



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

Software Release 1.0

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-16534-01

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0805R)

Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide for Window Vista
Copyright © 2008 Cisco Systems, Inc.
All rights reserved.



CONTENTS

Preface	ix
Audience	ix
Purpose	ix
Organization	x
Conventions	x
Related Publications	xii
Obtaining Documentation, Obtaining Support, and Security Guidelines	xii

CHAPTER 1

Product Overview and Installation	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
Network Configurations Using Client Adapters	1-4
Ad Hoc Wireless LAN	1-4
Wireless Infrastructure with Workstations Accessing a Wired LAN	1-5
Safety information	1-6
FCC Safety Compliance Statement	1-6
Safety Guidelines	1-6
Warnings	1-7
Unpacking the Client Adapter	1-7
Package Contents	1-8
System Requirements	1-8
Site Requirements	1-9
For Infrastructure Devices	1-9
For Client Devices	1-9
Inserting the Client Adapter	1-10
Inserting a PC-Cardbus Card	1-10
Inserting a PCI Card	1-11
Changing the Bracket	1-11

Inserting the Card	1-12
Assembling the Antenna	1-13
Mounting the Antenna	1-14
Obtaining Client Adapter Software	1-17
Installing the Client Adapter Driver and Software	1-18

CHAPTER 2

Configuring Wireless Profiles	2-1
Overview of Wireless Profiles	2-2
Accessing Microsoft Vista Network and Sharing Center	2-2
Creating a New Profile and Configuring Basic Settings	2-3
Security and Encryption Types	2-10
WEP (Shared) Security with Static WEP Keys	2-10
WPA and WPA2	2-10
802.1X with Dynamic WEP Keys	2-11
CCKM Fast Secure Roaming	2-12
Accessing a Profile That Was Created Previously	2-12
Viewing and Changing the Settings of a Profile	2-13
Radio Measurement	2-18
Advanced Roaming Setting	2-19

CHAPTER 3

Configuring EAP Types	3-1
Overview of EAP-FAST	3-1
How EAP-FAST Works	3-2
Two-Phase Tunneled Authentication	3-2
Protected Access Credentials	3-3
Server Certificate Validation	3-3
Configuring EAP-FAST	3-4
Accessing EAP-FAST Properties for Configuration	3-4
Configuring EAP-FAST Settings in the Connection Tab	3-5
Overview of the User Credentials Tab	3-9
Client Certificates	3-9
Usernames and Passwords	3-9
Configuring EAP-FAST Settings in the User Credentials Tab	3-10
Understanding PIN Mode and Token Mode with OTP	3-12
Configuring EAP-FAST Settings in the Authentication Tab	3-13
Finding the Version of the EAP-FAST Module	3-16
Overview of LEAP	3-17
How LEAP Works	3-17

Configuring LEAP	3-18
Accessing LEAP Properties for Configuration	3-18
Configuring LEAP Settings in the Network Credentials Tab	3-19
Finding the Version of the LEAP Module	3-21
Overview of PEAP-GTC	3-21
How PEAP-GTC Works	3-22
Configuring PEAP-GTC	3-23
Accessing PEAP-GTC Properties for Configuration	3-23
Configuring PEAP-GTC Settings in the Connection Tab	3-25
Configuring PEAP-GTC Settings in the User Credentials Tab	3-27
Understanding PIN Mode and Token Mode with OTP	3-29
Understanding PEAP-GTC Authentication	3-30
Finding the Version of the PEAP-GTC Module	3-30

CHAPTER 4**Performing Administrative Tasks 4-1**

Using Microsoft Tools to Perform Administrative Tasks	4-2
Overview of Group Policy Objects	4-2
Adding a Group Policy Object Editor	4-2
Creating a EAP Group Policy Object in Windows Vista	4-3
Configuring Machine Authentication for EAP-FAST	4-4
Configuring Single Sign-On for EAP-FAST	4-5
Configuring Machine Authentication for PEAP-GTC	4-5
Configuring Single Sign-On for PEAP-GTC and LEAP	4-5
The EAP-FAST XML Schema	4-6
The PEAP-GTC XML Schema	4-17
The LEAP XML Schema	4-23
Logging for EAP Modules	4-26
Configuring and Starting Logging	4-26
Disabling Logging and Flushing Internal Buffers	4-27
Locating Log Files	4-28

CHAPTER 5**Routine Procedures 5-1**

Removing a Client Adapter	5-2
Removing a PC-Cardbus Card	5-2
Removing a PCI Card	5-2
Upgrading the Client Adapter Software	5-3

CHAPTER 6

Troubleshooting and Diagnostics 6-1

- Troubleshooting with Cisco Aironet Client Diagnostics 6-2
- Enabling Client Reporting 6-6

APPENDIX A

EAP Messages A-1

- EAP-FAST Error Messages and Prompts A-1
- PEAP-GTC and LEAP Error Messages and Prompts A-6
- Creating Strong Passwords A-9
 - Characteristics of Strong Passwords A-9
 - Characteristics of Weak Passwords A-9
 - Password Security Basics A-10

APPENDIX B

Technical Specifications B-1

APPENDIX C

Translated Safety Warnings C-1

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

APPENDIX D

Declarations of Conformity and Regulatory Information D-1

- Manufacturer’s Federal Communication Commission Declaration of Conformity Statement D-2
- Department of Communications – Canada D-3
 - Canadian Compliance Statement D-3
- European Community, Switzerland, Norway, Iceland, and Liechtenstein D-3
 - Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC D-3
 - Declaration of Conformity Statement D-5
 - Cisco Aironet CB21AG Wireless LAN Client Adapter D-5
 - Cisco Aironet PI21AG Wireless LAN Client Adapter D-6
- Declaration of Conformity for RF Exposure D-7
- Guidelines for Operating Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters in Japan D-7
 - Japanese Translation D-7
 - English Translation D-7
- Administrative Rules for Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters in Taiwan D-8
 - 2.4- and 5-GHz Client Adapters D-8
 - Chinese Translation D-8
 - English Translation D-8
 - 5-GHz Client Adapters D-9

Chinese Translation D-9

English Translation D-9

Brazil/Anatel Approval D-9

AIR-CB21AG-W-K9 D-10

AIR-PI21AG-W-K9 D-11

APPENDIX E**Channels, Power Levels, and Antenna Gains E-1**

Channels E-2

IEEE 802.11a E-2

IEEE 802.11b/g E-3

Maximum Power Levels and Antenna Gains E-4

IEEE 802.11a E-4

IEEE 802.11b E-4

IEEE 802.11g E-5

APPENDIX F**Acknowledgments and Licensing F-1**

APPENDIX G**Abbreviations G-1**



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

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 that is running the Microsoft Windows Vista operating system. This person should understand Windows Vista and should be familiar with computing devices, network terms, and concepts.

Purpose

This publication describes the Cisco Aironet CB21AG and PI21AG client adapters on devices that are running Windows Vista.



Caution

This guide pertains specifically to Cisco Aironet CB21AG and PI21AG client adapters on devices that are running Windows Vista. For information about the Cisco Aironet CB21AG and PI21AG on devices that are running Windows XP or Cisco Aironet 340, 350, and CB20A wireless LAN client adapters, refer to the appropriate guides at this URL:

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

Organization

This publication contains the following chapters:

- [Chapter 1, “Product Overview and Installation,”](#) describes the Cisco Aironet CB21AG and PI21AG client adapters and their role in a wireless network. This chapter also provides information that you need to know before installing a client adapter and instructions for installing the client adapter hardware and software.
- [Chapter 2, “Configuring Wireless Profiles,”](#) explains how to use the Microsoft Vista Network and Sharing Center to create and manage profiles for your client adapter.
- [Chapter 3, “Configuring EAP Types,”](#) explains the Cisco EAP types that are used for authentication to wireless networks.
- [Chapter 4, “Performing Administrative Tasks,”](#) explains how to obtain Microsoft administrative tools to distribute wireless profiles to users and computers in an Active Directory environment. This chapter also provides the XML schemas for EAP-FAST, LEAP, and PEAP-GTC.
- [Chapter 5, “Routine Procedures,”](#) provides procedures for common tasks related to the client adapter.
- [Chapter 6, “Troubleshooting and Diagnostics,”](#) provides information about diagnosing problems that might occur when you try to operate the client adapter.
- [Appendix A, “EAP Messages,”](#) describes EAP-FAST, PEAP-GTC and LEAP error messages and prompts. This appendix also provides guidelines for creating strong passwords.
- [Appendix B, “Technical Specifications,”](#) provides technical specifications for the Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters.
- [Appendix C, “Translated Safety Warnings,”](#) 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.
- [Appendix D, “Declarations of Conformity and Regulatory Information,”](#) provides declarations of conformity and regulatory information for the Cisco Aironet CB21AG and PI21AG Wireless LAN client adapters.
- [Appendix E, “Channels, Power Levels, and Antenna Gains,”](#) lists the IEEE 802.11a, b, and g channels supported by the world's regulatory domains as well as the maximum power levels and antenna gains allowed per data rate.
- [Appendix F, “Acknowledgments and Licensing,”](#) provides information about open-source software that is used in the Cisco EAP modules.
- [Appendix G, “Abbreviations,”](#) includes commonly used abbreviations.

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

Release notes for Cisco Aironet 802.11a/b/g client adapters (CB21AG and PI21AG) for Windows Vista are located at this URL:

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

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 and Installation

This chapter describes the Cisco Aironet CB21AG and PI21AG client adapters and their role in a wireless network. This chapter also provides information that you need to know before installing a client adapter and instructions for installing the client adapter hardware and software.

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 1-4](#)
- [Safety information, page 1-6](#)
- [Unpacking the Client Adapter, page 1-7](#)
- [System Requirements, page 1-8](#)
- [Site Requirements, page 1-9](#)
- [Inserting the Client Adapter, page 1-10](#)
- [Obtaining Client Adapter Software, page 1-17](#)
- [Installing the Client Adapter Driver and Software, page 1-18](#)

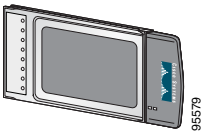
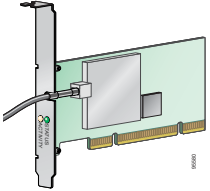
Introduction to the Client Adapters

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 system messages. [Table 1-2](#) provides interpretations of the the LEDs.

Table 1-2 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	

Table 1-2 LED Operating Messages (continued)

Status LED (green)	Activity LED (amber)	Condition
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).

Software Components

You can install both the driver for the CB21AG and PI21AG and the software that runs the adapter by running a single executable file that is available from Cisco.com. You must execute this file on devices that are running Windows Vista. This driver and software can be used only with CB21AG and PI21AG client adapters.

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:

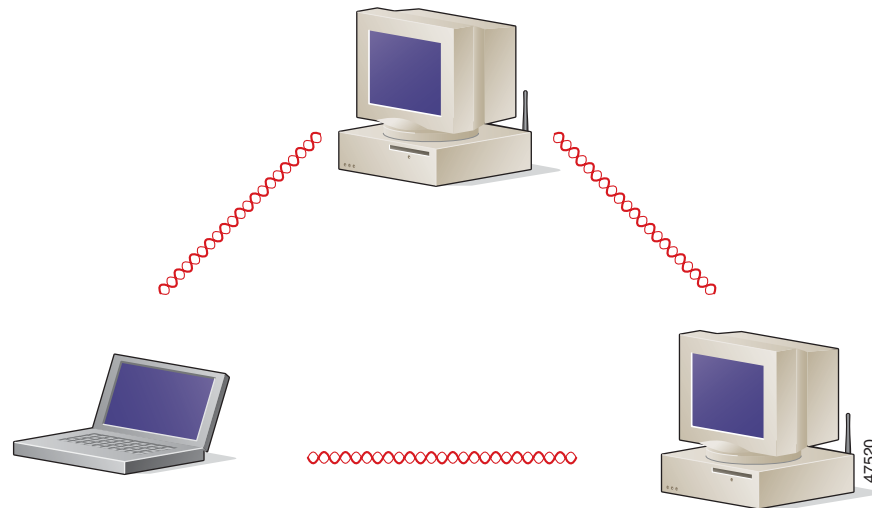
- Ad hoc wireless local area network (LAN)
- Wireless infrastructure with workstations accessing a wired LAN

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

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

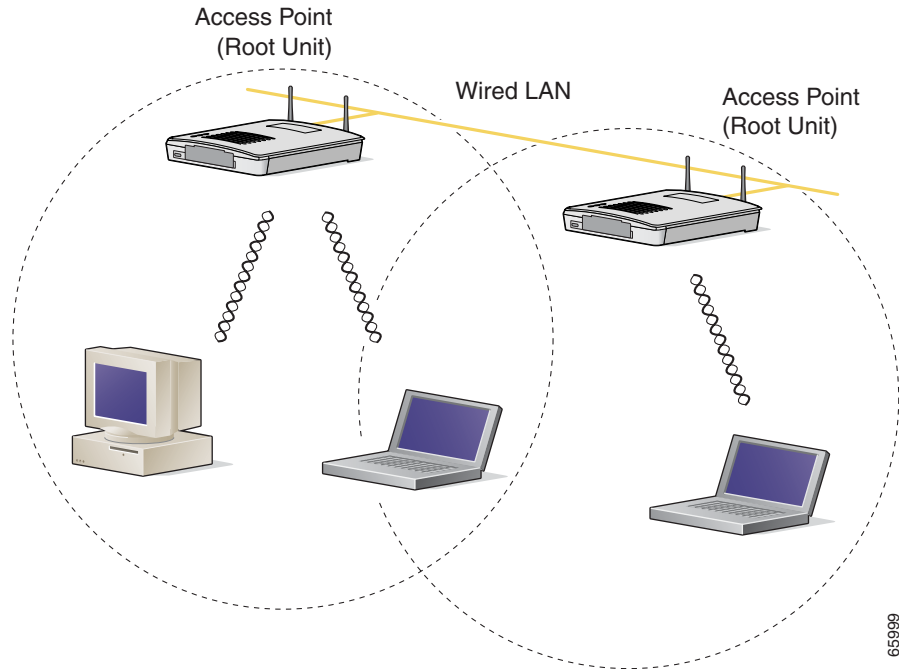


Wireless Infrastructure with Workstations Accessing a Wired LAN

A infrastructure 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*



66609

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.



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.



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.



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 the container.
 - 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 Vista.
 - Laptop or notebook computer equipped with a 32-bit Cardbus slot
 - Desktop personal computer equipped with an empty PCI expansion slot
- Windows Vista Service Pack 1 or Windows Vista with hotfix KB932063 and hotfix KB935222



Note You must obtain these hotfix patches from the Microsoft site. You must also contact Microsoft directly for any support that you need for these patches.

<http://support.microsoft.com/kb/932063>

<http://support.microsoft.com/kb/935222>



Note The client adapter software supports Windows Vista Business, Enterprise, and Ultimate operating systems.

- 1 GHz 32-bit (x86) or 64-bit (x64) processor.
- 1 GB of system memory
- 40 GB hard drive with at least 15 GB of available space
- 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
- 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.



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.

Inserting the 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.

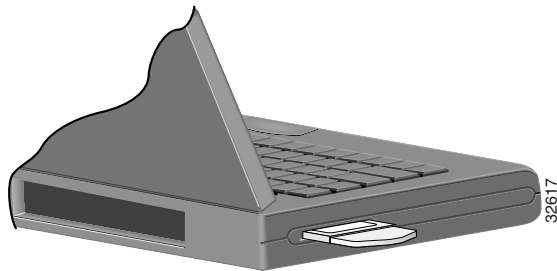
- Step 3** Hold the card with the Cisco label facing up and insert it into the Cardbus slot, applying just enough pressure to make sure it is fully seated (see [Figure 1-3](#)). The green LED lights when the card is inserted properly.



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 1-3 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 Driver and Software](#)” section on page 1-18.

Inserting a PCI Card

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

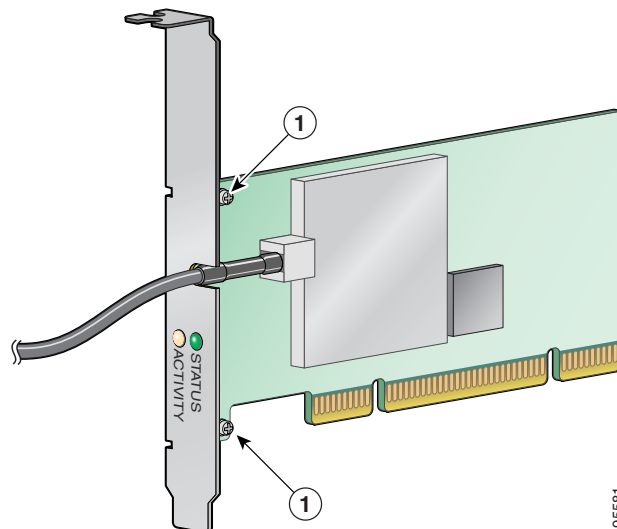
- If required, change the bracket (see the “[Changing the Bracket](#)” section on page 1-11).
- Insert the card (see the “[Inserting the Card](#)” section on page 1-12).
- Assemble the antenna (see the “[Assembling the Antenna](#)” section on page 1-13).
- Mount the antenna (see the “[Mounting the Antenna](#)” section on page 1-14).

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 1-4](#).

Figure 1-4 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 1-4](#)) 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.

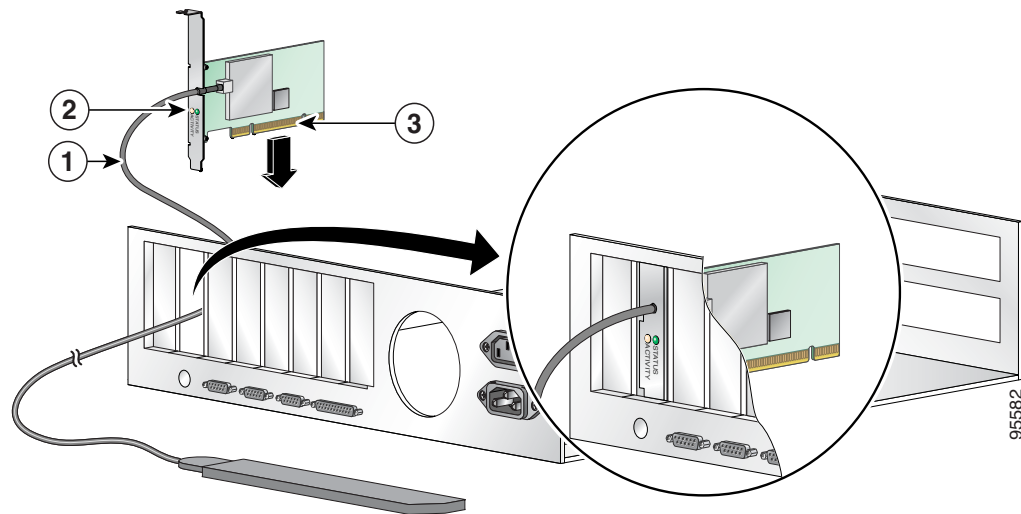
Step 3 Remove the screw from the top of the CPU back panel above an empty PCI expansion slot. This screw holds the metal bracket on the back panel.

**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 1-5](#).

Figure 1-5 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 1-5](#).

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.

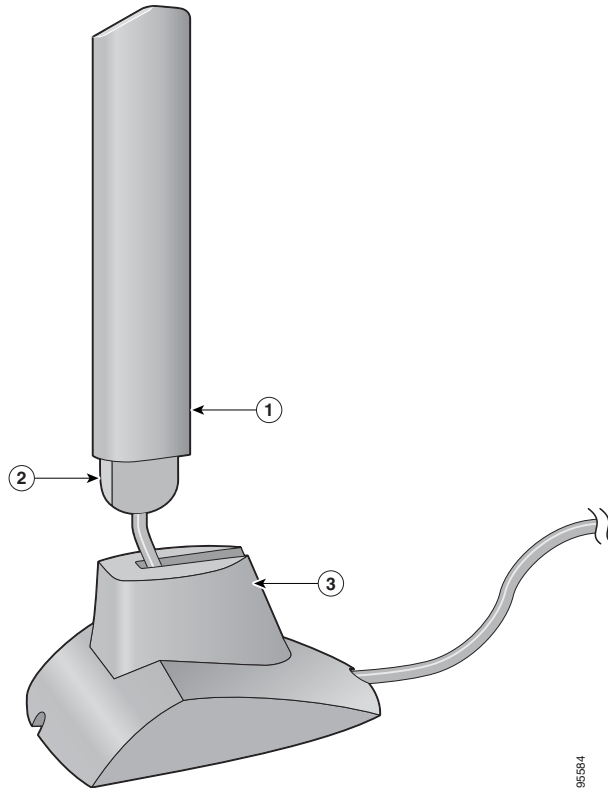
Step 8 Reinstall the screw on the CPU back panel and replace the computer cover.

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 1-6](#).

Figure 1-6 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 1-6](#).

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

Mounting the Antenna

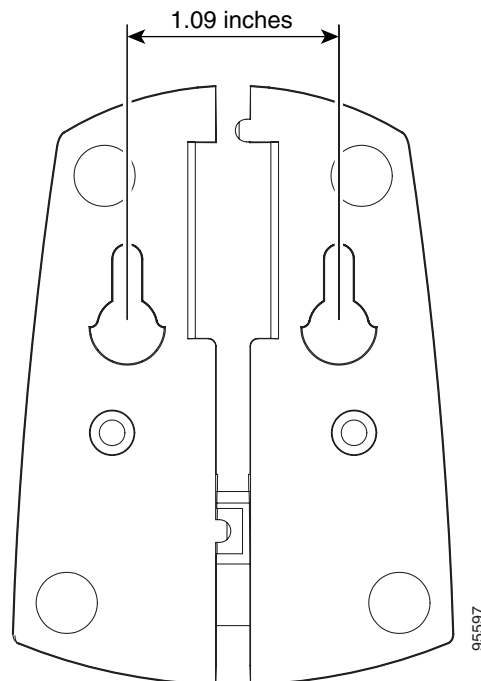
Because the PCI card is a radio device, it is susceptible to RF obstructions and common sources of interference that can reduce throughput and range. Follow these guidelines to ensure the best possible performance:

- 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.

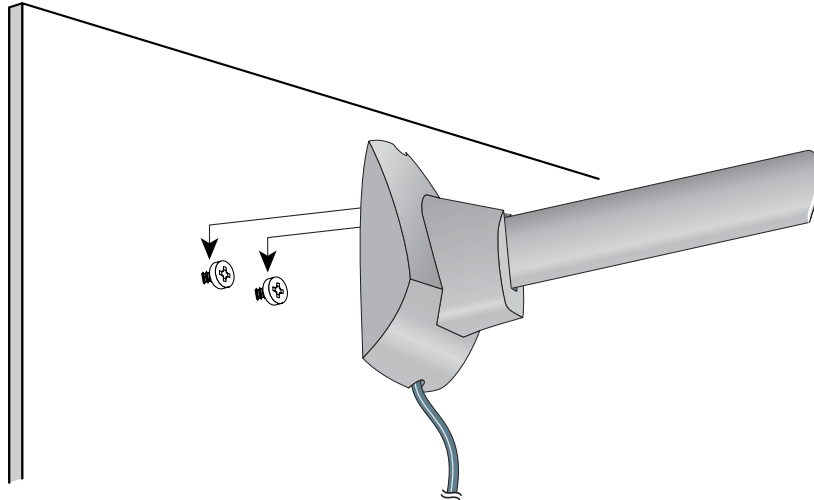
Follow the steps below to position the PCI card's antenna on a flat horizontal surface or to mount it to a wall.

- 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 1-7](#) shows the distance between the mounting holes on the bottom of the antenna base.

Figure 1-7 Bottom of Antenna Base

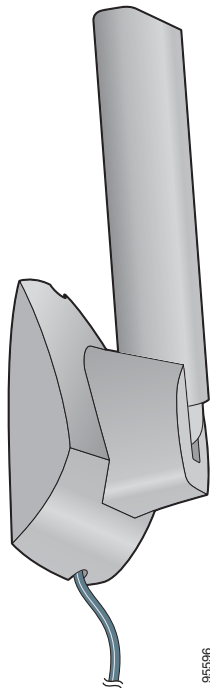


- Step 3** Tap the two supplied wall anchors into the holes.
- Step 4** Drive the two supplied screws into the wall anchors, leaving a small gap between the screw head and the anchor.
- Step 5** Position the mounting holes on the bottom of the antenna base over the screws (see [Figure 1-8](#)) and pull down to lock in place.

Figure 1-8 *Mounting the Antenna*

95595

Step 6 The antenna rotates 90 degrees from its base. For optimal reception, position the antenna so it is pointing straight up (see [Figure 1-9](#)).

Figure 1-9 *Rotating the Antenna*

95596

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 Driver and Software”](#) section on page 1-18.

Obtaining Client Adapter Software

The software is provided on the CD that shipped with your client adapter; however, Cisco recommends retrieving it from Cisco.com to ensure that you have the latest version.

- To obtain the version of the software on the CD, open the FileList.txt file on the CD root directory.
- To obtain the version of the latest software on Cisco.com, follow these steps:

-
- Step 1** Make sure that you have a Cisco.com username and password.
 - Step 2** If you do not have a Cisco.com username and password, go to Cisco's main page (<http://www.cisco.com>) and click **Register** (top). Follow the instructions to create a username and password.
 - Step 3** Use your computer's web browser to access the following URL:
 - Step 4** <http://www.cisco.com/public/sw-center/>
 - Step 5** Click **Wireless Software**.
 - Step 6** Click **Client Adapters and Client Software**.
 - Step 7** Click **Cisco Aironet Wireless LAN Client Adapters**.
 - Step 8** Follow one of these steps:
 - Step 9** If you are using a PC-Cardbus card, click **Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Adapter (CB21AG)**.
 - Step 10** If you are using a PCI card, click **Cisco Aironet 802.11a/b/g PCI Wireless LAN Client Adapter (PI21AG)**.
 - Step 11** When prompted, enter your Cisco.com username and password, and click **OK**.
 - Step 12** Click **Windows Vista**.
 - Step 13** Under Available Releases, determine whether the Install Wizard file on Cisco.com has a later version number than the file on the CD. If it does, proceed to the next step. If it does not, use the Install Wizard file on your CD.
 - Step 14** Click the link with the latest release number.
 - Step 15** Click the software file (**WinClient-802.11a-b-g-Vista-Ins-Wizard-vxx.exe**), where *xx* is the version number.
 - Step 16** Click the **Download** button.
 - Step 17** Read and accept the terms and conditions of the Software License Agreement. Click **Agree** to accept the terms and condition, or click **Decline** not to accept. Save the file to your device.
-

Installing the Client Adapter Driver and Software

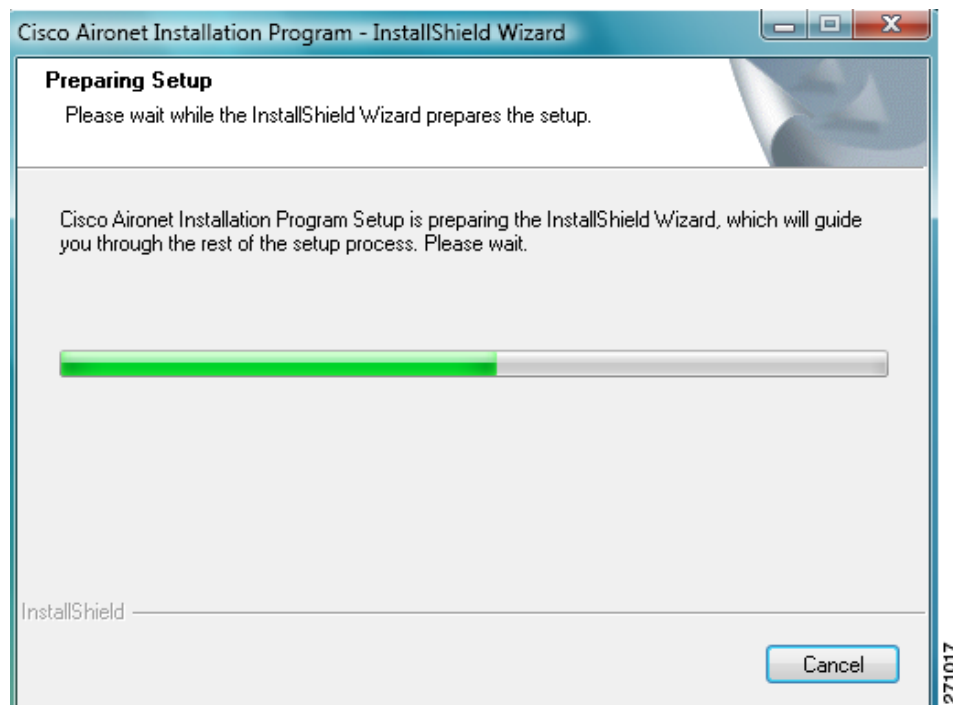

Caution

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

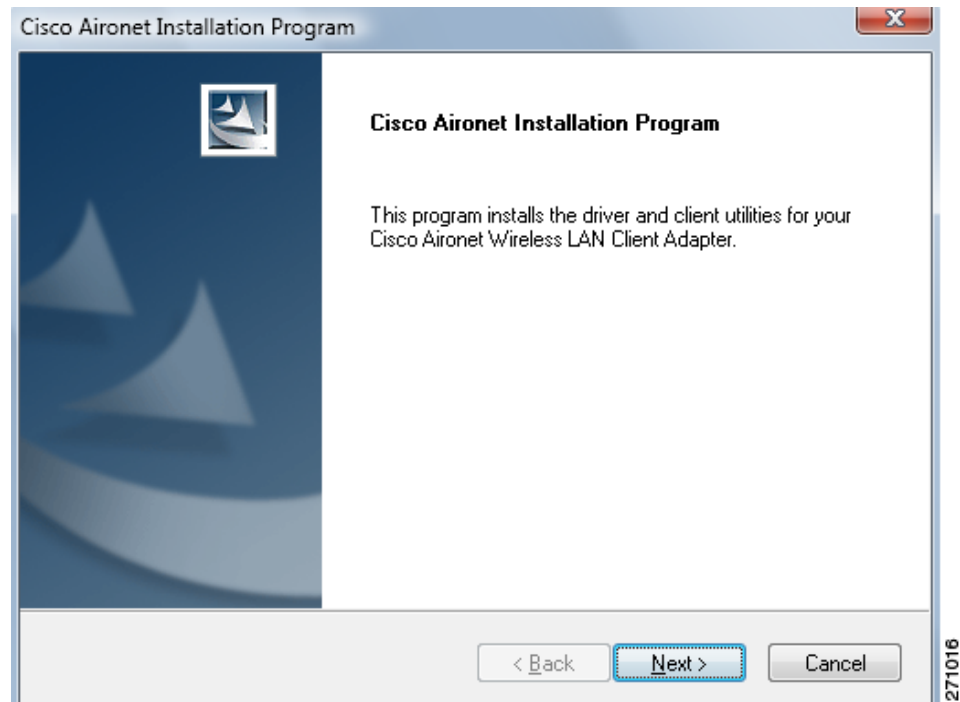
Follow these steps to use to install the client software on a device that is running Windows Vista.

