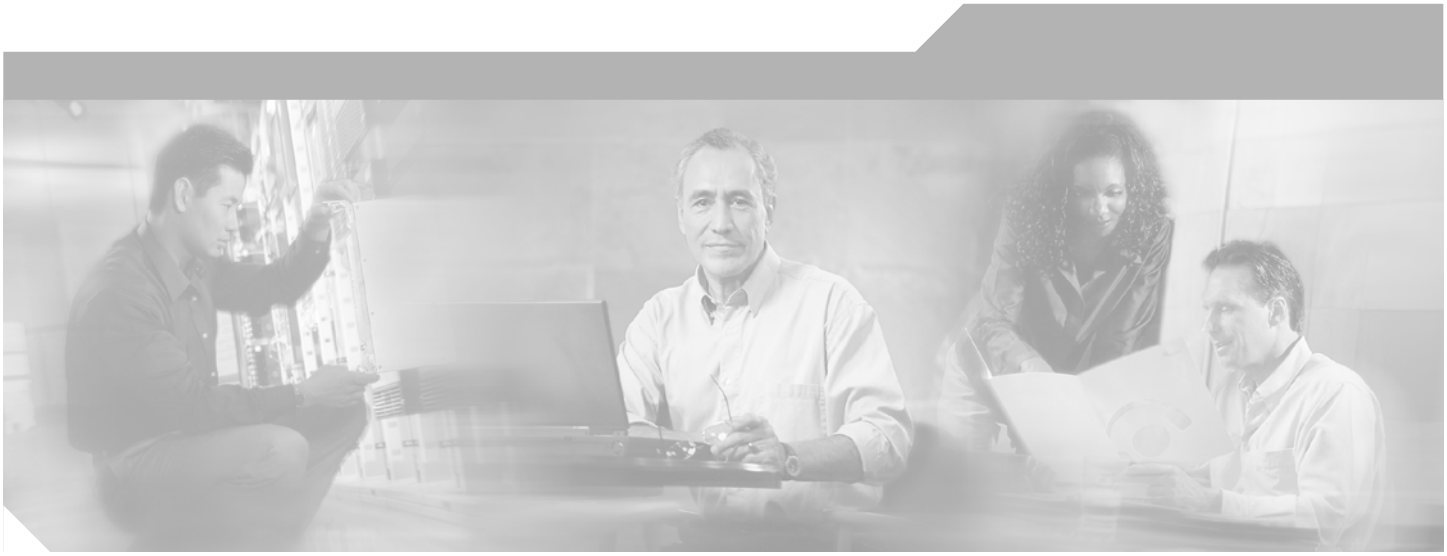


Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide

Software Release 3.0

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

Customer Order Number:
Text Part Number: OL-4211-05

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

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

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

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

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

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

Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide

Preface

The preface provides an overview of the *Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide* (OL-4211-04), references related publications, and explains how to obtain other documentation and technical assistance, if necessary.

The following topics are covered in this section:

Audience

This publication is for the person responsible for installing, configuring, and maintaining a Cisco Aironet IEEE 802.11a/b/g Wireless LAN Client Adapter (CB21AG or PI21AG) on a computer running the Microsoft Windows 2000 or XP operating system. This person should be familiar with computing devices and with network terms and concepts.

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

Purpose

This publication describes the Cisco Aironet CB21AG and PI21AG client adapters and explains how to install, configure, and troubleshoot them.

Caution 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 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows* if you are installing or using 340, 350, or CB20A cards.

Organization

This publication contains the following chapters:

- Chapter 1, "Product Overview," describes the client adapters and their hardware and software components and illustrates two common network configurations.
- Chapter 2, "Preparing for Installation," provides information that you need to know before installing a client adapter, such as safety information and system requirements.
- Chapter 3, "Installing the Client Adapter," provides instructions for installing the client adapter.
- Chapter 4, "Using the Profile Manager," explains how to use the Aironet Desktop Utility (ADU) profile manager feature to create and manage profiles for your client adapter.
- Chapter 5, "Configuring the Client Adapter," explains how to change the configuration parameters for a specific profile.
- Chapter 6, "Using EAP Authentication," explains the sequence of events that occurs and the actions you must take when a profile that is set for EAP authentication is activated.
- Chapter 7, "Viewing Status and Statistics," explains how to use ADU to view the client adapter's status and its transmit and receive statistics.
- Chapter 8, "Using the Aironet System Tray Utility (ASTU)," explains how to use ASTU to view status information about your client adapter and perform basic tasks.
- Chapter 9, "Routine Procedures," provides procedures for common tasks related to the client adapters, such as uninstalling client adapter software and opening ADU.
- Chapter 10, "Troubleshooting," provides information for diagnosing and correcting common problems that may be encountered when installing or operating a client adapter.

- Appendix A, "Technical Specifications," lists the physical, radio, power, and regulatory specifications for the client adapters.
- Appendix B, "Translated Safety Warnings," provides translations of client adapter safety warnings in nine languages.
- Appendix C, "Declarations of Conformity and Regulatory Information," provides declarations of conformity and regulatory information for the client adapters.
- Appendix D, "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 domain.
- Appendix E, "Configuring the Client Adapter through the Windows XP Operating System," explains how to configure and use your client adapter with the Microsoft Wireless Configuration Manager.
- Appendix F, "Performing a Site Survey" shows people who are responsible for conducting a site survey how they can use the site survey utility to determine the best placement for infrastructure devices within a wireless network.

Conventions

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

- Commands are in **boldface**.
- Variables are in *italics*.
- Configuration parameters are capitalized.
- Notes, cautions, and warnings 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.

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix "Translated Safety Warnings.")**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)**

Attention **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)**

Related Publications

For more information about Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters for Windows, refer to the following publication:

- *Release Notes for Cisco Aironet 802.11a/b/g Client Adapters (CB21AG and PI21AG) Install Wizard*

For more information about related Cisco Aironet products, refer to the publications for your infrastructure device. You can find Cisco Aironet technical documentation at this URL:

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

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you will find information about how to:

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

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

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

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

Reporting Security Problems in Cisco Products

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

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

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

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

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Product Overview

This chapter describes the Cisco Aironet CB21AG and PI21AG client adapters and illustrates their role in a wireless network.

The following topics are covered in this chapter:

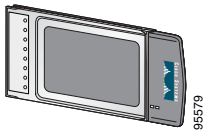
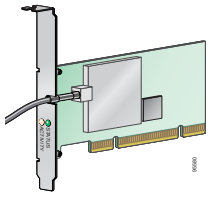
Introduction to the Client Adapters

The Cisco Aironet IEEE 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) are radio modules that provide wireless data communications among fixed, portable, and mobile devices within both wireless and wired network infrastructures. The client adapters are fully compatible when used in devices supporting "plug-and-play" (PnP) technology.

The primary function of the client adapters is to transfer data packets through the wireless infrastructure by communicating with other clients or with access points that are connected to a wired LAN. The adapters operate similarly to a standard network product except that radios rather than Ethernet cables make the connection to the wire. No special wireless networking functions are required, and all existing applications that operate over a network can operate using the adapters.

This document covers the two client adapters described in Table 1-1.

Table 1-1 Client Adapter Types

Client Adapter	Model Number	Description	Illustration
PC-Cardbus card	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. Host devices can include laptops and notebook computers.	
PCI card	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, such as a desktop personal computer.	

Terminology

The following terms are used throughout this document:

- **client adapter**—Refers to both types of adapters.
- **PC-Cardbus card** or **PCI card**—Refers to a specific adapter.
- **workstation** (or **station**)—Refers to a computing device with an installed client adapter.
- **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.

Hardware Components

The client adapters have three major hardware components: a radio, a radio antenna, and two LEDs.

Radio

The client adapters contain a dual-band radio that is both IEEE 802.11a and 802.11b/g compliant. The radio uses both direct-sequence spread spectrum (DSSS) technology and orthogonal frequency division multiplexing (OFDM) technology for client applications in the 2.4-GHz Industrial Scientific Medical (ISM) frequency band and OFDM technology in the 5-GHz Unlicensed National Information Infrastructure (UNII) frequency bands. The client adapters operate with other IEEE 802.11a or 802.11b/g-compliant client devices in ad hoc mode or with Cisco Aironet access points and other IEEE 802.11a or 802.11b/g-compliant infrastructure devices in infrastructure mode.

Radio Antenna

The type of antenna used depends on your client adapter:

- PC-Cardbus cards have an integrated, permanently attached 0-dBi gain, dual-band 2.4/5-GHz diversity antenna. The benefit of the diversity antenna system is improved coverage. The system works by enabling the card to sample and switch between its two antenna ports in order to select the optimum port for receiving data packets. As a result, the card has a better chance of maintaining the radio frequency (RF) connection in areas of interference. The antenna is housed within the section of the card that hangs out of the Cardbus slot when the card is installed.
- PCI cards have a 1-dBi gain, dual-band 2.4/5-GHz antenna that is permanently attached by a 6.6-foot (2-meter) cable. A base is provided with the antenna to enable it to be mounted to a wall or to sit upright on a desk or other horizontal surface.

LEDs

The client adapters have two LEDs that glow or blink to indicate the status of the adapter or to convey error messages. Refer to Chapter 10 for an interpretation of the LED codes.

Software Components

The client adapters have two major software components: a driver and client utilities. These components are installed together by running a single executable Install Wizard file that is available from Cisco.com. This file can be run on Windows 2000 or XP and can be used only with CB21AG and PI21AG client adapters.

Note Chapter 3 provides instructions on using the Install Wizard to install these software components.

Driver

The driver provides an interface between a computer's operating system and the client adapter, thereby enabling the operating system and the applications it runs to communicate with the adapter. The driver must be installed before the adapter can be used.

Client Utilities

Two client utilities are available for use with the client adapters: Aironet Desktop Utility (ADU) and Aironet System Tray Utility (ASTU). These utilities are optional applications that interact with the client adapter's radio to adjust settings and display information.

ADU enables you to create configuration profiles for your client adapter and perform user-level diagnostics. Because ADU performs a variety of functions, it is documented by function throughout this manual.

ASTU, which is accessible from an icon in the Windows system tray, provides a small subset of the features available through ADU. Specifically, it enables you to view status information about your client adapter and perform basic tasks. Chapter 8 provides detailed information and instructions on using ASTU.

Note If your computer is running Windows XP, you can configure your client adapter through the Microsoft Wireless Configuration Manager (or another third-party tool) instead of through ADU. Refer to Appendix E for information. However, ADU is recommended for configuring the client adapter.

Network Configurations Using Client Adapters

Client adapters can be used in a variety of network configurations. In some configurations, access points provide connections to your network or act as repeaters to increase wireless communication range. The maximum communication range is based on how you configure your wireless network.

This section describes and illustrates the two most common network configurations:

- Ad hoc wireless local area network (LAN)
- Wireless infrastructure with workstations accessing a wired LAN

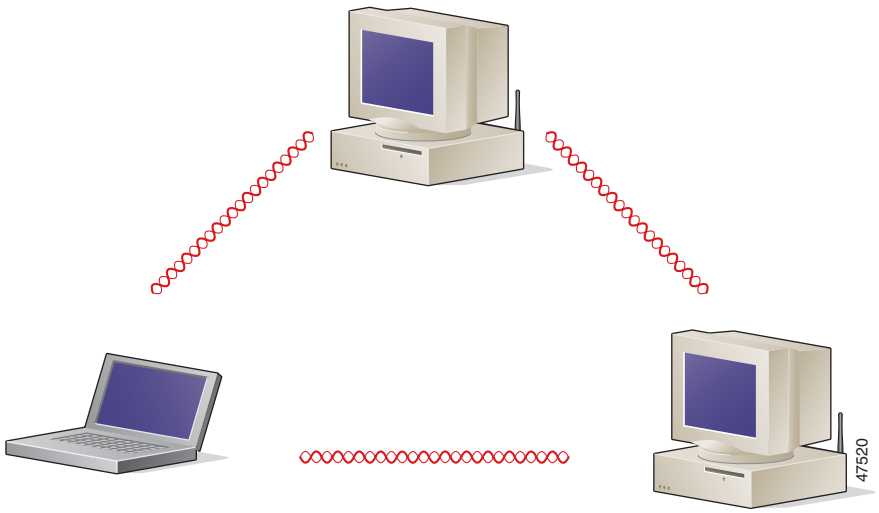
For examples of more complex network configurations involving client adapters and access points, refer to the documentation for your access point.

Note Refer to Chapter 5 for information on setting the client adapter's network type.

Ad Hoc Wireless LAN

An ad hoc (or *peer-to-peer*) wireless LAN (see Figure 1-1) is the simplest wireless LAN configuration. In a wireless LAN using an ad hoc network configuration, all devices equipped with a client adapter can be linked together and communicate directly with each other. The use of an infrastructure device, such as an access point, is not required.

Figure 1-1 Ad Hoc Wireless LAN

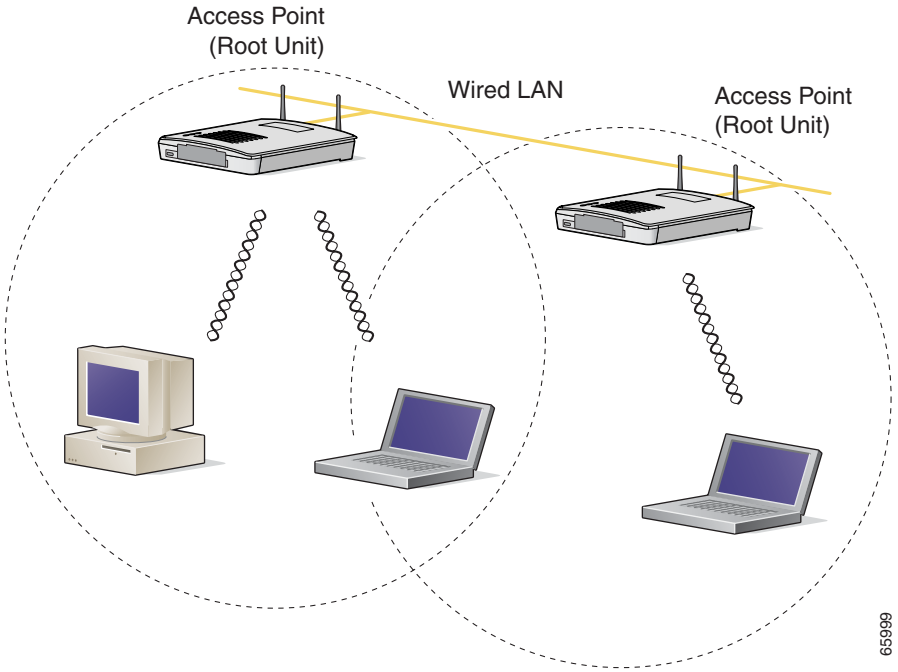


Wireless Infrastructure with Workstations Accessing a Wired LAN

A microcellular network can be created by placing two or more access points on a LAN. Figure 1-2 shows a microcellular network with workstations accessing a wired LAN through several access points.

This configuration is useful with portable or mobile stations because it enables them to be directly connected to the wired network even while moving from one microcell domain to another. This process is transparent, and the connection to the file server or host is maintained without disruption. The mobile station stays connected to an access point as long as it can. However, when the transfer of data packets needs to be retried or beacons are missed, the station automatically searches for and associates to another access point. This process is referred to as *seamless roaming*.

Figure 1-2 Wireless Infrastructure with Workstations Accessing a Wired LAN



Preparing for Installation

This chapter provides information that you need to know before installing a client adapter.

The following topics are covered in this chapter:

Safety information

Follow the guidelines in this section to ensure proper operation and safe use of the client adapter.

FCC Safety Compliance Statement

The FCC, with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication will result in user exposure substantially below the FCC recommended limits.

Safety Guidelines

- Do not touch or move the antenna while the unit is transmitting or receiving.
- Do not hold any component containing a radio such that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; otherwise, the radio may be damaged.
- Use in specific environments:
  - The use of wireless devices in hazardous locations is limited to the constraints posed by the safety directors of such environments.
  - The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).
  - The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.

Warnings

Observe the following warnings when operating the client adapter. The second warning pertains to the PI21AG client adapter, and the third warning pertains to the CB21AG client adapter.

Warning **Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.**

Warning **In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 7.9 inches (20 cm) or more from the body of all persons.**

Warning **This device has been tested and complies with FCC RF Exposure (SAR) limits in typical laptop computer configurations and this device can be used in desktop or laptop computers with side mounted PC Card slots that can provide at least 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. This device cannot be used with handheld PDAs (personal digital assistants). Use in other configurations may not ensure compliance with FCC RF exposure guidelines. This device and its antenna must not be co-located or operated in conjunction with any other antenna or transmitter.**

Translated versions of these safety warnings are provided in Appendix B.

Unpacking the Client Adapter

Follow these steps to unpack the client adapter:

Step 1 Open the shipping container and carefully remove the contents.

Step 2 Return all packing materials to the shipping container and save it.

Step 3 Ensure that all items listed in the "Package Contents" section below are included in the shipment. Check each item for damage.

Note If any item is damaged or missing, notify your authorized Cisco sales representative.

Package Contents

Each client adapter is shipped with the following items:

- 1-dBi gain antenna permanently attached by a 6.6-ft (2-m) cable, antenna base, low-profile bracket, two mounting screws, and two plastic wall anchors (PCI cards only)
- *Quick Start Guide: Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG)*
- Cisco Aironet 802.11a/b/g Wireless Adapters (CB21AG and PI21AG) CD

System Requirements

In addition to the items shipped with the client adapter, you also need the following items in order to install and use the adapter:

- One of the following computing devices running Windows 2000 or XP:
  - Laptop or notebook computer equipped with a 32-bit Cardbus slot
  - Desktop personal computer equipped with an empty PCI expansion slot

Note Cisco recommends a 300-MHz (or greater) processor.

- Service Pack 2 for Windows XP
- 20 MB of free hard disk space (minimum)
- 128 MB of RAM or greater (recommended)
- The appropriate tools for removing your computer's cover and expansion slot dust cover and for mounting the antenna base (for PCI cards)
- If your wireless network uses EAP-TLS or PEAP authentication, Certificate Authority (CA) and user certificates for EAP-TLS authentication or CA certificate for PEAP authentication
- If your wireless network uses PEAP (EAP-GTC) authentication with a One-Time Password (OTP) user database:
  - A hardware token device from OTP vendors or the Secure Computing SofToken program (version 2.1 or later)
  - Your hardware or software token password
- The Microsoft 802.1X supplicant, if your client adapter is installed on a Windows 2000 device and uses PEAP (EAP-MSCHAPV2) with machine authentication
- All necessary infrastructure devices (such as access points, servers, gateways, user databases, etc.) must be properly configured for any authentication type you plan to enable on the client.
- The following information from your system administrator:
  - The logical name for your workstation (also referred to as *client name*)
  - The protocols necessary to bind to the client adapter, such as TCP/IP
  - The case-sensitive service set identifier (SSID) for your RF network
  - If your network setup does not include a DHCP server, the IP address, subnet mask, and default gateway address of your computer
  - The wired equivalent privacy (WEP) keys of the access points with which your client adapter will communicate, if your wireless network uses static WEP for security
  - The username and password for your network account
  - Protected access credentials (PAC) file if your wireless network uses EAP-FAST authentication with manual PAC provisioning

Site Requirements

This section discusses the site requirements for both infrastructure and client devices.

For Infrastructure Devices

Because of differences in component configuration, placement, and physical environment, every network application is a unique installation. Therefore, before you install any wireless infrastructure devices (such as access points, bridges, and base stations, which connect your client adapters to a wired LAN), a site survey must be performed to determine the optimum placement of these devices to maximize range, coverage, and network performance. Appendix F, which is provided for people who are responsible for conducting a site survey, explains how the site survey utility can be used to determine the best placement for infrastructure devices within a wireless network.

Note Infrastructure devices are installed and initially configured prior to client devices.

For Client Devices

Because the client adapter is a radio device, it is susceptible to RF obstructions and common sources of interference that can reduce throughput and range. Follow these guidelines to ensure the best possible performance:

- Install the client adapter in an area where large steel structures such as shelving units, bookcases, and filing cabinets will not obstruct radio signals to and from the client adapter.
- Install the client adapter away from microwave ovens. Microwave ovens operate on the same frequency as the client adapter and can cause signal interference.

Installing the Client Adapter

This chapter provides instructions for installing the client adapter.

The following topics are covered in this chapter:

Inserting a Client Adapter

This section provides instructions for inserting a PC-Cardbus card or PCI card into your computer.

Caution These procedures and the physical connections they describe apply generally to conventional Cardbus slots and PCI expansion slots. In cases of custom or nonconventional equipment, be alert to possible differences in Cardbus slot and PCI expansion slot configurations.

Inserting a PC-Cardbus Card

Step 1 Before you begin, examine the card. One end has a dual-row, 68-pin connector. The card is keyed so it can be inserted only one way into the Cardbus slot.

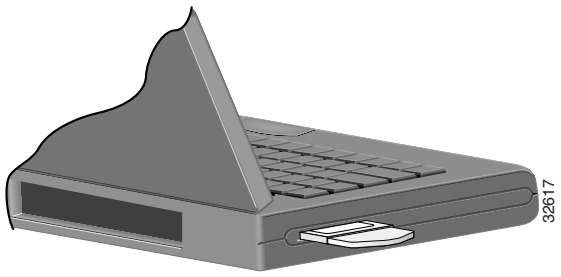
Note The PC-Cardbus slot, if supported, is usually on the left or right side of a laptop computer, depending on the model.

Step 2 Turn on your computer and let the operating system boot up completely.

Step 3 Hold the card with the Cisco label facing up and insert it into the Cardbus slot, applying just enough pressure to make sure it is fully seated (see Figure 3-1). The green LED lights when the card is inserted properly.

Caution Do not force the card into your computer's Cardbus slot. Forcing it will damage both the card and the slot. If the card does not insert easily, remove the card and reinsert it.

Figure 3-1 Inserting a PC-Cardbus Card into a Computer



Note The configuration profiles for PC-Cardbus cards are tied to the slot in which the card is inserted. Therefore, you must always insert your PC-Cardbus card into the same slot or create profiles for both slots. See Chapter 4 for information on creating profiles for your client adapter.

Step 4 If the Found New Hardware Wizard window appears, click **Cancel**.

Note If you do not click **Cancel**, the wizard will attempt to install software for the client adapter but will be unable to find it.

Step 5 Go to the "Installing the Client Adapter Software" section on page 3-9.

Inserting a PCI Card

You must perform the following procedures in the order listed below to insert a PCI card:

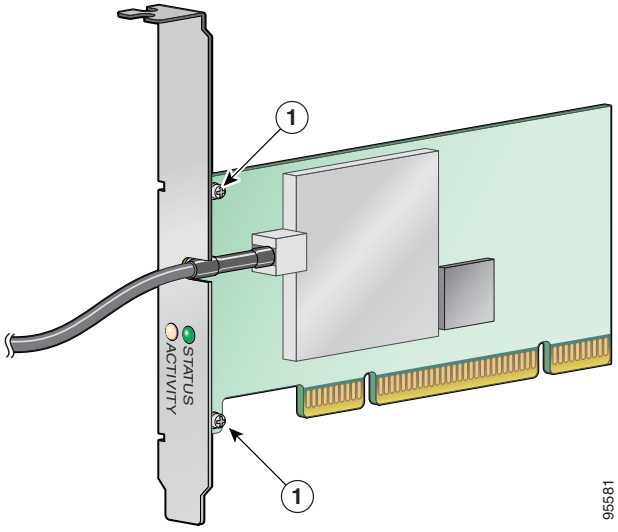
- Change the bracket (if required), see below
- Insert the card, page 3-4
- Assemble the antenna, page 3-5
- Mount the antenna, page 3-6

Changing the Bracket

The PCI card is shipped with a full-profile bracket attached. If the PC into which you are inserting the PCI card requires the card to use a low-profile bracket, follow these steps to change brackets.

Step 1 Remove the two screws that attach the bracket to the card. See Figure 3-2.

Figure 3-2 Changing the PCI Card Bracket



1	Bracket screws

Step 2 Slide the bracket away from the card; then tilt the bracket to free the antenna cable.

Caution Do not pull on the antenna cable or detach it from the PCI card. The antenna is meant to be permanently attached to the card.

Step 3 Hold the low-profile bracket to the card so that the LEDs slip through their corresponding holes on the bracket.

Step 4 Insert the screws that you removed in Step 1 into the holes on the populated side of the card near the bracket (see Figure 3-2) and tighten.

Inserting the Card

Follow the steps below to insert a PCI card into your PC.

Step 1 Turn off the PC and all its components.

Step 2 Remove the computer cover.

Note On most Pentium PCs, PCI expansion slots are white. Refer to your PC documentation for slot identification.

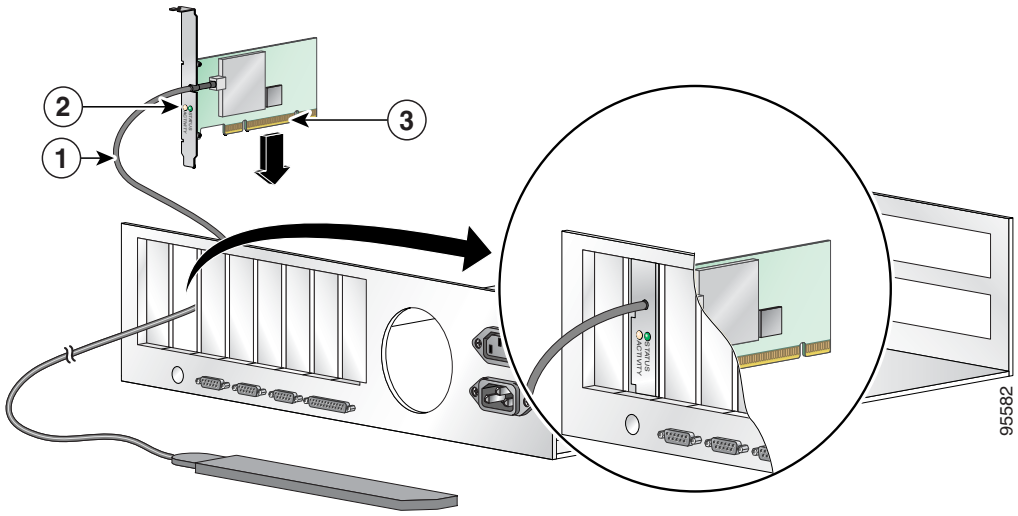
Step 3 Remove the screw from the top of the CPU back panel above an empty PCI expansion slot. This screw holds the metal bracket on the back panel.

