



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

Software Release 4.0

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number: OL-4211-07

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.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

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

Copyright © 2007 Cisco Systems, Inc.

All rights reserved.



CONTENTS

Preface xi

Audience xi

Purpose xi

Organization xii

Conventions xii

Related Publications xiv

Obtaining Documentation, Obtaining Support, and Security Guidelines xiv

CHAPTER 1

Product Overview 1-1

Introduction to the Client Adapters 1-2

Terminology 1-2

Hardware Components 1-3

Radio 1-3

Radio Antenna 1-3

LEDs 1-3

Software Components 1-4

Driver 1-4

Client Utilities 1-4

Network Configurations Using Client Adapters 1-5

Ad Hoc Wireless LAN 1-5

Wireless Infrastructure with Workstations Accessing a Wired LAN 1-6

CHAPTER 2

Preparing for Installation 2-1

Safety information 2-2

FCC Safety Compliance Statement 2-2

Safety Guidelines 2-2

Warnings 2-2

Unpacking the Client Adapter 2-3

Package Contents 2-3

System Requirements 2-4

Site Requirements 2-5

For Infrastructure Devices 2-5

For Client Devices 2-5

CHAPTER 3

Installing the Client Adapter	3-1
Inserting a Client Adapter	3-2
Inserting a PC-Cardbus Card	3-2
Inserting a PCI Card	3-3
Changing the Bracket	3-3
Inserting the Card	3-4
Assembling the Antenna	3-5
Mounting the Antenna	3-6
Installing the Client Adapter Software	3-9
Installing the Intermediate Driver Manually	3-20
Installing a Microsoft Hot Fix for Group Policy Delay	3-21

CHAPTER 4

Using the Profile Manager	4-1
Overview of Profile Manager	4-2
Opening Profile Manager	4-2
Creating a New Profile	4-4
Including a Profile in Auto Profile Selection	4-8
Selecting the Active Profile	4-10
Modifying a Profile	4-11
Editing a Profile	4-11
Deleting a Profile	4-11
Importing and Exporting Profiles	4-11
Importing a Profile	4-12
Exporting a Profile	4-12

CHAPTER 5

Configuring the Client Adapter	5-1
Overview	5-2
Setting General Parameters	5-3
Setting Advanced Parameters	5-6
Setting Security Parameters	5-14
Overview of Security Features	5-14
Static WEP Keys	5-15
EAP (with Dynamic WEP Keys)	5-15
WPA and WPA2	5-18
CCKM Fast Secure Roaming	5-19
Reporting Access Points that Fail LEAP Authentication	5-19
Additional WEP Key Security Features	5-20
Synchronizing Security Features	5-21

Enabling Static WEP	5-26
Enabling WPA/WPA2 Passphrase	5-28
Enabling LEAP	5-29
Enabling EAP-FAST	5-34
Enabling EAP-TLS or PEAP	5-44
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 Credentials	5-55
Configuring Advanced Settings	5-58
Disabling Static WEP, WPA/WPA2 Passphrase, or EAP	5-58
Enabling Wi-Fi Multimedia	5-59
Enabling the QoS Packet Scheduler on Windows 2000	5-59
Enabling the QoS Packet Scheduler on Windows XP	5-62
Setting Roaming Parameters in the Windows Control Panel	5-63
Configuring Band Usage	5-65

CHAPTER 6

Using EAP Authentication	6-1
Overview	6-2
Using LEAP or EAP-FAST	6-2
Using LEAP or EAP-FAST with the Windows Username and Password	6-4
After Profile Activation or Card Insertion	6-4
After a Reboot or Logon	6-4
After Your EAP-FAST Password Expires	6-5
Using LEAP or EAP-FAST with an Automatically Prompted Login	6-6
After Profile Activation or Card Insertion	6-6
After a Reboot or Logon	6-7
After Your EAP-FAST Password Expires	6-8
Using LEAP or EAP-FAST with a Manually Prompted Login	6-9
After Profile Activation	6-9
After a Reboot, Logon, or Card Insertion	6-10
After Your EAP-FAST Password Expires	6-12
Using LEAP or EAP-FAST with a Saved Username and Password	6-13
After Profile Activation or Card Insertion	6-13
After a Reboot or Logon	6-13
After Your EAP-FAST Password Expires	6-14
Using EAP-TLS	6-14
Using PEAP (EAP-GTC)	6-15

Windows NT or 2000 Domain Databases or LDAP Databases Only	6-15
OTP Databases Only	6-15
Using PEAP (EAP-MSCHAP V2)	6-16
Restarting the Authentication Process	6-16

CHAPTER 7

Viewing Status and Statistics 7-1

Overview of ADU Status and Statistics Tools	7-2
Setting Parameters that Affect ADU Status and Statistics Tools	7-2
Selecting the Software to Manage Your Client Adapter	7-4
Viewing the Current Status of Your Client Adapter	7-5
Viewing Statistics for Your Client Adapter	7-14

CHAPTER 8

Using the Aironet System Tray Utility (ASTU) 8-1

Overview of ASTU	8-2
The ASTU Icon	8-2
Tool Tip Window	8-3
Pop-Up Menu	8-5
Help	8-5
Exit	8-6
Open Aironet Desktop Utility	8-6
Troubleshooting	8-6
Preferences	8-6
Enable/Disable Radio	8-7
Manual Login	8-8
Reauthenticate	8-8
Select Profile	8-8
Show Connection Status	8-9

CHAPTER 9

Routine Procedures 9-1

Removing a Client Adapter	9-2
Removing a PC-Cardbus Card	9-2
Removing a PCI Card	9-2
Client Adapter Software Procedures	9-3
Upgrading the Client Adapter Software	9-3
Manually Installing or Upgrading the Client Adapter Driver	9-6
Uninstalling the Client Adapter Software	9-6
ADU Procedures	9-7
Opening ADU	9-8

Exiting ADU	9-8
Finding the Version of ADU and Other Software Components	9-9
Viewing Client Adapter Information	9-10
Accessing Online Help	9-10
ASTU Procedures	9-11
Enabling or Disabling Your Client Adapter's Radio	9-11

CHAPTER 10**Troubleshooting 10-1**

Accessing the Latest Troubleshooting Information	10-2
Interpreting the Indicator LEDs	10-2
Troubleshooting the Client Adapter	10-3
Using the Cisco Aironet Troubleshooting Utility	10-3
Diagnosing Your Client Adapter's Operation	10-4
Saving the Detailed Report to a Text File	10-7
Disabling the Microsoft Wireless Configuration Manager (Windows XP Only)	10-7
Disabling the Microsoft 802.1X Supplicant (Windows 2000 Only)	10-8
Client Adapter Recognition Problems	10-8
Resolving Resource Conflicts	10-8
Resolving Resource Conflicts in Windows 2000	10-9
Resolving Resource Conflicts in Windows XP	10-9
Problems Associating to an Access Point	10-10
Problems Connecting to the Network	10-10
Prioritizing Network Connections	10-11
Troubleshooting with Diagnostic Channel Mode	10-11
Parameters Missing from Profile Management Windows	10-17
Windows Wireless Network Connection Icon Shows Unavailable Connection (Windows XP Only)	10-17
Error Messages	10-18

APPENDIX A**Technical Specifications A-1****APPENDIX B****Translated Safety Warnings B-1**

Explosive Device Proximity Warning	B-2
Antenna Installation Warning	B-3
Warning for Laptop Users	B-4

APPENDIX C**Declarations of Conformity and Regulatory Information C-1**

Manufacturer's Federal Communication Commission Declaration of Conformity Statement	C-2
---	-----

Department of Communications – Canada	C-3
Canadian Compliance Statement	C-3
European Community, Switzerland, Norway, Iceland, and Liechtenstein	C-3
Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC	C-3
Declaration of Conformity Statement	C-5
Cisco Aironet CB21AG Wireless LAN Client Adapter	C-5
Cisco Aironet PI21AG Wireless LAN Client Adapter	C-6
Declaration of Conformity for RF Exposure	C-7
Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan	C-7
Japanese Translation	C-7
English Translation	C-7
Administrative Rules for Cisco Aironet Wireless LAN Client Adapters in Taiwan	C-8
2.4- and 5-GHz Client Adapters	C-8
Chinese Translation	C-8
English Translation	C-8
5-GHz Client Adapters	C-9
Chinese Translation	C-9
English Translation	C-9
Brazil/Anatel Approval	C-9
AIR-CB21AG-W-K9	C-9
AIR-PI21AG-W-K9	C-10

APPENDIX D

Channels, Power Levels, and Antenna Gains D-1

Channels	D-2
IEEE 802.11a	D-2
IEEE 802.11b/g	D-3
Maximum Power Levels and Antenna Gains	D-4
IEEE 802.11a	D-4
IEEE 802.11b	D-4
IEEE 802.11g	D-5

APPENDIX E

Configuring the Client Adapter through the Windows XP Operating System E-1

Overview	E-2
Overview of Security Features	E-2
Static WEP Keys	E-2
EAP (with Dynamic WEP Keys)	E-3
WPA	E-4
Configuring the Client Adapter	E-5

Enabling EAP-TLS Authentication	E-10
Enabling PEAP Authentication	E-13
Enabling PEAP (EAP-MSCHAP V2)	E-14
Enabling PEAP (EAP-GTC)	E-16
Associating to an Access Point Using Windows XP	E-18
Viewing the Current Status of Your Client Adapter	E-18

APPENDIX F

Performing a Site Survey F-1

Overview	F-2
Guidelines	F-2
Additional Information	F-2
Opening the Site Survey Utility	F-3
Selecting the Client Adapter	F-3
Using the Associated AP Status Tab	F-4
Specifying Display Units	F-4
Viewing the Access Point's Status	F-5
Using the AP Scan List Tab	F-8
Viewing the AP Scan List	F-9
Pausing the AP Scan List	F-13
Viewing AP Details	F-13
Generating an AP Scan Log File	F-16
Viewing an Accumulation of Access Points	F-18
Using the Proximity Beeper	F-18
Configuring the Proximity Beeper	F-18
Enabling the Proximity Beeper	F-20
Using Thresholds	F-20
Configuring Threshold Values	F-20
Enabling Threshold Triggers	F-23
Entering a Comment in the Threshold Log File	F-24
Viewing the Threshold Log File	F-24
Deleting the Threshold Log File	F-25
Using AP Scanning	F-26
Configuring AP Scan Logging	F-26
Enabling AP Scan Logging	F-28
Viewing the AP Scan Log	F-28
Deleting the AP Scan Log	F-30
Saving the AP Scan List	F-30
Opening the AP Scan List	F-31

Viewing the Status Bar	F-32
Status Messages	F-32
Indicators	F-33
Resize Tab	F-33
Finding the Version of the Site Survey Utility	F-33
Accessing Online Help	F-33
Exiting the Site Survey Utility	F-34
Uninstalling the Site Survey Utility	F-34

APPENDIX G

Using the Profile Migration Tool	G-1
Overview of the Profile Migration Tool	G-2
Rules Governing Profile Migration	G-2
Installing the Profile Migration Tool	G-3
Running the Profile Migration Tool	G-4
Command Line Options	G-5
Uninstalling the Profile Migration Tool	G-7

GLOSSARY

INDEX



Preface

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

The following topics are covered in this section:

- [Audience, page xi](#)
- [Purpose, page xi](#)
- [Organization, page xii](#)
- [Conventions, page xii](#)
- [Related Publications, page xiv](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page xiv](#)

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 802.11 a, 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 físicos. 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, Obtaining Support, and Security Guidelines

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

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



CHAPTER 1

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, page 1-2](#)
- [Hardware Components, page 1-3](#)
- [Software Components, page 1-4](#)
- [Network Configurations Using Client Adapters, page 1-5](#)

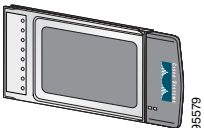
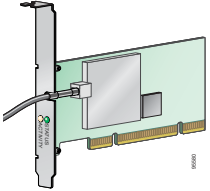
Introduction to the Client Adapters

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.



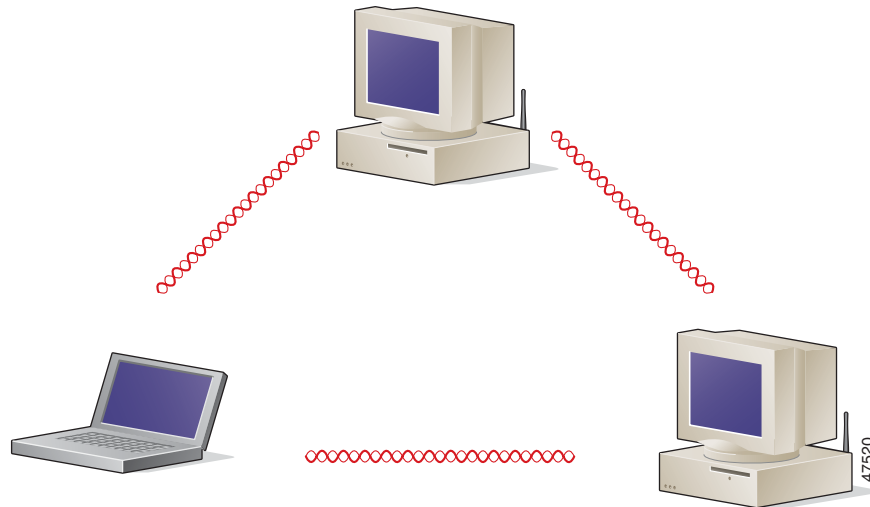
Note

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

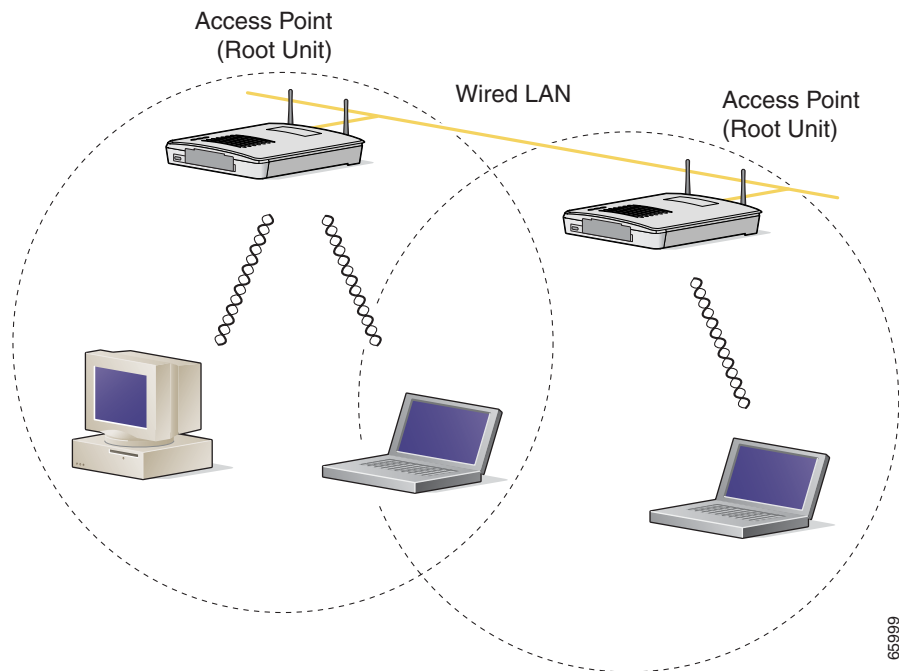


Wireless Infrastructure with Workstations Accessing a Wired LAN

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*





CHAPTER 2

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, page 2-2](#)
- [Unpacking the Client Adapter, page 2-3](#)
- [System Requirements, page 2-4](#)
- [Site Requirements, page 2-5](#)

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.



CHAPTER 3

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, page 3-2](#)
- [Installing the Client Adapter Software, page 3-9](#)
- [Installing the Intermediate Driver Manually, page 3-20](#)
- [Installing a Microsoft Hot Fix for Group Policy Delay, page 3-21](#)

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.

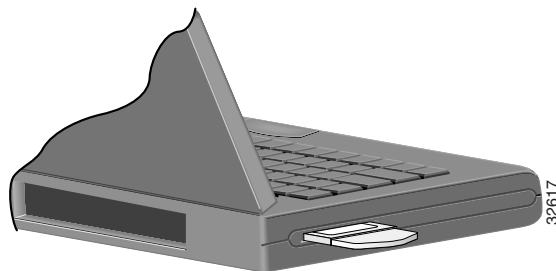
- Step 2** Turn on your computer and let the operating system boot up completely.

- 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:

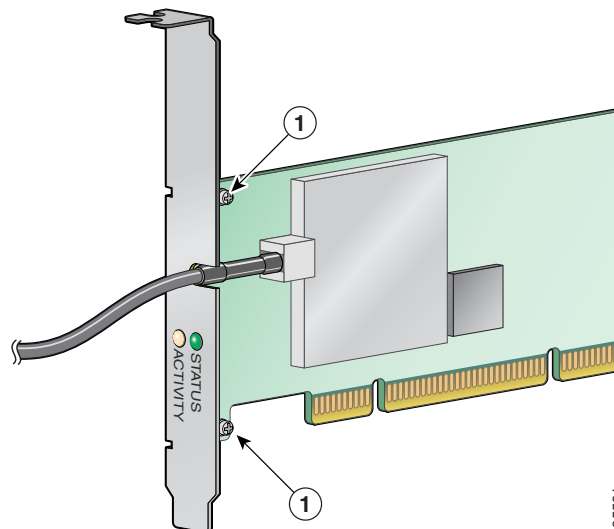
- Change the bracket (if required), see below
- Insert the card, [page 3-4](#)
- Assemble the antenna, [page 3-5](#)
- Mount the antenna, [page 3-6](#)

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.

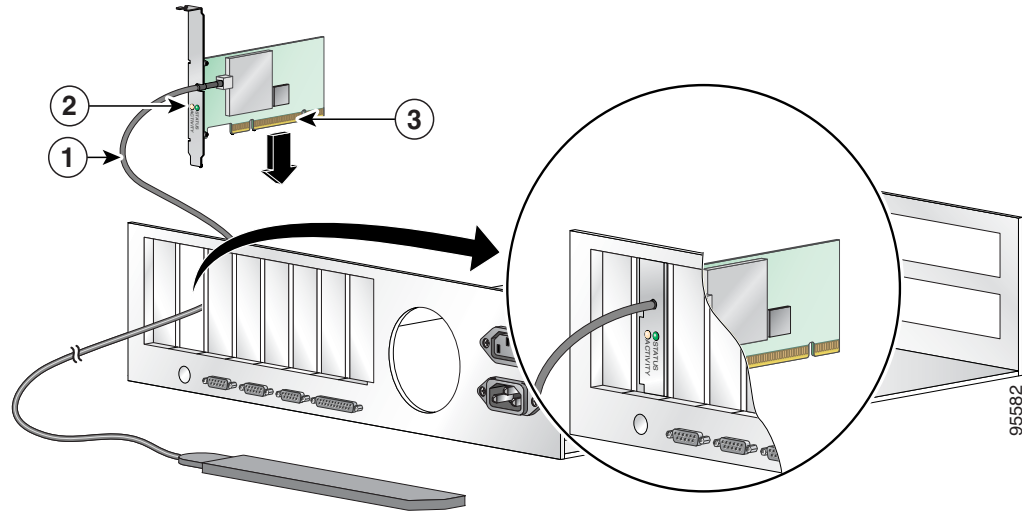
- Step 3** Remove the screw from the top of the CPU back panel above an empty PCI expansion slot. This screw holds the metal bracket on the back panel.

**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.

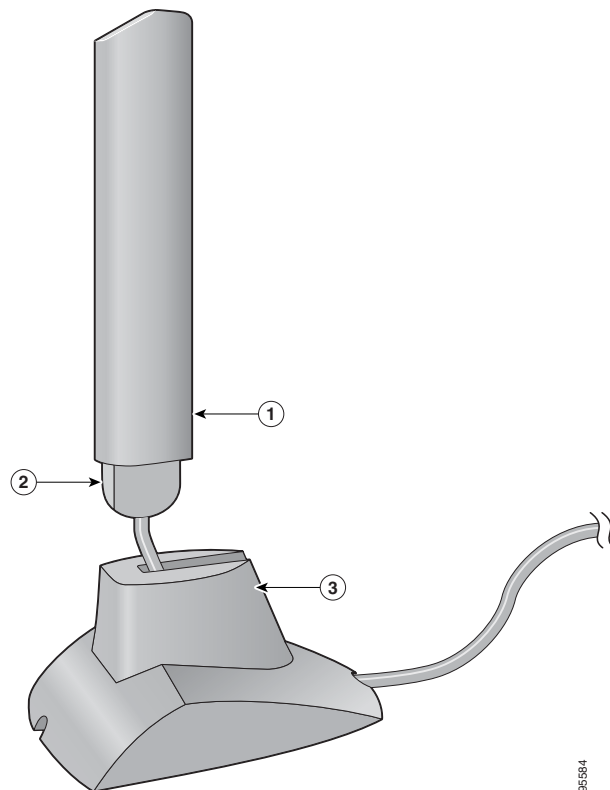
Step 8 Reinstall the screw on the CPU back panel and replace the computer cover.

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

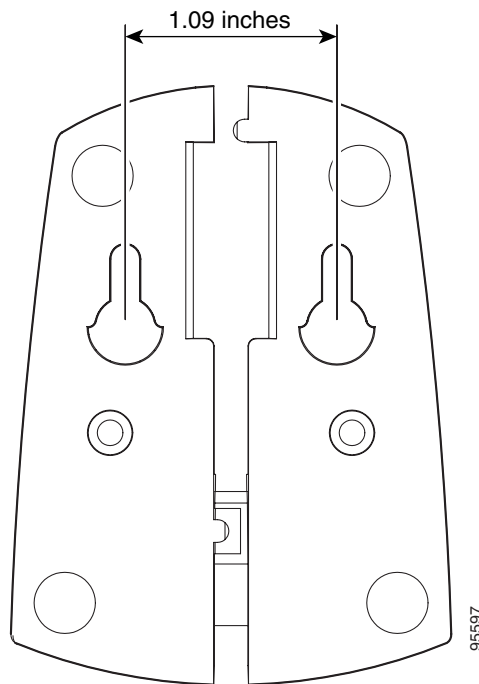
Because the PCI card is a radio device, it is susceptible to RF obstructions and common sources of interference that can reduce throughput and range. Follow these guidelines to ensure the best possible performance:

- 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.

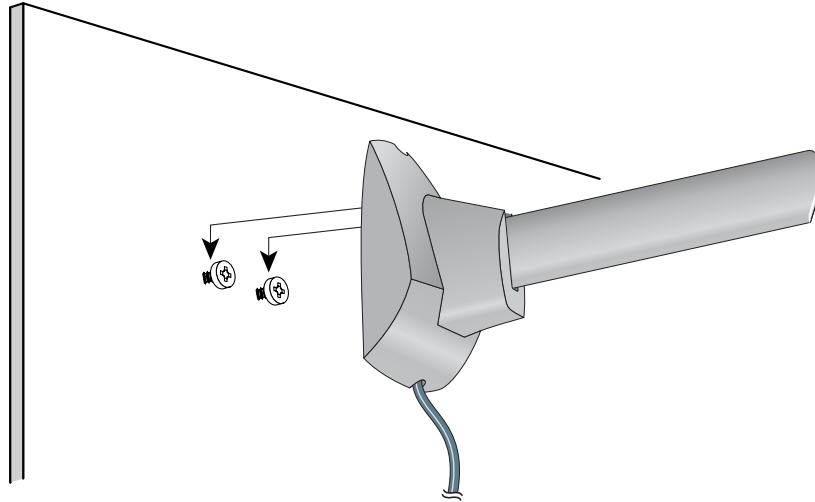
- Step 1** Perform one of the following:
- If you want to use the antenna on a flat horizontal surface, position the antenna so it is pointing straight up. Then go to [Step 7](#).
 - If you want to mount the antenna to a wall, go to [Step 2](#).
- Step 2** Drill two holes in the wall that are 1.09 in. (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*



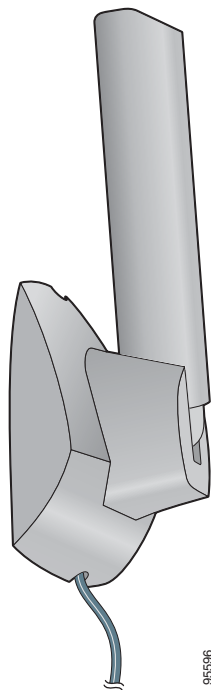
- Step 3** Tap the two supplied wall anchors into the holes.
- Step 4** Drive the two supplied screws into the wall anchors, leaving a small gap between the screw head and the anchor.
- Step 5** Position the mounting holes on the bottom of the antenna base over the screws (see [Figure 3-6](#)) and pull 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-vxx.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*

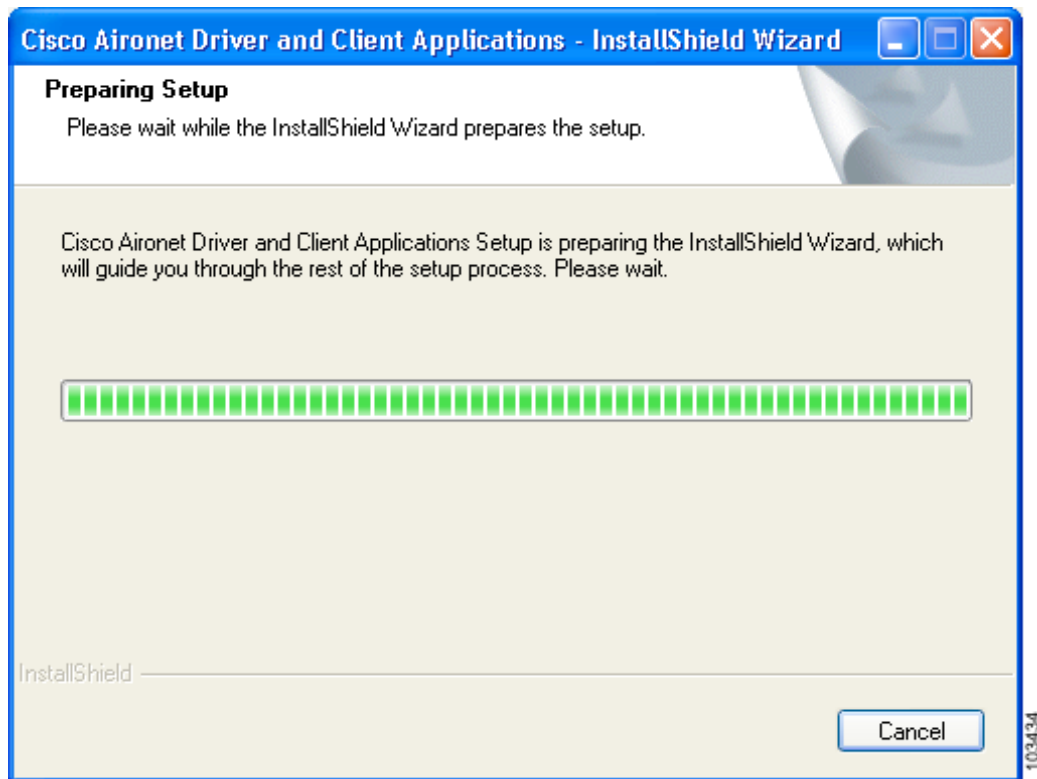
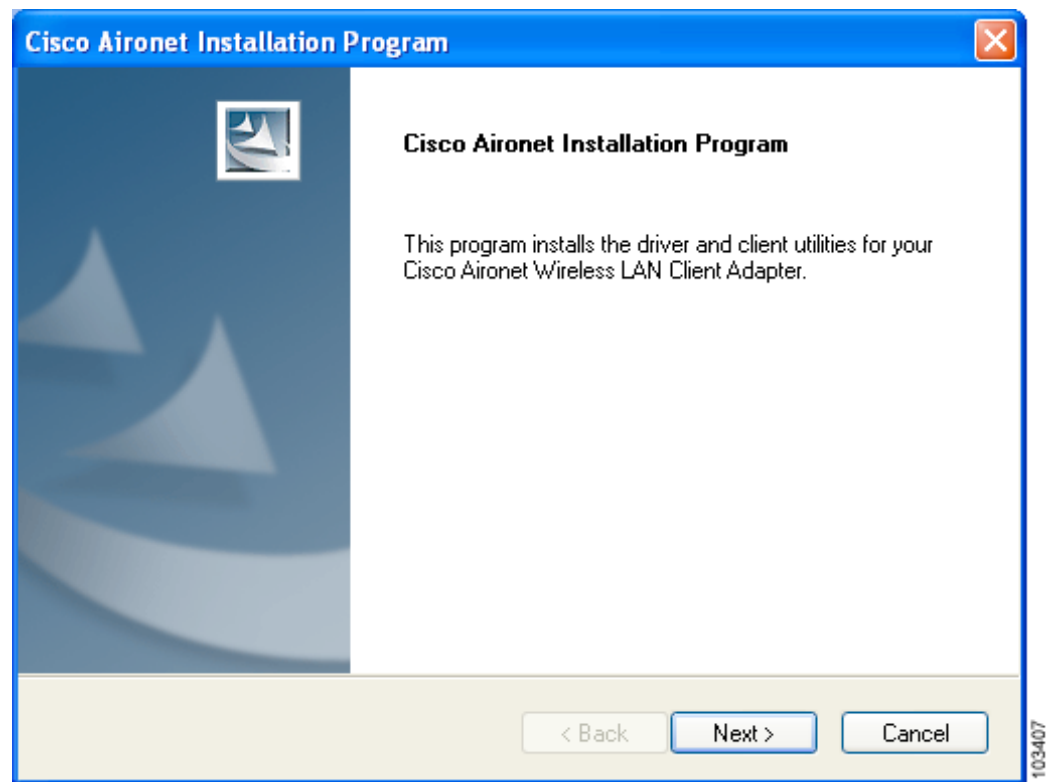
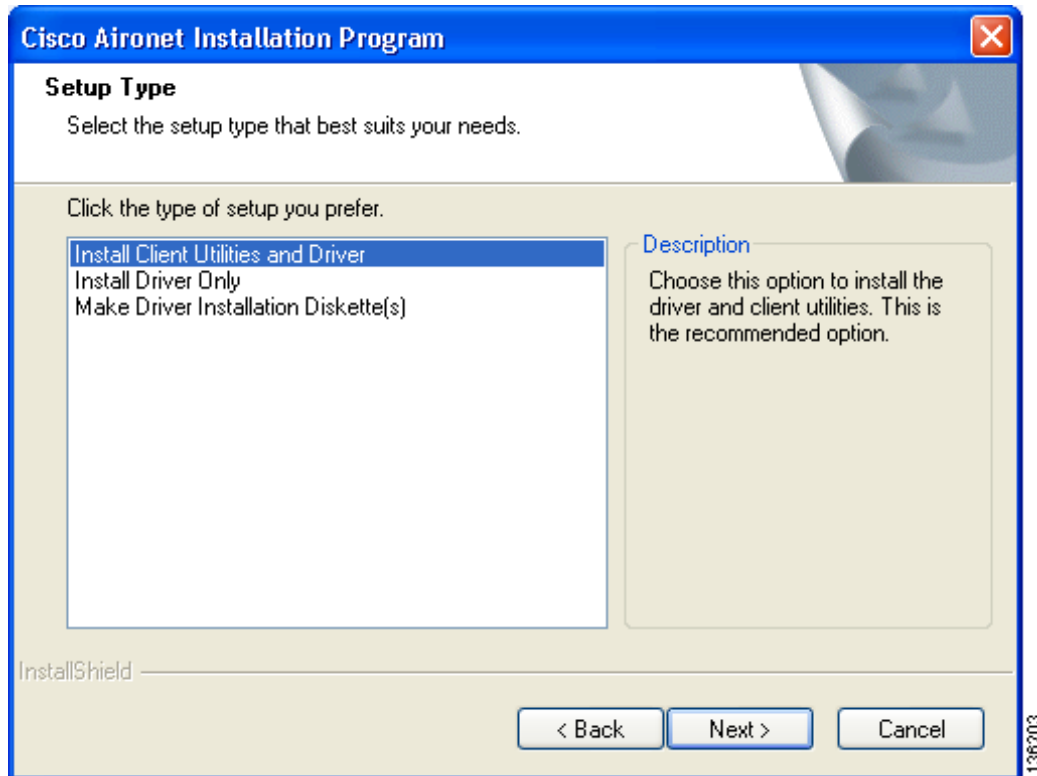


Figure 3-9 Cisco Aironet Installation Program Window



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.

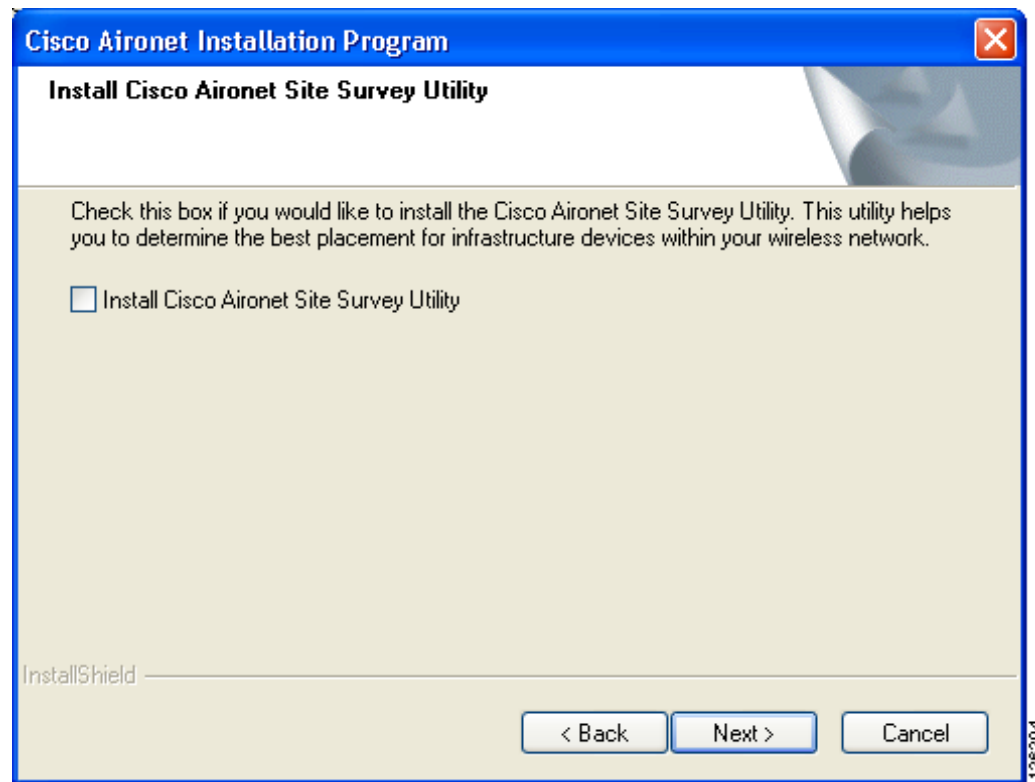
- **Install Client Utilities and Driver**—Installs the client adapter driver and client utilities.
- **Install Driver Only**—Installs only the client adapter driver. If you choose this option, click **Next** and go to [Step 32](#).
- **Make Driver Installation Diskette(s)**—Enables you to create driver 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.

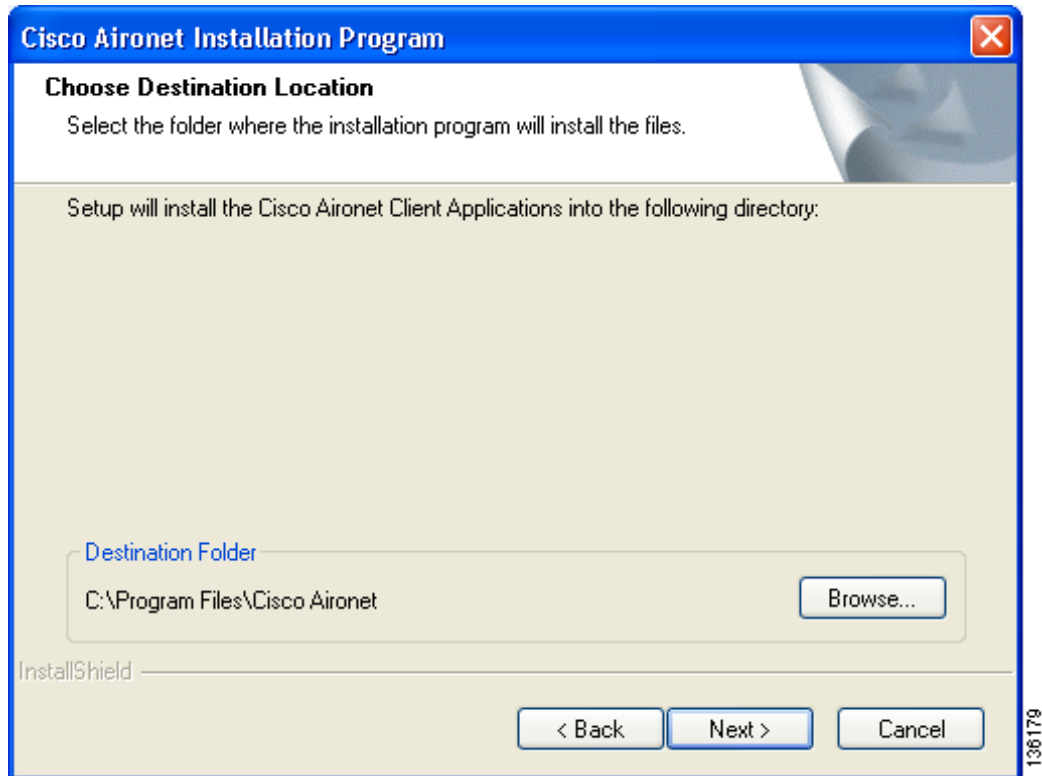
- Step 22** If a message appears indicating that you are required to restart your computer at the end of the installation process, click **Yes**.



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**.

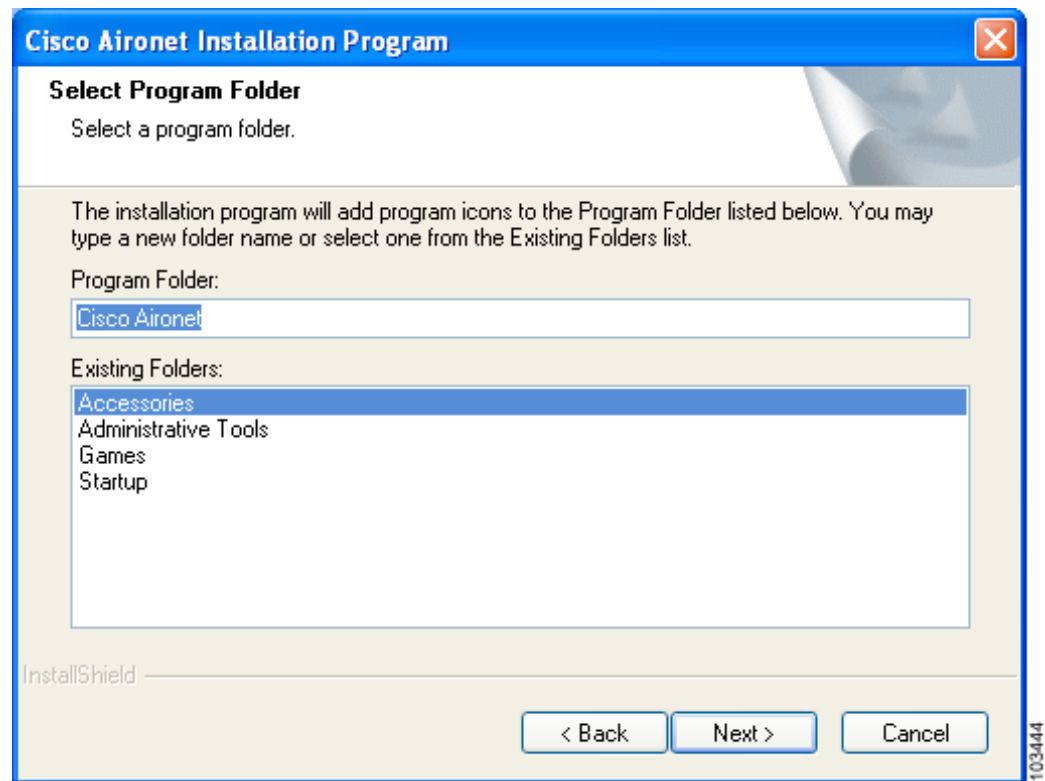
- If you chose the Make Driver Installation Diskette(s) option in [Step 20](#), insert a floppy disk into your computer and click **Next** to copy the driver to the diskette. Go to [Step 32](#).

**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.

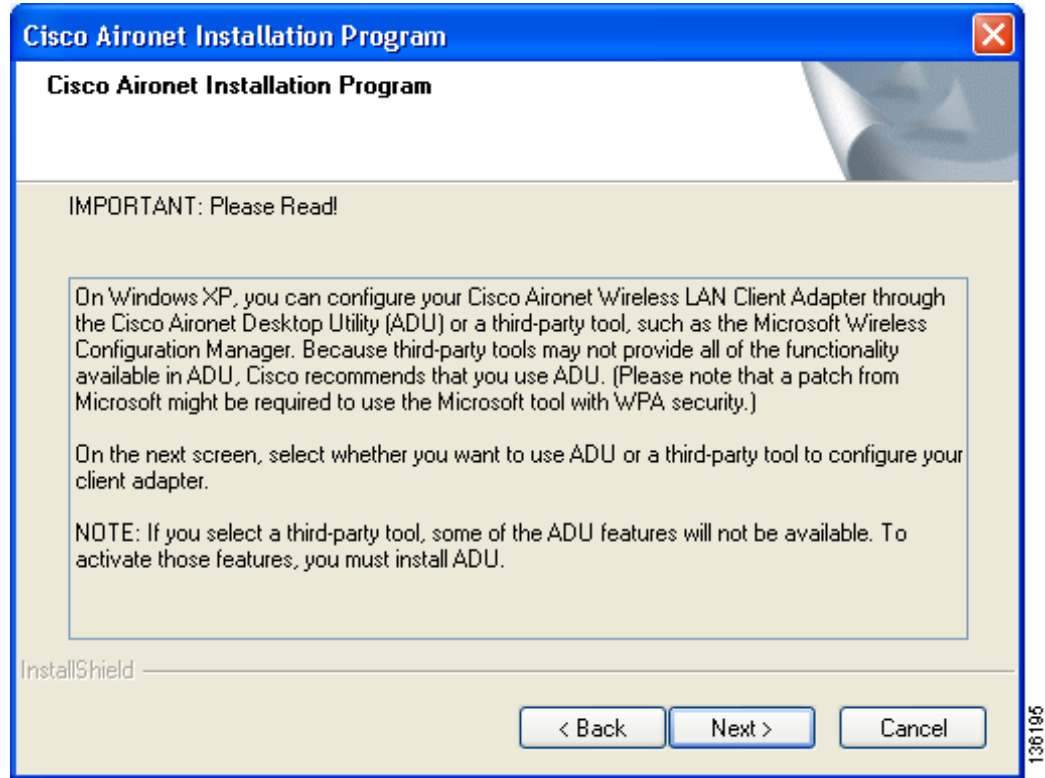


Note

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**.

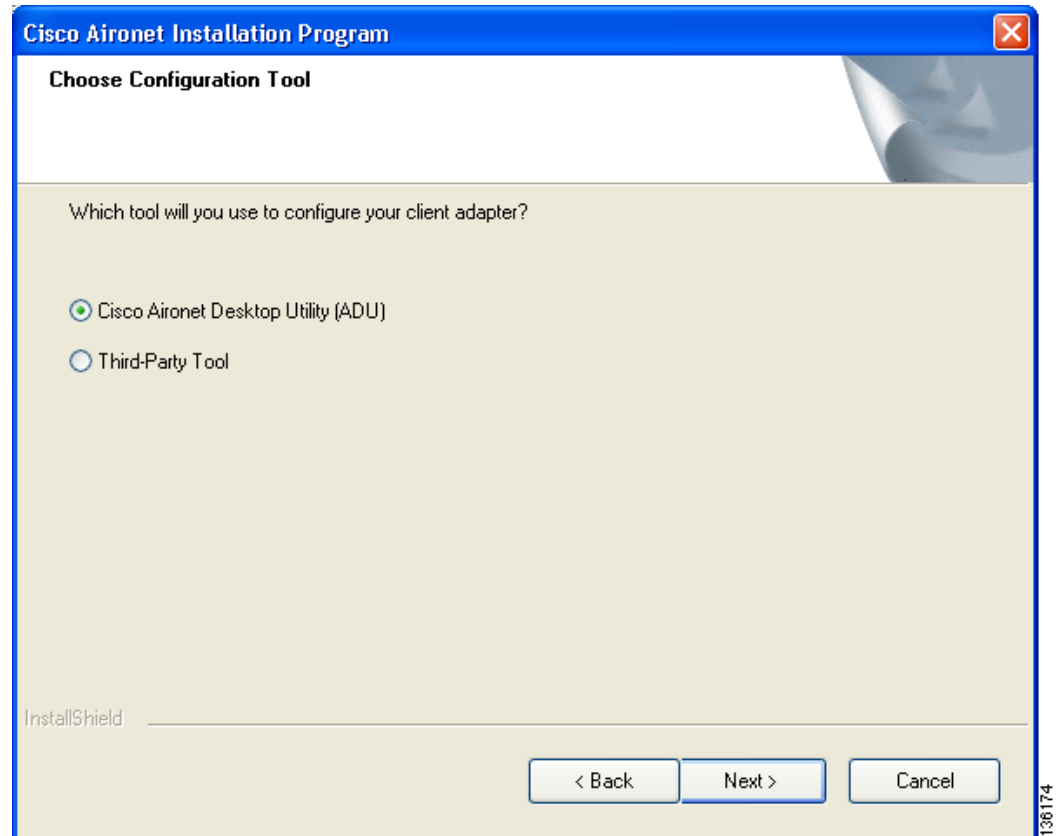
- Step 26** If your computer is running Windows 2000, go to [Step 32](#). If your computer is running Windows XP, the window titled **IMPORTANT: Please Read!** appears (see [Figure 3-14](#)).

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)

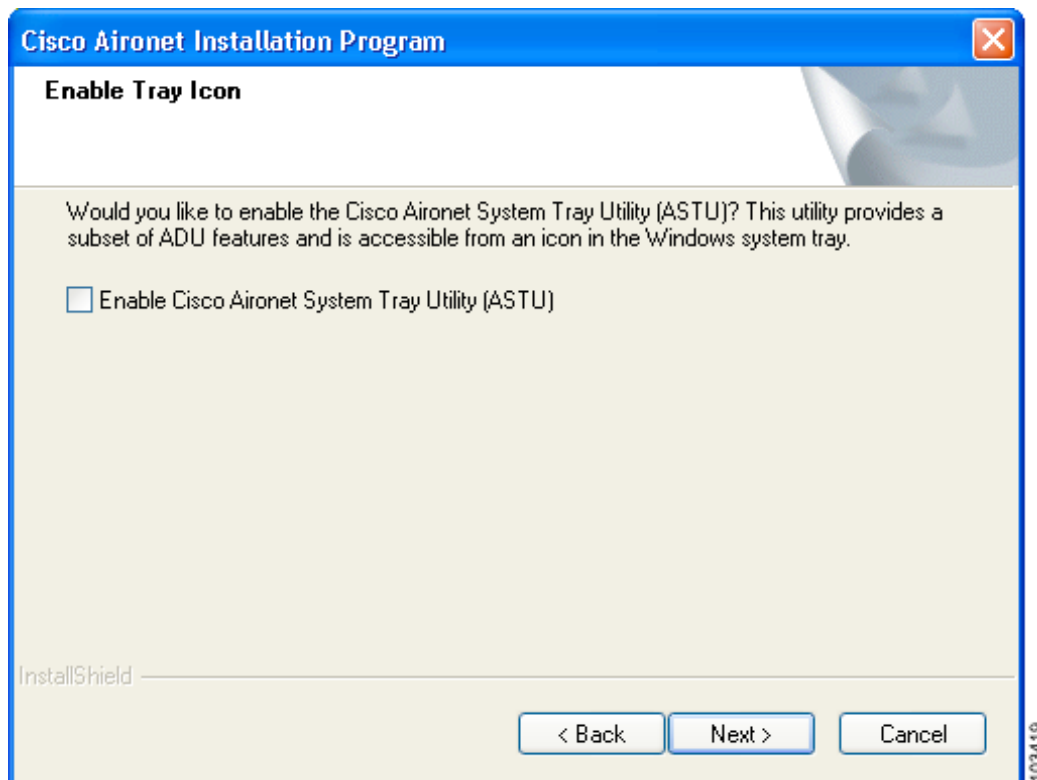
Feature	Windows XP	ADU
Security		
Static WEP	Yes	Yes
LEAP or EAP-FAST authentication with dynamic WEP	No	Yes
EAP-TLS or PEAP authentication	Yes	Yes
Status and statistics		
Status window	Limited	Extensive
Statistics window (transmit & receive)	No	Yes



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.

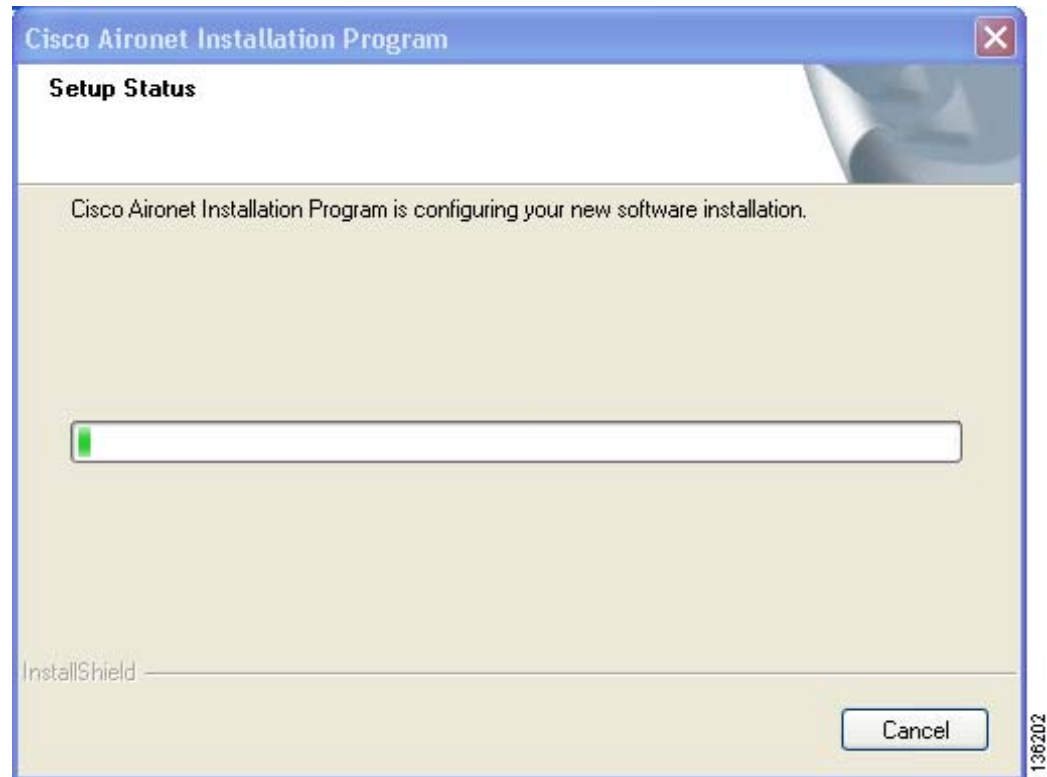
Step 29 Click **Next**.

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 CB21AG 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.
-



CHAPTER 4

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, page 4-2](#)
- [Opening Profile Manager, page 4-2](#)
- [Creating a New Profile, page 4-4](#)
- [Including a Profile in Auto Profile Selection, page 4-8](#)
- [Selecting the Active Profile, page 4-10](#)
- [Modifying a Profile, page 4-11](#)
- [Importing and Exporting Profiles, page 4-11](#)

Overview of Profile Manager

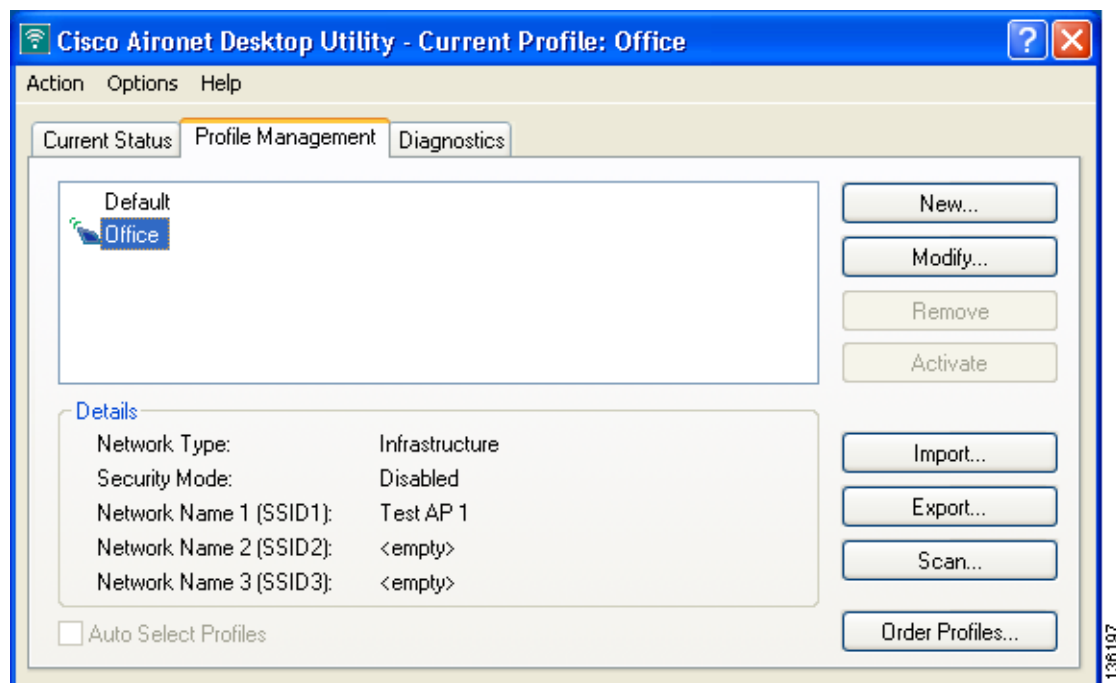
The ADU profile manager feature enables you to create and manage up to 16 *profiles* (saved configurations) for your client adapter. These profiles enable you to use your client adapter in different locations, each of which requires different configuration settings. For example, you may want to set up 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	<p>The type of network that is configured for the selected profile.</p> <p>Value: Infrastructure or Ad Hoc</p> <p>Note Refer to the Network Type parameter in Table 5-3 for instructions on setting the network type.</p>
Security Mode	<p>The type of security that is configured for the selected profile.</p> <p>Value: None, Pre-Shared Key, WPA/WPA2 Passphrase, LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), PEAP (EAP-MSCHAP V2), or Host Based EAP</p> <p>Note Refer to Chapter 5 for instructions on setting client adapter security.</p>
Network Name 1 (SSID1)	<p>The service set identifier (SSID) is the wireless network that is configured for the selected profile.</p> <p>Note Refer to the SSID1 parameter in Table 5-2 for instructions on setting SSID1.</p>
Network Name 2 (SSID2)	<p>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.</p> <p>Note Refer to the SSID2 parameter in Table 5-2 for instructions on setting SSID2.</p>
Network Name 3 (SSID3)	<p>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.</p> <p>Note Refer to the SSID3 parameter in Table 5-2 for instructions on setting SSID3.</p>

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

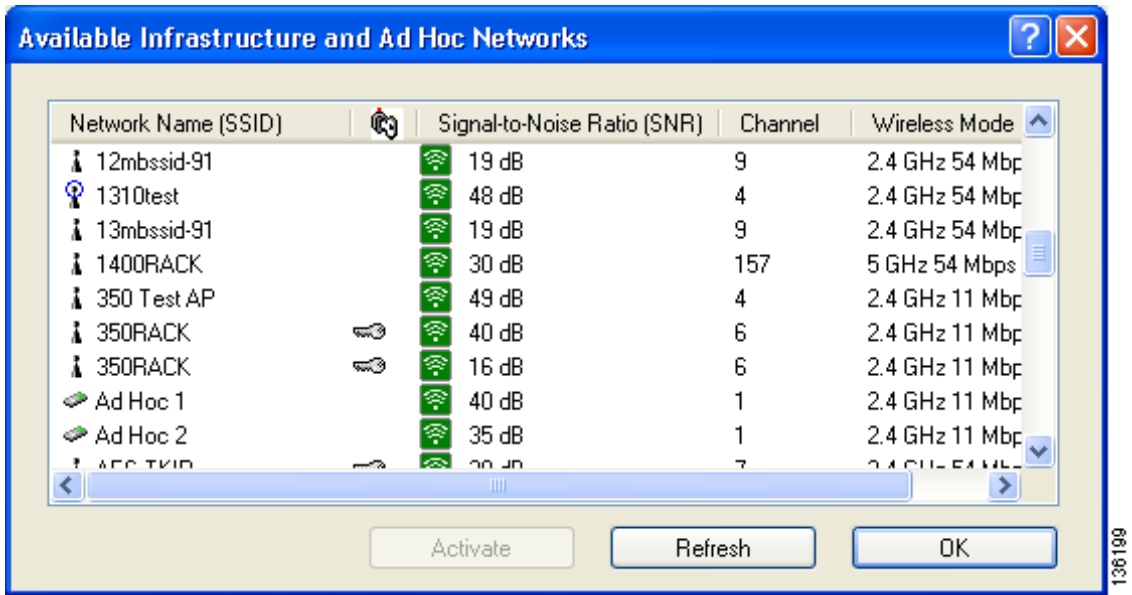
Follow the steps below to create a new profile.