- Step 1** Double-click **WinClient-802.11a-b-g-Vista-Ins-Wizard-vxx.exe**. A window appears that asks you if you want to run the software file.
- Step 2** Click **Run**. The Cisco Aironet Installation Program - InstallShield wizard window appears (see [Figure 1-10](#)).

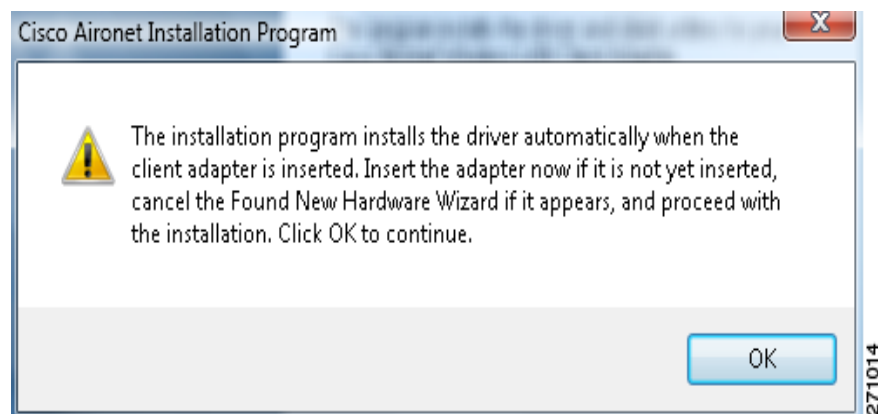
Figure 1-10 Cisco Aironet Installation Program—Installation Wizard Preparing Setup Window



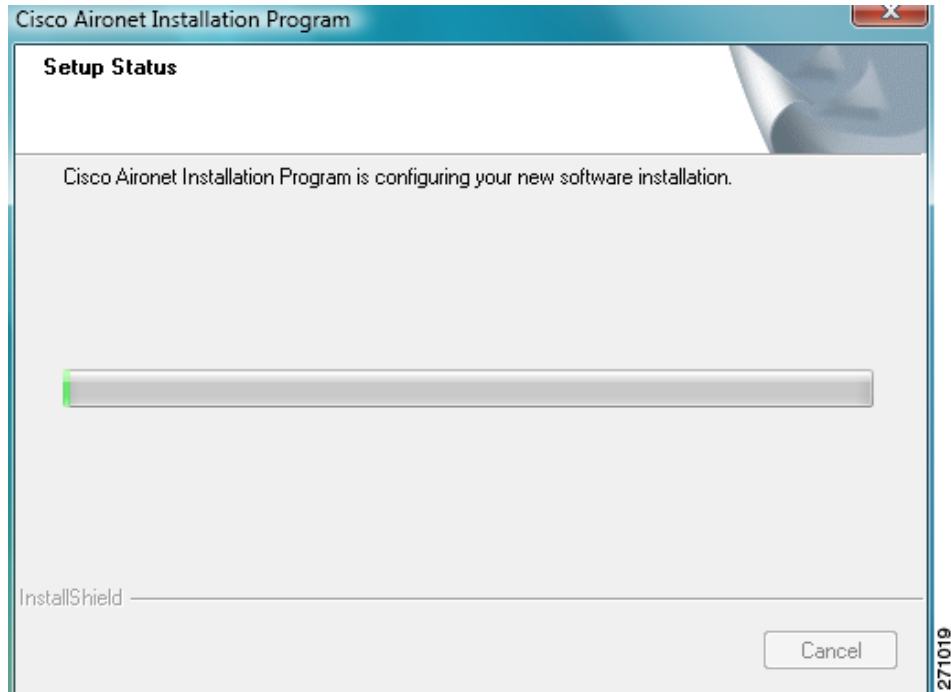
- Step 3** Allow the preparation sequence to finish. After the preparation sequence finishes, the next Cisco Aironet Installation Program window appears (see [Figure 1-11](#)).

Figure 1-11 Cisco Aironet Installation Program Window

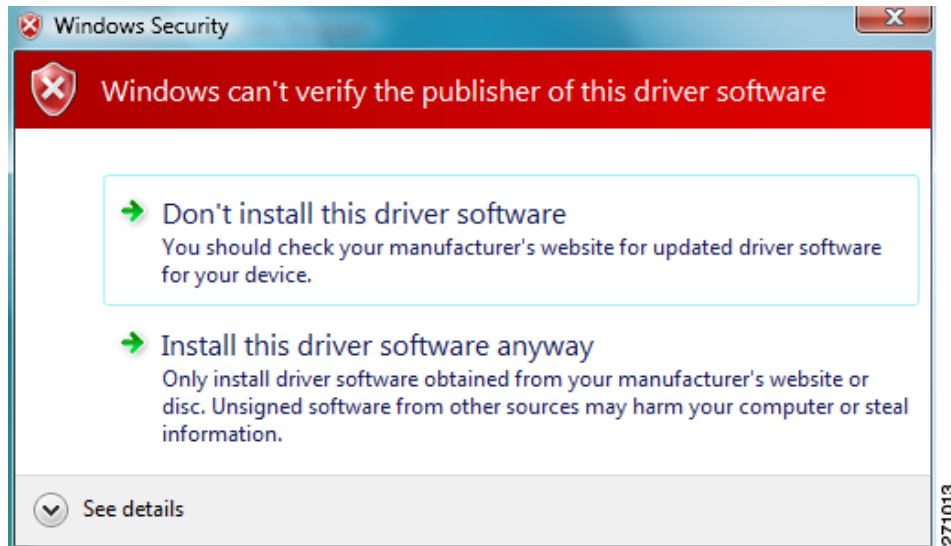
- Step 4** Click **Next**. A Cisco Aironet Installation Program dialog box that includes a message about driver and hardware installation appears (see [Figure 1-12](#)).

Figure 1-12 Cisco Aironet Installation Program Dialog Box—Driver Installation and Hardware Insertion

- Step 5** Click **OK**. The Cisco Aironet Installation Program—Setup Status window appears (see [Figure 1-13](#)).

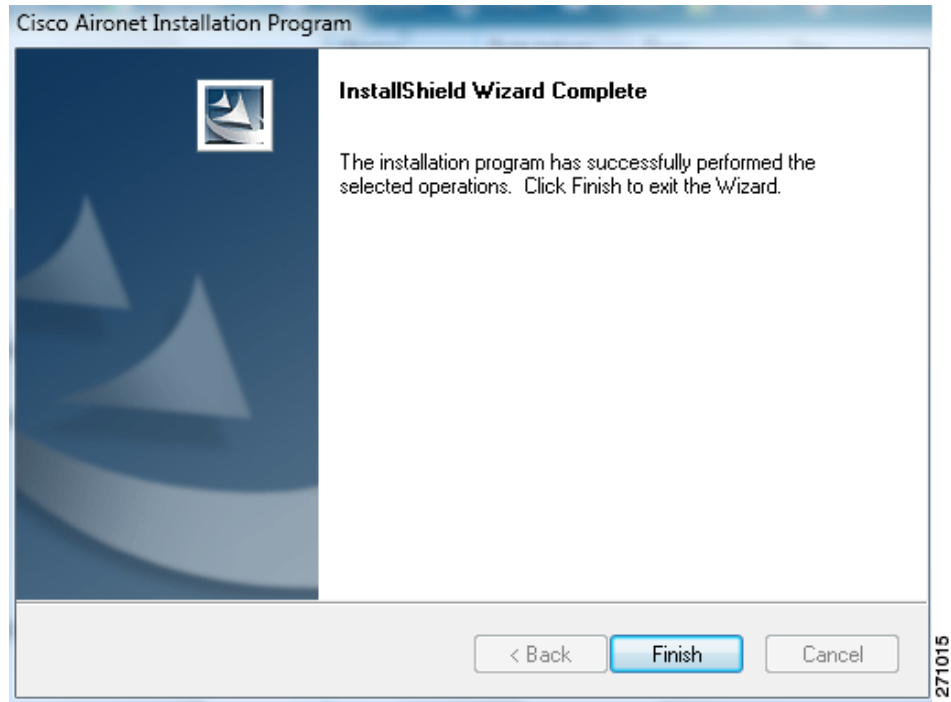
Figure 1-13 Cisco Aironet Installation Program—Setup Status Window

Step 6 Allow the software installation to finish. A Windows Security dialog box might appear (see [Figure 1-14](#)).

Figure 1-14 Windows Security—Windows can't verify the publisher of this driver software Dialog Box

Step 7 If this dialog box appears, double-click **Install this driver software anyway**. After the driver installation finishes, the Cisco Aironet Installation Program—InstallShield Wizard Complete window appears (see [Figure 1-15](#)).

Figure 1-15 Cisco Aironet Installation Program—InstallShield Wizard Complete Window



Step 8 Click **Finish**.



CHAPTER 2

Configuring Wireless Profiles

This chapter explains how to use the Microsoft Vista Network and Sharing Center to create and manage profiles for your client adapter.

The following topics are covered in this chapter:

- [Overview of Wireless Profiles, page 2-2](#)
- [Accessing Microsoft Vista Network and Sharing Center, page 2-2](#)
- [Creating a New Profile and Configuring Basic Settings, page 2-3](#)
- [Accessing a Profile That Was Created Previously, page 2-12](#)
- [Viewing and Changing the Settings of a Profile, page 2-13](#)

Overview of Wireless Profiles

A wireless profile is a set of configuration parameters that you (or your network administrator) can create and manage in the Microsoft Vista user interface. You can connect to a wireless network with the profile, which includes the wireless network name, the network security type, the network encryption type, and other feature configurations.

You can create several different profiles that enable you to connect to wireless networks in different locations. For example, you might want to create and manage profiles that allow you to use your client adapter at the office, at home, and in public areas, such as airport terminals. After the profiles are created, you can switch between them without having to configure your client adapter each time you move to a new location.

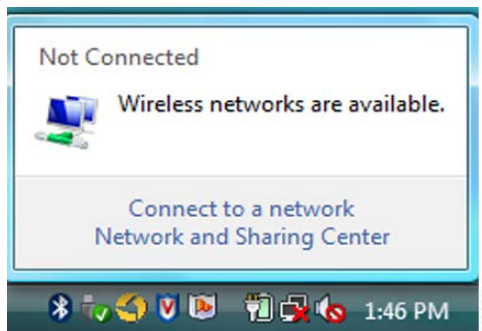
Accessing Microsoft Vista Network and Sharing Center

To create and manage wireless profiles, you must access the Microsoft Vista Network and Sharing Center.

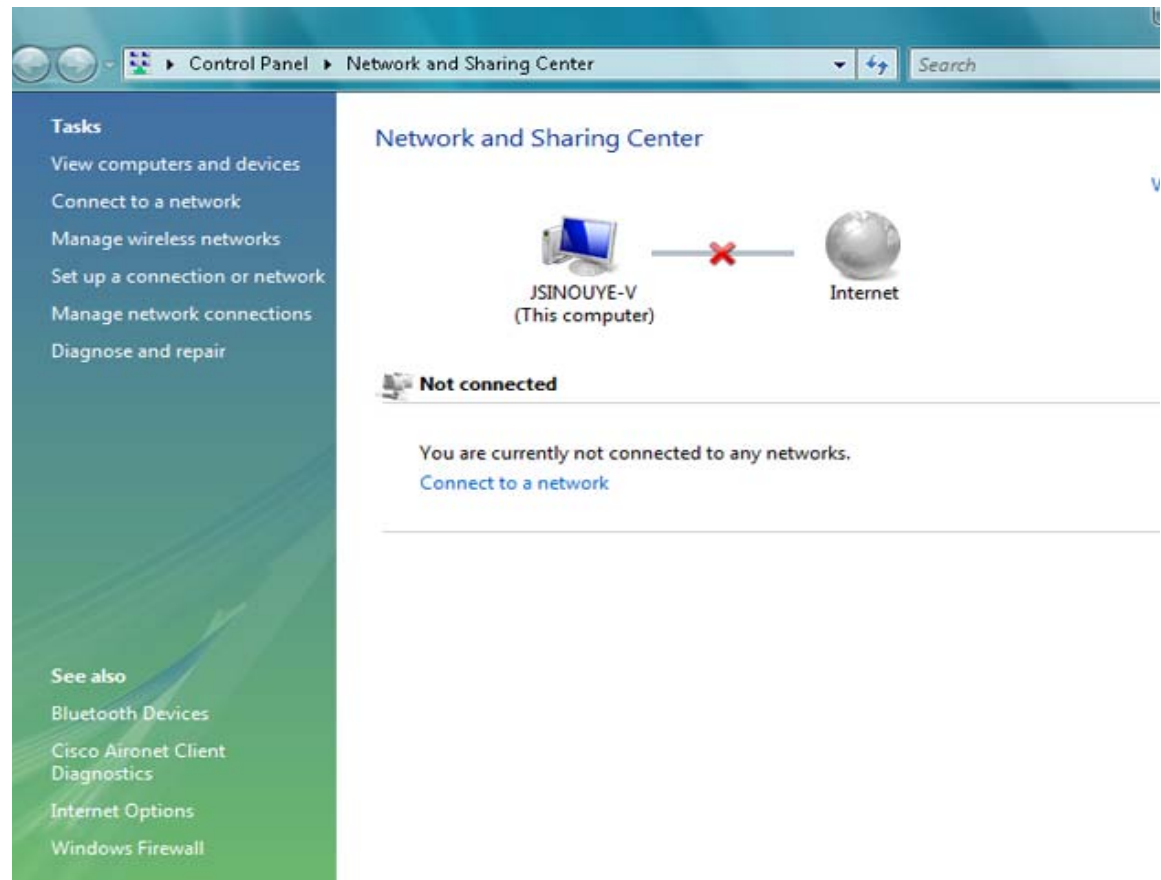
To access the Network and Sharing Center window, follow these steps:

- Step 1** Double-click the networking icon (two computer monitors) in the system tray at the bottom right corner of the screen. A small dialog box appears (see [Figure 2-1](#)).

Figure 2-1 Networking Icon in System Tray



- Step 2** Click **Network and Sharing Center**. The Network and Sharing window appears (see [Figure 2-2](#)).

Figure 2-2 Network and Sharing Center Window

Step 3 To set up a wireless profile, click **Set up a connection or network** in the Tasks area.

**Note**

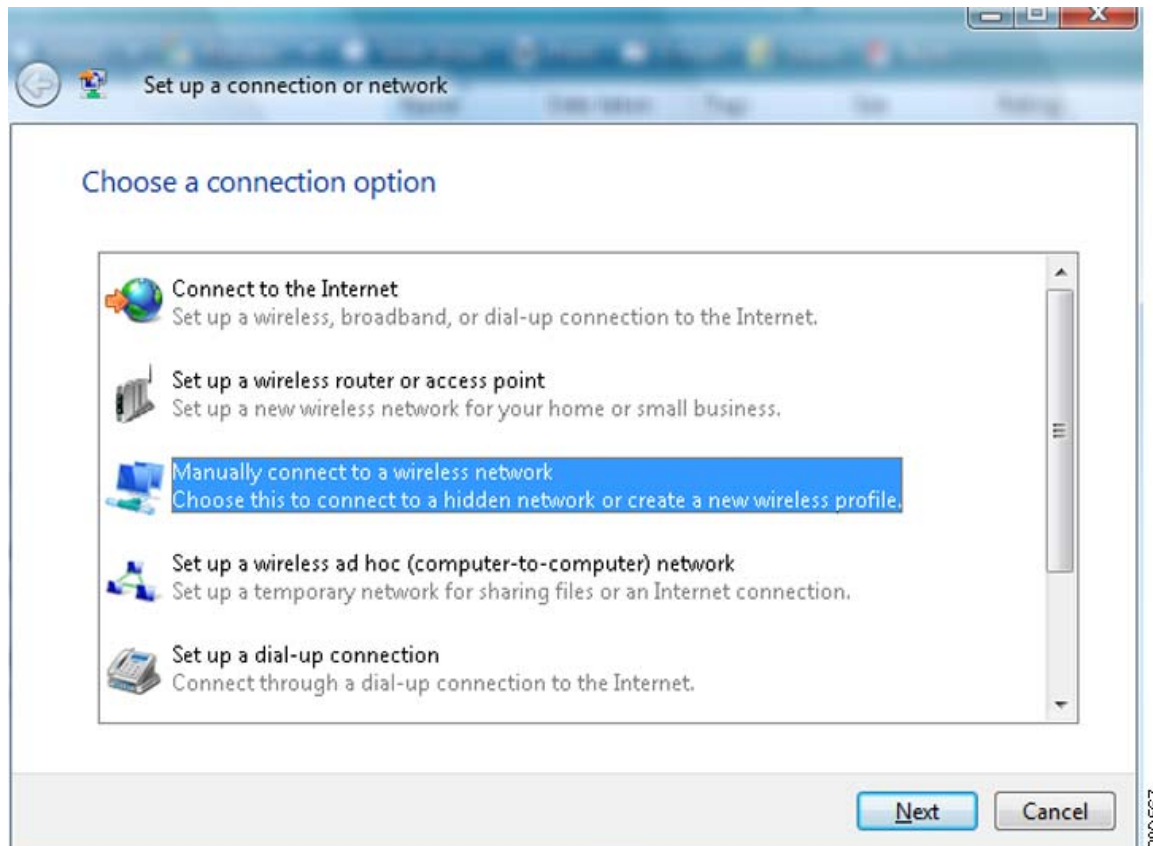
You can also access the Network and Sharing Center by choosing **Start > Control Panel > Network and Sharing Center**.

Creating a New Profile and Configuring Basic Settings

To create a wireless profile, follow these steps:

- Step 1** Open the Network and Sharing Center window (see the [“Accessing Microsoft Vista Network and Sharing Center”](#) section on page 2-2).
- Step 2** Click **Set up a connection or network** in the Tasks area. The Set up a connection or network dialog box appears (see [Figure 2-3](#)).

Figure 2-3 Set up a connection or network Dialog Box

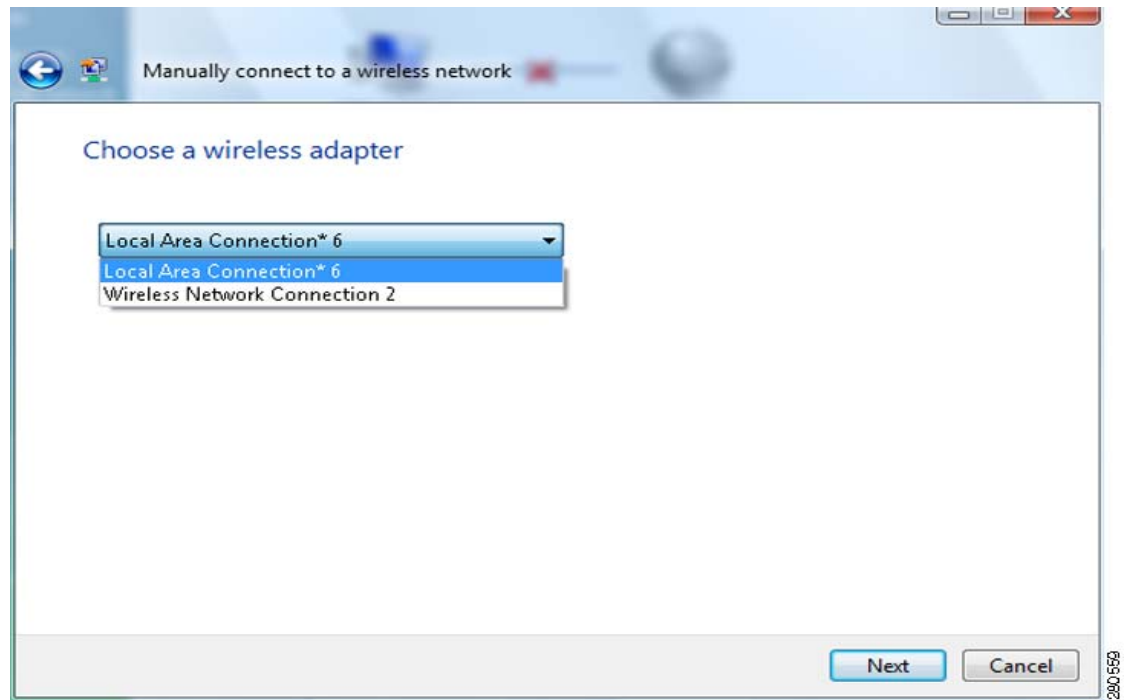


- Step 3** In the Choose a connection option area, click **Manually connect to a wireless network**.
- Step 4** Click **Next**. A Manually connect to a wireless network dialog box appears (see [Figure 2-4](#).)
- Step 5** From the Choose a wireless adapter drop-down list, choose the option for the Cisco Aironet 802.11a/b/g Wireless Adapter (see [Figure 2-4](#)).



Note Client adapters might not be easy to identify in the Choose a wireless adapter drop-down list because the adapters might be generically named (for example, Wireless Network Connection or Wireless Network Connection 2). If you have multiple client adapters on your device, choose **Network and Sharing Center > Manage network connections**. In the Views drop-down list, choose **Details** to see which generic name corresponds with which client adapter. When you view the details of available network connections, the client adapter is identified in the Device Name column.

Figure 2-4 Manually connect to a wireless network Dialog Box—Choose a wireless adapter



Step 6 Click **Next**. Another Manually connect to a wireless network dialog box appears (see [Figure 2-5](#)).

Figure 2-5 *Manually connect to a wireless network Dialog Box—Enter information for the wireless network you want to add*

Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type:

Encryption type:

Security Key/Passphrase: Display characters

Start this connection automatically

Connect even if the network is not broadcasting
Warning: If you select this option, your computer's privacy might be at risk.

Next Cancel

- Step 7** In this dialog box, enter information for the wireless network that you want to add. [Table 2-1](#) lists and describes general settings for the profile. Follow the instructions in the table to configure these settings.

Table 2-1 Profile Management General Settings

Setting	What to Enter
Network name	<p>Enter the service set identifier (SSID). The network name and the SSID are the same.</p> <p>Range: The network consists of 1 to 32 case-sensitive characters.</p> <p>Default: A blank field</p>
Security type	<p>From the Security type drop-down list, choose the method that is used to secure a connection to the wireless network. The choices are the following:</p> <ul style="list-style-type: none"> • No authentication (Open)—Open system authentication with no encryption • WEP (also called Shared)—Open system authentication with Wired Equivalent Privacy (WEP) • WPA2-Personal—Wi-Fi Protected Access 2 (WPA2) authentication with a preshared key (designed for networks without a RADIUS infrastructure) • WPA-Personal—WPA with a preshared key (designed for networks without a RADIUS infrastructure) • WPA2-Enterprise—802.1X authentication (designed for medium and large infrastructure mode networks) • WPA-Enterprise—802.1X authentication (designed for medium and large infrastructure mode networks) • 802.1x—802.1X authentication with WEP (also known as dynamic WEP). • CCKM—Cisco Centralized Key Management <p>For more information about these security types, see the “Security and Encryption Types” section on page 2-10.</p> <p>Default: None. You must choose a security type to create a wireless profile.</p>

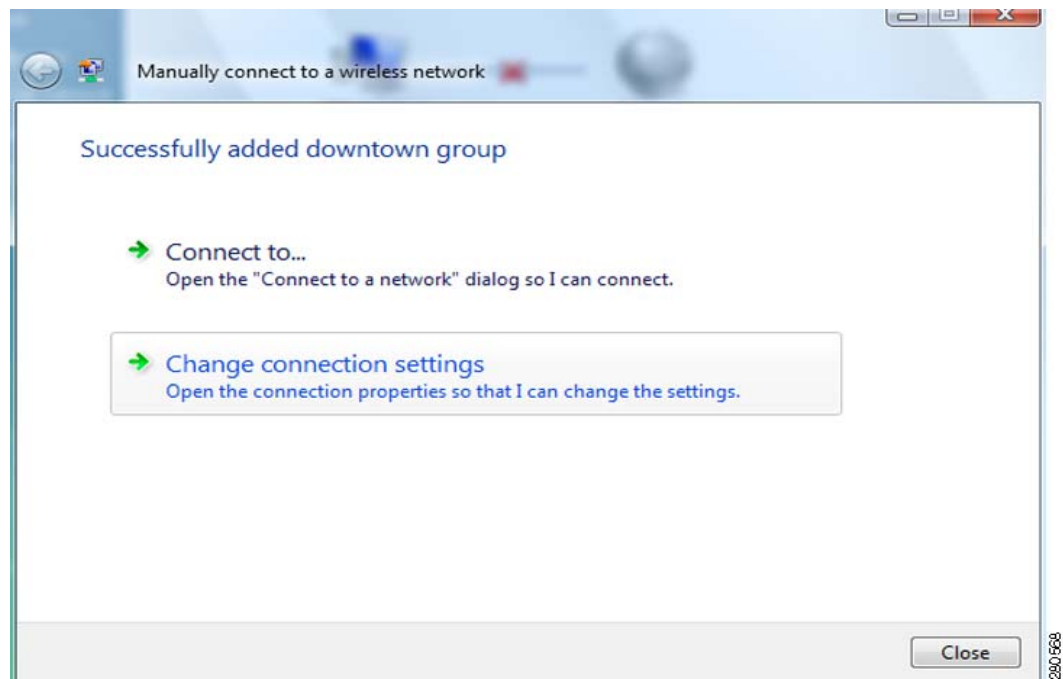
Table 2-1 Profile Management General Settings (continued)

Setting	What to Enter
Encryption type	<p>Encryption choices are determined by the security type that you choose. From the Encryption type drop-down list, choose an available method. The choices are the following:</p> <ul style="list-style-type: none"> • If you choose No authentication (Open), your encryption choice is None. • If you choose WEP, your only encryption choice is WEP. • If you choose WPA2-Personal, you can choose AES or TKIP. • If you choose WPA-Personal, you can choose AES or TKIP. • If you choose WPA2-Enterprise, your encryption choice is AES, TKIP, AES (MFP), or TKIP (MFP). • If you choose WPA-Enterprise, your encryption choice is AES or TKIP. • If you choose 802.1x, your only encryption choice is WEP. • If you choose CCKM, your encryption choices are WEP, AES, and TKIP. <p>For more information about these encryption types, see the “Security and Encryption Types” section on page 2-10.</p> <p>Default: The default that appear in the Encryption type drop-down list is determined by what you selected in the Security type drop-down list.</p>
Security Key/Passphrase	<ul style="list-style-type: none"> • If you choose No authentication (Open), a Security Key/Passphrase is not necessary. • If you choose the WEP security type, enter the WEP key. • If you choose the WPA2-Personal security type, enter the WPA2 preshared key. • If you choose the WPA-Personal security type, enter the WPA preshared key. • For the WPA2-Enterprise and WPA-Enterprise security types, see Chapter 3, “Configuring EAP Types.” The enterprise network EAP type determines the credentials that the client adapter must use for authentication. • If you choose the 802.1x security type, a Security Key/Passphrase is not necessary. <p>Note Contact the wireless network administrator for the network WEP key, the WPA2-Personal preshared key, or the WPA-Personal preshared key.</p>
Display characters	<p>Check this check box if you want to view the characters that you enter into the Security Key/Passphrase field. If you do not check this check box, the key or passphrase that you enter appears as black dots.</p> <p>Default: Not checked.</p>

Table 2-1 Profile Management General Settings (continued)

Setting	What to Enter
Start this connection automatically	Check this check box if you want the device to connect automatically whenever the wireless network is in range. If you do not check this check box, you must manually connect to this wireless network from the Connect to a network dialog box, which you can access through the Network and Sharing Center. Default: For the No authentication (Open) security type, this check box is unchecked. For all other security types, this check box is checked.
Connect even if the network is not broadcasting	Check this check box if you want the device to attempt to connect even if the wireless network is not broadcasting its name. Default: Not checked.

