



## **Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows**

### **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-1394-04



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.

CCIP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0208R)

*Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows*

Copyright © 2001-2002, Cisco Systems, Inc.

All rights reserved.



<b>Preface</b>	<b>xi</b>
<b>Audience</b>	<b>xii</b>
<b>Purpose</b>	<b>xii</b>
<b>Organization</b>	<b>xii</b>
<b>Conventions</b>	<b>xiii</b>
<b>Related Publications</b>	<b>xv</b>
<b>Obtaining Documentation</b>	<b>xv</b>
<b>World Wide Web</b>	<b>xv</b>
<b>Documentation CD-ROM</b>	<b>xv</b>
<b>Ordering Documentation</b>	<b>xvi</b>
<b>Documentation Feedback</b>	<b>xvi</b>
<b>Obtaining Technical Assistance</b>	<b>xvi</b>
<b>Cisco.com</b>	<b>xvi</b>
<b>Technical Assistance Center</b>	<b>xvii</b>
<b>Cisco TAC Web Site</b>	<b>xvii</b>
<b>Cisco TAC Escalation Center</b>	<b>xviii</b>

---

**CHAPTER 1**

<b>Product Overview</b>	<b>1-1</b>
<b>Introduction to the Client Adapters</b>	<b>1-2</b>
<b>Terminology</b>	<b>1-3</b>
<b>Hardware Components</b>	<b>1-3</b>
<b>Radio</b>	<b>1-3</b>
<b>Radio Antenna</b>	<b>1-4</b>
<b>LEDs</b>	<b>1-4</b>
<b>Software Components</b>	<b>1-5</b>
<b>Radio Firmware</b>	<b>1-5</b>
<b>Driver</b>	<b>1-5</b>
<b>Client Utility</b>	<b>1-5</b>
<b>Overview of ACU</b>	<b>1-6</b>
<b>Buttons on the ACU Screens</b>	<b>1-7</b>
<b>Network Configurations Using the Client Adapter</b>	<b>1-7</b>
<b>Ad Hoc Wireless LAN</b>	<b>1-8</b>
<b>Wireless Infrastructure with Workstations Accessing a Wired LAN</b>	<b>1-9</b>

**CHAPTER 2**

**Preparing for Installation 2-1**

- 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**

**Installing the Client Adapter 3-1**

- Determining the Latest Versions of the Driver and ACU 3-2**
- Installing the Driver 3-3**
  - Installing the Driver for Windows 95 3-4**
    - Windows 95 Version A 3-5**
    - Windows 95 Version B 3-6**
  - Installing the Driver for Windows 98 3-8**
  - Installing the Driver for Windows NT 3-11**
  - Installing the Driver for Windows 2000 3-13**
  - Installing the Driver for Windows Millennium Edition (Me) 3-15**
  - Installing the Driver for Windows XP 3-17**
- Installing ACU 3-20**
- Verifying Installation 3-23**
- Selecting from Two Installed Client Adapters 3-24**

**CHAPTER 4**

**Using the Profile Manager 4-1**

- Overview of Profile Manager 4-2**
- Opening Profile Manager 4-2**
- Creating a New Profile 4-3**
- Selecting the Active Profile 4-4**
- Modifying a Profile 4-6**
  - Editing a Profile 4-6**
  - Setting a Profile to Default Values 4-6**
  - Renaming a Profile 4-7**
  - Deleting a Profile 4-7**

Importing and Exporting Profiles	4-7
Importing a Profile	4-7
Exporting a Profile	4-8
Denying Access to Non-Administrative Users	4-8

**CHAPTER 5**

Configuring the Client Adapter	5-1
Overview	5-2
Setting System Parameters	5-3
Setting RF Network Parameters	5-6
Setting Advanced Infrastructure Parameters	5-13
Setting Advanced Ad Hoc Parameters	5-17
Setting Network Security Parameters	5-20
Setting the Allow Association To Mixed Cells Parameter	5-21
Overview of Security Features	5-21
Static WEP Keys	5-22
EAP (with Static or Dynamic WEP Keys)	5-22
Additional WEP Key Security Features	5-25
Synchronizing Security Features	5-26
Using Static WEP	5-28
Entering a New Static WEP Key	5-28
Overwriting an Existing Static WEP Key	5-30
Disabling Static WEP	5-30
Enabling LEAP	5-31
Enabling Host-Based EAP	5-34
Enabling EAP-TLS	5-36
Enabling EAP-MD5	5-37
Enabling PEAP	5-38
Enabling EAP-SIM	5-40
Disabling LEAP or Host-Based EAP	5-41
Disabling LEAP	5-41
Disabling Host-Based EAP	5-41

**CHAPTER 6**

Using EAP Authentication	6-1
Overview	6-2
Using LEAP	6-2

- Using LEAP with the Windows Username and Password 6-3
  - After Profile Selection or Card Insertion 6-3
  - After a Reboot or Logon 6-3
  - After Your LEAP Credentials Expire 6-4
- Using LEAP with an Automatically Prompted Login 6-5
  - After Profile Selection or Card Insertion 6-5
  - After a Reboot or Logon 6-6
  - After Your LEAP Credentials Expire 6-7
- Using LEAP with a Manually Prompted Login 6-8
  - After Profile Selection 6-8
  - After a Reboot, Logon, or Card Insertion 6-9
  - After Your LEAP Credentials Expire 6-10
- Using LEAP with a Saved Username and Password 6-11
  - After Profile Selection or Card Insertion 6-11
  - After a Reboot or Logon 6-11
  - After Your LEAP Credentials Expire 6-11
- Using EAP-TLS 6-12
  - After Profile Selection or Card Insertion 6-12
  - After a Reboot or Logon 6-12
- Using EAP-MD5 6-13
- Using PEAP 6-13
  - After Profile Selection, Card Insertion, Reboot, or Logon 6-13
    - Windows NT or 2000 Domain Databases or LDAP Databases Only 6-14
    - OTP Databases Only 6-15
  - After Your Password Expires (Windows NT or 2000 Domain Databases Only) 6-16
  - After Your PIN Expires (OTP Databases Only) 6-16
- Using EAP-SIM 6-17
  - If You Are Prompted for the PIN 6-17
  - If the PIN Is Stored on the Computer 6-19

**CHAPTER 7**

- Performing Diagnostics 7-1
  - Overview of ACU Diagnostic Tools 7-2
  - Setting Parameters that Affect ACU Diagnostic Tools 7-2
  - Viewing the Current Status of Your Client Adapter 7-4
  - Viewing Statistics for Your Client Adapter 7-12
  - Viewing the Link Status Meter 7-16
  - Running an RF Link Test 7-18

**CHAPTER 8**

<b>Routine Procedures</b>	<b>8-1</b>
<b>Inserting and Removing a Client Adapter</b>	<b>8-2</b>
<b>Inserting a Client Adapter</b>	<b>8-2</b>
<b>Inserting a PC Card or PC-Cardbus Card</b>	<b>8-2</b>
<b>Inserting a PCI Card</b>	<b>8-3</b>
<b>Removing a Client Adapter</b>	<b>8-4</b>
<b>Removing a PC Card or PC-Cardbus Card</b>	<b>8-4</b>
<b>Removing a PCI Card</b>	<b>8-4</b>
<b>Upgrading the Firmware</b>	<b>8-5</b>
<b>Determining the Firmware Version</b>	<b>8-5</b>
<b>Loading New Firmware</b>	<b>8-6</b>
<b>Driver Procedures</b>	<b>8-8</b>
<b>Determining the Driver Version</b>	<b>8-8</b>
<b>Upgrading the Driver</b>	<b>8-9</b>
<b>Upgrading the Driver for Windows 95 and 98</b>	<b>8-9</b>
<b>Upgrading the Driver for Windows NT</b>	<b>8-10</b>
<b>Upgrading the Driver for Windows 2000</b>	<b>8-11</b>
<b>Upgrading the Driver for Windows Me</b>	<b>8-12</b>
<b>Upgrading the Driver for Windows XP</b>	<b>8-13</b>
<b>Uninstalling the Driver</b>	<b>8-14</b>
<b>Uninstalling the 6.10 Driver</b>	<b>8-14</b>
<b>Uninstalling a Driver Other Than the 6.10 Driver</b>	<b>8-17</b>
<b>ACU Procedures</b>	<b>8-19</b>
<b>Opening ACU</b>	<b>8-19</b>
<b>Exiting ACU</b>	<b>8-20</b>
<b>Modifying ACU Installation Settings</b>	<b>8-20</b>
<b>Determining the Version of ACU</b>	<b>8-23</b>
<b>Upgrading ACU</b>	<b>8-24</b>
<b>Uninstalling ACU</b>	<b>8-27</b>
<b>Uninstalling ACU Versions Prior to 4.13</b>	<b>8-27</b>
<b>Uninstalling ACU Version 4.13 or Greater</b>	<b>8-27</b>
<b>Deleting the ACU Icon from the Desktop</b>	<b>8-28</b>
<b>Restarting the Client Adapter</b>	<b>8-28</b>
<b>Turning Your Client Adapter's Radio On or Off</b>	<b>8-29</b>
<b>From the Windows System Tray</b>	<b>8-29</b>
<b>From ACU</b>	<b>8-29</b>
<b>Uninstalling Microsoft Hot Fixes</b>	<b>8-29</b>

**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 Installing the Driver 9-3**
  - Problems Installing ACU 9-3**
  - Client Adapter Recognition Problems 9-4**
  - Resolving Resource Conflicts 9-4**
    - Resolving Resource Conflicts in Windows 95, 98, and Me 9-4**
    - Resolving Resource Conflicts in Windows NT 9-5**
    - Resolving Resource Conflicts in Windows 2000 9-5**
    - Resolving Resource Conflicts in Windows XP 9-6**
  - Problems Associating to an Access Point 9-7**
  - Problems Authenticating to an Access Point 9-7**
  - Problems Connecting to the Network 9-7**
  - Losing Association Upon Resuming from Suspend Mode (Windows NT and Mini PCI Card Only) 9-7**
  - Parameters Missing from ACU Properties Screens 9-8**
  - LEAP Login Screen Appears Before Windows Login Screen 9-8**
  - Microsoft Hot Fixes 9-8**
- Error Messages 9-9**
  - General Error Messages 9-9**
  - LEAP Authentication Error Messages 9-12**
  - PEAP Authentication Error Messages 9-15**
    - For All PEAP-Supported Databases 9-15**
    - For Windows NT or 2000 Domain Databases 9-15**
    - For All OTP Databases 9-16**
    - For OTP Databases Using Secure Computing SofToken Version 1.3 9-17**
    - For OTP Databases Using Secure Computing SofToken II Version 2.0 9-18**
    - For OTP Databases Using RSA SecurID Version 2.5 9-19**
  - EAP-SIM Authentication Error Messages 9-20**
- Getting Help 9-25**

**APPENDIX A**

**Technical Specifications A-1**

**APPENDIX B**

**Translated Safety Warnings B-1**

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



**APPENDIX C**

<b>Declarations of Conformity and Regulatory Information</b>	<b>C-1</b>
<b>Manufacturer's Federal Communication Commission Declaration of Conformity Statement</b>	<b>C-2</b>
<b>Department of Communications – Canada</b>	<b>C-3</b>
<b>Canadian Compliance Statement</b>	<b>C-3</b>
<b>European Community, Switzerland, Norway, Iceland, and Liechtenstein</b>	<b>C-4</b>
<b>Declaration of Conformity with Regard to the R&amp;TTE Directive 1999/5/EC</b>	<b>C-4</b>
<b>2.4-GHz Client Adapters</b>	<b>C-5</b>
<b>5-GHz Client Adapters</b>	<b>C-6</b>
<b>Declaration of Conformity for RF Exposure</b>	<b>C-6</b>
<b>Guidelines for Operating Cisco Aironet Wireless LAN Client Adapters in Japan</b>	<b>C-6</b>
<b>Japanese Translation</b>	<b>C-6</b>
<b>English Translation</b>	<b>C-7</b>

**APPENDIX D**

<b>Channels, Power Levels, and Antenna Gains</b>	<b>D-1</b>
<b>Channels</b>	<b>D-2</b>
<b>For IEEE 802.11a</b>	<b>D-2</b>
<b>For IEEE 802.11b</b>	<b>D-3</b>
<b>Maximum Power Levels and Antenna Gains</b>	<b>D-4</b>
<b>For IEEE 802.11a</b>	<b>D-4</b>
<b>For IEEE 802.11b</b>	<b>D-4</b>

**APPENDIX E**

<b>Configuring the Client Adapter through Windows XP</b>	<b>E-1</b>
<b>Overview</b>	<b>E-2</b>
<b>Overview of Security Features</b>	<b>E-2</b>
<b>Static WEP Keys</b>	<b>E-2</b>
<b>EAP (with Static or Dynamic WEP Keys)</b>	<b>E-2</b>
<b>Configuring the Client Adapter</b>	<b>E-5</b>
<b>Enabling EAP-TLS Authentication</b>	<b>E-8</b>
<b>Enabling EAP-MD5 Authentication</b>	<b>E-11</b>
<b>Enabling PEAP Authentication</b>	<b>E-13</b>
<b>Enabling EAP-SIM Authentication</b>	<b>E-16</b>
<b>Using Windows XP to Associate to an Access Point</b>	<b>E-18</b>
<b>Viewing the Current Status of Your Client Adapter</b>	<b>E-19</b>

---

**APPENDIX F**

- Performing a Site Survey F-1**
  - Overview F-2**
    - Guidelines F-2**
    - Additional Information F-2**
  - Specifying Signal Strength Units F-3**
  - Using Passive Mode F-3**
  - 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 Wireless LAN Client Adapters Installation and Configuration Guide for Windows*, 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 xii](#)
- [Purpose, page xii](#)
- [Organization, page xii](#)
- [Conventions, page xiii](#)
- [Related Publications, page xv](#)
- [Obtaining Documentation, page xv](#)
- [Obtaining Technical Assistance, page xvi](#)

# Audience

This publication is for the person responsible for installing, configuring, and maintaining a Cisco Aironet Wireless LAN Client Adapter on a computer running Windows 95, 98, NT, 2000, Me, or XP. This person should be familiar with computing devices and with network terms and concepts.

# Purpose

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

# 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 the Aironet Client Utility (ACU) as well as setting basic configuration parameters.
- [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 adapter, such as upgrading client software and restarting the adapter.
- [Chapter 9, “Troubleshooting,”](#) provides information for diagnosing and correcting common problems 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 802.11a and 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 XP,”](#) explains how to configure and use the client adapter with Windows XP.
- [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).)**

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

## Related Publications

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

- *Release Notes for Cisco Aironet Client Utilities for Windows*
- *Release Notes for Cisco Aironet Client Adapter Drivers for Windows*
- *Release Notes for Cisco Aironet Client Adapter Firmware*

For more information about related Cisco Aironet products, refer to the following publications:

- *Cisco Aironet Access Point Hardware Installation Guide (340 and 350 Series)*
- *Cisco Aironet Access Point Software Configuration Guide (340 and 350 Series)*
- *Release Notes for Cisco Aironet Access Points*
- *Cisco Aironet 1200 Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1200 Series Access Point Software Configuration Guide*
- *Release Notes for Cisco Aironet 1200 Series Access Points*

## Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

### World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at 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 is shipped separately from the CD that was included 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.

## Ordering Documentation

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/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM 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. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom 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: Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

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

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that 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

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco Technical Assistance Center (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 Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- 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.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

You can use the Cisco TAC Web Site 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 Web Site, 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 Web Site. The Cisco TAC Web Site requires 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://www.cisco.com/register/>

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

## 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.



# Product Overview

---

This chapter describes the Cisco Aironet 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 1-5](#)
- [Network Configurations Using the Client Adapter, page 1-7](#)

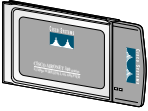

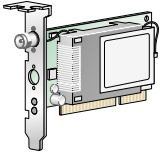
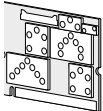
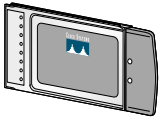
# Introduction to the Client Adapters

The Cisco Aironet Wireless LAN Client Adapters are 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 the five client adapters described in [Table 1-1](#).

**Table 1-1 Client Adapter Types**

Client Adapter	Model Number	Description	Illustration
PC card	AIR-PCM3xx	An IEEE 802.11b-compliant 11-Mbps 2.4-GHz PCMCIA card radio module that can be inserted into any device equipped with an <i>external</i> Type II or Type III PC card slot. Host devices can include laptops, notebook computers, personal digital assistants, and handheld or portable devices. The PC card is available in the 340 and 350 series.	 47519
LM card	AIR-LMC3xx	An IEEE 802.11b-compliant 11-Mbps 2.4-GHz PCMCIA card radio module that is usually preinstalled in a device equipped with an <i>internal</i> Type II or Type III PC card slot. Host devices usually include handheld or portable devices. The LM card is available in the 340 and 350 series.	 47893
PCI card	AIR-PCI3xx	An IEEE 802.11b-compliant 11-Mbps 2.4-GHz client adapter card radio module that can be inserted into any device equipped with an empty PCI expansion slot, such as a desktop personal computer. The PCI card is available in the 340 and 350 series.	 65189
Mini PCI card	AIR-MPI350	An IEEE 802.11b-compliant 11-Mbps 2.4-GHz client adapter card radio module that is preinstalled in a device equipped with an <i>internal</i> Type IIIA mini PCI card slot, such as a laptop computer. The mini PCI card is available only in the 350 series.	 65190
PC-Cardbus card	AIR-CB20A	An IEEE 802.11a-compliant 54-Mbps 5-GHz client adapter card radio module with a Cardbus interface that can be inserted into any device equipped with an <i>external</i> Type II or Type III Cardbus slot. Host devices can include laptops, notebook computers, personal digital assistants, and handheld or portable devices.	 74795

**Note**

In the first three product model numbers, the first *x* represents the client adapter series (340 or 350), and the second *x* indicates the wired equivalent privacy (WEP) level of the card, where 0 = no WEP capability, 1 = 40-bit WEP, and 2 = 128-bit WEP. If the last two product model numbers contain K9, the card is 128-bit WEP capable.

## Terminology

The following terms are used throughout this document:

- **client adapter**—Refers to all five types of adapters.
- **PC card, LM card, PCI card, mini PCI card, or PC-Cardbus card**—Refers to a specific adapter.
- **workstation (or station)**—Refers to a computing device with an installed client adapter.
- **infrastructure device**—Refers to a device that connects client adapters to a wired LAN, such as an access point, bridge, or base station. Throughout this document, *access point* is used to represent infrastructure devices in general.

## Hardware Components

The client adapter has three major hardware components: a radio, a radio antenna, and two LEDs.

### Radio

Different radios are used for the 2.4-GHz and 5-GHz client adapters:

- The Cisco Aironet 340 and 350 series PC, LM, PCI, and mini PCI 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 340 series 30-milliwatt (mW) radio and the 350 series 100-mW radio transmit data over a half-duplex radio channel operating at up to 11 Mbps. These cards interoperate with other IEEE 802.11b-compliant client devices in ad hoc (or *peer-to-peer*) mode or with Cisco Aironet 340, 350, 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.

- The Cisco Aironet AIR-CB20A PC-Cardbus card is an IEEE 802.11a-compliant client adapter. It contains an orthogonal frequency division multiplexing (OFDM) radio that operates in the Unlicensed National Information Infrastructure (UNII) 1 and UNII 2 license-free bands located in the lower 5-GHz portion of the radio frequency spectrum. The 20-mW radio transmits data over a half-duplex radio channel operating at up to 54 Mbps. This card interoperates with other IEEE 802.11a-compliant client devices in ad hoc mode or with Cisco Aironet 1200 Series Access Points (with a 5-GHz radio) and other IEEE 802.11a-compliant infrastructure devices in infrastructure mode. It is approved for indoor use only except in the United States, which allows for outdoor use on channels 52 through 64.

## 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.
- PCI cards are shipped with a 2-dBi dipole antenna that attaches to the card's antenna connector. However, other types of antennas may be used. PCI cards can be operated through the primary (or right) antenna port only.
- Mini PCI cards are designed to be used with either one or two antennas, which connect to the card's two antenna connectors. If two antennas are used, the radio automatically selects the antenna that presents the best RF signal. If only one antenna is used, the radio finds and uses it regardless of which connector it is plugged into.
- PC-Cardbus cards have an integrated, permanently attached non-diversity antenna that contains two antenna ports, one for transmitting and one for receiving. The card cannot switch and sample between the ports. The antenna is housed within the section of the card that hangs out of the Cardbus slot when the card is installed.

**Note**

---

Refer to the Antenna Mode (Transmit and Receive) parameters in [Table 5-4](#) and [Table 5-5](#) for information on setting the client adapter's antenna mode.

---

**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 with Regard to the R&TTE Directive 1999/5/EC”](#) section on page C-4 and the [“Maximum Power Levels and Antenna Gains”](#) section on page D-4.

---

## LEDs

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

**Note**

---

Mini PCI cards do not have LEDs.

---

# Software Components

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

## 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**

---

Cisco recommends using the most current version of radio firmware. [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 a computer running a Windows operating system and the client adapter, thereby enabling Windows and the applications it runs to communicate with the adapter. The driver is provided on the CD that shipped with the client adapter and must be installed before the adapter can be used. [Chapter 3](#) provides instructions for installing the driver.



**Note**

---

The CD has the latest version of the driver available at the time of pressing; however, a more recent version of the driver may be available from Cisco.com. Cisco recommends installing the most current version of the driver. [Chapter 3](#) provides instructions for installing the driver from either location.

---

## Client Utility

The client utility, which is entitled Aironet Client Utility (ACU), is an optional application that interacts with the radio firmware to adjust client adapter settings and display information about the adapter. ACU is provided on the CD that shipped with the client adapter. If you plan to use ACU, it should be installed before the adapter is used. [Chapter 3](#) provides instructions for installing ACU.



**Note**

---

The CD has the latest version of ACU available at the time of pressing; however, a more recent version of ACU may be available from Cisco.com. Cisco recommends installing the most current version of ACU. [Chapter 3](#) provides instructions for installing ACU from either location.

---



**Note**

---

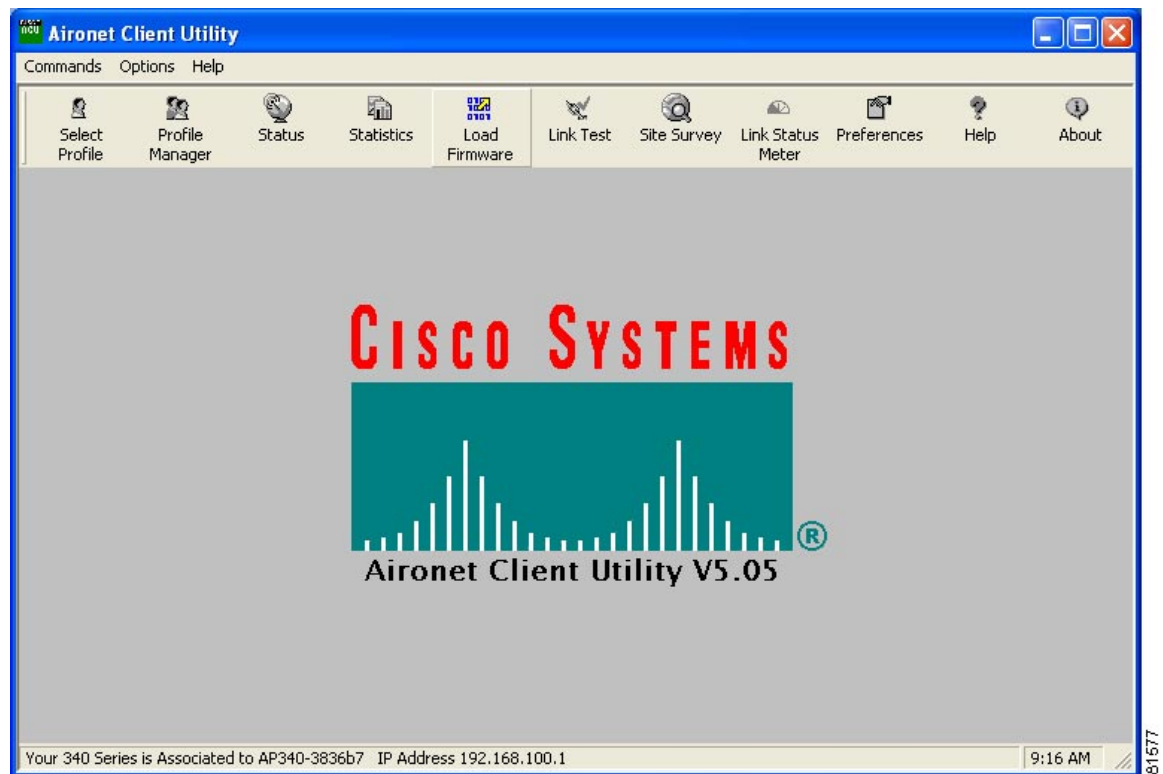
If your computer is running Windows XP, you can configure your client adapter through the Windows operating system instead of through ACU. Refer to [Appendix E](#) for information. However, ACU is recommended for configuring the client adapter.

---

## Overview of ACU

The Aironet Client Utility screen (see [Figure 1-1](#)) is ACU's primary screen.

**Figure 1-1 Aironet Client Utility Screen**



The status bar at the bottom of the Aironet Client Utility screen reflects the current state of your client adapter. Possible states include Associated, Not Associated, Not Inserted, Being Flashed with New Firmware, and Unable To Read Status from the Card.

If your client adapter is associated to an access point, the status bar shows the name of the access point, provided it was configured with one. If shown, the access point name is limited to 16 characters by the client adapter's radio firmware. The status bar also shows either the IP address or the MAC address of the access point to which the client adapter is associated. The information shown in the status bar is updated once per second.

The right side of the status bar shows the current time of day. If you set the clock to display seconds in the Aironet Client Utility Preferences screen, the time includes seconds in addition to hours and minutes.



### Note

To enable the clock to display seconds, open ACU, click the **Preferences** icon or select **Preferences** from the Options drop-down menu, select the **Display Seconds on Clock** check box, and click **OK**.



## Buttons on the ACU Screens

The buttons on the ACU screens are used to perform specific functions. [Table 1-2](#) describes the most common buttons.

**Table 1-2 Buttons on the ACU Screens**

Button	Description
Apply	Saves any changes without exiting the screen
Cancel	Exits the screen without saving any changes
Defaults	Displays the default value of each parameter
Help	Provides information on the screen and its parameters
OK	Saves any changes and exits the screen
Start	Initiates a test
Stop	Stops a test that is running

## 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.



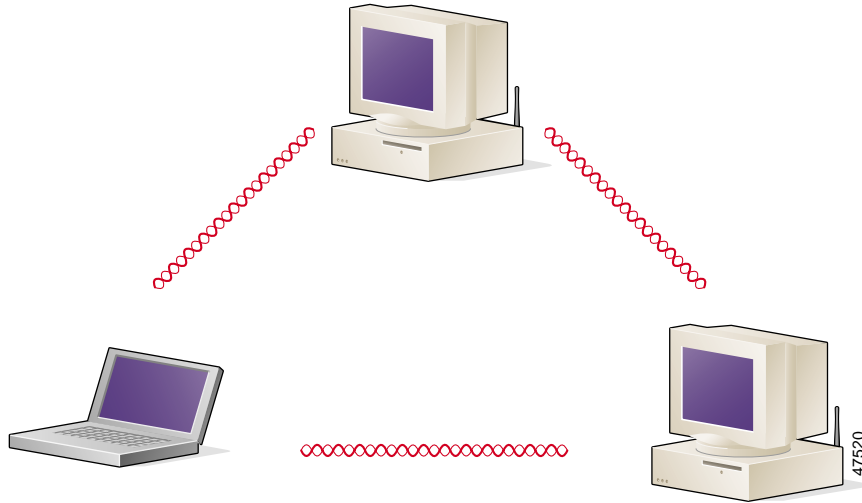
**Note**

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

**Figure 1-2 Ad Hoc Wireless LAN**

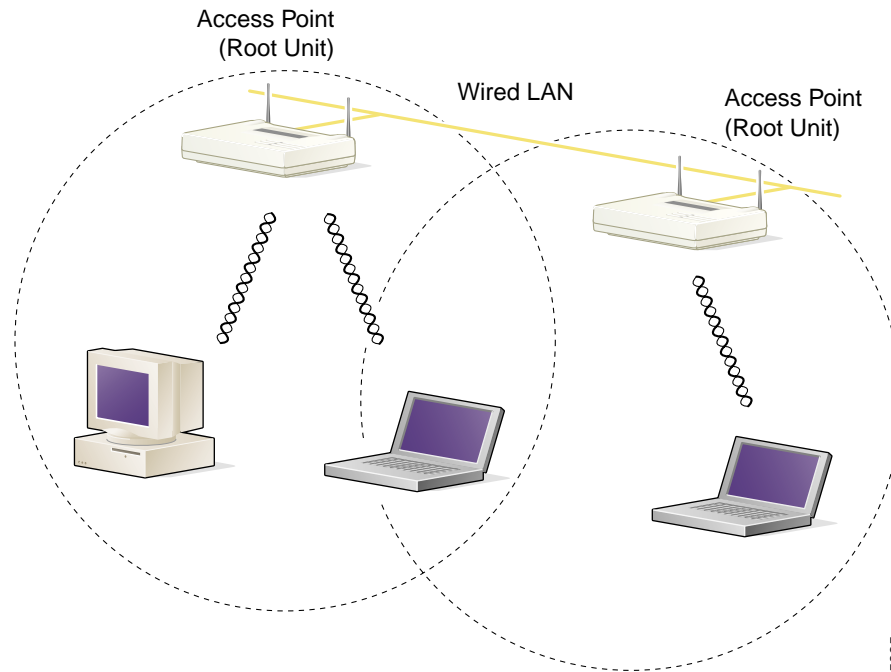


## Wireless Infrastructure with Workstations Accessing a Wired LAN

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, dipole 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:

- Standard 2-dBi dipole antenna (PCI cards only)
- *Quick Start Guide: Cisco Aironet Wireless LAN Client Adapters*
- Cisco Aironet Wireless LAN Client Adapters CD (for 2.4-GHz client adapters) or Cisco Aironet 5-GHz 54-Mbps Wireless Adapters CD (for 5-GHz client adapters)
- Cisco product registration card

# System Requirements

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

- One of the following computing devices running Windows 95, 98, NT, 2000, Me, or XP:
  - Laptop, notebook, or portable or handheld device equipped with a Type II or Type III PC card slot or Cardbus slot
  - Desktop personal computer equipped with an empty PCI expansion slot
  - Handheld or portable device with an embedded LM card
  - Laptop or other computing device with an embedded mini PCI card




---

**Note** Cisco recommends using a display with a minimum resolution of 800 x 600.

---




---

**Note** All drivers and supporting software (Card and Socket Services) for the PC card slot or Cardbus slot must be loaded and configured.

---

- Windows NT Service Pack 3 or greater if your computer is running Windows NT
- A Phillips screwdriver (for PCI cards)
- Windows 2000 (with Service Pack 3 or greater and the Windows 2000 Wireless 802.1X hot fix) or Windows XP, if your wireless network uses EAP-TLS, EAP-MD5, PEAP, or EAP-SIM authentication
- If your wireless network uses PEAP authentication with a One-Time Password (OTP) user database:
  - SofToken version 1.3, 2.0, or greater from Secure Computing; SecurID version 2.5 from RSA; or hardware token from OTP vendors
  - Your software token PIN or hardware token password
- If your wireless network uses EAP-SIM authentication:
  - PCSC-compliant smartcard reader installed in your computer's Type II or Type III PC card slot
  - Gemplus SIM+ smartcard inserted in the reader
  - The SIM card's PIN
- The following information from your system administrator:
  - The logical name for your workstation (also referred to as *client name*)
  - The protocols necessary to bind to the client adapter
  - The case-sensitive service set identifier (SSID) for your RF network
  - If your computer is not connected to a DHCP server, the IP address, subnet mask, and default gateway address of your computer
  - The Wired Equivalent Privacy (WEP) keys of the access points with which your client adapter will communicate, if your wireless network uses static WEP for security
  - The username and password for your network account



# 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**

---

As a rule, 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 the client utility.