- 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](#)).

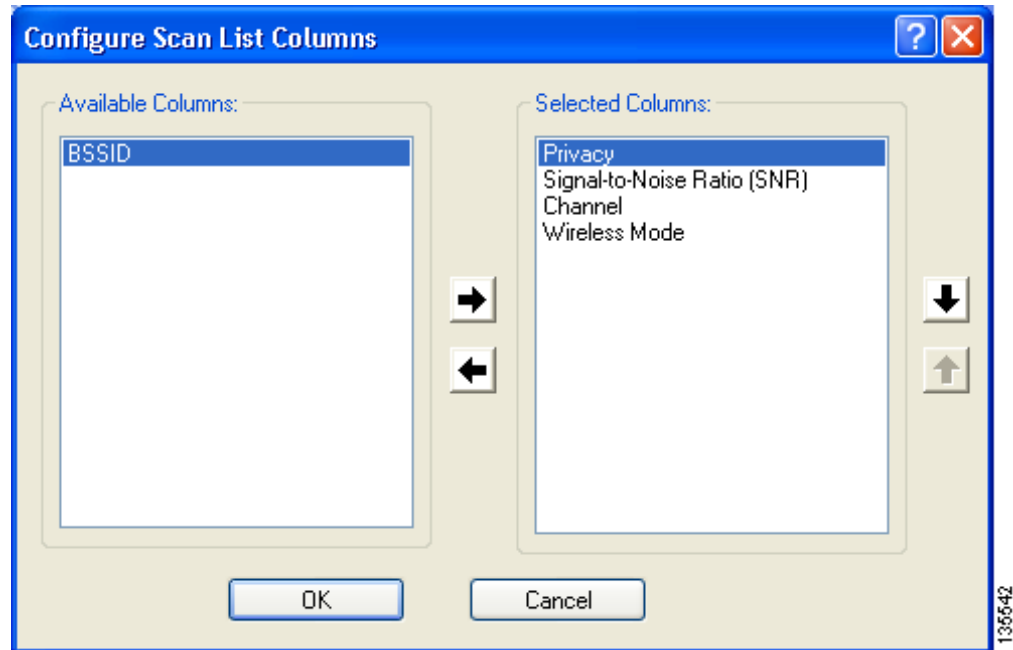
Figure 4-2 Available Infrastructure and Ad Hoc Networks Window



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)	<p>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.</p> <p>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).</p> <p>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.</p>
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.

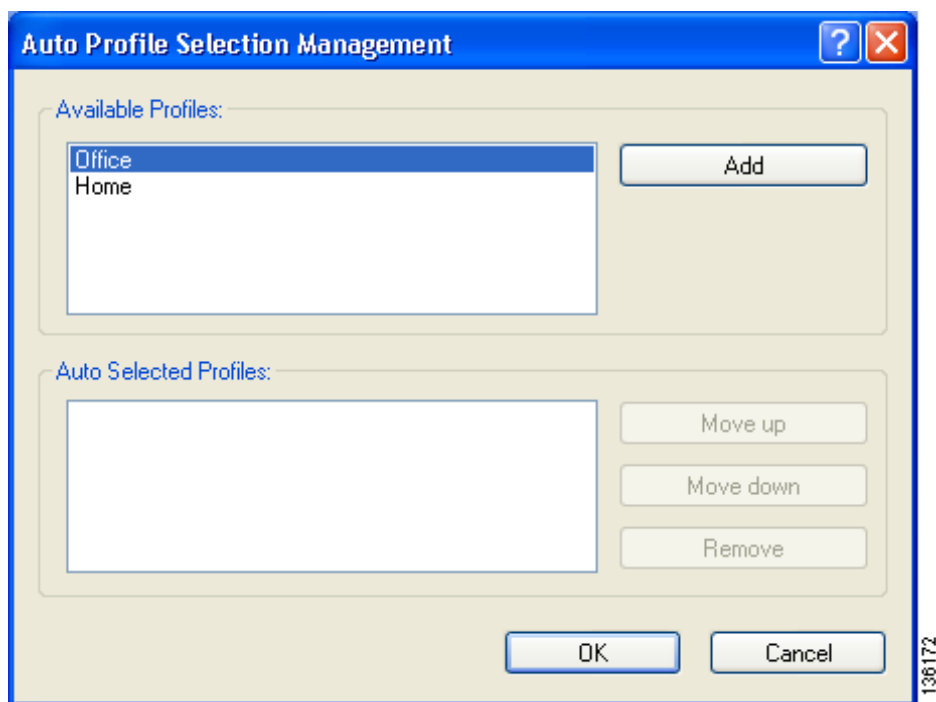
Including a Profile in Auto Profile Selection

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:

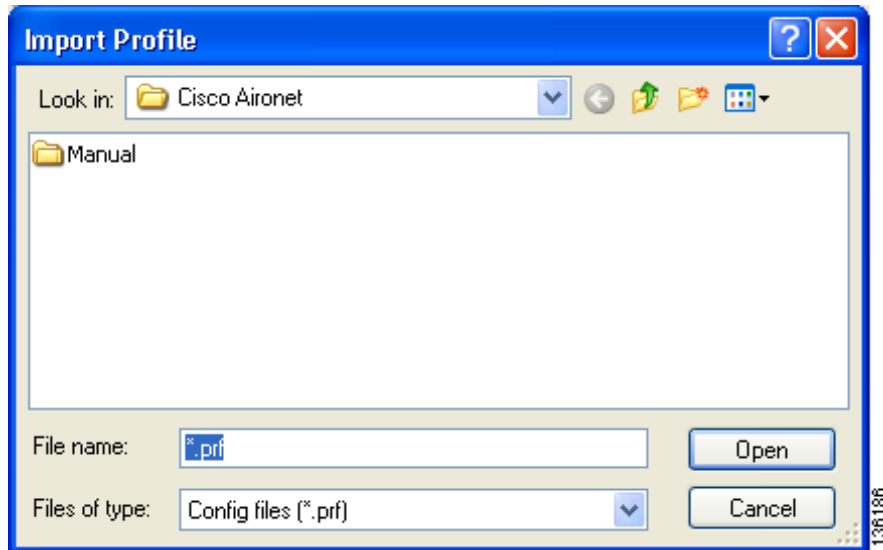
- To back up profiles before uninstalling client adapter software
- To export profiles for a PC-Cardbus card in one Cardbus slot and import them for use with a second Cardbus slot
- To set up your computer with a profile from another computer
- To export one of your profiles and use it to set up additional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

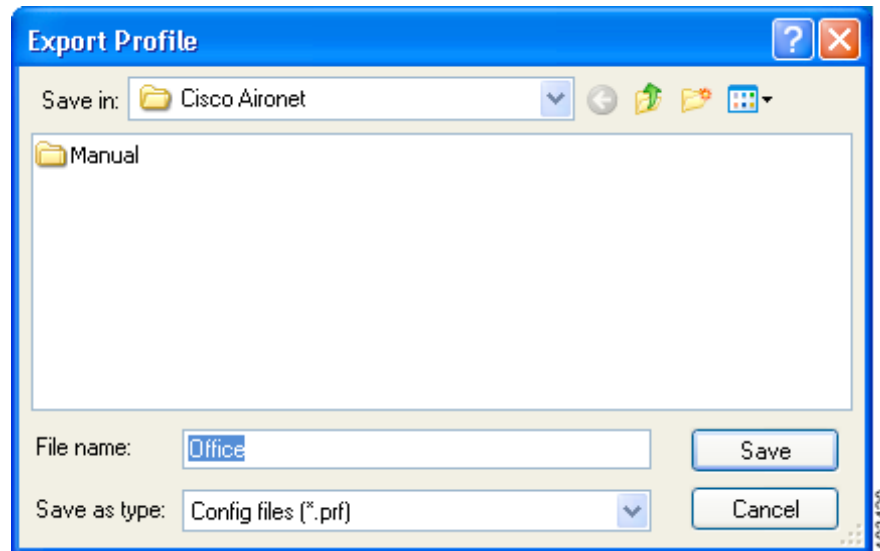


Note PACs are not exported with EAP-FAST profiles.

- 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.



CHAPTER 5

Configuring the Client Adapter

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

- [Overview, page 5-2](#)
- [Setting General Parameters, page 5-3](#)
- [Setting Advanced Parameters, page 5-6](#)
- [Setting Security Parameters, page 5-14](#)
- [Enabling Wi-Fi Multimedia, page 5-59](#)
- [Setting Roaming Parameters in the Windows Control Panel, page 5-63](#)

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	page 5-3
Advanced	page 5-6
Security	page 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”](#) section 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

The screenshot shows a window titled "Profile Management" with a blue title bar containing a help icon and a close button. Inside the window, there are three tabs: "General" (selected), "Security", and "Advanced". The "General" tab contains two sections: "Profile Settings" and "Network Names". The "Profile Settings" section has two text input fields labeled "Profile Name:" and "Client Name:". The "Network Names" section has three text input fields labeled "SSID1:", "SSID2:", and "SSID3:". At the bottom right of the window are "OK" and "Cancel" buttons. A vertical text label "136184" is visible on the right edge of the window frame.

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	<p>The name assigned to the configuration profile.</p> <p>Range: You can key in up to 32 ASCII characters.</p> <p>Default: A blank field</p>
Client Name	<p>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.</p> <p>Range: You can key in up to 16 ASCII characters.</p> <p>Default: The name of your computer</p> <p>Note Each computer on the network should have a unique client name.</p>
SSID1	<p>The service set identifier (SSID) identifies the specific wireless network that you want the client adapter to access.</p> <p>Range: You can key in up to 32 ASCII characters (case sensitive).</p> <p>Default: A blank field</p> <p>Note If you leave this parameter blank, your client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs. If the access point with which the client adapter is to communicate is not configured to allow broadcast SSIDs, the value of this parameter must match the SSID of the access point. Otherwise, the client adapter is unable to access the network.</p> <p>Note You must enter an SSID if this profile is configured for use in an ad hoc network.</p>

Table 5-2 **Profile Management General Parameters (continued)**

Parameter	Description
SSID2	<p>An optional SSID that identifies a second distinct network and enables the client adapter to roam to that network without having to be reconfigured.</p> <p>Range: You can key in up to 32 ASCII characters (case sensitive).</p> <p>Default: A blank field</p> <p>Note If a profile specifies more than one SSID, it cannot be included in auto profile selection or used with WPA/WPA2 passphrase.</p> <p>Note This field is unavailable for any profiles that are included in auto profile selection or configured for use in an ad hoc network.</p>
SSID3	<p>An optional SSID that identifies a third distinct network and enables the client adapter to roam to that network without having to be reconfigured.</p> <p>Range: You can key in up to 32 ASCII characters (case sensitive).</p> <p>Default: A blank field</p> <p>Note If a profile specifies more than one SSID, it cannot be included in auto profile selection or used with WPA/WPA2 passphrase.</p> <p>Note This field is unavailable for any profiles that are included in auto profile selection or configured for use in an ad hoc network.</p>

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

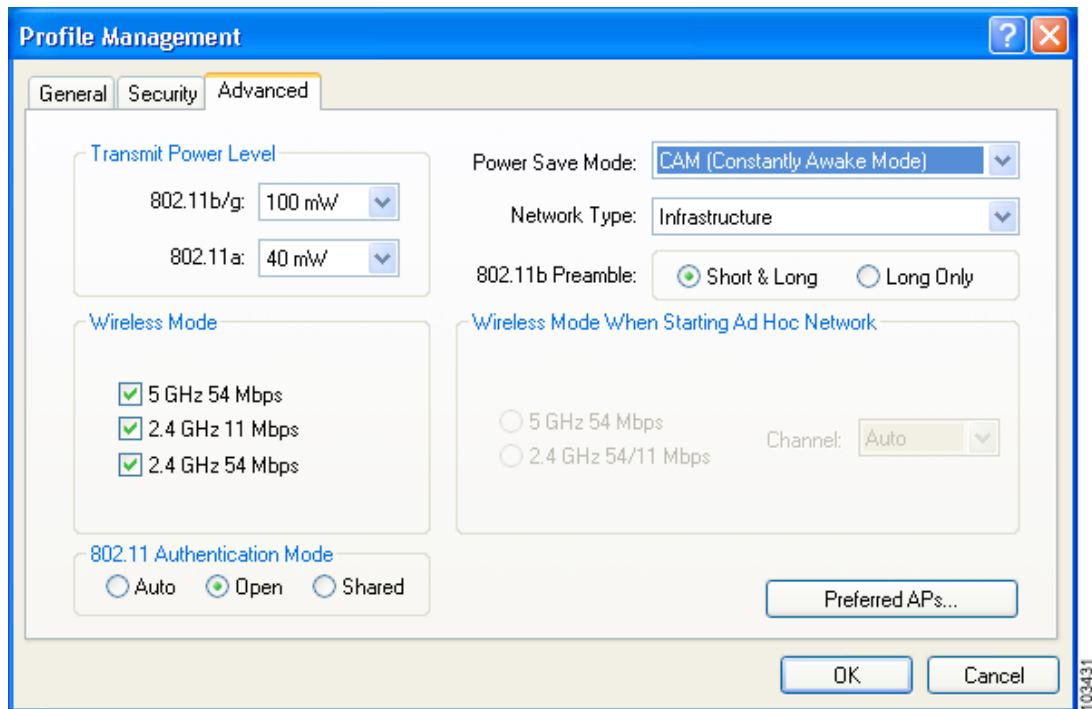


Table 5-3 lists and describes the client adapter's advanced parameters. Follow the instructions in the table to change any parameters.

Table 5-3 Profile Management Advanced Parameters

Parameter	Description						
Transmit Power Level	<p>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.).</p> <p>Options: Dependent on the radio band used and the power table programmed into the client adapter; see the table below.</p> <p>Default: The maximum power level programmed into the client adapter and allowed by your country's regulatory agency</p> <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> <p>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.</p> <p>Note Reducing the transmit power level conserves battery power but decreases radio range.</p> <p>Note If configured to control the client power level, access points can limit the maximum power of the client.</p>	Radio Band	Transmit Power Level	802.11b/g	10, 20, 32, 50, 63, or 100 mW	802.11a	10, 13, 20, 25, or 40 mW
Radio Band	Transmit Power Level						
802.11b/g	10, 20, 32, 50, 63, or 100 mW						
802.11a	10, 13, 20, 25, or 40 mW						

Table 5-3 *Profile Management Advanced Parameters (continued)*

Parameter	Description
Power Save Mode	<p>Sets your client adapter to its optimum power consumption setting.</p> <p>Options: CAM (Constantly Awake Mode), Fast PSP (Power Save Mode), or Max PSP (Max Power Saving)</p> <p>Default: CAM (Constantly Awake Mode)</p>
Power Save Mode	Description
CAM (Constantly Awake Mode)	<p>Keeps the client adapter powered up continuously so there is little lag in message response time.</p> <p>Consumes the most power but offers the highest throughput. Is recommended for desktop computers and devices that use AC power.</p>
Fast PSP (Power Save Mode)	<p>Switches between PSP mode and CAM mode, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets have been retrieved.</p> <p>Is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP.</p>
Max PSP (Max Power Saving)	<p>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.</p> <p>Conserves the most power but offers the lowest throughput. Is recommended for devices for which power consumption is the ultimate concern (such as small battery-powered devices).</p>
Note	If this profile is configured for use in an ad hoc network, CAM mode is used automatically.

Table 5-3 **Profile Management Advanced Parameters (continued)**

Parameter	Description	
Network Type	Specifies the type of network in which your client adapter is installed. Options: Infrastructure or Ad Hoc Default: Infrastructure	
	Network Type	Description
	Ad Hoc	Often referred to as <i>peer to peer</i> . Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point. For example, an ad hoc network could be set up between computers in a conference room so that users can share information in a meeting.
	Infrastructure	Indicates that your wireless network is connected to a wired Ethernet network through an access point.
802.11b Preamble	<p>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 <i>all</i> clients in that cell must use long headers, even if both this client and the access point have short radio headers enabled.</p> <p>Short radio headers improve throughput performance; long radio headers ensure compatibility with clients and access points that do not support short radio headers.</p> <p>Options: Short & Long or Long Only Default: Short & Long</p> <p>Note This parameter is disabled if the Wireless Mode parameter does not include the 2.4 GHz 11 Mbps option.</p>	

Table 5-3 *Profile Management Advanced Parameters (continued)*

Parameter	Description
Wireless Mode	<p>Specifies the frequency and rate at which your client adapter should transmit packets to or receive packets from access points.</p> <p>Options: 5 GHz 54 Mbps, 2.4 GHz 54 Mbps, and 2.4 GHz 11 Mbps</p> <p>Default: All options selected</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Wireless Mode When Starting Ad Hoc Network	<p>Specifies the frequency and rate at which your client adapter should transmit packets to or receive packets from other clients (in ad hoc mode).</p> <p>Options: 5 GHz 54 Mbps, 2.4 GHz 11 Mbps, or 2.4 GHz 54 Mbps</p> <p>Default: 5 GHz 54 Mbps</p> <p>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.</p> <p>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.</p> <p>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.</p>

Table 5-3 **Profile Management Advanced Parameters (continued)**

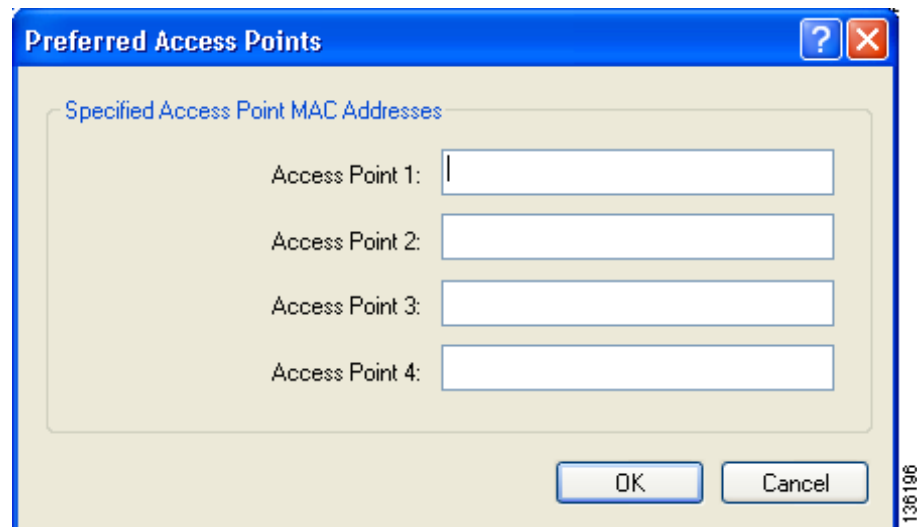
Parameter	Description
Channel	<p>Specifies the channel that your client adapter uses for communications in a 2.4-GHz ad hoc network. The available channels conform to the IEEE 802.11 Standard for your regulatory domain.</p> <p>The channel of the client adapter must be set to match the channel used by 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.</p> <p>Range: Dependent on regulatory domain Example: 1 to 11 (2412 to 2462 MHz) in North America</p> <p>Default: Auto (the client automatically determines the channel on which to start communications)</p> <p>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.</p> <p>Note Refer to Appendix D for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.</p>

Table 5-3 *Profile Management Advanced Parameters (continued)*

Parameter	Description								
802.11 Authentication Mode	<p>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.</p> <p>Options: Auto, Open, or Shared</p> <p>Default: Open</p> <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> <p>Enables your client adapter to authenticate and communicate only with access points that have the same WEP key.</p> <p>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.</p> </td></tr> </table> <p>Note Cisco recommends that Auto and Shared not be used because they present a security risk.</p> <p>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.</p> <p>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.</p>	802.11 Authentication Mode	Description	Auto	Causes the client adapter to attempt to authenticate using shared authentication. If it fails, the client adapter then attempts to authenticate using open authentication.	Open	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.	Shared	<p>Enables your client adapter to authenticate and communicate only with access points that have the same WEP key.</p> <p>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.</p>
802.11 Authentication Mode	Description								
Auto	Causes the client adapter to attempt to authenticate using shared authentication. If it fails, the client adapter then attempts to authenticate using open authentication.								
Open	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.								
Shared	<p>Enables your client adapter to authenticate and communicate only with access points that have the same WEP key.</p> <p>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.</p>								

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



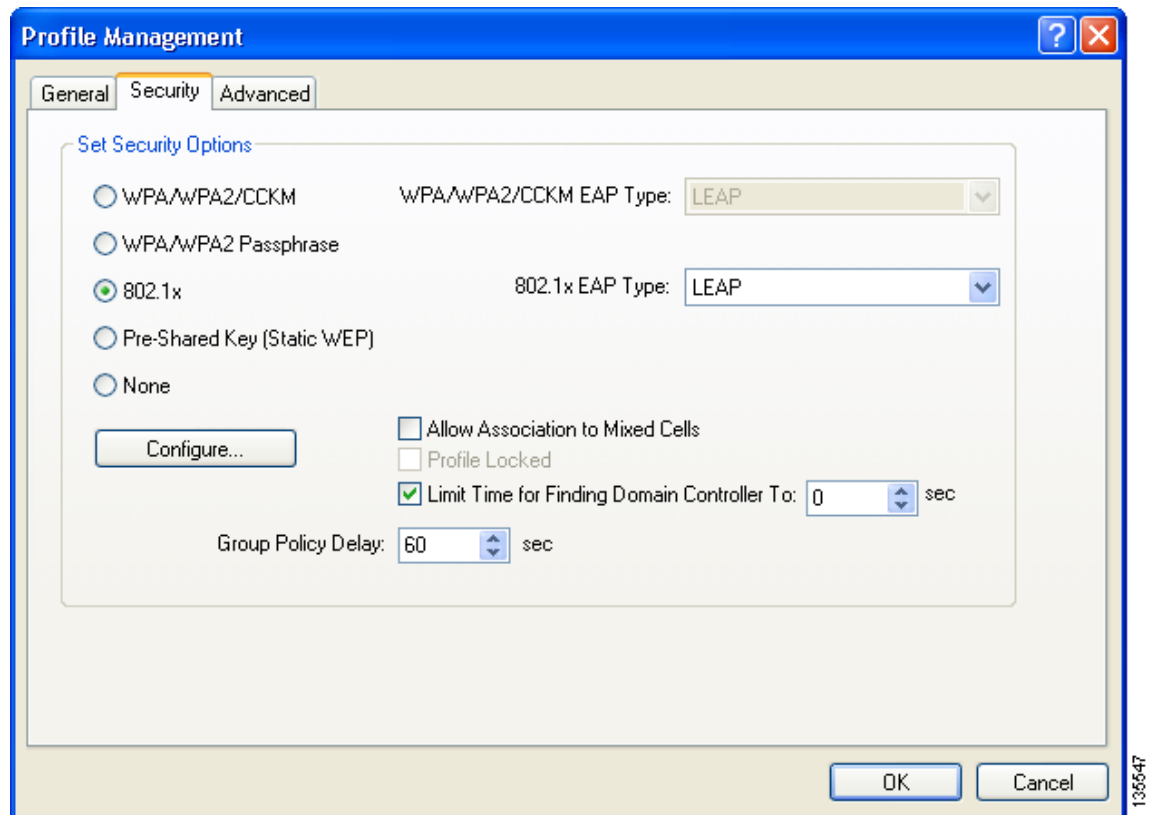
Leave the Access Point 1 through Access Point 4 fields blank or enter the MAC addresses of up to four preferred access points to which the client adapter can associate; then click **OK**. (The MAC address should consist of 12 hexadecimal characters.) If the specified access points are not found or the 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](#)” section on page 5-20 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](#)” section 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 experience 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 5-21](#) 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

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

Security Feature	Client Setting	Access Point Setting
LEAP authentication with WPA or WPA2	Choose WPA/WPA2/CCKM and LEAP; then set LEAP settings	<p>For WPA, choose a cipher suite that includes TKIP and enable Network-EAP and Open with EAP Authentication and WPA for the SSID</p> <p>For WPA2, choose a cipher suite that includes AES-CCMP and enable Network-EAP and Open with EAP Authentication and WPA for the SSID</p> <p>Note To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.</p>

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	<p>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</p> <p>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</p> <p>Note To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.</p>
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	<p>For WPA, choose a cipher suite that includes TKIP; then enable WPA and Open with EAP Authentication for the SSID</p> <p>For WPA2, choose a cipher suite that includes AES-CCMP; then enable WPA and Open with EAP Authentication for the SSID</p> <p>Note To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.</p>

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)*

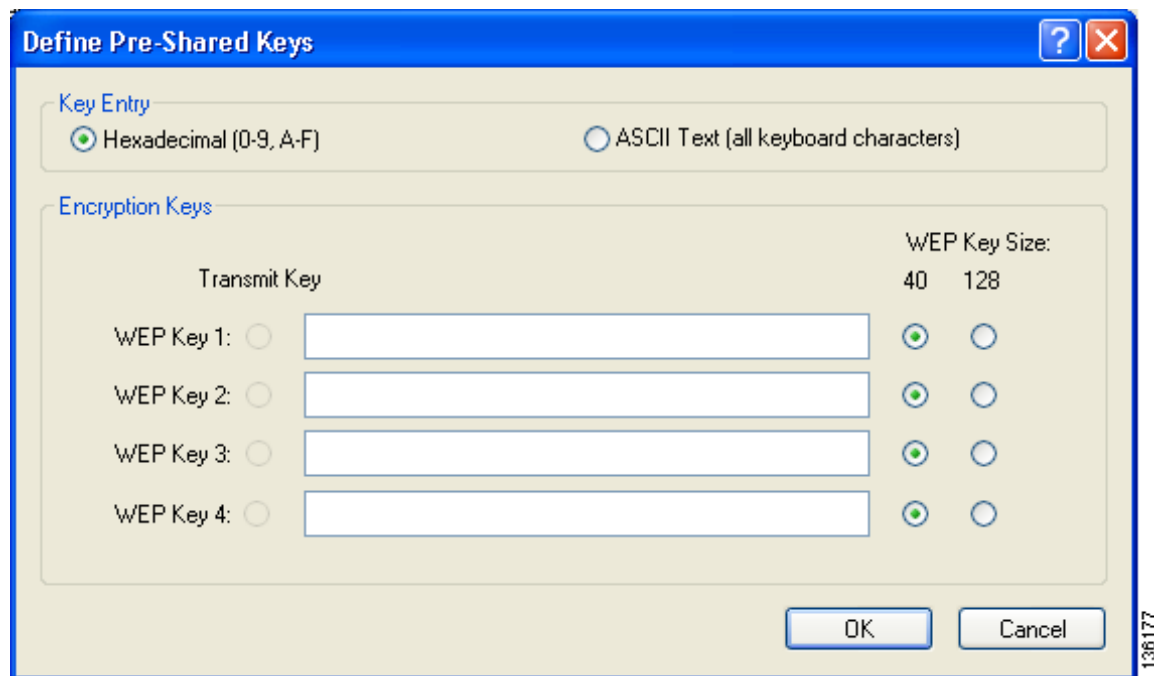
Security Feature	Client Setting	Access Point Setting
CCKM fast secure roaming	<p>Choose WPA/WPA2/CCKM and LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), or PEAP (EAP-MSCHAP V2); then set the EAP authentication settings</p> <p>Note If you want to enable CCKM, you must choose WPA/WPA2/CCKM, regardless of whether 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.</p>	<p>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)</p> <p>Note To allow both 802.1X clients and non-802.1X clients to use the SSID, enable optional CCKM.</p>
Reporting access points that fail LEAP authentication	No settings required; automatically enabled	No settings required; automatically enabled in the firmware versions listed on page 5-19 .
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

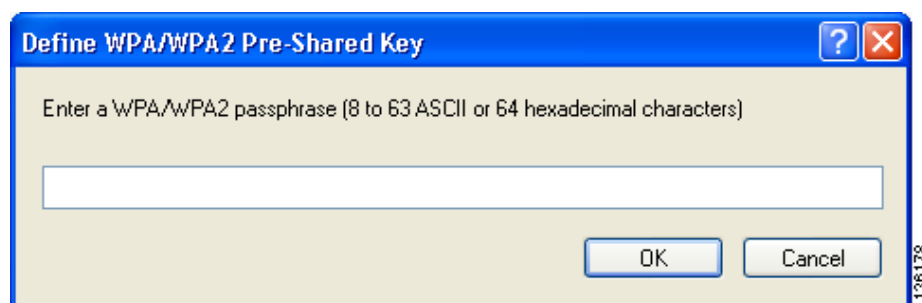
Follow the steps below to enable WPA/WPA2 passphrase (also known as *WPA/WPA2 pre-shared key*) for this profile.

**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”](#) section 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 5-21](#).

- 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.



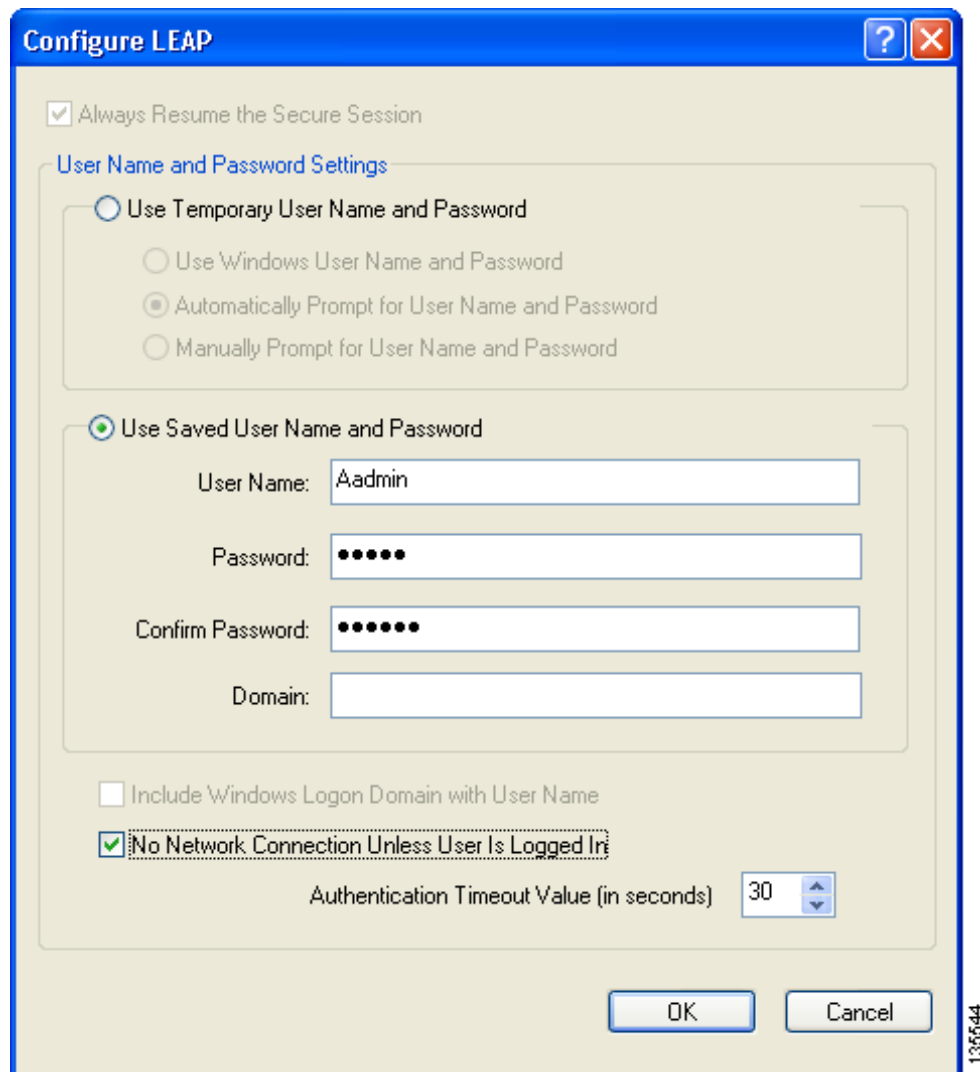
Note If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which your client adapter associates determines whether CCKM will be used with 802.1x, WPA,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



Note Refer to the [“WPA and WPA2”](#) section on [page 5-18](#) 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”](#) section 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 5-19](#).

**Note**

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

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

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

Step 1

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

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

**Note**

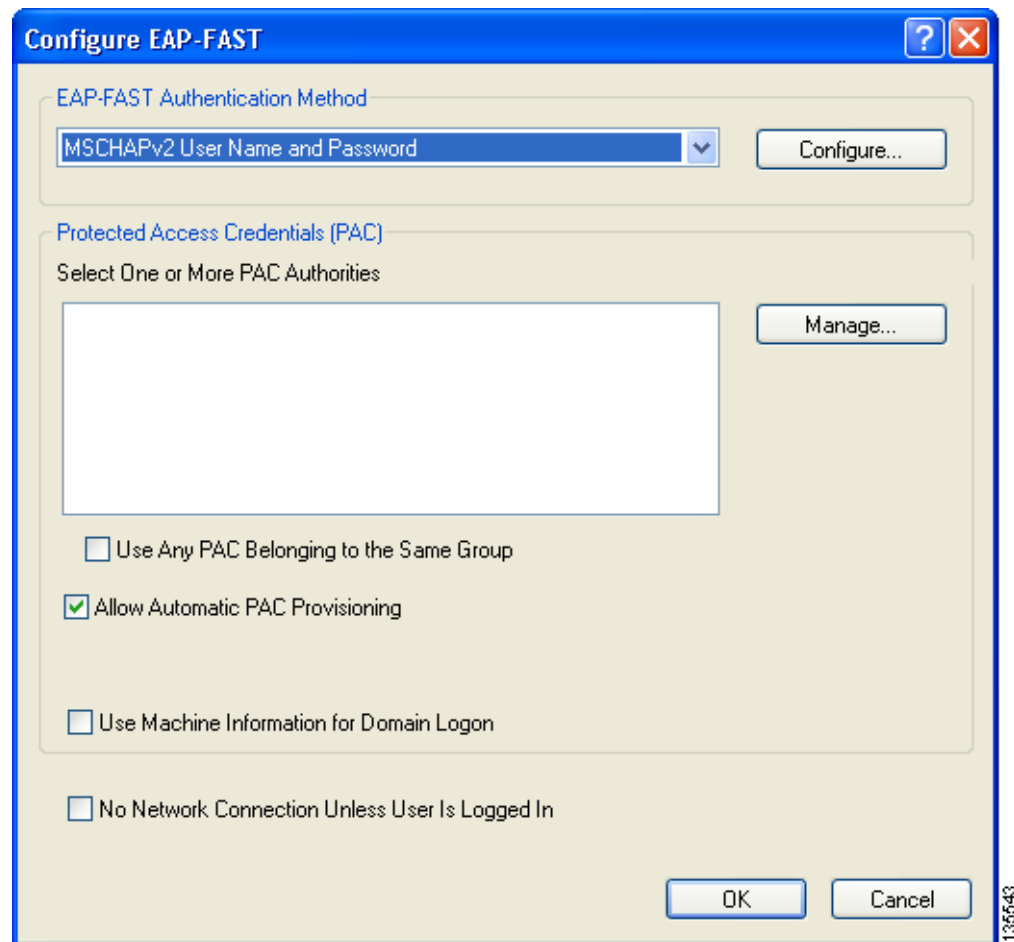
If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which your client adapter associates determines whether CCKM will be used with 802.1x, WPA, or WPA2.

**Note**

Refer to the [“WPA and WPA2”](#) section on [page 5-18](#) for additional information.

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

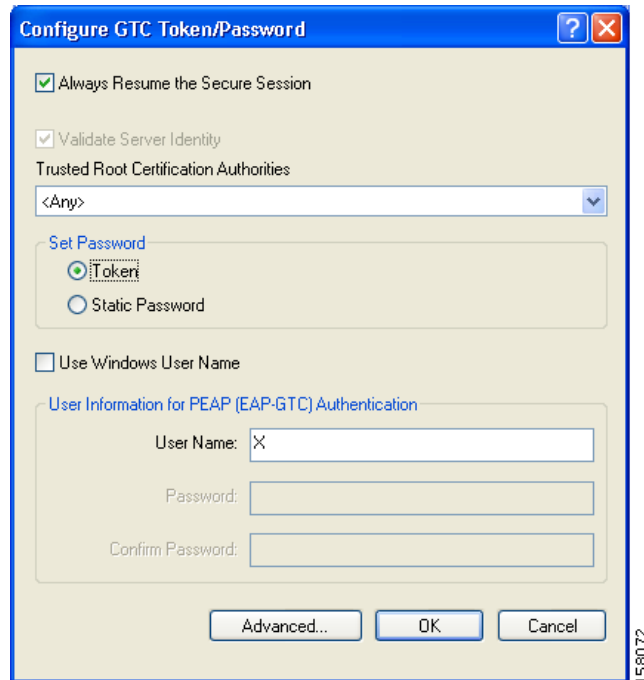
Figure 5-8 *Configure EAP-FAST Window*



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**.

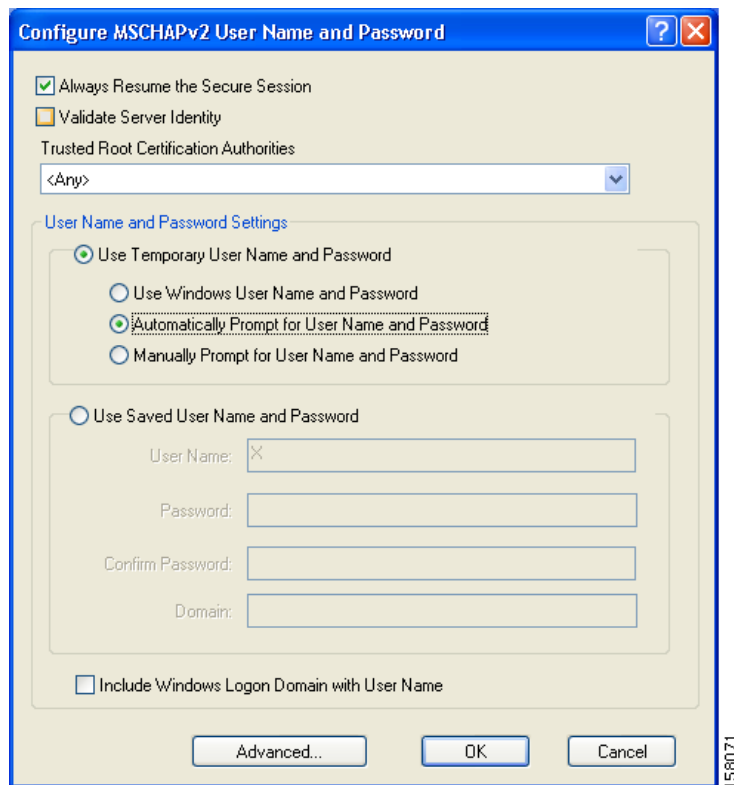
2. Check the **Validate Server Identity** check box to force the system to validate the identity of the server as an added level of security.

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)” section 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.

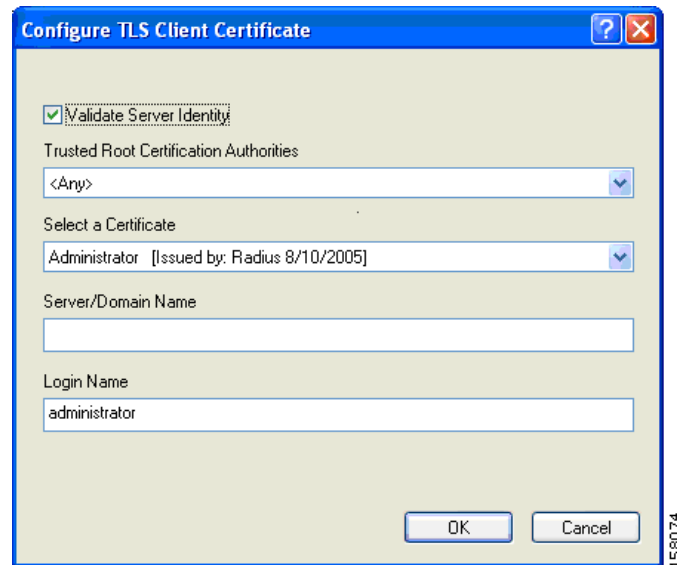

Note

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” section 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](#)” section 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.

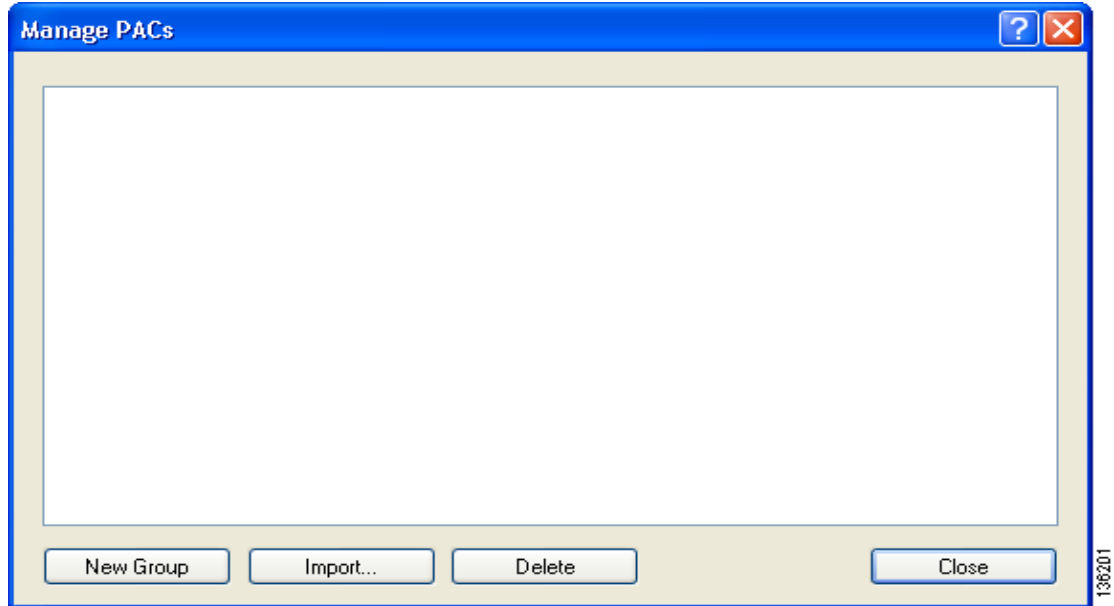


Note

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.

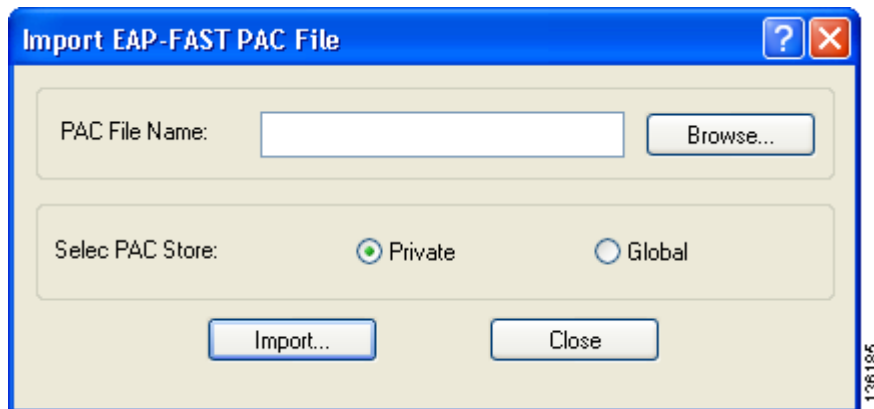
- Step 8** If necessary, follow these steps to import or modify the grouping of PAC files:
- Click **Manage**. The Manage PACs window appears (see [Figure 5-12](#)).

Figure 5-12 *Manage PACs Window*



- To create a new group, click **New Group**.
- To move a PAC from one group to another, just drag it to the destination group.
- Click **Import**. The Import EAP-FAST PAC File window appears (see [Figure 5-13](#)).

Figure 5-13 *Import EAP-FAST PAC File Window*



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

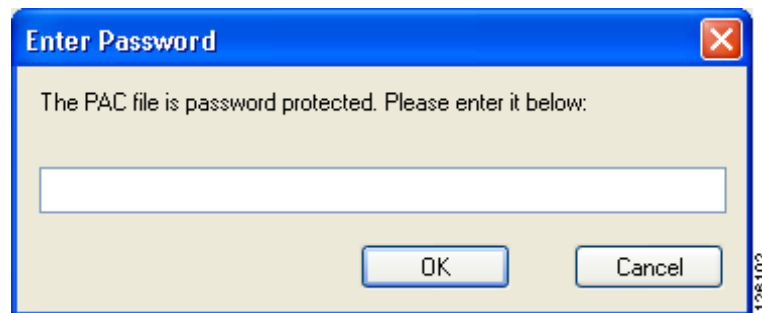


Note

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”](#) section 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, [page 5-45](#)
- Enabling PEAP (EAP-GTC), [page 5-48](#)
- Enabling PEAP (EAP-MSCHAP V2), [page 5-52](#)
- Enabling PEAP (EAP-MSCHAP V2) machine authentication with machine certificates, [page 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.



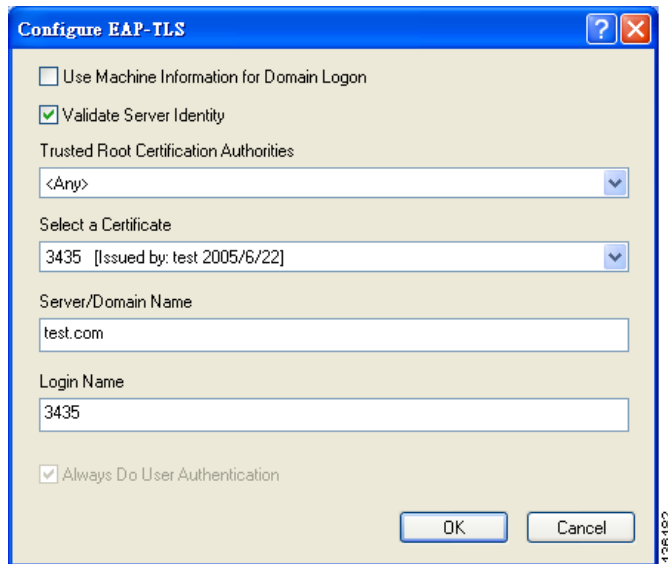
Note If you want to enable CCKM on the client adapter, you must choose the WPA/WPA2/CCKM security option, regardless of whether you want the adapter to use WPA or WPA2. The configuration of the access point to which your client adapter associates determines whether CCKM will be used with 802.1x, WPA,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



Note Refer to the [“WPA and WPA2” section on page 5-18](#) 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 login. 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”](#) section 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.

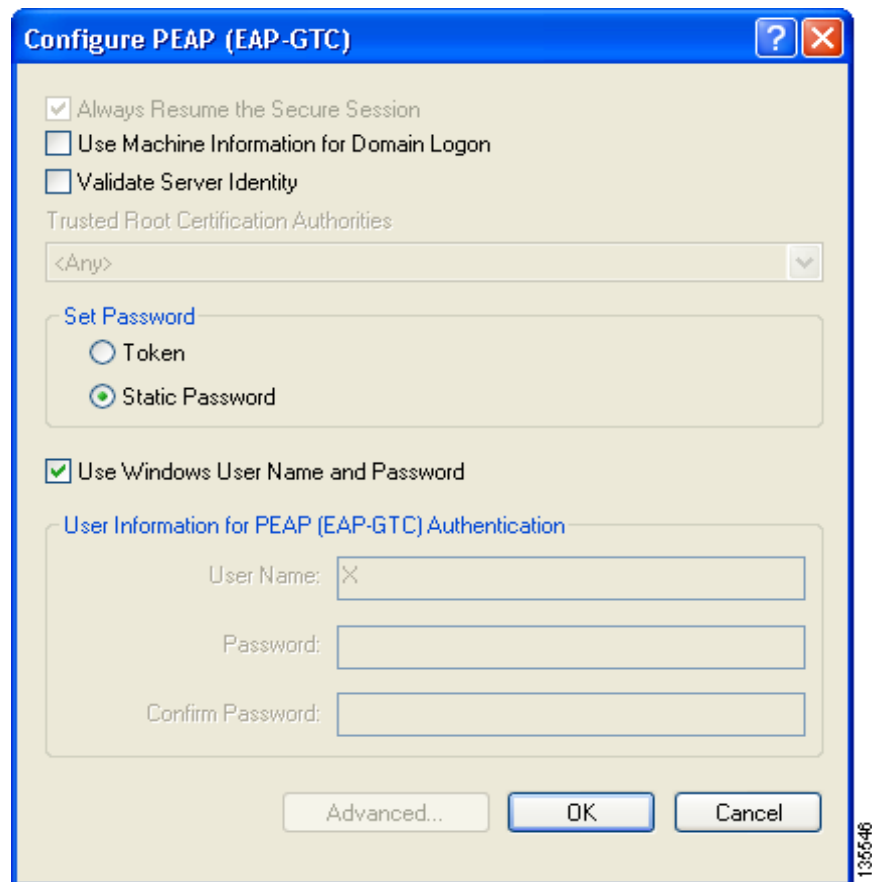


Note

Refer to the [“WPA and WPA2” section on page 5-18](#) 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”](#) section 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”](#) section 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” section on page 5-18](#) 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 login. 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.



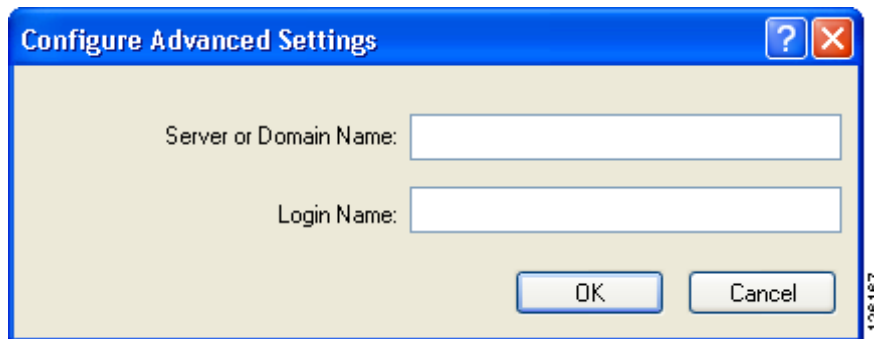
Note Your Windows username is filled in automatically. Simply delete your Windows username and enter your separate PEAP username.

- 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”](#) section 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 \(EAP-MSCHAP V2\)”](#) section 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”](#) section 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 \(EAP-MSCHAP V2\)” section on page E-14](#) 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.



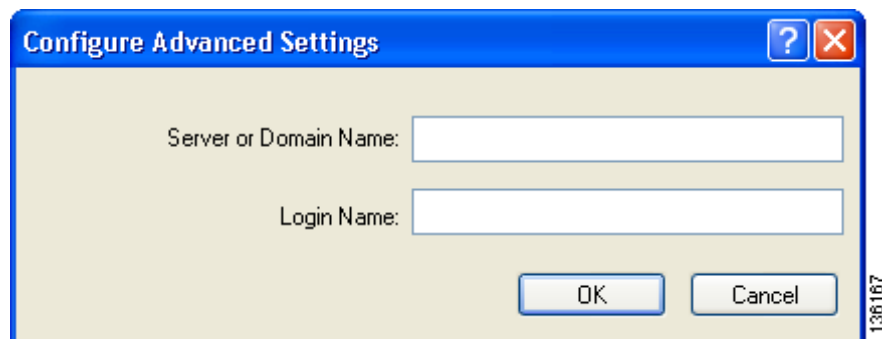
Note

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.

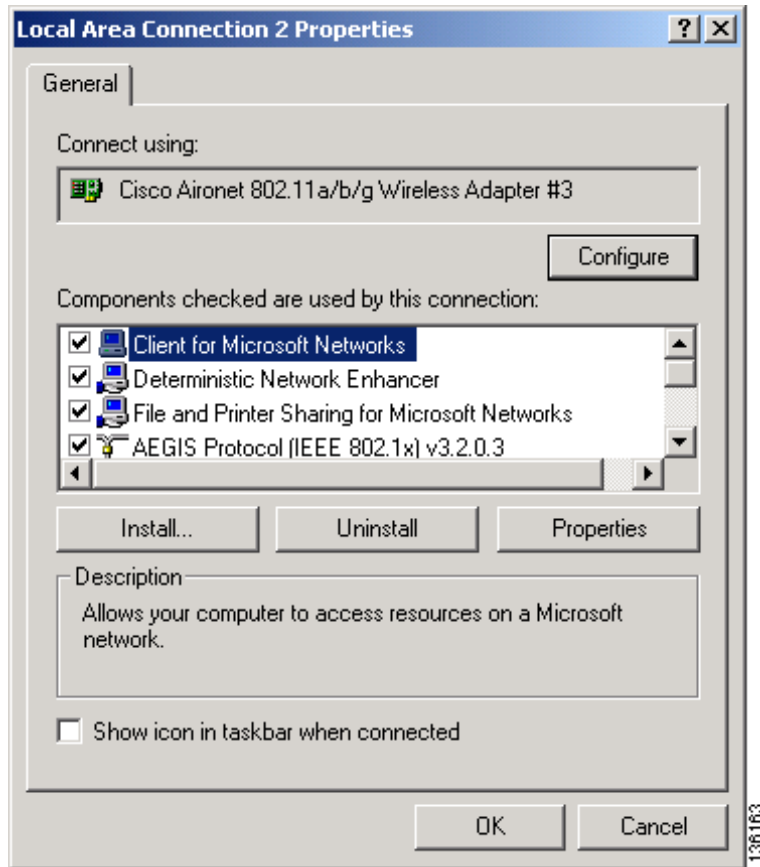
**Note**

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.

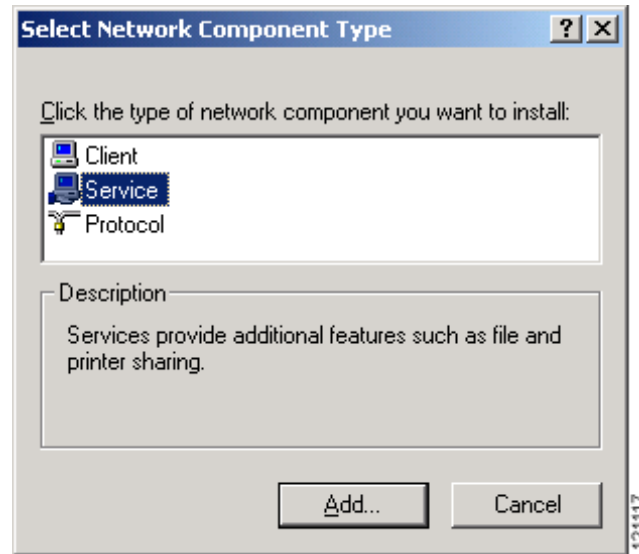
Enabling the QoS Packet Scheduler on Windows 2000

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

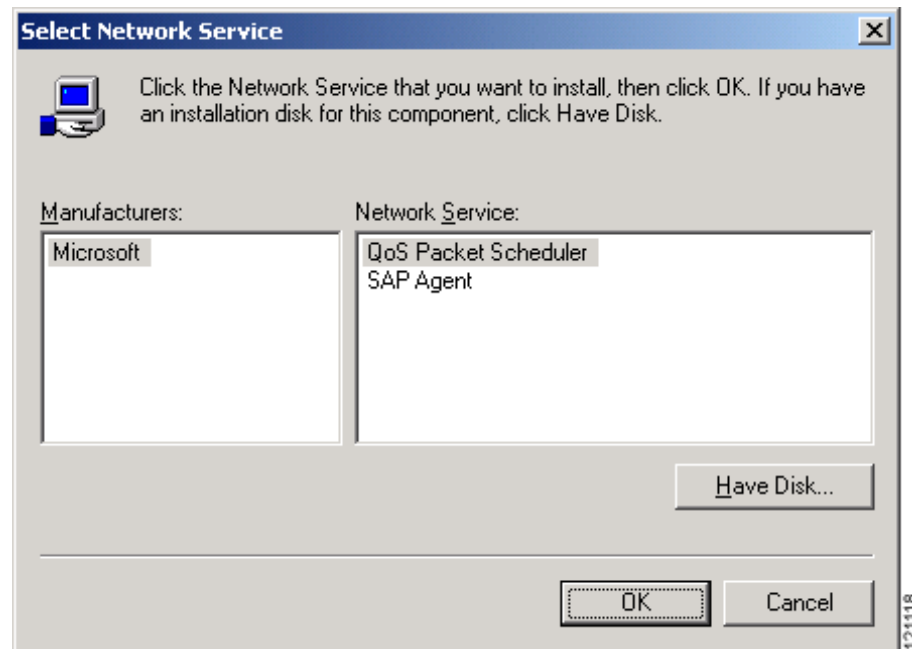
-
- Step 1** Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**.
 - Step 2** Right-click your wireless network connection.
 - Step 3** Click **Properties**. The Wireless Cisco Connection Properties window appears (see [Figure 5-20](#)).

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.

