select Enable network access control using IEEE 802.1X and PEAP as the EAP Type.	Select a cipher suite; set up and enable WEP; and enable EAP and Open Authentication, and WPA for the SSID. Note To enable both WPA and non-WPA client adapters to use the SSID, enable optional WPA.
EAP-SIM authentication		
If using ACAT or ACU to configure client adapter	Install EAP-SIM security module. Enable Host Based EAP and Dynamic WEP in ACAT or ACU and in Windows, select Enable network access control using IEEE 802.1X (or Enable IEEE 802.1X authentication for the network) and SIM Authentication as the EAP Type.	Set up and enable WEP and enable EAP and Open Authentication for the SSID.
If using Windows XP to configure client adapter	In Windows, select Enable network access control using IEEE 802.1X and SIM Authentication as the EAP Type.	Set up and enable WEP and enable EAP and Open Authentication for the SSID.
EAP-SIM authentication with WPA		
If using ACAT or ACU to configure client adapter	Install EAP-SIM security module. Enable WPA, Host Based EAP and Dynamic WEP in ACAT or ACU and in Windows, enable WPA or WPA-PSK and select Enable network access control using IEEE 802.1X (or Enable IEEE 802.1X authentication for the network) and SIM Authentication as the EAP Type.	Select a cipher suite; set up and enable WEP; and enable EAP, Open Authentication, and WPA for the SSID. Note To enable both WPA and non-WPA client adapters to use the SSID, enable optional WPA.
If using Windows XP to configure client adapter	In Windows, enable WPA or WPA-PSK and select Enable network access control using IEEE 802.1X and SIM Authentication as the EAP Type.	Select a cipher suite; set up and enable WEP; and enable EAP, Open Authentication, and WPA for the SSID. Note To enable both WPA and non-WPA client adapters to use the SSID, enable optional WPA.

Table 5-1 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
Fast roaming (CCKM)	Enable LEAP and select Allow Fast Roaming (CCKM).	Use Cisco IOS Release 12.2(11)JA or later, select a cipher suite, and enable EAP and CCKM for the SSID. Note To enable both WPA and non-WPA client adapters to use the SSID, enable optional WPA.
Reporting access points that fail LEAP authentication	No settings required; automatically enabled in firmware version 5.02.20 or later.	No settings required; automatically enabled in the following software releases: <ul style="list-style-type: none"> VxWorks release 12.00T or later (340, 350, and 1200 series access points) Cisco IOS Release 12.2(4)JA or later
MIC	No settings required; automatically enabled by the firmware included in the Install Wizard file.	Set up and enable WEP with full encryption, set MIC to MMH, and set Use Aironet Extensions to Yes.
TKIP	No settings required; automatically enabled by the firmware included in the Install Wizard file.	Set up and enable WEP, set TKIP to Cisco, and set Use Aironet Extensions to Yes.
Broadcast key rotation	Enable LEAP, EAP-TLS, PEAP or EAT-SIM and use the firmware included in the Install Wizard file.	Set up and enable WEP and set Broadcast WEP Key Rotation Interval to any value other than zero (0).
Reporting access points that fail LEAP authentication	No settings required; automatically enabled in firmware version 5.02.17 or later.	No settings required; automatically enabled in the following software releases: <ul style="list-style-type: none"> VxWorks release 12.00T or later (340, 350, and 1200 series access points) Cisco IOS Release 12.2(4)JA or later
Fast secure roaming	Enable LEAP and use firmware version 5.20.17 or later.	Use Cisco IOS Release 12.2(11)JA or later, select a cipher suite, and enable open authentication with EAP or CCKM. Note To enable both 802.1X clients and non 802.1X clients to use the SSID, enable optional CCKM.



Install Wizard Command Line Options

This appendix describes the Install Wizard 1.6 (IWSetup.exe) command line options, which can be used by system administrators to make the Install Wizard more usable in batch processes.