Caution Static electricity can damage your PCI card. Before removing the card from the anti-static packaging, discharge static by touching a metal part of a grounded PC.

Step 4 Locate an empty PCI expansion slot inside your computer.

Step 5 Slip your card's antenna through the opening near the empty expansion slot so that it is located outside of the computer. See Figure 3-3.

Figure 3-3 Inserting a PCI Card into a PC



1	Antenna cable
2	LEDs
3	Card edge connector

Step 6 Tilt the card to enable the LEDs to slip through the opening in the CPU back panel. See the enlarged view in Figure 3-3.

Step 7 Press the card into the empty slot until its connector is firmly seated.

Caution Do not force the card into the expansion slot; this could damage both the card and the slot. If the card does not insert easily, remove it and reinsert it.

Step 8 Reinstall the screw on the CPU back panel and replace the computer cover.

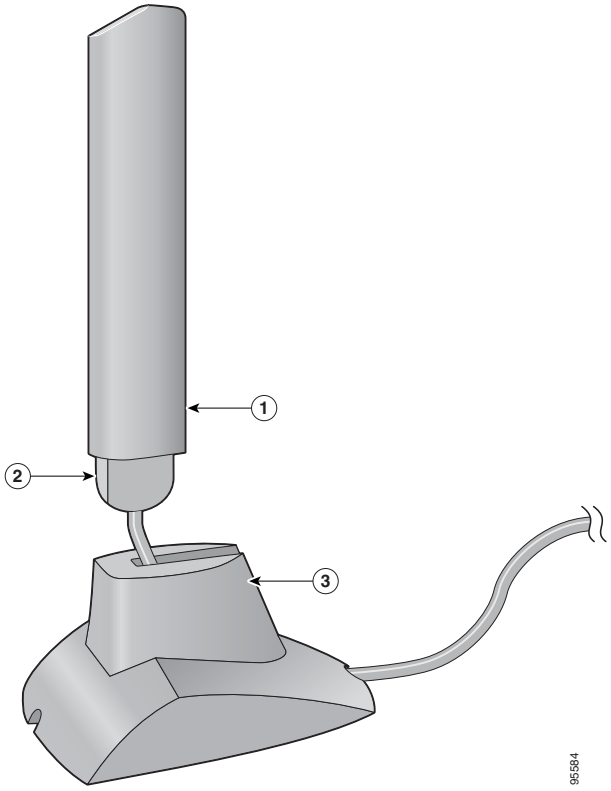
Assembling the Antenna

Follow the steps below to assemble the PCI card's antenna.

Step 1 Slide the antenna through the opening in the bottom of the antenna base.

Step 2 Position the antenna so its notches are facing the Cisco label on the front of the base. See Figure 3-4.

Figure 3-4 Inserting the Antenna into Its Base



1	Antenna
2	Notch
3	Antenna base

Step 3 Press the antenna cable into the receptacle on the top of the base as shown in Figure 3-4.

Step 4 Press the antenna straight down into the receptacle until it clicks into place.

Mounting the Antenna

Because the PCI card is a radio device, it is susceptible to RF obstructions and common sources of interference that can reduce throughput and range. Follow these guidelines to ensure the best possible performance:

- Place the PCI card's antenna in an area where large steel structures such as shelving units, bookcases, and filing cabinets will not obstruct radio signals being transmitted or received.
- Place the antenna away from microwave ovens and 2.4- and 5.8-GHz cordless phones. These products can cause signal interference because they operate in the same frequency range as the PCI card.

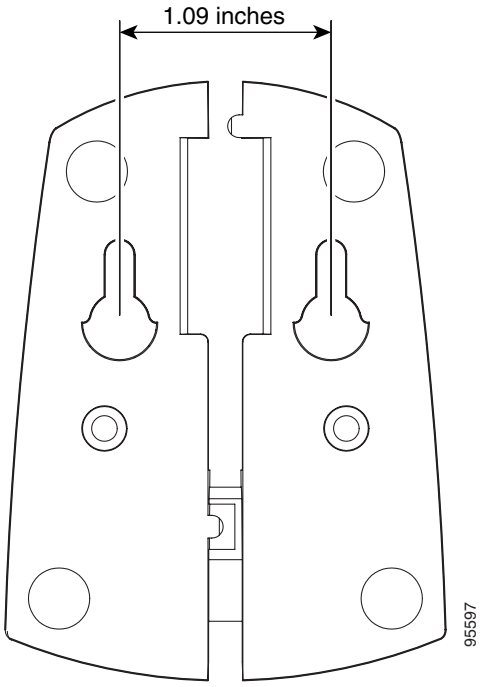
Follow the steps below to position the PCI card's antenna on a flat horizontal surface or to mount it to a wall.

Step 1 Perform one of the following:

- If you want to use the antenna on a flat horizontal surface, position the antenna so it is pointing straight up. Then go to Step 7.
- If you want to mount the antenna to a wall, go to Step 2.

Step 2 Drill two holes in the wall that are 1.09 in. (2.8 cm) apart. Figure 3-5 shows the distance between the mounting holes on the bottom of the antenna base.

Figure 3-5 Bottom of Antenna Base

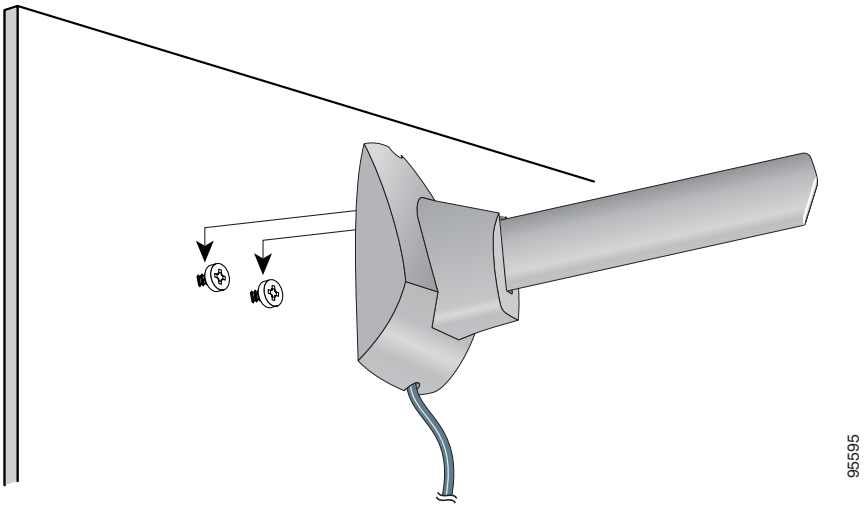


Step 3 Tap the two supplied wall anchors into the holes.

Step 4 Drive the two supplied screws into the wall anchors, leaving a small gap between the screw head and the anchor.

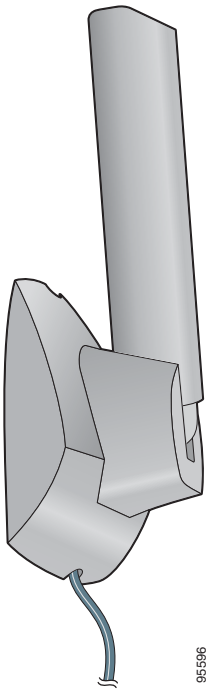
Step 5 Position the mounting holes on the bottom of the antenna base over the screws (see Figure 3-6) and pull down to lock in place.

Figure 3-6 Mounting the Antenna



Step 6 The antenna rotates 90 degrees from its base. For optimal reception, position the antenna so it is pointing straight up (see Figure 3-7).

Figure 3-7 Rotating the Antenna



Step 7 Boot up your PC. The green LED lights when the card is inserted properly.

Step 8 If the Found New Hardware Wizard window appears, click **Cancel**.

Step 9 Go to the "Installing the Client Adapter Software" section below.

Installing the Client Adapter Software

This section describes how to install Cisco Aironet CB21AG or PI21AG client adapter driver and utilities from a single executable file named *WinClient-802.11a-b-g-Ins-Wizard-vx.exe*, where *x* represents the release number. Follow these steps to install these client adapter software components on a computer running Windows 2000 or XP.

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 cards, and the Aironet Client Utility (ACU) must be used with all other Cisco Aironet client adapters.

Caution Do not eject your client adapter at any time during the installation process, including during the reboot.

Note This procedure is meant to be used the first time the Cisco Aironet CB21AG or PI21AG client adapter software is installed on your computer. If this software is already installed on your computer, follow the instructions in Chapter 9 to upgrade the client adapter software.

Note Only one CB21AG or PI21AG client adapter can be installed and used at a time. The software does not support the use of multiple CB21AG or PI21AG cards.

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**.

Step 9 Perform one of the following steps:

- If you are using a PC-Cardbus card, click **Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Adapter (CB21AG)**.
- If you are using a PCI card, click **Cisco Aironet 802.11a/b/g PCI Wireless LAN Client Adapter (PI21AG)**.

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

Step 11 Click **Aironet Client Installation Wizard (Firmware, Driver, Utility)**.

Step 12 Click **Windows 2000 or Windows XP**.

Step 13 Click the link with the greatest release number.

Step 14 Click the Install Wizard file (**WinClient-802.11a-b-g-Ins-Wizard-v*xx*.exe**), where ***xx*** is the version number.

Step 15 If prompted, enter your CCO username and password, and click **OK**.

Step 16 Complete the encryption authorization form, read and accept the terms and conditions of the Software License Agreement, select the file again to download it, and save the file on your computer's Desktop.

Step 17 Use Windows Explorer to find the installer.

Step 18 Double-click the installer. The "Starting InstallShield Wizard" message appears followed by the Preparing Setup window (see Figure 3-8) and the Cisco Aironet Installation Program window (see Figure 3-9).

Figure 3-8 Preparing Setup Window

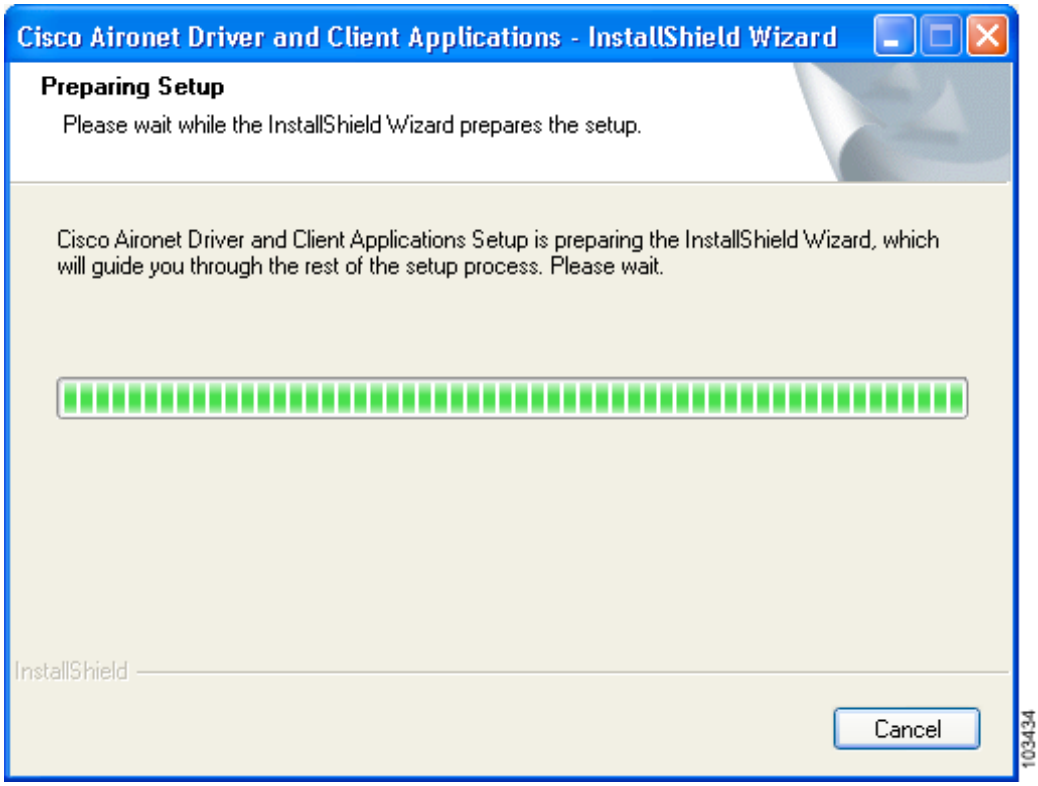
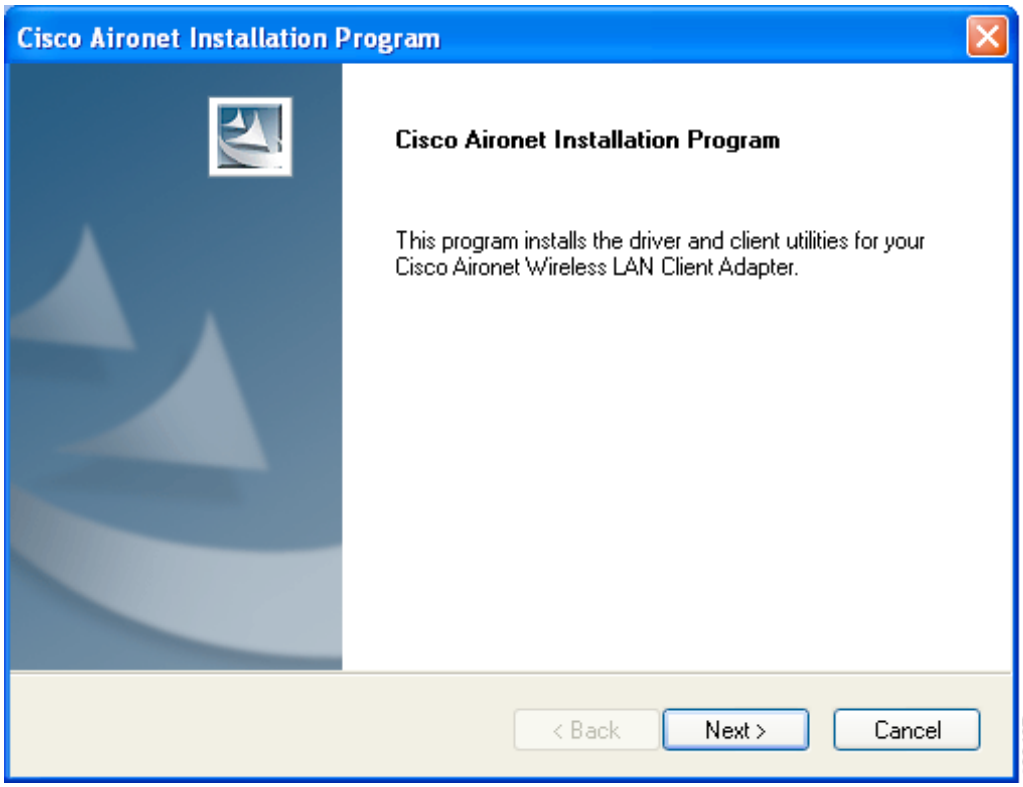
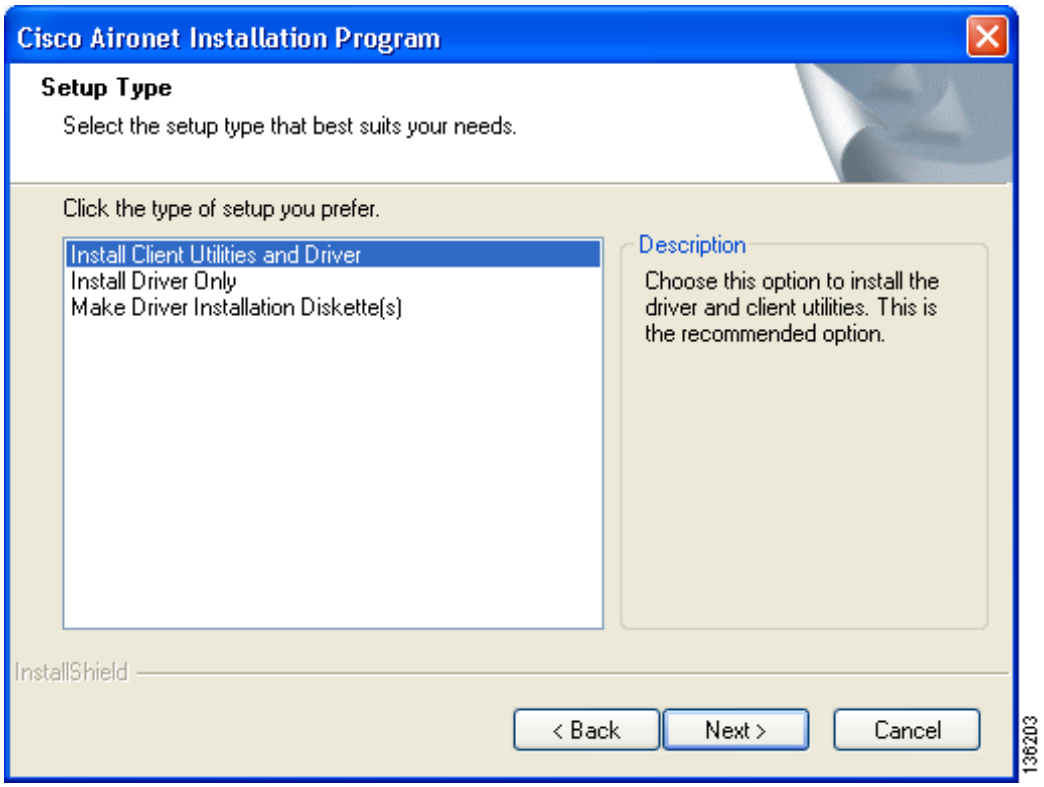


Figure 3-9 Cisco Aironet Installation Program Window



Step 19 Click **Next**. The Setup Type window appears (see Figure 3-10).

Figure 3-10 Setup Type Window



Step 20 Choose one of the following options and click **Next**:

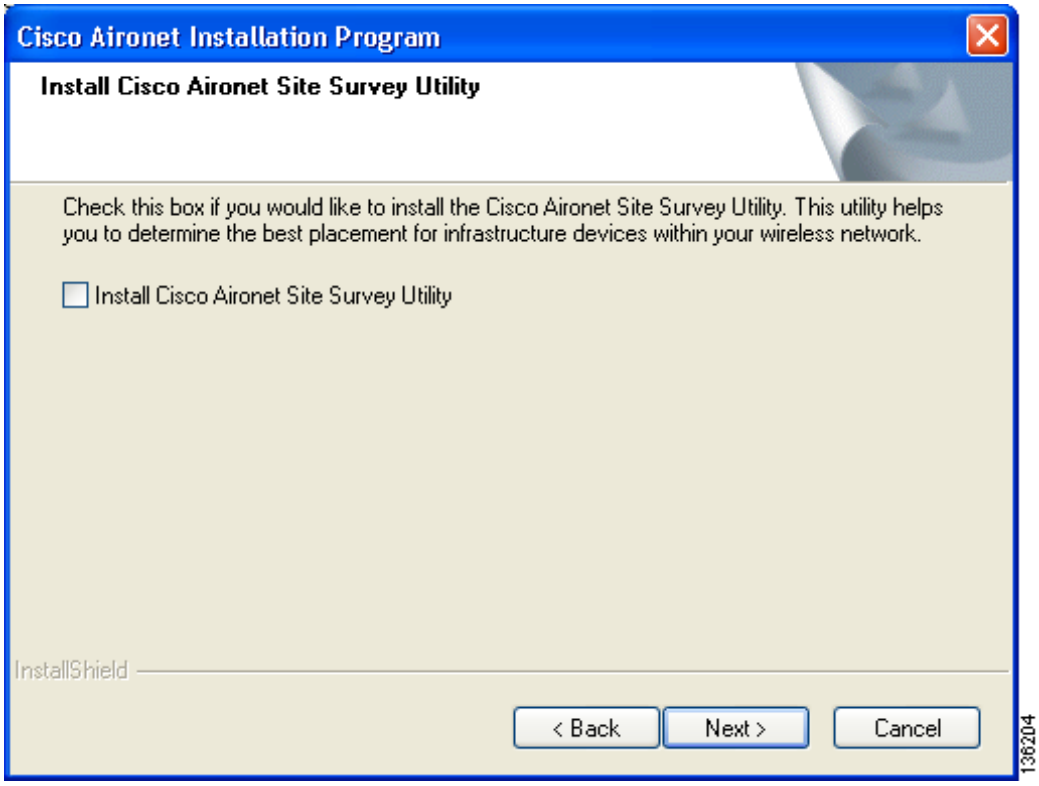
Note To ensure compatibility among software components, Cisco recommends that you install the client utilities and driver.

- **Install Client Utilities and Driver**—Installs the client adapter driver and client utilities.
- **Install Driver Only**—Installs only the client adapter driver. If you choose this option, click **Next** and go to Step 32.
- **Make Driver Installation Diskette(s)**—Enables you to create driver installation diskettes that can be used to install drivers using the Windows Device Manager.

Note If you choose one of the first two options and a client adapter is not inserted into your computer, the following message appears: "The device may not be present or could have been ejected/unplugged from the system. Insert or reinsert it now." Insert the client adapter and click **OK**. If you proceed without the client adapter inserted, the installation continues, but the driver installation is incomplete. You must manually install the driver later using the Update Device Driver Wizard. See the "Manually Installing or Upgrading the Client Adapter Driver" section on page 9-6 for instructions.

Step 21 When the Install Cisco Aironet Site Survey Utility window appears (see Figure 3-11), check the **Install Cisco Aironet Site Survey Utility** check box if you want to install a utility that helps you to determine the best placement of infrastructure devices within your wireless network. Click **Next**.

Figure 3-11 Install Cisco Aironet Site Survey Utility Window



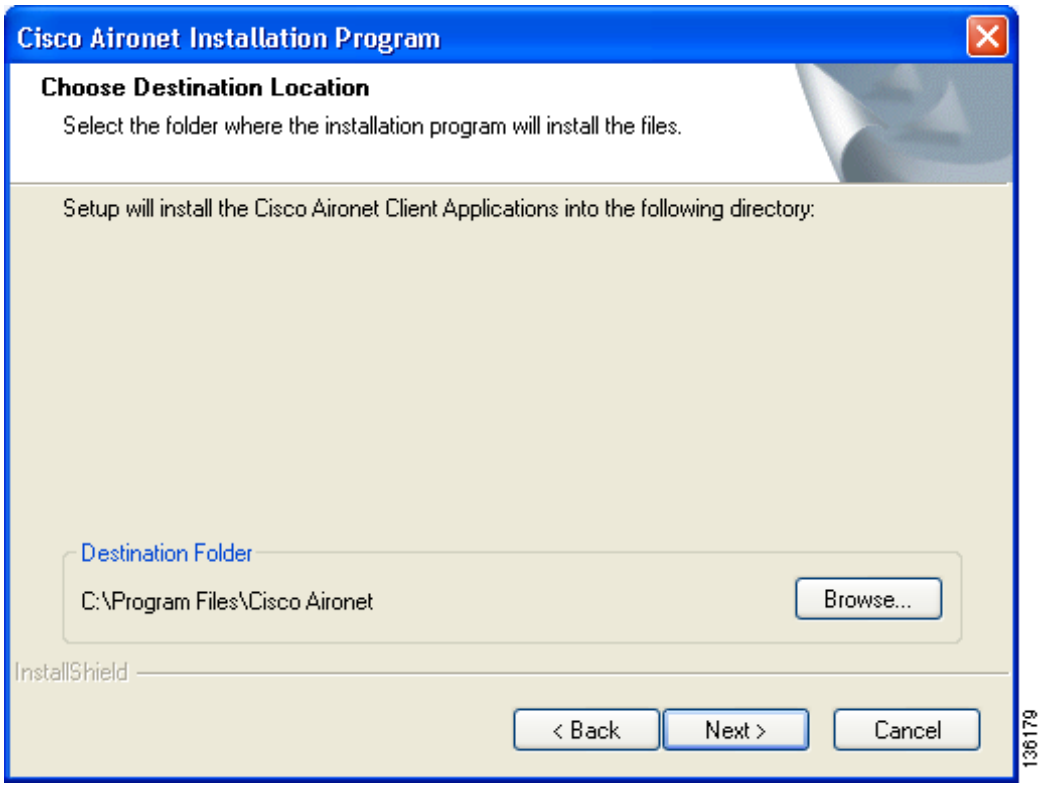
Note The site survey utility is a stand-alone application, separate from ADU, that runs from an executable file. If you check the Install Cisco Aironet Site Survey Utility check box, the Install Wizard installs the site survey executable file in the C:\Program Files\Cisco Aironet directory (unless you specify a different directory in Step 23). See Appendix F for instructions on using the utility.

Step 22 If a message appears indicating that you are required to restart your computer at the end of the installation process, click **Yes**.

Note If you click **No**, you are asked to confirm your decision. If you proceed, the installation process terminates.

The Choose Destination Location window appears (see Figure 3-12).

Figure 3-12 Choose Destination Location Window



Step 23 Perform one of the following:

- If you chose the first option in Step 20, click **Next** to install the client utility files in the C:\Program Files\Cisco Aironet directory.