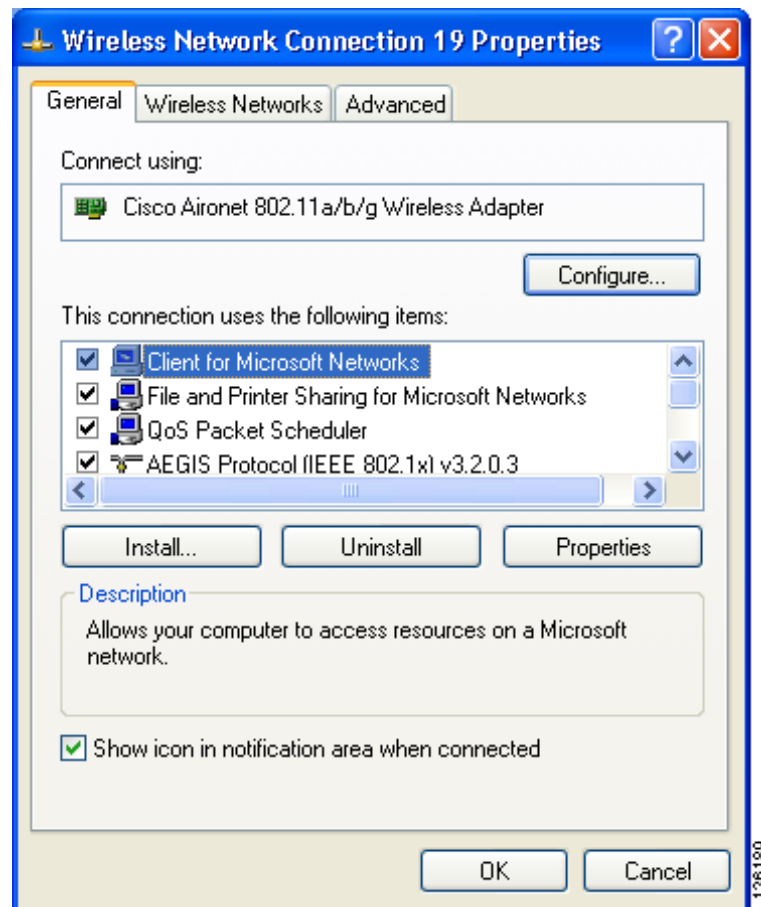
Step 9 Click **OK**.

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*

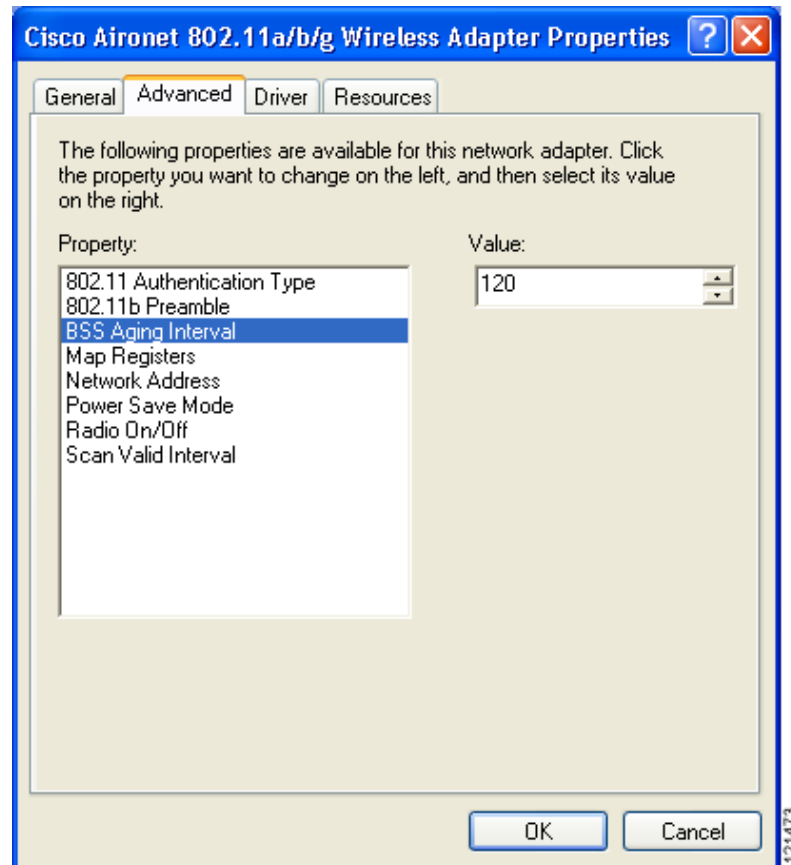


- Step 5** Check the **QoS Packet Scheduler** check box, which appears in the list of items that this connection uses.
- Step 6** Click **OK**.

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)*

Parameter	Description												
BSS Aging Interval	<p>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.</p> <p>Range: 20 to 300 seconds (in 10-second increments)</p> <p>Default: 120 seconds</p> <p>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.</p>												
Scan Valid Interval	<p>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.</p> <p>Range: 20 to 120 seconds (in 5-second increments)</p> <p>Default: 60 seconds</p> <p>Note The client does not scan for a new access point as long as it has a good connection and is passing data.</p> <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>	Wireless Mode	Signal Strength Threshold (dBm)	Transmit Rate Threshold (Mbps)	5 GHz, 54 Mbps or 2.4 GHz, 54 Mbps	24	24	2.4 GHz, 11 Mbps (other modes enabled)	24	9	2.4 GHz, 11 Mbps (only mode enabled)	24	5
Wireless Mode	Signal Strength Threshold (dBm)	Transmit Rate Threshold (Mbps)											
5 GHz, 54 Mbps or 2.4 GHz, 54 Mbps	24	24											
2.4 GHz, 11 Mbps (other modes enabled)	24	9											
2.4 GHz, 11 Mbps (only mode enabled)	24	5											

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.



CHAPTER 6

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, page 6-2](#)
- [Using LEAP or EAP-FAST, page 6-2](#)
- [Using LEAP or EAP-FAST with the Windows Username and Password, page 6-4](#)
- [Using LEAP or EAP-FAST with an Automatically Prompted Login, page 6-6](#)
- [Using LEAP or EAP-FAST with a Manually Prompted Login, page 6-9](#)
- [Using LEAP or EAP-FAST with a Saved Username and Password, page 6-13](#)
- [Using EAP-TLS, page 6-14](#)
- [Using PEAP \(EAP-GTC\), page 6-15](#)
- [Using PEAP \(EAP-MSCHAP V2\), page 6-16](#)
- [Restarting the Authentication Process, page 6-16](#)

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 6-4](#)
- 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.



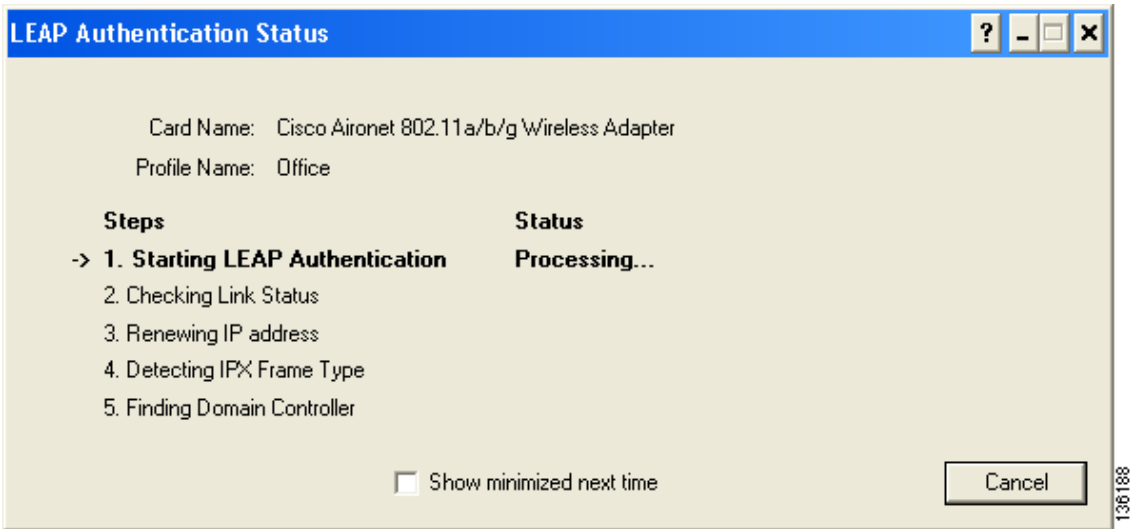
Note

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 10-18](#) 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 10-18](#) 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 10-18](#) 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

Please Change Password

User: wws1

Old Password:

New password:

Verify new password:

OK Cancel

136173

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.

**Note**

The Please Change Password window does not appear if you configured the profile to use Windows credentials for authentication.

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*.

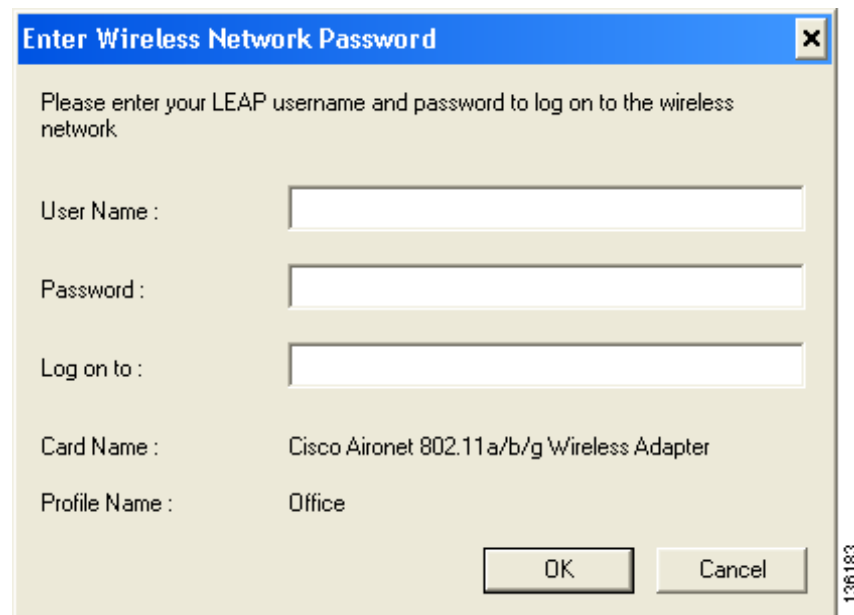
If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the [“Error Messages” section on page 10-18](#) for the necessary action to take.

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.

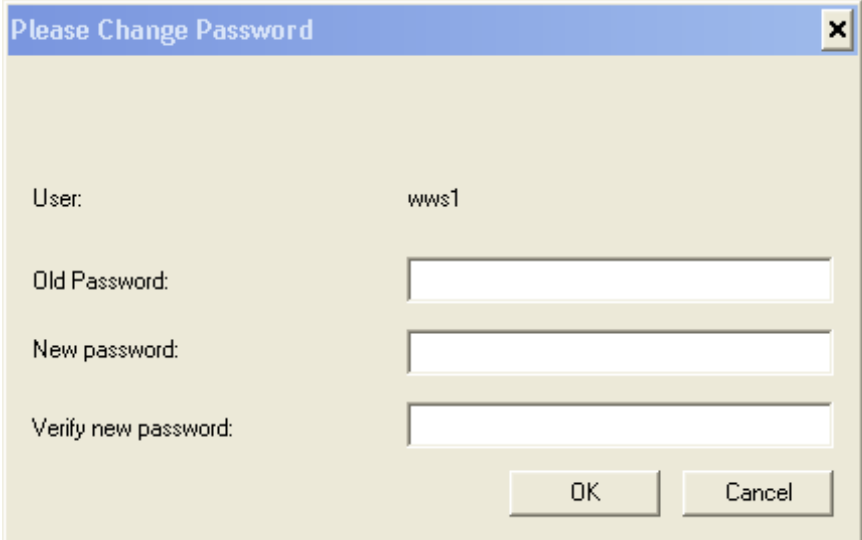
If the authentication attempt fails, an error message appears after the authentication timeout period has expired. Refer to the [“Error Messages”](#) section on page 10-18 for the necessary action to take.

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



The image shows a Windows-style dialog box titled "Please Change Password". The dialog has a blue title bar with a close button (X) in the top right corner. The main area is light beige. It contains four labels on the left: "User:", "Old Password:", "New password:", and "Verify new password:". The "User:" label is followed by the text "wwws1". The other three labels are followed by empty text input fields. At the bottom right of the dialog are two buttons: "OK" and "Cancel". A vertical text label "136173" is positioned to the right of the dialog box.

- 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

Enter Wireless Network Password

Please enter your LEAP username and password to log on to the wireless network

User Name :

Password :

Log on to :

Card Name : Cisco Aironet 802.11a/b/g Wireless Adapter

Profile Name : Office

OK Cancel

136183

The LEAP or EAP-FAST Authentication Status window appears.

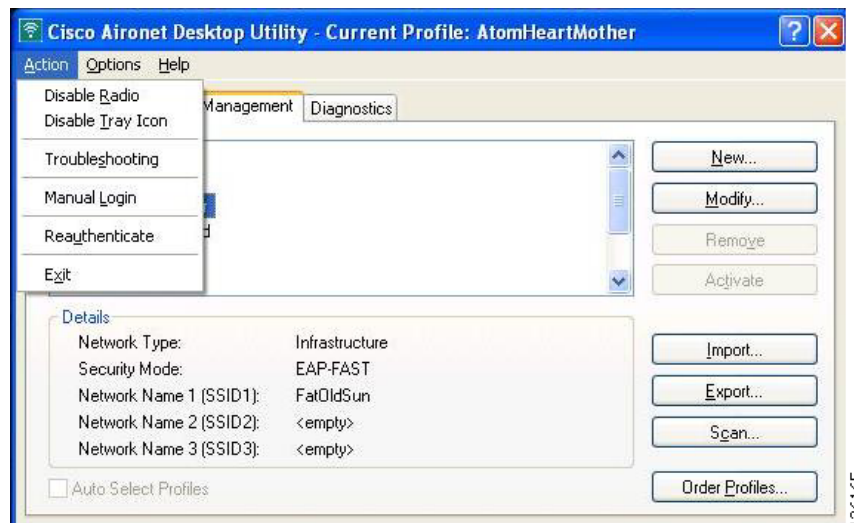
- Step 2** If your profile is configured for EAP-FAST and a message appears asking if you want to auto-provision a PAC, click **Yes**.
- Step 3** If your client adapter authenticates, the window shows that each stage was successful and then disappears. ASTU and the Link Status field on the ADU Current 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 10-18 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



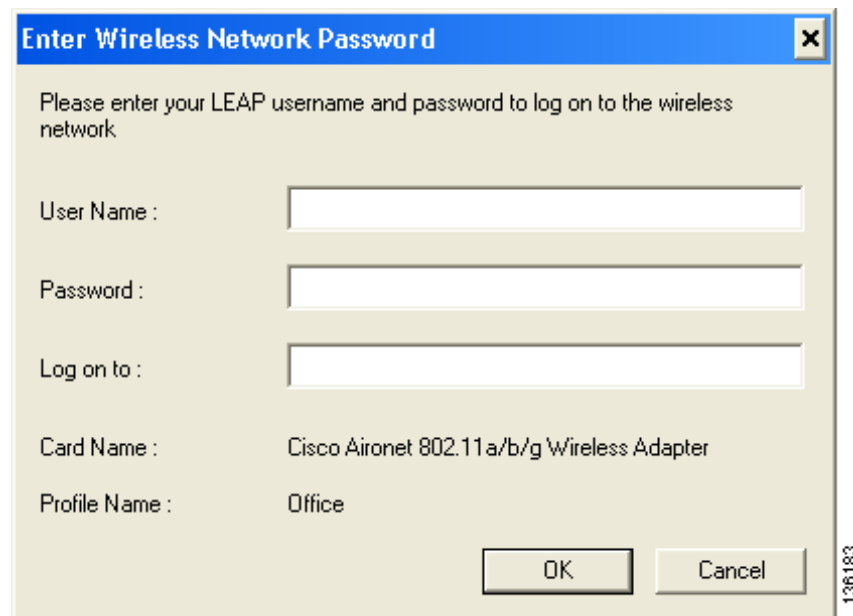
You can also choose the **Manual Login** option from the ASTU pop-up menu (see [Figure 6-8](#)).

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 10-18](#) 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 10-18](#) 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 10-18](#) for the necessary action to take.

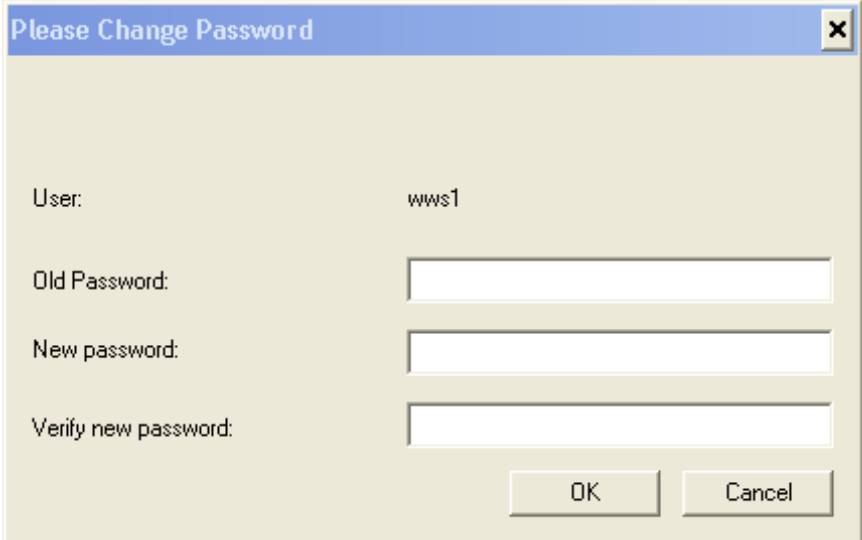
4. Windows continues to log you onto the system. ASTU and the Link Status field on the ADU Current Status window show *Authenticated*.

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

A screenshot of a Windows-style dialog box titled "Please Change Password". The dialog has a blue title bar with a close button (X) in the top right corner. The main area is light beige. It contains four labels on the left: "User:", "Old Password:", "New password:", and "Verify new password:". The "User:" field is pre-filled with the text "wwws1". The other three fields are empty text boxes. At the bottom right, there are two buttons: "OK" and "Cancel". A small vertical text "136173" is visible on the right edge of the dialog box.

Please Change Password

User: wwws1

Old Password:

New password:

Verify new password:

OK Cancel

- 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.

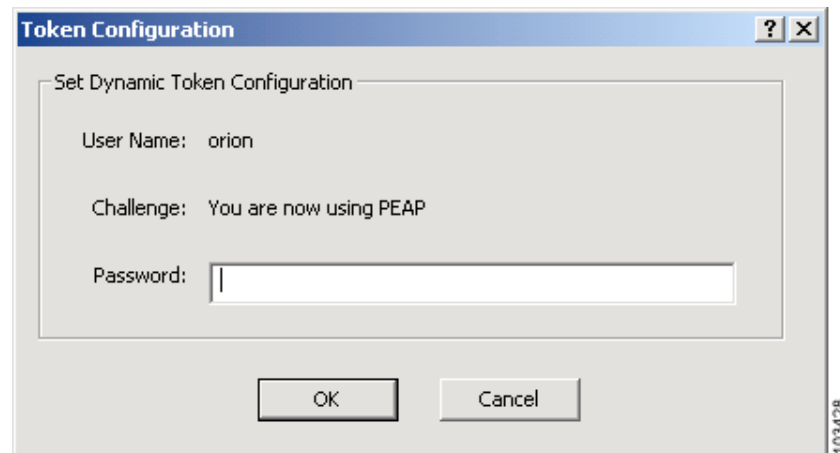
Windows NT or 2000 Domain Databases or LDAP Databases Only

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 SoftToken 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.



CHAPTER 7

Viewing Status and Statistics

This chapter explains how to use ADU to view the client adapter's status and its transmit and receive statistics.

The following topics are covered in this chapter:

- [Overview of ADU Status and Statistics Tools, page 7-2](#)
- [Setting Parameters that Affect ADU Status and Statistics Tools, page 7-2](#)
- [Selecting the Software to Manage Your Client Adapter, page 7-4](#)
- [Viewing the Current Status of Your Client Adapter, page 7-5](#)
- [Viewing Statistics for Your Client Adapter, page 7-14](#)

Overview of ADU Status and Statistics Tools

In addition to enabling you to configure your client adapter for use in various types of networks, ADU provides tools that enable you to assess the performance of the client adapter and other devices on the wireless network. These tools perform the following functions:

- Display your client adapter's current status and configured settings
- Display statistics pertaining to your client adapter's transmission and reception of data

Table 7-1 enables you to quickly find instructions for using ADU status and statistics tools.

Table 7-1 *Status and Statistics Tool Instructions*

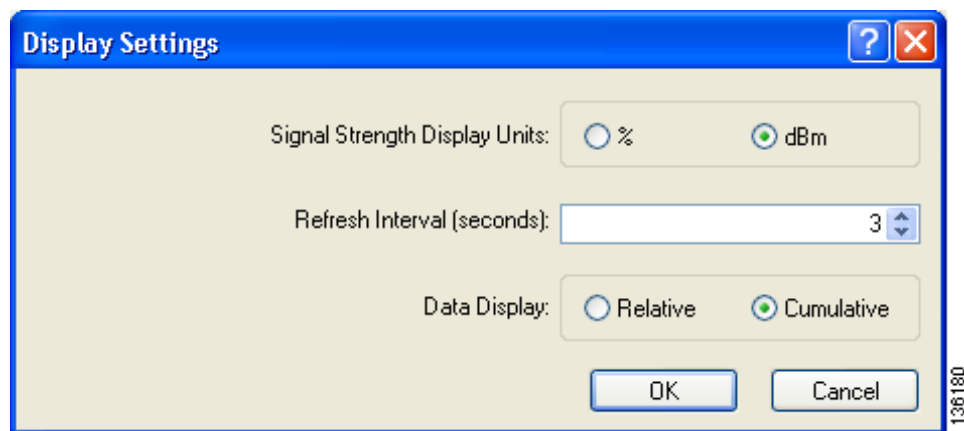
Tool	Page Number
Status	page 7-5
Statistics	page 7-14

Setting Parameters that Affect ADU Status and Statistics Tools

Several parameters affect the operation of ADU status and statistics tools. Follow these steps to set these parameters.

-
- Step 1** Open ADU.
- Step 2** Choose **Display Settings** from the Options drop-down menu. The Display Settings window appears (see [Figure 7-1](#)).

Figure 7-1 *Display Settings Window*



Step 3 Table 7-2 lists and describes the parameters that affect the operation of ADU status and statistics tools. Follow the instructions in the table to change any parameters.

Table 7-2 *Parameters Affecting ADU Status and Statistics Tools*

Parameter	Description	
Signal Strength Display Units	Specifies the units used to display signal strength on the Advanced Status window and signal-to-noise ratio (SNR) on the Available Infrastructure and Ad Hoc Networks window.	
	Options: % or dBm	
	Default: dBm	
	Units	Description
%	Displays the signal strength and signal-to-noise ratio as a percentage.	
dBm	Displays the signal strength in decibels with respect to milliwatts (dBm) and the signal-to-noise ratio in decibels (dB).	
Refresh Interval	Specifies how often the ADU status and statistics windows and the ASTU icon are updated.	
	Range: 1 to 5 seconds between updates (in 1-second increments)	
	Default: 3 seconds between updates	
Data Display	Specifies whether the data that is displayed on the Diagnostics and Advanced Statistics windows continue to increment until the driver is reloaded or only until an update occurs (every 1 to 5 seconds).	
	Options: Relative or Cumulative	
	Default: Cumulative	
	Data Display	Description
Relative	Displays statistical data collected since the last update, as specified by the Refresh Interval (1 to 5 seconds).	
Cumulative	Displays statistical data collected since the driver was loaded, upon card insertion or reboot.	

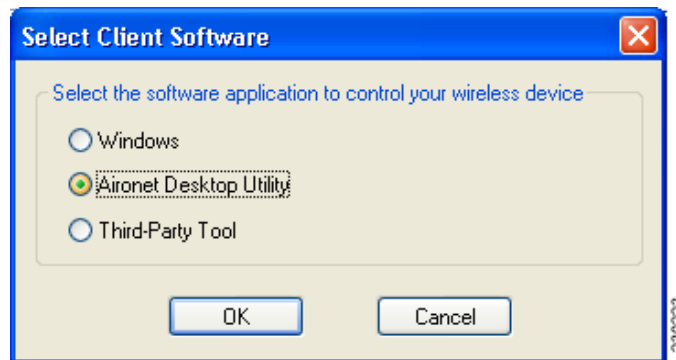
Step 4 Click **OK** to save your changes.

Selecting the Software to Manage Your Client Adapter

You can select the software that you would like to use to configure and display information about your wireless device. Follow these steps to choose the software.

-
- Step 1** Open ADU.
- Step 2** Choose **Select Client Software** from the Options drop-down menu. The Select Client Software window appears (see [Figure 7-2](#)).

Figure 7-2 *Select Client Software Window*



- Step 3** Click the radio button next to the software that you want to use to manage your wireless device.
-

Viewing the Current Status of Your Client Adapter

ADU enables you to view the current status of your client adapter as well as many of the settings that have been configured for the adapter. To view your client adapter's status and settings, open ADU. The Current Status window appears (see [Figure 7-3](#)).

Figure 7-3 Current Status Window

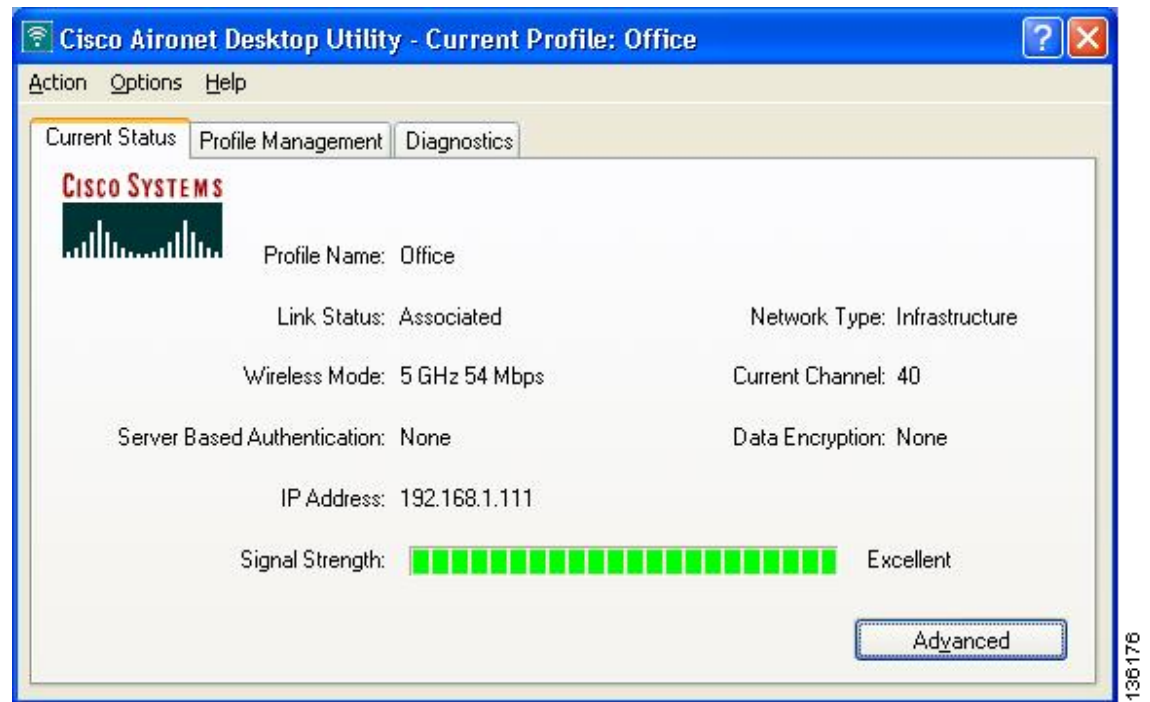


Table 7-3 interprets each element of the Current Status window.

Table 7-3 Basic Client Adapter Status

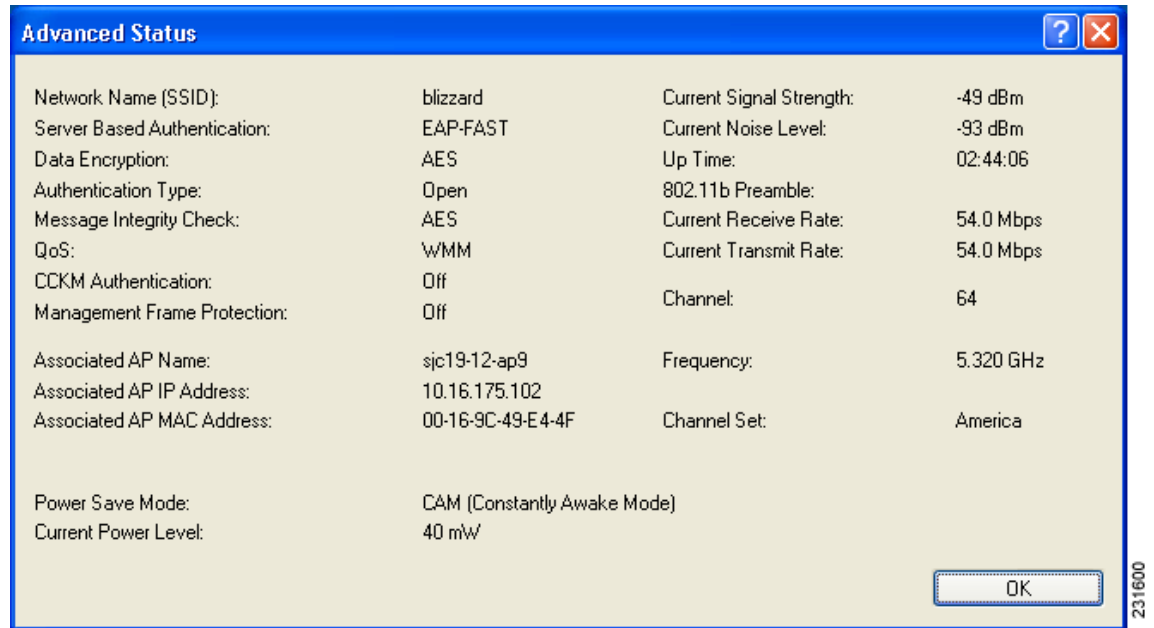
Status	Description														
Profile Name	<p>The network configuration (or profile) your client adapter is currently using.</p> <p>Note Refer to Chapter 4 for information on creating, modifying, and selecting profiles.</p>														
Link Status	<p>The operational mode of your client adapter.</p> <p>Value: Not Associated, Associated, Authenticating, Authenticated, Authentication Failed, or Authentication Failed Retrying</p> <table> <tr> <th>Link Status</th><th>Description</th></tr> <tr> <td>Not Associated</td><td>The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td></tr> <tr> <td>Associated</td><td>The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td></tr> <tr> <td>Authenticating</td><td>The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.</td></tr> <tr> <td>Authenticated</td><td>The client adapter is associated to an access point, and the user is EAP authenticated.</td></tr> <tr> <td>Authentication Failed</td><td>The client adapter is associated to an access point, but the user has failed to EAP authenticate.</td></tr> <tr> <td>Authentication Failed Retrying</td><td>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.</td></tr> </table>	Link Status	Description	Not Associated	The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).	Associated	The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).	Authenticating	The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.	Authenticated	The client adapter is associated to an access point, and the user is EAP authenticated.	Authentication Failed	The client adapter is associated to an access point, but the user has failed to EAP authenticate.	Authentication Failed Retrying	The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.
Link Status	Description														
Not Associated	The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).														
Associated	The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).														
Authenticating	The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.														
Authenticated	The client adapter is associated to an access point, and the user is EAP authenticated.														
Authentication Failed	The client adapter is associated to an access point, but the user has failed to EAP authenticate.														
Authentication Failed Retrying	The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.														
Wireless Mode	<p>The frequency and rate at which your current wireless connection is capable of transmitting or receiving packets.</p> <p>Value: 5 GHz 54 Mbps, 2.4 GHz 11 Mbps, or 2.4 GHz 54 Mbps</p> <p>Note Refer to the Wireless Mode parameter in Table 5-3 for information on setting the wireless mode for your client adapter.</p>														
Network Type	<p>The type of network in which your client adapter is being used.</p> <p>Value: Infrastructure or Ad Hoc</p> <p>Note Refer to the Network Type parameter in Table 5-3 for information on setting the network type.</p>														

Table 7-3 Basic Client Adapter Status (continued)

Status	Description
Server Based Authentication	<p>The method by which authentication to a back-end server is being performed to establish secure connectivity.</p> <p>Value: None, LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), PEAP (EAP-MSCHAP V2), or Host Based EAP</p> <p>Note Refer to the “Overview of Security Features” section on page 5-14 for details on these server-based authentication types.</p>
IP Address	The IP address of your client adapter.
Current Channel	<p>The channel that your client adapter is currently using for communications. This field displays <i>Scanning</i> while the client adapter searches for a channel.</p> <p>Value: Dependent on radio band and regulatory domain</p> <p>Note Refer to the Channel parameter in Table 5-3 for information on setting the channel for your client adapter.</p> <p>Note Refer to Appendix D for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.</p>
Data Encryption	<p>The data encryption type that was negotiated with the access point (in infrastructure mode) or another client (in ad hoc mode) upon association.</p> <p>Value: None, WEP, CKIP, TKIP, or AES</p> <p>Note Refer to the “Overview of Security Features” section on page 5-14 for details on these data encryption types.</p>
Signal Strength	<p>The signal strength for all received packets. The color of this parameter’s progress bar provides a visual interpretation of signal strength.</p> <p>Value: Excellent (green), Good (green), Fair (yellow), Poor (red), or No Link</p>

Click **Advanced** if you want to view more detailed status information for your client adapter. The Advanced Status window appears (see [Figure 7-4](#)).

Figure 7-4 *Advanced Status Window*



[Table 7-4](#) interprets each element of the Advanced Status window.

Table 7-4 *Advanced Client Adapter Status*

Status	Description
Network Name (SSID)	<p>The name of the network to which your client adapter is currently associated.</p> <p>Note Refer to the SSID1 parameter in Table 5-2 for information on setting the client adapter's SSID.</p>
Server Based Authentication	<p>The method by which authentication to a back-end server is being performed to establish secure connectivity.</p> <p>Value: None, LEAP, EAP-FAST, EAP-TLS, PEAP (EAP-GTC), PEAP (EAP-MSCHAP V2), or Host Based EAP</p> <p>Refer to the “Overview of Security Features” section on page 5-14 for details on these server-based authentication types.</p>
Data Encryption	<p>The data encryption type that was negotiated with the access point (in infrastructure mode) or another client (in ad hoc mode) upon association.</p> <p>Value: None, WEP, CKIP, TKIP, or AES</p> <p>Note Refer to the “Overview of Security Features” section on page 5-14 for details on these data encryption types.</p>

Table 7-4 **Advanced Client Adapter Status (continued)**

Status	Description								
Authentication Type	<p>Specifies whether the client adapter must share the same WEP keys as the access point in order to authenticate or can authenticate to the access point regardless of its WEP settings.</p> <p>Value: Open or Shared</p> <p>Note An incorrect WEP key setting prevents connectivity to the network regardless of the 802.11 authentication type selected.</p> <p>Note Refer to the “Setting Advanced Parameters” section on page 5-6 for information on setting the 802.11 authentication mode.</p>								
Message Integrity Check	<p>Indicates whether your client adapter is using message integrity check (MIC) to protect packets sent to and received from the access point.</p> <p>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.</p> <p>Note MIC is supported automatically by the client adapter’s driver, but it must be enabled on the access point.</p> <p>Value: None, MMH, or Michael</p> <table> <tr> <th>Message Integrity Check</th><th>Description</th></tr> <tr> <td>None</td><td>MIC is disabled.</td></tr> <tr> <td>MMH</td><td>MIC is enabled and is being used with CKIP.</td></tr> <tr> <td>Michael</td><td>MIC is enabled and is being used with WPA and TKIP.</td></tr> </table>	Message Integrity Check	Description	None	MIC is disabled.	MMH	MIC is enabled and is being used with CKIP.	Michael	MIC is enabled and is being used with WPA and TKIP.
Message Integrity Check	Description								
None	MIC is disabled.								
MMH	MIC is enabled and is being used with CKIP.								
Michael	MIC is enabled and is being used with WPA and TKIP.								

Table 7-4 **Advanced Client Adapter Status (continued)**

Status	Description						
QoS	<p>The type of quality of service that is currently being used by your client adapter. QoS on wireless LANs (WLAN) provides prioritization of traffic from the access point over the WLAN based on traffic classification.</p> <p>Value: None or WMM</p> <table> <tr> <th>QoS</th><th>Description</th></tr> <tr> <td>None</td><td>WMM standard QoS is not enabled.</td></tr> <tr> <td>WMM</td><td>Wi-Fi Multimedia, a component of the IEEE 802.11e WLAN standard for QoS, is enabled. For this value to appear, QoS and WMM must be enabled on the access point to which the client adapter is associated.</td></tr> </table> <p>Note 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 in the “Enabling Wi-Fi Multimedia” section on page 5-59 to enable the QoS Packet Scheduler.</p>	QoS	Description	None	WMM standard QoS is not enabled.	WMM	Wi-Fi Multimedia, a component of the IEEE 802.11e WLAN standard for QoS, is enabled. For this value to appear, QoS and WMM must be enabled on the access point to which the client adapter is associated.
QoS	Description						
None	WMM standard QoS is not enabled.						
WMM	Wi-Fi Multimedia, a component of the IEEE 802.11e WLAN standard for QoS, is enabled. For this value to appear, QoS and WMM must be enabled on the access point to which the client adapter is associated.						
CCKM Authentication	<p>Whether Cisco Centralized Key Management (CCKM) authentication is on or off.</p> <p>Using CCKM, an authenticated client device can roam from one access point to another without any perceptible delay during reassociation. For more information about CCKM, see the “CCKM Fast Secure Roaming” section on page 5-19.</p> <p>Value: On or Off</p>						
Management Frame Protection	<p>Whether management frame protection (MFP) is on or off.</p> <p>When MFP is enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, which causes devices that are configured to detect MFP frames to report the discrepancy.</p> <p>The client adapter software configures MFP automatically based on how MFP is configured on the access point to which the client adapter is associated. If the access point has MFP turned on, then the client adapter software turns on MFP. If the access point has MFP turned off, then the client adapter software turns off MFP.</p> <p>Value: On or Off</p>						
Associated AP Name	<p>The name of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode, the access point was configured with a name, and Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later).</p> <p>Note This field shows up to 15 characters although the name of the access point may be longer.</p>						

Table 7-4 **Advanced Client Adapter Status (continued)**

Status	Description
Associated AP IP Address	<p>The IP address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode, the access point was configured with an IP address, and Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later).</p> <p>Note If Aironet Extensions are disabled, the IP address of the associated access point is shown as 0.0.0.0.</p>
Associated AP MAC Address	<p>The MAC address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode.</p> <p>Note This field displays the MAC address of the access point's Ethernet port (for access points that do not run Cisco IOS software) or the MAC address of the access point's radio (for access points that run Cisco IOS software). The MAC address of the Ethernet port on access points that run Cisco IOS software is printed on a label on the back of the device.</p>
Power Save Mode	<p>The client adapter's current power consumption setting.</p> <p>Value: CAM (Constantly Awake Mode), Max PSP (Max Power Saving), or Fast PSP (Power Save Mode)</p> <p>Note Refer to the Power Save Mode parameter in Table 5-3 for information on setting the client adapter's power save mode.</p>
Current Power Level	<p>The power level at which your client adapter is currently transmitting. The maximum level is dependent upon the radio band used and your country's regulatory agency.</p> <p>Value: 10, 13, 20, 25, or 40 mW (802.11a band); 10, 20, 32, 50, 63, or 100 mW (802.11b/g band)</p> <p>Note Refer to the Transmit Power Level parameter in Table 5-3 for information on setting the client adapter's power level.</p>
Available Power Levels	<p>The power levels at which your client adapter is capable of transmitting. The maximum level is dependent upon the radio band used and your country's regulatory agency.</p> <p>Value: 10, 13, 20, 25, or 40 mW (802.11a band); 10, 20, 32, 50, 63, or 100 mW (802.11b/g band)</p> <p>Note Refer to the Transmit Power Level parameter in Table 5-3 for information on the client adapter's available power levels.</p>
Current Signal Strength	<p>The signal strength for all received packets. The higher the value, the stronger the signal.</p> <p>Range: 0 to 100% or 0 to -100 dBm</p>

Table 7-4 **Advanced Client Adapter Status (continued)**

Status	Description
Current Signal Quality	<p>The signal quality for all received packets. The higher the value, the clearer the signal.</p> <p>Range: 0 to 100%</p> <p>Note This field appears only if you selected signal strength to be displayed as a percentage. See the Signal Strength Display Units parameter in Table 7-2 for information.</p>
Current Noise Level	<p>The level of background radio frequency energy in the current radio band. The lower the value, the less background noise present.</p> <p>Range: 0 to –100 dBm</p> <p>Note This field appears only if you selected signal strength to be displayed in dBm. See the Signal Strength Display Units parameter in Table 7-2 for information.</p>
Up Time	<p>The amount of time (in hours:minutes:seconds) since the client adapter has been receiving power. If the adapter has been running for more than 24 hours, the time is displayed in days, hours:minutes:seconds.</p>
802.11b Preamble	<p>Indicates whether your client adapter is using only long radio headers or short and long radio headers.</p> <p>Value: Short & Long or Long Only</p> <p>Note This field contains a value only when the client adapter is operated in 2.4-GHz 11-Mbps or 2.4-GHz 54-Mbps mode.</p> <p>Note Refer to the 802.11b Preamble parameter in Table 5-3 for information on using radio headers.</p>
Current Receive Rate	<p>The rate at which your client adapter is currently receiving data packets.</p> <p>Value: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps</p>
Current Transmit Rate	<p>The rate at which your client adapter is currently transmitting data packets.</p> <p>Value: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps</p>
Channel	<p>The channel that your client adapter is currently using for communications. This field displays <i>Scanning</i> while the client adapter searches for a channel.</p> <p>Value: Dependent on radio band and regulatory domain</p> <p>Note Refer to the Channel parameter in Table 5-3 for information on setting the channel for your client adapter.</p> <p>Note Refer to Appendix D for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.</p>

Table 7-4 **Advanced Client Adapter Status (continued)**

Status	Description
Frequency	<p>The radio frequency that your client adapter is currently using for communications. This field displays <i>Scanning</i> while the client adapter searches for a frequency.</p> <p>Value: Dependent on radio band and regulatory domain</p> <p>Note Refer to the Wireless Mode parameter in Table 5-3 for information on setting the frequency for your client adapter.</p>
Channel Set	<p>The regulatory domain for which your client adapter is currently configured. This value is not user selectable.</p> <p>Value: America, EMEA, Japan, or Rest of World</p> <p>Note Refer to Appendix D for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.</p>

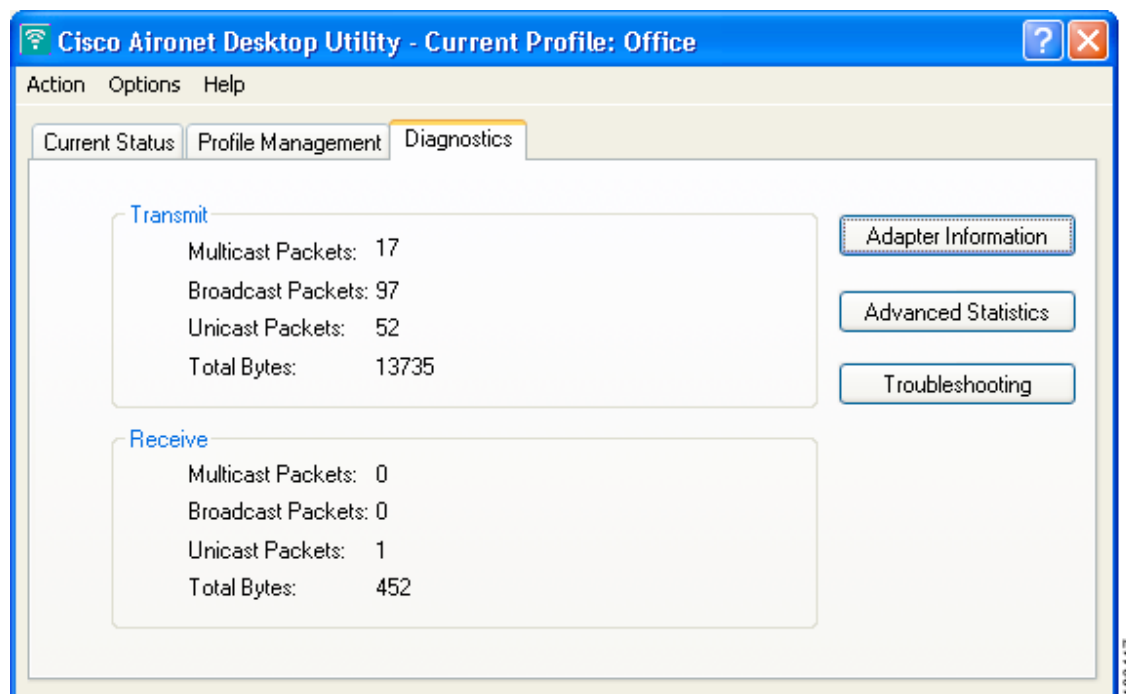
Click **OK** to close the Advanced Status window.

Viewing Statistics for Your Client Adapter

ADU enables you to view statistics that indicate how data is being received and transmitted by your client adapter.

To view your client adapter's statistics, open ADU and click the **Diagnostics** tab. The Cisco Aironet Desktop Utility (Diagnostics) window appears (see [Figure 7-5](#)).

Figure 7-5 Cisco Aironet Desktop Utility (Diagnostics) Window



This window displays basic transmit and receive statistics for your client adapter. The statistics are calculated on a relative or cumulative basis as specified by the Data Display parameter and are continually updated at the rate specified by the Refresh Interval parameter. Instructions for changing the Data Display and Refresh Interval settings are provided in [Table 7-2](#).



Note

The receive and transmit statistics are host statistics. That is, they show packets and errors received or sent by the Windows device.



Note

To run the Cisco Aironet Troubleshooting Utility, click **Troubleshooting**. Refer to [“Using the Cisco Aironet Troubleshooting Utility”](#) section on page 10-3 for more information.



Note

To view client adapter information, click **Adapter Information**. Refer to [“Viewing Client Adapter Information”](#) section on page 9-10 for more information.

Table 7-5 describes each statistic that is displayed for your client adapter.

Table 7-5 Basic Client Adapter Statistics

Statistic	Description
Transmit Statistics	
Multicast Packets	The number of multicast packets that were transmitted.
Broadcast Packets	The number of broadcast packets that were transmitted.
Unicast Packets	The number of unicast packets that were transmitted successfully.
Total Bytes	The number of bytes of data that were transmitted successfully.
Receive Statistics	
Multicast Packets	The number of multicast packets that were received.
Broadcast Packets	The number of broadcast packets that were received.
Unicast Packets	The number of unicast packets that were received successfully.
Total Bytes	The number of bytes of data that were received successfully.

Click **Advanced Statistics** if you want to view additional statistics for your client adapter. The Advanced Statistics window appears (see Figure 7-6).

Figure 7-6 Advanced Statistics Window

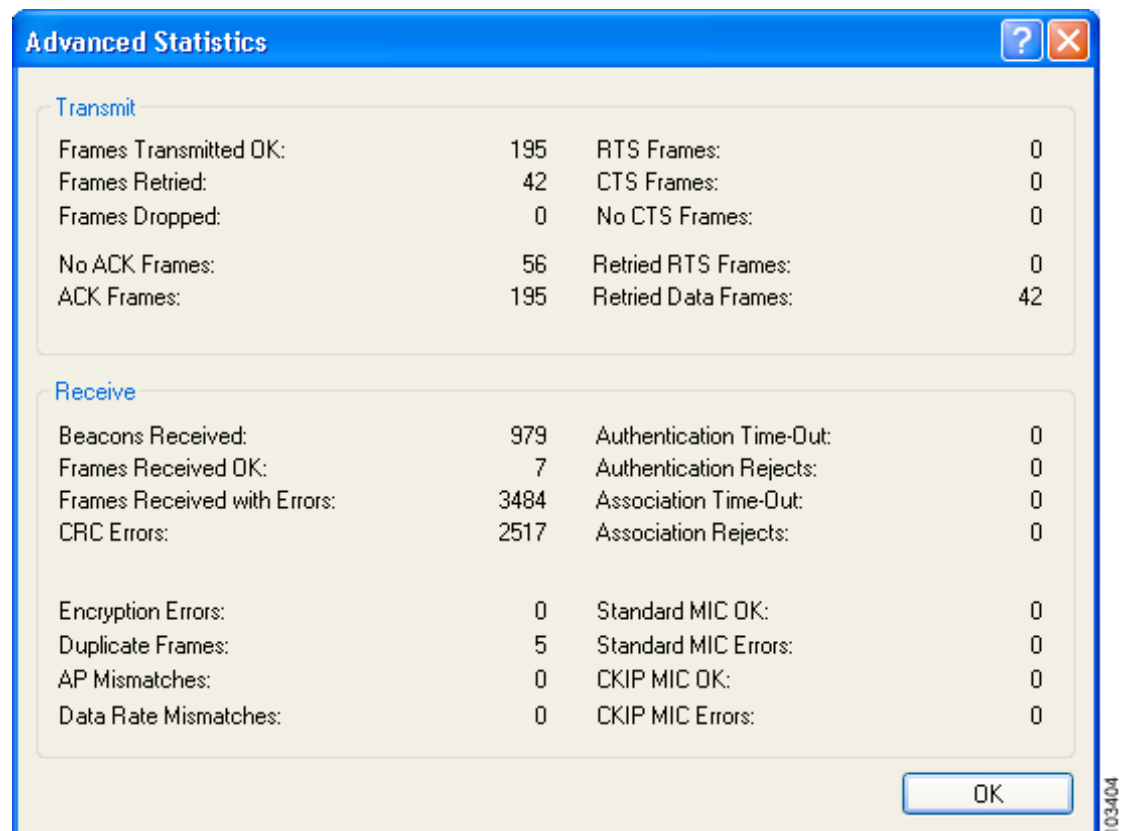


Table 7-6 interprets each element of the Advanced Statistics window.

Table 7-6 Advanced Client Adapter Statistics

Status	Description
Transmit Statistics	
Frames Transmitted OK	The number of frames that were transmitted successfully.
Frames Retried	The number of frames that were retried.
Frames Dropped	The number of frames that were dropped because of errors or collisions.
No ACK Frames	The number of transmitted frames that did not have their corresponding Ack frame received successfully.
ACK Frames	The number of transmitted frames that had their corresponding Ack frame received successfully.
RTS Frames	The number of request-to-send (RTS) transmissions that were attempted.
CTS Frames	The number of clear-to-send (CTS) frames that were received in response to a successfully transmitted RTS frame.
No CTS Frames	The number of request-to-send (RTS) transmissions that were unsuccessful. The access point sends CTS frames in response to the client's RTS frames. This field keeps track of each time the client does not receive a CTS back from the access point.
Retried RTS Frames	The number of request-to-send (RTS) frames that were retransmitted.
Retried Data Frames	The number of normal data frames that were retransmitted.
Receive Statistics	
Beacons Received	The number of beacon frames that were received successfully.
Frames Received OK	The number of all frames that were received successfully.
Frames Received with Errors	The number of frames that were received with an invalid checksum.
CRC Errors	The number of cyclic redundancy check (CRC) errors detected in the data portion of the frame.
Encryption Errors	The number of frames that were received with encryption errors.
Duplicate Frames	The number of duplicate frames that were received.
AP Mismatches	<p>The number of times the client adapter tried to associate to an access point but was unable to because the access point was not the adapter's specified access point.</p> <p>Note Refer to the Access Point 1 through Access Point 4 parameters on page 5-13 for information on specifying access points.</p>
Data Rate Mismatches	<p>The number of times the client adapter tried to associate to an access point but was unable to because the adapter's data rate was not supported by the access point.</p> <p>Note Refer to the Wireless Mode parameter in Table 5-3 for information on supported data rates.</p>

Table 7-6 **Advanced Client Adapter Statistics (continued)**

Status	Description
Authentication Time-Out	The number of times the client adapter tried to authenticate to an access point but was unable to because the access point did not respond fast enough (timed out).
Authentication Rejects	The number of times the client adapter tried to authenticate to an access point but was rejected.
Association Time-Out	The number of times the client adapter tried to associate to an access point but was unable to because the access point did not respond fast enough (timed out).
Association Rejects	The number of times the client adapter tried to associate to an access point but was rejected.
Standard MIC OK	The number of frames that were received with the correct message integrity check (MIC) value.
Standard MIC Errors	The number of frames that were discarded due to an incorrect message integrity check (MIC) value.
CKIP MIC OK	The number of frames that were received with the correct message integrity check (MIC) value when CKIP was being used. Note This field is displayed only if MIC is enabled on the access point.
CKIP MIC Errors	The number of frames that were discarded due to an incorrect message integrity check (MIC) value when CKIP was being used. Note This field is displayed only if MIC is enabled on the access point.

Click **OK** to close the Advanced Statistics window.



CHAPTER 8

Using the Aironet System Tray Utility (ASTU)

This chapter explains how to use the Aironet System Tray Utility (ASTU) to access status information about your client adapter and perform basic tasks.

The following topics are covered in this chapter:

- [Overview of ASTU, page 8-2](#)
- [The ASTU Icon, page 8-2](#)
- [Tool Tip Window, page 8-3](#)
- [Pop-Up Menu, page 8-5](#)

Overview of ASTU

ASTU is an optional application that provides a small subset of the features available through ADU. Specifically, it enables you to access status information about your client adapter and perform basic tasks. ASTU is accessible from an icon in the Windows system tray, making it easily accessible and convenient to use. The ASTU icon appears only if a client adapter is installed into your computer and you did not disable ASTU during installation.

ASTU provides information and options in the following ways:

- In the appearance of the icon itself
- Through a tool tip window that appears when you hover the cursor over the icon
- Through a pop-up menu that appears when you right-click the icon
- Through a Connection Status window that appears when you double-click the icon

The ASTU Icon

The appearance of the ASTU icon indicates the connection status of your client adapter. ASTU reads the client adapter status and updates the icon every 1 to 5 seconds, depending on the value entered for the Refresh Interval on the Display Settings window. [Table 8-1](#) interprets the different appearances of the ASTU icon.



Note

Windows 2000 and XP may display their own wireless network connection status icon in the system tray. Cisco recommends that you turn off the Windows icon and use the ASTU icon to monitor your wireless connection.

Table 8-1 *Interpreting the ASTU Icon*







Icon	Description
	A white icon indicates that the client adapter's radio is disabled.
	A dark gray icon indicates that the client adapter is not associated to an access point (in infrastructure mode) or another client (in ad hoc mode).
	A light gray icon indicates that the client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode) but the user is not EAP authenticated.
	A green icon indicates that the client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode), the user is authenticated if the client adapter is configured for EAP authentication, and the signal strength is excellent or good.

Table 8-1 *Interpreting the ASTU Icon (continued)*

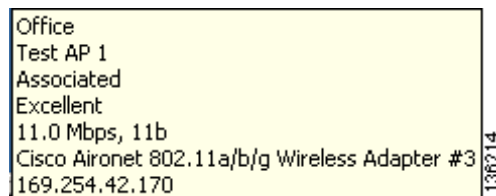
Icon	Description
	A yellow icon indicates that the client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode), the user is authenticated if the client adapter is configured for EAP authentication, and the signal strength is fair.
	A red icon indicates that the client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode), the user is authenticated if the client adapter is configured for EAP authentication, and the signal strength is poor.

Tool Tip Window

When you hover the cursor over the ASTU icon, the Tool Tip window appears (see [Figure 8-1](#)).


Note

If the client adapter's radio is disabled, a message appears instead of the Tool Tip window to inform you that the wireless network interface is disabled.

Figure 8-1 *Tool Tip Window*

This window provides information on the current status of your client adapter. [Table 8-2](#) lists and describes each element of the Tool Tip window.

