Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Administration Utility Administrator Guide

Software Release 4.0

Americas 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: 408 527-0883

Text Part Number: OL-7086-05

CONTENTS

Preface

The preface provides an overview of this guide, references related publications, and explains how to obtain other documentation and technical assistance.

The following topics are covered in this section:

Audience

This publication is for the administrator responsible for installing and configuring Cisco Aironet IEEE 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) in multiple PCs. The installer should be familiar with computing devices and with network structures, terms, and concepts.

Purpose

This publication describes version 4.0 of the Cisco Aironet CB21AG and PI21AG Client Administration Utility (hereafter referred to as *ACAU*). It provides instructions for installing ACAU and using it to set software installation options and create configuration profiles for CB21AG and PI21AG client adapters on computers running Windows 2000 or XP.

Note Windows 2000 and XP are the only supported operating systems.

Note This manual pertains specifically to Cisco Aironet CB21AG and PI21AG client adapters, whose software is incompatible with that of other Cisco Aironet client adapters. Refer to the *Cisco Aironet Configuration Administration Tool (ACAT) Administrator Guide for Windows* if you are installing and using the administrative tool designed for 340, 350, and CB20A client adapters.

Organization

This guide contains the following sections:

Chapter 1, "Overview," provides an introduction to ACAU, describes the ACAU components and configuration file, and identifies the supported client adapters.

Chapter 2, "Installing ACAU," describes how to obtain, install, run, and uninstall ACAU.

Chapter 3, "Using ACAU," describes how to use ACAU to create or modify configuration files and manage profiles.

Chapter 4, "Configuring Global Settings," describes the Global Settings tab parameters and how to configure them to override the client adapter's software installation settings.

Chapter 5, "Creating Profiles," explains how to use ACAU to create profiles that are saved to a configuration file and installed by the Install Wizard when a user installs the client adapter software.

Appendix A, "Declarations of Conformity and Regulatory Information," provides declarations of conformity and regulatory information for the CB21AG and PI21AG client adapters.

Appendix B, "Channels, Power Levels, and Antenna Gains" lists the IEEE 802.11a, b, and g channels supported by the world's regulatory domains as well as the maximum power levels and antenna gains allowed per data rate.

Appendix C, "Error Messages" lists error messages generated by ACAU. This appendix explains each message and provides a recommended action.

Appendix D, "Using the Profile Migration Tool," explains how to use the profile migration tool to migrate Cisco Aironet 350 series and CB20A wireless LAN client adapter profiles to profiles that can be used with Cisco Aironet CB21AG and PI21AG client adapters.

Conventions

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

- Commands are in **boldface** type.
- Variables are in *italic* type.
- Notes and cautions use the following conventions and symbols:

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 Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters, refer to these publications:

- *Quick Start Guide: Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG)*—Provides basic setup instructions and minimal configuration information for CB21AG and PI21AG client adapters.
- *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide*—Provides instructions for installing, configuring, and troubleshooting CB21AG and PI21AG client adapters on computers running the Microsoft Windows 2000 or XP operating system.
- *Release Notes for Cisco Aironet 802.11a/b/g Client Adapters (CB21AG and PI21AG) Install Wizard*—Describes new features and the open and resolved caveats in each Install Wizard release.
- *Release Notes for Cisco Aironet 802.11a/b/g (CB21AG and PI21AG) Client Administration Utility (ACAU)*—Describes new features and the open and resolved caveats in each ACAU release.

You can find these Cisco Aironet technical documents at this URL:

http://www.cisco.com/en/US/products/hw/wireless/ps4555/tsd_products_support_series_home.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Overview

This chapter provides an overview of the Cisco Aironet Client Administration Utility *(*ACAU).

The following topics are covered in this chapter:

Introduction to ACAU

ACAU is a utility used by administrators to set software installation options and create *profiles* (saved configurations) for users who install Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters in computers running the Windows 2000 or Windows XP operating system. Administrators save the installation settings and profiles to a configuration file. Then when the user installs the client adapter software (driver and client utilities), the Install Wizard uses the instructions in the configuration file to govern the installation and setup of the client utilities and load one or more preconfigured user profiles. Administrators can create configuration files to control the installation and configuration of client adapters for one user or groups of users.

Note To ensure proper operation, use ACAU version 2.5 only with Install Wizard version 2.5.

Terminology

The following terms are used throughout this document:

- **client adapter**—Refers to both types of adapters.
- **client adapter software**—Refers to the client adapter driver and client utilities that are installed by the Install Wizard. The client utilities include the Aironet Desktop Utility (ADU), Aironet System Tray Utility (ASTU), site survey utility, and profile migration tool.

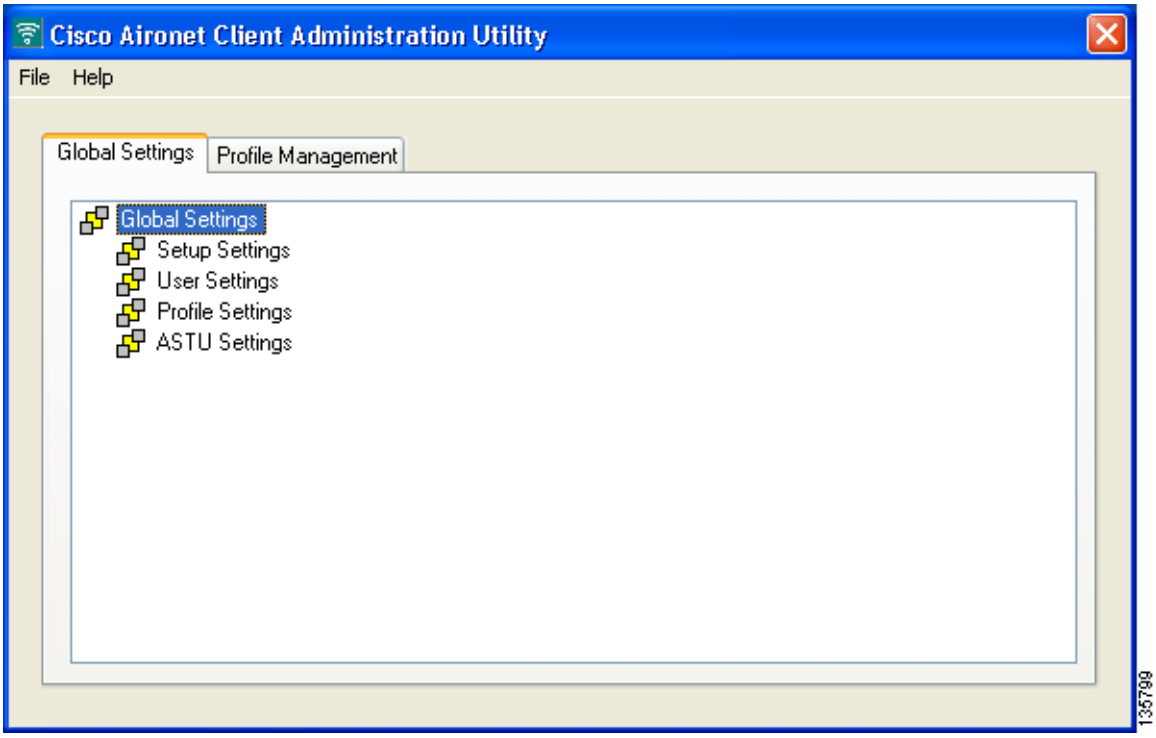
  Note Refer to the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for more information on the Install Wizard, the client adapter driver, and the client utilities.

- **infrastructure device**—Refers to a device that connects client adapters to a wired LAN, such as an access point, bridge, or base station. Throughout this document, *access point* is used to represent infrastructure devices in general.
- **PC-Cardbus card** or **PCI card**—Refers to a specific client adapter.

ACAU Components

Figure 1-1 shows the ACAU main window. ACAU contains two configuration tabs and two drop-down menus.

Figure 1-1 ACAU Main Window



ACAU Configuration Tabs

The ACAU main window provides two configuration tabs: Global Settings and Profile Management.

Global Settings Tab

The Global Settings tab enables you to set parameters that govern the installation and configuration of the client adapter software installed by the Install Wizard. It contains four groups of parameters:

- **Setup Settings**—Affect how the client adapter software is installed and configured on the user's computer
- **User Settings**—Specify user rights and privileges with regard to profiles
- **Profile Settings**—Control how profiles are managed on the user's computer
- **ASTU Settings**—Determine the Aironet System Tray Utility (ASTU) options that are available to the user

Note Chapter 4 describes the Global Settings tab parameters and explains how to configure them.

Profile Management Tab

The Profile Management tab enables you to create configuration profiles that govern the operation of the user's client adapter. This tab can also be used to modify, import, and export profiles.

Note Chapter 5 explains how to use the Profile Management tab to create, modify, import, and export profiles.

ACAU Menus

The ACAU main window provides two drop-down menus: File and Help.

File Menu

The File drop-down menu contains these options:

- **New**—Creates a new ACAU configuration file.
- **Open**—Opens an existing ACAU configuration file.
- **Save**—Saves the ACAU configuration file.
- **Save As**—Saves the ACAU configuration file to a specified location.
- **Read from registry**—Imports existing profiles from your computer's Windows registry.
- **Exit**—Closes ACAU.

Help Menu

The Help drop-down menu contains these options:

- **Contents**—Provides help on ACAU options and settings.

  Note Context-sensitive help is not available in ACAU.

- **About**—Provides the ACAU version number.

Configuration File

The configuration file stores the installation options that you set on the Global Settings tab and the profiles that you create on the Profile Management tab. The file is encrypted to protect sensitive security data such as SSIDs, WEP keys, and network security settings.

ACAU automatically names the configuration file *CiscoAdminConfig.dat* and prompts you to save it in the Cisco Aironet folder. When the user installs the client adapter software, the Install Wizard uses the configuration file to implement the installation settings and load the profiles you specified in ACAU.

Note You can create the configuration file before or after setting installation options and creating profiles; however, creating the configuration file first is the preferred method.

Note You must save the configuration file to the drive and directory in which the Install Wizard resides. If you save the file to any other location, it is not processed by the Install Wizard.

Note You can change the name of the configuration file; however, the name must be changed back to *CiscoAdminConfig.dat* before running the Install Wizard. Otherwise, the Install Wizard does not load the configuration file.

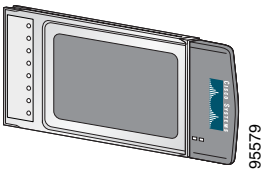
Note Chapter explains how to create new configuration files and modify existing configuration files.

Products Supported

ACAU supports these products:

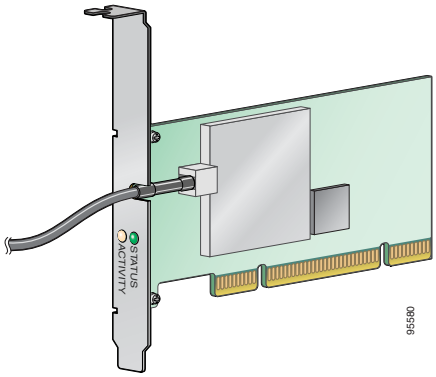
- **PC-Cardbus card** (model number: AIR-CB21AG)—An IEEE 802.11a/b/g-compliant 2.4- and 5-GHz 54-Mbps client adapter card radio module with a Cardbus interface that can be inserted into any device equipped with a 32-bit Cardbus slot. See Figure 1-2.

Figure 1-2 PC-Cardbus Card



- **PCI card** (model number: AIR-PI21AG)—An IEEE 802.11a/b/g-compliant 2.4- and 5-GHz 54-Mbps client adapter card radio module that can be inserted into any device equipped with an empty PCI expansion slot. See Figure 1-3.

Figure 1-3 PCI Card



Caution ACAU is compatible only with Cisco Aironet CB21AG and PI21AG client adapters. Other administration utilities are available for use with the Cisco Aironet 340, 350, and CB20A client adapters.

CHAPTER 2

Installing ACAU

This chapter provides instructions for obtaining, installing, and running ACAU.

The following topics are covered in this chapter:

Obtaining ACAU

Follow these steps to obtain the latest ACAU software from Cisco.com:

Step 1 Make sure the client adapter is inserted into your computer.

Step 2 Make sure that you have a Cisco Connection Online (CCO) username and password.

Step 3 If you do not have a CCO username and password, go to Cisco's main page (http://www.cisco.com) and click Register (top). Then, follow the instructions to create a CCO username and password.

Step 4 Browse to the following location:

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

Step 5 Click **Wireless Software**.

Step 6 Click **Wireless LAN Access**.

Step 7 Click **Cisco Wireless LAN Client Adapters**.

Step 8 Click **Cisco Aironet Wireless LAN Client Adapters Tools For Systems Administrators**.

Step 9 Click **Cisco Aironet CB21AG/PI21AG Wireless LAN Client Adapter Tools**.

Step 10 When prompted, enter your CCO username and password, and click **OK**.

Step 11 Click **Aironet Client Administration Utility (ACAU)**.

Step 12 Click the link with the greatest release number under Available Releases.

Step 13 Click the Install Wizard file (**acau-v*xx*.exe**), where ***xx*** is the version number.

Step 14 If prompted, enter your CCO username and password, and click **OK**.

Step 15 Complete the encryption authorization form, read and accept the terms and conditions of the Software License Agreement.

Step 16 In the Download page, click the **Download** button to download the installer, and save it on your computer's Desktop.

Before downloading the file, you will be prompted to enter your CCO username and password. You will also be prompted to agree to the software download rules.

Installing ACAU

Follow these steps to install ACAU on your computer for the first time:

Note If you are upgrading to a new version of ACAU or reinstalling the same version, follow the instructions in the "Upgrading ACAU" section on page 2-7 to upgrade or reinstall your ACAU software.

Step 1 Use Windows Explorer to find the installer.

Step 2 Double-click the installer.

The Preparing Setup window appears followed by the InstallShield Wizard window (see Figure 2-1 and Figure 2-2).

Figure 2-1 Preparing Setup Window

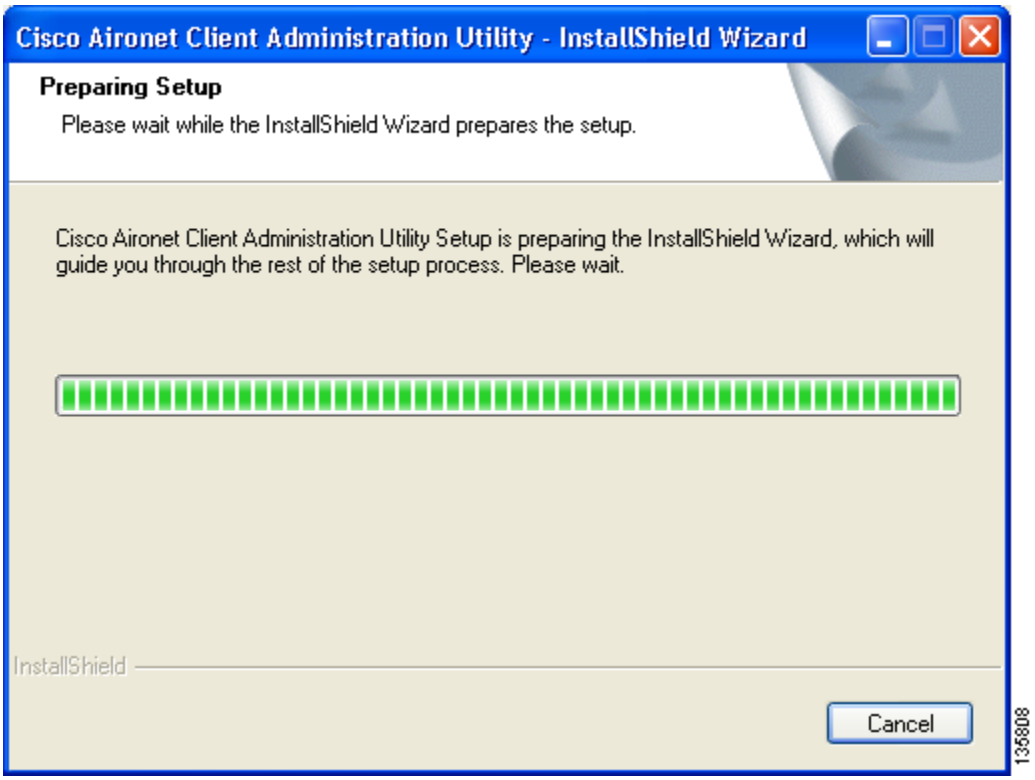
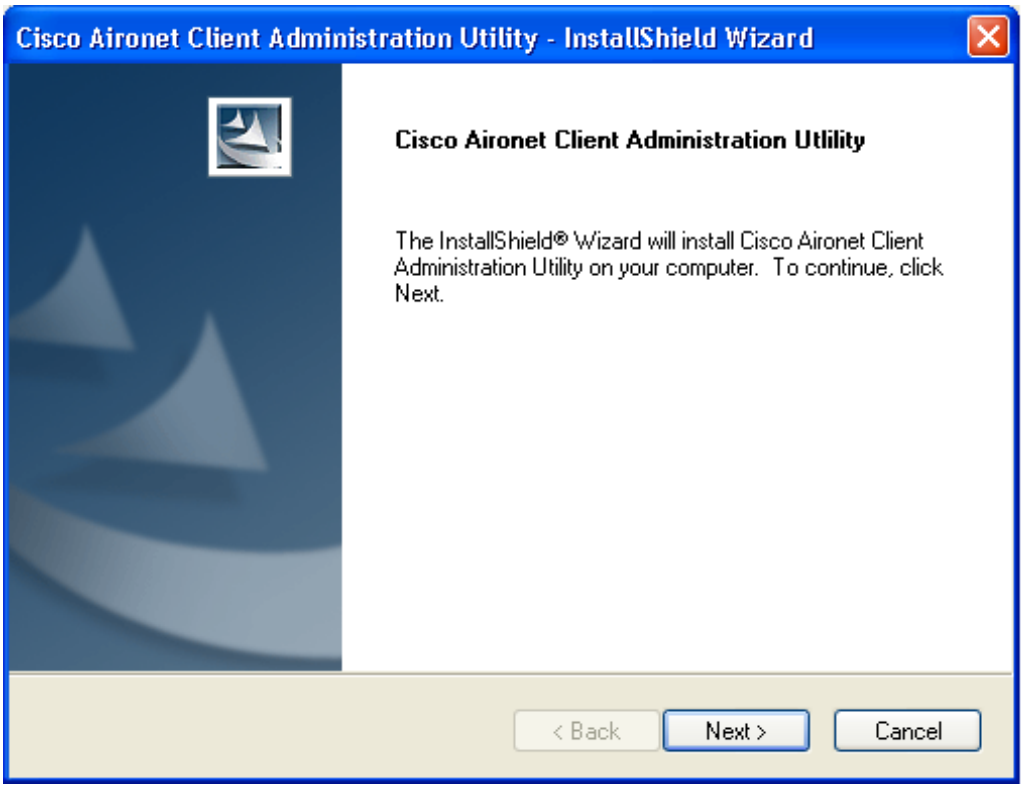
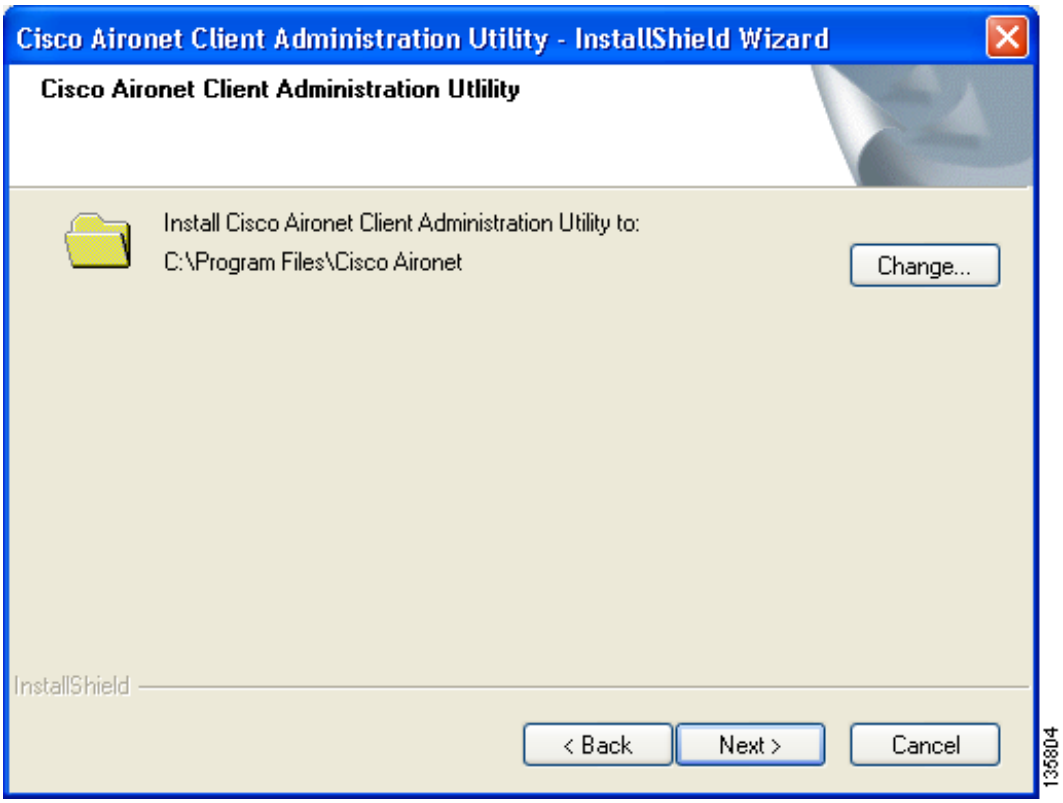


Figure 2-2 InstallShield Wizard Window



Step 3 Click **Next**. The Installation Location window appears showing the default location where ACAU will be installed (see Figure 2-3).

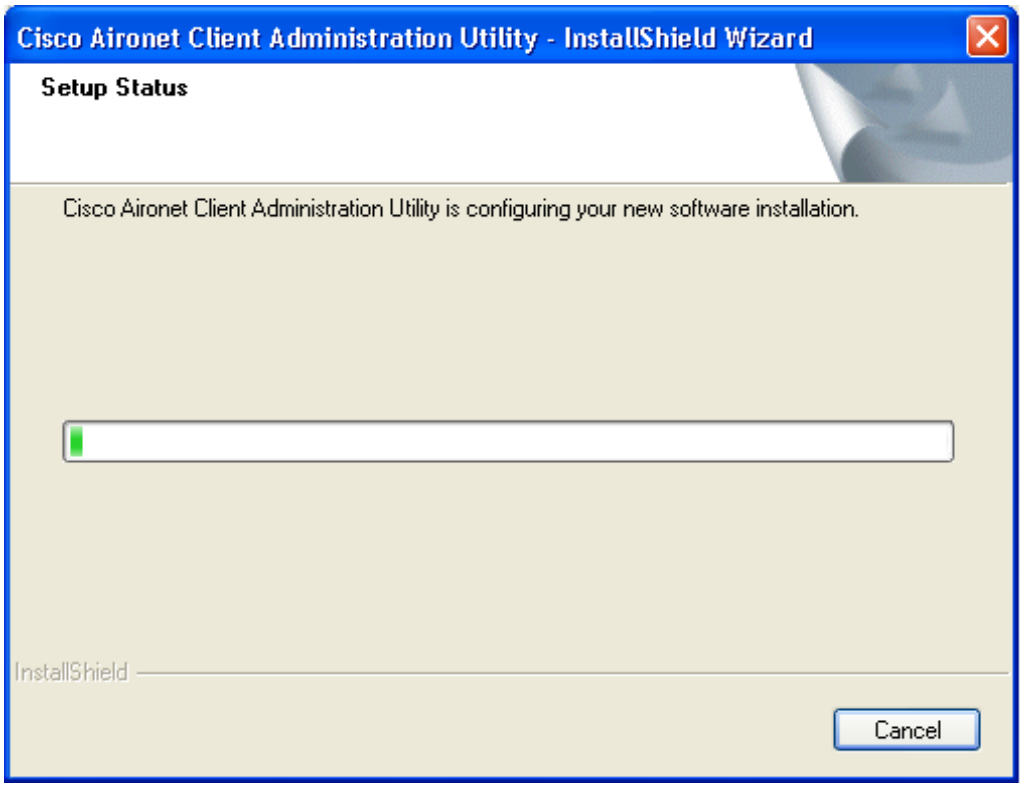
Figure 2-3 Installation Location Window



Step 4 If you want to change the default location, click **Change**, browse to the location of your choice, and click **OK**.

Step 5 Click **Next** to begin the installation process. The Setup Status window appears (see Figure 2-4).

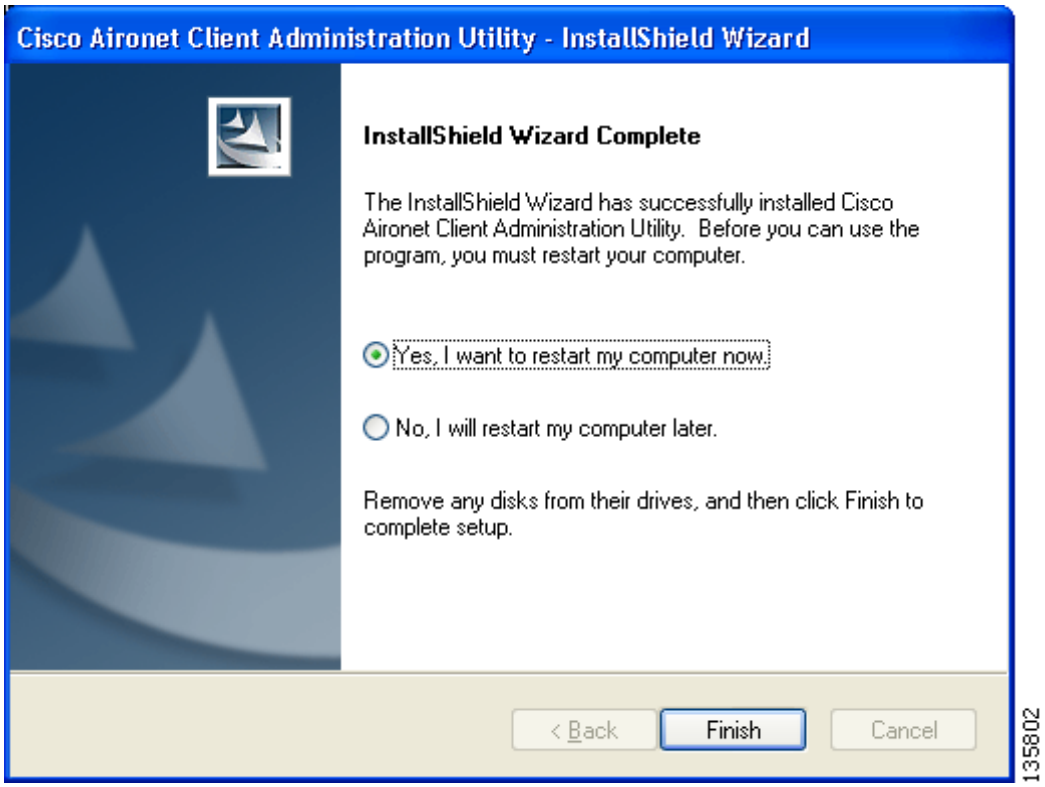
Figure 2-4 Setup Status Window



The installation process begins, and you are notified as each software component is installed.

Step 6 When ACAU is installed, the InstallShield Wizard Complete window appears (see Figure 2-5).

Figure 2-5 InstallShield Wizard Complete Window



Step 7 Click **Yes, I want to restart my computer now** to restart your computer after quitting the installer. Otherwise, click **No, I will restart my computer later** if need to install other programs before restarting your computer.

Note Before you can use ACAU, you must restart you computer.

Step 8 Click **Finish**. The installation is complete.

Upgrading ACAU

Follow these steps to upgrade your ACAU software to the latest ACAU release:

Step 1 Run the ACAU installer.

The Preparing Setup window appears followed by the Previous Installation Detected window (see Figure 2-6 and Figure 2-7).