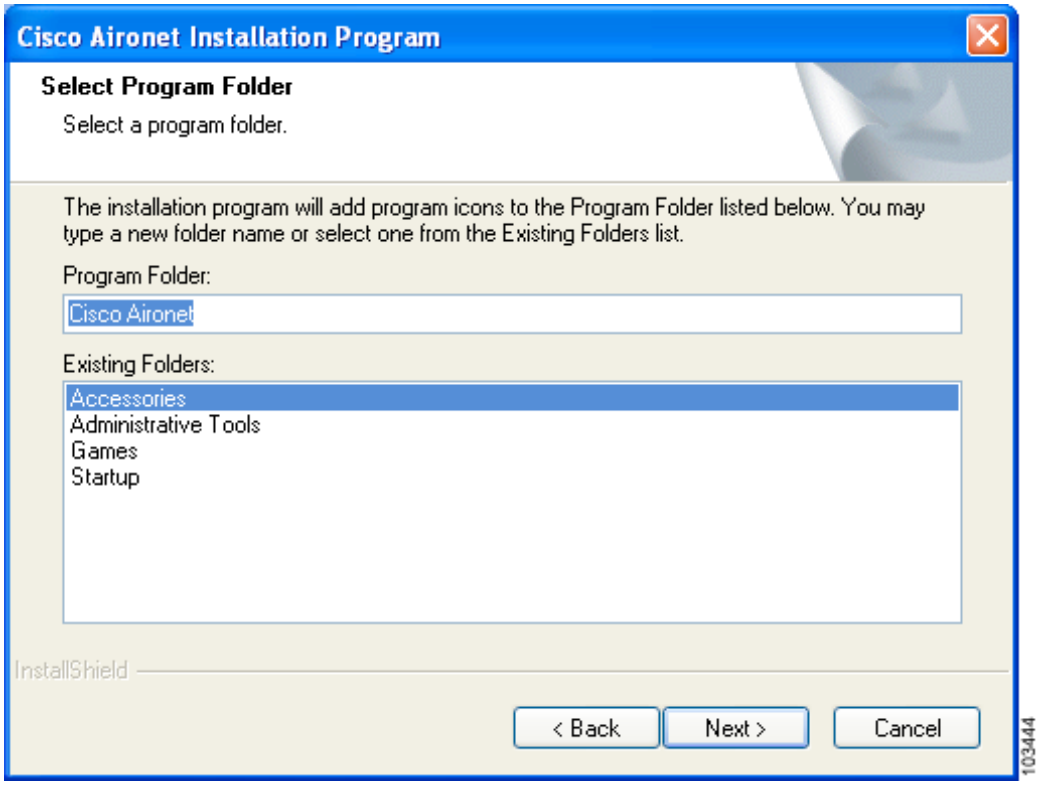
  Note If you want to install the client utilities in a different directory, click **Browse**, choose a different directory, click **OK**, and click **Next**.

- If you chose the Make Driver Installation Diskette(s) option in Step 20, insert a floppy disk into your computer and click **Next** to copy the driver to the diskette. Go to Step 32.

  Note If you want to copy the driver to a different drive or directory, click **Browse**, choose a new location, click **OK**, and click **Next**.

Step 24 The Select Program Folder window appears (see Figure 3-13).

Figure 3-13 Select Program Folder Window

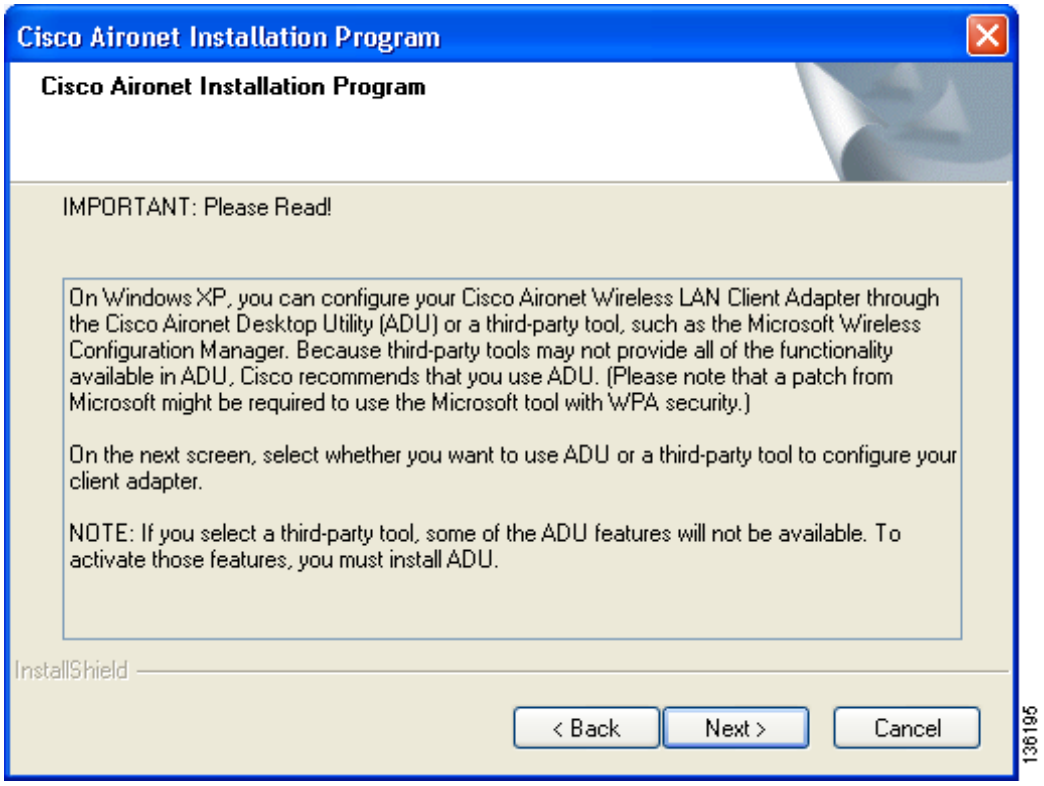


Step 25 Click **Next** to add program icons to the Cisco Aironet program folder.

Note If you want to specify a different program folder, choose a folder from the Existing Folders list or type a new folder name in the Program Folder field and click **Next**.

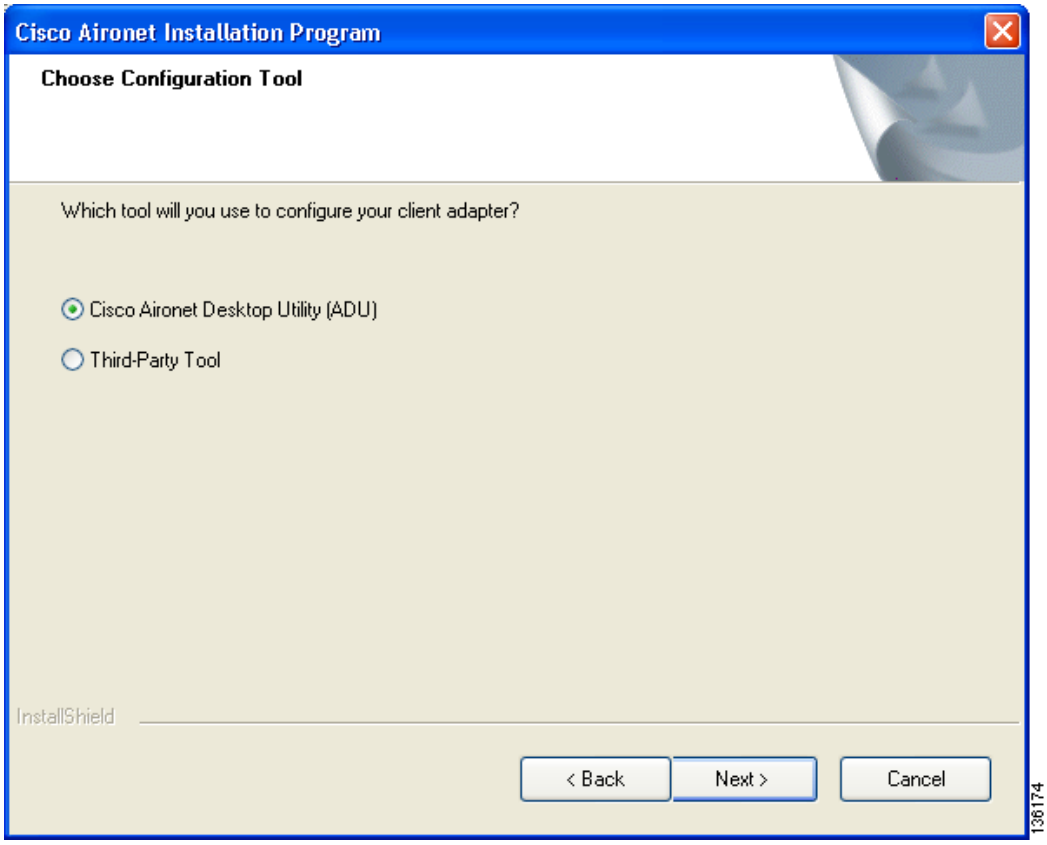
Step 26 If your computer is running Windows 2000, go to Step 32. If your computer is running Windows XP, the window titled IMPORTANT: Please Read! appears (see Figure 3-14).

Figure 3-14 IMPORTANT: Please Read! Window



Step 27 Read the information displayed and click **Next**. The Choose Configuration Tool window appears (see Figure 3-15).

Figure 3-15 Choose Configuration Tool Window



Step 28 Choose one of the following options:

- **Cisco Aironet Desktop Utility (ADU)**—Enables you to configure your client adapter using ADU.
- **Third-Party Tool**—Enables you to configure your client adapter using a third-party tool such as the Microsoft Wireless Configuration Manager in Windows XP.

Table 3-1 compares Windows XP and ADU client adapter features.

Table 3-1 Comparison of Windows XP and ADU Client Adapter Features

Feature	Windows XP	ADU
Configuration parameters	Limited	Extensive
Capabilities		
Create profiles	Yes	Yes
Enable/disable radio	No	Yes

Table 3-1 Comparison of Windows XP and ADU Client Adapter Features (continued)

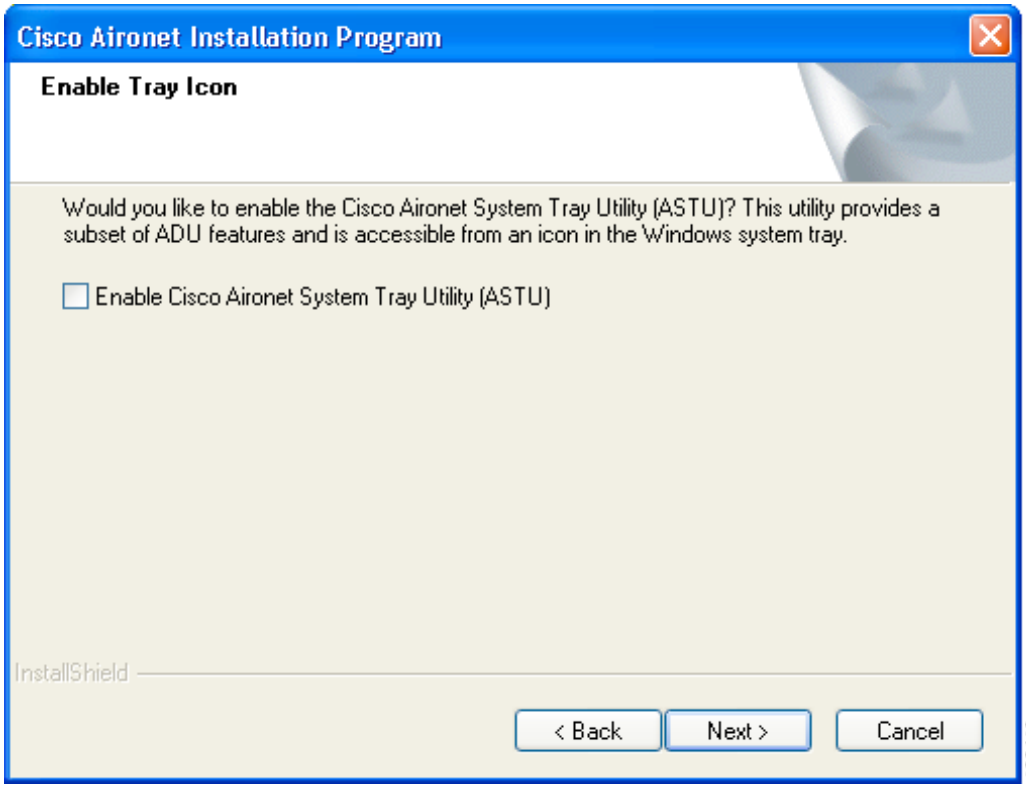
Feature	Windows XP	ADU
Security		
Static WEP	Yes	Yes
LEAP or EAP-FAST authentication with dynamic WEP	No	Yes
EAP-TLS or PEAP authentication	Yes	Yes
Status and statistics		
Status window	Limited	Extensive
Statistics window (transmit & receive)	No	Yes

Note If you choose Cisco Aironet Desktop Utility (ADU) above, the Microsoft Wireless Configuration Manager is disabled. If you ever manually enable it, you are prompted to disable it whenever ADU is activated.

Step 29 Click **Next**.

Step 30 If you chose Cisco Aironet Desktop Utility (ADU) in Step 28, go to Step 32. If you chose Third-Party Tool, the Enable Tray Icon window appears (see Figure 3-16).

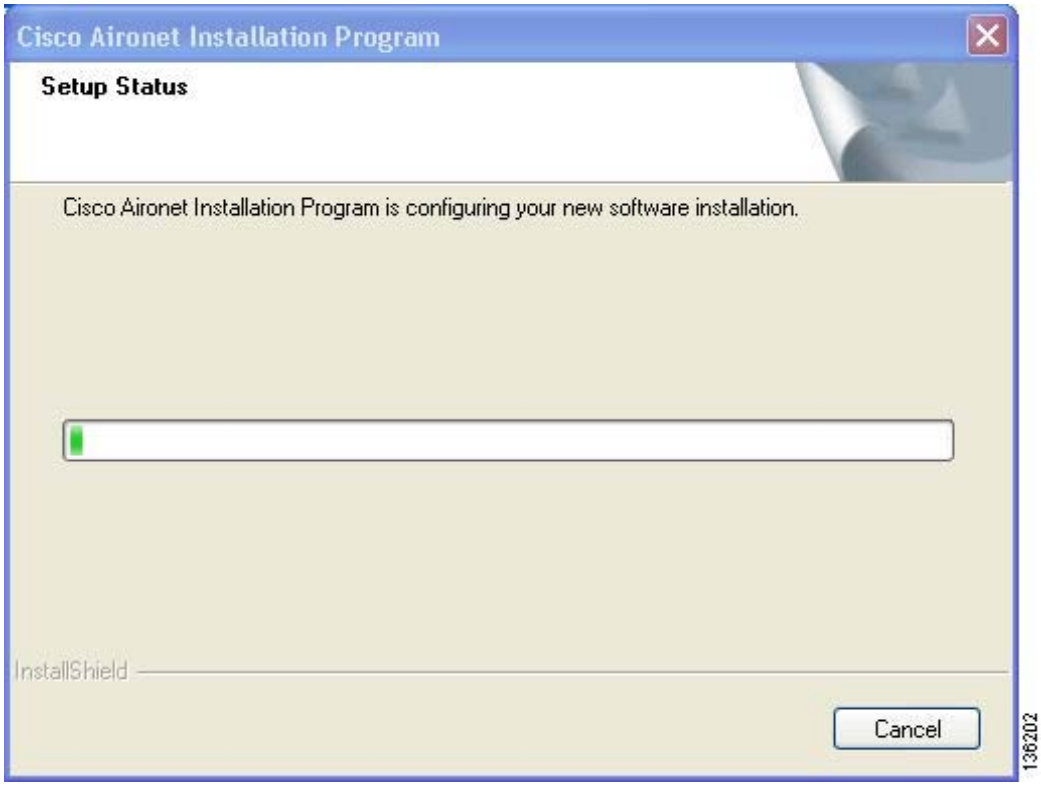
Figure 3-16 Enable Tray Icon Window



Step 31 Check the **Enable Cisco Aironet System Tray Utility (ASTU)** check box if you want to be able to use ASTU even though you have chosen to configure your client adapter through a third-party tool instead of ADU and click **Next**.

Step 32 When prompted to insert your client adapter, click **OK**. The Setup Status window appears (see Figure 3-17).

Figure 3-17 Setup Status Window



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

Step 33 When a message appears indicating that your computer needs to be rebooted, click **OK** and allow your computer to restart.

Step 34 If the Windows Found New Hardware Wizard appears after your computer reboots, click **Next**, allow the wizard to install the software for the client adapter, and click **Finish**.

Step 35 If your network setup does not include a DHCP server and you plan to use TCP/IP, follow these steps for your operating system.

- **Windows 2000**
  a. Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**.
  b. Right-click **Local Area Connection *x*** (where *x* represents the number of the connection).
  c. Click **Properties**.
  d. In the Components Checked Are Used by This Connection field, click **Internet Protocol (TCP/IP)** and **Properties**.

e. Choose **Use the following IP address** and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator).

f. Click **OK** to close each open window.

- **Windows XP**

a. Double-click **My Computer**, **Control Panel**, and **Network Connections**.

b. Right-click **Wireless Network Connection *x*** (where *x* represents the number of the connection).

c. Click **Properties**.

d. In the This Connection Uses the Following Items field, click **Internet Protocol (TCP/IP)** and **Properties**.

e. Choose **Use the following IP address** and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator).

f. Click **OK** to close each open window.

Step 36 If you are prompted to restart your computer, click **Yes**.

Step 37 Now that your client adapter is properly installed, it is ready to be configured.

- If you are planning to configure your client adapter through ADU, go to Chapter 4 to create configuration profiles.
- If you are planning to configure your client adapter through the Windows XP Wireless Configuration Manager, go to Appendix E.
- If you are planning to configure your client adapter through another third-party tool, refer to the documentation for that application.

Note If you want to be able to use ADU's Group Policy Delay parameter, follow the instructions below to download and install a necessary hot fix before configuring your client adapter.

Note If you experienced problems during or after installation, refer to Chapter 10 for troubleshooting information.

Installing the Intermediate Driver Manually

In some instances, the installation of the CB21AG software might not work as expected because the intermediate driver might not have installed correctly. In this situation, the installer might not detect this condition, and the rest of the software will not function correctly.

The CB21AG intermediate driver must be installed manually. To install the intermediate driver manually, follow these steps:

Step 1 Insert the client adapter.

Step 2 Click on "Network Connections" in the Start > Settings menu in Windows XP, or right click on "My Network Places" in Windows 2000. Find the CB21AGg instance.

Step 3 Right click on the Cisco CB21AG instance, and left click on Properties.

Step 4 Choose the "Install" option and then add a new service.

Step 5 Choose the "Have disk" button. Go to \windows\system32 directory and choose wsimd.inf.

Step 6 Highlight and select "Wireless Intermediate Driver" and click "ok" button. The wireless IMD is bound to the adapter.

Step 7 Reboot system.

Installing a Microsoft Hot Fix for Group Policy Delay

If you want to use the Group Policy Delay parameter on the Profile Management (Security) window in ADU, you must install a Microsoft hot fix on computers running Windows 2000. The hot fix is incorporated into Windows XP Service Pack 2 and later.

The Group Policy Delay parameter enables you to specify 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. Follow the steps below to obtain and install the hot fix.

Note You must be a registered Cisco customer and log into Cisco.com in order to download the hot fix. If you are unable to access the hot fix from Cisco.com, contact Microsoft Support to obtain it. The Windows 2000 support page provides the contact information:
http://support.microsoft.com/default.aspx?scid=fh;EN-US;win2000

Step 1 Use your computer's web browser to access the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/aironet_hotfix

Step 2 If prompted, enter your Cisco Connection Online (CCO) username and password, and click **OK**.

Note To create a CCO username and password, visit http://www.cisco.com.

Step 3 Click the hot fix file (userenv.zip).

Step 4 Complete the encryption authorization form and click **Submit**.

Step 5 Click the file again to download it.

Step 6 Save the file to your computer's hard drive.

Step 7 Find the file using Windows Explorer, double-click it, and extract its files to a folder.

Step 8 Reboot your computer and press **F8** while your computer is booting.

Step 9 When the boot menu appears, select **Safe Mode with Command Prompt**.

Note You must complete this procedure in safe mode; otherwise, system file protection (SFP) will silently restore the original version of the file you are replacing.

Step 10 Copy the hot fix file (userenv.dll) to %systemroot%\System32 and overwrite the existing version of this file.

Step 11 Delete the copy of userenv.dll in %systemroot%\System32\DllCache.

Step 12 Reboot your computer.

Using the Profile Manager

This chapter explains how to use the ADU profile manager feature to create and manage profiles for your client adapter.

The following topics are covered in this chapter:

Overview of Profile Manager

The ADU profile manager feature enables you to create and manage up to 16 *profiles* (saved configurations) for your client adapter. These profiles enable you to use your client adapter in different locations, each of which requires different configuration settings. For example, you may want to set up profiles for using your client adapter at the office, at home, and in public areas such as airports. After the profiles are created, you can easily switch between them without having to reconfigure your client adapter each time you enter a new location.

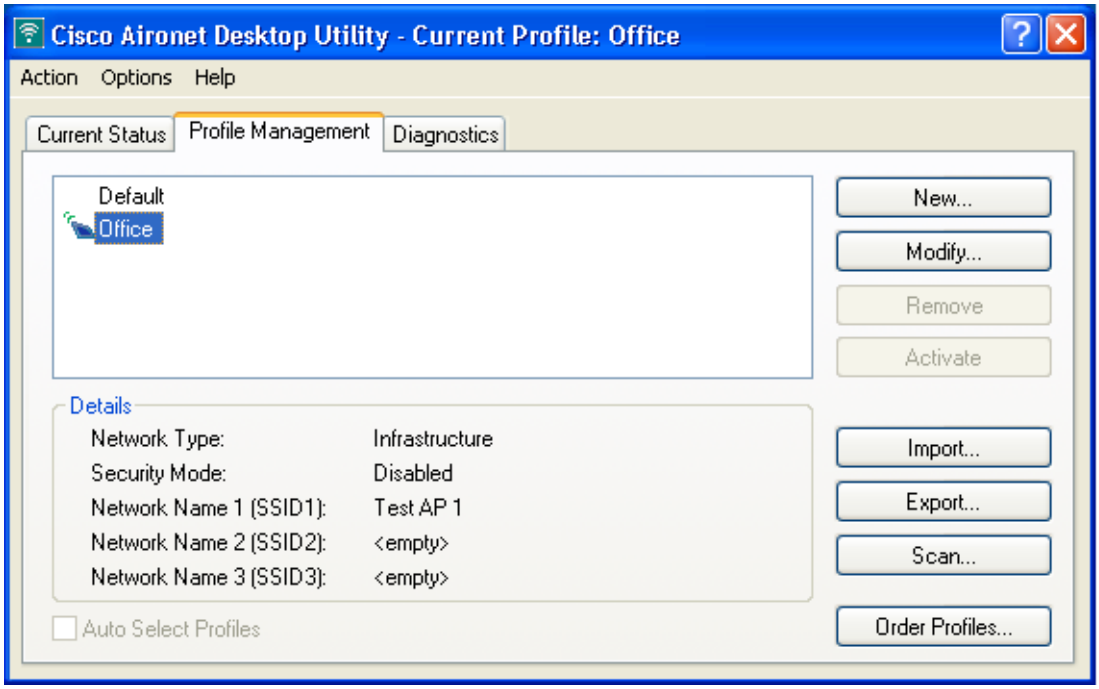
Profiles are stored in the registry and are lost if you uninstall the client adapter's software. To prevent your profiles from becoming lost, Cisco recommends that you back up your profiles using the profile manager's import/export feature. See the "Importing and Exporting Profiles" section on page 4-11 for details.

Opening Profile Manager

Step 1 To open the ADU profile manager, double-click the **Aironet Desktop Utility** icon on your desktop.

Step 2 Click the **Profile Management** tab. The Cisco Aironet Desktop Utility (Profile Management) window appears (see Figure 4-1).

Figure 4-1 Cisco Aironet Desktop Utility (Profile Management) Window



Note The profile manager feature provides you with a default profile that is configured to use default values. This profile is named *Default* and appears in the profiles list on the Cisco Aironet Desktop Utility (Profile Management) window. You can use this profile as is by double-clicking it or modify it by following the instructions in the "Modifying a Profile" section on page 4-11.

Table 4-1 provides a description of the status fields on the Cisco Aironet Desktop Utility (Profile Management) window.

Table 4-1 Description of Status Fields on Profile Management Window

Field	Description
Network Type	The type of network that is configured for the selected profile. **Value:** Infrastructure or Ad Hoc **Note** Refer to the Network Type parameter in Table 5-3 for instructions on setting the network type.
Security Mode	The type of security that is configured for the selected profile. **Value:** None, Pre-Shared Key, WPA/WPA2 Passphrase, LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), PEAP (EAP-MSCHAP V2), or Host Based EAP **Note** Refer to Chapter 5 for instructions on setting client adapter security.
Network Name 1 (SSID1)	The service set identifier (SSID) is the wireless network that is configured for the selected profile. **Note** Refer to the SSID1 parameter in Table 5-2 for instructions on setting SSID1.
Network Name 2 (SSID2)	An optional SSID that is configured for the selected profile. It identifies a second distinct network and enables the client adapter to connect and/or roam to that network without having to be reconfigured. **Note** Refer to the SSID2 parameter in Table 5-2 for instructions on setting SSID2.
Network Name 3 (SSID3)	An optional SSID that is configured for the selected profile. It identifies a third distinct network and enables the client adapter to connect and/or roam to that network without having to be reconfigured. **Note** Refer to the SSID3 parameter in Table 5-2 for instructions on setting SSID3.

Profile manager enables you to perform the following tasks related to the management of profiles:

- Create a new profile, page 4-4
- Include a profile in auto profile selection, page 4-8
- Select the active profile, page 4-10
- Edit a profile, page 4-11
- Delete a profile, page 4-11
- Import a profile, page 4-12
- Export a profile, page 4-12

Follow the instructions on the page indicated for the task you want to perform.

Note If your system administrator used an administrative tool to deactivate certain parameters, these parameters are disabled and cannot be selected.