Step 8 After you enter all required settings, click **Next**. Another Manually connect to a wireless network dialog box appears (see [Figure 2-6](#)).

Figure 2-6 Manually connect to a wireless network Dialog Box—Successfully added <network name>

Step 9 Click **Connect to** to connect to a wireless network, including the one for which you have created a profile. Or click **Change connection settings** to change the profile settings. See the “[Viewing and Changing the Settings of a Profile](#)” section on page 2-13 for more information.

Security and Encryption Types

The dialog box in [Figure 2-5](#) includes the settings that allow you to configure how the client adapter associates to an access point, authenticates to a wireless network, and encrypts and decrypts data. The following sections provide explanations of options that are available in the Security type drop-down list, the Encryption type drop-down list, and the Security Key/Passphrase field of this dialog box.

WEP (Shared) Security with Static WEP Keys

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 client adapter. Static WEP keys are either 40 or 128 bits in length. 128-bit WEP keys offer more security than 40-bit WEP keys.

Each profile can be assigned a static WEP keys. If the 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 the static WEP key each time the client adapter is inserted or the Windows device is rebooted because the key is stored (in an encrypted format for security reasons) in the Windows profile store.

You can obtain a static WEP key from your network administrator.

**Note**

WEP encryption is not considered safe enough for today's wireless networks. We do not recommend that you use it in enterprise wireless networks.

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 and WPA2 can use Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection or 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.

- WPA2-Personal—WPA2 authentication with a preshared key. WPA2-Personal is suitable for environments without a Remote Authentication Dial-In User Service (RADIUS) infrastructure (for example, a small office or home office network). WPA2-Personal supports the use of a preshared key (PSK). Obtain the preshared key from your system administrator. When you choose WPA2-Personal as your security type, your encryption type is TKIP or AES.
- WPA-Personal—WPA with a preshared key. Like WPA2-Personal, WPA-Personal is suitable for environments without a RADIUS infrastructure. Obtain the preshared key from your system administrator. When you choose WPA-Personal as your security type, your encryption type is TKIP or AES.
- WPA2-Enterprise—WPA2-Enterprise requires authentication in two phases: the first is an open system authentication, and the second uses 802.1X with an Extensible Authentication Protocol (EAP) authentication method. See chapter [Chapter 3, “Configuring EAP Types,”](#) for more information about supported EAP methods. When you choose WPA2-Enterprise as your security type, your encryption type is TKIP or AES.
- WPA-Enterprise—WPA-Enterprise also uses 802.1X authentication and is designed for medium and large infrastructure mode networks. See chapter for more information about supported EAP methods. When you choose WPA-Enterprise as you security type, your encryption type is TKIP or AES.

802.1X 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.

Dynamic WEP keys are created as part of the EAP authentication process. Dynamic WEP keys with EAP offer a higher degree of security than static WEP keys.

When you choose the 802.1X with WEP encryption, you can configure the profile to use five different authentication methods of dynamic WEP key creation:

- Smart Card or other certificate—for more information about smart cards and other certification authentication, go to the Microsoft site:
<http://technet2.microsoft.com/windowsserver/en/library/7c6b414a-80c7-4bc1-b952-6eca6585dff91033.msp?mfr=true>
- Protected EAP (PEAP)
- LEAP
- PEAP-GTC
- EAP-FAST



Note

For more information about EAP authentication methods, see [Chapter 3, “Configuring EAP Types.”](#)

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.

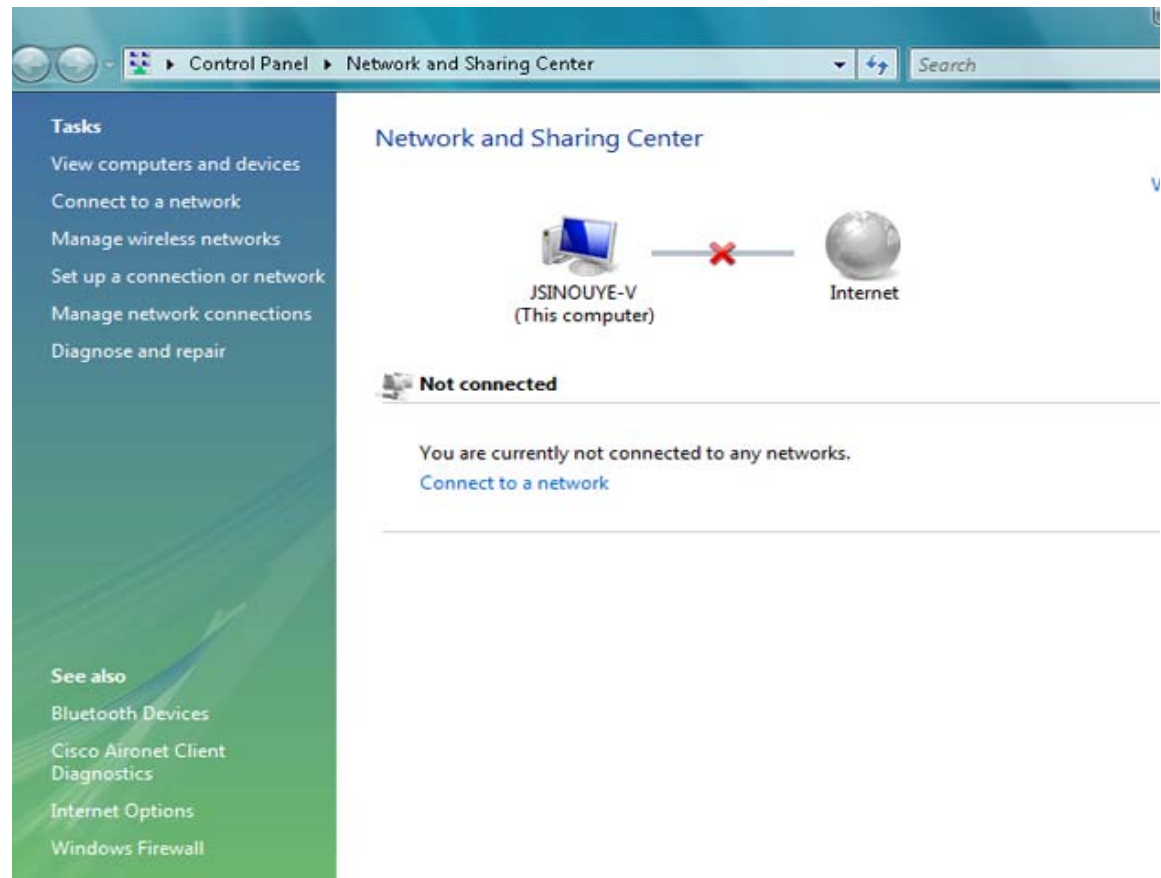
During normal operation, EAP-enabled clients mutually authenticate with a new access point by performing a complete EAP authentication, including communication with the main RADIUS server. However, when you configure your wireless LAN for CCKM fast secure roaming, EAP-enabled clients securely roam from 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.

Accessing a Profile That Was Created Previously

After you have created a profile and configured its basic settings (see the [“Creating a New Profile and Configuring Basic Settings”](#) section on page 2-3), you can change the settings by accessing the properties of the profile.

To access the profile, follow these steps:

-
- Step 1** Open the Network and Sharing Center (see the [“Accessing Microsoft Vista Network and Sharing Center”](#) section on page 2-2).
 - Step 2** In the Network and Sharing window (see [Figure 2-7](#)), click **Manage wireless networks** in the Tasks area.

Figure 2-7 Network and Sharing Center Window

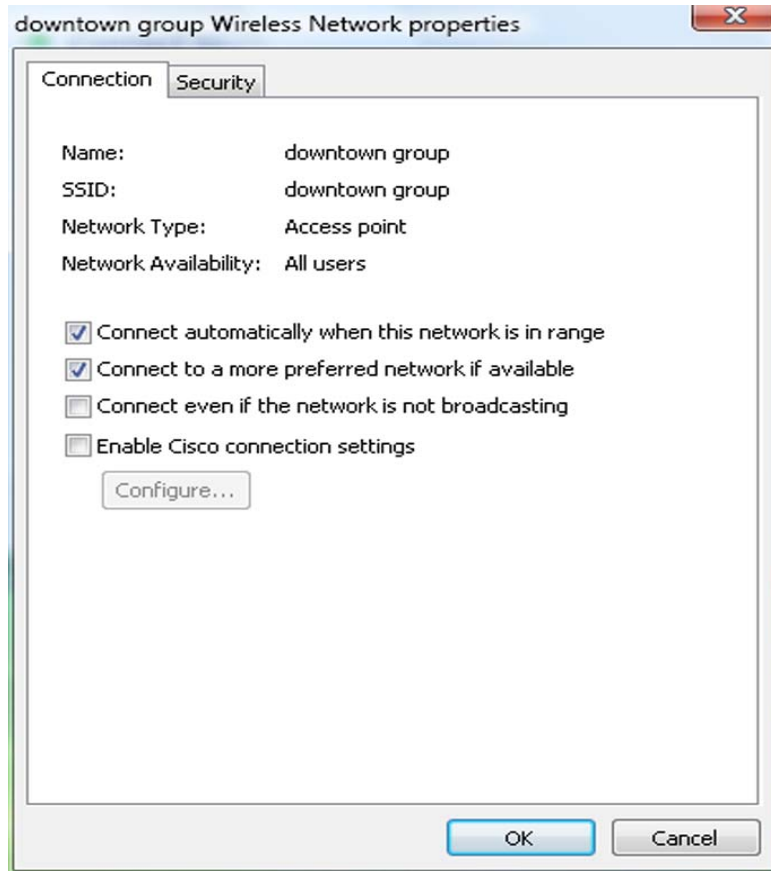
- Step 3** In the Manage wireless networks window that appears, double-click the profile that contains the settings that you want to change. A Wireless Network properties dialog box appears (see [Figure 2-8](#)). See the “[Viewing and Changing the Settings of a Profile](#)” section on page 2-13 for information about modifying the profile that you have selected.

Viewing and Changing the Settings of a Profile

To access a profile whose settings you want to view or change, follow the procedure in the “[Accessing a Profile That Was Created Previously](#)” section on page 2-12. To view or change the settings of a profile, follow these steps:

- Step 1** In the Connection tab of the Wireless Network properties dialog box (see [Figure 2-8](#)), view the wireless network's Name, SSID (service set identifier), Network Type (for example, Access point for an infrastructure-mode network), and the Network Availability (specifies the availability for types of users). You cannot change these settings in this dialog box.

Figure 2-8 Wireless Network properties Dialog Box—Connection Tab



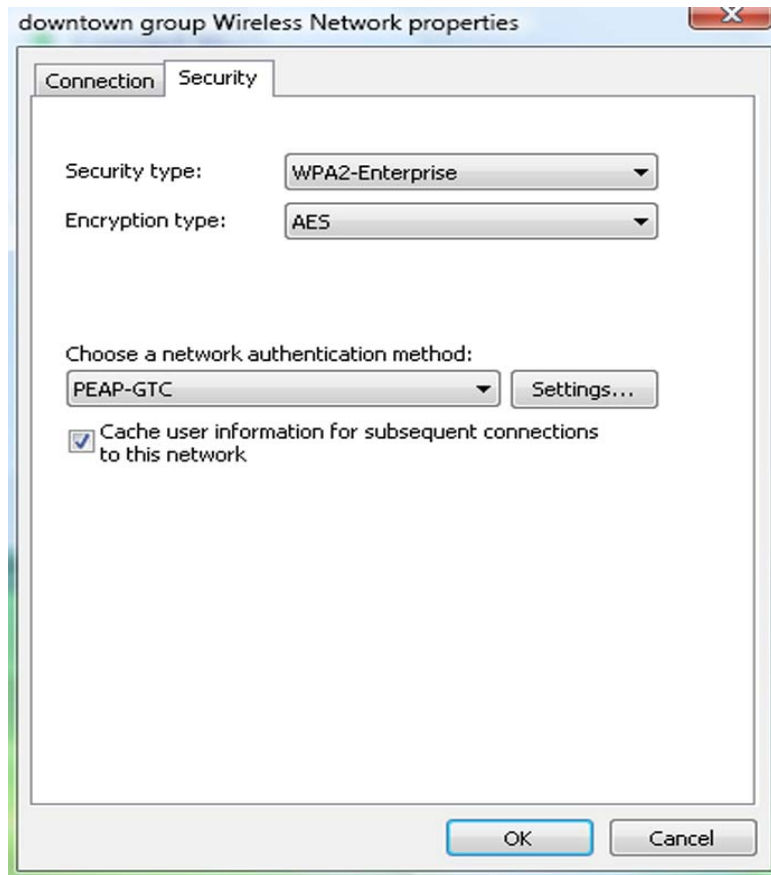
- Step 2** In the Connection tab, check or uncheck the check boxes that are available. [Table 2-2](#) lists and describes these check boxes. Follow the instructions in the table to configure these settings.

Table 2-2 Profile Management General Settings

Setting	What to Enter
Connect automatically when this network is in range	<p>Check this check box if you want the device to connect automatically whenever the wireless network is in range. If you do not check this check box, you must manually connect to this wireless network from the Connect to a network dialog box, which you can access through the Network and Sharing Center.</p> <p>Note You configured this setting when you first created the wireless profile. See the Start this connection automatically check box in Table 2-1 on page 2-7.</p>
Connect to a more preferred network if available.	<p>Check this check box to connect to a wireless network that you prefer more than the wireless network specified in this profile. To designate the order in which your profiles connect when more than one network is available, Choose Control Panel > Manage Wireless Networks. You can order your wireless profiles in this window.</p>
Connect even if the network is not broadcasting	<p>Check this check box if you want the device to attempt to connect even if the wireless network is not broadcasting its name.</p> <p>Note You configured this setting when you first created the wireless profile. See the Connect even if the network is not broadcasting check box in Table 2-1 on page 2-7.</p>
Enable Cisco connection settings	<p>Check this check box to view, configure, and enable Radio Measurement and Advanced Roaming. When you check the Enable Cisco connection settings check box, the Configure button is no longer dimmed. Click on the Configure Button to open the Cisco Connection Settings dialog box. See the “Radio Measurement” section on page 2-18 and the “Advanced Roaming Setting” section on page 2-19 for more information about these Cisco connection settings.</p>

Step 3 Click the **Security** tab to change security settings. The security settings on the Security tab appear (see [Figure 2-9](#)).

Figure 2-9 Wireless Network properties Dialog Box—Security Tab



- Step 4** In this dialog box, configure security settings that are available for this profile. [Table 2-3](#) lists and describes security settings. Follow the instructions in the table to configure these settings.

Table 2-3 Profile Management General Settings

Setting	What to Enter
Security type	<p>From Security type drop-down list, choose the method that is used to authenticate a connection to the wireless network. The choices are the following:</p> <ul style="list-style-type: none"> • No authentication (Open) • Shared • WPA2-Personal • WPA-Personal • WPA2-Enterprise • WPA-Enterprise • 802.1X • CCKM
Encryption type	<p>Encryption choices are determined by the security type that you choose. From the Encryption type drop-down list, choose an available method. The choices are the following:</p> <ul style="list-style-type: none"> • If you choose No authentication (Open), your encryption choice is None or WEP. • If you choose Shared, your only encryption choice is WEP. • If you choose WPA2-Personal you can choose AES or TKIP. • If you choose WPA-Personal, you can choose AES or TKIP. • If you choose, WPA2-Enterprise, you can choose AES, TKIP, AES (MFP), TKIP (MFP). • If you choose WPA-Enterprise, you can choose AES or TKIP. • If you choose 802.1x, your only encryption choice is WEP. • If you choose CCKM, you can choose AES, WEP, or TKIP.
Network security key	<p>Enter the network security key that you obtain from the network administrator.</p> <p>Note The Network security key field only appears when you choose No authentication (Open) with WEP encryption, Shared, WPA2-Personal, or WPA-Personal as the security type.</p>

Table 2-3 Profile Management General Settings (continued)

Setting	What to Enter
Choose a network authentication method	<p>From the Choose a network authentication method drop-down list, choose an authentication method. The choices are the following:</p> <ul style="list-style-type: none"> • Smart Card or other certificate • Protected EAP (PEAP) • LEAP • PEAP-GTC • EAP-FAST <p>Note Smart Card and Protected EAP (PEAP) are provided by Microsoft. These methods were not tested by Cisco on the CB21AG or the PI21AG client adapter.</p> <p>Note The Choose a network authentication method drop-down list appears only when you choose WPA2-Enterprise, WPA-Enterprise, 802.1X, or CCKM as the security type.</p> <p>Note After you choose the network authentication method, click the Settings button to configure the authentication methods. For more information about the authentication method settings, see the EAP-FAST, PEAP-GTC, and LEAP administrator guides.</p>
Cache user information for subsequent connections to this network	<p>Check this check box if you want user information stored for later connections through this profile to the network.</p> <p>Note The Cache user information for subsequent connections to this network check box appears only when you choose WPA2-Enterprise, WPA-Enterprise, 802.1X, or CCKM as the security type. These security types rely on a network authentication method that requires user credentials.</p>

Radio Measurement

You can enable or disable the radio measurement feature in the Cisco Connection Settings dialog box, which is available from the profile's Connection tab in the Wireless Network properties dialog box (see [Step 2](#) in the “[Viewing and Changing the Settings of a Profile](#)” section on page 2-13 to get to the Cisco Connection Settings dialog box).

When you check the **Enable Radio Measurement** check box, the radio measurement feature is enabled. The client driver advertises support for the Cisco wireless LAN radio measurement feature by including a radio measurement information element when the client associates with the access point. The client can then service radio measurement requests that the network infrastructure sends.

When you uncheck the **Enable Radio Measurement** check box, the client does not advertise the radio measurement information element. The client cannot service radio measurement requests that the network infrastructure sends.

Advanced Roaming Setting

You can enable or disable the advanced roaming feature in the Cisco Connection Settings dialog box, which is available from the profile's Connection tab in the Wireless Network properties dialog box (see [Step 2](#) in the “[Viewing and Changing the Settings of a Profile](#)” section on page 2-13 to get to the Cisco Connection Settings dialog box).

Check the **Enable Advanced Roaming Setting** check box to enable the advanced roaming feature. Uncheck the check box to disable the feature.

You can choose from five roaming policies to meet the needs of your wireless network. The roaming policy is the level of aggressiveness for roaming. From the Roaming Option drop-down list, choose roaming policy:

- **Very Low**—Roaming aggressiveness is very low. The client maintains connection with the current access point until its RSSI and transmit rate drop to the values where it may lose connection. The client roams to another access point only when it might lose connection with the current access point. This roaming policy prioritizes connection to the current AP rather than performance. This policy is best suited for environments in which only one access point is present.
- **Low**—Roaming aggressiveness is low. The client maintains connection with the current access point until its RSSI and transmit rate drop to values where performance is heavily degraded. This policy is best suited for environments in which access points are distributed sparsely.
- **Normal**—Roaming aggressiveness is normal. The client maintains connection with the current access point until its RSSI and transmit rate drop to values where performance is degraded. This policy gives balanced priorities to roaming aggressiveness and performance.
- **High**—Roaming aggressiveness is high. The RSSI and rate thresholds are set to high values to increase the aggressiveness of roaming. This policy is best suited for environments in which many access points are closely distributed and in which the user moves around at a faster pace.
- **Very High**—Roaming aggressiveness is very high. The RSSI and rate thresholds are set to values that give the best performance. This policy is best suited for environments in which multiple access points are present and in which the user can switch to the best performing access points at any time.
- **Default**—The default roaming policy is Normal. This roaming policy is set in the client driver.



CHAPTER 3

Configuring EAP Types

This chapter explains the EAP types that are used for authentication to wireless networks.

The following topics are covered:

- [Overview of EAP-FAST, page 3-1](#)
- [How EAP-FAST Works, page 3-2](#)
- [Configuring EAP-FAST, page 3-4](#)
- [Overview of LEAP, page 3-17](#)
- [How LEAP Works, page 3-17](#)
- [Configuring LEAP, page 3-18](#)
- [Overview of PEAP-GTC, page 3-21](#)
- [How PEAP-GTC Works, page 3-22](#)
- [Configuring PEAP-GTC, page 3-23](#)

Overview of EAP-FAST



Note

For additional information about EAP-FAST, see RFC4851.

EAP-FAST is an EAP method that enables secure communication between a client and an authentication server by using Transport Layer Security (TLS) to establish a mutually authenticated tunnel. Within the tunnel, data in the form of type, length, and value (TLV) objects are used to send further authentication-related data between the client and the authentication server.

EAP-FAST supports the TLS extension as defined in RFC 4507 to support the fast re-establishment of the secure tunnel without having to maintain per-session state on the server. EAP-FAST-based mechanisms are defined to provision the credentials for the TLS extension. These credentials are called Protected Access Credentials (PACs).

EAP-FAST provides the following:

- Mutual authentication
 - An EAP server must be able to verify the identity and authenticity of the client, and the client must be able to verify the authenticity of the EAP server.
- Immunity to passive dictionary attacks

Many authentication protocols require a password to be explicitly provided (either as cleartext or hashed) by the client to the EAP server. The communication of the weak credential (such as a password) must be immune from eavesdropping.

- Immunity to man-in-the-middle (MitM) attacks

In establishing a mutually authenticated protected tunnel, the protocol must prevent adversaries from successfully interjecting information into the communication between the client and the EAP server.

- Flexibility to enable support for most password authentication interfaces

Many different password interfaces exist to authenticate a client—for example, Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), Lightweight Directory Access Protocol (LDAP), and One-Time Password (OTP). EAP-FAST provides support for these different password types.

- Efficiency in computational and power resources

Especially when using wireless media, clients have limited computational and power resources. EAP-FAST enables network access communication to occur in a more efficient manner.

- Flexibility to extend the communications inside the tunnel

Because network infrastructures are becoming increasingly complex, authentication, authorization, and accounting is also becoming more complex. For example, there are instances in which multiple existing authentication protocols are required to achieve mutual authentication. Also, different protected conversations might be required to achieve the proper authorization when a client has successfully authenticated.

- Minimize authentication server requirements for per-user authentication

With large deployments, it is typical to have several servers that act as authentication servers for several clients. A client uses the same shared secret to secure a tunnel in much the same way that it uses a username and password to gain access to the network. EAP-FAST facilitates the use of a single strong shared secret by the client, while enabling the authentication servers to minimize the per-user and device state that they must cache and manage.

How EAP-FAST Works

The following sections describe how EAP-FAST works:

- [Two-Phase Tunneled Authentication, page 3-2](#)
- [Protected Access Credentials, page 3-3](#)
- [Server Certificate Validation, page 3-3](#)

Two-Phase Tunneled Authentication

EAP-FAST uses a two-phase tunneled authentication process.

In the first phase of authentication, EAP-FAST employs the TLS handshake to provide an authenticated key exchange and to establish a protected tunnel between the client and the authentication server. The tunnel protects client identity information from disclosure outside the tunnel. During this phase, the client and the server engage in EAP-FAST version negotiation to ensure that they are using a compatible version of the protocol.

After the tunnel is established, the second phase of authentication begins. The client and server communicate further to establish the required authentication and authorization policies. This phase consists of a series of requests and responses that are encapsulated in TLV objects. The TLV exchange includes the EAP method to be used within the protected tunnel. For more information about TLV objects and format, see section 4.2 of RFC 4851.

The EAP-FAST module offers a variety of EAP-FAST configuration options, including whether automatic or manual PAC provisioning is used to establish a tunnel, whether or not server certificate is used to establish a tunnel, what type of user credentials to use for authentication and provisioning, and what type of authentication method to use to in the established tunnel.

Protected Access Credentials

Protected Access Credentials (PACs) are credentials that are distributed to clients for optimized network authentication. PACs can be used to establish an authentication tunnel between the client and the authentication server (the first phase of authentication as described in the [“Two-Phase Tunneled Authentication” section on page 3-2](#)). A PAC consists of, at most, three components: a shared secret, an opaque element, and other information.

The shared secret component contains the pre-shared key between the client and authentication server. Called the PAC-Key, this pre-shared key establishes the tunnel in the first phase of authentication.

The opaque component is provided to the client and is presented to the authentication server when the client wants to obtain access to network resources. Called the PAC-Opaque, this component is a variable length field that is sent to the authentication server during tunnel establishment. The EAP server interprets the PAC-Opaque to obtain the required information to validate the client's identity and authentication. The PAC-Opaque includes the PAC-Key and may contain the PAC's client identity.

The PAC might contain other information. Called PAC-Info, this component is a variable length field that is used to provide, at a minimum, the authority identity of the PAC issuer (the server that created the PAC). Other useful but not mandatory information, such as the PAC-Key lifetime, can also be conveyed by the PAC-issuing server to the client during PAC provisioning or refreshment.

PACs are created and issued by a PAC authority, such as Cisco Secure ACS, and are identified by an ID. A user obtains his or her own copy of a PAC from a server, and the ID links the PAC to a profile.

Persistent PACs, such as machine PACs, are stored in the EAP-FAST registry and encrypted. These PACs are also protected with access control lists (ACLs) so only designated users (the owners of the PACs) and members of privileged user groups (for example, administrators) can access them. Machine PACs are stored globally so that all users of a machine can use the PACs.

All PACs are encrypted and tied to the host machine with Microsoft Crypto API (CryptoProtectData). PACs cannot be copied and used on other machines.

All non-persistent PACs, such as User Authorization PACs, are stored in volatile memory and do not persist after reboot or after a user has logged off.

Server Certificate Validation

As a part of TLS negotiation in the first phase of EAP-FAST authentication, the authentication server presents the client with a certificate. The client must verify the validity of the EAP server certificate and also examines the EAP server name that is presented in order to determine if the server can be trusted.