The following topics are covered in this appendix:

- [Command Line Options, page A-2](#)
- [Sample Application, page A-3](#)

Command Line Options

Install Wizard 1.6 supports these command line options. For most installations, they are intended to be run from an MS-DOS window in the C:\WINNT\Cisco\DInstall directory (on Windows 2000) or the C:\WINDOWS\Cisco\DInstall directory (on Windows XP).



Note

These commands are intended to be used only by system administrators.

- **/noclean**—Causes the installation files to remain on the computer after the client adapter software has been uninstalled. This command is typically used in conjunction with the */uninstall* command as shown in this example:

```
IWSetup /uninstall /noclean
```

This command line sequence removes the client utilities, driver, and firmware but leaves the installation files in the C:\WINNT or WINDOWS\Cisco\DInstall directory. After the uninstall process completes, the Install Wizard configuration binary file (CiscoAdminConfig.dat) can be replaced with a new binary file containing different installation options, and the Install Wizard can be rerun.

- **/noreboot**—Suppresses the Install Wizard reboot prompt. This command can be used during the installation or uninstall process, but it must be used in conjunction with the */silent* command as shown in these examples:

```
IWSetup /noreboot /silent
IWSetup /uninstall /noreboot /silent
```

These command line sequences allow a batch process to continue after the installation or uninstall process has completed. They rewrite the Install Wizard configuration binary file (CiscoAdminConfig.dat). Therefore, all subsequent Install Wizard operations do not prompt for a reboot until the binary file is replaced or rewritten.



Note

The *IWSetup /noreboot /silent* command line sequence has the same effect as the *Global Override Settings - Silent Setup Options - Do not reboot* setting in the Cisco Aironet Configuration Administration Tool (ACAT).

- **/silent**—Causes a process to behave silently with no user interaction required. It is typically used to guide the installation or uninstall process as shown in these examples:

```
IWSetup /silent
IWSetup /uninstall /silent
```

These command line sequences silently install or uninstall the client adapter software. They rewrite the Install Wizard configuration binary file (CiscoAdminConfig.dat). Therefore, all subsequent Install Wizard operations do not require user interaction until the binary file is replaced or rewritten.



Note



The client utility and driver installation screens appear, but the Install Wizard dialog is suppressed.

- **/uninstall**—Uninstalls the client adapter software. This command allows an uninstall to be performed as a batch operation. It is typically used with the */silent* command as shown in this example:

```
IWSetup /uninstall /silent
```

Sample Application

This sample procedure illustrates how the command line options could be used in an IT scenario. In this example, the objective is to remove the Cisco Aironet client utilities and the Gina file and replace them with third-party elements that use the Cisco Aironet drivers. Ordinarily this would be accomplished by uninstalling the client adapter software and reinstalling only the driver and firmware. However, the command line options enable the administrator to perform this operation as a batch process.

-
- Step 1** Install or upgrade to Install Wizard 1.6.
- Step 2** After the installation completes, run **IWSetup /uninstall /noreboot /noclean** from an MS-DOS window in the C:\WINNT or WINDOWS\Cisco\DIInstall directory. This command line sequence uninstalls the client adapter software but leaves the installation files.
-  **Note** The */noreboot* command suppresses the normal reboot prompt, and the */noclean* command leaves the installation files in the C:\WINNT or WINDOWS\Cisco\DIInstall directory.
-
- Step 3** Reboot the computer.
-  **Note** If a client adapter is inserted in the computer, ignore or cancel any prompts asking for the location of the driver.
-
- Step 4** Use ACAT to generate a configuration binary file (CiscoAdminConfig.dat) that installs only the driver and firmware.
- Step 5** Copy this configuration binary file to the C:\WINNT or WINDOWS\Cisco\DIInstall directory. This ACAT-generated file replaces the old Install Wizard configuration binary file.
- Step 6** Run **IWSetup /silent** from an MS-DOS window in the C:\WINNT or WINDOWS\Cisco\DIInstall directory and reboot. When the installation completes, only the Cisco Aironet client adapter driver and firmware are installed.
- Step 7** Install the desired third-party software.
-



- 802.11** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs operating in the 2.4-GHz band.
- 802.11a** The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 5-GHz frequency band.
- 802.11b** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps wireless LANs operating in the 2.4-GHz frequency band.

