



# Cisco Aironet 350 Series Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE

Software Release 2.60  
February 2005

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

Customer Order Number:  
Text Part Number: OL-1375-05



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

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

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

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

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

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

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

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

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

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

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

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0501R)

*Cisco Aironet 350 Series Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE*  
Copyright © 2005 Cisco Systems, Inc.  
All rights reserved.



<b>Preface</b>	<b>ix</b>
Audience	x
Purpose	x
Organization	x
Conventions	xi
Related Publications	xiii
Obtaining Documentation	xiii
Cisco.com	xiii
Documentation CD-ROM	xiii
Ordering Documentation	xiv
Documentation Feedback	xiv
Obtaining Technical Assistance	xiv
Cisco.com	xv
Technical Assistance Center	xv
Cisco TAC Website	xv
Cisco TAC Escalation Center	xvi
Obtaining Additional Publications and Information	xvi

---

## CHAPTER 1

<b>Product Overview</b>	<b>1-1</b>
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
Radio Firmware	1-4
Driver	1-4
Client Utilities	1-4
Overview of ACU	1-5
Buttons on the Client Utility Windows	1-6
Network Configurations Using the Client Adapter	1-6
Ad Hoc Wireless LAN	1-7
Wireless Infrastructure with Workstations Accessing a Wired LAN	1-8

---

CHAPTER 2

<b>Preparing for Installation</b>	<b>2-1</b>
Safety Information	2-2
FCC Safety Compliance Statement	2-2
Safety Guidelines	2-2
Warnings	2-3
Unpacking the Client Adapter	2-3
Package Contents	2-3
System Requirements	2-4
Site Requirements	2-5
For Infrastructure Devices	2-5
For Client Devices	2-5

---

CHAPTER 3

<b>Installing the Client Adapter</b>	<b>3-1</b>
Finding the Windows CE Version	3-2
Installing the Driver and Client Utilities	3-2
Verifying Installation	3-5
Deciding How to Configure Your Client Adapter (Windows CE .NET Only)	3-6

---

CHAPTER 4

<b>Using the Profile Manager</b>	<b>4-1</b>
Overview of Profile Manager	4-2
Opening Profile Manager	4-2
Creating a New Profile	4-3
Selecting the Active Profile	4-3
Modifying a Profile	4-4
Editing a Profile	4-4
Renaming a Profile	4-4
Deleting a Profile	4-5

---

CHAPTER 5

<b>Configuring the Client Adapter</b>	<b>5-1</b>
Configuring Your Client Adapter	5-2
Overview of Security Features	5-11
Static WEP Keys	5-11
Dynamic WEP Keys with EAP	5-12
Wi-Fi Protected Access (WPA)	5-14
Fast Roaming (CCKM)	5-14
Reporting Access Points that Fail LEAP or EAP-FAST Authentication	5-15

Additional WEP Key Security Features	5-16
Message Integrity Check (MIC)	5-16
Temporal Key Integrity Protocol (TKIP)	5-17
Broadcast Key Rotation	5-17
Synchronizing Security Features	5-17
Using Static WEP	5-20
Enabling Static WEP and Entering a New Static WEP Key	5-20
Overwriting an Existing Static WEP Key	5-21
Disabling Static WEP	5-22
Enabling LEAP	5-22
Enabling EAP-FAST	5-24
Obtaining a PAC File (Manual PAC Provisioning Only)	5-24
Enabling EAP-FAST	5-25
Enabling Host-Based EAP	5-28
Obtaining and Importing CA and User Certificates	5-28
Obtaining CA and User Certificates	5-28
Importing a CA Certificate	5-29
Importing a User Certificate	5-30
Enabling Host-Based EAP	5-31
Enabling EAP-TLS	5-32
Enabling PEAP	5-33
Disabling LEAP, EAP-FAST, or Host-Based EAP	5-35

---

## CHAPTER 6

<b>Using EAP Authentication</b>	6-1
Overview	6-2
Using LEAP or EAP-FAST	6-2
With a Temporary Username and Password	6-2
With a Saved Username and Password	6-4
After Your EAP-FAST Credentials Expire	6-4
Using EAP-TLS	6-5
Using PEAP	6-6
After Profile Selection, Card Insertion, or Reset	6-6
After Your Password Expires (Windows NT or 2000 Domain Databases Only)	6-8

CHAPTER 7

**Performing Diagnostics 7-1**

- Overview of ACU Diagnostic Tools 7-2
- Setting Signal Strength Display Units 7-2
- Viewing the Status of Your Client Adapter 7-3
- Viewing Statistics for Your Client Adapter 7-7

CHAPTER 8

**Routine Procedures 8-1**

- Inserting and Removing a PC Card 8-2
  - Inserting a PC Card into a Windows CE Device 8-2
  - Removing a PC Card from a Windows CE Device 8-2
- Upgrading the Client Adapter Software 8-3
  - Upgrading the Firmware 8-3
    - Finding the Firmware Version 8-3
    - Loading New Firmware 8-4
  - Upgrading the Driver and Client Utilities 8-6
    - Finding the Driver and Client Utility Versions 8-7
    - Uninstalling the Current Driver and Client Utilities 8-8
- Client Utility Procedures 8-8
  - Opening a Client Utility 8-8
  - Exiting a Client Utility 8-8
  - Finding the Version of a Client Utility 8-9
  - Deleting Client Utility Icons on HPC and Windows CE .NET Devices 8-9
- CA and User Certificate Procedures (Host-Based EAP on PPC 2002 Devices Only) 8-10
  - Viewing CA and User Certificates 8-10
  - Removing CA and User Certificates 8-11
- Restarting the Client Adapter 8-11

CHAPTER 9

**Troubleshooting 9-1**

- Accessing the Latest Troubleshooting Information 9-2
- Interpreting the Indicator LEDs 9-2
- Troubleshooting the Client Adapter 9-3
  - Problems Obtaining an IP Address 9-3
  - Problems Associating to an Access Point 9-3
  - Problems Authenticating to an Access Point 9-4
  - Problems Connecting to the Network 9-4
  - Reauthenticating After LEAP or EAP-FAST Times Out 9-4
  - Creating Strong Passwords 9-4

Error Messages	9-5
General Error Messages	9-5
Installation Error Messages	9-7
LEAP Authentication Error Messages	9-8
EAP-FAST Authentication Error Messages	9-10
EAP-TLS Authentication Error Messages	9-14
PEAP Authentication Error Messages	9-15
Getting Help	9-17
PPC Devices	9-17
HPC and Windows CE .NET Devices	9-17

---

APPENDIX A

**Technical Specifications** A-1

---

APPENDIX B

**Translated Safety Warnings** B-1

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

---

APPENDIX C

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

Manufacturer's Federal Communication Commission Declaration of Conformity Statement	C-2
Department of Communications – Canada	C-3
Canadian Compliance Statement	C-3
European Community, Switzerland, Norway, Iceland, and Liechtenstein	C-4
Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC	C-4
Declaration of Conformity for RF Exposure	C-6
Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan	C-7
Japanese Translation	C-7
English Translation	C-7
Administrative Rules for Cisco Aironet Wireless LAN Client Adapters in Taiwan	C-8
Chinese Translation	C-8
English Translation	C-8

---

APPENDIX D

**Channels, Power Levels, and Antenna Gains** D-1

Channels	D-2
Maximum Power Levels and Antenna Gains	D-3

---

APPENDIX E

**Configuring the Client Adapter through Windows CE .NET** E-1

- Overview E-2
  - Overview of Security Features E-2
    - Static WEP Keys E-2
    - Dynamic WEP Keys with EAP E-3
    - Wi-Fi Protected Access (WPA) E-4
- Preparing for Configuration (EAP-TLS and PEAP Only) E-4
  - System Requirements E-4
  - Obtaining and Importing CA and User Certificates E-5
    - Obtaining CA and User Certificates E-5
    - Importing a CA Certificate E-5
    - Importing a User Certificate E-7
- Configuring the Client Adapter E-8
  - Enabling EAP-TLS Authentication E-12
  - Enabling PEAP Authentication E-13
- Associating to an Access Point Using Windows CE .NET E-15

---

APPENDIX F

**Performing a Site Survey** F-1

- Overview F-2
  - Guidelines F-2
  - Additional Information F-2
- Setting Signal Strength Display Units F-3
- Using Passive Mode F-4
- Using Active Mode F-7
- Forcing the Client Adapter to Reassociate F-13

---

GLOSSARY

---

INDEX





## Preface

---

The preface provides an overview of the *Cisco Aironet 350 Series Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE*, 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 x](#)
- [Purpose, page x](#)
- [Organization, page x](#)
- [Conventions, page xi](#)
- [Related Publications, page xiii](#)
- [Obtaining Documentation, page xiii](#)
- [Obtaining Technical Assistance, page xiv](#)
- [Obtaining Additional Publications and Information, page xvi](#)

# Audience

This publication is for the person responsible for installing, configuring, and maintaining a Cisco Aironet 350 Series Wireless LAN Client Adapter on a Windows CE device. This person should be familiar with computing devices and with network terms and concepts.

# Purpose

This publication describes the Cisco Aironet client adapters in the 350 series and explains how to install, configure, and troubleshoot them.

**Note**

This version of the *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE* pertains specifically to client adapter driver and utility version 2.60. If you are using, installing, or upgrading to older versions of client adapter software, refer to a previous version of this manual for information and instructions.

**Note**

Client adapter driver and utility version 2.60 is not supported for use with Cisco Aironet 340 series client adapters.

# Organization

This publication contains the following chapters:

- [Chapter 1, “Product Overview,”](#) describes the types of client adapters and their hardware and software components and illustrates two common network configurations.
- [Chapter 2, “Preparing for Installation,”](#) provides information that you need to know before installing a client adapter, such as safety information and system requirements.
- [Chapter 3, “Installing the Client Adapter,”](#) provides instructions for installing the driver and client utilities.
- [Chapter 4, “Using the Profile Manager,”](#) explains how to use the ACU profile manager feature to create and manage profiles for your client adapter.
- [Chapter 5, “Configuring the Client Adapter,”](#) explains how to change the configuration parameters for a specific profile.
- [Chapter 6, “Using EAP Authentication,”](#) explains the sequence of events that occurs and the actions you must take when a profile that is set for EAP authentication is selected for use.
- [Chapter 7, “Performing Diagnostics,”](#) explains how to use ACU to perform user-level diagnostics.
- [Chapter 8, “Routine Procedures,”](#) provides procedures for common tasks related to the client adapters, such as upgrading software and restarting the adapter.
- [Chapter 9, “Troubleshooting,”](#) provides information for diagnosing and correcting common problems that may be encountered when installing or operating a client adapter.
- [Appendix A, “Technical Specifications,”](#) lists the physical, radio, power, and regulatory specifications for the client adapters.

- [Appendix B, “Translated Safety Warnings,”](#) provides translations of the client adapters’ safety warnings in nine languages.
- [Appendix C, “Declarations of Conformity and Regulatory Information,”](#) provides declarations of conformity and regulatory information for the client adapters.
- [Appendix D, “Channels, Power Levels, and Antenna Gains,”](#) lists the IEEE 802.11b channels supported by the world’s regulatory domains as well as the maximum power levels and antenna gains allowed per domain.
- [Appendix E, “Configuring the Client Adapter through Windows CE .NET,”](#) explains how to configure and use a client adapter with Windows CE .NET.
- [Appendix F, “Performing a Site Survey,”](#) shows people who are responsible for conducting a site survey how they can use ACU to determine the best placement for infrastructure devices within a wireless network.

## Conventions

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

- Commands and keywords 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 elkreter och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)

## Related Publications

For more information about Cisco Aironet Wireless LAN Client Adapters for Windows CE, refer to the following publications:

- *Release Notes for Cisco Aironet Client Utilities 2.60 and Driver 2.60 for Windows CE*
- *Release Notes for Cisco Aironet 350 and CB20A Client Adapter Firmware 5.40.10*

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

<http://www.cisco.com/en/US/products/hw/wireless/index.html>

## Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

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

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

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

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

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

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) Website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

## Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

## Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

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

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/en/US/support/index.html>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

## Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:  
[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac114/about\\_cisco\\_packet\\_magazine.html](http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html)
- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:  
[http://business.cisco.com/prod/tree.taf%3fasset\\_id=44699&public\\_view=true&kbns=1.html](http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html)
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:  
[http://www.cisco.com/en/US/learning/le31/learning\\_recommended\\_training\\_list.html](http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html)





# Product Overview

---

This chapter describes the Cisco Aironet 350 Series Wireless LAN Client Adapters and illustrates their role in a wireless network.

The following topics are covered in this chapter:

- [Introduction to the Client Adapters, page 1-2](#)
- [Hardware Components, page 1-3](#)
- [Software Components, page 1-4](#)
- [Network Configurations Using the Client Adapter, page 1-6](#)

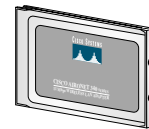
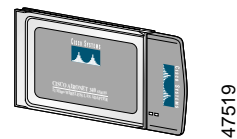
# Introduction to the Client Adapters

The Cisco Aironet 350 Series Wireless LAN Client Adapters are 100-milliwatt (mW) radio modules that provide transparent wireless data communications between fixed, portable, or mobile devices and other wireless devices or a wired network infrastructure. 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 transparently through the wireless infrastructure through an access point connected to a wired LAN. The adapters operate similarly to a standard network product except that the cable is replaced with a radio connection and an access point is required to 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 two types of client adapters:

- **PC card** (model number: AIR-PCM35x)—An IEEE 802.11b-compliant 2.4-GHz 11-Mbps PCMCIA card radio module that can be inserted into any device equipped with an *external* Type II or Type III PC card slot. Host devices can include laptops, notebook computers, personal digital assistants, and handheld or portable devices.
- **LM card** (model number: AIR-LMC35x)—An IEEE 802.11b-compliant 2.4-GHz 11-Mbps PCMCIA card radio module that is usually preinstalled in a device equipped with an *internal* Type II or Type III PC card slot. Host devices usually include handheld or portable devices.



## Note

The x in the product model number indicates the wired equivalent privacy (WEP) level of the card, where 0 = no WEP capability, 1 = 40-bit WEP, and 2 = 128-bit WEP. However, if the second x is a 0 but the model number contains K9, the card is 128-bit WEP capable.



## Note

Client adapter driver and utility version 2.60 is not supported for use with Cisco Aironet 340 series client adapters.

## Terminology

The following terms are used throughout this document:

- **client adapter**—Refers to both PC cards and LM cards.
- **PC card** or **LM card**—Refers to a specific client 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 adapter has three major hardware components: a radio, a radio antenna, and two LEDs.

## Radio

The Cisco Aironet 350 series PC and LM cards are IEEE 802.11b-compliant client adapters. They contain a direct-sequence spread spectrum (DSSS) radio that operates in the 2.4-GHz Industrial Scientific Medical (ISM) license-free band. The 350 series 100-mW radio transmits data over a half-duplex radio channel operating at up to 11 Mbps. These cards operate with other IEEE 802.11b-compliant client devices in ad hoc (or *peer-to-peer*) mode or with Cisco Aironet 340, 350, 1100, and 1200 Series Access Points (with a 2.4-GHz radio) and other IEEE 802.11b-compliant infrastructure devices in infrastructure mode. They are approved for indoor and outdoor use.

DSSS technology distributes a radio signal over a wide range of frequencies and then returns the signal to the original frequency range at the receiver. The benefit of this technology is its ability to protect the data transmission from interference. For example, if a particular frequency encounters noise or interference or both, enough redundancy is built into the signal on other frequencies that the client adapter usually will still be successful in its transmission.

## Radio Antenna

The type of antenna used depends on your client adapter:

- PC cards have an integrated, permanently attached diversity antenna. The benefit of the diversity antenna system is improved coverage. The system works by allowing the card to switch and sample 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 PC card slot when the card is installed.
- LM cards are shipped without an antenna; however, an antenna can be connected through the card's external connector.



### Note

External antennas used in combination with a power setting resulting in a radiated power level above 100 mW equivalent isotropic radiated power (EIRP) are not allowed for use within the European community and other countries that have adopted the European R&TTE directive or the CEPT recommendation Rec 70.03 or both. For more details on legal combinations of power levels and antennas in those countries, refer to the [“Declaration of Conformity for RF Exposure”](#) section on page C-6 and the [“Maximum Power Levels and Antenna Gains”](#) section on page D-3.

## LEDs

The client adapter has two LEDs that glow or blink to indicate the status of the adapter or to convey error messages. Refer to the [Chapter 9](#) for an interpretation of the LED codes.

# Software Components

The client adapter has three major software components: radio firmware, a driver, and client utilities.

## Radio Firmware

The firmware, which is contained in the client adapter's Flash memory, controls the adapter's radio. The client adapter is shipped with the firmware installed; however, a more recent version of the firmware may be available from Cisco.com.

**Note**

Firmware version 5.40.10 is recommended for use with client adapter driver and utility version 2.60. [Chapter 8](#) provides instructions for determining the version of your client adapter's firmware and upgrading it if necessary.

## Driver

The driver provides an interface between the Windows CE device and the client adapter, thereby enabling Windows CE and the applications it runs to communicate with the adapter. The driver must be installed before the adapter can be used. [Chapter 3](#) provides instructions for installing the driver.

## Client Utilities

Two client utilities are available for use with Cisco Aironet client adapters: Aironet Client Utility (ACU) and Wireless Login Module (WLM). These utilities are optional applications that interact with the radio firmware to adjust client adapter settings and display information about the adapter. The client utilities and online help files are installed with the driver.

ACU enables you to create configuration profiles for your client adapter and perform user-level diagnostics. Because ACU performs a variety of functions, it is documented by function throughout this manual. However, an overview of the utility is provided on the next page to familiarize you with its interface. WLM enables you to enter a temporary LEAP or EAP-FAST username and password for authentication to a RADIUS server. [Chapter 6](#) provides detailed information and instructions on using WLM.

**Note**

If your Windows CE device is running Windows CE .NET, you can configure your client adapter through the operating system instead of through ACU. Refer to [Appendix E](#) for information. However, ACU is recommended for configuring the client adapter.

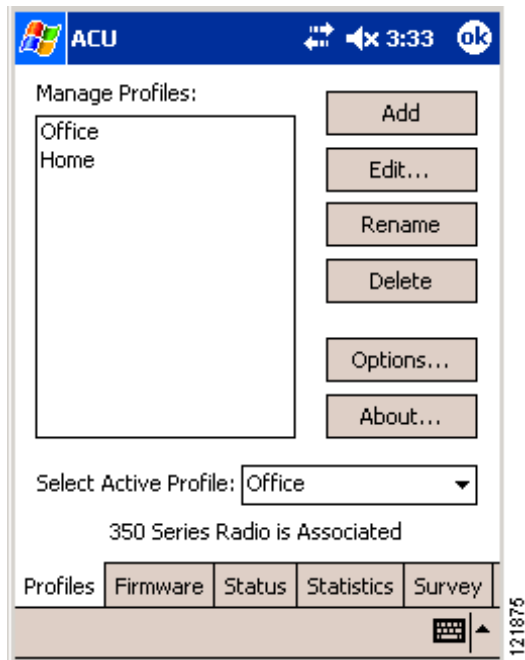
**Note**

All of the windows included in this manual were taken from a PPC 2002 or PPC 2003 device. The windows look slightly different on other Windows CE devices.

## Overview of ACU

The Profiles window (see [Figure 1-1](#)) is ACU's primary window. It appears when you open ACU.

**Figure 1-1** Profiles Window



The five tabs along the bottom of the window (for PPC devices) or top of the window (for HPC and Windows CE .NET devices) enable you to activate the following ACU features:

- **Profiles**—Enables you to use the profile manager feature to create and manage profiles for your client adapter. [Chapter 4](#) provides instructions for using this feature.
- **Firmware**—Enables you to load new firmware for your client adapter. [Chapter 8](#) provides instructions for upgrading firmware.
- **Status**—Enables you to view the current status of your client adapter. [Chapter 7](#) provides additional information on viewing the status.
- **Statistics**—Enables you to view transmit, receive, and MIC statistics for your client adapter. [Chapter 7](#) provides additional information on viewing statistics.
- **Survey**—Enables people who are responsible for conducting a site survey to determine the best placement of infrastructure devices within a wireless network. [Appendix F](#) provides instructions for using the site survey feature.

The status bar at the top or bottom of the Profiles window reflects the current state of your client adapter. The following states are possible: Not Associated, Associated, Authenticated, Ad Hoc Mode, and Cisco Wireless LAN Adapter Not Found.

## Buttons on the Client Utility Windows

The buttons on the client utility windows are used to perform specific functions. [Table 1-1](#) describes the most common buttons.

**Table 1-1** *Buttons on the Client Utility Windows*

Button	Description
Cancel	Exits the window without saving any changes
OK	Saves any changes and exits the window
Start	Initiates a test
Stop	Stops a test that is running
X	Exits the window without saving any changes
? (available on HPC and Windows CE .NET devices only)	Provides information on the window and its parameters

## Network Configurations Using the Client Adapter

The client adapter 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 hardware installation guide for your access point.



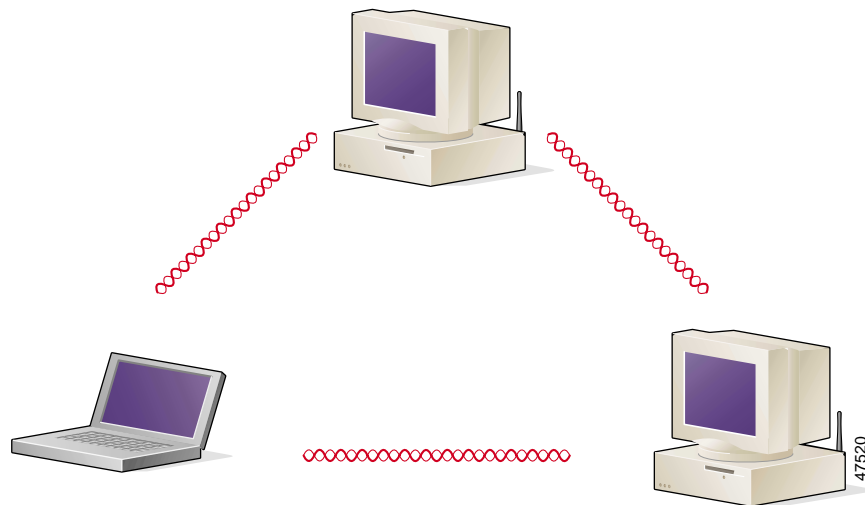
### Note

Refer to [Chapter 5](#) for information on setting the client adapter's network (or infrastructure) mode.

## Ad Hoc Wireless LAN

An ad hoc (or *peer-to-peer*) wireless LAN (see [Figure 1-2](#)) 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 1-2**      **Ad Hoc Wireless LAN**

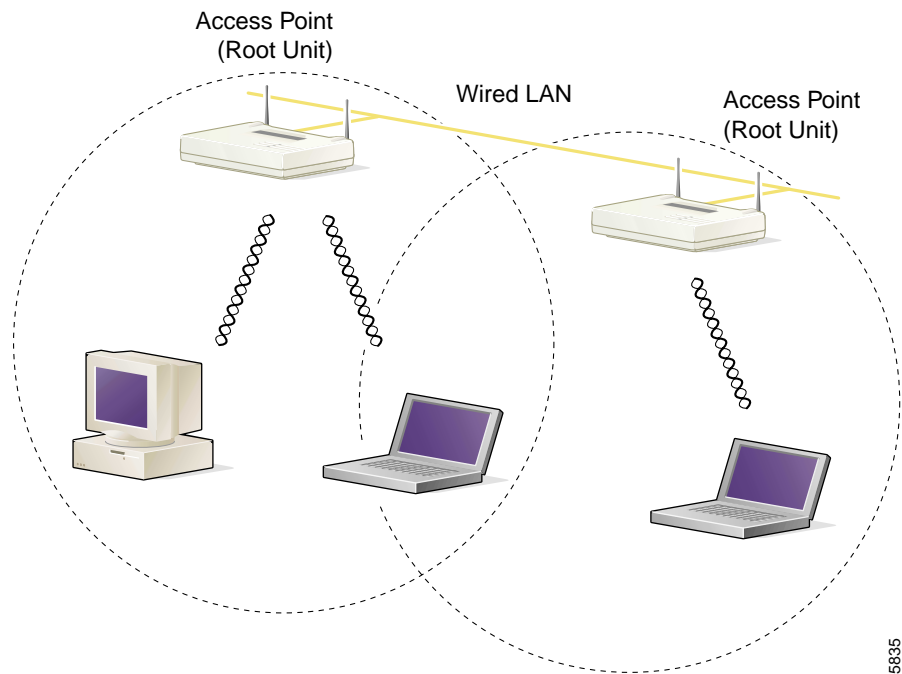


## Wireless Infrastructure with Workstations Accessing a Wired LAN

A microcellular network can be created by placing two or more access points on a LAN. [Figure 1-3](#) 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 allows 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, once 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 1-3**      **Wireless Infrastructure with Workstations Accessing a Wired LAN**







## Preparing for Installation

---

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

The following topics are covered in this chapter:

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

# Safety Information

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

## FCC Safety Compliance Statement

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

## Safety Guidelines

- Do not touch or move the antenna while the unit is transmitting or receiving.
- Do not hold any component containing a radio such that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; otherwise, the radio may be damaged.
- High-gain, wall-mount, or mast-mount antennas are designed to be professionally installed and should be located at a minimum distance of 12 inches (30 cm) or more from the body of all persons. Please contact your professional installer, VAR, or antenna manufacturer for proper installation requirements.
- 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:



**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.**



**In order to comply with RF exposure limits established in the ANSI C95.1 standards, it is recommended when using a laptop with a PC card client adapter that the adapter's integrated antenna is positioned more than 2 inches (5 cm) from your body or nearby persons during extended periods of transmitting or operating time. If the antenna is positioned less than 2 inches (5 cm) from the user, it is recommended that the user limit exposure time.**

Translated versions of these safety warnings are provided in [Appendix B](#).

## Unpacking the Client Adapter

Follow these steps to unpack the client adapter:

- 
- Step 1** Open the shipping container and carefully remove the contents.
- Step 2** Return all packing materials to the shipping container and save it.
- Step 3** Ensure that all items listed in the “[Package Contents](#)” section below are included in the shipment. Check each item for damage.



**Note**

If any item is damaged or missing, notify your authorized Cisco sales representative. Any remote antenna and its associated wiring are shipped separately.

---

## Package Contents

Each client adapter is shipped with the following items:

- *Quick Start Guide: Cisco Aironet Wireless LAN Client Adapters*
- Cisco Aironet Wireless LAN Client Adapters CD
- Cisco product registration card

# System Requirements

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

- One of the following Windows CE devices equipped with a Type II or Type III PC card slot:
  - HPC 2000 device running Windows CE 3.0 with an ARM, StrongARM, MIPS, SH4, or X86 platform
  - PPC 2000 device running Windows CE 3.0 with an ARM, StrongARM, MIPS, or SH3 platform
  - PPC 2002 device running Windows CE 3.0 with a StrongARM platform
  - PPC 2003 device running Windows CE .NET 4.2 with a StrongARM platform
  - Windows CE .NET device running Windows CE .NET 4.0 or 4.1 with an ARMv4I, ARMv4T, or MIPSII platform
  - Windows CE .NET device running Windows CE .NET 4.2 with a StrongARM (ARMv4), ARMv4I, or X86 platform
- Cisco Aironet 350 Series Wireless LAN Client Adapter (PC card or LM card)




---

**Note** Client adapter driver and utility version 2.60 is not supported for use with Cisco Aironet 340 series client adapters.

---

- Client adapter firmware version 5.40.10 (recommended)
- Laptop or PC running a Windows operating system and Microsoft ActiveSync
- ActiveSync connection (which can be serial, USB, etc.) to the Windows CE device
- A PPC 2002, PPC 2003, or Windows CE .NET 4.2 device, if your wireless network uses EAP-FAST, 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 authentication with a One-Time Password (OTP) user database:
  - The hardware token from an OTP vendor
  - Your hardware token password
- The following information from your system administrator:
  - The logical name for your Windows CE device (also referred to as *client name*)
  - The case-sensitive service set identifier (SSID) for your RF network
  - The primary and secondary Domain Name System (DNS) and Windows Internet Name Service (WINS) to be assigned to your Windows CE device
  - If your network setup does not include a DHCP server, the IP address, subnet mask, and default gateway address to be assigned to your device
  - 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

- Your username and password for LEAP, EAP-FAST, or PEAP authentication, if your wireless network uses one of these authentication types
- Your username for EAP-TLS authentication, if your wireless network uses EAP-TLS authentication
- Protected access credentials (PAC) file if your wireless network uses EAP-FAST authentication with manual PAC provisioning

## Site Requirements

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

### For Infrastructure Devices

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



Note

---

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

---

### For Client Devices

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

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





## Installing the Client Adapter

---

This chapter provides instructions for installing the client adapter driver and client utilities.

The following topics are covered in this chapter:

- [Finding the Windows CE Version, page 3-2](#)
- [Installing the Driver and Client Utilities, page 3-2](#)
- [Verifying Installation, page 3-5](#)
- [Deciding How to Configure Your Client Adapter \(Windows CE .NET Only\), page 3-6](#)

## Finding the Windows CE Version

The messages that appear during the installation of the client adapter driver and utilities (as well as the client utility windows themselves) vary depending on your Windows CE device. Follow the instructions below to find the version of Windows CE that your device is using.

- If your Windows CE device is a Pocket PC (PPC) device, tap **Start** > **Settings** > the **System** tab > **About**. The Windows CE version is shown.

**Note**

If the version is 4.20.xx, the device is a PPC 2003. If the version is 3.00.xx, you must check the build number. If the build number is lower than 11178, the device is a PPC 2000; otherwise, the device is a PPC 2002.

- If your Windows CE device is a Handheld PC (HPC) device, tap **Start** > **Settings** > **Control Panel** > **System** > **System** tab. The core system version indicates the version of Windows CE that the device is running (such as 3.0).
- If your Windows CE device is a CE .NET device, tap **Start** > **Settings** > **Control Panel** > **System**. The Windows CE version is shown under System on the General tab.

## Installing the Driver and Client Utilities

The WinCE-PCMCIA-LMC-v260.exe file is a self-extracting zip file that extracts all of the files necessary to install the driver and client utilities (version 2.60). The main installation utility extracted from this file is ceInstall.exe.

Follow these steps to install the driver and client utilities for your client adapter.

**Note**

This procedure is meant to be used the first time the driver and client utilities are installed on a Windows CE device. If Cisco Aironet client adapter software is already installed on your Windows CE device, follow the instructions in [Chapter 8](#) to first uninstall any existing software and then follow the instructions here to upgrade to new software.

**Note**

Firmware version 5.40.10 is recommended for use with client adapter driver and utility version 2.60. [Chapter 8](#) provides instructions for finding the version of your client adapter's firmware and upgrading it if necessary.

**Note**

Client adapter driver and utility version 2.60 is not supported for use with Cisco Aironet 340 series client adapters.

**Note**

The driver and client utilities must be installed before you insert a client adapter into a Windows CE device.



**Note**

Client adapter driver and utility version 2.60 is not yet available on the CD that ships with Cisco Aironet client adapters. If you are installing older versions of client adapter drivers and utilities, refer to a previous version of this manual for installation, configuration, and operation instructions.

**Step 1** Connect your Windows CE device to a laptop or PC running Microsoft ActiveSync. This is typically done using a serial or USB cable.

A message appears on the Windows CE device indicating that it is connecting to the host. After the Windows CE device is connected, the New Partnership window appears on the laptop or PC. This window asks if you want to set up a partnership.

**Note**

Cisco recommends that you install the latest version of ActiveSync.

**Step 2** Perform one of the following:

- If you want to establish a partnership that enables you to synchronize files between the laptop or PC and the Windows CE device, choose **Yes**, click **Next**, and follow the instructions on the window to specify the files to be synchronized and to finish setting up the partnership.
- If you do not want to synchronize files and want to connect as a “guest,” choose **No** and click **Next**. The window indicates that you are connected as a guest.

**Step 3** Use the laptop or PC’s web browser to access the following URL:

<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

**Step 4** Choose **Option #2: Aironet Wireless Software Display Tables**.

**Note**

You can download software from the Software Selector tool instead of the display tables. To do so, choose **Option #1: Aironet Wireless Software Selector**, follow the instructions on the window, and go to [Step 9](#).

**Step 5** Click **Cisco Aironet Wireless LAN Client Adapters**.

**Step 6** Find the section for Windows CE client adapter drivers and utilities.

**Step 7** Click the link for Windows CE 3.0 or Windows CE .NET, depending on your device’s operating system.

**Step 8** Click the **WinCE-PCMCIA-LMC-v260.exe** file.

**Step 9** Complete the encryption authorization form; then read and accept the terms and conditions of the Software License Agreement.

**Step 10** Click the **WinCE-PCMCIA-LMC-v260.exe** file again to download it.

**Step 11** Save the file to the hard drive of your laptop or PC.

**Step 12** Find the file using Windows Explorer, double-click it, and extract its files to a folder.

**Note**

Make sure you keep all of the extracted files together in one folder. Moving them to different locations may prevent the software from operating correctly.