Configuring EAP-FAST

This section explains how to configure EAP-FAST module settings, such as connection settings, user credentials, and authentication methods. The following topics are covered:

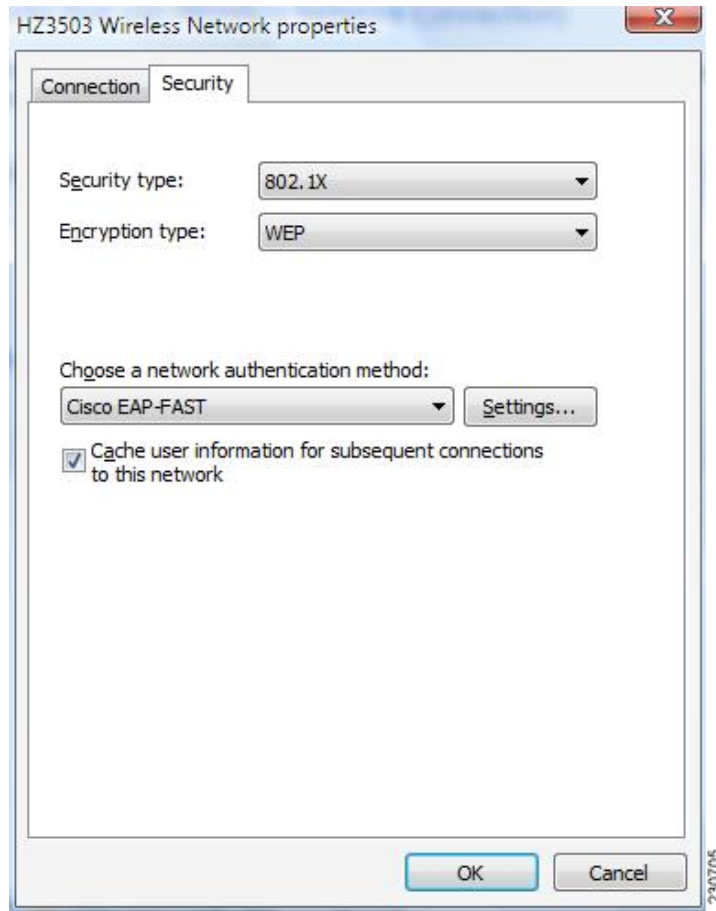
- [Accessing EAP-FAST Properties for Configuration, page 3-4](#)
- [Configuring EAP-FAST Settings in the Connection Tab, page 3-5](#)
- [Configuring EAP-FAST Settings in the User Credentials Tab, page 3-10](#)
- [Configuring EAP-FAST Settings in the Authentication Tab, page 3-13](#)
- [Finding the Version of the EAP-FAST Module, page 3-16](#)

Accessing EAP-FAST Properties for Configuration

To access the EAP-FAST Properties window, perform the following steps:

-
- Step 1** Click the **Start** button on the lower-left corner of the desktop.
 - Step 2** From the right pane, right-click **Network**.
 - Step 3** Select **Properties**.
 - Step 4** From the left pane, select **Manage wireless networks**.
 - Step 5** Double-click the wireless network.
 - Step 6** From the **Wireless Network properties** window, select the **Security** tab (see [Figure 3-1](#)).

Figure 3-1 Wireless Network Properties Window



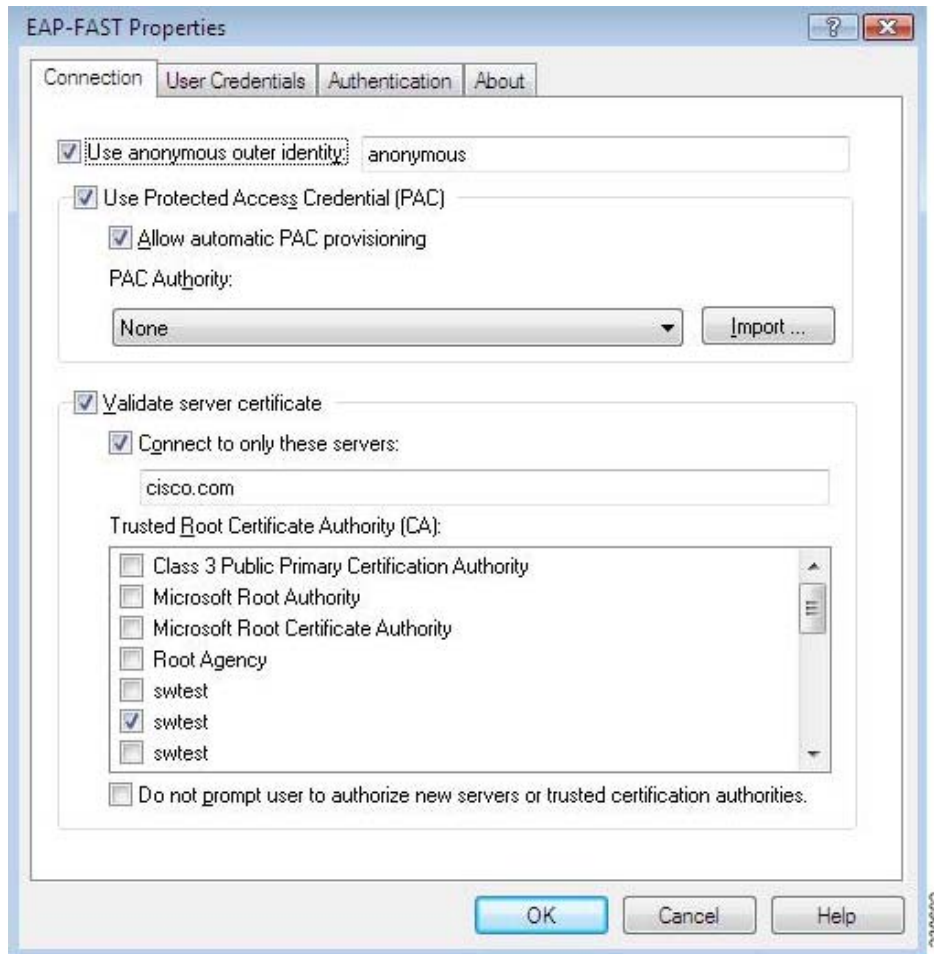
- Step 7** Select **Cisco EAP-FAST** from the "Choose a network authentication method" drop down list.
- Step 8** Click the **Settings** button.
- Step 9** Click the **Connection** tab, the **User Credentials** tab, the **Authentication** tab, or the **About** tab. For more information about configuring settings in those tabs, see the [“Configuring EAP-FAST Settings in the Connection Tab”](#) section on page 3-5, the [“Configuring EAP-FAST Settings in the User Credentials Tab”](#) section on page 3-10, and the [“Configuring EAP-FAST Settings in the Authentication Tab”](#) section on page 3-13. For information about finding the version of the module on the device, see the [“Finding the Version of the EAP-FAST Module”](#) section on page 3-16.

Configuring EAP-FAST Settings in the Connection Tab

The EAP-FAST Connection tab includes settings for the establishment of an outer Transport Layer Security (TLS) tunnel. Settings include identity protection, the use of a Protected Access Credential (PAC), PAC provisioning, the use of authenticated server certificates to establish the tunnel, and the use of a Trusted Root Certificate Authority (CA) from a list of Trusted Root CA certificates.

You can configure connection settings from the Connection tab (see [Figure 3-2](#)).

Figure 3-2 Connection Tab in EAP-FAST Properties Window



[Table 3-2](#) lists and describes all connection settings.

Table 3-1 Connection Settings

Connection Settings	Description
Use anonymous outer identity	Check this box to enable identity privacy protection. Default: On
Outer identity field	Enter an outer identity if the Use anonymous outer identity check box is checked. Follow an administrator's instructions, or follow RFC 4282 for guidelines about what to enter in the outer identity field. Default: anonymous Note The maximum number of characters allowed in this field is 256.

Table 3-1 Connection Settings (continued)

Connection Settings	Description
Use Protected Access Credential (PAC)	<p>Check this box to enable the use of a PAC to establish a tunnel. When this box is checked, PAC provisioning is requested. If this box is not checked, EAP-FAST acts as PEAP and uses only the authenticated server certificate to establish the tunnel every time.</p> <p>The PAC is a unique shared credential used to mutually authenticate a client and a server. The PAC is associated with a specific client username and a server authority ID. A PAC removes the need for PKI and digital certificates. The PAC is distributed or imported to the client automatically or manually.</p> <p>Manual PAC provisioning generates the PAC file locally on the AAA or EAP-FAST server. With manual provisioning, the user credentials are supplied to the server to generate the PAC file for that user. This PAC must then be manually installed on the client device.</p> <p>Default: On</p>
Allow automatic PAC provisioning	<p>Check this box to enable the automatic retrieval of a PAC during EAP-FAST authentication.</p> <p>Automatic PAC provisioning enables the automatic retrieval of a PAC during EAP-FAST authentication. Automatic PAC provisioning uses TLS with a Diffie-Hellman Key Agreement protocol to establish a secure tunnel. In addition, MSCHAPv2 is used to authenticate the client and for early man-in-the-middle (MITM) attack detection.</p> <p>Default: On</p>
PAC Authority	<p>Select a PAC authority from the drop-down list.</p> <p>Default: None</p> <p>Note The drop-down list contains the names of all of the PAC authorities from which you have previously provisioned a tunnel PAC. If you have not provisioned a PAC, then "none" is the only option. You can also select "none" to force the host to request provisioning a PAC.</p>
Import	<p>Click the Import button to manually import a PAC file. When you click on this button, the Import Protected Access Credentials (PAC) File window appears. If you need to enter a password for the PAC file that you have selected, a password window will appear.</p> <p>After you have selected and imported a valid PAC file, the PAC authority is added to the PAC authority drop-down list.</p> <p>Default: Enabled</p>

Table 3-1 Connection Settings (continued)

Connection Settings	Description
Validate server certificate	<p>Check this box to use an authenticated server certificate to establish a tunnel. You can check both the Use Protected Access Credentials (PAC) box and the Validate Server Certificate box at the same time. If both are checked, you can select one or more Trusted Root CA certificates from the list of trusted Certificate Authority certificates that are installed on the host system.</p> <p>The EAP-FAST module always tries to use the PAC first if both check boxes are checked. The module uses the server certificate if the PAC is missing or rejected by the server.</p> <p>If both check boxes are unchecked, EAP-FAST functions as PEAP does without validating server certificate. We do not recommend leaving both boxes unchecked because the module bypasses fundamental trust validation.</p> <p>Default: Off</p>
Connect to only these servers	<p>Check this box to enter an optional server name that must match the server certificate that is presented by the server. You can enter multiple server names; separate multiple server names with semicolons. The EAP-FAST module only allows connections to continue without prompting if the subject field (CN) in the server certificate matches the server names that you enter in this field.</p> <p>Default: Off</p> <p>Note You can use an asterisk (*) as a wildcard character in server names only if the asterisk appears before the first period (.) in the name.domain.com format. For example, "*.cisco.com" matches any server name that ends with ".cisco.com." If you put an asterisk anywhere else in the server name, it is not treated as a wildcard character.</p>
Trusted Root CA	<p>Select one of more Trusted Root CA certificates from the list of certificates that are installed on the system. Only trusted CA certificates that are installed on the host system are displayed in the drop-down list.</p> <p>To view details about the selected Trusted Root CA certificate, double-click the certificate name. Double-clicking the certificate name opens the Windows certificate property screen, where certificate details are available.</p> <p>Default: None</p>
Do not prompt user to authorize new servers or trusted certificate authorities.	<p>Check this box if you do not want the user to be prompted to authorize a connection when the server name does not match or the server certificate is not signed by one of the Trusted Root CA certificates that was selected. If this box is checked, the authentication fails.</p> <p>Default: Off</p>

Overview of the User Credentials Tab

The EAP-FAST module supports the use of both a client certificate and a username and password as user credentials for authentication and provisioning.

Client Certificates

If a client certificate is used, the EAP-FAST module automatically obtains the client certificate from the Windows certificate store of the current user. The EAP-FAST module finds the user certificate that matches the username of the user who is logged on. The certificate cannot be expired.

If multiple user certificates are available, the EAP-FAST module prompts the user to select one, and that selection is saved to the profile. By default, the user certificate is sent securely through TLS renegotiation or through the EAP-TLS inner method in the protected TLS tunnel. If the EAP-FAST server does not start TLS renegotiation to request the client certificate after the tunnel is established, then the EAP-FAST module sends the certificate through the EAP-TLS inner method.

The EAP-FAST module administrator can configure the EAP-FAST module XML schema to send the user certificate without using these security measures.

Usernames and Passwords

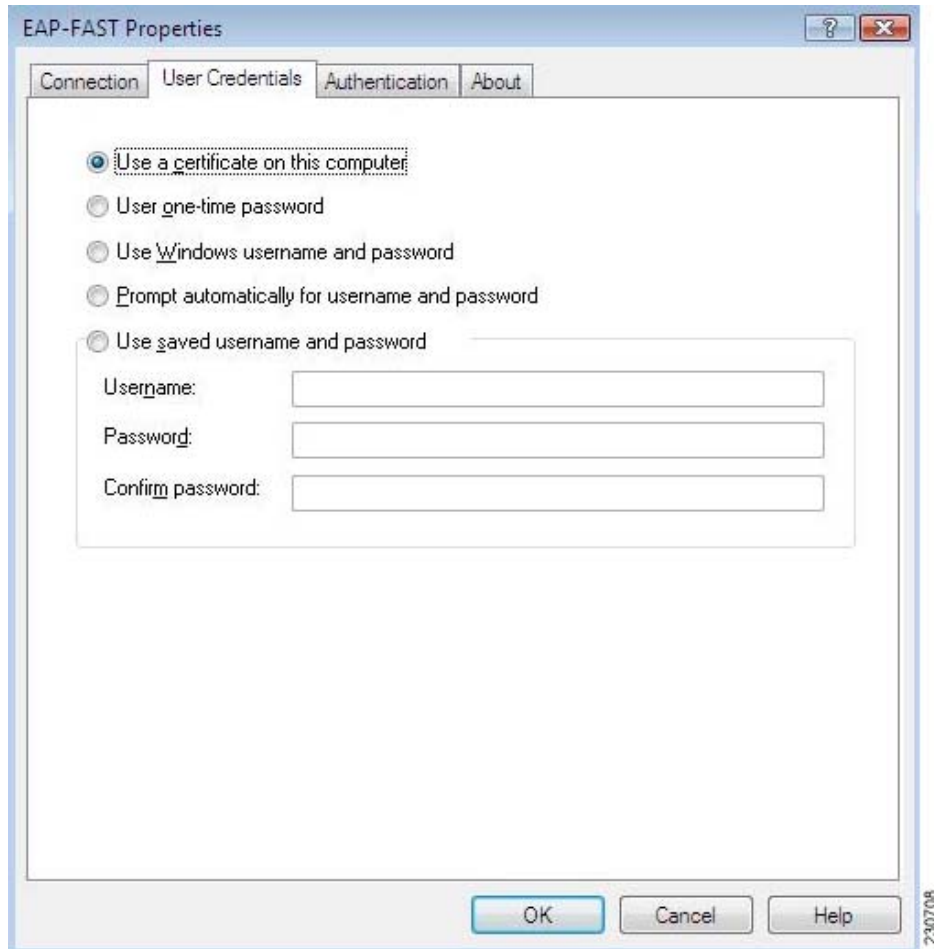
If a username and password are used, the user provide one of the following types of username and password:

- Windows username and password—The Windows username and password are used as network access credentials. The user is not prompted to enter the username and password unless the password is invalid or must be changed.
- Prompted user credentials—The user is prompted during authentication for credentials. These credentials are credentials that are separate from the Windows username and password, such as Lightweight Directory Access Protocol (LDAP) credentials.
- Saved user credentials—These are user credentials that are entered as part of the EAP-FAST configuration. The user is not prompted for credentials during authentication unless the saved credentials fail or have expired. New credentials that the user enters after successful authentication are saved automatically in the configuration. The user does not have to return to the configuration screen to change the old saved credentials.
- One-time password (OTP)—The user must manually enter a OTP. New PIN mode and next token mode for OTP are supported.

Configuring EAP-FAST Settings in the User Credentials Tab

The user can configure user credentials from the User Credentials tab (see [Figure 3-3](#)).

Figure 3-3 User Credentials Tab in EAP-FAST Properties Window



[Table 3-2](#) lists and describes all options for user credentials.

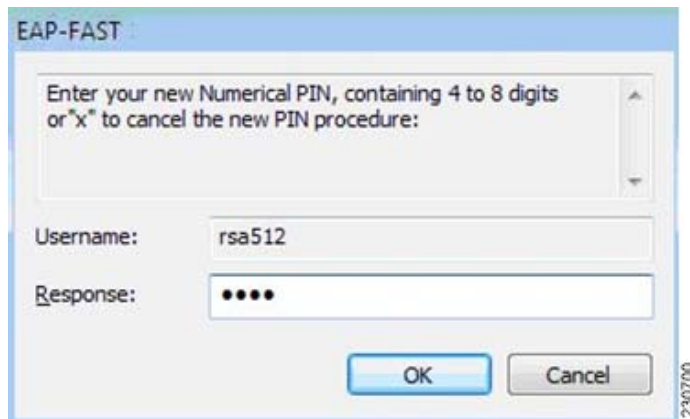
Table 3-2 **User Credentials Options**

User Credentials	Description
Use a certificate on this computer	Click this radio button to automatically obtain the client certificate from the Windows certificate store of the current user. Default: Off
Use one-time password	Click this radio button to use a one-time password (OTP). For more information about OTP, see the “Understanding PIN Mode and Token Mode with OTP” section on page 3-12. Default: Off
Use Windows username and password	Click this radio button to use the Windows username and password as the EAP-FAST username and password for network authentication. Default: On
Prompt automatically for username and password	Click this radio button to require the user to enter a separate EAP-FAST username and password in addition to a Windows username and password with every authentication attempt. This options supports non-Windows passwords, such as LDAP. Default: Off
Use saved username and password	Click this radio button so that the user is not required to enter an EAP-FAST username and password each time. Authentication occurs automatically as needed using a saved user name and password, which are registered with the backend server. Default: Off When selecting this option, the user must enter the following: <ul style="list-style-type: none"> • Username—Enter the username and the domain name in one of these two formats: <ul style="list-style-type: none"> – Domain-qualified user name—domain\user – User Principal Name (UPN)—user@domain.com • Password—Enter a password. This encrypted password is stored in the EAP-FAST configuration. • Confirm password—Enter the password again to verify that it was entered correctly. Note The maximum number of characters allowed for the username and password is 256.

Understanding PIN Mode and Token Mode with OTP

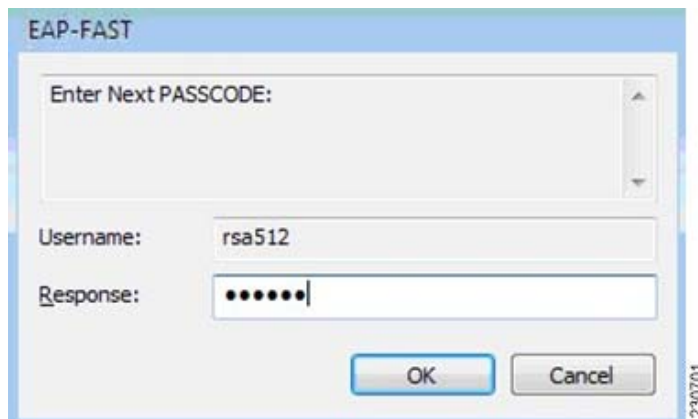
New PIN mode for OTP is supported. If a new PIN is needed, the backend server sends a text message (for example, “Enter New PIN”) to indicate that a new PIN is needed. The EAP-FAST module displays a prompt window that includes the text message from the server (see [Figure 3-4](#)). The backend server might prompt the user twice to confirm the new PIN that the user entered.

Figure 3-4 *New PIN Prompt Window*



Next Token mode for OTP is also supported. If the next token is needed, the backend server sends a text message (for example, “Enter Next PASSCODE:”) to indicate that the next token is needed. The EAP-FAST module displays a prompt window that includes the text message sent from the server (see [Figure 3-5](#)). The user must get the next token from the OTP device or from the software and enter it in the prompt field.

Figure 3-5 *Next Token Prompt Window*



Configuring EAP-FAST Settings in the Authentication Tab

The EAP-FAST module supports three authentication methods: EAP-GTC, EAP-MSCHAPv2, and EAP-TLS.

These three authentication methods use the following types of credentials:

- EAP-GTC—Active Directory password, OTP, Token, LDAP
- EAP-MSCHAPv2—Active Directory password
- EAP-TLS—certificate

The EAP-GTC module is bundled with the EAP-FAST module. The EAP-GTC module is not registered with the EAPHost framework; it is not available to other applications.

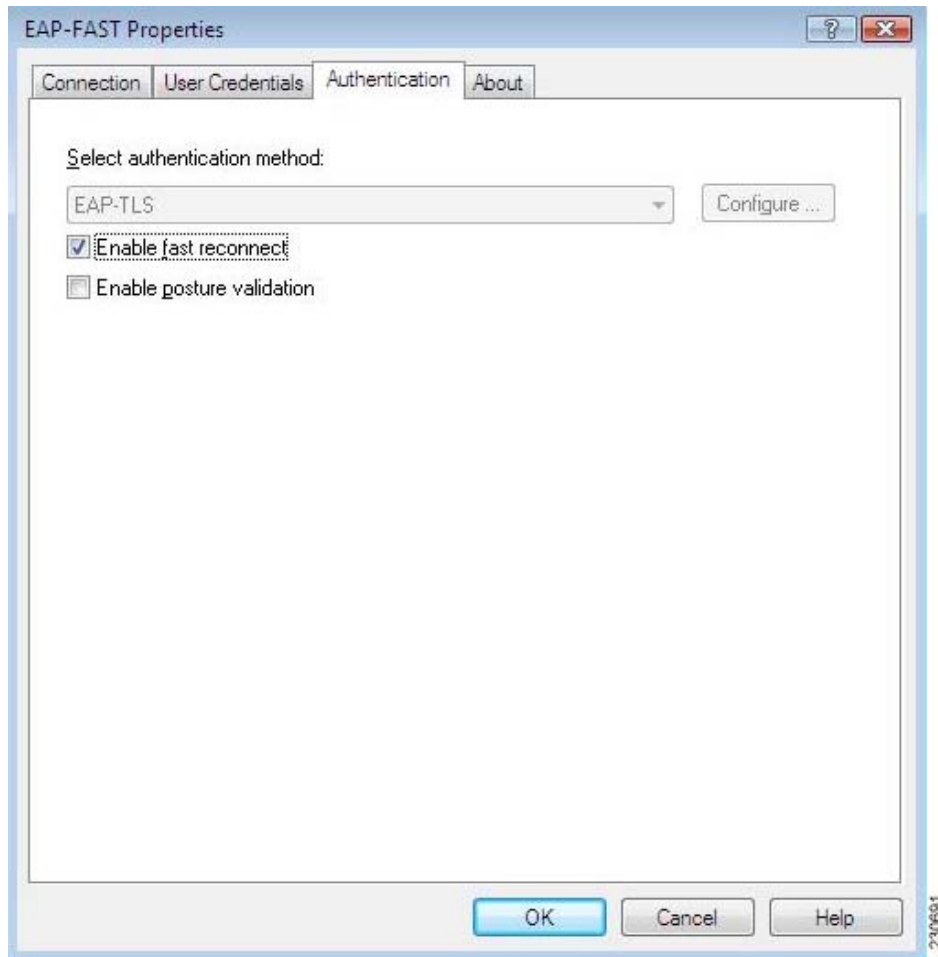
A modified version of the EAP-MSCHAPv2 module is also bundled with the EAP-FAST module. This modified version is used in anonymous TLS provisioning mode to support the modification of EAP-MSCHAPv2 challenges. This same module also supports user authentication in authentication mode without modification.

The EAP-FAST module uses the standard EAP-TLS module that is shipped with Windows Vista.

The user can select only one of these three inner authentication methods through the user interface. Although other third-party EAP methods are registered with the EAPHost framework and can be selected in the administrator interface, these methods have not been officially tested.


You can choose settings for authentication in the Authentication tab (see [Figure 3-6](#)).

Figure 3-6 Authentication Tab in EAP-FAST Properties Window



[Table 3-3](#) lists and describes options for authentication.

Table 3-3 Authentication Settings

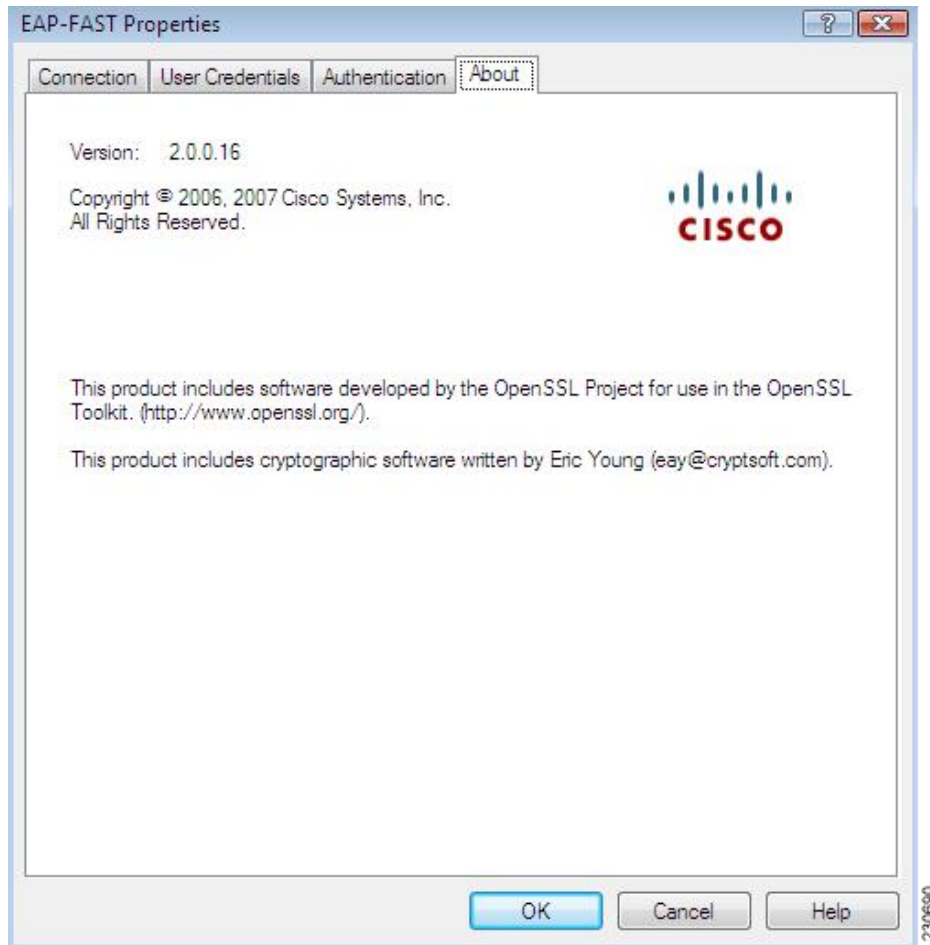
Authentication Settings	Description
Select an authentication method	<p>Select the inner tunnel EAP method from the drop-down list. Available methods are EAP-GTC, EAP-MSCHAPv2, EAP-TLS, and Any Method.</p> <p>The Any Method option allows the EAP-FAST module to choose any of the supported methods that the EAP server requests. The method must also be appropriate to the user credentials that are used.</p> <p>Default: Any Method</p> <p>Note EAP-GTC is the only option available if you selected the Use one-time password radio button in the User Credentials tab.</p> <p>Note EAP-TLS is the only option available if you selected the Use a certificate on this computer radio button in the User Credentials tab.</p> <hr/> <p> Note The use of the Any Method value to allow all methods is unsupported by Cisco or Microsoft and is not recommended. This configuration is used “as-is”; Cisco makes no guarantee that there will not be adverse performance to the system if unsupported methods are used. Unsupported methods should never be used in a production environment.</p>
Configure	<p>Click the Configure button to configure EAP-TLS options. This option is available only if EAP-TLS is the selected authentication method. When you click this button, the standard Windows Vista EAP-TLS Properties Screen appears.</p> <p>Default: Disabled</p>
Enable fast reconnect	<p>Check this box to allow session resumption.</p> <p>The EAP-FAST module supports fast reconnect (also called session resumption) by using the User Authorization PAC. When you enable fast reconnect, you can roam or return from suspend mode without re-entering your credentials. Fast reconnect can be used across different network access servers.</p> <p>Default: On</p> <p>Note If you switch profiles, logs off, or reboot, fast reconnect is not attempted. You must be reauthenticated.</p>
Enable posture validation	<p>Check this box to allow the health information of the host machine to be queried.</p>

Finding the Version of the EAP-FAST Module

Follow these steps to learn the current version of the EAP-FAST module on the device:

- Step 1** Access the EAP-FAST Properties window. The procedure for accessing this window is detailed in the “Accessing EAP-FAST Properties for Configuration” section on page 3-4.
- Step 2** Click the **About** tab (see Figure 3-7). The version number, copyright information, and open-source software information are in this tab.