Figure 2-6 Preparing Setup Window

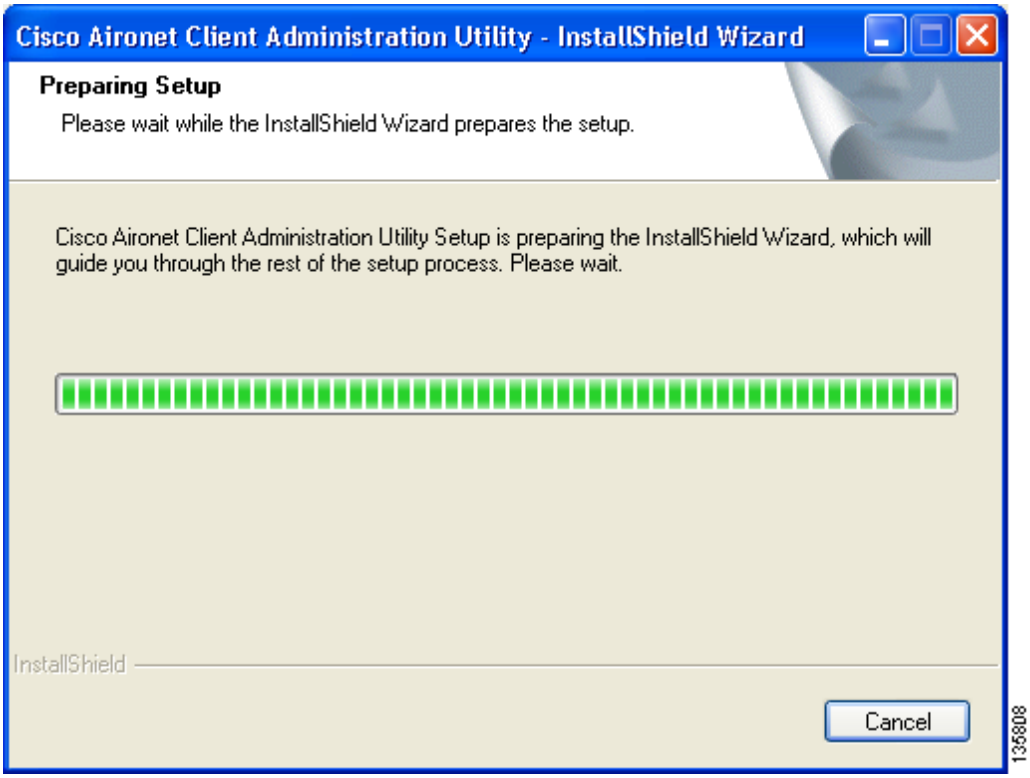
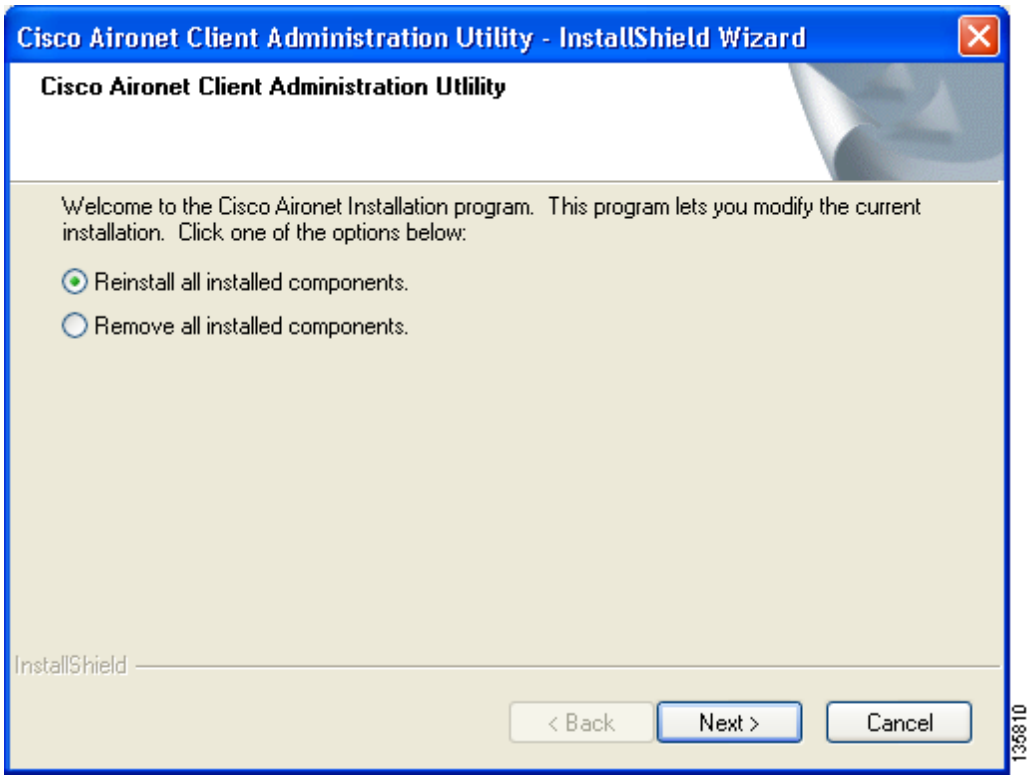


Figure 2-7 Previous Installation Detected Window



Step 2 Perform one of the following:

- If you want to upgrade your ACAU software using new installation settings, you must first uninstall the existing ACAU software from your computer. Follow these steps to do so:
  a. Choose **Remove all installed components** and click **Next**.
  b. Click **Yes** to confirm your decision.
  c. After ACAU has been uninstalled, click **Finish**.
  d. Follow the instructions in the "Installing ACAU" section on page 2-2 to install the new ACAU software.
- If you want to upgrade your ACAU software using the installation settings that were selected during the last installation, follow these steps:
  a. Choose **Reinstall all installed components** and click **Next**. The Setup Status window appears and notifies you as each software component is installed.
  b. When the upgrade finishes, the Maintenance Complete window appears. If the window contains an option to restart your computer, choose that option.
  c. Click **Finish** and allow your computer to restart if it begins the reboot process.

Running ACAU

When you install ACAU, the installation routine places an Aironet Client Administration Utility icon on your Windows desktop. Double-click the icon to start the utility.

Uninstalling ACAU

You can uninstall ACAU from your computer by opening the Windows Control Panel, selecting **Add or Remove Programs**, and choosing ACAU for removal.

Obtaining and Installing the Client Adapter Software

The CB21AG and PI21AG client adapter software is not part of the ACAU software package and must be obtained separately. Refer to the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for instructions on obtaining and installing the client adapter software.

Caution Cisco Aironet CB21AG and PI21AG client adapter software is incompatible with other Cisco Aironet client adapter software. The Aironet Desktop Utility (ADU) must be used with CB21AG and PI21AG adapters, and the Aironet Client Utility (ACU) must be used with all other Cisco Aironet client adapters.

Uninstalling the Client Adapter Software

If you set the ACAU Setup Settings - Installation Type parameter to Silent Uninstall, the client adapter software is uninstalled automatically when the user runs the Install Wizard. To uninstall the client adapter software without using ACAU, refer to the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for instructions.

CHAPTER

Using ACAU

This chapter describes how to use ACAU to create or modify configuration files and manage profiles.

The following topics are covered in this chapter:

Creating a New Configuration File

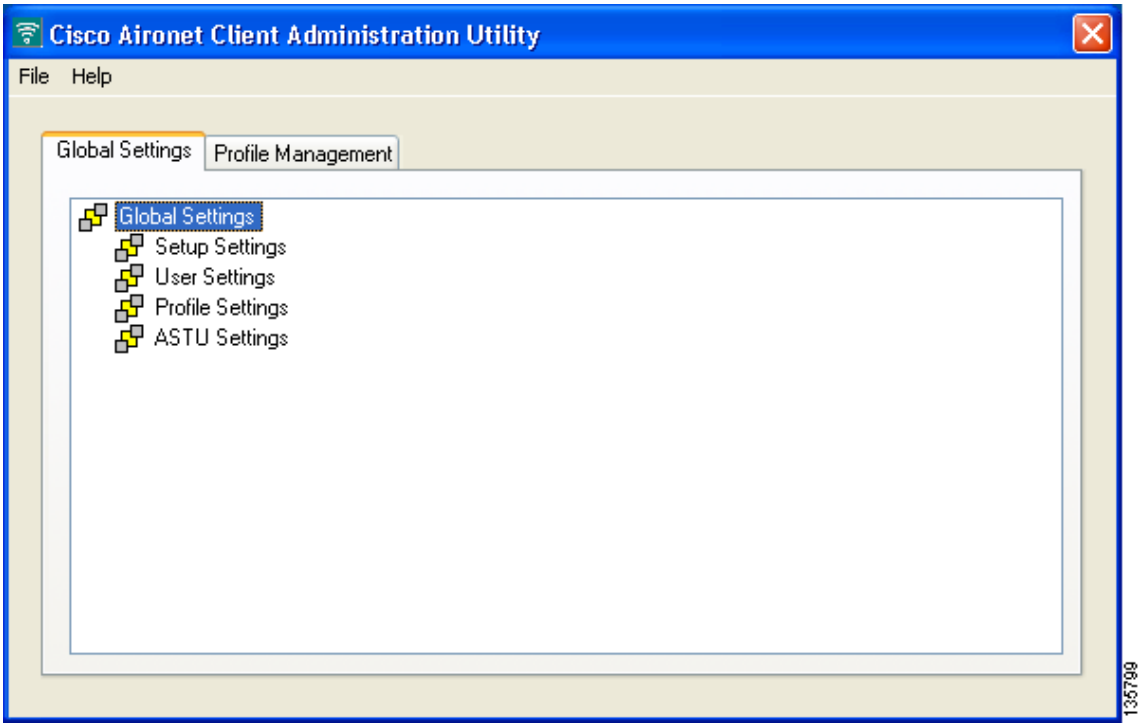
The configuration file is the file you create to govern the installation of client adapter software and load configuration profiles on a user's computer. Its settings are activated when the user uses the Install Wizard to install the client adapter software.

The configuration file contains two components: global settings and profiles. Global settings are administrative parameters that determine how the client adapter software is installed on a user's computer. You can override the default parameters using the Global Settings tab. Profiles are saved configurations that govern the operation of a user's client adapter. You can use the Profile Management tab to create profiles. Both components are saved in the configuration file, which is named *CiscoAdminConfig.dat.*

Follow these steps to create a new configuration file.

Step 1 Open ACAU. The Global Settings window appears (see Figure 3-1).

Figure 3-1 Global Settings Window



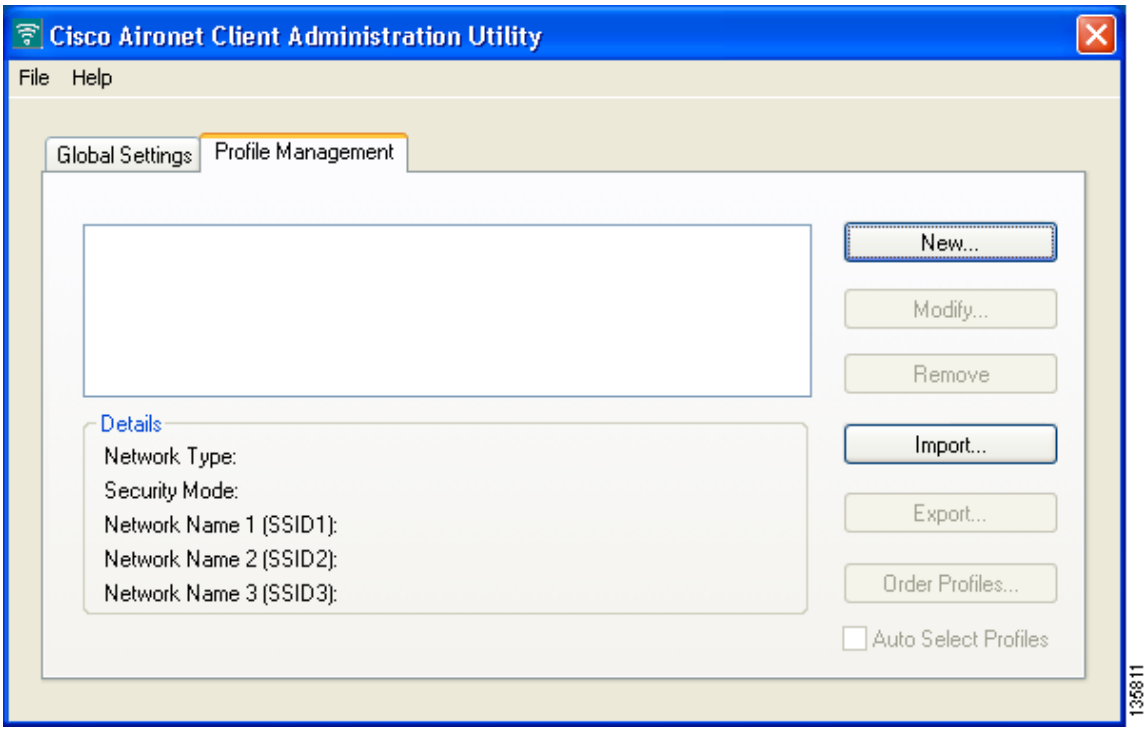
Step 2 Choose **New** from the File drop-down menu. ACAU names the file *New* and displays the name in the window's title bar.

Step 3 Under **Global Settings**, double-click each of the four groups of configurable parameters (Setup Settings, User Settings, Profile Settings, and ASTU Settings) to view its individual parameters.

Step 4 Follow the instructions in Chapter 4 to change the settings of any global parameters.

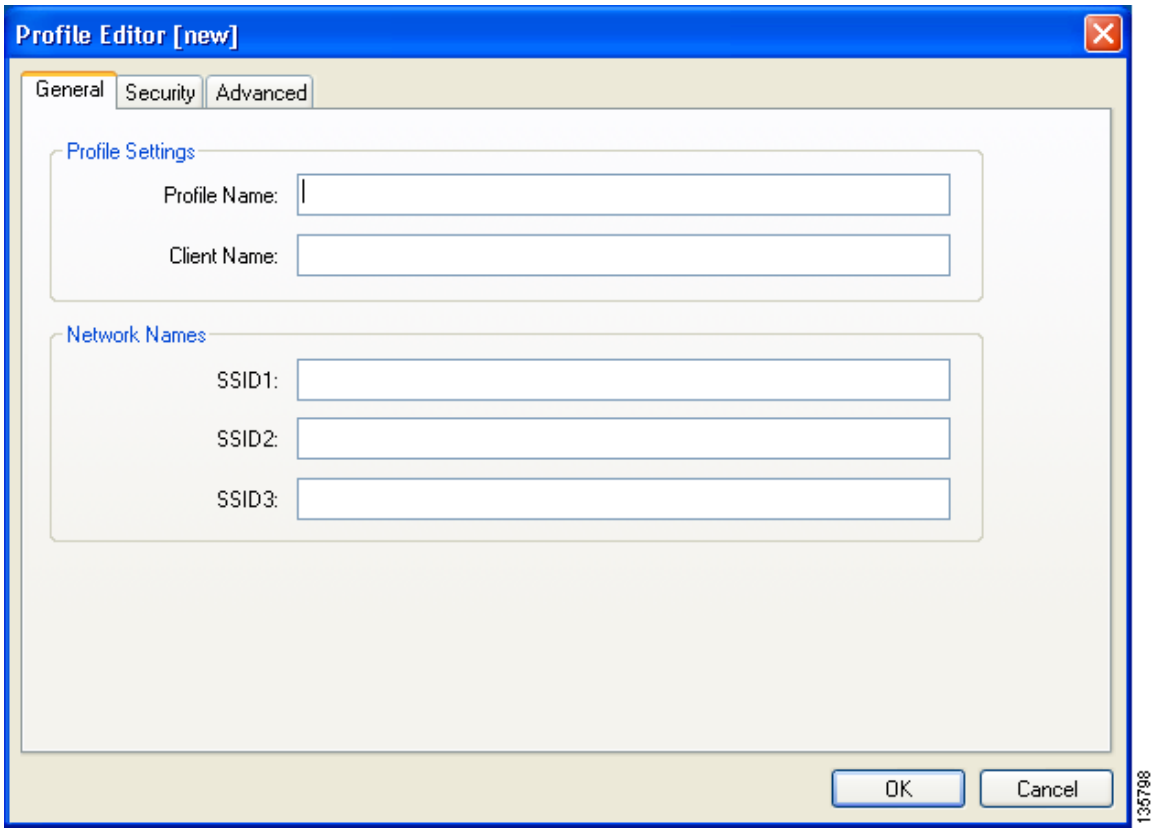
Step 5 Click the **Profile Management** tab to access the profile management options. The Profile Management window appears (see Figure 3-2).

Figure 3-2 Profile Management Window



Step 6 Click **New**. The Profile Editor (General) window appears (see Figure 3-3).

Figure 3-3 Profile Editor (General) Window



Step 7 Enter a profile name and SSID(s).

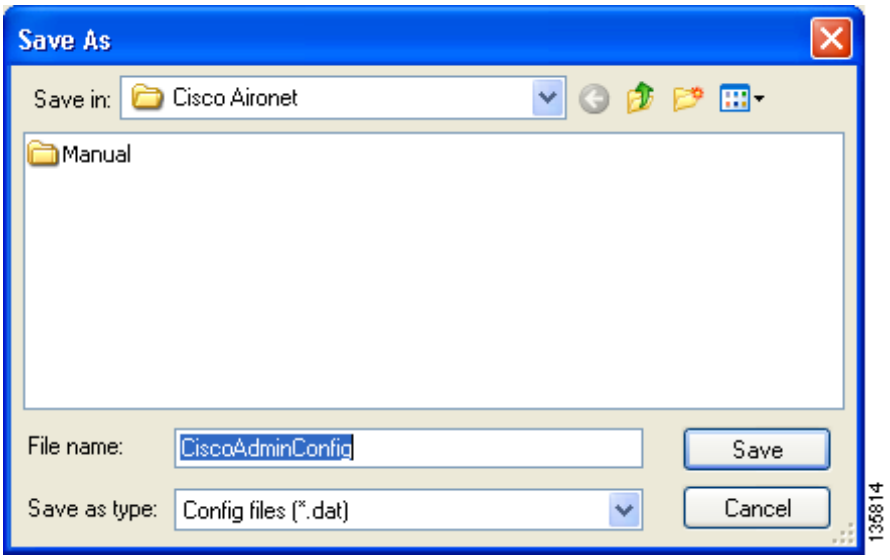
Step 8 Click the **Advanced** tab. Then follow the instructions in Chapter 5 to change any advanced settings for this profile.

Step 9 Click the **Security** tab. Then follow the instructions in Chapter 5 to change any security settings for this profile.

Step 10 (Optional) Repeat Steps 7 through 10 to create additional profiles.

Step 11 Choose **Save As** from the File drop-down menu to save the configuration file. The Save As window appears (see Figure 3-4).

Figure 3-4 Save As Window



Step 12 Use the Save in box to specify where the configuration file is saved.

Note You must save the configuration file to the drive and directory in which the Install Wizard resides. If you save the file to any other location, it is not processed by the Install Wizard.

Step 13 ACAU automatically names the file *CiscoAdminConfig.dat*. You can change the name by entering a new name in the File name field; however, the name must be changed back to *CiscoAdminConfig.dat* before running the Install Wizard. Otherwise, the Install Wizard does not load the configuration file.

Step 14 Click **Save** to save the configuration file.

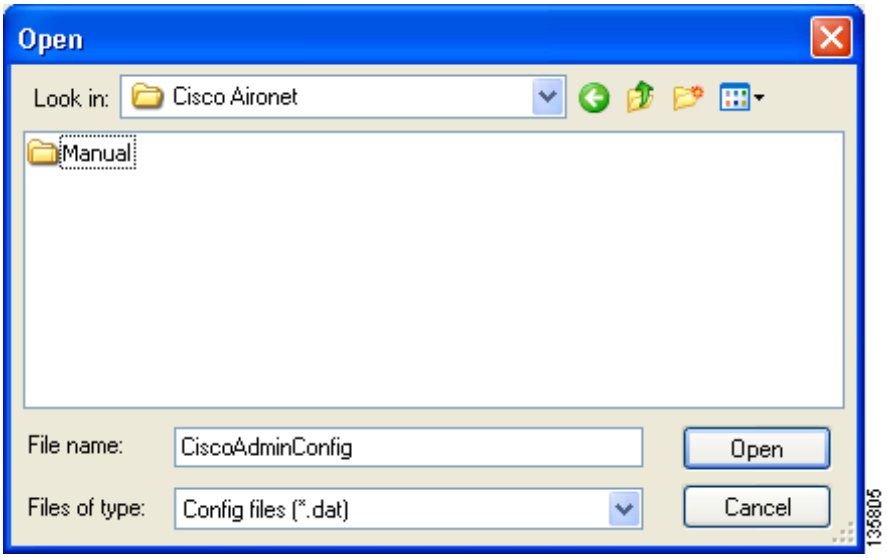
Modifying an Existing Configuration File

Follow these steps to modify an existing configuration file.

Step 1 Open ACAU.

Step 2 Choose **Open** from the File drop-down menu. The Open window appears (see Figure 3-5).

Figure 3-5 Open Window



Step 3 Use the Look in box to find the configuration file that you want to modify.

Note The default location is C:\Program Files\Cisco Aironet.

Step 4 Click **Open**. The ACAU Global Settings window appears with the name of the opened configuration file in the window's title bar.

Step 5 Modify the global settings as necessary.

Step 6 Click the **Profile Management** tab.

Step 7 Click **New** to create a new profile or **Modify** to modify an existing profile.

Step 8 Configure the profile as desired.

Step 9 Choose **Save** from the File drop-down menu to resave the configuration file.

Note If you attempt to close ACAU without saving your changes, ACAU informs you that the file has changed and asks if you want to save the changes. You must choose either **Yes** or **No** before ACAU can close.

Managing Profiles

This section explains how to use ACAU's Profile Management tab to manage the profiles that you create. Follow the instructions on the page indicated to perform the desired task:

- Remove a profile, page -7
- Import or export a profile, page -7
- Include a profile in auto profile selection, page -9
- Retrieve a profile from the computer's registry, page -12

Removing a Profile

Follow these steps to remove a profile from your configuration file.

Step 1 Choose **Open** from the File drop-down menu and select the configuration file containing the profile to be removed.

Step 2 When the file opens, click the **Profile Management** tab.

Step 3 In the profiles list, highlight the profile that you want to remove.

Step 4 Click **Remove**. The profile is removed.

Step 5 Choose **Save** from the File drop-down menu to save the modified configuration file.

Importing and Exporting Profiles

This section provides instructions for importing and exporting profiles. You may want to use the import/export feature for the following reasons:

- To export one or more profiles and use them to set up additional configuration files
- To export profiles and import them directly into ADU
- To import a profile created in and exported from ADU and use it in a configuration file

Follow the instructions below to import or export profiles.

Importing a Profile

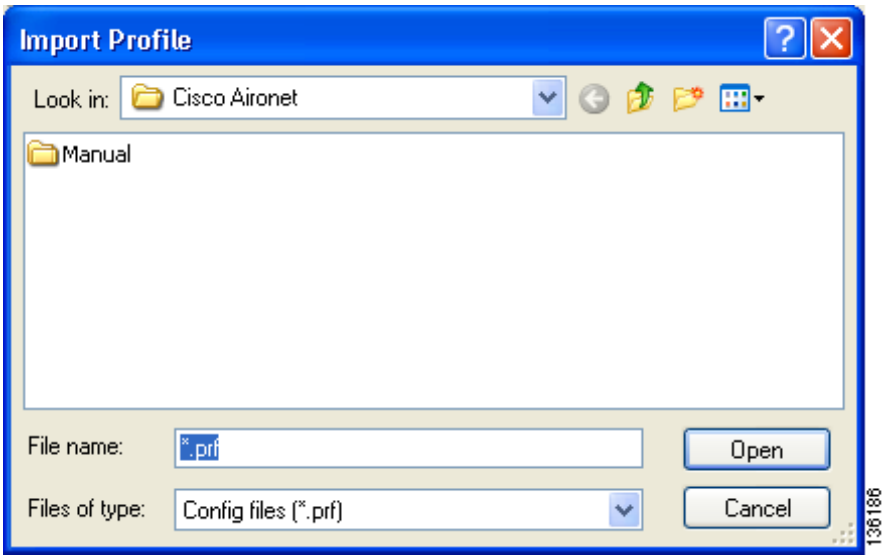
Step 1 If the profile that you want to import is on a disk, insert the disk into your computer's disk drive.

Step 2 Choose **Open** from the File drop-down menu and select the configuration file into which you want to import a profile.

Step 3 When the file opens, click the **Profile Management** tab.

Step 4 Click **Import**. The Import Profile window appears (see Figure 3-6).

Figure 3-6 Import Profile Window



Step 5 In the Look in drop-down box, find the directory where the profile is located.

Step 6 Click the profile so it appears in the File name field at the bottom of the window.

Step 7 Click **Open**. The imported profile appears in the profiles list on the Profile Management window.

Step 8 Choose **Save** from the File drop-down menu to save the modified configuration file.

Exporting a Profile

Note PACs are not exported with EAP-FAST profiles.

Step 1 Insert a disk into your computer's disk drive, if you wish to export a profile to a disk.

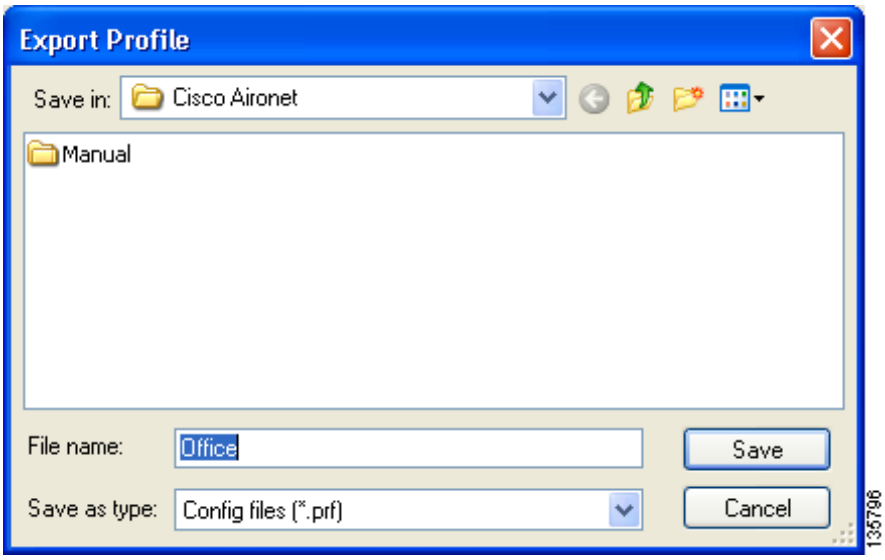
Step 2 Choose **Open** from the File drop-down menu and select the configuration file from which you want to export a profile.

Step 3 When the file opens, click the **Profile Management** tab.

Step 4 In the profiles list, highlight the profile that you want to export.

Step 5 Click **Export**. The Export Profile window appears (see Figure 3-7).

Figure 3-7 Export Profile Window



Step 6 The profile name appears in the File name field. Change the name, if desired.

Step 7 Choose a different directory (such as your computer's disk drive or a location on the network) from the Save in drop-down box.

Step 8 Click **Save**. The profile is exported to the specified location.

Note If a profile with the same name already exists, ACAU prompts you to replace it.

Step 9 Choose **Save** from the File drop-down menu to resave and close the configuration file.

Including a Profile in Auto Profile Selection

After you have created profiles, you can choose to include them in the profile manager's auto profile selection feature. Then when auto profile selection is enabled, the client adapter automatically selects a profile from the list of profiles that were included in auto profile selection and uses it to establish a connection to the network.

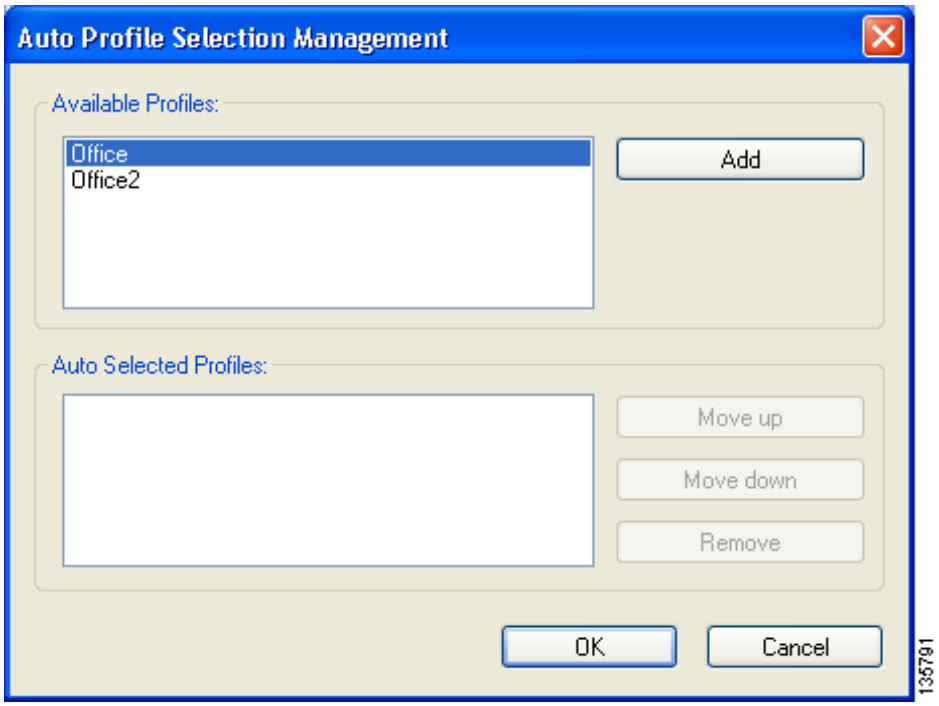
Follow these steps to include profiles in auto profile selection and establish the order in which the profiles are selected for use.

Step 1 Choose **Open** from the File drop-down menu and select the configuration file containing the profiles that you want to include in auto profile selection.