**Step 13** Double-click the **ceInstall.exe** file.

- Step 14** If you are using a PPC 2002 device, the Install 802.1X Support window appears. If you are planning to use EAP-TLS or PEAP authentication, click **Yes**. Otherwise, click **No**.



**Note** If you choose Yes, the PPC 2002 802.1X backport, which provides support for 802.1X security, is installed. The backport then becomes part of the base Windows CE operating system and cannot be uninstalled.

- Step 15** If you are using a PPC 2002, PPC 2003, or Windows CE .NET 4.2 device, the Cisco PEAP window appears. If you are planning to use Cisco PEAP authentication, make sure the **Install Cisco PEAP Support** check box is checked and click **Next**. Otherwise, uncheck the **Install Cisco PEAP Support** check box and click **Next**.



**Note** If you install the Cisco PEAP supplicant and later want to use the Microsoft PEAP supplicant, you must default your Windows CE device and reinstall the client adapter software.

- Step 16** If you installed the 802.1X backport on a PPC 2002 device, a message appears indicating that you must reset your device when the installation is complete. Click **OK**.

- Step 17** If you are not using a PPC 2002 device, the Cisco Aironet Wireless LAN Adapter Setup window appears. Click **Next** to start the Windows CE Application Manager (CeAppMgr), which is installed with ActiveSync. CeAppMgr interrogates the Windows CE device to determine its platform type.



**Note** If a Windows CE device is not connected to the laptop or PC (as instructed in [Step 1](#)), click **Exit** to quit the setup program and connect a Windows CE device or click **Next** to continue the installation. If you choose **Exit**, click **OK** to shut down CeAppMgr and start again beginning with [Step 1](#). If you choose **Next**, a message appears indicating that the software will be downloaded the next time a mobile device is connected. Click **OK**. The next time a Windows CE device is connected to the laptop or PC via ActiveSync, CeAppMgr starts automatically, and you are prompted to install the software.

- Step 18** When the Installing Applications dialog box appears asking if you want to install the client adapter using the default application installation directory, click **Yes**. The default directory is \Windows\Start Menu\Programs\Cisco on PPC devices and \Windows\Programs\Cisco on HPC and Windows CE .NET devices.

A message and a progress bar appear indicating that the client adapter (and 802.1X backport if you are using a PPC 2002 device) is being installed.

The driver and help files are copied to the \Windows directory, and the client utilities are installed in the \Windows\Start Menu\Programs\Cisco directory on PPC devices or the \Windows\Programs\Cisco directory on HPC and Windows CE .NET devices. Shortcuts to ACU and WLM are automatically added to the desktop on HPC and Windows CE .NET devices.

- Step 19** When the installation process is complete on the laptop or PC, a message appears asking you to view the window of the Windows CE device to see if any additional steps are required to complete the installation. Click **OK** to terminate the installation process on the laptop or PC.

- Step 20** Complete any required steps on the Windows CE device.

- Step 21** Disconnect the Windows CE device.

- Step 22** If you are using a PPC 2002 device and you installed the 802.1X backport, reset your Windows CE device now. (You should have been notified earlier that a reset would be required after installation.)

- Step 23** Insert the client adapter into the PC card slot of the Windows CE device. Refer to [Chapter 8](#) for specific instructions on inserting the client adapter.
- The Windows CE device should configure the client adapter, and the green LED on the adapter should blink. If this does not happen, remove the client adapter, reset the Windows CE device, and reinsert the client adapter.
- Step 24** The Cisco Wireless LAN Adapter Settings dialog box appears. If the dialog box does not appear, perform one of the following:
- Tap **Start > Settings > the Connections tab > Connections > Advanced > Network Card > Cisco Wireless LAN Adapter** on PPC 2003 devices.
  - Tap **Start > Settings > the Connections tab > Network Adapters > Cisco Wireless LAN Adapter > Properties** on PPC 2002 devices.
  - Tap **Start > Settings > Control Panel > Network > the Adapters tab > Cisco Wireless LAN Adapter > Properties** on HPC devices.
  - Tap **Start > Settings > Network and Dial-up Connections > the Cisco Wireless LAN Client Adapter icon** on Windows CE .NET devices.
- Step 25** Perform one of the following:
- If your device is connected to a DHCP server, choose **Obtain an IP address via DHCP** or **Use server-assigned IP address** and tap **OK**.
  - If your device is not connected to a DHCP server, choose **Specify an IP address** or **Use specific IP address** and follow these steps:
    - a. Enter the IP address, subnet mask, and default gateway address you want to assign to your device. They can be obtained from your system administrator.
    - b. Choose the **Name Servers** tab and enter the primary and secondary DNS and WINS you want to assign to your device. They can be obtained from your system administrator.
    - c. Tap **OK**.
- Step 26** The driver and client utility installation is complete. Go to the “[Verifying Installation](#)” section below to determine if the installation was successful.

## Verifying Installation

To verify that you have properly installed the driver and client utilities, check the client adapter’s LEDs. If the installation was successful, the client adapter’s green LED blinks.



### Note

If your installation was unsuccessful or you experienced problems during or after driver installation, refer to [Chapter 9](#) for troubleshooting information.

Now that your client adapter is properly installed, you are ready to go to [Chapter 4](#) to create profiles for your client adapter unless your device is running Windows CE .NET. If your device is running Windows CE .NET, go to the “[Deciding How to Configure Your Client Adapter \(Windows CE .NET Only\)](#)” section on page 3-6.

# Deciding How to Configure Your Client Adapter (Windows CE .NET Only)

Windows CE .NET is the only Windows CE operating system that enables you to configure your client adapter without using ACU. Therefore, if your device is running Windows CE .NET, you must decide whether to configure your client adapter through the operating system or ACU. To help you with your decision, [Table 3-1](#) compares the Windows CE .NET and ACU client adapter features.

**Table 3-1 Comparison of Windows CE .NET and ACU Client Adapter Features**

Feature	Windows CE .NET	ACU
Configuration parameters	Limited	Extensive
Capabilities		
Create profiles	Yes	Yes
Upgrade radio firmware	No	Yes
Security		
Static WEP	Yes	Yes
LEAP authentication with dynamic WEP	No	Yes
LEAP authentication with WPA	No	Yes (on Windows CE .NET 4.2 devices)
EAP-FAST authentication with dynamic WEP	No	Yes
EAP-FAST authentication with WPA	No	Yes (on Windows CE .NET 4.2 devices)
EAP-TLS authentication with dynamic WEP	Yes (on Windows CE .NET 4.2 devices)	Yes (on PPC 2002 devices)
PEAP authentication with dynamic WEP	Yes (on Windows CE .NET 4.2 devices)	Yes (on PPC 2002 devices)
Diagnostics		
Status window	Limited	Extensive
Statistics window (transmit & receive)	No	Yes
Site survey tool	No	Yes

Perform one of the following:

- If you are planning to configure your client adapter through ACU instead of through Windows CE .NET and you are using a PPC 2003 device, follow the instructions in [Chapter 4](#) and [Chapter 5](#) to configure your client adapter through ACU.
- If you are planning to configure your client adapter through ACU instead of through Windows CE .NET and you are using a device other than a PPC 2003, follow these steps:
  - a. Tap **Start > Settings > Network and Dial-up Connections** > the **Cisco Wireless LAN Client Adapter** icon > the **Wireless Networks** tab.
  - b. Uncheck the **Use Windows to configure my wireless network settings** check box.
  - c. Follow the instructions in [Chapter 4](#) and [Chapter 5](#) to configure your client adapter through ACU.
- If you are planning to configure your client adapter through Windows CE .NET instead of through ACU, go to [Appendix E](#) and follow the instructions there.
- If you are planning to configure your client adapter through Windows CE .NET but you want to use ACU's diagnostic tools, go to [Appendix E](#) to configure the adapter through Windows CE .NET; then follow the instructions in [Chapter 7](#) to use ACU's diagnostic tools.





## Using the Profile Manager

---

This chapter explains how to use ACU's profile manager feature to create and manage profiles for your client adapter.

The following topics are covered in this chapter:

- [Overview of Profile Manager, page 4-2](#)
- [Opening Profile Manager, page 4-2](#)
- [Creating a New Profile, page 4-3](#)
- [Selecting the Active Profile, page 4-3](#)
- [Modifying a Profile, page 4-4](#)

# Overview of Profile Manager

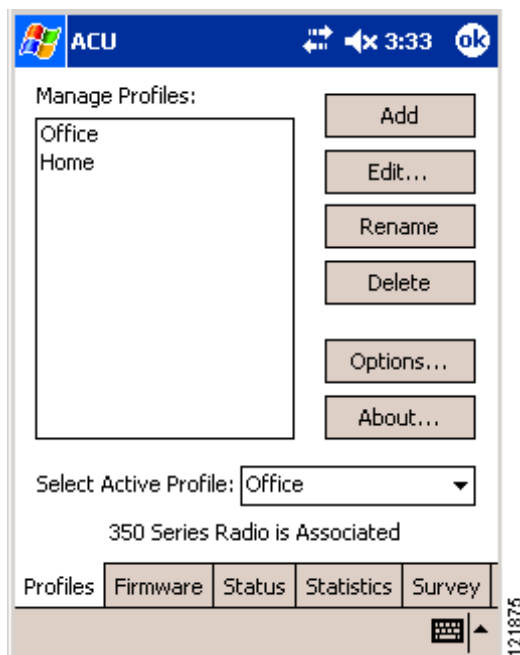
ACU's profile manager feature allows you to create and manage up to 16 *profiles* (or named groupings of saved configuration parameters) for your client adapter. These profiles enable you to use your client adapter in different locations, each of which requires different configuration settings. For example,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

Profiles are stored in the registry of the Windows CE device. They are lost only if the Windows CE device is defaulted (hard reset) or if both the primary and backup batteries run out of power.

## Opening Profile Manager

To open ACU's profile manager, double-tap the **ACU** icon on your desktop or tap **Start > Programs > Cisco > ACU**. The Profiles window appears (see [Figure 4-1](#)).

**Figure 4-1** Profiles Window



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

- Create a new profile, [page 4-3](#)
- Select the active profile, [page 4-3](#)
- Edit a profile, [page 4-4](#)
- Rename a profile, [page 4-4](#)
- Delete a profile, [page 4-5](#)

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



## Creating a New Profile

Follow these steps to create a new profile.

- Step 1** Tap the **Add** button on the Profiles window. A new profile named Profile $x$  (where  $x$  is the number of the profile) appears in the Manage Profiles box.
- Step 2** To change the profile name from Profile $x$  to something of your own choosing (for example, Office, Home, etc.), enter the name now.



**Note** You can enter up to 80 characters, but due to limited window size, long profile names may not be completely displayed.

- Step 3** Perform one of the following:
- If you want this profile to use the default values, tap on a blank part of the window. The profile is added to the list of profiles in the Manage Profiles box.
  - If you want to change any of the configuration parameter settings, tap the **Edit** button. The Properties window appears with the name of the profile in quotation marks. Follow the instructions in [Chapter 5](#) to change any of the configuration parameters for this profile.
- Step 4** To create another profile, repeat the previous steps.

## Selecting the Active Profile

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



**Note**

Because EAP-TLS and PEAP authentication are not enabled in ACU, you cannot switch between these authentication types simply by switching profiles in ACU. For PPC 2002 devices, you can create a profile in ACU that uses host-based EAP, but you must enable the specific authentication type in the Authentication Manager. In addition, only one authentication type can be set at a time; therefore, if you have more than one profile in ACU that uses host-based EAP and you want to use another authentication type, you must change the authentication type in the Authentication Manager after switching profiles in ACU. For PPC 2003 devices, you must select <External Settings> as the active profile in ACU and then configure your client adapter through Windows CE .NET.

- Step 1** Go to the Profiles window (see [Figure 4-1](#)).
- Step 2** From the Select Active Profile drop-down menu, choose the profile that you want your client adapter to use to attempt to establish a connection to an access point.



**Note**

The <External Settings> profile option on Windows CE .NET devices disables ACU profiles and enables the operating system or an application other than ACU to configure the client adapter. You must choose this option if you want to configure your card through the operating system but use ACU's diagnostic tools. Refer to [Appendix E](#) for information on configuring your client adapter through Windows CE .NET.

The client adapter immediately starts using the profile that you select. If the client adapter cannot associate to an access point or loses association while using the selected profile, the adapter does not attempt to associate using another profile. To associate, you must select a different profile.

---

## Modifying a Profile

This section provides instructions for modifying an existing profile. Follow the steps in the corresponding section below to edit, rename, or delete a profile.

### Editing a Profile

- 
- Step 1 Go to the Profiles window (see [Figure 4-1](#)).
  - Step 2 From the Manage Profiles box, select the profile that you want to edit and tap the **Edit** button or double-tap the profile. The Properties window appears with the name of the profile in quotation marks.
  - Step 3 Follow the instructions in [Chapter 5](#) to change any of the configuration parameters for this profile.
- 

### Renaming a Profile

- 
- Step 1 Go to the Profiles window (see [Figure 4-1](#)).
  - Step 2 From the Manage Profiles box, select the profile that you want to rename and tap the **Rename** button or tap the profile twice (pausing longer than for a double-tap). The profile becomes highlighted.
  - Step 3 Enter a new name for the profile.



**Note** You can enter up to 80 characters, but due to limited window size, long profile names may not be completely displayed.

---

- Step 4 Tap on a blank part of the window to save your change. The profile is renamed and added to the list of profiles.
-

## Deleting a Profile

- 
- Step 1** Go to the Profiles window (see [Figure 4-1](#)).
- Step 2** From the Manage Profiles box, select the profile that you want to delete.



---

**Note** You cannot delete the active profile.

---

- Step 3** Tap the **Delete** button.
- Step 4** When prompted to confirm your decision, tap **Yes**. The profile is deleted.
-





## Configuring the Client Adapter

---

This chapter explains how to change the configuration parameters for a specific profile using ACU.

The following topics are covered in this chapter:

- [Configuring Your Client Adapter, page 5-2](#)
- [Overview of Security Features, page 5-11](#)
- [Using Static WEP, page 5-20](#)
- [Enabling LEAP, page 5-22](#)
- [Enabling EAP-FAST, page 5-24](#)
- [Enabling Host-Based EAP, page 5-28](#)
- [Disabling LEAP, EAP-FAST, or Host-Based EAP, page 5-35](#)

# Configuring Your Client Adapter

When you choose to create a new profile or edit an existing profile on the Profiles window, the Properties window appears with the name of your profile in quotation marks. This window enables you to set the configuration parameters for that profile. Follow these steps to access the Properties window and complete the configuration process.

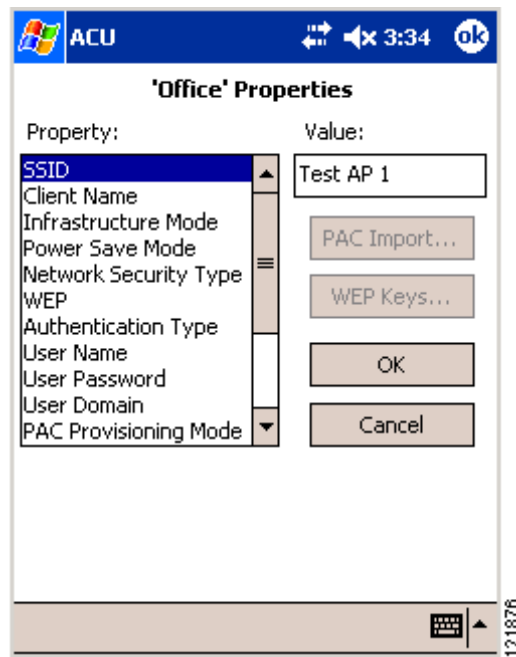


## Note

If you do not change any of the configuration parameters, the default values are used.

- Step 1** When you create or select a profile on the Profiles window and tap the **Edit** button, the Properties window appears (see [Figure 5-1](#)).

**Figure 5-1 Properties Window**



The Property box lists the configuration parameters that can be changed, and the Value box contains the highlighted parameter's current value. The Value box can appear as a drop-down menu with several possible values from which to choose or as a blank field in which characters are to be entered.

- Step 2** [Table 5-1](#) lists and describes the client adapter's configuration parameters. Follow the instructions in the table to initially set or change any parameters.



## Note

The security parameters (Network Security Type, WEP, User Name, User Password, User Domain, PAC Provisioning Mode, and PAC Authority) are listed at the end of the table because they require further action.

Table 5-1 Client Adapter Configuration Parameters

Parameter	Description						
SSID	<p>The service set identifier (SSID) identifies the specific wireless network that you want to access.</p> <p><b>Range:</b> You can key in up to 32 characters (case sensitive)</p> <p><b>Default:</b> A blank field</p> <p><b>Note</b> If you leave this parameter blank, your client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs (see the AP Radio Hardware page in the access point management system). If the access point with which the client adapter is to communicate is not configured to allow broadcast SSIDs, the value of this parameter must match the SSID of the access point. Otherwise, the client adapter cannot access the network.</p>						
Client Name	<p>A logical name for your Windows CE device. It allows an administrator to determine which devices are connected to the access point without having to memorize every MAC address. This name is included in the access point’s list of connected devices.</p> <p><b>Range:</b> You can enter up to 16 characters</p> <p><b>Default:</b> A blank field</p> <p><b>Note</b> Each computer on the network should have a unique client name.</p>						
Infrastructure Mode	<p>Specifies the type of network in which your client adapter is installed.</p> <p><b>Options:</b> Yes or No</p> <p><b>Default:</b> Yes</p> <table><tr><th>Infrastructure Mode</th><th>Description</th></tr><tr><td>Yes</td><td>Indicates that your wireless network is connected to a wired Ethernet network through an access point.</td></tr><tr><td>No</td><td>Often referred to as <i>ad hoc</i> or <i>peer-to-peer mode</i>. Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point.</td></tr></table>	Infrastructure Mode	Description	Yes	Indicates that your wireless network is connected to a wired Ethernet network through an access point.	No	Often referred to as <i>ad hoc</i> or <i>peer-to-peer mode</i> . Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point.
Infrastructure Mode	Description						
Yes	Indicates that your wireless network is connected to a wired Ethernet network through an access point.						
No	Often referred to as <i>ad hoc</i> or <i>peer-to-peer mode</i> . Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point.						

**Table 5-1** Client Adapter Configuration Parameters (continued)

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



Table 5-1 Client Adapter Configuration Parameters (continued)

Parameter	Description	
Authentication Type	Defines how your client adapter will attempt to authenticate to an access point. <b>Options:</b> Open or Shared Key <b>Default:</b> Open	
	Authentication	Description
	Open Authentication	Enables your client adapter, regardless of its WEP settings, to authenticate and attempt to communicate with an access point. If LEAP, EAP-FAST, or host-based EAP is enabled on your client adapter, Open Authentication is the only available option.
	Shared Key Authentication	Enables your client adapter to communicate only with access points that have the same WEP key. This option is available only if Static WEP Keys is selected.  The access point sends a known unencrypted “challenge packet” to the client adapter, which encrypts the packet and sends it back to the access point. The access point attempts to decrypt the encrypted packet and sends an authentication response packet indicating the success or failure of the decryption back to the client adapter.
	<b>Note</b>	Cisco recommends that shared key authentication not be used because it presents a security risk.
Mixed Mode	Indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations. <ul style="list-style-type: none"><li>• If the access point with which the client adapter is to associate has WEP set to Optional and WEP is enabled on the client adapter, you must enable Mixed Mode on the adapter. Otherwise, the client adapter cannot establish a connection with the access point.</li><li>• If the access point with which the client adapter is to associate does not have WEP set to Optional, Mixed Mode should be set to Disabled on the adapter.</li></ul> <b>Options:</b> Enabled or Disabled <b>Default:</b> Disabled <b>Note</b> For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP.	

**Table 5-1** *Client Adapter Configuration Parameters (continued)*

Parameter	Description												
World Mode	<p>Enables the client adapter to adopt the maximum transmit power level and the frequency range of the access point to which it is associated, provided the access point is also configured for world mode. This parameter is available only in infrastructure mode and is designed for users who travel between countries and want their client adapters to associate to access points in different regulatory domains.</p> <p><b>Options:</b> Enabled or Disabled</p> <p><b>Default:</b> Disabled</p> <p><b>Note</b> When World Mode is enabled, the client adapter is limited to the maximum transmit power level allowed by the country of operation's regulatory agency.</p>												
Data Rates	<p>Specifies the rate at which your client adapter should transmit or receive packets to or from access points (in infrastructure mode) or other clients (in ad hoc mode).</p> <p>Auto is recommended for infrastructure mode; setting a specific data rate is recommended for ad hoc mode.</p> <p><b>Options:</b> Auto, 1 Mb Only, 2 Mb Only, 5.5 Mb Only, or 11 Mb Only</p> <p><b>Default:</b> Auto</p> <table> <tr> <th>Data Rate</th><th>Description</th></tr> <tr> <td>Auto</td><td>Uses the 11-Mbps data rate when possible but drops to lower rates when necessary</td></tr> <tr> <td>1 Mb Only</td><td>Offers the greatest range but the lowest throughput</td></tr> <tr> <td>2 Mb Only</td><td>Offers less range but greater throughput than the 1 Mbps Only option</td></tr> <tr> <td>5.5 Mb Only</td><td>Offers less range but greater throughput than the 2 Mbps Only option</td></tr> <tr> <td>11 Mb Only</td><td>Offers the greatest throughput but the lowest range</td></tr> </table> <p><b>Note</b> Your client adapter's data rate must be set to Auto or must match the data rate of the access point (in infrastructure mode) or the other clients (in ad hoc mode) with which it is to communicate. Otherwise, your client adapter may not be able to associate to them.</p>	Data Rate	Description	Auto	Uses the 11-Mbps data rate when possible but drops to lower rates when necessary	1 Mb Only	Offers the greatest range but the lowest throughput	2 Mb Only	Offers less range but greater throughput than the 1 Mbps Only option	5.5 Mb Only	Offers less range but greater throughput than the 2 Mbps Only option	11 Mb Only	Offers the greatest throughput but the lowest range
Data Rate	Description												
Auto	Uses the 11-Mbps data rate when possible but drops to lower rates when necessary												
1 Mb Only	Offers the greatest range but the lowest throughput												
2 Mb Only	Offers less range but greater throughput than the 1 Mbps Only option												
5.5 Mb Only	Offers less range but greater throughput than the 2 Mbps Only option												
11 Mb Only	Offers the greatest throughput but the lowest range												

**Table 5-1** Client Adapter Configuration Parameters (continued)

Parameter	Description
Transmit Power	<p>Defines the power level at which your client adapter transmits. This value must not be higher than that allowed by your country's regulatory agency (FCC in the U.S., DOC in Canada, ETSI in Europe, MKK in Japan, etc.).</p> <p><b>Options:</b> Max, 100 mW, 50 mW, 30 mW, 20 mW, 5 mW, or 1 mW</p> <p><b>Default:</b> Max (the maximum level programmed into the client adapter and allowed by your country's regulatory agency)</p> <p><b>Note</b> Reducing the transmit power level conserves battery power but decreases radio range.</p> <p><b>Note</b> If the client adapter is running, ACU queries the adapter and displays the settings programmed into the adapter. If the client adapter is not running, ACU displays power level options based on the last known radio type.</p> <p><b>Note</b> When World Mode is enabled, the client adapter is limited to the maximum transmit power level allowed by the country of operation's regulatory agency.</p> <p><b>Note</b> If you are using an older version of a 350 series client adapter, your power level options may be different than those listed here.</p>
Offline Channel Scan	<p>Causes the client adapter to periodically scan for a better access point with the same SSID if the signal strength falls below 50%.</p> <p><b>Options:</b> Enabled or Disabled</p> <p><b>Default:</b> Enabled</p>

**Table 5-1** *Client Adapter Configuration Parameters (continued)*

Parameter	Description
WEP	<p>Specifies the type of wired equivalent privacy (WEP) that your client adapter will use.</p> <p><b>Options:</b> No WEP, Static WEP Keys, or Dynamic WEP Keys</p> <p><b>Default:</b> No WEP</p>
<b>WEP</b>	<b>Description</b>
No WEP	Disables WEP for your client adapter.
Static WEP Keys	<p>Enables static WEP for your client adapter after you enter a valid WEP key.</p> <p><b>Note</b> Go to <a href="#">Step 3</a> for instructions on entering a static WEP key and enabling WEP.</p>
Dynamic WEP Keys	<p>Enables WEP keys to be derived automatically during EAP authentication.</p> <p>If you set the Network Security Type to LEAP or EAP-FAST, Dynamic WEP Keys is set automatically. If, on a PPC 2002 device, you set the Network Security Type to Host Based EAP, you must set the WEP parameter to Dynamic WEP Keys.</p> <p><b>Note</b> Go to <a href="#">Step 3</a> for instructions on setting dynamic WEP keys.</p>

Table 5-1 Client Adapter Configuration Parameters (continued)

Parameter	Description	
Network Security Type	Specifies the type of 802.1X authentication that your client adapter will use. <b>Options:</b> None, LEAP, EAP-FAST, or Host Based EAP <b>Default:</b> None	
	Network Security Type	Description
	None	Disables 802.1X authentication for your client adapter.
	LEAP	Specifies that your client adapter use LEAP authentication. <b>Note</b> Go to <a href="#">Step 3</a> for instructions on enabling LEAP.
	EAP-FAST	Specifies that your client adapter use EAP-FAST authentication. <b>Note</b> Go to <a href="#">Step 3</a> for instructions on enabling EAP-FAST.
	LEAP(WPA)	Specifies that your client adapter use LEAP authentication with Wi-Fi Protected Access (WPA). <b>Note</b> Go to <a href="#">Step 3</a> for instructions on enabling LEAP with WPA.
	EAP-FAST(WPA)	Specifies that your client adapter use EAP-FAST authentication with WPA. <b>Note</b> Go to <a href="#">Step 3</a> for instructions on enabling EAP-FAST with WPA.
	Host Based EAP (PPC 2002 devices only)	Specifies that your client adapter use any 802.1X authentication type for which your operating system has support (such as EAP-TLS or PEAP). <b>Note</b> Go to <a href="#">Step 3</a> for instructions on enabling host-based EAP.
User Name	If you are planning to use saved LEAP or saved EAP-FAST credentials rather than entering them in WLM, this parameter specifies the username that is to be saved and used automatically for authentication. This parameter is available only if the Network Security Type is set to LEAP or EAP-FAST. <b>Note</b> Go to <a href="#">Step 3</a> for instructions on entering the LEAP or EAP-FAST username.	

**Table 5-1** Client Adapter Configuration Parameters (continued)

Parameter	Description						
User Password	<p>If you are planning to use saved LEAP or saved EAP-FAST credentials rather than entering them in WLM, this parameter specifies the password that is to be saved and used automatically for authentication. This parameter is available only if the Network Security Type is set to LEAP or EAP-FAST.</p> <p><b>Note</b> Go to <a href="#">Step 3</a> for instructions on entering the LEAP or EAP-FAST password.</p>						
User Domain	<p>If you are planning to use saved LEAP or saved EAP-FAST credentials rather than entering them in WLM, this parameter specifies the domain name (if required) that is to be saved and used automatically for authentication. This parameter is available only if the Network Security Type is set to LEAP or EAP-FAST.</p> <p><b>Note</b> Go to <a href="#">Step 3</a> for instructions on entering the LEAP or EAP-FAST domain name.</p>						
PAC Provisioning Mode	<p>Enables automatic or manual protected access credentials (PAC) provisioning for this profile. This parameter is available only if the Network Security Type is set to EAP-FAST.</p> <p><b>Options:</b> Automatic or Manual</p> <p><b>Default:</b> Automatic</p> <table> <tr> <th>PAC Provisioning Mode</th><th>Description</th></tr> <tr> <td>Automatic</td><td>Enables automatic PAC provisioning. A PAC file is obtained automatically as needed (for instance, when a PAC expires, when the client adapter accesses a different server, when the EAP-FAST username cannot be matched to a previously provisioned PAC, etc.).</td></tr> <tr> <td>Manual</td><td>Enables manual PAC provisioning. You must select a PAC authority or manually import a PAC file.</td></tr> </table> <p><b>Note</b> LDAP user databases support only manual PAC provisioning while Cisco Secure ACS internal, Cisco Secure ODBC, and Windows NT/2000/2003 domain user databases support both automatic and manual PAC provisioning.</p> <p><b>Note</b> Provisioning occurs only upon initial negotiation of the PAC or upon PAC expiration. After the PAC is provisioned, it serves as the key by which authentication transactions are secured.</p> <p><b>Note</b> Go to <a href="#">Step 3</a> for instructions on enabling automatic PAC provisioning or manually importing a PAC file.</p>	PAC Provisioning Mode	Description	Automatic	Enables automatic PAC provisioning. A PAC file is obtained automatically as needed (for instance, when a PAC expires, when the client adapter accesses a different server, when the EAP-FAST username cannot be matched to a previously provisioned PAC, etc.).	Manual	Enables manual PAC provisioning. You must select a PAC authority or manually import a PAC file.
PAC Provisioning Mode	Description						
Automatic	Enables automatic PAC provisioning. A PAC file is obtained automatically as needed (for instance, when a PAC expires, when the client adapter accesses a different server, when the EAP-FAST username cannot be matched to a previously provisioned PAC, etc.).						
Manual	Enables manual PAC provisioning. You must select a PAC authority or manually import a PAC file.						

**Table 5-1 Client Adapter Configuration Parameters (continued)**

Parameter	Description
PAC Authority	Contains the names of all the PAC authorities from which a PAC has previously been provisioned. If this profile is set for manual provisioning, you must select a PAC authority or import a PAC file. This parameter is available only if the Network Security Type is set to EAP-FAST.  <b>Note</b> Go to <a href="#">Step 3</a> for instructions on selecting a PAC authority.

- Step 3** If you plan to use any of the security features (static WEP, LEAP, EAP-FAST, EAP-TLS, or PEAP), read the [“Overview of Security Features”](#) section below and follow the instructions for the security feature you want to activate.
- Step 4** Tap **OK** on the Properties window to save any changes you have made. If the profile you just edited is the active profile and your client adapter is inserted, the changes are applied immediately.

## Overview of Security Features

When you use your client adapter with Windows CE, you can protect your data as it is transmitted through your wireless network by encrypting it through the use of wired equivalent privacy (WEP) encryption keys. With WEP encryption, the transmitting device encrypts each packet with a WEP key, and the receiving device uses that same key to decrypt each packet.

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

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



### Note

Refer to the [“Additional WEP Key Security Features”](#) section on page 5-16 for information on three security features that can make your WEP keys even more secure.

## Static WEP Keys

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

Static WEP keys are write-only and temporary; however, you do not need to re-enter them each time the client adapter is inserted or the Windows CE device is reset. This is because the keys are stored (in an encrypted format for security reasons) in the registry of the Windows CE device. When the driver loads and reads the client adapter’s registry parameters, it also finds the static WEP keys, unencrypts them, and stores them in volatile memory on the adapter.

The ACU Properties window enables you to view the current WEP key settings for the client adapter and then to assign new WEP keys or overwrite existing WEP keys as well as to enable or disable static WEP. Refer to the [“Using Static WEP” section on page 5-20](#) for instructions.

## Dynamic WEP Keys with EAP

The new standard for wireless LAN security, as defined by the Institute of Electrical and Electronics Engineers (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 Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.

Up to three 802.1X authentication types can be selected in ACU for use with Windows CE devices:

- **EAP-Cisco Wireless (or LEAP)**—Support for LEAP is provided not in the Windows CE operating system but in your client adapter’s firmware and the Cisco software that supports it. RADIUS servers that support LEAP include Cisco Secure ACS version 2.6 and later, Cisco Access Registrar version 1.7 and later, and Funk Software’s Steel-Belted RADIUS version 3.0 and later.

LEAP is enabled in ACU, and either a saved LEAP username and password are entered in ACU or a temporary LEAP username and password are entered in WLM. The username and password are used by the client adapter to perform mutual authentication with the RADIUS server through the access point. The temporary LEAP username and password are stored in the client adapter’s volatile memory and need to be re-entered whenever a LEAP profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset.

- **EAP-FAST**—This authentication type (Flexible Authentication via Secure Tunneling) is available on PPC 2002, PPC 2003, and Windows CE .NET 4.2 devices. EAP-FAST uses a three-phased tunneled authentication process to provide advanced 802.1X EAP mutual authentication.
  - Phase 0 enables the client to dynamically provision a protected access credentials (PAC) when necessary. During this phase, a PAC is generated securely between the user and the network.
  - Phase 1 uses the PAC to establish a mutually authenticated and secure tunnel between the client and the RADIUS server. RADIUS servers that support EAP-FAST include Cisco Secure ACS version 3.2.3 and later.
  - Phase 2 performs client authentication in the established tunnel.

EAP-FAST is enabled in ACU, and either a saved EAP-FAST username and password are entered in ACU or a temporary EAP-FAST username and password are entered in WLM. In addition, automatic or manual PAC provisioning is enabled in ACU. The client adapter uses the username, password, and PAC to perform mutual authentication with the RADIUS server through the access point. The temporary EAP-FAST username and password are stored in the client adapter’s volatile memory and need to be re-entered whenever an EAP-FAST profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset.