Table 8-2 *Tool Tip Window Elements*

Status Element	Description
Active profile	<p>The network configuration (or profile) that your client adapter is currently using.</p> <p>Note If auto profile selection is enabled, the active profile does not appear until the client is associated to an access point.</p>
SSID	<p>The name of the network to which your client adapter is currently associated.</p> <p>Note When the client adapter is not associated and auto profile selection is disabled, this field shows the profile's SSID. When the client adapter is not associated and auto profile selection is enabled, this field is left blank.</p> <p>Note Refer to the SSID1 parameter in Table 5-2 for information on setting the client adapter's SSID.</p>

Table 8-2 **Tool Tip Window Elements (continued)**

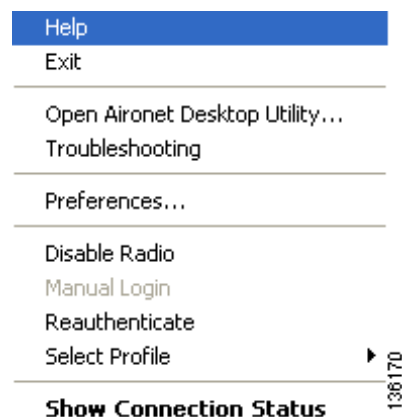
Status Element	Description														
Connection status	<p>The operational mode of your client adapter.</p> <p>Value: Not Associated, Associated, Authenticating, Authenticated, Authentication Failed, or Authentication Failed Retrying</p>														
	<table> <tr> <th>Connection Status</th><th>Description</th></tr> <tr> <td>Not Associated</td><td>The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td></tr> <tr> <td>Associated</td><td>The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td></tr> <tr> <td>Authenticating</td><td>The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.</td></tr> <tr> <td>Authenticated</td><td>The client adapter is associated to an access point, and the user is EAP authenticated.</td></tr> <tr> <td>Authentication Failed</td><td> <p>The client adapter is associated to an access point, but the user has failed to EAP authenticate.</p> <p>Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p> </td></tr> <tr> <td>Authentication Failed Retrying</td><td> <p>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.</p> <p>Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p> </td></tr> </table>	Connection Status	Description	Not Associated	The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).	Associated	The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).	Authenticating	The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.	Authenticated	The client adapter is associated to an access point, and the user is EAP authenticated.	Authentication Failed	<p>The client adapter is associated to an access point, but the user has failed to EAP authenticate.</p> <p>Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p>	Authentication Failed Retrying	<p>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.</p> <p>Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p>
Connection Status	Description														
Not Associated	The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).														
Associated	The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).														
Authenticating	The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.														
Authenticated	The client adapter is associated to an access point, and the user is EAP authenticated.														
Authentication Failed	<p>The client adapter is associated to an access point, but the user has failed to EAP authenticate.</p> <p>Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p>														
Authentication Failed Retrying	<p>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.</p> <p>Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p>														

Table 8-2 **Tool Tip Window Elements (continued)**

Status Element	Description
Link quality	The client adapter's signal strength for all received packets. Value: Excellent, Good, Fair, Poor, or No Link
Link speed and 802.11 mode	The rate at which your client adapter is currently transmitting data packets and the 802.11 mode that your client adapter is currently using for communications. Link speed value: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps 802.11 mode value: 11a, 11b, or 11g
Client adapter type	A description of your client adapter.
Client adapter IP address	The IP address of your client adapter.

Pop-Up Menu

When you right-click the ASTU icon, the ASTU pop-up menu appears (see [Figure 8-2](#)).

Figure 8-2 **ASTU Pop-Up Menu**

The following sections describe each ASTU pop-up menu option.



Note

If you used the Aironet System Tray Utility Preferences window or your system administrator used an administrative tool to deactivate certain ASTU menu options, these options do not appear in the menu and therefore cannot be selected.

Help

This option enables you to access the online help.

Exit

This option closes ADU and ASTU.



Note

To reactivate ADU, double-click the **Aironet Desktop Utility** icon on your computer desktop. To reactivate ASTU, choose the **Enable Tray Icon** option from the ADU Action drop-down menu.

Open Aironet Desktop Utility

This option activates ADU.

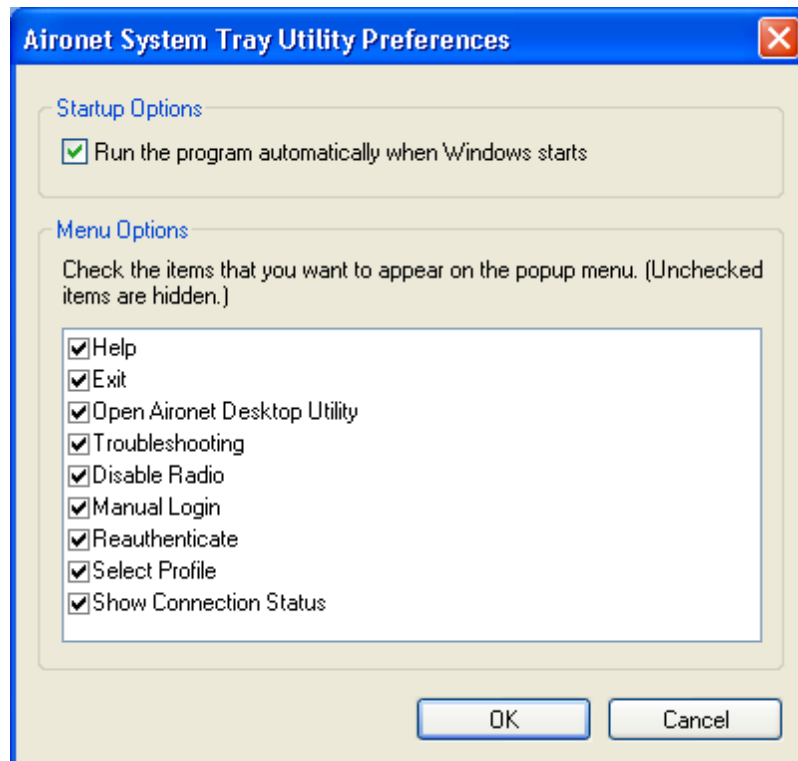
Troubleshooting

This option activates the troubleshooting utility, which enables you to identify and resolve configuration and association problems with your client adapter. Refer to the [“Using the Cisco Aironet Troubleshooting Utility” section on page 10-3](#) for detailed instructions on using this utility.

Preferences

When you choose this option, the Aironet System Tray Utility Preferences window appears (see [Figure 8-3](#)).

Figure 8-3 Aironet System Tray Utility Preferences Window



This window enables you to determine when ADU and ASTU run and to choose the options that appear on the ASTU pop-up menu. Follow these steps to make your selections.

- Step 1** If you want ASTU to run automatically when Windows starts, make sure the **Run the program automatically when Windows starts** check box is checked. Otherwise, uncheck this check box.



Note If you do not choose this option and later want to run ASTU, you must choose the **Enable Tray Icon** option from the Action drop-down menu in ADU.

- Step 2** In the Menu Options portion of the window, make sure the check boxes of all the options that you want to appear in the ASTU pop-up menu are checked. Any options that are not checked will not be included in the menu.



Note The Preferences option cannot be deselected. It always appears in the ASTU pop-up menu.

- Step 3** Click **OK** to save your changes.

Enable/Disable Radio

This option enables you to disable or enable the client adapter's radio. Disabling the radio prevents the adapter from transmitting RF energy. You might want to disable the client adapter's radio in the following situations:

- You are not transmitting data and want to conserve battery power.
- You are using a laptop on an airplane, hospital, or any other location where radio transmission is not allowed and want to prevent the adapter's transmissions from potentially interfering with the operation of certain devices.

When the radio is enabled, it periodically sends out probes even if it is not associated to an access point (in infrastructure mode) or another client (in ad hoc mode), as required by the 802.11 specification. Therefore, it is important to disable it around devices that are susceptible to RF interference.



Note If the client adapter's radio is disabled, your client adapter is not associated, and a message appears when you hover the cursor over the ASTU icon to inform you that the wireless network interface is disabled.



Note If your client adapter's radio is disabled before your computer enters standby or hibernate mode or before you reboot the computer, the radio remains disabled when the computer resumes. You must enable the radio to resume operation.

If the radio is enabled, choose **Disable Radio** to disable the radio.

If the radio is disabled, choose **Enable Radio** to enable the radio.

Manual Login

This option enables you to manually invoke the authentication process for a profile that is configured to use a manually prompted LEAP or EAP-FAST username and password. When you choose this option, the Enter Wireless Network Password window appears. Enter your LEAP or EAP-FAST credentials and click **OK**. The LEAP or EAP-FAST Authentication Status window appears, and the authentication process begins.



Note

Refer to [Chapter 5](#) for information on setting a manual LEAP or EAP-FAST profile and [Chapter 6](#) for details on the authentication process.

Reauthenticate

This option forces your client adapter to try to reauthenticate using the username and password of the current profile. It is available for all EAP-enabled profiles. 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.

Select Profile

This option enables you to select the active profile for your client adapter. When you choose this option, a profiles submenu appears (see [Figure 8-4](#)).

Figure 8-4 Profiles Submenu



From this menu, you can choose between the following options:

- **Use Auto Profile Selection**—Causes the client adapter's driver to automatically select a profile from the list of profiles that were set up in ADU 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 will 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 select a new profile.



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, the login scripts will run. However, if you authenticate and achieve full network connectivity after you log into the computer, the login scripts will not run.

- **A specific profile**—When you select a profile from the list of available profiles, the client adapter attempts to establish a connection to an access point (in infrastructure mode) or another client (in ad hoc mode) using the parameters that were configured for that profile.

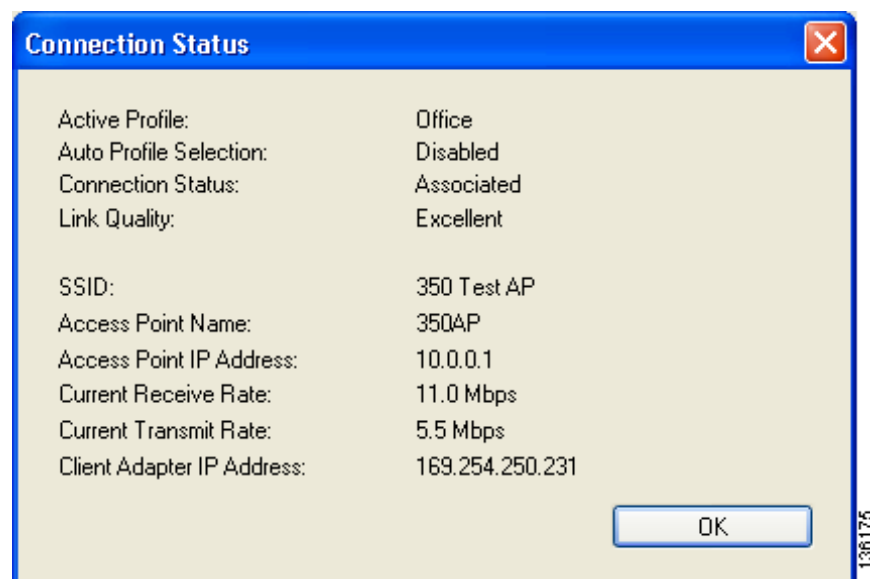
If the client adapter cannot associate to the access point (or other client) or loses association while using the selected profile, the adapter does not attempt to associate using another profile. To get it to associate, you must select a different profile or select Use Auto Profile Selection.

Simply click the desired profile to select it. A check mark appears beside the profile, and the client adapter attempts to establish a connection using the selected profile.

Show Connection Status

When you choose this option, the Connection Status window appears (see [Figure 8-5](#)).

Figure 8-5 **Connection Status Window**



This window provides information on the current status of your client adapter. [Table 8-3](#) interprets each element of the Connection Status window.

**Note**

You can also access the Connection Status window by double-clicking the ASTU icon.

Table 8-3 Connection Status Window Elements

Status Element	Description														
Active Profile	The network configuration (or profile) that your client adapter is currently using.														
Auto Profile Selection	Indicates whether your client adapter is using auto profile selection. Value: Enabled or Disabled														
Connection Status	<p>The operational mode of your client adapter.</p> <p>Value: Not Associated, Associated, Authenticating, Authenticated, Authentication Failed, or Authentication Failed Retrying</p> <table> <tr> <th>Connection Status</th><th>Description</th></tr> <tr> <td>Not Associated</td><td>The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td></tr> <tr> <td>Associated</td><td>The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).</td></tr> <tr> <td>Authenticating</td><td>The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.</td></tr> <tr> <td>Authenticated</td><td>The client adapter is associated to an access point, and the user is EAP authenticated.</td></tr> <tr> <td>Authentication Failed</td><td> <p>The client adapter is associated to an access point, but the user has failed to EAP authenticate.</p> <p>Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p> </td></tr> <tr> <td>Authentication Failed Retrying</td><td> <p>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.</p> <p>Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p> </td></tr> </table>	Connection Status	Description	Not Associated	The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).	Associated	The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).	Authenticating	The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.	Authenticated	The client adapter is associated to an access point, and the user is EAP authenticated.	Authentication Failed	<p>The client adapter is associated to an access point, but the user has failed to EAP authenticate.</p> <p>Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p>	Authentication Failed Retrying	<p>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.</p> <p>Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p>
Connection Status	Description														
Not Associated	The client adapter has not established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).														
Associated	The client adapter has established a connection to an access point (in infrastructure mode) or another client (in ad hoc mode).														
Authenticating	The client adapter is associated to an access point, and the EAP authentication process has begun but not yet succeeded.														
Authenticated	The client adapter is associated to an access point, and the user is EAP authenticated.														
Authentication Failed	<p>The client adapter is associated to an access point, but the user has failed to EAP authenticate.</p> <p>Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p>														
Authentication Failed Retrying	<p>The client adapter is associated to an access point, the user has failed to EAP authenticate, but another authentication attempt is being made.</p> <p>Note This status may appear very briefly or not at all as the authentication failure may result in the client adapter becoming disassociated, in which case the status reads <i>Not Associated</i>.</p>														

Table 8-3 *Connection Status Window Elements (continued)*

Status Element	Description
Link Quality	The client adapter's signal strength for all received packets. Value: Excellent, Good, Fair, Poor, or No Link
SSID	The name of the network to which your client adapter is currently associated. Note Refer to the SSID1 parameter in Table 5-2 for information on setting the client adapter's SSID.
Access Point Name	The name of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode, the access point was configured with a name, and Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later). Note This field shows up to 15 characters although the name of the access point may be longer.
Access Point IP Address	The IP address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode, the access point was configured with an IP address, and Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later). Note If Aironet Extensions are disabled, the IP address of the associated access point is shown as 0.0.0.0.
Current Receive Rate	The rate at which your client adapter is currently receiving data packets. Value: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps
Current Transmit Rate	The rate at which your client adapter is currently transmitting data packets. Value: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps
Client Adapter IP Address	The IP address of your client adapter.



CHAPTER 9

Routine Procedures

This chapter provides procedures for common tasks related to the client adapter.

The following topics are covered in this chapter:

- [Removing a Client Adapter, page 9-2](#)
- [Client Adapter Software Procedures, page 9-3](#)
- [Enabling or Disabling Your Client Adapter's Radio, page 9-11](#)

Removing a Client Adapter

Follow the instructions in this section to remove a PC-Cardbus card or PCI card from a computing device, when necessary.

**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.

Removing a PC-Cardbus Card

To remove a PC-Cardbus card after it is successfully installed and configured (such as when your laptop is to be transported), completely shut down your computer and pull the card directly out of the Cardbus slot. When the card is reinserted and the computer is rebooted, your connection to the network should be re-established.

**Note**

If you need to remove your PC-Cardbus card but do not want to shut down your computer, double-click the **Safely Remove Hardware** icon in the Windows system tray, choose the Cisco Aironet client adapter you want to remove under Hardware devices, click **Stop**, and click **OK** to close each open window. Then pull the card directly out of the card slot.

Removing a PCI Card

Because PCI client adapters are installed inside desktop computers, which are not designed for portable use, you should have little reason to remove the adapter. However, instructions are provided below in case you need to remove your PCI card.

-
- | | |
|---------------|--|
| Step 1 | Completely shut down your computer. |
| Step 2 | Remove the computer cover. |
| Step 3 | Remove the screw from the top of the CPU back panel above the PCI expansion slot that holds your client adapter. |
| Step 4 | Disassemble the antenna from the base. |
| Step 5 | Pull up firmly on the client adapter to release it from the slot and carefully tilt the adapter to slip its antenna through the opening near the slot. |
| Step 6 | Reinstall the screw on the CPU back panel and replace the computer cover. |
-

Client Adapter Software Procedures

This section provides instructions for the following procedures:

- Upgrading the client adapter software, [page 9-3](#)
- Manually installing or upgrading the client adapter driver, [page 9-6](#)
- Uninstalling the client adapter software, [page 9-6](#)
- ADU procedures, [page 9-7](#)
- ASTU procedures, [page 9-11](#)

Upgrading the Client Adapter Software

Follow these steps to upgrade your Cisco Aironet CB21AG or PI21AG client adapter software to a more recent release using the settings that were selected during the last installation.

**Note**

If you want to upgrade your client adapter software using new installation settings, uninstall the previous installation (see the instructions on [page 9-6](#)); then install the new software (see the instructions on [page 3-9](#)).

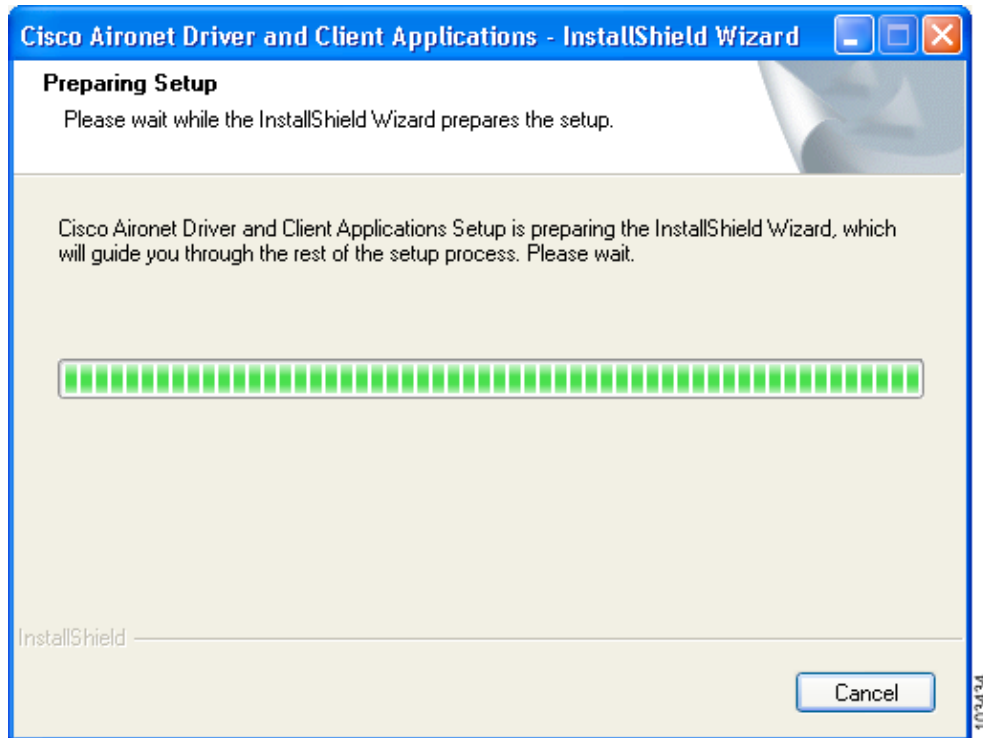
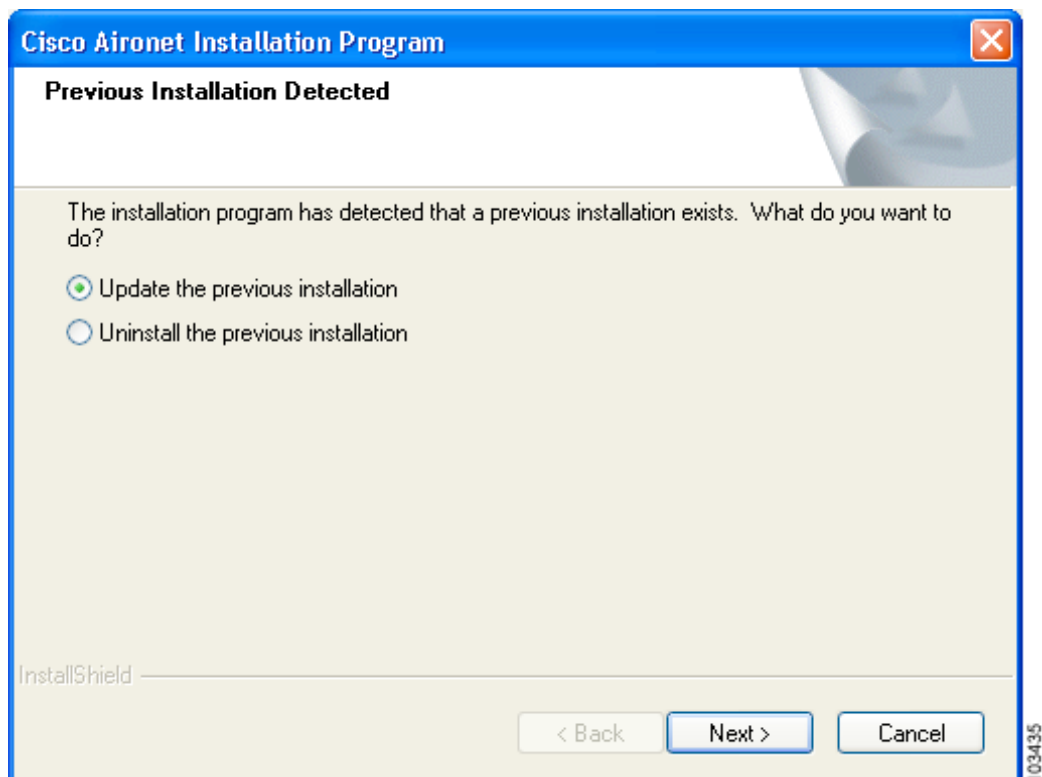
Step 1 Make sure the client adapter is inserted into your computer.

**Note**

If your client adapter is not inserted, the installation continues, but the driver installation is incomplete. You must manually upgrade 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 2 Use Windows Explorer to find the Install Wizard file.

Step 3 Double-click the file. The “Starting InstallShield Wizard” message appears followed by the Preparing Setup window (see [Figure 9-1](#)) and the Previous Installation Detected window (see [Figure 9-2](#)).

Figure 9-1 *Preparing Setup Window***Figure 9-2** *Previous Installation Detected Window*

Step 4 Choose **Update the previous installation** and click **Next**.

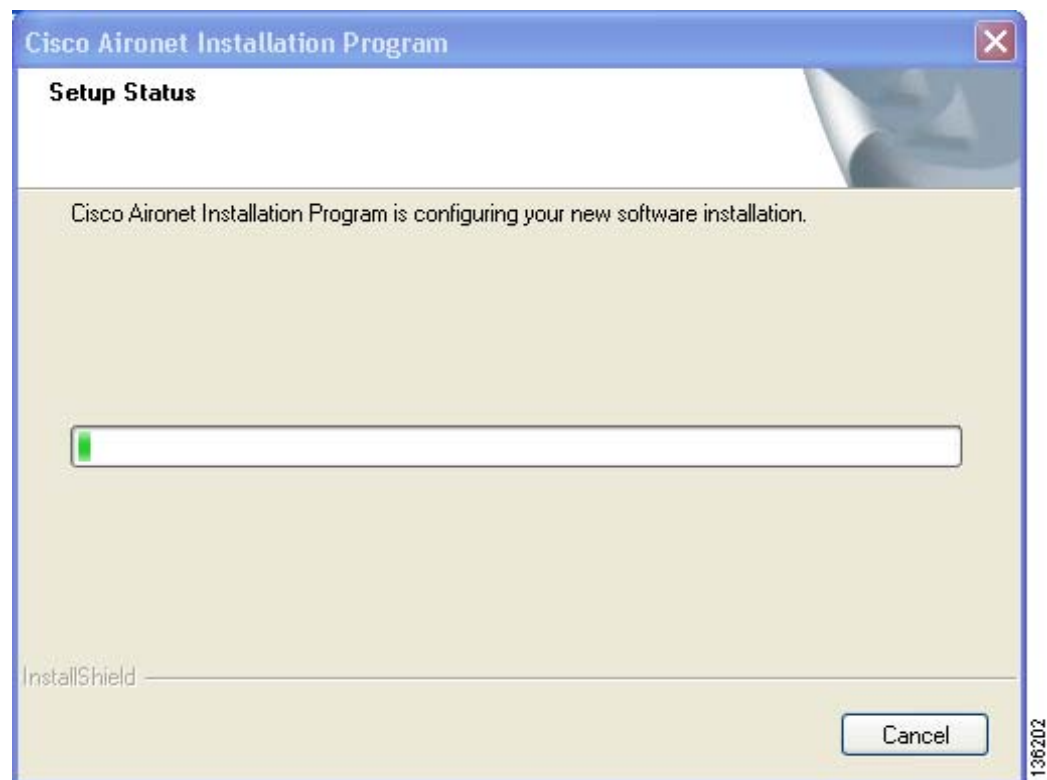
Step 5 When a message appears indicating that you are required to restart your computer at the end of the installation process, click **Yes**.



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

The Setup Status window appears (see [Figure 9-3](#)).

Figure 9-3 Setup Status Window



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

Step 6 When a message appears indicating that your computer needs to be rebooted, click **OK** and allow your computer to restart. The client adapter's software has been upgraded.

Manually Installing or Upgrading the Client Adapter Driver

If you installed or upgraded the client adapter software without the client adapter inserted into your computer, the driver installation is incomplete. Follow these steps to manually install or upgrade the client adapter driver.

-
- Step 1** Insert the client adapter into your computer.
- Step 2** Click **Start > Settings > Control Panel > Administrative Tools > Computer Management > Device Manager > Network Adapters**.
- Step 3** Right-click **Cisco Aironet 802.11a/b/g Wireless Adapter**.
- Step 4** Click **Properties**.
- Step 5** Choose the **Driver** tab and click **Update Driver**.
- Step 6** Use the update wizard to select the driver from the *root\windows\system32* directory (such as *C:\Windows\system32*) and finish the update procedure.
- Step 7** Follow these steps to activate the newly updated driver:
- Click **Start > Settings > Control Panel > Network Connections** or **Network and Dial-up Connections**.
 - Right-click the wireless connection.
 - Choose **Disable**.
 - Repeat Steps a and b.
 - Choose **Enable**.
-

Uninstalling the Client Adapter Software

This section provides instructions for uninstalling the software for your Cisco Aironet CB21AG or PI21AG client adapter. This procedure is necessary if you want to remove installed client adapter software from your computer or downgrade to a previous release.

**Note**

If you want to downgrade to an earlier release of client adapter software, use this procedure to uninstall the current software. Then install the older software.

**Note**

When you uninstall the client adapter software, any existing profiles and stored PAC files are removed. If you want to save your profiles for later use, follow the instructions in [Chapter 4](#) to export your profiles before uninstalling the software.

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



Note If your client adapter is not inserted, the driver cannot be uninstalled.

Step 2 Use Windows Explorer to find the Install Wizard file.



Note If you do not have the Install Wizard's setup.exe file, you can access the client adapter software by clicking **Control Panel > Add/Remove Programs > Cisco Aironet Installation Program > Remove**. Then follow the steps below beginning with the Preparing Setup window in [Step 3](#).

Step 3 Double-click the file. The "Starting InstallShield Wizard" message appears followed by the Preparing Setup window (see [Figure 9-1](#)) and the Previous Installation Detected window (see [Figure 9-2](#)).

Step 4 Choose **Uninstall the previous installation** and click **Next**.

Step 5 When a message appears indicating that you are required to restart your computer at the end of the operation, click **Yes**. (If you click **No**, you are asked to confirm your decision. If you proceed, the installation process terminates.)

Step 6 When prompted to confirm your decision, click **OK**. The process to uninstall the files begins.

Step 7 When prompted to uninstall the device driver, click **Yes**.

Step 8 When a message appears indicating that your computer needs to be rebooted, click **OK** and allow your computer to restart. The client adapter software and its program folder have been uninstalled.



Note This procedure does not remove the Install Wizard file. If you want to remove it from your computer, find the file using Windows Explorer and delete it.

ADU Procedures

This section provides instructions for the following procedures:

- Opening ADU, [page 9-8](#)
- Exiting ADU, [page 9-8](#)
- Finding the version of ADU and other software components, [page 9-9](#)
- Viewing client adapter information, [page 9-10](#)
- Accessing online help, [page 9-10](#)

Opening ADU

To open ADU, perform one of the following:

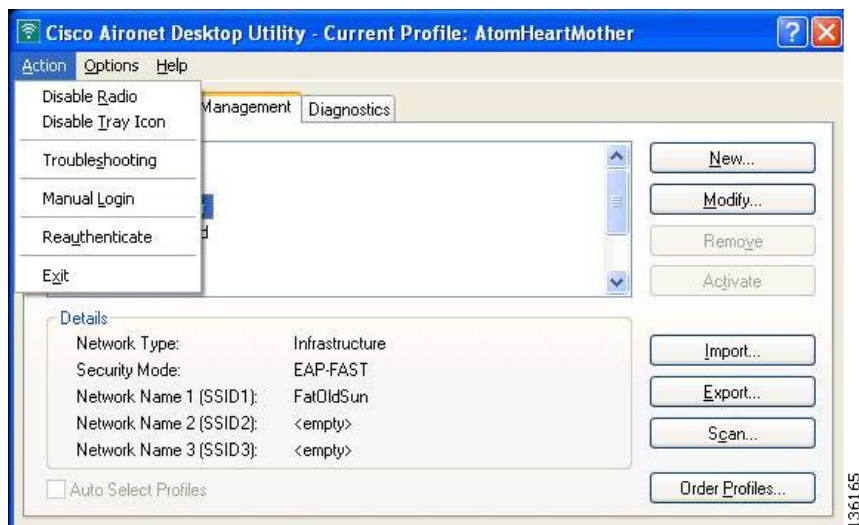
- Double-click the **Aironet Desktop Utility** icon on your desktop.
- Choose **Aironet Desktop Utility** from the folder in the Windows Start Menu that you chose during installation (the default location is **Start > Programs > Cisco Aironet > Aironet Desktop Utility**).
- Right-click the ASTU icon in the Windows system tray and choose **Open Aironet Desktop Utility**.

Exiting ADU

To exit ADU, perform one of the following:

- Choose **Exit** from the Action drop-down menu (see [Figure 9-4](#)).
- Right-click the ASTU icon in the Windows system tray and choose **Exit**.

Figure 9-4 Action Drop-Down Menu

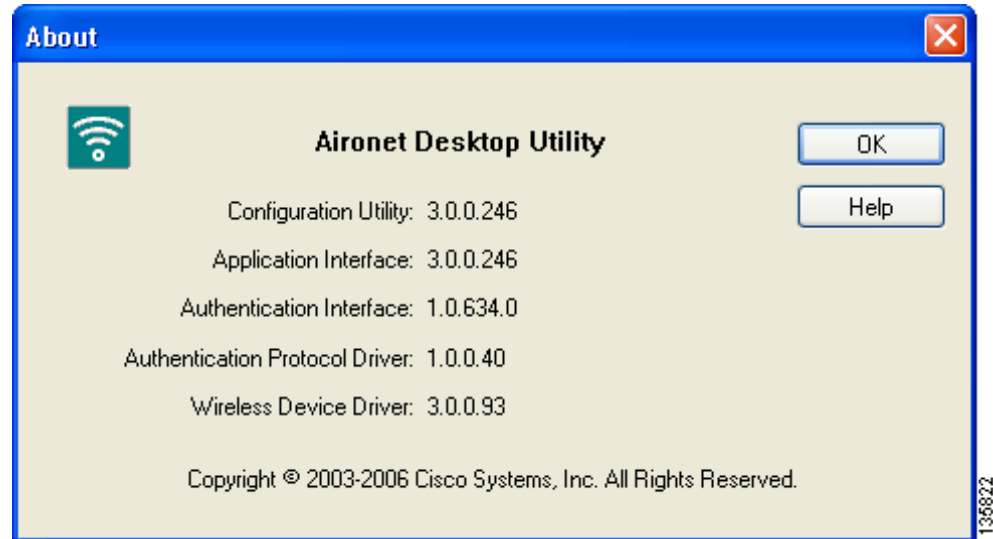


Finding the Version of ADU and Other Software Components

Follow these steps to find the current version of ADU and other software components.

-
- Step 1** Open ADU.
- Step 2** Choose the **About Aironet Desktop Utility** option from the Help drop-down menu. The About window appears (see [Figure 9-5](#)).

Figure 9-5 *About Window*



[Table 9-1](#) lists and describes the software components shown in the About window.

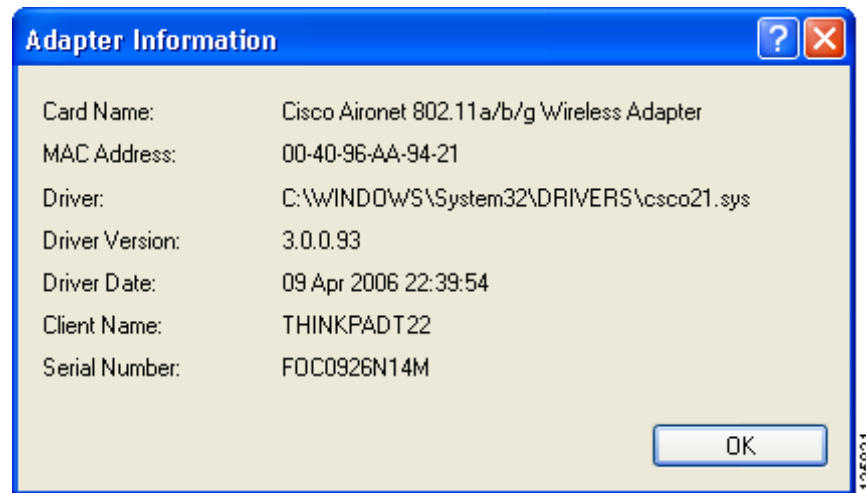
Table 9-1 *Software Components Shown in About Window*

Software Component	Description
Configuration Utility	Aironet Client Administration Utility (ACAU) version
Application Interface	Aironet Desktop Utility (ADU) version
Authentication Interface	Supplicant version
Authentication Protocol Driver	Protocol driver version
Wireless Device Driver	Windows NDIS miniport driver version

Viewing Client Adapter Information

To view information about your client adapter, open ADU. Click the **Diagnostics** tab and **Adapter Information**. The Adapter Information window appears (see [Figure 9-6](#)).

Figure 9-6 *Adapter Information Window*



[Table 9-2](#) interprets each element of the Adapter Information window.

Table 9-2 *Adapter Information*

Status	Description
Card Name	A description of your client adapter.
MAC Address	The MAC address assigned to your client adapter at the factory.
Driver	The filename and location of your client adapter's driver.
Driver Version	The version of the NDIS device driver that is currently installed on your computer.
Driver Date	The date that your client adapter's driver was created.
Client Name	The name your client adapter uses when it associates to an access point. Note Refer to the Client Name parameter in Table 5-2 for information on setting the client name.
Serial Number	The serial number of your client adapter.

Click **OK** to close the Adapter Information window.

Accessing Online Help

To access the ADU online help, open ADU. Then choose the **Aironet Desktop Utility Help** option from the Help drop-down menu.

ASTU Procedures

Refer to [Chapter 8](#) for instructions on using ASTU.

Enabling or Disabling Your Client Adapter's Radio

Your client adapter's radio can be enabled or disabled. Disabling the radio prevents the adapter from transmitting RF energy. You might want to disable the client adapter's radio in the following situations:

- You are not transmitting data and want to conserve battery power.
- You are using a laptop on an airplane and want to prevent the adapter's transmissions from potentially interfering with the operation of certain devices.

When the radio is enabled, it periodically sends out probes even if it is not associated to an access point (in infrastructure mode) or another client (in ad hoc mode), as required by the 802.11 specification. Therefore, it is important to disable it around devices that are susceptible to RF interference.

**Note**

Your client adapter is not associated while its radio is disabled.

**Note**

If your client adapter's radio is disabled before your computer enters standby or hibernate mode or before you reboot the computer, the radio remains disabled when the computer resumes. You must enable the radio to resume operation.

You can use ADU or ASTU to enable or disable the client adapter's radio. Follow the instructions below to use ADU or refer to the [“Enable/Disable Radio” section on page 8-7](#) to use ASTU.

If your client adapter's radio is enabled, open ADU and choose **Disable Radio** from the Action drop-down menu (see [Figure 9-4](#)) to disable the radio.

If your client adapter's radio is disabled, open ADU and choose **Enable Radio** from the Action drop-down menu (see [Figure 9-4](#)) to enable the radio.



CHAPTER 10

Troubleshooting

This chapter provides information for diagnosing and correcting common problems that may occur when you install and operate the client adapter.

The following topics are covered in this chapter:

- [Accessing the Latest Troubleshooting Information, page 10-2](#)
- [Interpreting the Indicator LEDs, page 10-2](#)
- [Troubleshooting the Client Adapter, page 10-3](#)
- [Disabling the Microsoft Wireless Configuration Manager \(Windows XP Only\), page 10-7](#)
- [Disabling the Microsoft 802.1X Supplicant \(Windows 2000 Only\), page 10-8](#)
- [Client Adapter Recognition Problems, page 10-8](#)
- [Resolving Resource Conflicts, page 10-8](#)
- [Problems Associating to an Access Point, page 10-10](#)
- [Problems Connecting to the Network, page 10-10](#)
- [Prioritizing Network Connections, page 10-11](#)
- [Troubleshooting with Diagnostic Channel Mode, page 10-11](#)
- [Parameters Missing from Profile Management Windows, page 10-17](#)
- [Windows Wireless Network Connection Icon Shows Unavailable Connection \(Windows XP Only\), page 10-17](#)
- [Error Messages, page 10-18](#)

Accessing the Latest Troubleshooting Information

This chapter provides basic troubleshooting tips for your client adapter. For more up-to-date and detailed troubleshooting information, refer to the TAC web site. To access this site, go to Cisco.com, click **Technical Support > Product Support > Wireless**. Then choose your product and click **Troubleshooting** to find information on the problem you are experiencing.

**Note**

We recommend that you use the latest firmware and the latest version of the Aironet Desktop Utility for all client adapters. You can download the latest versions at this URL:

<http://tools.cisco.com/support/downloads/pub/MDFTree.x?butype=wireless>

Interpreting the Indicator LEDs

The client adapter shows messages through its two LEDs. [Table 10-1](#) interprets the LED operating messages.

Table 10-1 *LED Operating Messages*

Status LED (green)	Activity LED (amber)	Condition
Off	Off	Client adapter is not receiving power.
Blinking slowly	Off	Client adapter is in power save mode.
On	Off	Client adapter has awakened from power save mode.
Alternating blink:		Client adapter is scanning for the wireless network for which it is configured.
On	Off	
Off	On	
Blinking slowly	Blinking slowly	Client adapter is associated to an access point (in infrastructure mode) or another client (in ad hoc mode).
Blinking quickly	Blinking quickly	Client adapter is transmitting or receiving data while associated to an access point (in infrastructure mode) or another client (in ad hoc mode).

Troubleshooting the Client Adapter

This section provides troubleshooting tips should you encounter problems with your client adapter. Use [Table 10-2](#) to quickly find specific troubleshooting information.

Table 10-2 **Troubleshooting Information**

Troubleshooting Information	Page Number
Using the troubleshooting utility	10-3
Disabling the Microsoft Wireless Configuration Manager	10-7
Disabling the Microsoft 802.1X supplicant	10-8
Client adapter recognition problems	10-8
Resolving resource conflicts	10-8
Problems associating to an access point	10-10
Problems connecting to the network	10-10
Prioritizing network connections	10-11
Parameters missing from Profile Management windows	10-17
Windows Wireless Network Connection icon shows unavailable connection (Windows XP only)	10-17

Using the Cisco Aironet Troubleshooting Utility

The Cisco Aironet Troubleshooting Utility enables you to identify and resolve configuration and association problems with your client adapter. It is meant to be used only when the client adapter is in infrastructure mode because it assesses the connection between the adapter and an access point.

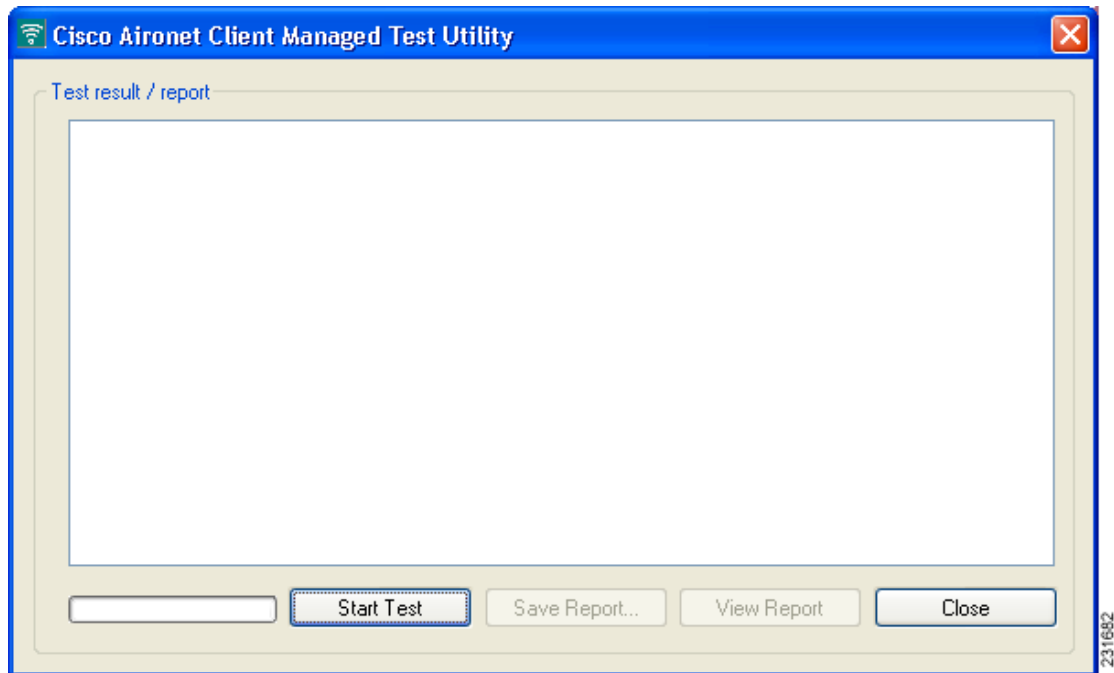
Follow the instructions in one of the subsections below to use the utility to diagnosis your client adapter's operation, save a detailed report to a text file, or access online help.

Diagnosing Your Client Adapter's Operation

- Step 1** Perform one of the following to activate the troubleshooting utility:
- Open ADU; choose **Client Managed Test** from the Action drop-down menu.
 - Open ADU; click the **Diagnostics** tab and **Client Managed Test**.
 - Right-click the ASTU icon; choose **Client Managed Test** from the pop-up menu.

The Cisco Aironet Troubleshooting Utility window appears (see [Figure 10-1](#)).]

Figure 10-1 Troubleshooting Utility Window

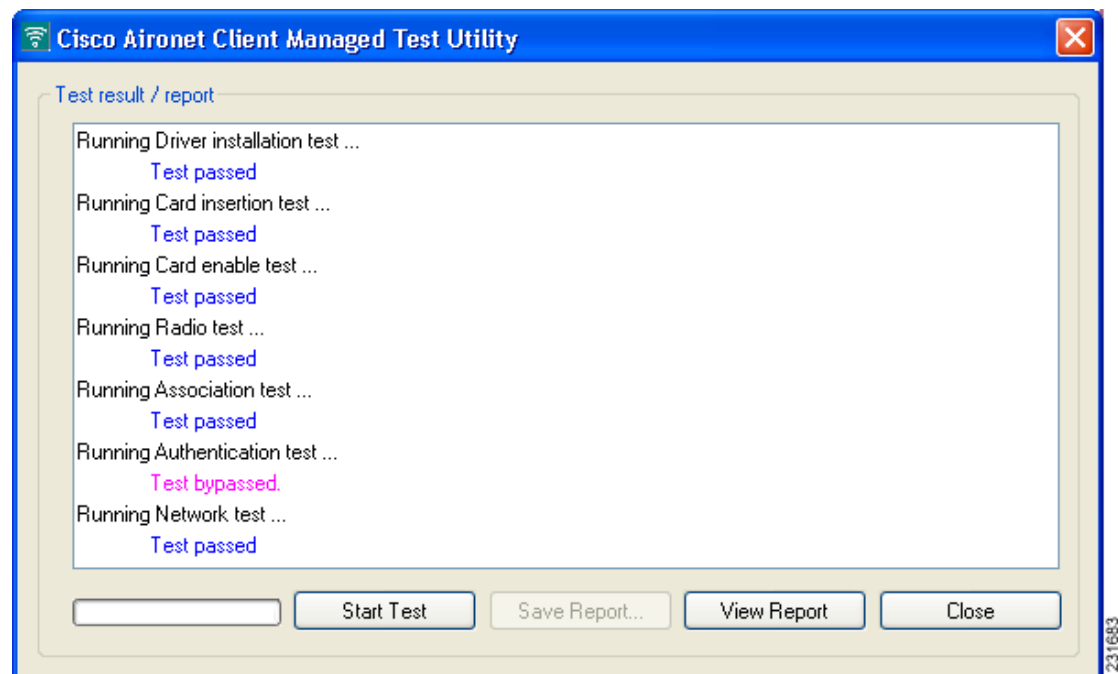


Step 2 Click **Start Test**. The utility performs the following series of seven tests to check the operation of your client adapter and to identify specific problems if they exist:

1. Driver installation test
2. Card insertion test
3. Card enable test
4. Radio test
5. Association test
6. Authentication test
7. Network test

The utility runs and then displays the results for each test (see [Figure 10-2](#)).

Figure 10-2 Troubleshooting Utility Window (with Test Results)



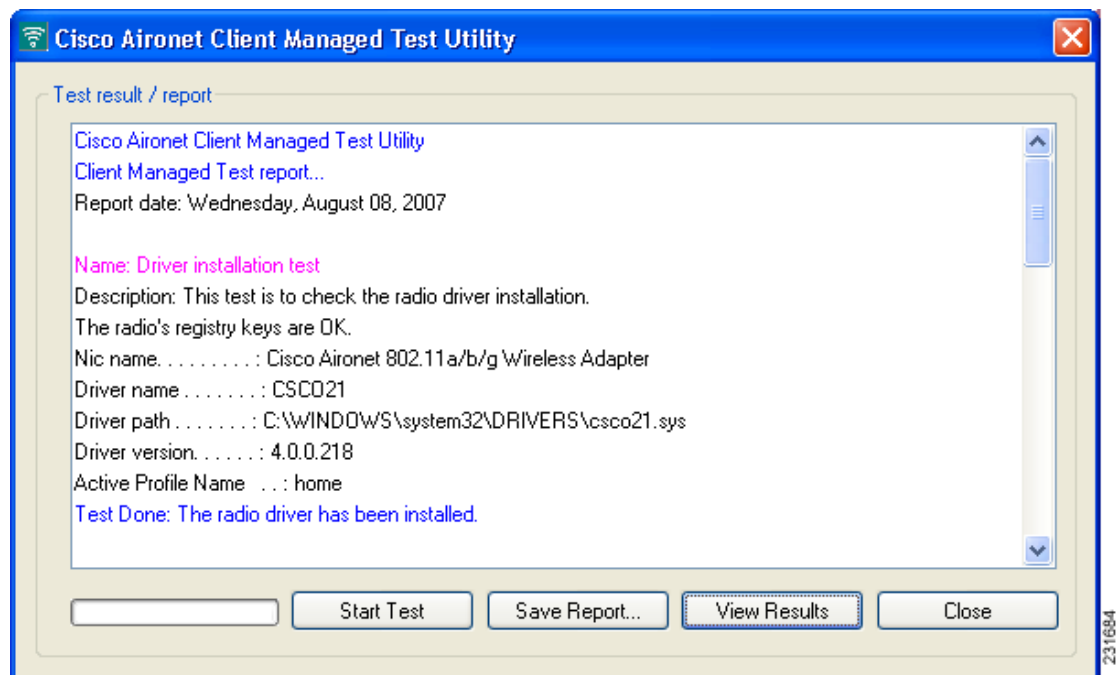
One of the following status messages appears for each test:

- **Test passed**—The test completed successfully.
- **Test bypassed**—The test was skipped because it was not required for the active profile.
- **Test failed**—The test failed. Follow the instructions in [Step 3](#) to obtain more details.



Note You can click **Stop Test** at any time to stop the testing process, or you can click **Start Test** after the testing process has stopped to run the test again.

Step 3 To view more detailed information, click **View Report**. A report appears that provides more detailed results for your client adapter (see [Figure 10-3](#)).

Figure 10-3 Troubleshooting Utility Window (Detailed Report)**Note**

The report contains valuable information that, if necessary, could be used by your system administrator or TAC to analyze any problems. Follow the instructions in the next section if you want to save the report to a text file.

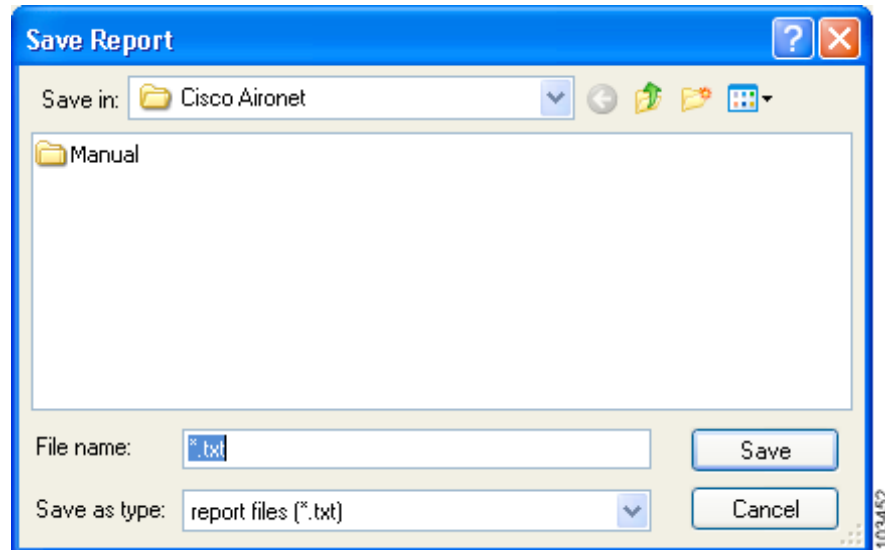
- Step 4** If a problem is discovered, the report provides some possible repair suggestions. Follow the repair instructions carefully and run the troubleshooting utility again.

Saving the Detailed Report to a Text File

Follow the steps below to save the detailed troubleshooting report to your computer's hard drive.

- Step 1** Click **Save Report**. The Save Report window appears (see [Figure 10-4](#)).

Figure 10-4 Save Report Window



- Step 2** Enter a name for the detailed report in the File name field. The report is saved as a *.txt file.
- Step 3** Use the Save in box at the top of the window to specify the location on your computer's hard drive where the file will be saved.



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

- Step 4** Click **Save**. The file is saved as a text file in the location specified.

Disabling the Microsoft Wireless Configuration Manager (Windows XP Only)

If any conflicts arise between ADU and the Microsoft Wireless Configuration Manager on a computer running Windows XP, follow these steps to disable the Microsoft configuration manager.



Note Disabling the Microsoft Wireless Configuration Manager on Windows XP also disables the Microsoft 802.1X supplicant. If you chose to configure your client adapter using ADU during installation, the Microsoft 802.1X supplicant should already be disabled.

-
- Step 1** Double-click **My Computer**, **Control Panel**, and **Network Connections**.
 - Step 2** Right-click **Wireless Network Connection** and click **Properties**.
 - Step 3** Click the **Wireless Networks** tab and uncheck the **Use Windows to configure my wireless network settings** check box.
 - Step 4** Click **OK** to save your settings.
-

Disabling the Microsoft 802.1X Supplicant (Windows 2000 Only)

The Microsoft 802.1X supplicant can be installed on a computer running Windows 2000 through either a Microsoft hot fix or Windows 2000 Service Pack 4. If any conflicts arise between ADU and the Microsoft 802.1X supplicant, follow these steps to disable the Microsoft supplicant on a Windows 2000 computer.



Note

The Microsoft 802.1X supplicant, if installed, should have been disabled during installation.

-
- Step 1** Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**. Right-click **Local Area Connection**. Click **Properties**. The Local Area Connection Properties window appears.
 - Step 2** Click the **Authentication** tab.
 - Step 3** Uncheck the **Enable network access control using IEEE 802.1X** or **Enable IEEE 802.1x authentication for this network** check box.
 - Step 4** Click **OK** to save your settings.
-

Client Adapter Recognition Problems

If your computer's PCMCIA adapter does not recognize your client adapter, check your computer's BIOS and make sure that the PC card controller mode is set to PCIC compatible.



Note

A computer's BIOS varies depending on the manufacturer. For support on BIOS-related issues, consult your computer's manufacturer.

Resolving Resource Conflicts

If you encounter problems while installing your client adapter on a computer running a Windows operating system, you may need to specify a different interrupt request (IRQ) or I/O range for the adapter.

The default IRQ for the client adapter is IRQ 10, which may not work for all systems. Follow the steps for your specific operating system to obtain an available IRQ.

During installation the adapter's driver installation script scans for an unused I/O range. The installation can fail if the I/O range found by the driver installation script is occupied by another device but not reported by Windows. An I/O range might not be reported if a device is physically present in the system but not enabled under Windows. Follow the steps for your specific operating system to obtain an available I/O range.

Resolving Resource Conflicts in Windows 2000

-
- 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** and the Cisco Systems Wireless LAN Adapter.
 - Step 4** In the General window, the Device Status field indicates if a resource problem exists. If a problem is indicated, click the **Resources** tab.
 - Step 5** Uncheck the **Use automatic settings** check box.
 - Step 6** Under Resource Settings or Resource Type, click **Input/Output Range**.
 - Step 7** Look in the Conflicting Device list at the bottom of the window. If it indicates that the range is being used by another device, click the **Change Setting** button.
 - Step 8** Scroll through the ranges in the Value dialog box and choose one that does not conflict with another device. The Conflict Information window at the bottom of the window indicates if the range is already being used.
 - Step 9** Click **OK**.
 - Step 10** Under Resource Settings or Resource Type, click **Interrupt Request**.
 - Step 11** Look in the Conflicting Device list at the bottom of the window. If it indicates that the IRQ is being used by another device, click the **Change Setting** button.
 - Step 12** Scroll through the IRQs in the Value dialog box and choose one that does not conflict with another device. The Conflict Information window at the bottom of the window indicates if the IRQ is already being used.
 - Step 13** Click **OK**.
 - Step 14** Reboot your computer.
-

Resolving Resource Conflicts in Windows XP

**Note**

These instructions assume you are using the Windows XP classic view, not the category view.

-
- Step 1** Double-click **My Computer**, **Control Panel**, and **System**.
 - Step 2** Click the **Hardware** tab and **Device Manager**.
 - Step 3** Under Network Adapters, double-click the Cisco Systems Wireless LAN Adapter.
 - Step 4** In the General window, the Device Status field indicates if a resource problem exists. If a problem is indicated, click the **Resources** tab.

- Step 5** Uncheck the **Use automatic settings** check box.
 - Step 6** Under Resource Settings, click **I/O Range**.
 - Step 7** Look in the Conflicting Device list at the bottom of the window. If it indicates that the range is being used by another device, click the **Change Setting** button.
 - Step 8** Scroll through the ranges in the Value dialog box and choose one that does not conflict with another device. The Conflict Information window at the bottom of the window indicates if the range is already being used.
 - Step 9** Click **OK**.
 - Step 10** Under Resource Settings, click **IRQ**.
 - Step 11** Look in the Conflicting Device list at the bottom of the window. If it indicates that the IRQ is being used by another device, click the **Change Setting** button.
 - Step 12** Scroll through the IRQs in the Value dialog box and choose one that does not conflict with another device. The Conflict Information window at the bottom of the window indicates if the IRQ is already being used.
 - Step 13** Click **OK**.
 - Step 14** Reboot your computer.
-

Problems Associating to an Access Point

Follow the instructions below if your client adapter fails to associate to an access point.

- If possible, move your workstation a few feet closer to an access point and try again.
- Make sure that the client adapter is securely inserted into your computer's client adapter slot.
- If you are using a PCI card, make sure that the antenna is securely attached.
- Make sure that the access point is turned on and operating.
- Check that all parameters are set properly for both the client adapter and the access point. These include the SSID, EAP authentication, WEP activation, network type, channel, etc.
- Follow the instructions in the previous section to resolve any resource conflicts.
- If the client adapter still fails to establish contact, refer to the [“Obtaining Technical Assistance”](#) section in the Preface for technical support information.



Note

A client might not be able to associate with an AP if the client is using a very old version of the firmware and the client utility. Use the latest version of the firmware and the client utility for all client adapters, and ensure that all client adapters in the WLAN use the same version of firmware.

Problems Connecting to the Network

After you have installed the appropriate driver and client utilities, contact your IS department if you have a problem connecting to the network. Proxy server, network protocols, and further authentication information might be needed to connect to the network.

**Note**

When using release 4.0, you might encounter a conflict with third-party supplicants (such as the Juniper Odyssey) that causes the Cisco client adapter to lose connection. If you encounter such a conflict, disable third-party supplicants.

Prioritizing Network Connections

If your computer has more than one network adapter enabled (such as a Cisco Aironet client adapter and an Ethernet card), you can choose which one to use by assigning a priority to your network connections.

Follow the steps below to prioritize your network connections.