The following topics are covered in this chapter:

- [Determining the Latest Versions of the Driver and ACU, page 3-2](#)
- [Installing the Driver, page 3-3](#)
- [Installing ACU, page 3-20](#)
- [Verifying Installation, page 3-23](#)
- [Selecting from Two Installed Client Adapters, page 3-24](#)

## Determining the Latest Versions of the Driver and ACU

The driver and the Aironet Client Utility (ACU) are provided on the CD that shipped with the client adapter; however, a more recent version of each may be available from Cisco.com. Cisco recommends installing the most current versions of the driver and ACU.


**Note**

Although the client adapter is shipped with the firmware installed, you may want to check Cisco.com to see if a more recent version is available. [Chapter 8](#) provides instructions for determining the version of your client adapter's firmware and upgrading it if necessary.


**Note**

Mini PCI cards, along with their driver and ACU, are generally preinstalled inside of computers. Therefore, the mini PCI software is not provided on the CD, and you do not need to follow the instructions in this chapter to install the card's driver and ACU. However, if you want to upgrade the mini PCI card's driver and ACU, refer to the instructions provided in [Chapter 8](#).

Follow the steps below to determine the most recent versions of the driver and ACU on your CD and Cisco.com.

- Step 1** To determine the version of the driver and ACU on the CD, open the FileList.txt file on the CD's root directory. This file lists the version numbers for all of the software files provided on the CD.


**Note**

If the FileList.txt file is not present on the root directory, your CD is obsolete, and more recent versions of the software are available on Cisco.com. Go to the ["Installing the Driver" section on page 3-3](#).

- Step 2** To determine the latest driver and ACU versions available on Cisco.com, follow the steps below:
- a. Use your computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - b. Click the link for Cisco Aironet Wireless LAN Client Adapters.
  - c. Perform one of the following:
    - If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as CB20A or 350 series). Find the bundled file with the greatest version number for your specific client adapter type (such as CB or MPI). The version numbers of the driver and ACU are provided in the description below the filename. These are the latest available versions on Cisco.com. Go to [Step 3](#).
    - If you want to select the client adapter's software files individually, go to [Step d](#).

- d. Find the section for Windows drivers and click the link for your computer's operating system. Find the driver file with the greatest version number for your specific client adapter type (such as CB or MPI). This is the latest available version on Cisco.com.



---

**Note** The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, the drivers for mini PCI cards are labeled *MPI*, and the drivers for PC-Cardbus cards are labeled *CB*.

---

- e. Return to the previous page and click the link for the Windows utility. Find the ACU file with the greatest version number. This is the latest available version on Cisco.com.

**Step 3** Go to the [“Installing the Driver”](#) section below. If the driver version on Cisco.com is greater than the version on the CD, follow the instructions for installing the driver from Cisco.com.

**Step 4** After you install the driver, go to the [“Installing ACU”](#) section on page 3-20. If the ACU version on Cisco.com is greater than the version on the CD, follow the instructions for installing ACU from Cisco.com.

---

## Installing the Driver



---

**Note** Cisco recommends that you install the driver before you install ACU.

---



---

**Note** If a 2.4-GHz client adapter is already installed in your computer and you want to also install a 5-GHz client adapter, make sure you reboot your computer immediately after installing the second adapter. Otherwise, the client adapter may not be able to connect to the network.

---



---

**Note** This procedure is meant to be used the first time a driver for a specific client adapter type (such as a 350 series PC card or a 5-GHz PC-Cardbus card) is installed on a computer running Windows 95, 98, NT, 2000, Me, or XP. If a Cisco Aironet client adapter driver is already installed on your computer for your client adapter type, follow the instructions in [Chapter 8](#) to upgrade to a new driver. However, if the 6.10 driver is installed on your Windows 95, 98, NT, or 2000 computer, you must remove this driver before you can install a more recent driver. Refer to the [“Uninstalling the 6.10 Driver”](#) section on page 8-14 for instructions.

---

The driver you use for your client adapter depends on which operating system your computer is running and your client adapter type. This section provides instructions for installing the correct driver for your operating system. Use [Table 3-1](#) to quickly locate the installation instructions for your specific operating system.

**Table 3-1 Locating Driver Installation Instructions**

Operating System	Page Number
Windows 95	3-4
Windows 98	3-8
Windows NT	3-11
Windows 2000	3-13
Windows Millennium Edition (Me)	3-15
Windows XP	3-17

**Note**

Before you begin the driver installation process, make sure you have the installation disks for your computer's operating system nearby. Some operating system files may be needed to complete the driver installation.

## Installing the Driver for Windows 95

**Note**

Windows 95 is supported only by 2.4-GHz client adapters. Therefore, a Windows 95 driver is not available for the 5-GHz client adapter.

**Note**


Windows 95 limits your computer's network connections to four. If you try to install a client adapter when four network devices (such as a PCMCIA Ethernet card, dial-up adapter, VPN adapter, docking station Ethernet card, etc.) are already connected to your computer, the new adapter cannot establish a network connection.

The driver installation instructions vary for Windows 95 Version A and Version B. You can determine which version your computer is running by double-clicking **My Computer**, **Control Panel**, **System**, and **General**. The version of your computer's operating system is located under the System heading. If you have Windows 95 Version B, the version number ends with the letter *B*.

- For Windows 95 Version A driver installation instructions, go to the [“Windows 95 Version A” section on page 3-5](#).
- For Windows 95 Version B driver installation instructions, go to the [“Windows 95 Version B” section on page 3-6](#).

## Windows 95 Version A

If your computer's operating system is Windows 95 Version A, follow these steps.

- 
- Step 1** If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to [Step 2](#).
- a. Use the computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - b. Click the link for Cisco Aironet Wireless LAN Client Adapters.
  - c. Perform one of the following:
    - If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as 340 or 350 series). Select the latest bundled file for Windows 95 and your specific client adapter type (such as PCMCIA or MPI).
    - If you want to select the client adapter's software files individually, find the section for Windows drivers and click the link for Windows 95. Select the driver file with the greatest version number for your specific client adapter type (such as PCMCIA or MPI).
-  **Note** The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, and the drivers for mini PCI cards are labeled *MPI*.
- 
- d. Read and accept the terms and conditions of the Software License Agreement.
  - e. Select the file again to download it.
  - f. Save the file to a floppy disk or to your computer's hard drive.
  - g. Find the file using Windows Explorer, double-click it, and extract its files to a folder.
  - h. Go to [Step 2](#).
- Step 2** Follow the instructions in [Chapter 8](#) to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards and PCI cards.
- Step 3** After you insert the client adapter into your computing device, Windows automatically detects it and opens the New Hardware Found window.
- Step 4** Select **Driver from disk provided by hardware manufacturer** and click **OK**.
- Step 5** Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.
- Step 6** In the Install From Disk window, enter the path to where the driver is located (CD, floppy disk, or hard drive). If you are installing the driver from the CD and your CD-ROM drive is drive D, the path should be D:\Win95.
- Step 7** Click **OK**.

- Step 8** If you are prompted to insert the Windows 95 operating system disk, click **OK** and do one of the following:
- If the Windows 95 operating system files are installed on your computer, they are usually located in the C:\Windows\Options\Cabs folder. Type **C:\Windows\Options\Cabs** in the Copy files from dialog box. Click **OK** to copy the required files.
  - If Windows 95 prompts for the Windows 95 operating system CD, insert this CD into your computer's CD-ROM drive. If your CD-ROM drive is drive D, the path in the dialog box should be D:\Win95. Click **OK** to copy the required files.
- Step 9** After the files are copied, remove any disks from your computer.
- Step 10** Double-click **My Computer**, **Control Panel**, and **Network**.
- Step 11** Select the Cisco Systems Wireless LAN Adapter and click **Properties**.
- Step 12** In the client adapter Properties window, click the **Advanced** tab.
- Step 13** Select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.
- Step 14** Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.
- Step 15** Click **OK**.
- Step 16** If you are prompted to restart your computer, click **Yes**.
- Step 17** If your computer is not connected to a DHCP server and you plan to use TCP/IP, double-click **My Computer**, **Control Panel**, and **Network**. Select **TCP/IP > Cisco Systems Wireless LAN Adapter**. Click the **Properties** button, select **Specify an IP address**, and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK** twice. When prompted to restart your computer, click **Yes**.




---

**Note** On Windows 95, TCP/IP is not installed by default.

---

The driver installation is complete.

---

## Windows 95 Version B

If your computer's operating system is Windows 95 Version B, follow these steps.

- Step 1** If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to [Step 2](#).
- a. Use the computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - b. Click the link for Cisco Aironet Wireless LAN Client Adapters.



- c. Perform one of the following:
  - If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as 340 or 350 series). Select the latest bundled file for Windows 95 and your specific client adapter type (such as PCMCIA or MPI).
  - If you want to select the client adapter's software files individually, find the section for Windows drivers and click the link for Windows 95. Select the driver file with the greatest version number for your specific client adapter type (such as PCMCIA or MPI).


**Note**

---

The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, and the drivers for mini PCI cards are labeled *MPI*.

---

- d. Read and accept the terms and conditions of the Software License Agreement.
  - e. Select the file again to download it.
  - f. Save the file to a floppy disk or to your computer's hard drive.
  - g. Find the file using Windows Explorer, double-click it, and extract its files to a folder.
  - h. Go to [Step 2](#).
- Step 2** Follow the instructions in [Chapter 8](#) to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards and PCI cards.
- Step 3** After you insert the client adapter into your computing device, Windows automatically detects it and briefly opens the New Hardware Found window.
- Step 4** Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.
- Step 5** The Update Device Driver Wizard dialog box opens and indicates that Windows will complete the installation of the client adapter. Click **Next**.
- Step 6** If the Update Device Driver Wizard indicates that Windows was unable to locate a driver for the client adapter, click **Other Locations**.
- Step 7** In the Select Other Location window, enter the path to where the driver is located (CD, floppy disk, or hard drive). If you are installing the driver from the CD and your CD-ROM drive is drive D, the path should be D:\Win95.
- Step 8** Click **OK**.
- Step 9** When the Update Device Driver Wizard indicates that it has found the driver, click **Finish**.
- Step 10** When the Insert Disk window appears prompting you to insert the Aironet Wireless LAN Adapter Installation Disk, click **OK**.
- Step 11** If a window appears indicating that the pcx50\*.sys file could not be found, enter the same path that you entered in [Step 7](#) and click **OK**.

- Step 12** If you are prompted to insert the Windows 95 operating system disk, click **OK** and do one of the following:
- If the Windows 95 operating system files are installed on your computer, they are usually located in the C:\Windows\Options\Cabs folder. Type **C:\Windows\Options\Cabs** in the Copy files from dialog box. Click **OK** to copy the required files.
  - If Windows 95 prompts for the Windows 95 operating system CD, insert this CD into your computer's CD-ROM drive. If your CD-ROM drive is drive D, the path in the dialog box should be D:\Win95. Click **OK** to copy the required files.
- Step 13** When prompted to restart your computer, remove any disks and click **Yes**.
- Step 14** When the computer restarts, double-click **My Computer**, **Control Panel**, and **Network**.
- Step 15** Select the Cisco Systems Wireless LAN Adapter and click **Properties**.
- Step 16** In the client adapter Properties window, click the **Advanced** tab.
- Step 17** Select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.
- Step 18** Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.
- Step 19** Click **OK**.
- Step 20** If your computer is not connected to a DHCP server and you plan to use TCP/IP, double-click **My Computer**, **Control Panel**, and **Network**. Select **TCP/IP > Cisco Systems Wireless LAN Adapter**. Click the **Properties** button, select **Specify an IP address**, and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK**.
- 
-  **Note** On Windows 95, TCP/IP is not installed by default.
- 
- Step 21** In the Network window, click **OK**.
- Step 22** When prompted to restart your computer, click **Yes**.
- The driver installation is complete.
- 


## Installing the Driver for Windows 98



### Note

Windows 98 limits your computer's network connections to eight. If you try to install a client adapter when eight network devices (such as a PCMCIA Ethernet card, dial-up adapter, VPN adapter, docking station Ethernet card, etc.) are already connected to your computer, the new adapter cannot establish a network connection.

If your computer's operating system is Windows 98, follow these steps.

- Step 1** If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to [Step 2](#).
- Use the computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - Click the link for Cisco Aironet Wireless LAN Client Adapters.
  - Perform one of the following:
    - If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as CB20A or 350 series). Select the latest bundled file for Windows 98 and your specific client adapter type (such as CB or MPI).
    - If you want to select the client adapter's software files individually, find the section for Windows drivers and click the link for Windows 98. Select the driver file with the greatest version number for your specific client adapter type (such as MPI).
-  **Note** The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, the drivers for mini PCI cards are labeled *MPI*, and the drivers for PC-Cardbus cards are labeled *CB*.
- Read and accept the terms and conditions of the Software License Agreement.
  - Select the file again to download it.
  - Save the file to a floppy disk or to your computer's hard drive.
  - Find the file using Windows Explorer, double-click it, and extract its files to a folder.
  - Go to [Step 2](#).
- Step 2** Follow the instructions in [Chapter 8](#) to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards, PC-Cardbus cards, and PCI cards.
- Step 3** After you insert the client adapter into your computing device, Windows automatically detects it, briefly opens the New Hardware Found window, and starts collecting information for a driver information database.
- The Add New Hardware Wizard dialog box opens and indicates that Windows is searching for new drivers.
- Step 4** Click **Next**. Another dialog box opens and asks what you want Windows to do.
- Step 5** Select **Display a list of all the drivers in a specific location, so you can select the driver you want** and click **Next**.
- Step 6** Select **Network adapters** from the drop-down list of devices and click **Next**.
- Step 7** Click **Have Disk**.
- Step 8** Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.

- Step 9** Enter or browse to the path where the driver is located (CD, floppy disk, or hard drive).
- If you are installing a 2.4-GHz driver from the Cisco Aironet Wireless LAN Client Adapters CD and your CD-ROM drive is drive D, the path should be D:\Win98.
  - If you are installing a 5-GHz driver from the Cisco Aironet 5-GHz 54-Mbps Wireless Adapters CD and your CD-ROM drive is drive D, the path should be D:.
- Step 10** Click **OK**.
- Step 11** Make sure the Cisco Systems Wireless LAN Adapter is selected in the Select Device screen and click **OK**. The wizard finds the installation files and displays the search results.
- Step 12** When the client adapter driver is displayed, click **Next** to copy the required files.
- Step 13** During driver installation, you may be prompted to enter a path to the Windows 98 operating system files. If so, do one of the following:
- If the Windows 98 operating system files are installed on your computer, they are usually located in the C:\Windows\Options\Cabs folder. Type **C:\Windows\Options\Cabs** in the Copy files from dialog box. Click **OK** to copy the required files.
  - If Windows 98 prompts for the Windows 98 operating system CD, insert this CD into your computer's CD-ROM drive. If your CD-ROM drive is drive D, the path in the dialog box should be D:\Win98. Click **OK** to copy the required files.
- Step 14** The Add New Hardware Wizard window opens and indicates that the installation is complete. Click **Finish**.
- Step 15** When prompted to restart your computer, remove the CD or floppy disk (if installed) and click **Yes**.
- Step 16** When the computer restarts, double-click **My Computer**, **Control Panel**, and **Network**.
- Step 17** Select the Cisco Systems Wireless LAN Adapter and click **Properties**.
- Step 18** In the client adapter Properties window, click the **Advanced** tab.
- Step 19** Select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.
- Step 20** Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.
- Step 21** Click **OK**.
- Step 22** If your computer is not connected to a DHCP server and you plan to use TCP/IP, double-click **My Computer**, **Control Panel**, and **Network**. Select **TCP/IP > Cisco Systems Wireless LAN Adapter**. Click the **Properties** button, select **Specify an IP address**, and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK**.
- Step 23** In the Network window, click **OK**.
- Step 24** When prompted to restart your computer, click **Yes**.
- The driver installation is complete.
-

## Installing the Driver for Windows NT

**Note**

Windows NT is supported only by 2.4-GHz client adapters. Therefore, a Windows NT driver is not available for the 5-GHz client adapter.

**Note**

This procedure requires that your computer has Windows NT Service Pack 3 or greater.

If your computer's operating system is Windows NT, follow these steps.

**Step 1**

If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to [Step 2](#).

- a. Use the computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
- b. Click the link for Cisco Aironet Wireless LAN Client Adapters.
- c. Perform one of the following:
  - If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as 340 or 350 series). Select the latest bundled file for Windows NT and your specific client adapter type (such as PCMCIA or MPI).
  - If you want to select the client adapter's software files individually, find the section for Windows drivers and click the link for Windows NT. Select the driver file with the greatest version number for your specific client adapter type (such as PCMCIA or MPI).

**Note**

The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, and the drivers for mini PCI cards are labeled *MPI*.

- d. Read and accept the terms and conditions of the Software License Agreement.
- e. Select the file again to download it.
- f. Save the file to a floppy disk or to your computer's hard drive.
- g. Find the file using Windows Explorer, double-click it, and extract its files to a folder.
- h. Go to [Step 2](#).

**Step 2**

Follow the instructions in [Chapter 8](#) to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards and PCI cards.

**Step 3**

After you insert the client adapter into your computer, an error message may appear indicating that at least one service or driver failed during system setup. If this message appears, click **OK**.

- Step 4** Follow the steps below to obtain an available interrupt request (IRQ):
- Select **Start > Programs > Administrative Tools > Windows NT Diagnostics**.
  - Click the **Resources** tab.
  - The used IRQs are listed in numerical order along the left side of the Resources window. Write down the number of an IRQ that is not being used. You will need this IRQ for [Step 15](#).
- Step 5** On your computer desktop, double-click **My Computer, Control Panel, and Devices**. Scroll down and select **Pcmcia**. Click **Startup**, select **Automatic**, and click **OK**.




---


**Note** For PC cards, also ensure that the Cardbus service is deselected.

---

- Step 6** Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.
- Step 7** Double-click **My Computer, Control Panel, and Network**.
- Step 8** Click the **Adapters** tab and select **Add**.
- Step 9** In the Select Network Adapter window, click **Have Disk**.
- Step 10** In the Insert Disk window, enter the path to where the driver is located (CD, floppy disk, or hard drive). If you are installing the driver from the CD and your CD-ROM drive is drive D, the path should be D:\WinNT4.
- Step 11** Click **OK**.
- Step 12** In the Select OEM Option box, select the Cisco Systems Wireless LAN Adapter and click **OK**.
- Step 13** In the Adapter Setup window, select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.
- Step 14** Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.
- Step 15** Enter an available IRQ number, which you obtained in [Step 4](#).
- Step 16** Click **OK** and **Close**.
- Step 17** The Microsoft TCP/IP Properties window should open. If it does not open, double-click **My Computer, Control Panel, and Network**. Click **Protocols, TCP/IP, and Properties**.
- Step 18** Perform one of the following:
- If your computer is connected to a DHCP server, select **Obtain an IP address from a DHCP server**. When asked if you want to enable DHCP, click **Yes** and **OK**.
  - If your computer is not connected to a DHCP server, select **Specify an IP address** and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK**.
- Step 19** When prompted to restart your computer, remove the CD or floppy disk (if installed) and click **Yes**. The driver installation is complete.
-

## Installing the Driver for Windows 2000

If your computer's operating system is Windows 2000, follow these steps.


- 
- Step 1** If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to [Step 2](#).
- a. Use the computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - b. Click the link for Cisco Aironet Wireless LAN Client Adapters.
  - c. Perform one of the following:
    - If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as CB20A or 350 series). Select the latest bundled file for Windows 2000 and your specific client adapter type (such as CB or MPI).
    - If you want to select the client adapter's software files individually, find the section for Windows drivers and click the link for Windows 2000. Select the driver file with the greatest version number for your specific client adapter type (such as CB or MPI).
-  **Note** The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, the drivers for mini PCI cards are labeled *MPI*, and the drivers for PC-Cardbus cards are labeled *CB*.
- 
- d. Read and accept the terms and conditions of the Software License Agreement.
  - e. Select the file again to download it.
  - f. Save the file to a floppy disk or to your computer's hard drive.
  - g. Find the file using Windows Explorer, double-click it, and extract its files to a folder.
  - h. Go to [Step 2](#).
- Step 2** Follow the instructions in [Chapter 8](#) to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards, PC-Cardbus cards, and PCI cards.
- Step 3** After you insert the client adapter into your computer, Windows 2000 automatically detects it and briefly opens the Found New Hardware window. The Found New Hardware Wizard window opens and indicates that the wizard will help you to install the driver.
- Step 4** Click **Next**. Another window opens and asks what you want the wizard to do.
- Step 5** Select **Display a list of the known drivers for this device so that I can choose a specific driver** and click **Next**.
- Step 6** Click **Have Disk**.
- Step 7** Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.

- Step 8** Enter or browse to the path where the driver is located (CD, floppy disk, or hard drive).
- If you are installing a 2.4-GHz driver from the Cisco Aironet Wireless LAN Client Adapters CD and your CD-ROM drive is drive D, the path should be D:\Win2000.
  - If you are installing a 5-GHz driver from the Cisco Aironet 5-GHz 54-Mbps Wireless Adapters CD and your CD-ROM drive is drive D, the path should be D:.
- Step 9** Click **OK**. The wizard finds the installation files and displays the search results.
- Step 10** When the client adapter driver is displayed, click **Next** to copy the required files.
- Step 11** When you receive a message indicating that Windows has finished the installation, click **Finish**.
- Step 12** Remove the CD or floppy disk (if installed).
- Step 13** Double-click **My Computer**, **Control Panel**, and **System**.
- Step 14** In the System Properties window, click the **Hardware** tab.
- Step 15** Click **Device Manager**.
- Step 16** In the Device Manager window, double-click **Network Adapters**.
- Step 17** Right-click the Cisco Systems Wireless LAN Adapter.
- Step 18** Click **Properties**.
- Step 19** In the client adapter Properties window, click the **Advanced** tab.
- Step 20** In the Advanced window, select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.
- Step 21** Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.
- Step 22** Click **OK**.
- Step 23** If your computer is not connected to a DHCP server and you plan to use TCP/IP, follow these steps:
- a. Double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**.
  - b. Right-click **Local Area Connection**.
  - c. Click **Properties**, **Internet Protocol (TCP/IP)**, and **Properties**.
  - d. Click **Use the following IP address** and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK**.
  - e. In the Local Area Connection Properties window, click **OK**.
- Step 24** If you are prompted to restart your computer, click **Yes**.
- The driver installation is complete.
-



## Installing the Driver for Windows Millennium Edition (Me)

The first release of Windows Me comes with driver version 6.15, which is installed automatically the first time you insert a client adapter. To upgrade to the driver on the CD that shipped with your client adapter or on Cisco.com, follow these steps.

- 
- Step 1** If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to [Step 2](#).
- a. Use the computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - b. Click the link for Cisco Aironet Wireless LAN Client Adapters.
  - c. Perform one of the following:
    - If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as CB20A or 350 series). Select the latest bundled file for Windows Me and your specific client adapter type (such as CB or MPI).
    - If you want to select the client adapter's software files individually, find the section for Windows drivers and click the link for Windows Me. Select the driver file with the greatest version number for your specific client adapter type (such as CB or MPI).
-  **Note** The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, the drivers for mini PCI cards are labeled *MPI*, and the drivers for PC-Cardbus cards are labeled *CB*.
- 
- d. Read and accept the terms and conditions of the Software License Agreement.
  - e. Select the file again to download it.
  - f. Save the file to a floppy disk or to your computer's hard drive.
  - g. Find the file using Windows Explorer, double-click it, and extract its files to a folder.
  - h. Go to [Step 2](#).
- Step 2** Follow the instructions in [Chapter 8](#) to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards, PC-Cardbus cards, and PCI cards.
- Step 3** Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.
- Step 4** Double-click **My Computer**, **Control Panel**, and **System**.
- Step 5** Click the **Device Manager** tab.
- Step 6** Double-click **Network Adapters**.
- Step 7** Select the Cisco Aironet Wireless LAN Adapter. Click **Properties**.
- Step 8** In the client adapter Properties window, click the **Driver** tab.
- Step 9** Click **Update Driver**. The Update Device Driver Wizard window appears.

- Step 10** Select **Specify the location of the driver (Advanced)** and click **Next**.
- Step 11** Select **Search for a better driver than the one your device is using now (Recommended)**.
- Step 12** Make sure the **Removable Media** check box is deselected.
- Step 13** Select the **Specify a location** check box and click **Browse**.
- Step 14** Find the location of the driver (on your CD, floppy disk, or computer's hard drive).
- If you are installing a 2.4-GHz driver from the Cisco Aironet Wireless LAN Client Adapters CD and your CD-ROM drive is drive D, the path should be D:\WinME.
  - If you are installing a 5-GHz driver from the Cisco Aironet 5-GHz 54-Mbps Wireless Adapters CD and your CD-ROM drive is drive D, the path should be D:.
- Step 15** Click **Next**.
- Step 16** When asked what you would like to install, select **The updated driver (recommended)** and click **Next**.
- Step 17** When a screen appears indicating the driver that will be installed and its location, click **Next**.
- Step 18** If Windows cannot find the pcx50\*.sys file, enter the same path that you browsed to in [Step 14](#) and click **OK**.
- Step 19** When you are notified that the installation is complete, click **Finish**.
- Step 20** When you are prompted to restart your computer, remove the CD or floppy disk (if installed) and click **No**.
- Step 21** Double-click **My Computer, Control Panel, and Network**.
- Step 22** Select the Cisco Systems Wireless LAN Adapter. Click **Properties**.
- Step 23** In the client adapter Properties window, click the **Advanced** tab.
- Step 24** In the Advanced window, select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.
- Step 25** Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.
- Step 26** Click **OK**.
- Step 27** If your computer is not connected to a DHCP server and you plan to use TCP/IP, double-click **My Computer, Control Panel, and Network**. Select **TCP/IP > Cisco Systems Wireless LAN Adapter**. Click the **Properties** button, select **Specify an IP address**, and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK**.
- Step 28** In the Network window, click **OK**.
- Step 29** When prompted to restart your computer, click **Yes**.  
The driver installation is complete.
-

## Installing the Driver for Windows XP


The first release of Windows XP comes with driver version 7.29, which is installed automatically the first time you insert a client adapter. To upgrade to the driver on the CD that shipped with your client adapter or on Cisco.com, follow these steps.

**Note**

If you do not upgrade from the 7.29 driver, you cannot specify an SSID through Windows XP's driver Advanced tab.

**Note**

These instructions assume you are using Windows XP's classic view rather than its category view.

- Step 1** If you are installing the driver from Cisco.com, follow the steps below. If you are installing the driver from the CD that shipped with your client adapter, go to [Step 2](#).
- Use the computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - Click the link for Cisco Aironet Wireless LAN Client Adapters.
  - Perform one of the following:
    - If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as CB20A or 350 series). Select the latest bundled file for Windows XP and your specific client adapter type (such as CB or MPI).
    - If you want to select the client adapter's software files individually, find the section for Windows drivers and click the link for Windows XP. Select the driver file with the greatest version number for your specific client adapter type (such as MPI).
-  **Note** The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, the drivers for mini PCI cards are labeled *MPI*, and the drivers for PC-Cardbus cards are labeled *CB*.
- Read and accept the terms and conditions of the Software License Agreement.
  - Select the file again to download it.
  - Save the file to a floppy disk or to your computer's hard drive.
  - Find the file using Windows Explorer, double-click it, and extract its files to a folder.
  - Go to [Step 2](#).
- Step 2** Follow the instructions in [Chapter 8](#) to insert the client adapter into your computer. The instructions vary by operating system and are different for PC cards, PC-Cardbus cards, and PCI cards.
- Step 3** Double-click **My Computer**, **Control Panel**, and **System**.
- Step 4** Click the **Hardware** tab and **Device Manager**.
- Step 5** Double-click **Network Adapters** and the Cisco Systems Wireless LAN Adapter.
- Step 6** Click the **Driver** tab.

- Step 7** Click **Update Driver**. The Welcome to the Hardware Update Wizard screen appears.
- Step 8** Select the **Install from a list or specific location (Advanced)** option and click **Next**.
- Step 9** When prompted to choose your search and installation options, select **Don't search. I will choose the driver to install** and click **Next**.
- Step 10** When prompted to select a network adapter to install, click **Have Disk**. The Install From Disk screen appears.
- Step 11** Insert the CD that shipped with your client adapter or a floppy disk containing the latest driver into your computer, unless you are installing the driver from your computer's hard drive.
- Step 12** Click **Browse**; find the location of the driver (on your CD, floppy disk, or computer's hard drive).
- If you are installing a 2.4-GHz driver from the Cisco Aironet Wireless LAN Client Adapters CD and your CD-ROM drive is drive D, the path should be D:\WinXP.
  - If you are installing a 5-GHz driver from the Cisco Aironet 5-GHz 54-Mbps Wireless Adapters CD and your CD-ROM drive is drive D, the path should be D:.
- Step 13** Click **Open**. The installation wizard finds the driver file.
- Step 14** Click **OK** on the Install From Disk screen.
- Step 15** The Select Network Adapter screen reappears. Select the Cisco Systems Wireless LAN Adapter and click **Next**.
- Step 16** The installation wizard copies the driver files from the CD, floppy disk, or computer's hard drive. When the installation is complete, click **Finish**.
- Step 17** Click **Close** on the Cisco Aironet Wireless LAN Adapter Properties screen and exit the Control Panel.




---

**Note** You must exit the Control Panel before opening it again in [Step 18](#). Otherwise, the SSID property option will not be available when you get to [Step 22](#).

---

- Step 18** Double-click **Control Panel** and **Network Connections**.
- Step 19** Right-click **Wireless Network Connection**.
- Step 20** Click **Properties**, **Configure**, and the **Advanced** tab.
- Step 21** In the Advanced window, select **Client Name**. Type your computer's unique client name, which can be obtained from your system administrator, in the Value dialog box.
- Step 22** Select **SSID**. Type your RF network's (case-sensitive) SSID, which can be obtained from your system administrator, in the Value dialog box.
- Step 23** Click **OK**.
- Step 24** If your computer is not connected to a DHCP server and you plan to use TCP/IP, right-click **Wireless Network Connection** and click **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**. Select **Use the following IP address** and enter the IP address, subnet mask, and default gateway address of your computer (which can be obtained from your system administrator). Click **OK**.
- Step 25** The driver installation is complete. Now you must decide whether to configure your client adapter through Windows XP or ACU. To help you with your decision, [Table 3-2](#) compares the Windows XP and ACU client adapter features.

**Table 3-2 Comparison of Windows XP and ACU Client Adapter Features**

Feature	Windows XP	ACU
Configuration parameters	Limited	Extensive
Capabilities		
Create profiles	No	Yes
Upgrade radio firmware	No	Yes
Restart client adapter without rebooting or ejecting card	No	Yes
Turn radio on or off	No	Yes
Security		
Static WEP	Yes	Yes
LEAP authentication with dynamic WEP	No	Yes
Host-based EAP authentication with static or dynamic WEP	Yes	Yes
Diagnostics		
Status screen	Limited	Extensive
Statistics screen (transmit & receive)	No	Yes
Site survey tool	No	Yes
RF link test tool	No	Yes
Link status meter (graphical display)	No	Yes

**Step 26** Perform one of the following:

- If you are planning to configure your client adapter through ACU instead of through Windows XP, follow the steps below:
  - a. Double-click **My Computer**, **Control Panel**, and **Network Connections**.
  - b. Right-click **Wireless Network Connection** and click **Properties**.
  - c. Select the **Wireless Networks** tab.
  - d. Deselect the **Use Windows to configure my wireless network settings** check box.
  - e. Follow the instructions in the “[Installing ACU](#)” section on page 3-20 to install ACU.
- If you are planning to configure your client adapter through Windows XP instead of through ACU, go to [Appendix E](#) and follow the instructions there.
- If you are planning to configure your client adapter through Windows XP but you want to use ACU’s diagnostic tools, go to [Appendix E](#) to configure the adapter through Windows XP; then install ACU but do not create any profiles.