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

- PACs are stored in a single PAC database and are available to all users of the device.
- PAC files can be added or replaced using the import feature, but they cannot be removed or exported.



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

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

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

- **Host Based EAP** (PPC 2002 devices only)—Selecting this option enables you to use any 802.1X authentication type for which your Windows CE device has support, such as EAP-TLS or PEAP. You can select this option only on PPC 2002 devices with the 802.1X backport installed.



**Note** PPC 2003 and other Windows CE .NET 4.2 devices can be configured for EAP-TLS or PEAP authentication if you configure your client adapter through Windows CE .NET instead of ACU. See [Appendix E](#) for instructions.

- **EAP-TLS**—EAP-TLS is enabled or disabled through the Authentication Manager and uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. EAP-TLS requires the use of certificates for authentication.

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

- **Cisco PEAP**—Cisco PEAP authentication (also known as *PEAP-GTC*) is designed to support One-Time Password (OTP), Windows NT or 2000 domain, and LDAP user databases over a wireless LAN. It is based on EAP-TLS authentication but uses a password instead of a client certificate for authentication. Cisco PEAP is enabled or disabled through the Authentication Manager and uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. Cisco PEAP requires you to enter your username and password in order to start the authentication process and gain access to the network. RADIUS servers that support Cisco PEAP authentication include Cisco Secure ACS version 3.1 or later.



**Note** To use Cisco PEAP authentication, you must have checked the **Install Cisco PEAP Support** check box during installation.

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

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



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

2. Communicating through the access point, the client and RADIUS server complete the authentication process, with the password (LEAP and PEAP), password and PAC (EAP-FAST), or certificate (EAP-TLS) being the shared secret for authentication. The password or PAC is never transmitted during the process.
3. If authentication is successful, the client and RADIUS server derive a dynamic, session-based WEP key that is unique to the client.

4. The RADIUS server transmits the key to the access point using a secure channel on the wired LAN.
5. For the length of a session, or time period, the access point and the client use this key to encrypt or decrypt all unicast packets (and broadcast packets if the access point is set up to do so) that travel between them.

Refer to one of these sections for instructions on enabling EAP authentication:

- [Enabling LEAP, page 5-22](#)
- [Enabling EAP-FAST, page 5-24](#)
- [Enabling Host-Based EAP, page 5-28](#)

**Note**

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

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur\\_c/scprt2/scrad.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt2/scrad.htm)

## Wi-Fi Protected Access (WPA)

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

Using WPA key management, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). The server generates the PMK dynamically and passes it to the access point.

When you configure your client adapter through ACU, only 350 series cards that are installed in Windows CE .NET 4.2 devices and running LEAP or EAP-FAST authentication can be used with WPA. Support for WPA is available in client adapter driver and utility version 2.60 or later.

Refer to one of these sections for instructions on enabling LEAP or EAP-FAST authentication with WPA:

- [Enabling LEAP, page 5-22](#)
- [Enabling EAP-FAST, page 5-24](#)

**Note**

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

## Fast Roaming (CCKM)

Some applications that run on a client device may require fast roaming between access points. Voice applications, for example, require seamless roaming to prevent delays and gaps in conversation. Support for fast roaming is available for LEAP- or EAP-FAST-enabled clients in firmware version 5.40.10.

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

This feature does not need to be enabled on the client adapter; it is supported automatically in client adapter firmware version 5.40.10. However, it must be enabled on the access point.

**Note**

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

## Reporting Access Points that Fail LEAP or EAP-FAST Authentication

The following client adapter and access point firmware versions support a feature that is designed to detect access points that fail LEAP or EAP-FAST authentication:

- Client adapter firmware version 5.40.10
- 12.00T or later (340, 350, and 1200 series access points)
- Cisco IOS Release 12.2(4)JA or later (1100 series access points)

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

The process takes place as follows:

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

**Note**

This feature does not need to be enabled on the client adapter or access point; it is supported automatically in the firmware of both devices. However, both the client and access point must use these firmware versions.

## Additional WEP Key Security Features

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



**Note**

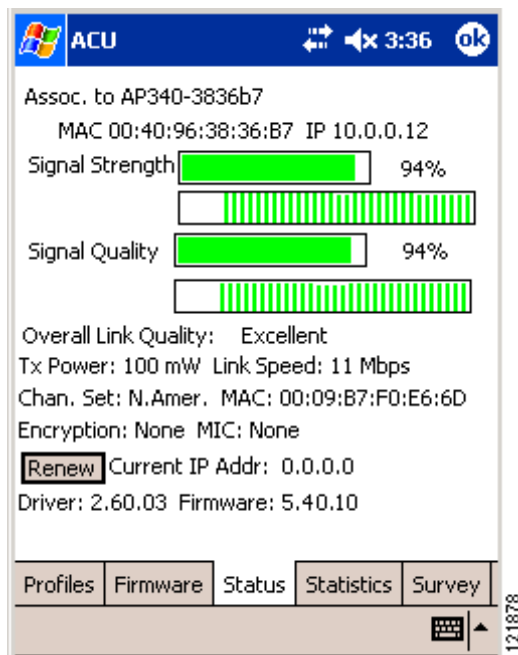
Access point firmware version 11.10T or later is required to enable these security features. Refer to the software configuration guide for your access point for instructions on enabling these features.

## Message Integrity Check (MIC)

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

The Status window indicates if MIC is supported by the client adapter's driver and is enabled on the access point. See [Figure 5-2](#).

**Figure 5-2** Status Window



**Note**

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

## Temporal Key Integrity Protocol (TKIP)

This feature, also referred to as *WEP key hashing*, defends against an attack on WEP in which the intruder uses the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs. It protects both unicast and broadcast WEP keys.



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

## Broadcast Key Rotation

EAP authentication provides dynamic unicast WEP keys for client devices but uses static broadcast, or multicast, keys. When you enable broadcast WEP key rotation, the access point provides a dynamic broadcast WEP key and changes it at the interval you select. When you enable this feature, only wireless client devices using LEAP, EAP-FAST, EAP-TLS, or PEAP authentication can associate to the access point. Client devices using static WEP (with open or shared key authentication) cannot associate.

## Synchronizing Security Features

In order to use any of the security features discussed in this section, both your client adapter and the access point to which it will associate must be set appropriately. [Table 5-2](#) indicates the client and access point settings required for each security feature. This chapter provides specific instructions for enabling the security features on your client adapter. Refer to the documentation for your access point for instructions on enabling any of these features on the access point.

**Table 5-2 Client and Access Point Security Settings**

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Create a WEP key and enable Static WEP Keys and Open Authentication	Set up and enable WEP and enable Open Authentication for the SSID
Static WEP with shared key authentication	Create a WEP key and enable Static WEP Keys and Shared Key Authentication	Set up and enable WEP and enable Shared Key Authentication for the SSID
LEAP authentication	Enable LEAP	Set up and enable WEP and enable Network-EAP for the SSID
LEAP authentication with WPA (on Windows CE .NET 4.2 devices only)	Enable LEAP(WPA)	Select a cipher suite that includes TKIP, set up and enable WEP, and enable Network-EAP and WPA for the SSID  <b>Note</b> To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.
EAP-FAST authentication	Enable EAP-FAST and enable automatic provisioning or import a PAC file	Set up and enable WEP and enable Network-EAP for the SSID

**Table 5-2 Client and Access Point Security Settings (continued)**

Security Feature	Client Setting	Access Point Setting
EAP-FAST authentication with WPA (on Windows CE .NET 4.2 devices only)	Enable EAP-FAST(WPA) and enable automatic provisioning or import a PAC file	<p>Select a cipher suite that includes TKIP, set up and enable WEP, and enable Network-EAP and WPA for the SSID</p> <p><b>Note</b> To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.</p>
EAP-TLS authentication		
If using ACU to configure card (on PPC 2002 devices)	Enable Host Based EAP and Dynamic WEP Keys in ACU and select TLS as the EAP Type in the Authentication Manager	Set up and enable WEP and enable Open Authentication for the SSID and specify the use of EAP
If using Windows CE .NET to configure card (on PPC 2003 and Windows CE .NET 4.2 devices)	Select Enable 802.1X Authentication on This Network and TLS as the EAP Type	Set up and enable WEP and enable Open Authentication for the SSID and specify the use of EAP
PEAP authentication		
If using ACU to configure card (on PPC 2002 devices)	Enable Host Based EAP and Dynamic WEP Keys in ACU and select Cisco PEAP (or PEAP if the Microsoft PEAP supplicant is installed) as the EAP Type in the Authentication Manager	Set up and enable WEP and enable Open Authentication for the SSID and specify the use of EAP
If using Windows CE .NET to configure card (on PPC 2003 and Windows CE .NET 4.2 devices)	Select Enable 802.1X Authentication on This Network and Cisco PEAP (or PEAP, which denotes the Microsoft PEAP supplicant) as the EAP Type	Set up and enable WEP and enable Open Authentication for the SSID and specify the use of EAP
Fast roaming (CCKM)	Enable LEAP or EAP-FAST and use firmware version 5.40.10	<p>Use firmware version 12.2(11)JA or later, select a cipher suite that is compatible with CCKM, and enable Network-EAP and CCKM for the SSID.</p> <p><b>Note</b> To allow both 802.1X clients and non-802.1X clients to use the SSID, enable optional CCKM.</p>

**Table 5-2 Client and Access Point Security Settings (continued)**

Security Feature	Client Setting	Access Point Setting
Fast roaming (CCKM) with TKIP	Enable LEAP(WPA) or EAP-FAST(WPA) and use firmware version 5.40.10	Use firmware version 12.2(11)JA or later, select a cipher suite that includes TKIP, and enable Network-EAP and CCKM for the SSID.  <b>Note</b> To allow both 802.1X clients and non-802.1X clients to use the SSID, enable optional CCKM.
Reporting access points that fail LEAP or EAP-FAST authentication	No settings required; automatically enabled in firmware version 5.40.10	No settings required; automatically enabled in the following firmware versions: 12.00T or later (340, 350, and 1200 series access points) or Cisco IOS Release 12.2(4)JA or later (1100 series access points)
MIC	Automatically enabled in driver	Set up and enable WEP with full encryption, set MIC to MMH or select Enable MIC check box, and set Use Aironet Extensions to Yes
TKIP	Automatically enabled in firmware	Set up and enable WEP, set TKIP to Cisco or select Enable Per Packet Keying check box, and set Use Aironet Extensions to Yes
Broadcast key rotation	Enable LEAP, EAP-FAST, EAP-TLS, or PEAP	Set up and enable WEP and set Broadcast WEP Key Rotation Interval to any value other than zero (0)

# Using Static WEP

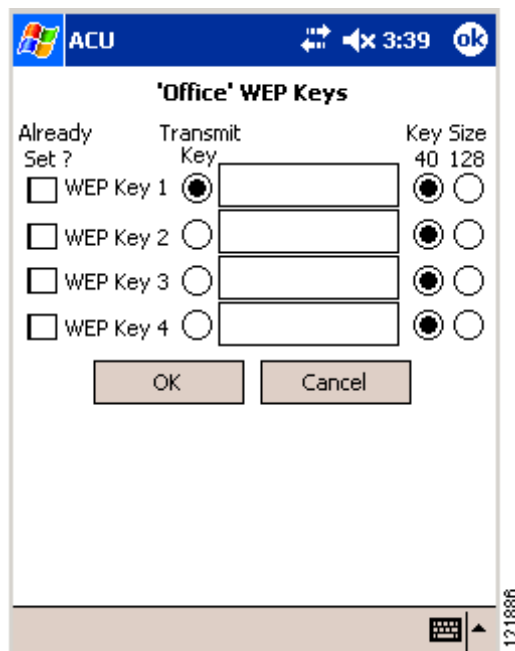
This section provides instructions for entering new static WEP keys or overwriting existing static WEP keys.

## Enabling Static WEP and Entering a New Static WEP Key

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

- Step 1 From the Properties window, select **Network Security Type** under Property and **None** from the list of options in the Value box.
- Step 2 Select **WEP** under Property and **Static WEP Keys** from the list of options in the Value box.
- Step 3 Tap the **WEP Keys** button. The WEP Keys window appears (see [Figure 5-3](#)).


**Figure 5-3** WEP Keys Window



This window allows you to create up to four static WEP keys.


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



- Step 5** Obtain the static WEP key from your system administrator and enter it in the blank field for the key you are creating. Follow the guidelines below to enter a new static WEP key:
- WEP keys can consist of the following hexadecimal characters: 0-9, A-F, and a-f.
  - WEP keys must contain the following number of characters:
    - 10 hexadecimal characters for 40-bit keys  
**Example:** 12345abcde
    - 26 hexadecimal characters for 128-bit keys  
**Example:** AB34CD78EFab01cd23ef456789
  - Your client adapter's WEP key must match the WEP key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.
  - When setting more than one WEP key, the keys must be assigned to the same WEP key numbers for all devices. For example, WEP key 2 must be WEP key number 2 on all devices. When multiple WEP keys are set, they must be in the same order on all devices.
-  **Note** After you enter a WEP key, you can write over it, but you cannot edit or delete it.
- Step 6** Tap the **Transmit Key** button to the left of the key you want to use to transmit packets. Only one WEP key can be selected as the transmit key.
- Step 7** Tap **OK** to write your WEP key(s) to the client adapter's volatile memory and the registry of the Windows CE device or tap **Cancel** to exit the WEP Keys window without updating the keys.
- Step 8** Tap **OK** to save your changes.

## Overwriting an Existing Static WEP Key

Follow these steps to overwrite an existing static WEP key.

- Step 1** From the Properties window, tap the **WEP Keys** button. The WEP Keys window appears (see [Figure 5-3](#)). A check mark appears in the Already Set? box for all existing static WEP keys.
-  **Note** For security reasons, the codes for existing static WEP keys do not appear on the window. Also, you can write over existing keys, but you cannot edit or delete them.
- Step 2** Decide which existing static WEP key you want to overwrite.
- Step 3** Tap within the blank field of that key.
- Step 4** Enter a new key, following the guidelines outlined in [Step 5](#) of the “[Enabling Static WEP and Entering a New Static WEP Key](#)” section on page 5-20.
- Step 5** Make sure the **Transmit Key** button to the left of your key is selected, if you want this key to be used to transmit packets.

- Step 6 Tap **OK** to write your new static WEP key to the client adapter's volatile memory and the registry of the Windows CE device or tap **Cancel** to exit the WEP Keys window without overwriting any keys.
- Step 7 Tap **OK** to save your changes.
- 

## Disabling Static WEP

Follow these steps if you ever need to disable static WEP.



**Note**

Selecting LEAP for the Network Security Type disables static WEP automatically.

---

- Step 1 Double-tap the **ACU** icon or select **Start > Programs > Cisco > ACU**. The Profiles window appears.
- Step 2 Select the profile that you want to change from the Manage Profiles box and tap the **Edit** button.
- Step 3 Select **WEP** under Property and **No WEP** from the list of options in the Value box.
- Step 4 Tap **OK** to save your changes.
- 

## Enabling LEAP

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

- Client adapters must support WEP.
- To use WPA, 350 series client adapters must be installed in Windows CE .NET 4.2 devices and use client adapter driver and utility version 2.60 or later.
- Access points to which your client adapter may attempt to authenticate must use the following firmware versions or later: 11.23T (340 and 350 series access points), 11.54T (1200 series access points), or Cisco IOS Release 12.2(4)JA (1100 series access points).



**Note**

To use WPA or fast roaming (CCKM), access points must use Cisco IOS Release 12.2(11)JA or later. To use the Reporting Access Points That Fail LEAP or EAP-FAST Authentication and Fast Roaming features, access points must use the firmware versions listed on [page 5-14](#).

---

- All necessary infrastructure devices such as access points and servers must be properly configured for LEAP authentication.



**Note**

Cisco recommends the use of strong passwords for LEAP authentication in order to minimize the risk of successful attacks by rogue access points. Refer to the [“Creating Strong Passwords” section on page 9-4](#) for tips on creating strong passwords.

---

Follow these steps to enable LEAP authentication for this profile.

**Step 1** From the Properties window, select **Network Security Type** under Property and **LEAP** or **LEAP(WPA)** from the list of options in the Value box. When LEAP or LEAP(WPA) is enabled, the following parameters on the Properties window are changed automatically:

- WEP is set to Dynamic WEP Keys.
- Authentication Type is set to Open.



**Note** If you select LEAP(WPA), TKIP is used for data encryption, and the Encryption field on the ACU Status window shows WPA TKIP.



**Note** Refer to the [“Wi-Fi Protected Access \(WPA\)” section on page 5-14](#) for additional information.

**Step 2** Perform one of the following:

- If you want to use a temporary username and password (which must be entered whenever a LEAP profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset in order to authenticate and gain access to the network), go to [Step 3](#).
- If you want to use a saved username and password (which do not need to be entered whenever a LEAP profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset because authentication occurs automatically as needed using your saved credentials), enter your LEAP username, password, and optional domain name in the User Name, User Password, and User Domain edit boxes.



**Note** Usernames are limited to 64 ASCII characters, and passwords are limited to 32 ASCII characters. However, if a domain name is entered in the User Domain field, the sum of the username and domain name is limited to 63 ASCII characters.

**Step 3** Tap **OK** to enable LEAP.

**Step 4** Refer to the [“Using LEAP or EAP-FAST” section on page 6-2](#) for instructions on authenticating using LEAP.

# Enabling EAP-FAST

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

- 350 series client adapters must be installed on a PPC 2002, PPC 2003, or Windows CE .NET 4.2 device.
- Client adapters must support WEP and use firmware version 5.40.10.
- To use WPA, client adapters must be installed in Windows CE .NET 4.2 devices and use client adapter driver and utility version 2.60 or later.
- Access points to which your client adapter may attempt to authenticate must use the following firmware versions or later: 11.23T (340 and 350 series access points), 11.54T (1200 series access points), or Cisco IOS Release 12.2(4)JA (1100 series access points).



## Note

To use WPA or fast roaming (CCKM), access points must use Cisco IOS Release 12.2(11)JA or later. To use the Reporting Access Points That Fail LEAP or EAP-FAST Authentication and Fast Roaming features, access points must use the firmware versions listed on [page 5-14](#).

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

## Obtaining a PAC File (Manual PAC Provisioning Only)

If you are planning to enable manual PAC provisioning for this EAP-FAST profile, you must obtain a PAC file before you can import it for use on your Windows CE device. Follow these steps if you have not yet obtained a PAC file.

- Step 1** Obtain the PAC file (\*.pac) from your system administrator.
- Step 2** Establish an ActiveSync connection between your laptop or PC and your Windows CE device.
- Step 3** Use **Windows Explorer** to copy the PAC file and paste it into a folder under **My Computer > Mobile Device**.



## Note

For PPC devices, the destination must be either the Business or Personal folder.

- Step 4** Follow the steps in the [“Enabling EAP-FAST”](#) section below to import the PAC file for your Windows CE device.

## Enabling EAP-FAST

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

- Step 1** From the Properties window, select **Network Security Type** under Property and **EAP-FAST** or **EAP-FAST(WPA)** from the list of options in the Value box. When EAP-FAST or EAP-FAST(WPA) is enabled, the following parameters on the Properties window are changed automatically:

- WEP is set to Dynamic WEP Keys.
- Authentication Type is set to Open.



**Note** If you select EAP-FAST(WPA), TKIP is used for data encryption, and the Encryption field on the ACU Status window shows WPA TKIP.



**Note** Refer to the [“Wi-Fi Protected Access \(WPA\)” section on page 5-14](#) for additional information.

- Step 2** Perform one of the following:
- If you want to use a temporary username and password (which must be entered whenever an EAP-FAST profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset in order to authenticate and gain access to the network), go to [Step 3](#).
  - If you want to use a saved username and password (which do not need to be entered whenever an EAP-FAST profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset because authentication occurs automatically as needed using your saved credentials), enter your EAP-FAST username, password, and optional domain name in the User Name, User Password, and User Domain edit boxes.



**Note** Usernames are limited to 64 ASCII characters, and passwords are limited to 32 ASCII characters. However, if a domain name is entered in the User Domain field, the sum of the username and domain name is limited to 63 ASCII characters.

- Step 3** Perform one of the following:
- If you want to enable automatic PAC provisioning, select **PAC Provisioning Mode** under Property and **Automatic** from the list of options in the Value box. A protected authentication credentials (PAC) file is obtained automatically as needed (for instance, when a PAC expires, when the client adapter accesses a different server, when the EAP-FAST username cannot be matched to a previously provisioned PAC, etc.). This is the default setting. If you select this option, go to [Step 5](#).
  - If you want to enable manual PAC provisioning, select **PAC Provisioning Mode** under Property and **Manual** from the list of options in the Value box. You must select a PAC authority or manually import a PAC file. If you select this option, go to [Step 4](#).



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

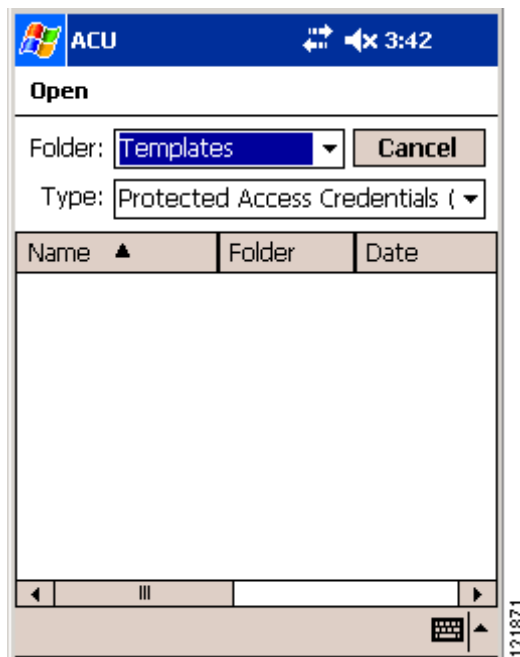
**Note**

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

**Step 4** Perform one of the following to enable manual PAC provisioning:

- Select **PAC Authority** under Property and select the PAC authority associated with the profile's SSID from the list of options in the Value box. The list contains the names of all the PAC authorities from which PACs have previously been provisioned.
- If the PAC authority list is empty or does not contain the name of a desired PAC authority, follow these steps to import a PAC file:
  - a. Tap the **PAC Import** button. The Open window appears (see [Figure 5-4](#)).

**Figure 5-4** Open Window



- b. Select the folder where the PAC file is located from the Folder drop-down menu. Then tap the file (\*.pac) in the Name field in the center of the window.

**Note**

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

- c. If the PAC Password window appears (see [Figure 5-5](#)), enter the PAC file password and tap **OK**.

Figure 5-5 PAC Password Window

**Note**

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

- d. If you try to import a PAC file with the same PAC ID as a previously imported PAC file, you are asked if you want to replace the existing PAC. If you tap **Yes**, the existing PAC is replaced by the new one from the imported file.
- e. The PAC file is imported, and the PAC authority that issued the PAC file is added to the PAC authority list as the active PAC authority.

**Step 5** Tap **OK** to enable EAP-FAST. If you imported a PAC file, it is now added to your PAC database.

**Step 6** Refer to the [“Using LEAP or EAP-FAST” section on page 6-2](#) for instructions on authenticating using EAP-FAST.

# Enabling Host-Based EAP

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

- The Windows CE device must be a PPC 2002 device.

**Note**

PPC 2003 and other Windows CE .NET 4.2 devices can be configured for EAP-TLS or PEAP authentication if you configure your client adapter through Windows CE .NET instead of ACU. See [Appendix E](#) for instructions.

- Client adapters must support WEP.
- Access points to which your client adapter will attempt to authenticate must use the following firmware versions or later: 11.23T (340 and 350 series access points), 12.2(4)JA (1100 series access points), or 11.54T (1200 series access points).
- All necessary infrastructure devices such as access points, servers, gateways, and user databases must be properly configured for the authentication type you plan to enable on the client.

## Obtaining and Importing CA and User Certificates

EAP-TLS and PEAP authentication require the use of certificates. EAP-TLS requires both a Certificate Authority (CA) certificate and a user certificate while PEAP requires only a CA certificate. After you import the necessary certificates, you should not have to repeat this procedure until the certificates expire (at a time that is predetermined by the certificate server).

**Note**

[Chapter 8](#) provides instructions for viewing and removing certificates, if necessary.

## Obtaining CA and User Certificates

If you have not yet obtained a CA certificate (for EAP-TLS or PEAP) and a user certificate (for EAP-TLS), follow these steps.

- Step 1** Obtain the certificate file(s) (\*.cer or \*.crt) from your system administrator.
- Step 2** Establish an ActiveSync connection between your laptop or PC and your Windows CE device.
- Step 3** Open **Windows Explorer** on your laptop or PC.
- Step 4** Copy the certificate file(s) and paste them into a folder under **My Computer > Mobile Device**.
- Step 5** Follow the steps in the “[Importing a CA Certificate](#)” section on page 5-29 and the “[Importing a User Certificate](#)” section on page 5-30 to import the certificate file(s) for your Windows CE device.

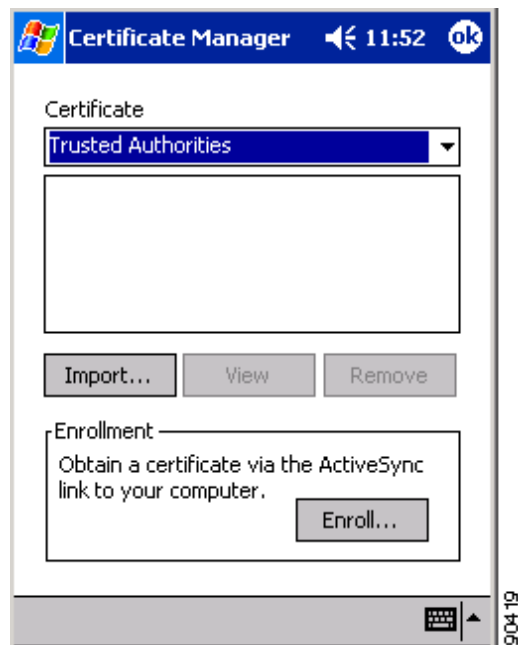


## Importing a CA Certificate

If you are planning to use EAP-TLS or PEAP authentication on a PPC 2002 device, follow these steps to import the CA certificate.

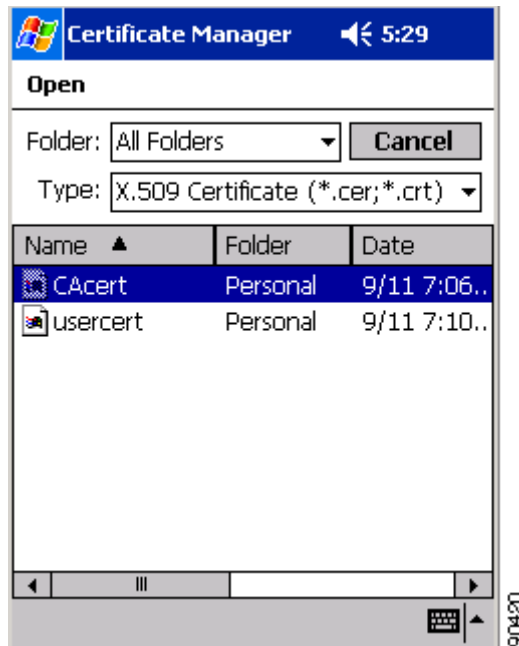
- Step 1** Select **Start > Programs > Cisco > CertMgr**. The Certificate Manager window appears (see [Figure 5-6](#)).

*Figure 5-6 Certificate Manager Window*



- Step 2** Make sure **Trusted Authorities** appears in the Certificate drop-down menu.
- Step 3** Tap the **Import** button.
- Step 4** The Certificate Manager Open window appears (see [Figure 5-7](#)).

Figure 5-7 Certificate Manager Open Window



- Step 5** Tap the CA certificate file.
- Step 6** The Certificate Manager window reappears with the name of the CA certificate server listed in the middle of the window.
- Step 7** Tap **OK** to close the Certificate Manager.

## Importing a User Certificate

If you are planning to use EAP-TLS authentication on a PPC 2002 device, follow these steps to import the user certificate.



### Note

As an alternative to the procedure below, you can use the Certificate Manager to import a user certificate. To do so, follow the steps in the [“Importing a CA Certificate”](#) section above, but make sure My Certificates (not Trusted Authorities) appears in the Certificate drop-down menu in [Step 2](#) and tap the user certificate file (not the CA certificate file) in [Step 5](#).

- Step 1** Make sure that your Windows CE device has an ActiveSync link to a laptop or PC that is on the same network as the certificate server you want to use.
- Step 2** Select **Start > Programs > Cisco > Enroll**. The Certificate Enrollment window appears (see [Figure 5-8](#)).

Figure 5-8 Certificate Enrollment Window



- Step 3** Enter your username, password, and server name for your certificate server, which can be obtained from your system administrator, in the appropriate fields.
- Step 4** Tap the **Enroll** button. The box at the bottom of the window indicates the status of the certificate enrollment by changing from *Ready* to *Processing*.
- If the operation is successful, the following message appears: “A certificate has been added to your device.”
- Step 5** Tap **OK** to close the Certificate Enrollment window.

## Enabling Host-Based EAP

Follow these steps to enable host-based EAP authentication (EAP-TLS or PEAP) for this profile on a PPC 2002 device.



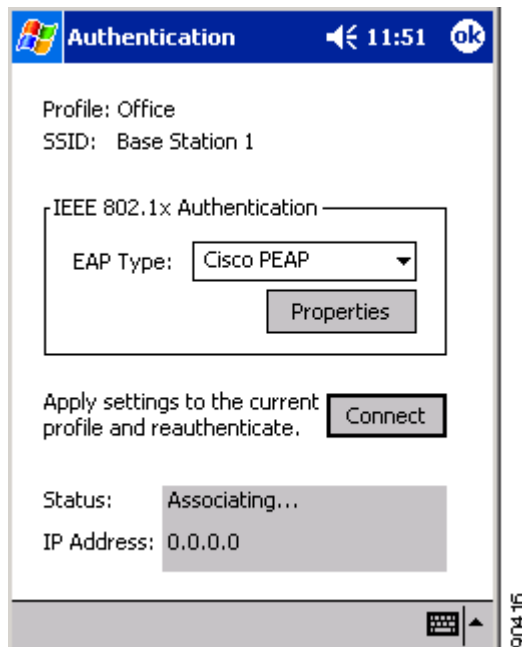
### Note

Because EAP-TLS and PEAP authentication are not enabled in ACU, you cannot switch between these authentication types simply by switching profiles in ACU. You can create a profile in ACU that uses host-based EAP, but you must enable the specific authentication type in the Authentication Manager. In addition, only one authentication type can be set at a time; therefore, if you have more than one profile in ACU that uses host-based EAP and you want to use another authentication type, you must change the authentication type in the Authentication Manager after switching profiles in ACU.

- Step 1** From the Properties window, select **Network Security Type** under Property and **Host Based EAP** from the list of options in the Value box.
- Step 2** Select **WEP** under Property and **Dynamic WEP Keys** from the list of options in the Value box.

- Step 3 Tap **OK** to save your changes.
- Step 4 Select **Start > Programs > Cisco > AuthMgr**. The Authentication window appears (see [Figure 5-9](#)).

**Figure 5-9 Authentication Window**



- Step 5 Perform one of the following, depending on the authentication type you want to use:
- If you are planning to use EAP-TLS, go to the [“Enabling EAP-TLS”](#) section below.
  - If you are planning to use PEAP, go to the [“Enabling PEAP”](#) section on page 5-33.

## Enabling EAP-TLS

Follow these steps to enable EAP-TLS for this profile.

- Step 1 For EAP Type, select **TLS**.
- Step 2 If your Windows CE device has more than one user certificate, tap the **Properties** button. On the Select Certificate window, select the user certificate that you want to use and tap **OK**.
- Step 3 The configuration is complete. Tap the **Connect** button on the Authentication window to start the EAP authentication process.



**Note** Any time you make a change to the active profile in ACU or the Authentication Manager, you must tap the **Connect** button on the Authentication window to start the authentication process.

- Step 4 Refer to the [“Using EAP-TLS”](#) section on page 6-5 for instructions on authenticating using EAP-TLS.

## Enabling PEAP

Follow these steps to enable PEAP for this profile.

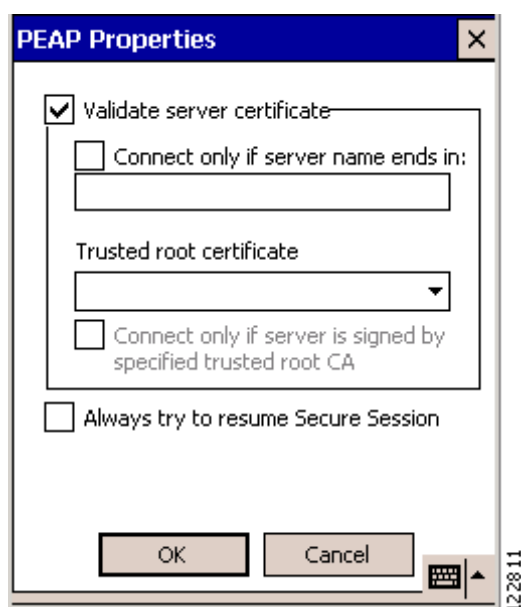
- Step 1** For EAP Type, select **Cisco PEAP** or **PEAP**. If you select Cisco PEAP, go to [Step 2](#). If you select PEAP, go to [Step 9](#).