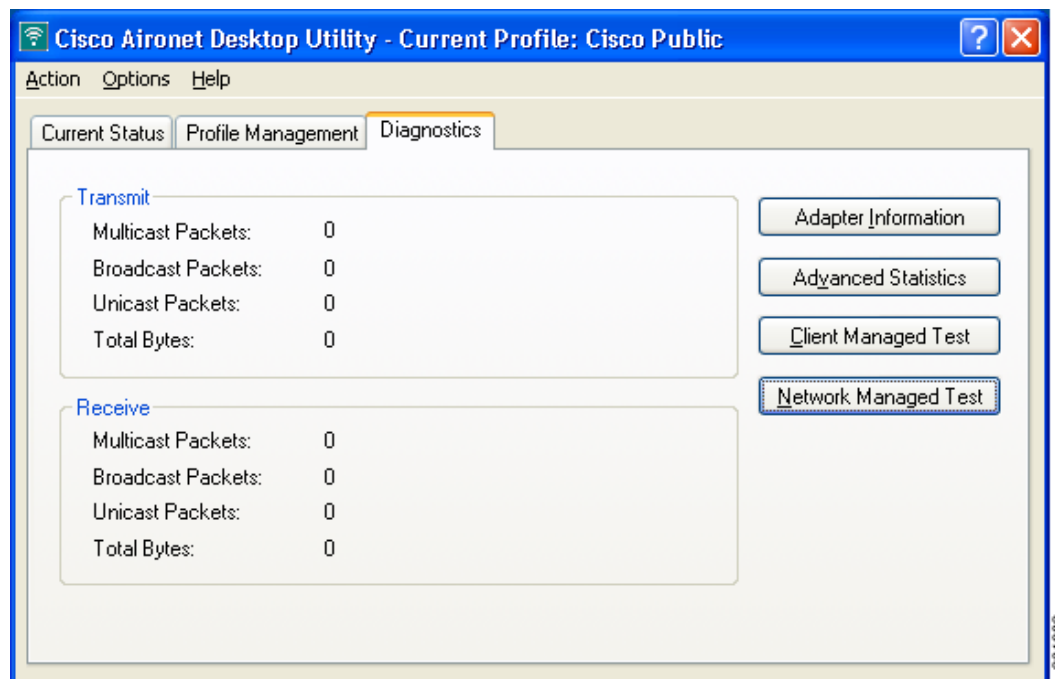
-
- Step 1** Right-click the **My Network Places** icon on your desktop.
 - Step 2** Click **Properties**.
 - Step 3** Choose the **Advanced** menu option at the top of the window.
 - Step 4** Click **Advanced Settings**. Your network connections are listed in the Connections box on the Adapters and Bindings tab.
 - Step 5** Use the arrows beside the Connections box to move the network connection that you want to use to the top.
 - Step 6** Click **OK**.

Troubleshooting with Diagnostic Channel Mode

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

DC mode can only be started manually. To start DC mode, follow these steps:

-
- Step 1** Verify that the client adapter radio is enabled. If the radio is not enabled, enable it.
 - Step 2** Open the ADU.
 - Step 3** Click the **Diagnostics** tab (see [Figure 10-5](#)).

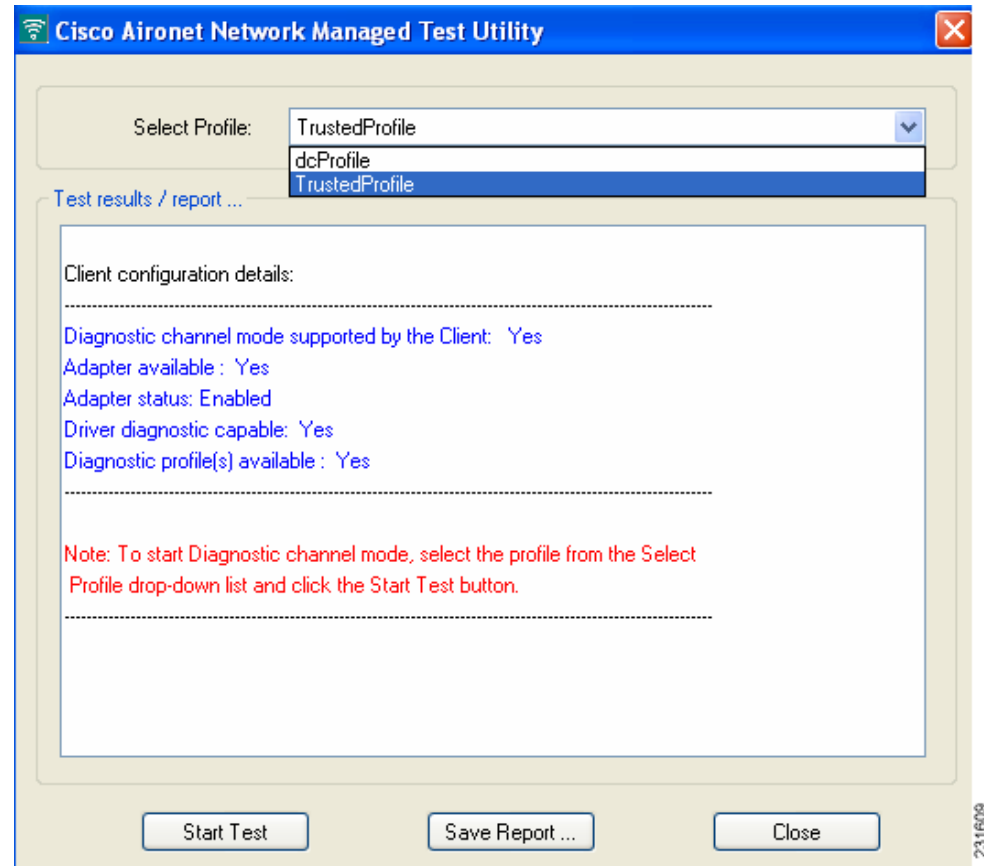
Figure 10-5 Cisco Aironet Desktop Utility—Diagnostics Tab

Step 4 In the Diagnostics tab, click the **Network Managed Test** button. The Cisco Aironet Network Managed Test Utility window appears and displays the results of a set of local pre-tests that the client adapter runs to determine if it can participate in DC mode testing: These pre-tests check the following:

- The client adapter is inserted.
- The client adapter is enabled.
- The client adapter supports DC mode.
- The driver version is adequate.
- There are no communication issues between the driver and the adapter; adequate communication is verified through the query of an OID.
- There is at least one profile that is capable of participating in DC mode testing.

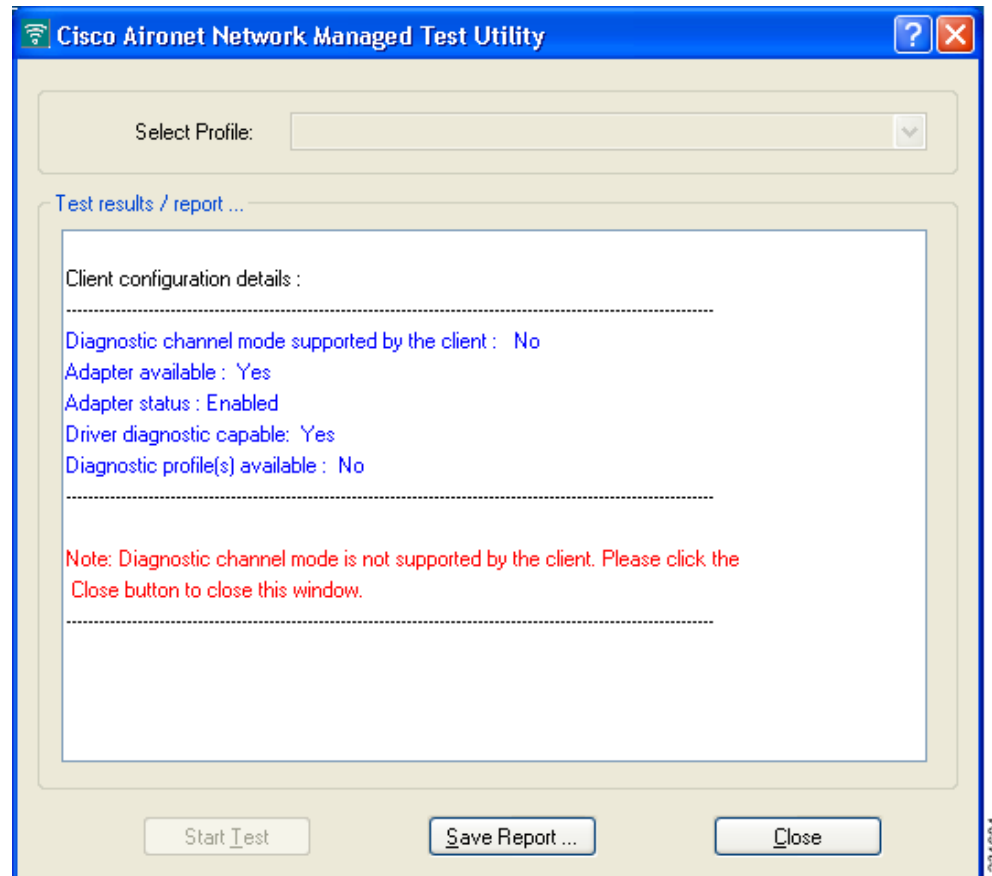
If the client adapter passes all pre-test conditions, the Select Profile drop-down list shows all profiles that can participate in DC mode(see [Figure 10-6](#)). Continue on to [Step 5](#).

Figure 10-6 Cisco Aironet Network Managed Test Utility—Pre-Test Success



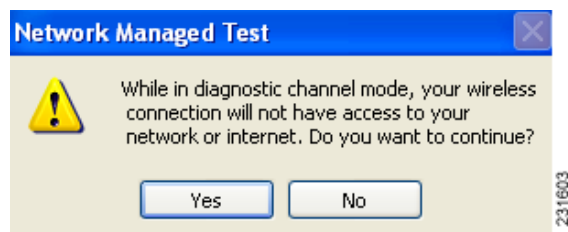
If the client adapter cannot participate in DC mode, the reason is displayed in the Network Managed Test Utility window, and the Select Profile drop-down list and the Start Test button are dimmed. (see Figure 10-7). The client adapter cannot continue. Click the **Close** button to close the window.

Figure 10-7 Cisco Aironet Network Managed Test Utility—Pre-Test Failure



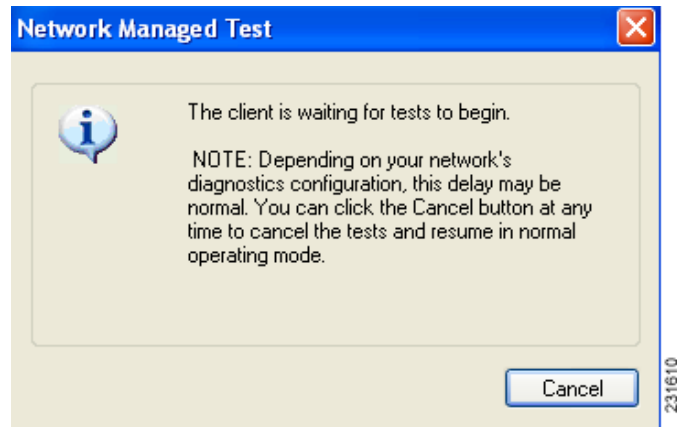
- Step 5** If the client adapter can participate in DC mode, select the desired profile from the **Select Profile** drop-down list. The current active profile is the default profile if it is capable of running in DC mode.
- Step 6** Click the **Start Test** button. A Network Managed Test warning window appears to remind you that you will not have access to network or the Internet while the client adapter is in DC mode (see Figure 10-8).

Figure 10-8 Network Managed Test—No Connection to Network or Internet



- Step 7** In the Network Managed Test warning window, click the **Yes** button to continue in DC mode. Click the **No** button to cancel. If the client adapter cannot associate in DC mode to the wireless LAN infrastructure device within five seconds, another Network Managed Test warning window appears to inform you that the client adapter is waiting for DC mode tests to begin (see [Figure 10-9](#)).

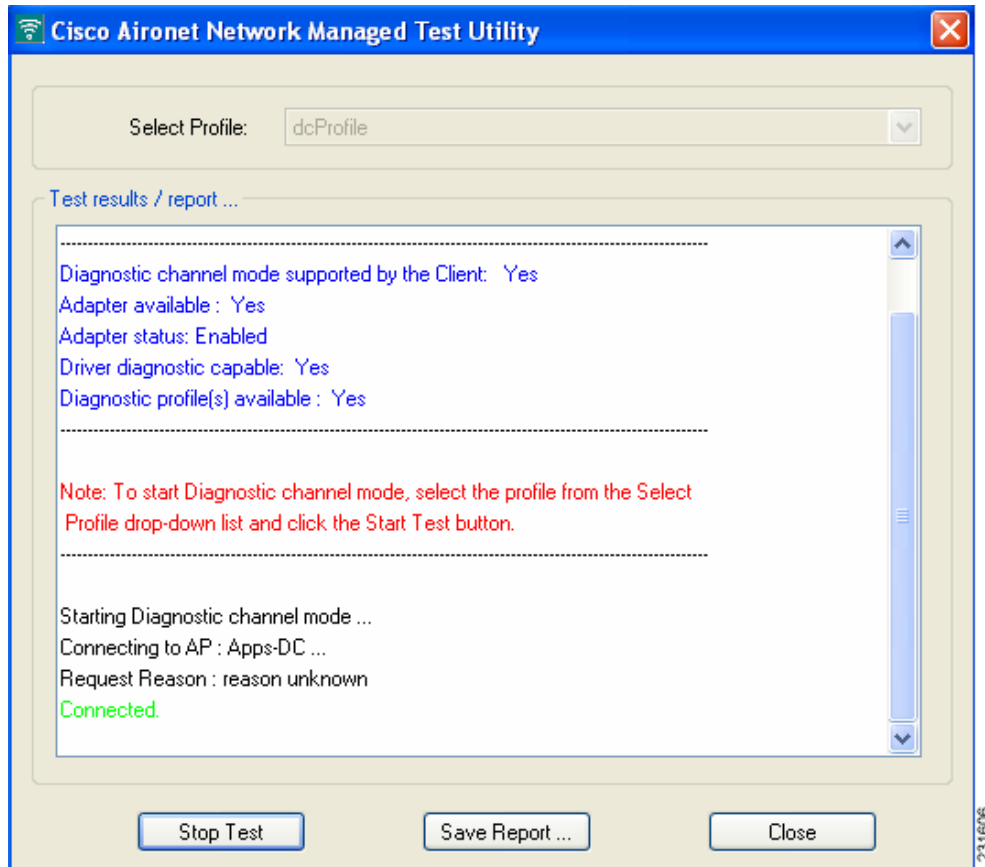
Figure 10-9 *Network Managed Test—Client Waiting for Tests to Begin*



Click the **Cancel** button to cancel DC mode testing and return to normal operating mode. If you want to continue DC mode testing, continue to wait.

- Step 8** During DC mode testing, you can follow test progress and examine test result in the Network Managed Test Utility window (see [Figure 10-10](#)).

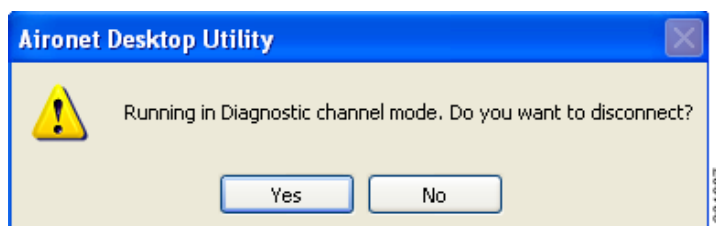
Figure 10-10 Cisco Aironet Network Managed Test Utility—Progress and Results



You can stop DC mode testing at any time by clicking on the **Stop Test** button.

While the client is in DC mode, if you click on the **Close** button, an Aironet Desktop Utility window appears to confirm that you want to stop running in DC mode (see [Figure 10-11](#)).

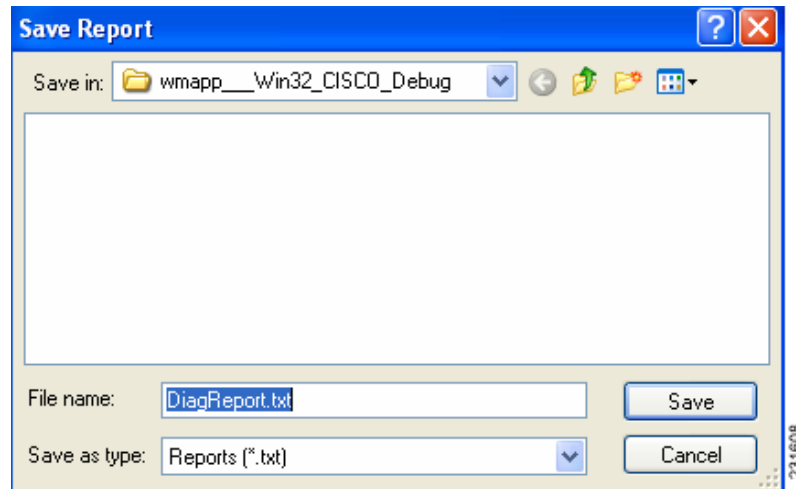
Figure 10-11 Aironet Desktop Utility—Stop Running in DC Mode



Click the **Yes** button to disconnect, or click the **No** button to continue.

- Step 9** You can click the **Save Report** button to save the test results. Clicking this button generates a text file that contains the results. You can save this file to the desired folder on your PC (see [Figure 10-12](#)). Your network administrator can then use the test results in this report to troubleshoot any issues between the client adapter and the infrastructure device.

Figure 10-12 Save Report Window



Note You can save a report even if the tests are not complete.

Parameters Missing from Profile Management Windows

If some parameters are unavailable on the Profile Management windows, your system administrator may have used an administrative tool to deactivate these parameters. In this case, these parameters cannot be selected.

Windows Wireless Network Connection Icon Shows Unavailable Connection (Windows XP Only)

If your computer is running Windows XP and you configured your client adapter using ADU, the Windows Wireless Network Connection icon in the Windows system tray may be marked with a red X and show an unavailable connection even though a wireless connection exists. This is caused by a conflict between the wireless network settings of ADU and Windows XP. Simply ignore the Windows icon and use the ASTU icon to check the status of your client adapter's wireless connection.

Error Messages

This section provides a list of error messages that may appear during the installation, configuration, or use of your client adapter. The messages are listed in alphabetical order within each section, and an explanation as well as a recommended user action are provided for each message.

Error Message ADU can hold only 16 profiles. To add another profile, either delete an existing profile or modify an existing profile.

Explanation You attempted to create a new profile, import a profile, or activate a profile from the scan list on the Available Infrastructure and Ad Hoc Networks window after the maximum number of profiles had already been reached.

Recommended Action Modify an existing profile or delete a profile and then create a new one.

Error Message An error occurred opening C:*directory**filename*

Explanation You selected the wrong file type while attempting to open the AP scan list file in the site survey utility.

Recommended Action Locate the AP scan list file (SST_APScanList.apsl) and open it.

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

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

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

Error Message At least one wireless checkbox must be selected.

Explanation You clicked **OK** or selected another Profile Management tab before selecting any Wireless Mode options on the Profile Management (Advanced) window.

Recommended Action Choose at least one of the Wireless Mode options.

Error Message Authentication failed.

Explanation The domain logon failed for an unknown reason.

Recommended Action Try again to authenticate. If this message reappears, verify that all of the proper certificates have been loaded onto your computer and that your client adapter's current profile has been configured properly. If the domain logon continues to fail, contact your system administrator.

Error Message Authentication failed because server rejected username or password.

Explanation The domain logon failed because your username or password is invalid.

Recommended Action Re-enter your username and password on the Define PEAP (EAP-GTC) Configuration window or the Define PEAP (EAP-MSCHAP V2) Configuration window and save your settings. Then try again to authenticate.

Error Message Authentication failed due to invalid client attributes (e.g., Login Name) .

Explanation The domain logon failed because of an invalid client configuration setting, such as a mistyped login name.

Recommended Action Return to the PEAP configuration windows, verify your settings, and make any necessary modifications.

Error Message Authentication failed due to invalid client certificate.

Explanation The domain logon failed because of an invalid client certificate.

Recommended Action Contact your system administrator to obtain a valid certificate.

Error Message Authentication failed due to invalid server certificate.

Explanation The domain logon failed because of an invalid server certificate.

Recommended Action Contact your system administrator.

Error Message Authentication failed due to invalid server/domain name.

Explanation The domain logon failed because of an invalid server/domain name.

Recommended Action Make sure the Specific Server or Domain field is blank on the Advanced Configuration window for PEAP (EAP-GTC) or PEAP (EAP-MSCHAP V2). Then follow the instructions in the [“Enabling PEAP \(EAP-GTC\)”](#) section on page 5-48 or the [“Enabling PEAP \(EAP-MSCHAP V2\) Machine Authentication with Machine Credentials”](#) section on page 5-55 to correctly enter your username in the Login Name field.

Error Message Authentication timed out. Do you want to retry?

Explanation LEAP or EAP-FAST authentication failed because the authentication server is down.

Recommended Action Click **Retry** to try to authenticate again using the same credentials or click **Cancel** to cancel the operation.

Error Message Cannot load oemres.dll.

Explanation The oemres.dll file cannot be installed.

Recommended Action Uninstall the current client adapter software; then install the latest release.

Error Message Cisco Aironet 802.11a/b/g wireless adapter software update can't proceed. Please insert the adapter in the system and try again.

Explanation You attempted to upgrade your client adapter's software when the adapter was not inserted into your computer.

Recommended Action Click **OK**, insert your client adapter, and start the upgrade process again.

Error Message DHCP failure.

Explanation The domain logon failed because of a DHCP failure.

Recommended Action Try again to authenticate. If this message reappears, contact your system administrator.

Error Message During installation, you chose not to use Microsoft Wireless Configuration Manager to control your Cisco Aironet Wireless LAN Client Adapter. However, it is currently enabled for this device. Do you want to disable it?

Explanation The Microsoft Wireless Configuration Manager is enabled and can be used to control your client adapter.

Recommended Action If you want to switch control from the Microsoft Wireless Configuration Manager to ADU, click **Yes**. Otherwise, click **No**.

Error Message Entry must be xx characters long. Please enter xx more characters.

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

Recommended Action Re-enter the static WEP key following the guidelines in the [“Enabling Static WEP”](#) section on page 5-26.

Error Message Error importing the EAP-FAST PAC file.

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

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

Error Message Failed to initialize supplicant. This error may be due to the absence of a valid machine certificate or the incomplete configuration of profiles.

Explanation The domain logon failed because the EAP supplicant could not be initialized.

Recommended Action Verify that a valid machine certificate has been loaded onto your computer and that your client adapter's current profile has been configured properly.

Error Message Failed to open PAC stores.

Explanation An error occurred when you attempted to access the global or private PAC store.

Recommended Action Try again. If the second attempt fails, contact your system administrator.

Error Message Gina error on bootup

Explanation A GINA error appears upon bootup.

Recommended Action Boot to the safe mode command prompt. Then copy the msgina.dll file in the WinNT\System32 directory (Windows 2000) or Windows\System32 directory (Windows XP) over to a file named cscogina.dll. The **copy** command enables you to copy a source file (msgina.dll) to a destination file (cscogina.dll) within the same directory.

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

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

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

Error Message Invalid profile data. Please enter valid profile data.

Explanation You improperly configured a profile (for example, you set up the profile to use EAP-TLS authentication, but no certificates are installed on your computer).

Recommended Action Modify the profile's configuration settings.

Error Message Make sure the same new password is entered twice.

Explanation You did not enter the same EAP-FAST password in both the New Password and Verify New Password fields on the Please Change Password window.

Recommended Action Carefully re-enter your new EAP-FAST password in both the New Password and Verify New Password fields on the Please Change Password window.

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

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

Recommended Action Perform one of the following:

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

Error Message Please enter a Passphrase.

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

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

Error Message Please enter a profile name.

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

Recommended Action Enter a profile name.

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

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

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

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

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

Recommended Action Leave the fields on the Preferred Access Points window empty or re-enter the MAC address for the specified access point, which must be exactly 12 characters.

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

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

Recommended Action Enter a new profile name.

Error Message The current EAP-FAST profile does not have a PAC or the configured PAC does not match the authentication server. Do you want to use another PAC found on your local system that matches the authentication server without reconfiguring the current EAP-FAST profile?

Explanation The client adapter's authentication attempt failed because a valid PAC was not found. ADU matches the username and server name that it is trying to use with those in the PAC. If they do not match or the configured PAC does not exist, ADU searches the private and global stores. If a matching PAC is found, the user is prompted with this message before the PAC is used.

Recommended Action Click **Yes** to attempt to authenticate using another PAC on your system without having to reconfigure your profile.

Error Message The device may not be present or could have been ejected/unplugged from the system. Insert or reinsert it now.

Explanation You attempted to install the client adapter software without the adapter being inserted into your computer.

Recommended Action 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.

Error Message The driver files you wish to remove will not be removed as the corresponding card is not inserted.

Explanation You attempted to uninstall the client adapter software without the adapter being inserted into your computer.

Recommended Action Insert the client adapter and click **OK**.

Error Message The EAP-FAST auto provisioning or PAC updating failed. The current profile is disabled until you correct the PAC configuration in the profile and reauthenticate.

Explanation PAC provisioning has failed. No PAC has been provisioned, and the profile is disabled.

Recommended Action Try again to authenticate using the existing profile. If automatic PAC provisioning is enabled, make sure to allow a PAC to be provisioned if prompted. If the authentication attempt fails again, modify the profile's PAC configuration settings.

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

Explanation You incorrectly entered the PAC file password.

Recommended Action Carefully re-enter the PAC file password.

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

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

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

Error Message The new password must be different from the old password.

Explanation You entered your old EAP-FAST password in the New Password and/or Verify New Password fields on the Please Change Password window.

Recommended Action Enter your new EAP-FAST password in the New Password and/or Verify New Password fields on the Please Change Password window.

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

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

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

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

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

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

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

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

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

Error Message The profile will be disabled until you select the Reauthentication option, Windows restarts, or the card is ejected and reinserted. Are you sure?

Explanation The username and password for your current profile have expired or are no longer valid. When the Enter Network Password window appeared, prompting you to enter your new username and password, you chose Cancel. The profile was disabled to prevent accidental authentication attempts in the future.

Recommended Action Click **No**, enter your username and password when the Enter Wireless Network Password window reappears, and click **OK**. The client adapter should authenticate using your new credentials. If the profile uses saved credentials, edit the profile in ADU by changing the username and password on the LEAP or EAP-FAST Settings window and save your changes. (If you click **Yes**, the profile is disabled until you choose Reauthenticate from ASTU or the Action drop-down menu in ADU, reboot your system, or eject and reinsert the card.)

Error Message The specified path does not exist. Please enter another path.

Explanation You chose the **Make Driver Installation Diskette(s)** option during installation, but a diskette was not inserted in the computer's A: drive.

Recommended Action Insert a floppy diskette into your computer's floppy disk drive, and choose the **Make Driver Installation Diskette(s)** option again.

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

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

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

Error Message This Device is controlled by the Windows XP Automatic Wireless Network Configuration. It may override Network Name, Security and other settings from this profile.

Explanation You attempted to activate ADU while the Microsoft Wireless Configuration Manager in Windows XP was enabled. When a message appeared asking if you wanted to disable the Microsoft configuration manager, you chose No.

Recommended Action If you want to use ADU to configure your client adapter, disable the Microsoft Wireless Configuration Manager.

Error Message This Product does not support this version of Windows. Please check the product documentation for the system requirements.

Explanation You tried to install the CB21AG and PI21AG client adapter software on an unsupported Windows operating system.

Recommended Action Install the CB21AG and PI21AG client adapter software on a computer running Windows 2000 or XP.

Error Message Unable to authenticate wireless user. Please make sure you have entered the right user name and password and try again. If you are using an old PAC with this profile and have not logged on to the network for a long period of time, you may also want to make sure the PAC you are using is not expired by either import a new PAC manually or delete the old PAC if auto provisioning is enabled.

Explanation The client adapter's authentication attempt failed either because the wrong user credentials were entered or the profile is using an old PAC.

Recommended Action Try to authenticate again using the existing profile. Make sure to enter your username and password correctly. If the authentication attempt fails again, import a new PAC or delete the old PAC if automatic PAC provisioning is enabled.

Error Message Unable to copy PAC data. Make sure you have access rights.

Explanation Your attempt to copy a PAC from the private store to the global store failed. You may not have the necessary permissions.

Recommended Action Try again. If your second attempt fails, contact your system administrator.

Error Message Unable to delete the PAC from the local system.

Explanation Your attempt to delete a PAC failed.

Recommended Action Try again. If your second attempt fails, contact your system administrator.

Error Message Unable to EAP-FAST authenticate the wireless user in the specified amount of time. Network infrastructure might be down. You may also want to increase the timeout value for this profile.

Explanation The client adapter was unable to EAP-FAST authenticate within the amount of time specified by the EAP-FAST authentication timeout value.

Recommended Action Try again to authenticate using the existing profile. If automatic PAC provisioning is enabled, make sure to allow a PAC to be provisioned if prompted. If the authentication attempt fails again, increase the authentication timeout value on the EAP-FAST Settings window and try again.

Error Message Unable to save imported PAC data. Access denied.

Explanation Your attempt to save an imported PAC file has failed. You may not have the necessary permissions.

Recommended Action Try again. If your second attempt fails, contact your system administrator.

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

Explanation You entered an incomplete static WEP key on the Define Pre-Shared Keys window and clicked **OK**.

Recommended Action Re-enter the static WEP key, making sure to enter the correct number of characters and click **OK**.

Error Message 'x' is not a hexadecimal character.

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

Recommended Action Re-enter the static WEP key following the guidelines in the [“Enabling Static WEP” section on page 5-26](#).

Error Message You are not registered with the authentication server. A security credential is required to register this device. Do you want to obtain a security credential?

Explanation Automatic PAC provisioning is enabled for this profile. However, a valid PAC matching the server to which the client adapter is connecting could not be found.

Recommended Action Click **Yes** to provision a new PAC for this server using your existing credentials or click **No** to cancel the operation. If you click **No**, the client adapter is unable to authenticate using the existing profile.

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

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

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

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

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

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

Error Message You chose not to copy your private PAC. If you experience wireless connection problems during Windows domain logon or logged off stage, you must reconfigure the profile to use a global PAC.

Explanation When you were prompted to copy your PAC to the global store so that it will be available when you are not logged on, you clicked No.

Recommended Action The profile will use the private PAC for authentication. However, if you experience any wireless connection problems, you may need to reconfigure your profile to use a global PAC.

Error Message You do not have a valid Protected Access Credentials (PAC), the PAC you provided does not match the authentication server, or the PAC is expired. You may proceed with authenticating if the server supports auto provisioning. Do you want to proceed and accept auto provisioning?

Explanation You activated an EAP-FAST profile that is configured for automatic PAC provisioning and does not specify a PAC authority for which you have a current valid PAC.

Recommended Action If you want to attempt to auto-provision a PAC from the server, click **Yes**. Otherwise, click **No**. If you choose No, a message appears indicating that the client adapter was unable to EAP-FAST authenticate.

Error Message You failed to change your EAP-FAST domain/network password. Make sure you enter a new password that complies with the password policy and try again. Do you want to retry now?

Explanation An error occurred when you attempted to change your EAP-FAST password.

Recommended Action Click **Yes** to try again. When the Enter Wireless Network Password window appears, enter your new password. Otherwise, click **No** to cancel the operation.

Error Message You have just changed your network password. You must change your saved password settings in the EAP-FAST profiles before connecting again.

Explanation Your network password has changed.

Recommended Action Update your EAP-FAST password on the EAP-FAST Settings window for any EAP-FAST profiles that are configured with a saved username and password.

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

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

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

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

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

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

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

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

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

Error Message You must enter the correct old password in order to change the new password.

Explanation You incorrectly entered your old EAP-FAST password on the Please Change Password window.

Recommended Action Carefully re-enter your old EAP-FAST password on the Please Change Password window.

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

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

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

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

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

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

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

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

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

Error Message Your security setting is invalid for an Ad Hoc network. If you want, security will be disabled for you. You can also configure security to Pre-shared keys. Do you want to disable security?

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

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

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

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

Recommended Action If you want a copy of the PAC to be added to the global store so that it will be available when 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**.



APPENDIX **A**

Technical Specifications

This appendix provides technical specifications for the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters.

The following topics are covered in this appendix:

- Physical Specifications, [page A-2](#)
- [Radio Specifications](#), [page A-3](#)
- Power Specifications, [page A-6](#)
- Safety and Regulatory Compliance Specifications, [page A-6](#)

Table A-1 lists the technical specifications for the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters.

Table A-1 **Technical Specifications for CB21AG and PI21AG Client Adapters**

Physical Specifications	
Size	
PC-Cardbus card	4.5 in. L x 2.1 in. W x 0.2 in. H (11.3 cm L x 5.4 cm W x 0.5 cm H)
PCI card	
Standard PCI card	4.7 in. L x 0.7 in. W x 4.8 in. H (12 cm L x 1.8 cm W x 12.1 cm H)
Low-profile PCI card	4.7 in. L x 0.7 in. W x 3.1 in. H (12 cm L x 1.8 cm W x 7.9 cm H)
Weight	
PC-Cardbus card	1.55 oz (44 g)
PCI card	
Standard PCI card with antenna	3.6 oz (103 g)
Standard PCI card without antenna	1.9 oz (55 g)
Low-profile PCI card with antenna	3.5 oz (98 g)
Low-profile PCI card without antenna	1.7 oz (49 g)
Enclosure	
PC-Cardbus card	Type II Cardbus
PCI card	Standard or low-profile Type II PCI
Connector	
PC-Cardbus card	68-pin Cardbus
PCI card	62-pin PCI
Status indicators	Green and amber LEDs; see Chapter 10
Operating temperature	32°F to 158°F (0°C to 70°C)
Storage temperature	32°F to 185°F (0°C to 85°C)
Humidity (non-operational)	90% relative humidity
ESD	15 kV (human body model)

Table A-1 **Technical Specifications for CB21AG and PI21AG Client Adapters (continued)**

Radio Specifications	
Type	
802.11a	Orthogonal frequency division multiplexing (OFDM)
802.11b/g	Direct-sequence spread spectrum (DSSS) and orthogonal frequency division multiplexing (OFDM)
Power output	
Note Refer to Appendix D for limitations on radiated power (EIRP) levels in the European community and other countries.	
802.11a	40 mW (16 dBm) @ 6, 9, 12, 18, 24 Mbps 25 mW (14 dBm) @ 6, 9, 12, 18, 24, 36 Mbps 20 mW (13 dBm) @ 6, 9, 12, 18, 24, 36, 48, 54 Mbps 13 mW (11 dBm) @ 6, 9, 12, 18, 24, 36, 48, 54 Mbps 10 mW (10 dBm) @ 6, 9, 12, 18, 24, 36, 48, 54 Mbps Note The maximum power setting varies according to individual country regulations.
802.11b/g	100 mW (20 dBm) @ 1, 2, 5.5, 11 Mbps 63 mW (18 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24 Mbps 50 mW (17 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36 Mbps 30 mW (15 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 Mbps 20 mW (13 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps 10 mW (10 dBm) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps Note The maximum power setting varies according to individual country regulations.
Operating frequency	
802.11a	5.15 to 5.25 GHz in the UNII 1 band* 5.25 to 5.35 GHz in the UNII 2 band* 5.470 to 5.725 GHz in the European band 5.725 to 5.825 GHz in the UNII 3 band* *Depending on the regulatory domain in which the client adapter is used
802.11b/g	2.400 to 2.497 GHz (depending on the regulatory domain in which the client adapter is used)
Usable channels	
802.11a	5170 to 5320 MHz, 5500 to 5700 MHz, and 5745 to 5805 MHz
802.11b/g	2412 to 2484 MHz in 5-MHz increments
Data rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
Modulation	Differential binary phase shift keying (DBPSK) - 1 Mbps Differential quaternary phase shift keying (DQPSK) - 2 Mbps Complementary code keying (CCK) - 5.5 and 11 Mbps Binary phase shift keying (BPSK) - 6 and 9 Mbps Quaternary phase shift keying (QPSK) - 12 and 18 Mbps 16-quadrature amplitude modulation (16-QAM) - 24 and 36 Mbps 64-quadrature amplitude modulation (64-QAM) - 48 and 54 Mbps

Table A-1 **Technical Specifications for CB21AG and PI21AG Client Adapters (continued)**

Receiver sensitivity	
802.11a	<p><u>5150 to 5250 MHz</u> –87 dBm @ 6, 9, 12, and 18 Mbps –82 dBm @ 24 Mbps –79 dBm @ 36 Mbps –74 dBm @ 48 Mbps –72 dBm @ 54 Mbps</p> <p><u>5250 to 5350 MHz</u> –89 dBm @ 6, 9, and 12 Mbps –85 dBm @ 18 Mbps –82 dBm @ 24 Mbps –79 dBm @ 36 Mbps –74 dBm @ 48 Mbps –72 dBm @ 54 Mbps</p> <p><u>5470 to 5725 MHz</u> –87 dBm @ 6, 9, 12, and 18 Mbps –82 dBm @ 24 Mbps –79 dBm @ 36 Mbps –74 dBm @ 48 Mbps –72 dBm @ 54 Mbps</p> <p><u>5725 to 5805 MHz</u> –84 dBm @ 6, 9, and 12 Mbps –83 dBm @ 18 Mbps –82 dBm @ 24 Mbps –79 dBm @ 36 Mbps –72 dBm @ 48 Mbps –65 dBm @ 54 Mbps</p>
802.11b/g	–94 dBm @ 1 Mbps –93 dBm @ 2 Mbps –92 dBm @ 5.5 Mbps –90 dBm @ 11 Mbps –86 dBm @ 6, 9, 12, and 18 Mbps –84 dBm @ 24 Mbps –80 dBm @ 36 Mbps –75 dBm @ 48 Mbps –71 dBm @ 54 Mbps

Table A-1 Technical Specifications for CB21AG and PI21AG Client Adapters (continued)

Receiver delay spread (multipath)		
802.11a/g	400 ns @ 6 Mbps 250 ns @ 9 and 12 Mbps 220 ns @ 18 Mbps 160 ns @ 24 Mbps 100 ns @ 36 Mbps 90 ns @ 48 Mbps 70 ns @ 54 Mbps	
802.11b	350 ns @ 1 Mbps 300 ns @ 2 Mbps 200 ns @ 5.5 Mbps 130 ns @ 11 Mbps	
Range		
802.11a	Indoor (typical) 500 ft (152 m) @ 6 Mbps 400 ft (122 m) @ 18 Mbps 90 ft (27 m) @ 54 Mbps Note The above range numbers assume that the client adapter is being used at maximum transmit power with a Cisco Aironet 1232AG Access Point with a 3.5-dBi dipole antenna. Different range characteristics are likely when using the client adapter with a different access point or a Cisco Aironet 1200 Series Access Point with a different antenna.	Outdoor (typical) 950 ft (290 m) @ 6 Mbps 800 ft (244 m) @ 18 Mbps 170 ft (52 m) @ 54 Mbps
802.11b/g	Indoor (typical) 410 ft (125 m) @ 1 Mbps 300 ft (91 m) @ 6 Mbps 220 ft (67 m) @ 11 Mbps 180 ft (55 m) @ 18 Mbps 90 ft (27 m) @ 54 Mbps Note The above range numbers assume that the client adapter is being used at maximum transmit power with a Cisco Aironet 1232AG Access Point with a 2.2-dBi dipole antenna. Different range characteristics are likely when using the client adapter with a different access point or a Cisco Aironet 1200 Series Access Point with a different antenna.	Outdoor (typical) 700 ft (213 m) @ 1 Mbps 650 ft (198 m) @ 6 Mbps 490 ft (149 m) @ 11 Mbps 400 ft (122 m) @ 18 Mbps 110 ft (34 m) @ 54 Mbps
Antennas		
PC-Cardbus card	Integrated 0-dBi dual-band 2.4/5-GHz diversity antenna	
PCI card	1-dBi dual-band 2.4/5-GHz antenna, permanently attached by 6.6-ft (2-m) cable	

Table A-1 **Technical Specifications for CB21AG and PI21AG Client Adapters (continued)**

Power Specifications	
Operational voltage	3.3 V (± 0.3 V)
Receive current steady state	
802.11a	318 mA maximum
802.11b	327 mA maximum
802.11g	282 mA maximum
Transmit current steady state	
802.11a	554 mA maximum
802.11b	539 mA maximum
802.11g	530 mA maximum
Sleep mode steady state	203 mA average
Safety and Regulatory Compliance Specifications	
Safety	Designed to meet: <ul style="list-style-type: none"> • UL 60950 • CSA 22.2 No. 60950 • IEC 60950 Second Ed., including Amendments 1-4 with all national deviations • EN 60950 Second Ed., including Amendments 1-4
EMI and susceptibility	FCC Part 15.107 & 15.109 Class B ICES-003 Class B (Canada) VCCI (Japan) EN 301.489-1 and EN-301.489-17 (Europe)
Radio approvals	FCC Part 15.247 FCC Part 15.401-15.407 Canada RSS-210 Europe EN-300.328, EN-301.893 ARIB STD-33, ARIB STD-66, ARIB STD-T71 (Japan) AS 4268.2 (Australia) AS/NZS 3548 (Australia and New Zealand)
RF exposure	FCC Bulletin OET-65C Industry Canada RSS-102



APPENDIX **B**

Translated Safety Warnings

This appendix provides translations of the safety warnings that appear in this publication. The second warning pertains to the PI21AG client adapter, and the third warning pertains to the CB21AG client adapter.

The following topics are covered in this appendix:

- [Explosive Device Proximity Warning, page B-2](#)
- [Antenna Installation Warning, page B-3](#)
- [Warning for Laptop Users, page B-4](#)

Explosive Device Proximity Warning



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.

Waarschuwing

Gebruik dit draadloos netwerkapparaat alleen in de buurt van onbeschermde ontstekers of in een omgeving met explosieven indien het apparaat speciaal is aangepast om aan de eisen voor een dergelijk gebruik te voldoen.

Varoitus

Älä käytä johdotonta verkkolaitetta suojaamattomien räjäytysnallien läheisyydessä tai räjäytysalueella, jos laitetta ei ole erityisesti muunnettu sopivaksi sellaiseen käyttöön.

Attention

Ne jamais utiliser un équipement de réseau sans fil à proximité d'un détonateur non blindé ou dans un lieu présentant des risques d'explosion, sauf si l'équipement a été modifié à cet effet.

Warnung

Benutzen Sie Ihr drahtloses Netzwerkgerät nicht in der Nähe ungeschützter Sprengkapseln oder anderer explosiver Stoffe, es sei denn, Ihr Gerät wurde eigens für diesen Gebrauch modifiziert und bestimmt.

Avvertenza

Non utilizzare la periferica di rete senza fili in prossimità di un detonatore non protetto o di esplosivi a meno che la periferica non sia stata modificata a tale proposito.

Advarsel

Ikke bruk den trådløse nettverksenheten nært inntil uisolerte fenghetter eller i et eksplosivt miljø med mindre enheten er modifisert slik at den tåler slik bruk.

Aviso

Não opere o dispositivo de rede sem fios perto de cápsulas explosivas não protegidas ou num ambiente explosivo, a não ser que o dispositivo tenha sido modificado para se qualificar especialmente para essa utilização.

¡Advertencia!

No utilizar un aparato de la red sin cable cerca de un detonador que no esté protegido ni tampoco en un entorno explosivo a menos que el aparato haya sido modificado con ese fin.

Varning!

Använd inte den trådlösa nätverksenheten i närheten av oskyddade tändhättar eller i en explosiv miljö om inte enheten modifierats för att kunna användas i sådana sammanhang.

Antenna Installation Warning



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.

Waarschuwing

Om te voldoen aan de FCC radiofrequentie (RF) blootstellingslimieten dienen antennes zich minstens 20 cm of meer van de lichamen van alle personen bevinden.

Varoitus

FCC:n antamien radiotaajuuksille altistumista koskevien rajoitusten mukaan antennien on sijaittava vähintään 20 cm:n päässä kaikista henkilöistä.

Attention

Pour se conformer aux limites d'exposition à la fréquence radio préconisées par la FCC (Federal Communications Commission), les antennes doivent se situer à un minimum de 20 cm de toute personne.

Warnung

Um die in den FCC-Richtlinien festgelegten Expositionshöchstgrenzen für Radiofrequenzen (RF) nicht zu überschreiten, sollten antennen mindestens 20 cm (7,9 Zoll) vom Körper aller Person entfernt aufgestellt werden.

Avvertenza

Per conformarsi ai limiti FCC di esposizione a radiofrequenza (RF), le antenne a devono stare ad una distanza minima di 20 cm dal corpo di ogni persona.

Advarsel

I henhold til eksponeringsgrensene for radiofrekvenser (RF), skal antenner befinne seg på en avstand av minst 20 cm eller mer fra mennesker.

Aviso

Para estar de acordo com as normas FCC de limites de exposição para frequência de rádio (RF), as antenas devem estar distantes no mínimo 20 cm (7,9 pol) do corpo de qualquer pessoa.

¡Advertencia!

Para cumplir con los límites de exposición de radio frecuencia (RF) de la Comisión Federal de Comunicaciones (FCC) es preciso ubicar las antenas a un mínimo de 20 cm (7,9 pulgadas) o más del cuerpo de las personas.

Varning!

För att följa FCC-exponeringsgränserna för radiofrekvens (RF), bör antenner placeras på minst 20 cm avstånd från alla människor.

Warning for Laptop Users



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.

Waarschuwing

Dit apparaat is getest en voldoet aan de FCC-beperkingen voor radiofrequentieblootstelling (SAR) bij standaardconfiguraties met een laptopcomputer. Dit apparaat kan worden gebruikt in desktop- of laptopcomputers met PC-kaartsleuven aan de zijkant, waarbij minimaal 1 cm afstand bestaat tussen de antenne en het lichaam van de gebruiker of een persoon in de buurt. Bij smalle laptopcomputers is mogelijk extra aandacht vereist om tijdens gebruik voldoende afstand tot de antenne te houden. Dit apparaat kan niet worden gebruikt in combinatie met mobiele PDA's (personal digital assistants; persoonlijke digitale assistenten). Als u dit apparaat gebruikt in andere configuraties, voldoet het wellicht niet meer aan de FCC-regelgeving met betrekking tot radiofrequentieblootstelling. Dit apparaat en de bijbehorende antenne mogen niet in combinatie met andere antennes of zenders worden gebruikt en ook niet in de buurt van andere antennes of zenders worden geplaatst.

Varoitus

Tämä laite on testattu ja se noudattaa FCC:n määrittämiä radiotaajuussäteilylle altistumisen (SAR) raja-arvoja tyypillisissä kannettavien tietokoneiden kokoonpanoissa. Tätä laitetta voidaan käyttää pöytä- tai kannettavissa tietokoneissa, joiden sivussa on PC-korttipaikka. Korttipaikassa olevan laitteen antennin etäisyyden käyttäjästä tai lähellä olevasta henkilöstä on oltava vähintään yksi senttimetri. Ohuita kannettavia tietokoneita on ehkä tarkkailtava erityisesti, jotta käyttäjän etäisyys antenniin olisi riittävä käytön aikana. Tätä laitetta ei voi käyttää yhdessä kämmentietokoneiden (PDA) kanssa. Jos laitetta käytetään muunlaisissa kokoonpanoissa, se ei ehkä vastaa FCC:n määrittämiä radiotaajuussäteilylle altistumisen ohjearvoja. Tätä laitetta ja sen antennia ei saa käyttää samassa pisteessä toisen antennin tai lähettimen kanssa tai liitettynä toiseen antenniin tai lähettimeen.

Attention

Cet appareil a été testé et respecte les limites (TAS - Taux d'absorption spécifique) d'exposition aux RF de la FCC relatives aux configurations standard des ordinateurs portables. Il peut être utilisé dans des ordinateurs de bureau ou portables dotés d'un emplacement pour carte PC latérales et peut fournir une distance de séparation d'au moins 1 cm entre l'antenne et le corps de l'utilisateur ou d'une personne avoisinante. Nous vous recommandons de porter une attention particulière lors de l'utilisation d'ordinateurs portatifs minces afin d'assurer le maintien de l'espacement de l'antenne. Cet appareil ne peut pas être utilisé avec des assistants numériques personnels de poche. L'utilisation dans d'autres configurations risque de ne pas être conforme aux lignes directrices de la FCC sur l'exposition aux RF. Cet appareil et son antenne ne doivent pas se trouver dans le même emplacement ou fonctionner conjointement avec une autre antenne ou un autre émetteur.

Warnung	Dieses Gerät wurde getestet und entspricht den durch die FCC-Richtlinien festgelegten Grenzwerten für Hochfrequenzstrahlung (SAR) für reguläre Laptop-Computerkonfigurationen. Es kann für Desktop- oder Laptop-Computer mit seitlichem PC-Kartensteckplatz genutzt werden, wobei der Abstand der Antenne vom Benutzer oder anderen in der Nähe befindlichen Personen mindestens 1 cm betragen muss. Insbesondere bei schmalen Laptop-Computern sollte darauf geachtet werden, dass der Abstand während des Betriebs genau eingehalten wird. Dieses Gerät kann nicht für tragbare Handheld-Geräte/PDAs verwendet werden. Bei Verwendung in anderen Konfigurationen ist u.U. die Einhaltung der durch die FCC-Richtlinien festgelegten Grenzwerte für Hochfrequenzstrahlung nicht gewährleistet. Dieses Gerät und die Antenne dürfen nicht zusammen mit anderen Antennen oder Übertragungsgeräten installiert oder verwendet werden.
Avvertenza	Questo dispositivo è stato testato ed è conforme alle norme sulle emissioni radio (SAR) nelle configurazione tipica di computer portatili. Questo dispositivo può essere utilizzato in desktop o computer portatili con slot per scheda PC laterale che garantisca un minimo spazio di 1 cm (0,394 pollici) tra l'antenna e l'utente o qualsiasi persona nelle vicinanze. I computer portatili sottili richiedono particolare attenzione al mantenimento dello spazio minimo quando in funzione. Questo dispositivo non può essere utilizzato con computer palmari (PDA). L'utilizzo in configurazione differenti non assicura la conformità alle norme sulle emissioni radio. Questo dispositivo e la propria antenna non devono operare congiuntamente and altre antenne o trasmettitori.
Advarsel	Denne enheten er testet og overholder grensene for FCC RF-eksponering (SAR) i vanlige konfigurasjoner for bærbare datamaskiner. Den kan brukes i stasjonære eller bærbare datamaskiner som har kortplass på siden, og der det er minst 1 cm avstand mellom antennen og brukeren eller andre personer. Ved bruk av flate bærbare PCer må du være ekstra påpasselig med antenneavstanden. Denne enheten kan ikke brukes sammen med håndholdte PDAer (personal digital assistant). Det er ikke sikkert at bruk i andre konfigurasjoner vil være i samsvar med retningslinjene for FCC RF-eksponering. Denne enheten og antennen må ikke plasseres på samme sted som eller brukes sammen med andre antenner eller sendere.
Aviso	Este dispositivo foi testado e está em conformidade com os limites SAR de exposição a radiofrequência (RF) da Comissão Federal de Comunicações (FCC), em configurações típicas de portátil, e pode ser utilizado em computadores de secretária ou portáteis com ranhuras de placa PC laterais que permitem um distanciamento mínimo de 1cm. entre a antena e o corpo do utilizador ou de alguém que esteja por perto. Os portáteis finos necessitam de uma atenção especial para manter a distância da antena durante o funcionamento. Este dispositivo não pode ser utilizado com PDAs (personal digital assistants) de mão. A utilização noutras configurações pode não assegurar a conformidade com as directrizes de exposição a radiofrequência (RF) da Comissão Federal de Comunicações (FCC). Este dispositivo e a respectiva antena não devem ser colocados nem postos a funcionar com outras antenas ou transmissores.
¡Advertencia!	El dispositivo ha sido probado y cumple los límites de la FCC sobre exposición a radiofrecuencia (SAR o tasa de absorción específica) en cualquier configuración tradicional de equipos portátiles. Además, puede utilizarse en equipos de escritorio o portátiles que cuenten con ranuras de tarjeta PC laterales a una distancia de, al menos, 1 cm (0,394 pulgadas) de la antena al usuario o persona más cercana. Puede que los equipos portátiles de menor grosor requieran atención especial a la hora de mantener la distancia de la antena al utilizarlos. No puede utilizarse este dispositivo con equipos digitales personales portátiles (PDA). Su utilización en otras configuraciones no garantiza el cumplimiento de las directivas de la FCC sobre exposición a radiofrecuencia. Este dispositivo y la antena no deben situarse o accionarse junto con otra antena o transmisor.

Varning! Den här enheten har testats och följer FCC-gränserna för radiofrekvensexponering (SAR) i vanliga konfigurationer för bärbara datorer. Den kan användas i stationära eller bärbara datorer med sidmonterade PC-kortöppningar som kan tillhandahålla minst 1 cm med separationsavstånd mellan antennen och användarens kropp eller annan person i närheten. Tunna, bärbara datorer kan behöva speciell uppmärksamhet för att upprätthålla antennavståndet under användning. Den här enheten kan inte användas med handdator/PDA. Vid användning i andra konfigurationer går det inte att garantera att FCC:s riktlinjer för radiofrekvens följs. Den här enheten och dess antenn får inte placeras tillsammans med eller användas i samband med någon annan antenn eller sändare/mottagare.

Figyelem Az eszköz tesztelésen esett át, melynek eredményeként megfelel az FCC RF-sugárzási (SAR) korlátozásainak tipikus laptop-konfigurációk esetén. Az eszköz beszerelhető asztali és laptop számítógépekben lévő, oldalra szerelt PC-kártya csatlakozókba, amennyiben legalább 1 cm távolság van az antenna és a felhasználó vagy egy közeli személy teste között. Vékony laptop számítógépek esetén különösen ügyelni kell használat közben az antennától való távolság betartására. Az eszköz nem használható kézi PDA-kkal (személyi digitális asszisztensekkel). Más konfigurációk esetén előfordulhat, hogy az eszköz nem felel meg az FCC RF-sugárzási előírásainak. Az eszközt és annak antennáját nem szabad más antennával vagy adó-vevővel egy helyen elhelyezni vagy üzemeltetni.

Предупреждение Это устройство протестировано и признано соответствующим ограничениям FCC, касающимся высокочастотного излучения (SAR), для обычных конфигураций портативных компьютеров. Оно может использоваться на переносных или портативных компьютерах с боковыми гнездами для плат PC, которые обеспечивают зазор не менее 0,394 дюйма (1 см) между антенной и телом пользователя или другого лица, находящегося в непосредственной близости. Возможно, потребуется соблюдать особую осторожность при обеспечении зазора антенны в тонких портативных компьютерах. Это устройство нельзя использовать для карманных компьютеров. Использование в других конфигурациях не может гарантировать соответствие директивам FCC, касающимся высокочастотного излучения. Это устройство и его антенну нельзя располагать рядом или использовать совместно с другой антенной или передатчиком.

警告 将本设备用于典型膝上型计算机配置已经过测试并且符合 FCC RF 辐射暴露 (SAR) 限制; 本设备可用于侧面安装有 PC 卡插槽的台式计算机或膝上型计算机, 该插槽可确保用户或周围的人与天线至少相距 0.394 英寸 (1 厘米)。使用超薄膝上型计算机时, 可能需要特别注意在操作过程中与天线保持一定距离。本设备不能与手持式 PDA (个人数字助理) 一起使用。在其他配置中使用本设备可能无法确保符合 FCC RF 辐射暴露限制规定。禁止将本设备及其天线与任何其他天线或发射器安装在一起或同时使用。

警告 この機器は既にテスト済みで、一般的なラップトップ コンピュータの構成における米国 FCC (連邦通信委員会) の無線周波 (RF) 照射 (SAR) 制限値に準拠しています。この機器は、デスクトップ コンピュータもしくは本体側面に PC カード スロットを備えたラップトップ コンピュータでの使用が可能です。いずれのコンピュータの場合も、アンテナと人体との間に、最低 1 cm の距離があることが前提です。薄型のラップトップ コンピュータの場合は、操作中アンテナとのスペースを維持するため、特別な注意が必要になることがあります。この機器は、ハンドヘルド式の PDA (携帯情報端末) には使用できません。他の配置構成での使用は、FCC の無線周波照射に関するガイドラインに準拠しない場合があります。この機器およびアンテナは、他のアンテナもしくはトランスミッタと同一の場所に配置したり、同時に使用してはなりません。



APPENDIX **C**

Declarations of Conformity and Regulatory Information

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

The following topics are covered in this appendix:

- [Manufacturer's Federal Communication Commission Declaration of Conformity Statement, page C-2](#)
- [Department of Communications – Canada, page C-3](#)
- [European Community, Switzerland, Norway, Iceland, and Liechtenstein, page C-3](#)
- [Declaration of Conformity for RF Exposure, page C-7](#)
- [Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan, page C-7](#)
- [Administrative Rules for Cisco Aironet Wireless LAN Client Adapters in Taiwan, page C-8](#)
- [Brazil/Anatel Approval, page C-9](#)

Manufacturer's Federal Communication Commission Declaration of Conformity Statement



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

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

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

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

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

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

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

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



Caution

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



Caution

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

Department of Communications – Canada

Canadian Compliance Statement

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

Cet appareil numérique de la classe B respecte les exigences du Règlement sur le matériel brouilleur du Canada.

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

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

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

European Community, Switzerland, Norway, Iceland, and Liechtenstein

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

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

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

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

<http://www.ciscofax.com>

The following standards were applied:

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

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



Note

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

Declaration of Conformity Statement

Cisco Aironet CB21AG Wireless LAN Client Adapter



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

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

Declare under our sole responsibility that the product,

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

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

The following standards were applied:

EMC **EN 301.489-1 v1.4.1: 2002-08; EN 301.489-17 v1.2.1: 2002-04**

Health & Safety **EN60950: 2000**

Radio **EN 300 328 v1.4.1: 2003-04**
EN 301.893 v1.2.3: 2003-08

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

The product carries the CE Mark:



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

Signature:

A handwritten signature in black ink, appearing to read "Tony Youssef".