# Installing ACU

After you have installed the appropriate driver for your computer's operating system and your client adapter type, follow the steps below to install the Aironet Client Utility (ACU).

**Note**

If you are planning to use EAP-TLS, EAP-MD5, PEAP, or EAP-SIM authentication on a computer running Windows 2000, you must install Service Pack 3 for Windows 2000 and the Windows 2000 Wireless 802.1X hot fix before you install ACU.

**Note**

Follow the procedure below if ACU has never been installed on your computer or if ACU version 4.13 or greater is currently installed. If a version of ACU prior to 4.13 is installed on your computer, follow the instructions in [Chapter 8](#) to uninstall it; then follow the steps below to install the latest version. Cisco does not recommend uninstalling ACU version 4.13 or greater before installing the latest version of ACU.

**Note**

ACU version 5.05.001 or greater must be used with one of the following software combinations:

- PCM/LMC/PCI card driver version 8.2 or greater and firmware version 4.25.30 or greater
- Mini PCI card driver version 3.4 or greater and firmware version 5.00.03 or greater
- PC-Cardbus card driver version 3.4 or greater and firmware version 4.99 or greater

**Step 1** Close any Windows programs that are running.

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

- If you are installing ACU from the CD that shipped with the client adapter, follow the steps below:
  - a. Insert the CD into your computer's CD-ROM drive.
  - b. Select **Start > Run**, enter the following path (where *D* is the letter of your CD-ROM drive): **D:\Aironet Client Utility\Setup.exe**, and click **OK**. The Aironet Client Utility Setup screen and the InstallShield Wizard appear.
  - c. Go to [Step 3](#).
- If you are installing ACU from a bundled file on Cisco.com, follow the steps below:
  - a. Using Windows Explorer, find the folders that were extracted from the bundle and double-click the ACU folder.
  - b. Select **Start > Run**, enter or browse to the path where the ACU files are located (for example, C:\temp\setup.exe), and click **OK**. The Aironet Client Utility Setup screen and the InstallShield Wizard appear.
  - c. Go to [Step 3](#).
- If you are installing ACU from an individual file on Cisco.com, follow the steps below:
  - a. Use the computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - b. Click the link for Cisco Aironet Wireless LAN Client Adapters.
  - c. Click the link for the Windows utility.
  - d. Select the latest ACU file.

- e. Read and accept the terms and conditions of the Software License Agreement.
- f. Select the ACU file to download it.
- g. Save the file to your computer's hard drive.
- h. Find the file using Windows Explorer, double-click it, and extract its files to a folder.
- i. Select **Start > Run**, enter or browse to the path where you extracted the files (for example, C:\temp\setup.exe), and click **OK**. The Aironet Client Utility Setup screen and the InstallShield Wizard appear.
- j. Go to [Step 3](#).

**Step 3** When the Welcome screen appears, click **Next**.

**Step 4** In the Select Options screen, select as many of the following options as desired and click **Next**:

Option	Description
LEAP	<p>Enables you to create a profile in ACU that uses LEAP authentication. If this option is not selected now and you later want to use LEAP, you must run this installation program again, select <b>Modify</b>, and select this option.</p> <p><b>Default:</b> Selected</p> <p><b>Note</b> Refer to <a href="#">Chapter 5</a> for information on enabling LEAP.</p> <p><b>Note</b> If you select LEAP on a Windows 95, 98, or 98 SE device, Microsoft hot fixes are installed during ACU installation to fix two problems related to the use of LEAP. Refer to <a href="#">Chapter 9</a> for more information on the hot fixes.</p> <p><b>Note</b> If you select LEAP on a Windows XP device, you cannot use Windows XP's fast user switching feature.</p>
Allow Saved LEAP User Name and Password	<p>Enables you to create a profile in ACU that uses a saved (rather than temporary) username and password for LEAP authentication. When such a profile is used, the saved username and password are used to start the LEAP authentication process, and you are not prompted to enter them.</p> <p><b>Default:</b> Selected</p> <p><b>Note</b> This option is available only if the LEAP option is selected.</p>

Option	Description
PEAP	<p>Installs the PEAP supplicant, which enables the client to support PEAP authentication. If this option is not selected now and you later want to use PEAP, you must run this installation program again, select <b>Modify</b>, and select this option.</p> <p><b>Default:</b> Selected</p> <p><b>Note</b> Refer to <a href="#">Chapter 5</a> for information on enabling PEAP.</p> <p><b>Note</b> PC-Cardbus cards do not support PEAP authentication.</p> <p><b>Note</b> This option appears for all operating systems except Windows 95; however, your client adapter can authenticate using PEAP only if your computer's operating system is Windows 2000 (with Service Pack 3 or greater and the Windows 2000 Wireless 802.1X hot fix) or Windows XP.</p> <p><b>Note</b> Service Pack 1 for Windows XP includes Microsoft's PEAP supplicant, which supports a Windows username and password only and does not interoperate with Cisco's PEAP supplicant. To use Cisco's PEAP supplicant, install ACU version 5.05 or greater after Service Pack 1 for Windows XP. Otherwise, it will be overwritten by Microsoft's PEAP supplicant.</p>
EAP-SIM	<p>Installs the EAP-SIM supplicant, which enables the client to support EAP-SIM authentication. If this option is not selected now and you later want to use EAP-SIM, you must run this installation program again, select <b>Modify</b>, and select this option.</p> <p><b>Default:</b> Deselected</p> <p><b>Note</b> Refer to <a href="#">Chapter 5</a> for information on enabling EAP-SIM.</p> <p><b>Note</b> PC-Cardbus cards do not support EAP-SIM authentication.</p> <p><b>Note</b> This option appears for all operating systems except Windows 95; however, your client adapter can authenticate using EAP-SIM only if your computer's operating system is Windows 2000 (with Service Pack 3 or greater and the Windows 2000 Wireless 802.1X hot fix) or Windows XP.</p>
Create ACU Icon on your Desktop	<p>Causes the installation program to add an ACU icon to your computer's desktop to provide quick access to the utility.</p> <p><b>Default:</b> Deselected</p>
Allow Non-Administrator Users to save profiles to the registry	<p>Enables users without administrative rights to modify profiles in ACU and save them to the registry on computers running Windows NT, 2000, or XP.</p> <p><b>Default:</b> Selected</p> <p><b>Note</b> This option is not available for Windows 95, 98, and Me because these versions of Windows do not support different classes of users.</p>



- Step 5** In the Choose Destination Location screen, perform one of the following:
- If you want the ACU program files to be installed in the default location (C:\Program Files, provided C:\Program Files is the default Windows program file folder), click **Next**.
  - If you want to specify a different destination location for the ACU program files, click **Browse**, select a location, and click **Next**.

- Step 6** In the Select Program Folder screen, specify a program folder name for ACU by selecting from the list of existing folders (the default name is Cisco Aironet) or entering a new folder name; then click **Next**.

A status screen displays the progress of the installation. Then one of two Setup Complete screens appears, depending on whether Windows needs to be restarted to complete the installation.

- Step 7** Perform one of the following:
- If your computer does not need to be rebooted, select either of the following options and click **Finish**:

Option	Description
View the README.TXT file	Opens a read-me file containing information about ACU.
Launch the Aironet Client Utility	Opens ACU so you can configure your client adapter.

- If your computer needs to be rebooted, select **Yes, I want to restart my computer now** or **No, I will restart my computer later**, remove the CD (if installed), and click **Finish**.



**Note** If you are prompted to reboot your computer, Cisco recommends that you select the **Yes, I want to restart my computer now** option.

- Step 8** The driver and client utility installation is complete. The client adapter has been installed and configured for basic operation. Go to the “[Verifying Installation](#)” section below to determine if the installation was successful. After you verify installation, go to [Chapter 4](#) if you want to create profiles for your client adapter.

## Verifying Installation

To verify that you have properly installed the driver and ACU and minimally configured your client adapter, 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.

Go to [Chapter 4](#) if you want to create profiles for your client adapter.



**Note** If two client adapters (such as a mini PCI card and a PC-Cardbus card) are installed in your computer, you must specify the one for which you currently wish to set up profiles in ACU. Go to the “[Selecting from Two Installed Client Adapters](#)” section on page 3-24 for instructions.

## Selecting from Two Installed Client Adapters

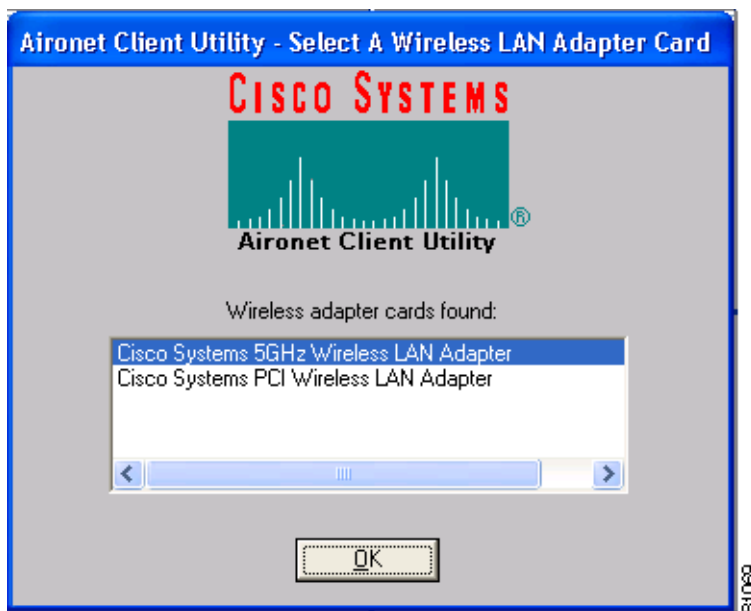
If two client adapters are installed in your computer, follow the instructions below to specify the one for which you want to set up profiles in ACU.

- Step 1** Double-click the **Aironet Client Utility (ACU)** icon on your desktop to open ACU. The Select A Wireless LAN Adapter Card screen appears (see [Figure 3-1](#)).



**Note** The Select A Wireless LAN Adapter Card screen appears when you start ACU only if more than one card is inserted in your computer or no cards are inserted but more than one card is installed.

**Figure 3-1** Select A Wireless LAN Adapter Card Screen



- Step 2** Select the card you wish to configure from the list of available cards and click **OK**.
- Step 3** Go to [Chapter 4](#) to create profiles for this card.



## 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 4-4](#)
- [Modifying a Profile, page 4-6](#)
- [Importing and Exporting Profiles, page 4-7](#)
- [Denying Access to Non-Administrative Users, page 4-8](#)

## Overview of Profile Manager

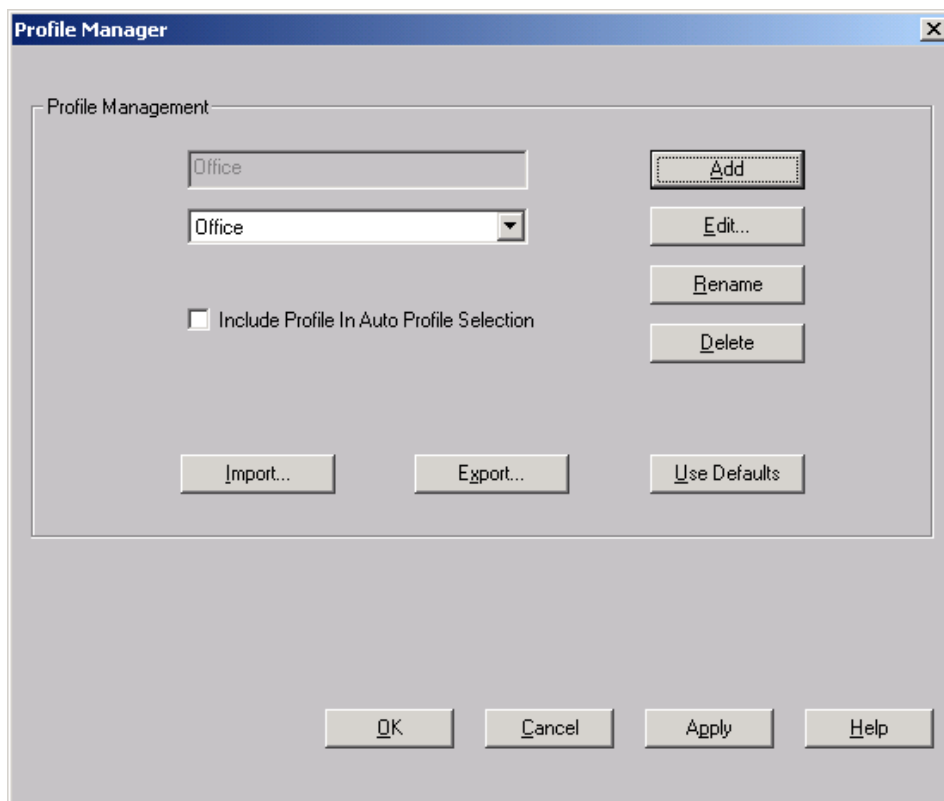
ACU's profile manager feature allows you to create and manage up to 16 *profiles* (or saved configurations) for your client adapter. These profiles enable you to use your client adapter in different locations, each of which requires different configuration settings. For example, you may want to set up profiles for using your client adapter at the office, at home, and in public areas such as airports. 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 part of the registry reserved for the client adapter driver and, therefore, are tied to radio type. Consequently, if you set up profiles for a 340 series PC card and later upgrade to a 350 series PC card, all of the profiles will be lost. Similarly, all profiles are lost if you uninstall the client adapter's driver. To prevent your profiles from becoming lost, Cisco recommends that you back up your profiles using the profile manager's import/export capability. See the [“Importing and Exporting Profiles” section on page 4-7](#) for details.

## Opening Profile Manager

To open ACU's profile manager, double-click the **Aironet Client Utility (ACU)** icon on your desktop to open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears (see [Figure 4-1](#)).

**Figure 4-1** Profile Manager Screen




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

- Create a new profile, see below
- Select the active profile, see [page 4-4](#)
- Edit a profile, see [page 4-6](#)
- Set a profile to default values, see [page 4-6](#)
- Rename a profile, see [page 4-7](#)
- Delete a profile, see [page 4-7](#)
- Import a profile, see [page 4-7](#)
- Export a profile, see [page 4-8](#)

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

## Creating a New Profile

Follow the steps below to create a new profile.

- 
- Step 1** Click **Add**. A cursor appears in the Profile Management edit box.
- Step 2** Enter the name for your new profile (for example, Office, Home, etc.).
- Step 3** Press **Enter**. The Properties screens appear with the name of your new profile in parentheses.
- Step 4** Perform one of the following:
- If you want this profile to use the default values, click **OK**. The profile is added to the list of profiles on the Profile Manager screen.
  - If you want to change any of the configuration parameter settings, follow the instructions in [Chapter 5](#). The profile is added to the list of profiles on the Profile Manager screen.
- Step 5** If you want this profile to be included in auto profile selection, select the **Include Profile in Auto Profile Selection** check box on the Profile Manager screen.
-  **Note** If your profile is configured to use LEAP, it can be included in auto profile selection *only* if it has a saved LEAP username and password. For more information on auto profile selection, see the [“Selecting the Active Profile” section on page 4-4](#).
- 
- Step 6** Click **OK** or **Apply** to save your profile.
-

## Selecting the Active Profile

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


**Note**

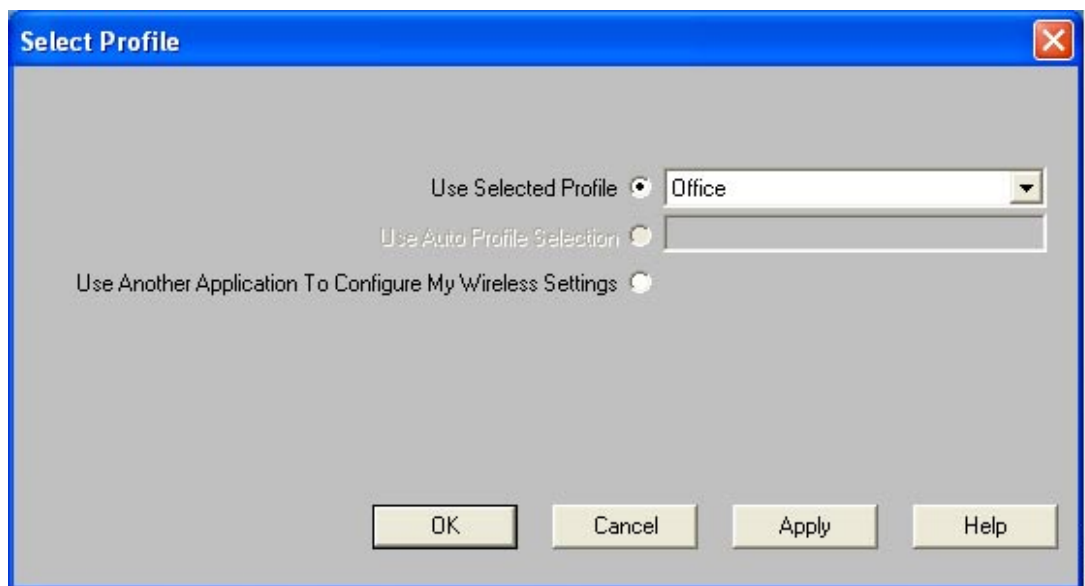
If this is the first time that you are using profile manager and no profiles have been set previously, the Use Selected Profile drop-down box is disabled but displays “Driver Advanced Tab Settings,” which indicates that the driver is using any settings that were set through the Control Panel.


**Note**

Because EAP-TLS, EAP-MD5, PEAP, and EAP-SIM authentication are enabled in the operating system and not 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 Windows 2000 (with Service Pack 3 or greater and the Windows 2000 Wireless 802.1X hot fix) or Windows XP. In addition, Windows can be set for only one authentication type 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 authentication types in Windows after switching profiles in ACU.

- Step 1** Open ACU; click the **Select Profile** icon or select **Select Profile** from the Commands drop-down menu. The Select Profile screen appears (see [Figure 4-2](#)).

**Figure 4-2** Select Profile Screen



**Step 2** Select one of the following options:

- **Use Selected Profile**—This option allows you to select one profile for the client adapter to use. If you choose this option, you also must select the desired profile from the drop-down box.

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 or select Use Auto Profile Selection.

- **Use Auto Profile Selection**—This option causes the client adapter's driver to automatically select a profile from the list of profiles that were set up to be included in auto profile selection. The name of the profile that is being used appears in the box to the right of the Use Auto Profile Selection option.

If the client adapter loses association for more than 10 seconds (or for more than the time specified by the LEAP authentication timeout value on the LEAP Settings screen if LEAP is enabled), the driver switches automatically to another profile that is included in auto profile selection. The adapter will not switch profiles as long as it remains associated or reassociates within 10 seconds (or within the time specified by the LEAP authentication timeout value). To force the client adapter to associate to a different access point, you must disable auto profile selection and select a new profile.



---

**Note** This option is available only if two or more profiles are included in auto profile selection and if the client adapter is using PCM/LMC/PCI card driver version 8.01 or greater, mini PCI card driver version 2.20 or greater, or PC-Cardbus card driver version 3.4 or greater.

---



---

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

---

- **Use Another Application To Configure My Wireless Settings**—This option allows an application other than ACU to configure the client adapter. Examples of such applications include Windows XP and Boingo.



---

**Note** You must select this option if you are configuring your card through Windows XP but want to use ACU's diagnostic tools. Refer to [Appendix E](#) for information on configuring your client adapter through Windows XP.

---

**Step 3** Click **OK** or **Apply** to save your selection. The client adapter starts using a profile based on the option selected above.

---

# Modifying a Profile

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

## Editing a Profile

- 
- Step 1** Open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears (see [Figure 4-1](#)).
  - Step 2** From the Profile Management drop-down box, select the profile that you want to edit.
  - Step 3** Click **Edit**. The Properties screens appear with the name of the profile in parentheses.
  - Step 4** Follow the instructions in [Chapter 5](#) to change any of the configuration parameters for this profile.
  - Step 5** If you want this profile to be included in auto profile selection, make sure the **Include Profile in Auto Profile Selection** check box on the Profile Manager screen is selected.



---

**Note** If your profile is configured to use LEAP, it can be included in auto profile selection only if it has a saved LEAP username and password.

---

- Step 6** Click **OK** or **Apply** to save your configuration changes.
- 

## Setting a Profile to Default Values

- 
- Step 1** Open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears (see [Figure 4-1](#)).
  - Step 2** From the Profile Management drop-down box, select the profile that you want to set to default values.
  - Step 3** Click **Use Defaults**.
  - Step 4** When prompted, click **Yes** to confirm your decision.
  - Step 5** Click **OK** or **Apply** to save your change. The profile is saved with default values.
-



## Renaming a Profile

- 
- Step 1** Open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears (see [Figure 4-1](#)).
  - Step 2** From the Profile Management drop-down box, select the profile that you want to rename.
  - Step 3** Click **Rename**. The Profile Management edit box becomes enabled.
  - Step 4** Enter a new name for the profile.
  - Step 5** Click **OK** or **Apply** to save your change. The profile is renamed and added to the list of profiles.
- 

## Deleting a Profile

- 
- Step 1** Open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears (see [Figure 4-1](#)).
  - Step 2** From the Profile Management drop-down box, select the profile that you want to delete.
  - Step 3** Click **Delete**.
  - Step 4** When prompted, click **Yes** to confirm your decision.
  - Step 5** Click **OK** or **Apply** to save your change. The profile is deleted.
- 

## Importing and Exporting Profiles

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

- To back up profiles before uninstalling the client adapter driver or changing radio types
- To set up your computer with a profile from another computer
- To export one of your profiles and use it to set up additional computers

Follow the steps in the corresponding section below to import or export profiles.

## Importing a Profile

- 
- Step 1** If the profile that you want to import is on a floppy disk, insert the disk into your computer's floppy drive.
  - Step 2** Open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears (see [Figure 4-1](#)).
  - Step 3** Click **Import**. The Import Profile screen appears.

- Step 4** Find the directory where the profile is located.
  - Step 5** Click the profile so it appears in the File name box at the bottom of the Import Profile screen.
  - Step 6** Click **Open**. The imported profile appears in the list of profiles on the Profile Manager screen.
- 

## Exporting a Profile

- Step 1** Insert a blank floppy disk into your computer's floppy drive, if you wish to export a profile to a floppy disk.
  - Step 2** Open ACU; click the **Profile Manager** icon or select **Profile Manager** from the Commands drop-down menu. The Profile Manager screen appears (see [Figure 4-1](#)).
  - Step 3** From the Profile Management drop-down box, select the profile that you want to export.
  - Step 4** Click **Export**. The Save Profile As screen appears. The default filename is *ProfileName.pro*, where *ProfileName* is the name of the selected profile, and the default directory is the directory in which ACU was installed.
  - Step 5** If you want to change the profile name, enter a new name in the File name edit box.
  - Step 6** Select a different directory (for example, your computer's floppy disk drive or a location on the network) from the Save in drop-down box.
  - Step 7** Click **Save**. The profile is exported to the specified location.
  - Step 8** Follow the instructions in the ["Importing a Profile"](#) section to import the profile on another computer.
- 

## Denying Access to Non-Administrative Users

By default, ACU allows regular-class users to modify and save profiles to the registry. However, if you have administrative rights, you can prevent regular-class users from saving profiles on computers running Windows NT, 2000, or XP. (This option is not available for Windows 95, 98, and Me because these versions of Windows do not support different classes of users.)



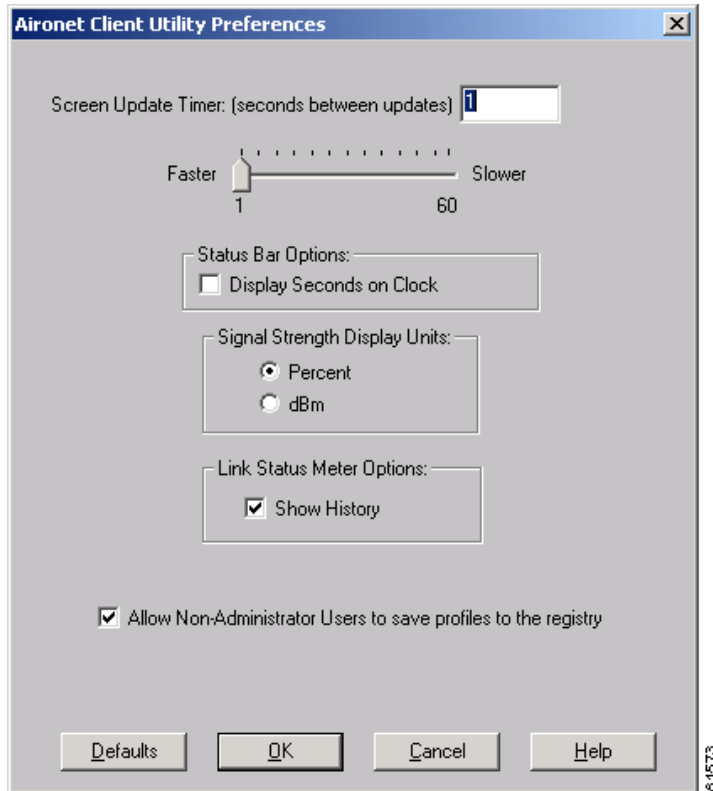
### Note

You were able to grant or deny access to non-administrative users during ACU installation. If you chose to deny access then, you can follow the steps below to change your decision.

Follow the steps below if you wish to prevent users without administrative rights from modifying and saving profiles (or to allow regular-class users to save profiles if permission was denied previously).

- Step 1** Open ACU by double-clicking the **Aironet Client Utility (ACU)** icon on your desktop.
- Step 2** Click the **Preferences** icon or select **Preferences** from the Options drop-down menu. The Aironet Client Utility Preferences screen appears (see [Figure 4-3](#)).

Figure 4-3 Aironet Client Utility Preferences Screen



- Step 3** Deselect the **Allow Non-Administrator Users to save profiles to the registry** check box (or select this check box if you wish to allow regular-class users to save profiles).
- Step 4** Click **OK** to save your changes.
-





## Configuring the Client Adapter

---

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

The following topics are covered in this chapter:

- [Overview, page 5-2](#)
- [Setting System Parameters, page 5-3](#)
- [Setting RF Network Parameters, page 5-6](#)
- [Setting Advanced Infrastructure Parameters, page 5-13](#)
- [Setting Advanced Ad Hoc Parameters, page 5-17](#)
- [Setting Network Security Parameters, page 5-20](#)

# Overview

When you choose to create a new profile or edit an existing profile on the Profile Manager screen, the Properties screens appear with the name of your profile in parentheses. These screens enable you to set the configuration parameters for that profile.


**Note**

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


**Note**

If you are planning to set parameters on more than one of the Properties screens, wait until you are finished with all of the screens before clicking OK. When you click OK, you are returned to the Profile Manager screen.

Each of the Properties screens (listed below) contains parameters that affect a specific aspect of the client adapter:

- **System Parameters**—Prepares the client adapter for use in a wireless network
- **RF Network**—Controls how the client adapter transmits and receives data
- **Advanced (Infrastructure)**—Controls how the client adapter operates within an infrastructure network
- **Advanced (Ad Hoc)**—Controls how the client adapter operates within an ad hoc (peer-to-peer) network
- **Network Security**—Controls how a client adapter associates to an access point, authenticates to the wireless network, and encrypts and decrypts data

[Table 5-1](#) enables you to quickly locate the instructions for setting each Properties screen's parameters.

**Table 5-1 Locating Configuration Instructions**

Parameter Category	Page Number
System	<a href="#">5-3</a>
RF network	<a href="#">5-6</a>
Advanced infrastructure	<a href="#">5-13</a>
Advanced ad hoc	<a href="#">5-17</a>
Network security	<a href="#">5-20</a>

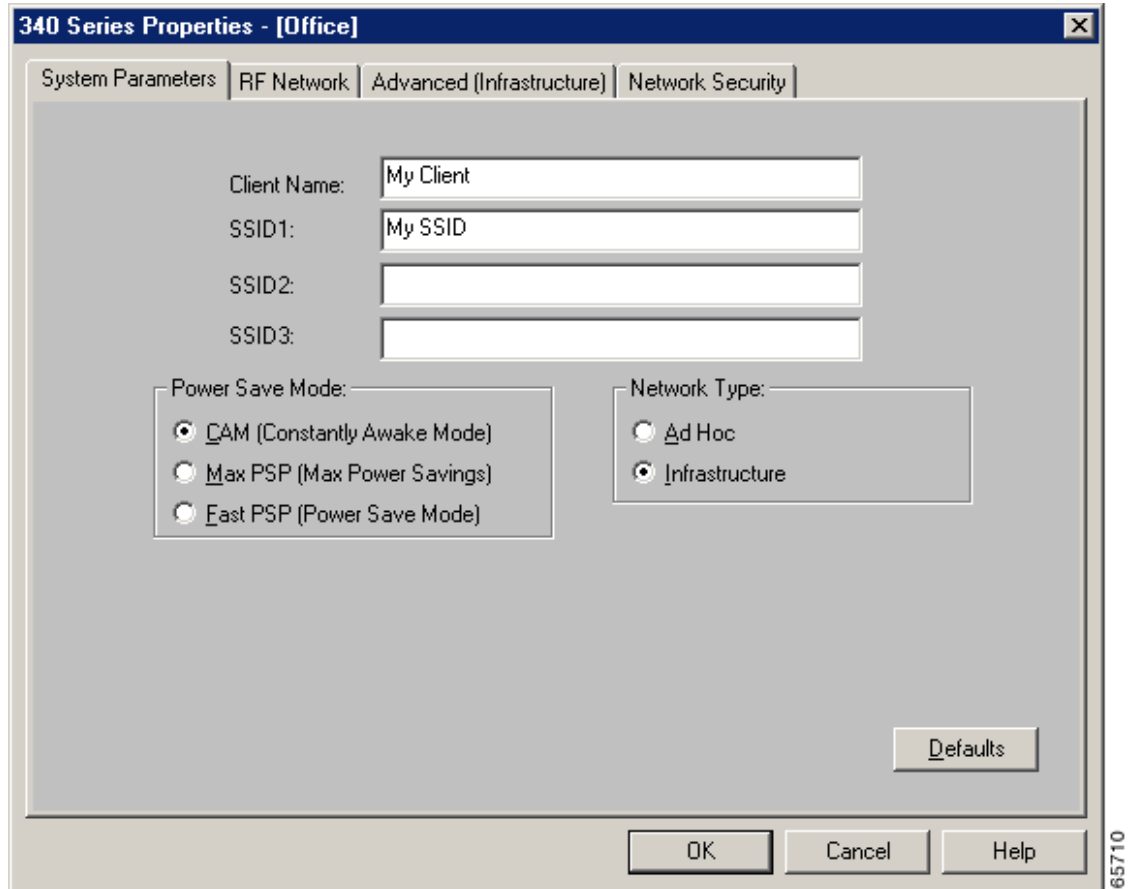

**Note**

If your system administrator used an auto-installer to deactivate certain parameters in ACU, these parameters are grayed out on the ACU Properties screens and cannot be selected.

# Setting System Parameters

The System Parameters screen (see [Figure 5-1](#)) enables you to set parameters that prepare the client adapter for use in a wireless network. This screen appears after you create and save a new profile or click Edit on the Profile Manager screen.