Step 2 When the file opens, click the **Profile Management** tab.

Step 3 Click **Order Profiles**. The Auto Profile Selection Management window appears (see Figure 3-8).

Figure 3-8 Auto Profile Selection Management Window



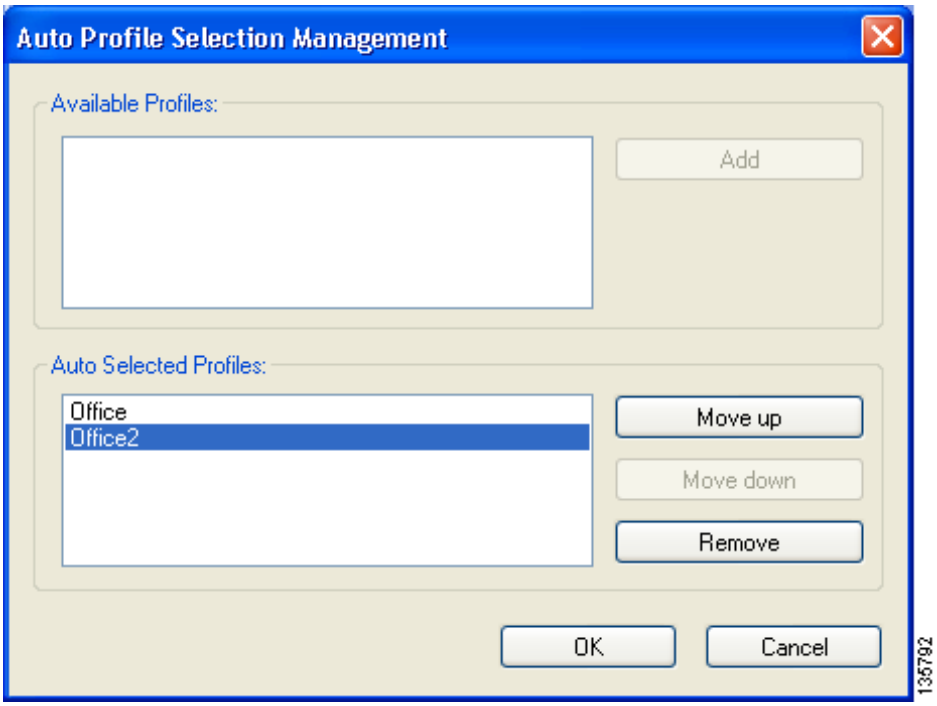
Step 4 All the profiles that you created for this configuration file are listed in the Available Profiles box. Highlight each one you want to include in auto profile selection and click the **Add** button. The profiles appear in the Auto Selected Profiles box.

The following rules apply to auto profile selection:

- You must include at least two profiles in the Auto Selected Profiles box.
- The profiles must specify an SSID; otherwise, they do not appear in the Available Profiles box.
- Profiles cannot specify multiple SSIDs; otherwise, they do not appear in the Available Profiles box.
- Each profile that is included in auto profile selection must have a unique SSID. For example, if Profile 1 and Profile 2 both have “ABCD” as their SSID, then only Profile 1 or Profile 2 (whichever one was created first) appears in the Available Profiles box and can be included in auto profile selection.

Step 5 Continue to highlight and add profiles as necessary. Figure 3-9 shows how the Auto Selected Profiles box may look.

Figure 3-9 Profiles Included in Auto Profile Selection



Step 6 The first profile in the Auto Selected Profiles box has the highest priority while the last profile has the lowest priority. To change the order (and priority) of your auto-selected profiles, select the profile that you want to move and click **Move up** or **Move down** to move the profile up or down, respectively.

Note You can remove a profile from the list by highlighting it and clicking **Remove**. The profile returns to the Available Profiles box.

Step 7 Click **OK** to save your selections and return to the Profile Management window.

Step 8 Check the **Auto Select Profiles** check box.

Note When this check box is checked, the client adapter scans for an available network. The profile with the highest priority and the same SSID as one of the found networks is the one that is used to connect to the network. If the connection fails, the client adapter tries the next highest priority profile that matches the SSID and so on.

Step 9 Choose **Save** from the File drop-down menu to save the modified configuration file.

Retrieving a Profile from the Registry

If you created profiles on your computer using a previous version of ACAU or ADU, they are saved in the registry. Follow these steps if you want to retrieve these profiles.

Note Profiles in the current ADU installation can be read from the registry, even if they were not originally created by ACAU.

Step 1 Choose **Open** from the File drop-down menu and select the configuration file into which you want to include profiles from the registry.

Step 2 When the file opens, click the **Profile Management** tab.

Step 3 Choose **Read from registry** from the File drop-down menu. ACAU queries the Windows registry for profiles and reads them into memory.

Step 4 When a message appears indicating that profiles have been read successfully from the registry, click **OK**. These profiles are added to the list of profiles in the Profile Management window.

Note All profiles read from the registry can be edited in ACAU. You can perform any of the following operations: modify, remove, import, export, or include in auto profile selection.

Step 5 Choose **Save** from the File drop-down menu to save the profiles read from the registry to the configuration file.

CHAPTER 4

Configuring Global Settings

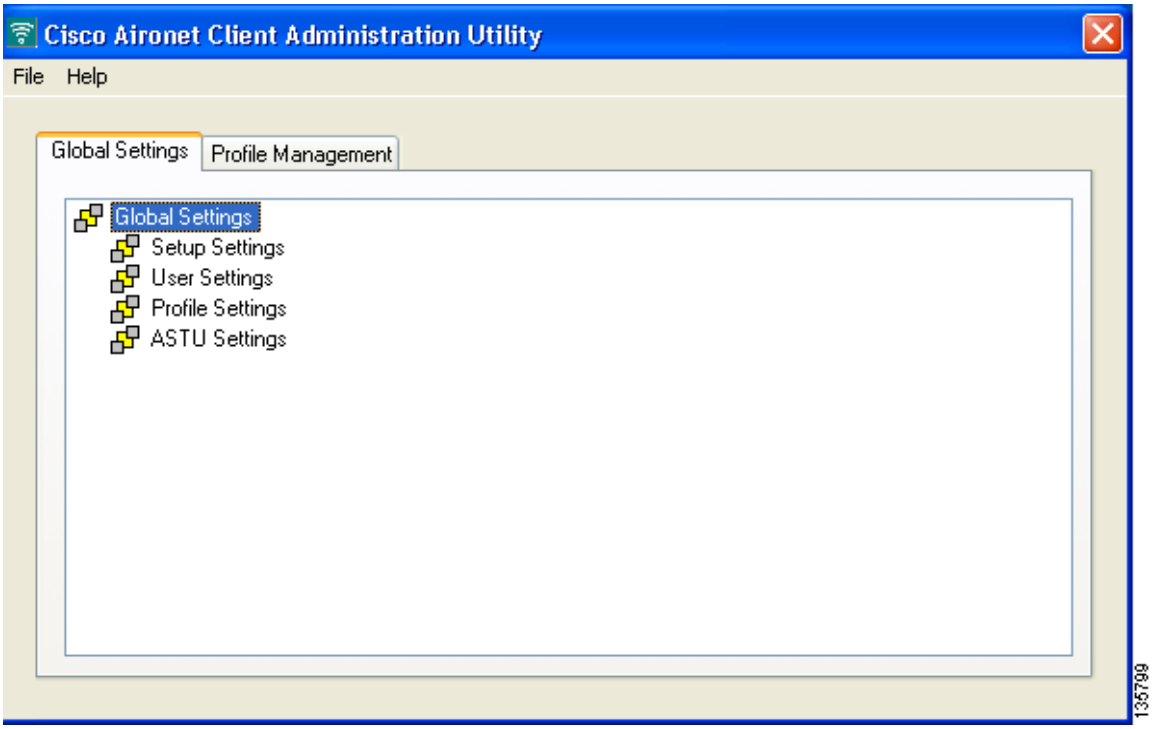
This chapter describes the Global Settings tab parameters and how to configure them to override the client adapter software installation settings.

The following topics are covered in this chapter:

Overview of the Global Settings Tab

The Global Settings tab enables you to set parameters that specify how the client adapter software is installed. The settings you choose are saved to a configuration file and invoked when the user uses the Install Wizard to install the client adapter software. The Global Settings tab is located on the ACAU main window (see Figure 4-1).

Figure 4-1 Global Settings Tab

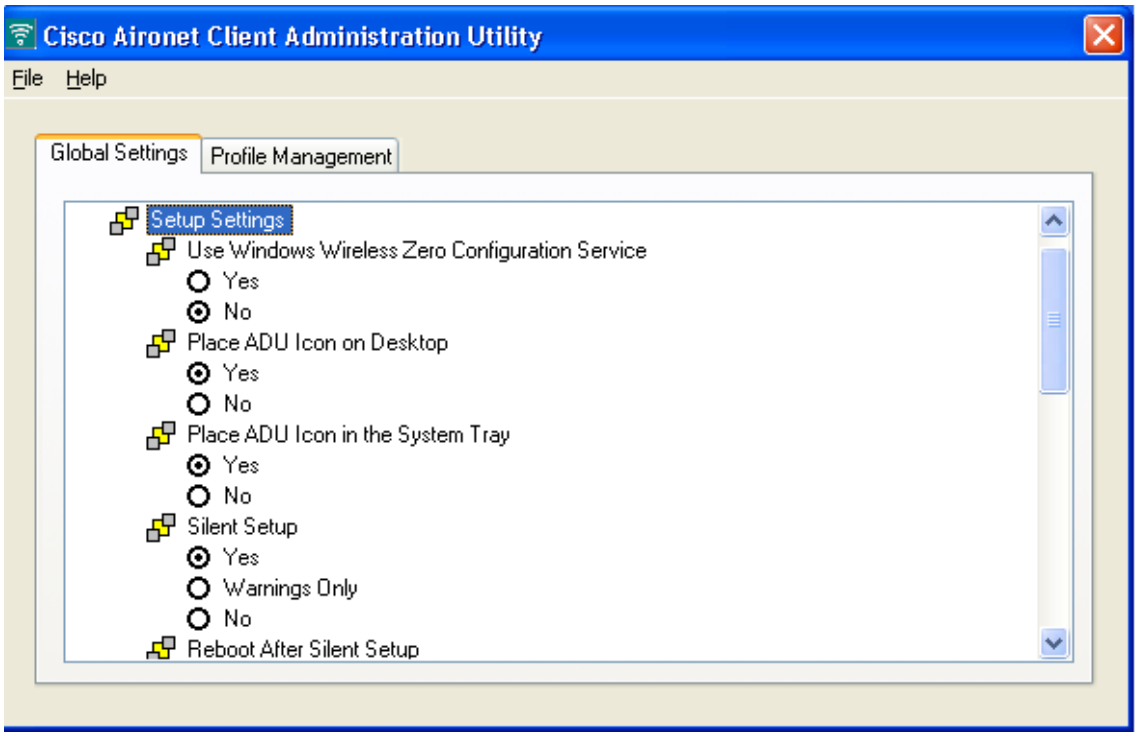


The Global Settings tab enables you to configure four groups of parameters:

- Setup Settings
- User Settings
- Profile Settings
- ASTU Settings

Double-click **Global Settings** to view these groups of parameters. Then double-click each group to see its individual parameters. Figure 4-2 shows the Setup Settings parameters.

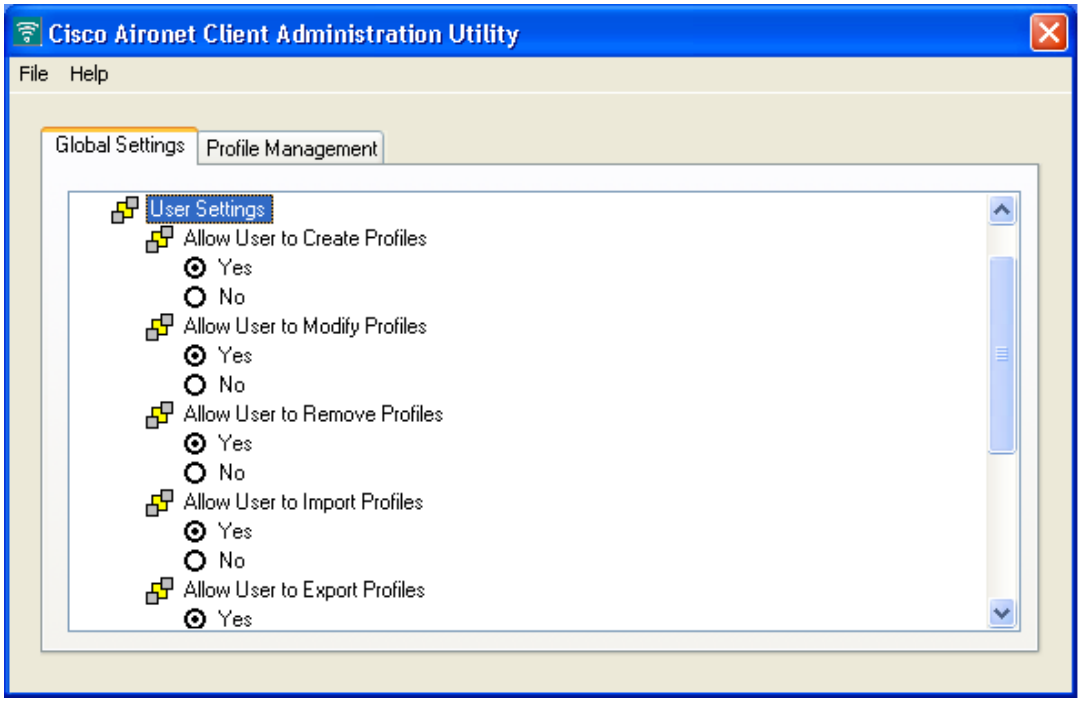
Figure 4-2 Setup Settings Parameters



Most parameters have two options: *Yes* or *No*. To change the value of a parameter, simply choose the desired option.

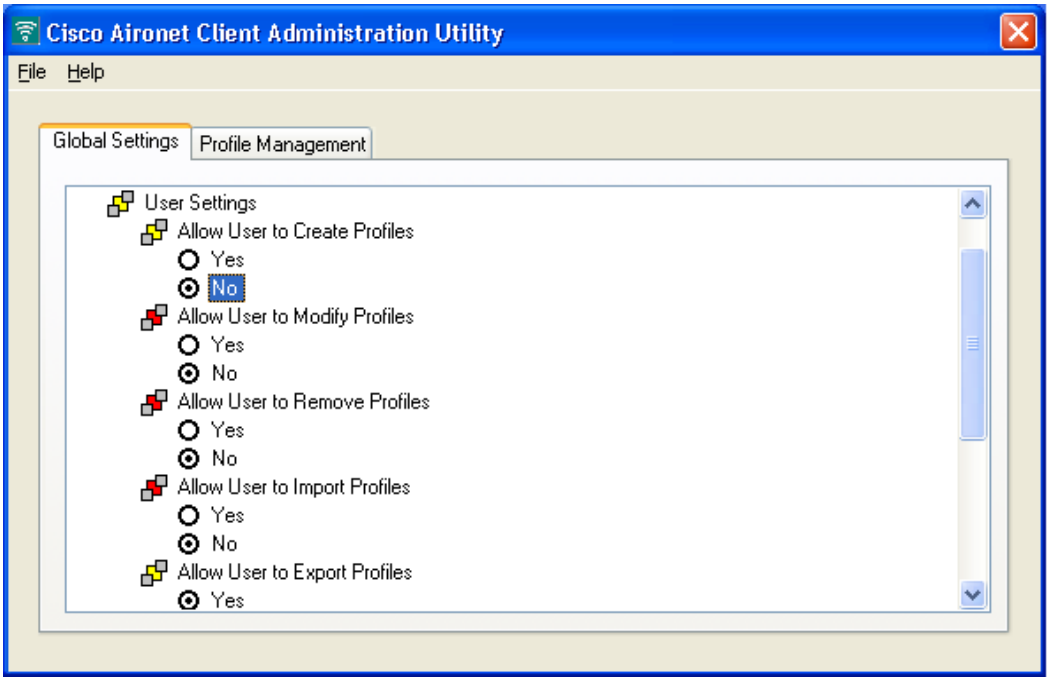
Some parameters are dependent on others. When you change the value of these parameters, the settings of other parameters may change. The icon next to a parameter changes color when its dependency changes. When there are no dependencies and parameter values can be changed, the icon consists of two gray boxes overlapping a yellow box (see Figure 4-3).

Figure 4-3 Changeable Parameter Icons



However, when dependencies exist and parameter values cannot be changed, the yellow box in the icon changes to red. For example, if you set the Allow User to Create a Profile parameter to *No*, many of the remaining User Settings parameters are also changed to *No,* and the yellow box in the icon changes to red (see Figure 4-4).

Figure 4-4 Unchangeable Parameter Icons



Configuring Setup Settings

The Setup Settings parameters enable you to configure the setup information that the Install Wizard uses to install the client adapter software on a user's computer. Double-click **Setup Settings** to view these parameters. Table 4-1 describes the Setup Settings parameters and lists their default values. Follow the instructions in the table to change any parameters.

Table 4-1 Setup Settings

Parameter	Description
Use Windows Wireless Zero Configuration Service	Determines whether the user's computer is configured to use the Windows XP Microsoft Wireless Configuration Manager rather than the Aironet Desktop Utility (ADU) to manage the client adapter. **Options:** Yes or No **Default:** No
Place ADU Icon on Desktop	Determines whether the ADU icon is placed on the desktop of the user's computer to provide quick access to the utility. **Options:** Yes or No **Default:** Yes

Table 4-1 Setup Settings (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Place ADU Icon in the System Tray</td><td>Determines whether the ADU icon is placed in the system tray of the user's computer.
Options: Yes or No
Default: Yes
Note When the ADU icon is in the system tray, the user is able to access the Aironet System Tray Utility (ASTU) by right-clicking the icon.</td></tr>
<tr><td>Silent Setup</td><td>Specifies whether user input is required during the installation of the client adapter software.
Options: Yes, Warnings Only, or No
Default: Yes
<table><tr><th>Silent setup</th><th>Description</th></tr><tr><td>Yes</td><td>The Install Wizard silently installs the client adapter software without any user input.
Note Be sure that the client adapter is inserted into the user's computer before the client adapter software is installed. Otherwise, the driver installation is incomplete, and the user is not notified.</td></tr><tr><td>Warnings Only</td><td>The Install Wizard displays any warning messages associated with the installation.</td></tr><tr><td>No</td><td>The Install Wizard prompts the user to make selections during the installation of the client adapter software.</td></tr></table></td></tr>
</table>

Table 4-1 Setup Settings (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Reboot After Silent Setup</td><td>Determines whether the user's computer reboots after the client adapter software is silently installed.
Options: Prompt for Reboot, Reboot without Prompting, or Do Not Reboot
Default: Reboot without prompting

<table><tr><th>Reboot after Silent Setup</th><th>Description</th></tr><tr><td>Prompt for Reboot</td><td>The Install Wizard prompts the user to reboot the computer after the client adapter software is silently installed.</td></tr><tr><td>Reboot without Prompting</td><td>The user's computer automatically reboots after the client adapter software is silently installed.</td></tr><tr><td>Do Not Reboot</td><td>The user's computer does not reboot after the client adapter software is silently installed.</td></tr></table></td></tr>
<tr><td>Installation Type</td><td>Specifies whether user input is required when the client adapter software is upgraded or uninstalled.
Options: Normal, Silent Upgrade, or Silent Uninstall
Default: Normal

<table><tr><th>Installation type</th><th>Description</th></tr><tr><td>Normal</td><td>The Install Wizard prompts the user to choose between uninstalling or upgrading the client adapter software.</td></tr><tr><td>Silent Upgrade</td><td>The Install Wizard upgrades the client adapter software without any user input.</td></tr><tr><td>Silent Uninstall</td><td>The Install Wizard uninstalls the client adapter software without any user input.</td></tr></table></td></tr>
<tr><td>Install Site Survey Utility</td><td>Determines whether the site survey utility is installed on the user's computer.
Options: Yes or No
Default: Yes</td></tr>
</table>

Table 4-1 Setup Settings (continued)

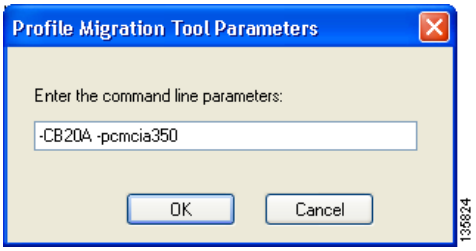
<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Profile Migration Tool</td><td>Determines whether the profile migration tool is installed and run on the user's computer. The tool is designed to migrate profiles used on Cisco Aironet 350 series and CB20A wireless LAN client adapters to profiles that can be used with Cisco Aironet CB21AG and PI21AG client adapters.

Options:Don't Install, Install, or Install & Run

Default: Don't Install

<table>
<tr><th>Profile Migration Tool</th><th>Description</th></tr>
<tr><td>Don't Install</td><td>The Install Wizard does not install the profile migration tool on the user's computer.</td></tr>
<tr><td>Install</td><td>The Install Wizard installs the profile migration tool on the user's computer (in the same directory as ADU).</td></tr>
<tr><td>Install & Run</td><td>The Install Wizard installs the profile migration tool on the user's computer (in the same directory as ADU) and runs the tool after installation.

If you choose this option, you can also enter command line options that let you specify how the tool operates. To do so, click Command Line, enter the desired command(s) on the Profile Migration Tool Parameters window as shown below, and click OK.

Note See Appendix D for the list of available command line options and more information on the profile migration tool.</td></tr>
</table>
</td></tr>
</table>

Table 4-1 Setup Settings (continued)

Parameter	Description
Limit Functionality to the System Tray Icon	Determines whether the user is limited to using only ASTU to manage the client adapter. **Options:** Yes or No **Default:** No **Note** If you choose *Yes*, the user cannot use the ADU icon on the Windows desktop. Only ASTU is available.

Configuring User Privileges

The User Settings parameters enable you to determine a user's privileges after the client adapter software is installed. Table 4-2 describes the User Settings parameters and lists their default values. Follow the instructions in the table to change any parameters.

Table 4-2 User Settings

Setting	Description
Allow User to Create a Profile	Determines whether a user can create a profile using ADU. **Options:** Yes or No **Default:** Yes **Note** If you choose *No*, all of the User Settings parameters are unavailable, with these exceptions: - Allow user to Export a Profile - Prompt the User Before Initiating Automatic PAC Provisioning
Allow User to Modify a Profile	Determines whether a user can modify a profile using ADU. **Options:** Yes or No **Default:** Yes
Allow User to Remove a Profile	Determines whether a user can remove a profile using ADU. **Options:** Yes or No **Default:** Yes **Note** Only profiles created by the user can be removed.
Allow User to Import a Profile	Determines whether a user can import a profile using ADU. **Options:** Yes or No **Default:** Yes
Allow User to Export a Profile	Determines whether a user can export a profile using ADU. **Options:** Yes or No **Default:** Yes

Table 4-2 User Settings (continued)

Setting	Description
Allow User to Modify Automatic PAC Provisioning in Profiles	Determines whether a user can disable automatic protected access credentials (PAC) provisioning for an EAP-FAST profile. **Options:** Yes or No **Default:** No **Note** Automatic PAC provisioning enables the automatic retrieval of a PAC over the wireless link during EAP-FAST authentication.
Prompt User Before Initiating Automatic PAC Provisioning	Determines whether a user is prompted to automatically provision a PAC for EAP-FAST authentication when a PAC is not found on the user's system. **Options:** Yes or No **Default:** No **Note** If you choose *Yes*, the user is prompted to automatically provision a PAC whenever a PAC cannot be found. If you choose *No*, a PAC is provisioned automatically (without prompting the user) whenever a PAC is not found.

Configuring Profile Settings

The Profile Settings parameters enable you to control how profiles are managed on the user's computer. Table 4-3 describes the Profile Settings parameters and lists their default values. Follow the instructions in the table to change any parameters.

Table 4-3 Profile Settings Parameters

Parameter	Description
Enable Profile Management	Specifies whether the ADU profile management feature is enabled on the user's computer. **Options:** Yes or No **Default:** Yes **Note** If you choose *No*, the Profile Management tab in ADU will not visible to the user, but the user can select a profile by right-clicking the ASTU icon and selecting the profile. **Note** If you choose *No*, all of the User Settings parameters are unavailable, with this exception: Prompt the User Before Initiating Automatic PAC Provisioning.

Table 4-3 Profile Settings Parameters (continued)

Parameter	Description
Update Existing Profiles	Determines how a user's existing profiles are affected when the Install Wizard installs new profiles from the ACAU configuration file. **Options:** Overwrite or Append **Default:** Overwrite

Update existing Profiles	Description
Overwrite	All existing profiles are deleted and replaced with new profiles from the ACAU configuration file.
Append	Existing profiles with the same name as those within the ACAU configuration file remain unchanged. All other existing profiles are retained.

Force Auto Select Profiles	Determines whether profiles are selected automatically in ADU or the user is allowed to manually select profiles. **Options:** Yes or No **Default:** No **Note** If you choose *Yes*, the user is unable to manually select profiles in ADU. Profiles are selected automatically. In addition, the Activate button on the ADU Profile Management and Available Infrastructure and Ad Hoc Networks windows only creates a new profile, but does not activate the network.

Configuring ASTU Settings

The ASTU Settings parameters enable you to configure the Aironet System Tray Utility (ASTU). ASTU is an optional application that provides a small subset of the features available through ADU. Specifically, it enables a user to access status information about the client adapter and perform basic tasks. ASTU is available from an icon in the Windows system tray, making it easily accessible and convenient to use. The icon appears in the system tray only if you set the Place ADU icon in the System Tray parameter to *Yes*.

The ASTU Settings parameters determine which ASTU features are available to the user. Table 4-4 describes the ASTU Settings parameters and lists their default values. Follow the instructions in the table to change any parameters.

Table 4-4 ASTU Settings Parameters

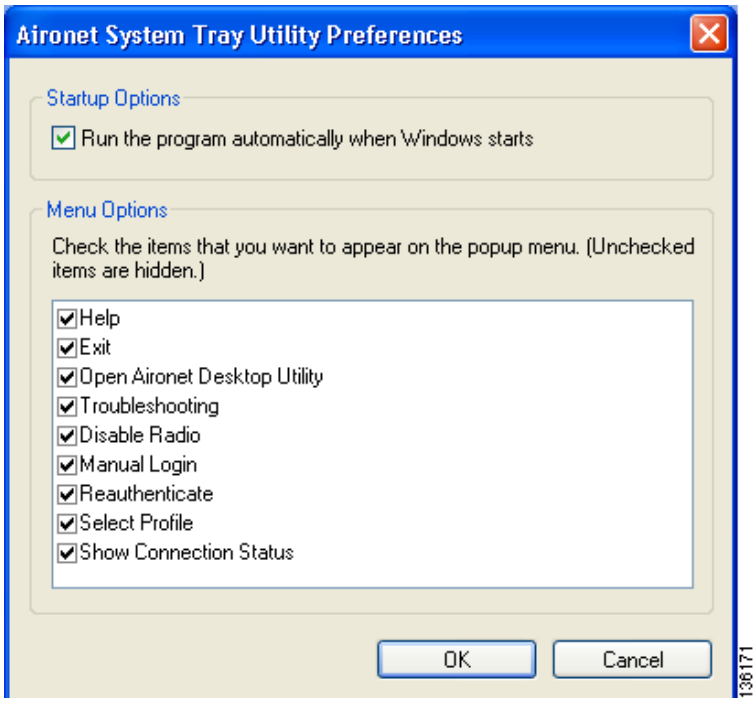
Parameter	Description
Preferences	Determines whether the user can access the Aironet System Tray Utility Preferences window, which enables the user to specify when ADU and ASTU run and choose the options that appear on the ASTU pop-up menu. **Options:** Yes or No **Default:** Yes **Note** If you choose *Yes*, the Aironet System Tray Utility Preferences window (shown below) appears when the user right-clicks the ADU icon in the system tray and clicks **Preferences**. If you choose *No*, the user is unable to open this window. 
Help	Determines whether the user can access online help from ASTU. **Options:** Yes or No **Default:** Yes **Note** If you choose *No*, online help is still available from the Help drop-down menu in ADU.
Exit	Determines whether the user can exit ADU from ASTU. **Options:** Yes or No **Default:** Yes **Note** If you choose *No*, the user can still exit ADU by selecting **Exit** from the ADU Action drop-down menu or clicking the **X** in the top right corner of any main ADU window.