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

DofC 340347

Cisco Aironet PI21AG Wireless LAN Client Adapter



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

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

Declare under our sole responsibility that the product,

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

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

The following standards were applied:

EMC **EN 301.489-1 v1.4.1: 2002-08; EN 301.489-17 v1.2.1: 2002-04**

Health & Safety **EN60950: 2000**

Radio **EN 300 328 v1.4.1: 2003-04**
 EN 301.893 v1.2.3: 2003-08

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

The product carries the CE Mark:



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

Signature:

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

DofC 340350

Declaration of Conformity for RF Exposure

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

Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan

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



Note

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

Japanese Translation

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

- 1 この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
- 2 万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等（例えば、パーティションの設置など）についてご相談して下さい。
- 3 その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先： 03-5549-6500

43768

English Translation

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

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

Contact Number: 03-5549-6500

Administrative Rules for Cisco Aironet Wireless LAN Client Adapters in Taiwan

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

2.4- and 5-GHz Client Adapters

Chinese Translation

低功率電波輻射性電機管理辦法

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

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

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

117710

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 14

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

Article 17

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

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

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

5-GHz Client Adapters

Chinese Translation

本設備限於室內使用¹¹⁷⁷¹¹

English Translation

This equipment is limited for indoor use.

Brazil/Anatel Approval

The following approval marks apply to the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters.

AIR-CB21AG-W-K9



"Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário."

AIR-PI21AG-W-K9**1052-05-1086****(01)07898362231469**

"Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário."



APPENDIX **D**

Channels, Power Levels, and Antenna Gains

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

The following topics are covered in this appendix:

- [Channels, page D-2](#)
- [Maximum Power Levels and Antenna Gains, page D-4](#)

Channels

IEEE 802.11a

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11a 20-MHz-wide channel are shown in [Table D-1](#).

Table D-1 Channels for IEEE 802.11a

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

**Note**

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

**Note**

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

IEEE 802.11b/g

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11b/g 22-MHz-wide channel are shown in [Table D-2](#).

Table D-2 Channels for IEEE 802.11b/g

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

**Note**

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

**Note**

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

Maximum Power Levels and Antenna Gains

IEEE 802.11a

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

Table D-3 *Maximum EIRP for IEEE 802.11a*

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

IEEE 802.11b

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

Table D-4 *Maximum EIRP for IEEE 802.11b*

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

IEEE 802.11g

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

Table D-5 **Maximum EIRP for IEEE 802.11g**

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



APPENDIX **E**

Configuring the Client Adapter through the Windows XP Operating System

This appendix explains how to configure and use the client adapter with Windows XP.

The following topics are covered in this appendix:

- [Overview, page E-2](#)
- [Configuring the Client Adapter, page E-5](#)
- [Associating to an Access Point Using Windows XP, page E-18](#)
- [Viewing the Current Status of Your Client Adapter, page E-18](#)

Overview

This appendix provides instructions for minimally configuring the client adapter through the Microsoft Wireless Configuration Manager in Windows XP (instead of through ADU) as well as for enabling the security options that are available for use with this operating system. The [“Overview of Security Features”](#) section below describes each of these options so that you can make an informed decision before you begin the configuration process.

In addition, this appendix also provides basic information on using Windows XP to specify the networks to which the client adapter associates and to view the current status of your client adapter.

**Note**

If you require more information about configuring or using your client adapter with Windows XP, refer to Microsoft's documentation for Windows XP.

Overview of Security Features

When you use your client adapter with Windows XP, 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.

Static WEP Keys

Each device 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.

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.

Two 802.1X authentication types are available when configuring your client adapter through Windows XP:

- **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.
- **Protected EAP (or PEAP)**—One of the following PEAP authentication types are available, depending on the software that is installed on your computer:

- **PEAP (EAP-MSCHAP V2)**—This PEAP authentication type is available if Cisco's PEAP security module (included in the Install Wizard file for Cisco Aironet 340, 350, and CB20A client adapters) was not previously installed on your computer or was installed prior to Service Pack 1 for Windows XP.

PEAP (EAP-MSCHAP V2) authentication is based on EAP-TLS authentication but uses a password instead of a 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.

- **PEAP (EAP-GTC)**—Although this authentication type is not officially supported for CB21AG and PI21AG client adapters, you may be able to use it successfully if Cisco's PEAP security module (included in the Install Wizard file for Cisco Aironet 340, 350, and CB20A client adapters) was previously installed on your computer and installed after Service Pack 1 for Windows XP.

PEAP (EAP-GTC) authentication is designed to support One-Time Password (OTP), Windows NT or 2000 domain, and LDAP user databases over a wireless LAN. It is based on EAP-TLS authentication but uses a password or PIN instead of a client certificate for authentication. PEAP (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 either a hardware token password or a software token PIN to start the EAP authentication process and gain access to the network. If your network uses a Windows NT or 2000 domain user database or an LDAP user database (such as NDS), PEAP (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 and Cisco Access Registrar release 3.5 or later.

When you enable EAP on your access point and configure your client adapter for EAP-TLS or PEAP using Windows XP, authentication to the network occurs in the following sequence:

1. The client adapter 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 (PEAP) or certificate (EAP-TLS) being the shared secret for authentication. The password is never transmitted during the process.
3. If authentication is successful, the client and RADIUS server derive a dynamic, session-based WEP key that is unique to the client.
4. The RADIUS server transmits the key to the access point using a secure channel on the wired LAN.
5. For the length of a session, or time period, the access point and the client use this key to encrypt or decrypt all unicast packets (and broadcast packets if the access point is set up to do so) that travel between them.



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

Wi-Fi Protected Access (WPA) is a standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification. WPA uses Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection and 802.1X for authenticated key management.

WPA supports two mutually exclusive key management types: WPA and WPA passphrase (also known as *WPA pre-shared key* or *WPA-PSK*). Using WPA, 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 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.

In order to use WPA, your computer must be running Windows XP Service Pack 2.



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

Configuring the Client Adapter

Follow the steps below to configure your client adapter using Windows XP.

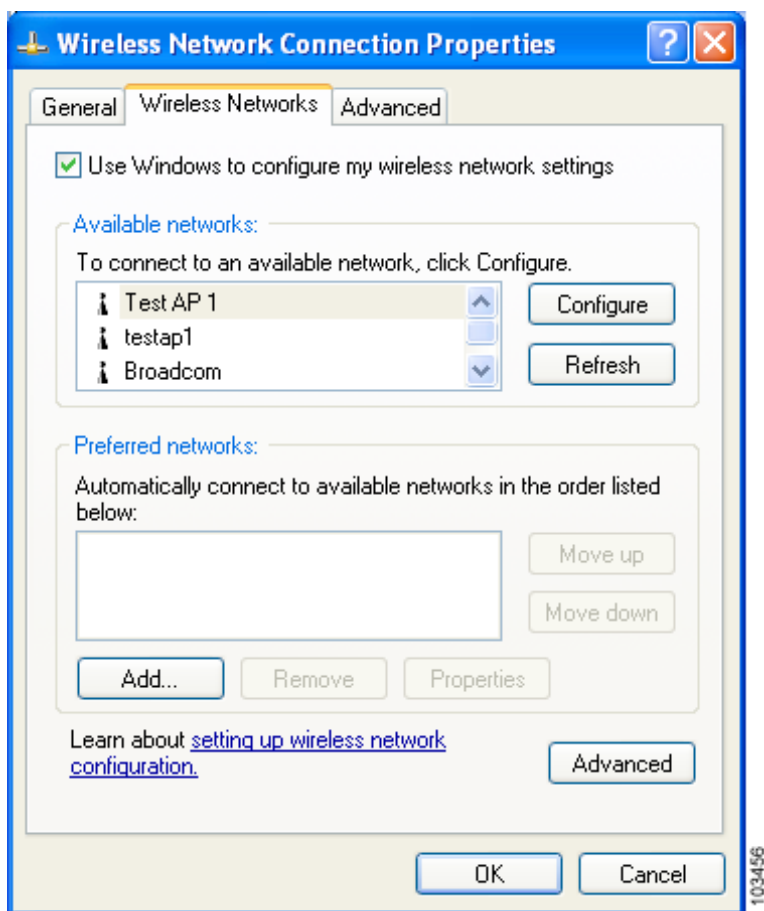
**Note**

These instructions assume you are using the Windows XP classic view rather than the category view. Otherwise, the windows you see will look different than those shown in this section.

**Note**

The appropriate certificates must be installed on your computer if you are planning to enable EAP-TLS or PEAP authentication. EAP-TLS requires both a Certificate Authority (CA) certificate and a user certificate while PEAP requires only a CA certificate. Contact your system administrator if you need help obtaining and importing the necessary certificates.

-
- Step 1** Make sure the client adapter's driver has been installed and the client adapter is inserted in the Windows XP device.
- Step 2** Double-click **My Computer**, **Control Panel**, and **Network Connections**.
- Step 3** Right-click **Wireless Network Connection**.
- Step 4** Click **Properties**. The Wireless Network Connection Properties window appears.
- Step 5** Click the **Wireless Networks** tab. The following window appears (see [Figure E-1](#)).

Figure E-1 Wireless Network Connection Properties Window (Wireless Networks Tab)

Step 6 Make sure that the **Use Windows to configure my wireless network settings** check box is checked.

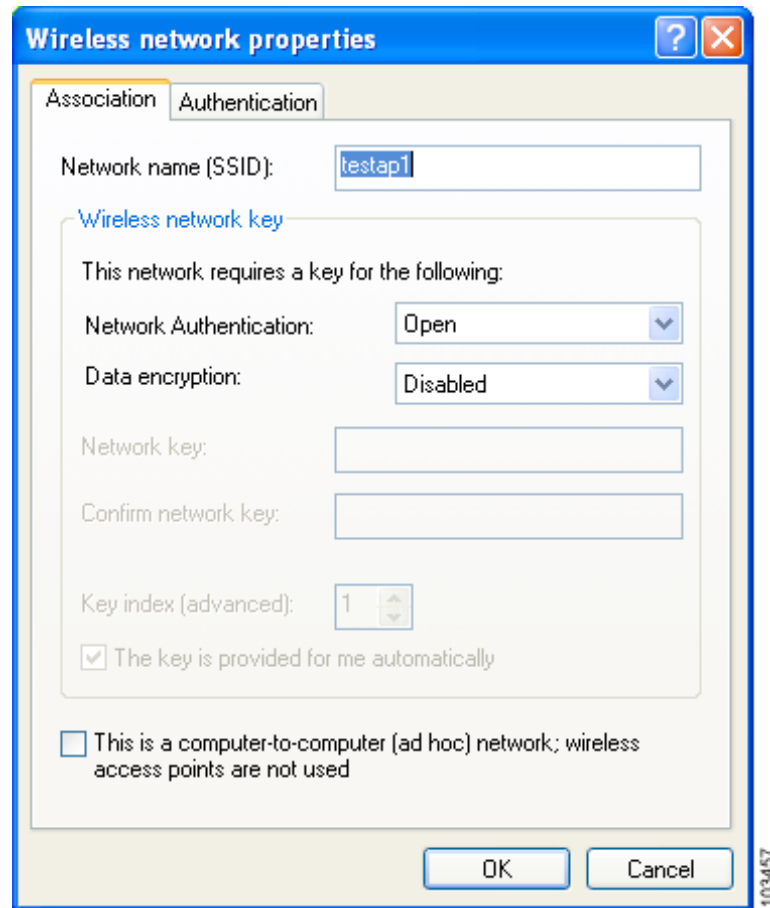
Step 7 Choose the SSID of the access point to which you want the client adapter to associate from the list of available networks and click **Configure**. If the SSID of the access point you want to use is not listed or you are planning to operate the client adapter in an *ad hoc network* (a computer-to-computer network without access points), click **Add**.

**Note**

The Allow Broadcast SSID to Associate option on the access point must be enabled for the SSID to appear in the list of available networks.

The Wireless Network Properties window appears (see [Figure E-2](#)).

Figure E-2 *Wireless Network Properties Window (Association Tab)*



Step 8 Perform one of the following:

- If you chose an SSID from the list of available networks, make sure the SSID appears in the Network name (SSID) field.
- If you clicked Add, enter the case-sensitive SSID of the access point or the ad hoc network to which you want the client adapter to associate in the Network name (SSID) field.

Step 9 Check the **This is a computer-to-computer (ad hoc mode) network; wireless access points are not used** check box at the bottom of the window if you are planning to operate the client adapter in an ad hoc network.

Step 10 Choose one of the following options from the Network Authentication drop-down list:

- **Open**—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. If your adapter is not using WEP, it will not attempt to authenticate to an access point that is using WEP and vice versa. This option is recommended if you want to use static WEP or EAP authentication without WPA.
- **Shared**—Enables your client adapter to authenticate and communicate only with access points that have the same WEP key. Cisco recommends that shared key authentication not be used because it presents a security risk.



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



Note EAP-TLS does not work with shared key authentication because shared key authentication requires the use of a WEP key, and a WEP key is not set for EAP-TLS until after the completion of EAP authentication.

- **WPA**—Enables WPA, which enables your client adapter to associate to access points using WPA.
- **WPA-PSK**—Enables WPA pre-shared key (WPA-PSK), which enables your client adapter to associate to access points using WPA-PSK.



Note The WPA-None option is not supported for use with the CB21AG or PI21AG client adapter.



Note Refer to the [“WPA” section on page E-4](#) for more information on WPA and WPA-PSK.

Step 11 Choose one of the following options from the Data encryption drop-down list:

- **Disabled**—Disables data encryption for your client adapter. This option is available only when Open or Shared has been selected for Network Authentication.
- **WEP**—Enables static or dynamic WEP for your client adapter. This option is recommended for use with open authentication.
- **TKIP**—Enables Temporal Key Integrity Protocol (TKIP) for your client adapter. This option is recommended for use with WPA and WPA-PSK unless the access point to which your client adapter will associate supports AES.
- **AES**—Enables the Advanced Encryption Standard (AES) encryption algorithm for your client adapter. This option provides a stronger encryption mechanism than TKIP and is therefore recommended for use with WPA and WPA-PSK, provided the access point to which your client adapter will associate supports AES.

Step 12 Follow the steps below to enter a static WEP key if you are planning to use static WEP.



Note If you are planning to use EAP-TLS or PEAP authentication, which uses dynamic WEP, go to [Step 13](#).

- a. Make sure the **The key is provided for me automatically** check box is unchecked.
- b. Obtain the WEP key for the access point (in an infrastructure network) or other clients (in an ad hoc network) from your system administrator and enter it in both the Network key and Confirm network key fields. 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 ASCII text WEP keys are not supported on Cisco Aironet 1200 Series Access Points, so you must enter hexadecimal characters if your client adapter will be used with these 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.
- c. In the Key index (advanced) field, choose the number of the WEP key you are creating (**1, 2, 3, or 4**).



Note The WEP key must be assigned to the same number on both the client adapter and the access point (in an infrastructure network) or other clients (in an ad hoc network).

- d. Click **OK** to save your settings and to add this SSID to the list of preferred networks (see [Figure E-1](#)). The configuration is complete for static WEP. The client adapter automatically attempts to associate to the network(s) in the order in which they are listed.

Step 13 If you enabled WPA-PSK, obtain the pre-shared key for the access point from your system administrator and enter it in both the Network key and Confirm network key fields. Follow the guidelines below to enter a pre-shared key:

- Pre-shared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.
- Your client adapter's pre-shared key must match the pre-shared key used by the access point with which you are planning to communicate.

Step 14 Check the **The key is provided for me automatically** check box if you are planning to use EAP-TLS or PEAP, which uses dynamic WEP keys.



Note This parameter is not available if you enabled WPA or WPA-PSK.

Step 15 Perform one of the following if you are planning to use EAP authentication:

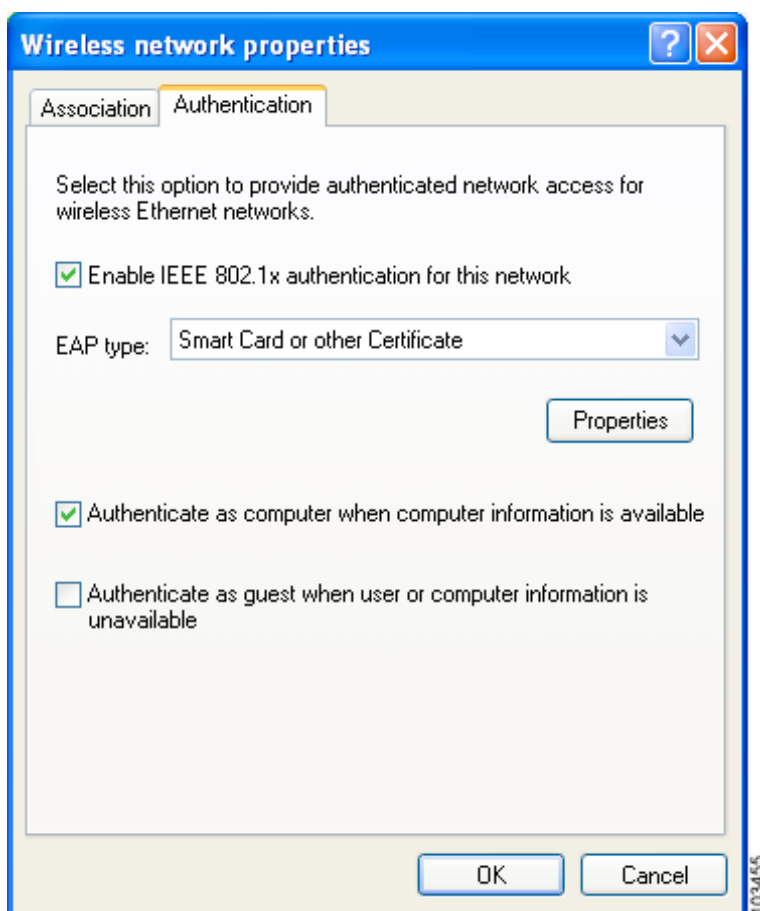
- If you are planning to use EAP-TLS authentication, follow the instructions in the “[Enabling EAP-TLS Authentication](#)” section on page E-10.
- If you are planning to use PEAP authentication, follow the instructions in the “[Enabling PEAP Authentication](#)” section on page E-13.

Enabling EAP-TLS Authentication

Follow the steps below to prepare the client adapter to use EAP-TLS authentication, provided you have completed the initial configuration.

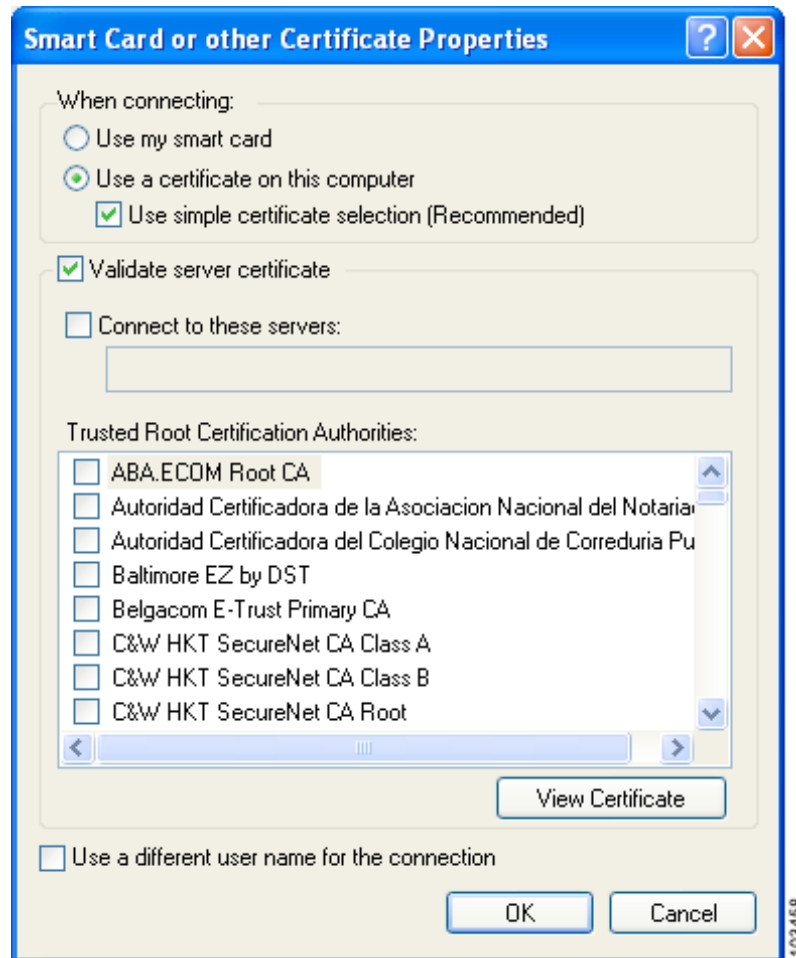
Step 1 Click the **Authentication** tab on the Wireless Network Properties window. The following window appears (see [Figure E-3](#)).

Figure E-3 Wireless Network Properties Window (Authentication Tab)



- Step 2** Check the **Enable IEEE 802.1x authentication for this network** check box if you did not enable WPA on the Association window.
- Step 3** For EAP type, choose **Smart Card or other Certificate**.
- Step 4** Click **Properties**. The Smart Card or other Certificate Properties window appears (see [Figure E-4](#)).

Figure E-4 Smart Card or other Certificate Properties Window



- Step 5** Choose the **Use a certificate on this computer** option.
- Step 6** Check the **Use simple certificate selection (Recommended)** check box.
- Step 7** Check the **Validate server certificate** check box if server certificate validation is required.

- Step 8** If you want to specify the name of the server to connect to, check the **Connect to these servers** check box and enter the server name in the field below.



Note If you enter a server name and the client adapter connects to a server that does not match the name you entered, you are prompted to accept or cancel the connection during the authentication process.



Note If you leave this field blank, the server name is not verified, and a connection is established as long as the certificate is valid.

- Step 9** In the Trusted Root Certification Authorities field, check the check box beside the name of the certificate authority from which the server certificate was downloaded.



Note If you leave all check boxes unchecked, you are prompted to accept a connection to the root certification authority during the authentication process.

- Step 10** Click **OK** in each window to save your settings. The configuration is complete.

- Step 11** If a pop-up message appears above the system tray informing you that you need to accept a certificate to begin the EAP authentication process, click the message and follow the instructions provided to accept the certificate.



Note You should not be prompted to accept a certificate for future authentication attempts. After you accept one, the same certificate is used subsequently.

- Step 12** If a message appears indicating the root certification authority for the server's certificate, and it is the correct certification authority, click **OK** to accept the connection. Otherwise, click **Cancel**.

- Step 13** If a message appears indicating the server to which your client adapter is connected, and it is the correct server to connect to, click **OK** to accept the connection. Otherwise, click **Cancel**.

The client adapter should now EAP authenticate.



Note Whenever the computer reboots and you enter your Windows username and password, the EAP authentication process begins automatically and the client adapter should EAP authenticate.

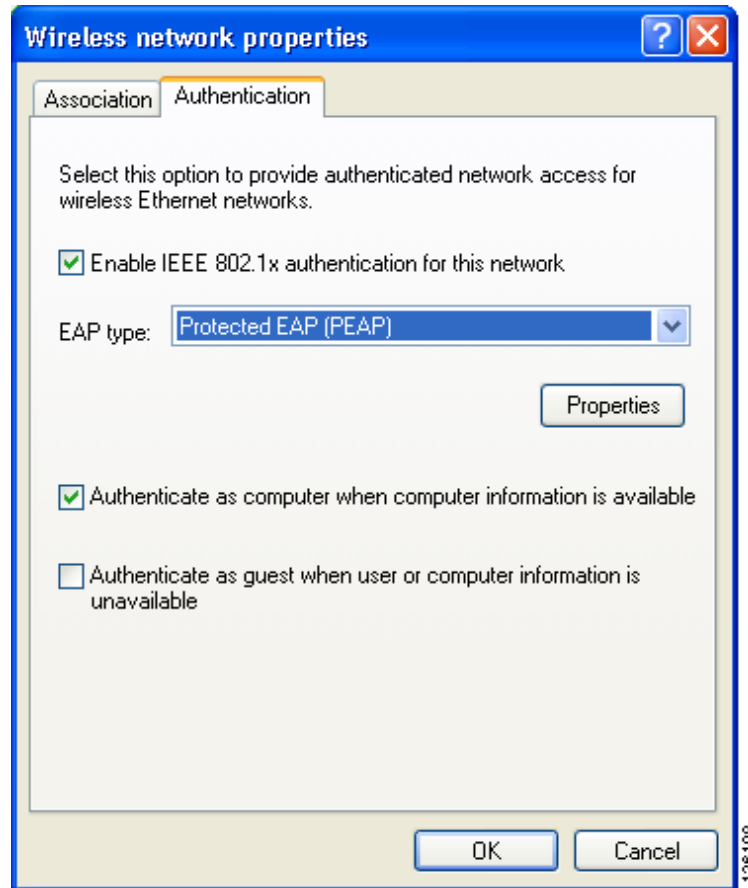
- Step 14** To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. Click **View** and **Refresh** to obtain the current status. If the client adapter is authenticated, the status reads *Authentication succeeded*.

Enabling PEAP Authentication

Follow the steps below to prepare the client adapter to use PEAP authentication, provided you have completed the initial configuration.

- Step 1** Click the **Authentication** tab on the Wireless Network Properties window. The following window appears (see [Figure E-5](#)).

Figure E-5 Wireless Network Properties Window (Authentication Tab)



- Step 2** Check the **Enable IEEE 802.1x authentication for this network** check box if you did not enable WPA on the Association window.
- Step 3** For EAP type, choose one of the following, depending on the software that is installed on your computer:
- **Protected EAP (PEAP)**—This option appears for PEAP (EAP-MSCHAP V2).
 - **PEAP**—This option appears for PEAP (EAP-GTC).



Note PEAP (EAP-GTC) is not officially supported for CB21AG and PI21AG client adapters, but you may be able to use it successfully if Cisco's PEAP security module (included in the Install Wizard file for Cisco Aironet 340, 350, and CB20A client adapters) was previously installed on your computer and installed after Service Pack 1 for Windows XP.

Step 4 Perform one of the following:

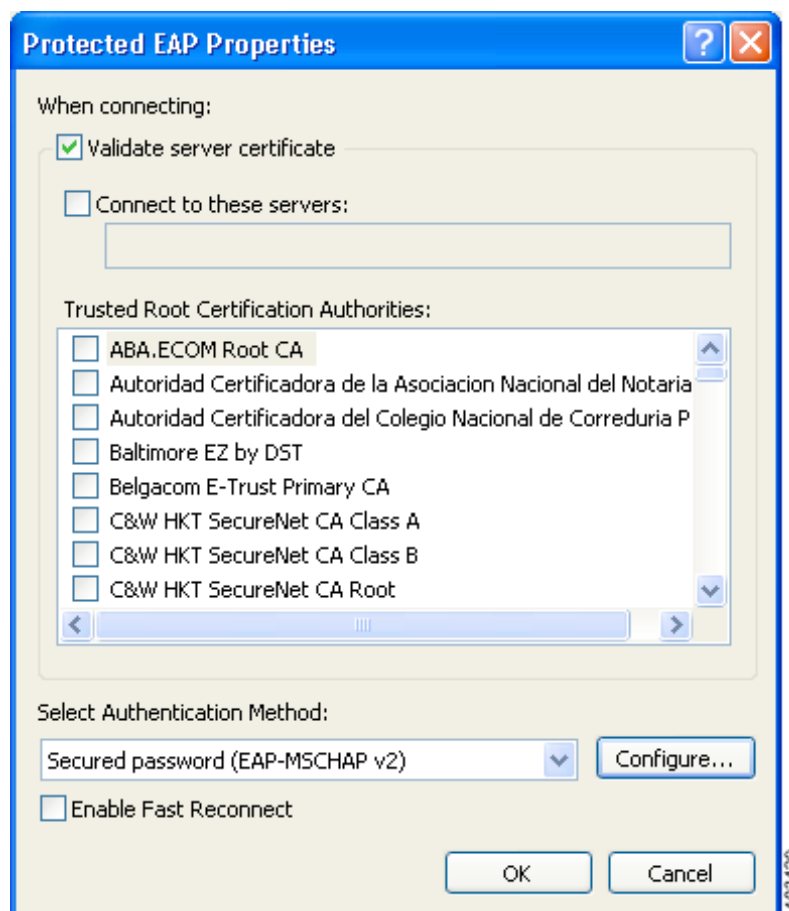
- If you chose Protected EAP (PEAP), follow the instructions in the “[Enabling PEAP \(EAP-MSCHAP V2\)](#)” section below.
- If you chose PEAP, follow the instructions in the “[Enabling PEAP \(EAP-GTC\)](#)” section on [page E-16](#).

Enabling PEAP (EAP-MSCHAP V2)

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

Step 1 Click **Properties**. The Protected EAP Properties window appears (see [Figure E-8](#)).

Figure E-6 Protected EAP Properties Window



Step 2 Check the **Validate server certificate** check box if server certificate validation is required (recommended).

- Step 3** If you want to specify the name of the server to connect to, check the **Connect to these servers** check box and enter the appropriate server name in the field below.



Note If you enter a server name and the client adapter connects to a server that does not match the name you entered, you are prompted to accept or cancel the connection during the authentication process.



Note If you leave this field blank, the server name is not verified, and a connection is established as long as the certificate is valid.

- Step 4** In the Trusted Root Certification Authorities field, choose the certificate authority from which the server certificate was downloaded.
- Step 5** In the Select Authentication Method drop-down box, choose **Secured password (EAP-MSCHAP v2)**.
- Step 6** Click **Configure**. The EAP MSCHAPv2 Properties window appears (see [Figure E-7](#)).

Figure E-7 EAP MSCHAPv2 Properties Window



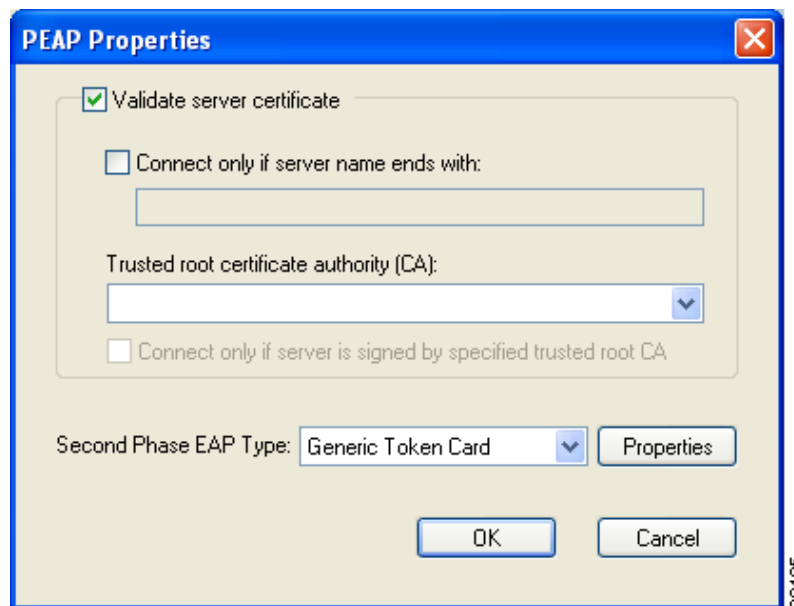
- Step 7** Make sure the **Automatically use my Windows logon name and password (and domain if any)** check box is checked.
- Step 8** Click **OK** in each window to save your settings. The configuration is complete.
- Step 9** The EAP authentication process begins automatically, and the client adapter should EAP authenticate using your Windows credentials. To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. Click **View** and **Refresh** to obtain the current status. If the client adapter is authenticated, the status reads *Authentication succeeded*.

Enabling PEAP (EAP-GTC)

Follow the steps below to enable PEAP (EAP-GTC).

- Step 1** Click **Properties**. The PEAP Properties window appears (see [Figure E-8](#)).

Figure E-8 PEAP Properties Window



- Step 2** Check the **Validate server certificate** check box if server certificate validation is required (recommended).
- Step 3** If you want to specify the name of the server to connect to, check the **Connect only if server name ends with** check box and enter the appropriate server name suffix in the field below.



Note If you enter a server name and the client adapter connects to a server that does not match the name you entered, you are prompted to accept or cancel the connection during the authentication process.



Note If you leave this field blank, the server name is not verified, and a connection is established as long as the certificate is valid.

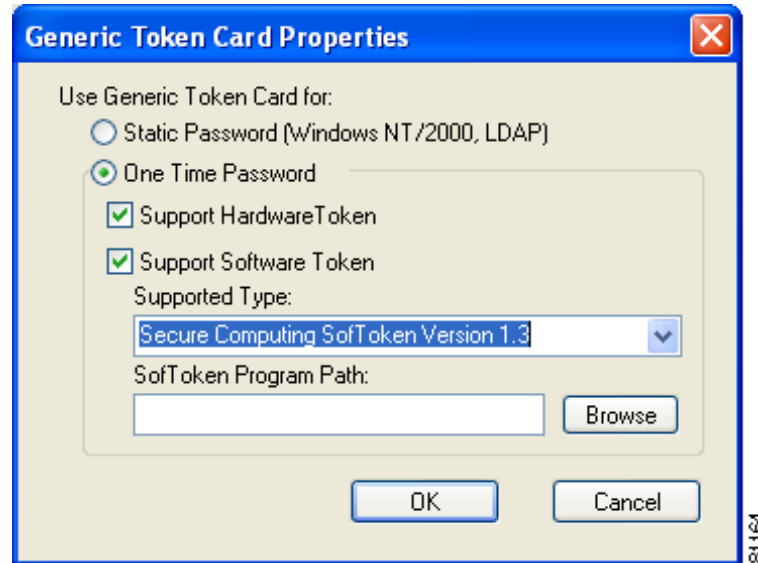
- Step 4** Make sure that the name of the certificate authority from which the server certificate was downloaded appears in the Trusted root certificate authority (CA) field. If necessary, click the arrow on the drop-down menu and choose the appropriate name.



Note If you leave this field blank, you are prompted to accept a connection to the root certification authority during the authentication process.

- Step 5** Check the **Connect only if server is signed by specified trusted root CA** check box if you want to ensure that the certificate server uses the trusted root certificate specified in the field above. This prevents the client from establishing connections to rogue access points.
- Step 6** Currently Generic Token Card is the only second phase EAP type available. Click **Properties**. The Generic Token Card Properties window appears (see [Figure E-9](#)).

Figure E-9 Generic Token Card Properties Window



- Step 7** Choose either the **Static Password (Windows NT/2000, LDAP)** or the **One Time Password** option, depending on your user database.
- Step 8** Perform one of the following:
- If you chose the **Static Password (Windows NT/2000, LDAP)** option in [Step 7](#), go to [Step 9](#).
 - If you chose the **One Time Password** option in [Step 7](#), check one or both of the following check boxes to specify the type of tokens that will be supported for one-time passwords:
 - **Support Hardware Token**—A hardware token device obtains the one-time password. You must use your hardware token device to obtain the one-time password and enter the password when prompted for your user credentials.
 - **Support Software Token**—The PEAP supplicant works with a software token program to retrieve the one-time password. You have to enter only the PIN, not the one-time password. If you check this check box, you must also choose from the Supported Type drop-down box the software token software that is installed on the client (such as Secure Computing SofToken Version 2.1, Secure Computing SofToken II 2.0, or RSA SecurID Software Token 2.5), and if Secure Computing SofToken Version 2.1 is selected, you must find the software program path using the Browse button.



Note

The SofToken Program Path field is unavailable if a software token program other than Secure Computing SofToken Version 2.1 is selected.

- Step 9** Click **OK** in each window to save your settings. The configuration is complete.
- Step 10** Refer to [Chapter 6](#) of the *Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows* (OL-1394-07 or later) for instructions on authenticating using PEAP (EAP-GTC).

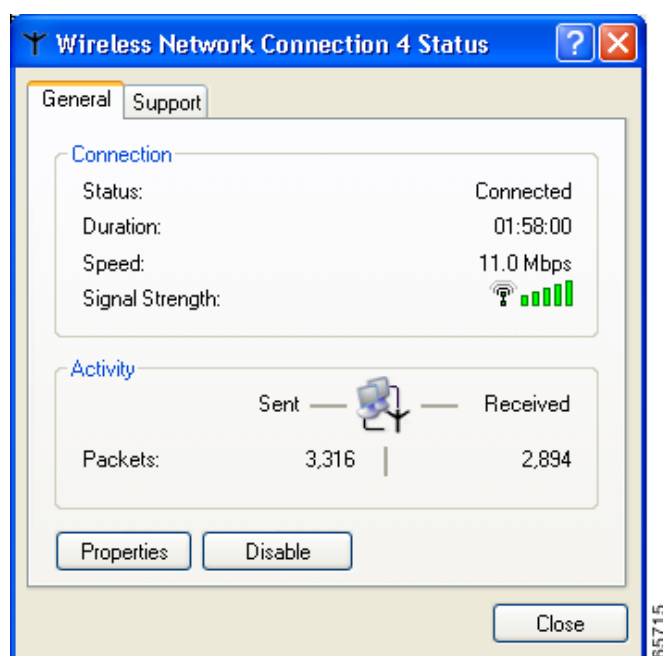
Associating to an Access Point Using Windows XP

Windows XP causes the client adapter's driver to automatically attempt to associate to the first network in the list of preferred networks (see [Figure E-1](#)). If the adapter fails to associate or loses association, it automatically switches to the next network in the list of preferred networks. The adapter does not switch networks as long as it remains associated to the access point. To force the client adapter to associate to a different access point, you must choose a different network from the list of available networks (and click **Configure** and **OK**).

Viewing the Current Status of Your Client Adapter

To view the status of your client adapter, click the icon of the two connected computers in the Windows system tray. The Wireless Network Connection Status window appears (see [Figure E-10](#)).

Figure E-10 Wireless Network Connection Status Window





APPENDIX **F**

Performing a Site Survey

This appendix explains how the site survey utility can be used when conducting a site survey.

The following topics are covered in this appendix:

- [Overview, page F-2](#)
- [Opening the Site Survey Utility, page F-3](#)
- [Selecting the Client Adapter, page F-3](#)
- [Using the Associated AP Status Tab, page F-4](#)
- [Using the AP Scan List Tab, page F-8](#)
- [Using the Proximity Beeper, page F-18](#)
- [Using Thresholds, page F-20](#)
- [Using AP Scanning, page F-26](#)
- [Viewing the Status Bar, page F-32](#)
- [Finding the Version of the Site Survey Utility, page F-33](#)
- [Accessing Online Help, page F-33](#)
- [Exiting the Site Survey Utility, page F-34](#)
- [Uninstalling the Site Survey Utility, page F-34](#)

Overview

**Note**

This appendix applies only to people who are responsible for conducting a site survey to determine the best placement of infrastructure devices within a wireless network.

The site survey utility can assist you in conducting a site survey. The utility operates at the RF level and is used to determine the best placement and coverage (overlap) for your network's infrastructure devices. During a site survey, the current status of the network is read from the client adapter, and the status display is updated four times per second so you can accurately gauge network performance. The feedback that you receive can help you to eliminate areas of low RF signal levels that can result in a loss of connection between the client adapter and its associated access point (or other infrastructure device).

The site survey utility operates in a passive mode. That is, it does not initiate any RF network traffic; it simply listens to the traffic that the client adapter hears and displays the results.

Guidelines

Keep the following guidelines in mind when preparing to perform a site survey:

- Perform the site survey when the RF link is functioning with all other systems and noise sources operational.
- Execute the site survey entirely from the mobile station.

Additional Information

Also consider the following operating and environmental conditions when performing a site survey:

- **Data rates**—Sensitivity and range are inversely proportional to data bit rates. Therefore, the maximum radio range is achieved at the lowest workable data rate, and a decrease in receiver threshold sensitivity occurs as the radio data increases.
- **Antenna type and placement**—Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height.
- **Physical environment**—Clear or open areas provide better radio range than closed or filled areas. Also, the less cluttered the work environment, the greater the range.
- **Obstructions**—A physical obstruction such as metal shelving or a steel pillar can hinder the performance of wireless devices. Avoid placing these devices in a location where a metal barrier is between the sending and receiving antennas.
- **Building materials**—Radio penetration is greatly influenced by the building material used in construction. For example, drywall construction allows greater range than concrete blocks, and metal or steel construction is a barrier to radio signals.

**Note**

Refer to the hardware installation guide for your infrastructure device for additional information on factors affecting placement.

Opening the Site Survey Utility

To open the site survey utility, choose **Start > Programs > Cisco Aironet > Aironet Site Survey Utility**.

**Note**

If you specified a different program folder during installation, you must access the site survey utility from that folder.

**Note**

The site survey utility is installed on your computer only if you checked the Install Site Survey Utility check box during the installation of the client adapter software. If you did not check this check box and want to use the site survey utility, uninstall the client adapter software and reinstall it, making sure to check the site survey check box.

Selecting the Client Adapter

**Note**

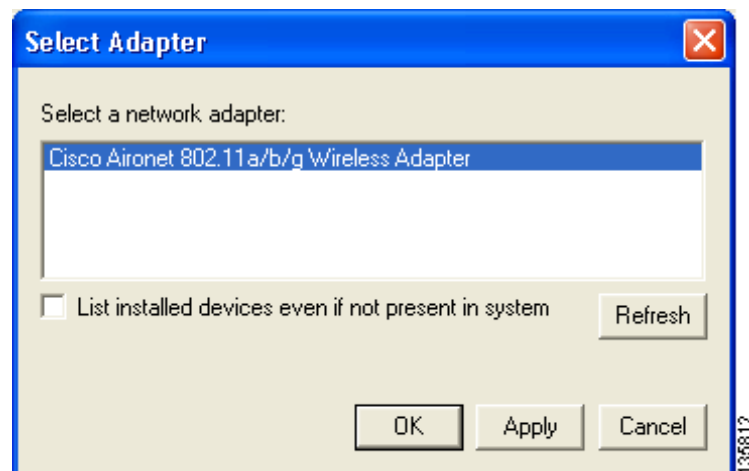
The site survey utility can be used only with CB21AG and PI21AG client adapters.

When the site survey utility starts, it scans for client adapters. If only one adapter is detected, it is selected automatically. However, if the utility detects multiple adapters or no adapters, the Select Adapter window appears (see [Figure F-1](#)).

**Note**

You can manually open this window at any time to select a different client adapter. Simply choose **Select Adapter** from the site survey utility's Action drop-down menu.

Figure F-1 Site Survey Utility - Select Adapter Window



Follow these steps to select the desired client adapter.

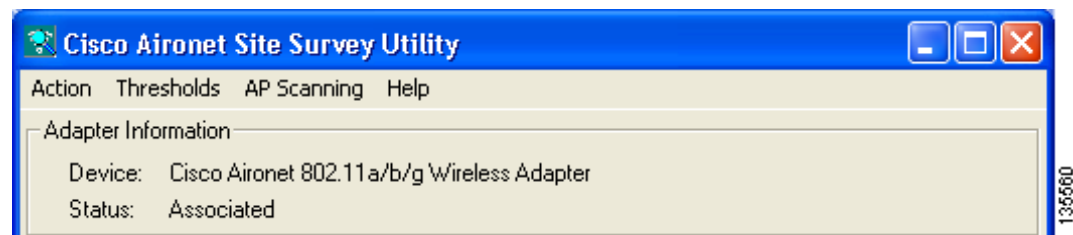
- Step 1** If you want to be able to choose client adapters that are installed but not physically present in your computer, check the **List installed devices even if not present in system** check box.
- Step 2** From the Select a Network Adapter list, select the client adapter that you want to use with the site survey utility.



Note Click **Refresh** to update the list of available client adapters (for instance, after an adapter has been ejected or inserted).

- Step 3** Click **OK** to save your selection and exit the Select Adapter window. The top of the site survey utility's main window (see [Figure F-2](#)) shows the client adapter that is being used with the utility and its current association status (Associated, Not Associated, Device Not Present, or Not a Wireless Adapter).

Figure F-2 Site Survey Utility - Top of Main Window



Using the Associated AP Status Tab

You can perform these functions from the Associated AP Status tab:

- Specify display units, [page F-4](#)
- View the access point's status, [page F-5](#)

Follow the instructions on the pages indicated to perform these functions.

Specifying Display Units

The **Display in percent** check box at the bottom of the Associated AP Status tab enables you to specify how display units are shown.

- Unchecking this check box causes the signal strength and noise level to be shown in decibels with respect to milliwatts (dBm) and the signal-to-noise ratio to be shown in decibels (db). This option, which is the default value, provides a more accurate representation of the data being presented than the percentage option.
- Checking this check box causes the signal strength, signal quality or beacons received, and overall link quality to be shown as a percentage.

Viewing the Access Point's Status

The Associated AP Status tab shows the status of the access point to which your client adapter is associated. Figure F-3 shows the tab with display units shown in dBm, and Figure F-4 shows the tab with display units shown as a percentage.

Figure F-3 Site Survey Utility - Associated AP Status Tab (with Display Units in dBm)

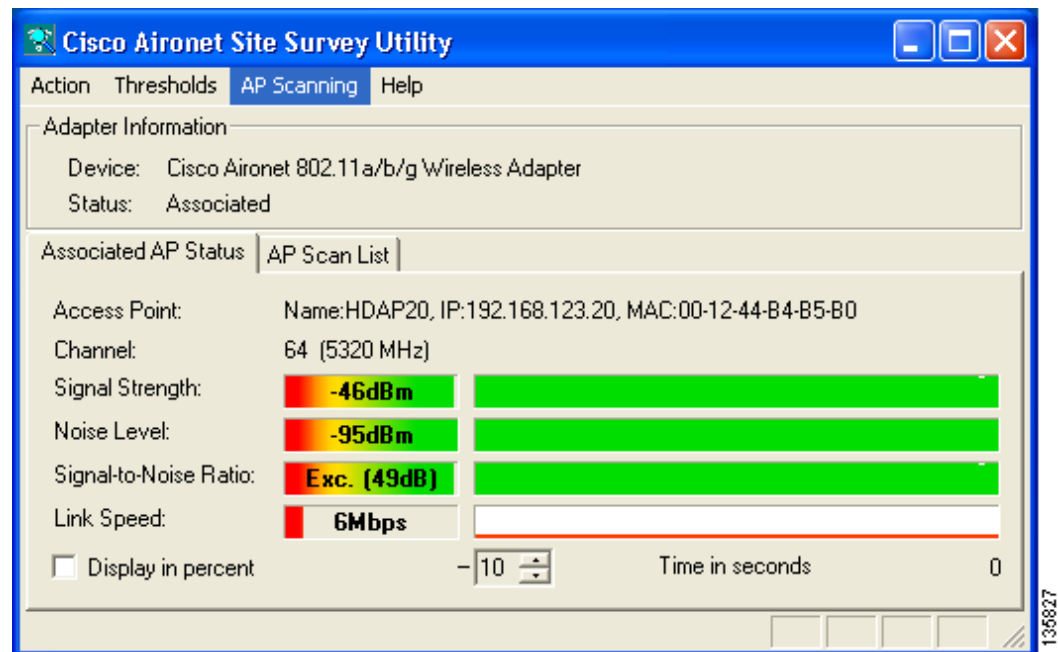


Figure F-4 Site Survey Utility - Associated AP Status Tab (with Display Units as a Percentage)

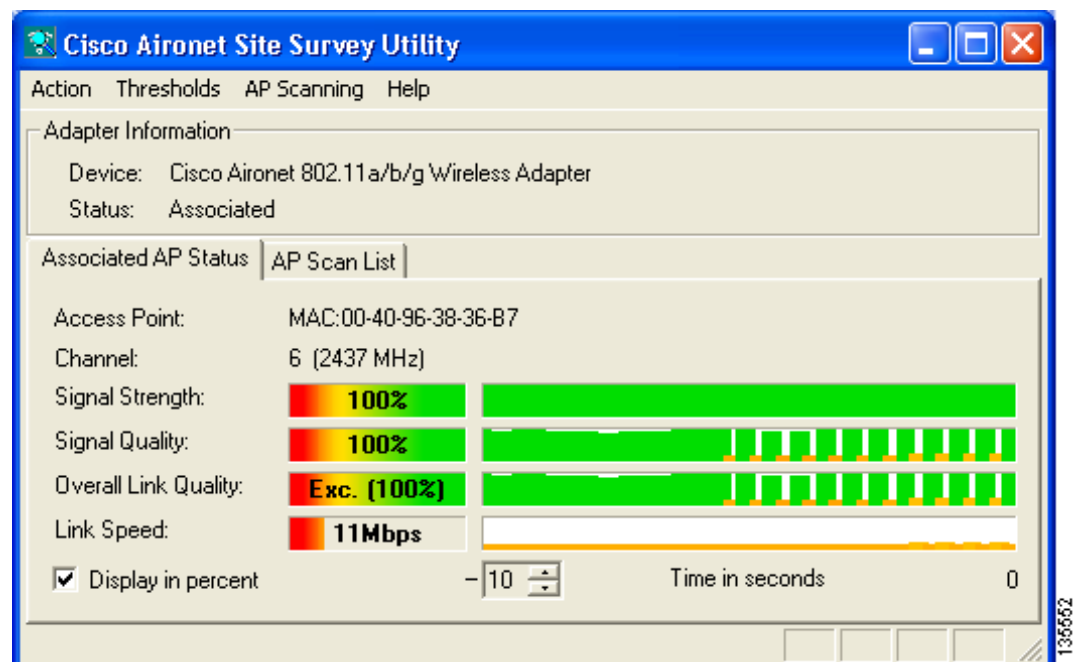


Table F-1 interprets the information that is displayed on the Associated AP Status tab.

**Note**

The trend graphs to the right of the smaller bar graphs provide a graphical representation of activity in the past 10 to 60 seconds. The height of an individual trend graph is proportional to the width of its corresponding bar graph. The time is displayed as a negative value to indicate that the data is older at the left edge of the graph than at the right. Use the up and down arrows to select the desired number of seconds from -10 through -60. The default value is -10.

Table F-1 Site Survey Utility - Associated AP Status

Associated AP Status Parameter	Description
Access Point	<p>The access point to which your client adapter is associated. This field may show the access point's name, IP address, and MAC address.</p> <p>Note This information is shown only if the access point was configured with a name or IP address, Aironet Extensions are enabled (on access points running Cisco IOS release 12.2(4)JA or greater), and the access point transmits this information.</p> <p>Note This field shows up to 15 characters for the access point name although the name may be longer.</p> <p>Note If Aironet Extensions are disabled, the IP address of the associated access point is shown as 0.0.0.0.</p> <p>Note This field displays the MAC address of the access point's Ethernet port (for access points that do not run Cisco IOS software) or the MAC address of the access point's radio (for access points that run Cisco IOS software). The MAC address of the Ethernet port on access points that run Cisco IOS software is printed on a label on the back of the device.</p>
Channel	<p>The channel and radio frequency (in MHz) that the access point is currently using for communications.</p> <p>Value: Dependent on radio band and regulatory domain</p>
Signal Strength	<p>The signal strength of the most recently received packets. The higher the value and the wider the bar graph, the stronger the signal.</p> <p>The trend graph to the right of the bar graph provides a visual interpretation of the signal strength over time. Differences in signal strength are indicated by the following colors: green (strongest), yellow (middle of the range), and red (weakest).</p> <p>Range: -95 to -45 dBm or 0 to 100%</p> <p>Note The actual dBm reading could exceed the stated range.</p>

Table F-1 **Site Survey Utility - Associated AP Status (continued)**

Associated AP Status Parameter	Description
Noise Level	<p>The level of background radio frequency energy. The lower the value and the wider the bar graph, the less background noise present.</p> <p>The trend graph to the right of the bar graph provides a visual interpretation of the level of background noise over time. Differences in background noise level are indicated by the following colors: green (low noise), yellow (middle of the range), and red (high noise).</p> <p>Range: –45 to –95 dBm</p> <p>Note The actual reading could exceed the stated range.</p> <p>Note This parameter appears only if the Display in Percent check box is unchecked.</p>
Signal Quality	<p>The signal quality of the most recently received packets. The higher the value and the wider the bar graph, the clearer the signal.</p> <p>The trend graph to the right of bar graph provides a visual interpretation of the signal quality over time. Differences in signal quality are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality).</p> <p>Range: 0 to 100%</p> <p>Note This parameter appears only if the Display in Percent check box is checked.</p>
Beacons Received	<p>The percentage of beacon packets received from the access point versus those expected to have been sent. The higher the value and the wider the bar graph, the clearer the signal.</p> <p>The trend graph to the right of bar graph provides a visual interpretation of the signal clarity over time. Differences in signal clarity are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality).</p> <p>Example: The access point sends out 10 beacons per second, so you would expect the client adapter to receive 50 beacon packets in 5 seconds. If it receives only 40 packets, the percentage of beacons received would be 80%.</p> <p>Range: 0 to 100%</p> <p>Note This parameter appears only if the Display in Percent check box is checked and the client adapter does not provide a signal quality value.</p>

Table F-1 **Site Survey Utility - Associated AP Status (continued)**

Associated AP Status Parameter	Description
Signal-to-Noise Ratio	<p>The difference between the signal strength and the noise level. The higher the value and the wider the bar graph, the better the client adapter's ability to communicate with the access point.</p> <p>The trend graph to the right of the bar graph provides a visual interpretation of the signal-to-noise ratio over time. Differences in the client adapter's ability to communicate are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality).</p> <p>Range: Poor, Fair, Good, Excellent; 0 to 50 dB</p> <p>Note This parameter appears only if the Display in Percent check box is unchecked.</p>
Overall Link Quality	<p>A combination of signal strength and signal quality. The higher the value and the wider the bar graph, the better the client adapter's ability to communicate with the access point.</p> <p>The trend graph to the right of the bar graph provides a visual interpretation of the overall link quality over time. Differences in quality are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality).</p> <p>Value: Poor, Fair, Good, Excellent; 0 to 100%</p> <p>Note This parameter appears only if the Display as Percent check box is checked.</p>
Link Speed	<p>The site survey utility monitors transmitted network traffic, and the link speed reflects the current transmit rate of data packets.</p> <p>The trend graph provides a visual interpretation of the packet transmit rate over time. Differences in link speed are indicated by the following colors: green (fastest), yellow (middle of the range), and red (slowest).</p> <p>Value: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps, depending on radio band</p>

Using the AP Scan List Tab

You can perform these functions from the AP Scan List tab:

- View the AP scan list, [page F-9](#)
- Pause the AP scan list, [page F-13](#)
- View AP details, [page F-13](#)
- Generate an AP scan log file, [page F-16](#)
- View an accumulation of access points, [page F-18](#)

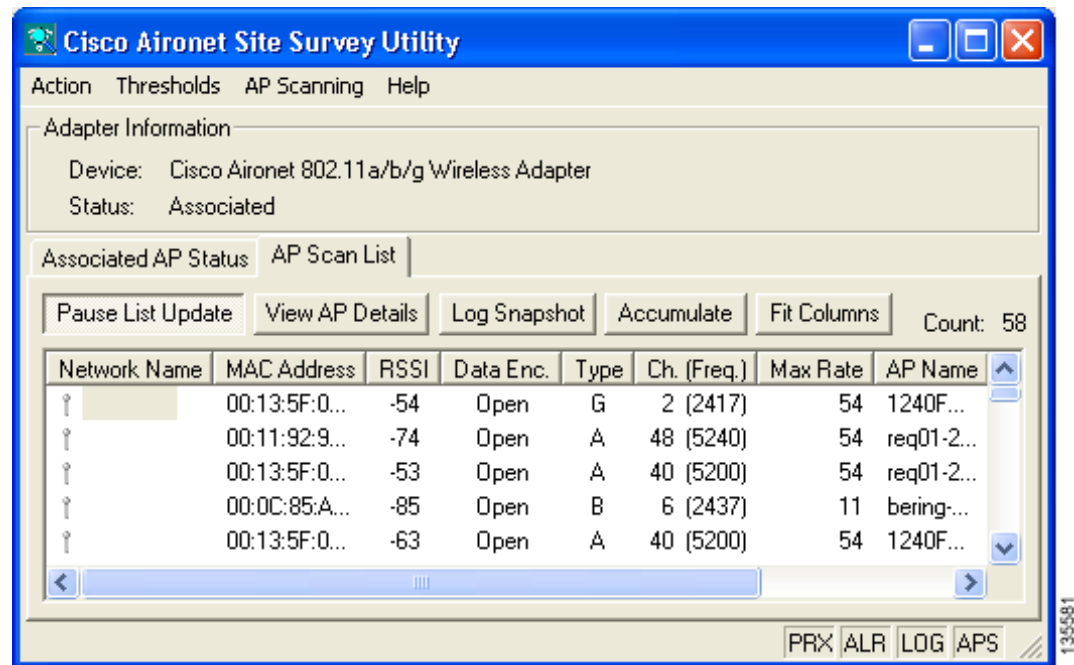
Follow the instructions on the pages indicated to perform these functions.

Viewing the AP Scan List


Your client adapter can detect nearby access points by the beacon signals that the access points continually transmit. The AP scan list displays a continuously updated list of the access points detected by your client adapter as well as the information contained in their beacons.

To view the AP scan list, click the **AP Scan List** tab. The AP scan list appears (see [Figure F-5](#)).

Figure F-5 Site Survey Utility - AP Scan List



To view the entire list of access points and all their information, perform one of the following:

- Click the resize tab in the lower right corner of the main window and drag it until the window reaches the desired size. 
- Use the vertical and horizontal scroll bars.
- Click the middle button in the top right corner of the window.



Note

Clicking **Fit Columns** resizes the columns on the AP scan list so that they are as wide as their widest text. This feature enables you to view the text in each column without it being truncated. However, you can also manually resize the columns by clicking on the edges of the column headers and dragging.

[Table F-2](#) interprets the information that is displayed in the AP scan list.



Note

The AP Detailed Information window provides details for many of the parameters listed in [Table F-2](#). See the [“Viewing AP Details”](#) section on [page F-13](#) for additional information.

**Note**

The AP Scanning drop-down menu contains options that enable you to save and open the AP scan list. These two options are available only when the AP Scan List tab is selected. See the [“Using AP Scanning” section on page F-26](#) for more information.