**Note** **PEAP** appears as an EAP Type option on a PPC 2002 device if the Microsoft PEAP supplicant (rather than the Cisco PEAP supplicant) is installed.

- Step 2** Tap the **Properties** button. The PEAP Properties window appears (see [Figure 5-10](#)).

**Figure 5-10** PEAP Properties Window



- Step 3** Make sure that the **Validate server certificate** check box is checked if server certificate validation is required (recommended).
- Step 4** If you want to specify the name of the server to connect to, check the **Connect only if server name ends in** check box and enter the appropriate server name suffix in the field below.



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



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

- Step 5** Make sure that the name of the certificate authority from which the server certificate was downloaded appears in the Trusted root certificate field. If necessary, tap the arrow on the drop-down menu and select the appropriate name.



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

- Step 6** Check the **Connect only if server is signed by specified trusted root CA** check box if you want to ensure that the certificate server uses the trusted root certificate specified in the field above. This prevents the client from establishing connections to rogue access points.

- Step 7** Perform one of the following:

- Check the **Always try to resume Secure Session** check box if you want the PEAP protocol to always attempt to resume the previous session before prompting you to re-enter your credentials.
- Uncheck the **Always try to resume Secure Session** check box if you want to be prompted to re-enter your username and password whenever your client adapter's radio becomes disassociated (for example, when the card is ejected, the radio is turned off, you wander out of range of an access point, you switch profiles, and so on).



**Note** Checking this check box gives you the convenience of not having to re-enter your username and password when your client adapter experiences momentary losses of association. The PEAP Session Timeout setting on the Cisco Secure ACS System Configuration - Global Authentication Setup window controls how long the resume feature is active (that is, the amount of time during which the PEAP session can be resumed without re-entering user credentials). If you leave your device unattended during this timeout period, be aware that someone can resume your PEAP session and access the network.

- Step 8** Tap **OK** to save your settings. The configuration is complete.

- Step 9** Tap the **Connect** button on the Authentication window to start the EAP authentication process.



**Note** Any time you make a change to the active profile in ACU or the Authentication Manager, you must tap the **Connect** button on the Authentication window to start the authentication process.

- Step 10** Refer to the [“Using PEAP” section on page 6-6](#) for instructions on authenticating using PEAP.

## Disabling LEAP, EAP-FAST, or Host-Based EAP

Follow these steps to disable LEAP, EAP-FAST, or host-based EAP (EAP-TLS or PEAP) for a particular profile on a PPC 2002 device.

- 
- Step 1** Double-tap the **ACU** icon or select **Start > Programs > Cisco > ACU**. The Profiles window appears.
  - Step 2** Select the profile that you want to change from the Manage Profiles box and tap the **Edit** button.
  - Step 3** Select **Network Security Type** under Property and **None** from the list of options in the Value box.
  - Step 4** Tap **OK** to save your changes.
-







## Using EAP Authentication

---

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

The following topics are covered in this chapter:

- [Overview, page 6-2](#)
- [Using LEAP or EAP-FAST, page 6-2](#)
- [Using EAP-TLS, page 6-5](#)
- [Using PEAP, page 6-6](#)

# Overview

This chapter explains the sequence of events that occurs as soon as you select a profile that uses EAP authentication as well as after you eject and reinsert the client adapter, reset the Windows CE device, or are informed that your username and password have expired. The chapter contains three sections based on the profile's authentication type:

- Using LEAP or EAP-FAST, see below
- Using EAP-TLS, [page 6-5](#)
- Using PEAP, [page 6-6](#)

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

**Note**

If any error messages appear during authentication, refer to [Chapter 9](#) for explanations and recommended actions.

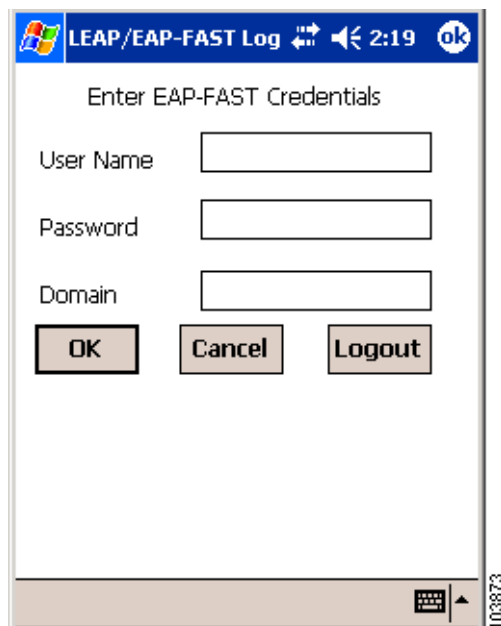
## Using LEAP or EAP-FAST

### With a Temporary Username and Password

After you select a profile that uses LEAP or EAP-FAST authentication (with a temporary username and password) or you eject and reinsert the client adapter or reset your Windows CE device while this profile is selected, follow these steps to authenticate using LEAP or EAP-FAST.

- Step 1** The Wireless Login Module window appears (see [Figure 6-1](#)).

**Figure 6-1** Wireless Login Module Window



**Note**

You can also start WLM by selecting **Start > Programs > Cisco > Wireless Login Module**. You may want to do this if you inadvertently exited WLM after it started or if you roam to a different part of the network where a different login is required.

**Step 2** Obtain your LEAP or EAP-FAST username and password from your system administrator.

**Note**

The password is optional because not all host accounts on the RADIUS server are set up with a password.

**Step 3** Enter your LEAP or EAP-FAST username in the User Name field.

**Step 4** Enter your LEAP or EAP-FAST password in the Password field if your RADIUS server account was set up with a password.

**Note**

For security reasons, the characters entered for the password are displayed as asterisks.

**Step 5** If your RADIUS server account specifies a domain, enter the domain name in the Domain field.

**Step 6** Tap **OK**. If the username and password were entered correctly, they are written to volatile memory on the client adapter. The username and password remain on the client adapter until a different profile is selected, the client adapter is ejected and reinserted, or the Windows CE device is reset.

**Note**

If you want to terminate the LEAP or EAP-FAST session, tap the **Logout** button. If you want to exit WLM, tap the **Cancel** button.

**Step 7** One of three scenarios occurs:

1. The client adapter authenticates to the RADIUS server using your username and password and receives a dynamic, session-based WEP key. The ACU Profiles window indicates if your client adapter is authenticated to an access point.
2. If you enter the username or password incorrectly or enter ones that are not valid for the RADIUS server on the network, the Wireless Login Module window reappears with a message indicating that your login was incorrect. You are able to retry immediately by re-entering the username and password.
3. The client adapter times out while trying to authenticate, possibly because it is out of range of an access point. After 30 seconds, a message appears indicating that the authentication attempt timed out and that you need to rerun WLM.

## With a Saved Username and Password

After you select a profile that uses LEAP or EAP-FAST authentication (with a saved username and password) or you eject and reinsert the client adapter or reset your Windows CE device while this profile is selected, the client adapter should authenticate automatically. The ACU Profiles window indicates if your client adapter is authenticated to an access point.

**Note**

If you entered your username or password incorrectly in the ACU Properties window or entered ones that are not valid for the RADIUS server on the network, the Wireless Login Module window appears with a message indicating that your login was incorrect. Tap **Cancel**; then change your username or password on the ACU Properties window and tap **OK**.

**Note**

If you want to log out of a LEAP or EAP-FAST session, select **Start > Programs > Cisco > Wireless Login Module** and tap the **Logout** button on the Wireless Login Module window.

## After Your EAP-FAST Credentials Expire

If the EAP-FAST credentials (username and password) for your current profile expire or become invalid, follow these steps to change your password.

- Step 1** When the Password Expired window appears (see [Figure 6-2](#)) to indicate that your password has expired, enter your old password in the Old Password field.

**Figure 6-2 Password Expired Window**



- Step 2** Enter your new password in both the New Password and Confirm New fields and tap **OK**.
- Step 3** If prompted, log off and on again in order to update your local cached account with your new password.

## Using EAP-TLS

After you select a profile that uses host-based EAP authentication and configure the card for EAP-TLS, follow these steps to EAP authenticate.



**Note**

These instructions are applicable after profile selection, card ejection and reinsertion, or reset.

- Step 1** If a message appears informing you that you need to accept a certificate to begin the EAP authentication process, tap the message and follow the instructions provided to accept the certificate.

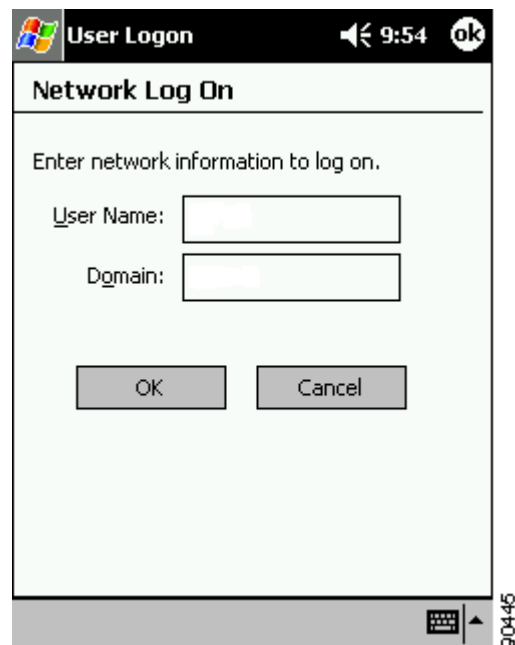


**Note**

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

- Step 2** If a message appears indicating the root certification authority for the server's certificate and it is the correct certification authority, tap **OK** to accept the connection. Otherwise, tap **Cancel**.
- Step 3** If a message appears indicating the server to which your client adapter is connected and it is the correct server to connect to, tap **OK** to accept the connection. Otherwise, tap **Cancel**.
- Step 4** The User Logon window appears (see [Figure 6-3](#)).

**Figure 6-3** User Logon Window



- Step 5** Enter your EAP-TLS username and optional domain name (which are registered with the RADIUS server) in the appropriate fields. For example, if your EAP-TLS username is *jsmith* and the domain name is *corporate*, you would enter **jsmith** in the User Name field and **corporate** in the Domain field.

**Note**

If your network uses a Cisco Secure ACS server, you must leave the Domain field blank and enter the fully qualified domain name in the User Name field as follows: *username@fully.qualified.domain*. For example, if your EAP-TLS username is *jsmith* and the domain name is *corporate on Cisco.com*, you would enter **jsmith@corporate.cisco.com** in the User Name field and leave the Domain field blank.

**Step 6** Tap **OK**. The client adapter should now EAP authenticate.

To verify authentication on a PPC 2002 device, select **Start > Programs > Cisco > AuthMgr**. The Status field at the bottom of the window shows the authentication status. If the authentication is successful, the Status field displays *Authenticated*, and the IP Address field displays the IP address of the client adapter.

## Using PEAP

### After Profile Selection, Card Insertion, or Reset

After you select a profile that uses host-based EAP authentication and configure the card for PEAP, follow these steps to EAP authenticate.

**Note**

These instructions are applicable for use with Windows NT or 2000 domain, LDAP, or OTP user databases after profile selection, card ejection and reinsertion, or reset.

- Step 1** If a message appears informing you that you need to select a certificate or other credentials to access the network, tap this message.
- Step 2** If a message appears indicating the root certification authority for the server's certificate and it is the correct certification authority, tap **OK** to accept the connection. Otherwise, tap **Cancel**.
- Step 3** If a message appears indicating the server to which your client adapter is connected and it is the correct server to connect to, tap **OK** to accept the connection. Otherwise, tap **Cancel**.
- Step 4** The Static Password window appears (see [Figure 6-4](#)).

**Note**

If a message appears prompting you to process your logon information for your wireless network, tap this message. Then the Static Password window appears.

Figure 6-4 Static Password Window

**Step 5** Enter your PEAP username and password (which are registered with the RADIUS server) in the appropriate fields.

**Step 6** If applicable, enter your domain name in the Domain field.



**Note** A domain name is not required for OTP databases.

**Step 7** Tap **OK**. The client adapter should now EAP authenticate.

To verify authentication on a PPC 2002 device, select **Start > Programs > Cisco > AuthMgr**. The Status field at the bottom of the window shows the authentication status. If the authentication is successful, the Status field displays *Authenticated*, and the IP Address field displays the IP address of the client adapter.

## After Your Password Expires (Windows NT or 2000 Domain Databases Only)

If you are using a Windows NT or 2000 domain database with PEAP and the password for your current username expires, follow these steps to change your password.

- Step 1** When the Change Password window appears (see [Figure 6-5](#)) to indicate that your password has expired, enter your old password in the Old Password field.

**Figure 6-5** Change Password Window



- Step 2** Enter your new password in both the New Password and Confirm New Password fields.



**Note** The password is also changed in the Windows NT or 2000 domain user database.

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





## Performing Diagnostics

---

This chapter explains how to use ACU to perform user-level diagnostics.

The following topics are covered in this chapter:

- [Overview of ACU Diagnostic Tools, page 7-2](#)
- [Setting Signal Strength Display Units, page 7-2](#)
- [Viewing the Status of Your Client Adapter, page 7-3](#)
- [Viewing Statistics for Your Client Adapter, page 7-7](#)

# Overview of ACU Diagnostic Tools

The ACU diagnostic tools enable you to assess the performance of your client adapter within the wireless network. These tools perform the following functions:

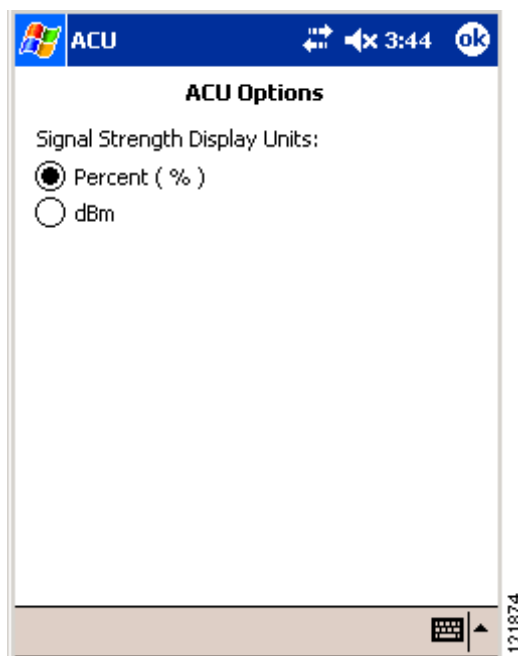
- Display your client adapter's current status
- Display statistics pertaining to your client adapter's transmission and reception of data

## Setting Signal Strength Display Units

Follow these steps to specify the units used to display signal strength on the ACU Status window.

- 
- Step 1** Double-tap the **ACU** icon or select **Start > Programs > Cisco > ACU**. The Profiles window appears.
- Step 2** Tap the **Options** button. The ACU Options window appears (see [Figure 7-1](#)).

*Figure 7-1 ACU Options Window*



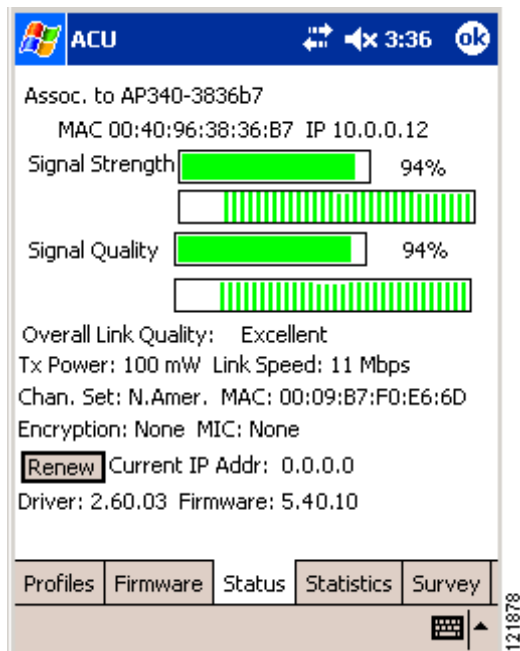
- Step 3** Select one of the following options for Signal Strength Display Units:
- **Percent (%)**—Displays the signal strength as a percentage. This is the default setting.
  - **dBm**—Displays the signal strength in decibels with respect to milliwatts.
- Step 4** Tap **OK** to save your changes.
-

## Viewing the Status of Your Client Adapter

Follow these steps to view the current status of your client adapter.

- Step 1** From the Profiles window, tap the **Status** tab. The Status window appears. [Figure 7-2](#) shows the Status window with the signal strength values displayed as percentages, and [Figure 7-3](#) shows the same window with the signal strength values displayed in decibels with respect to milliwatts (dBm).

**Figure 7-2** Status Window (with Signal Strength as a Percentage)



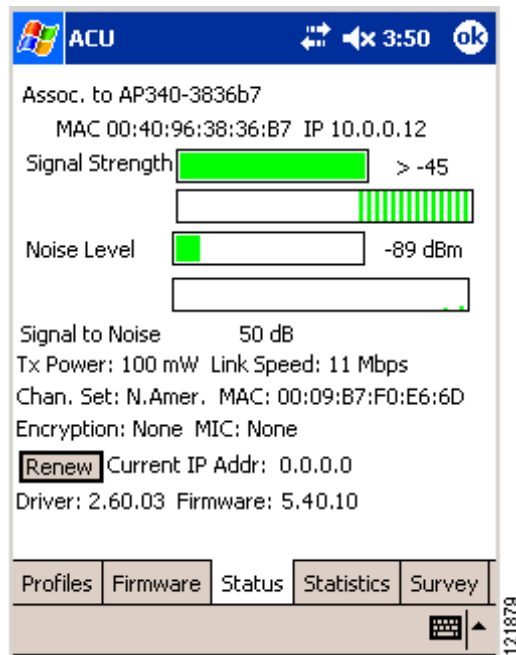
**Figure 7-3** Status Window (with Signal Strength in dBm)

Table 7-1 interprets each element of the Status window.

**Table 7-1** Client Adapter Status

Status	Description
The first line of the Status window	<p>Indicates the operational mode of your client adapter and the name of any associated access point.</p> <p><b>Value:</b> Not Associated, Associated, Authenticated, or Ad Hoc Mode</p> <p><b>Note</b> The access point name is shown only if the client adapter is in infrastructure mode and Aironet Extensions are enabled (on access points running Cisco IOS release 12.2(4)JA or later).</p>
Associated Access Point MAC Address	<p>The MAC address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode.</p> <p><b>Note</b> This field displays the MAC address of the access point's Ethernet port (for access points that do not run Cisco IOS) or the MAC address of the access point's radio (for access points that run Cisco IOS). The MAC address of the Ethernet port on access points that run Cisco IOS is printed on a label on the back of the device.</p>

Table 7-1 Client Adapter Status (continued)

Status	Description
Associated Access Point IP Address	<p>The IP address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode, the access point was configured with an IP address, and Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later).</p> <p><b>Note</b> If Aironet Extensions are disabled, the IP address of the associated access point is shown as 0.0.0.0.</p>
Signal Strength	<p>The signal strength for all received packets. The higher the value and the more green the bar graph is, the stronger the signal.</p> <p>The histogram below the bar graph provides a visual interpretation of the current signal strength. Differences in signal strength are indicated by the following colors: green (strongest), yellow (middle of the range), and red (weakest).</p> <p><b>Range:</b> 0 to 100% or –95 to –45 dBm</p>
Signal Quality	<p>The signal quality for all received packets. The higher the value and the more green the bar graph is, the clearer the signal.</p> <p>The histogram below the bar graph provides a visual interpretation of the current signal quality. Differences in signal quality are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality).</p> <p><b>Range:</b> 0 to 100%</p> <p><b>Note</b> This setting appears only if you selected signal strength to be displayed as a percentage. See the <a href="#">“Setting Signal Strength Display Units”</a> section on page 7-2 for information.</p>
Noise Level	<p>The level of background radio frequency energy in the 2.4-GHz band. The lower the value and the more green the bar graph is, the less background noise present.</p> <p><b>Range:</b> –100 to –45 dBm</p> <p><b>Note</b> This setting appears only if you selected signal strength to be displayed in dBm. See the <a href="#">“Setting Signal Strength Display Units”</a> section on page 7-2 for information.</p>
Overall Link Quality	<p>The client adapter’s ability to communicate with the access point, which is determined by the combined result of the adapter’s signal strength and signal quality.</p> <p><b>Value:</b> Not Associated, Poor, Fair, Good, Excellent</p> <p><b>Note</b> This setting appears only if you selected signal strength to be displayed as a percentage. See the <a href="#">“Setting Signal Strength Display Units”</a> section on page 7-2 for information.</p>

Table 7-1 Client Adapter Status (continued)

Status	Description	
Signal to Noise Ratio	<p>The difference between the signal strength and the current noise level. The higher the value, the better the client adapter’s ability to communicate with the access point.</p> <p><b>Range:</b> 0 to 90 dB</p> <p><b>Note</b> This setting appears only if you selected signal strength to be displayed in dBm. See the “<a href="#">Setting Signal Strength Display Units</a>” section on page 7-2 for information.</p>	
Transmit Power	<p>The power level at which your client adapter is currently transmitting. The maximum level is dependent upon your country’s regulatory agency.</p> <p><b>Value:</b> 1, 5, 20, 30, 50, or 100 mW</p> <p><b>Note</b> Refer to the Transmit Power parameter in <a href="#">Table 5-1</a> for information on setting the client adapter’s power level.</p>	
Link Speed	<p>The rate at which your client adapter is currently transmitting data packets.</p> <p><b>Value:</b> 1, 2, 5.5, or 11 Mbps</p>	
Channel Set	<p>The regulatory domain for which your client adapter is currently configured, such as North America. This value is not user selectable.</p> <p><b>Note</b> Refer to <a href="#">Appendix D</a> for a list of channel identifiers, channel center frequencies, and regulatory domains for each channel.</p>	
MAC Address	The MAC address assigned to your client adapter at the factory.	
Encryption	Indicates the type of encryption that is being used for data packets.	
	<b>Value:</b> None, WEP, Cisco TKIP, or WPA TKIP	
	<b>Note</b> Refer to the “ <a href="#">Overview of Security Features</a> ” section on page 5-11 for details on these encryption types.	
	Encryption	Description
	None	Data encryption is disabled.
	WEP	Static or dynamic WEP is enabled, but neither MMH MIC nor WPA is enabled.
Cisco TKIP	MMH MIC is enabled.	
WPA TKIP	WPA is enabled.	

**Table 7-1** *Client Adapter Status (continued)*

Status	Description								
Message Integrity Check (MIC)	<p>Indicates whether your client adapter is using message integrity check (MIC) to protect packets sent to and received from the access point.</p> <p>MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate.</p> <p><b>Note</b> MIC is supported automatically by the client adapter's driver, but it must be enabled on the access point.</p> <p><b>Value:</b> None, MMH, or Michael</p> <table> <tr> <th>Message Integrity Check</th><th>Description</th></tr> <tr> <td>None</td><td>MIC is disabled.</td></tr> <tr> <td>MMH</td><td>MIC is enabled and is being used with Cisco TKIP.</td></tr> <tr> <td>Michael</td><td>MIC is enabled and is being used with WPA TKIP.</td></tr> </table>	Message Integrity Check	Description	None	MIC is disabled.	MMH	MIC is enabled and is being used with Cisco TKIP.	Michael	MIC is enabled and is being used with WPA TKIP.
Message Integrity Check	Description								
None	MIC is disabled.								
MMH	MIC is enabled and is being used with Cisco TKIP.								
Michael	MIC is enabled and is being used with WPA TKIP.								
Current IP Address	<p>The IP address of the client adapter. If your Windows CE device is set up to obtain an IP address from a DHCP server, you can press the Renew button to initiate a release and renew of the IP address.</p> <p><b>Note</b> This parameter and the Renew button appear only on PPC 2002, PPC 2003, HPC 2000, and CE .NET devices.</p>								
Driver Version	The version of the client adapter driver that is installed on your Windows CE device.								
Firmware Version	The version of the firmware that is currently running on your client adapter.								

**Step 2** Tap **OK** to exit the Status window.

## Viewing Statistics for Your Client Adapter

ACU enables you to view statistics that indicate how data is being received and transmitted by your client adapter. It also shows message integrity check (MIC) statistics if your client adapter's driver supports MIC and MIC is enabled on the access point.



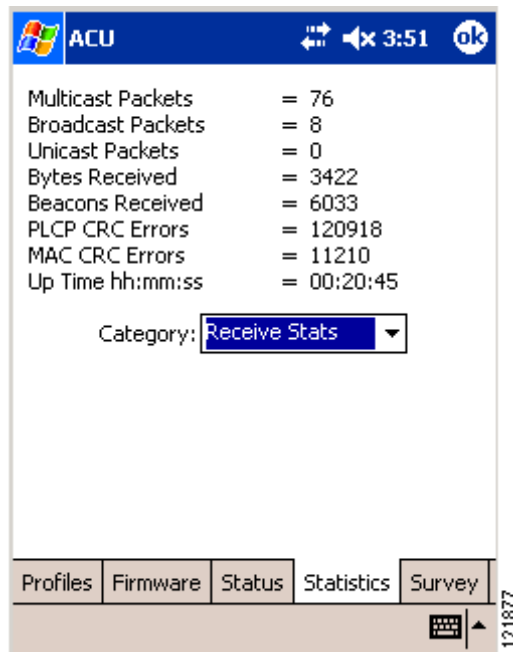
### Note

The receive and transmit statistics are host statistics. That is, they show packets and errors received or sent by the Windows CE device. Link status tests from the access point or ACU site survey tool are performed at the firmware level; therefore, they have no effect on the statistics shown by the Statistics window.

Follow these steps to view your client adapter's statistics.

- Step 1** From the Profiles window, tap the **Statistics** tab. The Receive Statistics window appears (see [Figure 7-4](#)).

**Figure 7-4** Receive Statistics Window



The statistics are calculated as soon as your client adapter is started.

[Table 7-2](#) describes each receive statistic that is displayed for your client adapter.

**Table 7-2** Receive Statistics

Statistic	Description
Multicast Packets	The number of multicast packets that were received successfully.
Broadcast Packets	The number of broadcast packets that were received successfully.
Unicast Packets	The number of unicast packets that were received successfully.
Bytes Received	The number of bytes of data that were received successfully.
Beacons Received	The number of beacon packets that were received successfully.



**Table 7-2** *Receive Statistics (continued)*

Statistic	Description
PLCP CRC Errors	<p>The number of times the client adapter started to receive an 802.11 Physical Layer Convergence Protocol (PLCP) header but the rest of the packet was ignored due to a cyclic redundancy check (CRC) error in the header.</p> <p><b>Note</b> CRC errors can be attributed to packet collisions caused by a dense population of client adapters, overlapping access point coverage on a channel, high multipath conditions from bounced signals, or the presence of other 2.4-GHz signals from devices such as microwave ovens, wireless handset phones, etc.</p>
MAC CRC Errors	<p>The number of packets that had a valid 802.11 PLCP header but contained a CRC error in the data portion of the packet.</p> <p><b>Note</b> CRC errors can be attributed to packet collisions caused by a dense population of client adapters, overlapping access point coverage on a channel, high multipath conditions from bounced signals, or the presence of other 2.4-GHz signals from devices such as microwave ovens, wireless handset phones, etc.</p>
Up Time (hh:mm:ss)	The amount of time (in hours:minutes:seconds) since your client adapter was started. If the client adapter has been running for more than 24 hours, the time is displayed in days, hours:minutes:seconds.

- Step 2** To view the transmit statistics for your client adapter, tap the arrow in the Category drop-down menu and select **Transmit Stats**. The Transmit Statistics window appears (see [Figure 7-5](#)).

Figure 7-5 Transmit Statistics Window

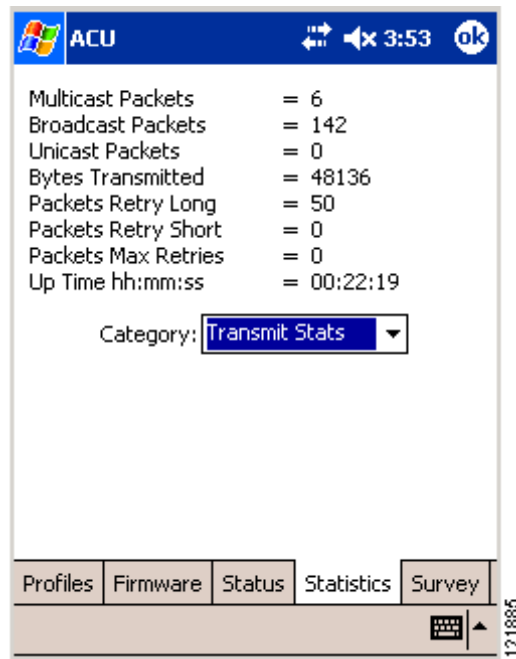


Table 7-3 describes each transmit statistic that is displayed for your client adapter.

Table 7-3 Transmit Statistics

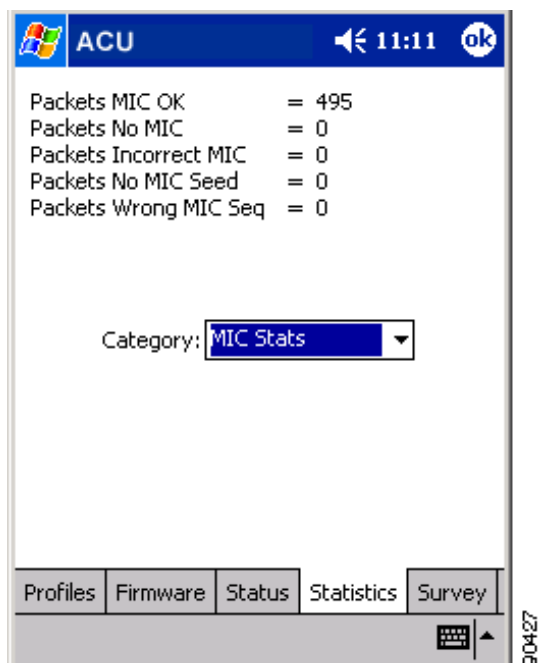
Statistic	Description
Multicast Packets	The number of multicast packets that were transmitted successfully.
Broadcast Packets	The number of broadcast packets that were transmitted successfully.
Unicast Packets	The number of unicast packets that were transmitted successfully.
Bytes Transmitted	The number of bytes of data that were transmitted successfully.
Packets Retry Long	The number of normal data packets that were retransmitted.
Packets Retry Short	The number of request-to-send (RTS) packets that were retransmitted.
Packets Max Retries	The number of packets that failed to be transmitted successfully after exhausting the maximum number of retries.
Up Time (hh:mm:ss)	The amount of time (in hours:minutes:seconds) since your client adapter was started. If the client adapter has been running for more than 24 hours, the time is displayed in days, hours:minutes:seconds.

- Step 3** To view the MIC statistics for your client adapter, tap the arrow in the Category drop-down menu and select **MIC Stats**. The MIC Statistics window appears (see [Figure 7-6](#)).



**Note** The MIC Stats option is available only if your client adapter's driver supports MIC and only if MIC is enabled on the access point.

**Figure 7-6** MIC Statistics Window



[Table 7-4](#) describes each MIC statistic that is displayed for your client adapter.

**Table 7-4** MIC Statistics

Statistic	Description
Packets MIC OK	The number of packets that were received successfully with a valid MIC.
Packets No MIC	The number of packets that were discarded due to no MIC being found.
Packets Incorrect MIC	The number of packets that were discarded due to an incorrect MIC value.
Packets No MIC Seed	The number of packets that were discarded due to no MIC seed being received.
Packets Wrong MIC Seq	The number of packets that were discarded due to the MIC sequence number being wrong.

- Step 4** Tap **OK** to exit the Statistics window.





## Routine Procedures

---

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

The following topics are covered in this chapter:

- [Inserting and Removing a PC Card, page 8-2](#)
- [Upgrading the Client Adapter Software, page 8-3](#)
- [Client Utility Procedures, page 8-8](#)
- [CA and User Certificate Procedures \(Host-Based EAP on PPC 2002 Devices Only\), page 8-10](#)
- [Restarting the Client Adapter, page 8-11](#)

# Inserting and Removing a PC Card

This section provides instructions for inserting a PC card into or removing a PC card from a Windows CE device.

## Inserting a PC Card into a Windows CE Device

Follow these steps to insert a PC card into a Windows CE device.



**Caution**

This procedure and the physical connections it describes apply generally to conventional PC card slots. In cases of custom or nonconventional equipment, be alert to possible differences in PC card slot configurations.