Table 4-4 ASTU Settings Parameters (continued)

Parameter	Description
Open Aironet Desktop Utility	Determines whether the user can open ADU from ASTU. **Options:** Yes or No **Default:** Yes **Note** If you choose *No* and the Setup Settings - Place ADU icon on Desktop parameter is set to *Yes*, the user can open ADU from an icon on the Windows desktop.
Troubleshooting	Determines whether the user can run troubleshooting tests from ASTU. **Options:** Yes or No **Default:** Yes **Note** If you choose *No*, the user can still run troubleshooting tests from ADU by selecting **Troubleshooting** from either the Action drop-down menu or the Diagnostics tab.
Disable Radio	Determines whether the user can disable the client adapter's radio from ASTU. **Options:** Yes or No **Default:** Yes **Note** If you choose *No*, the radio can still be disabled by selecting **Disable Radio** from the ADU Action drop-down menu.
Manual Login	Determines whether the user can use ASTU to manually invoke the authentication process for a profile that is configured to use a manually prompted LEAP or EAP-FAST username and password. **Options:** Yes or No **Default:** Yes **Note** Refer to the "Setting Security Parameters" section on page 5-16 for information on setting a manual LEAP or EAP-FAST profile and for details on the authentication process.
Reauthenticate	Determines whether the user can use ASTU to force the client adapter to try to reauthenticate using the username and password of the active profile. **Options:** Yes or No **Default:** Yes **Note** This feature is available only for EAP-enabled profiles. **Note** If you choose *No*, the user can still reauthenticate by selecting **Reauthenticate** from the ADU Action drop-down menu.

Table 4-4 ASTU Settings Parameters (continued)

Parameter	Description
Select Profile	Determines whether the user can use ASTU to activate a profile. **Options:** Yes or No **Default:** Yes **Note** When the user selects a profile in ASTU, the client adapter attempts to establish a connection to an access point using the parameters that were configured for that profile. If the client adapter cannot associate to the access point or loses association while using the selected profile, the adapter does not attempt to associate using another profile. **Note** If you choose *No*, the user can still activate profiles using the ADU profile manager.
Show Connection Status	Determines whether the user can display the ASTU Connection Status window. **Options:** Yes or No **Default:** Yes **Note** If you choose *No*, the ASTU Connection Status window is not available to the user. However, status information is available from the ADU Current Status and Advanced Status windows.

CHAPTER 5

Creating Profiles

This chapter explains how to use ACAU to create profiles that are saved to a configuration file and installed by the Install Wizard when a user installs the client adapter software.

The following topics are covered in this chapter:

Overview of the Profile Management Tab

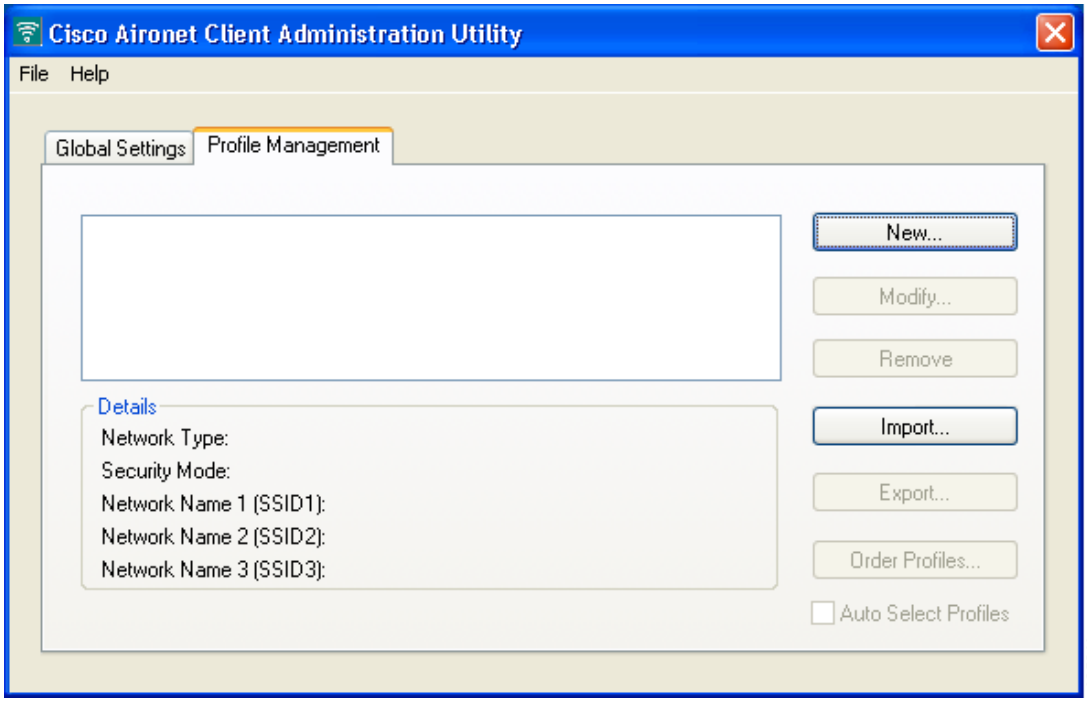
ACAU's Profile Management tab enables you to create or modify up to 16 *profiles* (saved configurations) for users' client adapters. The parameters that you set for each profile govern the operation of the adapters. After you create the profiles, you must save them to an ACAU configuration file where they are stored until the Install Wizard installs them during the installation of the client adapter software.

Note In addition to creating profiles, you can also use the Profile Management tab to remove, import, export, or auto-select profiles. See the "Managing Profiles" section on page -7 for more information.

Opening the Profile Manager

To open ACAU's profile manager, click the **Profile Management** tab. The Profile Management window appears (see Figure 5-1).

Figure 5-1 Profile Management Window



When you choose to create a new profile or modify an existing profile, the Profile Editor windows appear. These windows enable you to set the configuration parameters for that profile.

Each of the Profile Editor windows (listed below) contains parameters that affect a specific aspect of the client adapter:

- **General**—Prepares the client adapter for use in a wireless network
- **Advanced**—Controls how the client adapter operates within an infrastructure or ad hoc network
- **Security**—Controls how a client adapter associates to an access point, authenticates to the wireless network, and encrypts and decrypts data

Table 5-1 enables you to quickly locate instructions for setting each Profile Editor window's parameters.

Table 5-1 Locating Configuration Instructions

Parameter Category	Page Number
General	page 5-3
Advanced	page 5-8
Security	page 5-16

Setting General Parameters

The Profile Editor (General) window (see Figure 5-2) enables you to set parameters that prepare the client adapter for use in a wireless network. This window appears after you select the Profile Management tab and click **New** or **Modify** on the Profile Management window.

Figure 5-2 Profile Editor (General) Window

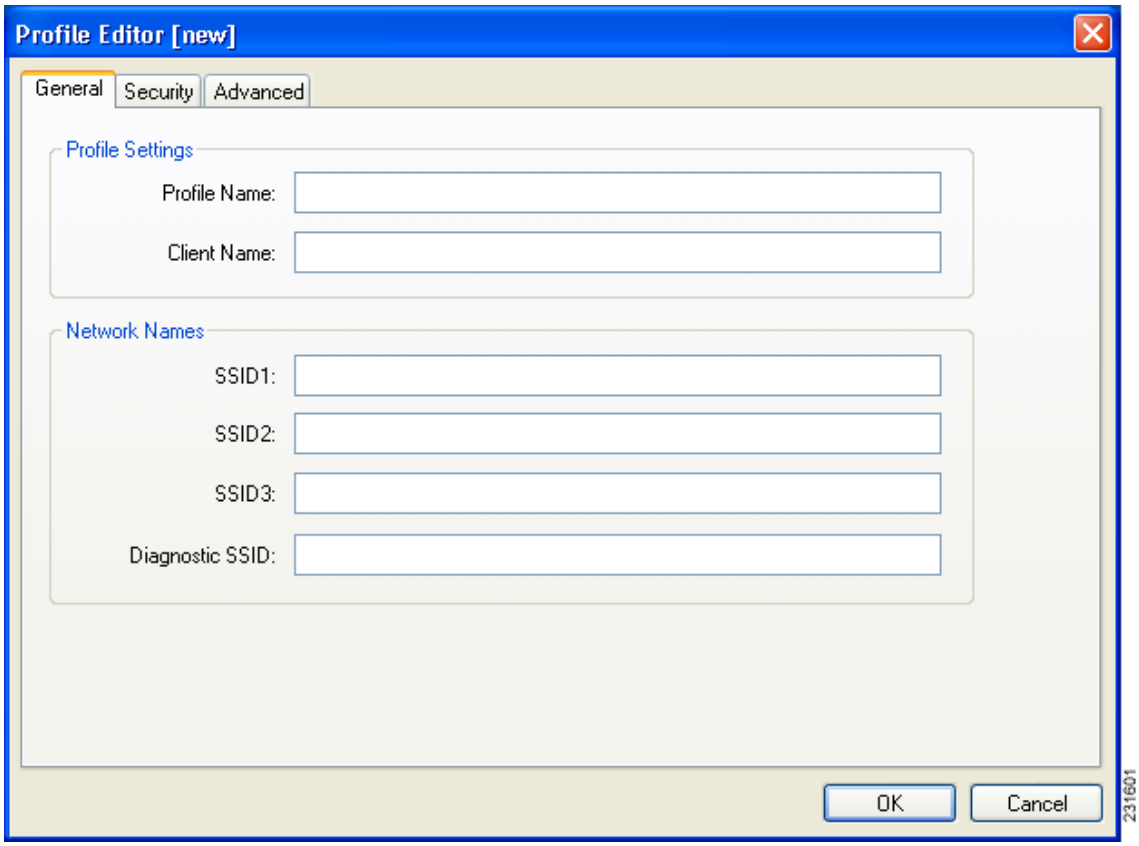


Table 5-2 lists and describes the profile's general parameters. Follow the instructions in the table to change any parameters.

Table 5-2 General Parameters

Parameter	Description
Profile Name	The name assigned to the configuration profile. **Range:** Up to 32 ASCII characters **Default:** A blank field
Client Name	A logical workstation name. It enables an administrator to determine which devices are connected to the access point without having to memorize every MAC address. This name is included in the access point's list of connected devices. The client name is filled in automatically but can be changed. **Range:** Up to 16 ASCII characters **Default:** The computer name **Note** Each computer on the network should have a unique client name.

Table 5-2 General Parameters (continued)

Parameter	Description
SSID1	The service set identifier (SSID) identifies the specific wireless network that you want the client adapter to access. **Range:** Up to 32 ASCII characters (case sensitive) **Default:** A blank field **Note** If you leave this parameter blank, the client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs. 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. **Note** If you leave this parameter blank, the profile cannot be added to the auto profile selection list. **Note** This parameter must contain a value if the profile is set for ad hoc mode. If the parameter is blank, you are prompted to enter a network name or reset the network type to *infrastructure*.

Table 5-2 General Parameters (continued)

Parameter	Description
SSID2 and SSID3	An optional SSID that identifies a second or third distinct wireless network and enables the client adapter to roam to that network without having to be reconfigured. **Range:** Up to 32 ASCII characters (case sensitive) **Default:** A blank field **Note** If a profile specifies more than one SSID, it cannot be included in auto profile selection, used with WPA/WPA2 passphrase, or set for ad hoc mode.
Diagnostic SSID	The diagnostic service set identifier (SSID) that you want the client adapter to access in order to use diagnostic channel mode. If you do not provide a diagnostic SSID, the client uses the value diagSSID in the Diagnostic SSID field. For the client adapter to use diagnostic channel mode, the profile does not have to be a trusted profile. However, an untrusted profile has limited reporting privileges. If the profile is untrusted, only the results of the following tests are reported: • ping test • DHCP test • IP connectivity test • DNS ping test • DNS name resolution test • 802.11 association test • 802.11X authentication test To make the profile a trusted profile, check the **Profile Trusted** check box in the Profile Editor Security tab. **Range:** Up to 32 ASCII characters (case sensitive) **Default:** A blank field

Go to the next section to set additional parameters or click **OK** to return to the Profile Management window.

Troubleshooting with Diagnostic Channel Mode

Diagnostic channel (DC) mode is a mode that identifies communication problems between the client adapter and a wireless LAN infrastructure device. When in DC mode, the client adapter and the infrastructure device proceed through a defined set of tests. The results of these tests can assist in isolating conditions that require troubleshooting.

DC mode testing can be started only from the Aironet Desktop Utility (ADU) for a profile that is capable of running in DC mode. For more information about running DC mode tests, see the "Troubleshooting" chapter of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide, Software Release 4.0*.

From the ACAU, you can specify the diagnostic SSID that you want the client adapter to access for a specific profile in order to use diagnostic channel mode. You can specify that diagnostic SSID in the Profile Editor General tab.

From the ACAU, you can also make the profile a trusted profile. The client adapter can still participate in DC mode testing even when the profile is untrusted, but an untrusted profile has limited reporting privileges. For more information on making a profile a trusted profile, which can be done from the Profile Editor Security tab, see "Trusting a Profile" section on page 5-17.

Setting Advanced Parameters

The Profile Editor (Advanced) window (see Figure 5-3) enables you to set parameters that control how the client adapter operates within an infrastructure or ad hoc network. To open this window, click the **Advanced** tab from any Profile Editor window.

Figure 5-3 Profile Editor (Advanced) Window

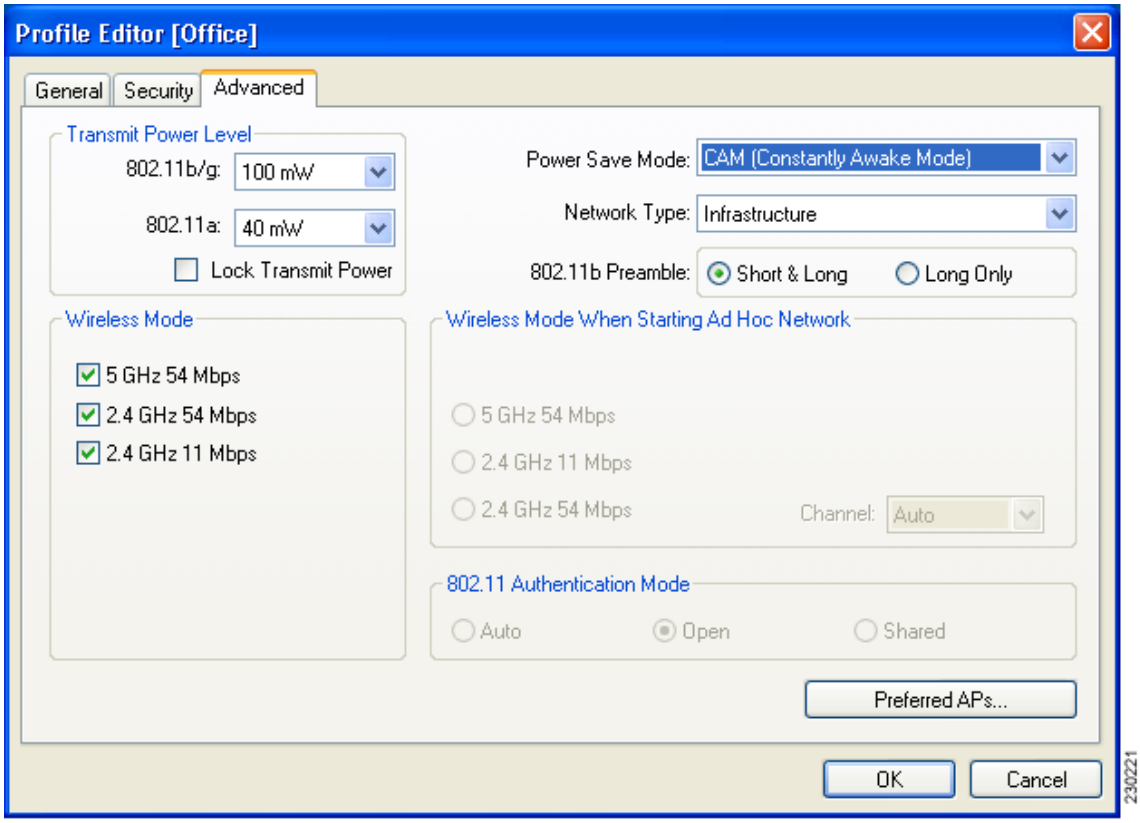


Table 5-3 lists and describes the profile's advanced parameters. Follow the instructions in the table to change any parameters.

Table 5-3 Advanced Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Transmit Power Level</td><td>Specifies the preferred power level at which the client adapter transmits. Although the adapter supports up to 100 mW, the transmit power level actually used is limited to the maximum value allowed by your country's regulatory agency (FCC in the U.S., DOC in Canada, ETSI in Europe, TELEC in Japan, etc.).

Options: Dependent on the radio band used and the power table programmed into the client adapter; see the table below

Default: The maximum power level programmed into the client adapter and allowed by your country's regulatory agency

<table>
<tr><th>Radio Band</th><th>Transmit Power Level</th></tr>
<tr><td>802.11b/g</td><td>1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 20, 32, 50, 63, or 100 mW</td></tr>
<tr><td>802.11a</td><td>1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 13, 20, 25, or 40 mW</td></tr>
</table>
Note When the client adapter operates in 802.11g mode, the maximum transmit power may be capped at a lower level than when operating in the 802.11b mode. This is due to 802.11g-specific regulatory limitations in some countries.

Note Reducing the transmit power level conserves battery power but decreases radio range.</td></tr>
<tr><td>Lock Transmit Power</td><td>Specifies whether or not the transmit power level is set and locked in the ACAU. If you check the Lock Transmit Power check box in the ACAU, a user cannot choose a transmit power level in the ADU. The transmit power level is only displayed in the ADU.

Options: Checked box means that the transmit power level is locked through the ACAU; unchecked box means that the transmit power level is not locked through the ACAU.

Default: Transmit power level not locked in the ACAU

Note The Lock Transmit Power parameter applies to both 802.11a and 802.11b/g settings.</td></tr>
</table>

Table 5-3 Advanced Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Power Save Mode</td><td>Sets the client adapter to its optimum power consumption setting.
Options: CAM (Constantly Awake Mode), Fast PSP (Power Save Mode), or Max PSP (Max Power Saving)
Default: CAM (Constantly Awake Mode)
<table>
<tr><th>Power Save Mode</th><th>Description</th></tr>
<tr><td>CAM (Constantly Awake Mode)</td><td>Keeps the client adapter powered up continuously so there is little lag in message response time.
Consumes the most power but offers the highest throughput. Is recommended for desktop computers and devices that use AC power.
Note This is the only mode available in an ad hoc network.</td></tr>
<tr><td>Fast PSP (Power Save Mode)</td><td>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 have been retrieved.
Is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP.
Note This mode is not available in an ad hoc network.</td></tr>
<tr><td>Max PSP (Max Power Saving)</td><td>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.
Conserves the most power but offers the lowest throughput. Is recommended for devices for which power consumption is the ultimate concern (such as small battery-powered devices).
Note This mode is not available in an ad hoc network.</td></tr>
</table></td></tr>
</table>

Table 5-3 Advanced Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Network Type</td><td>Specifies the type of network in which the client adapter is installed.
Options:Infrastructure or Ad Hoc
Default: Infrastructure

<table><tr><th>Network Type</th><th>Description</th></tr><tr><td>Ad Hoc</td><td>Often referred to as peer to peer. Indicates that the 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 the wireless network is connected to a wired Ethernet network through an access point.</td></tr></table></td></tr>
<tr><td>802.11b Preamble</td><td>Determines whether the client adapter will use both short and long radio headers or only long radio headers. 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 all clients in that cell must also use long headers, even if both this client and the access point have short radio headers enabled.

Short radio headers improve throughput performance; long radio headers ensure compatibility with clients and access points that do not support short radio headers.

Options:Short & Long or Long Only

Default: Short & Long

Note This parameter is disabled if the Wireless Mode parameter does not include the 2.4 GHz 11 Mbps option.</td></tr>
</table>

Table 5-3 Advanced Parameters (continued)

Parameter	Description
Wireless Mode	Specifies the frequency and rate at which the client adapter should transmit packets to or receive packets from access points. **Options:**5 GHz 54 Mbps, 2.4 GHz 54 Mbps, and 2.4 GHz 11 Mbps **Default:** All options selected **Note** When more than one option is selected, the client adapter attempts to use the wireless modes in this order: 5 GHz 54 Mbps, 2.4 GHz 54 Mbps, 2.4 GHz 11 Mbps. **Note** If you choose 2.4 GHz 11 Mbps, the client adapter can associate to access points containing an 802.11b or 802.11g radio at 802.11b data rates. If you choose 2.4 GHz 54 Mbps, the client adapter can associate to access points containing an 802.11b radio at 802.11b data rates or to access points containing an 802.11g radio at 802.11b or 802.11g data rates. **Note** When you enable auto profile selection, the client adapter ignores the selected profile's wireless mode setting and scans the wireless modes specified by all the profiles in the auto profile selection list for an available network. Using this method, the client does not need to disassociate nor change the current profile while looking for networks in other profiles. **Note** The client adapter's wireless mode must match that of the access points with which it is to communicate. Otherwise, the client adapter may not be able to associate to them.
Wireless Mode When Starting Ad Hoc Network	Specifies the frequency and rate at which the client adapter should transmit packets to or receive packets from other clients (in ad hoc mode). **Options:**5 GHz 54 Mbps, 2.4 GHz 11 Mbps, or 2.4 GHz 54 Mbps **Default:** 5 GHz 54 Mbps **Note** The client scans the band(s) specified by the Wireless Mode parameter before creating a new ad hoc cell based on the band specified by the Wireless Mode When Starting Ad Hoc Network parameter. **Note** The client adapter's wireless mode must match that of the other clients with which it is to communicate. Otherwise, the client adapter may not be able to associate to them. **Note** The 2.4 GHz 54 Mbps wireless mode may not be functional on some vendors' products. In this case, the client adapter uses the 2.4 GHz 11 Mbps wireless mode.

Table 5-3 Advanced Parameters (continued)

Parameter	Description
Channel	Specifies the channel that the client adapter uses for communications in a 2.4-GHz ad hoc network. The available channels conform to the IEEE 802.11 Standard for your regulatory domain. The channel of the client adapter must be set to match the channel used by the other clients in the wireless network. If the client adapter does not find any other ad hoc clients, this parameter specifies the channel with which the adapter will start its cell. **Range:** Dependent on regulatory domain **Example:** 1 to 11 (2412 to 2462 MHz) in North America **Default:** Auto (the client automatically determines the channel on which to start communications) **Note** This parameter is available only when 2.4 GHz 11 Mbps or 2.4 GHz 54 Mbps is selected for the Wireless Mode When Starting Ad Hoc Network parameter. When 5 GHz 54 Mbps is selected, the Channel parameter is set to Auto automatically. **Note** Refer to Appendix B for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.

Table 5-3 Advanced Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>802.11 Authentication Mode</td><td>Specifies how the client adapter attempts to authenticate to an access point. Open and shared authentication do not rely on a RADIUS server on the user's network.

Options: Auto, Open, or Shared

Default: Open

<table>
<tr><th>802.11 Authentication Mode</th><th>Description</th></tr>
<tr><td>Auto</td><td>Causes the client adapter to attempt to authenticate using shared authentication. If it fails, the client adapter then attempts to authenticate using open authentication.</td></tr>
<tr><td>Open</td><td>Enables the client adapter, regardless of its WEP settings, to authenticate and attempt to communicate with an access point. However, communication can occur only if the adapter's WEP key matches that of the access point.</td></tr>
<tr><td>Shared</td><td>Enables the client adapter to authenticate and communicate only with access points that have the same WEP key.

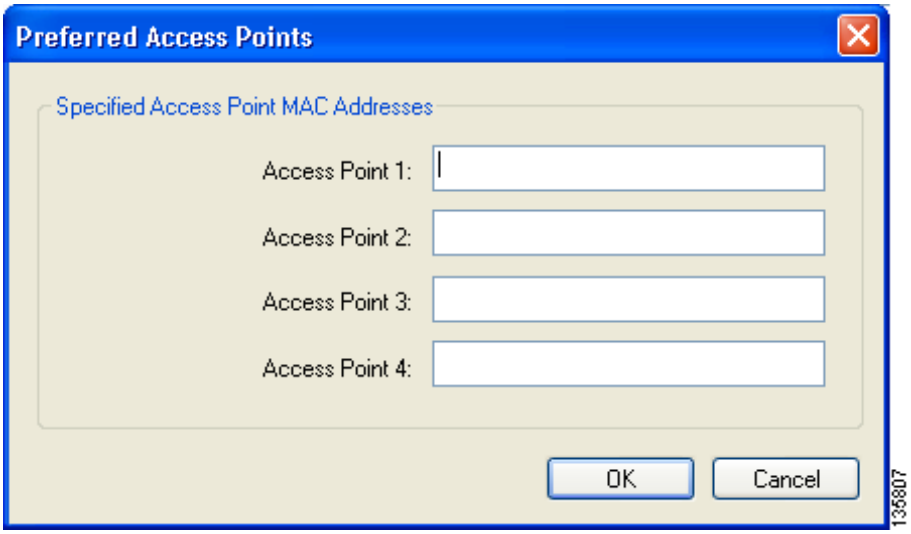
During shared key authentication, the access point sends an encrypted challenge packet to the client adapter, which encrypts the packet and sends it back to the access point. The access point attempts to decrypt the encrypted packet and sends an authentication response packet indicating the success or failure of the decryption back to the client adapter. If the packet is successfully encrypted/decrypted, the user is considered to be authenticated.</td></tr>
</table>
Note Cisco recommends that Auto and Shared not be used because they present a security risk.

Note The client adapter's 802.11 authentication mode setting must match that of the access points with which it is to communicate. Otherwise, the client adapter may not be able to authenticate to them.

Note If this profile is configured for use in an adhoc network or is not configured to use static WEP, this parameter is unavailable, and Open authentication is used.</td></tr>
</table>

If this profile is configured for use in an infrastructure network and you want to specify up to four access points to which the client adapter should attempt to associate, click **Preferred APs**. The Preferred Access Points window appears (see Figure 5-4).

Figure 5-4 Preferred Access Points Window



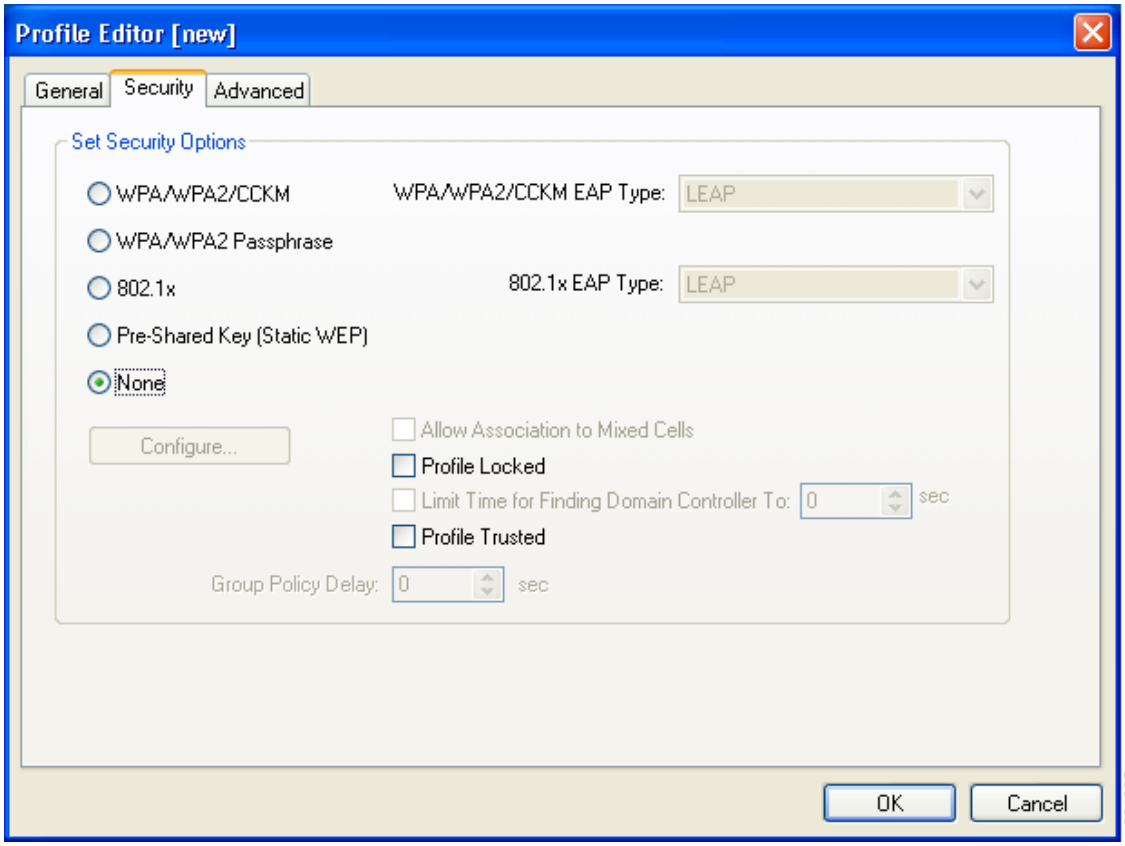
Leave the Access Point 1-4 fields blank or enter the MAC addresses of up to four preferred access points to which the client adapter can associate; then click **OK**. (The MAC address should consist of 12 hexadecimal characters.) If the specified access points are not found or the client adapter roams out of range, the adapter may associate to another access point.

Go to the next section to set security parameters or click **OK** to return to the Profile Management window.

Setting Security Parameters

The Profile Editor (Security) window (see Figure 5-5) 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. To open this window, click the **Security** tab from any Profile Editor window.