Figure 3-7 About Tab in EAP-FAST Properties Window



Overview of LEAP

Cisco LEAP is an authentication protocol that is designed for use in IEEE 802.11 wireless local area networks (WLANs). Important features of LEAP include the following:

- Mutual authentication between the network infrastructure and the user.
- Secure derivation of random, user-specific cryptographic session keys.
- Compatibility with existing and widespread network authentication mechanisms (for example, RADIUS).
- Computational speed.

Although Cisco LEAP is a Cisco proprietary protocol, it is based on existing IETF and IEEE standards. Cisco LEAP relies on the following:

- Extensible Authentication Protocol (EAP)

EAP was originally designed to provide a framework so that new authentication methods could be introduced into Point-to-Point Protocol (PPP). Before EAP existed, entirely new PPP authentication protocols had to be defined to create new authentication methods. However, with EAP, new authentication types simply require the definition of a new EAP type. A new EAP type comprises a set of set of EAP request and response messages and their associated semantics.

- Extensible Authentication Protocol over LAN (EAPOL)

Although originally designed to operate as part of PPP, EAP is flexible enough to be mapped to most types of framed link layer. With a wireless access point, this link layer is a wireless LAN, not PPP. The IEEE 802.1X EAP over LAN (EAPOL) specifies a method for encapsulating EAP packets in Ethernet packets so that they can be transmitted over a LAN.

- Encryption and Key Exchange

The 802.11 specification allows for data traffic between the client and access point to be encrypted using an encryption key. As a result of key exchange through WPA, WPA2, CCKM, or WEP, the client and the network access device derive the same pair of keys—one key for broadcast and multicast traffic from the network access device and another key for all other packets.

- Remote Authentication Dial-In User Service (RADIUS) Servers

Network access servers (such as WLAN access points) often rely on a centralized AAA server to authenticate clients on their behalf. One of the more popular types of AAA servers is a RADIUS server. Extensions to the RADIUS protocol have been defined to allow the transfer of the EAP packets between the authentication server and the network access server. In this case, the network access server is a relay agent; the authentication conversation takes place between the client and the RADIUS server. The RADIUS server informs the access point of the result of the authentication and whether to allow the client to access the network. Other parameters might be returned as well, including session keys for use between the client and the access point.

How LEAP Works

Because most RADIUS servers support the MS Challenge Handshake Authentication Protocol (MS-CHAP), MS-CHAP is the basis for LEAP. The protocol consists of the authenticator sending a random challenge to client. The client's data encryption standard (DES) encrypts the challenge by using an MD4 hash of the password. The authenticator then verifies the response by using its knowledge of the client username and password.

During authentication, the access point acts as a transparent relay for the conversation between the client and the RADIUS server. The EAPOL header is removed from EAPOL packets that come from the client. The contents of the EAPOL packet are added as an EAP attribute to a RADIUS request packet and sent to the RADIUS server. RADIUS packets from the server have the EAP attribute contents added to an EAPOL packet and sent to the client. The access point never examines the contents of the EAP data.

When the client associates to an access point, the access point sends an EAP identity request to the client. The client responds with a username. The RADIUS server then formats a LEAP challenge EAP attribute. The client sends a LEAP challenge response back to the RADIUS server.

If the user is invalid, the RADIUS server sends a RADIUS access-deny message that contains an EAP failure attribute. If the user is valid, the server sends a RADIUS access-challenge packet with an EAP success attribute. The client responds with a LEAP challenge. The server responds with a RADIUS access-accept packet that contains an EAP attribute with the LEAP challenge response. This packet also contains a Cisco vendor-specific attribute that informs the access point of the value of the encryption key. The client verifies the challenge response. If the response is invalid, client disassociates and attempts to find another access point.

802.11 supports the use of up to four encryption keys for the traffic between a client and its access point. The access point uses one of the key indices for the session key. This key has a different value for each connection between the client and the access point.

The session key is derived from the user password and the contents of the LEAP challenges and responses that go to and from the client. 802.11 encryption might be based on a 40-bit key or a 128-bit key. The key derivation routines provide a key that is longer than needed.

Configuring LEAP

This section explains how to configure LEAP module settings. The following topics are covered in this section:

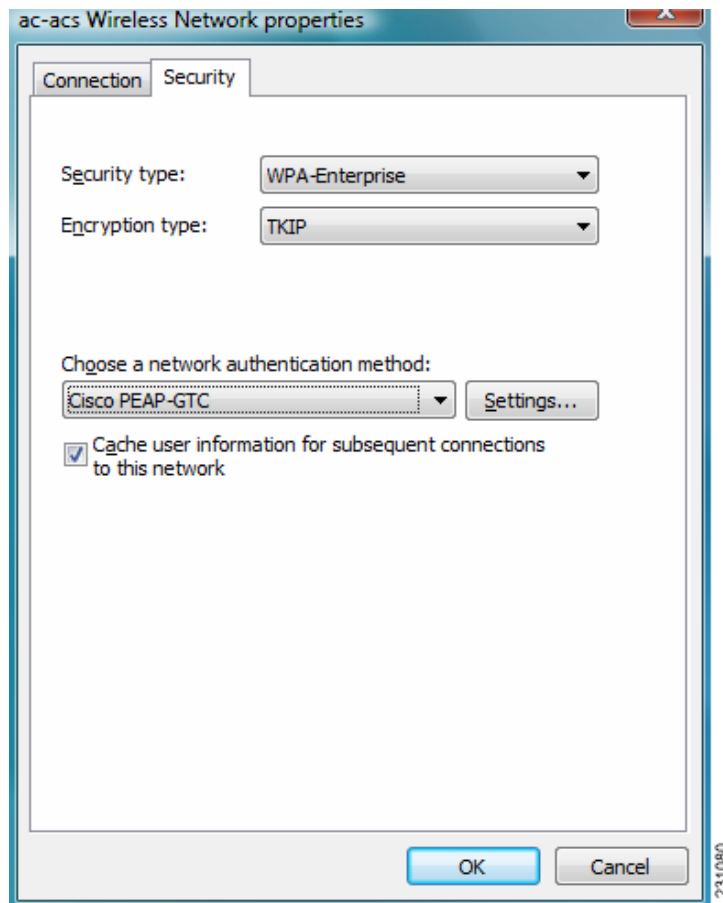
- [Accessing LEAP Properties for Configuration, page 3-18](#)
- [Configuring LEAP Settings in the Network Credentials Tab, page 3-19](#)
- [Finding the Version of the LEAP Module, page 3-21](#)

Accessing LEAP Properties for Configuration

To access the LEAP Properties window, perform the following steps:

-
- Step 1** Click the **Start** button on the lower-left corner of the desktop.
 - Step 2** From the right pane, right-click **Network**.
 - Step 3** Select **Properties**.
 - Step 4** From the left pane, select **Manage Wireless Networks**.
 - Step 5** Double-click the wireless network.
 - Step 6** From the **Wireless Network properties** window, select the **Security** tab (see [Figure 3-1](#)).

Figure 3-8 Wireless Network Properties Window



Step 7 Select **LEAP** from the "Choose a network authentication method" drop down list.

Step 8 Click the **Settings** button. You are now ready to configure settings for LEAP.

Configuring LEAP Settings in the Network Credentials Tab

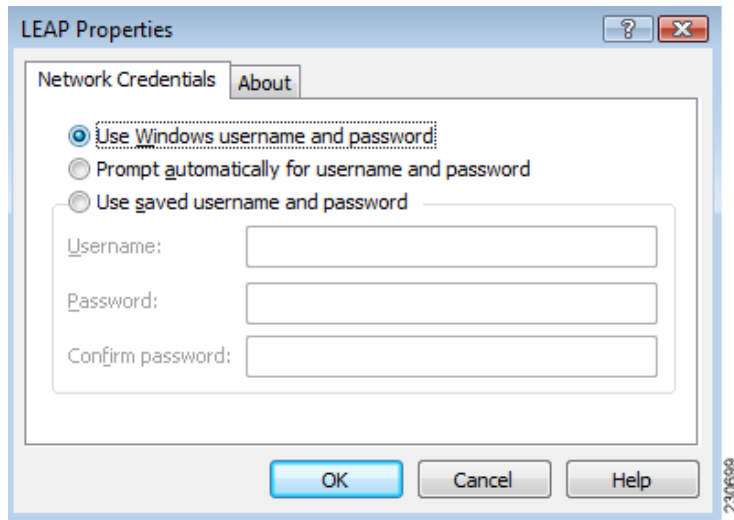
The user provides one of the following types of network credentials:

- Windows username and password—The Windows username and password are used as network access credentials. The user is not prompted to enter a username and password if this option is selected.
- Prompted user credentials—The user is prompted during authentication for credentials. These credentials are credentials that are separate from the Windows username and password, such as Lightweight Directory Access Protocol (LDAP) credentials.

- Saved user credentials—These are user credentials that are entered as part of the LEAP configuration. The user is not prompted for credentials during authentication unless the saved credentials fail or have expired. New credentials that the user enters after successful authentication are saved automatically in the configuration. The user does not have to return to the configuration screen to change the old saved credentials.

You can configure LEAP network credentials settings from the Network Credentials tab (see [Figure 3-9](#)).

Figure 3-9 Network Credentials Tab in LEAP Properties Window



[Table 3-4](#) lists and describes LEAP network credentials settings.

Table 3-4 LEAP Network Credentials Settings

LEAP Network Credentials Settings	Description
Use Windows username and password	Click this radio button to use the Windows username and password as the LEAP username and password for network authentication. Default: On

Table 3-4 LEAP Network Credentials Settings (continued)

LEAP Network Credentials Settings	Description
Prompt automatically for username and password	Click this radio button to require the user to enter a separate LEAP username and password, which are registered with the backend server, in addition to a Windows username and password with every authentication attempt. Default: Off
Use saved username and password	Click this radio button so that the user is not required to enter a LEAP username and password with each Windows login. Authentication occurs automatically as needed using a saved username and password, which are registered with the backend server. Default: Off When selecting this option, the user must do the following: <ul style="list-style-type: none"> • Enter a username in the Username field. • Enter a password in the Password field. • Confirm password—Enter the password again to verify that it was entered correctly. Note The maximum number of characters allowed for the username and password is 256.

The following three scenarios for credentials entry are supported by the LEAP module:

- **Boot time**—During this state, no users are logged on. The LEAP module uses machine credentials for network authentication. The LEAP module does not prompt the user for information but instead obtains the machine credentials by using Microsoft's Local Security Authority (LSA) API.
- **Pre-Logon**—During this state, Microsoft's Layer 2 credential provider (L2NA) queries the LEAP module through Microsoft's EAPHost APIs for types of credentials that are needed. The LEAP module indicates the appropriate type: Windows, network, or none. The user enters the appropriate credentials in a Microsoft L2NA prompt.
- **Post-Logon**—Although the user has already logged on, the LEAP module might need to prompt the user for network credentials because a card was inserted or because network authentication failed. The LEAP module invokes the EapInvokeInteractiveUI API, which is a Microsoft EAPHost API. A LEAP credentials prompt appears, and the user must enter a username and password.

Finding the Version of the LEAP Module

The LEAP module version number, copyright information, and open-source software information are in About tab (see [Figure 3-9](#)).

Overview of PEAP-GTC

Extensible Authentication Protocol (EAP) provides support for multiple authentication methods. While EAP was originally created for use with PPP, it has since been adopted for use with IEEE 802.1X, which is Network Port Authentication. Since its deployment, a number of weaknesses in EAP have become

apparent. These weaknesses include a lack of protection of user identity, notification messages, or the EAP negotiation; no standardized mechanism for key exchange; no built-in support for fragmentation and reassembly; no support for acknowledged success or failure indicators; and a lack of support for fast reconnect.

Protected Extensible Authentication Protocol (PEAP) addresses these weaknesses by wrapping the EAP protocol within a Transport Layer Security (TLS) channel. Any EAP method running within PEAP is provided with the following:

- Identity protection—The identity exchange is encrypted, and client certificates are provided after negotiation of the TLS channel.
- Header protection—Because the EAP method conversation is conducted within a TLS channel, the EAP header is protected against modification.
- Protected negotiation—Within PEAP, the EAP conversation is authenticated; integrity and replay are protected on a per-packet basis; and the EAP method negotiation that occurs within PEAP is protected, as are error messages sent within the TLS channel.
- Support for key exchange—To provide keying material for a wide range of link-layer ciphersuites, EAP methods should provide a key hierarchy that generates authentication and encryption keys, as well as initialization vectors. By relying on the TLS key derivation method, PEAP provides the required keying material for any EAP method running within it.
- Packet fragmentation and reassembly—Because EAP does not include support for fragmentation and reassembly, individual EAP methods need to include this capability. By including support for fragmentation and reassembly within PEAP, methods leveraging PEAP do not need to support fragmentation and reassembly on their own.
- Acknowledged success or failure indications—By sending success or failure indications within the TLS channel, PEAP provides support for protected termination of the EAP conversation. Acknowledged indications prevent an attacker from carrying out denial-of-service (DOS) attacks by spoofing EAP failure messages or by tricking the EAP peer into accepting a rogue NAS by spoofing an EAP success message.
- Fast reconnect—Where EAP is used for authentication in wireless networks, the EAP method should be able to quickly reauthenticate when the client is roaming between access points. PEAP supports fast reconnect by leveraging the TLS session resumption facility. Any EAP method running within PEAP can use fast reconnect.
- Dictionary attack resistance—By conducting the EAP conversation within a TLS channel, PEAP protects an EAP method that might be subject to offline dictionary attacks if the EAP conversation had been conducted in the clear.

How PEAP-GTC Works

PEAP-GTC works in two phases.

In phase 1, an authentication server performs TLS authentication to create an encrypted tunnel and to achieve server-side authentication in a manner that is similar to Web server authentication that uses Secure Sockets Layer (SSL). When phase 1 of PEAP is successfully completed, all data is encrypted, including all sensitive user information.

Phase 2 is extensible. The client can authenticate by using the GTC method within the TLS tunnel.

Configuring PEAP-GTC

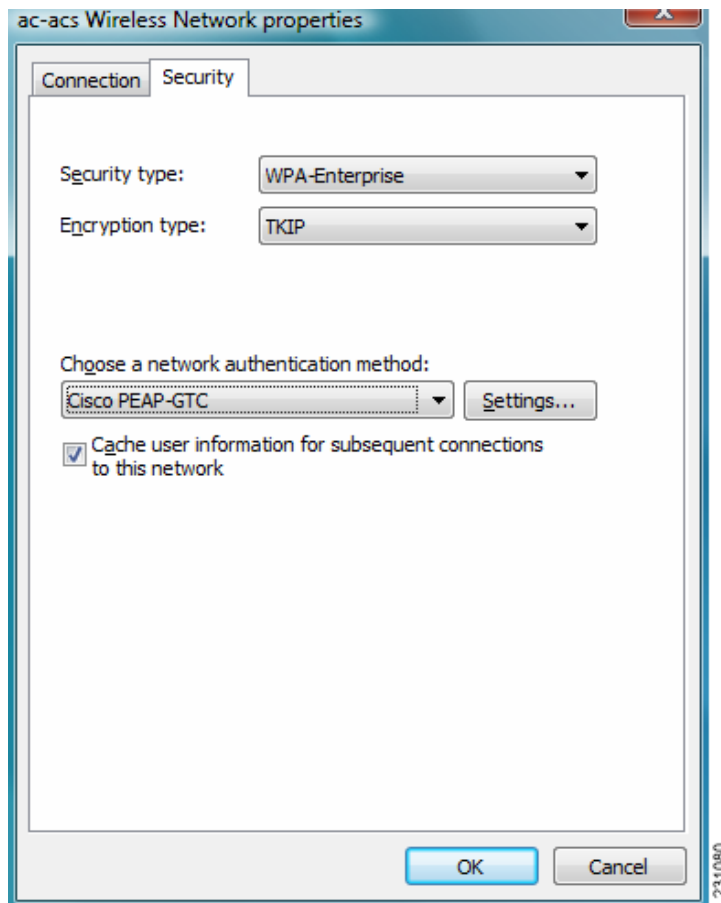
This section explains how to configure PEAP-GTC module settings. The following topics are covered:

- [Accessing PEAP-GTC Properties for Configuration, page 3-23](#)
- [Configuring PEAP-GTC Settings in the Connection Tab, page 3-25](#)
- [Configuring PEAP-GTC Settings in the User Credentials Tab, page 3-27](#)

Accessing PEAP-GTC Properties for Configuration

To access the PEAP-GTC Properties window, perform the following steps:

-
- Step 1** Click the **Start** button on the lower-left corner of the desktop.
 - Step 2** From the right pane, right-click **Network**.
 - Step 3** Select **Properties**.
 - Step 4** From the left pane, select **Manage Wireless Networks**.
 - Step 5** Double-click the wireless network.
 - Step 6** From the **Wireless Network properties** window, select the **Security** tab (see [Figure 3-10](#)).

Figure 3-10 Wireless Network Properties Window

Step 7 Select **PEAP-GTC** or **LEAP** from the "Choose a network authentication method" drop down list.

Step 8 Click the **Settings** button. You are now ready to configure settings for PEAP-GTC.

Configuring PEAP-GTC Settings in the Connection Tab

You can configure connection settings from the PEAP-GTC Connection tab (see [Figure 3-11](#)).

Figure 3-11 Connection Tab in PEAP-GTC Properties Window

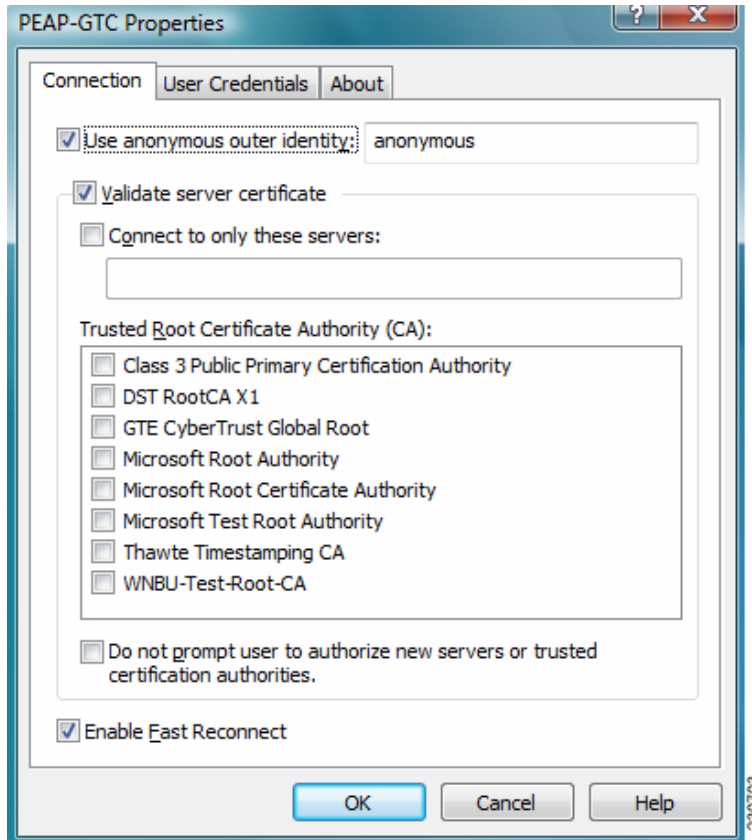


Table 3-5 lists and describes PEAP-GTC connection settings.

Table 3-5 PEAP-GTC Connection Settings

PEAP-GTC Connection Settings	Description
Use anonymous outer identity	<p>Check this box to enable identity privacy protection. If this box is checked, the Outer identity field is enabled, and the outer identity in this field is used in response to an EAP identity request, which is sent in the clear.</p> <p>Default: On</p>
Outer identity field	<p>Enter an outer identity if the Use anonymous outer identity check box is checked. Follow an administrator's instructions, or follow RFC 4282 for guidelines about what to enter in the outer identity field.</p> <p>Default: anonymous</p> <p>Note The maximum number of characters allowed in this field is 256.</p>
Validate server certificate	<p>Check this box to validate the server certificate that is used to establish a tunnel.</p> <p>If the Validate server certificate box is checked and the Do not prompt user to authorize new servers or trusted certificate authorities box is checked, you must select one or more Trusted Root CA certificates from the list of trusted Certificate Authority certificates that are installed on the host system.</p> <p>If the Validate server certificate box is checked but the Do not prompt user to authorize new servers or trusted certificate authorities box is not checked, the list can be empty, and the user is prompted to validate the certificate. If authentication succeeds, then the Root CA that signed the server certificate is marked as trusted in the profile. The name of the server is then added to the Connect to only these servers field.</p> <p>Default: On</p>
Connect to only these servers	<p>Check this box to enter an optional server name that must match the server certificate that is presented by the server. You can enter multiple server names; separate multiple server names with semicolons. The PEAP-GTC module only allows connections to continue without prompting if the subject field (CN) or the subject alternative name in the server certificate matches the server names that you enter in this field.</p> <p>Default: Off</p> <p>Note You can use an asterisk (*) as a wildcard character in server names only if the asterisk appears before the first period (.) in the name.domain.com format. For example, "*.cisco.com" matches any server name that ends with ".cisco.com." If you put an asterisk anywhere else in the server name, it is not treated as a wildcard character.</p>

Table 3-5 PEAP-GTC Connection Settings (continued)

PEAP-GTC Connection Settings	Description
Trusted Root Certificate Authority (CA)	<p>Select one of more Trusted Root CA certificates from the list of certificates that are installed on the system. Only trusted CA certificates that are installed on the host system are displayed in the drop-down list, so you must make sure that the desired trusted root CA certificate is installed.</p> <p>To view details about the selected Trusted Root CA certificate, double-click the certificate name. Double-clicking the certificate name opens the Windows certificate property screen, where certificate details are available.</p> <p>Default: None</p>
Do not prompt user to authorize new servers or trusted certificate authorities.	<p>Check this box if you do not want the user to be prompted to authorize a connection when the server name does not match or the server certificate is not signed by one of the Trusted Root CA certificates that was selected. If this box is checked and the server certificate is not trusted, the authentication fails.</p> <p>Default: Off</p>
Enable fast reconnect	<p>Check this box to allow session resumption.</p> <p>The PEAP-GTC module supports fast reconnect (also called session resumption). When you enable fast reconnect, you can roam without re-entering your credentials. Fast reconnect can be used across different network access servers.</p> <p>Default: On</p> <p>Note If you switch profiles, log off, or reboot, fast reconnect is not attempted. You must be reauthenticated.</p>

Configuring PEAP-GTC Settings in the User Credentials Tab

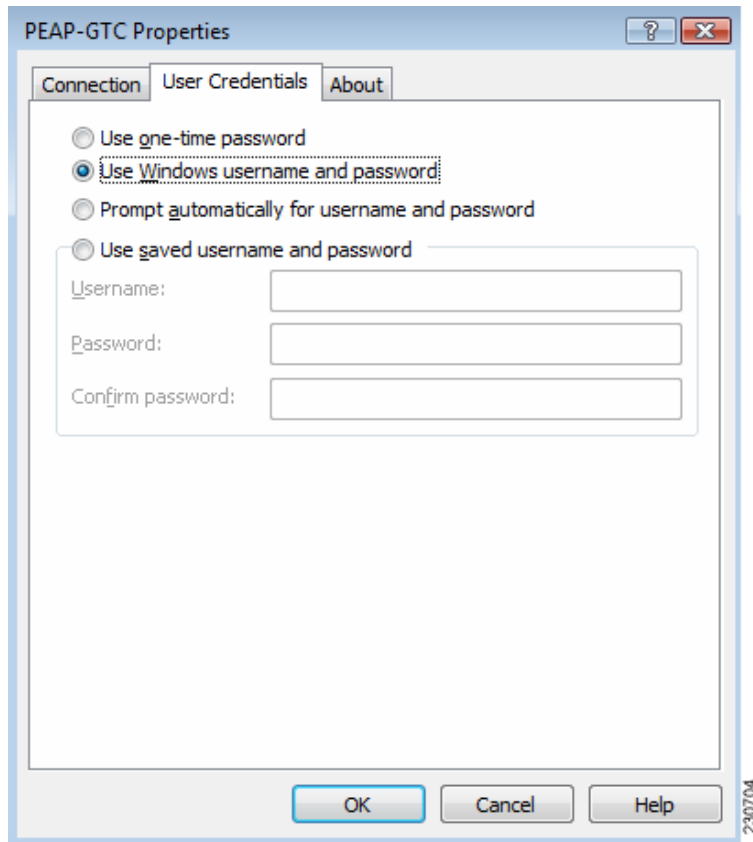
The PEAP-GTC module supports OTP and a username and password as user credentials for authentication.

The user provides one of the following types of username and password:

- One-time password (OTP)—The user must manually enter a OTP. New PIN mode and next token mode for OTP are supported.
- Windows username and password—The Windows username and password are used as network access credentials. The user is always prompted to enter a password unless PEAP-GTC is configured to use single sign-on (SSO) or the password is cached.
- Prompted user credentials—The user is prompted during authentication for credentials. These credentials are credentials that are separate from the Windows username and password, such as Lightweight Directory Access Protocol (LDAP) credentials.
- Saved user credentials—These are user credentials that are entered as part of the PEAP-GTC configuration. The user is not prompted for credentials during authentication unless the saved credentials fail or have expired. New credentials that the user enters after successful authentication are saved automatically in the configuration. The user does not have to return to the configuration screen to change the old saved credentials.

The user can configure PEAP-GTC user credentials from the User Credentials tab (see [Figure 3-12](#)).

Figure 3-12 User Credentials Tab in PEAP-GTC Properties Window



[Table 3-2](#) lists and describes options for PEAP-GTC user credentials.

Table 3-6 PEAP-GTC User Credentials Options

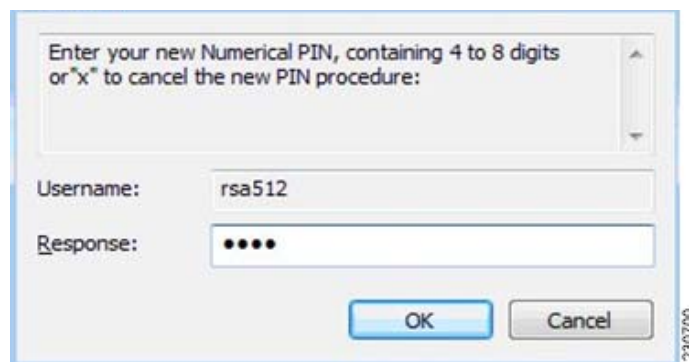
User Credentials	Description
Use one-time password	<p>Click this radio button to use a one-time password (OTP). In this mode, credentials are never cached. Each time the server asks for credentials, the user is prompted to supply credentials.</p> <p>For more information about OTP, see the “Understanding PIN Mode and Token Mode with OTP” section on page 3-12.</p> <p>Default: Off</p>
Use Windows username and password	<p>Click this radio button to use the Windows username and password as the PEAP-GTC username and password for network authentication. This mode only affects single sign-on authentication when the login screen has one set of credentials instead of two sets of credentials, which is the case for the Prompt automatically for username and password option.</p> <p>Default: On</p>

Table 3-6 PEAP-GTC User Credentials Options (continued)

User Credentials	Description
Prompt automatically for username and password	Click this radio button to require the user to enter a separate PEAP-GTC username and password, which are registered with a RADIUS server, in addition to a Windows username and password with every authentication attempt. This option supports non-Windows passwords, such as LDAP. Default: Off
Use saved username and password	Click this radio button so that the user is not required to enter a PEAP-GTC username and password with each Windows login. Authentication occurs automatically as needed using a saved username and password, which are registered with the backend server. Default: Off When selecting this option, the user must enter the following: <ul style="list-style-type: none"> Username—Enter the username and the domain name in one of these two formats: <ul style="list-style-type: none"> Domain-qualified username—domain\user UPN—user@domain.com Password—Enter a password. This encrypted password is stored in the PEAP-GTC configuration. Confirm password—Enter the password again to verify that it was entered correctly. Note The maximum number of characters allowed for the username and password is 256.