**Figure 5-1** System Parameters Screen



[Table 5-2](#) lists and describes the client adapter's system parameters. Follow the instructions in the table to change any parameters.

Table 5-2 System Parameters

Parameter	Description
Client Name	<p>A logical name for your workstation. 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 key in up to 16 ASCII 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>
SSID1	<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 ASCII 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 is unable to access the network.</p>
SSID2	<p>An optional SSID that identifies a second distinct network and enables you to roam to that network without having to reconfigure your client adapter.</p> <p><b>Range:</b> You can key in up to 32 ASCII characters (case sensitive)</p> <p><b>Default:</b> A blank field</p>
SSID3	<p>An optional SSID that identifies a third distinct network and enables you to roam to that network without having to reconfigure your client adapter.</p> <p><b>Range:</b> You can key in up to 32 ASCII characters (case sensitive)</p> <p><b>Default:</b> A blank field</p>



Table 5-2 System Parameters (continued)

Parameter	Description								
Power Save Mode	<p>Sets your client adapter to its optimum power consumption setting.</p> <p><b>Options:</b> CAM, Max PSP, or Fast PSP</p> <p><b>Default:</b> CAM (Constantly Awake Mode)</p>								
	<table border="1"> <thead> <tr> <th>Power Save Mode</th> <th>Description</th> </tr> </thead> <tbody> <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>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> <p><b>Note</b> When you set Max PSP mode and close ACU, the following message appears the next time you open ACU: “Maximum Power Save mode will be temporarily disabled while you are running this application.” While ACU is open, Fast PSP mode is active. When you close ACU, the card returns to Max PSP mode.</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> </tbody> </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>	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> <p><b>Note</b> When you set Max PSP mode and close ACU, the following message appears the next time you open ACU: “Maximum Power Save mode will be temporarily disabled while you are running this application.” While ACU is open, Fast PSP mode is active. When you close ACU, the card returns to Max PSP mode.</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>
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>								
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> <p><b>Note</b> When you set Max PSP mode and close ACU, the following message appears the next time you open ACU: “Maximum Power Save mode will be temporarily disabled while you are running this application.” While ACU is open, Fast PSP mode is active. When you close ACU, the card returns to Max PSP mode.</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>								

Table 5-2 System Parameters (continued)

Parameter	Description	
Network Type	Specifies the type of network in which your client adapter is installed. <b>Options:</b> Ad Hoc or Infrastructure <b>Default:</b> Infrastructure	
	Network Type	Description
	Ad Hoc	Often referred to as <i>peer to peer</i> . Indicates that your wireless network consists of a few wireless devices that are not connected to a wired Ethernet network through an access point. For example, an ad hoc network could be set up between computers in a conference room so users can share information in a meeting.
	Infrastructure	Indicates that your wireless network is connected to a wired Ethernet network through an access point.

Go to the next section to set additional parameters or click **OK** to return to the Profile Manager screen. On the Profile Manager screen, click **OK** or **Apply** to save your changes.

## Setting RF Network Parameters

The RF Network screen (see [Figure 5-2](#)) enables you to set parameters that control how and when the client adapter transmits and receives data. To access this screen, select the **RF Network** tab from the Properties screens.

Figure 5-2 RF Network Screen

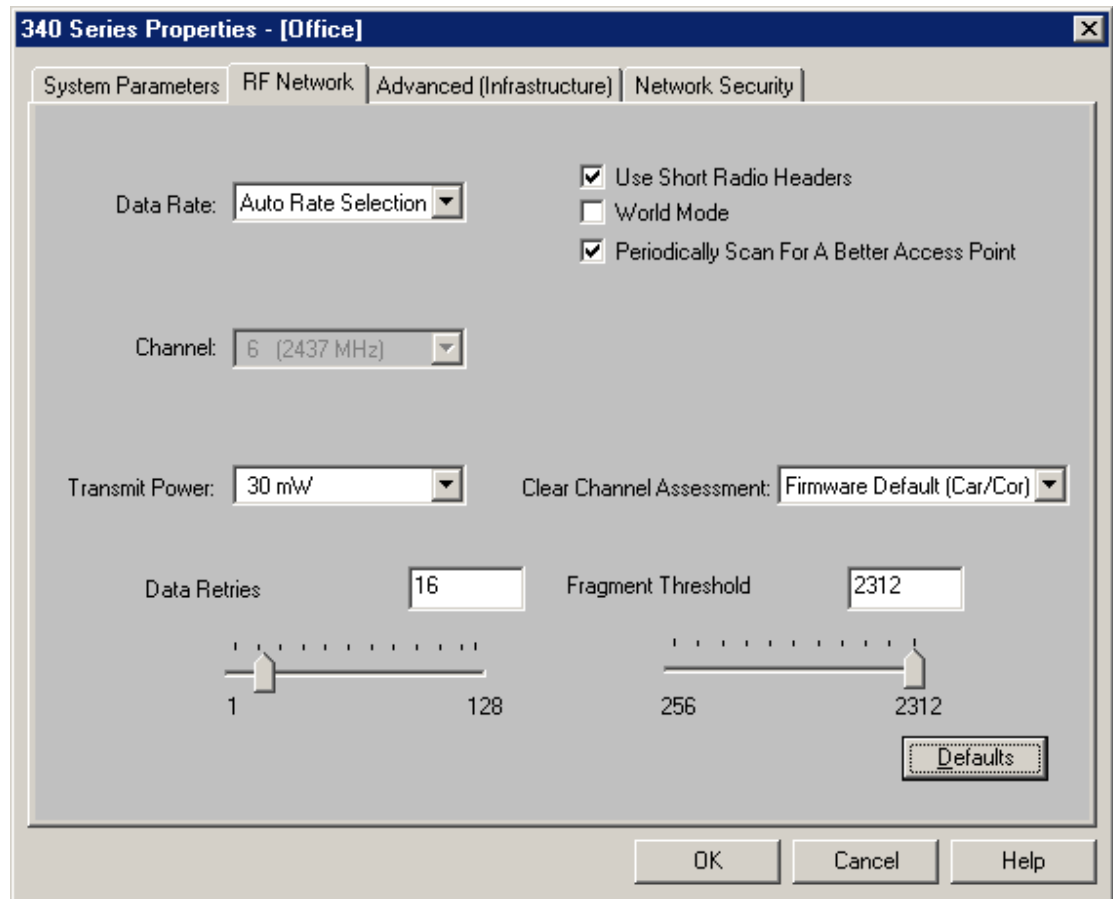


Table 5-3 lists and describes the client adapter's RF network parameters. Follow the instructions in the table to change any parameters.

74318

Table 5-3 RF Network Parameters

Parameter	Description		
Data Rate	<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 Rate Selection is recommended for infrastructure mode; setting a specific data rate is recommended for ad hoc mode.</p> <p><b>Options:</b> Auto Rate Selection, 1 Mbps Only, 2 Mbps Only, 5.5 Mbps Only, or 11 Mbps Only (2.4-GHz client adapters); Auto Rate Selection, 6 Mbps Only, 9 Mbps Only, 12 Mbps Only, 18 Mbps Only, 24 Mbps Only, 36 Mbps Only, 48 Mbps Only, or 54 Mbps Only (5-GHz client adapters)</p> <p><b>Default:</b> Auto Rate Selection</p>		
	Data Rate		Description
	2.4-GHz Client Adapters	5-GHz Client Adapters	
	Auto Rate Selection	Auto Rate Selection	Uses the 11-Mbps (for 2.4-GHz client adapters) or 54-Mbps (for 5-GHz client adapters) data rate when possible but drops to lower rates when necessary.
	1 Mbps Only	6 Mbps Only	Offers the greatest range but the lowest throughput.
	2 Mbps Only and 5.5 Mbps Only	9 Mbps Only to 48 Mbps Only	Progressively offers less range but greater throughput than the 1 Mbps Only (for 2.4-GHz client adapters) or 6 Mbps Only (for 5-GHz client adapters) option.
	11 Mbps Only	54 Mbps Only	Offers the greatest throughput but the lowest range.
	<p><b>Note</b> Your client adapter's data rate must be set to Auto Rate Selection 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>		

Table 5-3 RF Network Parameters (continued)

Parameter	Description
Use Short Radio Headers	<p>Selecting this check box sets your client adapter to use short radio headers. However, the adapter can use short radio headers only if the access point is also configured to support them and is using them. If any clients associated to an access point are using long headers, then <i>all</i> clients in that cell must also use long headers, even if both this client and the access point have short radio headers enabled.</p> <p>Short radio headers improve throughput performance; long radio headers ensure compatibility with clients and access points that do not support short radio headers.</p> <p><b>Default:</b> Selected</p> <p><b>Note</b> This parameter is available only for 2.4-GHz client adapters.</p> <p><b>Note</b> This parameter is referred to as <i>Preambles</i> on the access point screens.</p>
World Mode	<p>Selecting this check box 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>Default:</b> Deselected</p> <p><b>Note</b> This parameter is available only for 2.4-GHz client adapters.</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>
Periodically Scan For A Better Access Point	<p>Selecting this check box causes the client to look for a better access point if its signal strength becomes low and to switch associations if it finds one.</p> <p><b>Default:</b> Selected</p> <p><b>Note</b> This parameter is available only for 2.4-GHz client adapters.</p> <p><b>Note</b> This parameter is available only if your client adapter is using PCM/LMC/PCI card firmware version 4.25.30 or greater or mini PCI card firmware version 5.00.03 or greater.</p>

Table 5-3 RF Network Parameters (continued)

Parameter	Description
Channel	<p data-bbox="696 308 1487 405">Specifies which frequency your client adapter will use as the channel for communications. These channels conform to the IEEE 802.11 Standard for your regulatory domain.</p> <ul data-bbox="708 422 1482 621" style="list-style-type: none"> <li data-bbox="708 422 1482 548">• In infrastructure mode, this parameter is set automatically and cannot be changed. The client adapter listens to the entire spectrum, selects the best access point to associate to, and uses the same frequency as that access point.</li> <li data-bbox="708 562 1482 621">• In ad hoc mode, the channel of the client adapter must be set to match the channel used by the other clients in the wireless network.</li> </ul> <p data-bbox="696 638 1446 667"><b>Range:</b> Dependent on client adapter radio and regulatory domain</p> <p data-bbox="805 669 1252 699"><b>Example for 2.4-GHz client adapters:</b></p> <p data-bbox="805 701 1325 730">1 to 11 (2412 to 2462 MHz) in North America</p> <p data-bbox="805 732 1230 762"><b>Example for 5-GHz client adapters:</b></p> <p data-bbox="805 764 1468 827">36, 40, 44, 48, 52, 56, 60, and 64 (5180, 5200, 5220, 5240, 5260, 5280, 5300, and 5320 MHz) in North America</p> <p data-bbox="696 842 1446 871"><b>Default:</b> Dependent on client adapter radio and regulatory domain</p> <p data-bbox="805 873 1252 903"><b>Example for 2.4-GHz client adapters:</b></p> <p data-bbox="805 905 1170 934">6 (2437 MHz) in North America</p> <p data-bbox="805 936 1230 966"><b>Example for 5-GHz client adapters:</b></p> <p data-bbox="805 968 1182 997">36 (5180 MHz) in North America</p> <p data-bbox="696 1012 1468 1075"><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>

Table 5-3 RF Network 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> Dependent on the power table programmed into the client adapter; see the table below</p> <p><b>Default:</b> The maximum level programmed into the client adapter and allowed by your country's regulatory agency</p> <table border="1"> <thead> <tr> <th>Possible Power Levels</th> <th>Client Adapter Type</th> </tr> </thead> <tbody> <tr> <td>30 mW or 1 mW</td> <td>340 series PC cards</td> </tr> <tr> <td>30 mW, 15 mW, 5 mW, or 1 mW</td> <td>340 series LM cards and PCI cards</td> </tr> <tr> <td>100 mW, 50 mW, 30 mW, 20 mW, 5 mW, or 1 mW</td> <td>350 series client adapters</td> </tr> <tr> <td>20 mW, 10 mW, or 5 mW</td> <td>PC-Cardbus card</td> </tr> </tbody> </table> <p><b>Note</b> Reducing the transmit power level conserves battery power but decreases radio range.</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 340 or 350 series client adapter, your power level options may be different than those listed here.</p>	Possible Power Levels	Client Adapter Type	30 mW or 1 mW	340 series PC cards	30 mW, 15 mW, 5 mW, or 1 mW	340 series LM cards and PCI cards	100 mW, 50 mW, 30 mW, 20 mW, 5 mW, or 1 mW	350 series client adapters	20 mW, 10 mW, or 5 mW	PC-Cardbus card
Possible Power Levels	Client Adapter Type										
30 mW or 1 mW	340 series PC cards										
30 mW, 15 mW, 5 mW, or 1 mW	340 series LM cards and PCI cards										
100 mW, 50 mW, 30 mW, 20 mW, 5 mW, or 1 mW	350 series client adapters										
20 mW, 10 mW, or 5 mW	PC-Cardbus card										

Table 5-3 RF Network Parameters (continued)

Parameter	Description										
Clear Channel Assessment	<p>Specifies the method that determines whether the channel on which your client adapter will operate is clear prior to the transmission of data.</p> <p><b>Options:</b> Firmware Default (XXX), Carrier/Correlation (Car/Cor), Energy Detect (ED), or ED or Car/Cor</p> <p><b>Default:</b> Firmware Default (XXX)</p>										
	<table border="1"> <thead> <tr> <th>Method</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Firmware Default (XXX)</td> <td> <p>The Clear Channel Assessment (CCA) mechanism will report that the channel is busy based on the default value of the client adapter's firmware. The firmware's CCA default value is shown in parentheses.</p> <p><b>Note</b> The CCA default value for PCM/LMC/PCI card firmware is Car/Cor; the default value for mini PCI card firmware is ED.</p> </td> </tr> <tr> <td>Carrier/Correlation (Car/Cor)</td> <td> <p>The CCA mechanism will report that the channel is busy upon detection of a direct-sequence spread spectrum (DSSS) signal. This signal may be above or below the ED threshold.</p> </td> </tr> <tr> <td>Energy Detect (ED)</td> <td> <p>The CCA mechanism will report that the channel is busy upon detection of any energy above the ED threshold.</p> </td> </tr> <tr> <td>ED or Car/Cor</td> <td> <p>The CCA mechanism will report that the channel is busy upon detection of a DSSS signal or any energy above the ED threshold.</p> </td> </tr> </tbody> </table>	Method	Description	Firmware Default (XXX)	<p>The Clear Channel Assessment (CCA) mechanism will report that the channel is busy based on the default value of the client adapter's firmware. The firmware's CCA default value is shown in parentheses.</p> <p><b>Note</b> The CCA default value for PCM/LMC/PCI card firmware is Car/Cor; the default value for mini PCI card firmware is ED.</p>	Carrier/Correlation (Car/Cor)	<p>The CCA mechanism will report that the channel is busy upon detection of a direct-sequence spread spectrum (DSSS) signal. This signal may be above or below the ED threshold.</p>	Energy Detect (ED)	<p>The CCA mechanism will report that the channel is busy upon detection of any energy above the ED threshold.</p>	ED or Car/Cor	<p>The CCA mechanism will report that the channel is busy upon detection of a DSSS signal or any energy above the ED threshold.</p>
Method	Description										
Firmware Default (XXX)	<p>The Clear Channel Assessment (CCA) mechanism will report that the channel is busy based on the default value of the client adapter's firmware. The firmware's CCA default value is shown in parentheses.</p> <p><b>Note</b> The CCA default value for PCM/LMC/PCI card firmware is Car/Cor; the default value for mini PCI card firmware is ED.</p>										
Carrier/Correlation (Car/Cor)	<p>The CCA mechanism will report that the channel is busy upon detection of a direct-sequence spread spectrum (DSSS) signal. This signal may be above or below the ED threshold.</p>										
Energy Detect (ED)	<p>The CCA mechanism will report that the channel is busy upon detection of any energy above the ED threshold.</p>										
ED or Car/Cor	<p>The CCA mechanism will report that the channel is busy upon detection of a DSSS signal or any energy above the ED threshold.</p>										
	<p><b>Note</b> This parameter is available only for 2.4-GHz client adapters using PCM/LMC/PCI card firmware version 4.25.30 or greater (or mini PCI card firmware version 5.00.03 or greater).</p>										



**Table 5-3 RF Network Parameters (continued)**

Parameter	Description
Data Retries	<p>Defines the number of times a packet is resent if the initial transmission is unsuccessful.</p> <p><b>Range:</b> 1 to 128</p> <p><b>Default:</b> 16 (2.4-GHz client adapters) or 32 (5-GHz client adapters)</p> <p><b>Note</b> If your network protocol performs its own retries, set this to a smaller value than the default. This way notification of a “bad” packet is sent up the protocol stack quickly so the application can retransmit the packet if necessary.</p>
Fragment Threshold	<p>Defines the threshold above which an RF data packet is split up or fragmented. If one of those fragmented packets experiences interference during transmission, only that specific packet would need to be resent.</p> <p>Throughput is generally lower for fragmented packets because the fixed packet overhead consumes a higher portion of the RF bandwidth.</p> <p><b>Range:</b> 256 to 2312</p> <p><b>Default:</b> 2312</p>

Go to the next section to set additional parameters or click **OK** to return to the Profile Manager screen. On the Profile Manager screen, click **OK** or **Apply** to save your changes.

## Setting Advanced Infrastructure Parameters



### Note

You can set advanced infrastructure parameters only if your client adapter has been set to operate in an infrastructure network. See the Network Type parameter in [Table 5-2](#).

The Advanced (Infrastructure) screen (see [Figure 5-3](#)) enables you to set parameters that control how the client adapter operates within an infrastructure network. To access this screen, select the **Advanced (Infrastructure)** tab from the Properties screens.

Figure 5-3 Advanced (Infrastructure) Screen

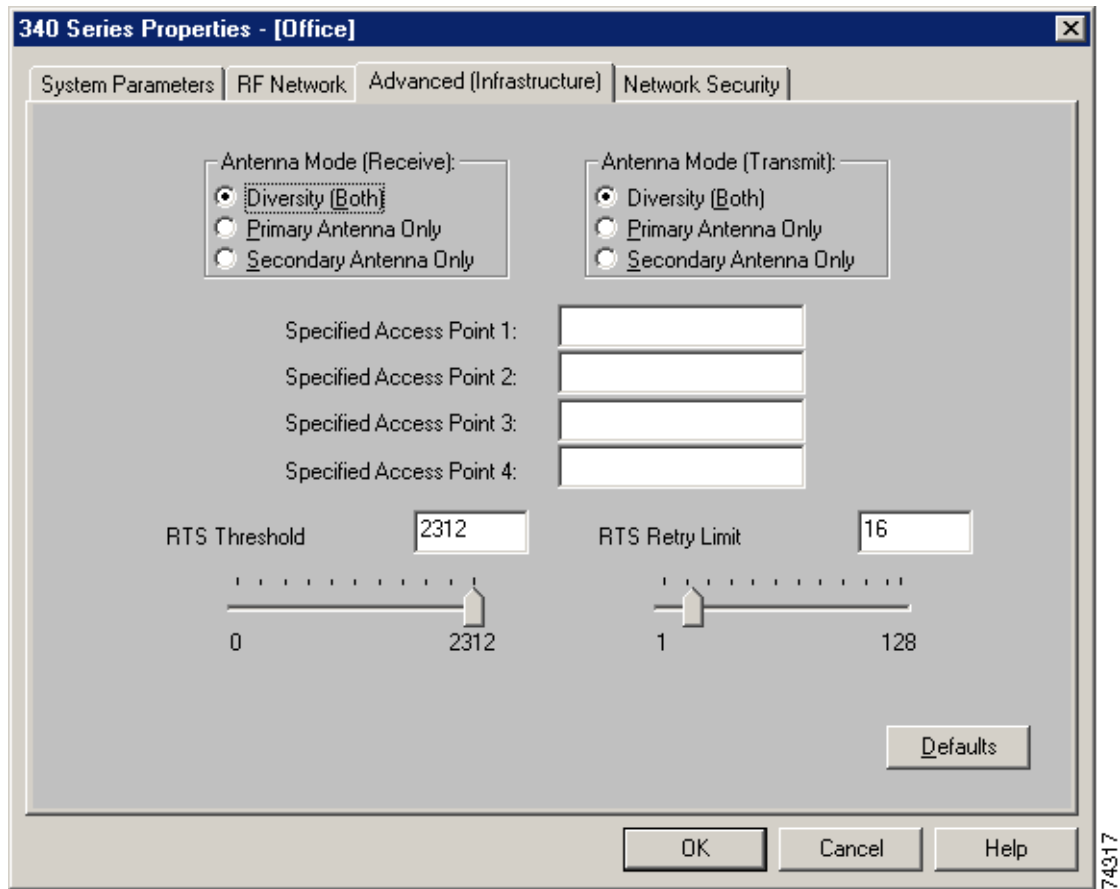


Table 5-4 lists and describes the client adapter's advanced infrastructure parameters. Follow the instructions in the table to change any parameters.

Table 5-4 Advanced (Infrastructure) Parameters

Parameter	Description
Antenna Mode (Receive)	<p>Specifies the antenna that your client adapter uses to receive data.</p> <ul style="list-style-type: none"> <li>• PC card—The PC card’s integrated, permanently attached antenna operates best when used in diversity mode. Diversity mode allows the card to use the better signal from its two antenna ports. <b>Options:</b> Diversity (Both), Primary Antenna Only, Secondary Antenna Only <b>Default:</b> Diversity (Both)</li> <li>• LM card—The LM card is shipped without an antenna; however, an antenna can be connected through the card’s external connector. If a snap-on antenna is used, diversity mode is recommended. Otherwise, select the mode that corresponds to the antenna port to which the antenna is connected. <b>Options:</b> Diversity (Both), Primary Antenna Only, Secondary Antenna Only <b>Default:</b> Diversity (Both)</li> <li>• PCI card—The PCI card must use the Primary Antenna Only option. <b>Default:</b> Primary Antenna Only</li> <li>• Mini PCI card—The mini PCI card, which can be used with one or two antennas, operates best in diversity mode. Diversity mode allows the card to use the better signal from its two antenna connectors. <b>Options:</b> Diversity (Both), Primary Antenna Only, Secondary Antenna Only <b>Default:</b> Diversity (Both)</li> </ul> <p><b>Note</b> This parameter is available only for 2.4-GHz client adapters.</p> <p><b>Note</b> The Primary Antenna Only and Secondary Antenna Only options were formerly named Right Antenna Only and Left Antenna Only, respectively.</p>
Antenna Mode (Transmit)	<p>Specifies the antenna that your client adapter uses to transmit data. See the Antenna Mode (Receive) parameter above for information on the options available for your client adapter.</p> <p><b>Note</b> This parameter is available only for 2.4-GHz client adapters.</p>

Table 5-4 Advanced (Infrastructure) Parameters (continued)

Parameter	Description
Specified Access Point 1- 4	<p>Specifies the MAC addresses of up to four preferred access points with which the client adapter can associate. If the specified access points are not found or the client adapter roams out of range, the adapter may associate to another access point.</p> <p>You can enter the MAC addresses of the access points in the edit boxes or choose not to specify access points by leaving the boxes blank.</p> <p><b>Default:</b> Blank fields</p> <p><b>Note</b> This parameter should be used only for access points that are in repeater mode. For normal operation, leave these fields blank because specifying an access point slows down the roaming process.</p>
RTS Threshold	<p>Specifies the size of the data packet that the low-level RF protocol issues to a request-to-send (RTS) packet.</p> <p>Setting this parameter to a small value causes RTS packets to be sent more often. When this occurs, more of the available bandwidth is consumed and the throughput of other network packets is reduced, but the system is able to recover faster from interference or collisions, which may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p><b>Range:</b> 0 to 2312</p> <p><b>Default:</b> 2312</p> <p><b>Note</b> Refer to the IEEE 802.11 Standard for more information on the RTS/CTS mechanism.</p>
RTS Retry Limit	<p>Specifies the number of times the client adapter resends a request-to-send (RTS) packet if it does not receive a clear-to-send (CTS) packet from the previously sent RTS packet.</p> <p>Setting this parameter to a large value decreases the available bandwidth whenever interference is encountered but makes the system more immune to interference and collisions, which may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p><b>Range:</b> 1 to 128</p> <p><b>Default:</b> 16 (2.4-GHz client adapters) or 32 (5-GHz client adapters)</p> <p><b>Note</b> Refer to the IEEE 802.11 Standard for more information on the RTS/CTS mechanism.</p>

Go to the next section to set additional parameters or click **OK** to return to the Profile Manager screen. On the Profile Manager screen, click **OK** or **Apply** to save your changes.

# Setting Advanced Ad Hoc Parameters

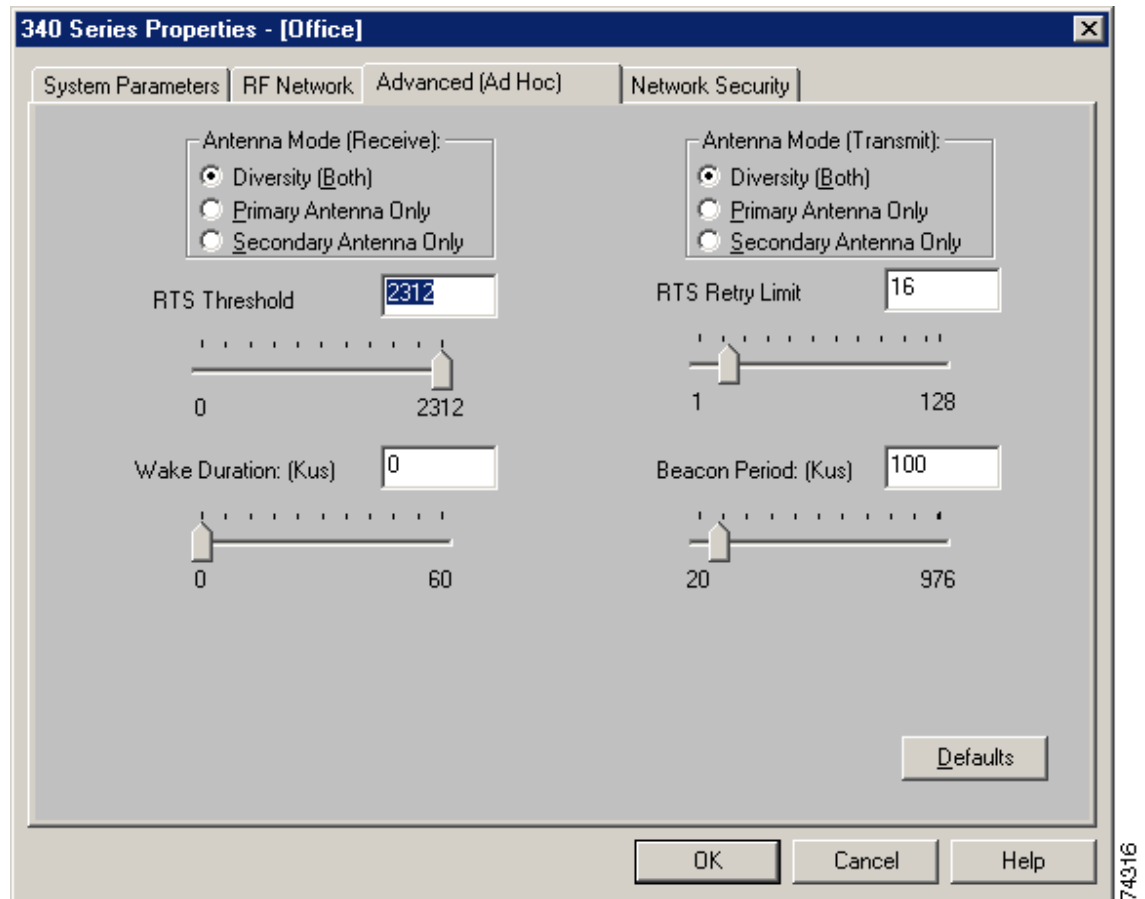


## Note

You can set advanced ad hoc parameters only if your client adapter has been set to operate in an ad hoc network. See the Network Type parameter in [Table 5-2](#).

The Advanced (Ad Hoc) screen (see [Figure 5-4](#)) enables you to set parameters that control how the client adapter operates within an ad hoc network. To access this screen, select the **Advanced (Ad Hoc)** tab from the Properties screens.

**Figure 5-4** Advanced (Ad Hoc) Screen



[Table 5-5](#) lists and describes the client adapter's advanced ad hoc parameters. Follow the instructions in the table to change any parameters.