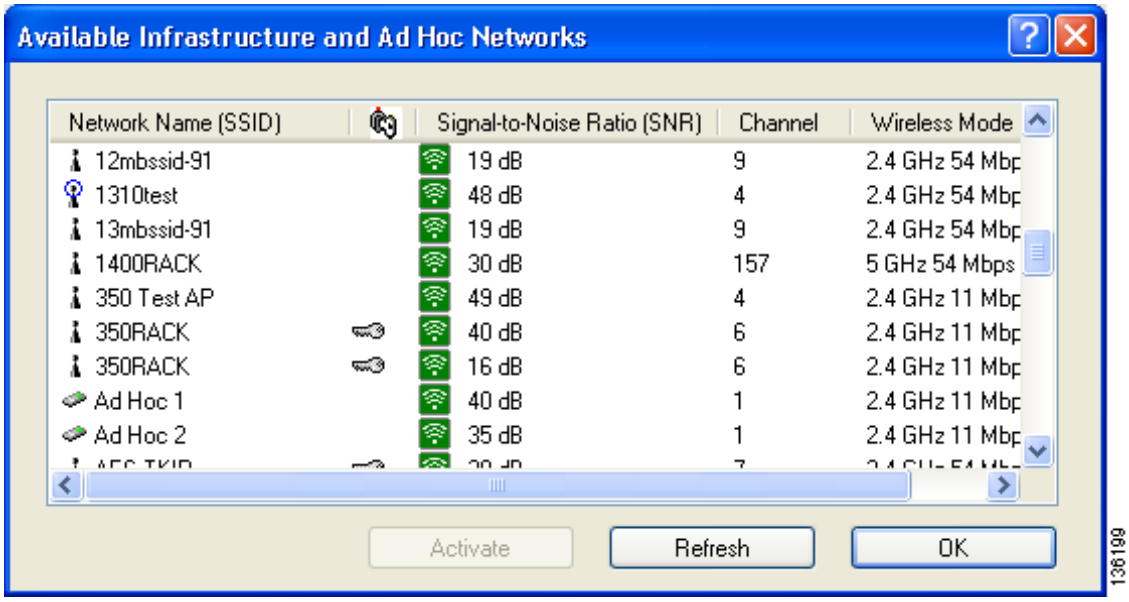
Creating a New Profile

Follow the steps below to create a new profile.

Step 1 Perform one of the following:

- If you want to create a new profile from scratch, click **New** on the Cisco Aironet Desktop Utility (Profile Management) window. Then go to Step 4.
- If you want to find an available network and create a profile based on it, click **Scan** on the Cisco Aironet Desktop Utility (Profile Management) window. The Available Infrastructure and Ad Hoc Networks window appears (see Figure 4-2).

Figure 4-2 Available Infrastructure and Ad Hoc Networks Window

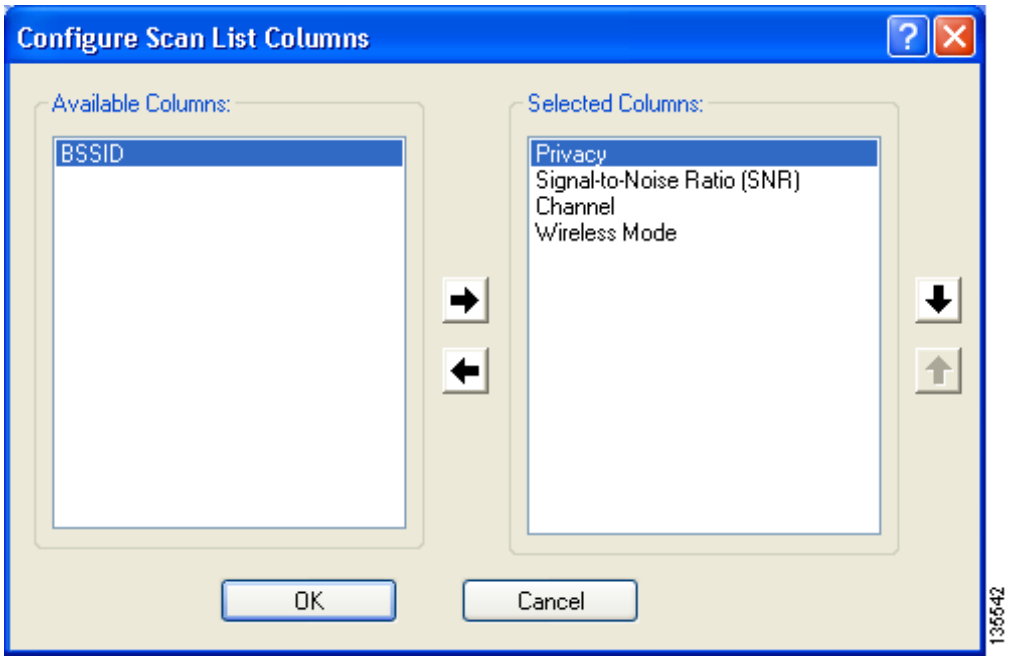


This window displays a list of all available networks. Click the **Refresh** button when you want to refresh the window and update the list of available networks.

Note The SSID of a Cisco IOS access point appears in the list of available networks only if a Guest Mode SSID is enabled or the Broadcast SSID in Beacon option is selected. Refer to the software configuration guide for your access point for additional information.

Table 4-2 provides a description of the default fields on the Available Infrastructure and Ad Hoc Networks window. If you want to be able to view additional fields, choose **Scan List Settings** from the Options drop-down menu. The Configure Scan List Columns window appears (see Figure 4-3).

Figure 4-3 Configure Scan List Columns Window



All of the fields that can be displayed on the Available Infrastructure and Ad Hoc Networks window appear in the Available Columns box. Highlight the fields that you want to be displayed and click the **right arrow** to move those fields to the Selected Columns box. You can use the **left arrow** to move any undesired fields from the Selected Columns box to the Available Columns box and the **up** and **down arrows** to change the order in which the fields are presented on the Available Infrastructure and Ad Hoc Networks window. Click **OK** to save your changes.

Table 4-2 Description of Fields on Available Infrastructure and Ad Hoc Networks Window

Field	Description	
Network Name (SSID)	The service set identifier (SSID) indicates the name of an available wireless network. The icons to the left of the SSIDs provide information on network type and link status.	
	Icon	**Description**
		An available infrastructure network.
		The infrastructure network to which your client adapter is currently associated.
		An available ad hoc network.
		The ad hoc network to which your client adapter is currently associated.

Table 4-2 Description of Fields on Available Infrastructure and Ad Hoc Networks Window

Field	Description
Key icon 	SSIDs that are designated with a key icon are being advertised as secure networks.
Signal-to-Noise Ratio (SNR)	The difference between the signal strength and the current noise level. The higher the value, the better the client adapter's ability to communicate with the access point. **Note** The color of this parameter's icon provides a visual interpretation of the signal-to-noise ratio: Excellent or Good (green), Fair (yellow), Poor (red). **Note** The signal-to-noise ratio is displayed either in decibels (dB) or as a percentage (%), depending on the value selected for the Signal Strength Display Units parameter on the Display Settings window. See the "Setting Parameters that Affect ADU Status and Statistics Tools" section on page 7-2 for more information.
Channel	The channel that the access point (in infrastructure mode) or the other client (in ad hoc mode) is using for communications.
Wireless Mode	The frequency and rate at which the access point (in infrastructure mode) or the other client (in ad hoc mode) is configured to transmit and receive packets.
BSSID	The basic service set identifier (BSSID) is the MAC address of the access point.

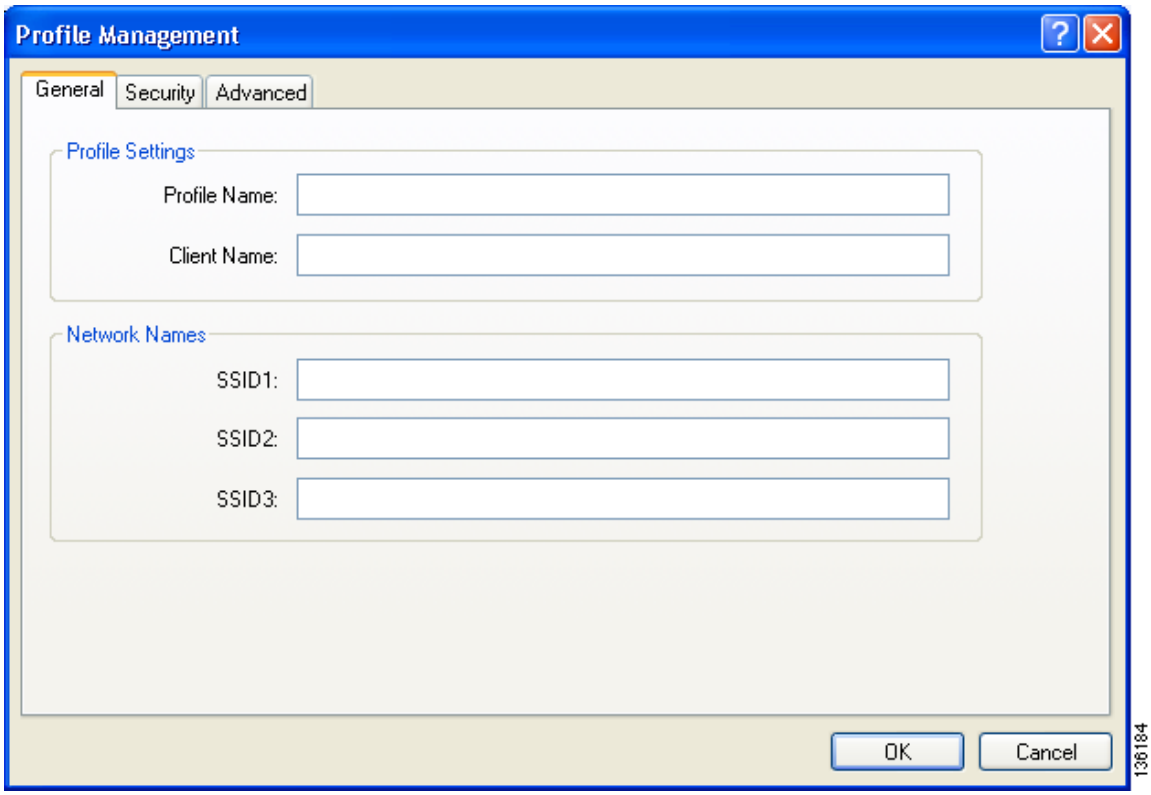
Step 2 Scroll down to see the full list of available networks.

Step 3 Click the SSID of the network to which you want your client adapter to associate and click **Activate**.

Note If the SSID is blank, you cannot activate the network.

Step 4 When the Profile Management (General) window appears (see Figure 4-4), enter a name for your new profile (such as *Office*, *Home*, etc.) in the Profile Name field.

Figure 4-4 Profile Management (General) Window



Note If you are creating a profile after scanning for an available network, the SSID of the network appears in the SSID1 field.

Step 5 Perform one of the following:

- If you want this profile to use the default values, click **OK**. The profile is added to the profiles list on the Cisco Aironet Desktop Utility (Profile Management) window.
- If you want to change any of the configuration parameter settings, follow the instructions in Chapter 5. The profile is added to the profiles list on the Cisco Aironet Desktop Utility (Profile Management) window.

Note The profiles for PC-Cardbus cards are tied to the slot in which the card is inserted. Therefore, you must always insert your PC-Cardbus card into the same slot, create profiles for both slots, or export the profiles from one slot and import them for the other slot.

Step 6 Go to the "Including a Profile in Auto Profile Selection" section on page 4-8 to enable the profile to be selected automatically or go to the "Selecting the Active Profile" section on page 4-10 to activate the profile.

Including a Profile in Auto Profile Selection

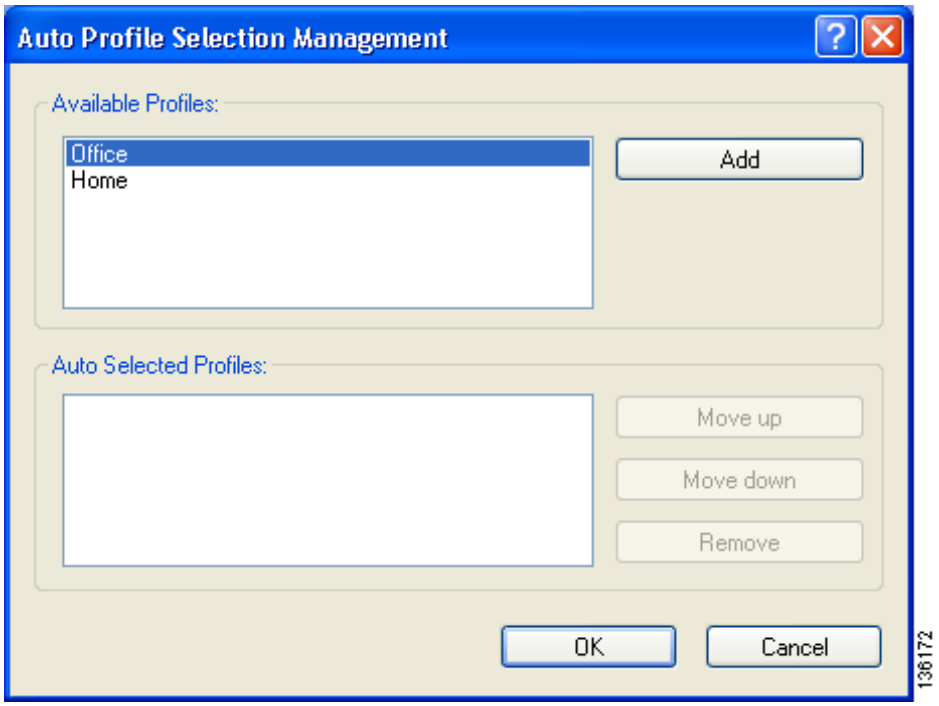
After you have created profiles for your client adapter, you can choose to include them in the profile manager's auto profile selection feature. Then when auto profile selection is enabled, the client adapter automatically selects a profile from the list of profiles that were included in auto profile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

Follow these steps to include any of your profiles in auto profile selection and to establish the order in which the profiles will be selected for use.

Step 1 Open ADU and click the **Profile Management** tab.

Step 2 Click **Order Profiles**. The Auto Profile Selection Management window appears (see Figure 4-5).

Figure 4-5 Auto Profile Selection Management Window



Step 3 The profiles that you created are listed in the Available Profiles box. Highlight each one that 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 A and Profile B both have "ABCD" as their SSID, only Profile A or Profile B (whichever was created first) appears in the Available Profiles box and can be included in auto profile selection.

Note To remove a profile from auto profile selection, select the profile in the Auto Selected Profiles box and click **Remove**. The profile is removed from the Auto Selected Profiles box.

Step 4 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-selectable profiles, select the profile that you want to move and click **Move up** or **Move down** to move the profile up or down, respectively.

Step 5 Click **OK** to save your changes.

When auto profile selection is enabled (see the "Selecting the Active Profile" section on page 4-10 for instructions), 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.

Note When you enable auto profile selection, the client adapter scans the wireless modes specified by all the profiles in the auto profile selection list for an available network. The client ignores the selected profile's wireless mode setting, which was configured on the ADU Profile Management (Advanced) window. Using this method, the client does not need to disassociate nor change the current profile while looking for networks in other profiles.

Step 6 Go to the "Selecting the Active Profile" section on page 4-10 to enable auto profile selection.

Selecting the Active Profile

Follow the steps below to specify the profile that the client adapter is to use.

Note You can use ASTU instead of the ADU Profile Manager to select the active profile. Refer to Chapter 8 for instructions.

Step 1 Open ADU and click the **Profile Management** tab. The Cisco Aironet Desktop Utility (Profile Management) window appears (see Figure 4-1).

Step 2 Perform one of the following:

- Select one profile for the client adapter to use either by double-clicking that profile in the profiles list or by clicking that profile in the profiles list and then clicking **Activate**.

  If the client adapter cannot *associate* (or establish a connection) to an access point (in infrastructure mode) or another client (in ad hoc mode) or loses association while using the selected profile, the adapter does not attempt to associate using another profile. To associate, you must select a different profile or enable auto profile selection.

- Enable auto profile selection by checking the **Auto Select Profiles** check box.

  This option causes the client adapter's driver to automatically select a profile from the list of profiles that were set up to be included in auto profile selection.

  If the client adapter loses association for more than 10 seconds (or for more than the time specified by the LEAP/EAP-FAST authentication timeout value on the LEAP/EAP-FAST Settings window if LEAP/EAP-FAST is enabled), the driver switches automatically to another profile that is included in auto profile selection. The adapter does not switch profiles as long as it remains associated or reassociates within 10 seconds (or within the time specified by the LEAP/EAP-FAST authentication timeout value). To force the client adapter to associate to a different access point (in infrastructure mode) or another client (in ad hoc mode), you must uncheck the **Auto Select Profiles** check box and select a new profile from the profiles list.

  Note This option is available only if two or more profiles are included in auto profile selection.

  Note Login scripts are not reliable if you use auto profile selection with LEAP or EAP-FAST. If you authenticate and achieve full network connectivity before or at the same time as you log into the computer, login scripts will run. However, if you authenticate and achieve full network connectivity after you log into the computer, login scripts will not run.

- Click **Scan**. The Available Infrastructure and Ad Hoc Networks window appears (see Figure 4-2). Double-click the SSID of a network that is used by one of your profiles and click **OK**.

The client adapter starts using a profile based on the option selected above. The active profile is designated by the following icon in the profiles list:

Modifying a Profile

Follow the steps in the appropriate section below to edit or delete an existing profile.

Editing a Profile

Step 1 Open ADU and click the **Profile Management** tab. The Cisco Aironet Desktop Utility (Profile Management) window appears (see Figure 4-1).

Step 2 In the profiles list, select the profile that you want to edit.

Step 3 Click **Modify**.

Step 4 Follow the instructions in Chapter 5 to change any of the configuration parameters for this profile.

Deleting a Profile

Step 1 Open ADU and click the **Profile Management** tab. The Cisco Aironet Desktop Utility (Profile Management) window appears (see Figure 4-1).

Step 2 In the profiles list, select the profile that you want to delete.

Note You cannot delete the active profile.

Step 3 Click **Remove**. The profile is deleted.

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 back up profiles before uninstalling client adapter software
- To export profiles for a PC-Cardbus card in one Cardbus slot and import them for use with a second Cardbus slot
- To set up your computer with a profile from another computer
- To export one of your profiles and use it to set up additional computers

Follow the instructions on the following pages to import or export profiles.

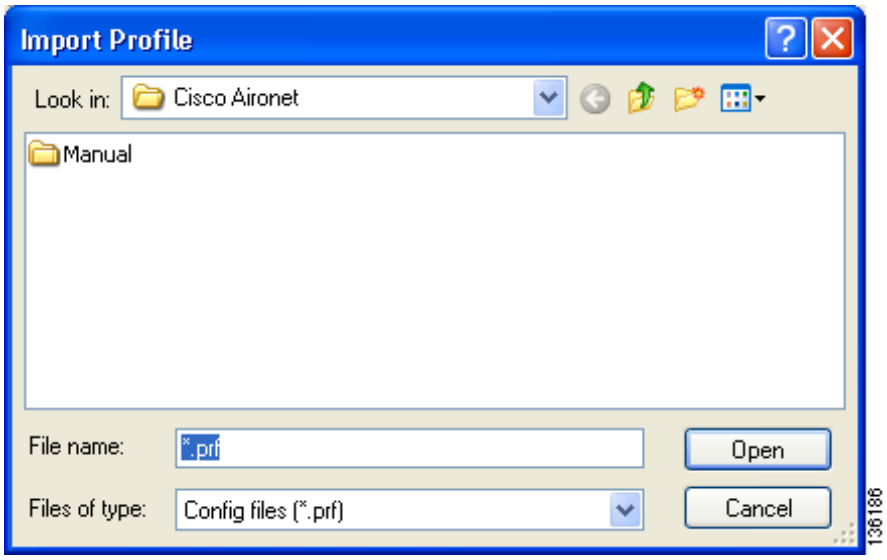
Importing a Profile

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

Step 2 Open ADU and click the **Profile Management** tab. The Cisco Aironet Desktop Utility (Profile Management) window appears (see Figure 4-1).

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

Figure 4-6 Import Profile Window



Step 4 In the Look in drop-down box, find the directory containing the profile.

Step 5 Select the profile that you want to import so it appears in the File name box at the bottom of the window.

Step 6 Click **Open**. The imported profile appears in the profiles list on the Cisco Aironet Desktop Utility (Profile Management) window.

Exporting a Profile

Note PACs are not exported with EAP-FAST profiles.

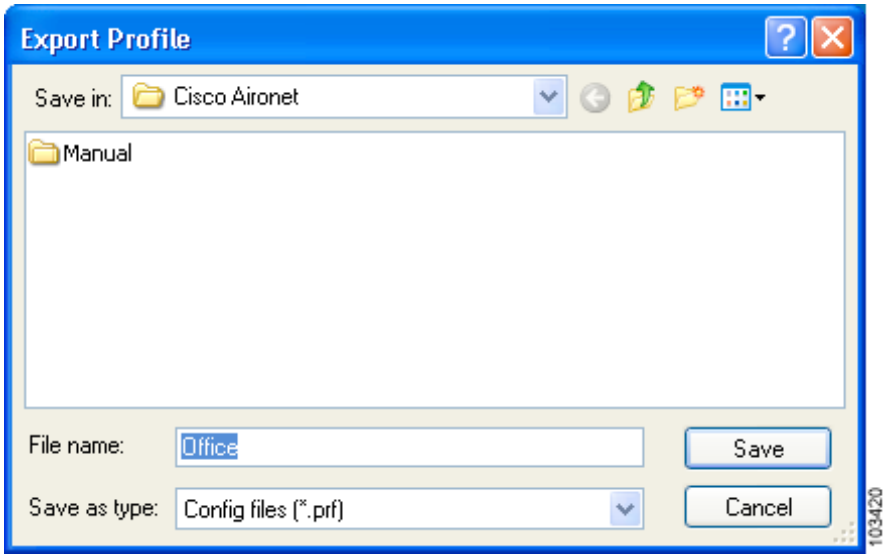
Step 1 Insert a blank floppy disk into your computer's floppy drive, if you wish to export a profile to a floppy disk.

Step 2 Open ADU and click the **Profile Management** tab. The Cisco Aironet Desktop Utility (Profile Management) window appears (see Figure 4-1).

Step 3 In the profiles list, select the profile that you want to export.

Step 4 Click **Export**. The Export Profile window appears (see Figure 4-7).

Figure 4-7 Export Profile Window



The profile name appears in the File name box.

Step 5 Choose a directory (such as your computer's floppy disk drive or a location on the network) from the Save in drop-down box.

Note The default location is the directory where ADU is installed (such as C:\Program Files\Cisco Aironet).

Step 6 Click **Save**. The profile is exported to the specified location.

Step 7 Follow the instructions in the "Importing a Profile" section to import the profile on another computer.

Configuring the Client Adapter

This chapter explains how to configure profile parameters. The following topics are covered in this chapter:

Overview

When you choose to create a new profile or modify an existing profile on the Cisco Aironet Desktop Utility (Profile Management) window, the Profile Management windows appear. These windows enable you to set the configuration parameters for that profile.

Note If you do not change any of the configuration parameters for a newly created profile, the default values are used.

Note If you are planning to set parameters on more than one of the Profile Management windows, wait until you are finished with all of the windows before clicking **OK**. When you click **OK**, you are returned to the Cisco Aironet Desktop Utility (Profile Management) window.

Each of the Profile Management 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 Management window's parameters.

Table 5-1 Locating Configuration Instructions

Parameter Category	Page Number
General	5-3
Advanced	5-6
Security	5-14

Note If your system administrator used an administrative tool to deactivate certain parameters, these parameters are disabled on the Profile Management windows and cannot be selected.

Note You can also set two roaming parameters for your client adapter outside of ADU using the Windows Control Panel. Refer to the "Setting Roaming Parameters in the Windows Control Panel" on page 5-63 for details.

Setting General Parameters

The Profile Management (General) window (see Figure 5-1) enables you to set parameters that prepare the client adapter for use in a wireless network. This window appears after you click **New** or **Modify** on the Cisco Aironet Desktop Utility (Profile Management) window.

Figure 5-1 Profile Management (General) Window

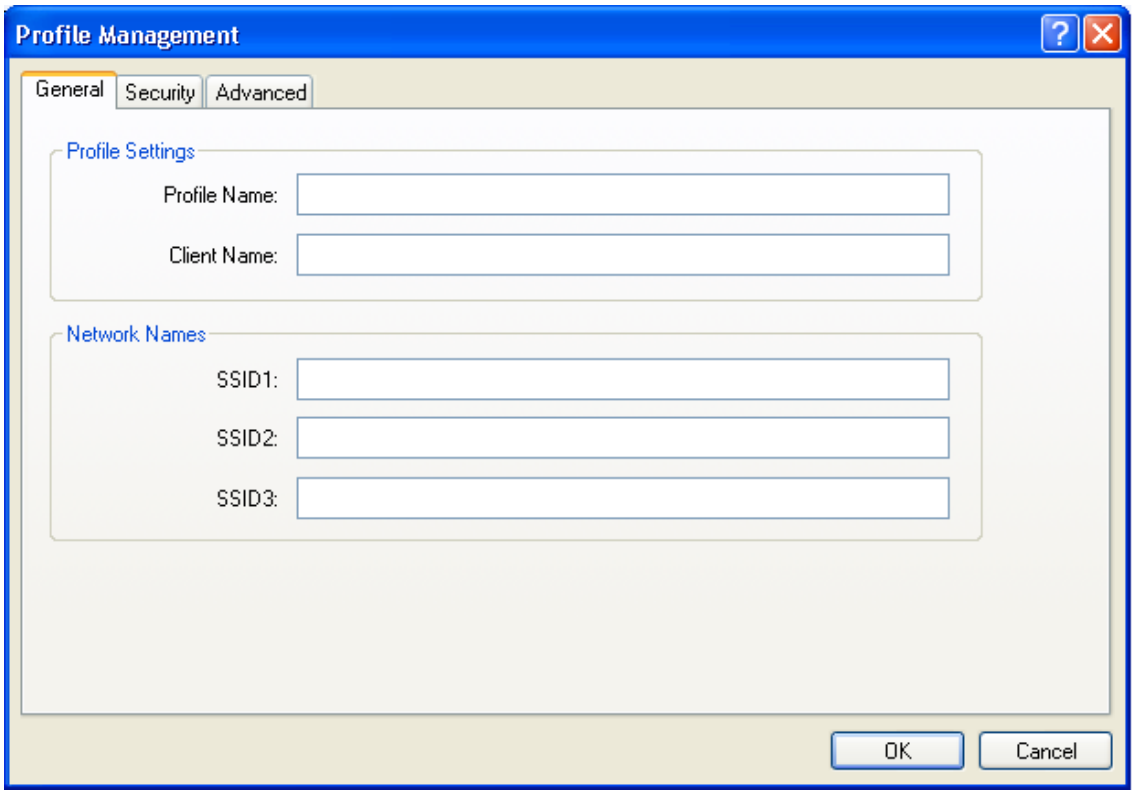


Table 5-2 lists and describes the client adapter's general parameters. Follow the instructions in the table to change any parameters.