Figure 5-5 Profile Editor (Security) Window



This window is different from the other Profile Editor windows in that it includes many 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. Therefore, this section provides an overview of the security features as well as procedures for enabling them. Before moving on, however, you must decide whether to lock this particular profile. See the section below for more information.

Limiting Time for Finding a Domain Controller

If you want to limit the amount of time that is spent searching for a domain controller during the authentication process, check the **Limit Time for Finding Domain Controller To** check box. Then in the edit box, enter the amount of time (in seconds) to which you want to limit the search for the domain controller. A timeout value of 0 causes the authentication process to bypass the "Finding Domain Controller" step altogether.

Range of timeout value: 0 to 300 seconds

Default: Unchecked; 0 seconds

Locking a Profile

As an added security measure, ACAU gives you the option of locking individual profiles, which prevents users from being able to modify or remove these profiles. This feature ensures a high level of security and consistent configurations. It is especially useful if you want to create a standard profile for the corporate network, distribute it to each user, and ensure that it cannot be modified or removed.

The following rules apply to locked profiles:

- Locked profiles can be created only by an administrator using ACAU.
- A profile can be individually locked or unlocked; however, a user's ability to modify profiles (through ACAU's Global Settings - User Settings parameters) takes precedence. For example, if a user is not permitted to modify a profile, he or she is also unable to modify an unlocked profile.
- A locked profile cannot be overwritten, either by import or from the conversion of a 350 or CB20A profile through the profile migration tool.
- When a locked profile is exported and then imported onto another machine, the profile remains locked.
- All fields in a locked profile are read-only except password fields, which can be edited.

Perform one of the following:

- If you want to prevent users from being able to modify or remove this profile, check the **Profile Locked** check box.
- If you want to allow users to modify or remove this profile, uncheck the **Profile Locked** check box. This is the default setting.

Trusting a Profile

Check the **Profile Trusted** check box so that the profile can have full reporting privileges in diagnostic channel mode. If you do not check this check box, the profile is untrusted, and only the results of the following diagnostic channel mode tests are reported:

- ping test
- DHCP test
- IP connectivity test
- DNS ping test
- DNS name resolution test
- 802.11 association test
- 802.11X authentication test

You can specify a diagnostic SSID in the Profile Editor General tab. If you do not provide a diagnostic SSID, the client uses the value diagSSID in the Diagnostic SSID field. For more information, see the "Troubleshooting with Diagnostic Channel Mode" section on page 5-6.

Overview of Security Features

You can protect the user's data as it is transmitted through the wireless network by encrypting it through the use of 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 the adapter or dynamically created as part of the EAP authentication process. The information in the "Static WEP Keys" and "EAP (with 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 in length. 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 5-24 for information on three security features that can make WEP keys even more secure.

Static WEP Keys

Each device (or profile) within the 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.

The user does not need to re-enter static WEP keys 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 Configure Pre-Shared Keys (Static WEP) window enables you to view the WEP key settings for a particular profile and to assign new WEP keys or overwrite existing WEP keys. Refer to the "Enabling Static WEP" section on page 5-28 for instructions.

EAP (with Dynamic WEP Keys)

The standard for wireless LAN security, as defined by 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.

Five 802.1X authentication types are available in ACAU for use with Windows 2000 or XP:

- **EAP-Cisco Wireless** (or **LEAP**)—This authentication type leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. ACAU offers a variety of LEAP configuration options, including how 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 need to be re-entered each time the client adapter is inserted or the Windows device is rebooted unless the client adapter is using a profile with saved LEAP credentials.

  RADIUS servers that support LEAP include Cisco Secure ACS release 2.6 or later, Cisco Access Registrar release 1.7 or later, Funk Software's Steel-Belted RADIUS release 4.1 or later, and Meetinghouse Data Communications' AEGIS release 1.1 or later.

- **EAP-FAST**—This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunneled authentication process to provide advanced 802.1X EAP mutual authentication.

  - Phase 0 enables the client to dynamically provision a protected access credentials (PAC) when necessary. During this phase, a PAC is generated securely between the user and the network.
  - Phase 1 uses the PAC to establish a mutually authenticated and secure tunnel between the client and the RADIUS server. RADIUS servers that support EAP-FAST include Cisco Secure ACS version 3.2.3 and later.
  - Phase 2 performs client authentication in the established tunnel.

  ACAU offers a variety of EAP-FAST configuration options, including how and when a username and password are entered to begin the authentication process and whether automatic or manual PAC provisioning is used.

The client adapter uses the username, password, and PAC 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 the client adapter is using a profile with 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. When manual PAC provisioning is enabled, the PAC is manually copied from the server and imported onto the client device. The following rules govern PAC storage:

- PACs are stored as encrypted data files in either the global or private store on the user's computer.
  - Global PACs can be accessed and used by any user at any logon stage. They are available before or during logon or after the user is logged off if the profile is not configured with the No Network Connection Unless User Is Logged In option.
  - Private PACs can be accessed and used only by the user who provisioned them or the system administrator.

  Note Global PACs are stored on C:\Document and Settings\All Users\Application Data\Cisco\cscostore, and private PACs are stored on C:\Document and Settings*user*\Application Data\Cisco\cscostore.

- If automatic PAC provisioning is enabled and it occurs after the user is logged on, the PAC is stored in the private store of the currently logged-on user. Otherwise, the PAC is stored in the global store.
- PAC files can be added or overwritten using the import feature.
- PAC files can be removed using the delete feature. They are also deleted when the client adapter software is uninstalled.
- PAC files are tied to the machine, so they cannot be used if copied to another machine.

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.

- **EAP-TLS**—This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It uses a client certificate for authentication.

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

- **PEAP (EAP-GTC)**—This PEAP authentication type 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 instead of a client certificate for authentication. PEAP (EAP-GTC) uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. If the user's network uses an OTP user database, PEAP (EAP-GTC) requires the user to enter a hardware or software token password to start the EAP authentication process and gain access to the network. If the user's network uses a Windows NT or 2000 domain user database or an LDAP user database (such as NDS), PEAP (EAP-GTC) requires the user to enter a username, password, and domain name in order to start the authentication process.

  RADIUS servers that support PEAP (EAP-GTC) authentication include Cisco Secure ACS release 3.1 or later.

- **PEAP (EAP-MSCHAP V2)**—This PEAP authentication type is based on EAP-TLS authentication but uses a password or client certificate for authentication. PEAP (EAP-MSCHAP V2) uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.

  RADIUS servers that support PEAP (EAP-MSCHAP V2) authentication include Cisco Secure ACS release 3.2 or later.

When the access point is configured as indicated in Table 5-4 on page 5-24 and the client adapter is configured for LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2), 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 and PEAP), PAC (EAP-FAST), or certificate (EAP-TLS and PEAP) being the shared secret for authentication. The password and PAC are 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 following pages for instructions on enabling these EAP types:

- LEAP, page 5-31
- EAP-FAST, page 5-35
- EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2), page 5-47

Note 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/ios120/12cgcr/secur_c/scprt2/scrad.htm

WPA and WPA2

Wi-Fi Protected Access (WPA) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification; WPA2 is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard.

WPA uses Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Both WPA and WPA2 use 802.1X for authenticated key management.

Both WPA and WPA2 support two mutually exclusive key management types: WPA/WPA2 and WPA/WPA2 passphrase (also known as *WPA pre-shared key* or *WPA-PSK*). Using WPA or WPA2, 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). The server generates the PMK dynamically and passes it to the access point. Using WPA or WPA2 passphrase, however, you configure a passphrase (or pre-shared key) on both the client and the access point, and that passphrase is used as the PMK.

Refer to the following pages for instructions on enabling these WPA variations:

- WPA/WPA2 passphrase, page 5-30
- LEAP with WPA/WPA2, page 5-31
- EAP-FAST with WPA/WPA2, page 5-22
- EAP-TLS with WPA/WPA2, page 5-48
- PEAP (EAP-GTC) with WPA/WPA2, page 5-51
- PEAP (EAP-MSCHAP V2) with WPA/WPA2, page 5-55

Note WPA must also be enabled on the access point. To use WPA, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2, access points must use Cisco IOS Release 12.3(2)JA or later. Refer to the documentation for your access point for instructions on enabling this feature.

CCKM Fast Secure Roaming

Some applications that run on a client device may require fast roaming between access points. Voice applications, for example, require it to prevent delays and gaps in conversation. CCKM fast secure roaming is enabled automatically for CB21AG and PI21AG clients using WPA/WPA2/CCKM with LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2). However, this feature must be enabled on the access point.

During normal operation, EAP-enabled clients mutually authenticate with a new access point by performing a complete EAP authentication, including communication with the main RADIUS server. However, when you configure your wireless LAN for CCKM fast secure roaming, EAP-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 Cisco client devices to roam from one access point to another typically in under 150 milliseconds (ms). CCKM fast secure 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.

Note If you want to enable CCKM fast secure roaming on the client adapter, you must choose the WPA/WPA2/CCKM security option on the Profile Editor (Security) window, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which the client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

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

Note The Microsoft Wireless Configuration Manager and the Microsoft 802.1X supplicant, if installed on the user's computer, must be disabled in order for CCKM fast secure roaming to operate correctly. If the computer is running Windows XP and the user chooses to configure the client adapter using ADU during installation, these features should already be disabled. Similarly, if the computer is running Windows 2000, the Microsoft 802.1X supplicant, if installed, should already be disabled.

Reporting Access Points that Fail LEAP Authentication

The CB21AG and PI21AG client adapters and the following access point firmware versions support a feature that is designed to detect access points that fail LEAP authentication:

- 12.00T or later (access points running VxWorks)
- Cisco IOS Release 12.2(4)JA or later (1100 series access points)
- Cisco IOS Release 12.2(8)JA or later (1200 series access points)
- Cisco IOS Release 12.2(13)JA or later (350 series access points)

An access point running one of these firmware versions records a message in the system log when the client discovers and reports another access point in the wireless network that has failed LEAP authentication.

The process takes place as follows:

1. A client with a LEAP profile attempts to associate to access point A.
2. Access point A does not handle LEAP authentication successfully, perhaps because the access point does not understand LEAP or cannot communicate to a trusted LEAP 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 by both devices. However, the access points must use the specified firmware versions 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 client adapter software. However, they must be enabled on the access point.

Note 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.

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 TKIP is enabled automatically when WPA is enabled, and it is disabled when WPA is disabled.

Broadcast Key Rotation

When you enable broadcast WEP key rotation, the access point provides a dynamic broadcast WEP key and changes it at the interval you select.

Synchronizing Security Features

In order to use any of the security features discussed in this section, both the client adapter and the access point to which it will associate must be set appropriately. Table 5-4 indicates the client and access point settings required for each security feature. This chapter provides specific instructions for enabling the security features on the client adapter. Refer to the documentation for your access point for instructions on enabling any of these features on the access point.

Table 5-4 Client and Access Point Security Settings

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Choose Open authentication and Pre-Shared Key (Static WEP) and create a WEP key	Set up and enable WEP and enable Open Authentication for the SSID
Static WEP with shared key authentication	Choose Shared authentication and Pre-Shared Key (Static WEP) and create a WEP key	Set up and enable WEP and enable Shared Key Authentication for the SSID

Table 5-4 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
WPA or WPA2 passphrase (or WPA or WPA2 pre-shared key)	Choose WPA/WPA2 Passphrase and enter the passphrase	Choose a cipher suite, enable Open Authentication and WPA for the SSID, and enter a WPA pre-shared key **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
LEAP authentication	Choose 802.1x and LEAP; then set LEAP settings	Set up and enable WEP and enable Network-EAP Authentication for the SSID
LEAP authentication with WPA or WPA2	Choose WPA/WPA2/CCKM and LEAP; then set LEAP settings	For WPA, choose a cipher suite that includes TKIP and enable Network-EAP and Open with EAP Authentication and WPA for the SSID For WPA2, choose a cipher suite that includes AES-CCMP and enable Network-EAP and Open with EAP Authentication and WPA for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
EAP-FAST authentication	Choose 802.1x and EAP-FAST, set EAP-FAST settings, and enable automatic provisioning or import a PAC file	Set up and enable WEP and enable both Network-EAP and Open with EAP Authentication for the SSID
EAP-FAST authentication with WPA or WPA2	Choose WPA/WPA2/CCKM and EAP-FAST, set EAP-FAST settings, and enable automatic provisioning or import a PAC file	For WPA, choose a cipher suite that includes TKIP and enable both Network-EAP and Open with EAP Authentication as well as WPA for the SSID For WPA2, choose a cipher suite that includes AES-CCMP and enable both Network-EAP and Open with EAP Authentication as well as WPA for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.

Table 5-4 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
EAP-TLS authentication	Choose 802.1x and EAP-TLS; then set EAP-TLS settings	Set up and enable WEP and enable Open with EAP Authentication for the SSID
EAP-TLS authentication with WPA or WPA2	Choose WPA/WPA2/CCKM and EAP-TLS; then set EAP-TLS settings	For WPA, choose a cipher suite that includes TKIP; then enable WPA and Open with EAP Authentication for the SSID For WPA2, choose a cipher suite that includes AES-CCMP; then enable WPA and Open with EAP Authentication for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
PEAP authentication	Choose 802.1x and PEAP (EAP-GTC) or PEAP (EAP-MSCHAP V2); then set PEAP settings	Set up and enable WEP and enable Open with EAP Authentication for the SSID
PEAP authentication with WPA or WPA2	Choose WPA/WPA2/CCKM and PEAP (EAP-GTC) or PEAP (EAP-MSCHAP V2); then set PEAP settings	For WPA, choose a cipher suite that includes TKIP; then enable WPA and Open with EAP Authentication for the SSID For WPA2, choose a cipher suite that includes AES-CCMP; then enable WPA and Open with EAP Authentication for the SSID **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.

Table 5-4 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
CCKM fast secure roaming	Choose WPA/WPA2/CCKM and LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP MSCHAP V2); then set the EAP authentication settings **Note** If you want to enable CCKM, you must choose WPA/WPA2/CCKM, regardless of whether you want the client adapter to use WPA or WPA2. The configuration of the access point to which the client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.	Use Cisco IOS Release 12.2(11)JA or later, choose a cipher suite that is compatible with CCKM, enable both Network-EAP and Open with EAP Authentication and CCKM for the SSID, and configure for participation in wireless domain services (WDS) **Note** To allow both 802.1X clients and non-802.1X clients to use the SSID, enable optional CCKM.
Reporting access points that fail LEAP authentication	No settings required; automatically enabled	No settings required; automatically enabled in the firmware versions listed on page 5-23.
MIC	No settings required; automatically enabled	Set up and enable WEP with full encryption, set MIC to MMH or check the Enable MIC check box, and set Use Aironet Extensions to Yes
TKIP	No settings required; automatically enabled	Set up and enable WEP, set TKIP to Cisco or check the Enable Per Packet Keying check box, and set Use Aironet Extensions to Yes
Broadcast key rotation	Enable LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2)	Set up and enable WEP and set Broadcast WEP Key Rotation Interval to any value other than zero (0)

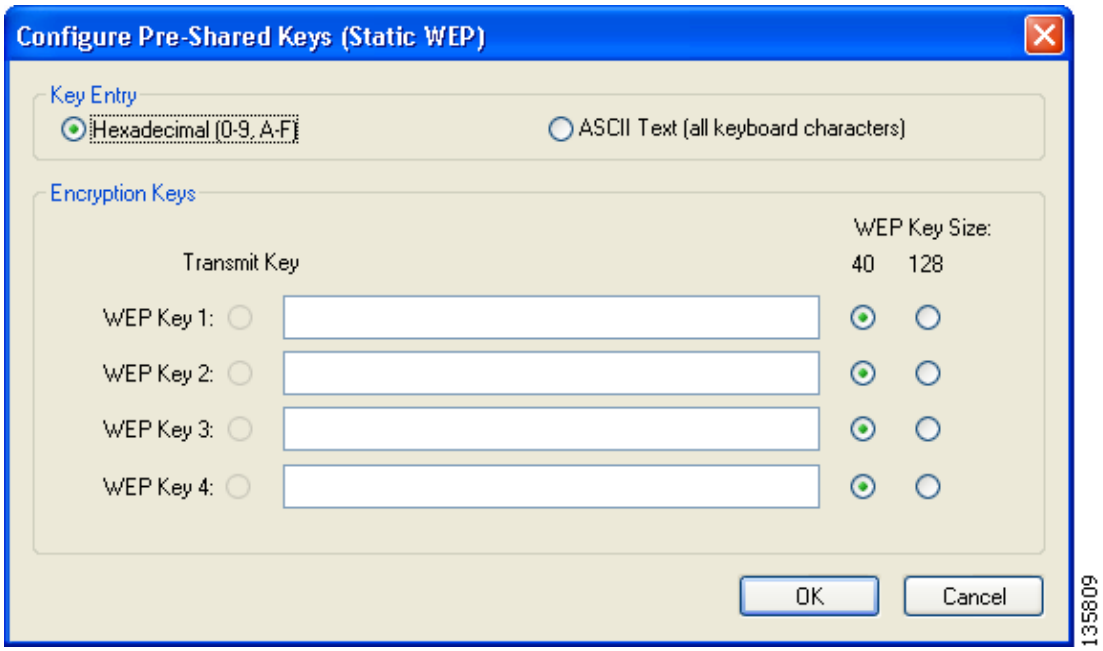
Enabling Static WEP

Follow the steps below to enable static WEP for this profile.

Step 1 Select **Pre-Shared Key (Static WEP)** on the Profile Editor (Security) window.

Step 2 Click **Configure**. The Configure Pre-Shared Keys (Static WEP) window appears (see Figure 5-6).

Figure 5-6 Configure Pre-Shared Keys (Static WEP) Window



Step 3 Choose one of the following WEP key entry methods:

- **Hexadecimal (0-9, A-F)**—Specifies that the WEP key will be entered in hexadecimal characters, which include 0-9, A-F, and a-f.
- **ASCII Text (all keyboard characters)**—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 the Cisco Aironet 1200 Series Access Points, so you must choose the Hexadecimal (0-9, A-F) option if the client adapter may be used with these access points.

Step 4 For the static WEP key that you are entering (1, 2, 3, or 4), select a WEP key size of 40 or 128 on the right side of the window. 128-bit client adapters can use 40- or 128-bit keys, but 40-bit adapters can use only 40-bit keys. If 128 bit is not supported by the client adapter, this option is unavailable.

Step 5 Enter the static WEP key 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)

Note You must enter hexadecimal characters if the client adapter may be used with Cisco Aironet 1200 Series Access Points.

- The client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode).
- 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.

Note All existing static WEP keys are displayed as bullets for security reasons. If you need to modify a WEP key, simply click in the WEP key field, delete the bullets, and enter a new key.

Step 6 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 7 Click **OK** to save your changes and return to the Profile Editor (Security) window.

Step 8 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. 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 to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

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. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 9 Click **OK** to save your settings and return to the Profile Management window.

Enabling WPA/WPA2 Passphrase

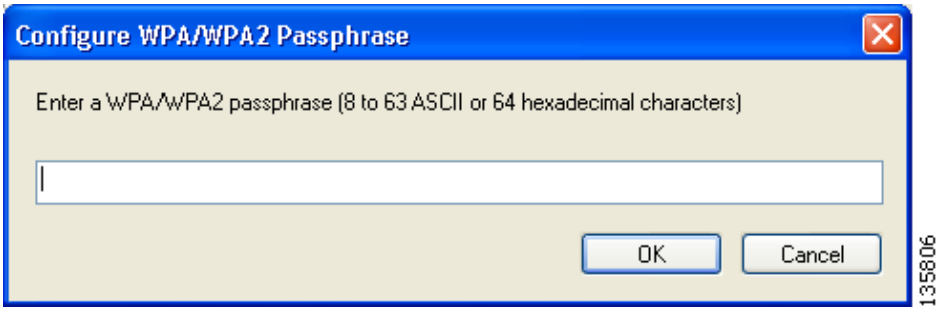
Follow the steps below to enable WPA/WPA2 passphrase (also known as *WPA/WPA2 pre-shared key*) for this profile.

Note To use WPA passphrase, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2 passphrase, access points must use Cisco IOS Release 12.3(2)JA or later.

Step 1 Select **WPA/WPA2 Passphrase** on the Profile Editor (Security) window.

Step 2 Click **Configure**. The Configure WPA/WPA2 Passphrase window appears (see Figure 5-7).

Figure 5-7 Configure WPA/WPA2 Passphrase Window



Step 3 Enter the WPA/WPA2 passphrase for the access point (in an infrastructure network) or other clients (in an ad hoc network) in the WPA/WPA2 passphrase field. Follow the guidelines below to enter a passphrase:

- WPA/WPA2 passphrases must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
- The client adapter's WPA/WPA2 passphrase must match the passphrase used by the access point.

Step 4 Click **OK** to save the passphrase and return to the Profile Editor (Security) window.

Step 5 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the user's computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 6 Click **OK** to save your settings and return to the Profile Management window.

Enabling LEAP

In order to use LEAP authentication, the devices on the user's network must meet the following requirements:

- Access points to which the client adapter may attempt to authenticate must use the following firmware versions or later: 11.23T (access points running VxWorks), Cisco IOS Release 12.2(4)JA (1100 series access points), Cisco IOS Release 12.2(8)JA (1200 series access points), or Cisco IOS Release 12.2(13)JA (350 series access points).

Note To use WPA or CCKM, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2, access points must use Cisco IOS Release 12.3(2)JA or later. To use the Reporting Access Points That Fail LEAP Authentication feature, access points must use the firmware versions listed on page 5-24.

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

Follow the steps below to enable LEAP authentication for this profile.

Step 1 Perform one of the following on the Profile Editor (Security) window:

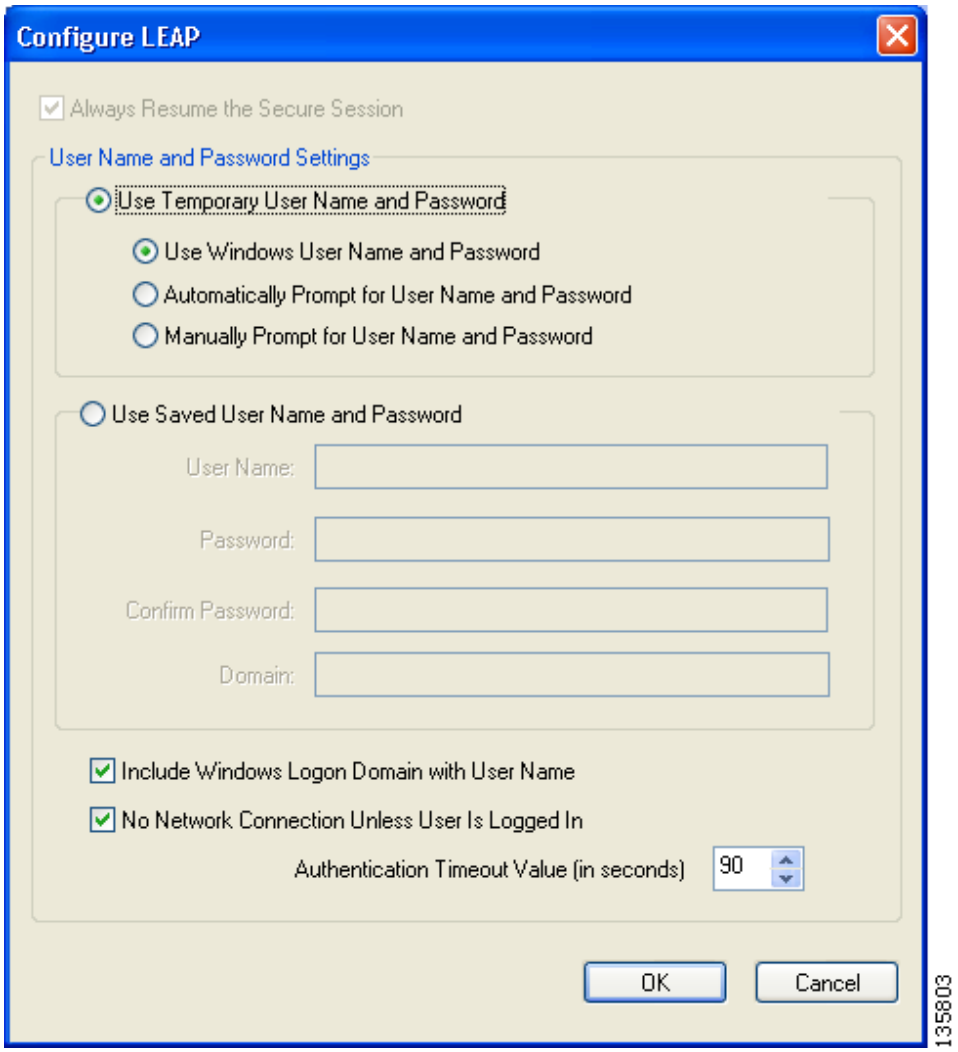
- If you want to enable LEAP without WPA or WPA2, choose **802.1x** under Set Security Options and **LEAP** in the 802.1x EAP Type drop-down box.
- If you want to enable LEAP with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **LEAP** in the WPA/WPA2/CCKM EAP Type drop-down box.

Note If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which the client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" section on page 5-22 for additional information.

Step 2 Click **Configure**. The Configure LEAP window appears (see Figure 5-8).

Figure 5-8 Configure LEAP Window



Step 3 Choose one of the following LEAP username and password setting options:

- **Use Temporary User Name and Password**—Requires the user to enter the 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**—Does not require the user to enter a LEAP username and password each time the computer reboots. Authentication occurs automatically as needed using a saved username and password (which are registered with the RADIUS server).

Step 4 Perform one of the following:

- If you selected Use Temporary User Name and Password in Step 3, select one of the following options:
  - **Use Windows User Name and Password**—Causes the user's Windows username and password to also serve as the LEAP username and password, giving the user only one set of credentials to remember. After the user logs in, the LEAP authentication process begins automatically. This option is the default setting.
  - **Automatically Prompt for User Name and Password**—Requires the user to enter a separate LEAP username and password (which are registered with the RADIUS server) in addition to the regular Windows login in order to start the LEAP authentication process.
  - **Manually Prompt for User Name and Password**—Requires the user to manually invoke the LEAP authentication process as needed using the Manual Login option in the ADU Action drop-down menu or ASTU. The user is 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.
- If you chose Use Saved User Name and Password in Step 3, follow these steps:
  a. Enter a username and password in the appropriate fields.
  b. Re-enter the password in the Confirm Password field.
  c. If you wish to specify a domain name that is passed to the RADIUS server along with the username, enter it in the Domain field.

Step 5 If you chose Automatically Prompt for User Name and Password or Manually Prompt for User Name and Password in Step 4, perform one of the following:

- Check the **Always Resume the Secure Session** check box at the top of the window if you want the LEAP supplicant to always attempt to resume the previous session without prompting the user to re-enter his or her credentials whenever the client adapter becomes disassociated. Session resume occurs after the client temporarily loses connection to the access point (such as by roaming in and out of range) or wakes up from suspend or hibernate mode. This is the default setting.
- Uncheck the **Always Resume the Secure Session** check box if you want the user to be prompted to re-enter his or her LEAP username and password whenever the client adapter temporarily loses association by roaming out of range or wakes up from suspend or hibernate mode.

Note Checking this check box gives the user the convenience of not having to re-enter his or her username and password when the client adapter experiences momentary losses of association. However, if the user leaves the device unattended during the period of time when the LEAP session can be resumed without re-entering user credentials, be aware that someone can resume the user's LEAP session and access the network.

Note The Always Resume the Secure Session check box is disabled if you chose Use Windows User Name and Password or Use Saved User Name and Password in Step 4.

Step 6 If the user works in an environment with multiple domains and you want the Windows login domain to be passed to the RADIUS server along with the username, check the **Include Windows Logon Domain with User Name** check box. The default setting is checked.

Note If you chose to use a saved username and password but do not check the Include Windows Logon Domain with User Name check box, the saved domain name is not passed to the RADIUS server.

Step 7 If you want to force the client adapter to disassociate after the user logs off so that another user cannot gain access to the wireless network using the user's credentials, check the **No Network Connection Unless User Is Logged In** check box. The default setting is checked.

Step 8 In the Authentication Timeout Value field, choose the amount of time (in seconds) before a LEAP authentication attempt is considered to be failed and an error message appears.

Range: 30 to 300 seconds

Default: 90 seconds

Step 9 Click **OK** to save your changes and return to the Profile Editor (Security) window.

Step 10 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. 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 to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x or Pre-Shared Keys (Static WEP) security option is selected.

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. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 11 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the user's computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 12 Click **OK** to save your settings and return to the Profile Management window.

Enabling EAP-FAST

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

- Access points to which your client adapter may attempt to authenticate must use the following firmware versions or later: 11.23T (340 and 350 series access points), 11.54T (1200 series access points), Cisco IOS Release 12.3(4)JA (1130 series and BR 1310 series access points), Cisco IOS Release 12.3(7)JA (1240 series access points), or Cisco IOS Release 12.2(4)JA (1100 series access points).

  Note To use WPA or CCKM, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2, access points must use Cisco IOS Release 12.3(2)JA or later. To use the Reporting Access Points That Fail LEAP or EAP-FAST Authentication feature, access points must use the firmware versions listed on page 5-23.