Table 5-5 Advanced (Ad Hoc) Parameters

Parameter	Description
Antenna Mode (Receive)	<p>Specifies the antenna that your client adapter uses to receive data.</p> <ul style="list-style-type: none"> <li>PC card—The PC card’s integrated, permanently attached antenna operates best when used in diversity mode. Diversity mode allows the card to use the better signal from its two antenna ports. <b>Options:</b> Diversity (Both), Primary Antenna Only, Secondary Antenna Only <b>Default:</b> Diversity (Both)</li> <li>LM card—The LM card is shipped without an antenna; however, an antenna can be connected through the card’s external connector. If a snap-on antenna is used, diversity mode is recommended. Otherwise, select the mode that corresponds to the antenna port to which the antenna is connected. <b>Options:</b> Diversity (Both), Primary Antenna Only, Secondary Antenna Only <b>Default:</b> Diversity (Both)</li> <li>PCI card—The PCI card must use the Primary Antenna Only option. <b>Default:</b> Primary Antenna Only</li> <li>Mini PCI card—The mini PCI card, which can be used with one or two antennas, operates best in diversity mode. Diversity mode allows the card to use the better signal from its two antenna connectors. <b>Options:</b> Diversity (Both), Primary Antenna Only, Secondary Antenna Only <b>Default:</b> Diversity (Both)</li> </ul> <p><b>Note</b> This parameter is available only for 2.4-GHz client adapters.</p> <p><b>Note</b> The Primary Antenna Only and Secondary Antenna Only options were formerly named Right Antenna Only and Left Antenna Only, respectively.</p>
Antenna Mode (Transmit)	<p>Specifies the antenna that your client adapter uses to transmit data. See the Antenna Mode (Receive) parameter above for information on the options available for your client adapter.</p> <p><b>Note</b> This parameter is available only for 2.4-GHz client adapters.</p>

Table 5-5 Advanced (Ad Hoc) Parameters (continued)

Parameter	Description
RTS Threshold	<p>Specifies the size of the data packet that the low-level RF protocol issues to a request-to-send (RTS) packet.</p> <p>Setting this parameter to a small value causes RTS packets to be sent more often. When this occurs, more of the available bandwidth is consumed and the throughput of other network packets is reduced, but the system is able to recover faster from interference or collisions, which may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p><b>Range:</b> 0 to 2312</p> <p><b>Default:</b> 2312</p> <p><b>Note</b> Refer to the IEEE 802.11 Standard for more information on the RTS/CTS mechanism.</p>
RTS Retry Limit	<p>Specifies the number of times the client adapter resends a request-to-send (RTS) packet if it does not receive a clear-to-send (CTS) packet from the previously sent RTS packet.</p> <p>Setting this parameter to a large value decreases the available bandwidth whenever interference is encountered but makes the system more immune to interference and collisions, which may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p><b>Range:</b> 1 to 128</p> <p><b>Default:</b> 16 (2.4-GHz client adapters) or 32 (5-GHz client adapters)</p> <p><b>Note</b> Refer to the IEEE 802.11 Standard for more information on the RTS/CTS mechanism.</p>
Wake Duration (K $\mu$ s)	<p>Specifies the amount of time following a beacon that the client adapter stays awake to receive announcement traffic indication message (ATIM) packets, which are sent to the adapter to keep it awake until the next beacon.</p> <p>Refer to the Power Save Mode parameter in <a href="#">Table 5-2</a>.</p> <p><b>Range:</b> 0 K<math>\mu</math>s (in CAM mode); 5 to 60 K<math>\mu</math>s (in Max PSP or Fast PSP mode)</p> <p><b>Default:</b> 5 K<math>\mu</math>s</p> <p><b>Note</b> If your client adapter is set to CAM mode, you must set the wake duration to 0 K<math>\mu</math>s. If your client adapter is set to Max PSP or Fast PSP mode, you must set the wake duration to a minimum of 5 K<math>\mu</math>s.</p> <p><b>Note</b> K<math>\mu</math>s is a unit of measurement in software terms. K = 1024, <math>\mu</math> = 10<sup>-6</sup>, and s = seconds, so K<math>\mu</math>s = .001024 seconds, 1.024 milliseconds, or 1024 microseconds.</p>

Table 5-5 Advanced (Ad Hoc) Parameters (continued)

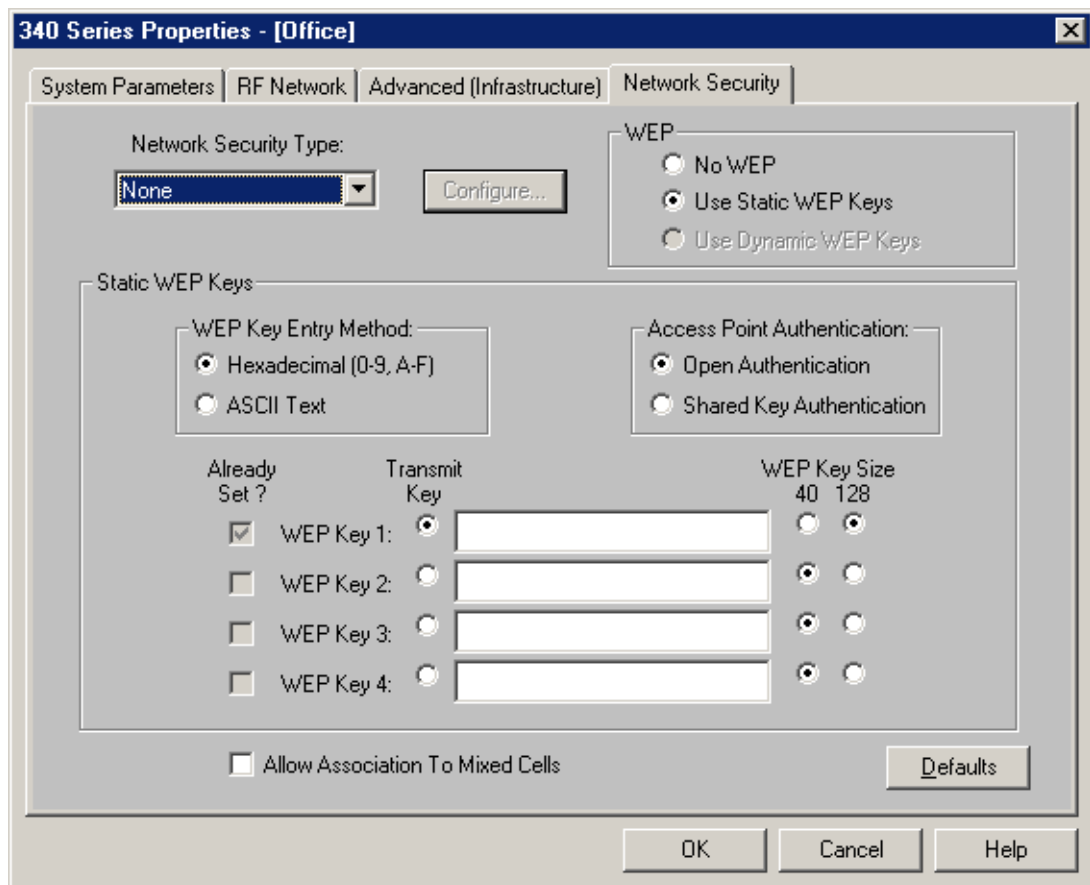
Parameter	Description
Beacon Period (Kμs)	Specifies the duration between beacon packets, which are used to help clients find each other in ad hoc mode. <b>Range:</b> 20 to 976 Kμs <b>Default:</b> 100 Kμs

Go to the next section to set additional parameters or click **OK** to return to the Profile Manager screen. On the Profile Manager screen, click **OK** or **Apply** to save your changes.

## Setting Network Security Parameters

The Network Security screen (see Figure 5-5) enables you to set parameters that control how the client adapter associates to an access point, authenticates to the wireless network, and encrypts and decrypts data. To access this screen, select the **Network Security** tab from the Properties screens.

Figure 5-5 Network Security Screen





This screen is different from the other Properties screens in that it presents several security features, each of which involves a number of steps. In addition, the security features themselves are complex and need to be understood before they are implemented. Therefore, this section provides an overview of the security features as well as procedures for using them.

However, before you determine the appropriate security settings for your client adapter, you must decide how to set the **Allow Association To Mixed Cells** parameter, which appears at the bottom of the Network Security screen and is not associated to any of the security features. See the “[Setting the Allow Association To Mixed Cells Parameter](#)” section below.

## Setting the Allow Association To Mixed Cells Parameter

The Allow Association To Mixed Cells parameter indicates whether the client adapter can associate to an access point that allows both WEP and non-WEP associations. Follow the steps below to set this parameter.

- 
- Step 1** Perform one of the following:
- Select the **Allow Association To Mixed Cells** check box 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. Otherwise, the client is unable to establish a connection with the access point.
  - Deselect the **Allow Association To Mixed Cells** check box if the access point with which the client adapter is to associate does not have WEP set to Optional. This is the default setting.



---

**Note** For security reasons, Cisco recommends that WEP-enabled and WEP-disabled clients not be allowed in the same cell because broadcast packets are sent unencrypted, even to clients running WEP.

---

- Step 2** Perform one of the following:
- If you do not want to change any other parameters on the Network Security screen, click **OK** to return to the Profile Manager screen; then click **OK** or **Apply** to save your changes
  - If you want to change some of the other parameters on the Network Security screen, go to the next section.
- 

## Overview of Security Features

You can protect your data as it is transmitted through your wireless network by encrypting it through the use of Wired Equivalent Privacy (WEP) encryption keys. With WEP encryption, the transmitting device encrypts each packet with a WEP key, and the receiving device uses that same key to decrypt each packet.

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

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

**Note**

Refer to the [“Additional WEP Key Security Features”](#) section on page 5-25 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; therefore, they cannot be read back from the client adapter, and they are lost when power to the adapter is removed or the Windows device is rebooted. Although the keys are temporary, you do not need to re-enter them each time the client adapter is inserted or the Windows device is rebooted. This is because the keys are stored (in an encrypted format for security reasons) in the registry of the Windows device. When the driver loads and reads the client adapter’s registry parameters, it also finds the static WEP keys, unencrypts them, and stores them in volatile memory on the adapter.

The Network Security screen 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 5-28 for instructions.

## EAP (with Static or Dynamic WEP Keys)

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.

Two 802.1X authentication types can be selected in ACU for use with Windows operating systems:

- **EAP-Cisco Wireless** (or **LEAP**)—This authentication type is available for Windows 95, 98, NT, 2000, Me, and XP, as well as non-Windows systems. Support for LEAP is provided not in the Windows 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 greater, Cisco Access Registrar version 1.7 and greater, and Funk Software’s Steel-Belted RADIUS version 3.0 and greater.

LEAP is enabled or disabled for a specific profile through ACU, provided LEAP was selected during ACU installation. Once enabled, a variety of configuration options are available, including how and when a username and password are entered to begin the authentication process.

The username and password are used by the client adapter to perform mutual authentication with the RADIUS server through the access point. The username and password are stored in the client adapter’s volatile memory; therefore, they are temporary and need to be re-entered whenever power is removed from the adapter, typically due to the client adapter being ejected or the system powering down.



**Note** If LEAP was not selected during installation, the LEAP option is unavailable in ACU. If you want to be able to enable and disable LEAP, you must run the installation program again and select **Modify** and **LEAP**.

- **Host Based EAP**—Selecting this option enables you to use any 802.1X authentication type for which your operating system has support. For example, Windows 2000 (with Service Pack 3 or greater and the Windows 2000 Wireless 802.1X hot fix) and Windows XP provide native support for EAP-TLS and EAP-MD5 authentication and general support for PEAP and EAP-SIM authentication.



**Note** To use EAP-TLS, EAP-MD5, PEAP, or EAP-SIM with Windows 2000, you must install Windows Service Pack 3, the Windows 2000 Wireless 802.1X hot fix, and ACU; configure your client adapter using ACU; and enable Network-EAP on the access point.



**Note** To use PEAP or EAP-SIM authentication, you must also install either the PEAP or EAP-SIM supplicant during ACU installation.



**Note** PC-Cardbus cards do not support PEAP and EAP-SIM authentication.

- **EAP-TLS**—EAP-TLS 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. Once enabled, a few configuration parameters must be set within the operating system.

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



**Note** EAP-TLS requires the use of a certificate. Refer to Microsoft's documentation for information on downloading and installing the certificate.

- **EAP-MD5**—EAP-MD5 is enabled or disabled through the operating system and uses static WEP to encrypt data. EAP-MD5 requires you to enter a separate EAP username and password (in addition to your standard Windows network login) in order to start the EAP authentication process and gain access to the network.

RADIUS servers that support EAP-MD5 include Cisco Secure ACS version 3.0 or greater and Cisco Access Registrar version 1.8 or greater.



**Note** If you want to authenticate without encrypting the data that is transmitted over your network, you can use EAP-MD5 without static WEP.

- **Protected EAP (or PEAP)**—PEAP authentication is designed to support One-Time Password (OTP), Windows NT or 2000 domain, and LDAP user databases over a wireless LAN. It is based on EAP-TLS authentication but uses a password or PIN instead of a client certificate for authentication. PEAP 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. If your network uses an OTP user database, PEAP requires you to enter either a hardware token password or a software token PIN to start the EAP authentication process and gain access to the network. If your network uses a Windows NT or 2000 domain user database or an LDAP user database (such as NDS), PEAP requires you to enter your username, password, and domain name in order to start the authentication process.

RADIUS servers that support PEAP authentication include Cisco Secure ACS version 3.1 or greater.



**Note** Service Pack 1 for Windows XP includes Microsoft's PEAP supplicant, which supports a Windows username and password only and does not interoperate with Cisco's PEAP supplicant. To use Cisco's PEAP supplicant, install ACU version 5.05 or greater after Service Pack 1 for Windows XP. Otherwise, it will be overwritten by Microsoft's PEAP supplicant.

- **EAP-SIM**—EAP-SIM authentication is designed for use in public wireless LANs with clients containing Gemplus SIM+ smartcards in PCSC-compliant smartcard readers. EAP-SIM 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-SIM requires you to enter a user verification code, or *PIN*, for communication with the SIM card. You can choose to have the PIN stored in your computer or to be prompted to enter it only after a reboot or prior to every authentication attempt.

RADIUS servers that support EAP-SIM include Cisco Access Registrar version 3.0 or greater.



**Note** Because EAP-TLS, EAP-MD5, PEAP, and EAP-SIM authentication are enabled in the operating system and not 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 Windows 2000 (with Service Pack 3 or greater and the Windows 2000 Wireless 802.1X hot fix) or Windows XP. In addition, Windows can be set for only one authentication type 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 authentication types in Windows after switching profiles in ACU.

When you enable Network-EAP or Require EAP on your access point and configure your client adapter for LEAP, EAP-TLS, EAP-MD5, PEAP, or EAP-SIM, authentication to the network occurs in the following sequence:

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



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

2. Communicating through the access point, the client and RADIUS server complete the authentication process, with the password (LEAP, EAP-MD5, and PEAP), certificate (EAP-TLS), or internal key stored on the SIM card and in the service provider's Authentication Center (EAP-SIM) being the shared secret for authentication. The password, certificate, or internal key is never transmitted during the process.



---

**Note** The authentication process is now complete for EAP-MD5. For LEAP, EAP-TLS, PEAP, and EAP-SIM, the process continues.

---

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

Refer to the “Enabling LEAP” section on page 5-31 for instructions on enabling LEAP or to the “Enabling Host-Based EAP” section on page 5-34 for instructions on enabling EAP-TLS, EAP-MD5, PEAP, or EAP-SIM.



**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)

---

## 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 are supported in the following client adapter software releases:

- PCM/LMC/PCI card firmware version 4.25.23 or greater and driver version 8.01 or greater
- Mini PCI card firmware version 5.0 or greater and driver version 2.20 or greater
- PC-Cardbus card firmware version 4.99 or greater and driver version 3.4 or greater

These features do not need to be enabled on the client adapter; they are supported automatically in the firmware and driver versions listed above. However, they must be enabled on the access point.



**Note**

---

Access point firmware version 11.10T or greater is required to enable these security features. Refer to the Software Configuration Guide for your access point for instructions on enabling these security features.

---

## Message Integrity Check (MIC)

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

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

**Note**

If you enable MIC on the access point, your client adapter's driver must support these features; 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 these features; 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-TLS, PEAP, or EAP-SIM authentication can associate to the access point. Client devices using static WEP (with open, shared key, or EAP-MD5 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 5-6](#) 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 Software Configuration Guide for your access point for instructions on enabling any of these features.

**Table 5-6 Client and Access Point Security Settings**

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Create a WEP key and enable Use Static WEP Keys and Open Authentication	Set up and enable WEP and enable Open Authentication
Static WEP with shared key authentication	Create a WEP key and enable Use Static WEP Keys and Shared Key Authentication	Set up and enable WEP and enable Shared Key Authentication
LEAP authentication	Enable LEAP	Set up and enable WEP and enable Network-EAP

**Table 5-6 Client and Access Point Security Settings (continued)**

Security Feature	Client Setting	Access Point Setting
EAP-TLS authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select Enable network access control using IEEE 802.1X and Smart Card or Other Certificate as the EAP Type in Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix) or Windows XP	Set up and enable WEP and enable Network-EAP
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP Type	Set up and enable WEP and enable Require EAP and Open Authentication
EAP-MD5 authentication		
If using ACU to configure card	Create a WEP key, enable Host Based EAP, and enable Use Static WEP Keys in ACU and select Enable network access control using IEEE 802.1X and MD5-Challenge as the EAP Type in Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix) or Windows XP	Set up and enable WEP and enable Network-EAP
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and MD5-Challenge as the EAP Type	Set up and enable WEP and enable Require EAP and Open Authentication
PEAP authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select Enable network access control using IEEE 802.1X and PEAP as the EAP Type in Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix) or Windows XP	Set up and enable WEP and enable Network-EAP
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and PEAP as the EAP Type	Set up and enable WEP and enable Require EAP and Open Authentication

**Table 5-6 Client and Access Point Security Settings (continued)**

Security Feature	Client Setting	Access Point Setting
EAP-SIM authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select Enable network access control using IEEE 802.1X and SIM Authentication as the EAP Type in Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix) or Windows XP	Set up and enable WEP with full encryption and enable Network-EAP
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and SIM Authentication as the EAP Type	Set up and enable WEP with full encryption and enable Require EAP and Open Authentication
MIC	Use PCM/LMC/PCI card driver version 8.01 or greater, mini PCI card driver version 2.20 or greater, or PC-Cardbus card driver version 3.4 or greater	Set up and enable WEP with full encryption, set MIC to MMH, and set Use Aironet Extensions to Yes
TKIP	Use PCM/LMC/PCI card firmware version 4.25.23 or greater, mini PCI card firmware version 5.0 or greater, or PC-Cardbus card firmware version 4.99 or greater	Set up and enable WEP, set TKIP to Cisco, and set Use Aironet Extensions to Yes
Broadcast key rotation	Use PCM/LMC/PCI card firmware version 4.25.23 or greater, mini PCI card firmware version 5.0 or greater, or PC-Cardbus card firmware version 4.99 or greater and enable LEAP	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.

### Entering a New Static WEP Key

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

- 
- Step 1** Select **None** from the Network Security Type drop-down box on the Network Security screen.
  - Step 2** Select **Use Static WEP Keys** under WEP.



**Step 3** Select one of the following WEP key entry methods:

- **Hexadecimal (0-9, A-F)**—Specifies that the WEP key will be entered in hexadecimal characters, which include 0-9, A-F, and a-f.
- **ASCII Text**—Specifies that the WEP key will be entered in ASCII text, which includes alpha characters, numbers, and punctuation marks.



**Note** ASCII text WEP keys are not supported on the Cisco Aironet 1200 Series Access Points, so you must select the Hexadecimal (0-9, A-F) option if you are planning to use your client adapter with these access points.

**Step 4** Select one of the following access point authentication options, which defines how your client adapter will attempt to authenticate to an access point:

- **Open Authentication**—Allows your client adapter, regardless of its WEP settings, to authenticate and attempt to communicate with an access point. Open Authentication is the default setting.
- **Shared Key Authentication**—Allows your client adapter to communicate only with access points that have the same WEP key. This option is available only if **Use Static WEP Keys** is selected.

In shared key authentication, 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. If the packet is successfully encrypted/decrypted, the user is considered to be authenticated.



**Note** Cisco recommends that shared key authentication not be used because it presents a security risk.

**Step 5** 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 screen. 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 6** Obtain the static WEP key from your system administrator and enter it in the blank field for the key you are creating. Follow the guidelines below to enter a new static WEP key:

- WEP keys must contain the following number of characters:
  - 10 hexadecimal characters or 5 ASCII text characters for 40-bit keys  
**Example:** 5A5A313859 (hexadecimal) or ZZ18Y (ASCII)
  - 26 hexadecimal characters or 13 ASCII text characters for 128-bit keys  
**Example:** 5A583135333554595549333534 (hexadecimal) or ZX1535TYUI354 (ASCII)



**Note** You must enter hexadecimal characters for 5-GHz client adapters if these adapters will be used with Cisco Aironet 1200 Series Access Points.

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




---

**Note** After you enter a WEP key, you can write over it, but you cannot edit or delete it.

---

- Step 7** Click the **Transmit Key** button to the left of the key you want to use to transmit packets. Only one WEP key can be selected as the transmit key.
- Step 8** Click **OK** to return to the Profile Manager screen; then click **OK** or **Apply** to save your changes.
- 

## Overwriting an Existing Static WEP Key

Follow the steps below to overwrite an existing static WEP key.




---

**Note** You can overwrite existing WEP keys, but you cannot edit or delete them.

---

- Step 1** Look at the current WEP key settings in the middle of the Network Security screen. A checkmark 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 screen.

---

- Step 2** Decide which existing static WEP key you want to overwrite.
- Step 3** Click within the blank field of that key.
- Step 4** Enter a new key, following the guidelines outlined in [Step 6](#) of the “[Entering a New Static WEP Key](#)” section on page 5-28.
- 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** Click **OK** to return to the Profile Manager screen; then click **OK** or **Apply** to save your changes.
- 

## Disabling Static WEP

If you ever need to disable static WEP for a particular profile, select **No WEP** under WEP on the Network Security screen, click **OK**, and click **OK** or **Apply** on the Profile Manager screen.




---

**Note** Selecting **LEAP** from the Network Security Type drop-down box on the Network Security screen disables static WEP automatically.

---

## Enabling LEAP

**Note**

LEAP authentication is supported only on client adapters that support WEP and use PCM/LMC/PCI card firmware version 4.13 or greater, mini PCI card firmware version 5.0 or greater, or PC-Cardbus card firmware version 4.99 or greater.

**Note**

In order to use LEAP authentication, your client adapter and access point firmware must have matching 802.1X draft standards. That is, if the access point uses draft 8 firmware (prior to 11.06) or has draft 8 selected, the client adapter must use draft 8 firmware (prior to 4.25.x). Similarly, if the access point uses draft 10 firmware (11.06 or later) and has draft 10 selected, the client adapter must use draft 10 firmware (4.25.x or later). Mini PCI card firmware and PC-Cardbus card firmware were first released at draft 10.

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

**Step 1**

Select **LEAP** from the Network Security Type drop-down box on the bottom of the Network Security screen.

**Note**

When you select this option, dynamic WEP is set automatically.

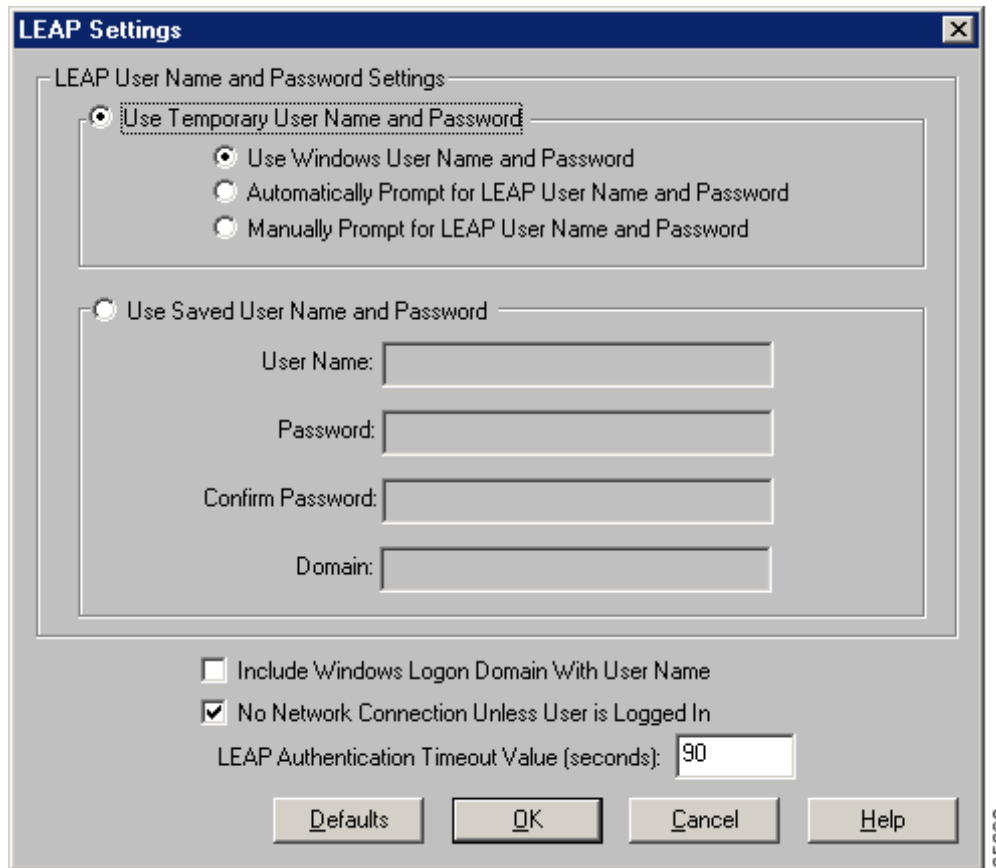
**Note**

The LEAP option is available only if you selected LEAP during the ACU installation process and the firmware supports it.

**Step 2**

Click **Configure** to the right of the Network Security Type drop-down box. The LEAP Settings screen appears (see [Figure 5-6](#)).

Figure 5-6 LEAP Settings Screen



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

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



**Note** The Use Saved User Name and Password option is available only if the Allow Saved LEAP User Name and Password check box was selected during installation.



**Note** If a profile is using LEAP, it can be included in auto profile selection only if it has a saved username and password. The Include Profile In Auto Profile Selection check box on the Profile Manager screen is grayed out and cannot be selected for profiles that are using LEAP without a saved username and password.

**Step 4** Perform one of the following:

- If you selected Use Temporary User Name and Password in [Step 3](#), select one of the following options:
  - **Use Windows User Name and Password**—Causes your Windows username and password to also serve as your LEAP username and password, giving you only one set of credentials to remember. After you log in, the LEAP authentication process begins automatically. This option is the default setting.
  - **Automatically Prompt for LEAP User Name and Password**—Requires you to enter a separate LEAP username and password (which are registered with the RADIUS server) in addition to your regular Windows login in order to start the LEAP authentication process.
  - **Manually Prompt for LEAP User Name and Password**—Requires you to manually invoke the LEAP authentication process as needed using the Manual LEAP Login option from the Commands drop-down menu. You are not prompted to enter a LEAP username and password during the Windows login. This option might be used to support a software token one-time password system or other systems that require additional software that is not available at login.
- If you selected Use Saved User Name and Password in [Step 3](#), follow the steps below:
  - a. Enter a username and password in the appropriate fields.




---

**Note** Usernames and passwords are limited to 32 ASCII characters each. However, if a domain name is entered in the Domain field, the sum of the username and domain name is limited to 31 ASCII characters.

---

- b. Re-enter the password in the Confirm Password field.
- c. If you wish to specify a domain name that will be passed to the RADIUS server along with your username, enter it in the Domain field.

**Step 5** If you work in an environment with multiple domains and, therefore, want your Windows login domain to be passed to the RADIUS server along with your username, select the **Include Windows Login Domain With User Name** check box. The default setting is selected.




---

**Note** If you selected to use a saved username and password but do not select the Include Windows Login Domain With User Name check box, the Domain field becomes unavailable, and a domain name is not passed to the RADIUS server.

---

**Step 6** If you want to force the client adapter to disassociate after you log off so that another user cannot gain access to the wireless network using your credentials, select the **No Network Connection Unless User is Logged In** check box. The default setting is selected.

**Step 7** In the LEAP Authentication Timeout Value field, enter the amount of time (in seconds) before a LEAP authentication is considered to be failed and an error message appears.

**Range:** 30 to 300 seconds

**Default:** 90 seconds

- Step 8** Click **OK** to exit the LEAP Settings screen.
- Step 9** Click **OK** to exit the Network Security screen and return to the Profile Manager screen. On the Profile Manager screen, click **OK** or **Apply** to save your changes



**Note** [Chapter 6](#) describes the sequence of events that occurs when a profile that is set for LEAP authentication is selected for use.

## Enabling Host-Based EAP

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

- Client adapters must support WEP and use PCM/LMC/PCI card firmware version 4.25 or greater, mini PCI card firmware version 5.0 or greater, or PC-Cardbus card firmware version 4.99 or greater.
- Client adapters and access points must use firmware that supports 802.1X draft 10, which is functionally equivalent to the ratified 802.1X standard.
- PEAP and EAP-SIM authentication are supported only by ACU version 5.05 or greater, 2.4-GHz client adapters, and 340 and 350 series access points running firmware version 11.23T or 1200 series access points running firmware version 11.54T.
- Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix must be installed if your computer is running Windows 2000.
- 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.

Follow the steps below to enable host-based EAP authentication (EAP-TLS, EAP-MD5, PEAP, or EAP-SIM) for this profile.



**Note** Because EAP-TLS, EAP-MD5, PEAP, and EAP-SIM authentication are enabled in the operating system and not 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 Windows 2000 (with Service Pack 3 or greater and the Windows 2000 Wireless 802.1X hot fix) or Windows XP. In addition, Windows can be set for only one authentication type 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 authentication types in Windows after switching profiles in ACU.

- Step 1** Select **Host Based EAP** from the Network Security Type drop-down box on the Network Security screen.



**Note** The Host Based EAP option is available for all operating systems except Windows 95; however, your client adapter can EAP authenticate only if your computer's operating system is Windows 2000 (with Service Pack 3 or greater and the Windows 2000 Wireless 802.1X hot fix) or Windows XP.

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

- If you are planning to use EAP-TLS, PEAP, or EAP-SIM authentication, select **Use Dynamic WEP Keys** under WEP.
- If you are planning to use EAP-MD5 authentication with static WEP, select **Use Static WEP Keys** under WEP. Then follow [Step 3](#) through [Step 7](#) in the “[Entering a New Static WEP Key](#)” section to create a new static WEP key or follow the steps in the “[Overwriting an Existing Static WEP Key](#)” section to overwrite an existing static WEP key.
- If you are planning to use EAP-MD5 authentication without WEP, select **No WEP** under WEP.

**Step 3** Click **OK** to return to the Profile Manager screen.

**Step 4** Click **OK** or **Apply** on the Profile Manager screen to save your changes.

**Step 5** Perform one of the following, depending on your computer’s operating system:

- If your computer is running Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix), double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**. Right-click **Local Area Connection**. Click **Properties**. The Local Area Connection Properties screen appears.
- If your computer is running Windows XP, double-click **My Computer**, **Control Panel**, and **Network Connections**. Right-click **Wireless Network Connection**. Click **Properties**. The Wireless Network Connection Properties screen appears.



---

**Note** These instructions assume you are using Windows XP’s classic view rather than its category view.

---

**Step 6** Click the **Authentication** tab. The following screen appears (see [Figure 5-7](#)).

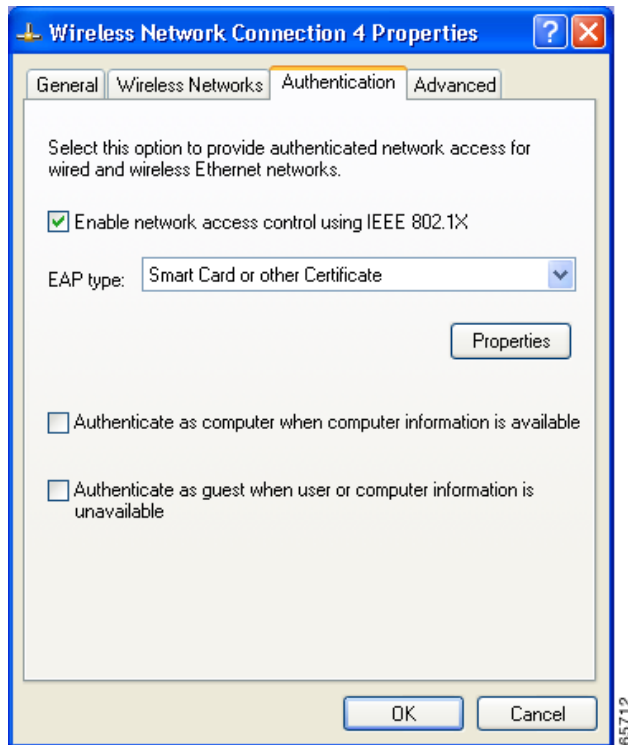


---

**Note** When Service Pack 1 for Windows XP is released, the Authentication tab may move from its current location. To access it, click the **Wireless Networks** tab, select the network that you are configuring in the Preferred network list, and click **Properties**.

---

Figure 5-7 Wireless Network Connection Properties Screen (Authentication Tab)



- Step 7** Select the **Enable network access control using IEEE 802.1X** check box.
- Step 8** 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 EAP-MD5, go to the [“Enabling EAP-MD5”](#) section on page 5-37.
  - If you are planning to use PEAP, go to the [“Enabling PEAP”](#) section on page 5-38.
  - If you are planning to use EAP-SIM, go to the [“Enabling EAP-SIM”](#) section on page 5-40.

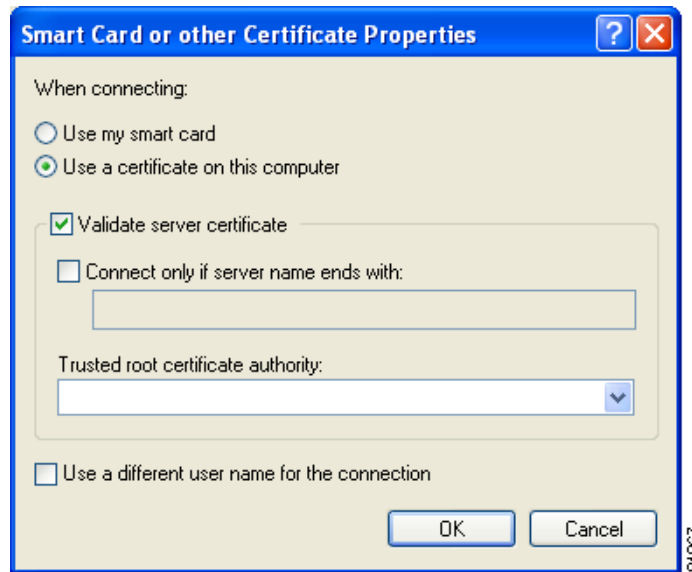
## Enabling EAP-TLS

Follow the steps below to enable EAP-TLS.