**Step 1**

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



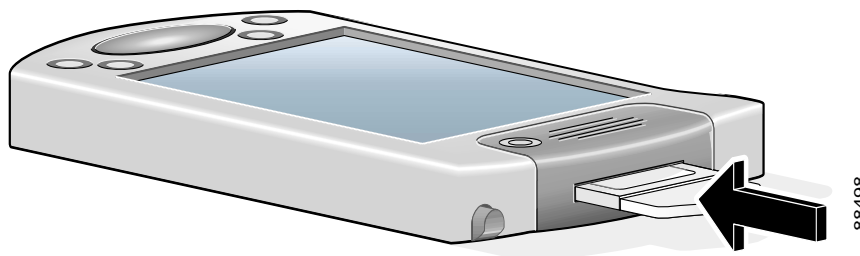
**Caution**

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

**Step 2**

Insert the PC card into the PC card slot, applying just enough pressure to make sure it is fully seated (see [Figure 8-1](#)).

**Figure 8-1** Inserting a PC Card into a Computing Device



## Removing a PC Card from a Windows CE Device

Follow the instructions below whenever you need to remove the PC card from your Windows CE device.

To remove a PC card after it is successfully installed and configured, press the Eject button and pull the card out of the PC card slot. When the PC card is reinserted, your connection to the network should be re-established.

# Upgrading the Client Adapter Software

This section provides instructions for the following procedures:

- Upgrading the firmware, see below
- Upgrading the driver and client utilities, [page 8-6](#)

## Upgrading the Firmware

The client adapter is shipped with the firmware installed in its Flash memory; however, a more recent version of the firmware may be available from Cisco.com. Cisco recommends using the most current version of radio firmware. Follow the instructions in this section to find the version of your client adapter's firmware and to upgrade it if a more recent version is available from Cisco.com.



**Note**

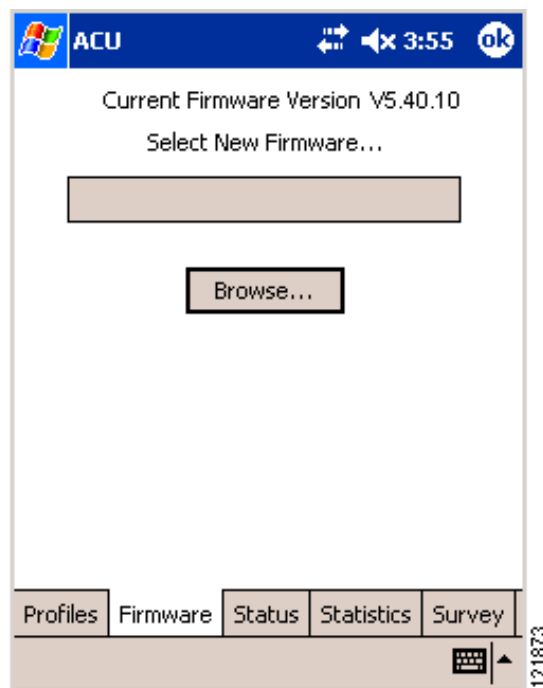
Firmware version 5.40.10 is recommended for use with client adapter driver and utility version 2.60.

## Finding the Firmware Version

Follow these steps to determine if you need to upgrade the client adapter's firmware.

- Step 1** To find the version of firmware that your client adapter is currently using, follow these steps:
- a. Double-tap the **ACU** icon or select **Start > Programs > Cisco > ACU**.
  - b. Tap the **Firmware** tab. The Firmware window appears (see [Figure 8-2](#)).

**Figure 8-2** Firmware Window



The current version of your client adapter's firmware is shown at the top of the window, provided a client adapter is inserted in your Windows CE device.

- Step 2** To find the latest firmware version available on Cisco.com, follow these steps:
- Use your computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - Select **Option #2: Aironet Wireless Software Display Tables**.
  - Select **Cisco Aironet Wireless LAN Client Adapters**.
  - Find the section for client adapter firmware.
  - Select the link for your client adapter's series (for example, 350 Series).
  - Look at the available filenames for radio firmware. The numbers that follow the "v" indicate the version number. For example, v50219 indicates a firmware version of 5.02.19.
- Step 3** If the firmware available from Cisco.com has a higher number than the firmware currently installed in your client adapter, follow the instructions in the "[Loading New Firmware](#)" section below to upgrade the firmware.
- 

## Loading New Firmware



### Caution

To minimize the risk of a power failure during the firmware flashing process, which could render your client adapter inoperable, Cisco recommends that your Windows CE device be plugged into AC power or have a fully charged battery at the start of flashing. If a power failure does occur, follow the instructions in the "[Technical Assistance Center](#)" section of the Preface to contact TAC for assistance.

Follow the instructions below to load new firmware into your client adapter.

---

- Step 1** Connect your Windows CE device to a laptop or PC running Microsoft ActiveSync. This is typically done using a serial or USB cable.
- A message appears on the Windows CE device indicating that it is connecting to the host. After the Windows CE device is connected, the New Partnership window appears on the laptop or PC. This window asks if you want to set up a partnership.
- Step 2** Perform one of the following:
- If you want to establish a partnership that allows you to synchronize files between the laptop or PC and the Windows CE device, select **Yes**, click **Next**, and follow the instructions on the window to specify the files to be synchronized and to finish setting up the partnership.
  - If you do not want to synchronize files and want to connect as a "guest," select **No** and click **Next**. The window indicates that you are connected as a guest.
- Step 3** Use the laptop or PC's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>



**Step 4** Select **Option #2: Aironet Wireless Software Display Tables**.



**Note** You can download software from the Software Selector tool instead of the display tables. To do so, select **Option #1: Aironet Wireless Software Selector**, follow the instructions on the window, and go to [Step 9](#).

**Step 5** Select **Cisco Aironet Wireless LAN Client Adapters**.

**Step 6** Find the section for client adapter firmware.

**Step 7** Select the link for your client adapter's series (for example, 350 Series).

**Step 8** Select the latest firmware file for your client adapter.

**Step 9** Complete the encryption authorization form; then read and accept the terms and conditions of the Software License Agreement.

**Step 10** Select the firmware file again to download it.

**Step 11** Save the file to a floppy disk or to the hard drive of your laptop or PC.

**Step 12** Locate the file using Windows Explorer, double-click it, and extract the image file (\*.img) to a folder.

**Step 13** In the ActiveSync window on the laptop or PC, click the **Explore** button to view the files on the Windows CE device.

**Step 14** Drag and drop the firmware image from Windows Explorer to a location in the ActiveSync window.



**Note** If your Windows CE device is a PPC running Windows CE 3.0, you must copy the firmware image to the My Documents folder or a folder under My Documents.

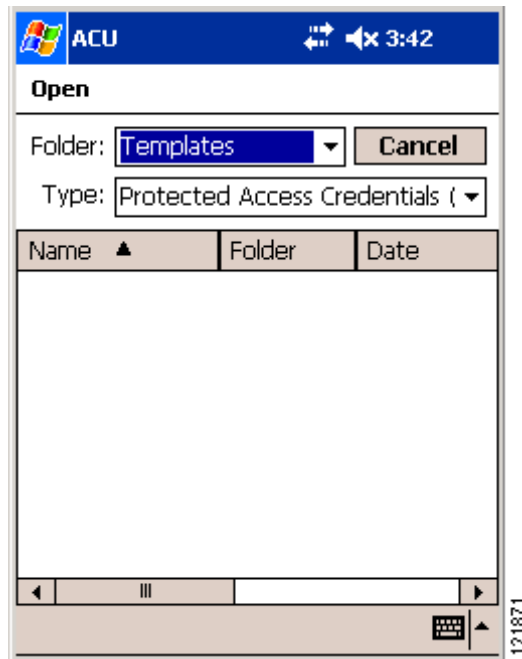
**Step 15** After the file is copied, disconnect the Windows CE device.

**Step 16** Make sure the client adapter is installed in your Windows CE device and is operational.

**Step 17** On your Windows CE device, open ACU and tap the **Firmware** tab. The Firmware window appears (see [Figure 8-2](#)).

**Step 18** Tap the **Browse** button. The Open window appears (see [Figure 8-3](#)).

Figure 8-3 Open Window



**Step 19** Perform one of the following:

- If you are using a PPC device, select the folder from the Folder drop-down menu where the new firmware image is located. Then tap the new firmware image file (\*.img) in the Name field in the center of the window.
- If you are using an HPC or Windows CE .NET device, locate the new firmware image file (\*.img) and select it so that it appears in the Name field at the bottom of the window.

**Step 20** Tap **OK**.



**Note** If the OK button is unavailable, tap the **Enter** key on the Windows CE device's keyboard.

A progress bar displays as the new firmware is loaded. If the selected image is loaded successfully into the client adapter's Flash memory, a "Firmware Upgrade Complete!" message appears.

**Step 21** Tap **OK** to exit the Firmware window.

## Upgrading the Driver and Client Utilities

Follow the instructions in this section to find the versions of your client adapter's driver and client utilities and to upgrade them if more recent versions are available from Cisco.com.



**Note** The driver, client utilities, and online help files are installed together.

## Finding the Driver and Client Utility Versions

Follow the instructions in this section to determine if you need to upgrade the client adapter's driver or client utilities.

- 
- Step 1** To find the version of the driver that your client adapter is currently using, follow these steps:
- Double-tap the **ACU** icon or select **Start > Programs > Cisco > ACU** to open ACU.
  - Tap the **Status** tab. The current version of your client adapter's driver is shown on the Status window, provided the adapter is installed in the Windows CE device and is operational.
- Step 2** To find the version of ACU or WLM that your client adapter is using, follow these steps:
- To find the version of ACU, tap the **About** button on the Profiles window. The About window displays the current version of ACU.
  - To find the version of WLM, double-tap the **Wireless Login Module** icon or select **Start > Programs > Cisco > Wireless Login Module**. The current version of the utility is shown below the Password field on the Wireless Login Module window.
- Step 3** To find the latest driver and client utility versions available on Cisco.com, follow these steps:
- Use your computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - Select **Option #2: Aironet Wireless Software Display Tables**.
  - Select **Cisco Aironet Wireless LAN Client Adapters**.
  - Find the section for Windows CE client adapter drivers and utilities.
  - Select the link for Windows CE 3.0 or Windows CE .NET, depending on your device's operating system.




---

**Note** If you are not sure which version of Windows CE your device is running, refer to the [“Finding the Windows CE Version”](#) section on page 3-2 for instructions.

---

- Look at the release numbers of the driver and client utilities in the description below the filename. These are the latest available versions on Cisco.com.
- Step 4** If the driver or client utility version available from Cisco.com is greater than the version currently being used by your client adapter, follow the instructions in the [“Uninstalling the Current Driver and Client Utilities”](#) section below to remove the current driver and client utilities and then follow the instructions in the [“Installing the Driver and Client Utilities”](#) section on page 3-2 to install the new driver and client utilities.
-

## Uninstalling the Current Driver and Client Utilities

Cisco recommends that you uninstall the existing driver and client utilities for your client adapter before upgrading to more recent versions. Follow these steps to uninstall your client adapter's current driver and client utilities.

- 
- Step 1 Eject the client adapter and remove it from the Windows CE device.
  - Step 2 Tap **Start > Settings > System** tab > **Remove Programs** (on a PPC device) or **Start > Settings > Control Panel > Remove Programs** (on an HPC or Windows CE .NET device).
  - Step 3 Tap **Cisco Wireless LAN Adapter**.
  - Step 4 Tap the **Remove** button.
  - Step 5 When asked to verify your decision to remove the adapter, tap **Yes**.
  - Step 6 Tap **OK**. The driver, client utilities, registry entries, and Cisco directory are removed.
  - Step 7 Go to the [“Installing the Driver and Client Utilities” section on page 3-2](#) for instructions on loading a new driver and client utilities.
- 

## Client Utility Procedures

This section provides instructions for the following procedures:

- Opening a client utility, [page 8-8](#)
- Exiting a client utility, [page 8-8](#)
- Finding the version of a client utility, [page 8-9](#)
- Deleting client utility icons on HPC and Windows CE .NET devices, [page 8-9](#)

### Opening a Client Utility

To open ACU on your Windows CE device, double-tap the **ACU** icon or select **Start > Programs > Cisco > ACU**. The Profiles window appears.

To open WLM on your Windows CE device, double-tap the **Wireless Login Module** icon or select **Start > Programs > Cisco > Wireless Login Module**. The Wireless Login Module window appears.

### Exiting a Client Utility

To exit ACU or WLM, tap **OK**.

## Finding the Version of a Client Utility

To find the version of ACU and WLM that your client adapter is using, tap the **About** button on the Profiles window. The About window appears (see [Figure 8-4](#)).

**Figure 8-4** About Window



The About window displays the current version of ACU. The WLM version is the same as the ACU version.

## Deleting Client Utility Icons on HPC and Windows CE .NET Devices

Icons for ACU and WLM are automatically added to the desktop of HPC and Windows CE .NET devices when you install the client utilities. If you wish to remove these icons from your desktop, hold down the **Alt** key and tap the icon. Then tap **Delete** and **Yes** to confirm your decision.



**Note**

You can also use File Explorer or Windows Explorer to browse to the desktop, select the icon, and delete it.

# CA and User Certificate Procedures (Host-Based EAP on PPC 2002 Devices Only)

Follow the instructions in this section to view or remove CA and user certificates for use with EAP-TLS or PEAP authentication on PPC 2002 devices.



Note

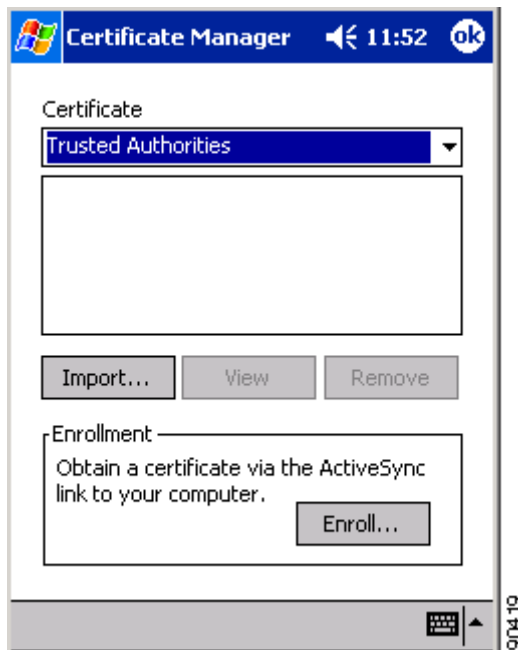
Refer to [Chapter 5](#) for instructions on obtaining and importing CA and user certificates.

## Viewing CA and User Certificates

Follow these steps to view details about the CA and user certificates for your PPC 2002 device.

- Step 1** Select **Start > Programs > Cisco > CertMgr**. The Certificate Manager window appears (see [Figure 8-5](#)).

*Figure 8-5 Certificate Manager Window*



- Step 2** Select **Trusted Authorities** (if you want to view a CA certificate) or **My Certificates** (if you want to view a user certificate) in the Certificate drop-down menu.
- Step 3** Select the certificate that you want to view.
- Step 4** Tap the **View** button. A window appears that enables you to access information about the certificate, including its issuer, expiration date, and serial number.

## Removing CA and User Certificates

- 
- |        |  |
|--------|--|
| Step 1 | Select <b>Start &gt; Programs &gt; Cisco &gt; CertMgr</b> . The Certificate Manager window appears (see <a href="#">Figure 8-5</a> ).  |
| Step 2 | Select <b>Trusted Authorities</b> (if you want to remove a CA certificate) or <b>My Certificates</b> (if you want to remove a user certificate) in the Certificate drop-down menu. |
| Step 3 | Select the certificate that you want to remove.  |
| Step 4 | Tap the <b>Remove</b> button. The certificate is removed.  |
- 

## Restarting the Client Adapter

ACU enables you to restart the client adapter when necessary. For example, you might want to restart the adapter for the following reasons:

- If your client adapter is experiencing poor throughput, you might want to restart the client adapter to try to force it to disassociate from the access point to which it is currently associated in the hope that it will reassociate to an access point with a stronger signal.
- If you use LEAP and then disable it in ACU, you might want to restart the client adapter to ensure that the adapter stops using the dynamic WEP key assigned during LEAP authentication.

Follow these steps to restart the client adapter.

- 
- |        |  |
|--------|--|
| Step 1 | Go to the ACU Profiles window.   |
| Step 2 | Perform one of the following: <ul style="list-style-type: none"><li>• Change the active profile and then select it again.</li><li>• Select the active profile in the Manage Profiles box, tap the <b>Edit</b> button, and tap <b>OK</b>.</li></ul> |

The driver stops the client adapter's radio, writes the configuration (although no parameter settings have been changed), and restarts the radio.

---







# Troubleshooting

---

This chapter provides information for diagnosing and correcting common problems that may be encountered when installing or operating the client adapter.

The following topics are covered in this chapter:

- [Accessing the Latest Troubleshooting Information, page 9-2](#)
- [Interpreting the Indicator LEDs, page 9-2](#)
- [Troubleshooting the Client Adapter, page 9-3](#)
- [Error Messages, page 9-5](#)
- [Getting Help, page 9-17](#)

# Accessing the Latest Troubleshooting Information

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

## Interpreting the Indicator LEDs

The client adapter shows messages and error conditions through its two LEDs:

- **Link Integrity/Power LED (green)**—This LED lights when the client adapter is receiving power and blinks slowly when the adapter is linked with the network.
- **Link Activity LED (amber)**—This LED blinks quickly when the client adapter is receiving or transmitting data and blinks in a repeating pattern to indicate an error condition.

[Table 9-1](#) interprets the LED messages during normal operation. [Table 9-2](#) interprets the LED error condition messages.

**Table 9-1 LED Normal Operating Messages**

Green LED	Amber LED	Condition
Blinking quickly	Blinking quickly	Power is on, self-test is OK, and client adapter is scanning for a network.
Blinking slowly	Blinking quickly	Client adapter is associated to an access point.
Continuously on or blinking slowly	Blinking quickly	Client adapter is transmitting or receiving data while associated to an access point.
Off	Blinking quickly	Client adapter is in power save mode.
On continuously	Blinking quickly	Client adapter is in ad hoc mode.

**Table 9-2 LED Error Condition Messages**

Green LED	Amber LED	Condition/Recommended Action
Off	Off	Client adapter is not receiving power, or an error has occurred.
Off	1 blink at 2-second rate	RAM failure. Refer to the <a href="#">“Obtaining Technical Assistance”</a> section in the Preface for technical support information.
Off	2-second pause, 2 fast blinks, 1-second pause, 1 blink	A configuration error has occurred (for example, static WEP is enabled in ACU, but the client adapter has not been programmed with a valid WEP key). Recheck your client adapter’s configuration settings.

*Table 9-2 LED Error Condition Messages (continued)*

Green LED	Amber LED	Condition/Recommended Action
Off	2 fast blinks, 2-second pause	Flash boot block checksum failure. Refer to the <a href="#">“Obtaining Technical Assistance”</a> section in the Preface for technical support information.
Off	3 fast blinks, 2-second pause	Firmware checksum failure. Reload the firmware.
Off	4 fast blinks, 2-second pause	MAC address error (error reading MAC chip). Reload the firmware.
Off	5 fast blinks, 2-second pause	Physical layer (PHY) access error. Refer to the <a href="#">“Obtaining Technical Assistance”</a> section in the Preface for technical support information.
Off	6 fast blinks, 2-second pause	Incompatible firmware. Load the correct firmware version.

## Troubleshooting the Client Adapter

This section provides troubleshooting tips should you encounter problems with your client adapter.

### Problems Obtaining an IP Address

If your network is set up to use DHCP to acquire an IP address, the DHCP lease renewal may fail, especially in suspend/resume situations. To force DHCP to try to reacquire an IP address, tap the **Renew** button on the ACU Status window, power your Windows CE device off and on, or eject and reinsert your client adapter.

### Problems Associating to an Access Point

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

- If possible, move your Windows CE device a few feet closer to an access point and try again.
- Make sure the client adapter is securely inserted in your device’s PC card slot.
- Make sure that the access point is turned on and operating.
- Ensure that all parameters are set properly for both the client adapter and the access point. These include the SSID, WEP activation, EAP activation, infrastructure mode, etc.
- If the client adapter still fails to establish contact, refer to the [“Obtaining Technical Assistance”](#) section in the Preface for technical support information.

## Problems Authenticating to an Access Point

If your client adapter is a 40-bit card and EAP authentication is enabled, the adapter can associate to but not authenticate to access points using 128-bit encryption. To authenticate to an access point using 128-bit encryption, you have two options:

- Purchase a 128-bit client adapter. This is the most secure option.
- Disable static WEP for the client adapter and configure the adapter and the access point to associate to mixed cells. This option presents a security risk because your data is not encrypted as it is sent over the RF network.

## Problems Connecting to the Network

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

## Reauthenticating After LEAP or EAP-FAST Times Out

If your client adapter times out while trying to authenticate using LEAP or EAP-FAST, open WLM, enter your LEAP or EAP-FAST credentials, and try again to authenticate.



**Note**

If you use the same password for your laptop or PC as for your Windows CE device, your session may expire on your Windows CE device if you change the password on your laptop or PC. In this event, simply open WLM, enter your new password, and try again to authenticate.

## Creating Strong Passwords

Cisco recommends the use of strong passwords for LEAP authentication. Because strong passwords are difficult to guess, they minimize the risk of successful attacks by rogue access points. Some characteristics of strong passwords include:

- A minimum of 10 characters
- A mixture of uppercase and lowercase letters
- At least one numeric character or one non-alphanumeric character, such as !#\$%&'
- No form of your username or user ID
- A word that is not found in the dictionary (domestic or foreign)

Some examples of strong passwords include:

- cnw84FriDAY, which comes from "Cannot wait for Friday"
- 4yosc10cP!, which comes from "For your own safety, choose a 10-character password!"



**Note**

Cisco recommends that you create your own strong passwords rather than use these sample passwords.

# Error Messages

This section provides a list of error messages that may appear during the installation, configuration, or use of your client adapter. The error messages are divided into six sections (general, installation, LEAP authentication, EAP-FAST authentication, EAP-TLS authentication, and PEAP authentication). The messages are listed in alphabetical order within each section, and an explanation as well as a recommended user action are provided for each message. [Table 9-3](#) enables you to quickly locate the error messages you need.

**Table 9-3** Locating Error Messages

Error Message Category	Page Number
General	<a href="#">9-5</a>
Installation	<a href="#">9-7</a>
LEAP authentication	<a href="#">9-8</a>
EAP-FAST authentication	<a href="#">9-10</a>
EAP-TLS authentication	<a href="#">9-14</a>
PEAP authentication	<a href="#">9-15</a>

## General Error Messages

This section lists general error messages that may appear at any time and are not related to installation or authentication attempts.

**Error Message** Can't delete active profile

**Explanation** An attempt was made to delete the active profile, which cannot be removed.

**Recommended Action** Tap **OK**. Then select a different active profile and delete the profile that you want to remove.

**Error Message** Cisco Wireless LAN Adapter Not Found!

**Explanation** ACU or WLM was activated without a client adapter being inserted in the Windows CE device, or the client adapter was ejected while ACU was running. WLM cannot execute if a client adapter is not running because it needs to be able to read from and write to the adapter.

**Recommended Action** Tap **OK** to acknowledge the message on WLM. Insert a client adapter into the Windows CE device.

**Error Message** Client adapter not found.

**Explanation** A client adapter is not inserted in the Windows CE device.

**Recommended Action** Insert a client adapter if you want to start wireless communications. If necessary, reset the Windows CE device.

**Error Message** File not valid for this radio! Firmware Upgrade Failed!

**Explanation** Your attempt to upgrade the client adapter firmware failed because an invalid file was selected. The firmware file should have a .img extension.

**Recommended Action** Tap the **Browse** button and select a new firmware image file.

**Error Message** An internal error has occurred.

**Explanation** An error has occurred.

**Recommended Action** Reset the Windows CE device and try the operation again.

**Error Message** This name already exists. Please use a different name.

**Explanation** An attempt was made to create or rename a profile using the name of an existing profile.

**Recommended Action** Tap **OK**. Then create or rename the profile using a unique name.

**Error Message** No profiles found. (Use ACU to create a profile.)

**Explanation** Profiles have not been created for your client adapter.

**Recommended Action** Create a profile in ACU for the client adapter to use. If necessary, reset the Windows CE device.

**Error Message** Please select one of the profiles.

**Explanation** The Edit, Rename, or Delete button on the ACU Profiles window was tapped before a profile was selected.

**Recommended Action** Tap **OK** to acknowledge the message. Then select a profile and tap the button for the action you want to take.

**Error Message** The selected profile does not support EAP. (Use ACU to modify the security settings.)

**Explanation** The Authentication Manager (AuthMgr) was activated although the current profile does not have host-based EAP enabled.

**Recommended Action** Tap **OK** twice. Then select a profile in ACU that uses host-based EAP and reactivate the Authentication Manager. If necessary, reset the Windows CE device.

**Error Message** WEP Key x must be 10 Hex digits!

**Explanation** An invalid number of characters or an incorrect character was entered for the WEP key indicated. 40-bit keys must have 10 characters.

**Recommended Action** Tap **OK** to acknowledge the message; then re-enter the characters for the invalid key.

**Error Message** WEP Key x must be 26 Hex digits!

**Explanation** An invalid number of characters or an incorrect character was entered for the WEP key indicated. 128-bit keys must have 26 characters.

**Recommended Action** Tap **OK** to acknowledge the message; then re-enter the characters for the invalid key.

**Error Message** You must enter a WEP Key!

**Explanation** A WEP key was not entered on the WEP Keys window.

**Recommended Action** Tap **OK** to acknowledge the message. Then enter a WEP key on the WEP Keys window and tap **OK** to save the WEP key settings or tap **Cancel** to exit the WEP Keys window without entering a WEP key.

## Installation Error Messages

This section lists error messages that may appear during installation of the client adapter's software components.

**Error Message** Cisco Aironet Wireless LAN Adapter does not support the connected device type. Application Manager will make the application available for installation when a supported device type is connected.

**Explanation** The client adapter software does not support the Windows CE device on which the adapter is being installed. Refer to the [“System Requirements” section on page 2-4](#) for the list of Windows CE devices that are supported by the client adapter.

**Recommended Action** Tap **OK** to acknowledge the message and terminate the installation process. To install the client adapter's driver and client utilities on a supported Windows CE device, follow the instructions in the [“Installing the Driver and Client Utilities” section on page 3-2](#).

**Error Message** Could NOT find all of the appropriate files for this installation. Make sure that all of the files are installed to the same directory.

**Explanation** Some of the client adapter installation files could not be found.

**Recommended Action** Download the **WinCE-PCMCIA-LMC-v250.exe** file again and extract its files to a folder, making sure that you keep all of the extracted files together in the one folder.

**Error Message** No CE services are currently running on this computer. Please run ActiveSync and make sure you are connected to a supported device. NOTE: This Install is for 3.0 CE devices and greater.

**Explanation** An attempt was made to install the client adapter installation file without an ActiveSync connection established between your laptop or PC and your Windows CE device.

**Recommended Action** Follow the instructions in the [“Installing the Driver and Client Utilities” section on page 3-2](#) to establish an ActiveSync connection.

**Error Message** Unable to load the Wireless Zero Configuration interface.

**Explanation** An error occurred during installation, or the system is not working properly.

**Recommended Action** Reset the Windows CE device; then reinstall the client adapter software.

**Error Message** Windows CE Services not found on this computer. Setup cannot continue and will now exit.

**Explanation** The driver installation utility cannot locate the ActiveSync directory on the laptop or PC. This directory and the files it contains are needed to copy the client adapter’s driver and client utility files from the laptop or PC to a Windows CE device.

**Recommended Action** Tap **OK** to acknowledge the message and terminate the installation utility. Then install Windows CE Services on the laptop or PC and start the driver installation procedure again.



**Note**

Windows CE Services can be obtained from the CD that shipped with your Windows CE device or from the device manufacturer.

## LEAP Authentication Error Messages

This section lists error messages that may occur during LEAP authentication.

**Error Message** Authentication attempt timed out. Rerun WLM and try again.

**Explanation** The client adapter was unable to authenticate within a specified amount of time.

**Recommended Action** Tap **OK**. Then open WLM, enter your LEAP credentials, and try to authenticate again.



**Error Message** First Authentication Attempt Timed Out. Radio Will Continue Trying.

**Explanation** The client adapter timed out while trying to authenticate, possibly because it is out of range of an access point. The client adapter continues trying to authenticate.

**Recommended Action** Tap **OK** to acknowledge the message and terminate WLM. Then perform one of the following: 1) move the Windows CE device closer to an access point so that WLM will continue trying to authenticate or 2) enter a different saved or temporary LEAP username and password.

**Error Message** Incorrect Login -- Please Re-Enter

**Explanation** The LEAP username or password was entered incorrectly in the Wireless Login Module window or was not valid for the RADIUS server on the network.

**Recommended Action** Re-enter the LEAP username and password and tap **OK**.

**Error Message** LEAP or EAP-FAST Not Enabled on the Cisco Wireless LAN Adapter! Start ACU and Enable LEAP or EAP-FAST First.

**Explanation** An attempt was made to start WLM before LEAP was enabled on the client adapter.

**Recommended Action** Tap **OK** to acknowledge the message and terminate the utility. Then enable LEAP in ACU. WLM restarts automatically, provided you are using a temporary LEAP username and password.

**Error Message** Must set a User Name

**Explanation** A password was entered in the Wireless Login Module window, but a username was not entered. The password is an optional entry, but if a password is entered, a username must also be entered.

**Recommended Action** Tap **OK** to acknowledge the message. Then enter your LEAP username in the User Name field on the Wireless Login Module window and tap **OK**.

**Error Message** Name and Domain length is greater than the maximum allowable size of xx.

**Explanation** The combination of characters entered for the LEAP username and domain name in the Wireless Login Module window exceeds the maximum number supported by LEAP, which is 64.

**Recommended Action** Enter a username and domain name with fewer characters.

## EAP-FAST Authentication Error Messages

This section lists error messages that may occur during EAP-FAST authentication.

**Error Message** Authentication Attempt Timed Out. Rerun WLM and try again.

**Explanation** The client adapter was unable to authenticate within a specified amount of time.

**Recommended Action** Tap **OK**. Then open WLM, enter your EAP-FAST credentials, and try to authenticate again.

**Error Message** Can't validate PAC! Either retry your credentials, change the PAC with the ACU or auto-provision a new PAC (if it is enabled to do so in the ACU).

**Explanation** Either your username or password was entered incorrectly or the profile is not properly configured for automatic or manual provisioning (for example, a PAC authority was not selected for manual provisioning).

**Recommended Action** Perform one of the following:

- Tap **Retry** to attempt to authenticate again using your current username and password.
- Tap **Auto-Provision** to automatically provision a new PAC if the profile is set for automatic provisioning. After a new PAC is provisioned, the client adapter tries again to authenticate. If a message appears indicating that your password has expired, follow the instructions in the [“After Your EAP-FAST Credentials Expire”](#) section on page 6-4 to change your password.
- Tap **Cancel** to acknowledge the message. Then select a different PAC authority or import a new PAC file in ACU and try again to authenticate.

**Error Message** Current PAC doesn't match the server you are trying to authenticate to. There is one available that does match the server, would you like to try to authenticate with it?

**Explanation** The current PAC does not match the server to which the client adapter is attempting to authenticate, but another PAC is available to try.

**Recommended Action** Tap **OK** to attempt to authenticate using the PAC that matches the server or tap **Cancel** to cancel the operation. If you tap Cancel, the client adapter is unable to authenticate using the existing profile.

**Error Message** Error Changing Password!!!!

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

**Recommended Action** Re-enter your password on the Password Expired window.

**Error Message** Error Changing Password! Could be system policy, check with your system administrator.

**Explanation** The Cisco Secure ACS server reported an error when you attempted to change your EAP-FAST password.

**Recommended Action** Re-enter your password on the Password Expired window. If the error occurs again, contact your system administrator to discuss your organization's policy on changing passwords.

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

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

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

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

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

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

**Error Message** Error!! This version of WLM requires version 5.40.xx or newer to support EAP-FAST!

**Explanation** You enabled the client adapter for EAP-FAST authentication; however, WLM detected a firmware version that does not support this authentication type.

**Recommended Action** Follow the instructions in [Chapter 8](#) to upgrade the client adapter's firmware to version 5.40.10.

**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?

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

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

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

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

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

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

**Explanation** The PAC file that you tried to import has an incorrect format or cannot be decrypted.

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

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

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

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

**Error Message** An internal error occurred.

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

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

**Error Message** Invalid PAC found for one or more authorities listed in the local PAC database.

**Explanation** An error occurred while the PAC authority drop-down list was being initialized. One or more PAC files could not be read successfully.

**Recommended Action** Obtain new PAC files from your system administrator and import them.

**Error Message** LEAP or EAP-FAST Not Enabled on the Cisco Wireless LAN Adapter! Start ACU and Enable LEAP or EAP-FAST First.

**Explanation** An attempt was made to start WLM before EAP-FAST was enabled on the client adapter.

**Recommended Action** Tap **OK** to acknowledge the message and terminate the utility. Then enable EAP-FAST in ACU. WLM restarts automatically, provided you are using a temporary EAP-FAST username and password.