Table 5-2 Profile Management General Parameters

Parameter	Description
Profile Name	The name assigned to the configuration profile. **Range:** You can key in up to 32 ASCII characters. **Default:** A blank field
Client Name	A logical name for your workstation. It enables an administrator to ascertain 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:** You can key in up to 16 ASCII characters. **Default:** The name of your computer **Note** Each computer on the network should have a unique client name.
SSID1	The service set identifier (SSID) identifies the specific wireless network that you want the client adapter to access. **Range:** You can key in up to 32 ASCII characters (case sensitive). **Default:** A blank field **Note** If you leave this parameter blank, your client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs. 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** You must enter an SSID if this profile is configured for use in an ad hoc network.

Table 5-2 Profile Management General Parameters (continued)

Parameter	Description
SSID2	An optional SSID that identifies a second distinct network and enables the client adapter to roam to that network without having to be reconfigured. **Range:** You can key in 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 or used with WPA/WPA2 passphrase. **Note** This field is unavailable for any profiles that are included in auto profile selection or configured for use in an ad hoc network.
SSID3	An optional SSID that identifies a third distinct network and enables the client adapter to roam to that network without having to be reconfigured. **Range:** You can key in 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 or used with WPA/WPA2 passphrase. **Note** This field is unavailable for any profiles that are included in auto profile selection or configured for use in an ad hoc network.

Go to the next section to set additional parameters, or click **OK** to save your changes and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Setting Advanced Parameters

The Profile Management (Advanced) window (see Figure 5-2) 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 Management window.

Figure 5-2 Profile Management (Advanced) Window

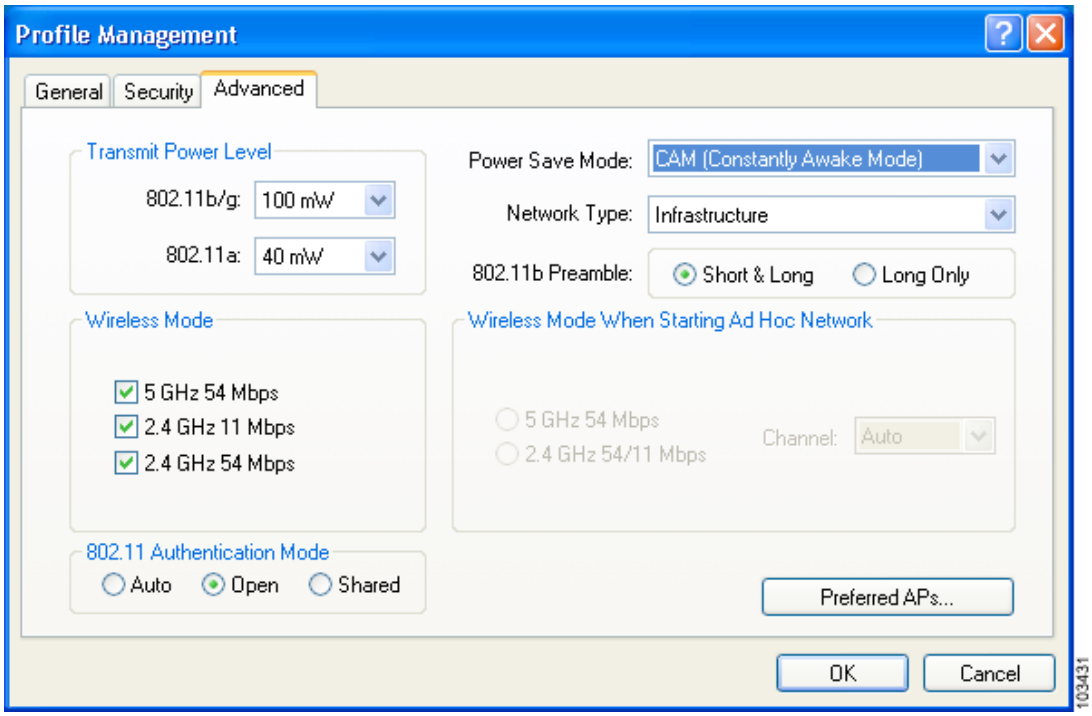


Table 5-3 lists and describes the client adapter's advanced parameters. Follow the instructions in the table to change any parameters.

Table 5-3 Profile Management 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 your client adapter transmits. Although the adapter supports up to 100 mW, the transmit power level that is 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>10, 20, 32, 50, 63, or 100 mW</td></tr>
<tr><td>802.11a</td><td>10, 13, 20, 25, or 40 mW</td></tr>
</table>
Note The client adapter's maximum transmit power level may be lower when operating in 802.11g mode than when operating in 802.11b mode due to 802.11g-specific regulatory limitations in some countries.

Note Reducing the transmit power level conserves battery power but decreases radio range.

Note If configured to control the client power level, access points can limit the maximum power of the client.</td></tr>
</table>

Table 5-3 Profile Management Advanced Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Power Save Mode</td><td>Sets your 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.</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.</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).</td></tr>
<tr><td colspan="2">Note If this profile is configured for use in an ad hoc network, CAM mode is used automatically.</td></tr>
</table>
</td></tr>
</table>

Table 5-3 Profile Management 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 your 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 your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point. For example, an ad hoc network could be set up between computers in a conference room so that users can share information in a meeting.</td></tr><tr><td>Infrastructure</td><td>Indicates that your wireless network is connected to a wired Ethernet network through an access point.</td></tr></table></td></tr>
<tr><td>802.11b Preamble</td><td>Determines whether your client adapter uses 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 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 Profile Management Advanced Parameters (continued)

Parameter	Description
Wireless Mode	Specifies the frequency and rate at which your 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** Your client adapter's wireless mode must match that of the access points with which it is to communicate. Otherwise, your client adapter may not be able to associate to them.
Wireless Mode When Starting Ad Hoc Network	Specifies the frequency and rate at which your 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** Your client adapter's wireless mode must match that of the other clients with which it is to communicate. Otherwise, your 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 Profile Management Advanced Parameters (continued)

Parameter	Description
Channel	Specifies the channel that your 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 D for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.

Table 5-3 Profile Management Advanced Parameters (continued)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>802.11 Authentication Mode</td><td>Specifies how your client adapter attempts to authenticate to an access point. Open and shared authentication do not rely on a RADIUS server on your 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 your 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 your client adapter to authenticate and communicate only with access points that have the same WEP key.

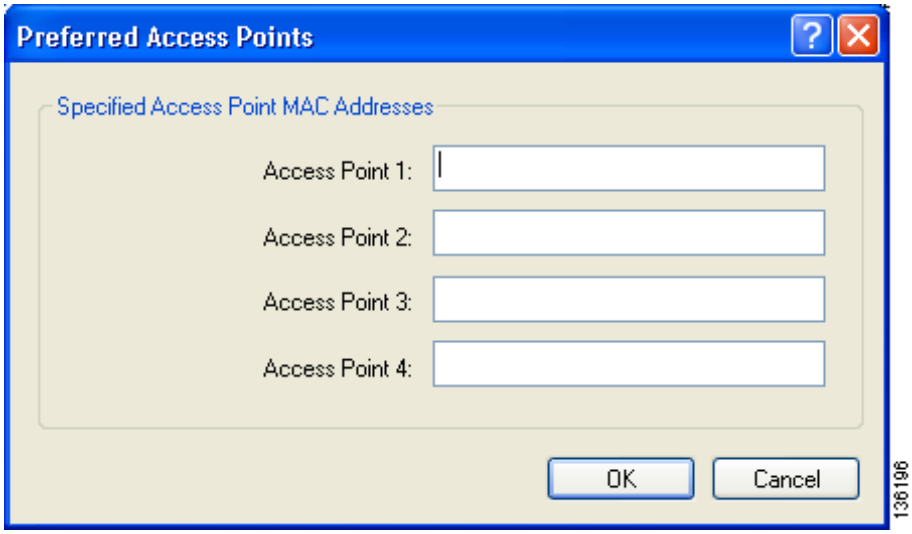
During shared key authentication, the access point sends an unencrypted challenge packet to the client adapter, which encrypts the packet and sends it back to the access point. The access point attempts to decrypt the encrypted packet and sends an authentication response packet indicating the success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

Note Your client adapter’s 802.11 authentication mode setting must match that of the access points with which it is to communicate, or be set to auto. Otherwise, your client adapter may not be able to authenticate to them.

Note If this profile is configured for use in an ad hoc 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 5-3).

Figure 5-3 Preferred Access Points Window



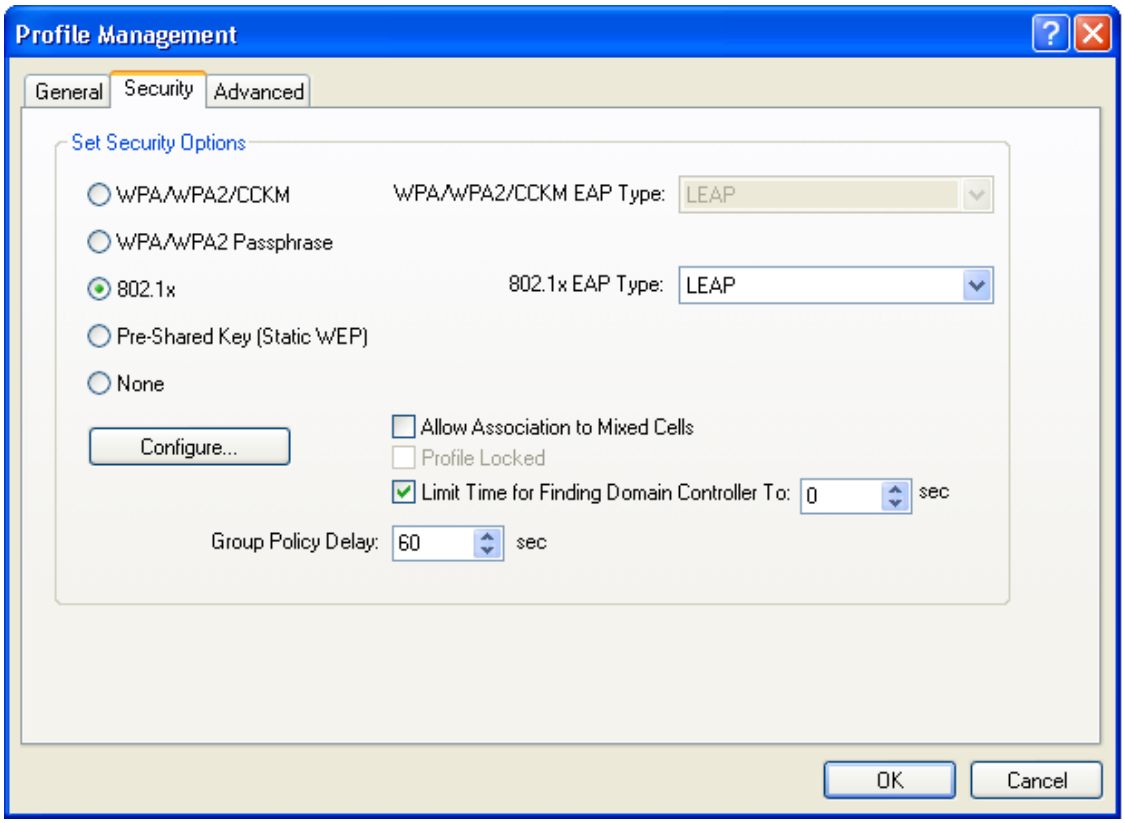
Leave the Access Point 1 through Access Point 4 fields blank or enter the MAC addresses of up to four preferred access points to which the client adapter can associate; then click **OK**. (The MAC address should consist of 12 hexadecimal characters.) If the specified access points are not found or the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

Go to the next section to set additional parameters or click **OK** to save your changes and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Setting Security Parameters

The Profile Management (Security) window (see Figure 5-4) 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 access this window, click the **Security** tab from any Profile Management window.

Figure 5-4 Profile Management (Security) Window



This window is different from the other Profile Management 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.

Note If your system administrator used an administrative tool to lock this profile, the **Profile Locked** check box is checked. Locked profiles cannot be modified (with the exception of password fields), written over, or removed.

Overview of Security Features

You can protect your data as it is transmitted through your 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 your 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 you want 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" on page 5-21 for information on three security features that can make your WEP keys even more secure.

Static WEP Keys

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

You do 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 Define Pre-Shared Keys 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" on page 5-26 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 ADU 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. ADU 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 you configure your adapter to use 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 credential (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.

  ADU 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 you configure your adapter to use saved EAP-FAST credentials.

  PACs are created by Cisco Secure ACS and are identified by an ID. The user obtains his or her own copy of the PAC from the server, and the ID links the PAC to the profile created in ADU. 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 you uninstall the client adapter software.
  - 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.

Note PACs that are created by ACS version 3.x.xx are not compatible with ACS version 4.0.xx. Client stations must import new PACs. If you select auto-provisioning, new PACs will automatically be generated and used. However, if you select manual provisioning, you must manually export new PACs to the client stations. If a user wants to authenticate to ACS version 4.0.xx and version 3.x.xx at different times, both PACs must remain on the client station. The ADU is capable of automatically selecting the appropriate PAC. However, if you experiences authentication failures after upgrading the software, delete all the PACs provisioned from the 3.x.xx server.

- **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 your network uses an OTP user database, PEAP (EAP-GTC) requires you to enter a hardware or software token password to start the EAP authentication process and gain access to the network. If your network uses a Windows NT or 2000 domain user database or an LDAP user database (such as NDS), PEAP (EAP-GTC) requires you to enter your 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 you configure your access point as indicated in Table 5-4 on page 5-22 and configure your client adapter 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 5-29
- EAP-FAST, page 5-34
- EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2), page 5-44

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/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ab.html

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 5-28
- LEAP with WPA/WPA2, page 5-29
- EAP-FAST with WPA/WPA2, page 5-34
- EAP-TLS with WPA/WPA2, page 5-45
- PEAP (EAP-GTC) with WPA/WPA2, page 5-48
- PEAP (EAP-MSCHAP V2) with WPA/WPA2, page 5-52

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 Management (Security) window, 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 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, must be disabled in order for CCKM fast secure roaming to operate correctly. If your computer is running Windows XP and you chose to configure your client adapter using ADU during installation, these features should already be disabled. Similarly, if your computer is running Windows 2000, the Microsoft 802.1X supplicant, if installed, should already be disabled. Refer to Chapter 10 if you need additional information.

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)
- 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)

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.

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

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.

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 your 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 your 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
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.

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

Security Feature	Client Setting	Access Point Setting
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.
EAP-TLS authentication		
If using ADU to configure card	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
If using Windows XP to configure card	Choose Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP Type	Set up and enable WEP and enable Open with EAP Authentication for the SSID
EAP-TLS authentication with WPA or WPA2		
If using ADU to configure card	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.

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

Security Feature	Client Setting	Access Point Setting
If using Windows XP to configure card	Enable WPA and choose Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP Type **Note** WPA2 is not yet available in the Microsoft Wireless Configuration Manager in Windows XP.	For WPA, choose a cipher suite that includes TKIP; 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		
If using ADU to configure card	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
If using Windows XP to configure card	Choose Enable network access control using IEEE 802.1X and PEAP as the EAP Type	Set up and enable WEP and enable Open with EAP Authentication for the SSID
PEAP authentication with WPA or WPA2		
If using ADU to configure card	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.
If using Windows XP to configure card	Enable WPA and choose Enable network access control using IEEE 802.1X and PEAP as the EAP Type **Note** WPA2 is not yet available in the Microsoft Wireless Configuration Manager in Windows XP.	For WPA, choose a cipher suite that includes TKIP; 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 your 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 5-20.
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)

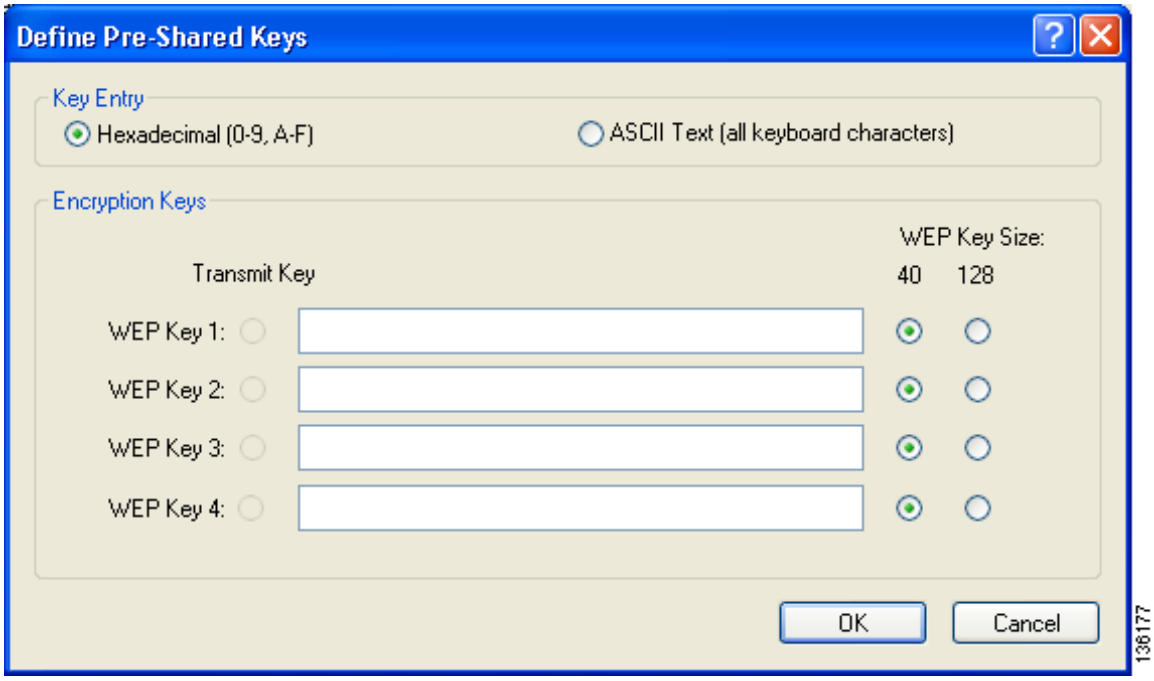
Enabling Static WEP

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

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

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

Figure 5-5 Define Pre-Shared Keys 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 you are planning to use your client adapter with these access points.

Step 4 For the static WEP key that you are entering (1, 2, 3, or 4), choose a WEP key size of 40 or 128 on the right side of the window. 21AG client adapters can use 40- or 128-bit keys.

Step 5 Obtain the static WEP key from your system administrator and enter it in the blank field for the key you are creating. Follow the guidelines below to enter a new static WEP key:

- WEP keys must contain the following number of characters:
  - 10 hexadecimal characters or 5 ASCII text characters for 40-bit keys

    Example: 5A5A313859 (hexadecimal) or ZZ18Y (ASCII)
  - 26 hexadecimal characters or 13 ASCII text characters for 128-bit keys

    Example: 5A583135333554595549333534 (hexadecimal) or ZX1535TYUI354 (ASCII)

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

- Your client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.
- When setting more than one WEP key, the keys must be assigned to the same WEP key numbers for all devices. For example, WEP key 2 must be WEP key number 2 on all devices. When multiple WEP keys are set, they must be in the same order on all devices.

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 settings and return to the Profile Management (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 Cisco Aironet Desktop Utility (Profile Management) window.

Enabling WPA/WPA2 Passphrase

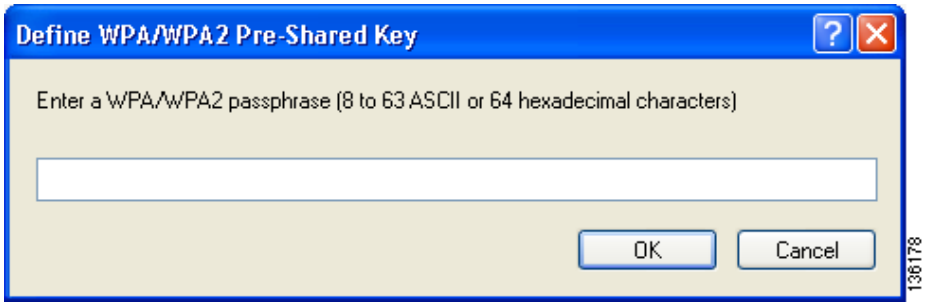
Follow the steps below to enable WPA/WPA2 passphrase (also known as *WPA/WPA2 pre-shared key*) for this profile.

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 Choose **WPA/WPA2 Passphrase** on the Profile Management (Security) window.

Step 2 Click **Configure**. The Define WPA/WPA2 Pre-Shared Key window appears (see Figure 5-6).

Figure 5-6 Define WPA/WPA2 Pre-Shared Key Window



Step 3 Obtain the WPA/WPA2 passphrase for the access point (in an infrastructure network) or other clients (in an ad hoc network) from your system administrator and enter it 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.
- Your client adapter's WPA/WPA2 passphrase must match the passphrase used by the access point with which you are planning to communicate.

Step 4 Click **OK** to save the passphrase and return to the Profile Management (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 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. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" on page 3-21 for information on obtaining and installing the hot fix.

Step 6 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Enabling LEAP

Before you can enable LEAP 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 (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), 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(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 5-22.

- All necessary infrastructure devices (such as 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 Management (Security) window:

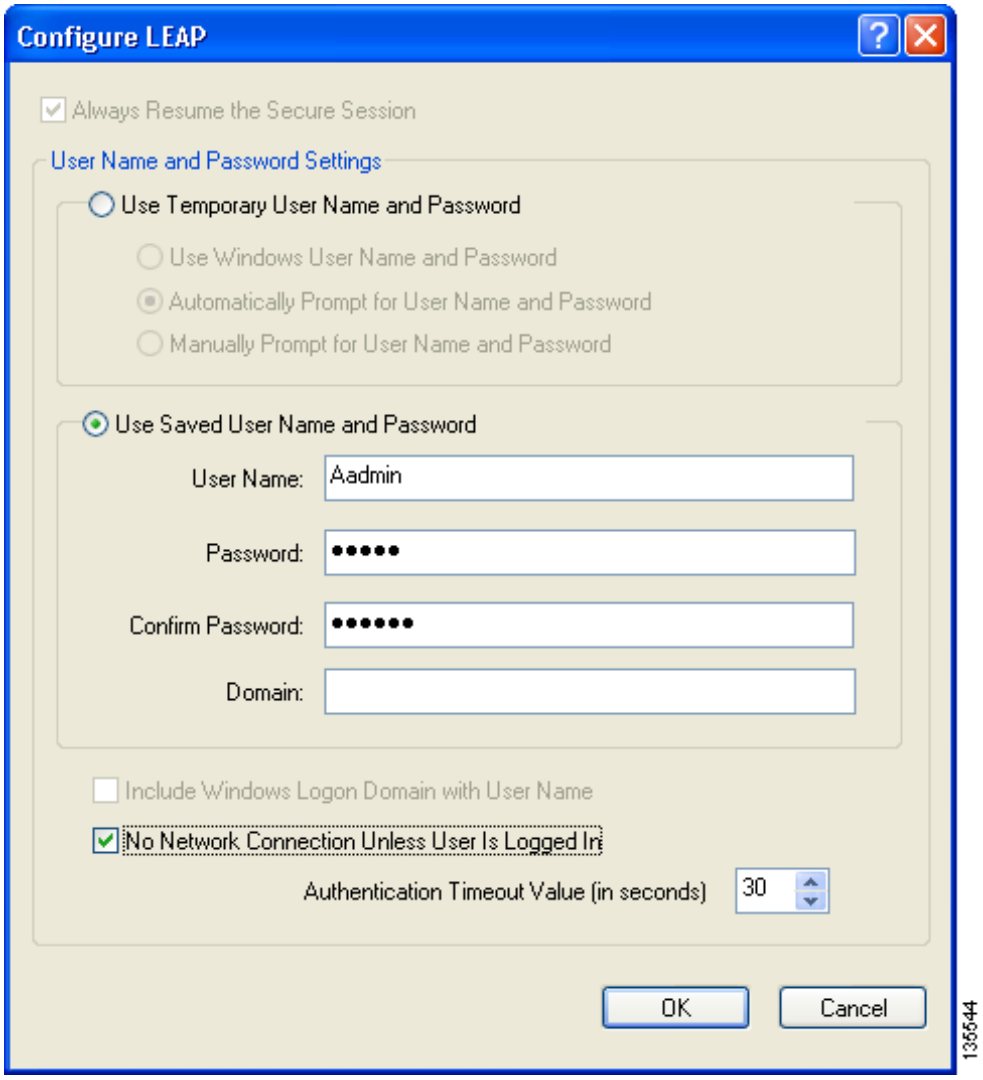
- If you want to enable LEAP without WPA or WPA2, choose **802.1x** under Set Security Options and **LEAP** in the 802.1x EAP Type drop-down box.
- If you want to enable LEAP with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **LEAP** in the WPA/WPA2/CCKM EAP Type drop-down box.

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 your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" on page 5-19 for additional information.

Step 2 Click **Configure**. The Configure LEAP window appears (see Figure 5-7).

Figure 5-7 Configure LEAP Window



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

- **Use Temporary User Name and Password**—Requires you to enter the LEAP 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**.
- **Use Saved User Name and Password**—Does not require you 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 chose Use Temporary User Name and Password in Step 3, choose one of the following options:
  - **Use Windows User Name and Password—**Causes your Windows username and password to also serve as your LEAP username and password, giving you only one set of credentials to remember. After you log in, the LEAP authentication process begins automatically. This option is the default setting.
  - **Automatically Prompt for User Name and Password**—Requires you to enter a separate LEAP username and password (which are registered with the RADIUS server) in addition to your regular Windows login in order to start the LEAP authentication process.
  - **Manually Prompt for User Name and Password**—Requires you to manually invoke the LEAP authentication process as needed using the Manual Login option in the Action drop-down menu or ASTU. You are not prompted to enter a LEAP username and password during the Windows login. This option might be used to support a software token one-time password system or other systems that require additional software that is not available at login.
- 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 will be passed to the RADIUS server along with your 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 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 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 to be prompted to re-enter your LEAP username and password whenever your client adapter temporarily loses association by roaming out of range or wakes up from suspend or hibernate mode.