A

- access point** A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.
- ad hoc network** A wireless network composed of stations without access points.
- antenna gain** The gain of an antenna is a measure of the antenna's ability to direct or focus radio energy over a region of space. High gain antennas have a more focused radiation pattern in a specific direction.
- associated** A station is configured properly to allow it to wirelessly communicate with an Access Point.

B

- beacon** A wireless LAN packet that signals the availability and presence of the wireless device. Beacon packets are sent by access points and base stations; however, client radio cards send beacons when operating in computer to computer (Ad Hoc) mode.
- BOOTP** Boot Protocol. A protocol used for the static assignment of IP addresses to devices on the network.
- BPSK** A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mbps.
- broadcast packet** A single data message (packet) sent to all addresses on the same subnet.

C

- CCK** Complementary Code Keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.

cell	The area of radio range or coverage in which the wireless devices can communicate with the base station. The size of the cell depends upon the speed of the transmission, the type of antenna used, and the physical environment, as well as other factors.
client	A radio device that uses the services of an access point to communicate wirelessly with other devices on a local area network.
CSMA	Carrier Sense Multiple Access. A wireless LAN media access method specified by the IEEE 802.11 specification.

D

data rates	The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).
dBi	A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain, and the more acute the angle of coverage.
DHCP	Dynamic Host Configuration Protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.
dipole	A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.
domain name	The text name that refers to a grouping of networks or network resources based on organization-type or geography; for example: name.com—commercial; name.edu—educational; name.gov—government; ISPname.net—network provider (such as an ISP); name.ar—Argentina; name.au—Australia; and so on.
DNS	Domain Name System server. A server that translates text names into IP addresses. The server maintains a database of host alphanumeric names and their corresponding IP addresses.
DSSS	Direct Sequence Spread Spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

E

- EAP** Extensible Authentication Protocol. An optional IEEE 802.1x security feature ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server.
- Ethernet** The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to allow computers to share a network and operates at 10, 100, or 1000 Mbps, depending on the physical layer used.

F

- file server** A repository for files so that a local area network can share files, mail, and programs.
- firmware** Software that is programmed on a memory chip.

G

- gateway** A device that connects two otherwise incompatible networks together.
- GHz** Gigahertz. One billion cycles per second. A unit of measure for frequency.

I

- IEEE** Institute of Electrical and Electronic Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.
- infrastructure** The wired Ethernet network.
- IP address** The Internet Protocol (IP) address of a station.
- IP subnet mask** The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway. This number is expressed in a form similar to an IP address; for example: 255.255.255.0.
- Isotropic** An antenna that radiates its signal in a spherical pattern.

M

- MAC** Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device, such as an access point or your client adapter.
- modulation** Any of several techniques for combining user information with a transmitter's carrier signal.

multipath The echoes created as a radio signal bounces off of physical objects.

multicast packet A single data message (packet) sent to multiple addresses.

O

omni-directional This typically refers to a primarily circular antenna radiation pattern.

Orthogonal Frequency Division Multiplex (OFDM) A modulation technique used by IEEE 802.11a-compliant wireless LANs for transmission at 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

P

packet A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

Q

Quadruple Phase Shift Keying A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 2 Mbps.

R

range A linear measure of the distance that a transmitter can send a signal.

receiver sensitivity A measurement of the weakest signal a receiver can receive and still correctly translate it into data.

RF Radio Frequency. A generic term for radio-based technology.

roaming A feature of some access points that allows users to move through a facility while maintaining an unbroken connection to the LAN.

RP-TNC A connector type unique to Cisco Aironet radios and antennas. Part 15.203 of the FCC rules covering spread spectrum devices limits the types of antennas that may be used with transmission equipment. In compliance with this rule, Cisco Aironet, like all other wireless LAN providers, equips its radios and antennas with a unique connector to prevent attachment of non-approved antennas to radios.

S

- spread spectrum** A radio transmission technology that spreads the user information over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.
- SSID** Service Set Identifier (also referred to as Radio Network Name). A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

T

- transmit power** The power level of radio transmission.