- Step 1** For EAP type, select **Smart Card or other Certificate**.
- Step 2** Click **Properties**. The Smart Card or other Certificate Properties screen appears (see [Figure 5-8](#)).



Figure 5-8 Smart Card or other Certificate Properties Screen



**Step 3** Select the **Use a certificate on this computer** option.

**Step 4** Select the **Validate server certificate** check box.

**Step 5** Make sure that the name of the certificate authority from which the EAP-TLS certificate was downloaded appears in the Trusted root certificate authority field.



**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** Click **OK** to save your settings. The configuration is complete.



**Note** [Chapter 6](#) describes the sequence of events that occurs when a profile that is set for EAP authentication is selected for use.

## Enabling EAP-MD5

Follow the steps below to enable EAP-MD5.

**Step 1** For EAP type, select **MD5-Challenge**.

**Step 2** Click **OK** to save your settings. The configuration is complete.



**Note** [Chapter 6](#) describes the sequence of events that occurs when a profile that is set for EAP authentication is selected for use.

## Enabling PEAP

Follow the steps below to enable PEAP.

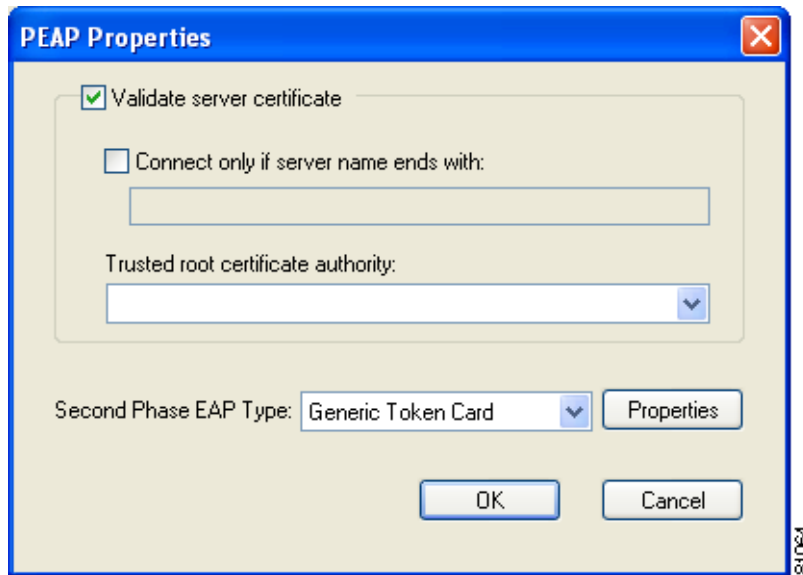


**Note** PC-Cardbus cards do not support PEAP authentication.

**Step 1** For EAP type, select **PEAP**.

**Step 2** Click **Properties**. The PEAP Properties screen appears (see [Figure 5-9](#)).

**Figure 5-9 PEAP Properties Screen**



**Step 3** Select the **Validate server certificate** check box if server certificate validation is required (recommended).

**Step 4** Select the **Connect only if server name ends with** 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.

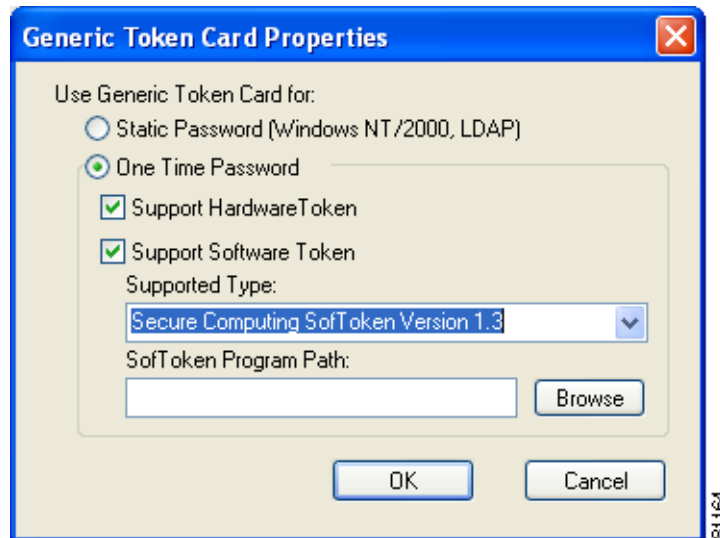
**Step 5** Make sure that the name of the certificate authority from which the server certificate was downloaded appears in the Trusted root certificate authority field.



**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** Currently Generic Token Card is the only second phase EAP type available. Click **Properties**. The Generic Token Card Properties screen appears (see [Figure 5-10](#)).

Figure 5-10 Generic Token Card Properties Screen



**Step 7** Select either the **Static Password (Windows NT/2000, LDAP)** or the **One Time Password** option, depending on your user database.

**Step 8** Perform one of the following:

- If you selected the **Static Password (Windows NT/2000, LDAP)** option in [Step 7](#), go to [Step 9](#).
- If you selected the **One Time Password** option in [Step 7](#), select one or both of the following check boxes to specify the type of tokens that will be supported for one-time passwords:
  - **Support Hardware Token**—A hardware token device obtains the one-time password. You must use your hardware token device to obtain the one-time password and enter the password when prompted for your user credentials.
  - **Support Software Token**—The PEAP supplicant works with a software token program to retrieve the one-time password. You have to enter only the PIN, not the one-time password. If you select this check box, you must also select from the Supported Type drop-down box the software token software that is installed on the client (such as Secure Computing SofToken Version 1.3, Secure Computing SofToken II 2.0, or RSA SecurID Software Token v 2.5), and if Secure Computing SofToken Version 1.3 is selected, you must locate the software program path using the Browse button.



**Note** The SofToken Program Path field is unavailable if a software token program other than Secure Computing SofToken Version 1.3 is selected.

**Step 9** Click **OK** to save your settings. The configuration is complete.



**Note** [Chapter 6](#) describes the sequence of events that occurs when a profile that is set for EAP authentication is selected for use.

## Enabling EAP-SIM

Follow the steps below to enable EAP-SIM.



### Note

PC-Cardbus cards do not support EAP-SIM authentication.

- Step 1** For EAP type, select **SIM Authentication**.
- Step 2** Click **Properties**. The SIM Authentication Properties screen appears (see [Figure 5-11](#)).

**Figure 5-11** SIM Authentication Properties Screen



- Step 3** To access any resources (data or commands) on the SIM, the EAP-SIM supplicant must provide a valid PIN to the SIM card, which must match the PIN stored on the SIM. Select one of the following options to specify how the EAP-SIM supplicant should handle the SIM card's PIN:
- **Ask for my PIN once after I turn my computer on (recommended)**—The software does not permanently store the PIN. It prompts you for the PIN once, on the first authentication of every session, where a *session* is defined as the time between power-up and shutdown or reboot.
  - **Ask for my PIN every time the network asks for authentication**—The software never stores the PIN; it prompts you for the PIN every time an EAP-SIM authentication is performed. This option is not recommended if your client will be roaming between access points or if session timeouts are implemented (such as for accounting and security purposes).
  - **Let me give my PIN to the computer now and never ask me again; PIN will be encrypted and stored on computer (not recommended)**—You need to enter the PIN only once, in the Enter PIN edit box below this option. The software stores the PIN in the registry and retrieves it from there when required. If you select this option, you must enter the PIN now. The PIN is validated when an authentication attempt is made.



**Note** This option is not recommended because it enables others to use the SIM without knowing the PIN.

- Step 4** Click **OK** to save your settings. The configuration is complete.
- Step 5** If you are prompted to restart your client adapter, turn off your client adapter's radio, wait a few seconds, and then turn the radio back on. Refer to the "[Turning Your Client Adapter's Radio On or Off](#)" section on page 8-29 for instructions.



**Note** [Chapter 6](#) describes the sequence of events that occurs when a profile that is set for EAP authentication is selected for use.

## Disabling LEAP or Host-Based EAP

If you ever need to disable LEAP or host-based EAP for a particular profile, follow the instructions below for your EAP authentication type.

### Disabling LEAP

To disable LEAP for a particular profile, select **None** from the Network Security Type drop-down box on the Network Security screen in ACU, click **OK**, and click **OK** or **Apply** on the Profile Manager screen.

### Disabling Host-Based EAP

To disable host-based EAP (EAP-TLS, EAP-MD5, PEAP, or EAP-SIM) for a particular profile, follow the steps below:

- Step 1** Select **None** from the Network Security Type drop-down box on the Network Security screen in ACU and click **OK**.
- Step 2** Click **OK** or **Apply** on the Profile Manager screen.
- Step 3** Perform one of the following, depending on your computer's operating system:
- If your computer is running Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix), double-click **My Computer**, **Control Panel**, and **Network and Dial-up Connections**. Right-click **Local Area Connection**. Click **Properties**. The Local Area Connection Properties screen appears.
  - If your computer is running Windows XP, double-click **My Computer**, **Control Panel**, and **Network Connections**. Right-click **Wireless Network Connection**. Click **Properties**. The Wireless Network Connection Properties screen appears.

**Step 4** Click the **Authentication** tab.



---

**Note** When Service Pack 1 for Windows XP is released, the Authentication tab may move from its current location. To access it, click the **Wireless Networks** tab, select the network that you are configuring in the Preferred network list, and click **Properties**.

---

**Step 5** Deselect the **Enable network access control using IEEE 802.1X** check box.

**Step 6** Click **OK**.

---



## 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, page 6-2](#)
- [Using LEAP with the Windows Username and Password, page 6-3](#)
- [Using LEAP with an Automatically Prompted Login, page 6-5](#)
- [Using LEAP with a Manually Prompted Login, page 6-8](#)
- [Using LEAP with a Saved Username and Password, page 6-11](#)
- [Using EAP-TLS, page 6-12](#)
- [Using EAP-MD5, page 6-13](#)
- [Using PEAP, page 6-13](#)
- [Using EAP-SIM, page 6-17](#)

# Overview

This chapter explains the sequence of events that occurs as soon as you or ACU's auto profile selection feature selects a profile that uses EAP authentication as well as after you eject and reinsert the client adapter, reboot the computer, log on while this profile is selected, or are informed that your username and password have expired. The chapter contains eight sections based on the profile's authentication type and its username and password settings: LEAP (with the Windows username and password, with an automatically prompted login, with a manually prompted login, or with a saved username and password), EAP-TLS, EAP-MD5, PEAP, and EAP-SIM.

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


**Note**

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

## Using LEAP

When LEAP authentication begins, the "LEAP Authentication in progress" message appears. This message provides information about the status of authentication. [Table 6-1](#) lists and explains the stages of LEAP authentication.

**Table 6-1 Stages of LEAP Authentication**

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



# Using LEAP with the Windows Username and Password

## After Profile Selection or Card Insertion

After you (or auto profile selection) select a profile that uses LEAP authentication and specifies that your Windows username and password also serve as your LEAP username and password or you eject and reinsert the client adapter while this profile is selected, the following events occur:

1. The “LEAP Authentication in progress” message appears.
2. If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows “LEAP Authenticated.”

If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the “Error Messages” section in [Chapter 9](#) for the necessary action to take.

## After a Reboot or Logon

After your computer reboots or you log on, follow the steps below to LEAP authenticate.

- Step 1** When the Windows login screen appears (see [Figure 6-1](#) and [Figure 6-2](#)), enter your Windows username and password and click **OK**. The domain name is optional.



**Note** If your computer is running Windows NT, 2000, or XP and has Novell Client 32 software installed, a separate LEAP login screen appears before the Novell login screen. If this occurs, enter your Windows and Novell username and password in the login screens and click **OK**.

**Figure 6-1** Windows Login Screen (Windows 95, 98, and Me)

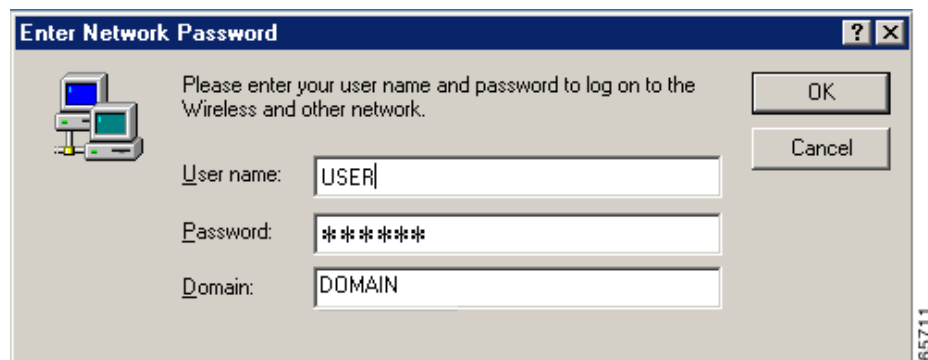


Figure 6-2 Windows Login Screen (Windows 2000)



**Note** The Windows login screens shown above appear on computers running Windows 95, 98, and Me (Figure 6-1) and Windows 2000 (Figure 6-2), respectively. The login screen looks slightly different on computers running Windows NT and XP.

The “LEAP Authentication in progress” message appears.

**Step 2** If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows “LEAP Authenticated.”

If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the “Error Messages” section in Chapter 9 for the necessary action to take.

**Step 3** Windows continues to log you onto the system.

## After Your LEAP Credentials Expire

If the LEAP credentials (username and password) for your current profile expire or become invalid, follow the steps below to reauthenticate.



**Note**

If your computer is running Windows NT, 2000, or XP and you change your Windows password using the standard Windows Change Password function, the client updates the LEAP password automatically and maintains its connection to the access point if the current profile uses the Windows username and password. If your computer is running Windows 95, 98, or Me and you change your Windows password, the client loses association from the access point, and you are prompted to enter your new credentials.

- Step 1** Click **OK** when the following message appears: “The user name and password entered for profile 'xxx' are no longer valid and have failed the LEAP authentication. Please enter a new user name and password.”
- Step 2** When the Windows login screen appears, enter your new username and password and click **OK**. The client adapter should authenticate using your new credentials.



**Note** If you click Cancel rather than OK on the Windows login screen, the following message appears: “The current profile will be disabled until the system restarts or you eject and reinsert the card. Are you sure?” If you click No, the Windows login reappears and allows you to enter your new credentials. If you click Yes, the current profile is disabled until you reboot your computer or eject and reinsert the card. The Current Profile field on the Status screen lists the profile as being “Disabled.”

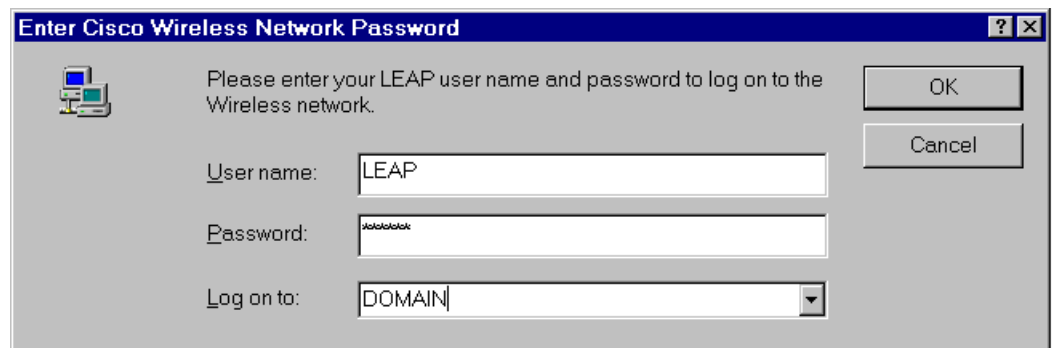
## Using LEAP with an Automatically Prompted Login

### After Profile Selection or Card Insertion

After you (or auto profile selection) select a profile that uses LEAP authentication but specifies that you be automatically prompted to enter a separate LEAP username and password or you eject and reinsert the client adapter while this profile is selected, follow the steps below to LEAP authenticate.

- Step 1** When the LEAP login screen appears (see [Figure 6-3](#)), enter your LEAP username and password and click **OK**. The domain name is optional.

**Figure 6-3** LEAP Login Screen



**Note** The LEAP login screen shown above appears on computers running Windows NT, 2000, or XP. The LEAP login screen looks slightly different on computers running other Windows operating systems.

The “LEAP Authentication in progress” message appears.

- Step 2** If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows “LEAP Authenticated.”

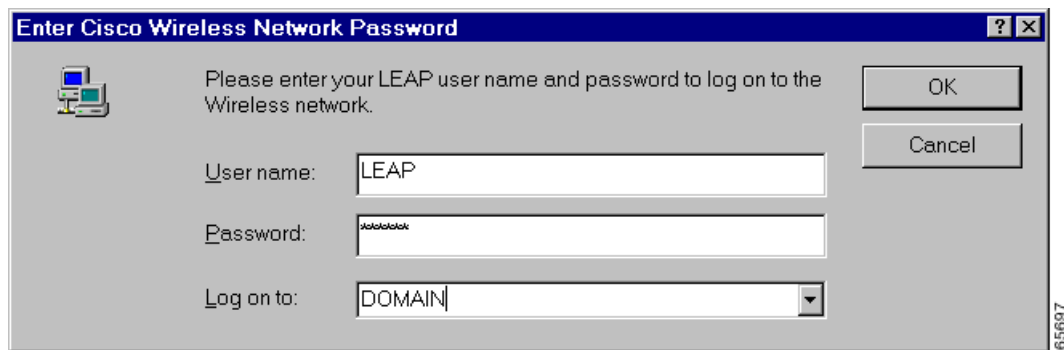
If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the “Error Messages” section in [Chapter 9](#) for the necessary action to take.

## After a Reboot or Logon

After your computer reboots or you log on, follow the steps below to LEAP authenticate.

- Step 1** When the LEAP login screen appears (see [Figure 6-4](#)), enter your LEAP username and password and click **OK**. The domain name is optional.

**Figure 6-4** LEAP Login Screen



**Note** The LEAP login screen shown above appears on computers running Windows NT, 2000, or XP. The LEAP login screen looks slightly different on computers running other Windows operating systems.

The “LEAP Authentication in progress” message appears.

- Step 2** If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows “LEAP Authenticated.”

If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the “Error Messages” section in [Chapter 9](#) for the necessary action to take.

- Step 3** When the network login screen appears (see [Figure 6-5](#) and [Figure 6-6](#)), enter your network username and password and click **OK**.



**Note** [Figure 6-5](#) shows an example network login screen that may appear on computers running Windows 95, 98, and Me. Your screen may look different. [Figure 6-6](#) shows the network login screen that appears on Windows 2000 systems. The login screen looks slightly different on computers running Windows NT and XP.

Figure 6-5 Network Login Screen (Windows 95, 98, and Me)

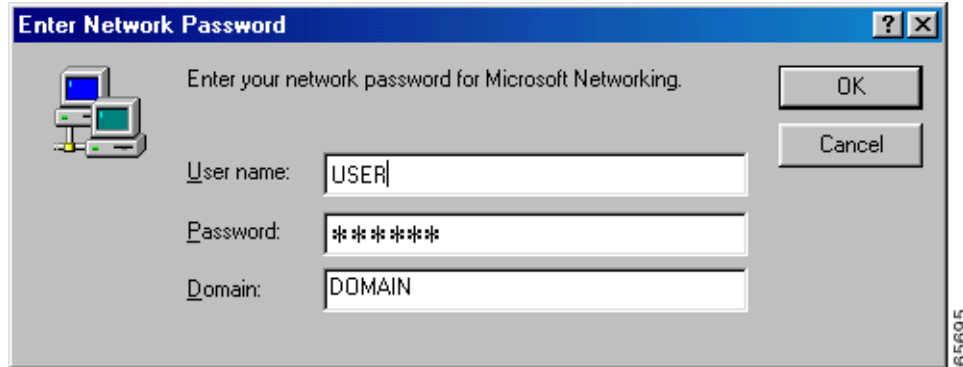


Figure 6-6 Network Login Screen (Windows 2000)



## After Your LEAP Credentials Expire

If the LEAP credentials (username and password) for your current profile expire or become invalid, follow the steps below to reauthenticate.

- Step 1** Click **OK** when the following message appears: “The user name and password entered for profile 'xxx' are no longer valid and have failed the LEAP authentication. Please enter a new user name and password.”
- Step 2** When the LEAP login screen appears, enter your new username and password and click **OK**. The client adapter should authenticate using your new credentials.

**Note**

If you click Cancel rather than OK on the LEAP login screen, the following message appears: “The current profile will be disabled until the system restarts or you eject and reinsert the card. Are you sure?” If you click No, the LEAP login reappears and allows you to enter your new credentials. If you click Yes, the current profile is disabled until you reboot your computer or eject and reinsert the card. The Current Profile field on the Status screen lists the profile as being “Disabled.”

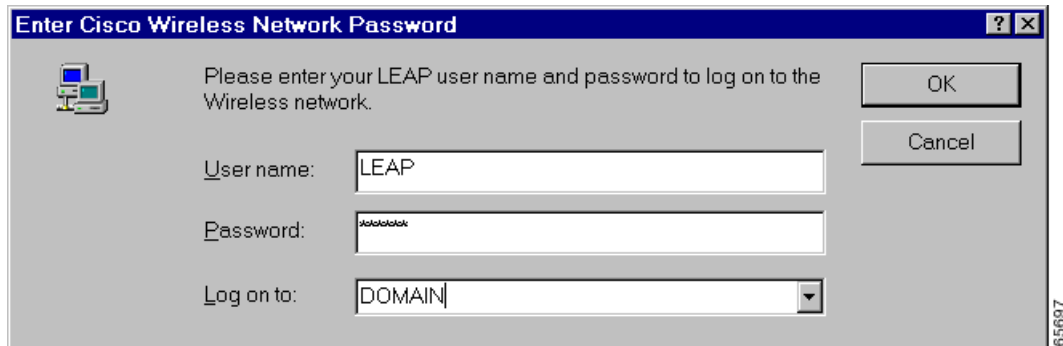
## Using LEAP with a Manually Prompted Login

### After Profile Selection

After you (or auto profile selection) select a profile that uses LEAP authentication but specifies that the process be manually invoked, follow the steps below to LEAP authenticate.

- Step 1** When the LEAP login screen appears (see [Figure 6-7](#)), enter your LEAP username and password and click **OK**. The domain name is optional.

**Figure 6-7** LEAP Login Screen

**Note**

The LEAP login screen shown above appears on computers running Windows NT, 2000, or XP. The LEAP login screen looks slightly different on computers running other Windows operating systems.

The “LEAP Authentication in progress” message appears.

- Step 2** If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows “LEAP Authenticated.”

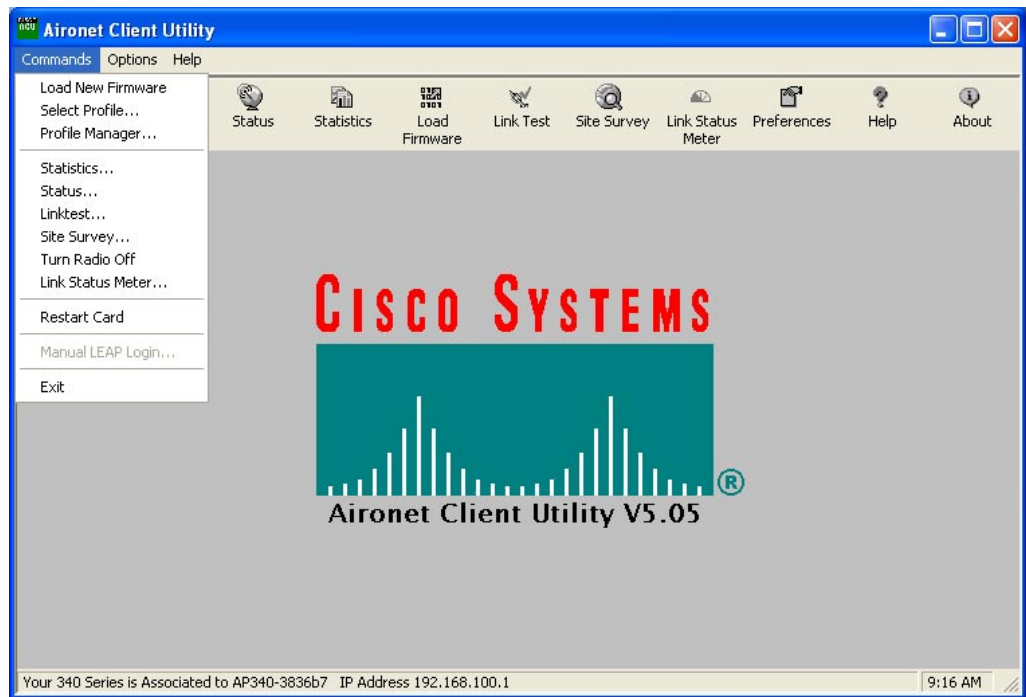
If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the “[Error Messages](#)” section in [Chapter 9](#) for the necessary action to take.

## After a Reboot, Logon, or Card Insertion

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

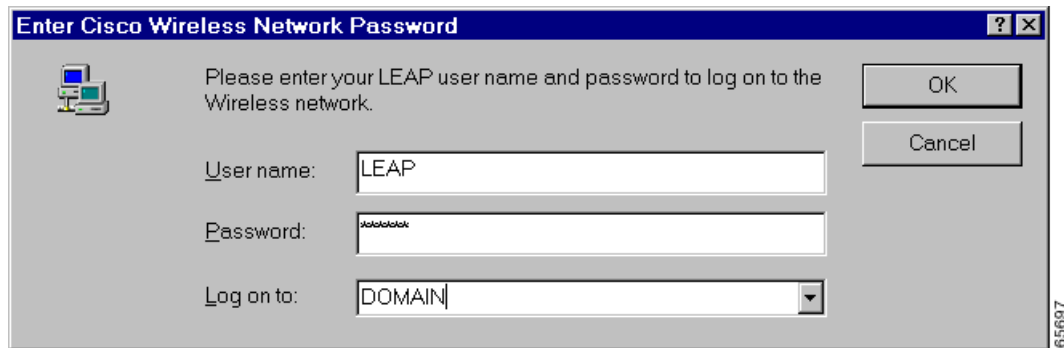
- Step 1** If you rebooted your computer or logged on, complete your standard Windows login.
- Step 2** Double-click the **Aironet Client Utility (ACU)** icon on your desktop to open ACU.
- Step 3** Select the **Manual LEAP Login** option from the Commands drop-down menu (see [Figure 6-8](#)).

**Figure 6-8** Commands Drop-Down Menu



- Step 4** When the LEAP login screen appears (see [Figure 6-9](#)), enter your LEAP username and password and click **OK**. The domain name is optional.

Figure 6-9 LEAP Login Screen



**Note** The LEAP login screen shown above appears on computers running Windows NT, 2000, or XP. The LEAP login screen looks slightly different on computers running other Windows operating systems.

The “LEAP Authentication in progress” message appears.

- Step 5** If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows “LEAP Authenticated.”

If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the “[Error Messages](#)” section in [Chapter 9](#) for the necessary action to take.

## After Your LEAP Credentials Expire

If the LEAP credentials (username and password) for your current profile expire or become invalid, follow the steps below to reauthenticate.

- Step 1** Click **OK** when the following message appears: “The user name and password entered for profile 'xxx' are no longer valid and have failed the LEAP authentication. Please enter a new user name and password.”
- Step 2** When the LEAP login screen appears, enter your new username and password and click **OK**. The client adapter should authenticate using your new credentials.



**Note** If you click Cancel rather than OK on the LEAP login screen, the following message appears: “The current profile will be disabled until the system restarts or you eject and reinsert the card. Are you sure?” If you click No, the LEAP login reappears and allows you to enter your new credentials. If you click Yes, the current profile is disabled until you reboot your computer or eject and reinsert the card. The Current Profile field on the Status screen lists the profile as being “Disabled.”



# Using LEAP with a Saved Username and Password

## After Profile Selection or Card Insertion

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

1. The “LEAP Authentication in progress” message appears.
2. If your client adapter authenticates, the message disappears, and the Server Based Authentication field on the ACU Status screen shows “LEAP Authenticated.”

If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the “[Error Messages](#)” section in [Chapter 9](#) for the necessary action to take.

## After a Reboot or Logon

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

1. After you enter your Windows username and password, the LEAP authentication process begins automatically using your saved LEAP username and password.
2. If your client adapter authenticates, the “LEAP Authentication in progress” message disappears, and the Server Based Authentication field on the ACU Status screen shows “LEAP Authenticated.”

If the authentication attempt fails, an error message appears after the LEAP timeout period has expired. Refer to the “[Error Messages](#)” section in [Chapter 9](#) for the necessary action to take.

3. Windows continues to log you onto the system.

## After Your LEAP Credentials Expire

If the LEAP credentials (username and password) for your current profile expire or become invalid, follow the steps below to reauthenticate.

- 
- Step 1** Click **OK** when the following message appears: “The user name and password entered for saved profile 'xxx' are no longer valid and have failed the LEAP authentication. Please enter a new user name and password. Please also remember to change them permanently in the saved profile using the ACU Profile Manager.”
- Step 2** When the LEAP login screen appears, enter your new username and password and click **OK**. The client adapter should authenticate using your new credentials.



**Note**

If you click Cancel rather than OK on the LEAP login screen, the following message appears: “The current profile will be disabled until the system restarts or you eject and reinsert the card. Are you sure?” If you click No, the LEAP login reappears and allows you to enter your new credentials. If you click Yes, the current profile is disabled until you reboot your computer or eject and reinsert the card. The Current Profile field on the Status screen lists the profile as being “Disabled.”

---

- Step 3** Edit the profile in ACU by changing the saved username and password on the LEAP Settings screen.
- Step 4** Save the changes to your profile.
- 

## Using EAP-TLS

### After Profile Selection or Card Insertion

After you (or auto profile selection) select a profile that uses host-based EAP authentication and you configure the card in Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix) or XP for EAP-TLS authentication or you eject and reinsert the client adapter while this profile is selected, follow the steps below to EAP authenticate.

- Step 1** If your computer is running Windows XP and a pop-up message appears above the Windows system tray informing you that you need to accept a certificate to begin the EAP authentication process, click the message and follow the instructions provided to accept the certificate.



**Note** You should not 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, click **OK** to accept the connection. Otherwise, click **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, click **OK** to accept the connection. Otherwise, click **Cancel**.
- Step 4** The client adapter should now EAP authenticate. To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. Click **View** and **Refresh** to obtain the current status. The status appears to the right of your Wireless Network Connection. If the client adapter is authenticated, the status reads, "Authentication succeeded."
- 

### After a Reboot or Logon

After your computer reboots or you log on using your Windows username and password, the EAP authentication process begins automatically and the client adapter should EAP authenticate.

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

## Using EAP-MD5

After you (or auto profile selection) select a profile that uses host-based EAP authentication and configure the card in Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix) or XP for EAP-MD5 authentication, follow the steps below to EAP authenticate.

**Note**

---

These instructions are applicable after profile selection, card ejection and re-insertion, reboot, or logon.

---

- Step 1** Perform one of the following:
- If your computer is running Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix), the Wireless Network Connection screen appears.
  - If your computer is running Windows XP, a pop-up message appears above the Windows system tray informing you that you need to enter your credentials to access the network. Click this message, and the Wireless Network Connection screen appears.
- Step 2** Enter your EAP-MD5 authentication username, password, and optional domain name (which are registered with the RADIUS server) and click **OK**.
- Step 3** The client adapter should now EAP authenticate. To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. Click **View** and **Refresh** to obtain the current status. The status appears to the right of your Wireless Network Connection. If the client adapter is authenticated, the status reads, "Authentication succeeded."
- 

## Using PEAP

### After Profile Selection, Card Insertion, Reboot, or Logon

After you (or auto profile selection) select a profile that uses host-based EAP authentication and you configure the card in Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix) or XP for PEAP authentication, follow the steps in one of the sections below, depending on your user database, to EAP authenticate.