  Note The access point to which your client adapter will associate must be configured for open authentication.

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

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

Step 1 Perform one of the following on the Profile Management (Security) window:

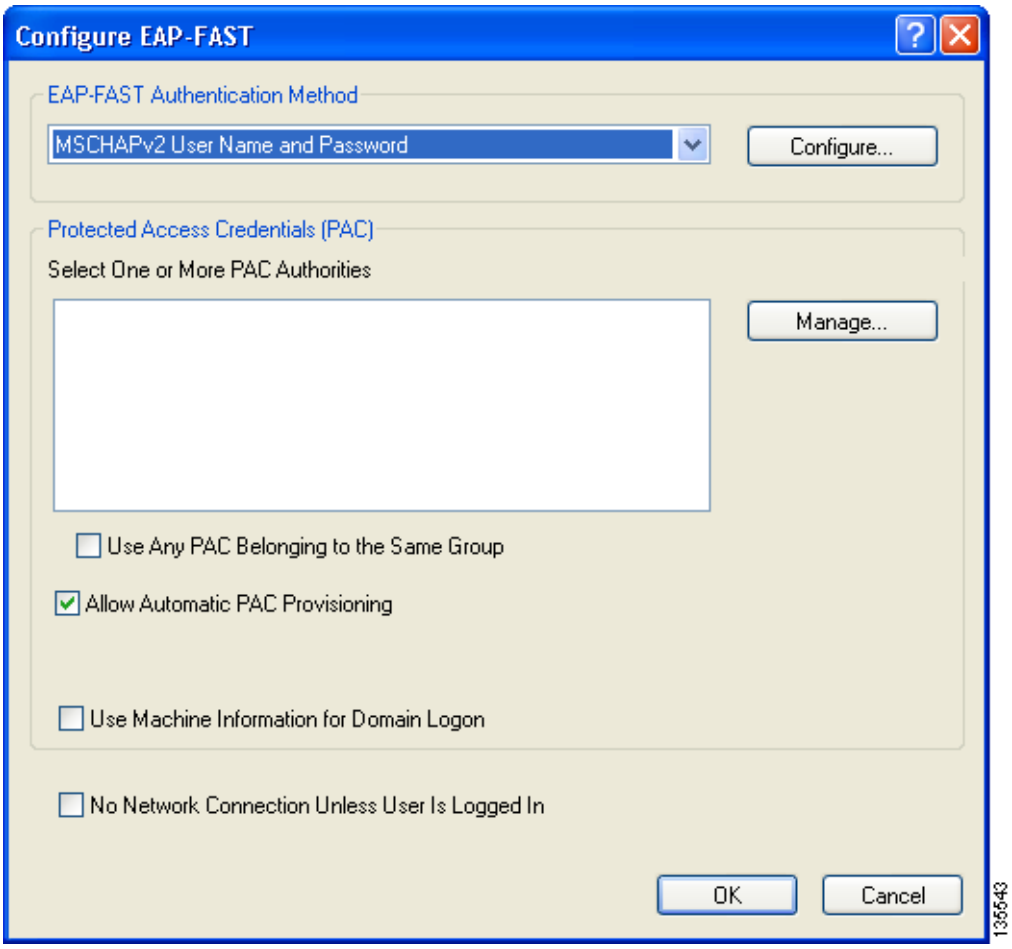
- If you want to enable EAP-FAST without WPA or WPA2, choose **802.1x** under Set Security Options and **EAP-FAST** in the 802.1x EAP Type drop-down box.
- If you want to enable EAP-FAST with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **EAP-FAST** in the WPA/WPA2/CCKM EAP Type drop-down box.

Note If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" section on page 5-22 for additional information.

Step 2 Click **Configure**. The Configure EAP-FAST window appears (see Figure 5-9).

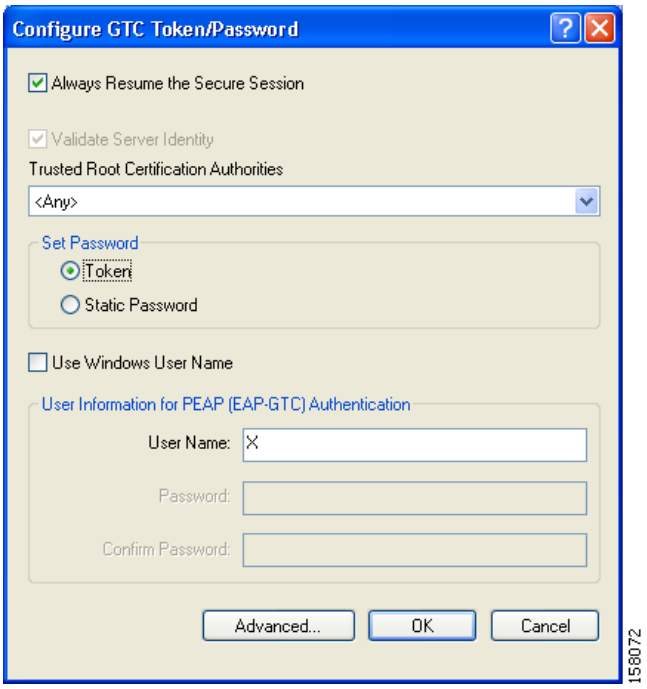
Figure 5-9 Configure EAP-FAST Window



Step 3 Choose an authentication method from the EAP-FAST Authentication Method drop-down list and click Configure.

Step 4 If you chose **GTC Token/Password** in Step 3, do the following in the Configure GTC Token/Password window (see Figure 5-10):

Figure 5-10 Configure GTC Token/Password Window



a. Check the **Always Resume the Secure Session** check box at the top of the window if you want the EAP-FAST supplicant to always attempt to resume the previous session without prompting you to re-enter your credentials whenever the client adapter becomes disassociated. The session resumes after the client temporarily loses connection to the access point (such as by roaming in and out of coverage) or wakes up from suspend or hibernate mode. This is the default setting.

Uncheck the **Always Resume the Secure Session** check box if you want to be prompted to re-enter your EAP-FAST username and password whenever your client adapter temporarily loses association by roaming out of coverage or wakes up from suspend or hibernate mode.

Note Checking this check box gives you the convenience of not having to re-enter your network credentials when your client adapter experiences momentary losses of association. However, if you leave your device unattended during the period of time when the EAP-FAST session can be resumed without re-entering user credentials, be aware that someone can resume your EAP-FAST session and access the network.

Note The Always Resume the Secure Session check box is disabled if you chose **Static Password**.

b. Check the **Validate Server Identity** check box to force the system to validate the identity of the server as an added level of security.

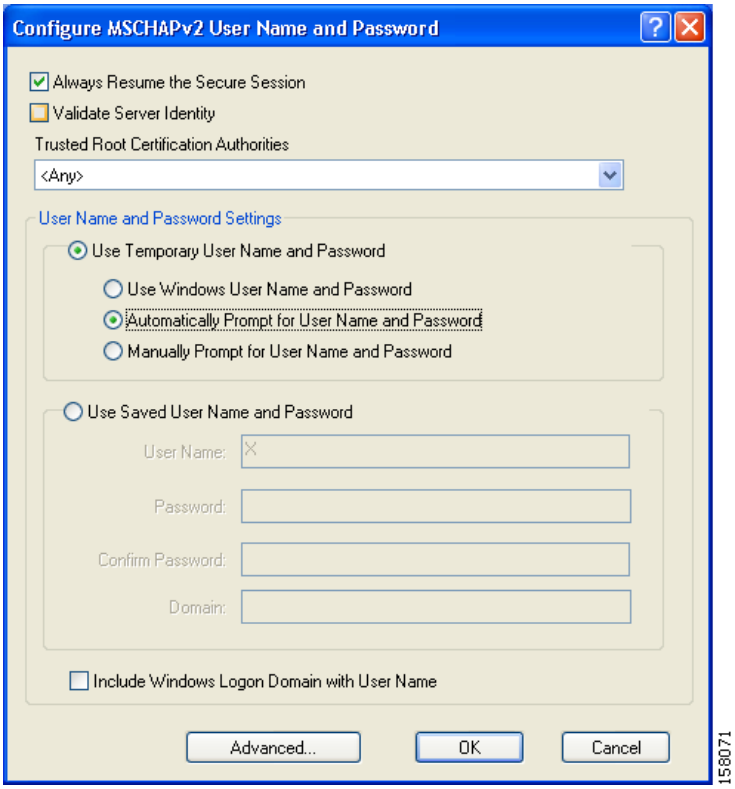
If you uncheck this box, only user credentials will be validated.

c. To configure the remaining options in this window, refer to "Enabling PEAP (EAP-GTC)" section on page 5-51.

d. Click **OK** to save your settings and return to the Configure EAP-FAST window.

Step 5 If you chose **MSCHAPv2 User Name and Password** in Step 3, do the following in the Configure MSCHAPv2 User Name and Password window (see Figure 5-11):

Figure 5-11 Configure MSCHAPv2 User Name and Password Window



1. Check the **Always Resume the Secure Session** check box at the top of the window if you want the EAP-FAST supplicant to always attempt to resume the previous session without prompting you to re-enter your credentials whenever the client adapter becomes disassociated. The session resumes after the client temporarily loses connection to the access point (such as by roaming in and out of coverage) or wakes up from suspend or hibernate mode. This is the default setting.

   Uncheck the **Always Resume the Secure Session** check box if you want to be prompted to re-enter your EAP-FAST username and password whenever your client adapter temporarily loses association by roaming out of coverage or wakes up from suspend or hibernate mode.

Note To check or uncheck the **Always Resume the Secure Session** check box, you must first choose **Automatically Prompt for User Name and Password** or **Manually Prompt for User Name and Password** under Use Temporary User Name and Password.

2. Check the **Validate Server Identity** check box to force the system to validate the identity of the server as an added level of security.

   If you uncheck this box, only user credentials will be validated.

3. Choose a certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box, or, if applicable, choose **<Any>**.
4. To use a temporary username and password, choose **Use Temporary User Name and Password**.

   This option requires you to enter the EAP-FAST username and password each time the computer reboots in order to authenticate and gain access to the network, unless you choose **Use Windows User Name and Password**.

   Choose one of the following options under Use Temporary User Name and Password:

   - **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 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 RADIUS server) in addition to your regular Windows login in order to start the authentication process.
   - **Manually Prompt for User Name and Password**—Requires you to manually invoke the EAP-FAST authentication process as needed using the Manual Login option in the Action drop-down menu or ASTU. You are not prompted to enter an 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.
5. To use a saved username and password, choose **Use Saved User Name and Password**.

   This option does not require you to enter an EAP-FAST username and password each time the computer reboots. Authentication occurs automatically as needed using a saved username and password (which are registered with the RADIUS server).

   Follow these steps to specify the username and password to use for EAP-FAST authentication:

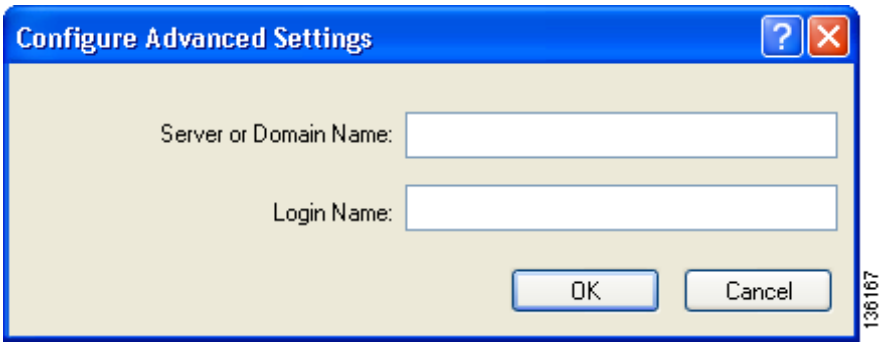
   a. Enter a username and password in the appropriate fields.
   b. Re-enter the password in the Confirm Password field.
   c. If you wish to specify a domain name that will be passed to the RADIUS server along with your username, enter it in the Domain field.
6. If you work in an environment with multiple domains and therefore want your Windows login domain to be passed to the RADIUS server along with your username, check the **Include Windows Logon Domain with User Name** check box. The default setting is checked.

Note If you chose to use a saved username and password but do not check the Include Windows Logon Domain with User Name check box, the saved domain name is not passed to the RADIUS server.

Step 6 If the Use Windows User Name and Password check box is unchecked and you want to implement added security, follow these steps:

a. Click **Advanced**. The Configure Advanced Settings window appears (see Figure 5-19).

Figure 5-12 Configure Advanced Settings Window



b. Leave the Specific Server or Domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the selected certificate authority or enter the domain name of the server from which the client will accept a certificate.

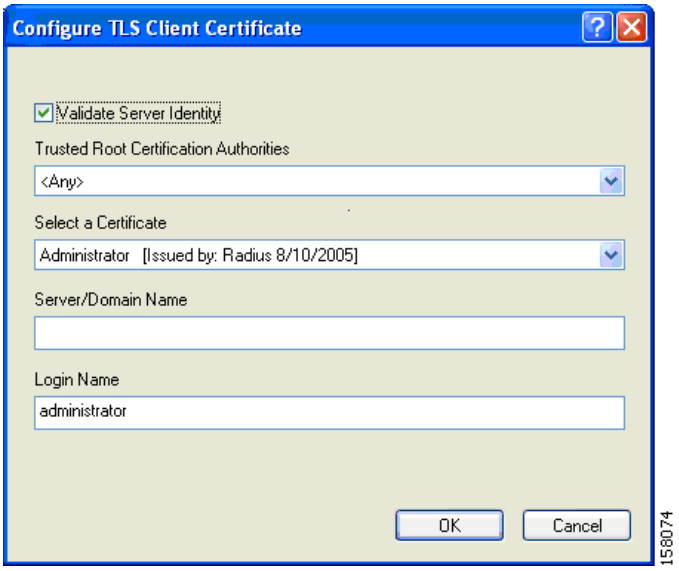
c. If the Login Name field is not filled in automatically, enter the username with nothing after it (for example, jsmith).

d. Click **OK** to save your settings.

Step 7 Click **OK** to save your settings and return to the Configure EAP-FAST window.

Step 8 If you chose **TLS Client Certificate** in Step 3, refer to "Enabling EAP-TLS" section on page 5-48 (Step 5 to Step 10) to configure the options in the Configure TLS Client Certificate window (Figure 5-13).

Figure 5-13 Configure TLS Client Certificate Window



Step 9 In the Select One or More PAC Authorities list, select the PAC authorities and PAC authority groups that are associated with the network defined by the profile's SSID. The list contains the names of all the authentication servers from which you have previously provisioned a PAC.

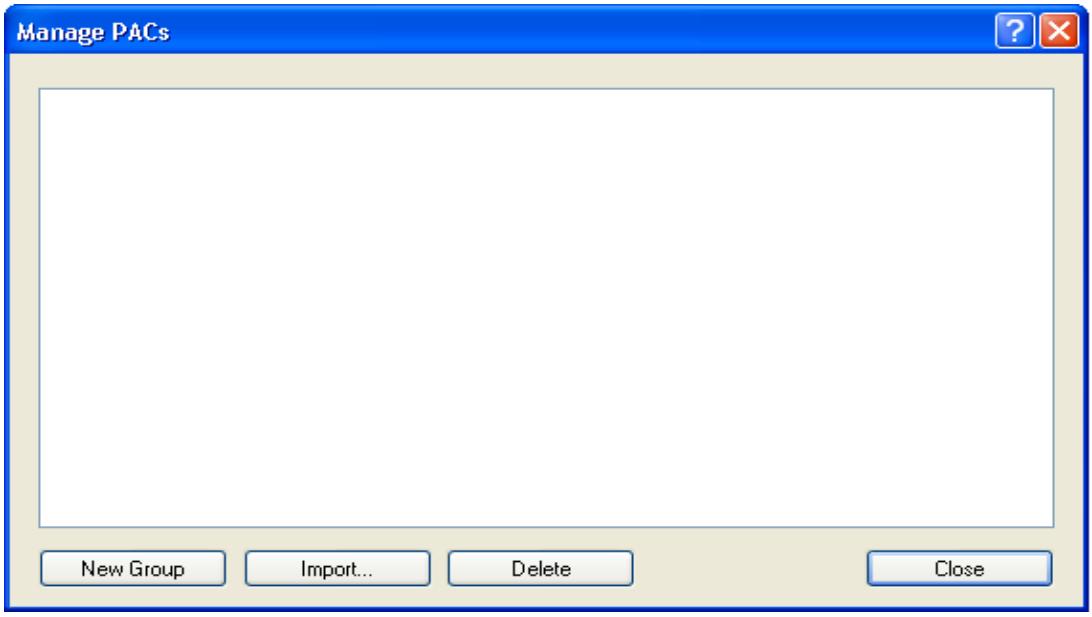
If the Select One or More PAC Authorities list is empty or does not contain the name of a desired PAC authority, go to Step 10 to import a PAC file.

Note This step is required for manual PAC provisioning but optional for automatic PAC provisioning. If automatic provisioning is enabled, automatic provisioning will be initiated during the authentication process of the EAP-FAST profile if no PAC authority was selected, the PAC could not be found, or the specified PAC does not match the server ID.

Step 10 If necessary, follow these steps to import or modify the grouping of PAC files:

a. Click **Manage**. The Manage PACs window appears (see Figure 5-14).

Figure 5-14 Manage PACs Window

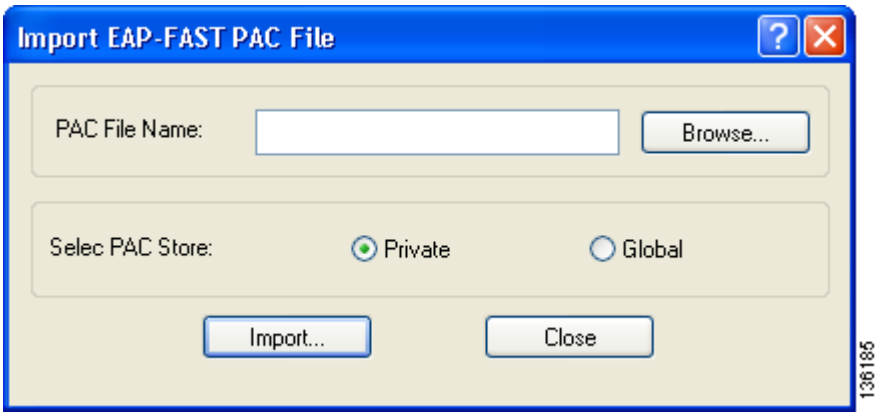


b. To create a new group, click **New Group**.

c. To move a PAC from one group to another, just drag it to the destination group.

d. Click **Import**. The Import EAP-FAST PAC File window appears (see Figure 5-15).

Figure 5-15 Import EAP-FAST PAC File Window



e. Find the location of the PAC file (*.pac) in the Look in box. The default location is C:\Program Files\Cisco Aironet.

Note The filename and extension of a PAC file is determined by the PAC authority that issues it, but the standard file extension is *pac*.

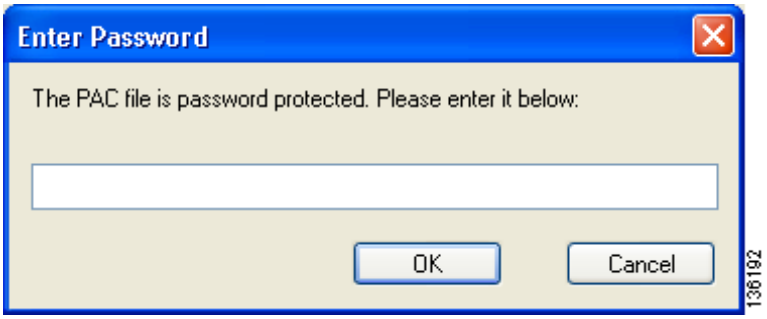
f. Choose one of these PAC store options to determine where the imported PAC file will be stored and to whom it will be accessible:

- **Global**—PACs that are stored in the global PAC store can be accessed and used by any user at any logon stage. Global PACs are available before or during logon or after the user is logged off if the profile is not configured with the No Network Connection Unless User Is Logged In option.
- **Private**—PACs that are stored in the private store can be accessed and used only by the user who provisioned them or the system administrator. They are not accessible until the user is logged onto the local system. This is the default option.

g. Click **Import**.

h. If the Enter Password window appears (see Figure 5-16), enter the PAC file password, which can be obtained from your system administrator, and click **OK**.

Figure 5-16 Enter Password Window



Note PAC file passwords are optional. The PAC authority determines whether to issue PAC files that require user-supplied passwords. Nevertheless, all PAC files (even those without passwords) are encrypted and protected. PAC file passwords are different from EAP-FAST passwords and need to be entered only once, at the time a PAC is imported.

i. If you try to import a PAC file with the same PAC ID as a previously imported PAC file, you are asked if you want to update the existing PAC. If you click **Yes**, the existing PAC is replaced by the new one from the imported file.

j. If the PAC file was imported successfully, the following message appears: "The EAP-FAST PAC file was imported and is ready for use." Click **OK** to return to the Manage PACs window.

k. The imported PAC now appears in the PAC tree on the Manage PACs window.

l. To delete a group or manually provisioned PAC file from storage, select the item and click **Delete**. When a message appears asking you to confirm your decision, click **Yes**. The PAC file is removed from the tree.

m. Click **Close** to return to the Configure EAP-FAST window.

n. The name of the PAC authority that issued the PAC now appears in the PAC authority list on the Configure EAP-FAST window. Select the desired PAC authorities or groups from the list.

Step 11 Check the **Use Any PAC Belonging to the Same Group** check box to use any PAC authority in the selected groups for PAC provisioning.

Step 12 Perform one of the following to configure PAC provisioning:

- If you want to enable automatic PAC provisioning, make sure the **Allow Automatic PAC Provisioning** check box is checked. A protected access credentials (PAC) is automatically obtained as needed (for example, when a PAC expires, when the client adapter accesses a different server or when the EAP-FAST username cannot be matched to a previously provisioned PAC).
- If you want to enable manual PAC provisioning, uncheck the **Allow Automatic PAC Provisioning** check box. This option requires you to choose a PAC authority or manually import a PAC file.

Note LDAP user databases support only manual PAC provisioning while Cisco Secure ACS internal, Cisco Secure ODBC, and Windows NT/2000/2003 domain user databases support both automatic and manual PAC provisioning.

Note Provisioning occurs only upon initial negotiation of the PAC or upon PAC expiration. After the PAC is provisioned, it serves as the per-user key by which authentication transactions are secured.

Step 13 Check the **Use Machine Information for Domain Logon** check box if you want the client to attempt to log into a domain using machine authentication with a machine certificate and machine credentials rather than user authentication. Doing so enables your computer to connect to the network prior to user logon. The default setting is unchecked.

Note If you do not check the Use Machine Information for Domain Logon check box, machine authentication is not performed. Authentication does not occur until you log on.

Step 14 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 Unless User Is Logged In** check box. The default setting is checked.

Step 15 Click **OK** to save your settings and return to the Profile Management (Security) window.

Note If you selected a private PAC and the No Network Connection Unless User Is Logged In check box is unchecked, a message appears indicating that the PAC may not be accessible during the domain logon process or when you are logged off. If you want a copy of the PAC to be added to the global store so that it will be available when you are not logged on, click **Yes**. If you do not want a copy of the PAC to be added to the global store, click **No**; then click **OK** when a message appears indicating that you may need to later reconfigure your profile to use a global PAC if you experience wireless connection problems during domain logon or when you are not logged on.

Step 16 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. 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 to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x security option is selected.

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. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 17 If you want to limit the amount of time that is spent searching for a domain controller during the authentication process, check the **Limit Time for Finding Domain Controller To** check box. Then in the edit box, enter the amount of time (in seconds) to which you want to limit the search for the domain controller. A timeout value of 0 causes the authentication process to bypass the "Finding Domain Controller" step altogether.

Range of timeout value: 0 to 300 seconds

Default: Unchecked; 0 seconds

Note When the "Finding Domain Controller" step is reached during the authentication process, a timer starts based on the number of seconds you specified for finding the domain controller. If either this value or the EAP-FAST authentication timeout value expires before the domain controller is found, the authentication process times out. 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. However, if authentication happens quickly, the software might reach the "Finding Domain Controller" step in 5 seconds. If the domain controller could not be found within 10 seconds, the authentication process would timeout in just 15 seconds.

Note The finding domain controller timeout value can never extend the authentication process beyond the EAP-FAST authentication timeout value, even if the finding domain controller timeout value is greater than the EAP-FAST authentication timeout value.

Note If you require domain services such as login scripts and roaming desktops, Cisco recommends that you uncheck the **Limit Time for Finding Domain Controller To** 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 18 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 19 Click **OK** to save your settings and return to the Profile Management window.

Enabling EAP-TLS or PEAP

In order to use EAP-TLS or PEAP authentication, the devices on the user's network must meet the following requirements:

- The user must have a valid Windows username and password, and the password cannot be blank.
- The appropriate certificates must be installed on the user's computer. EAP-TLS requires both a Certificate Authority (CA) certificate and a user certificate while PEAP requires only a CA certificate.
- To support EAP-TLS machine authentication with machine credentials:
  - A machine certificate must be obtained from the server, and client machine access must be enabled on the server.
  - Permissions for the MachineKeys folder, which stores the certificate pair keys for both the computer and users, must be set correctly. Refer to Microsoft knowledgebase article Q278381 for information on correctly setting up folder permissions:

    http://support.microsoft.com/default.aspx?scid=kb;en-us;Q278381

    Note If you ever change permissions on higher-level directories and those settings are applied to all subdirectories, you may need to reset the permissions for the MachineKeys folder.

- Access points to which the client adapter may attempt to authenticate must use the following firmware versions or later: 12.00T (access points running VxWorks), Cisco IOS Release 12.2(4)JA (1100 series access points), Cisco IOS Release 12.2(8)JA (1200 series access points), or Cisco IOS Release 12.2(13)JA (350 series access points).

  Note To use WPA or CCKM, access points must use Cisco IOS Release 12.2(11)JA or later. To use WPA2, access points must use Cisco IOS Release 12.3(2)JA or later.

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

Follow the instructions in one of the sections below to enable EAP-TLS or PEAP authentication for this profile:

- Enabling EAP-TLS, page 5-48
- Enabling PEAP (EAP-GTC), page 5-51
- Enabling PEAP (EAP-MSCHAP V2), page 5-55
- Enabling PEAP (EAP-MSCHAP V2) machine authentication with machine certificates, page 5-59

Enabling EAP-TLS

Follow the steps below to enable EAP-TLS authentication for this profile.

Step 1 Perform one of the following on the Profile Editor (Security) window:

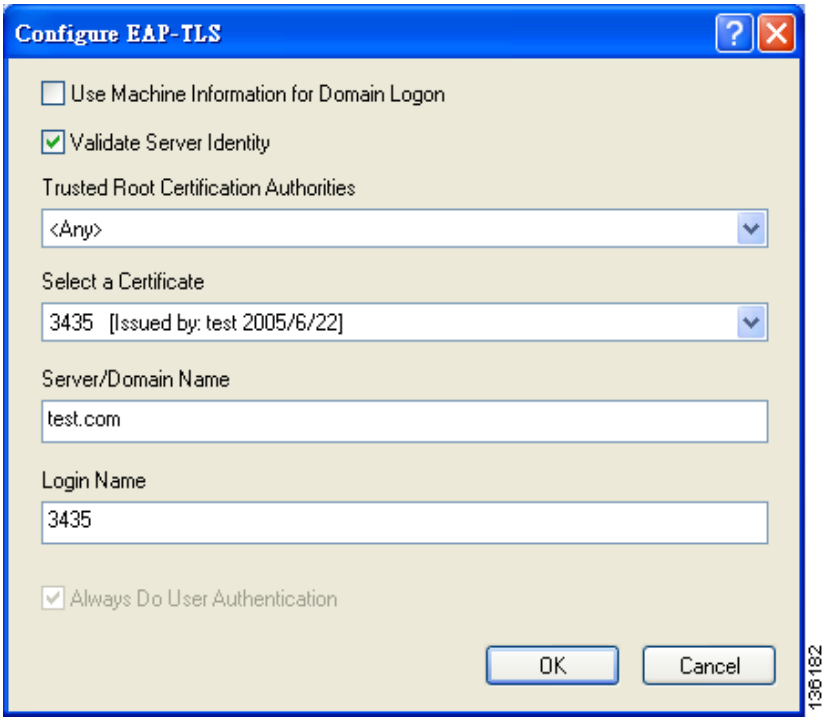
- If you want to enable EAP-TLS without WPA or WPA2, choose **802.1x** under Set Security Options and **EAP-TLS** in the 802.1x EAP Type drop-down box.
- If you want to enable EAP-TLS with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **EAP-TLS** in the WPA/WPA2/CCKM EAP Type drop-down box.

Note If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which the client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" section on page 5-22 for additional information.

Step 2 Click **Configure**. The Configure EAP-TLS window appears (see Figure 5-17).

Figure 5-17 Configure EAP-TLS Window



Step 3 Check the **Use Machine Information For Domain Logon** check box if you want the client to attempt to log into a domain using machine authentication with a machine certificate and machine credentials rather than user authentication. Doing so enables your computer to connect to the network prior to user logon. The default setting is unchecked.