U

- UNII** Unlicensed National Information Infrastructure—regulations for UNII devices operating in the 5.15 to 5.35 GHz and 5.725 to 5.825 GHz frequency bands.
- UNII-1** Regulations for UNII devices operating in the 5.15 to 5.25 GHz frequency band.
- UNII-2** Regulations for UNII devices operating in the 5.25 to 5.35 GHz frequency band.
- UNII-3** Regulations for UNII devices operating in the 5.725 to 5.825 GHz frequency band.
- unicast packet** A single data message (packet) sent to a specific IP address.

W

- WEP** Wired Equivalent Privacy. An optional security mechanism defined within the 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable.
- workstation** A computing device with an installed client adapter.



Numerics

- 802.1X
 - authentication types in ACU [5-3](#)
 - defined [5-3](#)

A

ACAT

- client adapters supported [1-2](#)
- help [1-5](#)
- obtaining software [1-3](#)
- operating systems supported [1-2](#)
- overview [1-2](#)
- security options [1-6](#)

access point

- MAC address, specifying [4-33](#)
- security settings [5-9 to 5-13](#)

ACU

- permitting non-administrator use [2-4](#)
- ad hoc network parameters [4-35](#)
- Allow Association To Mixed Cells parameter [4-14](#)
- Antenna Mode (Receive) parameter
 - infrastructure mode [4-27](#)
- Antenna Mode (Transmit) parameter
 - infrastructure mode [4-27](#)
- audience [viii](#)
- authentication process [5-6](#)
- Automatically Prompt for LEAP User Name and Password option [4-19, 4-23](#)
- auto profile selection [2-6, 4-38](#)
- auto provisioning [4-12](#)

B

- Beacon Period parameter [4-37](#)
- broadcast key rotation
 - described [5-9](#)
 - setting on client and access point [5-13](#)

C

- card type, defined [4-5](#)
- carrier/correlation (Car/Cor) [4-30](#)
- Caution, defined [viii](#)
- channel
 - determining if clear [4-30](#)
- Cisco Centralized Key Management (CCKM)
 - defined [5-7](#)
 - enabling [4-13](#)
- Clear Channel Assessment parameter [4-30](#)
- command line options, Install Wizard 1.6 [A-2](#)
- configuration file, ACAT [1-6](#)
- configuration tabs [1-5](#)
- conventions [viii](#)
- create profiles [4-2](#)

D

- Data Rate parameter, in RF network [4-28](#)
- Data Retries parameter, in RF network [4-31](#)
- dat file [1-6](#)
- diversity mode [4-27](#)
- document organization [viii](#)
- drivers, client adapter [2-3](#)
- dynamic WEP keys, overview [5-3 to 5-6](#)

E

- EAP authentication overview [5-3 to 5-6](#)
- EAP-FAST authentication
 - described [5-3](#)
 - enabling [4-12, 4-20 to 4-24](#)
 - RADIUS servers supported [5-3](#)
 - setting on client and access point [5-10](#)
 - username and password [4-22](#)
- EAP-SIM authentication
 - described [5-5 to 5-6](#)
 - setting on client and access point [5-12](#)
- EAP-SIM parameter [2-8](#)
- EAP-TLS authentication
 - described [5-4 to 5-6](#)
 - enabling [4-24](#)
 - RADIUS servers supported [5-4](#)
 - setting on client and access point [5-10, 5-11](#)
- energy detect (ED) [4-30](#)
- existing profiles [3-4](#)
- export profiles [3-3](#)

F

- fast roaming
 - defined [5-7](#)
 - enabling [4-13](#)
- File menu [1-5](#)
- firmware [2-3](#)
- fragmented packets [4-31](#)
- Fragment Threshold parameter [4-31](#)

H

- host-based EAP
 - enabling [4-24](#)

I

- import profiles [3-3, 4-2](#)
- Include Windows Login Domain With User Name parameter [4-19, 4-23](#)
- infrastructure network parameters [4-32](#)