Table F-2 Site Survey Utility - AP Scan List







AP Scan List Parameter	Description						
Count	<p>The number of rows, or access points, in the scan list.</p> <p>Note This parameter appears above the AP scan list and to the right.</p>						
Network Name	<p>The network name, or service set identifier (SSID), indicates the name of an available wireless network. The icon to the left of the SSID provides information on link status.</p> <table border="1"> <thead> <tr> <th>Icon</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td>An available wireless network.</td></tr> <tr> <td></td><td>The wireless network to which your client adapter is currently associated.</td></tr> </tbody> </table> <p>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.</p>	Icon	Description		An available wireless network.		The wireless network to which your client adapter is currently associated.
Icon	Description						
	An available wireless network.						
	The wireless network to which your client adapter is currently associated.						
MAC Address	<p>The access point's MAC address.</p> <p>Note This field displays the MAC address of the access point's Ethernet port (for access points that do not run Cisco IOS software) or the MAC address of the access point's radio (for access points that run Cisco IOS software). The MAC address of the Ethernet port on access points that run Cisco IOS software is printed on a label on the back of the device.</p>						
RSSI	<p>The received signal strength indicator (RSSI) is a measure of signal strength in decibels with respect to milliwatts (dBm).</p>						
Time of Day	<p>The date and time when the signal strength of each access point was at its maximum. They appear in this format: 2005-07-20 16:13:09.</p> <p>Note The time is based on a 24-hour clock.</p> <p>Note This field is visible only in Accumulate mode. See the “Viewing an Accumulation of Access Points” section on page F-18 for information on the Accumulate mode.</p>						

Table F-2 Site Survey Utility - AP Scan List (continued)

AP Scan List Parameter	Description						
Data Encryption	Indicates whether the data exchanged with this access point is encrypted. Value: Secure or Open						
	<table> <tr> <th>Value</th><th>Description</th></tr> <tr> <td>Secure</td><td>The data exchanged with this access point is encrypted.</td></tr> <tr> <td>Open</td><td>The data exchanged with this access point is unencrypted.</td></tr> </table>	Value	Description	Secure	The data exchanged with this access point is encrypted.	Open	The data exchanged with this access point is unencrypted.
Value	Description						
Secure	The data exchanged with this access point is encrypted.						
Open	The data exchanged with this access point is unencrypted.						
Type	The IEEE 802.11 standard that describes the access point's radio band. Value: A, B, or G						
Channel (Frequency)	The channel and radio frequency (in MHz) that the access point is currently using for communications. Value: Dependent on radio band and regulatory domain						
Max Rate	The maximum rate at which the client adapter can transfer data with an access point. The supported rates of both the client adapter and the access point are examined, and the highest rate that they have in common is the one that is used.						
AP Name	The access point's name. It is shown only if the access point was configured with a name, Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later), and the access point transmits this information. Note This field shows up to 15 characters although the name of the access point may be longer.						
Load	The access point's channel utilization in terms of traffic and throughput. Value: 0 to 100% Note This parameter is shown only if the access point is using QoS Basis Service Set (QBSS) or call admission control (CAC). If neither is used, this field is left blank. If both are used, the value comes from the QBSS.						
CCX	The version of Cisco Compatible Extensions (CCX) supported by the access point. It is shown only if the access point transmits this information. Value: 1, 2, 3, or 4						

Table F-2 Site Survey Utility - AP Scan List (continued)

AP Scan List Parameter	Description																						
Other Information	<p>A list of miscellaneous values that may appear depending on the access point's current status and the information that it transmits.</p> <p>Values: See table below.</p> <table> <tr> <th>Value</th><th>Description</th></tr> <tr> <td>Ad-Hoc</td><td>Indicates that the device is not an access point but another client adapter operating in ad hoc mode.</td></tr> <tr> <td>CAC</td><td>Indicates that the access point is using distributed call admission control (CAC).</td></tr> <tr> <td>CEC</td><td>Indicates that the access point is using Cisco extended capabilities (CEC).</td></tr> <tr> <td>Power</td><td>Indicates that the access point can limit the transmitting power of the client adapter. The power limit is shown in milliwatts (mW).</td></tr> <tr> <td>Qos</td><td>Indicates that the access point is using quality of service (QoS). QoS on wireless LANs (WLAN) provides prioritization of traffic from the access point over the WLAN based on traffic classification.</td></tr> <tr> <td>RM-Normal RM-APScan RM-CliWlk</td><td>Indicates that the access point is using radio management. RM-Normal indicates normal status, RM-APScan indicates AP radio scan, and RM-CliWlk indicates client walkabout. Any unrecognized value appears as RM-State?.</td></tr> <tr> <td>Ssidl</td><td>Indicates that the access point is using the SSID List feature. The number of hidden SSIDs is shown as a number (for example, Ssidl:2).</td></tr> <tr> <td>WMM</td><td>Indicates that the access point is using Wi-Fi Multimedia (WMM), a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS).</td></tr> <tr> <td>WPA</td><td>Indicates that the access point is using Wi-Fi Protected Access (WPA), a standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification. WPA uses TKIP and MIC for data protection and 802.1X for authenticated key management.</td></tr> <tr> <td>WPA2</td><td>Indicates that the access point is using Wi-Fi Protected Access 2 (WPA2), the next generation of Wi-Fi security. It is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard. WPA2 uses AES-CCMP for data protection and 802.1X for authenticated key management.</td></tr> </table>	Value	Description	Ad-Hoc	Indicates that the device is not an access point but another client adapter operating in ad hoc mode.	CAC	Indicates that the access point is using distributed call admission control (CAC).	CEC	Indicates that the access point is using Cisco extended capabilities (CEC).	Power	Indicates that the access point can limit the transmitting power of the client adapter. The power limit is shown in milliwatts (mW).	Qos	Indicates that the access point is using quality of service (QoS). QoS on wireless LANs (WLAN) provides prioritization of traffic from the access point over the WLAN based on traffic classification.	RM-Normal RM-APScan RM-CliWlk	Indicates that the access point is using radio management. RM-Normal indicates normal status, RM-APScan indicates AP radio scan, and RM-CliWlk indicates client walkabout. Any unrecognized value appears as RM-State?.	Ssidl	Indicates that the access point is using the SSID List feature. The number of hidden SSIDs is shown as a number (for example, Ssidl:2).	WMM	Indicates that the access point is using Wi-Fi Multimedia (WMM), a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS).	WPA	Indicates that the access point is using Wi-Fi Protected Access (WPA), a standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification. WPA uses TKIP and MIC for data protection and 802.1X for authenticated key management.	WPA2	Indicates that the access point is using Wi-Fi Protected Access 2 (WPA2), the next generation of Wi-Fi security. It is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard. WPA2 uses AES-CCMP for data protection and 802.1X for authenticated key management.
Value	Description																						
Ad-Hoc	Indicates that the device is not an access point but another client adapter operating in ad hoc mode.																						
CAC	Indicates that the access point is using distributed call admission control (CAC).																						
CEC	Indicates that the access point is using Cisco extended capabilities (CEC).																						
Power	Indicates that the access point can limit the transmitting power of the client adapter. The power limit is shown in milliwatts (mW).																						
Qos	Indicates that the access point is using quality of service (QoS). QoS on wireless LANs (WLAN) provides prioritization of traffic from the access point over the WLAN based on traffic classification.																						
RM-Normal RM-APScan RM-CliWlk	Indicates that the access point is using radio management. RM-Normal indicates normal status, RM-APScan indicates AP radio scan, and RM-CliWlk indicates client walkabout. Any unrecognized value appears as RM-State?.																						
Ssidl	Indicates that the access point is using the SSID List feature. The number of hidden SSIDs is shown as a number (for example, Ssidl:2).																						
WMM	Indicates that the access point is using Wi-Fi Multimedia (WMM), a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS).																						
WPA	Indicates that the access point is using Wi-Fi Protected Access (WPA), a standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification. WPA uses TKIP and MIC for data protection and 802.1X for authenticated key management.																						
WPA2	Indicates that the access point is using Wi-Fi Protected Access 2 (WPA2), the next generation of Wi-Fi security. It is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard. WPA2 uses AES-CCMP for data protection and 802.1X for authenticated key management.																						

Pausing the AP Scan List

The AP scan list is updated continually. To pause the current list, click **Pause List Update** above the AP scan list.



Note

AP scanning continues to occur in the background when the Pause List Update button is depressed. For example, the threshold based on the AP scan list count continues to function.



Note

Clicking this button again resumes the list update.

Viewing AP Details

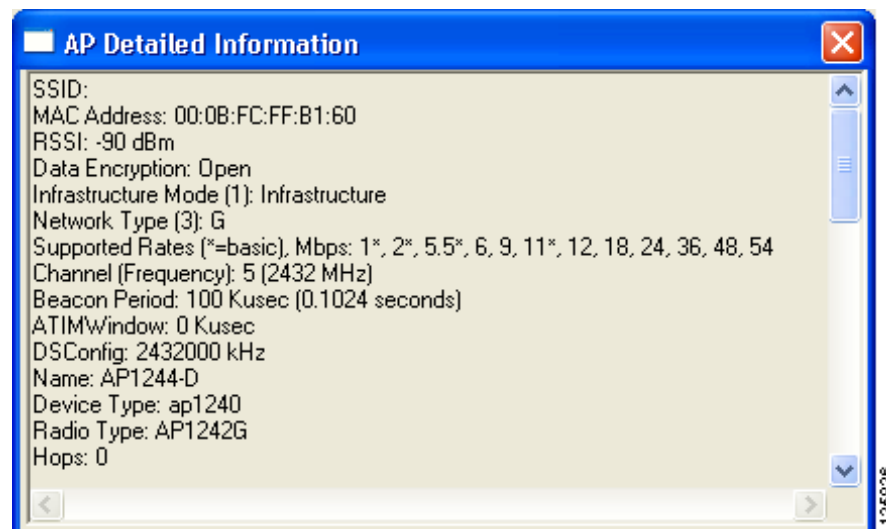
To view details for a particular access point in the AP scan list, select the desired network name in the scan list and click **View AP Details**. The AP Detailed Information window appears (see [Figure F-6](#)).



Note

You can also open the AP Detailed Information window by double-clicking in the first column of the desired row.

Figure F-6 Site Survey Utility - AP Detailed Information Window



[Table F-3](#) interprets the information that is displayed in the AP Detailed Information window.



Note

The AP Detailed Information window contains text summaries of all the information elements present in the access point's beacon or probe response. As a result, the window may contain different information than that described in [Table F-3](#).

**Note**

If you also want the AP Detailed Information window to display debugging information, including a hexadecimal debug-style dump of raw access point scan data, choose **Options** from the site survey utility's Action drop-down menu and check the **Enable Expert Mode for AP Detailed Information** check box. The debug information appears at the bottom of the AP Detailed Information window under the "Expert Mode (Debug Dump)" heading.

Table F-3 Site Survey Utility - AP Detailed Information

Detailed Information Parameter	Description
SSID	The network name, or service set identifier (SSID), indicates the name of the access point's wireless network.
MAC Address	<p>The access point's MAC address.</p> <p>Note This field displays the MAC address of the access point's Ethernet port (for access points that do not run Cisco IOS software) or the MAC address of the access point's radio (for access points that run Cisco IOS software). The MAC address of the Ethernet port on access points that run Cisco IOS software is printed on a label on the back of the device.</p>
RSSI	The received signal strength indicator (RSSI) is a measure of signal strength in decibels with respect to milliwatts (dBm).
Data Encryption	<p>Indicates whether the data exchanged with this access point is encrypted.</p> <p>Value: Secure or Open</p>
Infrastructure Mode	<p>Indicates whether the device is an access point operating in infrastructure mode or another client adapter operating in ad hoc mode.</p> <p>Value: Infrastructure or Ad-Hoc</p>
Network Type	<p>The IEEE 802.11 standard that describes the access point's radio band.</p> <p>Value: A, B, or G</p>
Supported Rates	<p>The rates at which the access point is capable of transmitting and receiving data packets.</p> <p>Value: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps</p>
Channel (Frequency)	<p>The channel and radio frequency that the access point is currently using for communications.</p> <p>Value: Dependent on radio band and regulatory domain</p>
Beacon Period	<p>The amount of time between access point beacons in Kilomicroseconds (Kμsec).</p> <p>Note One Kμsec equals 1,024 microseconds.</p>
ATIMWindow	<p>Announcement traffic information message (ATIM) window. The brief time period immediately following the transmission of each beacon in an ad hoc network. This value is expressed in Kilomicroseconds (Kμsec).</p> <p>Note One Kμsec equals 1,024 microseconds.</p> <p>Note This parameter's value is 0 when the device is operating in infrastructure mode.</p>

Table F-3 Site Survey Utility - AP Detailed Information (continued)

Detailed Information Parameter	Description
DSConfig	The frequency of the selected channel. Range: 2,412,000 to 2,484,000 kHz (802.11b/g); 5,000,000 to 6,000,000 kHz (802.11a)
Name	The access point's name. It is shown only if the access point was configured with a name, Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later), and the access point transmits this information. Note This field shows up to 15 characters although the name of the access point may be longer.
Device Type	The access point's model number.
Radio Type	The type of radio used in the access point.
Hops	The number of hops that the packets must take to get to the root. For example, if there is a repeater between your client adapter and the access point to which it is associated, the number of hops is 1.
Load	The access point's channel utilization in terms of traffic and throughput. Note This parameter is shown only if the access point is using QoS Basis Service Set (QBSS) or call admission control (CAC). If neither is used, this field is left blank. If both are used, the value comes from the QBSS.
CWmin	The minimum value used by the access point to calculate a contention window (CW). Note Contention occurs when two or more radios in the same area try to transmit at the same time. When this occurs, the radios wait for a certain amount of time before trying again. Because contention can occur more than once, the radios use a series of progressively longer wait periods, or "windows," each time they encounter contention for a given packet.
CWmax	The maximum value used by the access point to calculate a contention window (CW). Note Contention occurs when two or more radios in the same area try to transmit at the same time. When this occurs, the radios wait for a certain amount of time before trying again. Because contention can occur more than once, the radios use a series of progressively longer wait periods, or "windows," each time they encounter contention for a given packet.
Associations	The number of associations currently being maintained by the access point.
CCX Version	The version of Cisco Compatible Extensions (CCX) supported by the access point.

Table F-3 **Site Survey Utility - AP Detailed Information (continued)**

Detailed Information Parameter	Description
Power Limit	The power limit that the access point has set for the client adapter. It is shown in milliwatts (mW).
RM-Normal RM-APScan RM-CliWlk	Indicates that the access point is using radio management. RM-Normal indicates normal status, RM-APScan indicates AP radio scan, and RM-CliWlk indicates client walkabout. Any unrecognized value appears as RM-State?.

Generating an AP Scan Log File

To enter the current contents of the AP scan list into a log file, click **Log Snapshot**. The “Logged current AP Scan List” message appears below the scan list, and the log file is saved. The default filename is SST_APScanLog.txt, and the default location is the directory where the site survey utility is installed.

**Note**

If desired, you can change the filename and its location using the AP Scan List Logging Configuration window. See the [“Configuring AP Scan Logging” section on page F-26](#) for more information.

If the AP scan list is paused when you click Log Snapshot, the currently displayed data (not the latest available data) is added to the log. Each time you click **Log Snapshot**, the new scan list is written at the end of the existing log file.

To view the log file, choose **View AP Scan Log** from the AP Scanning drop-down menu. The log file opens in the configured viewer (see [Figure F-7](#)).

**Note**

The log file can be viewed in Notepad or any other viewer. However, because it is written in a comma-separated values (CSV) format, it can also be opened by a spreadsheet or database program (such as Microsoft Excel). If the file is renamed with a .csv extension, Microsoft Excel would automatically place the values in separate columns.

Figure F-7 Site Survey Utility - AP Scan Log File

```

SST_APScanLog - Notepad
File Edit Format View Help
2005-07-26 11:58:36 ,wnac_134,00:13:5F:0E:3D:B0,-80,Secure,G,8 (2447),54,wnac_208,,3,"QoS, WI
2005-07-26 11:58:36 ,wnac_134,00:12:44:B1:F6:60,-85,Secure,G,5 (2432),54,wnac_203,,3,"QoS, WI
2005-08-08 09:34:06 ,00:0C:30:50:78:38,-81,2005-08-08 09:34:06 ,Secure,B,3 (2422),11*,mukun
2005-08-08 09:34:06 ,00:13:5F:0E:CA:40,-63,2005-08-08 09:34:06 ,open,G,2 (2417),54,1240FRED
2005-08-08 09:34:06 ,00:0F:F7:2D:D4:D0,-80,2005-08-08 09:34:06 ,open,G,3 (2422),54,1300FRED
2005-08-08 09:34:06 ,00:11:92:90:A5:00,-84,2005-08-08 09:34:06 ,Secure,A,44 (5220),54,req01
2005-08-08 09:34:06 ,00:13:5F:0E:CC:40,-58,2005-08-08 09:34:06 ,open,A,40 (5200),54,1240FRE
2005-08-08 09:34:06 ,00:13:5F:0E:CD:20,-41,2005-08-08 09:34:06 ,open,A,40 (5200),54,req01-2:
2005-08-08 09:34:06 ,00:0D:BD:43:E9:DB,-88,2005-08-08 09:34:06 ,open,B,3 (2422),11*,jjgu-wd
2005-08-08 09:34:06 ,00:11:92:90:A2:B0,-76,2005-08-08 09:34:06 ,open,A,48 (5240),54,req01-2:
2005-08-08 09:34:06 ,00:12:00:EF:30:A1,-87,2005-08-08 09:34:06 ,Secure,G,1 (2412),54,AP1200
2005-08-08 09:34:06 ,00:0D:28:88:D5:C1,-78,2005-08-08 09:34:06 ,open,B,4 (2427),11*,req01-2:
2005-08-08 09:34:06 ,00:0C:CE:B5:B7:75,-83,2005-08-08 09:34:06 ,Secure,A,36 (5180),54,req01
2005-08-08 09:34:06 ,00:05:9A:3D:ED:23,-87,2005-08-08 09:34:06 ,Secure,G,11 (2462),54,DD_Ca
2005-08-08 09:34:06 ,00:0D:28:88:D5:D3,-89,2005-08-08 09:34:06 ,Secure,B,1 (2412),11*,req01
2005-08-08 09:34:06 ,00:13:5F:0E:CB:20,-53,2005-08-08 09:34:06 ,open,G,1 (2412),54,req01-21
2005-08-08 09:34:06 ,00:0D:28:88:CA:B9,-89,2005-08-08 09:34:06 ,Secure,B,4 (2427),11*,req01
2005-08-08 09:34:06 ,1400RACK,00:0C:85:32:C7:25,-67,2005-08-08 09:34:06 ,open,A,161 (5805),5.
2005-08-08 09:34:06 ,350RACK,00:40:96:59:9D:4F,-70,2005-08-08 09:34:06 ,open,B,6 (2437),11*,
2005-08-08 09:34:06 ,aes-range,00:0B:85:52:65:C1,-72,2005-08-08 09:34:06 ,open,A,36 (5180),5.
2005-08-08 09:34:06 ,akita-ma-wpa2,00:13:5F:0E:59:BC,-88,2005-08-08 09:34:06 ,Secure,A,64 (5
2005-08-08 09:34:06 ,akita-ma-wpa2,00:0B:85:23:EA:D3,-86,2005-08-08 09:34:06 ,Secure,A,44 (5
2005-08-08 09:34:06 ,akita-ma1,00:13:5F:0E:59:BD,-88,2005-08-08 09:34:06 ,open,A,64 (5320),5.
2005-08-08 09:34:06 ,akita-ma1,00:0B:85:23:EA:D2,-86,2005-08-08 09:34:06 ,open,A,44 (5220),5.
2005-08-08 09:34:06 ,akita1,00:13:5F:0E:59:BF,-86,2005-08-08 09:34:06 ,Secure,A,64 (5320),54
2005-08-08 09:34:06 ,akita1,00:0B:85:23:EA:D0,-87,2005-08-08 09:34:06 ,Secure,A,44 (5220),54
2005-08-08 09:34:06 ,akita1,00:0B:85:04:73:FF,-76,2005-08-08 09:34:06 ,open,B,11 (2462),11*,
2005-08-08 09:34:06 ,akita1,00:0B:85:04:73:F0,-81,2005-08-08 09:34:06 ,open,A,149 (5745),54,
2005-08-08 09:34:06 ,akita1,00:0E:83:19:28:DF,-75,2005-08-08 09:34:06 ,open,A,36 (5180),54,,
2005-08-08 09:34:06 ,akita1,00:0E:83:19:28:D0,-88,2005-08-08 09:34:06 ,open,B,11 (2462),11*,
2005-08-08 09:34:06 ,akita_dd,00:0B:85:04:73:F3,-78,2005-08-08 09:34:06 ,open,A,149 (5745),5.
2005-08-08 09:34:06 ,akita_dd,00:0E:83:19:28:DC,-72,2005-08-08 09:34:06 ,open,A,36 (5180),54
2005-08-08 09:34:06 ,akita_eap,00:0B:85:04:73:F2,-78,2005-08-08 09:34:06 ,Secure,A,149 (5745
2005-08-08 09:34:06 ,akita_eap,00:0E:83:19:28:DD,-72,2005-08-08 09:34:06 ,Secure,A,36 (5180)

```

The log entries are time-stamped and appear in ASCII text. Each line typically represents a different access point.

**Note**

If the Accumulate button is depressed when you click Log Snapshot, two timestamps appear on each line. The timestamp in column one of the log file is the time when the log entry is made. The second timestamp, which appears only when the Accumulate button is depressed, is the Time of Day. This value indicates the date and time when the signal strength of each access point was at its maximum. Both timestamps appear in this format: 2005-07-20 16:13:09. The time is based on a 24-hour clock. For example, the first two lines in [Figure F-7](#) show only one timestamp while the remaining lines show both timestamps.

**Note**

As an alternative to using the Log Snapshot button, you can configure the site survey utility to automatically copy the contents of the AP scan list to a log file using the AP Scanning drop-down menu options. See the [“Using AP Scanning”](#) section on page F-26 for more information.

Viewing an Accumulation of Access Points

Clicking the **Accumulate** button changes the behavior of the AP scan list. Instead of displaying only the current AP scan list, the list includes all of the access points (based on MAC address) that have appeared in the scan list since the Accumulate button was last clicked.

After a scan line is added to the list, it is never removed nor updated with new scan information unless the signal strength (RSSI) of the latest scan is greater than or equal to any detected previously from that access point. The Time of Day field, which appears only in Accumulate mode, indicates the date and time when the signal strength of each access point was at its maximum.

The Accumulate mode provides a convenient way to list all access points within a facility, not just those that may be visible at one time from a particular location. By using the information in the Time of Day field with a site map and a wristwatch, you may be able to determine the approximate location of each access point in the list.

**Note**

Clicking the Accumulate button again deactivates the Accumulate mode and returns the current AP scan list.

**Note**

You can use the Save AP Scan List and Open AP Scan List options in the AP Scanning drop-down menu to save and reload accumulated scan lists back into the application at a later time.

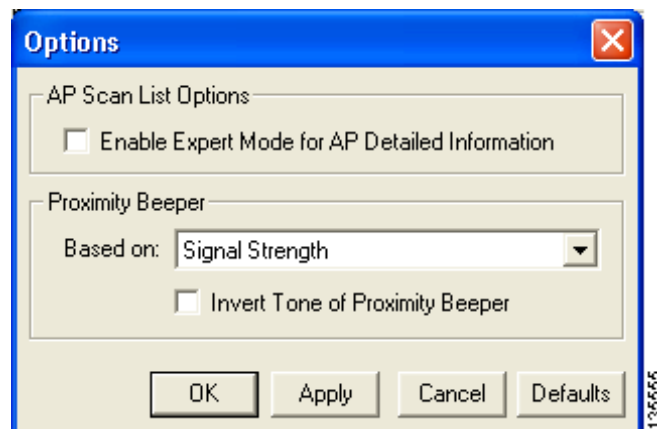
Using the Proximity Beeper

You can use the site survey utility's proximity beeper to identify areas where wireless coverage is good or weak based on the client adapter's proximity to access points within a particular area. The beeper can be set to sound as the client adapter approaches or moves farther away from an access point.

Configuring the Proximity Beeper

Follow these steps to configure the proximity beeper.

- Step 1** Choose **Options** from the site survey utility's Action drop-down menu. The Options window appears (see [Figure F-8](#)).

Figure F-8 Site Survey Utility - Options Window

Step 2 Choose one of these options on which the proximity beeper will be based:

Proximity Beeper Option	Description
Signal Strength	The beeper sounds as an access point's signal becomes stronger. Note This is the default value.
Noise Level/Signal Quality	The beeper sounds as the level of background radio frequency energy decreases or the signal quality of the most recently received packets improves.
Signal-to-Noise Ratio/ Overall Link Quality	The beeper sounds as the client adapter's ability to communicate with an access point improves.
Link Speed	The beeper sounds as the transmit rate of data packets between the client adapter and an access point becomes faster.

Step 3 Perform one of the following to set the tone of the proximity beeper:

- Uncheck the **Invert Tone of Proximity Beeper** check box if you want the beeper's rate and pitch to increase in response to the option selected in [Step 2](#). The beeps become more alarming as the client adapter moves closer to an access point, enabling you to identify areas of good coverage. This is the default setting.
- Check the **Invert Tone of Proximity Beeper** check box if you want the beeper's rate and pitch to decrease in response to the option selected in [Step 2](#). The beeps become more alarming as the client adapter approaches areas of weaker coverage.

Step 4 Click **OK** to save your changes.

Step 5 Follow the instructions in the [“Enabling the Proximity Beeper”](#) section below to enable the proximity beeper.

Enabling the Proximity Beeper

To enable the proximity beeper, choose **Enable Proximity Beeper** from the Action drop-down menu or press **F6**. When the beeper is enabled, a check mark appears next to the Enable Proximity Beeper menu option, and PRX appears in the site survey utility's status bar.

**Note**

To disable the proximity beeper, choose the **Enable Proximity Beeper** menu option again so that the check mark disappears or re-press **F6**.

Using Thresholds

You can perform these threshold-related functions:

- Configure threshold values, [page F-20](#)
- Enable threshold triggers, [page F-23](#)
- Enter a comment in the threshold log file, [page F-24](#)
- View the threshold log file, [page F-24](#)
- Delete the threshold log file, [page F-25](#)

Follow the instructions on the pages indicated to perform these functions.

Configuring Threshold Values

Follow these steps to configure threshold values that trigger audible alerts, entries in the threshold log file, or both.

-
- Step 1** Choose **Configure Thresholds** from the site survey utility's Thresholds drop-down menu. The Threshold Logging Configuration window appears (see [Figure F-9](#)).

Figure F-9 Site Survey Utility - Threshold Logging Configuration Window

Threshold Logging Configuration

Triggers

Select the conditions that you want to trigger logging events:

☐ A change in the client adapter's association status

☐ Connectivity with this URL or IP Address:

www.cisco.com

An Associated AP Status value crosses a given threshold:

☐ Signal Strength -75 dBm

☐ Noise Level -65 dBm

☐ Signal-to-Noise Ratio 20 dB

☐ Link Speed 11 Mbps

Hysteresis

☒ Events are triggered only if the conditions persist for

3 seconds

Log File

Filename: SST_ThreshLog.txt Browse...

Viewer: notepad.exe Browse...

OK Apply Cancel Defaults

135559

Step 2 Check the check box for each condition below for which you want to trigger audible alerts, text entries in the threshold log file, or both. You can check as many as you like.

Condition	Description
A change in the client adapter's association status	Triggers audible alerts, log file entries, or both when the client adapter's association status changes. Default: Unchecked
Connectivity with this URL or IP Address	Triggers audible alerts, log file entries, or both when the client adapter is able to successfully access the specified URL or IP address after associating to an access point. When the client adapter associates to an access point, the connectivity test transmits ping requests to the specified URL or IP address at a rate of 4 per second for up to 10 seconds or until a ping reply is received. If a reply is received within that time, the test ends successfully. Otherwise, the test fails, and no triggers are generated. No further ping requests are sent until the client adapter loses association and reassociates. If you check this check box, be sure to also enter the URL or IP address that invokes the triggers. Default: Unchecked

Condition	Description
Signal Strength	<p>Triggers audible alerts, log file entries, or both when the Signal Strength value reaches or crosses over the specified threshold value. If you check this check box, be sure to also choose a threshold value.</p> <p>Threshold Value Range: –95 to –45 dBm or 0 to 100%</p> <p>Default: Unchecked; –75 dBm or 40%</p> <p>Note The actual dBm reading could exceed the stated threshold value range.</p> <p>Note The Display in percent check box on the Associated AP Status tab determines which threshold value units are used.</p>
Noise Level/Signal Quality	<p>Triggers audible alerts, log file entries, or both when the Noise Level or Signal Quality value reaches or crosses over the specified threshold value. If you check this check box, be sure to also choose a threshold value.</p> <p>Threshold Value Range: –45 to –95 dBm or 0 to 100%</p> <p>Default: Unchecked; –65 dBm or 40%</p> <p>Note The actual dBm reading could exceed the stated threshold value range.</p> <p>Note The Display in percent check box on the Associated AP Status tab determines which condition and threshold value units are used.</p>
Signal-to-Noise Ratio/Link Quality	<p>Triggers audible alerts, log file entries, or both when the Signal-to-Noise Ratio or Link Quality value reaches or crosses over the specified threshold value. If you check this check box, be sure to also choose a threshold value.</p> <p>Threshold Value Range: 0 to 50 dBm or 0 to 100%</p> <p>Default: Unchecked; 20 dBm or 40%</p> <p>Note The actual dBm reading could exceed the stated threshold value range.</p> <p>Note The Display in percent check box on the Associated AP Status tab determines which condition and threshold value units are used.</p>
Link Speed	<p>Triggers audible alerts, log file entries, or both when the Link Speed value reaches or crosses over the specified threshold value. If you check this check box, be sure to also choose a threshold value.</p> <p>Threshold Value Range: 0 to the maximum rate of the current connection</p> <p>Default: Unchecked; 11 Mbps</p>

**Note**

When a value reaches a threshold and stays there, continuous triggers are not generated. After a value reaches a threshold, it must become not equal to the threshold value before another trigger is generated.

Step 3 If you want to specify the length of time that the above conditions must exist before triggering audible alerts, log file entries, or both, check the **Hysteresis** check box and choose a value in seconds.

Range: 1 to 10 seconds

Default: Checked; 3 seconds



Note The Hysteresis setting does not apply to the connectivity test. Connectivity is achieved if just one ping response is returned.

Step 4 The Filename field specifies the name and location of the threshold log file. If you want to change the name of the log file, enter a new name in the Filename field. If you want to change the location of the log file, click **Browse**, navigate to the desired location, and click **OK**.

Default Name: SST_ThreshLog.txt

Default Location: The directory where the site survey utility is installed

Step 5 The Viewer field specifies the name and location of the program that is used to view the threshold log file. (To view the log file, choose **View Threshold Log** from the Thresholds drop-down menu.) If you want a different program to be used, click **Browse**, navigate to the location of the desired program, and click **OK**.

Default Program: Notepad.exe

Step 6 Click **OK** to save your changes.

Step 7 Follow the instructions in the [“Enabling Threshold Triggers”](#) section below to enable the threshold triggers.

Enabling Threshold Triggers

In the previous section, you specified the conditions under which threshold triggers are generated, provided those triggers are enabled.

To enable audible alerts when a threshold condition occurs, choose **Enable Threshold Alerts** from the Thresholds drop-down menu or press **F7**. When threshold alerts are enabled, a check mark appears next to the Enable Threshold Alerts menu option, and ALR appears in the site survey utility’s status bar.

To enable the logging of text messages to the threshold log file when a threshold condition occurs, choose **Enable Threshold Logging** from the Thresholds drop-down menu or press **F8**. When threshold logging is enabled, a check mark appears next to the Enable Threshold Logging menu option, and LOG appears in the site survey utility’s status bar.



Note You can enable one or both triggers.



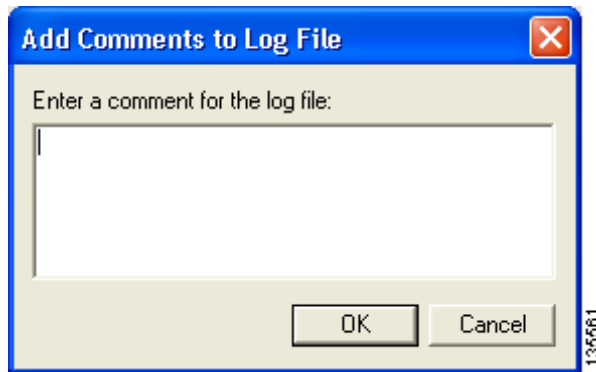
Note To disable the threshold triggers, choose the **Enable Threshold Alerts** and **Enable Threshold Logging** menu options again so that the check mark disappears or re-press **F7** and **F8**.

Entering a Comment in the Threshold Log File

Follow these steps if you want to enter a comment in the threshold log file.

- Step 1** Choose **Add User Comment** from the Thresholds drop-down menu. The Add Comments to Log File window appears (see [Figure F-10](#)).

Figure F-10 Site Survey Utility - Add Comments to Log File Window



- Step 2** Type one or more lines of text or paste text copied from another application.
- Step 3** Click **OK** to have your comments entered into the threshold log file.



Note User comments are entered in the threshold log file even if threshold logging is not currently enabled.

Viewing the Threshold Log File

Follow these steps to view the threshold log file from within the site survey utility.



Note You can also open the threshold log file from Windows Explorer.

- Step 1** Choose **View Threshold Log** from the Thresholds drop-down menu. The log file opens in the configured viewer (see [Figure F-11](#)).

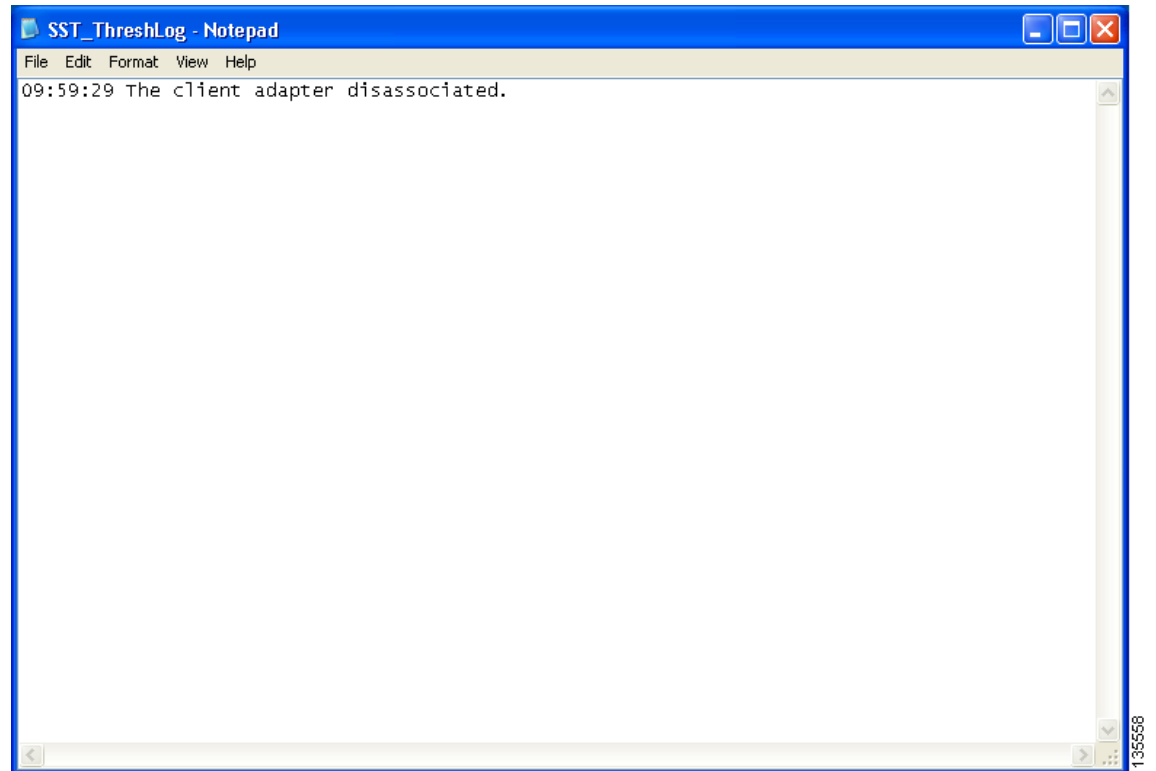


Note The View Threshold Log menu option is disabled if the log file does not exist.



Note [Figure F-11](#) shows the threshold log file in Notepad, but other viewers can be used.

Figure F-11 Site Survey Utility - Threshold Log File Window



- Step 2** Click the **X** in the upper right-hand corner of the window to close the window.
-

Deleting the Threshold Log File

Follow these steps to delete the threshold log file.

- Step 1** Choose **Delete Threshold Log** from the Thresholds drop-down menu.



Note The Delete Threshold Log menu option is disabled if the log file does not exist.

- Step 2** Click **Yes** when asked to confirm your decision.
-

Using AP Scanning

You can perform these functions related to AP scanning:

- Configure AP scan logging, [page F-26](#)
- Enable AP scan logging, [page F-28](#)
- View the AP scan log, [page F-28](#)
- Delete the AP scan log, [page F-30](#)
- Save the AP scan list, [page F-30](#)
- Open the AP scan list, [page F-31](#)

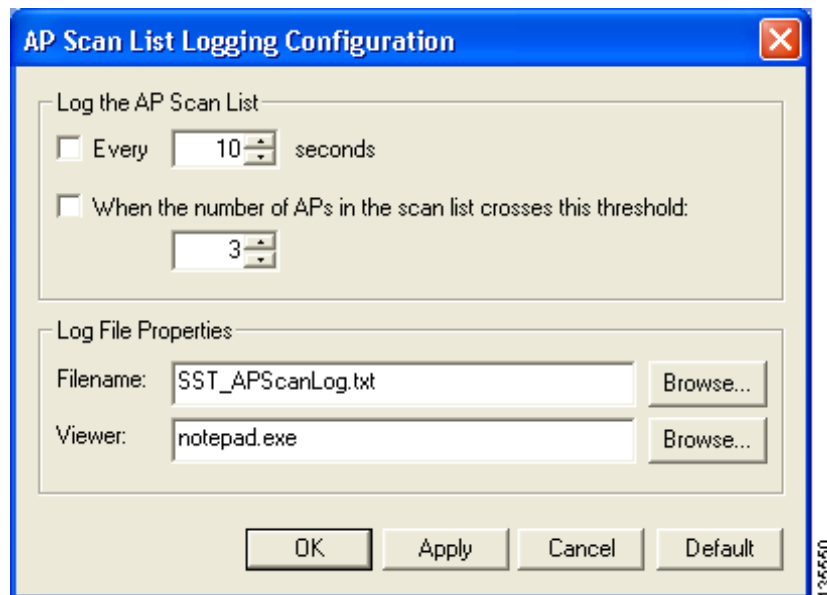
Follow the instructions on the pages indicated to perform these functions.

Configuring AP Scan Logging

Follow these steps to configure the site survey utility to automatically copy the contents of the AP scan list to a log file.

- Step 1** Choose **Configure AP Scan Logging** from the AP Scanning drop-down menu. The AP Scan List Logging Configuration window appears (see [Figure F-12](#)).

Figure F-12 Site Survey Utility - AP Scan List Logging Configuration Window



- Step 2** Check the check box and select a numerical value for each condition below that you want to cause the contents of the AP scan list to be automatically copied to a log file. You can check one or both.

Condition	Description
Every XXX seconds	<p>Causes the contents of the AP scan list to be copied to a log file after a specified amount of time elapses. For example, if you set the value to 60, the AP scan list is logged to a file every 60 seconds.</p> <p>Default: Unchecked; 10 seconds</p>
When the number of APs in the scan list crosses this threshold	<p>Causes the contents of the AP scan list to be copied to a log file whenever the number of access points in the scan list reaches or crosses over the specified threshold value. For example, if you set the value to 5, the AP scan list is logged to a file each time the number of access points in the scan list rises to or above 5 or falls to or below 5. However, if the number of access points in the scan list stays at 5, continuous triggers are not generated.</p> <p>Default: Unchecked; 3</p> <p>Note If threshold alerts are enabled (on the Thresholds drop-down menu), an audible alert sounds whenever the number of access points in the scan list reaches or crosses over the specified threshold value. Likewise, if threshold logging is enabled, a text entry is made to the threshold log file whenever this condition is met.</p>

- Step 3** The Filename field specifies the name and location of the AP scan log file. If you want to change the name of the log file, enter a new name in the Filename field. If you want to change the location of the log file, click **Browse**, navigate to the desired location, and click **OK**.

Default Name: SST_APScanLog.txt

Default Location: The directory in which the site survey utility is installed



Note The filename and location that you choose here also applies to the log file that is created when you click the Log Snapshot button on the AP Scan List tab.

- Step 4** The Viewer field specifies the name and location of the program that is used to view the AP scan log file. (To view the log file, choose **View AP Scan Log** from the AP Scanning drop-down menu.) If you want a different program to be used, click **Browse**, navigate to the location of the desired program, and click **OK**.

Default Program: Notepad.exe



Note The log file can be viewed in Notepad or any other viewer. However, because it is written in a comma-separated values (CSV) format, it can also be opened by a spreadsheet or database program (such as Microsoft Excel). If the file is renamed with a .csv extension, Microsoft Excel would automatically place the values in separate columns.

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

- Step 6** Follow the instructions in the [“Enabling AP Scan Logging”](#) section below to enable AP scan logging.

Enabling AP Scan Logging

To enable the site survey utility to automatically copy the contents of the AP scan list to a log file under the conditions specified above, choose **Enable AP Scan Logging** from the AP Scanning drop-down menu or press **F9**. When AP scan logging is enabled, a check mark appears next to the Enable AP Scan Logging menu option, and APS appears in the site survey utility's status bar.

**Note**

When AP scan logging is enabled, log entries are made even when the AP Scan List tab is not visible and when it is visible with updates paused.

**Note**

To disable AP scan logging, choose the **Enable AP Scan Logging** menu option again so that the check mark disappears or re-press **F9**.

Viewing the AP Scan Log

Follow these steps to view the AP scan log file from within the site survey utility.

**Note**

You can also open the AP scan log file from Windows Explorer.

Step 1

Choose **View AP Scan Log** from the AP Scanning drop-down menu. The log file opens in the configured viewer (see [Figure F-13](#)).

**Note**

The View AP Scan Log menu option is disabled if the log file does not exist.

**Note**

[Figure F-13](#) shows the AP scan log file in Notepad, but other viewers can be used.

Figure F-13 Site Survey Utility - AP Scan Log File

```

2005-07-26 11:58:36 ,wnac_134,00:13:5F:0E:3D:B0,-80,Secure,G,8 (2447),54,wnac_208,,3,"QoS, WI
2005-07-26 11:58:36 ,wnac_134,00:12:44:B1:F6:60,-85,Secure,G,5 (2432),54,wnac_203,,3,"QoS, WI
2005-08-08 09:34:06 ,00:0C:30:50:78:38,-81,2005-08-08 09:34:06 ,Secure,B,3 (2422),11*,mukun
2005-08-08 09:34:06 ,00:13:5F:0E:CA:40,-63,2005-08-08 09:34:06 ,open,G,2 (2417),54,1240FRED
2005-08-08 09:34:06 ,00:0F:F7:2D:D4:D0,-80,2005-08-08 09:34:06 ,open,G,3 (2422),54,1300FRED
2005-08-08 09:34:06 ,00:11:92:90:A5:00,-84,2005-08-08 09:34:06 ,Secure,A,44 (5220),54,req01
2005-08-08 09:34:06 ,00:13:5F:0E:CC:40,-58,2005-08-08 09:34:06 ,open,A,40 (5200),54,1240FRE
2005-08-08 09:34:06 ,00:13:5F:0E:CD:20,-41,2005-08-08 09:34:06 ,open,A,40 (5200),54,req01-2:
2005-08-08 09:34:06 ,00:0D:BD:43:E9:DB,-88,2005-08-08 09:34:06 ,open,B,3 (2422),11*,jjgu-wd
2005-08-08 09:34:06 ,00:11:92:90:A2:B0,-76,2005-08-08 09:34:06 ,open,A,48 (5240),54,req01-2:
2005-08-08 09:34:06 ,00:12:00:EF:30:A1,-87,2005-08-08 09:34:06 ,Secure,G,1 (2412),54,AP1200
2005-08-08 09:34:06 ,00:0D:28:88:D5:C1,-78,2005-08-08 09:34:06 ,open,B,4 (2427),11*,req01-2:
2005-08-08 09:34:06 ,00:0C:CE:B5:B7:75,-83,2005-08-08 09:34:06 ,Secure,A,36 (5180),54,req01
2005-08-08 09:34:06 ,00:05:9A:3D:ED:23,-87,2005-08-08 09:34:06 ,Secure,G,11 (2462),54,DD_Ca
2005-08-08 09:34:06 ,00:0D:28:88:D5:D3,-89,2005-08-08 09:34:06 ,Secure,B,1 (2412),11*,req01
2005-08-08 09:34:06 ,00:13:5F:0E:CB:20,-53,2005-08-08 09:34:06 ,open,G,1 (2412),54,req01-21
2005-08-08 09:34:06 ,00:0D:28:88:CA:B9,-89,2005-08-08 09:34:06 ,Secure,B,4 (2427),11*,req01
2005-08-08 09:34:06 ,1400RACK,00:0C:85:32:C7:25,-67,2005-08-08 09:34:06 ,open,A,161 (5805),5.
2005-08-08 09:34:06 ,350RACK,00:40:96:59:9D:4F,-70,2005-08-08 09:34:06 ,open,B,6 (2437),11*,
2005-08-08 09:34:06 ,aes-range,00:0B:85:52:65:C1,-72,2005-08-08 09:34:06 ,open,A,36 (5180),5.
2005-08-08 09:34:06 ,akita-ma-wpa2,00:13:5F:0E:59:BC,-88,2005-08-08 09:34:06 ,Secure,A,64 (5
2005-08-08 09:34:06 ,akita-ma-wpa2,00:0B:85:23:EA:D3,-86,2005-08-08 09:34:06 ,Secure,A,44 (5
2005-08-08 09:34:06 ,akita-ma1,00:13:5F:0E:59:BD,-88,2005-08-08 09:34:06 ,open,A,64 (5320),5.
2005-08-08 09:34:06 ,akita-ma1,00:0B:85:23:EA:D2,-86,2005-08-08 09:34:06 ,open,A,44 (5220),5.
2005-08-08 09:34:06 ,akita1,00:13:5F:0E:59:BF,-86,2005-08-08 09:34:06 ,Secure,A,64 (5320),54
2005-08-08 09:34:06 ,akita1,00:0B:85:23:EA:D0,-87,2005-08-08 09:34:06 ,Secure,A,44 (5220),54
2005-08-08 09:34:06 ,akita1,00:0B:85:04:73:FF,-76,2005-08-08 09:34:06 ,open,B,11 (2462),11*,
2005-08-08 09:34:06 ,akita1,00:0B:85:04:73:F0,-81,2005-08-08 09:34:06 ,open,A,149 (5745),54,
2005-08-08 09:34:06 ,akita1,00:0E:83:19:28:DF,-75,2005-08-08 09:34:06 ,open,A,36 (5180),54,,
2005-08-08 09:34:06 ,akita1,00:0E:83:19:28:D0,-88,2005-08-08 09:34:06 ,open,B,11 (2462),11*,
2005-08-08 09:34:06 ,akita_dd,00:0B:85:04:73:F3,-78,2005-08-08 09:34:06 ,open,A,149 (5745),5.
2005-08-08 09:34:06 ,akita_dd,00:0E:83:19:28:DC,-72,2005-08-08 09:34:06 ,open,A,36 (5180),54
2005-08-08 09:34:06 ,akita_eap,00:0B:85:04:73:F2,-78,2005-08-08 09:34:06 ,Secure,A,149 (5745
2005-08-08 09:34:06 ,akita_eap,00:0E:83:19:28:DD,-72,2005-08-08 09:34:06 ,Secure,A,36 (5180)

```

The log entries are time-stamped and appear in ASCII text. Each line typically represents a different access point.

**Note**

The log file can be viewed in Notepad or any other viewer. However, because it is written in a comma-separated values (CSV) format, it can also be opened by a spreadsheet or database program (such as Microsoft Excel). If the file is renamed with a .csv extension, Microsoft Excel would automatically place the values in separate columns.

**Note**

If the Accumulate button was depressed when you saved the AP scan log, two timestamps appear on each line. The timestamp in column one of the log file is the time when the log entry is made. The second timestamp, which appears only when the Accumulate button is depressed, is the Time of Day. This value indicates the date and time when the signal strength of each access point was at its maximum. Both timestamps appear in this format: 2005-07-20 16:13:09. The time is based on a 24-hour clock. For example, the first two lines in [Figure F-13](#) show only one timestamp while the remaining lines show both timestamps.

Step 2 Click the **X** in the upper right-hand corner of the window to close the window.

Deleting the AP Scan Log

Follow these steps to delete the AP scan log file.

- Step 1** Choose **Delete AP Scan Log** from the AP Scanning drop-down menu.



Note The Delete AP Scan Log menu option is disabled if the log file does not exist.

- Step 2** Click **Yes** when asked to confirm your decision.

Saving the AP Scan List

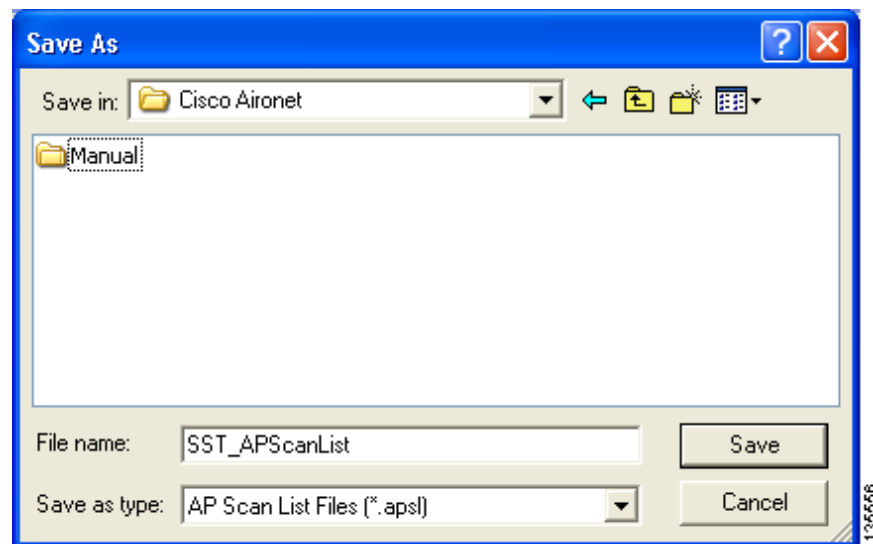
Follow these steps to save the current contents of the AP scan list to a file.

- Step 1** Choose **Save AP Scan List** from the AP Scanning drop-down menu. The Save As window appears (see [Figure F-14](#)).



Note The Save AP Scan List option is available only if the AP Scan List tab is selected.

Figure F-14 Site Survey Utility - Save As Window



- Step 2** From the Save in drop-down box, choose the location where you want to save the AP scan list file.



Note The initial default location is the directory where the site survey utility is installed. However, after you save the AP scan list file the first time, the default directory becomes the one that was last used to open or save the AP scan list file.

- Step 3** The default filename (SST_APScanList.apsl) appears in the File name box at the bottom of the window. If desired, type in a new filename.
- Step 4** Click **Save**.

Opening the AP Scan List

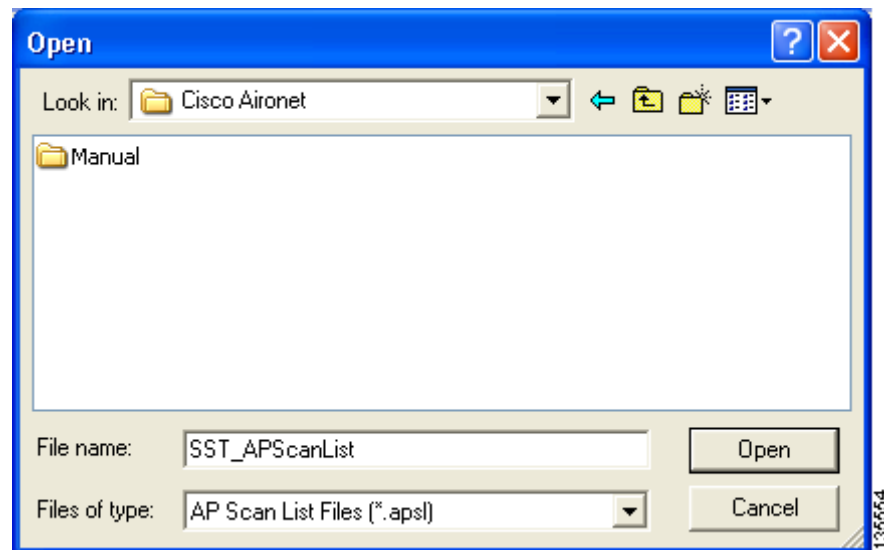
Follow these steps to open a saved AP scan list file.

- Step 1** Choose **Open AP Scan List** from the AP Scanning drop-down menu. The Open window appears (see [Figure F-15](#)).



Note The Open AP Scan List option is available only if the AP Scan List tab is selected.

Figure F-15 Site Survey Utility - Open Window



- Step 2** From the Look in drop-down box, find the AP scan list file.



Note The default directory is the one that was last used to open or save the AP scan list file.

- Step 3** Click the AP scan list file (SST_APScanList.apsl) so that it appears in the File name box at the bottom of the window.

- Step 4** Click **Open**. The contents of the AP scan list file appear in the AP scan list window.

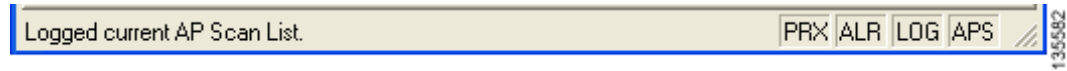


Note Updating of the AP scan list is paused automatically.

Viewing the Status Bar

The site survey utility's status bar runs along the bottom of the window (see [Figure F-16](#)).

Figure F-16 Site Survey Utility - Status Bar



It consists of three sections:

- A message area
- Four indicators
- A resize handle

Status Messages

The left side of the status bar displays status messages from the site survey utility. [Table F-4](#) lists and explains the messages that may appear.



Note

The messages disappear after a short period of time.

Table F-4 Site Survey Utility - Status Messages

Status Message	Description
"Added remarks to log file"	The comments you entered in the Add Comments to Log File window have been added to the threshold log file.
"The client adapter associated (<access point string as shown on main screen>)"	Your client adapter is associated to the specified access point.
"The client adapter disassociated"	Your client adapter has lost its connection to the access point.
"Connectivity test succeeded (<user's URL or IP address setting>)"	Your client adapter successfully accessed the specified URL or IP address after associating to an access point.
"Logged current AP Scan List"	The current contents of the AP scan list were logged to a file.
Threshold crossing notifications of the form: <status-parameter> (<value><units>) rose above or to the threshold value of (<value>)	<ul style="list-style-type: none"> • <status-parameter>—Can be any value that appears on the Associated AP Status tab • <value>—A number in the range appropriate for the parameter • <units>—The scientific units of the parameter <p>Note "Rose above or to" is replaced by "fell below or to" depending on the direction of crossing.</p>

Indicators

The right side of the status bar can show up to four indicators:

- PRX—The proximity beeper is enabled.
- ALR—Threshold alerts are enabled.
- LOG—Threshold logging is enabled.
- APS—Automatic AP scan list logging is enabled.

**Note**

The indicators do not appear when their corresponding features are disabled.

Resize Tab

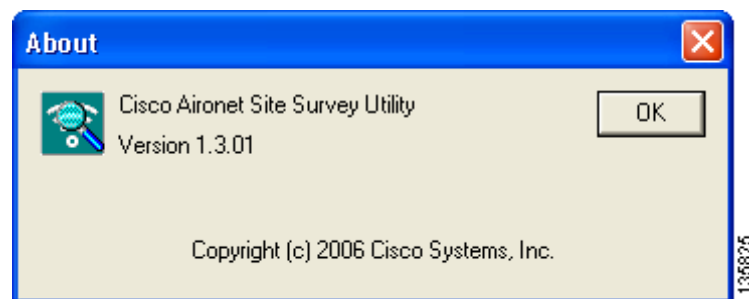
The resize tab in the right corner of the status bar can be used to change the size of the site survey utility's main window. Simply click the resize tab and drag it until the window reaches the desired size.



Finding the Version of the Site Survey Utility

To find the current version of the site survey utility, choose **About** from the Help drop-down menu. The About window appears (see [Figure F-17](#)).

Figure F-17 Site Survey Utility - About Window



Accessing Online Help

To access the site survey utility's online help, choose **Contents** from the Help drop-down menu.

Exiting the Site Survey Utility

To exit the site survey utility, perform one of the following:

- Click the **X** in the top right corner of the main window.
- Choose **Exit** from the Action drop-down menu.

Uninstalling the Site Survey Utility

Uninstalling the client adapter software also uninstalls the site survey utility. Refer to the [“Uninstalling the Client Adapter Software”](#) section on page 9-6 for instructions.