**Error Message** Must set a User Name

**Explanation** A password was entered in the Wireless Login Module window, but a username was not entered. The password is an optional entry, but if a password is entered, a username must also be entered.

**Recommended Action** Tap **OK** to acknowledge the message. Then enter your EAP-FAST username in the User Name field on the Wireless Login Module window and tap **OK**.

**Error Message** Name and Domain length is greater than the maximum allowable size of xx.

**Explanation** The combination of characters entered for the EAP-FAST username and domain name in the Wireless Login Module window exceeds the maximum number supported by EAP-FAST, which is 64.

**Recommended Action** Enter a username and domain name with fewer characters.

**Error Message** The password is incorrect.

**Explanation** You entered an incorrect password for a password-protected PAC file.

**Recommended Action** Re-enter the password.

**Error Message** Provisioning Exit Value xx

**Explanation** An error occurred during automatic PAC provisioning. No PAC has been provisioned for this profile.

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

**Error Message** Timed out Provisioning!!!!

**Explanation** Automatic PAC provisioning is enabled, but a PAC was not successfully provisioned within 90 seconds.

**Recommended Action** Try again to authenticate using this profile or switch to manual PAC provisioning.

**Error Message** Unable to access a PAC for one or more authorities listed in the local PAC database.

**Explanation** An error occurred while the PAC authority drop-down list was being initialized. One or more PAC files could not be read successfully.

**Recommended Action** Obtain new PAC files from your system administrator and import them.

**Error Message** Warning: This version of WLM requires driver 2.50.xx or higher to work properly. Current driver version is xx.yy.zz.

**Explanation** Your client adapter's driver does not support this version of WLM.

**Recommended Action** Follow the instructions in [Chapter 8](#) to uninstall the client adapter's existing driver and client utilities; then follow the instructions in [Chapter 3](#) to upgrade to the latest client adapter software.

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

**Explanation** You tapped **OK** on the Properties window when automatic provisioning was disabled and no PAC authority was selected.

**Recommended Action** Either enable automatic provisioning or select a PAC authority from the drop-down list. If the list is empty, import a PAC file.

**Error Message** You must specify an SSID for Ad Hoc mode.

**Explanation** You tapped **OK** on the Properties window when Infrastructure Mode was set to No and the SSID was blank.

**Recommended Action** Enter an SSID or set the Infrastructure Mode to Yes.

## EAP-TLS Authentication Error Messages

This section lists error messages that may occur during EAP-TLS authentication.

**Error Message** Certificate enrollment failed.

**Explanation** Your attempt to import a user certificate failed.

**Recommended Action** Re-enter your username, password, and server name for your certificate server on the Certificate Enrollment window and tap the **Enroll** button. If the second attempt also fails, try to import a new certificate.

**Error Message** The certificate server was not found.

**Explanation** A certificate server could not be found during certificate enrollment.

**Recommended Action** Re-enter your username, password, and server name for your certificate server on the Certificate Enrollment window and tap the **Enroll** button. If the second attempt also fails, enter your credentials for a different certificate server on your network.

**Error Message** The object or property already exists.

**Explanation** An attempt was made to import a certificate file that was already installed.

**Recommended Action** Tap **OK** and select a different certificate to import.

**Error Message** Unable to configure connection settings.

**Explanation** An error occurred after you tapped the Connect button on the Authentication window.

**Recommended Action** Reset the Windows CE device and try the operation again.

**Error Message** You have connected to a server that is signed by Root Certification Authority xxx, which is different than the specified trusted CA. Do you want to accept this connection? Warning: Connecting to a server signed with untrusted CA might compromise your security.

**Explanation** The client adapter has established a connection to a certificate server other than the specified trusted CA.

**Recommended Action** If you want the client adapter to connect to this server although it may present a security risk, tap **Yes**. Otherwise, tap **No**.

**Error Message** You have connected to server xxx. Do you want to accept the connection? Warning: Connecting to an unsecured server might compromise your security.

**Explanation** The client adapter has established a connection to the server specified.

**Recommended Action** If you want the client adapter to connect to this server although it may present a security risk, tap **Yes**. Otherwise, tap **No**.

## PEAP Authentication Error Messages

This section lists error messages that may occur during PEAP authentication.

**Error Message** The combination of the domain name and user name is too long. It exceeds the maximum of 255 characters allowed. Please use shorter ones.

**Explanation** The combination of characters entered for the username and domain name in the Static Password window exceeds the maximum number supported by PEAP, which is 255.

**Recommended Action** Enter a set of credentials (username, password, and domain name) with fewer characters.

**Error Message** New Password and Confirm New Password entered do not match. Please try it again.

**Explanation** Different values were entered in the New Password and Confirm New Password fields on the Change Password window. They must be identical.

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

**Error Message** The object or property already exists.

**Explanation** An attempt was made to import a certificate file that was already installed.

**Recommended Action** Tap **OK** and select a different certificate to import.

**Error Message** The old password you supplied doesn't match what you entered previously. Please try it again.

**Explanation** The password entered in the Old Password field on the Change Password window does not match the password that was used previously.

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

**Error Message** PEAP failed initialization. Please make sure that PEAP is installed correctly and Trusted Root Certificate Authority certificate is installed correctly.

**Explanation** The PEAP authentication process failed during initialization, most likely because the specified root certificate is missing from the system.

**Recommended Action** Make sure that PEAP and the Trusted Root Certificate Authority certificate are installed correctly.

**Error Message** Unable to configure connection settings.

**Explanation** An error occurred after you tapped the Connect button on the Authentication window.

**Recommended Action** Reset the Windows CE device and try the operation again.

**Error Message** You have connected to a server that is signed by Root Certification Authority xxx, which is different than the specified trusted CA. Do you want to accept this connection? Warning: Connecting to a server signed with untrusted CA might compromise your security.

**Explanation** The client adapter has established a connection to a certificate server other than the specified trusted CA.

**Recommended Action** If you want the client adapter to connect to this server although it may present a security risk, tap **Yes**. Otherwise, tap **No**.

**Error Message** You have connected to server xxx. Do you want to accept the connection? Warning: Connecting to an unsecured server might compromise your security.

**Explanation** The client adapter has established a connection to the server specified.

**Recommended Action** If you want the client adapter to connect to this server although it may present a security risk, tap **Yes**. Otherwise, tap **No**.

**Error Message** You must enter a server name.

**Explanation** The server name for your certificate server was not entered on the Certificate Enrollment window.

**Recommended Action** Enter the server name for your certificate server. Then tap the **Enroll** button.



**Error Message** You must enter a user name.

**Explanation** Your username for your certificate server was not entered on the Certificate Enrollment window.

**Recommended Action** Enter your username for your certificate server. Then tap the **Enroll** button.

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

**Explanation** The password that you have been using to PEAP authenticate has expired.

**Recommended Action** Follow the instructions in the [“After Your Password Expires \(Windows NT or 2000 Domain Databases Only\)”](#) section on page 6-8 to change your password.

## Getting Help

To access online help for ACU, follow the instructions below for your specific Windows CE device.

### PPC Devices

To access help related to ACU on a PPC device, open ACU and select **Start > Help**. Select the topic for which you want information.

### HPC and Windows CE .NET Devices

To access help related to ACU on an HPC or Windows CE .NET device, open ACU and tap the ? button on the top of the window. Select the topic for which you want information.





## Technical Specifications

---

This appendix provides technical specifications for the Cisco Aironet 350 Series Wireless LAN Client Adapters.

The following topics are covered in this appendix:

- Physical Specifications, [page A-2](#)
- Radio Specifications, [page A-3](#)
- Power Specifications, [page A-4](#)
- Safety and Regulatory Compliance Specifications, [page A-4](#)

[Table A-1](#) lists the technical specifications for the Cisco Aironet 350 Series Wireless LAN Client Adapters.



**Note**

If a distinction is not made between client adapter type, the specification applies to both 350 series PC and LM cards.

**Table A-1** *Technical Specifications for the 350 Series Client Adapters*

**Physical Specifications**

Size	
PC 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)
LM card	3.4 in. L x 2.1 in. W x 0.2 in. H (8.6 cm L x 5.4 cm W x 0.5 cm H)
Weight	1.3 oz (0.037 kg)
Enclosure	
PC card	Extended Type II PC card
LM card	Standard Type II PC card with RF connectors
Connector	68-pin PCMCIA
Status indicators	Green and amber LEDs; see <a href="#">Chapter 9</a>
Operating temperature	–22°F to 158°F (–30°C to 70°C)
Storage temperature	–40°F to 185°F (–40°C to 85°C)
Humidity (non-operational)	95% relative humidity
Altitude	<b>Operational</b> 9843 ft (3000 m) @ room temperature for 2 hours  <b>Non-operational</b> 15,000 ft (4572 m) @ room temperature for 20 hours
ESD	15 kV (human body model)

**Table A-1** Technical Specifications for the 350 Series Client Adapters (continued)

Radio Specifications	
Type	Direct-sequence spread spectrum (DSSS) IEEE 802.11b compliant
Power output	100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 5 mW (7 dBm) 1 mW (0 dBm)  <b>Note</b> Refer to <a href="#">Appendix D</a> for limitations on radiated power (EIRP) levels in the European community and other countries.  <b>Note</b> If you are using an older version of a 350 series client adapter, your power level options may be different than those listed here.
Operating frequency	2.400 to 2.497 GHz (depending on the regulatory domain in which the client adapter is used)
Usable channels	2412 to 2484 MHz in 5-MHz increments
Interference rejection	–35 dB adjacent channel rejection
Data rates	1, 2, 5.5, and 11 Mbps
Modulation	Binary phase shift keying (BPSK) - 1 Mbps Quaternary phase shift keying (QPSK) - 2 Mbps Complementary code keying (CCK) - 5.5 and 11 Mbps
Receiver sensitivity	–94 dBm @ 1 Mbps –91 dBm @ 2 Mbps –89 dBm @ 5.5 Mbps –85 dBm @ 11 Mbps
Receiver delay spread (multipath)	500 ns @ 1 Mbps 400 ns @ 2 Mbps 300 ns @ 5.5 Mbps 140 ns @ 11 Mbps

**Table A-1** Technical Specifications for the 350 Series Client Adapters (continued)

Range	<b>Outdoor</b> 2000 ft (609.6 m) @ 1 Mbps 1500 ft (457.2 m) @ 2 Mbps 1000 ft (304.8 m) @ 5.5 Mbps 800 ft (243.8 m) @ 11 Mbps  <b>Indoor</b> 350 ft (106.7 m) @ 1 Mbps 250 ft (76.2 m) @ 2 Mbps 200 ft (61 m) @ 5.5 Mbps 150 ft (45.7 m) @ 11 Mbps  <b>Note</b> The above range numbers assume the use of a snap-on antenna with the LM card.
Antenna	
PC card	Integrated diversity antenna
LM card	Two MMCX antenna connectors
<b>Power Specifications</b>	
Operational voltage	5.0 V ( $\pm$ 0.25 V)
Receive current steady state	Typically 250 mA
Transmit current steady state	Typically 450 mA @ 20 dBm
Sleep mode steady state	Typically 15 mA
<b>Safety and Regulatory Compliance Specifications</b>	
Safety	Designed to meet: <ul style="list-style-type: none"> <li>• UL 1950 Third Ed.</li> <li>• CSA 22.2 No. 950-95</li> <li>• IEC 60950 Second Ed., including Amendments 1-4 with all 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) EN 55022 B AS/NZS 3548 Class B VCCI Class B EN 55024
Radio approvals	FCC Part 15.247 Canada RSS-139-1, RSS-210 Japan Telec 33B EN 300.328
RF exposure	OET-65C RSS-102 ANSI C95.1



## Translated Safety Warnings

---

This appendix provides translations of the safety warnings that appear in this publication.

The following topics are covered in this appendix:

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

# Explosive Device Proximity Warning



## Warning

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

## Waarschuwing

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

## Varoitus

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

## Attention

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

## Warnung

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

## Avvertenza

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

## Advarsel

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

## Aviso

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

## ¡Advertencia!

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

## Varning!

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



# Antenna Installation Warning



## Warning

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

## Waarschuwing

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

## Varoitus

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

## Attention

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

## Warnung

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

## Avvertenza

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

## Advarsel

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

## Aviso

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

## ¡Advertencia!

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

## Varning!

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

# Warning for Laptop Users



## Warning

In order to comply with RF exposure limits established in the ANSI C95.1 standards, it is recommended when using a laptop with a PC card client adapter that the adapter's integrated antenna is positioned more than 2 inches (5 cm) from your body or nearby persons during extended periods of transmitting or operating time. If the antenna is positioned less than 2 inches (5 cm) from the user, it is recommended that the user limit exposure time.

## Waarschuwing

In het kader van een in de ANSI C95.1 norm vastgelegde limiet voor blootstelling aan straling veroorzaakt door radiofrequenties, dient u bij langdurig gebruik van een laptop met client adapter pc-kaart een afstand van meer dan 5 centimeter aan te houden tussen de geïntegreerde antenne van de adapter en uzelf en enige andere personen. Als deze afstand niet kan worden aangehouden, dient u de tijd dat het apparaat gebruikt wordt te beperken.

## Varoitus

ANSI C95.1 -standardin radiotaajuuksille asettamien altistumisrajojen mukaisesti on suositeltavaa, että käytettäessä kannettavaa tietokonetta, jossa on PC-kortti-asiakas-adapteri, adapterin integroitu antenni on käännetty yli viisi cm pois vartalosta tai lähellä olevista henkilöistä pitkäaikaisten lähetys- tai käyttöjaksojen aikana. Jos antenni on käännetty alle viisi 5 cm käyttäjästä, on suositeltavaa, että käyttäjä rajoittaa altistumisaikaa.

## Attention

Afin de respecter les limitations en matière d'exposition aux fréquences radioélectriques définies par les normes ANSI C95.1, il est recommandé aux utilisateurs d'ordinateurs portables dotés d'adaptateurs client pour carte PC ou aux personnes se trouvant à proximité de se placer à plus de 5 cm de l'antenne de l'adaptateur lors de longues périodes de transmission ou de fonctionnement. Si l'utilisateur se trouve à moins de 5 cm de l'antenne, il est préférable de limiter le temps d'exposition.

## Warnung

In Übereinstimmung mit den in den Sicherheitsstandards ANSI C95.1 verzeichneten Höchstwerten für den Kontakt mit Radiofrequenz (RF) wird für die Benutzung eines Laptops mit PC-Adapterkarten für Clients empfohlen, bei längerer Inbetriebnahme oder Datenübertragung die integrierte Antenne des Adapters mindestens 5 cm vom Benutzer und anderen sich in der Nähe aufhaltenden Personen entfernt aufzustellen. Befindet sich die Antenne weniger als 5 cm vom Benutzer entfernt, sollte die Benutzungsdauer des Geräts eingeschränkt werden.

## Avvertenza

In conformità con i limiti sull'esposizione a frequenze radio stabiliti nelle direttive ANSI C95.1, quando si utilizza un computer portatile con una scheda PC dotata di adattatore client è consigliabile mantenere l'antenna integrata dell'adattatore a più di 5 cm di distanza durante periodi di esposizione prolungati. Se l'antenna è posizionata a meno di 5 cm di distanza dall'utente, è consigliabile limitare i tempi di esposizione alle frequenze.

## Advarsel

Du må overholde begrensningene for RF-eksponering som er fastsatt i ANSI C95.1-standardene. Derfor anbefaler vi, når du bruker en bærbar PC med et klientkort i PC-format, at kortets innebygde antenne plasseres mer enn 5 cm fra deg eller personer i nærheten under lengre perioder med overføring eller bruk. Hvis antennen er plassert mindre enn 5 cm fra brukeren, anbefaler vi at brukeren begrenser eksponeringstiden.

Aviso	Para estar em conformidade com os limites de exposição RF estabelecidos nas normas ANSI C95.1 recomenda-se que, aquando da utilização de um laptop com um adaptador de cliente PC card, a antena integrada do adaptador esteja posicionada a mais de 5 cm do seu corpo ou de pessoas na vizinhança durante longos períodos de tempo de transmissão ou operação. Se a antena estiver posicionada a menos de 5 cm do utilizador, recomenda-se que o utilizador limite o tempo de exposição.
¡Advertencia!	Para cumplir los límites de exposición a radiofrecuencia (RF) que se establecen en la norma ANSI C95.1, al utilizar un equipo portátil con un adaptador cliente de tarjeta PC, sitúe la antena del adaptador al menos a 2 pulgadas(5 cm) del usuario o de las personas adyacentes durante periodos largos de transmisión o funcionamiento. Si la distancia es inferior a 2 pulgadas (5 cm), se recomienda limitar el tiempo de exposición.
Varning!	För att följa de regler för radiosändare som utfärdats enligt ANSI-standarden C95.1, rekommenderar vi att PC Card-adapters inbyggda antenn befinner sig minst 5 cm från dig själv och andra personer när du använder en bärbar dator med PC Card-adapter under en längre tid. Om antennen befinner sig mindre än 5 cm från användaren, rekommenderar vi inte användning under längre tid.

---





## Declarations of Conformity and Regulatory Information

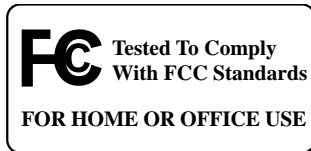
---

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 350 Series Wireless LAN Client Adapters.

The following topics are covered in this appendix:

- [Manufacturer's Federal Communication Commission Declaration of Conformity Statement, page C-2](#)
- [Department of Communications – Canada, page C-3](#)
- [European Community, Switzerland, Norway, Iceland, and Liechtenstein, page C-4](#)
- [Declaration of Conformity for RF Exposure, page C-6](#)
- [Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan, page C-7](#)
- [Administrative Rules for Cisco Aironet Wireless LAN Client Adapters in Taiwan, page C-8](#)

# Manufacturer's Federal Communication Commission Declaration of Conformity Statement



**Models:** AIR-PCM341, AIR-PCM342, AIR-LMC341, AIR-LMC342, AIR-PCM351, AIR-PCM352, AIR-LMC351, AIR-LMC352, AIR-PCM350-A-K9, AIR-PCM350-40-A-K9, AIR-LMC350-A-K9, AIR-LMC350-40-A-K9

**FCC Certification Number:** LDK102038 (AIR-PCM34x),  
LDK102035 (AIR-LMC34x),  
LDK102040 (AIR-xxx35x)

**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.

This equipment has been tested and found to comply with the limits of a Class B 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 residential environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician.



## Caution

The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using integrated antennas or those listed in [Table C-1](#). Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

**Table C-1 2.4-GHz Antennas**

Cisco Part Number	Model	Gain
AIR-ANT3338	Parabolic dish	21
AIR-ANT1949	Yagi	13.5
AIR-ANT4121	Omni-directional	12.0
AIR-ANT3549	Patch	8.5
AIR-ANT2012	Spatial diversity	6.5
AIR-ANT1729	Patch	6.0
AIR-ANT2506	Omni-directional	5.1
AIR-ANT3213	Omni-directional	5.0
AIR-ANT1728	Omni-directional	5.0
AIR-ANT3195	Patch	3.0
AIR-ANT5959	Omni-directional	2.0
AIR-ANT4941	Dipole	2.2

**Note**

AIR-ANT3338 is approved for use with only the LM card.

## 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.

The device is certified to the requirements of RSS-139-1 and RSS-210 for 2.4-GHz spread spectrum devices. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

# European Community, Switzerland, Norway, Iceland, and Liechtenstein

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

English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Deutsch:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Dansk:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Español:	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/EC.
Ελληνας:	Αυτός ο εξοπλισμός συμμορφώνεται με τις ουσιώδεις απαιτήσεις και τις λοιπές διατάξεις της Οδηγίας 1999/5/EK.
Français:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska:	Þessi búnaður samrýmist lögboðnum kröfum og öðrum ákvæðum tilskipunar 1999/5/ESB.
Italiano:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/EC.
Nederlands:	Deze apparatuur voldoet aan de belangrijkste eisen en andere voorzieningen van richtlijn 1999/5/EC.
Norsk:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 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 statement for the European Union countries is provided on the next page. Any other Declaration of Conformity statements related to this product can be found at the following URL:

<http://www.ciscofax.com>





**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-LMC350 / 2.4 GHz 11 Mbps Wireless LAN Module***  
***Variants : AIR-LMC351, AIR-LMC352, AIR-PCM350, AIR-PCM351, AIR-PCM352***

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

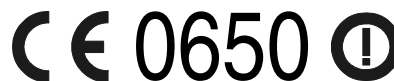
The following standards were applied:

<b>EMC</b>	<b>EN 301.489-1: 2000-08; EN 301.489-17: 2000-09</b>
<b>Health &amp; Safety</b>	<b>EN60950: 1992+A1+A2+A3+A4</b>
<b>Radio</b>	<b>EN 300.328-1 and -2: 2000-7</b>

The conformity assessment procedure referred to in Article 10 and Annex IV of Directive 1999/5/EC has been followed in association with the notified body listed below:

**BelcomLab, Perronstraat 6, B 8400 Oostende – Belgium.**

The product carries the CE Mark:



Date & Place of Issue: 30 July 2001 - Paris

Signature:

A handwritten signature in black ink, appearing to read 'Frank Dewachter'.

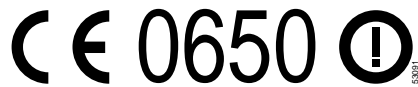
**Frank Dewachter**  
**Manager Corporate Compliance EMEA**  
11, rue Camille Desmoulins  
92782, Issy Les Moulineaux Cedex 9 France

*DofC 98741 rev1*

For the 350 series, the following standards were applied:

- Radio: EN 300.328-1, EN 300.328-2
- EMC: EN 301 489-1, EN 301 489-17
- Safety: EN 60950

The following CE mark is affixed to the 350 series equipment:



The above CE mark is required as of April 8, 2000 but might change in the future.



**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.



**Note**

Combinations of power levels and antennas resulting in a radiated power level above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and other countries that have adopted the European R&TTE directive 1999/5/EC or the CEPT recommendation Rec 70.03 or both. For more details on legal combinations of power levels and antennas, refer to the [“Maximum Power Levels and Antenna Gains” section on page D-3](#).

## Declaration of Conformity for RF Exposure

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

# Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan

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

## Japanese Translation

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

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

連絡先： 03-5549-6500

43768

## English Translation

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

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

Contact Number: 03-5549-6500

# Administrative Rules for Cisco Aironet Wireless LAN Client Adapters in Taiwan

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

## Chinese Translation

### 低功率電波輻射性電機管理辦法

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

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

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

95815

## English Translation

Administrative Rules for Low-power Radio-Frequency Devices:

### Article 14

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

### Article 17

The operation of the low-power radio-frequency devices is subject to the condition 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.



## Channels, Power Levels, and Antenna Gains

---

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

The following topics are covered in this appendix:

- [Channels, page D-2](#)
- [Maximum Power Levels and Antenna Gains, page D-3](#)

# Channels

The channel identifiers, channel center frequencies, and regulatory domains of each IEEE 802.11b 22-MHz-wide channel are shown in [Table D-1](#).

**Table D-1 Channels**

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		Americas (-A)	EMEA (-E)	Israel (-I)	Japan (-J)
1	2412	X	X	—	X
2	2417	X	X	—	X
3	2422	X	X	—	X
4	2427	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
10	2457	X	X	—	X
11	2462	X	X	—	X
12	2467	—	X	—	X
13	2472	—	X	—	X
14	2484	—	—	—	X



## Note

Mexico is included in the Americas 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.

# Maximum Power Levels and Antenna Gains

An improper combination of power level and antenna gain can result in equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain. [Table D-2](#) indicates the maximum power levels and antenna gains allowed for each IEEE 802.11b regulatory domain.

**Table D-2 Maximum Power Levels Per Antenna Gain**

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
Americas (-A) (4 W EIRP maximum)	0	100
	2.2	100
	5.2	100
	6	100
	8.5	100
	12	100
	13.5	100
	21	20
EMEA (-E) (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1
Israel (-I) (100 mW EIRP maximum)	0	100
	2.2	50
	5.2	30
	6	30
	8.5	5
	12	5
	13.5	5
	21	1

**Table D-2** *Maximum Power Levels Per Antenna Gain (continued)*

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
Japan (-J) (10 mW/MHz EIRP maximum)	0	50
	2.2	30
	5.2	30
	6	30
	8.5	n/a
	12	n/a
	13.5	5
	21	n/a





## Configuring the Client Adapter through Windows CE .NET

---

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

The following topics are covered in this appendix:

- [Overview, page E-2](#)
- [Preparing for Configuration \(EAP-TLS and PEAP Only\), page E-4](#)
- [Configuring the Client Adapter, page E-8](#)
- [Associating to an Access Point Using Windows CE .NET, page E-15](#)

# Overview

This appendix provides instructions for configuring the client adapter through Windows CE .NET (instead of through ACU). The [“Overview of Security Features”](#) section below describes the security options that are available for use with this operating system so that you can make an informed decision before you begin the configuration process. In addition, the appendix also provides basic information on using Windows CE .NET to specify the networks to which the client adapter associates.

**Note**

The instructions in this appendix are specific to PPC 2003 devices. The same configuration parameters must be set on other Windows CE .NET devices; however, the procedure used to set those parameters may differ. If you require more information on configuring or using your client adapter with Windows CE .NET, refer to the documentation that came with your device and Microsoft’s documentation for Windows CE .NET.

## Overview of Security Features

When you use your client adapter with Windows CE .NET, you can protect your data as it is transmitted through your wireless network by encrypting it through the use of wired equivalent privacy (WEP) encryption keys. With WEP encryption, the transmitting device encrypts each packet with a WEP key, and the receiving device uses that same key to decrypt each packet.

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

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

## Static WEP Keys

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

Static WEP keys are write-only and temporary; however, you do not need to re-enter them each time the client adapter is inserted or the Windows CE .NET device is reset. This is because the keys are stored (in an encrypted format for security reasons) in the registry of the device. When the driver loads and reads the client adapter’s registry parameters, it also finds the static WEP keys, unencrypts them, and stores them in volatile memory on the adapter.

## Dynamic WEP Keys with EAP

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

Two 802.1X authentication types are available for PPC 2003 and other Windows CE .NET 4.2 devices when you configure your client adapter through Windows CE .NET:

- **EAP-TLS**—This authentication type is enabled or disabled through the operating system and uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. EAP-TLS requires the use of certificates for authentication.

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

- **Cisco PEAP**—Cisco PEAP authentication (also known as *PEAP-GTC*) is designed to support One-Time Password (OTP), Windows NT or 2000 domain, and LDAP user databases over a wireless LAN. It is based on EAP-TLS authentication but uses a password instead of a client certificate for authentication. Cisco PEAP is enabled or disabled through the operating system and uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. Cisco PEAP requires you to enter your username and password in order to start the authentication process and gain access to the network. RADIUS servers that support Cisco PEAP authentication include Cisco Secure ACS version 3.1 or later.



**Note** To use Cisco PEAP authentication, you must have checked the **Install Cisco PEAP Support** check box during installation.

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

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



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

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



**Note**

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

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur\\_c/scprt2/scrad.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt2/scrad.htm)

## Wi-Fi Protected Access (WPA)

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

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

WPA and WPA-PSK are supported in the Windows CE .NET 4.2 operating system. However, for these features to be available on your Windows CE .NET 4.2 device when you configure your client adapter through Windows CE .NET, the device manufacturer must have included the WPA supplicant in its operating system build.

Only 350 series cards that are running EAP authentication can be used with WPA. Refer to the [“Configuring the Client Adapter” section on page E-8](#) for instructions on enabling WPA or WPA-PSK.



### Note

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

## Preparing for Configuration (EAP-TLS and PEAP Only)

If you are planning to use EAP-TLS or PEAP authentication with your Windows CE .NET device, you must make sure that your system meets certain requirements and obtain any necessary certificates before you can configure your client adapter. If you are not planning to use EAP-TLS or PEAP authentication, go to the [“Configuring the Client Adapter” section on page E-8](#).

## System Requirements

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

- The Windows CE device must be a PPC 2003 or other Windows CE .NET 4.2 device.
- Client adapters must support WEP and use firmware version 5.40.10.
- Access points to which your client adapter will attempt to authenticate must use the following firmware versions or later: 11.23T (340 and 350 series access points), 12.2(4)JA (1100 series access points), or 11.54T (1200 series access points).
- All necessary infrastructure devices (for example, access points, servers, gateways, user databases, etc.) must be properly configured for the authentication type you plan to enable on the client.

## Obtaining and Importing CA and User Certificates

EAP-TLS and PEAP authentication require the use of certificates. EAP-TLS requires both a Certificate Authority (CA) certificate and a user certificate while PEAP requires only a CA certificate. After you import the necessary certificates, you should not have to repeat this procedure until the certificates expire (at a time that is predetermined by the certificate server).



Note

[Chapter 8](#) provides instructions for viewing and removing certificates, if necessary.

### Obtaining CA and User Certificates

If you have not yet obtained a CA certificate (for EAP-TLS or PEAP) and a user certificate (for EAP-TLS), follow these steps.

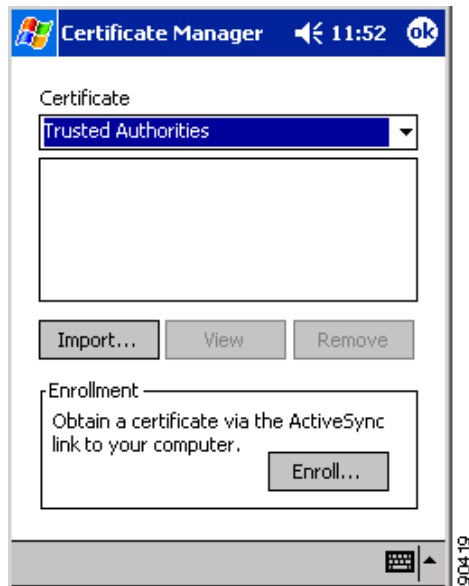
- 
- Step 1 Obtain the certificate file(s) (\*.cer or \*.crt) from your system administrator.
  - Step 2 Establish an ActiveSync connection between your laptop or PC and your Windows CE device.
  - Step 3 Open **Windows Explorer** on your laptop or PC.
  - Step 4 Copy the certificate file(s) and paste them into a folder under **My Computer** > **Mobile Device**.
  - Step 5 Follow the steps in the [“Importing a CA Certificate” section on page E-5](#) and the [“Importing a User Certificate” section on page E-7](#) to import the certificate file(s) for your Windows CE device.
- 

### Importing a CA Certificate

If you are planning to use EAP-TLS or PEAP authentication on your Windows CE .NET 4.2 device, follow these steps to import the CA certificate.

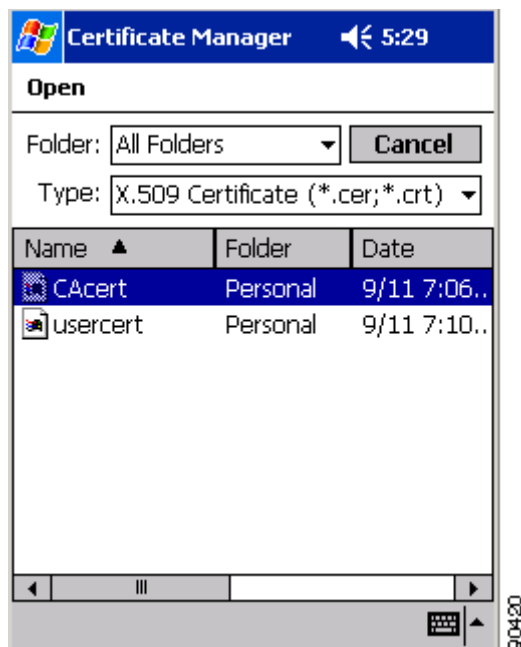
- 
- Step 1 Select **Start** > **Programs** > **Cisco** > **CertMgr**. The Certificate Manager window appears (see [Figure E-1](#)).

Figure E-1 Certificate Manager Window



- Step 2 Make sure **Trusted Authorities** appears in the Certificate drop-down menu.
- Step 3 Tap the **Import** button.
- Step 4 The Certificate Manager Open window appears (see [Figure E-2](#)).

Figure E-2 Certificate Manager Open Window



- Step 5** Tap the CA certificate file.
- Step 6** The Certificate Manager window reappears with the name of the CA certificate server listed in the middle of the window.
- Step 7** Tap **OK** to close the Certificate Manager.

## Importing a User Certificate

If you are planning to use EAP-TLS authentication on your Windows CE .NET 4.2 device, follow these steps to import the user certificate.



### Note

As an alternative to the procedure below, you can use the Certificate Manager to import a user certificate. To do so, follow the steps in the [“Importing a CA Certificate”](#) section above, but make sure My Certificates (not Trusted Authorities) appears in the Certificate drop-down menu in [Step 2](#) and tap the user certificate file (not the CA certificate file) in [Step 5](#).