L

- LEAP authentication
 - described [5-3, 5-6](#)
 - RADIUS servers supported [5-3](#)
- LEAP Authentication Timeout Value parameter [4-19](#)
- LEAP option [2-7, 4-17](#)
- LEAP Settings screen [4-18](#)
- Log File [3-3](#)
- long radio headers, using [4-30](#)

M

- MAC address
 - of access point, specifying [4-33](#)
- Manually Prompt for LEAP User Name and Password option [4-19, 4-23](#)
- message integrity check (MIC)
 - described [5-8](#)
 - setting on client and access point [5-13](#)

N

- network security parameters
 - described [4-10](#)
- new profiles, adding [4-3](#)
- No Network Connection Unless User is Logged In parameter [4-19, 4-23](#)
- Note, defined [viii](#)

O

open authentication [4-14](#)

P

packets

- beacon [4-37](#)
- fragmented [4-31](#)
- RTS [4-34, 4-36](#)

parameters

- ACM [2-5](#)
- ACU [2-4](#)
- Global Override [3-3](#)
- LEAP [2-7](#)
- PEAP [2-8](#)

paramters

- EAP-SIM [2-8](#)

PC card antenna [4-27](#)

PCI card antenna [4-27](#)

PEAP [2-8](#)

PEAP authentication

- described [5-5 to 5-6](#)
- RADIUS servers supported [5-5](#)
- setting on client and access point [5-11](#)

Protected EAP

- See PEAP authentication

R

RADIUS servers

- additional information [5-6](#)
- defined [5-3](#)
- supported [5-3](#)

range [4-28](#)

removing

- ACAT software [1-7](#)
- installed software components [1-7](#)

RTS packets

- advanced ad hoc parameters [4-36](#)
- advanced infrastructure parameters [4-34](#)

RTS Retry Limit parameter

- ad hoc mode [4-36](#)
- infrastructure mode [4-34](#)

RTS Threshold parameter

- ad hoc mode [4-36](#)
- infrastructure mode [4-34](#)

S

saved username and password

- described [4-18, 4-22](#)

security features

- overview [5-9](#)
- synchronizing [5-9 to 5-13](#)

shared key authentication [4-15](#)

short radio headers, using [4-30](#)

silent setup [3-4](#)

Specified Access Point 1- 4 parameters [4-33](#)

static WEP

- disabling [4-16](#)
- procedures [4-15, 4-16](#)
- with open authentication [5-9](#)
- with shared key authentication [5-9](#)

static WEP keys

- entering [4-15](#)
- guidelines for entering, in ACU [4-16](#)
- overview [5-2](#)
- selecting transmit key [4-16](#)
- size of [4-15](#)

T

tab

- Ad Hoc [4-35](#)
- Connection [4-6](#)
- Global Override Settings [3-1](#)
- Infrastructure [4-32](#)
- Installed Components [2-2](#)
- Profiles [4-39](#)
- Profile Settings [4-4](#)
- RF Settings [4-26](#)
- Security [4-10](#)

Temporal Key Integrity Protocol (TKIP)

- described [5-9](#)
- setting on client and access point [5-13](#)

temporary username and password

- automatically prompt for [4-19, 4-23](#)
- described [4-18, 4-22](#)
- manually prompt for [4-19, 4-23](#)
- selecting options [4-19, 4-23](#)
- using Windows credentials [4-19, 4-23](#)

throughput [4-28, 4-30, 4-31](#)transmit key [4-16](#)Transmit Power parameter [4-29](#)

UUse Saved User Name and Password option [4-18, 4-22](#)Use Short Radio Headers parameter [4-30](#)Use Temporary User Name and Password option [4-18, 4-22](#)Use Windows User Name and Password option [4-19, 4-23](#)

WWake Duration parameter [4-36](#)WEP [3-3](#)

keys

- additional security features [5-8 to 5-9](#)
- defined [5-2](#)
- size of [5-2](#)
- types of [5-2](#)

WEP Key Entry Method parameter [4-15](#)WEP key hashing [5-9](#)World Mode parameter [4-31](#)

WPA authentication

- defined [5-6](#)
- enabling [4-11](#)