Note If you do not check the Use Machine Information For Domain Logon check box, machine authentication is not performed. Authentication does not occur until you log on.

Step 4 If you checked the Use Machine Information For Domain Logon check box in the previous step, the Always Do User Authentication check box at the bottom of the window becomes active. Perform one of the following:

- Check the **Always Do User Authentication** check box if you want the client to switch from using machine authentication to using user authentication after you log on using your username and password. This is the default setting.
- Uncheck the **Always Do User Authentication** check box if you want the client to continue to use machine authentication after your computer logs into the domain.

Step 5 Check the **Validate Server Identity** check box to force the system to validate the identity of the server as an added level of security. If you uncheck this box, only user credentials will be validated.

Step 6 Choose the certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box.

Step 7 Choose your server certificate in the Select a Certificate drop-down box.

Step 8 Perform one of the following:

- Leave the Server/Domain Name field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the certificate authority listed in the Trusted Root Certification Authorities drop-down box. This is the recommended option.
- In the Server/Domain Name field, enter the domain name of the server from which the client will accept a certificate.

Step 9 If the Login Name field is not filled in automatically, enter your username in this format: *username@domain* (for example, jsmith@acs-test.cisco.com).

Step 10 Click **OK** to save your settings and return to the Profile Management (Security) window.

Step 11 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. 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 to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x security option is selected.

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. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 12 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the user's computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 13 Click **OK** to save your settings and return to the Profile Management window.

Enabling PEAP (EAP-GTC)

Follow these steps to enable PEAP (EAP-GTC) authentication for this profile.

Step 1 Perform one of the following:

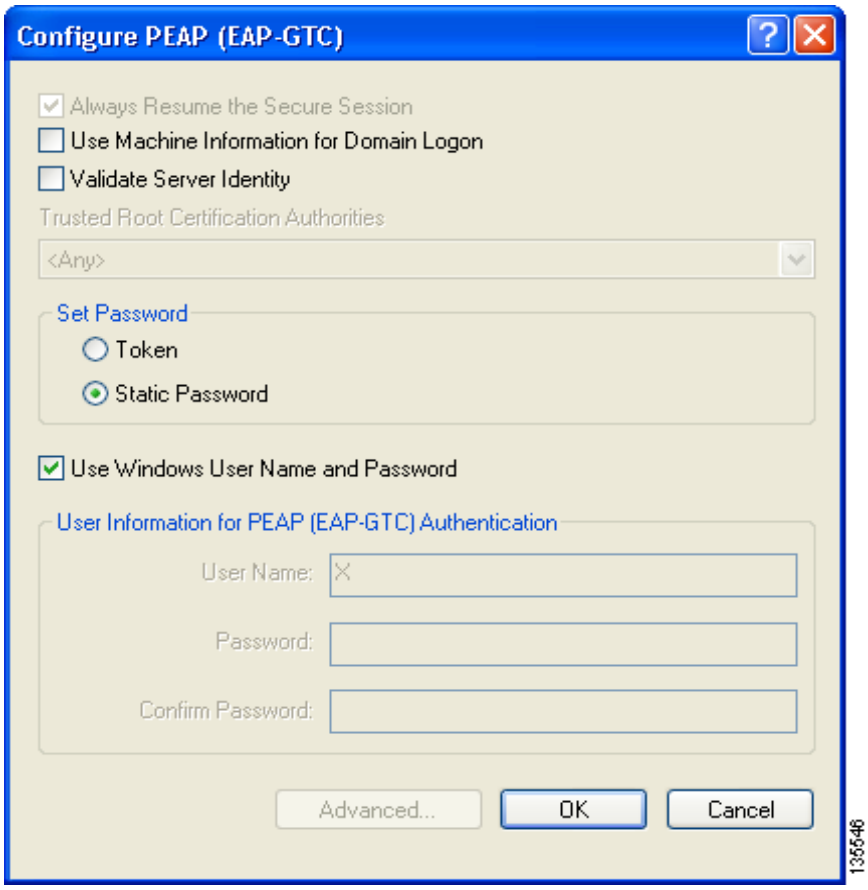
- If you want to enable PEAP (EAP-GTC) without WPA or WPA2, choose **802.1x** under Set Security Options and **PEAP (EAP-GTC)** in the 802.1x EAP Type drop-down box.
- If you want to enable PEAP (EAP-GTC) with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **PEAP (EAP-GTC)** in the WPA/WPA2/CCKM EAP Type drop-down box.

Note If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which the client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" section on page 5-22 for additional information.

Step 2 Click **Configure**. The Configure PEAP (EAP-GTC) window appears (see Figure 5-18).

Figure 5-18 Configure PEAP (EAP-GTC) Window



Step 3 Check the **Use Machine Information For Domain Logon** check box if you want the client to attempt to log into a domain using machine authentication with user credentials rather than user authentication. Doing so enables the computer to connect to the network prior to user logon. The default setting is checked.

Note If you do not check the Use Machine Information For Domain Logon check box, machine authentication is not performed. Authentication does not occur until the user logs on.

Step 4 Check the **Validate Server Identity** check box to force the system to validate the identity of the server as an added level of security. If you uncheck this box, only user credentials will be validated.

Step 5 Choose the certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box, or, if applicable, choose **<Any>**.

Step 6 Select either **Token** or **Static Password**, depending on the user's database.

Note If you choose Token, the user must use a hardware token device or the Secure Computing SofToken program (version 2.1 or later) to obtain the one-time password and enter the password when prompted during the authentication process. Secure Computing PremierAccess version 3.1.1 or later is the only supported token server.

Step 7 If you chose Token in Step 6, perform one of the following:

- Check the **Always Resume the Secure Session** check box at the top of the window if you want the PEAP (EAP-GTC) supplicant to always attempt to resume the previous session without prompting the user to re-enter his or her credentials whenever the client adapter becomes disassociated. The session resumes after the client temporarily loses connection to the access point (such as by roaming in and out of coverage) or wakes up from suspend or hibernate mode. This is the default setting.
- Uncheck the **Always Resume the Secure Session** check box if you want the user to be prompted to re-enter his or her PEAP (EAP-GTC) username and password whenever the client adapter temporarily loses association by roaming out of coverage or wakes up from suspend or hibernate mode.

Note Checking this check box gives the user the convenience of not having to re-enter his or her username and password when the client adapter experiences momentary losses of association. However, if the user leaves the device unattended during the period of time when the PEAP (EAP-GTC) session can be resumed without re-entering user credentials, be aware that someone can resume the user's PEAP (EAP-GTC) session and access the network.

Note The Always Resume the Secure Session check box is disabled if you chose Static Password in Step 6.

Step 8 Perform one of the following to specify the username that will be used for inner PEAP tunnel authentication:

- If you want the user's Windows username to also serve as the PEAP username, check the **Use Windows User Name** check box. This option gives the user only one username to remember.

  Note If you chose the Static Password option in Step 6, the check box reads *Use Windows User Name and Password*.

- If you want the user to enter a separate PEAP username (which is registered with the RADIUS server) in addition to his or her regular Windows username in order to start the PEAP authentication process, enter the PEAP username in the User Name field.

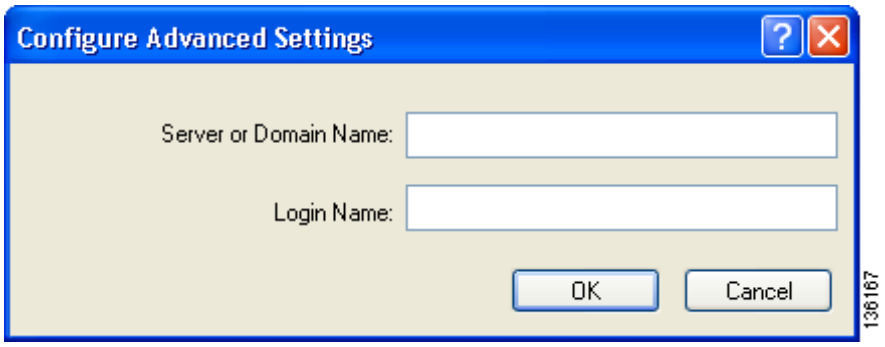
  Note Your Windows username is filled in automatically. Simply delete your Windows username and enter a separate PEAP username.

Step 9 If you entered a PEAP username in the previous step and chose the Static Password option in Step 6, enter your PEAP authentication password (which is registered with the RADIUS server) in both the Password and Confirm Password fields.

Step 10 If the Use Windows User Name and Password check box is unchecked and you want to implement added security by further refining the network certificate that will be accepted and controlling the string used to set up the outer PEAP tunnel, follow these steps:

a. Click **Advanced**. The Configure Advanced Settings window appears (see Figure 5-19).

Figure 5-19 Configure Advanced Settings Window



b. Leave the Specific Server or Domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the selected certificate authority or enter the domain name of the server from which the client will accept a certificate.

c. If the Login Name field is not filled in automatically, enter the username with nothing after it (for example, jsmith).

d. Click **OK** to save your settings.

Step 11 Click **OK** to save your settings and return to the Profile Editor (Security) window.

Step 12 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. 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 to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x security option is selected.

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. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 13 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the user's computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 14 Click **OK** to save your settings and return to the Profile Management window.

Enabling PEAP (EAP-MSCHAP V2)

Follow the steps below to enable PEAP (EAP-MSCHAP V2) for this profile.

Step 1 Perform one of the following:

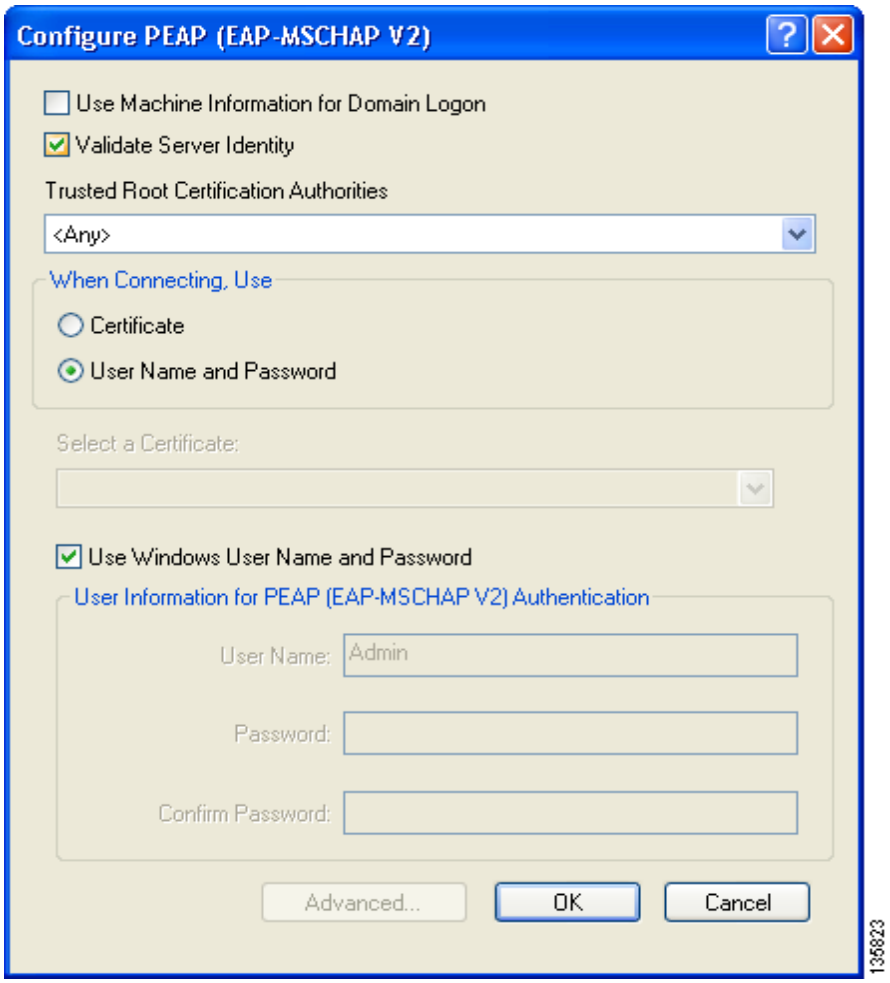
- If you want to enable PEAP (EAP-MSCHAP V2) without WPA or WPA2, choose **802.1x** under Set Security Options and **PEAP (EAP-MSCHAP V2)** in the 802.1x EAP Type drop-down box.
- If you want to enable PEAP (EAP-MSCHAP V2) with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **PEAP (EAP-MSCHAP V2)** in the WPA/WPA2/CCKM EAP Type drop-down box.

Note If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which the client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" section on page 5-22 for additional information.

Step 2 Click **Configure**. The Configure PEAP (EAP-MSCHAP V2) window appears (see Figure 5-20).

Figure 5-20 Configure PEAP (EAP-MSCHAP V2) Window



Step 3 Check the **Use Machine Information For Domain Logon** check box if you want the client to attempt to log into a domain using machine authentication with user credentials rather than user authentication. Doing so enables the computer to connect to the network prior to user logon. The default setting is checked.

Note If you do not check the Use Machine Information For Domain Logon check box, machine authentication is not performed. Authentication does not occur until the user logs on.

Step 4 Check the **Validate Server Identity** check box to force the system to validate the identity of the server as an added level of security. If you uncheck this box, only user credentials will be validated.

Step 5 Choose the certificate authority from which the server certificate was downloaded in the Trusted Root Certification Authorities drop-down box, or, if applicable, choose **<Any>**.

Step 6 Perform one of the following to specify how you want the user to establish a network connection:

- If you want the user to connect using a username and password, choose **User Name and Password** and go to Step 7.
- If you want the user to connect using a user certificate installed on the user's computer, choose **Certificate**, select a certificate from the drop-down box, and go to Step 8.

Step 7 Perform one of the following to specify the username and password that will be used for inner PEAP tunnel authentication:

- If you want the user's Windows username and password to also serve as the PEAP username and password, check the **Use Windows User Name and Password** check box.
- If you want to use a distinct username and password (which are registered with the RADIUS server) to start the PEAP authentication process, follow these steps:

  a. Enter the PEAP username and password in the corresponding fields.

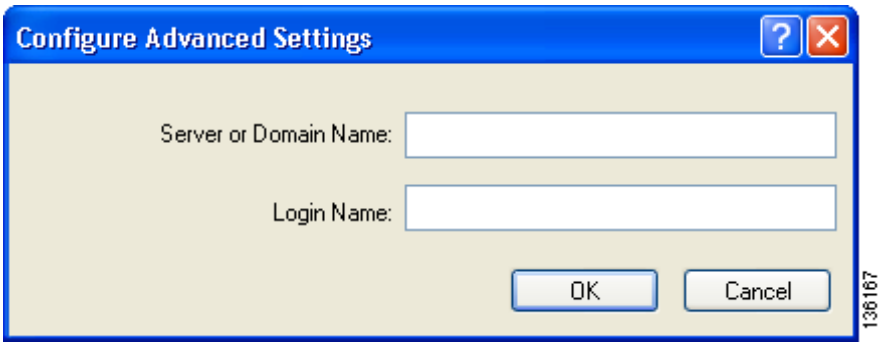
  Note Your Windows username is filled in automatically. Simply delete your Windows username and enter the separate PEAP username.

  b. Re-enter the password in the Confirm Password field.

Step 8 If you selected a certificate or entered a distinct username and password and you want to implement added security by further refining the network certificate that will be accepted and controlling the string used to set up the outer PEAP tunnel, follow these steps:

a. Click **Advanced**. The Configure Advanced Settings window appears (see Figure 5-19).

Figure 5-21 Configure Advanced Settings Window



b. Leave the Specific Server or Domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the selected certificate authority or enter the domain name of the server from which the client will accept a certificate.

c. If the Login Name field is not filled in automatically, enter the username with nothing after it (for example, jsmith).

Note Some RADIUS servers require that the same name be entered for both the inner and outer PEAP tunnels. That is, the same name may need to be entered in both the Login Name field and the User Name field on the Configure PEAP (EAP-MSCHAP V2) window.

d. Click **OK** to save your settings.

Step 9 Click **OK** to save your settings and return to the Profile Editor (Security) window.

Step 10 Perform one of the following to set the Allow Association to Mixed Cells parameter, which indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations:

- Check the **Allow Association to Mixed Cells** check box if the access point to which the client adapter is to associate (or the VLAN to which the client will be assigned) has WEP set to Optional. 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 to which the client adapter is to associate (or the VLAN to which the client will be assigned) does not have WEP set to Optional. This is the default setting.

Note This parameter is available only if the 802.1x security option is selected.

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. However, you can enable VLANs on the access point to separate WEP-enabled and WEP-disabled clients.

Step 11 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the user's computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 12 Click **OK** to save your settings and return to the Profile Management window.

Enabling PEAP (EAP-MSCHAP V2) Machine Authentication with Machine Credentials

The Host Based EAP option in the 802.1x EAP Type drop-down box on the Profile Editor (Security) window enables client adapters that are configured through ADU to attempt to log into a domain using PEAP (EAP-MSCHAP V2) machine authentication with machine credentials. Doing so enables the user's computer to connect to the network prior to user logon. Follow these steps to enable this authentication type.

Note This procedure enables the client adapter to use PEAP (EAP-MSCHAP V2) machine authentication with *machine* credentials. If you want to enable PEAP (EAP-MSCHAP V2) machine authentication with *user* credentials, follow the instructions in the "Enabling PEAP (EAP-MSCHAP V2)" section on page 5-55.

Note Because this feature requires the Microsoft Wireless Configuration Manager to start and stop as the user switches between host-based EAP and non-host-based EAP profiles, it works only for users with administrator or power-user privileges. An error message appears if you attempt to switch to or from a host-based EAP profile and you do not have the proper permissions.

Note To use this feature on a computer running Windows 2000, the computer must have the Microsoft 802.1X supplicant installed.

Note Host Based EAP is not included in the list of WPA/WPA2/CCKM EAP Type options on the Profile Editor (Security) window because this feature is not supported for use with WPA or WPA2.

Step 1 Choose **802.1x** under Set Security Options and **Host Based EAP** in the 802.1x EAP Type drop-down box.

Step 2 If you want to change the value of the Group Policy Delay parameter, enter a new value or use the up and down arrows to select a value between 0 and 65535 seconds. (Microsoft supports only values between 30 and 600 seconds. The default value is 60 seconds.)

The Group Policy Delay parameter specifies how much time elapses before the Windows logon process starts Group Policy, a Windows feature used by administrators to specify configuration options for groups of users. The objective is to delay the start of Group Policy until wireless network authentication occurs. The value that you set for this parameter goes into effect after the user's computer reboots with this profile set as the active profile.

Note A Microsoft hot fix is required in order to use this parameter on computers running Windows 2000 or computers running Windows XP without Service Pack 2 or later. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" section in Chapter 3 of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* for information on obtaining and installing the hot fix.

Step 3 Click **OK** to save your settings. The remaining steps must be completed on the user's computer after the Install Wizard has been used to install the client adapter software and this profile from the ACAU configuration file.

Step 4 Activate this profile on the Profile Management window. The Microsoft Wireless Configuration Manager starts.

Step 5 Click **Start > Settings > Control Panel > Network and Dial-up Connections** or **Network Connections**.

Step 6 Right-click the wireless connection.

Step 7 Click **Properties**. The Connection Properties window appears.

Step 8 Perform one of the following:

- On Windows 2000, click the **Authentication** tab.
- On Windows XP, choose the **Wireless Networks** tab, make sure that the **Use Windows to configure my wireless network settings** check box is checked, click the SSID of the access point to which the client adapter is to associate from the list of available networks, click **Configure**, and choose the **Authentication** tab.

Step 9 For EAP type, choose **Protected EAP (PEAP)**.

Step 10 Configure any applicable settings on the Protected EAP Properties window and subwindows.

Step 11 After the configuration is finished, PEAP authentication should begin. Depending on the configuration settings selected, the user may be prompted for a PEAP username, password, and domain name. ADU may need to be minimized to access the pop-up window that prompts for user credentials.

Note Multiple host-based EAP profiles can exist in ADU, but the Microsoft Wireless Configuration Manager maintains only one configuration. To use different PEAP property settings for different host-based EAP profiles, the user must repeat the previous steps beginning with Step 4 every time he or she switches to a different host-based EAP profile.

Note When a host-based EAP profile is activated, the Microsoft Wireless Configuration Manager takes control of the client adapter's authentication attempt. However, when a non-host-based EAP profile is activated, ADU assumes this control.

Note If problems occur while using a host-based EAP profile, make sure that 802.1X authentication is disabled for any other network connection.

APPENDIX A

Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters.

The following topics are covered in this appendix:

Manufacturer's Federal Communication Commission Declaration of Conformity Statement

Models: AIR-CB21AG-A-K9, AIR-PI21AG-A-K9

FCC Certification Number: LDK102050 (CB21AG)
LDK102051 (PI21AG)

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

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

The CB21AG client adapter has been tested and complies with FCC RF Exposure (SAR) limits in typical laptop computer configurations, and this device can be used in laptop computers with side-mounted PCMCIA slots which can provide 0.394 in (1 cm) separation distance from the antenna to the body of the user or a nearby person. Thin laptop computers may need special attention to maintain antenna spacing while operating.

The PI21AG client adapter has been tested and complies with FCC RF Exposure (SAR) limits in typical desktop computer configurations. A separation distance of 7.9 in (20 cm) must be maintained between this device's antenna and the body of the user or a nearby person.

These devices cannot be used with handheld personal digital assistants (PDAs). Use in other configurations may not ensure compliance with FCC RF exposure guidelines. These devices and their antennas must not be co-located or operated in conjunction with any other antenna or transmitter.

Caution The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using integrated antennas. Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

Caution Within the 5.15-to-5.25-GHz band, UNII devices are restricted to indoor operations to reduce any potential for harmful interference to co-channel Mobile Satellite Systems (MSS) operations.

Department of Communications – Canada

Canadian Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe B respecte les exigences du Reglement sur le material broilleur du Canada.

This device complies with Class B Limits of Industry Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters are certified to the requirements of RSS-210 for 2.4-GHz and 5-GHz devices. The use of these devices in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC

English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Deutsch:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprecheneden Vorgaben der Richtlinie 1999/5/EU.
Dansk:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Directiv 1999/5/EF.
Español:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directive 1999/5/EC.
Έλληνας:	Αυτός ο εξοπλισμός συμμορφώνεται με τις ουσιώδεις απαιτήσεις και τις λοιπές διατάξεις της Οδηγίας 1999/5/ΕΚ.
Français:	Cet appareil est conforme aux exigencies essentialles et aux autres dispositions pertinantes de la Directive 1999/5/EC.
Íslenska:	Þessi búnaður samrýmist lögboðnum kröfum og öðrum ákvæðum tilskipunar 1999/5/ESB.
Italiano:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/EC.

Nederlands:	Deze apparatuur voldoet aan de belangrijkste eisen en andere voorzieningen van richtlijn 1999/5/EC.
Norsk:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-directiv 1999/5/EC.
Português:	Este equipamento satisfaz os requisitos essenciais e outras provisões da Directiva 1999/5/EC.
Suomalainen:	Tämä laite täyttää direktiivin 1999/5/EY oleelliset vaatimukset ja on siinä asetettujen muidenkin ehtojen mukainen.
Svenska:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

The Declaration of Conformity related to this product can be found at the following URL:

http://www.ciscofax.com

The following standards were applied:

- Radio: EN 300.328-1, EN 300.328-2 (2.4-GHz operation);
  EN 301.893 (5-GHz operation)
- EMC: EN 301.489-1, EN 301.489-17
- Safety: EN 60950

The following CE mark is affixed to the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters:

CE !

Note This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact your customer service representative.

Declaration of Conformity Statement

Cisco Aironet CB21AG Wireless LAN Client Adapter

CISCO SYSTEMS

DECLARATION OF CONFORMITY
with regard to the R&TTE Directive 1999/5/EC
according to EN 45014

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134 - USA

Declare under our sole responsibility that the product,

AIR-CB21AG-E-K9 / Cisco Aironet 802.11a/b/g Wireless CardBus Adapter

Fulfils the essential requirements of the Directive 1999/5/EC.

The following standards were applied:

EMC	**EN 301.489-1** v1.4.1**: 2002-08; EN 301.489-17** v1.2.1**: 2002-04**
Health & Safety	**EN60950: 2000**
Radio	**EN 300 328** v1.4.1**: 2003-04** **EN 301.893** v1.2.3**: 2003-08**

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

The product carries the CE Mark: CE !

Date & Place of Issue: 1 January 2004, San Jose

Signature:

Tony Youssef
Director Corporate Compliance
125 West Tasman Drive
San Jose, CA 95134 - USA

DofC 340347

Cisco Aironet PI21AG Wireless LAN Client Adapter

CISCO SYSTEMS

DECLARATION OF CONFORMITY

with regard to the R&TTE Directive 1999/5/EC

according to EN 45014

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134 - USA

Declare under our sole responsibility that the product,

AIR-PI21AG-E-K9 / Cisco Aironet 802.11a/b/g Wireless PCI Adapter

Fulfils the essential requirements of the Directive 1999/5/EC.

The following standards were applied:

EMC	**EN 301.489-1** v1.4.1**: 2002-08; EN 301.489-17** v1.2.1**: 2002-04**
Health & Safety	**EN60950: 2000**
Radio	**EN 300 328** v1.4.1**: 2003-04** **EN 301.893** v1.2.3**: 2003-08**

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

The product carries the CE Mark: CE !

Date & Place of Issue: 1 January 2004, San Jose

Signature:

Tony Youssef
Director Corporate Compliance
125 West Tasman Drive
San Jose, CA 95134 - USA

DofC 340350

Declaration of Conformity for RF Exposure

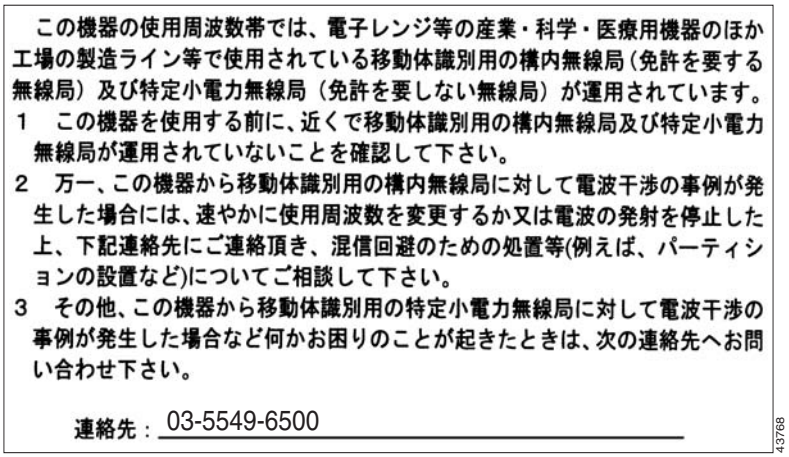
The radio module has been evaluated under FCC Bulletin OET 65C and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices.

Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet Wireless LAN Client Adapters in Japan. These guidelines are provided in both Japanese and English.

Note The use of 5-GHz devices is limited to indoor use in Japan.

Japanese Translation


この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。
1　この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
2　万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。
3　その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。
連絡先：03-5549-6500
43768

English Translation

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.
2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.
3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

Contact Number: 03-5549-6500

Administrative Rules for Cisco Aironet Wireless LAN Client Adapters in Taiwan

This section provides administrative rules for operating Cisco Aironet Wireless LAN Client Adapters in Taiwan. The rules are provided in both Chinese and English.

2.4- and 5-GHz Client Adapters

Chinese Translation

低功率電波輻射性電機管理辦法

第十四條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十七條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

95815

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 14

For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

Article 17

The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with COMMUNICATION ACT.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

5-GHz Client Adapters

Chinese Translation

English Translation

This equipment is limited to indoor use.

APPENDIX B

Channels, Power Levels, and Antenna Gains

This appendix lists the IEEE 802.11a, b, and g channels supported by the world's regulatory domains as well as the maximum power levels and antenna gains allowed per data rate.

The following topics are covered in this appendix:

Channels

IEEE 802.11a

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11a 20-MHz-wide channel are shown in Table B-1.

Table B-1 Channels for IEEE 802.11a

Channel Identifier	Frequency (in MHz)	Regulatory Domains				
		America (-A)	EMEA (-E)	Japan (-J)	Japan (-P)	Rest of World (-W)
34	5170	—	—	X	X	—
36	5180	X	X	—	X	X
38	5190	—	—	X	X	—
40	5200	X	X	—	X	X
42	5210	—	—	X	X	—
44	5220	X	X	—	X	X
46	5230	—	—	X	X	—
48	5240	X	X	—	X	X
52	5260	X	X	—	X	X
56	5280	X	X	—	X	X
60	5300	X	X	—	X	X
64	5320	X	X	—	X	X
100	5500	X	X	—	—	X
104	5520	X	X	—	—	X
108	5540	X	X	—	—	X
112	5560	X	X	—	—	X
116	5580	X	X	—	—	X
120	5600	X	X	—	—	X
124	5620	X	X	—	—	X
128	5640	X	X	—	—	X
132	5660	X	X	—	—	X
136	5680	X	X	—	—	X
140	5700	X	X	—	—	X
149	5745	X	—	—	—	X
153	5765	X	—	—	—	X
157	5785	X	—	—	—	X
161	5805	X	—	—	—	X

Note All channel sets are restricted to indoor usage except America (-A), which allows for indoor and outdoor use on channels 52 through 161 in the United States.