Understanding PIN Mode and Token Mode with OTP

New PIN mode for OTP is supported. If a new PIN is needed, the backend server sends a text message (for example, “Enter New PIN”) to indicate that a new PIN is needed. The PEAP-GTC module displays a prompt window that includes the text message from the server (see [Figure 3-13](#)). The backend server might prompt the user twice to confirm the new PIN that the user entered.

Figure 3-13 New PIN Prompt Window

Next Token mode for OTP is also supported. If the next token is needed, the backend server sends a text message (for example, “Enter Next PASSCODE:”) to indicate that the next token is needed. The PEAP-GTC module displays a prompt window that includes the text message sent from the server (see [Figure 3-14](#)). The user must get the next token from the OTP device or from the software and enter it in the prompt field.

Figure 3-14 Next Token Prompt Window



Understanding PEAP-GTC Authentication

The PEAP-GTC module prompts the user for a username and password (or PIN for OTP) if the supplicant is configured to prompt for credentials during Windows logon or after the user is notified of an authentication error or failure.

If the user password expires, the PEAP-GTC modules prompts the user to enter a new password and to confirm the new password.

Finding the Version of the PEAP-GTC Module

The PEAP-GTC module version number, copyright information, and open-source software information are in About tab (see [Figure 3-12](#)).



CHAPTER 4

Performing Administrative Tasks

This chapter explains how to obtain Microsoft administrative tools to distribute wireless profiles to users and computers in an Active Directory environment. This chapter also provides the XML schemas for EAP-FAST, LEAP, and PEAP-GTC.

The following topics are covered in this chapter:

- [Using Microsoft Tools to Perform Administrative Tasks, page 4-2](#)
- [The EAP-FAST XML Schema, page 4-6](#)
- [The PEAP-GTC XML Schema, page 4-17](#)
- [The LEAP XML Schema, page 4-23](#)
- [Logging for EAP Modules, page 4-26](#)

Using Microsoft Tools to Perform Administrative Tasks

You must perform administrative tasks, such as the distribution of wireless profiles to users and computers within an Active Directory environment, by creating Microsoft Group Policy Objects with a Microsoft Group Policy Object Editor. Detailed discussion of these Microsoft solutions and their functionality is beyond the scope of this Cisco document.

The following sections contain preliminary information and references to assist you in finding out more about performing administrative tasks with Microsoft tools:

- [Overview of Group Policy Objects, page 4-2](#)
- [Adding a Group Policy Object Editor, page 4-2](#)
- [Creating a EAP Group Policy Object in Windows Vista, page 4-3](#)

Overview of Group Policy Objects

Group Policy is an infrastructure that allows you to specify managed configurations for users and computers in an Active Directory directory service environment. Group Policy settings are contained in Group Policy objects (GPOs). GPOs exist in a domain and can be linked to the following Active Directory containers: sites, domains, or organizational units (OUs).

For more information about GPOs and the GPO Editor, refer to the Microsoft Windows Server TechCenter at this URL:

<http://technet2.microsoft.com/windowsserver/en/technologies/featured/gp/faq.mspx>

Microsoft provides a program snap-in that allows you to use the Group Policy Object editor in the Microsoft Management Console (MMC).

For more information about the MMC, refer to the Microsoft Management Console Help at this URL:

<http://www.microsoft.com/technet/WindowsVista/library/ops/06e1cb7b-19c9-4c49-9db8-a941f6f593c3.mspx>

Adding a Group Policy Object Editor

Before you configure a Group Policy Object, you must add a Group Policy Object Editor snap-in. To add the snap-in, perform the following steps:

-
- Step 1** Open the MMC:
- Click the **Start** button on the lower-left corner of the desktop.
 - Enter **mmc** in the **Search box** and press **Enter**.

**Note**

To open an existing or saved MMC console, browse to the snap-in console or a shortcut to the snap-in console in Windows Explorer, and then double-click it.

You can also open an existing MMC console from another console in which you are working. To do this, click the **File** menu, and then click **Open**.

- Step 2** Add the Group Policy Object Editor snap-in:
- a. Go to **File > Add/Remove Snap-in...**
The **Add or Remove Snap-ins** dialog box is displayed.
 - b. From the **Add or Remove Snap-ins** dialog box, highlight **Group Policy Object Editor** in the **Available snap-ins** list, and click the **Add** button.
The **Select Group Policy Object** dialog box is displayed.
 - c. From the **Select Group Policy Object** dialog box, click **Browse**.
The **Browse for a Group Policy Object** dialog box is displayed.
 - d. From the **Browse for a Group Policy Object** dialog box, select the **Domains/O Us** tab.
 - e. Select your domain controller from the **Look in** drop down list.
 - f. Click **OK**.
 - g. From the **Select Group Policy Object** dialog box, click **Finish**.
 - h. From the **Add or Remove Snap-ins** dialog box, click **OK**.
-

Now the Group Policy Object Editor is ready for use.

Creating a EAP Group Policy Object in Windows Vista

To create a new EAP group policy object , perform the following steps:

-
- Step 1** In the **Default Domain Policy** pane, select **Windows Settings > Security Settings > Wireless Network Policies**.
- Step 2** Right-click **Wireless Network Policies** and select **Create a New Policy**.
- Step 3** Set your wireless network properties, such as SSID, encryption, and authentication method.
- Step 4** Select the EAP method.
- Step 5** Open properties for the desired EAP modules and configure the settings.
- EAP-FAST—In the **Advanced Security** screen, you can configure supplicant settings such as machine authentication and SSO. For more information about machine authentication, see the [“Configuring Machine Authentication for EAP-FAST”](#) section on page 4-4. For more information about SSO see the [“Configuring Single Sign-On for EAP-FAST”](#) section on page 4-5.
 - PEAP-GTC—In the **Advanced Security** screen, you can configure supplicant settings such as machine authentication and SSO. For more information about machine authentication, see the [“Configuring Machine Authentication for PEAP-GTC”](#) section on page 4-5. For more information about SSO see the [“Configuring Single Sign-On for PEAP-GTC and LEAP”](#) section on page 4-5
 - LEAP—In the **Advanced Security** screen, you can configure supplicant settings for SSO. For more information about SSO, see the [“Configuring Single Sign-On for PEAP-GTC and LEAP”](#) section on page 4-5



Note You can configure settings for a wired network by selecting the **Wired Network Policy** object.

- Step 6** After you are done, save the GPO. You can refresh the Vista client by running "gpupdate /force" to force update of the GPO. You should see the new profile being added to Vista machine.
-

After you create a GPO network profile, it cannot be changed by the user on the Vista machine.

On the General tab of a wireless network policy, you can configure a name and description for the policy, specify whether the WLAN AutoConfig service is enabled, and configure a list of wireless network policies and their settings in a preferred order. You can also export profiles as XML files and import XML files as wireless profiles.

For detailed information about configuring policies, exporting profiles, and importing profiles, see the following documentation:

- *Windows Vista Wireless Networking Evaluation Guide*

<http://technet2.microsoft.com/WindowsVista/en/library/f0b0d1fd-6dff-46a2-8e6a-bdd152d2337f1033.mspx?mfr=true>

- *Wireless Group Policy Settings for Windows Vista*

<http://www.microsoft.com/technet/technetmag/issues/2007/04/CableGuy/default.asp>

Configuring Machine Authentication for EAP-FAST

You can enable machine authentication from the Advanced Security screen when you create a Group Policy Object.

The EAPHost notifies the EAP-FAST module that the current authentication is a machine authentication.

Machine authentication is achieved by using one of the following:

- a machine PAC
- a machine certificate
- a machine password

The EAP-FAST module attempts to fetch the machine PAC first. If a machine PAC is unavailable, the EAP-FAST module attempts to fetch a machine certificate. If a machine certificate is unavailable, the EAP-FAST module attempts to fetch the machine password for the machine account in the Active Directory.

When the machine is authenticated with either a machine certificate or a machine password, the EAP-FAST module then requests the provisioning of a machine PAC for subsequent use. If neither a machine certificate nor a machine password is available, the EAP-FAST module requests a machine PAC during the next successful user authentication after a user has logged on. If an existing machine PAC is invalid or expired, the EAP-FAST module relies on this process to request a new machine PAC.

Because machine authentication is integrated with and supported by the Windows 802.1X supplicant, the EAP-FAST module is only responsible for authentication to gain network access. Additional network operations to support machine authentication, such as DHCP, machine-level GPO, and other related network services, are the responsibility of the operating system and the 802.1X supplicant.

Configuring Single Sign-On for EAP-FAST

SSO is supported by Microsoft Windows Vista in the following ways:

- Windows user credentials are passed to the EAP-FAST module through the EAPHost interface. The system does not prompt the user to provide additional credentials if the EAP-FAST module is configured to use Windows user credentials for network authentication and if the network profile is configured for single sign-on.
- Non-Windows network credentials are collected during the Microsoft Windows Vista logon process. The EAP-FAST module requests the logon module to prompt the user for these network credentials.
- If necessary, the EAP-FAST module is able to prompt the user for additional network credentials before the user logs in to Microsoft Windows Vista.

If network credentials are stored in the configuration, the EAP-FAST module has access to these credentials before the user logs in to Microsoft Windows Vista.

Configuring Machine Authentication for PEAP-GTC

The PEAP-GTC module supports machine authentication only via the machine password. The PEAP-GTC module gets the machine password from Windows through Microsoft's Local Security Authority (LSA) API. The user is not prompted for the password.

Machine authentication is enabled and configured on the supplicant.

Configuring Single Sign-On for PEAP-GTC and LEAP

For both the PEAP-GTC module and the LEAP module, single sign-on (SSO) is supported by Microsoft Windows Vista in the following ways:

- Windows user credentials are passed to the module through the EAPHost interface. The system does not prompt the user to provide additional credentials if the module is configured to use Windows user credentials for network authentication and if the network profile is configured for single sign-on.
- Non-Windows network credentials are collected during the Microsoft Windows Vista logon process. The module requests the logon module to prompt the user for these network credentials.
- The Windows 802.1X supplicant handles the Group Policy process and ensures that it is synchronized and exercised with the Window's logon process.
- If necessary, the module is able to prompt the user for additional network credentials before the user logs in to Microsoft Windows Vista.
- If network credentials are stored in the configuration, the module has access to these credentials before the user logs in to Microsoft Windows Vista.

The EAP-FAST XML Schema

The EAP-FAST module stores all settings in the Native EAP method section of the network profile as XML by using the following schema:

```
<?xml version="1.0"?>

<!--
*****
                Cisco EAP-FAST Schema                (1.0.40)
Copyright 2006-2007, Cisco Systems, Inc.                All rights reserved.
*****
-->

<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.cisco.com/CCX"
  targetNamespace="http://www.cisco.com/CCX"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xs:element name="eapFast" type="EapFast"/>

  <xs:complexType name="EapFast">
    <xs:complexContent>
      <xs:extension base="TunnelMethods">
        <xs:sequence>
          <xs:choice>
            <xs:element name="usePac">
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="allowUnauthPacProvisioning" type="xs:boolean" default="true">
                    <xs:annotation>
                      <xs:documentation>Will accept a PAC from an unauthenticated server.</xs:documentation>
                    </xs:annotation>
                  </xs:element>
                  <xs:element name="autoGrouping" type="xs:boolean" default="true">
                    <xs:annotation>
```

```

    <xs:documentation>
An aid-group is a set of A-IDs that are all trusted equally. Any A-ID in the group can be utilized.
Auto-grouping means that when an untrusted A-ID is accepted by the end-user then that A-ID is grouped
with the A-ID(s) that were already trusted for that profile, hence automatically creating and growing an
A-ID group based on user actions. The advantage of an A-ID group is that if a profile initially starts
with the same trusted A-ID(1) and then at some point the end-user authorizes the use of a new A-ID(2)
when using this profile it will accept A-ID(2) without bothering the end-user a second
time.</xs:documentation>
    </xs:annotation>
</xs:element>
    <xs:element name="userValidatesServerIdFromUnauthProv" type="xs:boolean"
default="true">
    <xs:annotation>
    <xs:documentation>
If true, then when the client is about to do unauthenticated provisioning, the user will be prompted to
allow or disallow the unauthenticated provisioning.</xs:documentation>
    </xs:annotation>
</xs:element>
    <xs:element name="unauthProvAllowedTilPacReceived" type="xs:boolean" default="false">
    <xs:annotation>
    <xs:documentation>if true, then unauthenticated provisioning is allowed to occur until it
succeeds and a PAC is received, then only authenticated provisioning will be
allowed.</xs:documentation>
    </xs:annotation>
</xs:element>
    <xs:choice>
    <xs:element name="validateWithSpecificPacs" type="ValidateWithSpecificPacs">
    <xs:annotation>
    <xs:documentation>This indicates that only those PACs referenced in this element (as
well as PACs that are auto-provisioned to this profile when this profile is in use) shall be used for
validation. </xs:documentation>
    </xs:annotation>
</xs:element>
    </xs:choice>
</xs:sequence>
</xs:complexType>
</xs:element>
    <xs:element name="doNotUsePac" type="Empty">
    <xs:annotation>
    <xs:documentation>Will not utilize PAC for authentication.</xs:documentation>
    </xs:annotation>

```

```

    </xs:element>
  </xs:choice>
  <xs:element name="enablePosture" type="xs:boolean" default="false">
    <xs:annotation>
      <xs:documentation>Allow posture information to be processed.</xs:documentation>
    </xs:annotation>
  </xs:element>
  <xs:element name="authMethods">
    <xs:complexType>
      <xs:choice>
        <xs:element name="builtinMethods">
          <xs:complexType>
            <xs:choice>
              <xs:element name="authenticateWithPassword">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="protectedIdentityPattern" type="IdentityPattern" minOccurs="0">
                      <xs:annotation>
                        <xs:documentation>Format rules same as for unprotectedIdentityPattern. Typical
pattern: [username]@[domain] or if password source is this profile then the pattern would be the actual
string to send as the username. </xs:documentation>
                      </xs:annotation>
                    </xs:element>
                    <xs:element name="passwordSource" type="PasswordSource"/>
                    <xs:element name="methods">
                      <xs:annotation>
                        <xs:documentation>At least 1 child element is required.</xs:documentation>
                      </xs:annotation>
                    <xs:complexType>
                      <xs:all>
                        <xs:element name="eapMschapv2" type="Empty" minOccurs="0"/>
                        <xs:element name="eapGtc" type="Empty" minOccurs="0"/>
                      </xs:all>
                    </xs:complexType>
                  </xs:element>
                </xs:sequence>
              </xs:complexType>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:complexType>
  </xs:element>

```

```

<xs:element name="authenticateWithToken">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="protectedIdentityPattern" type="IdentityPattern" minOccurs="0">
        <xs:annotation>
          <xs:documentation>Format rules same as for unprotectedIdentityPattern. Typical
pattern: [username]@[domain] </xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="tokenSource" type="TokenSource"/>
      <xs:element name="methods">
        <xs:complexType>
          <xs:all>
            <xs:element name="eapGtc" type="Empty"/>
          </xs:all>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="authenticateWithCertificate">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="protectedIdentityPattern" type="IdentityPattern" minOccurs="0">
        <xs:annotation>
          <xs:documentation>Format rules same as for unprotectedIdentityPattern. Typical
pattern: [username]@[domain] </xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="certificateSource" type="CertificateSource"/>
      <xs:choice>
        <xs:element name="doNotUseInnerMethod">
          <xs:complexType>
            <xs:choice>
              <xs:element name="sendWheneverRequested" type="Empty"/>
              <xs:element name="sendSecurelyOnly" type="Empty"/>
            </xs:choice>
          </xs:complexType>
        </xs:element>
      </xs:choice>
    </xs:sequence>
  </xs:complexType>
</xs:element>

```

```

        </xs:element>
        <xs:element name="sendViaInnerMethod">
            <xs:complexType>
                <xs:all>
                    <xs:element name="eapTls" type="Empty"/>
                </xs:all>
            </xs:complexType>
        </xs:element>
    </xs:choice>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:choice>
</xs:complexType>
</xs:element>
    <xs:element name="extendedInnerMethods" type="ExtendedInnerEapMethod"
maxOccurs="unbounded"/>
    </xs:choice>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>

<xs:complexType name="IdentityPattern">
    <xs:simpleContent>
        <xs:extension base="NonEmptyString">
            <xs:attribute name="encryptContent" type="xs:boolean" use="optional" default="true">
                <xs:annotation>
                    <xs:documentation>this is defaulted to 'true' as an indication to the post-process tool that it
should encrypt this element.</xs:documentation>
                </xs:annotation>
            </xs:attribute>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>

```

```
<xs:complexType name="PasswordFromProfile">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="encryptContent" type="xs:boolean" use="optional" default="true">
        <xs:annotation>
          <xs:documentation>this is defaulted to 'true' as an indication to the post-process tool that it
should encrypt this element.</xs:documentation>
        </xs:annotation>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="PasswordSource">
  <xs:choice>
    <xs:element name="passwordFromLogon" type="Empty"/>
    <xs:element name="passwordFromUser" type="Empty"/>
    <xs:element name="passwordFromProfile" type="PasswordFromProfile"/>
  </xs:choice>
</xs:complexType>

<xs:complexType name="TokenSource">
  <xs:choice>
    <xs:element name="passwordFromOtherToken" type="Empty">
      <xs:annotation>
        <xs:documentation>this will result in a prompt to user to obtain identity and otp from
token</xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:choice>
</xs:complexType>

<xs:complexType name="CertificateSource">
  <xs:choice>
    <xs:element name="certificateFromUser" type="Empty">
      <xs:annotation>
        <xs:documentation>
```

The client certificate to use during authentication is the one that the end-user selects from a list presented to them.</xs:documentation>

```
</xs:annotation>
```

```
</xs:element>
```

```
<xs:element name="certificateFromLogon" type="Empty">
```

```
<xs:annotation>
```

<xs:documentation>The client certificate to use during authentication is the one the end-user used in order to logon to windows.</xs:documentation>

```
</xs:annotation>
```

```
</xs:element>
```

```
<xs:element name="certificateFromProfile" type="ClientCertificate">
```

```
<xs:annotation>
```

<xs:documentation>The client user certificate to use during authentication is indicated here.</xs:documentation>

```
</xs:annotation>
```

```
</xs:element>
```

```
</xs:choice>
```

```
</xs:complexType>
```

```
<xs:complexType name="ExtendedInnerEapMethod">
```

```
<xs:sequence>
```

```
<xs:element name="methodName" type="xs:string"/>
```

```
<xs:element name="methodEapId" type="xs:unsignedInt"/>
```

```
<xs:element name="vendorId" type="xs:integer" default="0"/>
```

```
<xs:element name="AuthorName" type="xs:string"/>
```

```
<xs:element name="AuthorId" type="xs:unsignedInt"/>
```

```
<xs:any namespace="##any" processContents="lax" minOccurs="0"/>
```

```
</xs:sequence>
```

```
</xs:complexType>
```

```
<xs:complexType name="TunnelMethods">
```

```
<xs:sequence>
```

```
<xs:choice>
```

```
<xs:element name="validateServerCertificate" type="serverCertificateValidationParameters"/>
```

```
<xs:element name="doNotValidateServerCertificate" type="Empty"/>
```

```
</xs:choice>
```

```
<xs:element name="unprotectedIdentityPattern" type="IdentityPattern" minOccurs="0">
```

```
<xs:annotation>
```


`<xs:documentation>`If the [username] and/or [domain] placeholders are used in the pattern then: if a client certificate is used for authentication then placeholder's values shall be obtained from the CN field of the client certificate. if the credentials are obtained from the end-user then these shall be obtained from the information the user enters. if the credentials are obtained from the operating system then these shall be obtained from the information the logon provides. Typical pattern: anonymous@[domain] for tunneled methods or [username]@[domain] for non-tunneled methods. If the credential source is this profile then the pattern would be the actual string to send as the username (no placeholders).`</xs:documentation>`

```
</xs:annotation>
```

```
</xs:element>
```

```
<xs:choice>
```

```
<xs:element name="enableFastReconnect">
```

```
<xs:complexType>
```

```
<xs:complexContent>
```

```
<xs:extension base="Empty">
```

```
<xs:choice>
```

```
<xs:element name="alwaysAttempt" type="Empty"/>
```

```
</xs:choice>
```

```
</xs:extension>
```

```
</xs:complexContent>
```

```
</xs:complexType>
```

```
</xs:element>
```

```
<xs:element name="disableFastReconnect" type="Empty"/>
```

```
</xs:choice>
```

```
</xs:sequence>
```

```
</xs:complexType>
```

```
<xs:complexType name="ClientCertificate">
```

```
<xs:choice>
```

```
<xs:element name="certificateId" type="CertificateIdentifier">
```

```
<xs:annotation>
```

```
<xs:documentation>This is a reference to an OS pre-stored certificate.</xs:documentation>
```

```
</xs:annotation>
```

```
</xs:element>
```

```
</xs:choice>
```

```
</xs:complexType>
```

```
<xs:complexType name="CertificateContainer">
```

```
<xs:choice minOccurs="0" maxOccurs="unbounded">
```

```
<xs:element name="certificateId" type="CertificateIdentifier">
```

```

    <xs:annotation>
      <xs:documentation>This is a reference to an OS pre-stored certificate.</xs:documentation>
    </xs:annotation>
  </xs:element>
</xs:choice>
</xs:complexType>

<xs:complexType name="CertificateIdentifier">
  <xs:simpleContent>
    <xs:annotation>
      <xs:documentation>SHA 1 hash over the whole binary certificate in X509 format that uniquely
      identifies a certificate in the global list of trusted CAs for the machine (OS managed store in
      windows).</xs:documentation>
    </xs:annotation>
    <xs:extension base="NonEmptyString">
      <xs:attribute name="reference" type="xs:boolean">
        <xs:annotation>
          <xs:documentation>true means the element value is a file reference to a certificate in PEM format,
          the post-process tool will retrieve the certificate file, convert to a hash, populate the certificateId
          element, and set the reference to false to indicate this is the SHA1 hash over that
          certificate.</xs:documentation>
        </xs:annotation>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="Empty"/>

<xs:simpleType name="NonEmptyString">
  <xs:restriction base="xs:string">
    <xs:minLength value="1"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="ServerRuleFormat">
  <xs:simpleContent>
    <xs:extension base="NonEmptyString">
      <xs:attribute name="match" use="required">

```

```

    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:enumeration value="exactly"/>
        <xs:enumeration value="endsWith"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
</xs:extension>
</xs:simpleContent>
</xs:complexType>

<xs:complexType name="ServerValidationRules">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:annotation>
      <xs:documentation>
Optional only when product allows user to trust server. In which case it allows a profile that has no server
validations rules to start with and when a user validates an untrusted server the validation process still
validates the server name.</xs:documentation>
      </xs:annotation>
      <xs:element name="matchSubjectAlternativeName" type="ServerRuleFormat">
        <xs:annotation>
          <xs:documentation>DNSName: typically takes the form of a Fully Qualified Domain Name
(FQDN)</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="matchSubject" type="ServerRuleFormat">
        <xs:annotation>
          <xs:documentation>Either Subject: CN (Common Name) - typically a simple ASCII string.Or
Subject: DN (Domain Name) - a composite of a set of DC (Domain Component)
attributes</xs:documentation>
        </xs:annotation>
      </xs:element>
    </xs:choice>
  </xs:complexType>

<xs:complexType name="serverCertificateValidationParameters">
  <xs:sequence>
    <xs:choice>
      <xs:element name="serverNameValidationRules" type="ServerValidationRules"/>

```

```

<xs:element name="anyServerName" type="Empty">
  <xs:annotation>
    <xs:documentation>the server name within the certificate will not be tested.</xs:documentation>
  </xs:annotation>
</xs:element>
</xs:choice>
<xs:choice>
  <xs:element name="validateChainWithSpecificCa">
    <xs:complexType>
      <xs:complexContent>
        <xs:extension base="CertificateContainer"/>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>
  <xs:element name="validateChainWithAnyCaFromOs" type="Empty">
    <xs:annotation>
      <xs:documentation>the certificate chain will be trusted if it ends in a CA cert from the global
CA cert store.</xs:documentation>
    </xs:annotation>
  </xs:element>
</xs:choice>
<xs:element name="userValidatesUntrustedServerCertificate" type="xs:boolean">
  <xs:annotation>
    <xs:documentation>if the server certificate fails to validate then if this is true the end-user will be
asked to validate the server. If they do so then appropriate trustedCaCerts will be remembered as well
as the server name fields so it will be automatically trusted in the future.</xs:documentation>
  </xs:annotation>
</xs:element>
</xs:sequence>
</xs:complexType>

<xs:complexType name="ValidateWithSpecificPacs">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:annotation>
      <xs:documentation>This is optional because it allows the profile to indicate that we want the engine
to validate the server PACs but that the PACs will be dynamically added by the end-user actions or via
unauthenticated provisioning rather than being statically defined here in the
profile.</xs:documentation>
    </xs:annotation>

```

```

    <xs:element name="trustPacFromGlobalPacStoreWithThisId" type="xs:string">
      <xs:annotation>
        <xs:documentation>
          Utilized when there is a global store used for PACs (rather than just per-profile).</xs:documentation>
        </xs:annotation>
      </xs:element>
    </xs:choice>
  </xs:complexType>

</xs:schema>

```

The PEAP-GTC XML Schema

The PEAP-GTC module stores all settings in the Native EAP method section of the network profile as XML by using the following schema:

```

<?xml version="1.0"?>

<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.cisco.com/CCX"
  targetNamespace="http://www.cisco.com/CCX"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified">

  <xs:element name="eapPeap" type="EapPeap"/>

  <xs:complexType name="EapPeap">
    <xs:complexContent>
      <xs:extension base="TunnelMethods">
        <xs:sequence>
          <xs:element name="authMethods">
            <xs:complexType>
              <xs:choice>
                <xs:element name="builtinMethods">
                  <xs:complexType>
                    <xs:choice>

```

```

<xs:element name="authenticateWithPassword">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="protectedIdentityPattern" type="IdentityPattern" minOccurs="0"/>
      <xs:element name="passwordSource" type="PasswordSource"/>
      <xs:element name="methods">
        <xs:complexType>
          <xs:all>
            <xs:element name="eapGtc" type="Empty" minOccurs="0"/>
          </xs:all>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="authenticateWithToken">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="protectedIdentityPattern" type="IdentityPattern" minOccurs="0"/>
      <xs:element name="tokenSource" type="TokenSource"/>
      <xs:element name="methods">
        <xs:complexType>
          <xs:all>
            <xs:element name="eapGtc" type="Empty"/>
          </xs:all>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:choice>
</xs:complexType>
</xs:element>
</xs:choice>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:extension>

```

```
</xs:complexContent>
</xs:complexType>

<xs:complexType name="IdentityPattern">
  <xs:simpleContent>
    <xs:extension base="NonEmptyString">
      <xs:attribute name="encryptContent" type="xs:boolean" use="optional" default="true">
        <xs:annotation>
          <xs:documentation>this is defaulted to 'true' as an indication to the post-process tool that it
            should encrypt this element, if the element is not already encrypted (within an XML Security
            envelope).</xs:documentation>
        </xs:annotation>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="PasswordFromProfile">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="encryptContent" type="xs:boolean" use="optional" default="true">
        <xs:annotation>
          <xs:documentation>this is defaulted to 'true' as an indication to the post-process tool that it
            should encrypt this element, if the element is not already encrypted (within an XML Security
            envelope).</xs:documentation>
        </xs:annotation>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="PasswordSource">
  <xs:choice>
    <xs:element name="passwordFromLogon" type="Empty"/>
    <xs:element name="passwordFromUser" type="Empty"/>
    <xs:element name="passwordFromProfile" type="PasswordFromProfile"/>
  </xs:choice>
</xs:complexType>
```

```

<xs:complexType name="TokenSource">
  <xs:choice>
    <xs:element name="passwordFromOtherToken" type="Empty">
      <xs:annotation>
        <xs:documentation>this will result in a prompt to user to obtain identity and otp from
token</xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:choice>
</xs:complexType>

<xs:complexType name="TunnelMethods">
  <xs:sequence>
    <xs:choice>
      <xs:element name="validateServerCertificate" type="serverCertificateValidationParameters"/>
      <xs:element name="doNotValidateServerCertificate" type="Empty"/>
    </xs:choice>
    <xs:element name="unprotectedIdentityPattern" type="IdentityPattern" minOccurs="0">
      <xs:annotation>
        <xs:documentation>If the [username] and/or [domain] placeholders are used in the pattern then:
if a client certificate is used for authentication then placeholder's values shall be obtained from the CN
field of the client certificate. if the credentials are obtained from the end-user then they shall be obtained
from the information the user enters. if the credentials are obtained from the operating system then they
shall be obtained from the information the logon provides.</xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
  <xs:choice>
    <xs:element name="enableFastReconnect">
      <xs:complexType>
        <xs:complexContent>
          <xs:extension base="Empty">
            <xs:choice>
              <xs:element name="alwaysAttempt" type="Empty"/>
            </xs:choice>
          </xs:extension>
        </xs:complexContent>
      </xs:complexType>
    </xs:element>
    <xs:element name="disableFastReconnect" type="Empty"/>
  </xs:choice>
</xs:complexType>