Note Checking this check box gives you the convenience of not having to re-enter your username and password when your client adapter experiences momentary losses of association. However, if you leave your 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 your 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 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, the **Include Windows Logon Domain with User Name** check box is grayed out and the saved domain name is passed to the RADIUS server.

Step 7 If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, check the **No Network Connection 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 settings and return to the Profile Management (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 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 LEAP 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 time out in just 15 seconds.

Note The finding domain controller timeout value can never extend the authentication process beyond the LEAP authentication timeout value, even if the finding domain controller timeout value is greater than the LEAP 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 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 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. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" on page 3-21 for information on obtaining and installing the hot fix.

Step 13 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Step 14 Refer to Chapter 6 for instructions on authenticating using LEAP.

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 5-20.

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:

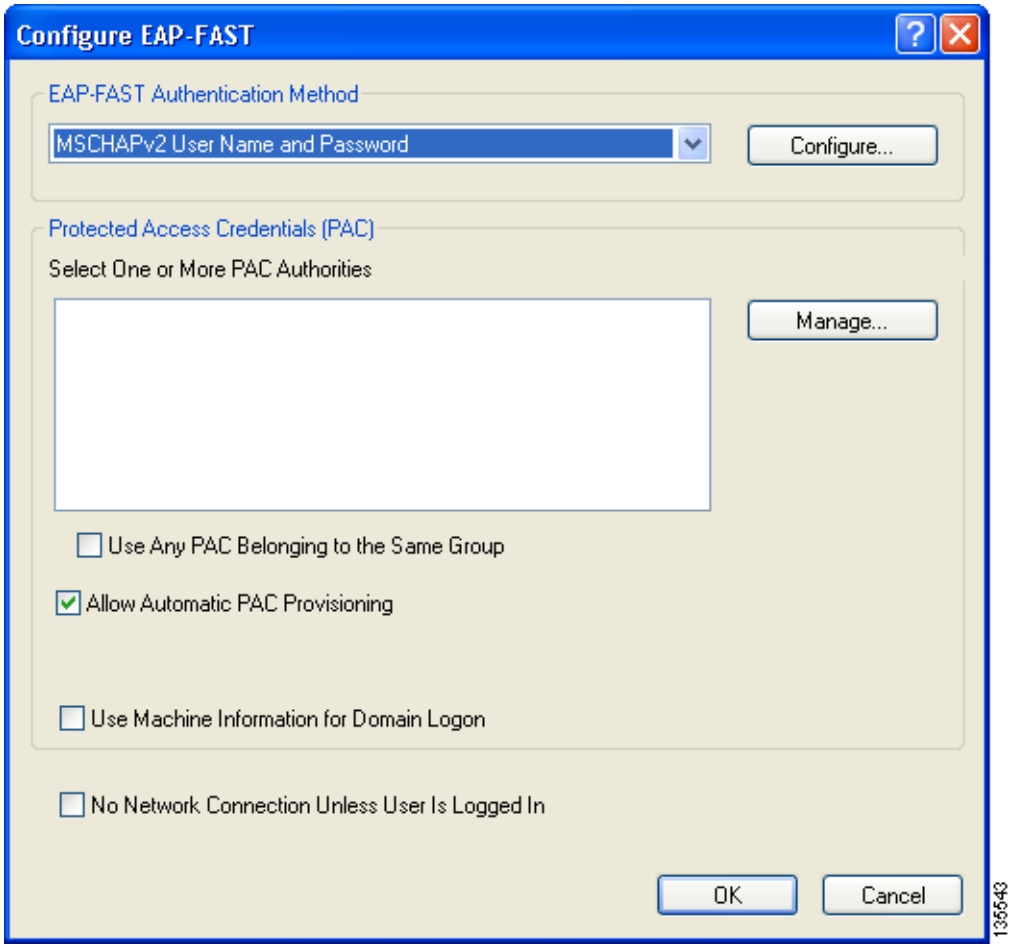
- If you want to enable EAP-FAST without WPA or WPA2, choose **802.1x** under Set Security Options and **EAP-FAST** in the 802.1x EAP Type drop-down box.
- If you want to enable EAP-FAST with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **EAP-FAST** in the WPA/WPA2/CCKM EAP Type 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" on page 5-19 for additional information.

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

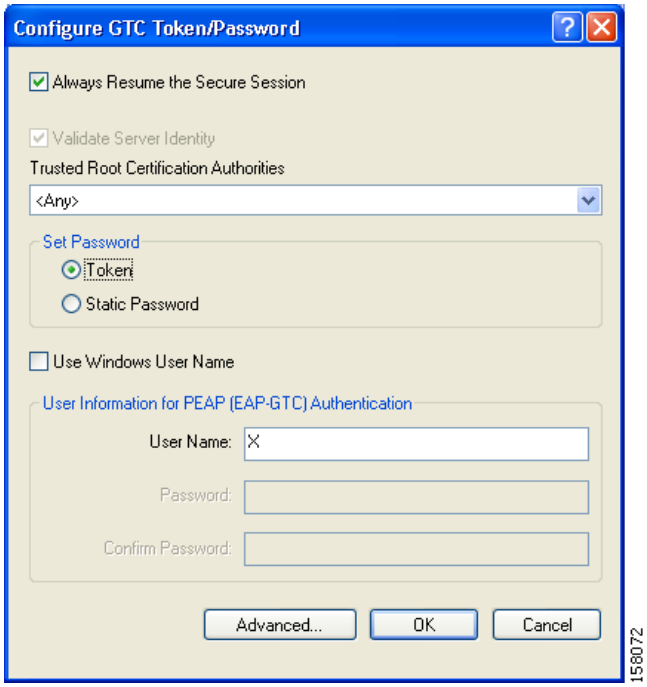
Figure 5-8 Configure EAP-FAST Window



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 5-9):

Figure 5-9 Configure GTC Token/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 Checking this check box gives you the convenience of not having to re-enter your username and password 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**.

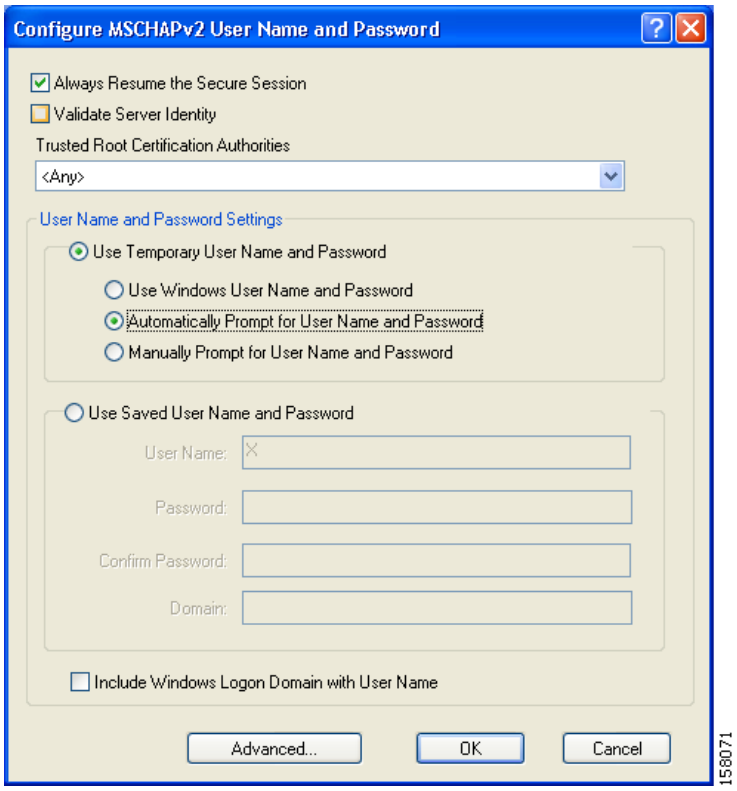
2. Check the **Validate Server Identity** check box to force the system to validate the identity of the server as an added level of security.

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

3. To configure the remaining options in this window, refer to "Enabling PEAP (EAP-GTC)" on page 5-48.
4. 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 5-10):

Figure 5-10 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.

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:

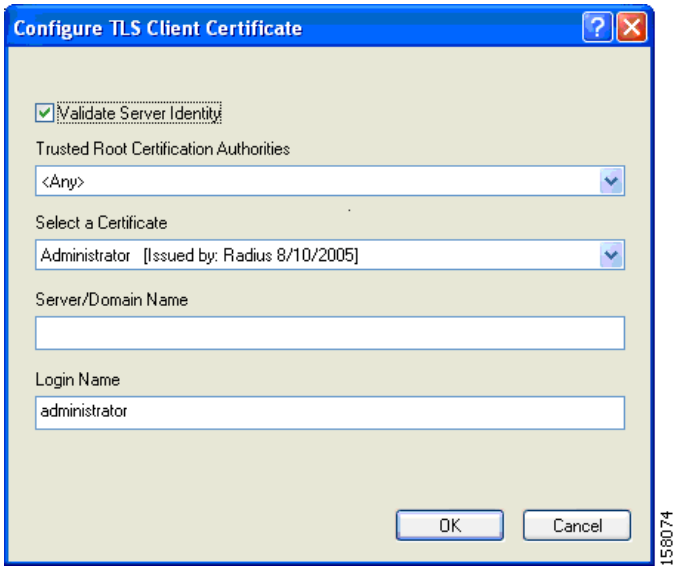
   a. Enter a username and password in the appropriate fields.
   b. Re-enter the password in the Confirm Password field.
   c. If you wish to specify a domain name that will be passed to the RADIUS server along with your username, enter it in the Domain field.
6. If you work in an environment with multiple 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.

7. To specify a server or domain name and a login name to use for authenticating user credentials, click **Advanced** and follow the instructions in "Configuring Advanced Settings" on page 5-58.
8. Click **OK** to save your settings and return to the Configure EAP-FAST window.

Step 6 If you chose **TLS Client Certificate** in Step 3, refer to "Enabling EAP-TLS" on page 5-45 (Step 5 to Step 10) to configure the options in the Configure TLS Client Certificate window (Figure 5-11).

Figure 5-11 Configure TLS Client Certificate Window



Step 7 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.

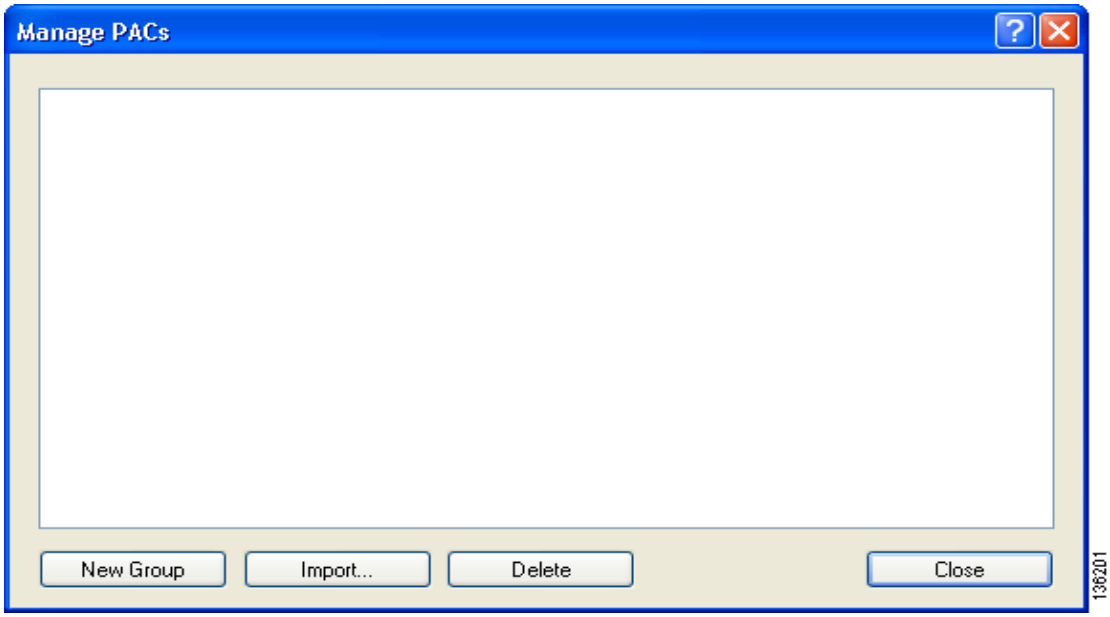
If the Select One or More PAC Authorities list is empty or does not contain the name of a desired PAC authority, go to Step 8 to import a PAC file.

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

a. Click **Manage**. The Manage PACs window appears (see Figure 5-12).

Figure 5-12 Manage PACs Window

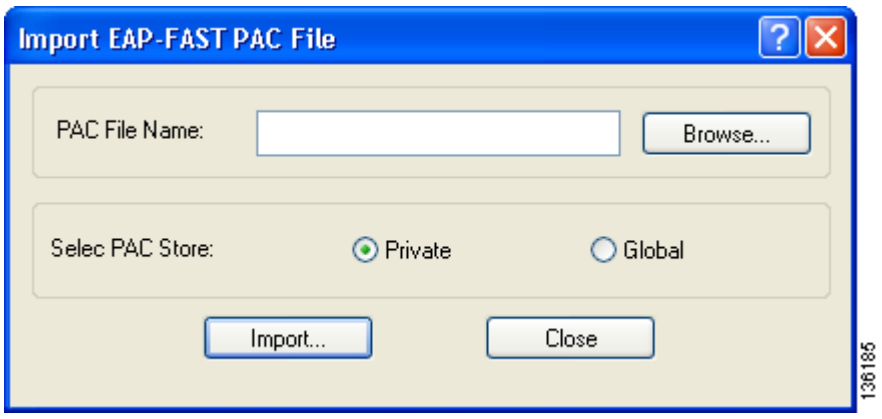


b. To create a new group, click **New Group**.

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 5-13).

Figure 5-13 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*.

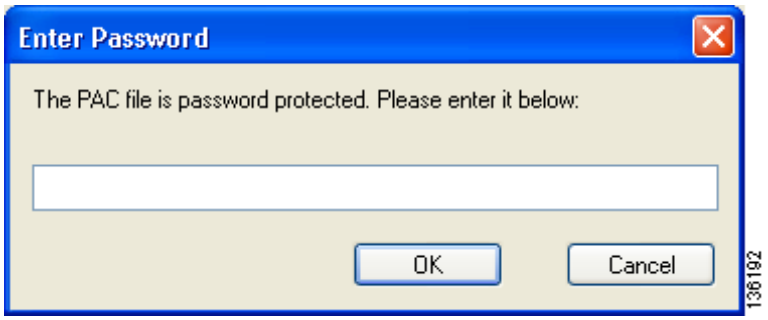
f. Choose one of these PAC store options to determine where the imported PAC file will be stored and to whom it will be accessible:

- **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 5-14), enter the PAC file password, which can be obtained from your system administrator, and click **OK**.

Figure 5-14 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 9 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 10 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 11 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 12 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 13 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 14 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 15 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 16 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. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" on page 3-21 for information on obtaining and installing the hot fix.

Step 17 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Step 18 Refer to Chapter 6 for instructions on authenticating using EAP-FAST.

Enabling EAP-TLS or PEAP

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

- You must have a valid Windows username and password, and the password cannot be blank.
- The appropriate certificates must be installed on your computer. EAP-TLS requires both a Certificate Authority (CA) certificate and a user certificate while PEAP requires only a CA certificate.

  Note Contact your system administrator if you need help obtaining and importing the necessary certificates.

- 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 your 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), 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(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, 5-45
- Enabling PEAP (EAP-GTC), 5-48
- Enabling PEAP (EAP-MSCHAP V2), 5-52
- Enabling PEAP (EAP-MSCHAP V2) machine authentication with machine certificates, 5-55

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 Management (Security) window:

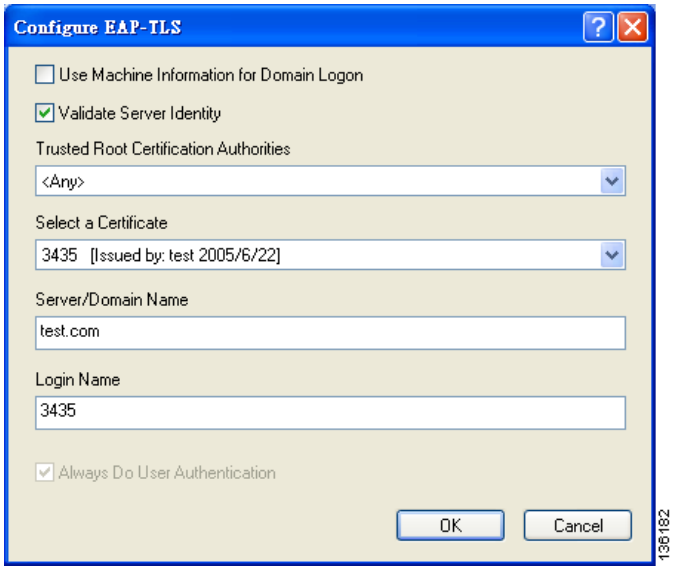
- If you want to enable EAP-TLS without WPA or WPA2, choose **802.1x** under Set Security Options and **EAP-TLS** in the 802.1x EAP Type drop-down box.
- If you want to enable EAP-TLS with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **EAP-TLS** in the WPA/WPA2/CCKM EAP Type drop-down 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 your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" on page 5-19 for additional information.

Step 2 Click **Configure**. The Configure EAP-TLS window appears (see Figure 5-15).

Figure 5-15 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 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. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" on page 3-21 for information on obtaining and installing the hot fix.

Step 13 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Step 14 Refer to Chapter 6 for instructions on authenticating using EAP-TLS.

Enabling PEAP (EAP-GTC)

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

Step 1 Perform one of the following:

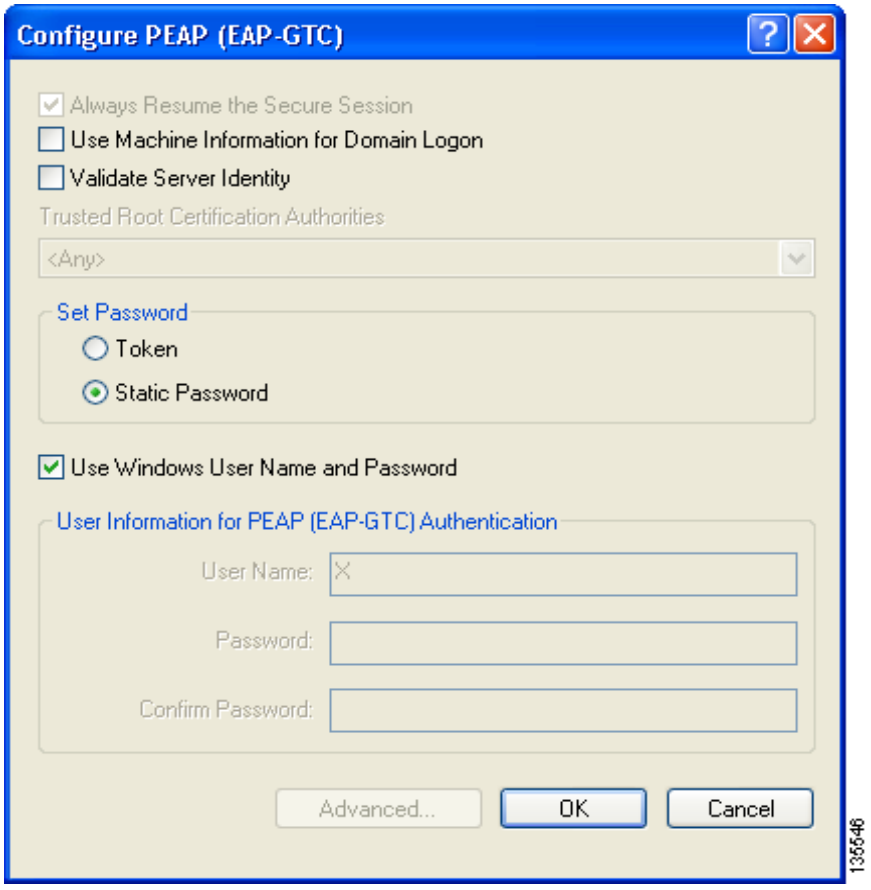
- If you want to enable PEAP (EAP-GTC) without WPA or WPA2, choose **802.1x** under Set Security Options and **PEAP (EAP-GTC)** in the 802.1x EAP Type drop-down box.
- If you want to enable PEAP (EAP-GTC) with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **PEAP (EAP-GTC)** in 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 your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

Note Refer to the "WPA and WPA2" on page 5-19 for additional information.

Step 2 Click **Configure**. The Configure PEAP (EAP-GTC) window appears (see Figure 5-16).

Figure 5-16 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 your 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 you log 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 Choose either **Token** or **Static Password**, depending on your user database.

Note If you choose Token, you must use a hardware token device or the Secure Computing SofToken program (release 2.1 or later) to obtain the one-time password and enter the password when prompted during the authentication process. Secure Computing PremierAccess release 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 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 PEAP (EAP-GTC) 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 username and password when your client adapter experiences momentary losses of association. However, if you leave your 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 your 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 your Windows username to also serve as your PEAP username, check the **Use Windows User Name** check box. This option gives you 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 to enter a separate PEAP username (which is registered with the RADIUS server) in addition to your regular Windows username in order to start the PEAP authentication process, enter your PEAP username in the User Name field.

  Note Your Windows username is filled in automatically. Simply delete your Windows username and enter your 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 the steps in "Configuring Advanced Settings" on page 5-58.

Step 11 Click **OK** to save your settings and return to the Profile Management (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 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. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" on page 3-21 for information on obtaining and installing the hot fix.

Step 14 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Step 15 Refer to Chapter 6 for instructions on authenticating using PEAP (EAP-GTC).

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:

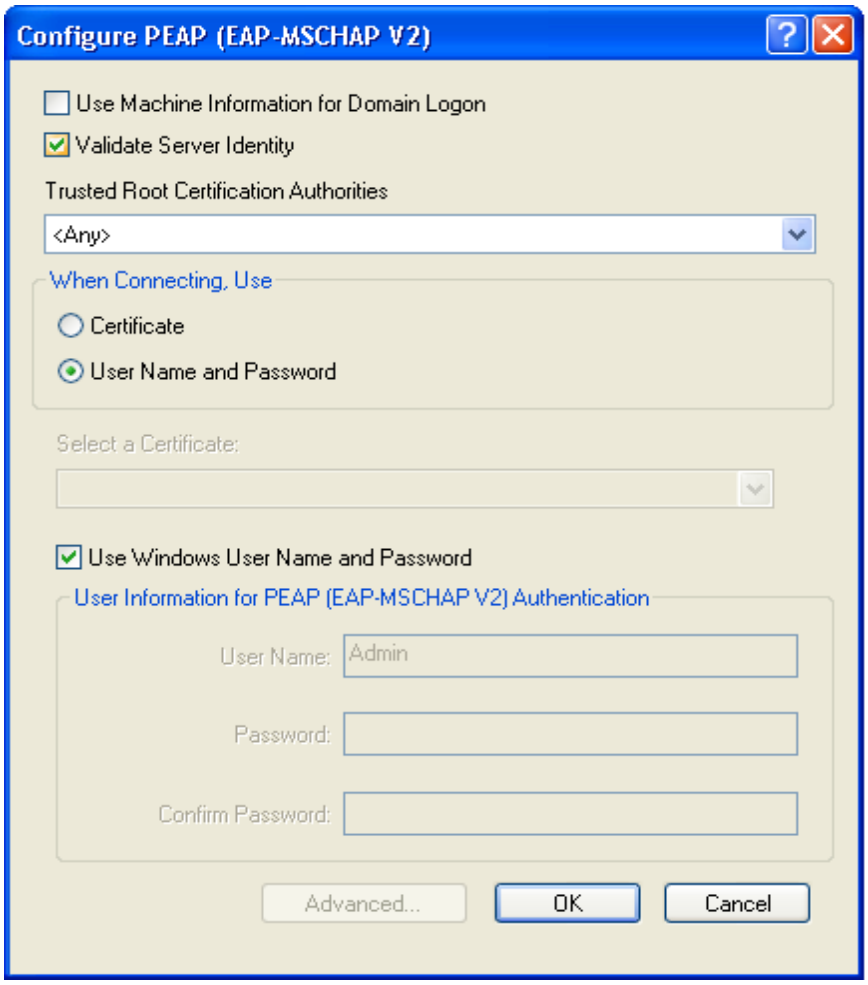
- If you want to enable PEAP (EAP-MSCHAP V2) without WPA or WPA2, choose **802.1x** under Set Security Options and **PEAP (EAP-MSCHAP V2)** in the 802.1x EAP Type drop-down box.
- If you want to enable PEAP (EAP-MSCHAP V2) with WPA or WPA2, choose **WPA/WPA2/CCKM** under Set Security Options and **PEAP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

Note Refer to the "WPA and WPA2" on page 5-19 for additional information.

Step 2 Click **Configure**. The Configure PEAP (EAP-MSCHAP V2) window appears (see Figure 5-17).

Figure 5-17 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 your 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 you log 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 to establish a network connection:

- If you want to connect using a username and password, choose **User Name and Password** and go to Step 7.
- If you want to connect using a user certificate installed on your 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 your Windows username and password to also serve as your 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 your PEAP username and password in the corresponding fields.

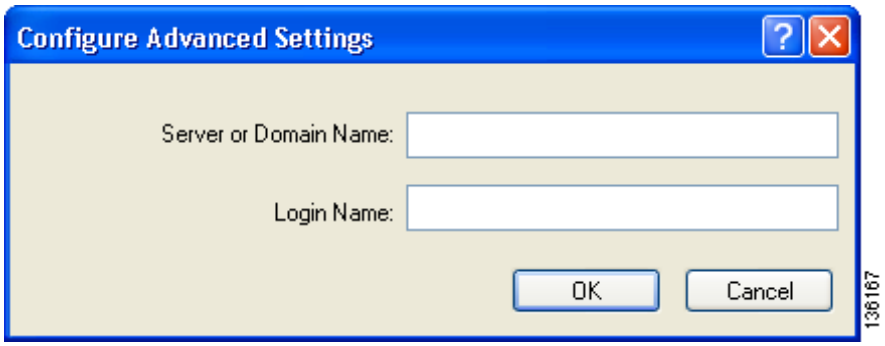
  Note Your Windows username is filled in automatically. Simply delete your Windows username and enter your separate PEAP username.

  b. Re-enter your 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 Configuration Settings window appears (see Figure 5-18).