Note The Japan (-J) channels apply only to AIR-CB21AG-J-K9 and AIR-PI21AG-J-K9 client adapters, and the Japan (-P) channels apply only to AIR-CB21AG-P-K9 and AIR-PI21AG-P-K9 client adapters.

IEEE 802.11b/g

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11b/g 22-MHz-wide channel are shown in Table B-2.

Table B-2 Channels for IEEE 802.11b/g

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		America (-A)	EMEA (-E)	Japan (-J)	Rest of World (-W)
1	2412	X	X	X	X
2	2417	X	X	X	X
3	2422	X	X	X	X
4	2427	X	X	X	X
5	2432	X	X	X	X
6	2437	X	X	X	X
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	X	X
11	2462	X	X	X	X
12	2467	–	X	X	X
13	2472	–	X	X	X
14	2484	–	–	X	–

Note Mexico is included in the Rest of World regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of Mexico.

Note In Japan, channel 14 is not supported for 802.11g mode.

Maximum Power Levels and Antenna Gains

IEEE 802.11a

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table B-3 indicates the maximum EIRP allowed for each data rate in the IEEE 802.11a regulatory domains.

Table B-3 Maximum EIRP for IEEE 802.11a

	Maximum EIRP for PC-Cardbus Card with 0-dBi Antenna Gain and PCI Card with 1-dBi Antenna Gain	
Data Rate	**mW**	**dBm**
6 Mbps	40	16
9 Mbps	40	16
12 Mbps	40	16
18 Mbps	40	16
24 Mbps	40	16
36 Mbps	25.1	14
48 Mbps	20	13
54 Mbps	20	13

IEEE 802.11b

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table B-4 indicates the maximum EIRP allowed for each data rate in the IEEE 802.11b regulatory domains.

Table B-4 Maximum EIRP for IEEE 802.11b

	Maximum EIRP for PC-Cardbus Card with 0-dBi Antenna Gain and PCI Card with 1-dBi Antenna Gain	
Data Rate	**mW**	**dBm**
1 Mbps	100	20
2 Mbps	100	20
5.5 Mbps	100	20
11 Mbps	100	20

IEEE 802.11g

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. Table B-5 indicates the maximum EIRP allowed for each data rate in the IEEE 802.11g regulatory domains.

Table B-5 Maximum EIRP for IEEE 802.11g

	Maximum EIRP for PC-Cardbus Card with 0-dBi Antenna Gain and PCI Card with 1-dBi Antenna Gain	
Data Rate	**mW**	**dBm**
6 Mbps	50	17
9 Mbps	50	17
12 Mbps	50	17
18 Mbps	50	17
24 Mbps	50	17
36 Mbps	40	16
48 Mbps	31.6	15
54 Mbps	20	13

APPENDIX C

Error Messages

This appendix provides a list of error messages that may appear during the installation, configuration, and use of ACAU.

The following topic is covered in this appendix:

Error Messages

ACAU may display these error messages. The messages are listed in alphabetical order, and an explanation as well as a recommended user action are provided for each message.

Error Message `Are you sure you want to delete this PAC from your local system? If deleted, you may disrupt authentication with the EAP-FAST profiles that use this PAC.`

Explanation You are about to delete a PAC from either the Global or Private PAC store.

Recommended Action If you want to delete the PAC, click **Yes**. Otherwise, click **No**.

Error Message `At least one wireless checkbox must be selected.`

Explanation You did not choose a Wireless Mode on the Profile Editor (Advanced) window.

Recommended Action Choose at least one Wireless Mode option.

Error Message `CiscoAdminConfig.dat File not found. Please verify the correct file name was given.`

Explanation You tried to open the CiscoAdminConfig.dat file, but the file was not found.

Recommended Action Click **OK** and look in another directory for the CiscoAdminConfig.dat file.

Error Message `Error importing the EAP-FAST PAC file.`

Explanation An error occurred while a PAC file was being imported. The operation was not completed.

Recommended Action Try again to import the PAC file. If the same message appears, obtain a new PAC file and import it.

Error Message `Error: Unknown data file format.`

Explanation You attempted to open a file that ACAU cannot read.

Recommended Action Open only configuration files that have been created by ACAU.

Error Message `File Format Error`

Explanation You attempted to import a file in a format other than .prf.

Recommended Action Select the correct file to import.

Error Message `In order to select an Ad Hoc network, you must have a Network Name. Do you want to enter a Network Name?`

Explanation You chose Ad Hoc for Network Type on the Profile Editor (Advanced) window, but a network name was not entered on the Profile Editor (General) window.

Recommended Action If you want to specify an ad hoc network, click **Yes** and enter a network name in the SSID1 field on the Profile Editor (General) window. Otherwise, click **No**.

Error Message `No user certificates were found on your computer. Machine certificates will be used for Domain Logon if "Use Machine Information For Domain Logon" check box is checked.`

Explanation You chose the EAP-TLS option on the Profile Editor (Security) window, but no user certificates were found on your computer.

Recommended Action Perform one of the following:

- If you want the client to attempt to log into a domain using machine authentication with a machine certificate and machine credentials, check the **Use Machine Information For Domain Logon** check box when the Define Certificate window appears.
- If you want the client to authenticate using user credentials, install the appropriate user certificate on your computer.

Error Message `Please enter a Passphrase.`

Explanation You clicked **OK** on the Define WPA/WPA2 Pre-Shared Key window before entering a passphrase.

Recommended Action Enter a WPA/WPA2 passphrase on the Define WPA/WPA2 Pre-Shared Key window and then click **OK**.

Error Message `Please enter a profile name.`

Explanation While creating a new profile, you clicked **OK** or chose another Profile Editor tab before entering a profile name on the Profile Editor (General) window.

Recommended Action Enter a valid profile name.

Error Message `Please enter at least one Pre-Shared Key.`

Explanation You clicked **OK** on the Define Pre-Shared Keys window before entering a static WEP key.

Recommended Action Enter at least one static WEP key on the Define Pre-Shared Keys window.

Error Message `Please enter exactly 12 characters, or leave the entry field empty.`

Explanation You entered fewer than 12 characters in one of the fields on the Preferred Access Points window.

Recommended Action Enter a valid MAC address for the access point or leave the field blank.

Error Message `The configuration name you entered is already being used. Enter a unique name.`

Explanation While creating a new profile, you entered a profile name on the Profile Editor (General) window that already exists.

Recommended Action Enter a unique profile name.

Error Message `The entered password was incorrect. Please try again.`

Explanation You incorrectly entered the PAC file password.

Recommended Action Carefully re-enter the PAC file password.

Error Message `The imported PAC already exists on your local machine. Do you want to update it anyway?`

Explanation You tried to import a PAC file with the same PAC ID as a previously imported PAC file.

Recommended Action Click **Yes** to replace the existing PAC with the new one from the imported file or click **No** to cancel the operation.

Error Message `The Passphrase must be between 8 and 64 characters.`

Explanation The WPA/WPA2 passphrase that you entered on the Define WPA/WPA2 Pre-Shared Key window did not contain the correct number of characters.

Recommended Action Enter a WPA/WPA2 passphrase with 8 to 63 ASCII text characters or 64 hexadecimal characters.

Error Message `The password is empty. Please enter a password.`

Explanation You chose the Use Saved User Name and Password option on the LEAP or EAP-FAST Settings window but did not enter a password.

Recommended Action Enter the LEAP or EAP-FAST password in the Password field.

Error Message `The passwords you entered do not match. Please enter them again.`

Explanation The passwords that you entered in the Password and Confirm Password fields on the LEAP or EAP-FAST Settings window do not match.

Recommended Action Re-enter the LEAP or EAP-FAST password in both fields.

Error Message `The user name is empty. Please enter a user name.`

Explanation You chose the Use Saved User Name and Password option on the LEAP or EAP-FAST Settings window but did not enter a username.

Recommended Action Enter the LEAP or EAP-FAST username in the User Name field.

Error Message `WEP Key x must be y characters long. Please enter z more characters.`

Explanation The static WEP key that you entered on the Define Pre-Shared Keys window does not contain the correct number of characters.

Recommended Action Re-enter the static WEP key following the guidelines in the "Enabling Static WEP" section on page 5-28.

Error Message `'x' is not a hexadecimal character.`

Explanation The character you entered on the Define Pre-Shared Keys window is not a hexadecimal character.

Recommended Action Re-enter the static WEP key following the guidelines in the "Enabling Static WEP" section on page 5-28.

Error Message `You can have only one SSID in an Ad Hoc Network. The SSID selections on the General Page will be adjusted.`

Explanation You chose the Ad Hoc option on the Profile Editor (Advanced) window when multiple SSIDs were specified on the Profile Editor (General) window.

Recommended Action Click **OK**. Only SSID1 now appears on the Profile Editor (General) window. If you want to specify multiple SSIDs, choose **Infrastructure** for the Network Type parameter on the Profile Editor (Advanced) window.

Error Message `You can have only one SSID in a WPA Passphrase network. The other SSIDs on the General tab will be disabled. Do you want to continue?`

Explanation You chose the WPA/WPA2 Passphrase security option on the Profile Editor (Security) window when multiple SSIDs were specified on the Profile Editor (General) window.

Recommended Action Click **Yes** to disable SSID2 and SSID3 for this profile or click **No** to cancel the operation.

Error Message `You must configure the PEAP-GTC settings properly. User information, password, or machine information is incomplete.`

Explanation You improperly configured a PEAP (EAP-GTC) profile.

Recommended Action Modify the profile's configuration settings, making sure to enter all necessary information.

Error Message `You must define a certificate to use EAP-TLS. Click Configure to select a certificate.`

Explanation You chose the EAP-TLS option on the Profile Editor (Security) window and clicked **OK** without selecting a certificate.

Recommended Action Click **Configure** and select a certificate on the Define Certificate window.

Error Message `You must enter a valid login name to use EAP-TLS. Click Configure to enter a login name.`

Explanation You chose the EAP-TLS option on the Profile Editor (Security) window and clicked **OK** without entering an EAP-TLS login name.

Recommended Action Click **Configure** and enter the EAP-TLS login name on the Define Certificate window.

Error Message `You must select a PAC or enable Allow Automatic PAC Provisioning.`

Explanation While configuring a profile for EAP-FAST, you did not enable automatic PAC provisioning or select a PAC authority from the drop-down list on the EAP-FAST Settings window.

Recommended Action Choose a PAC authority from the drop-down list on the EAP-FAST Settings window. If the list is empty, import a PAC file.

Error Message `You must select a Passphrase to use WPA/WPA2.`

Explanation You chose the WPA/WPA2 Passphrase option on the Profile Editor (Security) window and clicked **OK** without entering a passphrase.

Recommended Action Enter a WPA/WPA2 passphrase on the Define WPA/WPA2 Pre-Shared Key window.

Error Message `You must set at least one Pre-Shared Key.`

Explanation You chose the Pre-Shared Key (Static WEP) option on the Profile Editor (Security) window and clicked **OK** without entering a static WEP key.

Recommended Action Enter a static WEP key on the Define Pre-Shared Keys window and then click **OK**.

Error Message `Your security setting is invalid for an Ad Hoc network. Security will be disabled. You can configure security to use Pre-shared keys later on the Security screen. Do you want to continue?`

Explanation Pre-Shared Key (Static WEP) is the only valid security option for an ad hoc network. You chose Ad Hoc for Network Type on the Profile Editor (Advanced) window when a security option other than static WEP was already selected.

Recommended Action If you want to configure this profile for use in an ad hoc network, click **Yes** to disable security. Otherwise, click **No**.

Error Message `You selected a private PAC for EAP-FAST authentication. It may not be accessible when the user is logged off or during the domain logon process. Confirm if you want to copy the selected PAC into the global PAC store.`

Explanation You selected a private PAC and the No Network Connection Unless User Is Logged In check box is unchecked. Therefore, the PAC may not be accessible during domain logon or when the user is logged off.

Recommended Action If you want a copy of the PAC to be added to the global store so that it will be available when the user is not logged on, click **Yes**. If you do not want a copy of the PAC to be added to the global store, click **No**.

APPENDIX D

Using the Profile Migration Tool

This appendix explains how to use the profile migration tool to migrate Cisco Aironet 350 series and CB20A wireless LAN client adapter profiles to profiles that can be used with Cisco Aironet CB21AG and PI21AG client adapters.

The following topics are covered in this appendix:

Overview of the Profile Migration Tool

The profile migration tool is designed to migrate Cisco Aironet 350 series and CB20A wireless LAN client adapter profiles to profiles that can be used with Cisco Aironet CB21AG and PI21AG client adapters. The tool is meant to migrate profiles with minimal modification, but its behavior can be altered by command line options. The legacy 350 and CB20A profiles are not deleted or modified in any way.

Cisco expects the profile migration tool to be executed once, most likely immediately after installing or updating the CB21AG/PI21AG client adapter software. Upon completion, the profile migration tool may be removed from the user's system.

Note Profile migration tool 1.0 can be used only with ACAU and Install Wizard 2.5. To find the current version number of the profile migration tool, find the PMT.exe file in the directory where ADU is installed, right-click the file, and click **Properties** and the **Version** tab.

Rules Governing Profile Migration

These rules govern the operation of the profile migration tool:

- Legacy profiles that are configured for host-based EAP are not migrated.
- Passwords that are stored in LEAP and EAP-FAST profiles may or may not be migrated, depending on the encryption method used for those passwords. Passwords that are not migrated must be re-entered after the migration.
- The PAC files for EAP-FAST profiles are not migrated. They must be reprovisioned after the migration.
- A profile's auto profile selection properties are migrated only if auto profile selection is enabled.
- Legacy profiles that were created using older versions of the Aironet Client Utility (ACU) may experience problems during migration. In such cases, the profile migration tool migrates the information that it can and ignores any additional information.
- If multiple instances of the same profile name exist, the names are mangled unless overridden by command line options. The default name-mangling scheme causes subsequent profiles with the same name to have an *_a* or *_b* appended to the end of the name, indicating whether the profile migrated from an 802.11a (CB20A) or 802.11b (350) radio. A third instance would have an *_aa* or *_bb* appended and so on (for example, *Office*, *Office_a*, *Office_aa*).

  Note If the original name is too long to be appended, it is shortened by truncating as necessary.

- CB21AG and PI21AG client adapters have a limit of 16 profiles, so the total number of profiles that can be migrated is 16 minus the number of existing CB21AG and PI21AG profiles. If the number of profiles to migrate is greater than the number of profiles that can be migrated, some legacy profiles are not migrated. In this case, the client adapter priority is as follows, unless overridden by command line options:

  1.350 PCMCIA

  2.350 PCI

  3.350 mini PCI

  4.CB20A

  For each client adapter, profiles are migrated in this order:

  1.Default profiles

  2.Auto-selectable profiles

  3.Any current profiles for inserted legacy client adapters that have not already been migrated

  4.Any remaining profiles

- Profile names that existed before the migration are preserved unless the **-replace** command is executed.

Installing the Profile Migration Tool

When the CB21AG/PI21AG client adapter software is installed, the Install Wizard also automatically installs the profile migration tool, unless the Don't Install option was chosen in ACAU. It is saved in the same directory as ADU.

Note If the Install Wizard is run without using an ACAU-generated configuration file, the profile migration tool is still installed automatically and saved in the same directory as ADU.

Note The name of the PMT installation log is migrate.log. It is saved at the root level of your hard drive (C:\).

Running the Profile Migration Tool

Follow these steps to run the profile migration tool to migrate 350 and CB20A profiles to CB21AG/PI21AG profiles.

Note The best time to run the profile migration tool is immediately after the Install Wizard has installed the client adapter software.

Note The following conditions must be true before the profile migration tool can be run successfully:
- Your computer must contain the 350 and CB20A profiles that you want to migrate.
- ADU must be installed on the same computer but must not be running during the profile migration.
- A CB21AG or PI21AG client adapter must be inserted in your computer.

Step 1 Perform one of the following:

- If you chose the Install & Run option for the ACAU Setup Settings - Profile Migration Tool parameter, the profile migration tool runs automatically after the Install Wizard installs the client adapter software. Go to Step 4.
- If ACAU was not used to generate a configuration file, you did not choose the ACAU Install & Run option, or you want to rerun the profile migration tool (provided that you previously used the **-AllowReRun** command line option), open the Windows Command Prompt from **Start > Programs > Accessories**.

Step 2 Use MS-DOS commands to access the directory where the profile migration tool (PMT.exe) is located on your computer.

Step 3 Type **PMT** and press **Enter**. The profile migration tool runs and displays the results.

Note See the "Command Line Options" section below if you want to alter the behavior of the profile migration tool before running it.

Step 4 Restart your computer.

Step 5 Open ADU. Your migrated 350 and CB20A profiles now appear as CB21AG/PI21AG profiles on the Profile Management window and are ready for use.

Step 6 Re-enter the WEP keys in ADU.

Step 7 If desired, you can view the log file generated by the profile migration tool. This file shows the profiles that were processed, their status, and the reason why any profiles were not migrated.

Note Unless you changed the default name and location of the log file using the **-logfile** command, you can find the log file at C:\migrate.log.

Step 8 If desired, you can remove the profile migration tool from your computer.

Command Line Options

Command line options can be used to alter the behavior of the profile migration tool. They can be entered in one of two ways:

- If you are entering the command line options on the ACAU Profile Migration Tool Parameters window, which appears when you choose Install & Run for the Setup Settings - Profile Migration Tool parameter and click the Command Line box, enter only the command (such as ***-command***).
- If you are entering the command line options from the Windows Command Prompt, type **PMT** and then the command (such as **PMT *-command***).

Note Leave a space between multiple commands (such as ***-command -command***).

These command line options are available:

- **-AllowReRun—**Enables the profile migration tool to be run multiple times. When you rerun the tool, it migrates all the existing profiles, even the ones that were already migrated. If you have modified any of the previously migrated profiles, the modifications are lost.

  Example: PMT -AllowReRun

  Note If you do not use this command, you can run the profile migration tool only once. If you attempt to run it again, a message appears indicating that the profiles have already been migrated and that the tool does not need to be run again.

- **-CardOrder <cardtype> <cardtype>...**—Specifies the order in which profiles are migrated when multiple client adapters are selected.

  Example: PMT -CardOrder -pci350 -pcmcia350

- **-CB20A**—Selects only CB20A profiles for migration. This command can be used alone or in conjunction with the **-CardOrder <cardtype> <cardtype>...** command to specify the order in which client adapter profiles are migrated.

  Examples: PMT -CB20A
  PMT -CardOrder -CB20A -pcmcia350

- **-ConfigFile <filename> <filename>...**—Enables you to run the profile migration tool using multiple command lines that are specified within one or more configuration files. You can create the configuration file(s) using a text editor such as Notepad. To do so, simply type the desired commands (such as **-miniPCI -replace**) in the text editor and save the file. (Do not include **PMT** when typing the commands in the text editor.) After you have created the configuration file(s), use the **-ConfigFile** command with the file(s) you created.

  Examples: PMT -ConfigFile filename1.txt
  PMT -ConfigFile filename1.txt filename2.txt

  Note If more than one file is specified, the profile migration tool performs all its functions for each file. It ignores all other command line options and executes only the options in the file(s) in order to prevent confusion regarding command priority.

- **-logfile <logfile name>**—Enables you to change the name and location of the log file, which identifies the migrated and unmigrated profiles after you run the profile migration tool. The default name is *migrate.log*, and its default location is the system drive root (for example, C:).

  Examples: PMT -logfile logfile.log
  PMT -logfile C:\Cisco Aironet\migrate.log

  Note If you specify a new location for the log file, that location must already exist. Otherwise, the file is saved to the system drive root (for example, C:).

  Note If the **-logfile** command is used without the **<logfile name>** parameter, a log file is not generated.

- **-miniPCI**—Selects only 350 mini PCI profiles for migration. This command can be used alone or in conjunction with the **-CardOrder <cardtype> <cardtype>...** command to specify the order in which client adapter profiles are migrated.

  Examples: PMT -miniPCI
  PMT -CardOrder -CB20A -miniPCI -pci350

- **-pci350**—Selects only 350 PCI profiles for migration. This command can be used alone or in conjunction with the **-CardOrder <cardtype> <cardtype>...** command to specify the order in which client adapter profiles are migrated.

  Examples: PMT -pci350
  PMT -CardOrder -miniPCI -pci350

- **-pcmcia350**—Selects only 350 PCMCIA profiles for migration. This command can be used alone or in conjunction with the **-CardOrder <cardtype> <cardtype>...** command to specify the order in which client adapter profiles are migrated.

  Examples: PMT -pcmcia350
  PMT -CardOrder -pcmcia350 -pci350

- **-replace**—Causes legacy profiles with the same name as existing CB21AG/PI21AG profiles to replace the existing profiles. This command is intended to minimize the number of similarly named profiles on your system.

  For example, if both a 350 PCI legacy profile and a CB21AG profile have the same name (such as *Office*), the legacy profile replaces the CB21AG profile, resulting in only one *Office* profile. If this command is not used, you have two profiles after migration: *Office* and *Office_b*.

  Example: PMT -replace

  Note If you have multiple legacy profiles with the same name (such as *Home*), only one *Home* profile is available after migration.

Uninstalling the Profile Migration Tool

The profile migration tool is uninstalled automatically when the client adapter software is uninstalled. If you want to uninstall only the profile migration tool, find the PMT.exe file in the directory where ADU is installed and delete it.

GLOSSARY

802.1X Also called *802.1X for 802.11*. 802.1X is the standard for wireless LAN security, as defined by the Institute of Electrical and Electronics Engineers (IEEE). 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 Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.

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 frequency band.

802.11a The IEEE standard that governs the deployment of 5-GHz OFDM systems. It specifies the implementation of the physical layer for wireless UNII bands (see UNII, UNII 1, and UNII 2) and provides four channels per 100 MHz of bandwidth.

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.

802.11g The IEEE standard that specifies carrier sense media access control and physical layer specifications for 54-Mbps 2.4-GHz wireless LANs.

802.11i The IEEE standard that defines security standards for wireless LANs. It specifies encryption, authentication, and key management strategies for wireless data and system security. It includes the TKIP and AES-CCMP data-confidentiality protocols.

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.

AES-CCMP Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES-CCMP is the encryption protocol in the 802.11i standard.

alphanumeric A set of characters that contains both letters and numbers.

antenna gain A measure of an antenna's ability to direct or focus radio energy over a region of space. High-gain antennas have a focused radiation pattern in a specific direction.

associated A station is configured properly to allow it to wirelessly communicate with an access point.

B

bandwidth Specifies the amount of the frequency spectrum that is usable for data transfer. It identifies the maximum data rate that a signal can attain on the medium without encountering significant power loss.

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 adapters 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 Binary phase shift keying. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 1 Mbps.

broadcast key rotation A security feature for use with dynamic WEP keys. If your client adapter uses LEAP, EAP-FAST, EAP-TLS, or PEAP authentication and you enable this feature, the access point changes the dynamic broadcast WEP key that it provides at the interval you select.

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.

CCKM Cisco Centralized Key Management. Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point.

cell The area of radio range or coverage in which wireless devices can communicate with an access point. 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.

CKIP Cisco Key Integrity Protocol. Cisco’s WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.

client adapter A radio device that uses the services of an access point to communicate wirelessly with other devices on a local area network.

client adapter software The client adapter driver and client utilities that are installed by the Install Wizard. The client utilities include the Aironet Desktop Utility (ADU), Aironet System Tray Utility (ASTU), site survey utility, and profile migration tool.

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.

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.

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.

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. EAP is the protocol for the optional IEEE 802.1X wireless LAN security feature. An access point that supports 802.1X and EAP acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.

EAP-FAST Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling. An 802.1X authentication type that is available for use with Windows 2000 and XP. With EAP-FAST, a username, password, and PAC are used by the client adapter to perform mutual authentication with the RADIUS server through an access point.

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 megabits per second (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.

fragmentation threshold The size at which packets are fragmented and transmitted a piece at a time instead of all at once. The setting must be within the range of 64 to 2312 bytes.

full duplex A means of communication whereby each node receives and transmits simultaneously (two-way). See also half duplex.

G

gateway A device that connects two otherwise incompatible networks together.

GHz Gigahertz. One billion cycles per second. A unit of measure for frequency.

H

half duplex A means of communication whereby each node receives and transmits in turn (one-way). See also full duplex.

hexadecimal A set of characters consisting of ten numbers and six letters (0-9, A-F, and a-f).

I

IEEE Institute of Electrical and Electronics 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.

infrastructure device A device (such as an access point, bridge, or base station) that connects client adapters to a wired LAN.

IP address The Internet Protocol 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.

L

LEAP LEAP, or *EAP-Cisco Wireless*, is an 802.1X authentication type. With LEAP, a username and password are used by the client adapter to perform mutual authentication with the RADIUS server through an access point.

M

MAC address The Media Access Control (MAC) address is a unique serial number assigned to a networking device by the manufacturer.

MIC Message integrity check. 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 client adapter's driver must support MIC functionality, and MIC must be enabled on the access point.

modulation Any of several techniques for combining user information with a transmitter's carrier signal.

multicast packets Packets transmitted to multiple stations.

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

O

OFDM Orthogonal frequency division multiplexing. A modulation technique used by IEEE 802.11a-compliant wireless LANs for transmission at 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

omni-directional Typically refers to a circular antenna radiation pattern.

P

PAC Protected access credentials. Credentials that are either automatically or manually provisioned and used to perform mutual authentication with the RADIUS server during EAP-FAST authentication. PACs are created by the Cisco Secure ACS server and are identified by an ID. A user obtains his or her own copy of the PAC from the server, and the ID links the PAC to the profile created in ADU. When manual PAC provisioning is enabled, the PAC file is manually copied from the server and imported onto the client device.

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

PC-Cardbus card A client adapter card radio module with a Cardbus interface that can be inserted into any device equipped with a 32-bit Cardbus slot.

PCI card A client adapter card radio module that can be inserted into any device equipped with an empty PCI expansion slot.

Q

QoS Quality of service. QoS on wireless LANs provides prioritization of traffic from the access point over the WLAN based on traffic classification. The benefits of QoS become more obvious as the load on the wireless LAN increases, keeping the latency, jitter, and loss for selected traffic types within an acceptable range.

QPSK Quadruple phase shift keying. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 2 Mbps.

R

radio channel The frequency at which a radio operates.

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 enables users to move through a facility while maintaining an unbroken connection to the LAN.

S

spread spectrum A radio transmission technology that spreads data 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. A unique identifier that 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

TKIP Temporal Key Integrity Protocol. Also referred to as *WEP key hashing*. A security feature that 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.

transmit power The power level of radio transmission.

U

unicast packet A single data message (packet) sent to a specific IP address.

UNII Unlicensed National Information Infrastructure. An FCC regulatory domain for 5-GHz wireless devices. UNII bands are 100 MHz wide and divided into four channels when using 802.11a OFDM modulation.

UNII 1 A UNII band dedicated to in-building wireless LAN applications. UNII 1 is located at 5.15 to 5.25 GHz and allows for a maximum transmit power of 40 mW (or 16 dBm) with an antenna up to 6 dBi. UNII 1 regulations require a nonremovable, integrated antenna.

UNII 2 A UNII band dedicated to in-building wireless LAN applications. UNII 2 is located at 5.25 to 5.35 GHz and allows for a maximum transmit power of 200 mW (or 23 dBm) with an antenna up to 6 dBi. UNII 2 regulations allow for an auxiliary, user-installable antenna.

UNII 3 A UNII band dedicated to wireless LAN applications. UNII 3 is located at 5.725 to 5.825 GHz and allows for a maximum transmit power of 1 Watt (or 30 dBm) with an antenna up to 6 dBi. UNII 3 regulations allow for an auxiliary, user-installable antenna.

V

VLAN A switched network that is logically segmented, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN regardless of their physical connections to the network or the fact that they might be intermingled with other teams. You use VLANs to reconfigure the network through software rather than physically unplugging and moving devices or wires.

A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment such as LAN switches that operate bridging protocols between them with a separate group for each VLAN.

W

WDS Wireless domain services (WDS). An access point providing WDS on your wireless LAN maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the WDS access point forwards the client's credentials to the new access point with the multicast key. Only two packets pass between the client and the new access point, greatly shortening the reassociation time.

WEP Wired equivalent privacy. An optional security mechanism defined within the 802.11 standard designed to protect your data as it is transmitted through your wireless network by encrypting it through the use of encryption keys.

workstation A computing device with an installed client adapter.

WPA Wi-Fi Protected Access. A standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification. WPA uses TKIP and MIC for data protection and 802.1X for authenticated key management.

WPA2 Wi-Fi Protected Access 2. The next generation of Wi-Fi security. It is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard. WPA2 uses AES-CCMP for data protection and 802.1X for authenticated key management.

INDEX

Numerics

A

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

W