- Step 1** Make sure that your Windows CE device has an ActiveSync link to a laptop or PC that is on the same network as the certificate server you want to use.
- Step 2** Select **Start > Programs > Cisco > Enroll**. The Certificate Enrollment window appears (see [Figure E-3](#)).

**Figure E-3** Certificate Enrollment Window

- Step 3** Enter your username, password, and server name for your certificate server, which can be obtained from your system administrator, in the appropriate fields.

- Step 4** Tap the **Enroll** button. The box at the bottom of the window indicates the status of the certificate enrollment by changing from *Ready* to *Processing*.
- If the operation is successful, the following message appears: “A certificate has been added to your device.”
- Step 5** Tap **OK** to close the Certificate Enrollment window.
- 

## Configuring the Client Adapter

Follow these steps to configure your client adapter using Windows CE .NET.



### Note

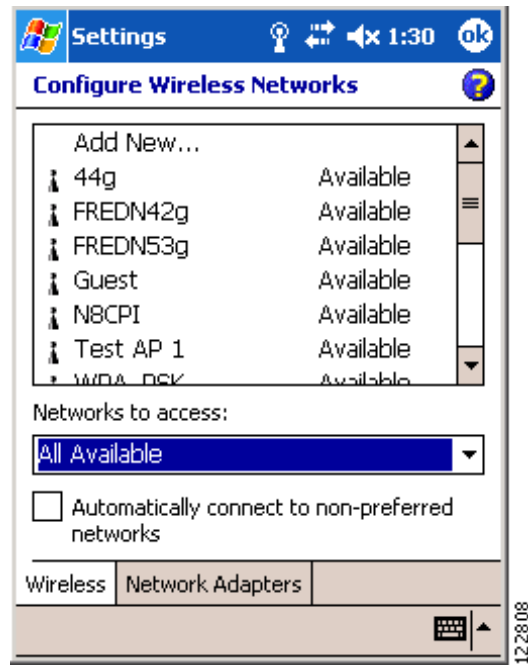
These instructions assume you are using a Windows CE .NET 4.2 device (specifically a PPC 2003) with the WPA supplicant installed. If you use a Windows CE .NET 4.0 or 4.1 device or a Windows CE .NET 4.2 device without the WPA supplicant, the windows you see will look different than those shown in this section. Refer to version OL-1375-04 of this manual if you need instructions on configuring a client adapter through Windows CE .NET without the WPA supplicant.

---

- Step 1** Make sure the client adapter is inserted in the Windows CE .NET device.
- Step 2** Double-tap the **ACU** icon on your desktop or select **Start > Programs > Cisco > ACU**.
- Step 3** On the Profiles window, select **<External Settings>** from the Select Active Profile drop-down menu.
- Step 4** When prompted, tap **OK**. Then reset your Windows CE .NET device or eject and reinsert the client adapter.
- Step 5** Tap **OK** to save your settings.
- Step 6** Select **Start > Settings > the Connections tab > Connections > the Advanced tab > Network Card**. The Configure Wireless Networks window (Wireless tab) appears (see [Figure E-4](#)).



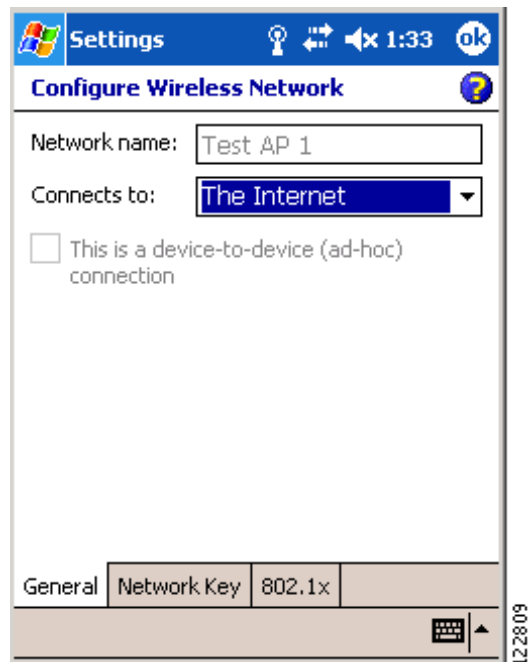
Figure E-4 Configure Wireless Networks Window (Wireless Tab)



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

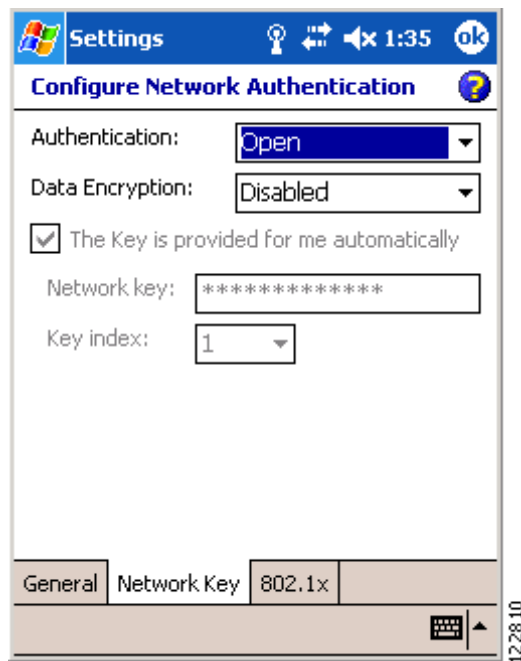
The Configure Wireless Network window (General tab) appears (see [Figure E-5](#)).

Figure E-5 Configure Wireless Network Window (General Tab)



- Step 8** Perform one of the following:
- If you selected an SSID from the list of wireless networks, make sure the SSID appears in the Network name field.
  - If you selected Add New, enter the case-sensitive SSID of the access point to which you want the client adapter to associate or the name of the ad hoc network in the Network name field.
- Step 9** Check the **This is a device-to-device (ad-hoc) connection** check box if you are planning to operate the client adapter in an ad hoc network.
- Step 10** Tap the **Network Key** tab. The Configure Network Authentication window (Network Key tab) appears (see Figure E-6).

**Figure E-6** Configure Network Authentication Window (Network Key Tab)



- Step 11** Choose one of the following options from the Authentication drop-down list:
- **Open**—Enables your client adapter, regardless of its WEP settings, to authenticate and attempt to communicate with an access point. This option is recommended if you want to use static WEP or EAP authentication without WPA.
  - **Shared**—Enables your client adapter to communicate only with access points that have the same WEP key. Cisco recommends that shared key authentication not be used because it presents a security risk.



**Note**

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

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



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

**Step 12** Choose one of the following options from the Data Encryption drop-down list:

- **Disabled**—Disables data encryption for your client adapter. This option is available only when Open or Shared has been selected for Authentication.
- **WEP**—Enables static or dynamic WEP for your client adapter. This option is recommended for use with open authentication.
- **TKIP**—Enables Temporal Key Integrity Protocol (TKIP) for your client adapter. This option is recommended for use with WPA and WPA-PSK.

**Step 13** Follow these steps to enter a static WEP key if you are planning to use static WEP.



**Note** If you are planning to use EAP-TLS or PEAP authentication, which uses dynamic WEP, go to [Step 15](#).

- a. Make sure the **The key is provided for me automatically** check box is unchecked.
- b. Obtain the WEP key for the access point (in an infrastructure network) or other clients (in an ad hoc network) from your system administrator.
- c. Enter the WEP key in the Network key field. In order to communicate, the client adapter must use the same WEP key as the access point or other clients.
- d. In the Key index field, select the number of the WEP key you are creating (**1, 2, 3, or 4**).



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

**Step 14** If you enabled WPA-PSK, obtain the pre-shared key for the access point (in an infrastructure network) or other clients (in an ad hoc network) from your system administrator and enter it in the Network key field.



**Note** Your client adapter's pre-shared key must match the pre-shared key used by the access point (in infrastructure mode) or clients (in ad hoc mode) with which you are planning to communicate.

**Step 15** Check the **The key is provided for me automatically** check box if you are planning to use EAP-TLS or PEAP authentication, which uses dynamic WEP keys.



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

**Step 16** Perform one of the following:

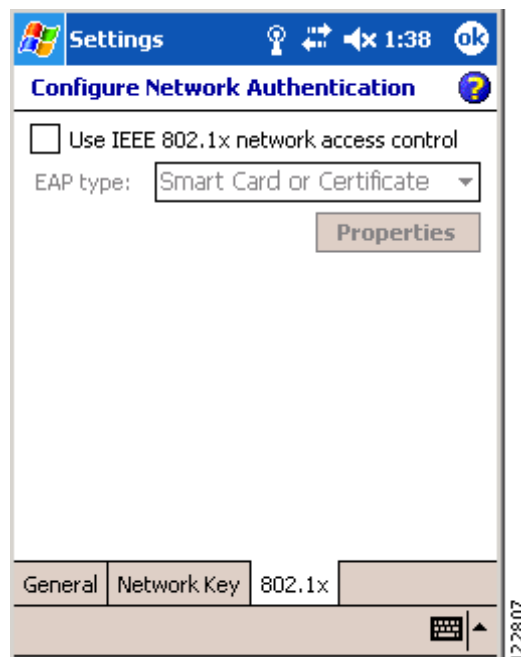
- If you are not planning to use EAP authentication, tap **OK** to save your settings and to add this SSID to the list of wireless networks (see [Figure E-4](#)). The client adapter automatically attempts to associate to the network(s) in the order in which they are listed. When the client adapter is associated to an access point, the word *Connected* appears to the right of the network name in the list of wireless networks.
- If you are planning to use EAP-TLS authentication, follow the instructions in the “[Enabling EAP-TLS Authentication](#)” section below.
- If you are planning to use PEAP authentication, follow the instructions in the “[Enabling PEAP Authentication](#)” section on page E-13.

## Enabling EAP-TLS Authentication

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

**Step 1** Tap the **802.1x** tab. The Configure Network Authentication window (802.1x tab) appears (see [Figure E-7](#)).

**Figure E-7** Configure Network Authentication Window (802.1x Tab)



**Step 2** Check the **Use IEEE 802.1x network access control** check box.

**Step 3** Select **Smart Card or Certificate** in the EAP type drop-down box.

**Step 4** If your Windows CE .NET device has more than one user certificate, tap the **Properties** button. On the Select Certificate window, select the user certificate that you want to use and tap **OK**.

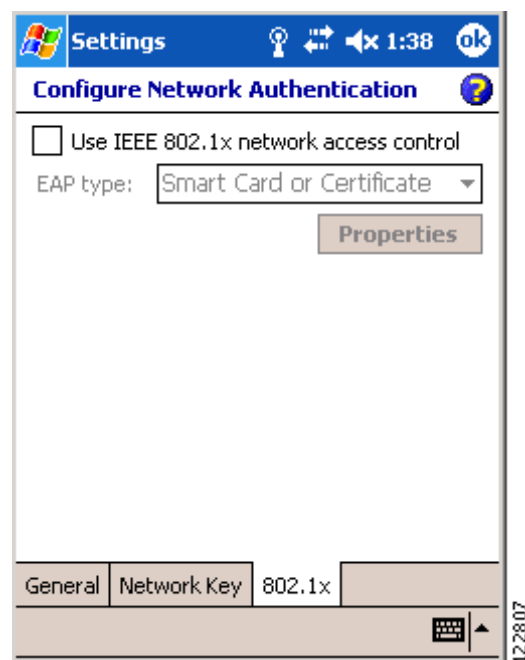
- Step 5** Tap **OK** to save your settings. The configuration is complete. The client adapter automatically attempts to associate to the network(s) in the order in which they are listed. When the client adapter is associated to an access point, the word *Connected* appears to the right of the network name in the list of wireless networks.
- Step 6** Refer to the [“Using EAP-TLS” section on page 6-4](#) for instructions on authenticating using EAP-TLS.

## Enabling PEAP Authentication

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

- Step 1** Tap the **802.1x** tab. The Configure Network Authentication window (802.1x tab) appears (see [Figure E-8](#)).

**Figure E-8** Configure Network Authentication Window (802.1x Tab)



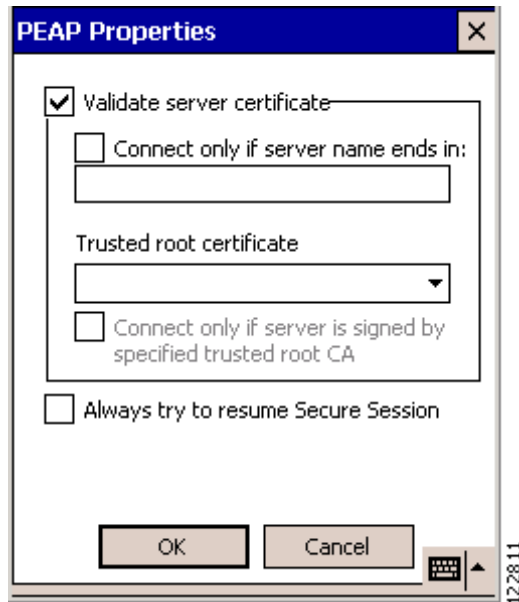
- Step 2** Check the **Use IEEE 802.1x network access control** check box.
- Step 3** Select **Cisco PEAP** in the EAP type drop-down box.



**Note** If the Microsoft PEAP supplicant is installed (rather than the Cisco PEAP supplicant), **PEAP** (rather than Cisco PEAP) appears in the EAP type drop-down box. Follow the instructions in your Microsoft documentation to configure your client adapter to use Microsoft PEAP.

- Step 4** Tap the **Properties** button. The PEAP Properties window appears (see [Figure E-9](#)).

Figure E-9 PEAP Properties Window



**Step 5** Make sure the **Validate server certificate** check box is checked if server certificate validation is required (recommended).

**Step 6** Check the **Connect only if server name ends in** check box and enter the appropriate server name suffix in the text box below.



**Note** If you leave this field blank, you are prompted to accept a connection to the server to which your client adapter is connected during the authentication process.

**Step 7** Make sure that the name of the certificate authority from which the server certificate was downloaded appears in the Trusted root certificate field. If necessary, tap the arrow on the drop-down box and select the appropriate name.



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

**Step 8** Check the **Connect only if server is signed by specified trusted root CA** check box if you want to ensure that the certificate server uses the trusted root certificate specified in the field above. This prevents the client from establishing connections to rogue access points.

**Step 9** Perform one of the following:

- Check the **Always try to resume Secure Session** check box if you want the PEAP protocol to always attempt to resume the previous session before prompting you to re-enter your credentials.
- Uncheck the **Always try to resume Secure Session** check box if you want to be prompted to re-enter your username and password whenever your client adapter's radio becomes disassociated (for example, when the card is ejected, the radio is turned off, you wander out of range of an access point, you switch profiles, and so on).

**Note**

Checking this check box gives you the convenience of not having to re-enter your username and password when your client adapter experiences momentary losses of association. The PEAP Session Timeout setting on the Cisco Secure ACS System Configuration - Global Authentication Setup window controls how long the resume feature is active (that is, the amount of time during which the PEAP session can be resumed without re-entering user credentials). If you leave your device unattended during this timeout period, be aware that someone can resume your PEAP session and access the network.

- Step 10** Tap **OK** on each open window to save your settings. The configuration is complete. The client adapter automatically attempts to associate to the network(s) in the order in which they are listed. When the client adapter is associated to an access point, the word *Connected* appears to the right of the network name in the list of wireless networks.
- Step 11** Refer to the [“Using PEAP” section on page 6-5](#) for instructions on authenticating using PEAP.

## Associating to an Access Point Using Windows CE .NET

Windows CE .NET causes the client adapter’s driver to automatically attempt to associate to the first network in the list of wireless networks (see [Figure E-4](#)). If the adapter fails to associate or loses association, it automatically switches to the next network in the list of wireless networks. The adapter does not switch networks as long as it remains associated to the access point. To force the client adapter to associate to a different access point, you must select a different network from the list of available networks and tap **OK**.







## Performing a Site Survey

---

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

The following topics are covered in this appendix:

- [Overview, page F-2](#)
- [Setting Signal Strength Display Units, page F-3](#)
- [Using Passive Mode, page F-4](#)
- [Using Active Mode, page F-7](#)
- [Forcing the Client Adapter to Reassociate, page F-13](#)

# Overview

**Note**

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

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

The site survey tool can be operated in two modes:

- **Passive Mode** – This is the default site survey mode. It does not initiate any RF network traffic; it simply listens to the traffic that the client adapter hears and displays the results. Follow the instructions in the [“Using Passive Mode” section on page F-4](#) to activate the passive mode.
- **Active Mode** – This mode causes the client adapter to actively send or receive low-level RF packets to or from its associated access point and provides information on the success rate. It also enables you to set parameters governing how the site survey is performed (such as the data rate). Follow the instructions in the [“Using Active Mode” section on page F-7](#) to activate the active mode.

## Guidelines

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

- Perform the site survey when the RF link is functioning with all other systems and noise sources operational.
- Execute the site survey entirely from the mobile station.
- When using the active mode, conduct the site survey with all variables set to operational values.

## Additional Information

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

- **Data rates** – Sensitivity and range are inversely proportional to data bit rates. Therefore, the maximum radio range is achieved at the lowest workable data rate, and a decrease in receiver threshold sensitivity occurs as the radio data increases.
- **Antenna type and placement** – Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height.
- **Physical environment** – Clear or open areas provide better radio range than closed or filled areas. Also, the less cluttered the work environment, the greater the range.

- **Obstructions** – A physical obstruction such as metal shelving or a steel pillar can hinder the performance of wireless devices. Avoid placing these devices in a location where a metal barrier is between the sending and receiving antennas.
- **Building materials** – Radio penetration is greatly influenced by the building material used in construction. For example, drywall construction allows greater range than concrete blocks, and metal or steel construction is a barrier to radio signals.

**Note**

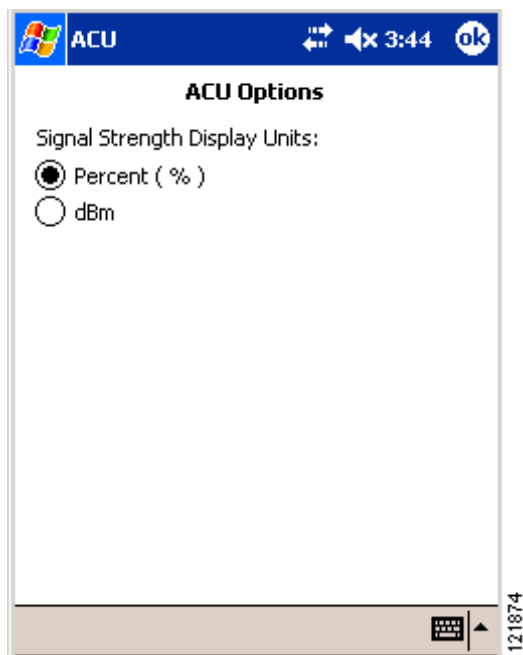
Refer to the hardware installation guide for your infrastructure device for additional information on factors affecting placement.

## Setting Signal Strength Display Units

Follow these steps to specify the units used to display signal strength on the Survey window.

- Step 1** Double-tap the **ACU** icon or select **Start > Programs > Cisco > ACU**. The Profiles window appears.
- Step 2** Tap the **Options** button. The ACU Options window appears (see [Figure F-1](#)).

**Figure F-1** ACU Options Window



- Step 3** Select one of the following options for Signal Strength Display Units:
- **Percent (%)**—Displays the signal strength as a percentage. This is the default setting.
  - **dBm**—Displays the signal strength in decibels with respect to milliwatts.
- Step 4** Tap **OK** to save your changes.

# Using Passive Mode

Follow these steps to activate the site survey passive mode and obtain current information about RF network traffic.

- Step 1
- From the Profiles window, tap the **Survey** tab. The Site Survey - Passive window appears (see [Figure F-2](#)), provided a client adapter is installed in the Windows CE device and is running.

[Figure F-2](#) shows the Site Survey - Passive Mode window with the signal strength values displayed as percentages, and [Figure F-3](#) shows the same window with the signal strength values displayed in dBm.

Figure F-2 Site Survey - Passive Window (with Signal Strength as a Percentage)

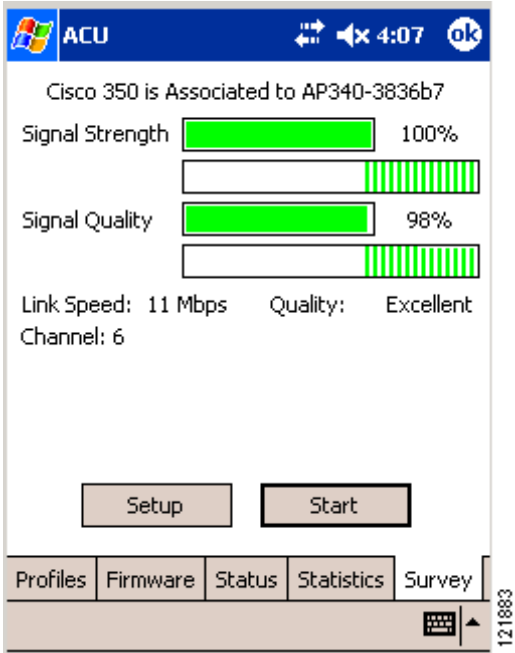


Figure F-3 Site Survey - Passive Window (with Signal Strength in dBm)

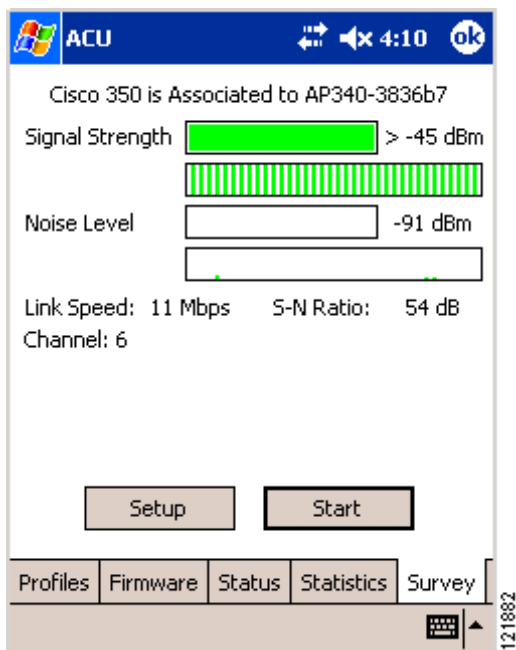


Table F-1 interprets the information that is displayed on the Site Survey - Passive window.

Table F-1 Site Survey Passive Mode Statistics

Statistic	Description
The first line of the Site Survey - Passive window	<p>Indicates the operational mode of your client adapter and the name or MAC address of any associated access point.</p> <p><b>Value:</b> Not Associated, Associated, Authenticated, or Ad Hoc Mode</p> <p><b>Note</b> The access point name or MAC address is shown only if the client adapter is in infrastructure mode and Aironet Extensions are enabled (on access points running Cisco IOS release 12.2(4)JA or later).</p>
Signal Strength	<p>The signal strength for all received packets. The higher the value and the more green the bar graph is, the stronger the signal.</p> <p>The histogram below the bar graph provides a visual interpretation of the current signal strength. Differences in signal strength are indicated by the following colors: green (strongest), yellow (middle of the range), and red (weakest).</p> <p><b>Range:</b> 0 to 100% or -95 to -45 dBm</p>

Table F-1 Site Survey Passive Mode Statistics (continued)

Statistic	Description
Signal Quality	<p>The signal quality for all received packets. The higher the value and the more green the bar graph is, the clearer the signal.</p> <p>The histogram below the bar graph provides a visual interpretation of the current signal quality. Differences in signal quality are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality).</p> <p><b>Range:</b> 0 to 100%</p> <p><b>Note</b> This setting appears only if you selected signal strength to be displayed as a percentage. See the <a href="#">“Setting Signal Strength Display Units”</a> section on page F-3 for information.</p>
Noise Level	<p>The level of background radio frequency energy in the 2.4-GHz band. The lower the value and the more green the bar graph is, the less background noise present.</p> <p>The histogram below the bar graph provides a visual interpretation of the current level of background noise. Differences in background noise level are indicated by the following colors: green (low noise), yellow (middle of the range), and red (high noise).</p> <p><b>Range:</b> –100 to –45 dBm</p> <p><b>Note</b> This setting appears only if you selected signal strength to be displayed in dBm. See the <a href="#">“Setting Signal Strength Display Units”</a> section on page F-3 for information.</p>
Link Speed	<p>In passive mode, the site survey tool monitors transmitted network traffic, and the data rate reflects the rate at which the packets are being transmitted.</p> <p><b>Value:</b> 1, 2, 5.5, or 11 Mbps</p>
Quality	<p>The client adapter’s ability to communicate with the access point.</p> <p><b>Value:</b> Not Associated, Poor, Fair, Good, Excellent</p> <p><b>Note</b> This setting appears only if you selected signal strength to be displayed as a percentage. See the <a href="#">“Setting Signal Strength Display Units”</a> section on page F-3 for information.</p>
Signal to Noise (S-N) Ratio	<p>The difference between the signal strength and the noise level. The higher the value, the better the client adapter’s ability to communicate with the access point.</p> <p><b>Range:</b> 0 to 90 dB</p> <p><b>Note</b> This setting appears only if you selected signal strength to be displayed in dBm. See the <a href="#">“Setting Signal Strength Display Units”</a> section on page F-3 for information.</p>
Channel	<p>The frequency that your client adapter is currently using as the channel for communications.</p> <p><b>Value:</b> Dependent on regulatory domain</p>

- Step 2** If you want to activate the site survey active mode, go to the “Using Active Mode” section below. Otherwise, tap **OK** to exit the site survey tool.

## Using Active Mode

Follow these steps to activate the site survey active mode and obtain current information about your client adapter’s ability to transmit and receive RF packets.

- Step 1** From the Site Survey - Passive window (see [Figure F-2](#)), tap the **Setup** button. The Active Mode Setup window appears (see [Figure F-4](#)).

**Figure F-4 Active Mode Setup Window**

ACU 4:12 ok

Destination MAC Address: 00:40:96:38:36:B7

☒ Destination Is Another Cisco Aironet Device

Number of Packets: 100

☐ Continuous Link Test

Packet Size: 512

Delay Between Packets (ms.): 0

Percent Success Threshold: 75

Data Retries: ☒ None ☐ Default Retries

Tx Type: ☒ Unicast ☐ Multicast

Data: ☐ 500 Kbps ☐ 1 Mbps ☒ 2 Mbps ☐ 5.5 Mbps ☐ 11 Mbps

Defaults OK Cancel

[Table F-2](#) lists and describes the parameters that affect how the site survey is performed. Follow the instructions in the table to set any parameters.

**Table F-2 Site Survey Active Mode Parameters**

Parameter	Description
Destination MAC Address	<p>The MAC address of the access point (in infrastructure mode) or other clients (in ad hoc mode) that will be used in the test.</p> <p><b>Default:</b> The MAC address of the access point (in infrastructure mode) to which your client adapter is associated</p> <p><b>Note</b> During the test, the client adapter does not roam to other access points so that the size of a single cell can be determined.</p>
Destination Is Another Cisco Aironet Device	<p>Checking this check box indicates that the device you named in the Destination MAC Address field is a Cisco Aironet access point (in infrastructure mode) or client (in ad hoc mode). In this case, packets sent to the client from the Cisco Aironet device contain additional information, such as lost to source, lost to target, and percent retries, and this information is displayed in the Site Survey - Active window.</p> <p>If the device specified in the Destination MAC Address field is not a Cisco Aironet device, do not check this check box. In this case, the test sends out loopback packets, which originate from and return to the client adapter.</p> <p><b>Default:</b> Checked</p>
Number of Packets	<p>The number of packets that will be sent during the test.</p> <p><b>Range:</b> 1 to 999</p> <p><b>Default:</b> 100</p>
Data Rate	<p>The bit rate at which packets are transmitted. Rate shifting does not occur during the test because the echo test built into the radio firmware does not support it</p> <p><b>Value:</b> 1, 2, 5.5, or 11 Mbps</p> <p><b>Default:</b> 11 Mbps</p>
Continuous Link Test	<p>Checking this check box causes the test to run until you tap <b>OK</b> or <b>Stop</b>. The test loops repeatedly for the number of packets specified in the Number of Packets field.</p> <p><b>Default:</b> Unchecked</p>
Packet Size	<p>The size of the packets that are sent during the test. Select a size that is typical during normal system use.</p> <p><b>Range:</b> 30 to 1450</p> <p><b>Default:</b> 512</p>
Delay Between Packets	<p>The delay (in milliseconds) between successive transmissions.</p> <p><b>Range:</b> 1 to 2048 ms</p> <p><b>Default:</b> 1 ms</p>



**Table F-2** Site Survey Active Mode Parameters (continued)

Parameter	Description						
Percent Success Threshold	<p>The percentage of packets that are not lost.</p> <p>This parameter controls the red line on the Percent Successful histogram. Percentages greater than or equal to this value are displayed as green bars; percentages below this value are displayed as yellow bars.</p> <p><b>Range:</b> 0 to 100%</p> <p><b>Default:</b> 75</p>						
Data Retries	<p>The number of times a transmission is retried if an acknowledgment (Ack) is not returned by the destination device.</p> <p><b>Default:</b> None</p> <table> <tr> <th>Retry Value</th><th>Description</th></tr> <tr> <td>None</td><td>No retries will occur.</td></tr> <tr> <td>Default Retries</td><td>The firmware's default value for retries (16) will be used.</td></tr> </table>	Retry Value	Description	None	No retries will occur.	Default Retries	The firmware's default value for retries (16) will be used.
Retry Value	Description						
None	No retries will occur.						
Default Retries	The firmware's default value for retries (16) will be used.						
Tx Type	<p>The packet type that is transmitted during the test.</p> <p><b>Default:</b> Unicast</p> <table> <tr> <th>Packet Type</th><th>Description</th></tr> <tr> <td>Unicast</td><td>When unicast packets are used, the system expects to receive an acknowledgment from the destination, and retries can occur.</td></tr> <tr> <td>Multicast</td><td>When multicast packets are used, no packet retries occur during the test.</td></tr> </table>	Packet Type	Description	Unicast	When unicast packets are used, the system expects to receive an acknowledgment from the destination, and retries can occur.	Multicast	When multicast packets are used, no packet retries occur during the test.
Packet Type	Description						
Unicast	When unicast packets are used, the system expects to receive an acknowledgment from the destination, and retries can occur.						
Multicast	When multicast packets are used, no packet retries occur during the test.						

**Step 2** After setting any parameters, tap **OK** to save your settings. The Site Survey - Passive window appears (see [Figure F-2](#)).

**Step 3** Tap the **Start** button to run the site survey test. The Site Survey - Active window appears.

[Figure F-5](#) shows the Site Survey - Active window with the signal strength values displayed as percentages, and [Figure F-6](#) shows the same window with the signal strength values displayed in dBm.

Figure F-5 Site Survey - Active Window (with Signal Strength as a Percentage)

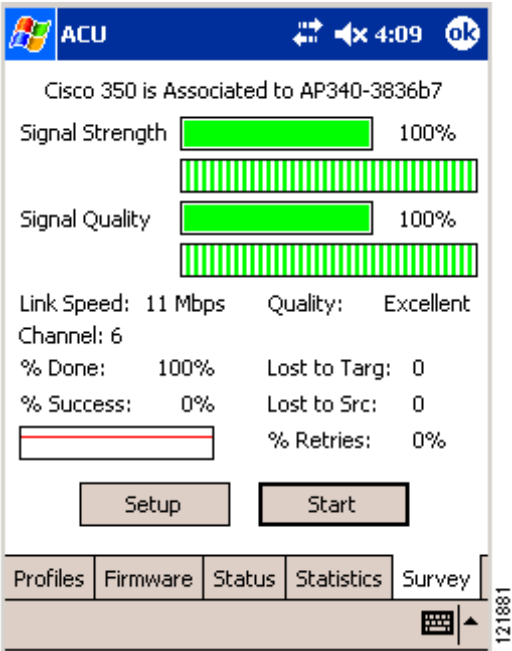


Figure F-6 Site Survey - Active Window (with Signal Strength in dBm)

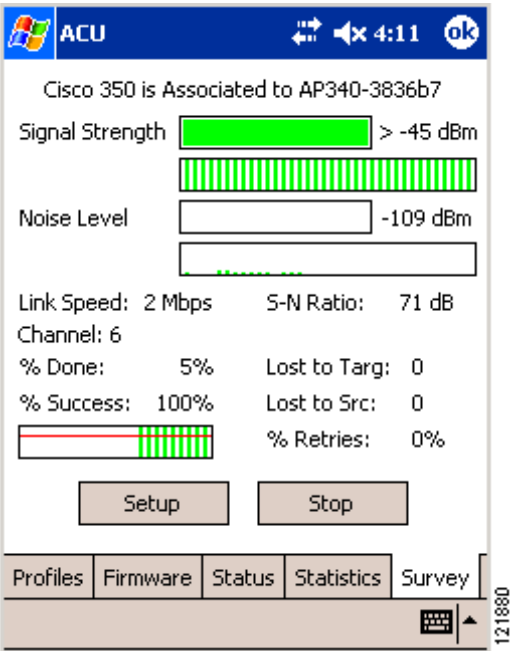


Table F-3 interprets the information that is displayed on the Site Survey - Active window while the site survey test is running.