```



```

    </xs:choice>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="CertificateContainer">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:element name="certificateId" type="CertificateIdentifier"/>
  </xs:choice>
</xs:complexType>

<xs:complexType name="CertificateIdentifier">
  <xs:simpleContent>
    <xs:annotation>
      <xs:documentation>SHA 1 hash over the whole binary certificate in X509 format that uniquely
      identifies a certificate in the global list of trusted CAs for the machine (OS managed store in
      windows).</xs:documentation>
    </xs:annotation>
    <xs:extension base="NonEmptyString">
      <xs:attribute name="reference" type="xs:boolean">
        <xs:annotation>
          <xs:documentation>true means this is a file reference to a certificate in PEM format, false means
          this is the SHA1 hash over that certificate. This is so the admin does not need to find, cut and paste the
          hash, but rather just point at a file and post process tool will convert it to a hash.</xs:documentation>
        </xs:annotation>
      </xs:attribute>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="Empty"/>

<xs:simpleType name="NonEmptyString">
  <xs:restriction base="xs:string">
    <xs:minLength value="1"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="ServerRuleFormat">
  <xs:simpleContent>

```

```

<xs:extension base="NonEmptyString">
  <xs:attribute name="match" use="required">
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:enumeration value="exactly"/>
        <xs:enumeration value="endsWith"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
</xs:extension>
</xs:simpleContent>
</xs:complexType>

```

```

<xs:complexType name="ServerValidationRules">
  <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:annotation>
      <xs:documentation>

```

This is optional so that the Vista product may allow a profile that has no server validations rules to start with and when a user validates an untrusted server the validation process still validates the server name.</xs:documentation>

```

    </xs:annotation>
    <xs:element name="matchSubjectAlternativeName" type="ServerRuleFormat"/>
    <xs:element name="matchSubject" type="ServerRuleFormat"/>
  </xs:choice>
</xs:complexType>

```

```

<xs:complexType name="serverCertificateValidationParameters">
  <xs:sequence>
    <xs:choice>
      <xs:element name="serverNameValidationRules" type="ServerValidationRules"/>
      <xs:element name="anyServerName" type="Empty">
        <xs:annotation>
          <xs:documentation>the server name within the certificate will not be tested.</xs:documentation>
        </xs:annotation>
      </xs:element>
    </xs:choice>
  </xs:sequence>
  <xs:choice>
    <xs:element name="validateChainWithSpecificCa">

```

```

    <xs:complexType>
      <xs:complexContent>
        <xs:extension base="CertificateContainer"/>
      </xs:complexContent>
    </xs:complexType>
  </xs:element>
  <xs:element name="validateChainWithAnyCaFromOs" type="Empty">
    <xs:annotation>
      <xs:documentation>the certificate chain will be trusted if it ends in a CA cert from the global
      CA cert store.</xs:documentation>
    </xs:annotation>
  </xs:element>
</xs:choice>
<xs:element name="userValidatesUntrustedServerCertificate" type="xs:boolean">
  <xs:annotation>
    <xs:documentation>if the server certificate fails to validate then if this is true the end-user will be
    asked to validate the server. If they do so then appropriate trustedCaCerts will be remembered as well
    as the server name fields so it will be automatically trusted in the future.</xs:documentation>
  </xs:annotation>
</xs:element>
</xs:sequence>
</xs:complexType>

</xs:schema>

```

The LEAP XML Schema

The LEAP module stores all settings in the Native EAP method section of the network profile as XML by using the following schema:

```

<?xml version="1.0"?>

<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.cisco.com/CCX"
  targetNamespace="http://www.cisco.com/CCX"
  elementFormDefault="qualified"

```

```
attributeFormDefault="unqualified">
```

```
<xs:element name="eapLeap" type="EapLeap"/>
```

```
<xs:complexType name="EapLeap">
```

```
<xs:complexContent>
```

```
<xs:extension base="PasswordMethods"/>
```

```
</xs:complexContent>
```

```
</xs:complexType>
```

```
<xs:complexType name="IdentityPattern">
```

```
<xs:simpleContent>
```

```
<xs:extension base="NonEmptyString">
```

```
<xs:attribute name="encryptContent" type="xs:boolean" use="optional" default="true">
```

```
<xs:annotation>
```

<xs:documentation>this is defaulted to 'true' as an indication to the post-process tool that it should encrypt this element, if the element is not already encrypted (within an XML Security envelope).</xs:documentation>

```
</xs:annotation>
```

```
</xs:attribute>
```

```
</xs:extension>
```

```
</xs:simpleContent>
```

```
</xs:complexType>
```

```
<xs:complexType name="PasswordFromProfile">
```

```
<xs:simpleContent>
```

```
<xs:extension base="xs:string">
```

```
<xs:attribute name="encryptContent" type="xs:boolean" use="optional" default="true">
```

```
<xs:annotation>
```

<xs:documentation>this is defaulted to 'true' as an indication to the post-process tool that it should encrypt this element, if the element is not already encrypted (within an XML Security envelope).</xs:documentation>

```
</xs:annotation>
```

```
</xs:attribute>
```

```
</xs:extension>
```

```
</xs:simpleContent>
```

```
</xs:complexType>
```

```
<xs:complexType name="PasswordSource">
```

```
<xs:choice>
  <xs:element name="passwordFromLogon" type="Empty"/>
  <xs:element name="passwordFromUser" type="Empty"/>
  <xs:element name="passwordFromProfile" type="PasswordFromProfile"/>
</xs:choice>
</xs:complexType>

<xs:complexType name="PasswordMethods">
  <xs:sequence>
    <xs:element name="unprotectedIdentityPattern" type="IdentityPattern" minOccurs="0"/>
    <xs:element name="passwordSource" type="PasswordSource"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="Empty"/>

<xs:simpleType name="NonEmptyString">
  <xs:restriction base="xs:string">
    <xs:minLength value="1"/>
  </xs:restriction>
</xs:simpleType>

</xs:schema>
```

Logging for EAP Modules

To generate logs to assist with troubleshooting, the EAP-FAST, LEAP, and PEAP-GTC modules utilize Windows Event Log Service. The logs include information such as the type of event, the event location, the function that was affected by the event, and the date and time of the event.

The following sections contain information about logging:

- [Configuring and Starting Logging, page 4-26](#)
- [Disabling Logging and Flushing Internal Buffers, page 4-27](#)
- [Locating Log Files, page 4-28](#)

Configuring and Starting Logging

To access the administrator command prompt and to configure and start logging, perform the following steps:

-
- Step 1** Choose **Start > All Programs > Accessories**.
- Step 2** Right-click **Command Prompt** and select **Run as administrator**.
- Step 3** At the prompt, enter the following command to configure and start logging:
- For EAP-FAST
`wevtutil sl Cisco-EAP-FAST/Debug /e:true /k:category_mask /l:log_level`
 - For PEAP-GTC
`wevtutil sl Cisco-EAP-PEAP/Debug /e:true /k:category_mask /l:log_level`
 - For LEAP
`wevtutil sl Cisco-EAP-LEAP/Debug /e:true /k:category_mask /l:log_level`

Syntax Description		
<i>category_mask</i>		Bitmask of categories of logging to be turned on. Valid values are as follows: <ul style="list-style-type: none"> • 0—logs all categories. • 1—logs all messages not falling into the next two categories. • 2—logs the flow of function entry and exit points with return code only on Verbose log level. • 4—logs packet dumps only on Verbose log level. The default value is 0.
<i>log_level</i>		Level of logging to be turned on. Valid values are as follows: <ul style="list-style-type: none"> • 0—all log levels. • 1—critical. • 2—error. • 3—warning. • 4—informational. • 5—verbose. The default value is 0.

**Note**

If you must shut down the device on which logging was running before logging finishes, logging resumes after reboot. When logging is started either automatically or manually, however, the logs are cleared.

Disabling Logging and Flushing Internal Buffers

After you have collected the information that you need, the following command stops logging and flushes all internal buffers:

- For EAP-FAST


```
wevtutil sl Cisco-EAP-FAST/Debug /e:false
```
- For PEAP-GTC


```
wevtutil sl Cisco-EAP-PEAP/Debug /e:false
```
- For LEAP


```
wevtutil sl Cisco-EAP-LEAP/Debug /e:false
```

**Note**

You must enter this command before you can analyze the .etl file.

Locating Log Files

By default, an .etl file that you can use for analysis and debugging are created at this location:

C:\Windows\System32\Winevt\Logs\Cisco-EAP-FAST%4Debug.etl

If you would like to change this location, enter this command at the administrator prompt:

- For EAP-FAST
wevtutil sl Cisco-EAP-FAST/Debug /fn:"path_to_etl_log_file"
- For PEAP-GTC
wevtutil sl Cisco-EAP-PEAP/Debug /fn:"path_to_etl_log_file"
- For LEAP
wevtutil sl Cisco-EAP-LEAP/Debug /fn:"path_to_etl_log_file"



Note Logging must not be running when you enter the command to change the path to the log file.

You can also change the path to the .etl file when you start logging. To start logging and specify the location of the .etl file, enter this command at the administrator prompt:

- For EAP-FAST
wevtutil sl Cisco-EAP-FAST/Debug /e:true /fn:"path_to_etl_log_file"
- For PEAP-GTC
wevtutil sl Cisco-EAP-PEAP/Debug /e:true /fn:"path_to_etl_log_file"
- For LEAP
wevtutil sl Cisco-EAP-LEAP/Debug /e:true /fn:"path_to_etl_log_file"



CHAPTER 5

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 5-2](#)
- [Upgrading the Client Adapter Software, page 5-3](#)

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 that are not designed for portable use, you should have little reason to remove the adapter. However, instructions are provided below if 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.
-

Upgrading the Client Adapter Software

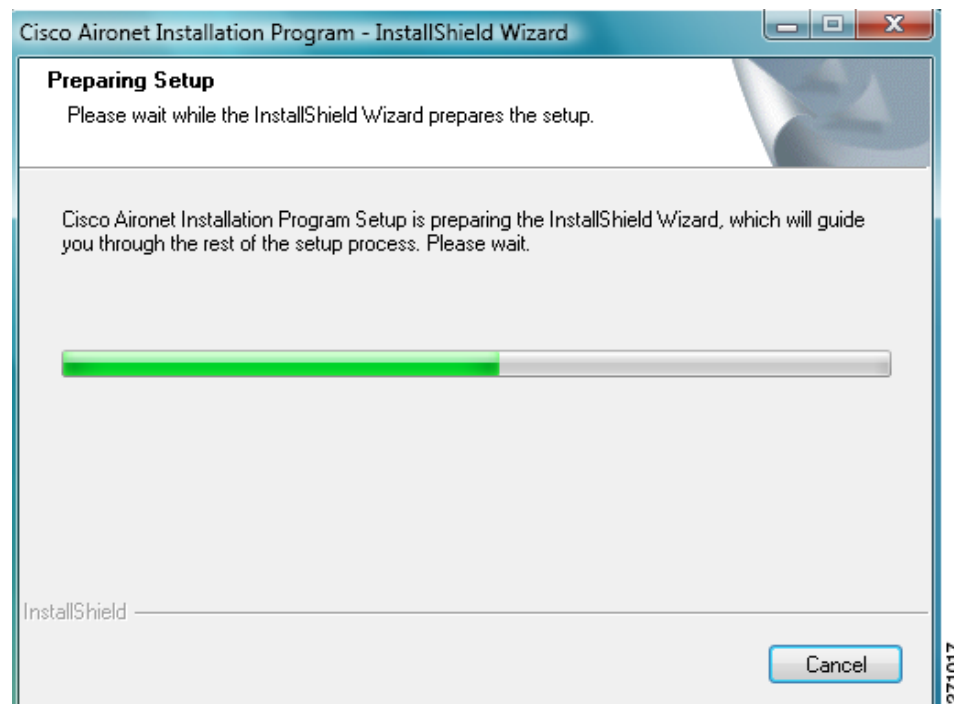
**Note**

Before you upgrade the software, ensure that the client adapter is inserted properly.

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

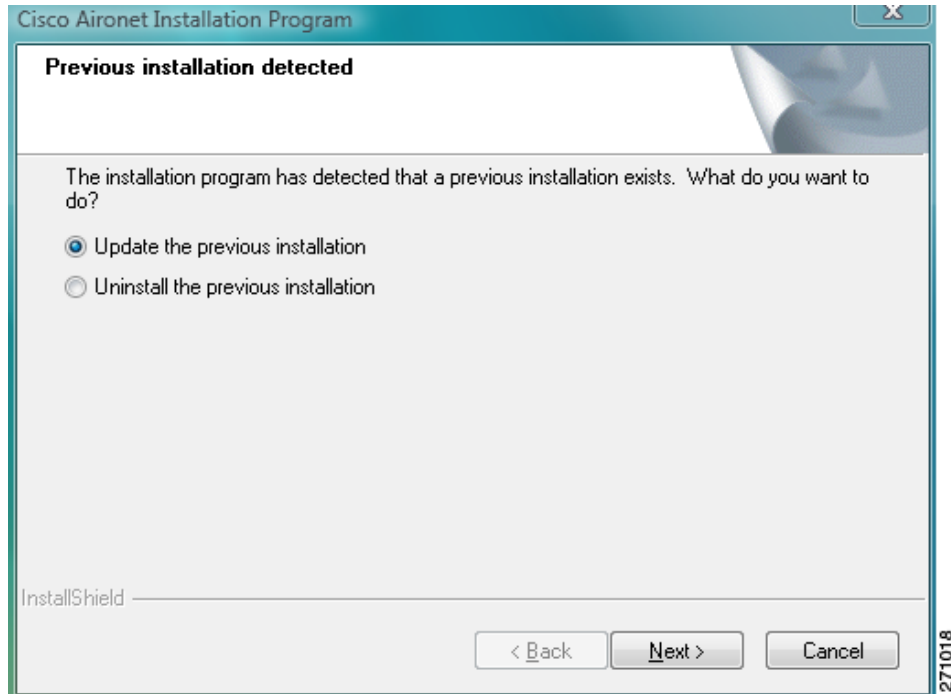
- Step 1** Obtain the desired software release. For instructions on obtaining software from Cisco.com, see the [“Obtaining Client Adapter Software”](#) section of Chapter 1 “Product Overview and Installation.”
- Step 2** Double-click the software **WinClient-802.11a-b-g-Vista-Ins-Wizard-vxx.exe** file that you have saved on the device on which the client adapter is inserted. A window appears that asks you if you want to run the software file.
- Step 3** Click **Run**. The Cisco Aironet Installation Program - InstallShield window appears (see [Figure 5-1](#)).

Figure 5-1 Cisco Aironet Installation Program—Installation Wizard Preparing Setup Window



- Step 4** Allow the preparation sequence to finish. After the preparation sequence finishes, the Cisco Aironet Installation Program—Previous installation detected window appears (see [Figure 5-2](#)).

Figure 5-2 Cisco Aironet Installation Program—Previous installation detected Window



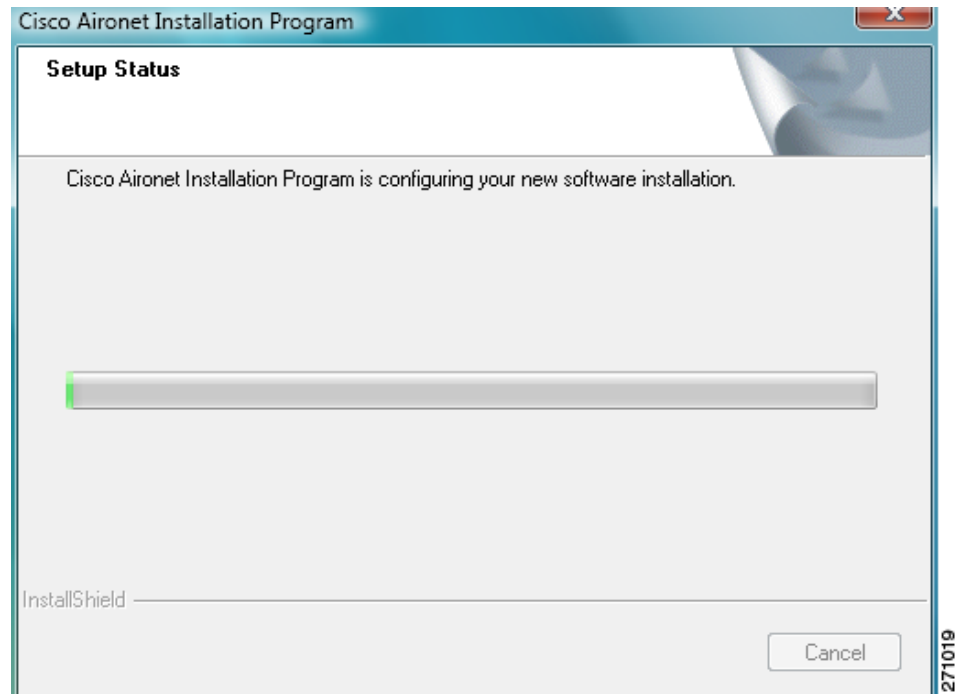
Step 5 Click **Update the previous installation**.



Note If you click **Uninstall the previous installation**, a dialog box asks you to confirm the complete removal of the previous installation. If you remove the previous installation instead of updating it, you remove all configured wireless profiles.

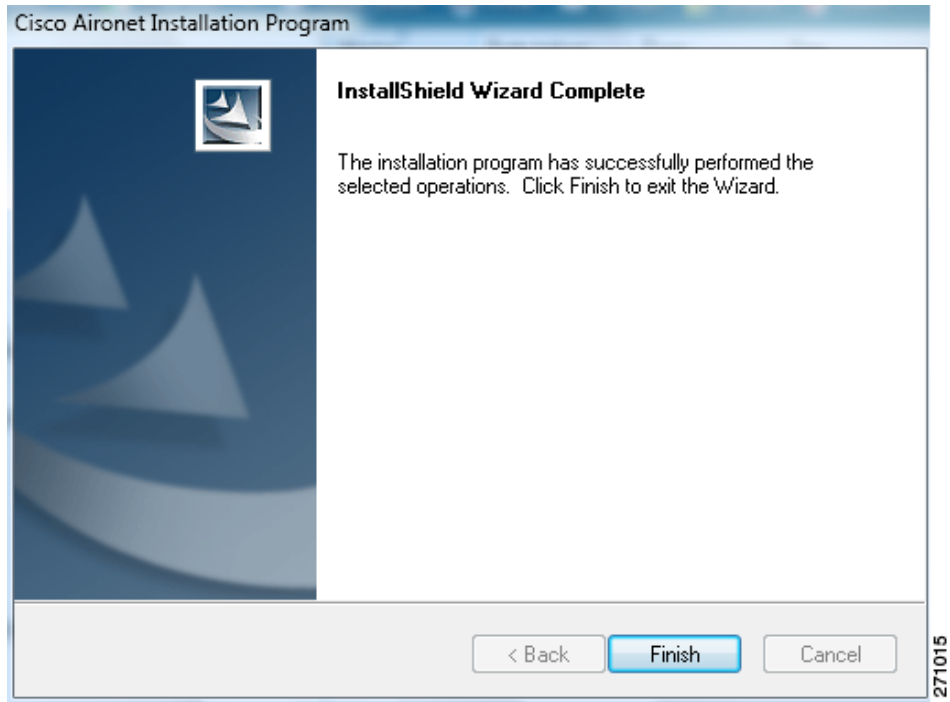
Step 6 Click **Next**. The Cisco Aironet Installation Program—Setup Status window appears (see [Figure 5-3](#)).

Figure 5-3 Cisco Aironet Installation Program—Setup Status Window



- Step 7** Allow the software installation to finish. After the installation finishes, the Cisco Aironet Installation Program—InstallShield Wizard Complete window appears (see [Figure 5-4](#)).

Figure 5-4 Cisco Aironet Installation Program—InstallShield Wizard Complete Window



Step 8 Click **Finish**.



CHAPTER 6

Troubleshooting and Diagnostics

This chapter provides information about diagnosing problems that might occur when you try to operate the client adapter.

The following topics are covered in this chapter:

- [Troubleshooting with Cisco Aironet Client Diagnostics, page 6-2](#)
- [Enabling Client Reporting, page 6-6](#)

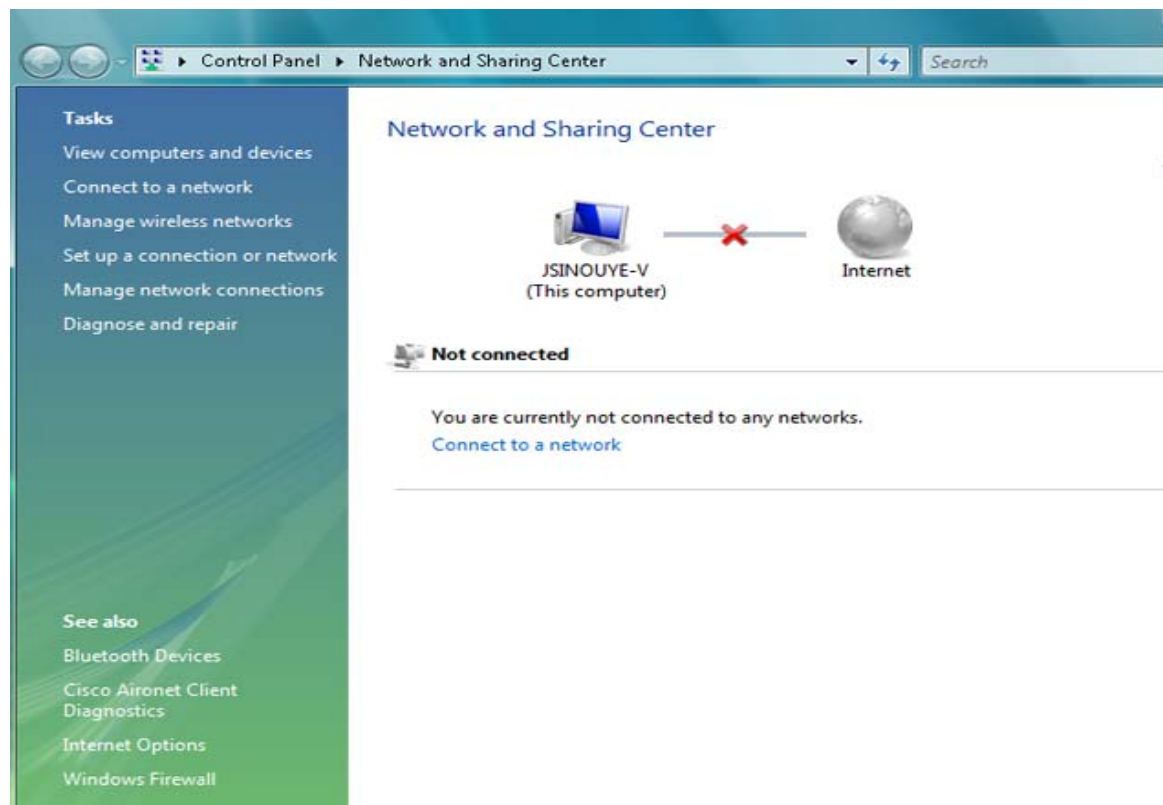
Troubleshooting with Cisco Aironet Client Diagnostics

Cisco Aironet Client Diagnostics is a mode that identifies communication problems between the client adapter and a wireless LAN infrastructure device. When in this mode, the client adapter and the infrastructure device proceed through a defined set of tests. The results of these tests can assist in isolating conditions that require troubleshooting.

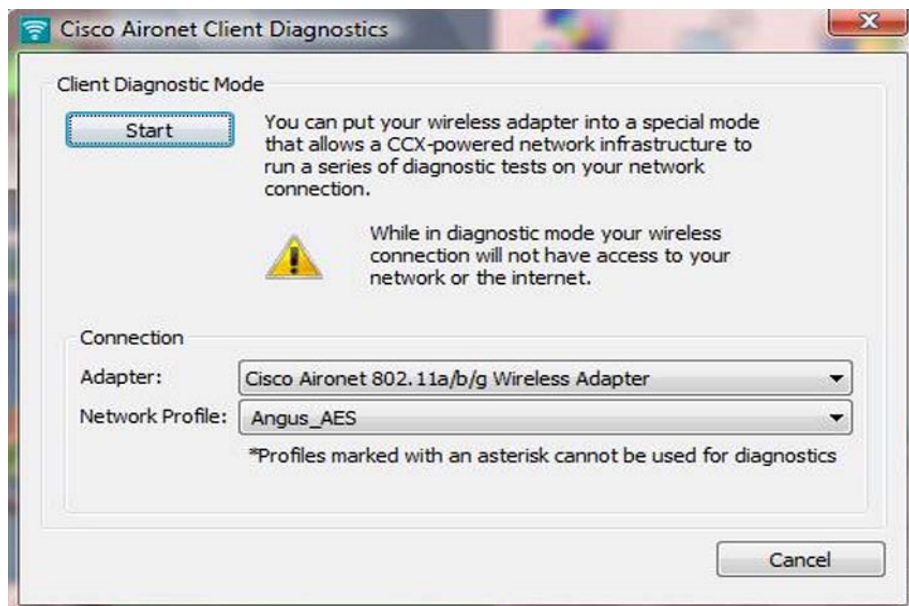
Cisco Aironet Client Diagnostics can only be started manually. To start this mode, follow these steps:

- Step 1** Verify that the client adapter radio is enabled. If the radio is not enabled, enable it.
- Step 2** Choose **Start > Control Panel > Network and Sharing Center**. The Network and Sharing Center window opens (see [Figure 6-1](#)).

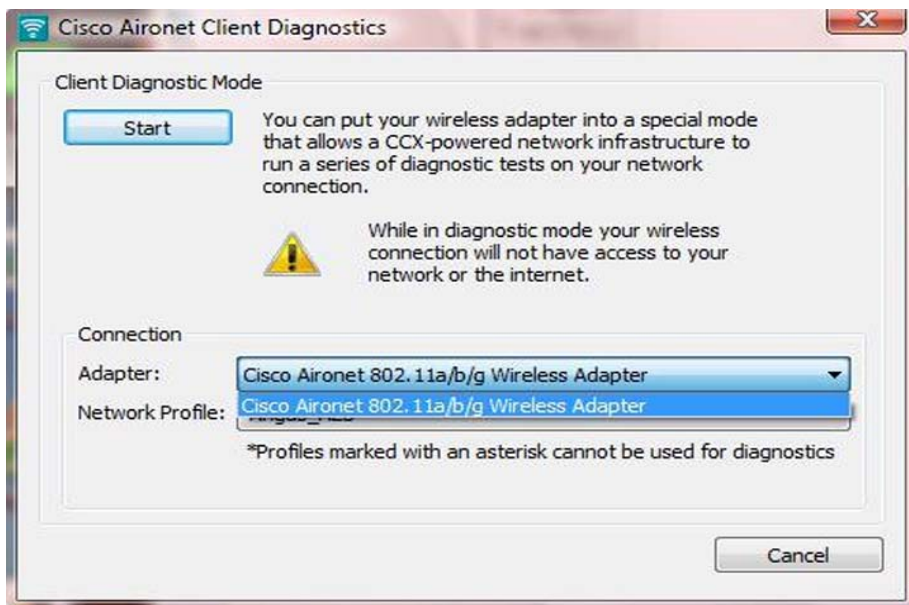
Figure 6-1 Network and Sharing Center Window



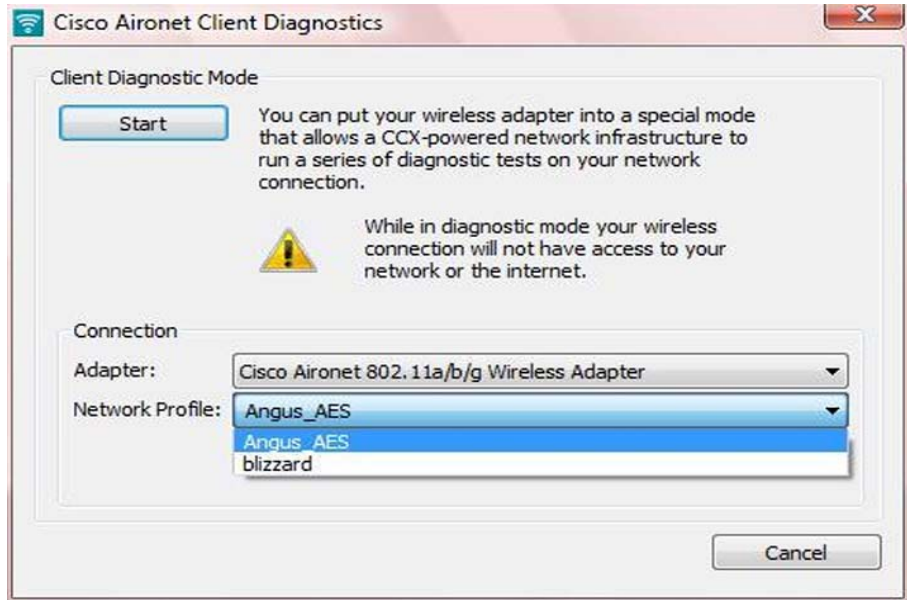
- Step 3** Click **Cisco Aironet Client Diagnostics**. The Cisco Aironet Client Diagnostics dialog box appears (see [Figure 6-2](#)).