Figure 5-18 Configuration 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 certificate authority listed in the Trusted Root Certification Authorities drop-down box on the Configure PEAP (EAP-MSCHAP V2) window (this is the recommended option) 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 your 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. Contact your system administrator for information.

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

Step 9 Click **OK** to save your settings and return to the Profile Management (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 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. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" on page 3-21 for information on obtaining and installing the hot fix.

Step 12 Click **OK** to save your settings and return to the Cisco Aironet Desktop Utility (Profile Management) window.

Step 13 Refer to Chapter 6 for instructions on authenticating using PEAP (EAP-MSCHAP V2).

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 Management (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 your computer to connect to the network prior to user logon. Follow these steps to enable this authentication type.

Note This procedure enables you 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)" on page 5-52.

Note Because this feature requires the Microsoft Wireless Configuration Manager to start and stop as you switch 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, your 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 Management (Security) window in ADU 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 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. Refer to the "Installing a Microsoft Hot Fix for Group Policy Delay" on page 3-21 for information on obtaining and installing the hot fix.

Step 3 Click **OK** to save your settings.

Step 4 Activate this profile on the Cisco Aironet Desktop Utility (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 your 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 you want the client adapter 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.

Note Refer to the "Enabling PEAP (EAP-MSCHAP V2)" on page E-66 if you need help configuring the PEAP (EAP-MSCHAP V2) settings.

Step 11 After you have finished the configuration, PEAP authentication should begin. Depending on the configuration settings you selected, you may be prompted for your PEAP username, password, and domain name. Note that you may need to minimize ADU in order to access the pop-up window that prompts you for your credentials.

Note You can have multiple host-based EAP profiles in ADU, but the Microsoft Wireless Configuration Manager maintains only one configuration. If you want to use different PEAP property settings for different host-based EAP profiles, you need to repeat the previous steps beginning with Step 4 every time you switch to a different host-based EAP profile.

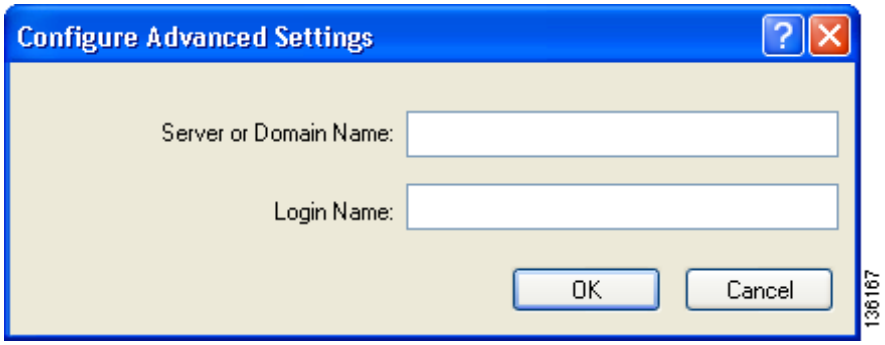
Note When you activate a host-based EAP profile, the Microsoft Wireless Configuration Manager takes control of the client adapter's authentication attempt. However, when you activate a non-host-based EAP profile, ADU assumes this control.

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

Configuring Advanced Settings

To specify a server or domain name and a login name to use for authenticating user credentials (see Figure 5-19), follow these steps:

Figure 5-19 Configure Advanced Settings



Step 1 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.

Step 2 If the Login Name field is not filled in automatically, enter your username with nothing after it (for example, jsmith).

Step 3 Click **OK** to save your settings.

Disabling Static WEP, WPA/WPA2 Passphrase, or EAP

To disable static WEP, WPA/WPA2 passphrase, or EAP authentication [LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2)] for a particular profile, choose **None** on the Profile Management (Security) window and click **OK**.

Note Choosing any security option other than Pre-Shared Key (Static WEP) on the Profile Management (Security) window disables static WEP automatically.

Note Choosing **Pre-Shared Key (Static WEP)** or **WPA/WPA2 Passphrase** on the Profile Management (Security) window disables EAP automatically.

Enabling Wi-Fi Multimedia

Wi-Fi Multimedia (WMM) is a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS). It specifically supports priority tagging and queuing. QoS is an access point feature that enables networking professionals to provide preferential treatment to certain traffic at the expense of other traffic. Without QoS, the access point offers best-effort service to each packet, regardless of the packet contents or size. Implementing QoS in a wireless LAN makes network performance more predictable and bandwidth usage more effective.

Cisco recommends that you enable WMM if your computer is running a time-sensitive application for QoS-aware clients such as voice or video (for example, Cisco IP SoftPhone).

QoS and WMM must be enabled on the access point to which the client will associate. These features are supported on the access point in Cisco IOS Release 12.3(2)JA or later. Refer to the documentation for your access point for instructions on enabling these features.

WMM is supported automatically in the client adapter software. However, you must enable the Windows QoS Packet Scheduler to ensure WMM support. Follow the instructions below to enable the QoS Packet Scheduler on Windows 2000 or XP.

Note The QoS Packet Scheduler must be installed before you can enable it. It comes preinstalled on Windows XP; however, you must install it on Windows 2000.

Enabling the QoS Packet Scheduler on Windows 2000

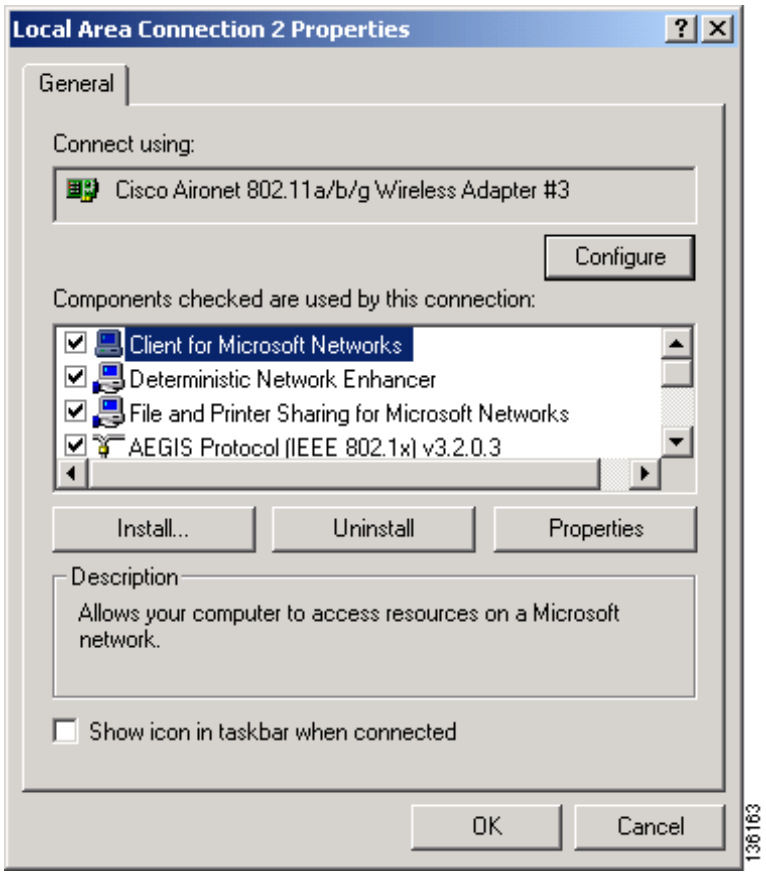
Follow these steps to enable the QoS Packet Scheduler on a computer running Windows 2000.

Step 1 Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**.

Step 2 Right-click your wireless network connection.

Step 3 Click **Properties**. The Wireless Cisco Connection Properties window appears (see Figure 5-20).

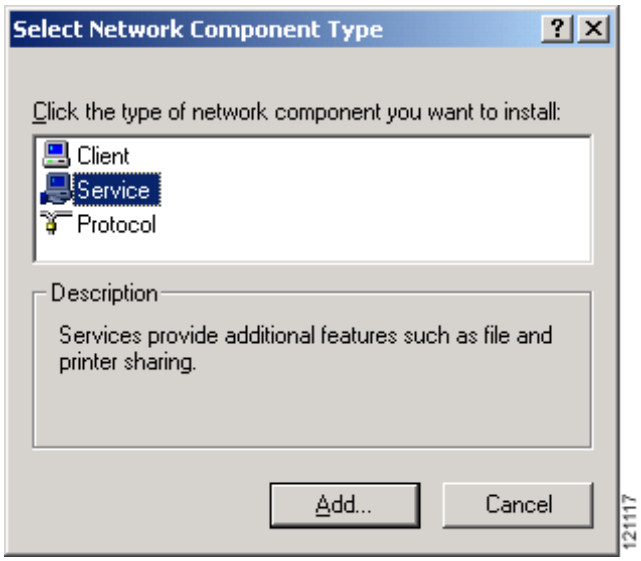
Figure 5-20 Wireless Cisco Connection Properties Window



Step 4 If the QoS Packet Scheduler is already installed, it is included in the list of components that this connection uses. If it appears in the list, go to Step 8. Otherwise, go to the next step to install it.

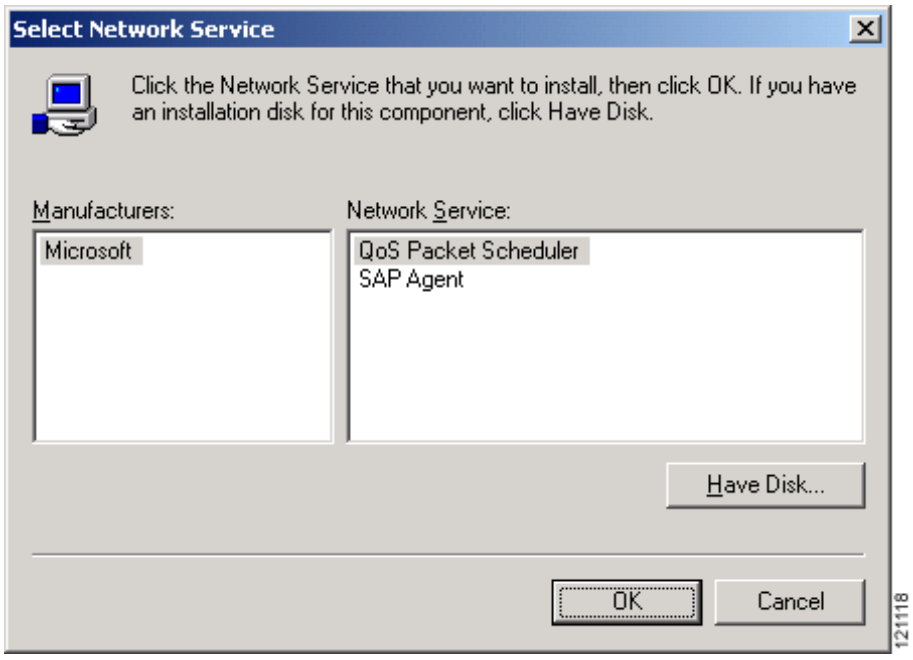
Step 5 Click **Install**. The Select Network Component Type window appears (see Figure 5-21).

Figure 5-21 Select Network Component Type Window



Step 6 Choose **Service** and click **Add**. The Select Network Service window appears (see Figure 5-22).

Figure 5-22 Select Network Service Window



Step 7 Click **QoS Packet Scheduler** and **OK**. The Wireless Cisco Connection Properties window reappears, and the QoS Packet Scheduler is included in the list of connections.

Step 8 Check the **QoS Packet Scheduler** check box if it is not checked.

Step 9 Click **OK**.

Enabling the QoS Packet Scheduler on Windows XP

Follow these steps to enable the QoS Packet Scheduler on a computer running Windows XP.

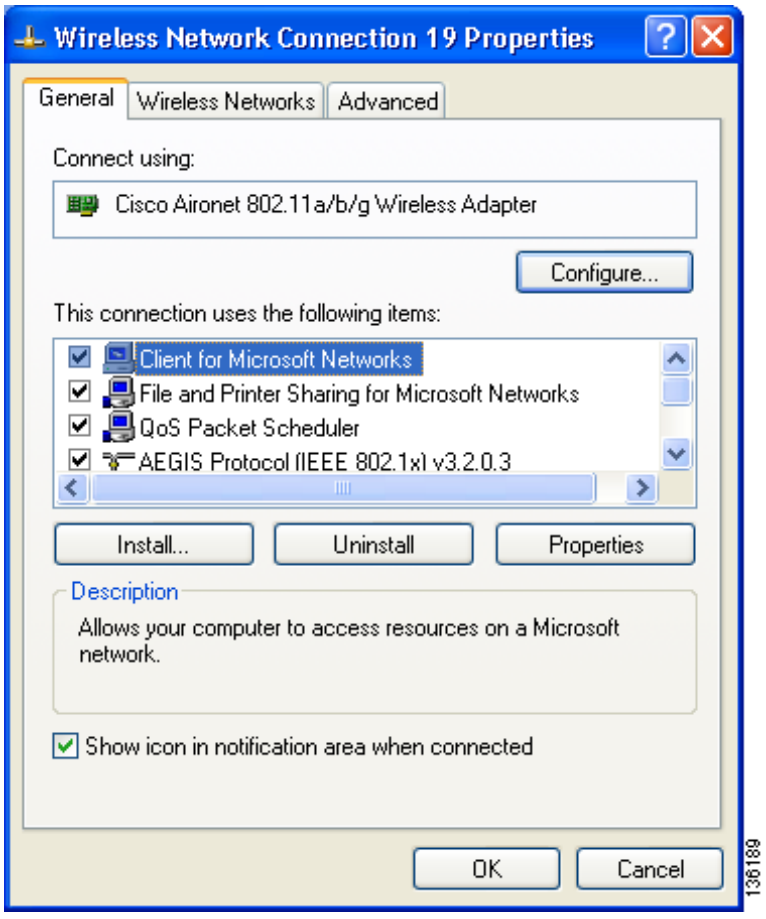
Step 1 Click **Control Panel**.

Step 2 Double-click **Network Connections**.

Step 3 Right-click your wireless network connection.

Step 4 Click **Properties**. The Wireless Network Connection Properties window appears (see Figure 5-23).

Figure 5-23 Wireless Network Connection Properties Window



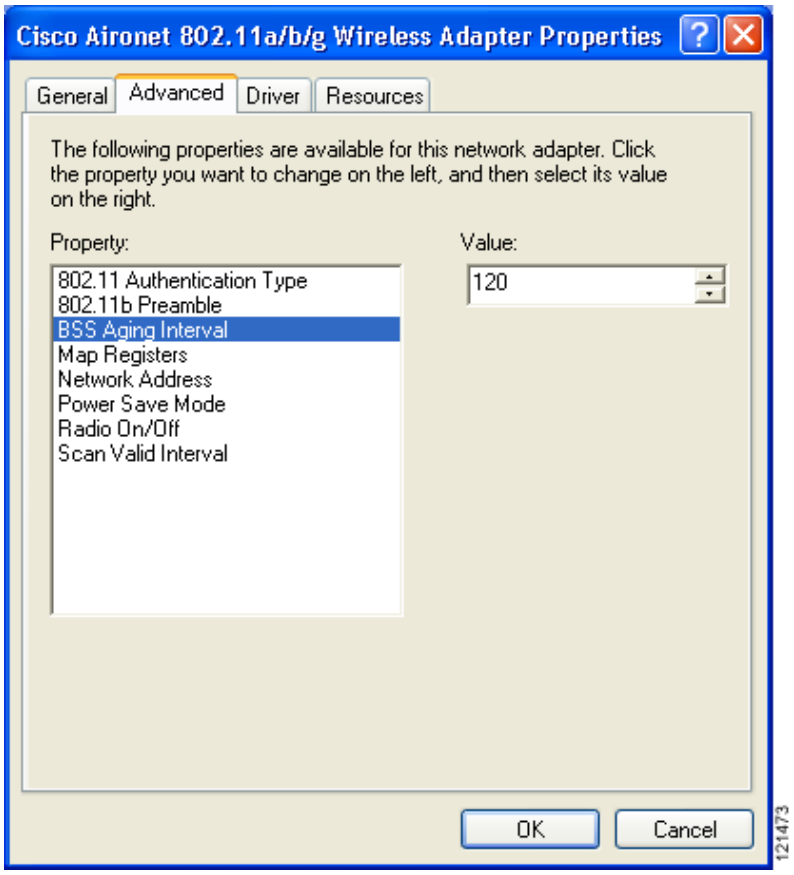
Step 5 Check the **QoS Packet Scheduler** check box, which appears in the list of items that this connection uses.

Step 6 Click **OK**.

Setting Roaming Parameters in the Windows Control Panel

The Cisco Aironet 802.11a/b/g Wireless Adapter Properties window (see Figure 5-24) in the Windows Control Panel enables you to set two parameters that regulate the client adapter's roaming capabilities.

Figure 5-24 Cisco Aironet 802.11a/b/g Wireless Adapter Properties Window



Follow these steps to access the roaming parameters.

Step 1 Double-click **My Computer**, **Control Panel**, and **System**.

Step 2 Click the **Hardware** tab and **Device Manager**.

Step 3 Double-click **Network Adapters**.

Step 4 Right-click **Cisco Aironet 802.11a/b/g Wireless Adapter**.

Step 5 Click **Properties** and the **Advanced** tab. The roaming parameters appear in the Property list. Table 5-5 lists and describes the client adapter's roaming parameters. Follow the instructions in the table to change the parameters.

Table 5-5 Roaming Parameters (in the Windows Control Panel)

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>BSS Aging Interval</td><td>The amount of time (in seconds) that the client keeps an access point in its roaming scanlist after it can no longer communicate to that device. The higher the value, the greater the number of access points to which the client may roam.
Range: 20 to 300 seconds (in 10-second increments)
Default: 120 seconds
Note Cisco recommends that you set the BSS Aging Interval to twice the value of the Scan Valid Interval. For example, if the Scan Valid Interval is 50, the BSS Aging Interval would be 100.</td></tr>
<tr><td>Scan Valid Interval</td><td>The amount of time (in seconds) before the client starts scanning for a better access point after reaching the roaming threshold or missing beacons. (See the threshold criteria in the table below.) The higher the value, the less time the client spends scanning for a better access point and the more time it has to send data.
Range: 20 to 120 seconds (in 5-second increments)
Default: 60 seconds
Note The client does not scan for a new access point as long as it has a good connection and is passing data.
<table>
<tr><th>Wireless Mode</th><th>Signal Strength Threshold (dBm)</th><th>Transmit Rate Threshold (Mbps)</th></tr>
<tr><td>5 GHz, 54 Mbps or
2.4 GHz, 54 Mbps</td><td>24</td><td>24</td></tr>
<tr><td>2.4 GHz, 11 Mbps
(other modes enabled)</td><td>24</td><td>9</td></tr>
<tr><td>2.4 GHz, 11 Mbps
(only mode enabled)</td><td>24</td><td>5</td></tr>
</table></td></tr>
</table>

The default configuration of the client adapter software is optimized for high throughput and the lowest power consumption. However, in some environments, this configuration can cause the client adapter to unnecessarily stay with the currently associated access point longer than necessary.

If your application requires a faster roaming response, configure the BSS Aging Interval and Scan Valid Interval parameters as follows:

- Set the **BSS Aging Interval** parameter to 20
- Set the **Scan Valid Interval** parameter to 20

Note If you are using client software prior to 2.7.0.2, you will not be able to set the BSS Aging Interval parameter to 20. In that case, set it to 30.

Configuring Band Usage

If your AP coverage permits it, follow these steps to configure the client profile only in ADU to use the 5GHz (802.11a) or 2.4GHz (802.11b/g) band, *not* both:

Step 1 Launch ADU.

Step 2 Click **Profile Management**.

Step 3 Select the profile of interest and click **Modify**.

Step 4 Click **Advanced**.

Step 5 Under Wireless Mode, uncheck the rates that you do not intend to use.

If you do not use ADU to manage CB21AG, then you must use registry settings to select the rates. Follow these steps:

1. Launch regedit and navigate to the following entry:

   HKLM\System\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}

2. Right-click and choose **Find** and find the variable called "NetBand."

   This variable will be under a four-digit subkey whose DriverDesc value is "Cisco Aironet 802.11a/b/g Wireless Adapter."

   The NetBand REG_SZ variable is a bitmask of supported rates. By default, this variable it is set to 15 decimal (0x0F). The supported values are:

   - 802.11a 0x01
   - (not used) 0x02
   - 802.11b 0x04
   - 802.11g 0x08
   - (not used) 0x10

For example, to support only 11b and 11g rates, the bitmask would be 0x04 + 0x08 = 0x0C = 12 decimal.

Using EAP Authentication

This chapter explains the sequence of events that occurs and the actions you must take when a profile that is set for EAP authentication is activated.

The following topics are covered in this chapter:

Overview

This chapter explains the sequence of events that occurs after you (or auto profile selection) activate a profile that uses EAP authentication or you eject and reinsert the client adapter, reboot the computer, log on while this profile is active, or are informed that your password has expired or is invalid. The chapter contains seven sections based on the profile's authentication type and its username and password settings:

- LEAP or EAP-FAST with the Windows username and password, page 6-3
- LEAP or EAP-FAST with an automatically prompted login, page 6-6
- LEAP or EAP-FAST with a manually prompted login, page 6-9
- LEAP or EAP-FAST with a saved username and password, page 6-13
- EAP-TLS, page 6-14
- PEAP (EAP-GTC), page 6-15
- PEAP (EAP-MSCHAP V2), page 6-16

Also provided are an overview of LEAP and EAP-FAST authentication (below) and instructions for restarting the authentication process when necessary (page 6-16).

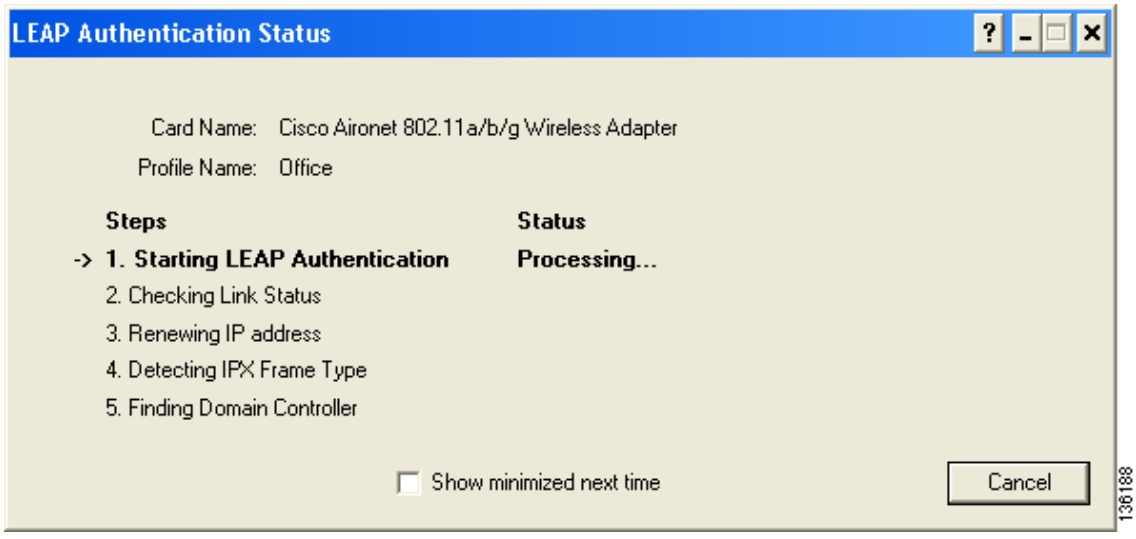
Follow the instructions for your profile's authentication type and credential settings to successfully authenticate.

Note If any error messages appear during authentication, refer to Chapter 10 for explanations and recommended actions.

Using LEAP or EAP-FAST

When LEAP or EAP-FAST authentication begins, the LEAP or EAP-FAST Authentication Status window appears (see Figure 6-1).

Figure 6-1 LEAP or EAP-FAST Authentication Status Window



This window provides information about the status of LEAP or EAP-FAST authentication. Table 6-1 lists and explains the stages of LEAP or EAP-FAST authentication. As each stage is completed, a status message (such as *Success)* appears in the Status field. If any error messages appear, refer to the "Error Messages" section on page 10-12 for an explanation and the recommended action to take.

Table 6-1 Stages of LEAP or EAP-FAST Authentication

Stage	Explanation
Starting LEAP or EAP-FAST Authentication	The client adapter associates to an access point, and the LEAP or EAP-FAST authentication process begins.
Checking Link Status	The client adapter is EAP authenticated, and the network connection is verified.
Renewing IP Address	If DHCP is enabled, the IP address is released and renewed.
Detecting IPX Frame Type	The IPX frame type is reset if AutoDetect is enabled.
Finding Domain Controller	If you are logging into a domain and the active profile specifies that the domain name be included, an attempt is made to find the domain controller to make sure subsequent access to the domain is successful.

If you do not want the LEAP or EAP-FAST Authentication Status window to appear each time the client adapter attempts to authenticate using LEAP or EAP-FAST, check the **Show minimized next time** check box at the bottom of the window. On future LEAP or EAP-FAST authentication attempts, the LEAP or EAP-FAST Authentication Status window appears minimized in the Windows taskbar.

Note To make the LEAP or EAP-FAST Authentication Status window reappear once it has been minimized, click the **LEAP Authentication Status** or **EAP-FAST Authentication Status** tab in the Windows taskbar and uncheck the **Show minimized next time** check box. The LEAP or EAP-FAST Authentication Status window should now appear for all future LEAP or EAP-FAST authentication attempts.