**Table F-3 Site Survey Active Mode Statistics**

Statistic	Description
The first line of the Site Survey - Active window	<p>Indicates the operational mode of your client adapter and the name or MAC address of any associated access point.</p> <p><b>Value:</b> Not Associated, Associated, Authenticated, or Ad Hoc Mode</p> <p><b>Note</b> The access point name or MAC address is shown only if the client adapter is in infrastructure mode and Aironet Extensions are enabled (on access points running Cisco IOS release 12.2(4)JA or later).</p>
Signal Strength	<p>The signal strength for all received packets. The higher the value and the more green the bar graph is, the stronger the signal.</p> <p>The histogram below the bar graph provides a visual interpretation of the current signal strength. Differences in signal strength are indicated by the following colors: green (strongest), yellow (middle of the range), and red (weakest).</p> <p><b>Range:</b> 0 to 100% or -95 to -45 dBm</p>
Signal Quality	<p>The signal quality for all received packets. The higher the value and the more green the bar graph is, the clearer the signal.</p> <p>The histogram below the bar graph provides a visual interpretation of the current signal quality. Differences in signal quality are indicated by the following colors: green (highest quality), yellow (average), and red (lowest quality).</p> <p><b>Range:</b> 0 to 100%</p> <p><b>Note</b> This setting appears only if you selected signal strength to be displayed as a percentage. See the <a href="#">“Setting Signal Strength Display Units”</a> section on page F-3 for information.</p>
Noise Level	<p>The level of background radio frequency energy in the 2.4-GHz band. The lower the value and the more green the bar graph is, the less background noise present.</p> <p>The histogram below the bar graph provides a visual interpretation of the current level of background noise. Differences in background noise level are indicated by the following colors: green (low noise), yellow (middle of the range), and red (high noise).</p> <p><b>Range:</b> -100 to -45 dBm</p> <p><b>Note</b> This setting appears only if you selected signal strength to be displayed in dBm. See the <a href="#">“Setting Signal Strength Display Units”</a> section on page F-3 for information.</p>
Link Speed	<p>The rate at which your client adapter is transmitting packets to or from its associated access point.</p> <p><b>Value:</b> 1, 2, 5.5, or 11 Mbps</p>

**Table F-3 Site Survey Active Mode Statistics (continued)**

Statistic	Description
Quality	<p>The client adapter's ability to communicate with the access point.</p> <p><b>Value:</b> Not Associated, Poor, Fair, Good, Excellent</p> <p><b>Note</b> This setting appears only if you selected signal strength to be displayed as a percentage. See the <a href="#">“Setting Signal Strength Display Units”</a> section on page F-3 for information.</p>
Signal to Noise (S-N) Ratio	<p>The difference between the signal strength and the noise level. The higher the value, the better the client adapter's ability to communicate with the access point.</p> <p><b>Range:</b> 0 to 90 dB</p> <p><b>Note</b> This setting appears only if you selected signal strength to be displayed in dBm. See the <a href="#">“Setting Signal Strength Display Units”</a> section on page F-3 for information.</p>
Channel	<p>The frequency that your client adapter is currently using as the channel for communications.</p> <p><b>Value:</b> Dependent on regulatory domain</p>
Percent Done	The percentage of packets that have been transmitted based on the number specified in the Number of Packets field.
Percent Successful	<p>The percentage of packets that were transmitted successfully.</p> <p>The Percent Successful histogram provides a visual interpretation of the percentage of packets that are not lost. The value you set for the Percent Success Threshold is indicated by the red line. Percentages greater than or equal to this value are displayed as green bars; percentages below this value are displayed as yellow bars.</p> <p><b>Note</b> Refer to the Percent Success Threshold parameter in <a href="#">Table F-2</a> for more information.</p>
Lost To Target	The number of packets that were not transmitted successfully to the access point.
Lost To Source	The number of packets that were not received successfully from the access point.
Percent Retries	<p>The percentage of packets that were retried for transmission.</p> <p><b>Note</b> This value is calculated as follows:  <math display="block">(\text{number of retries} \times 100) / \text{number of packets sent}</math> <p>If a lot of packets get lost, the number of retries could be greater than the number of packets sent. Then this field would show a value greater than 100%.</p> </p>

- Step 4** When you tap the **Stop** button or when the Percent Complete reaches 100%, the active mode changes back to the passive mode.
- Step 5** Tap **OK** to exit the site survey tool.
- 

## Forcing the Client Adapter to Reassociate

The client adapter will attempt to maintain its association to an access point for as long as it can. Therefore if you are on a fringe area while conducting a site survey, you may want to reinitialize (or restart) the client adapter in an attempt to force it to disassociate from the access point to which it is currently associated and reassociate to another access point.

Follow these steps to attempt to force the client adapter to disassociate from its current access point and reassociate to another during a site survey.

---

- Step 1** Tap the **Profiles** tab.
- Step 2** Perform one of the following:
- Change the active profile and then select it again.
  - Select the active profile in the Manage Profiles box, tap the **Edit** button, and tap **OK**.
- Step 3** Tap the **Survey** tab to return to the Site Survey window. The first line of the Site Survey window displays *Not Associated* while the client adapter disassociates from its current access point and then displays *Associated* once the adapter is reassociated to an access point.
-





## GLOSSARY

- 802.1X** Also called *802.1X for 802.11*. 802.1X is the new standard for wireless LAN security, as defined by the Institute of Electrical and Electronics Engineers (IEEE). An access point that supports 802.1X and its protocol, Extensible Authentication Protocol (EAP), acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.
- 802.11** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) 2.4-GHz wireless LANs.
- 802.11b** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps wireless LANs.

---

### A

- Access Point** A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.
- ActiveSync** A Microsoft program that enables a desktop-to-Windows CE device connection in order to transfer files.
- Ad Hoc Network** A wireless network composed of stations without access points.
- Alphanumeric** A set of characters that contains both letters and numbers.
- Associated** A station is configured properly to allow it to wirelessly communicate with an access point.

---

### B

- Bandwidth** Specifies the amount of the frequency spectrum that is usable for data transfer. It identifies the maximum data rate that a signal can attain on the medium without encountering significant power loss.
- BPSK** Binary phase shift keying. A modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 1 Mbps.
- Broadcast key rotation** A security feature for use with dynamic WEP keys. If your client adapter uses LEAP, EAP-FAST, EAP-TLS, or PEAP authentication and you enable this feature, the access point changes the dynamic broadcast WEP key that it provides at the interval you select.

---

C

<b>CCK</b>	Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.
<b>CeAppMgr</b>	Windows CE Application Manager. The desktop Windows CE Services component that provides a desktop-to-device application management tool. It is responsible for adding and removing applications on the Windows CE device and for deleting the application files from the desktop computer. CeAppMgr is included with every installation of Windows CE Services.
<b>Cisco TKIP</b>	Also referred to as Cisco Key Integrity Protocol (CKIP). Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.
<b>Client</b>	A radio device that uses the services of an access point to communicate wirelessly with other devices on a local area network.
<b>CSMA</b>	Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.
<b>Cyclic Redundancy Check (CRC)</b>	A method of checking for errors in a received packet.

---

D

<b>Data Rates</b>	The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).
<b>dBi</b>	A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain and the more acute the angle of coverage.
<b>DHCP</b>	Dynamic Host Configuration Protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.
<b>Dipole</b>	A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.
<b>Domain Name Server</b>	A network server that translates text names to IP addresses.
<b>Domain Name System (DNS)</b>	Provides names for computers using alphanumeric characters instead of numbers like IP addresses use. Maintains a database of the host alphanumeric names and their corresponding IP addresses.
<b>DSSS</b>	Direct-sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.
<b>Duplicate Packets</b>	Packets that were received twice because an acknowledgement got lost and the sender retransmitted the packet.



---

**E**

<b>EAP</b>	Extensible Authentication Protocol. EAP is the protocol for the optional IEEE 802.1X wireless LAN security feature. An access point that supports 802.1X and EAP acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network.
<b>EAP-FAST</b>	Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling. An 802.1X authentication type that is available for use with PPC 2002, PPC 2003, and Windows CE .NET 4.2 devices. Support for EAP-FAST is provided in the client adapter's firmware and the Cisco software that supports it, rather than in the operating system. With EAP-FAST, a username, password, and PAC are used by the client adapter to perform mutual authentication with the RADIUS server through an access point.
<b>Ethernet</b>	The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to allow computers to share a network and operates at 10, 100, or 1000 megabits per second (Mbps), depending on the physical layer used.

---

**F**

<b>File Server</b>	A repository for files so that a local area network can share files, mail, and programs.
<b>Firmware</b>	Software that is programmed on a memory chip and kept in a computer's semi-permanent memory.
<b>Fragmentation Threshold</b>	The size at which packets are fragmented and transmitted a piece at a time instead of all at once. The setting must be within the range of 64 to 2312 bytes.

---

**G**

<b>Gateway</b>	A device that connects two otherwise incompatible networks together.
<b>GHz</b>	Gigahertz. One billion cycles per second. A unit of measure for frequency.

---

**H**

<b>Hexadecimal</b>	A set of characters consisting of ten numbers and six letters (0-9, A-F, and a-f).
<b>HPC</b>	Handheld Personal Computer. One of the three defined types of Windows CE devices.

---

**I**

<b>IEEE</b>	Institute of Electrical and Electronic Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.
<b>Infrastructure</b>	The wired Ethernet network.

<b>Infrastructure Device</b>	A device (such as an access point, bridge, or base station) that connects client adapters to a wired LAN.
<b>IP Address</b>	The Internet Protocol (IP) address of a station.
<b>IP Subnet Mask</b>	The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway.
<b>Isotropic</b>	An antenna that radiates its signal 360 degrees both vertically and horizontally in a perfect sphere.

---

L

<b>LEAP</b>	LEAP, or <i>EAP-Cisco Wireless</i> , is an 802.1X authentication type that is available on Windows CE devices. Support for LEAP is provided in the client adapter's firmware and the Cisco software that supports it, rather than in the operating system. With LEAP, a username and password are used by the client adapter to perform mutual authentication with the RADIUS server through an access point.
-------------	---

---

M

<b>MAC Address</b>	The Media Access Control (MAC) address is a unique serial number assigned to a networking device by the manufacturer.
<b>MIC</b>	Message integrity check. MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The client adapter's driver must support MIC functionality, and MIC must be enabled on the access point.
<b>Modulation</b>	Any of several techniques for combining user information with a transmitter's carrier signal.
<b>Multicast Packets</b>	Packets transmitted to multiple stations.
<b>Multipath</b>	The echoes created as a radio signal bounces off of physical objects.

---

O

<b>Overrun Packets</b>	Packets that were discarded because the access point had a temporary overload of packets to handle.
------------------------	---

---

P

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

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

**PPC** Pocket-sized Personal Computer. One of the three defined types of Windows CE devices.

---

## Q

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

---

## R

**Radio Channel** The frequency at which a radio operates.

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

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

**RF** Radio frequency. A generic term for radio-based technology.

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

**RTS Threshold** The packet size at which an access point will issue a request to send (RTS) before sending the packet.

---

## S

**Spread Spectrum** A radio transmission technology that spreads the user information over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.

**SSID** Service set identifier. A unique identifier that stations must use to be able to communicate with an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

---

## T

**TKIP** Temporal Key Integrity Protocol. Also referred to as *WEP key hashing*. A security feature that defends against an attack on WEP in which the intruder uses the initialization vector (IV) in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs.

**Transmit Power** The power level of radio transmission.

---

U

**Unicast Packets**      Packets transmitted in point-to-point communication.

---

W

**WEP**      Wired equivalent privacy. An optional security mechanism defined within the 802.11 standard designed to protect your data as it is transmitted through your wireless network by encrypting it through the use of encryption keys.

**Workstation**      A computing device with an installed client adapter.

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



## Symbols

? button, function of [1-6](#)

## Numerics

802.1X [5-12, E-3](#)

802.1X backport, installing [3-4](#)

## A

### About

button [8-7](#)

window [8-9](#)

### access point

IP address [7-5](#)

MAC address [7-4](#)

### access points

associating to in Windows CE .NET [E-15](#)

in wireless infrastructure [1-8](#)

problems associating to [9-3](#)

problems authenticating to [9-4](#)

reporting those that fail LEAP or EAP-FAST authentication [5-15, 5-19](#)

role in wireless network [1-6](#)

security settings [5-17](#)

Active Mode Setup window [F-7](#)

ActiveSync, using [3-3, 5-24, 5-28, 5-30, 8-4, E-5, E-7](#)

ACU Options window [7-2, F-3](#)

ad hoc mode [5-3](#)

### ad hoc network

defined [E-9](#)

displayed [1-7](#)

selecting in Windows CE .NET [E-10](#)

### Aironet Client Utility (ACU)

buttons [1-6](#)

deleting icon [8-9](#)

described [1-4](#)

exiting [8-8](#)

feature comparison to Windows CE .NET [3-6 to 3-7](#)

finding version [8-7, 8-9](#)

installing [3-2 to 3-5](#)

opening [8-8](#)

overview [1-5 to 1-6](#)

uninstalling [8-8](#)

upgrading [8-6 to 8-7](#)

### antenna

described [1-3](#)

gains [D-3 to D-4](#)

options [C-3](#)

placement [F-2](#)

specifications [A-4](#)

type [F-2](#)

audience of document [x](#)

### authentication

after LEAP or EAP-FAST times out [9-4](#)

process [5-13, E-3](#)

Authentication Manager, using [5-31 to 5-34](#)

Authentication Type parameter [5-5](#)

Authentication window [5-32](#)

automatic PAC provisioning [5-10, 5-12, 5-25](#)

---

## B

- beacon packets, number received [7-8](#)
- broadcast key rotation
  - described [5-17](#)
  - setting on client and access point [5-19](#)
- broadcast packets
  - number received [7-8](#)
  - number transmitted [7-10](#)
- buttons on client utilities, described [1-6](#)
- bytes
  - number received [7-8](#)
  - number transmitted [7-10](#)

---

## C

- CAM [5-4](#)
- Canadian compliance statement [C-3](#)
- Cancel button, function of [1-6](#)
- caution, defined [xi](#)
- CCKM
  - See fast roaming
- Certificate Authority (CA) certificates
  - importing [5-29 to 5-30, E-5 to E-7](#)
  - obtaining [5-28, E-5](#)
  - removing [8-11](#)
  - viewing [8-10](#)
- Certificate Enrollment window [5-31, E-7](#)
- Certificate Manager
  - Open window [5-30, E-6](#)
  - using [5-29 to 5-30, E-5 to E-7](#)
  - window [5-29, 8-10, E-6](#)
- Change Password window [6-8](#)
- channel
  - in active site survey [F-12](#)
  - in passive site survey [F-6](#)
- channel set [7-6](#)

- Cisco.com
  - obtaining documentation [xiii](#)
  - obtaining technical assistance [xv](#)
- Cisco Centralized Key Management (CCKM)
  - See fast roaming
- Cisco PEAP
  - See PEAP authentication
- Cisco PEAP option [5-33](#)
- Cisco TKIP [7-6](#)
- Client Name parameter [5-3](#)
- client utilities
  - See Aironet Client Utility (ACU) and Wireless Login Module (WLM)
- Configure Network Authentication window (802.1x tab) - Windows CE .NET [E-12, E-13](#)
- Configure Network Authentication window (Network Key tab) - Windows CE .NET [E-10](#)
- Configure Wireless Networks window (Wireless tab) - Windows CE .NET [E-9](#)
- Configure Wireless Network window (General tab) - Windows CE .NET [E-9](#)
- configuring client adapter
  - deciding between ACU and Windows CE .NET [3-6 to 3-7](#)
  - in ACU [5-2 to 5-35](#)
  - through Windows CE .NET [E-8 to E-15](#)
- Connect button [5-32, 5-34](#)
- Continuous Link Test parameter [F-8](#)
- conventions of document [xi to xii](#)
- CRC errors [7-9](#)

---

## D

- Data Rate parameter [F-8](#)
- data rates [A-3, F-2](#)
- Data Rates parameter [5-6](#)
- Data Retries parameter [F-9](#)

## declarations of conformity

European community, Switzerland, Norway, Iceland,  
and Liechtenstein [C-4 to C-6](#)

FCC [C-2 to C-3](#)

RF exposure [C-6](#)

Delay Between Packets parameter [F-8](#)

Destination Is Another Cisco Aironet Device  
parameter [F-8](#)

Destination MAC Address parameter [F-8](#)

## diagnostic tools

overview [7-2](#)

setting parameters [7-2, F-3](#)

using [7-1 to 7-11](#)

disassociating client adapter from access point [8-11](#)

diversity antenna [1-3](#)

## document

audience [x](#)

conventions [xi to xii](#)

organization [x](#)

purpose [x](#)

software versions covered [x](#)

windows used in [1-4](#)

## documentation

CD-ROM [xiii](#)

feedback [xiv](#)

obtaining [xiii to xiv, xvi](#)

ordering [xiv](#)

domain name, entering for LEAP or EAP-FAST [6-3](#)

## driver

current version [7-7](#)

described [1-4](#)

finding version [8-7](#)

installing [3-2 to 3-5](#)

uninstalling [8-8](#)

upgrading [8-6 to 8-7](#)

verifying installation [3-5](#)

dynamic WEP keys, overview [5-12 to 5-14, E-3](#)

Dynamic WEP Keys option [5-8, 5-31](#)

## E

### EAP authentication

described [5-12, E-3](#)

overview [6-2](#)

using [6-1 to 6-8](#)

EAP-FAST(WPA) option [5-9, 5-25](#)

### EAP-FAST authentication

authenticating after your credentials expire [6-4](#)

authenticating with saved username and password [6-4](#)

authenticating with temporary username and  
password [6-2 to 6-3](#)

described [5-12](#)

disabling [5-35](#)

enabling [5-24 to 5-27](#)

error messages [9-10 to 9-14](#)

RADIUS servers supported [5-12](#)

requirements [5-24](#)

setting on client and access point [5-17](#)

user databases supported [5-13](#)

EAP-FAST option [5-9, 5-25](#)

### EAP-TLS authentication

authenticating after profile selection/card  
insertion/reset [6-5 to 6-6](#)

described [5-13, E-3](#)

enabling

in ACU [5-31 to 5-32](#)

in Windows CE .NET [E-12](#)

error messages [9-14 to 9-15](#)

importing CA certificates [5-29 to 5-30, E-5 to E-7](#)

importing user certificates [5-30 to 5-31, E-7 to E-8](#)

obtaining CA and user certificates [5-28, E-5](#)

preparing for configuration in Windows CE .NET [E-4](#)

RADIUS servers supported [5-13, E-3](#)

requirements for configuring in Windows CE .NET [E-4](#)

setting on client and access point [5-18](#)

Edit button [5-35](#)

EIRP, maximum [1-3, D-3 to D-4](#)

encryption, current setting [7-6](#)

Enroll button [5-31, E-8](#)

## error messages

EAP-FAST authentication [9-10 to 9-14](#)

EAP-TLS authentication [9-14 to 9-15](#)

general [9-5 to 9-7](#)

installation [9-7 to 9-8](#)

LEAP authentication [9-8 to 9-9](#)

PEAP authentication [9-15 to 9-17](#)

External Settings profile option [4-3, E-8](#)

## F

Fast PSP [5-4](#)

## fast roaming

described [5-14](#)

setting on client and access point [5-18 to 5-19](#)

## FCC

declaration of conformity statement [C-2 to C-3](#)

safety compliance statement [2-2](#)

## Firmware

### tab

described [1-5](#)

using [8-3, 8-5](#)

window [8-3](#)

## firmware

current version [7-7](#)

described [1-4](#)

finding version [8-3 to 8-4](#)

loading [8-4 to 8-6](#)

upgrading [8-3 to 8-6](#)

version required [3-2](#)

frequencies [D-2](#)

## G

general error messages [9-5 to 9-7](#)

## H

hardware components of client adapter [1-3](#)

## help

on HPC devices [9-17](#)

on PPC devices [9-17](#)

on Windows CE .NET devices [9-17](#)

## host-based EAP authentication

described [5-13](#)

disabling [5-35](#)

enabling [5-28 to 5-34](#)

requirements [5-28](#)

Host Based EAP option [5-9, 5-31](#)

## I

## infrastructure devices

defined [1-2](#)

site requirements [2-5](#)

Infrastructure Mode parameter [5-3](#)

inserting PC card into Windows CE device [8-2](#)

installation error messages [9-7 to 9-8](#)

Install Cisco PEAP Support installation option [3-4](#)

interference [2-5](#)

## IP address

obtaining or specifying [3-5](#)

of associated access point [7-5](#)

of client adapter [7-7](#)

problems obtaining [9-3](#)

## J

Japan, guidelines for operating client adapters [C-7](#)



---

**L**

- LEAP(WPA) option [5-9, 5-23](#)
- LEAP authentication
  - authenticating with saved username and password [6-4](#)
  - authenticating with temporary username and password [6-2 to 6-3](#)
  - described [5-12](#)
  - disabling [5-35](#)
  - enabling [5-22 to 5-23](#)
  - error messages [9-8 to 9-9](#)
  - RADIUS servers supported [5-12](#)
  - requirements [5-22](#)
  - setting on client and access point [5-17](#)
- LEAP option [5-9, 5-23](#)
- LEDs
  - described [1-3](#)
  - interpreting [9-2 to 9-3](#)
  - using to verify installation [3-5](#)
- link quality
  - current [7-5](#)
  - in active site survey [F-12](#)
  - in passive site survey [F-6](#)
- link speed
  - current [7-6](#)
  - in active site survey [F-11](#)
  - in passive site survey [F-6](#)
- LM card
  - antenna [1-3](#)
  - described [1-2](#)
- Logout button [6-3, 6-4](#)

---

**M**

- MAC address
  - of associated access point [7-4](#)
  - of client adapter [7-6](#)
- MAC CRC errors [7-9](#)
- manual PAC provisioning [5-10, 5-12, 5-24, 5-25](#)

- Max PSP [5-4](#)
- message integrity check (MIC)
  - current status [7-7](#)
  - described [5-16](#)
  - setting on client and access point [5-19](#)
  - statistics [7-11](#)
  - types of [7-7](#)
- Michael MIC [7-7](#)
- microcellular network [1-8](#)
- MIC Statistics window [7-11](#)
- Mixed Mode parameter [5-5](#)
- MMH MIC [7-7](#)
- multicast packets
  - in active site survey [F-9](#)
  - number received [7-8](#)
  - number transmitted [7-10](#)

---

**N**

- network
  - configurations [1-6 to 1-8](#)
  - problems connecting to [9-4](#)
- Network Security Type parameter [5-9, 5-20, 5-23, 5-25, 5-31, 5-35](#)
- noise level
  - current [7-5](#)
  - in active site survey [F-11](#)
  - in passive site survey [F-6](#)
- None option [5-9, 5-35](#)
- note, defined [xi](#)
- No WEP option [5-8, 5-22](#)
- Number of Packets parameter [F-8](#)

---

**O**

- Offline Channel Scan parameter [5-7](#)
- OK button, function of [1-6](#)
- open authentication [5-5, E-10](#)
- Open window [5-26, 8-6](#)

Options button [7-2, F-3](#)  
 organization of document [x](#)

## P

PAC Authority parameter [5-11, 5-26](#)  
 PAC Import button [5-26](#)  
 package contents [2-3](#)  
 packets  
   discarded due to MIC error [7-11](#)  
   encryption used [7-6](#)  
   lost to source in active site survey [F-12](#)  
   lost to target in active site survey [F-12](#)  
   max retries [7-10](#)  
   percent retried in active site survey [F-12](#)  
   received with MIC [7-11](#)  
   retry long [7-10](#)  
   retry short [7-10](#)  
 Packet Size parameter [F-8](#)  
 PAC Password window [5-27](#)  
 PAC provisioning [5-10, 5-12, 5-24, 5-25](#)  
 PAC Provisioning Mode parameter [5-10, 5-25](#)  
 PACs  
   described [5-10, 5-12, 5-25](#)  
   entering password [5-26](#)  
   importing [5-26 to 5-27](#)  
   obtaining [5-24](#)  
   rules for storage [5-12](#)  
 Password Expired window [6-4](#)  
 passwords, creating [9-4](#)  
 PC card  
   antenna [1-3](#)  
   described [1-2](#)  
   inserting into Windows CE device [8-2](#)  
   removing from Windows CE device [8-2](#)

PEAP authentication  
   authenticating after profile selection/card  
     insertion/reset [6-6 to 6-7](#)  
   authenticating after your password expires (Windows  
     NT or 2000 domain databases) [6-8](#)  
   described [5-13, E-3](#)  
   enabling  
     in ACU [5-31 to 5-34](#)  
     in Windows CE .NET [E-13 to E-15](#)  
   error messages [9-15 to 9-17](#)  
   importing CA certificates [5-29 to 5-30, E-5 to E-7](#)  
   obtaining CA certificates [5-28, E-5](#)  
   preparing for configuration in Windows CE .NET [E-4](#)  
   RADIUS servers supported [5-13, E-3](#)  
   requirements for configuring in Windows CE .NET [E-4](#)  
   setting on client and access point [5-18](#)  
 PEAP option [5-33](#)  
 PEAP Properties window [5-33, E-14](#)  
 peer-to-peer wireless LAN [1-7](#)  
 Percent Successful histogram [F-9, F-12](#)  
 Percent Success Threshold parameter [F-9](#)  
 physical specifications [A-2](#)  
 PLCP CRC errors [7-9](#)  
 power level  
   current [7-6](#)  
   maximum [D-3 to D-4](#)  
   options [A-3](#)  
 Power Save Mode parameter [5-4](#)  
 power specifications [A-4](#)  
 profile, defined [4-2](#)  
 profile manager  
   creating a new profile [4-3](#)  
   deleting a profile [4-5](#)  
   editing a profile [4-4](#)  
   opening [4-2](#)  
   overview [4-2](#)  
   renaming a profile [4-4](#)  
   selecting the active profile [4-3 to 4-4](#)

## Profiles tab

- described [1-5](#)
- using [4-2](#)

## Profiles window

- displayed [1-5, 4-2](#)
- tabs [1-5](#)

Properties window [5-2](#)purpose of document [x](#)


---

**R**

## radio

- described [1-3](#)
- specifications [A-3 to A-4](#)

RADIUS servers [5-12 to 5-14, E-3](#)range [5-6](#)reassociating client adapter [F-13](#)receive statistics [7-8](#)Receive Statistics window [7-8](#)

## regulatory

- domains [7-6, D-2](#)
- information [C-2 to C-8](#)
- specifications [A-4](#)

related publications [xiii](#)removing PC card from Windows CE device [8-2](#)Renew button [7-7](#)restarting client adapter [8-11](#)RF obstructions [2-5, F-3](#)roaming [1-8](#)RTS packets, number retransmitted [7-10](#)


---

**S**

## safety

- information [2-2 to 2-3](#)
- specifications [A-4](#)

seamless roaming [1-8](#)

## security features

- overview [5-11 to 5-19, E-2 to E-3](#)
- synchronizing [5-17](#)

sensitivity [A-3](#)shared key authentication [5-5, E-10](#)

## signal quality

- current [7-5](#)
- in active site survey [F-11](#)
- in passive site survey [F-6](#)

## signal strength

- as a percentage [7-2, F-3](#)
- current [7-5](#)
- in active site survey [F-11](#)
- in dBm [7-2, F-3](#)
- in passive site survey [F-5](#)

Signal Strength Display Units parameter [7-2, F-3](#)

## signal to noise ratio

- current [7-6](#)
- in active site survey [F-12](#)
- in passive site survey [F-6](#)

## site requirements

- for client devices [2-5](#)
- for infrastructure devices [2-5](#)

## site survey

- active mode [F-2, F-7 to F-13](#)
- guidelines [F-2](#)
- overview [F-2 to F-3](#)
- passive mode [F-2, F-4 to F-7](#)

Site Survey - Active window [F-10](#)Site Survey - Passive window [F-4, F-5](#)software, upgrading [8-3 to 8-8](#)software components of client adapter [1-4 to 1-6](#)software required for WPA [5-14, E-4](#)software versions covered in document [x](#)

## specifications

- physical [A-2](#)
- power [A-4](#)
- radio [A-3 to A-4](#)

- regulatory compliance [A-4](#)
- safety [A-4](#)
- spread spectrum [1-3](#)
- SSID parameter [5-3](#)
- Start button, function of [1-6](#)
- Static Password window [6-7](#)
- static WEP
  - disabling [5-22](#)
  - enabling [5-20 to 5-21](#)
  - with open authentication, setting on client and access point [5-17](#)
  - with shared key authentication, setting on client and access point [5-17](#)
- static WEP keys
  - entering [5-20 to 5-21, E-11](#)
  - guidelines for entering
    - in ACU [5-21](#)
    - in Windows CE .NET [E-11](#)
  - overview [5-11, E-2](#)
  - overwriting [5-21 to 5-22](#)
  - selecting transmit key [5-21](#)
  - size of [5-20](#)
- Static WEP Keys option [5-8, 5-20](#)
- statistics of client adapter, viewing [7-7 to 7-11](#)
- Statistics tab
  - described [1-5](#)
  - using [7-8](#)
- Status
  - tab
    - described [1-5](#)
    - using [7-3, 8-7](#)
  - window [7-3](#)
- status of client adapter
  - in active site survey [F-11](#)
  - in ACU status bar [1-5](#)
  - in passive site survey [F-5](#)
  - in Status window [7-4](#)
  - viewing [7-3 to 7-7](#)

- Status window [5-16](#)
- Stop button, function of [1-6](#)
- strong passwords, creating [9-4](#)
- Survey tab
  - described [1-5](#)
  - using [F-4](#)
- system requirements [2-4](#)

---

## T

- Taiwan, rules for operating client adapters [C-8](#)
- technical assistance, obtaining [xiv to xvi](#)
- Technical Assistance Center, contacting [xv to xvi](#)
- Temporal Key Integrity Protocol (TKIP)
  - described [5-17](#)
  - setting on client and access point [5-19](#)
  - status of [7-6](#)
- throughput [5-4, 5-6, 8-11](#)
- TKIP option [E-11](#)
- TLS option [5-32](#)
- Transmit Key button [5-21](#)
- Transmit Power parameter [5-7](#)
- transmit statistics [7-10](#)
- Transmit Statistics window [7-10](#)
- troubleshooting information [9-2 to 9-17](#)
- Tx Type parameter [F-9](#)

---

## U

- unicast packets
  - in active site survey [F-9](#)
  - number received [7-8](#)
  - number transmitted [7-10](#)
- unpacking the client adapter [2-3](#)
- up time [7-9, 7-10](#)
- user certificates
  - importing [5-30 to 5-31, E-7 to E-8](#)
  - obtaining [5-28, E-5](#)

- removing [8-11](#)
- viewing [8-10](#)
- User Domain parameter [5-10](#)
- User Logon window [6-5](#)
- User Name parameter [5-9](#)
- User Password parameter [5-10](#)
- Use Windows to configure my wireless network settings option [3-7](#)

---

## W

### warning

- antenna [2-3, B-3](#)
- defined [xi to xii](#)
- explosive device proximity [2-3, B-2](#)
- laptop users [2-3, B-4](#)

### WEP

- indication in product model number [1-2](#)
- keys
  - additional security features [5-16 to 5-17](#)
  - defined [5-11, E-2](#)
  - size of [5-11, E-2](#)
- parameter [5-8, 5-20, 5-22, 5-31](#)
- status of [7-6](#)

WEP key hashing [5-17](#)

### WEP Keys

- button [5-20, 5-21](#)
- window [5-20](#)

WEP option [E-11](#)

### Wi-Fi Protected Access (WPA)

See WPA

windows, used in document [1-4](#)

### Windows CE

- finding version [3-2](#)
- supported devices [2-4](#)

### Windows CE .NET

- associating to access point [E-15](#)
- configuring client adapter through [E-8 to E-15](#)
- enabling EAP-TLS authentication [E-12](#)

- enabling PEAP authentication [E-13 to E-15](#)

External Settings profile option [4-3](#)

guidelines for entering static WEP keys [E-11](#)

making a configuration decision [3-6 to 3-7](#)

preparing to configure client adapter [E-4](#)

wireless infrastructure [1-8](#)

### Wireless Login Module (WLM)

- buttons [1-6](#)
- deleting icon [8-9](#)
- described [1-4](#)
- exiting [8-8](#)
- finding version [8-7, 8-9](#)
- installing [3-2 to 3-5](#)
- opening [8-8](#)
- uninstalling [8-8](#)
- upgrading [8-6 to 8-7](#)

Wireless Login Module window [6-2](#)

### workstation

- defined [1-2](#)
- in wireless infrastructure [1-8](#)

World Mode parameter [5-6](#)

### WPA

- described [5-14, E-4](#)
- option [E-11](#)
- requirements [5-22, 5-24](#)
- software required [5-14, E-4](#)

### WPA-PSK

- described [E-4](#)
- entering pre-shared key [E-11](#)
- option [E-11](#)

WPA TKIP [7-6](#)

---

## X

X button, function of [1-6](#)