Figure 6-2 Cisco Aironet Client Diagnostics Dialog Box

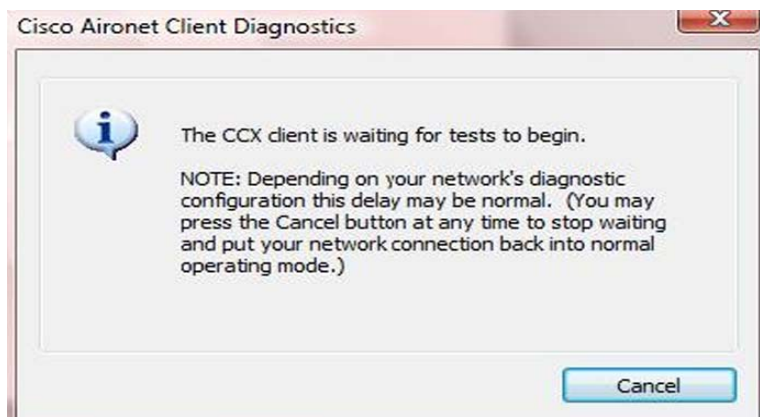
- Step 4** In the Cisco Aironet Client Diagnostics dialog box, choose **Cisco Aironet 802.11a/b/g Wireless Adapter** in the Adapter field (see [Figure 6-3](#)).

Figure 6-3 Cisco Aironet Client Diagnostics Dialog Box—Choose Adapter

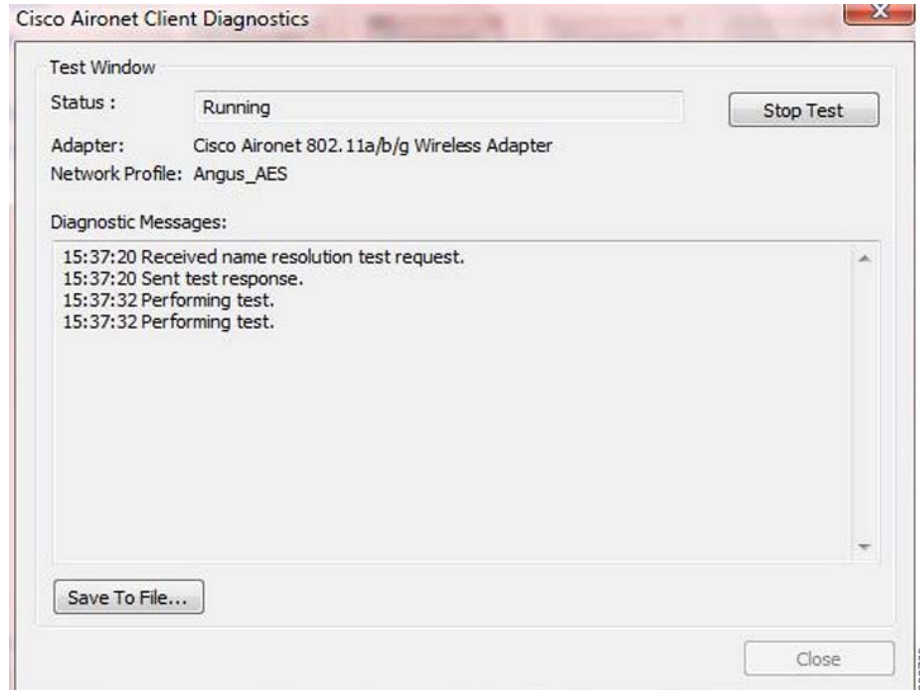
- Step 5** Choose the profile for diagnostics testing in the Network Profile field (see [Figure 6-4](#)).

Figure 6-4 Cisco Aironet Client Diagnostics Dialog Box—Choose Network Profile

- Step 6** Click **Start** to run the diagnostics. If testing does not begin immediately, a message appears to explain the delay (see [Figure 6-5](#)).

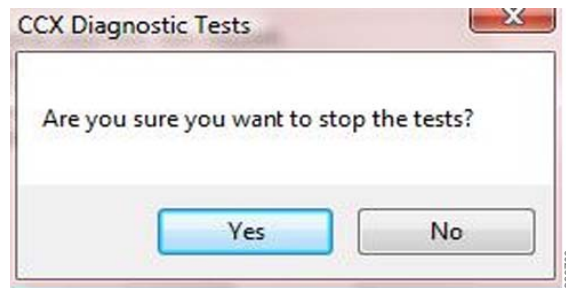
Figure 6-5 Cisco Aironet Client Diagnostics Dialog Box—Testing Delay

- Step 7** Monitor the status of diagnostics testing in the Cisco Aironet Client Diagnostics Test Window (see [Figure 6-6](#)).

Figure 6-6 Cisco Aironet Client Diagnostics Dialog Box—Test Window

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

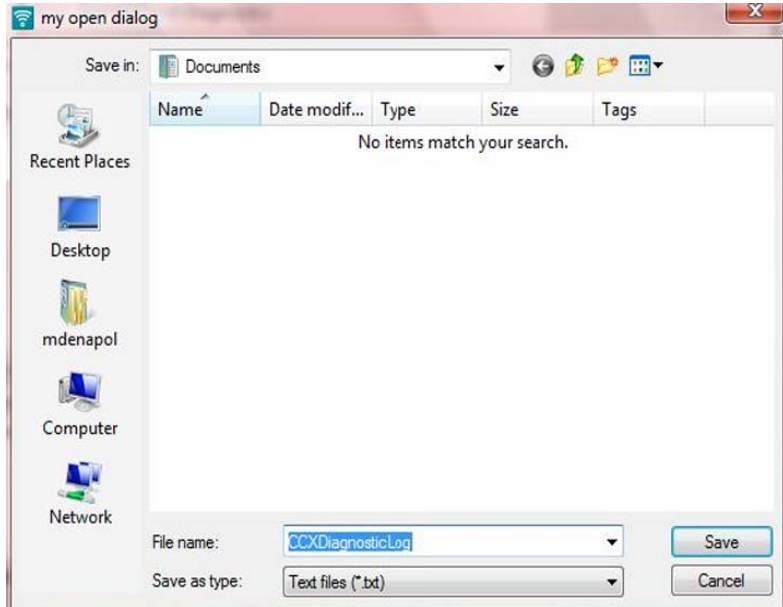
While the client is in diagnostics testing mode, if you click on the **Close** button, an Aironet Desktop Utility window appears to confirm that you want to stop running in DC mode (see [Figure 6-7](#)).

Figure 6-7 Aironet Desktop Utility—Stop Running Diagnostics

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

- Step 8** When diagnostic testing is complete, you can click the **Save To File** 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 6-8](#)). 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 6-8 Saving Diagnostics Testing Report—Documents Window



Enabling Client Reporting

A network administrator must enable a profile for client reporting so that the profile can participate in Cisco Aironet Client Diagnostics.

To enable a profile for client reporting, follow these steps:

-
- Step 1** With the Microsoft Group Policy Object Editor, locate the XML portion of the profile that is related to client reporting. Here is a sample CCX profile section that shows the XML element for client reporting:
- ```
<Diagnostics>
 <AuthorizedProfile>true</AuthorizedProfile>
 <Channel>
 <EnableClientReporting>true</EnableClientReporting>
 </Channel>
</Diagnostics>
```
- Step 2** For the EnableClientReporting XML element, change the value to **true** to enable client reporting. Change the value to **false** to disable client reporting.
- 

For more information about Microsoft Group Policy Objects, see the “[Using Microsoft Tools to Perform Administrative Tasks](#)” section of Chapter 4, “Performing Administrative Tasks.”



# APPENDIX **A**

## EAP Messages

---

This appendix describes EAP-FAST, PEAP-GTC and LEAP error messages and prompts. This appendix also provides guidelines for creating strong passwords.

The following topics are covered in this appendix:

- [EAP-FAST Error Messages and Prompts, page A-1](#)
- [PEAP-GTC and LEAP Error Messages and Prompts, page A-6](#)
- [Creating Strong Passwords, page A-9](#)

## EAP-FAST Error Messages and Prompts

**Error Message** Automatic PAC provisioning is enabled for this profile. However, a valid PAC that matches the server to which the client adapter is connecting could not be found. Do you wish to obtain a new security credential (PAC)?

**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 will fail the authentication.



### Caution

---

To prevent possible attacks from rogue access points, do not reprovision a PAC unless it is necessary.

---

**Error Message** While attempting to provision your PAC during auto-provisioning, the network access device failed to authenticate itself. This condition might indicate an attack on your password by a rogue access device. Try again with your current password?

**Recommended Action** Click **Yes** to attempt to reauthenticate with your current password. Click **No** to cancel the operation.



### Note

---

If the authentication attempt fails again, contact your system administrator to report a rogue access device. Use strong passwords in the future to reduce the chance of your password being compromised; see the [“Creating Strong Passwords”](#) section on page A-9 for tips on creating strong passwords.

---

**Error Message** While attempting to provision your PAC, the network access device timed out. A timeout might indicate an attack on your password by a rogue access device. However, a timeout could be caused by a server outage or a faulty connection. Try again with your current password?

**Recommended Action** Click **Yes** to attempt to reauthenticate with your current password. Click **No** to cancel the operation.

**Note**

If a timeout occurs again, contact your system administrator to report a potential rogue access device. Use strong passwords in the future to reduce the chance of your password being compromised; see the [“Creating Strong Passwords”](#) section on page A-9 for tips on creating strong passwords.

**Error Message** A valid PAC was not found for your username <username>. Click **OK**. Re-enter your username in the credential prompt or the User Credentials tab of the EAP-FAST Properties screen. If you entered your username correctly, go to the Connection tab of the EAP-FAST Properties screen either to enable automatic PAC provisioning or Validate server certificate or import a PAC file.

**Recommended Action** Click **OK**. Then perform one of the following:

- Re-enter your username.
- If you entered your username correctly, go to the Connection tab of the EAP-FAST Properties screen either to enable automatic PAC provisioning or to import a PAC file.

**Error Message** The EAP-FAST authentication attempt failed because you entered the wrong username and password. Please re-enter your username and password.

**Recommended Action** Click **OK**. Then re-enter your EAP-FAST credentials when the Enter Wireless Network Password screen appears.

**Error Message** The EAP-FAST authentication attempt failed because you might have entered the wrong username and password. Please re-enter your username and password.

Warning: If you are sure that you have typed in the right username and password, you may have connected to a rogue device. This can indicate an attack on your password. Using a strong password will reduce the chance of your password being compromised. If this failure happens again, contact your system administrator to report a potential rogue access device.

**Recommended Action** Click **OK**. Then perform one of the following:

- If you entered your EAP-FAST credentials correctly, contact your system administrator to report a potential rogue access point. Use strong passwords in the future to reduce the chance of your password being compromised. See the [“Creating Strong Passwords”](#) section on page A-9 for tips on creating strong passwords.
- If you entered your EAP-FAST credentials incorrectly, re-enter your credentials at the Enter Wireless Network Password screen.

- If the username does not match the provisioned PAC, and automatic provisioning is enabled for this profile, click **Yes** at the following message: “You do not appear to be registered with the authentication server. Registration requires that this device be initialized with a security credential. Do you wish to obtain a security credential?”
- If the username does not match the provisioned PAC, and manual provisioning is enabled for this profile, go to the Connection tab of the EAP-FAST properties dialog box and either enable automatic PAC provisioning or import a PAC file.

**Error Message** PAC provisioning has failed. This failure is not related to an issue with the username and password. This failure is commonly caused by a server configuration issue. Contact your administrator for assistance.

**Recommended Action** Contact your system administrator for assistance.

**Error Message** The PAC that you selected for this profile does not match the server to which the client is connecting. However, a matching PAC has been found in your PAC database. Would you like to use this matching credential authority and save it to the profile?

**Recommended Action** Click **Yes** to use the matching PAC and to update the profile with this new PAC, or click **No** to cancel the operation and to leave the profile as it is. If you click **No**, the client adapter will be unable to authenticate using the existing profile.

**Error Message** You entered different values in the New Password field and the Confirm New Password field. The passwords must be identical. Please try again.

**Recommended Action** Re-enter your new password in both fields.

**Error Message** The password that you entered in the Old Password field does not match the password that you previously used. Please try again.

**Recommended Action** Re-enter your old password in the Old Password field.

**Error Message** An error occurred when you attempted to change your EAP-FAST password. The new password might not conform to the server's password policy. Please try again.

**Recommended Action** Re-enter your password in the Change Password screen.

**Error Message** The EAP-FAST authentication process failed during initialization. Make sure that EAP-FAST and the Trusted Root Certificate Authority certificate are installed correctly.

**Recommended Action** Ensure that EAP-FAST and the Trusted Root Certificate Authority certificate are installed correctly.

**Error Message** You have connected to a server with the following server name

<server\_name>

The server certificate is signed by the following Root Certification Authority (CA):

<root\_ca>

This Root CA does not match the specified trusted Root CA(s).

Do you want to accept this connection?

Warning: Connecting to a server signed with untrusted CA might compromise your security.

**Recommended Action** If you want the client adapter to connect to this server even though doing so might present a security risk, click **Yes**. Otherwise, click **No**.

**Error Message** You have connected to a server with the following server name:

<server\_name>

This server name does not match the specified server name(s).

Do you want to accept this connection?

Warning: Connecting to an unsecured server might compromise your security.

**Recommended Action** If you want the client adapter to connect to this server even though doing so might present a security risk, click **Yes**. Otherwise, click **No**.

**Error Message** Your password has expired. Please enter a new password.

**Recommended Action** Enter a new password to change the expired password.

**Error Message** You entered an empty username, which is not allowed.

**Recommended Action** Enter a username.

**Error Message** You must select a PAC when using manual PAC provisioning.

**Recommended Action** You clicked **OK** on the EAP-FAST Properties screen when automatic provisioning was disabled and no PAC authority was selected. Either enable automatic provisioning or choose a PAC authority from the drop-down list. If the list is empty, import a PAC file.

**Error Message** Error opening or reading file: <filename>.

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



**Error Message** The file is not a valid PAC file: <filename>.

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

**Error Message** The file does not contain a valid PAC: <filename>.

**Recommended Action** Try to import the PAC file again. If the same message appears, obtain a new PAC file from your system administrator and import it using the EAP-FAST Settings screen.

**Error Message** The file contains a PAC that will replace an existing PAC already provisioned on your system. Would you like to replace the existing PAC?

**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 password you entered to import the PAC file is incorrect. Please try again.

**Recommended Action** Try entering your password again.

**Error Message** The PAC file import operation has been aborted because of three or more attempts of incorrect passwords.

**Recommended Action** Press **OK** to continue.

**Error Message** An internal error occurred.

**Recommended Action** An internal error occurred when the PAC was being imported. Try importing the PAC again.

**Error Message** Insufficient memory or other system error.

**Recommended Action** Close other programs and free up some more memory.

**Error Message** You must select "Validate server certificate" or a PAC to use user's certificate or one-time password for authentication.

**Recommended Action** One-time password or user certificate is selected as the user credential, but there is no PAC selected or Validate Server Certificate option is not checked. Change the settings.

**Error Message** You tried to import a PAC file with the same PAC ID as a previously imported or provisioned PAC. Would you like to replace the existing PAC?

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

# PEAP-GTC and LEAP Error Messages and Prompts

**Error Message** There is an error in the configuration profile. Please verify the configuration and save it.

**Recommended Action** Authentication with this profile fails until the profile is fixed. Contact your network administrator for assistance with fixing the profile.

**Error Message** No trusted CA(s) selected.

**Recommended Action** Select at least one trusted CA, or allow the user to authorize new trusted CAs.

**Error Message** You entered an empty username, which is not allowed.

**Recommended Action** Enter a username.

**Error Message** You entered different values in the Password field and the Confirm password field. The passwords must be identical.

**Recommended Action** Re-enter your password in both fields.

**Error Message** You entered different values in the New Password field and the Confirm New Password field. The passwords must be identical.

**Recommended Action** Re-enter your password in both fields.

**Error Message** The password that you entered in the Old password field does not match the password that was used previously.

**Recommended Action** Re-enter your old password in the Old password field.

**Error Message** You have connected to a server with the following server name:

<server-name>

This server name does not match the specified server name(s).

In addition, the server certificate is signed by the following Root Certification Authority (CA):

<ca-name>

This Root CA does not match the specified trusted Root CA(s).

Do you want to accept this connection?

Warning: You might compromise your security if you connect to an unsecured server that is signed by an untrusted Root CA.

**Recommended Action** If you want to connect to this server even though it may present a security risk, click **Yes**. Otherwise, click **No**.

**Error Message** You have connected to a server with the following server name:

<server-name>

The server certificate is signed by the following Root Certification Authority (CA):

<ca-name>

This Root CA does not match the specified trusted Root CA(s).

Do you want to accept this connection?

Warning: You might compromise your security if you connect to an unsecured server that is signed by an untrusted Root CA.

**Recommended Action** If you want to connect to this server even though it may present a security risk, click **Yes**. Otherwise, click **No**.

**Error Message** You have connected to a server with the following server name:

<server-name>

This server name does not match the specified server name(s).

Do you want to accept this connection?

Warning: You might compromise your security if you connect to an unsecured server.

**Recommended Action** If you want to connect to this server even though it may present a security risk, click **Yes**. Otherwise, click **No**.

**Error Message** The operation was canceled by the user.

**Recommended Action** Contact your network administrator for further assistance.

**Error Message** The authentication failed because Windows does not have the authentication method required for this network.

**Recommended Action** Contact your network administrator for further assistance.

**Error Message** Windows cannot connect to this network.

The user credentials were rejected by the server.

**Recommended Action** Contact your network administrator for further assistance.

**Error Message** Windows cannot connect to this network.

There is a problem with the certificate on the server required for authentication.

**Recommended Action** Contact your network administrator for further assistance.

**Error Message** Windows cannot connect to "<network-name>"

Wireless authentication failed.

**Recommended Action** Contact your network administrator for assistance with the specified network.

**Error Message** The authentication failed because of unknown reason. The error condition was reported by cryptographic subsystem.

**Recommended Action** Contact your network administrator for further assistance.

**Error Message** The network device failed to authenticate itself.

The failure can indicate an attack on your password.

**Recommended Action** Use a strong password to reduce the risk of compromising your password. For more information about creating a strong password, see the [“Creating Strong Passwords” section on page A-9](#). If the authentication attempt fails again, contact your system administrator to report a rogue access device.

# Creating Strong Passwords

Never write passwords down, on paper or online. Instead, create passwords that you can remember easily but no one can guess easily. One way to do this is create a password that is based on a song title, affirmation, or other phrase. For example, the phrase could be “This May Be One Way To Remember” and the password could be “TmB1w2R!” or “Tmb1W>r~” or some other variation.

**Note**

---

Do not use either of those examples as passwords.

---

## Characteristics of Strong Passwords

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Contain numerals and punctuation as well as letters (e.g., 0-9, !@#%&^&\*()\_+!~ =\`{}[]:;'<>?,./)
- Are at least five alphanumeric characters long.
- Are not a word in any language.
- Are not slang, dialect, or jargon.
- Are not based on personal information, such as the names of family members.

## Characteristics of Weak Passwords

A weak password has the following characteristics:

- Contains fewer than eight characters.
- Is a word found in a dictionary (English or foreign)
- Is any other term that is easily guessed or found in common usage. The following are examples of terms that are easily guessed:
  - The name of family, pet, friend, coworker, or fantasy character.
  - A computing term or name, such as a command, site, company, model, or application.
  - A birthday or another kind of personal information, such as an address or telephone number.
  - A predictable letter pattern or number pattern, such as aaabbb, qwerty, zyxwvuts, or 123321.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit.

## Password Security Basics

Follow these basic guidelines when dealing with passwords:

- Never reveal a password, even to family members.
- Never talk about a password in front of others.
- Never hint at the format of a password (such as “my family name”).
- Never use characters from outside the standard ASCII character set. Some symbols, such the pound sterling symbol (£), are known to cause login problems on some systems.



# APPENDIX **B**

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

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

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

<b>Physical Specifications</b>	
<b>Size</b>	
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)
<b>Weight</b>	
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)
<b>Enclosure</b>	
PC-Cardbus card	Type II Cardbus
PCI card	Standard or low-profile Type II PCI
<b>Connector</b>	
PC-Cardbus card	68-pin Cardbus
PCI card	62-pin PCI
Status indicators	Green and amber LEDs; see <a href="#">Chapter 1</a>
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 B-1** Technical Specifications for CB21AG and PI21AG Client Adapters (continued)

<b>Radio Specifications</b>	
Type	
802.11a	Orthogonal frequency division multiplexing (OFDM)
802.11b/g	Direct-sequence spread spectrum (DSSS) and orthogonal frequency division multiplexing (OFDM)
Power output	
<b>Note</b> Refer to <a href="#">Appendix E</a> 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 <b>Note</b> 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 <b>Note</b> 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 B-1** Technical Specifications for CB21AG and PI21AG Client Adapters (continued)

Receiver sensitivity	
802.11a	<p><b><u>5150 to 5250 MHz</u></b>            –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><b><u>5250 to 5350 MHz</u></b>            –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><b><u>5470 to 5725 MHz</u></b>            –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><b><u>5725 to 5805 MHz</u></b>            –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 B-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	<b>Indoor (typical)</b> 500 ft (152 m) @ 6 Mbps 400 ft (122 m) @ 18 Mbps 90 ft (27 m) @ 54 Mbps  <b>Note</b> 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.	<b>Outdoor (typical)</b> 950 ft (290 m) @ 6 Mbps 800 ft (244 m) @ 18 Mbps 170 ft (52 m) @ 54 Mbps
802.11b/g	<b>Indoor (typical)</b> 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  <b>Note</b> 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.	<b>Outdoor (typical)</b> 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 B-1** Technical Specifications for CB21AG and PI21AG Client Adapters (continued)

<b>Power Specifications</b>	
Operational voltage	3.3 V ( $\pm$ 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
<b>Safety and Regulatory Compliance Specifications</b>	
Safety	Designed to meet: <ul style="list-style-type: none"> <li>• UL 60950</li> <li>• CSA 22.2 No. 60950</li> <li>• IEC 60950 Second Ed., including Amendments 1-4 with all national deviations</li> <li>• EN 60950 Second Ed., including Amendments 1-4</li> </ul>
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 **C**

# 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 C-2](#)
- [Antenna Installation Warning, page C-3](#)
- [Warning for Laptop Users, page C-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 onbeschermd 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 tändhattar eller i en explosiv miljö om inte enheten modifierats för att kunna användas i sådana sammanhang.

# Antenna Installation Warning



---

<b>Warning</b>	<b>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.</b>
<b>Waarschuwing</b>	<b>Om te voldoen aan de FCC radiofrequentie (RF) blootstellingslimieten dienen antennes zich minstens 20 cm of meer van de lichamen van alle personen bevinden.</b>
<b>Varoitus</b>	<b>FCC:n antamien radiotaajuuksille altistumista koskevien rajoitusten mukaan antennien on sijaittava vähintään 20 cm:n päässä kaikista henkilöistä.</b>
<b>Attention</b>	<b>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.</b>
<b>Warnung</b>	<b>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.</b>
<b>Avvertenza</b>	<b>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.</b>
<b>Advarsel</b>	<b>I henhold til eksponeringsgrensene for radiofrekvenser (RF), skal antenner befinne seg på en avstand av minst 20 cm eller mer fra mennesker.</b>
<b>Aviso</b>	<b>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.</b>
<b>¡Advertencia!</b>	<b>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.</b>
<b>Varning!</b>	<b>För att följa FCC-exponeringsgränserna för radiofrekvens (RF), bör antenner placeras på minst 20 cm avstånd från alla människor.</b>

---

# 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-bepalingen 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 anteeniin 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 ohjeita. Tätä laitetta ja sen antennia ei saa käyttää samassa pisteessä toisen antennin tai lähettimen kanssa tai liitettynä toiseen anteeniin 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 portatile. 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 ad 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 radiofrekvens exponering (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 antennenavståndet 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 **D**

# 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 D-2](#)
- [Department of Communications – Canada, page D-3](#)
- [European Community, Switzerland, Norway, Iceland, and Liechtenstein, page D-3](#)
- [Declaration of Conformity for RF Exposure, page D-7](#)
- [Guidelines for Operating Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters in Japan, page D-7](#)
- [Administrative Rules for Cisco Aironet CB21AG and PI21AG Wireless LAN Client Adapters in Taiwan, page D-8](#)
- [Brazil/Anatel Approval, page D-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.
Ελληνικά:	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*

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

The following standards were applied:

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

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 that reads "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 CB21AG and PI21AG Wireless LAN Client Adapters in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet CB21AG and PI21AG 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 : 03-6434-6500

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 CB21AG and PI21AG 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

### 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****1051-05-1086****(01)07898362231452**

"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 **E**

# 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 E-2](#)
- [Maximum Power Levels and Antenna Gains, page E-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 E-1](#).

**Table E-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 E-2](#).

**Table E-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 E-3](#) indicates the maximum EIRP supported for all regulatory domains for each 5 GHz IEEE 802.11a data rate.

**Table E-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 E-4](#) indicates the maximum EIRP supported for all regulatory domains for each 2.4 GHz IEEE 802.11b data rate.

**Table E-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 E-5](#) indicates the maximum EIRP supported for all regulatory domains for each 2.4 GHz IEEE 802.11g data rate.

**Table E-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 **F**

## Acknowledgments and Licensing

---

This product includes software developed by the OpenSSL Project for use in the OpenSSL toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

OpenSSL License  
-----

```
/* =====
* Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
```

```
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
* =====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
```

```
Original SSLeay License

```

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the rouines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
```

```
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```







## Abbreviations

---

Table G-1 defines the acronyms used in this publication.

**Table G-1** List of Acronyms

Acronym	Expansion
AAA	authentication, authorization, and accounting
API	application program interface
ASCII	American Standard Code for Information Interchange
CA	Certificate Authority
CCX	Cisco Compatible eXtensions
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol—Flexible Authentication via Secure Tunneling
EAP-GTC	Extensible Authentication Protocol—Generic Token Card
EAP-MSCHAPv2	Extensible Authentication Protocol—Microsoft Challenge Handshake Authentication Protocol Version 2
EAP-TLS	Extensible Authentication Protocol—Transport Layer Security
ETW	Vista’s Event Tracing for Windows
GPO	Group Policy Object
LDAP	Lightweight Directory Access Protocol
MITM	man-in-the-middle
MMC	Microsoft Management Console
MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol Version 2
OTP	one-time password
OU	organizational unit
PAC	Protected Access Credential
PEAP	Protected Extensible Authentication Protocol
PIN	personal identification number
PKI	public-key infrastructure

**Table G-1**      **List of Acronyms (continued)**

<b>Acronym</b>	<b>Expansion</b>
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
SDK	Software Development Kit
SSID	Service Set Identifier
SSO	single sign-on
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
UPN	User Principal Name
XML	eXtensible Markup Language