APPENDIX **G**

Using the Profile Migration Tool

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

The following topics are covered in this appendix:

- [Overview of the Profile Migration Tool, page G-2](#)
- [Rules Governing Profile Migration, page G-2](#)
- [Installing the Profile Migration Tool, page G-3](#)
- [Running the Profile Migration Tool, page G-4](#)
- [Command Line Options, page G-5](#)
- [Uninstalling the Profile Migration Tool, page G-7](#)

Overview of the Profile Migration Tool

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

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



Note

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

Rules Governing Profile Migration

These rules govern the operation of the profile migration tool:

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



Note

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

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

1.350 PCMCIA

2.350 PCI

3.350 mini PCI

4.CB20A

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

1.Default profiles

2.Auto-selectable profiles

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

4.Any remaining profiles

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

Installing the Profile Migration Tool

When you install the client adapter software, the Install Wizard automatically installs the profile migration tool, unless your system administrator used an administrative tool to prevent its installation. It is saved in the same directory as ADU.



Note

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

Running the Profile Migration Tool

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

**Note**

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

**Note**

The following conditions must be true before the profile migration tool can be run successfully:

- Your computer must contain the 350 and CB20A profiles that you want to migrate.
- ADU must be installed on the same computer but must not be running during the profile migration.
- A CB21AG or PI21AG client adapter must be inserted into your computer.

Step 1

Perform one of the following:

- If the profile migration tool runs automatically after the Install Wizard installs the client adapter software, go to [Step 4](#).
- If you want to manually activate the profile migration tool, open the Windows Command Prompt from **Start > Programs > Accessories**. Go to [Step 2](#).

Step 2

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

Step 3

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

**Note**

See the [“Command Line Options”](#) section below if you want to alter the behavior of the profile migration tool before running it.

Step 4

Restart your computer.

Step 5

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

Step 6

Re-enter the WEP keys in ADU.

Step 7

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

**Note**

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

Step 8

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

Command Line Options

These command line options can be used to alter the behavior of the profile migration tool. The correct format is **PMT -command**.



Note

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

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

Example: PMT -AllowReRun



Note

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

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

Example: PMT -CardOrder -pci350 -pcmcia350

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

Examples: PMT -CB20A

PMT -CardOrder -CB20A -pcmcia350

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

Examples: PMT -ConfigFile filename1.txt

PMT -ConfigFile filename1.txt filename2.txt



Note

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

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

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



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



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

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

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

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

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

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

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

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

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

Example: PMT -replace



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

Uninstalling the Profile Migration Tool

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



GLOSSARY

16-QAM	Quadrature amplitude modulation. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 24 and 36 Mbps.
64-QAM	Quadrature amplitude modulation. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 48 and 54 Mbps.
802.1X	Also called <i>802.1X for 802.11</i> . 802.1X is the standard for wireless LAN security, as defined by the Institute of Electrical and Electronics Engineers (IEEE). An access point that supports 802.1X and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.
802.11	The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs operating in the 2.4-GHz band.
802.11a	The IEEE standard that governs the deployment of 5-GHz OFDM systems. It specifies the implementation of the physical layer for wireless UNII bands (see UNII , UNII 1 , and UNII 2) and provides four channels per 100 MHz of bandwidth.
802.11b	The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps 2.4-GHz wireless LANs.
802.11g	The IEEE standard that specifies carrier sense media access control and physical layer specifications for 54-Mbps 2.4-GHz wireless LANs.
802.11i	The IEEE standard that defines security standards for wireless LANs. It specifies encryption, authentication, and key management strategies for wireless data and system security. It includes the TKIP and AES-CCMP data-confidentiality protocols.

A

access point	A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.
ad hoc network	A wireless network composed of stations without access points.
AES-CCMP	Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES-CCMP is the encryption protocol in the 802.11i standard.
alphanumeric	A set of characters that contains both letters and numbers.
associated	A station is configured properly to enable it to wirelessly communicate with an access point.

B

bandwidth	Specifies the amount of the frequency spectrum that is usable for data transfer. It identifies the maximum data rate that a signal can attain on the medium without encountering significant power loss.
BPSK	Binary phase shift keying. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 1 Mbps.
broadcast key rotation	A security feature for use with dynamic WEP keys. If your client adapter uses LEAP, EAP-FAST, EAP-TLS, or PEAP authentication and you enable this feature, the access point changes the dynamic broadcast WEP key that it provides at the interval you select.

C

CCK	Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.
CCKM	Cisco Centralized Key Management. Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point.
CKIP	Cisco Key Integrity Protocol. Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.
client adapter	A radio device that uses the services of an access point to communicate wirelessly with other devices on a local area network.
CSMA	Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.
CRC	Cyclic redundancy check. A method of checking for errors in a received packet.

D

data rates	The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).
dBi	A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain and the more acute the angle of coverage.
DHCP	Dynamic Host Configuration Protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.

DSSS Direct-sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

duplicate packets Packets that were received twice because an acknowledgement got lost and the sender retransmitted the packet.

E

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

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

Ethernet The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to enable computers to share a network and operates at 10, 100, or 1000 megabits per second (Mbps), depending on the physical layer used.

F

file server A repository for files so that a local area network can share files, mail, and programs.

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

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

G

gateway A device that connects two otherwise incompatible networks together.

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

H

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

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

I

IEEE	Institute of Electrical and Electronics Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.
infrastructure	The wired Ethernet network.
infrastructure device	A device (such as an access point, bridge, or base station) that connects client adapters to a wired LAN.
IP address	The Internet Protocol address of a station.
IP subnet mask	The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.
IPX	Internetwork Packet Exchange. The NetWare network layer protocol used for transferring data from servers to workstations.

L

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

M

MAC address	The Media Access Control (MAC) address is a unique serial number assigned to a networking device by the manufacturer.
MFP	<p>Management frame protection (MFP) is a feature that allows management frames to be transmitted more securely. When MFP is enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, which causes devices that are configured to detect MFP frames to report the discrepancy.</p> <p>The client adapter software configures MFP automatically based on how MFP is configured on the access point.</p>
MIC	Message integrity check. MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The client adapter's driver must support MIC functionality, and MIC must be enabled on the access point.
modulation	Any of several techniques for combining user information with a transmitter's carrier signal.
multicast packets	Packets transmitted to multiple stations.
multipath	The echoes created as a radio signal bounces off of physical objects.

O

- OFDM** Orthogonal frequency division multiplexing. A multicarrier modulation method for broadband wireless communications.
- overflow packets** Packets that were discarded because the access point had a temporary overload of packets to handle.

P

- PAC** Protected access credentials. Credentials that are either automatically or manually provisioned and used to perform mutual authentication with the RADIUS server during EAP-FAST authentication. PACs are created by the Cisco Secure ACS server and are identified by an ID. 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 file is manually copied from the server and imported onto the client device.
- packet** A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

Q

- QoS** Quality of service. QoS on wireless LANs provides prioritization of traffic from the access point over the WLAN based on traffic classification. The benefits of QoS become more obvious as the load on the wireless LAN increases, keeping the latency, jitter, and loss for selected traffic types within an acceptable range.
- QPSK** Quadruple phase shift keying. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 2 Mbps.

R

- radio channel** The frequency at which a radio operates.
- range** A linear measure of the distance that a transmitter can send a signal.
- receiver sensitivity** A measurement of the weakest signal a receiver can receive and still correctly translate it into data.
- RF** Radio frequency. A generic term for radio-based technology.
- roaming** A feature of some access points that enables users to move through a facility while maintaining an unbroken connection to the LAN.
- RTS threshold** The packet size at which an access point issues a request to send (RTS) before sending the packet.

S

- spread spectrum** A radio transmission technology that spreads data over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.
- SSID** Service set identifier. A unique identifier that stations must use to be able to communicate with an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

T

- TKIP** Temporal Key Integrity Protocol. Also referred to as *WEP key hashing*. A security feature that defends against an attack on WEP in which the intruder uses the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs.
- transmit power** The power level of radio transmission.

U

- unicast packets** Packets transmitted in point-to-point communication.
- UNII** Unlicensed National Information Infrastructure. An FCC regulatory domain for 5-GHz wireless devices. UNII bands are 100 MHz wide and divided into four channels when using 802.11a OFDM modulation.
- UNII 1** A UNII band dedicated to in-building wireless LAN applications. UNII 1 is located at 5.15 to 5.25 GHz and allows for a maximum transmit power of 40 mW (or 16 dBm) with an antenna up to 6 dBi. UNII 1 regulations require a nonremovable, integrated antenna.
- UNII 2** A UNII band dedicated to in-building wireless LAN applications. UNII 2 is located at 5.25 to 5.35 GHz and allows for a maximum transmit power of 200 mW (or 23 dBm) with an antenna up to 6 dBi. UNII 2 regulations allow for an auxiliary, user-installable antenna.
- UNII 3** A UNII band dedicated to wireless LAN applications. UNII 3 is located at 5.725 to 5.825 GHz and allows for a maximum transmit power of 1 Watt (or 30 dBm) with an antenna up to 6 dBi. UNII 3 regulations allow for an auxiliary, user-installable antenna.

V

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

A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment such as LAN switches that operate bridging protocols between them with a separate group for each VLAN.

W

WDS Wireless domain services (WDS). An access point providing WDS on your wireless LAN maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the WDS access point forwards the client's credentials to the new access point with the multicast key. Only two packets pass between the client and the new access point, greatly shortening the reassociation time.

WEP Wired equivalent privacy. An optional security mechanism defined within the 802.11 standard designed to protect your data as it is transmitted through your wireless network by encrypting it through the use of encryption keys.

WMM 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.

workstation A computing device with an installed client adapter.

WPA Wi-Fi Protected Access. A standards-based security solution from the Wi-Fi Alliance that provides data protection and access control for wireless LAN systems. It is compatible with the IEEE 802.11i standard but was implemented prior to the standard's ratification. WPA uses TKIP and MIC for data protection and 802.1X for authenticated key management.

WPA2 Wi-Fi Protected Access 2. The next generation of Wi-Fi security. It is the Wi-Fi Alliance's implementation of the ratified IEEE 802.11i standard. WPA2 uses AES-CCMP for data protection and 802.1X for authenticated key management.



INDEX

Numerics

- 802.11 Authentication Mode parameter [5-12](#)
- 802.11b preamble, status of [7-12](#)
- 802.11b Preamble parameter [5-9](#)
- 802.11 mode, in ASTU [8-5](#)
- 802.1X
 - authentication types
 - in ADU [5-15 to 5-18](#)
 - in Windows XP [E-3](#)
 - defined [5-15, E-3](#)
- 802.1x EAP Type parameter [5-29, 5-34, 5-45, 5-48, 5-52, 5-56](#)
- 802.1x option [5-29, 5-34, 5-45, 5-48, 5-52, 5-56](#)

A

- About Aironet Desktop Utility, ADU menu option [9-9](#)
- About window
 - in ADU [9-9](#)
 - in site survey utility [F-33](#)
- access point
 - CCX version supported [F-11, F-15](#)
 - channel, in site survey utility [F-6, F-11, F-14](#)
 - currently associated to [7-10, 8-11](#)
 - data rates, in site survey utility [F-14](#)
 - frequency, in site survey utility [F-6, F-11, F-14](#)
 - in wireless infrastructure [1-6](#)
 - IP address
 - in ADU [7-11](#)
 - in ASTU [8-11](#)
 - in site survey utility [F-6](#)
 - load, in site survey utility [F-11, F-15](#)
 - MAC address

- in ADU [7-11](#)
 - in site survey utility [F-6, F-10, F-14](#)
- maximum transmit data rate, in site survey utility [F-11](#)
- mismatches [7-16](#)
- model number [F-15](#)
- name
 - in ADU [7-10](#)
 - in ASTU [8-11](#)
 - in site survey utility [F-6, F-11, F-15](#)
- number of associations [F-15](#)
- problems associating to [10-10](#)
- radio [F-15](#)
- radio band, in site survey utility [F-11, F-14](#)
- role in wireless network [1-5](#)
- security settings [5-21 to 5-25](#)
- Access Point 1 through 4 parameters [5-13](#)
- access points
 - associating to in Windows XP [E-18](#)
 - number displayed in site survey utility [F-10](#)
 - preferred, setting [5-13](#)
 - reporting those that fail LEAP authentication [5-19 to 5-20, 5-25](#)
 - viewing an accumulation of [F-18](#)
 - viewing details in site survey utility [F-13 to F-16](#)
 - viewing status in site survey utility [F-5 to F-8](#)
- Accumulate button, in site survey utility [F-17, F-18](#)
- ACK frames [7-16](#)
- Action drop-down menu
 - in ADU [6-10, 9-8](#)
 - in site survey utility [F-3, F-20, F-34](#)
- Activate button [4-6, 4-10](#)
- Adapter Information
 - button [9-10](#)

- window [9-10](#)
- Add Comments to Log File window (site survey utility) [F-24](#)
- Add User Comment, site survey utility menu option [F-24](#)
- ad hoc mode, in site survey utility [F-12](#)
- ad hoc network
 - defined [E-6](#)
 - selecting in ADU [5-9](#)
 - selecting in Windows XP [E-7](#)
 - setting wireless mode [5-10](#)
 - wireless LAN configuration [1-5](#)
- ADU
 - See Aironet Desktop Utility (ADU)
- Advanced button [7-8](#)
- advanced parameters
 - described [5-2](#)
 - setting [5-6 to 5-13](#)
- Advanced Statistics
 - button [7-15](#)
 - window [7-15](#)
- Advanced Status window [7-8](#)
- AES, status of [7-7, 7-8](#)
- AES-CCMP, with WPA2 [5-18](#)
- AES option, in Windows XP [E-8](#)
- Aironet Desktop Utility (ADU)
 - accessing help [9-10](#)
 - described [1-4](#)
 - exiting [9-8](#)
 - feature comparison to Windows XP [3-17 to 3-18](#)
 - finding version [9-9](#)
 - icon [9-8](#)
 - opening [9-8](#)
 - Profile Management windows, overview [5-2](#)
 - selecting software to manage wireless device [7-4](#)
 - status and statistics tools
 - overview [7-2](#)
 - setting parameters [7-2 to 7-3](#)
 - using [7-5 to 7-17](#)
- Aironet Desktop Utility Help, ADU menu option [9-10](#)
- Aironet System Tray Utility (ASTU)
 - accessing help [8-5](#)
 - described [1-4](#)
 - exiting [8-6](#)
 - icon [8-2 to 8-3, 9-8](#)
 - opening [8-6](#)
 - overview [8-2](#)
 - pop-up menu [8-5 to 8-11](#)
 - selecting the active profile [8-8 to 8-9](#)
 - setting preferences [8-6 to 8-7](#)
 - specifying pop-up menu options [8-7](#)
 - Tool Tip window [8-3 to 8-5](#)
 - using [8-1 to 8-11](#)
 - using to open ADU [8-6](#)
 - using to open troubleshooting utility [8-6](#)
- Aironet System Tray Utility Preferences window [8-6](#)
- Allow Association to Mixed Cells parameter
 - setting with EAP-FAST [5-42 to 5-43](#)
 - setting with EAP-TLS [5-47](#)
 - setting with LEAP [5-32](#)
 - setting with PEAP (EAP-GTC) [5-51](#)
 - setting with PEAP (EAP-MSCHAP V2) [5-55](#)
 - setting with static WEP [5-27](#)
- Allow Automatic PAC Provisioning for this Profile parameter [5-42](#)
- AllowReRun, profile migration tool command line option [G-5](#)
- ALR, in site survey utility [F-33](#)
- Always Resume the Secure Session parameter
 - for LEAP [5-31](#)
 - for PEAP (EAP-GTC) [5-50](#)
- antenna
 - assembling [3-5 to 3-6](#)
 - described [1-3](#)
 - gains
 - IEEE 802.11a [D-4](#)
 - IEEE 802.11b [D-4](#)
 - IEEE 802.11g [D-5](#)
 - mounting [3-6 to 3-8](#)

- placement [F-2](#)
 - rotating [3-8](#)
 - specifications [A-5](#)
 - antenna base, mounting [3-6 to 3-8](#)
 - AP detailed information parameters (site survey utility) [F-14 to F-16](#)
 - AP Detailed Information window (site survey utility) [F-13](#)
 - APS, in site survey utility [F-33](#)
 - AP scan list, in site survey utility
 - displayed [F-9](#)
 - opening [F-31](#)
 - parameters [F-10 to F-12](#)
 - pausing [F-13](#)
 - saving [F-30 to F-31](#)
 - viewing [F-9 to F-12](#)
 - AP Scan List Logging Configuration window (site survey utility) [F-26](#)
 - AP Scan List tab (site survey utility), using [F-8 to F-18](#)
 - AP scan log, in site survey utility
 - deleting [F-30](#)
 - viewing [F-28 to F-29](#)
 - AP scan log file, in site survey utility
 - displayed [F-17, F-29](#)
 - generating [F-16 to F-17](#)
 - name and location [F-27](#)
 - AP scan logging, in site survey utility
 - configuring [F-26 to F-27](#)
 - disabling [F-28](#)
 - enabling [F-28](#)
 - AP scanning, using in site survey utility [F-26 to F-31](#)
 - associated AP status parameters (site survey utility) [F-6 to F-8](#)
 - Associated AP Status tab (site survey utility)
 - units as a percentage [F-5](#)
 - units in dBm [F-5](#)
 - using [F-4 to F-8](#)
 - association
 - rejections [7-17](#)
 - time-outs [7-17](#)
 - associations, in site survey utility [F-15](#)
 - ASTU
 - See Aironet System Tray Utility (ASTU)
 - ATIM Window, in site survey utility [F-14](#)
 - authentication
 - process [5-17, E-4](#)
 - rejections [7-17](#)
 - time-outs [7-17](#)
 - type
 - setting [5-12](#)
 - status of [7-9](#)
 - Authentication Timeout Value parameter
 - for LEAP [5-32](#)
 - Automatically Prompt for User Name and Password option
 - for EAP-FAST [5-38](#)
 - for LEAP [5-31](#)
 - auto profile selection
 - enabling [4-10](#)
 - including a profile in [4-8 to 4-9](#)
 - prioritizing profiles [4-9](#)
 - removing a profile from [4-9](#)
 - restrictions [4-9](#)
 - status of [8-10](#)
 - using [8-8](#)
 - Auto Profile Selection Management window [4-8](#)
 - Auto Select Profiles parameter [4-10](#)
 - Available Infrastructure and Ad Hoc Networks window [4-4](#)
-
- ## B
- beacon period, in site survey utility [F-14](#)
 - beacons received
 - in ADU [7-16](#)
 - in site survey utility [F-7](#)
 - broadcast key rotation
 - described [5-21](#)
 - setting on client and access point [5-25](#)
 - broadcast packets

- number received [7-15](#)
- number transmitted [7-15](#)
- broadcast SSIDs [5-4, E-6](#)
- BSS Aging Interval parameter (Windows Control Panel) [5-64](#)
- bytes
 - number received [7-15](#)
 - number transmitted [7-15](#)

C

- call admission control (CAC), in site survey utility [F-12](#)
- CAM
 - See Constantly Awake Mode (CAM)
- Canadian compliance statement [C-3](#)
- card name [9-10](#)
- CardOrder, profile migration tool command line option [G-5](#)
- CB20A, profile migration tool command line option [G-5](#)
- CCKM fast secure roaming
 - described [5-19](#)
 - enabling with EAP-FAST [5-34](#)
 - enabling with EAP-TLS [5-45](#)
 - enabling with LEAP [5-29](#)
 - enabling with PEAP (EAP-GTC) [5-48](#)
 - enabling with PEAP (EAP-MSCHAP V2) [5-52](#)
 - setting on client and access point [5-25](#)
- CCX, version supported by access point [F-11, F-15](#)
- certificates, required for EAP-TLS and PEAP authentication [5-44](#)
- channel of access point
 - in ADU [4-6](#)
 - in site survey utility [F-6, F-11, F-14](#)
- channel of client adapter [7-7, 7-12](#)
- Channel parameter [5-11](#)
- channels, supported by regulatory domains
 - IEEE 802.11a [D-2](#)
 - IEEE 802.11b/g [D-3](#)

- channel set, for which client adapter is configured [7-13](#)
- Choose Destination Location window (Install Wizard) [3-14](#)
- Cisco Aironet 802.11a/b/g Wireless Adapter Properties window [5-63](#)
- Cisco Aironet Desktop Utility (Diagnostics) window [7-14](#)
- Cisco Aironet Desktop Utility (Profile Management) window [4-2](#)
- Cisco Aironet Installation Program window (Install Wizard) [3-11](#)
- Cisco Centralized Key Management (CCKM)
 - See CCKM fast secure roaming
- Cisco extended capabilities (CEC), in site survey utility [F-12](#)
- Cisco Key Integrity Protocol (CKIP)
 - statistics [7-17](#)
 - status of [7-7](#)
 - with LEAP [5-15](#)
- client adapter
 - association status in site survey utility [F-4](#)
 - selecting in site survey utility [F-3 to F-4](#)
- client name [9-10](#)
- Client Name parameter [5-4](#)
- client utilities
 - See Aironet Desktop Utility (ADU) and Aironet System Tray Utility (ASTU)
- command line options, for profile migration tool [G-5 to G-6](#)
- ConfigFile, profile migration tool command line option [G-5](#)
- Configuration Settings window
 - for PEAP (EAP-MSCHAP V2) [5-54](#)
- Configure AP Scan Logging, site survey utility menu option [F-26](#)
- Configure Scan List Columns window [4-5](#)
- Configure Thresholds, site survey utility menu option [F-20](#)
- configuring AP scan logging in site survey utility [F-26 to F-27](#)
- configuring client adapter
 - deciding between ADU and Windows XP [3-17 to 3-18](#)
 - in ADU [5-1 to 5-58](#)

- in Windows XP [E-5 to E-10](#)
- configuring scan list columns [4-5](#)
- configuring threshold values in site survey utility [F-20 to F-23](#)
- connection status [8-4, 8-10](#)
- Connection Status window (ASTU) [8-9](#)
- Constantly Awake Mode (CAM) [5-8](#)
- Contents, site survey utility menu option [F-33](#)
- CRC errors [7-16](#)
- CTS frames [7-16](#)
- Current Status window [7-5](#)
- CWmax, in site survey utility [F-15](#)
- CWmin, in site survey utility [F-15](#)

D

- Data Display parameter [7-3, 7-14](#)
- data encryption
 - in ADU [7-8](#)
 - in site survey utility [F-11, F-14](#)
- data frames [7-16](#)
- data rate
 - in ADU [7-6](#)
 - mismatches [7-16](#)
 - of access point, in site survey utility [F-14](#)
 - setting [5-10](#)
 - specifications [A-3](#)
 - when performing a site survey [F-2](#)
- DC mode
 - See diagnostic channel mode
- debugging information, in site survey utility [F-14](#)
- declarations of conformity
 - European community, Switzerland, Norway, Iceland, and Liechtenstein [C-3 to C-7](#)
 - FCC [C-2](#)
 - RF exposure [C-7](#)
- default values, using [5-2](#)
- Define Certificate window [5-46](#)
- Define PEAP (EAP-GTC) Configuration window [5-49](#)

- Define PEAP (EAP-MSCHAP V2) Configuration window [5-53](#)
- Define Pre-Shared Keys window [5-26](#)
- Define WPA/WPA2 Pre-Shared Key window [5-28](#)
- Delete AP Scan Log, site survey utility menu option [F-30](#)
- Delete Threshold Log, site survey utility menu option [F-25](#)
- diagnosing client adapter operation [10-4 to 10-6](#)
- diagnostic channel mode [10-11 to 10-17](#)
- Diagnostics window [7-14](#)
- Disable Radio
 - ADU menu option [9-11](#)
 - ASTU menu option [8-7](#)
- Display in Percent parameter (site survey utility) [F-4](#)
- Display Settings
 - ADU menu option [7-2](#)
 - window [7-2](#)
- display units, specifying in site survey utility [F-4](#)
- diversity antenna [1-3](#)
- domain name
 - including in Windows login
 - for EAP-FAST [5-38](#)
 - for LEAP [5-32](#)
 - specifying for saved user name and password
 - for EAP-FAST [5-38](#)
 - for LEAP [5-31](#)
- driver
 - current version [9-9, 9-10](#)
 - date [9-10](#)
 - described [1-4](#)
 - manually installing or upgrading [9-6](#)
 - name [9-10](#)
- DSConfig, in site survey utility [F-15](#)
- duplicate frames, number received [7-16](#)
- dynamic WEP keys, overview [5-15 to 5-18, E-3 to E-4](#)

E

- EAP authentication

- described [E-4](#)
- overview [5-15 to 5-18, 6-2, E-3 to E-4](#)
- restarting [6-16](#)
- using [6-1 to 6-16](#)

EAP-Cisco Wireless

- See LEAP authentication

EAP-FAST authentication

- authenticating after a reboot/logon
 - with automatically prompted login [6-7](#)
 - with saved username and password [6-13](#)
 - with Windows username and password [6-4](#)
- authenticating after a reboot/logon/card insertion, with manually prompted login [6-10 to 6-12](#)
- authenticating after EAP-FAST password expires
 - with automatically prompted login [6-8](#)
 - with manually prompted login [6-12](#)
 - with saved username and password [6-14](#)
 - with Windows username and password [6-5](#)
- authenticating after profile activation, with manually prompted login [6-9 to 6-10](#)
- authenticating after profile activation/card insertion
 - with automatically prompted login [6-6](#)
 - with saved username and password [6-13](#)
 - with Windows username and password [6-4](#)
- described [5-16 to 5-18](#)
- disabling [5-58](#)
- enabling [5-34](#)
- overview [6-2 to 6-3](#)
- RADIUS servers supported [5-16](#)
- requirements [5-34](#)
- setting on client and access point [5-23](#)
- stages of [6-3](#)
- user databases supported [5-17](#)

EAP-FAST Authentication Status window

- displayed [6-2](#)
- minimizing [6-3](#)

EAP-FAST option [5-34](#)

EAP-FAST Settings window [5-35, 5-36](#)

EAP MSCHAPv2 Properties window - Windows XP [E-15](#)

EAP-TLS authentication

- authenticating after profile activation/card insertion/reboot/logon [6-14](#)
- described [5-17 to 5-18, E-3, E-4](#)
- disabling [5-58](#)
- enabling
 - in ADU [5-44 to 5-47](#)
 - in Windows XP [E-10 to E-12](#)

RADIUS servers supported [5-17, E-3](#)

- requirements [5-44](#)
- setting on client and access point [5-23](#)

EAP-TLS machine authentication with machine credentials

- requirements [5-44](#)
- setting [5-42, 5-46](#)

EAP-TLS option [5-45](#)

EIRP, maximum supported by regulatory domains

- IEEE 802.11a [D-4](#)
- IEEE 802.11b [D-4](#)
- IEEE 802.11g [D-5](#)

Enable AP Scan Logging, site survey utility menu option [F-28](#)

Enable Expert Mode for AP Detailed Information parameter (site survey utility) [F-14](#)

Enable Radio

- ADU menu option [9-11](#)
- ASTU menu option [8-7](#)

Enable Threshold Alerts, site survey utility menu option [F-23](#)

Enable Threshold Logging, site survey utility menu option [F-23](#)

Enable Tray Icon, ADU menu option [8-6](#)

encryption errors [7-16](#)

Enter Password window [5-41](#)

Enter Wireless Network Password window [6-6, 6-7, 6-9, 6-11](#)

error messages [10-18 to 10-30](#)

errors

- CRC [7-16](#)
- encryption [7-16](#)
- MIC [7-17](#)

Exit menu option
 in ADU [9-8](#)
 in ASTU [8-6, 9-8](#)
 in site survey utility [F-34](#)

Export button [4-13](#)

Export Profile window [4-13](#)

F

Fast PSP [5-8](#)

FCC

 declaration of conformity statement [C-2](#)

 safety compliance statement [2-2](#)

finding domain controller timeout value

 for EAP-FAST [5-43](#)

 for LEAP [5-32](#)

Fit Columns parameter (site survey utility) [F-9](#)

frames

 ACK [7-16](#)

 CTS [7-16](#)

 duplicate [7-16](#)

 number dropped [7-16](#)

 number received successfully [7-16](#)

 number received with errors [7-16](#)

 number retried [7-16](#)

 number transmitted successfully [7-16](#)

 RTS [7-16](#)

frequencies, supported by regulatory domains

 IEEE 802.11a [D-2](#)

 IEEE 802.11b/g [D-3](#)

frequency

 in ADU [7-6, 7-13](#)

 of access point, in site survey utility [F-11, F-14](#)

 setting [5-10](#)

G

general parameters

 described [5-2](#)

 setting [5-3 to 5-5](#)

Generic Token Card Properties window - Windows XP [E-17](#)

global PACs [5-16, 5-41](#)

Group Policy, described [3-21](#)

Group Policy Delay parameter

 installing hot fix for [3-21 to 3-22](#)

 setting with EAP-FAST [5-44](#)

 setting with EAP-TLS [5-47](#)

 setting with LEAP [5-33](#)

 setting with PEAP (EAP-GTC) [5-51](#)

 setting with PEAP (EAP-MSCHAP V2) [5-55](#)

 setting with PEAP (EAP-MSCHAP V2) machine authentication with machine credentials [5-56](#)

 setting with WPA/WPA2 passphrase [5-28](#)

H

hardware components of client adapter [1-3](#)

help

 in ADU [9-10](#)

 in ASTU [8-5](#)

 in site survey utility [F-33](#)

hops, in site survey utility [F-15](#)

Host Based EAP option [5-56](#)

host devices [2-4](#)

Hysteresis parameter (site survey utility) [F-23](#)

I

I/O range [10-8](#)

Import button [4-12](#)

Import EAP-FAST PAC File window [5-40](#)

Import Profile window [4-12](#)

Include Windows Logon Domain with User Name parameter

 for EAP-FAST [5-38](#)

 for LEAP [5-32](#)

- indicators, in site survey utility [F-33](#)
 - information about client adapter [9-10](#)
 - infrastructure device, defined [1-2](#)
 - infrastructure mode, in site survey utility [F-14](#)
 - infrastructure network
 - selecting in ADU [5-9](#)
 - wireless LAN configuration [1-6](#)
 - inserting client adapter [3-2 to 3-8](#)
 - Install Cisco Aironet Site Survey Utility window (Install Wizard) [3-13](#)
 - installing
 - client adapter software [3-9 to 3-20](#)
 - profile migration tool [G-3](#)
 - Install Wizard file
 - described [1-4](#)
 - installing [3-9 to 3-20](#)
 - name [3-9](#)
 - removing [9-7](#)
 - interference [2-5, 3-6](#)
 - interrupt request (IRQ) [10-8](#)
 - introduction to client adapters [1-2](#)
 - IP address
 - of access point
 - in ADU [7-11](#)
 - in ASTU [8-11](#)
 - in site survey utility [F-6](#)
 - of client adapter [7-7, 8-5, 8-11](#)
-
- ## J
-
- Japan, guidelines for operating client adapters [C-7](#)
-
- ## K
-
- key icon [4-6](#)
-
- ## L
-
- LEAP authentication
 - authenticating after a reboot/logon
 - with automatically prompted login [6-7](#)
 - with saved username and password [6-13](#)
 - with Windows username and password [6-4](#)
 - authenticating after a reboot/logon/card insertion, with manually prompted login [6-10 to 6-12](#)
 - authenticating after profile activation, with manually prompted login [6-9 to 6-10](#)
 - authenticating after profile activation/card insertion
 - with automatically prompted login [6-6](#)
 - with saved username and password [6-13](#)
 - with Windows username and password [6-4](#)
 - described [5-15 to 5-18](#)
 - disabling [5-58](#)
 - enabling [5-29 to 5-33](#)
 - overview [6-2 to 6-3](#)
 - RADIUS servers supported [5-15](#)
 - requirements [5-29](#)
 - setting on client and access point [5-21](#)
 - stages of [6-3](#)
 - timeout value [4-10, 8-8](#)
 - using with login scripts [4-10](#)
 - LEAP Authentication Status window
 - displayed [6-2](#)
 - minimizing [6-3](#)
 - LEAP option [5-29](#)
 - LEAP Settings window [5-30](#)
 - LEDs
 - described [1-3](#)
 - interpreting [10-2](#)
 - link quality
 - in ASTU [8-5, 8-11](#)
 - in site survey utility [F-8](#)
 - link speed
 - in ASTU [8-5](#)
 - in site survey utility [F-8](#)
 - List Installed Devices Even If Not Present in System parameter (site survey utility) [F-4](#)
 - load, in site survey utility [F-11, F-15](#)
 - Locked Profile parameter [5-14](#)

- locked profiles [5-14](#)
- LOG, in site survey utility [F-33](#)
- log file, generating in site survey utility [F-17](#)
- logfile, profile migration tool command line option [G-6](#)
- login scripts, using with LEAP [4-10, 8-9](#)
- Log Snapshot button, in site survey utility [F-16](#)
- long radio headers
 - status of [7-12](#)
 - using [5-9](#)

M

- MAC address
 - of access point
 - in site survey utility [F-6, F-10, F-14](#)
 - specifying [5-13](#)
 - viewing [7-11](#)
 - of client adapter [9-10](#)
- machine authentication with machine credentials
 - using EAP-TLS [5-42, 5-46](#)
 - using PEAP (EAP-MSCHAP V2) [5-55 to 5-57](#)
- machine authentication with user credentials
 - using PEAP (EAP-GTC) [5-49](#)
 - using PEAP (EAP-MSCHAP V2) [5-53](#)
- management frame protection
 - described [7-10](#)
- Manual Login
 - ADU menu option [5-31, 6-10](#)
 - ASTU menu option [8-8](#)
- Manually Prompt for User Name and Password option
 - for EAP-FAST [5-38](#)
 - for LEAP [5-31](#)
- Max PSP [5-8](#)
- message integrity check (MIC)
 - described [5-20, 7-9](#)
 - errors [7-17](#)
 - setting on client and access point [5-25](#)
 - statistics [7-17](#)
 - status of [7-9](#)

- types of [7-9](#)
- with WPA [5-18](#)
- MFP
 - See management frame protection
- Michael MIC, status of [7-9](#)
- microcellular network [1-6](#)
- Microsoft 802.1X supplicant, disabling [10-7](#)
- Microsoft hot fix
 - installing [3-21 to 3-22](#)
 - required for Group Policy Delay parameter [3-21](#)
- Microsoft Wireless Configuration Manager
 - disabling [10-7](#)
 - enabling in Install Wizard [3-17](#)
 - role in switching between host-based EAP and non-host-based EAP profiles [5-56, 5-57](#)
- miniPCI, profile migration tool command line option [G-6](#)
- MMH MIC
 - status of [7-9](#)
 - with LEAP [5-15](#)
- Modify button [4-11, 5-3](#)
- multicast packets
 - number received [7-15](#)
 - number transmitted [7-15](#)

N

- network
 - configurations [1-5 to 1-6](#)
 - prioritizing connections [10-11](#)
 - problems connecting to [10-10](#)
 - type, current [4-3, 7-6](#)
- network name
 - in ADU [5-4, 7-8](#)
 - in ASTU [8-3](#)
 - in site survey utility [F-10, F-14](#)
- Network Type parameter [5-9](#)
- New button [4-4, 5-3](#)
- noise level

in ADU [7-12](#)

in site survey utility [F-7](#)

No Network Connection Unless User Is Logged In
parameter

for EAP-FAST [5-42, 6-13](#)

for LEAP [5-32, 6-13](#)

O

online help

for ADU [9-10](#)

for ASTU [8-5](#)

for site survey utility [F-33](#)

Open Aironet Desktop Utility, ASTU menu option [8-6, 9-8](#)

Open AP Scan List, site survey utility menu option [F-31](#)

open authentication

setting [5-12, E-8](#)

status of [7-9](#)

Open window (site survey utility) [F-31](#)

operating systems supported [2-4, 3-9](#)

Options, site survey utility menu option [F-14, F-18](#)

Options window (site survey utility) [F-19](#)

Order Profiles button [4-8](#)

P

PAC authority, selecting [5-39, 5-41](#)

package contents [2-3](#)

packets

broadcast [7-15](#)

multicast [7-15](#)

unicast [7-15](#)

PAC provisioning

automatic [5-42](#)

manual [5-42](#)

PACs

copying from private store to global store [5-42](#)

described [5-16, 5-42](#)

entering password for [5-41](#)

importing [5-40 to 5-41](#)

rules for storage [5-16](#)

types of [5-16](#)

PAC stores

selecting [5-41](#)

types of [5-41](#)

Pause List Update button, in site survey utility [F-13](#)

PC-Cardbus card

antenna [1-3](#)

described [1-2](#)

inserting [3-2](#)

profiles tied to slot [4-7](#)

removing [9-2](#)

-pci350, profile migration tool command line option [G-6](#)

PCI card

antenna

assembling [3-5 to 3-6](#)

described [1-3](#)

mounting [3-6 to 3-8](#)

rotating [3-8](#)

changing bracket [3-3](#)

described [1-2](#)

inserting [3-3 to 3-8](#)

removing [9-2](#)

-pcmcia350, profile migration tool command line
option [G-6](#)

PEAP (EAP-GTC) authentication

authenticating after profile activation/card
insertion/reboot/logon [6-15](#)

described [5-17, E-3, E-4](#)

disabling [5-58](#)

enabling

in ADU [5-48 to 5-51](#)

in Windows XP [E-13 to E-14, E-16 to E-18](#)

RADIUS servers supported [5-17, E-3](#)

requirements [5-44](#)

setting on client and access point [5-24](#)

user databases supported [5-17](#)

PEAP (EAP-GTC) machine authentication with user
credentials, setting [5-49](#)

- PEAP (EAP-GTC) option [5-48](#)
- PEAP (EAP-MSCHAP V2) authentication
 - authenticating after profile activation/card insertion/reboot/login [6-16](#)
 - Certificate option [5-53](#)
 - described [5-17 to 5-18](#), [E-3](#), [E-4](#)
 - disabling [5-58](#)
 - enabling
 - in ADU [5-52 to 5-55](#)
 - in Windows XP [E-13 to E-15](#)
 - RADIUS servers supported [5-17](#), [E-3](#)
 - requirements [5-44](#)
 - setting on client and access point [5-24](#)
 - User Name and Password option [5-53](#)
- PEAP (EAP-MSCHAP V2) machine authentication with machine credentials, setting [5-55 to 5-57](#)
- PEAP (EAP-MSCHAP V2) machine authentication with user credentials, setting [5-53](#)
- PEAP (EAP-MSCHAP V2) option [5-52](#)
- PEAP Properties window - Windows XP [E-16](#)
- peer-to-peer network [1-5](#), [5-9](#)
- physical specifications [A-2](#)
- Please Change Password window [6-5](#), [6-8](#), [6-12](#), [6-14](#)
- power level, current [7-11](#)
- power levels, available [7-11](#)
- power save mode, currently being used [7-11](#)
- Power Save Mode parameter [5-8](#)
- power specifications [A-6](#)
- Preferences, ASTU menu option [8-6](#)
- Preferred Access Points window [5-13](#)
- Preparing Setup window (Install Wizard) [3-10](#), [9-3](#)
- Pre-Shared Key (Static WEP) option [5-26](#)
- Previous Installation Detected window (Install Wizard) [9-4](#)
- private PACs [5-16](#), [5-41](#)
- product model numbers [1-2](#)
- profile
 - active [4-10](#), [8-3](#), [8-10](#)
 - default [4-2](#)
 - described [4-2](#)
 - locked [5-14](#)
- Profile Management (Advanced) window [5-6](#)
- Profile Management (General) window [4-7](#)
- Profile Management (Security) window [5-14](#)
- Profile Management window [4-2](#)
- Profile Management windows, parameters missing [10-17](#)
- profile manager
 - auto profile selection feature [4-8 to 4-9](#)
 - creating a new profile [4-4 to 4-7](#)
 - deleting a profile [4-11](#)
 - editing a profile [4-11](#)
 - exporting a profile [4-12 to 4-13](#)
 - importing a profile [4-12](#)
 - opening [4-2 to 4-3](#)
 - parameters missing [4-3](#), [10-17](#)
 - selecting the active profile [4-10](#)
- profile migration tool
 - command line options [G-5 to G-6](#)
 - compatibility with Install Wizard [G-2](#)
 - entering multiple commands [G-5](#)
 - finding version number [G-2](#)
 - installing [G-3](#)
 - name and location of generated log file [G-4](#), [G-6](#)
 - name mangling [G-2](#)
 - overview [G-2](#)
 - rules governing profile migration [G-2 to G-3](#)
 - running [G-4](#)
 - running multiple times [G-5](#)
 - uninstalling [G-7](#)
 - using [G-1 to G-7](#)
 - viewing generated log file [G-4](#)
- Profile Name parameter [5-4](#)
- profiles, losing [9-6](#)
- profiles submenu (ASTU) [8-8](#)
- Protected EAP
 - See PEAP (EAP-GTC) authentication and PEAP (EAP-MSCHAP V2) authentication
- Protected EAP Properties window - Windows XP [E-14](#)
- protocol driver, finding version [9-9](#)

proximity beeper

- configuring [F-18 to F-19](#)
- disabling [F-20](#)
- enabling [F-20](#)
- inverting the tone of [F-19](#)
- using [F-18 to F-20](#)

PRX, in site survey utility [F-33](#)

Q

QoS

- See quality of service

QoS Packet Scheduler

- enabling on Windows 2000 [5-59 to 5-61](#)
- enabling on Windows XP [5-62](#)

quality of service (QoS)

- described [5-59](#)
- in site survey utility [F-12](#)
- status of [7-10](#)

R

radio

- described [1-3](#)
- enabling or disabling [8-7, 9-11](#)
- specifications [A-3 to A-5](#)

radio band of access point, in site survey utility [F-11, F-14](#)

RADIUS servers

- additional information [5-18, E-4](#)
- defined [5-15, E-3](#)
- supported [5-15 to 5-18, E-3](#)

range [5-7](#)

Reauthenticate menu option

- in ADU [6-16](#)
- in ASTU [6-16, 8-8](#)

receive rate [7-12, 8-11](#)

receive statistics [7-15, 7-16 to 7-17](#)

Refresh button [4-4](#)

Refresh Interval parameter [7-3, 7-14](#)

regulatory

- domains
 - IEEE 802.11a [D-2](#)
 - IEEE 802.11b/g [D-3](#)
- information [C-2 to C-9](#)
- specifications [A-6](#)

Remove button [4-11](#)

removing client adapter [9-2](#)

-replace, profile migration tool command line option [G-6](#)

resize tab, on site survey utility [F-33](#)

resource conflicts, resolving

- in Windows 2000 [10-9](#)
- in Windows XP [10-9 to 10-10](#)

Restrict Time Finding Domain Controller parameter

- setting with EAP-FAST [5-43](#)
- setting with LEAP [5-32 to 5-33](#)

RF obstructions [2-5, 3-6, F-2](#)

RM-APScan, in site survey utility [F-12, F-16](#)

RM-CliWlk, in site survey utility [F-12, F-16](#)

RM-Normal, in site survey utility [F-12, F-16](#)

roaming

- described [1-6](#)
- parameters, setting in the Windows Control Panel [5-63 to 5-64](#)
- threshold [5-64](#)

RSSI, in site survey utility [F-10, F-14](#)

RTS frames [7-16](#)

Run Test button, in troubleshooting utility [10-5](#)

S

safety

- information [2-2 to 2-3](#)
- specifications [A-6](#)

Save AP Scan List, site survey utility menu option [F-30](#)

Save As window (site survey utility) [F-30](#)

saved username and password

- described

- for LEAP [5-30](#)
- entering
 - for EAP-FAST [5-38](#)
 - for LEAP [5-31](#)
- Save Report, in troubleshooting utility
 - button [10-7](#)
 - window [10-7, 10-12, 10-13, 10-14, 10-15, 10-16, 10-17](#)
- Scan button [4-4](#)
- scan list columns, configuring [4-5](#)
- Scan List Settings, ADU menu option [4-4](#)
- Scan Valid Interval parameter (Windows Control Panel) [5-64](#)
- seamless roaming [1-6](#)
- security features
 - overview [5-14 to 5-21](#)
 - synchronizing [5-21 to 5-25](#)
- security mode [4-3](#)
- security parameters
 - described [5-2](#)
 - setting [5-14 to 5-57](#)
- Select Adapter
 - site survey utility menu option [F-3](#)
 - window (site survey utility) [F-3](#)
- Select Client Software
 - ADU menu option [7-4](#)
 - window [7-4](#)
- Select Network Component Type window [5-61](#)
- Select Network Service window [5-61](#)
- Select Profile, ASTU menu option [8-8 to 8-9](#)
- sensitivity [A-4](#)
- serial number of client adapter [9-10](#)
- server-based authentication, currently being used [7-8](#)
- Setup Status window (Install Wizard) [9-5](#)
- Setup Type window (Install Wizard) [3-12](#)
- shared authentication
 - setting [5-12, E-8](#)
 - status of [7-9](#)
- short radio headers
 - status of [7-12](#)
- using [5-9](#)
- Show Connection Status, ASTU menu option [8-9](#)
- signal quality
 - in ADU [7-12](#)
 - in site survey utility [F-7](#)
- signal strength
 - as a percentage [7-3](#)
 - in ADU [7-7, 7-11](#)
 - in ASTU [8-5](#)
 - in dBm [7-3](#)
- Signal Strength Display Units parameter [7-3](#)
- signal-to-noise ratio (SNR)
 - as a percentage [7-3](#)
 - in ADU [4-6](#)
 - in dB [7-3](#)
 - in site survey utility [F-8](#)
- site requirements
 - for client devices [2-5](#)
 - for infrastructure devices [2-5](#)
- site survey
 - environmental considerations [F-2](#)
 - guidelines [F-2](#)
 - performing [F-1 to F-34](#)
- site survey utility
 - About window [F-33](#)
 - accessing help [F-33](#)
 - Accumulate button [F-17, F-18](#)
 - AP detailed information parameters [F-14 to F-16](#)
 - AP Detailed Information window [F-13](#)
 - AP scan list
 - parameters [F-10 to F-12](#)
 - pausing [F-13](#)
 - viewing [F-9 to F-12](#)
 - associated AP status parameters [F-6 to F-8](#)
 - client adapter association status [F-4](#)
 - configuring
 - AP scan logging [F-26 to F-27](#)
 - proximity beeper [F-18 to F-19](#)
 - threshold values [F-20 to F-23](#)

- debugging information [F-14](#)
- deleting
 - AP scan log [F-30](#)
 - threshold log file [F-25](#)
- disabling
 - AP scan logging [F-28](#)
 - proximity beeper [F-20](#)
 - threshold triggers [F-23](#)
- enabling
 - AP scan logging [F-28](#)
 - proximity beeper [F-20](#)
 - threshold triggers [F-23](#)
- exiting [F-34](#)
- finding version of [F-33](#)
- Fit Columns parameter [F-9](#)
- generating AP scan log file [F-16 to F-17](#)
- indicators [F-33](#)
- inverting tone of proximity beeper [F-19](#)
- log file [F-17](#)
- Log Snapshot button [F-16](#)
- opening [F-3](#)
- opening AP scan list [F-31](#)
- overview [F-2](#)
- Pause List Update button [F-13](#)
- resize tab [F-33](#)
- resizing columns [F-9](#)
- saving AP scan list [F-30 to F-31](#)
- selecting client adapter [F-3 to F-4](#)
- specifying
 - directory [3-13](#)
 - display units [F-4](#)
- status bar [F-32 to F-33](#)
- status messages [F-32](#)
- top of main window [F-4](#)
- trend graph, explained [F-6](#)
- uninstalling [F-34](#)
- using
 - AP Scan List tab [F-8 to F-18](#)
 - AP scanning [F-26 to F-31](#)
 - thresholds [F-20 to F-25](#)
 - View AP Details button [F-13](#)
 - viewing
 - access point details [F-13 to F-16](#)
 - an accumulation of access points [F-18](#)
 - AP scan log [F-28 to F-29](#)
 - status of access point [F-5 to F-8](#)
 - threshold log file [F-24 to F-25](#)
- Smart Card or other Certificate Properties window - Windows XP [E-11](#)
- software
 - compatibility with Cisco Aironet client adapters [3-9](#)
 - installing [3-9 to 3-20](#)
 - procedures [9-3 to 9-11](#)
 - uninstalling [9-6 to 9-7](#)
 - upgrading [9-3 to 9-5](#)
- software components
 - described [1-4](#)
 - finding versions [9-9](#)
- specifications
 - physical [A-2](#)
 - power [A-6](#)
 - radio [A-3 to A-5](#)
 - regulatory compliance [A-6](#)
 - safety [A-6](#)
- spread spectrum [1-3](#)
- SSID
 - setting [5-4](#)
 - viewing
 - in ADU [4-3, 4-5, 7-8](#)
 - in ASTU [8-3, 8-11](#)
 - in site survey utility [F-10, F-14, F-19](#)
- SSID1 parameter [5-4](#)
- SSID2 parameter [5-5](#)
- SSID3 parameter [5-5](#)
- Ssidl, in site survey utility [F-12](#)
- Start Test button, in troubleshooting utility [10-5](#)
- static WEP
 - disabling [5-58](#)

- enabling [5-26 to 5-27](#)
 - with open authentication, setting on client and access point [5-21](#)
 - with shared key authentication, setting on client and access point [5-21](#)
 - static WEP keys
 - guidelines for entering
 - in ADU [5-27](#)
 - in Windows XP [E-9](#)
 - overview [5-15, E-2](#)
 - selecting transmit key [5-27](#)
 - size of [5-26](#)
 - statistics
 - method of calculation [7-14](#)
 - receive [7-15, 7-16 to 7-17](#)
 - transmit [7-15, 7-16](#)
 - viewing [7-14 to 7-17](#)
 - status bar, in site survey utility [F-32 to F-33](#)
 - status messages, in site survey utility [F-32](#)
 - status of client adapter
 - in ADU Advanced Status window [7-8 to 7-13](#)
 - in ADU Current Status window [7-5 to 7-7](#)
 - in ASTU Connection Status window [8-9 to 8-11](#)
 - in ASTU Tool Tip window [8-4](#)
 - in Windows XP [E-18](#)
 - Stop Test button, in troubleshooting utility [10-5](#)
 - supplicant, finding version [9-9](#)
 - system requirements [2-4](#)
-
- ## T
- Taiwan, administrative rules for client adapters [C-8 to C-9](#)
 - Temporal Key Integrity Protocol (TKIP)
 - described [5-20](#)
 - setting on client and access point [5-25](#)
 - with WPA [5-18](#)
 - temporary username and password
 - automatically prompt for
 - for LEAP [5-31](#)
 - described
 - for EAP-FAST [5-37, 5-38](#)
 - for LEAP [5-30](#)
 - manually prompt for
 - for EAP-FAST [5-38](#)
 - for LEAP [5-31](#)
 - selecting options
 - for EAP-FAST [5-38](#)
 - for LEAP [5-31](#)
 - using Windows credentials
 - for LEAP [5-31](#)
 - third-party tool, enabling in Install Wizard [3-17](#)
 - threshold log file
 - adding a comment to [F-24](#)
 - deleting in site survey utility [F-25](#)
 - name and location [F-23](#)
 - viewing in site survey utility [F-24 to F-25](#)
 - Threshold Log File window (site survey utility) [F-25](#)
 - Threshold Logging Configuration window (site survey utility) [F-21](#)
 - thresholds, using in site survey utility [F-20 to F-25](#)
 - threshold triggers
 - disabling in site survey utility [F-23](#)
 - enabling in site survey utility [F-23](#)
 - throughput [5-8, 5-9](#)
 - time of day, in site survey utility [F-10, F-17, F-18](#)
 - TKIP
 - option in Windows XP [E-8](#)
 - status of [7-7](#)
 - Token Configuration window [6-15](#)
 - translated safety warnings [B-1 to B-6](#)
 - transmit key [5-27](#)
 - transmit power, in site survey utility [F-12, F-16](#)
 - Transmit Power Level parameter [5-7](#)
 - transmit rate [7-12, 8-11](#)
 - transmit statistics [7-15, 7-16](#)
 - Troubleshooting
 - ASTU menu option [8-6](#)

troubleshooting information, accessing [10-2](#)

troubleshooting utility

saving detailed report to text file [10-7](#)

using [10-3 to 10-7](#)

Troubleshooting Utility window

detailed report [10-6](#)

initial window [10-4](#)

with test results [10-5](#)

U

unicast packets

number received [7-15](#)

number transmitted [7-15](#)

uninstalling

client adapter software [9-6 to 9-7](#)

profile migration tool [G-7](#)

unpacking the client adapter [2-3](#)

upgrading client adapter software [9-3 to 9-5](#)

up time, status of [7-12](#)

Use Auto Profile Selection, ASTU menu option [8-8](#)

Use Machine Information For Domain Logon parameter

for EAP-TLS [5-42, 5-46](#)

for PEAP (EAP-GTC) [5-49](#)

for PEAP (EAP-MSCHAP V2) [5-53](#)

Use Saved User Name and Password option

for EAP-FAST [5-38](#)

for LEAP [5-30](#)

Use Temporary User Name and Password option

for EAP-FAST [5-37, 5-38](#)

for LEAP [5-30](#)

Use Windows to Configure My Wireless Network Settings parameter - Windows XP [E-6](#)

Use Windows User Name and Password option

for EAP-FAST [5-38](#)

for LEAP [5-30, 5-31, 5-38](#)

V

View AP Details button, in site survey utility [F-13](#)

View AP Scan Log, site survey utility menu option [F-16, F-28](#)

viewer, name and location [F-23, F-27](#)

View Report button, in troubleshooting utility [10-5](#)

View Threshold Log, site survey utility menu option [F-24](#)

W

warning

antenna [2-2, B-3](#)

explosive device proximity [2-2, B-2](#)

laptop users [2-3, B-4 to B-6](#)

WEP

keys

additional security features [5-20 to 5-21](#)

defined [5-14, E-2](#)

entry method [5-26](#)

size of [5-15, E-2](#)

types of [5-15, E-2](#)

status of [7-7](#)

WEP key hashing, described [5-20](#)

WEP option, in Windows XP [E-8](#)

Wi-Fi Multimedia (WMM)

enabling [5-59 to 5-62](#)

in site survey utility [F-12](#)

status of [7-10](#)

Wi-Fi Protected Access (WPA)

described [5-18, E-4](#)

enabling in Windows XP [E-8](#)

enabling with EAP-FAST [5-34](#)

enabling with EAP-TLS [5-45](#)

enabling with LEAP [5-29](#)

enabling with PEAP (EAP-GTC) [5-48](#)

enabling with PEAP (EAP-MSCHAP V2) [5-52](#)

in site survey utility [F-12](#)

software required [E-4](#)

Wi-Fi Protected Access 2 (WPA2)

- described [5-18](#)
- enabling with EAP-FAST [5-34](#)
- enabling with EAP-TLS [5-45](#)
- enabling with LEAP [5-29](#)
- enabling with PEAP (EAP-GTC) [5-48](#)
- enabling with PEAP (EAP-MSCHAP V2) [5-52](#)
- in site survey utility [F-12](#)

Windows 2000

- disabling Microsoft 802.1X supplicant [10-8](#)
- resolving resource conflicts [10-9](#)

Windows Wireless Network Connection icon, shows unavailable connection [10-17](#)

Windows XP

- associating to an access point [E-18](#)
- configuring client adapter through [E-5 to E-10](#)
- disabling Microsoft Wireless Configuration Manager [10-7](#)
- enabling EAP-TLS authentication [E-10 to E-12](#)
- enabling PEAP authentication [E-13 to E-18](#)
- feature comparison to ADU [3-17 to 3-18](#)
- making a configuration decision [3-17 to 3-18](#)
- resolving resource conflicts [10-9 to 10-10](#)
- security features [E-2 to E-4](#)
- viewing status of client adapter [E-18](#)

Wireless Cisco Connection Properties window - Windows 2000 [5-60](#)

wireless infrastructure [1-6](#)

wireless mode, current [4-6, 7-6](#)

Wireless Mode parameter [5-10](#)

Wireless Mode When Starting Ad Hoc Network parameter [5-10](#)

Wireless Network Connection Properties window (Wireless Networks Tab) - Windows XP [E-6](#)

Wireless Network Connection Properties window - Windows XP [5-62](#)

Wireless Network Connection Status window - Windows XP [E-18](#)

Wireless Network Properties window (Association Tab) - Windows XP [E-7](#)

Wireless Network Properties window (Authentication Tab) - Windows XP [E-10, E-13](#)

WMM

See Wi-Fi Multimedia (WMM)

workstation

- defined [1-2](#)
- in wireless infrastructure [1-6](#)

WPA

See Wi-Fi Protected Access (WPA)

WPA/WPA2/CKKM EAP Type parameter

- with EAP-FAST [5-34](#)
- with EAP-TLS [5-45](#)
- with LEAP [5-29](#)
- with PEAP (EAP-GTC) [5-48](#)
- with PEAP (EAP-MSCHAP V2) [5-52](#)

WPA/WPA2/CKKM option

- used to enable CKKM fast secure roaming [5-19](#)
- with EAP-FAST [5-34](#)
- with EAP-TLS [5-45](#)
- with LEAP [5-29](#)
- with PEAP (EAP-GTC) [5-48](#)
- with PEAP (EAP-MSCHAP V2) [5-52](#)

WPA/WPA2 Passphrase option [5-28](#)

WPA2

See Wi-Fi Protected Access 2 (WPA2)

WPA2 passphrase

- described [5-18](#)
- disabling [5-58](#)
- enabling [5-28](#)
- setting on client and access point [5-21](#)

WPA option, in Windows XP [E-8](#)

WPA passphrase

- described [5-18, E-4](#)
- disabling [5-58](#)
- enabling [5-28](#)
- setting on client and access point [5-21](#)

WPA Pre-Shared Key

See WPA passphrase or WPA2 passphrase

WPA-PSK

described [5-18, E-4](#)

option in Windows XP [E-8](#)