Using LEAP or EAP-FAST with the Windows Username and Password

After Profile Activation or Card Insertion

After you (or auto profile selection) activate a profile that uses your Windows username and password for LEAP or EAP-FAST authentication or you eject and reinsert the client adapter while this profile is active, the following events occur:

1. The LEAP or EAP-FAST Authentication Status window appears.
2. If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.
3. If your client adapter authenticates, the window shows that each stage was successful and then disappears. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

   If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

After a Reboot or Logon

After your computer reboots or you log on, follow these steps to authenticate using LEAP or EAP-FAST.

Step 1 When the Windows login window appears, enter your Windows username and password and click **OK**. The domain name is optional.

Note If your computer has Novell Client 32 software installed, a separate LEAP or EAP-FAST login window appears before the Novell login window. If this occurs, enter your Windows and Novell username and password in the login windows and click **OK**.

The LEAP or EAP-FAST Authentication Status window appears.

Step 2 If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.

Step 3 If your client adapter authenticates, the window shows that each stage was successful and then disappears.

If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

Step 4 Windows continues to log you onto the system. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

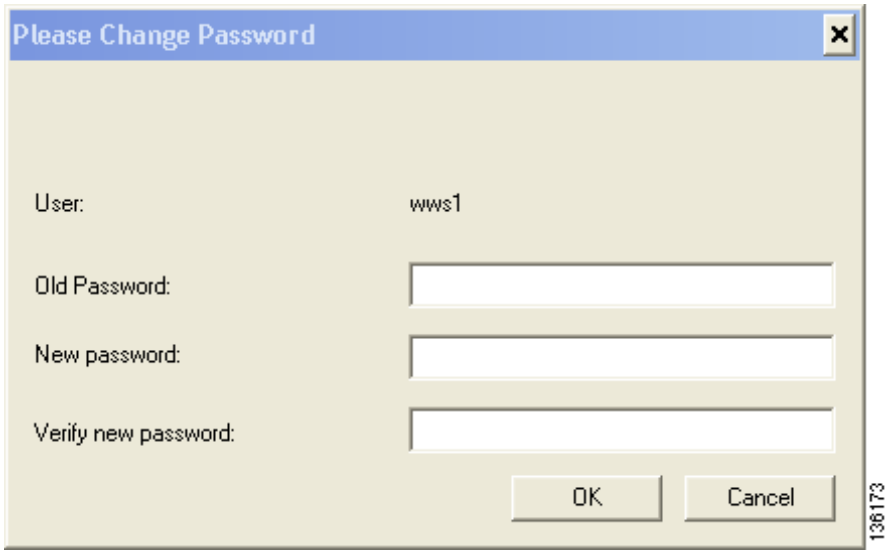
After Your EAP-FAST Password Expires

If the EAP-FAST password for your current profile expires or becomes invalid, follow these steps to change your password.

Note If you change your Windows password using the standard Windows Change Password function, the client updates the EAP-FAST password automatically and maintains its connection to the access point if the current profile uses the Windows username and password. However, data packets may be dropped during this process.

Step 1 When the Please Change Password window appears (see Figure 6-2) to indicate that your password is invalid, enter your old password in the Old Password field.

Figure 6-2 Please Change Password Window



Step 2 Enter your new password in both the New Password and Verify New Password fields and click **OK**.

Step 3 If prompted, log off and on again in order to update your local cached account with your new password.

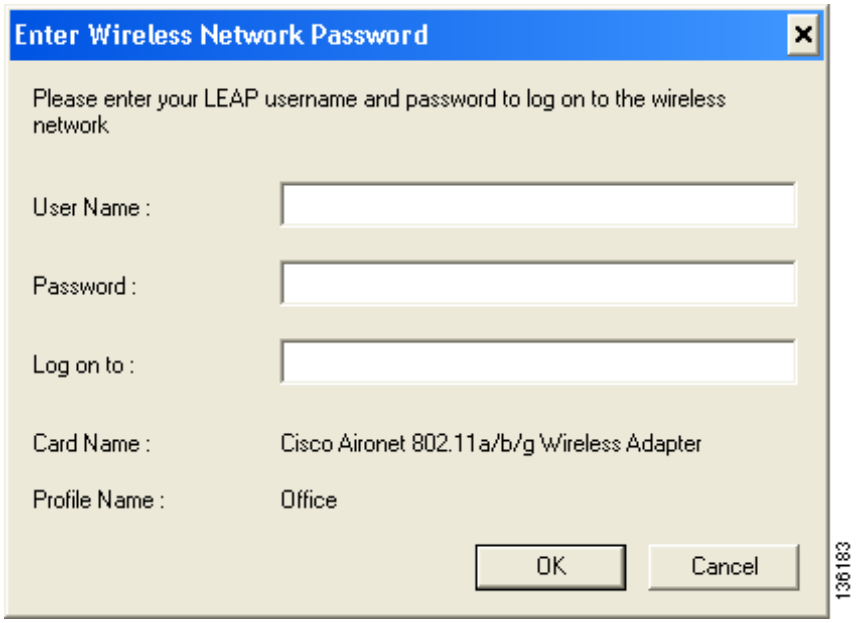
Using LEAP or EAP-FAST with an Automatically Prompted Login

After Profile Activation or Card Insertion

After you (or auto profile selection) activate a profile that uses a separate username and password for LEAP or EAP-FAST authentication or you eject and reinsert the client adapter while this profile is active, follow these steps to authenticate.

Step 1 When the Enter Wireless Network Password window appears (see Figure 6-3), enter your LEAP or EAP-FAST username and password and click **OK**. The domain name can be entered in the Log On To field; it is optional.

Figure 6-3 Enter Wireless Network Password Window



The LEAP or EAP-FAST Authentication Status window appears.

Step 2 If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.

Step 3 If your client adapter authenticates, the LEAP or EAP -FAST Authentication Status window shows that each stage was successful and then disappears. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

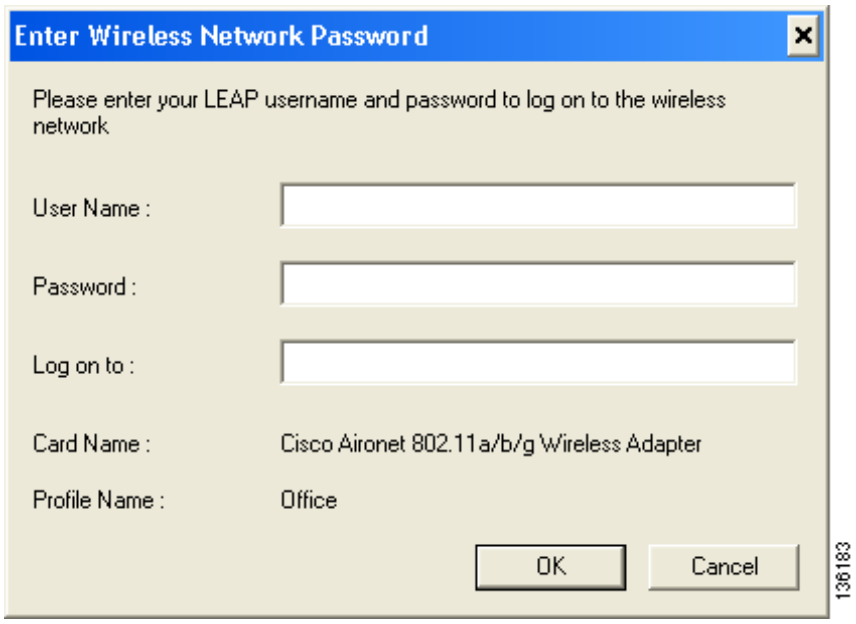
After a Reboot or Logon

After your computer reboots or you log on, follow these steps to authenticate using LEAP or EAP-FAST.

Step 1 When the Windows login window appears, enter your Windows username and password and click **OK**.

Step 2 When the Enter Wireless Network Password window appears (see Figure 6-4), enter your LEAP or EAP-FAST username and password and click **OK**. The domain name can be entered in the Log On To field; it is optional.

Figure 6-4 Enter Wireless Network Password Window



The LEAP or EAP-FAST Authentication Status window appears.

Step 3 If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.

Step 4 If your client adapter authenticates, the window shows that each stage was successful and then disappears. The logon or boot-up process completes.

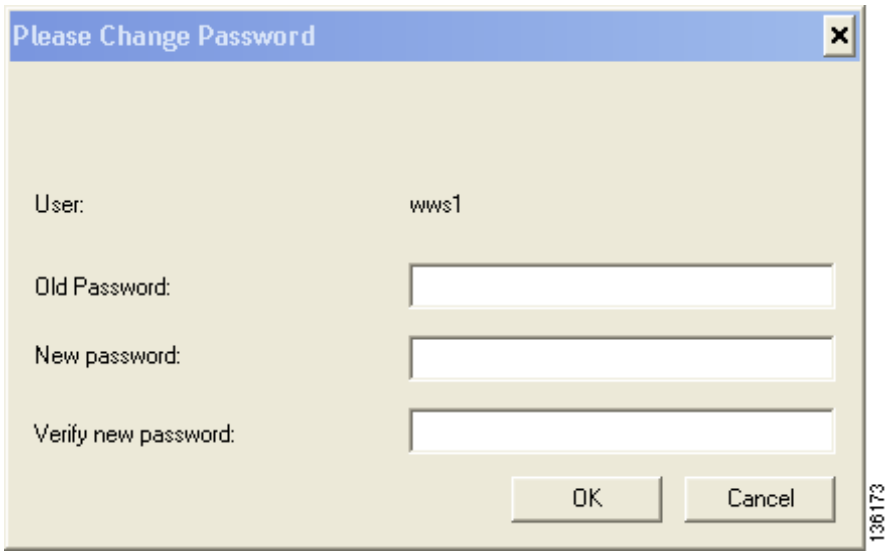
If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

After Your EAP-FAST Password Expires

If the EAP-FAST password for your current profile expires or becomes invalid, follow these steps to change your password.

Step 1 When the Please Change Password window appears (see Figure 6-5) to indicate that your password is invalid, enter your old password in the Old Password field.

Figure 6-5 Please Change Password Window



Step 2 Enter your new password in both the New Password and Verify New Password fields.

Step 3 Click **OK**. The client adapter should authenticate using your new password.

Using LEAP or EAP-FAST with a Manually Prompted Login

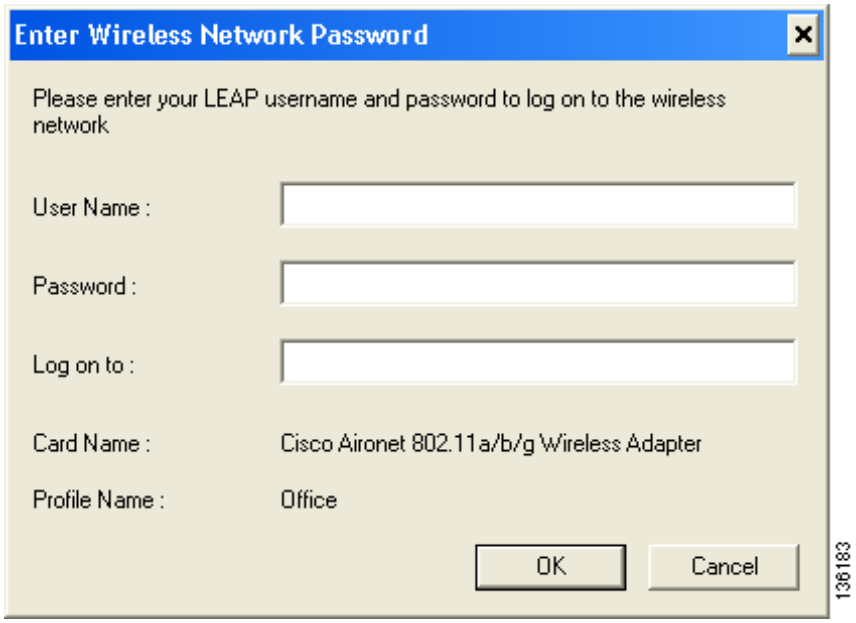
After Profile Activation

After you (or auto profile selection) activate a profile that uses LEAP or EAP-FAST authentication with a manually prompted login, follow these steps to authenticate.

Note If auto profile selection is enabled, this procedure is applicable the first time auto profile selection activates a manual LEAP or manual EAP-FAST profile. After you follow these steps to enter your LEAP or EAP-FAST credentials, you can switch profiles without having to re-enter your credentials until you reboot your computer, eject and reinsert your client adapter, or change the profile in any way (including its priority in auto profile selection). If auto profile selection is disabled, you must re-enter your credentials every time you activate a manual LEAP or manual EAP-FAST profile.

Step 1 When the Enter Wireless Network Password window appears (see Figure 6-6), enter your LEAP or EAP-FAST username and password and click **OK**. The domain name can be entered in the Log On To field; it is optional.

Figure 6-6 Enter Wireless Network Password Window



The LEAP or EAP-FAST Authentication Status window appears.

Step 2 If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.

Step 3 If your client adapter authenticates, the window shows that each stage was successful and then disappears. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

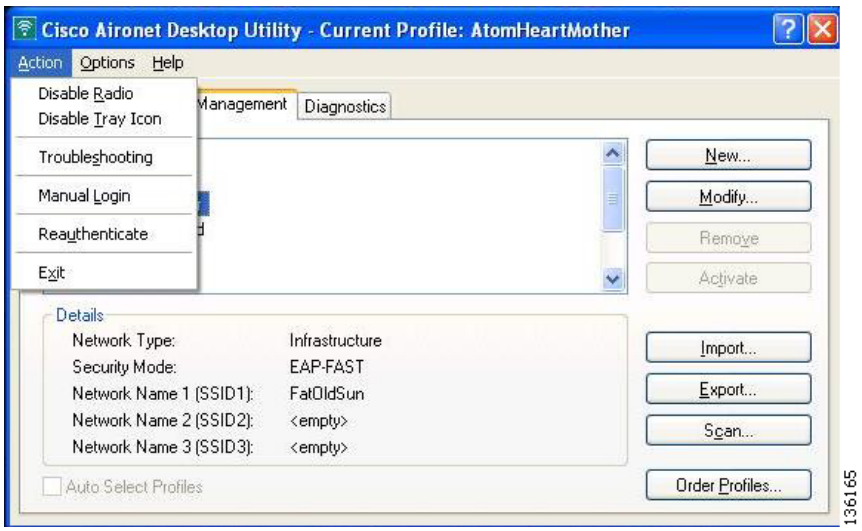
After a Reboot, Logon, or Card Insertion

After your computer reboots, you log on, or you eject and reinsert the client adapter, the adapter does not automatically attempt to authenticate. You must manually invoke the authentication process. To do so, follow these steps.

Step 1 If you rebooted your computer or logged on, complete your standard Windows login. Then open ASTU or ADU.

Step 2 Choose the **Manual Login** option from the ADU Action drop-down menu (see Figure 6-7).

Figure 6-7 Action Drop-Down Menu



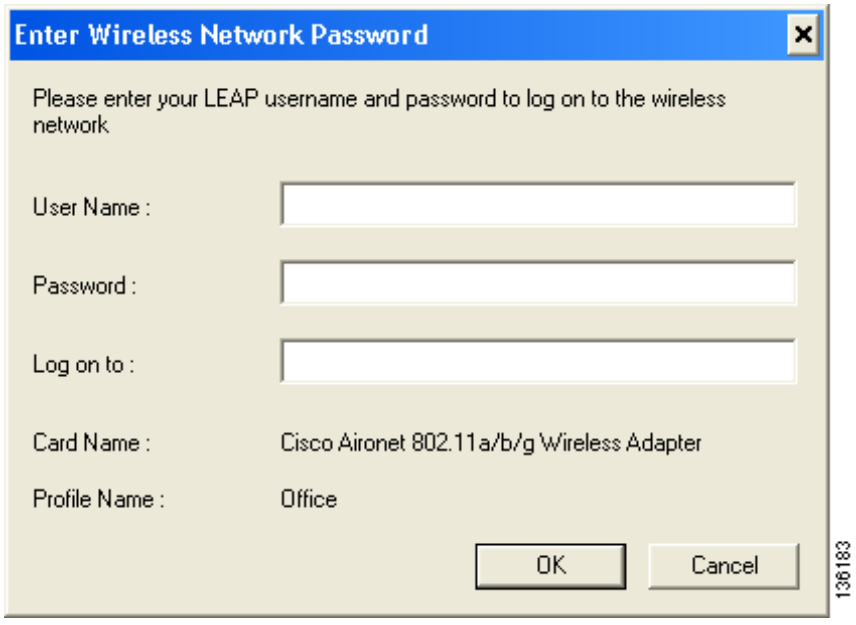
You can also choose the **Manual Login** option from the ASTU pop-up menu (see Figure 6-8).

Figure 6-8 ASTU Pop-Up Menu

Note In ACAU, you can enable the Manual Login option in ASTU by clicking the Global Settings tab, double-clicking Global Settings, double-clicking ASTU Settings, and choosing Yes under Manual Login.

Step 3 When the Enter Wireless Network Password window appears (see Figure 6-9), enter your LEAP or EAP-FAST username and password and click **OK**. The domain name can be entered in the Log On To field; it is optional.

Figure 6-9 Enter Wireless Network Password Window



The LEAP or EAP-FAST Authentication Status window appears.

Step 4 If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.

Step 5 If your client adapter authenticates, the window shows that each stage was successful and then disappears. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

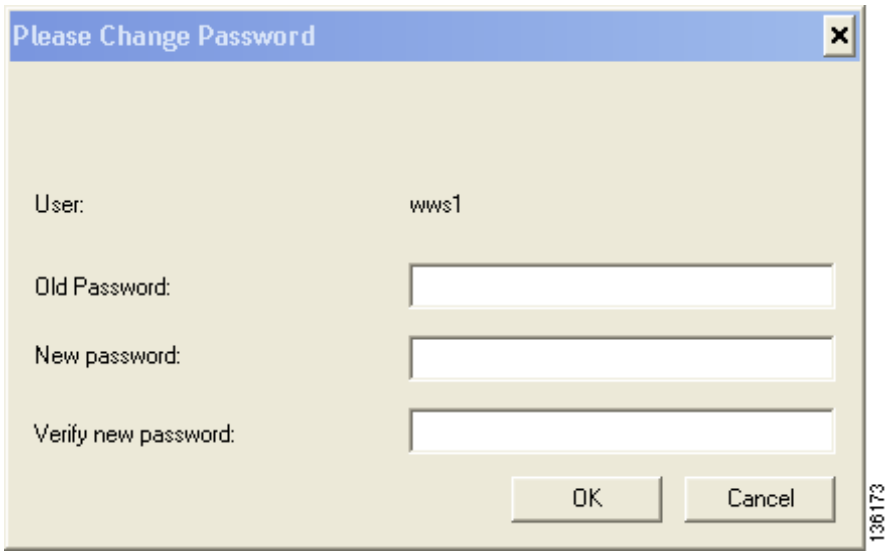
If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

After Your EAP-FAST Password Expires

If the EAP-FAST password for your current profile expires or becomes invalid, follow these steps to change your password.

Step 1 When the Please Change Password window appears (see Figure 6-10) to indicate that your password is invalid, enter your old password in the Old Password field.

Figure 6-10 Please Change Password Window



Step 2 Enter your new password in both the New Password and Verify New Password fields.

Step 3 Click **OK**. The client adapter should authenticate using your new password.

Using LEAP or EAP-FAST with a Saved Username and Password

After Profile Activation or Card Insertion

After you (or auto profile selection) activate a profile that uses LEAP or EAP-FAST authentication with a saved LEAP or EAP-FAST username and password or you eject and reinsert the client adapter while this profile is active, the following events occur:

1. The LEAP or EAP-FAST Authentication Status window appears.
2. If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.
3. If your client adapter authenticates, the window shows that each stage was successful and then disappears. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

   If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.

After a Reboot or Logon

After your computer reboots or you log on, the following events occur:

1. After you enter your Windows username and password, the authentication process begins automatically using your saved LEAP or EAP-FAST username and password.

   Note If you unchecked the **No Network Connection Unless User Is Logged In** check box on the LEAP Settings window or EAP-FAST Settings window, the EAP authentication process begins before the Windows login window appears.

2. If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.
3. If your client adapter authenticates, the LEAP or EAP-FAST Authentication Status window shows that each stage was successful and then disappears.

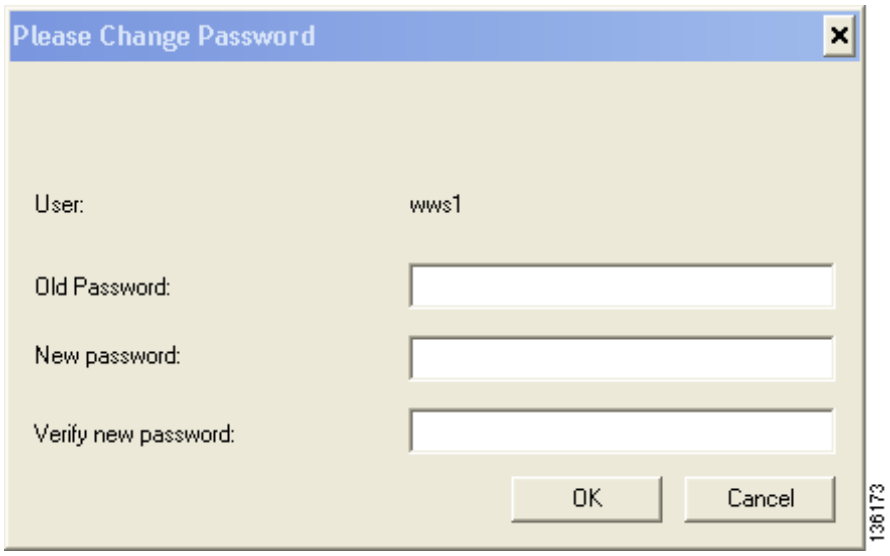
   If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the "Error Messages" section on page 10-12 for the necessary action to take.
4. Windows continues to log you onto the system. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

After Your EAP-FAST Password Expires

If the EAP-FAST password for your current profile expires or becomes invalid, follow these steps to change your password.

Step 1 When the Please Change Password window appears (see Figure 6-11) to indicate that your password is invalid, enter your old password in the Old Password field.

Figure 6-11 Please Change Password Window



Step 2 Enter your new password in both the New Password and Verify New Password fields.

Step 3 Click **OK**. The client adapter should authenticate using your new password.

Step 4 Edit the profile in ADU by changing the saved username and password on the EAP-FAST Settings window.

Using EAP-TLS

After you (or auto profile selection) activate a profile that uses EAP-TLS authentication or you eject and reinsert the client adapter, reboot the computer, or log on while this profile is active, the EAP authentication process begins automatically, and the client adapter should EAP authenticate.

If your client adapter authenticates, ASTU and the Link Status field on the ADU Current Status window show *Authenticated*. If the authentication attempt fails, ASTU and ADU show *Authentication Failed*.

Using PEAP (EAP-GTC)

After you (or auto profile selection) activate a profile that uses PEAP (EAP-GTC) authentication or you eject and reinsert the client adapter, reboot the computer, or log on while this profile is active, follow the steps in one of the sections below to EAP authenticate. Choose the section appropriate for your user database.

Windows NT or 2000 Domain Databases or LDAP Databases Only

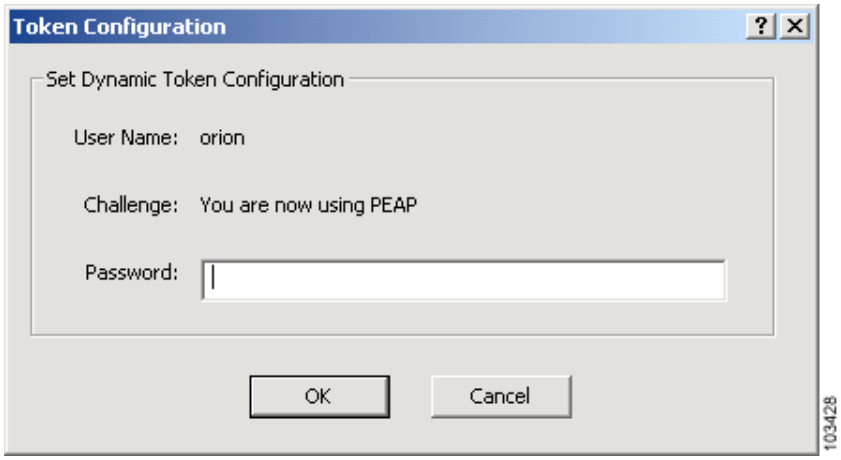
The EAP authentication process begins automatically. The client adapter should EAP authenticate using either your Windows credentials or the username and password entered in the Define PEAP (EAP-GTC) Configuration window. If your client adapter authenticates, ASTU and the Link Status field on the ADU Current Status window show *Authenticated*. If the authentication attempt fails, ASTU and ADU show *Authentication Failed*.

OTP Databases Only

Step 1 Use your hardware token device or SofToken program to obtain the one-time password.

Step 2 When the Token Configuration window appears (see Figure 6-12), enter the one-time password.

Figure 6-12 Token Configuration Window



Note The username is filled in automatically.

Step 3 Click **OK** to begin the authentication process.

Note If the password is invalid or entered incorrectly, the Token Configuration window reappears, enabling you to re-enter it.

If your client adapter authenticates, ASTU and the Link Status field on the ADU Current Status window show *Authenticated*. If the authentication attempt fails, ASTU and ADU show *Authentication Failed*.

Using PEAP (EAP-MSCHAP V2)

After you (or auto profile selection) activate a profile that uses PEAP (EAP-MSCHAP V2) authentication or you eject and reinsert the client adapter, reboot the computer, or log on while this profile is active, the EAP authentication process begins automatically. The client adapter should EAP authenticate using either your Windows credentials or the username and password entered in the Define PEAP (EAP-MSCHAP V2) Configuration window.

If your client adapter authenticates, ASTU and the Link Status field on the ADU Current Status window show *Authenticated*. If the authentication attempt fails, ASTU and ADU show *Authentication Failed*.

Restarting the Authentication Process

To force your client adapter to try to reauthenticate using the username and password of the current profile, choose **Reauthenticate** from the ASTU pop-up menu or the ADU Action drop-down menu. When you choose this option, the authentication process begins.

If your client adapter is unable to authenticate using the specified username and password, you may be prompted to re-enter them. If you click **Cancel**, a message appears indicating that the current profile will be disabled until you choose the Reauthenticate option, reboot your computer, or eject and reinsert the client adapter.