**Note**

---

These instructions are applicable after profile selection, card ejection and re-insertion, reboot, or logon.

---

## Windows NT or 2000 Domain Databases or LDAP Databases Only

- Step 1** If your computer is running Windows XP, a pop-up message appears above the Windows system tray informing you that you need to select a certificate or other credentials to access the network. Click 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, click **OK** to accept the connection. Otherwise, click **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, click **OK** to accept the connection. Otherwise, click **Cancel**.
- Step 4** Perform one of the following:
- If your computer is running Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix), the Static Password screen appears (see [Figure 6-10](#)). Go to [Step 5](#).
  - If your computer is running Windows XP, a pop-up message appears above the Windows system tray prompting you to process your logon information for your wireless network. Click this message. The Static Password screen appears (see [Figure 6-10](#)).

**Figure 6-10** Static Password Screen



- Step 5** Enter your PEAP authentication username and password (which are registered with the RADIUS server).
- Step 6** Select your domain name from the drop-down list or type it in if applicable and click **OK**. The client adapter should now EAP authenticate.
- Step 7** If you also have a locally cached Windows password, you must change it manually in Windows to synchronize your passwords. To do so, press **Ctrl-Alt-Delete**, select **Change Password**, and enter your old password once and your new password twice.

## OTP Databases Only

- Step 1** If your computer is running Windows XP, a pop-up message appears above the Windows system tray informing you that you need to select a certificate or other credentials to access the network. Click 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, click **OK** to accept the connection. Otherwise, click **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, click **OK** to accept the connection. Otherwise, click **Cancel**.
- Step 4** Perform one of the following:
- If your computer is running Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix), the One Time Password screen appears (see [Figure 6-11](#)).
  - If your computer is running Windows XP, a pop-up message appears above the Windows system tray prompting you to process your logon information for your wireless network. Click this message. The One Time Password screen appears (see [Figure 6-11](#)).

**Figure 6-11 One Time Password Screen**



- Step 5** Enter your PEAP authentication username in the User Name field.
- Step 6** Select either the **Hardware Token** or **Software Token** option. If you select the Software Token option, the Password field on the One Time Password screen changes to the PIN field.



**Note** The Hardware Token and Software Token options are available only if you selected both of them on the Generic Token Card Properties screen during configuration. Otherwise, only the option you selected will be available.

- Step 7** Enter either your hardware token password or your software token PIN.
- Step 8** Click **OK**. The client adapter should now EAP authenticate.

## 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 user ID expires, follow the steps below to change your password.

- Step 1** When the Change Password screen appears (see [Figure 6-12](#)) to indicate that your password has expired, enter your old password in the Old Password field.

**Figure 6-12** Change Password Screen



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

## After Your PIN Expires (OTP Databases Only)

If you are using an OTP database with PEAP and the PIN for your current user ID expires, follow the steps below to change your PIN.

- Step 1** When the Change PIN screen appears (see [Figure 6-13](#)) to indicate that your PIN has expired, enter your old PIN in the Old PIN field.

Figure 6-13 Change PIN Screen

- Step 2** Enter your new PIN in both the New PIN and Confirm New PIN fields.
- Step 3** Enter a word that will help you to remember your PIN in the PIN Hint Phrase field.
- Step 4** Click **OK**. The client adapter should authenticate using your new PIN.



**Note** You should use the new PIN for future authentication attempts.

## Using EAP-SIM

After you (or auto profile selection) select a profile that uses host-based EAP authentication and you configure the card in Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix) or XP for EAP-SIM authentication, the authentication process varies depending on the configuration option you selected for the SIM card's PIN.

## If You Are Prompted for the PIN

If you chose to be prompted for the PIN after a power-up or reboot or at every authentication request, follow the steps below to EAP authenticate.



**Note** These instructions are applicable after profile selection, card ejection and re-insertion, reboot, or logon.

- Step 1** Perform one of the following:
- If your computer is running Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix), the Enter PIN screen appears (see [Figure 6-14](#)).
  - If your computer is running Windows XP, a pop-up message appears above the Windows system tray informing you that you need to enter your credentials to access the network. Click this message. The Enter PIN screen appears (see [Figure 6-14](#)).

**Figure 6-14 Enter PIN Screen**



- Step 2** Enter your PIN and click **OK**. The computer now retrieves information from the SIM card. If you enter the PIN incorrectly, you will receive an error message.



**Note** If you exceed the maximum number of retries for entering the PIN, the card locks up.

- Step 3** The client adapter should now EAP authenticate. To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. Click **View** and **Refresh** to obtain the current status. The status appears to the right of your Wireless Network Connection. If the client adapter is authenticated, the status reads, "Authentication succeeded."



**Note** ACU and the Windows Network Connection icon on the Windows XP taskbar may indicate a connection status when authentication is still in the pending state or the authentication server fails to respond.



## If the PIN Is Stored on the Computer

**Note**

---

These instructions are applicable after profile selection, card ejection and re-insertion, reboot, or logon.

---

If you chose to store the PIN in the computer's registry, the EAP authentication process begins automatically and the client adapter should EAP authenticate and use the saved PIN to access the SIM card.

**Note**

---

If the stored PIN is wrong and therefore rejected by the SIM, the EAP-SIM supplicant temporarily changes the prompt mode to the default setting (Ask for my PIN once after I turn my computer on) in order to prevent the SIM from locking up. Unless changed manually, this setting stays in effect until your computer is powered off. Change your stored PIN on the SIM Authentication Properties screen.

---

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

**Note**

---

ACU and the Windows Network Connection icon on the Windows XP taskbar may indicate a connection status when authentication is still in the pending state or the authentication server fails to respond.

---





## 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 Parameters that Affect ACU Diagnostic Tools, page 7-2](#)
- [Viewing the Current Status of Your Client Adapter, page 7-4](#)
- [Viewing Statistics for Your Client Adapter, page 7-12](#)
- [Viewing the Link Status Meter, page 7-16](#)
- [Running an RF Link Test, page 7-18](#)

## Overview of ACU Diagnostic Tools

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

- Display your client adapter's current status and configured settings
- Display statistics pertaining to your client adapter's transmission and reception of data
- Display a graphical image of your client adapter's RF link
- Run an RF link test to assess the performance of the RF link between your client adapter and its associated access point

[Table 7-1](#) enables you to quickly locate the instructions for using each of the diagnostic tools.

**Table 7-1** *Locating Diagnostic Instructions*

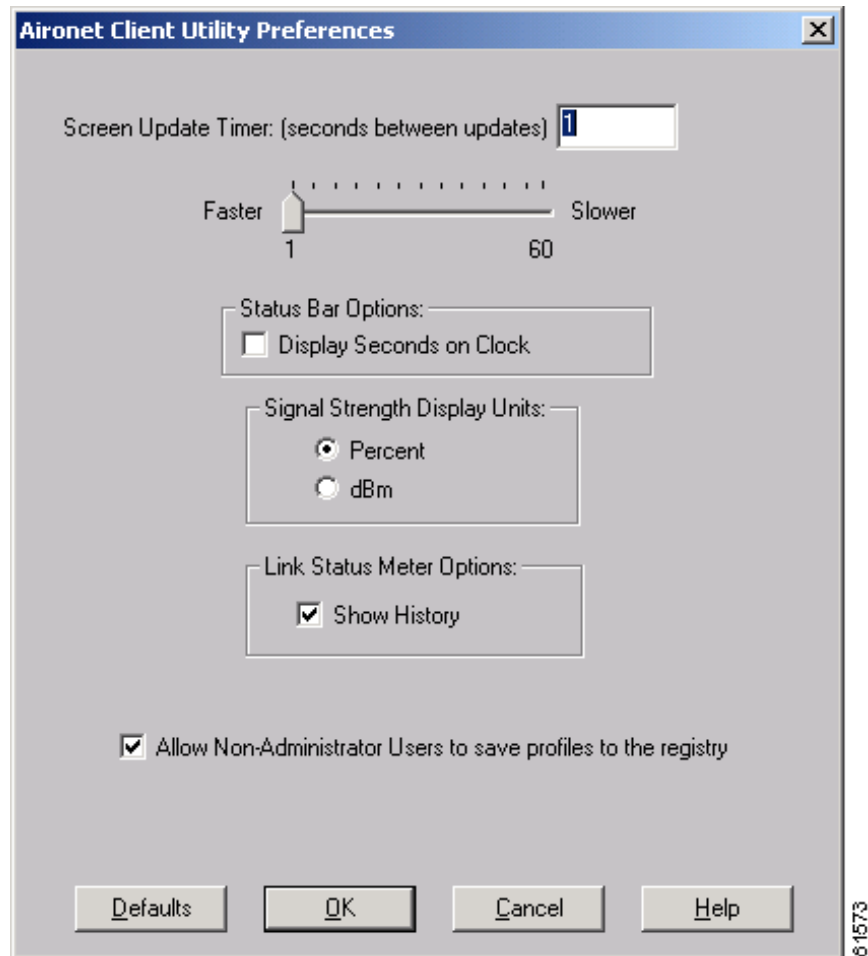
Diagnostic Tool	Page Number
Status	<a href="#">7-4</a>
Statistics	<a href="#">7-12</a>
Link status meter	<a href="#">7-16</a>
RF link test	<a href="#">7-18</a>

## Setting Parameters that Affect ACU Diagnostic Tools

Several parameters affect the operation of ACU diagnostic tools. Follow the steps below to set these parameters.

- 
- Step 1** Double-click the **Aironet Client Utility (ACU)** icon on your desktop to open ACU.
- Step 2** Click the **Preferences** icon or select **Preferences** from the Options drop-down menu. The Aironet Client Utility Preferences screen appears (see [Figure 7-1](#)).

Figure 7-1 Aironet Client Utility Preferences Screen



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

**Table 7-2 Parameters Affecting ACU Diagnostic Tools**

Parameter	Description						
Screen Update Timer (seconds between updates)	Specifies how often the Status and Statistics screens are updated. You can type a number in the edit box or use the slider to change this value. <b>Range:</b> 1 to 60 seconds between updates (in 1-second increments) <b>Default:</b> 1 second between updates						
Signal Strength Display Units	Specifies the units used to display signal strength on the Status, Linktest, and Site Survey screens. <b>Default:</b> Percent						
	<table border="1"> <thead> <tr> <th>Units</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Percent</td> <td>Displays the signal strength as a percentage.</td> </tr> <tr> <td>dBm</td> <td>Displays the signal strength in decibels with respect to milliwatts.</td> </tr> </tbody> </table>	Units	Description	Percent	Displays the signal strength as a percentage.	dBm	Displays the signal strength in decibels with respect to milliwatts.
	Units	Description					
	Percent	Displays the signal strength as a percentage.					
dBm	Displays the signal strength in decibels with respect to milliwatts.						
<b>Note</b> dBm can be selected only if your client adapter is using PCM/LMC/PCI card firmware version 3.92 or greater, mini PCI card firmware version 5.0 or greater, or PC-Cardbus card firmware version 4.99 or greater.							
Show History	Selecting this check box causes the Link Status Meter graphical display to show a recent history of the RF performance between your client adapter and its associated access point. Black dots on the graphical display show the performance of the last 50 signals. <b>Default:</b> Selected						

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

## Viewing the Current Status of Your Client Adapter

ACU enables you to view the current status of your client adapter as well as many of the settings that have been configured for the adapter.

To view your client adapter's status and settings, open ACU; then click the **Status** icon or select **Status** from the Commands drop-down menu. The Status screen appears. [Figure 7-2](#) shows the Status screen with the signal strength values displayed as percentages, and [Figure 7-3](#) shows the bottom of the same screen with the signal strength values displayed in decibels with respect to milliwatts (dBm).



**Note**

The name of the current profile appears in parentheses at the top of the screen.

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

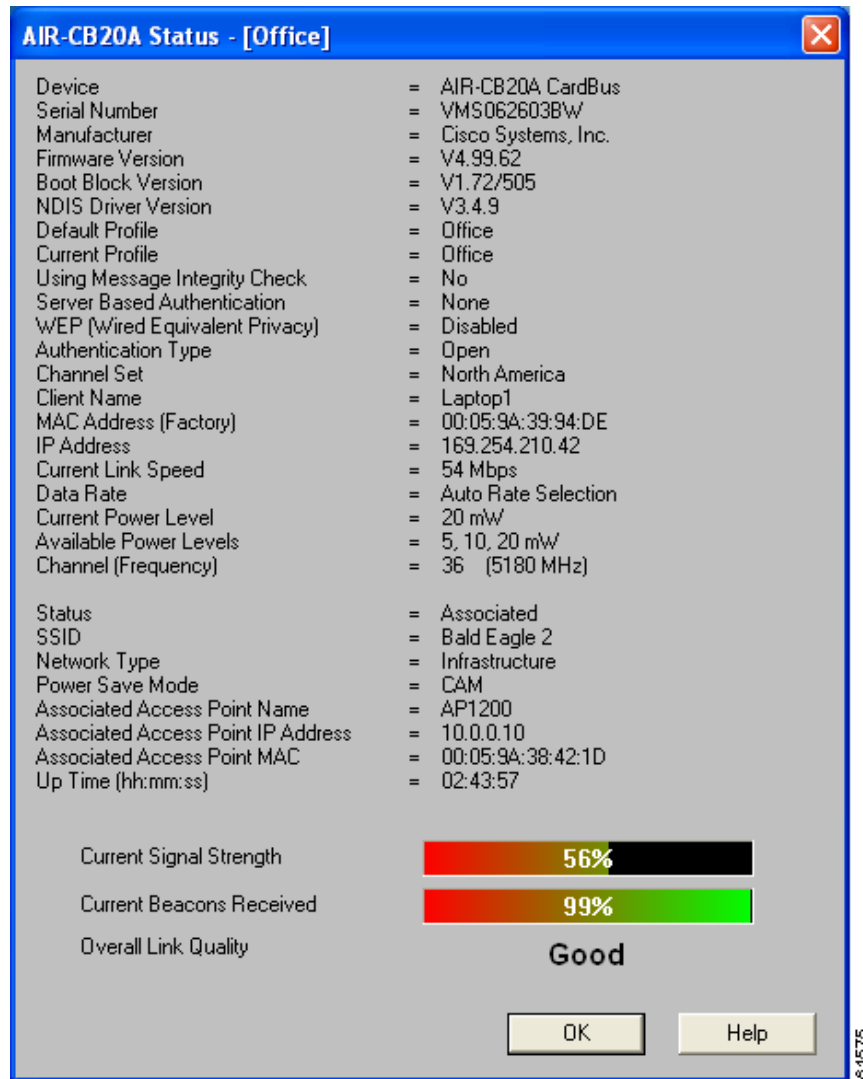


Figure 7-3 Bottom of Status Screen (with Signal Strength in dBm)

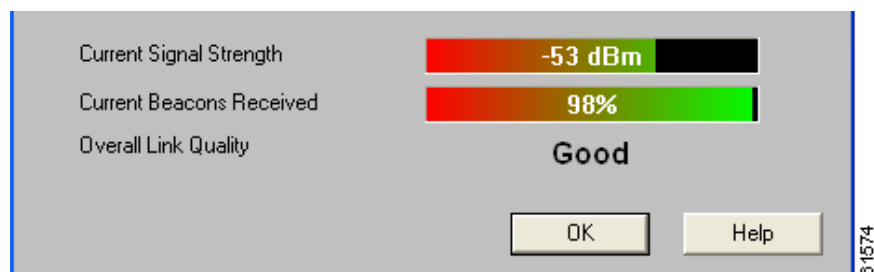


Table 7-3 interprets each element of the Status screen.

**Table 7-3 Client Adapter Status**

Status	Description
Device	A description of your client adapter.
Serial Number	The serial number of your client adapter.  <b>Note</b> The serial number appears only if the number has been programmed into your card and you are using ACU version 5.03.009 or greater.
Manufacturer	The manufacturer of your client adapter.
Firmware Version	The version of the firmware that is currently running on your client adapter.
Boot Block Version	The version of the boot block firmware that is currently in your client adapter. The boot block firmware contains identification information for the client adapter and functions to start up the radio and pass control to the main firmware, which (unlike the boot block) can be modified and upgraded by the user.
NDIS Driver Version	The version of the NDIS device driver that is currently installed on your computer.
Default Profile	The network configuration (or profile) shown in the Use Selected Profile drop-down box on the Profile Manager screen, if your driver supports auto profile selection. This is the profile that you have selected as the active profile.  <b>Note</b> The current profile may be different than the default profile if you are using auto profile selection. The client adapter will not switch profiles as long as it remains associated to the access point or reassociates within 10 seconds (or within the time specified by the LEAP authentication timeout value if LEAP is enabled). Refer to <a href="#">Chapter 4</a> for information on creating and using profiles.  <b>Note</b> Auto profile selection is supported in PCM/LMC/PCI card driver version 8.01 or greater, mini PCI card driver version 2.20 or greater, and PC-Cardbus card driver version 3.4 or greater.



**Table 7-3 Client Adapter Status (continued)**

Status	Description
Current Profile	<p>The network configuration (or profile) your client adapter is currently using, if your driver supports auto profile selection.</p> <p><b>Note</b> The current profile may be different than the default profile if you are using auto profile selection. The client adapter does not switch profiles as long as it remains associated to the access point or reassociates within 10 seconds (or within the time specified by the LEAP authentication timeout value if LEAP is enabled). Refer to <a href="#">Chapter 4</a> for information on creating and using profiles.</p> <p><b>Note</b> If your current profile becomes disabled due to an invalid LEAP username and password, this field lists the profile as (Disabled).</p> <p><b>Note</b> Auto profile selection is supported in PCM/LMC/PCI card driver version 8.01 or greater, mini PCI card driver version 2.20 or greater, and PC-Cardbus card driver version 3.4 or greater.</p>
Using Short Radio Headers	<p>Indicates whether your client adapter is actually using short radio headers.</p> <p><b>Value:</b> Yes or No</p> <p><b>Note</b> This setting appears only for 2.4-GHz client adapters.</p> <p><b>Note</b> Refer to the Use Short Radio Headers parameter in <a href="#">Table 5-3</a> for information on using short radio headers.</p>
Using Message Integrity Check	<p>Indicates whether your client adapter is using message integrity check (MIC) to protect packets sent to and received from the access point.</p> <p>MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. To use MIC, client adapters must use one of the following driver versions, and MIC must be enabled on the access point:</p> <ul style="list-style-type: none"> <li>• PCM/LMC/PCI card driver version 8.01 or greater</li> <li>• Mini PCI card driver version 2.20 or greater</li> <li>• PC-Cardbus card driver version 3.4 or greater.</li> </ul> <p><b>Note</b> If the access point is using MIC, your client adapter's driver must support MIC; otherwise, the client is unable to associate.</p> <p><b>Value:</b> Yes or No</p>

Table 7-3 Client Adapter Status (continued)

Status	Description										
Server Based Authentication	<p>Indicates the configuration of the access point to which your client adapter is associated.</p> <p><b>Value:</b> None, WEP Key In Use, Cell Is Secure, or LEAP Authenticated</p> <table border="1"> <thead> <tr> <th>Server Based Authentication</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>None</td> <td>The access point is configured for No Encryption.</td> </tr> <tr> <td>WEP Key In Use</td> <td>The access point is configured for Optional encryption.</td> </tr> <tr> <td>Cell Is Secure</td> <td> <p>The access point is configured for Full Encryption.</p> <p><b>Note</b> If the client's current profile does not have Allow Association To Mixed Cells enabled, the client can associate only to access points that use full encryption.</p> </td> </tr> <tr> <td>LEAP Authenticated</td> <td>The client is using LEAP and is authenticated to an access point that has WEP and Network-EAP enabled.</td> </tr> </tbody> </table>	Server Based Authentication	Description	None	The access point is configured for No Encryption.	WEP Key In Use	The access point is configured for Optional encryption.	Cell Is Secure	<p>The access point is configured for Full Encryption.</p> <p><b>Note</b> If the client's current profile does not have Allow Association To Mixed Cells enabled, the client can associate only to access points that use full encryption.</p>	LEAP Authenticated	The client is using LEAP and is authenticated to an access point that has WEP and Network-EAP enabled.
Server Based Authentication	Description										
None	The access point is configured for No Encryption.										
WEP Key In Use	The access point is configured for Optional encryption.										
Cell Is Secure	<p>The access point is configured for Full Encryption.</p> <p><b>Note</b> If the client's current profile does not have Allow Association To Mixed Cells enabled, the client can associate only to access points that use full encryption.</p>										
LEAP Authenticated	The client is using LEAP and is authenticated to an access point that has WEP and Network-EAP enabled.										
WEP (Wired Equivalent Privacy)	<p>Your client adapter's current WEP status.</p> <p><b>Value:</b> Enabled, Not Enabled, or Need Firmware Upgrade</p> <p><b>Note</b> Refer to the <a href="#">“Setting Network Security Parameters”</a> section on page 5-20 for information on enabling WEP.</p>										
Authentication Type	<p>Indicates whether the client adapter must share the same WEP keys as the access point in order to communicate or can communicate with the access point regardless of its WEP settings.</p> <p><b>Value:</b> Open or Shared Key</p> <p><b>Note</b> Refer to the <a href="#">“Setting Network Security Parameters”</a> section on page 5-20 for information on setting the authentication type.</p>										
Antenna Selection	<p>The antenna mode that your client adapter is currently using.</p> <p><b>Value:</b> Diversity, Primary Only, Secondary Only (Primary Only is the only option available for PCI client adapters)</p> <p><b>Note</b> This setting appears only for 2.4-GHz client adapters.</p> <p><b>Note</b> The Primary Only and Secondary Only values were formerly named Right Only and Left Only, respectively. Refer to the Antenna Mode (Receive) and Antenna Mode (Transmit) parameters in <a href="#">Table 5-4</a> and <a href="#">Table 5-5</a> for information on setting the antenna mode.</p>										

**Table 7-3 Client Adapter Status (continued)**

Status	Description
Channel Set	<p>The regulatory domain for which your client adapter is currently configured, such as Americas. (For the Japan channel set, the Call ID is also displayed.) 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>
Client Name	<p>The name your client adapter uses when it associates to an access point.</p> <p><b>Note</b> Refer to the Client Name parameter in <a href="#">Table 5-2</a> for information on setting the client name.</p>
MAC Address	The MAC address assigned to your client adapter at the factory.
IP Address	The IP address of your client adapter.
Current 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 (2.4-GHz client adapters); 6, 9, 12, 18, 24, 36, 48, or 54 Mbps (5-GHz client adapters)</p>
Data Rate	<p>The rate at which your client adapter has been configured to transmit or receive data packets.</p> <p><b>Value:</b> 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, or Auto Rate Selection (2.4-GHz client adapters); 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps, or Auto Rate Selection (5-GHz client adapters)</p> <p><b>Note</b> Refer to the Data Rate parameter in <a href="#">Table 5-3</a> for information on setting the client adapter's data rate.</p>
Current Power Level	<p>The power level at which your client adapter is currently transmitting. The maximum level is dependent upon the radio installed in your client adapter and your country's regulatory agency.</p> <p><b>Value:</b> 1, 5, 15, or 30 mW (340 series client adapters); 1, 5, 20, 30, 50, or 100 mW (350 series client adapters); 5, 10, or 20 mW (5-GHz client adapters)</p> <p><b>Note</b> Refer to the Transmit Power parameter in <a href="#">Table 5-3</a> for information on setting the client adapter's power level.</p>
Available Power Levels	<p>The power levels at which your client adapter is capable of transmitting. The maximum level is dependent upon the radio installed in your client adapter and your country's regulatory agency.</p> <p><b>Value:</b> 1, 5, 15, or 30 mW (340 series client adapters); 1, 5, 15, 20, 30, 50, or 100 mW (350 series client adapters); 5, 10, or 20 mW (5-GHz client adapters)</p> <p><b>Note</b> Refer to the Transmit Power parameter in <a href="#">Table 5-3</a> for information on the client adapter's available power levels.</p>

**Table 7-3 Client Adapter Status (continued)**

Status	Description
Channel (Frequency)	The frequency that your client adapter is currently using as the channel for communications. <b>Value:</b> Dependent on client adapter radio and regulatory domain <b>Note</b> Refer to the Channel parameter in <a href="#">Table 5-3</a> for information on selecting the frequency for your client adapter.
Status	The operational mode of your client adapter. <b>Value:</b> Error, Configured, Associated, Not Associated, or Ad Hoc Mode
SSID	The SSID that your client adapter is currently using. <b>Note</b> Refer to the SSID1 parameter in <a href="#">Table 5-2</a> for information on the client adapter's SSID.
Network Type	The type of network in which your client adapter is being used. <b>Value:</b> Infrastructure or Ad Hoc <b>Note</b> Refer to the Network Type parameter in <a href="#">Table 5-2</a> for information on setting the network type.
Power Save Mode	The client adapter's current power consumption setting. <b>Value:</b> CAM, Max PSP, or Fast PSP <b>Note</b> Refer to the Power Save Mode parameter in <a href="#">Table 5-2</a> for information on setting the client adapter's power save mode.
Associated Access Point Name	The name of the access point to which your client adapter is associated. It is shown only if the access point was configured with a name and the client adapter is in infrastructure mode.
Associated Access Point IP Address	The IP address of the access point to which your client adapter is associated. It is shown only if the access point was configured with an IP address and the client adapter is in infrastructure mode.
Associated Access Point MAC Address	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.
Beacon Period	Specifies the duration between beacon packets, which are used to help clients find each other in ad hoc mode. <b>Range:</b> Approximately 20 to 999 milliseconds (ms) <b>Note</b> The beacon period is shown only if your client adapter is in ad hoc mode.
Up Time (hh:mm:ss)	The amount of time (in hours:minutes:seconds) that the client adapter has been receiving power. If the adapter has been running for more than 24 hours, the time is displayed in days, hours:minutes:seconds.
Current Signal Strength	The signal strength for all received packets. The higher the value and the more green the bar graph is, the stronger the signal. <b>Range:</b> 0 to 100% or -95 to -45 dBm

**Table 7-3 Client Adapter Status (continued)**

Status	Description
Current Signal Quality (2.4-GHz client adapters)	<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><b>Range:</b> 0 to 100%</p> <p><b>Note</b> This setting appears only for 2.4-GHz client adapters and only if you selected signal strength to be displayed as a percentage. See the Signal Strength Display Units parameter in <a href="#">Table 7-2</a> for information.</p>
Current Noise Level (2.4-GHz client adapters)	<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 for 2.4-GHz client adapters and only if you selected signal strength to be displayed in dBm. See the Signal Strength Display Units parameter in <a href="#">Table 7-2</a> for information.</p>
Current Beacons Received (5-GHz client adapters)	<p>The percentage of beacon packets received versus those expected to be received. The higher the value and the more green the bar graph is, the clearer the signal.</p> <p><b>Example:</b> The access point sends out 10 beacons per second, so you would expect the client adapter to receive 50 beacon packets in 5 seconds. If it receives only 40 packets, the percentage of beacons received would be 80%.</p> <p><b>Range:</b> 0 to 100%</p> <p><b>Note</b> This setting appears only for 5-GHz client adapters.</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 for 2.4-GHz client adapters (but only if you selected signal strength to be displayed as a percentage) and for 5-GHz client adapters. See the Signal Strength Display Units parameter in <a href="#">Table 7-2</a> for information.</p>
Signal To Noise Ratio (2.4-GHz client adapters)	<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 for 2.4-GHz client adapters and only if you selected signal strength to be displayed in dBm. See the Signal Strength Display Units parameter in <a href="#">Table 7-2</a> for information.</p>

## 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.

To view your client adapter's statistics, open ACU; then click the **Statistics** icon or select **Statistics** from the Commands drop-down menu. The Statistics screen appears (see [Figure 7-4](#)).

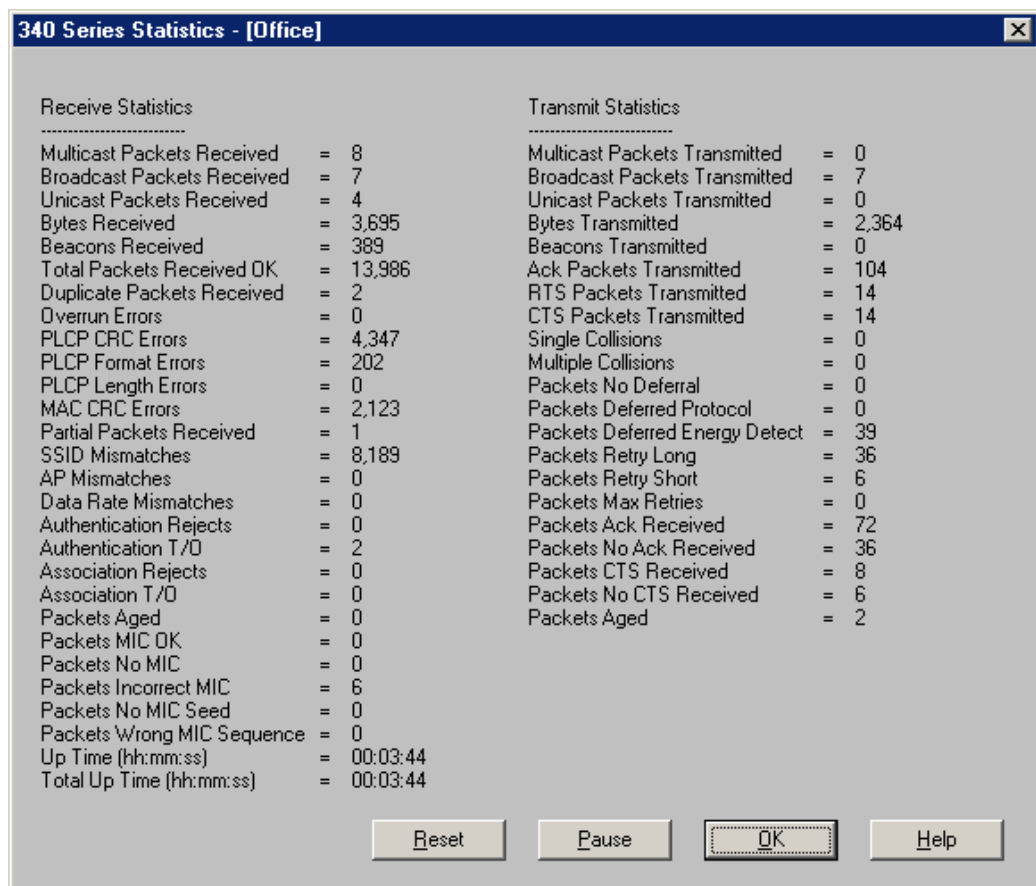

**Note**

The name of the current profile appears in parentheses at the top of the screen.


**Note**

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

**Figure 7-4 Statistics Screen**



The statistics are calculated as soon as your client adapter is started or the Reset button is selected and are continually updated at the rate specified by the Screen Update Timer. Instructions for changing the Screen Update Timer setting are provided in [Table 7-2](#).

Table 7-4 describes each statistic that is displayed for your client adapter.

**Table 7-4 Client Adapter Statistics**

Statistic	Description
<b>Receive Statistics</b>	
Multicast Packets Received	The number of multicast packets that were received successfully.
Broadcast Packets Received	The number of broadcast packets that were received successfully.
Unicast Packets Received	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.
Total Packets Received OK	The number of all packets that were received successfully.
Duplicate Packets Received	The number of duplicate packets that were received successfully.
Overrun Errors	The number of packets received when no receive buffers were available. These errors usually occur when the host does not read the received packets from the client adapter fast enough.
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 due to bounced signals, or the presence of other 2.4-GHz signals from devices such as microwave ovens, wireless handset phones, etc.</p>
PLCP Format Errors	The number of times an 802.11 PLCP header was received with a valid CRC but the rest of the packet was ignored due to an unknown value in the header.
PLCP Length Errors	The number of times an 802.11 PLCP header was received but the rest of the packet was ignored due to an illegal header length.
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 due to bounced signals, or the presence of other 2.4-GHz signals from devices such as microwave ovens, wireless handset phones, etc.</p>
Partial Packets Received	The number of fragments that were discarded because the entire packet was not received successfully.
SSID Mismatches	The number of times the client adapter tried to associate to an access point but was unable to because the adapter's SSID was not the same as the access point's.

**Table 7-4 Client Adapter Statistics (continued)**

Statistic	Description
AP Mismatches	The number of times the client adapter tried to associate to an access point but was unable to because the access point was not the adapter's specified access point. <b>Note</b> Refer to the Specified Access Point 1- 4 parameter in <a href="#">Table 5-4</a> for information on specifying access points.
Data Rate Mismatches	The number of times the client adapter tried to associate to an access point but was unable to because the adapter's data rate was not supported by the access point. <b>Note</b> Refer to the Data Rate parameter in <a href="#">Table 5-3</a> for information on supported data rates.
Authentication Rejects	The number of times the client adapter tried to authenticate to an access point but was rejected.
Authentication T/O	The number of times the client adapter tried to authenticate to an access point but was unable to because the access point did not respond fast enough (timed out).
Association Rejects	The number of times the client adapter tried to associate to an access point but was rejected.
Association T/O	The number of times the client adapter tried to associate to an access point but was unable to because the access point did not respond fast enough (timed out).
Packets Aged	The number of packets received successfully but discarded by the client adapter because either all fragments were not received within 10 seconds or the host did not read the packet from the adapter within 10 seconds.
Packets MIC OK	The number of packets that were received successfully with a valid message integrity check (MIC). <b>Note</b> This field is not displayed if the client adapter's driver does not support MIC functionality or MIC is not enabled on the access point.
Packets No MIC	The number of packets that were discarded due to no MIC being found. <b>Note</b> This field is not displayed if the client adapter's driver does not support MIC functionality or MIC is not enabled on the access point.
Packets Incorrect MIC	The number of packets that were discarded due to an incorrect MIC value. <b>Note</b> This field is not displayed if the client adapter's driver does not support MIC functionality or MIC is not enabled on the access point.



**Table 7-4 Client Adapter Statistics (continued)**

<b>Statistic</b>	<b>Description</b>
Packets No MIC Seed	The number of packets that were discarded due to no MIC seed being received.  <b>Note</b> This field is not displayed if the client adapter's driver does not support MIC functionality or MIC is not enabled on the access point.
Packets Wrong MIC Sequence	The number of packets that were discarded due to the MIC sequence number being wrong.  <b>Note</b> This field is not displayed if the client adapter's driver does not support MIC functionality or MIC is not enabled on the access point.
Up Time (hh:mm:ss)	The amount of time (in hours:minutes:seconds) since the Reset button was selected. If the client adapter has been running for more than 24 hours, the time is displayed in days, hours:minutes:seconds.
Total Up Time (hh:mm:ss)	The amount of time (in hours:minutes:seconds) that the client adapter has been receiving power. The total up time continues to increment even if the Reset button is selected. If the adapter has been running for more than 24 hours, the time is displayed in days, hours:minutes:seconds.
<b>Transmit Statistics</b>	
Multicast Packets Transmitted	The number of multicast packets that were transmitted successfully.
Broadcast Packets Transmitted	The number of broadcast packets that were transmitted successfully.
Unicast Packets Transmitted	The number of unicast packets that were transmitted successfully.
Bytes Transmitted	The number of bytes of data that were transmitted successfully.
Beacons Transmitted	The number of beacon packets that were transmitted successfully (in ad hoc mode only).
Ack Packets Transmitted	The number of acknowledgment (Ack) packets that were transmitted in response to successfully received unicast packets.
RTS Packets Transmitted	The number of request-to-send (RTS) packets that were transmitted successfully.
CTS Packets Transmitted	The number of clear-to-send (CTS) packets that were transmitted in response to a successfully received RTS packet.
Single Collisions	The number of packets that had to be retransmitted once due to a collision.
Multiple Collisions	The number of packets that had to be retransmitted more than once due to additional collisions.
Packets No Deferral	The number of packets that were able to be transmitted immediately without being delayed due to energy detect or protocol deferral.
Packets Deferred Protocol	The number of packets that were delayed due to 802.11 protocol reasons (such as not enough time left to send the packet).

**Table 7-4 Client Adapter Statistics (continued)**

Statistic	Description
Packets Deferred Energy Detect	The number of packets that were delayed because RF energy was already detected. This condition is usually caused by another radio transmitting a packet or by some other RF source jamming the signal (such as a microwave oven).
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.
Packets Ack Received	The number of transmitted packets that had their corresponding acknowledgment (Ack) packet received successfully.
Packets No Ack Received	The number of transmitted packets that did not have their corresponding Ack packet received successfully.
Packets CTS Received	The number of clear-to-send (CTS) packets that were received in response to an RTS packet.
Packets No CTS Received	The number of packets for which no CTS packet was received in response to an RTS packet.
Packets Aged	The number of packets that were discarded by the client adapter because they were not transmitted successfully within 5 seconds.

## Viewing the Link Status Meter

ACU's link status meter can be used to assess the performance of your client adapter's RF link. If this tool is used to assess the RF link at various locations, you can avoid areas where performance is weak and eliminate the risk of losing the connection between your client adapter and an access point.

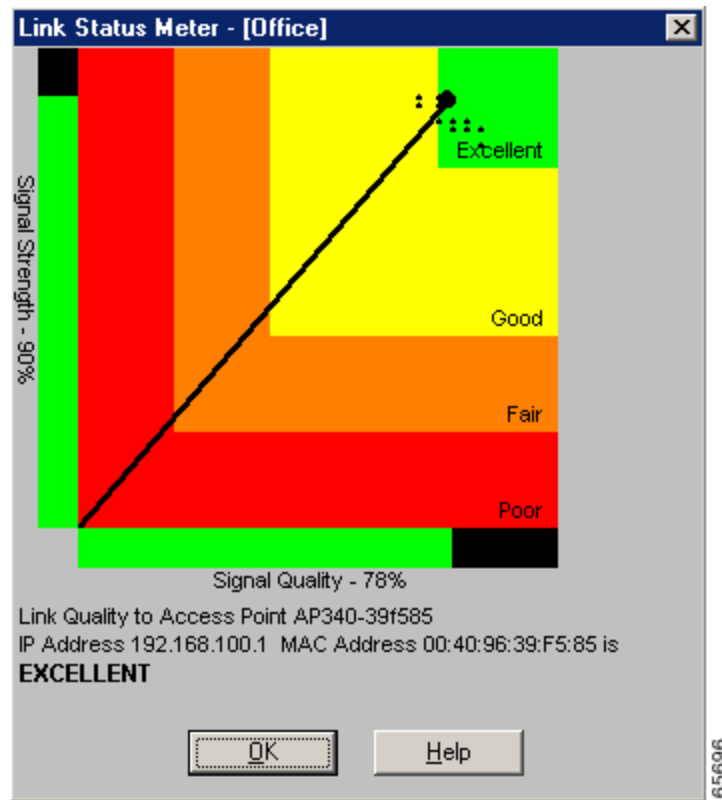
To open the link status meter, open ACU; then click the **Link Status Meter** icon or select **Link Status Meter** from the Commands drop-down menu. The Link Status Meter screen appears (see [Figure 7-5](#)).



### Note

The name of the current profile appears in parentheses at the top of the screen.

Figure 7-5 Link Status Meter Screen



The Link Status Meter screen provides a graphical display of the following:

- **Signal strength**—The strength of the client adapter’s radio signal at the time packets are being received. It is displayed as a percentage along the vertical axis.
- **Signal quality**—The quality of the client adapter’s radio signal at the time packets are being received. It is displayed as a percentage along the horizontal axis.

The combined result of the signal strength and signal quality is represented by a diagonal line (see Figure 7-5). Where the line falls on the graphical display determines whether the RF link between your client adapter and its associated access point is poor, fair, good, or excellent. The access point that is associated to your client adapter and its MAC address are indicated at the bottom of the display.



**Note**

ACU’s Status screen also shows signal strength and signal quality. However on the Status screen, these data are represented by histograms.

If you want to see a recent history of the RF performance between your client adapter and its associated access point, select the **Show History** check box on the Aironet Client Utility Preferences screen. Black dots on the graphical display show the performance of the last 50 signals.

## Running an RF Link Test

ACU's link test tool sends out pings to assess the performance of the RF link. The test is designed to be performed multiple times at various locations throughout your area and is run at the data rate set on ACU's RF Network Properties screen (see the Data Rate parameter in [Table 5-3](#)). The results of the link test can be used to determine RF network coverage and ultimately the required number and placement of access points in your network. The test also helps you to avoid areas where performance is weak, thereby eliminating the risk of losing the connection between your client adapter and its associated access point.

Because the link test operates above the RF level, it does more than test the RF link between two network devices. It also checks the status of wired sections of the network and verifies that TCP/IP and the proper drivers have been loaded.


**Note**

A link test can also be run from an access point through a Telnet session. Refer to the Software Configuration Guide for your access point for information.

The following prerequisites are required before you can run an RF link test:

- The TCP/IP protocol must be installed on your system.


**Note**

See the Help section of your Windows operating system for information on installing and setting up TCP/IP.

- An IP address must be configured for the access point (or other computer in ad hoc mode).

Follow the steps below to run an RF link test.

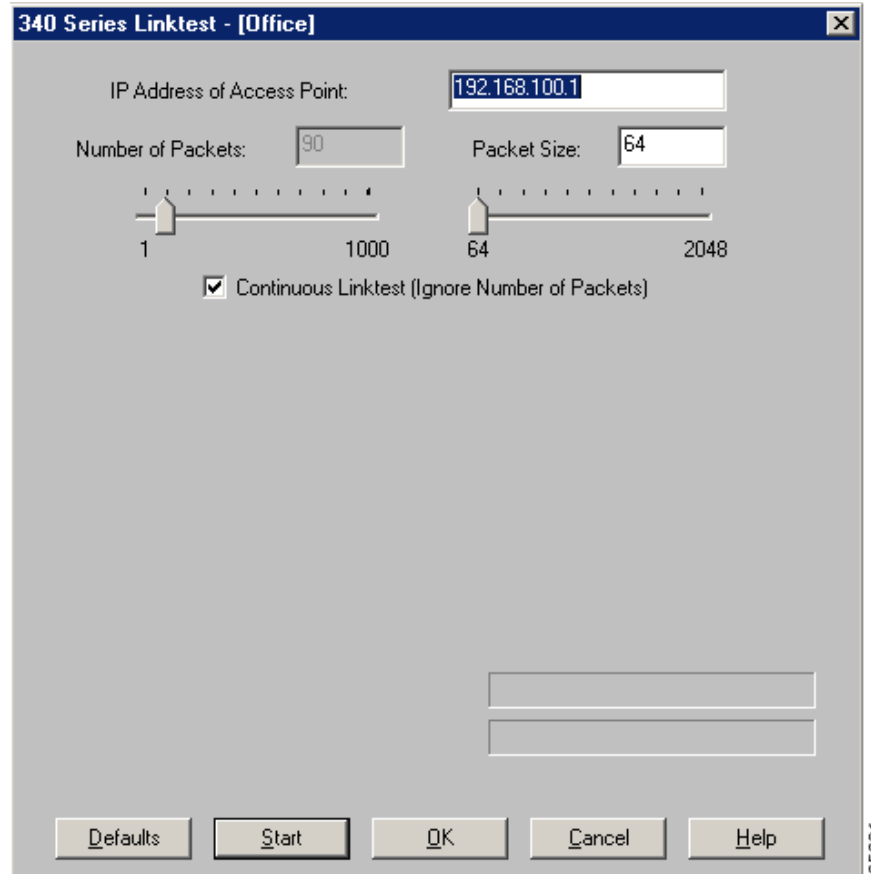
**Step 1**

Open ACU; then click the **Link Test** icon or select **Linktest** from the Commands drop-down menu. The Linktest screen appears (see [Figure 7-6](#)).


**Note**

The name of the current profile appears in parentheses at the top of the screen.

Figure 7-6 Linktest Screen



- Step 2** In the IP Address of Access Point field, enter the IP address of the access point or other wireless device with which you want to test the RF link.
- Step 3** You can set the link test to run until it has attempted to send a specific number of packets or to run until you stop it. Follow one of the steps below to determine how long the link test will run:
- Select the number of packets that the link test should attempt to send. You can type a number in the Number of Packets field or use the slider to select this value. (The Number of Packets parameter is ignored if the Continuous Linktest check box is selected.)
 

**Range:** 1 to 1000

**Default:** 4
  - Select the Continuous Linktest check box to allow the link test to run continuously.
 

**Default:** Deselected
- Step 4** Select the size of the data packet that is to be sent to the access point. You can type a number in the Packet Size field or use the slider to select this value.
- Range:** 64 to 2048
- Default:** 100

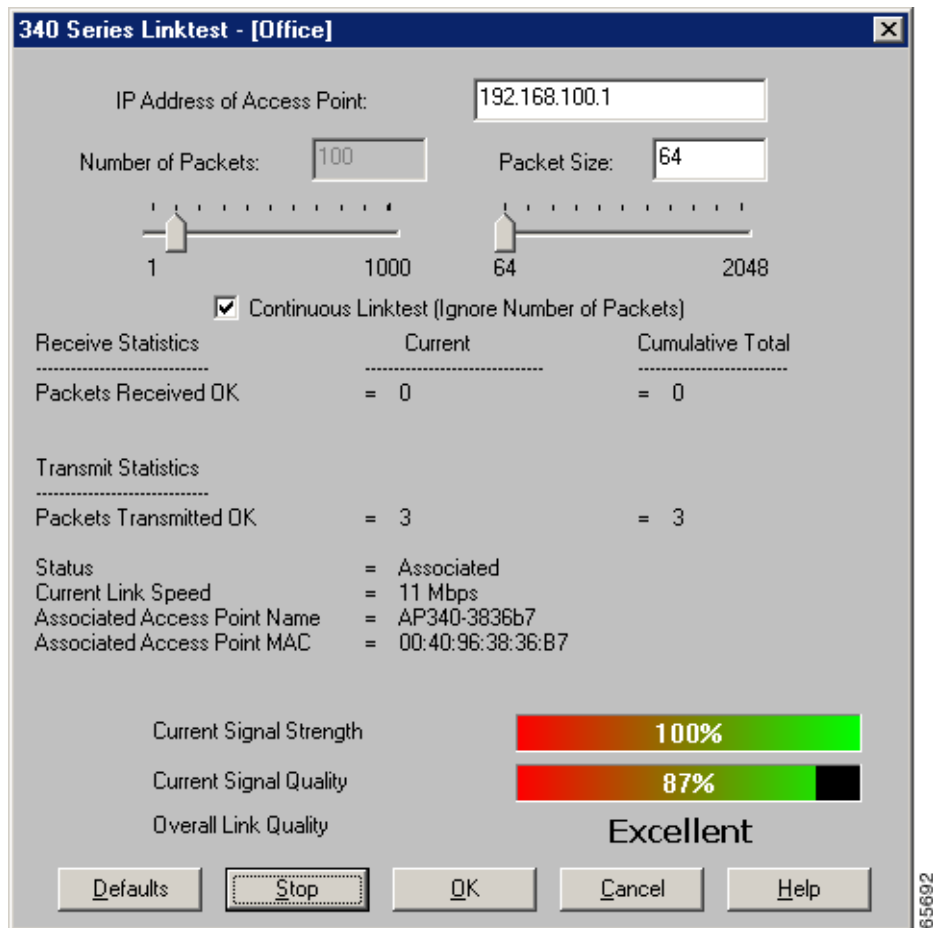


**Note** The Windows TCP/IP stack fragments (splits up) packets that are greater than 512 bytes. Therefore, the number of transmitted packets does not match the number of received packets (even if none are lost) if the packet size is greater than 512 bytes.

**Step 5** Click the **Start** button to run the link test. While the test is running, statistics are displayed and updated periodically.

Figure 7-7 shows the Linktest screen with the signal strength values displayed as percentages, and Figure 7-8 shows the bottom of the same screen with the signal strength values displayed in dBm.

**Figure 7-7 Linktest Screen (with Test Running and Signal Strength as a Percentage)**



**Figure 7-8 Bottom of Linktest Screen (with Test Running and Signal Strength in dBm)**



Table 7-5 interprets the statistics that are displayed on the Linktest screen while the link test is running.

**Table 7-5 Linktest Statistics**

Linktest Statistic	Description
Packets Received OK	The number of packets of the specified size that have been received successfully.
Packets Transmitted OK	The number of packets of the specified size that have been transmitted successfully.
Status	The operational mode of your client adapter. <b>Value:</b> Error, Configured, Associated, Not Associated, or Ad Hoc Mode
Current Link Speed	The rate at which your client adapter is currently transmitting data packets. <b>Value:</b> 1, 2, 5.5, or 11 Mbps (2.4-GHz client adapters); 6, 9, 12, 18, 24, 36, 48, or 54 Mbps (5-GHz client adapters)
Associated Access Point Name	The name of the access point to which your client adapter is associated. It is shown only if the access point was configured with a name and the client adapter is in infrastructure mode.
Associated Access Point MAC Address	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.
Current Signal Strength	The signal strength for all received packets. The higher the value and the more green the bar graph is, the stronger the signal. <b>Range:</b> 0 to 100% or -95 to -45 dBm
Current Signal Quality (2.4-GHz client adapters)	The signal quality for all received packets. The higher the value and the more green the bar graph is, the clearer the signal. <b>Range:</b> 0 to 100% <b>Note</b> This setting appears only for 2.4-GHz client adapters and only if you selected signal strength to be displayed as a percentage. See the Signal Strength Display Units parameter in Table 7-2 for information.
Current Noise Level (2.4-GHz client adapters)	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. <b>Range:</b> -100 to -45 dBm <b>Note</b> This setting appears only for 2.4-GHz client adapters and only if you selected signal strength to be displayed in dBm. See the Signal Strength Display Units parameter in Table 7-2 for information.

Table 7-5 Linktest Statistics (continued)

Linktest Statistic	Description
Current Beacons Received (5-GHz client adapters)	<p>The percentage of beacon packets received versus those expected to be received. The higher the value and the more green the bar graph is, the clearer the signal.</p> <p><b>Example:</b> The access point sends out 10 beacons per second, so you would expect the client adapter to receive 50 beacon packets in 5 seconds. If it receives only 40 packets, the percentage of beacons received would be 80%.</p> <p><b>Range:</b> 0 to 100%</p> <p><b>Note</b> This setting appears only for 5-GHz client adapters.</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 for 2.4-GHz client adapters (but only if you selected signal strength to be displayed as a percentage) and for 5-GHz client adapters. See the Signal Strength Display Units parameter in <a href="#">Table 7-2</a> for information.</p>
Signal To Noise Ratio (2.4-GHz client adapters)	<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 for 2.4-GHz client adapters and only if you selected signal strength to be displayed in dBm. See the "Signal Strength Display Units" parameter in <a href="#">Table 7-2</a> for information.</p>

- Step 6** If you did not set the link test to run continuously, the test ends after the specified number of packets is sent, and the Stop button changes back to the Start button. To stop the link test at any time, click **Stop**, **OK**, or **Cancel**.





## 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 Client Adapter, page 8-2](#)
- [Upgrading the Firmware, page 8-5](#)
- [Driver Procedures, page 8-8](#)
- [ACU Procedures, page 8-19](#)
- [Restarting the Client Adapter, page 8-28](#)
- [Turning Your Client Adapter's Radio On or Off, page 8-29](#)
- [Uninstalling Microsoft Hot Fixes, page 8-29](#)

# Inserting and Removing a Client Adapter

This section provides instructions for inserting and removing PC cards, PC-Cardbus cards, and PCI cards. Instructions are not provided for LM cards and mini PCI cards because they are pre-installed inside computing devices and are not meant to be installed or removed by the user.



## Caution

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

## Inserting a Client Adapter

Follow the instructions in one of the sections below to insert a PC card, PC-Cardbus card, or PCI card into a computing device.

### Inserting a PC Card or PC-Cardbus Card

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



**Note** The PC card slot or Cardbus slot is on the left or right side of the computer, depending on the model.

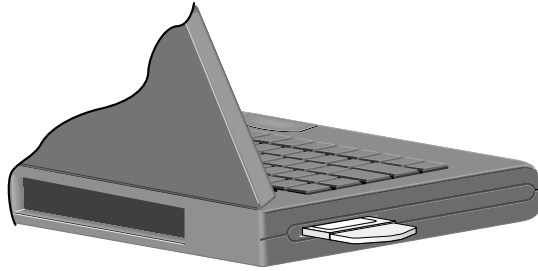
- Step 2** Follow the instructions below for your specific operating system:
- **Windows 95, 98, 2000, Me, or XP**—Turn on your computer, let the operating system boot up completely, and follow the remaining steps in this section to insert the card.
  - **Windows NT**—Turn off your computer, follow the remaining steps in this section to insert the card, and reboot your computer.



## Caution

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

- Step 3** Hold the card with the Cisco logo facing up and insert it into the PC card slot or Cardbus slot, applying just enough pressure to make sure it is fully seated (see [Figure 8-1](#)).

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

- Step 4** Go to the “[Installing the Driver](#)” section on page 3-3 to install the driver for your computer’s operating system.

## Inserting a PCI Card

- Step 1** Turn off the PC and all its components.

- Step 2** Remove the computer cover.



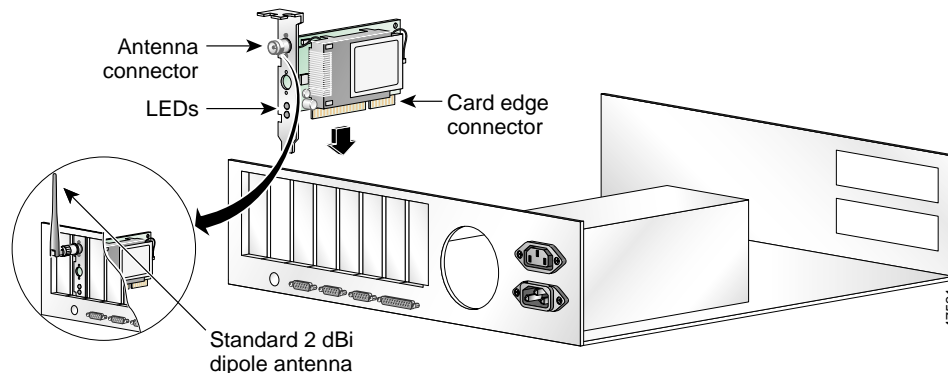
**Note** On most Pentium PCs, PCI expansion slots are white. Refer to your PC documentation for slot identification.

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



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

- Step 4** Examine the PCI card. The antenna connector and the LEDs face out of your computer and are visible when you put the cover back on. The bottom edge of the card is the connector you will insert into an empty expansion slot in your computer. See [Figure 8-2](#).

**Figure 8-2** Inserting a PCI Card into a PC

**Step 5** Tilt the card to allow the antenna connector and LEDs to slip through the opening in the CPU back panel.

**Step 6** Press the card into the empty slot until the connector is firmly seated.



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

---

**Step 7** Reinstall the screw on the CPU back panel and replace the computer cover.

**Step 8** Attach the 2-dBi antenna to the card's antenna connector until it is finger-tight. Do *not* overtighten.

**Step 9** For optimal reception, position the antenna so it is straight up.

**Step 10** Boot up your PC.

---

## Removing a Client Adapter

Follow the instructions in one of the sections below to remove a PC card, PC-Cardbus card, or PCI card from a computing device, when necessary.

### Removing a PC Card or PC-Cardbus Card

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

### Removing a PCI Card

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

---

**Step 1** Completely shut down your computer.

**Step 2** Disconnect the client adapter's antenna.

**Step 3** Remove the computer cover.

**Step 4** Remove the screw from the top of the CPU back panel above the PCI expansion slot that holds your client adapter.

**Step 5** Pull up firmly on the client adapter to release it from the slot and carefully tilt the adapter to allow it to clear the opening in the CPU back panel.

**Step 6** Reinstall the screw on the CPU back panel and replace the computer cover.

---

# 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 determine the version of your client adapter's firmware and to upgrade it if a more recent version is available from Cisco.com.

## Determining the Firmware Version

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

---

**Step 1** To determine the version of firmware that your client adapter is currently using, open ACU; then click the **Status** icon or select **Status** from the Commands drop-down menu. The Status screen displays the current version of your adapter's firmware in the Firmware Version field.

**Step 2** To determine the latest firmware version available on Cisco.com, follow the steps below:



---

**Note** This step enables you to determine the version numbers of individual firmware files on Cisco.com. If you downloaded a bundled file from Cisco.com, find the folders that were extracted from the bundle. Look at the firmware folder (the one that doesn't specify ACU or the Windows operating system). The version number is included in the folder name.

---

- a. Use your computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
- b. Click the link for Cisco Aironet Wireless LAN Client Adapters.
- c. Find the section for client adapter firmware.
- d. Click the link that corresponds to your client adapter's model number (such as CB20A or 350 series).
- e. Find the firmware file with the greatest version number for your specific client adapter type (such as CB or MPI). This is the latest available version on Cisco.com.



---

**Note** The firmware for PC, LM, and PCI cards is labeled *PCMCIA-LMC-PCI*, the firmware for mini PCI cards is labeled *mini PCI* or *MPI*, and the firmware for PC-Cardbus cards is labeled *CB*.

---



---

**Note** In order to use LEAP authentication, your client adapter and access point firmware must have matching 802.1X draft standards. That is, if the access point uses draft 8 firmware (prior to 11.06) or has draft 8 selected, the client adapter must use draft 8 firmware (prior to 4.25.x). Similarly, if the access point uses draft 10 firmware (11.06 or later) and has draft 10 selected, the client adapter must use draft 10 firmware (4.25.x or later). Mini PCI card firmware and PC-Cardbus card firmware were first released at draft 10.

---

**Note**

In order to use host-based authentication with Windows 2000 (with Service Pack 3 and the Windows 2000 Wireless 802.1X hot fix) or XP, your client adapter and access point must use firmware that supports 802.1X draft 10, which is functionally equivalent to the ratified 802.1X standard.

- 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**

If a power failure occurs while you are loading new firmware, your client adapter may become inoperable. If this occurs, 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** Perform one of the following:

- If you are installing firmware from a bundled file on Cisco.com, follow the steps below:
  - a. Using Windows Explorer, find the folders that were extracted from the bundle and double-click the firmware folder (the one that doesn't specify ACU or the Windows operating system).
  - b. Go to [Step 2](#).
- If you are installing firmware from an individual file on Cisco.com, follow the steps below:
  - a. Use the computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - b. Click the link for Cisco Aironet Wireless LAN Client Adapters.
  - c. Find the section for client adapter firmware.
  - d. Click the link that corresponds to your client adapter's model number (such as CB20A or 350 series).
  - e. Select the latest firmware file for your specific client adapter type (such as CB or MPI).

**Note**

The firmware for PC, LM, and PCI cards is labeled *PCMCIA-LMC-PCI*, the firmware for mini PCI cards is labeled *mini PCI* or *MPI*, and the firmware for PC-Cardbus cards is labeled *CB*.

**Note**

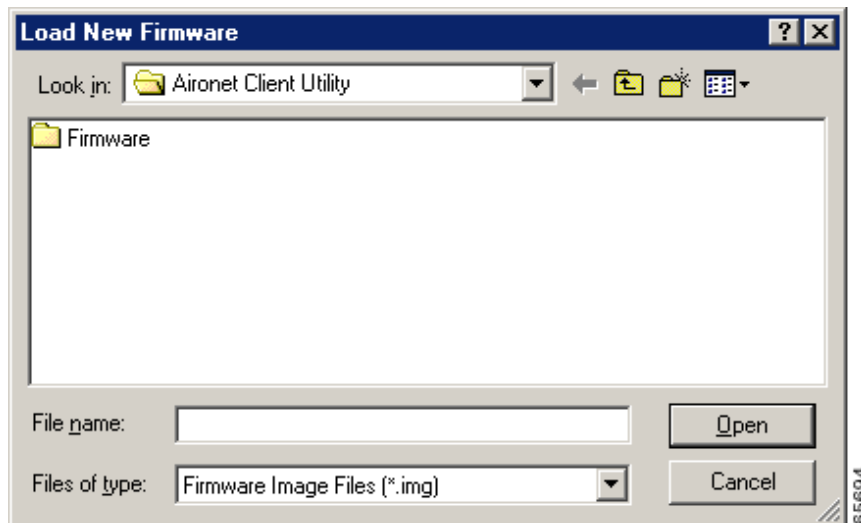
If your wireless network uses LEAP authentication, remember to select radio firmware of the same draft standard as the access points to which your client adapter will be authenticating. Mini PCI card firmware and PC-Cardbus card firmware were first released at draft 10.

**Note**

If your wireless network uses host-based authentication, remember to select radio firmware that supports 802.1X draft 10, which is functionally equivalent to the ratified 802.1X standard.

- f. Read and accept the terms and conditions of the Software License Agreement.
  - g. Select the firmware file again to download it.
  - h. Save the file to a floppy disk or to your computer's hard drive.
  - i. Find the file using Windows Explorer, double-click it, and extract the image file to a folder.
  - j. Go to [Step 2](#).
- Step 2** Make sure the client adapter is installed in your computer and is operational.
- Step 3** Open ACU; then click the **Load Firmware** icon or select **Load New Firmware** from the Commands drop-down menu. The Open window appears (see [Figure 8-3](#)).

**Figure 8-3** Open Window



- Step 4** Find the location of the new firmware in the Look in box. The default location is *InstallPath*\Firmware, where *InstallPath* is the directory that ACU was installed in.
- Step 5** Click the firmware image file (\*.img) so that it appears in the File name box at the bottom of the Open window.
- Step 6** Click the **Open** button. A progress bar appears while the selected image is loaded into the client adapter's Flash memory.
- Step 7** Click **OK** when the "Firmware Upgrade Complete!" message appears. The OK button cannot be selected until the process is complete or an error occurs. If an error occurs, refer to the "[Error Messages](#)" section in [Chapter 9](#).

# Driver Procedures

This section includes the following procedures:

- Determining the driver version, see below
- Upgrading the driver, see 8-9
- Uninstalling the driver, see 8-14

## Determining the Driver Version

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

- Step 1** To determine the version of the driver that your client adapter is currently using, open ACU; then click the **Status** icon or select **Status** from the Commands drop-down menu. The Status screen displays the current version of your adapter's driver in the NDIS Driver Version field.
- Step 2** To determine the latest driver version available on Cisco.com, follow the steps below:
- Use your computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - Click the link for Cisco Aironet Wireless LAN Client Adapters.
  - Perform one of the following:
    - If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as CB20A or 350 series). Find the bundled file with the greatest version number for your specific client adapter type (such as CB or MPI). The driver version number is provided in the description below the filename. This is the latest available version on Cisco.com. Go to [Step 3](#).
    - If you want to select the client adapter's software files individually, go to [Step d](#).
  - Find the section for Windows drivers and click the link for your computer's operating system. Find the driver with the greatest version number for your specific client adapter type (such as CB or MPI). This is the latest available version on Cisco.com.



**Note**

The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, the drivers for mini PCI cards are labeled *MPI*, and the drivers for PC-Cardbus cards are labeled *CB*.

- Step 3** If the driver available from Cisco.com has a higher number than the driver currently being used by your client adapter, follow the instructions in the “[Upgrading the Driver](#)” section on page 8-9 to upgrade the driver.



**Note**

If the 6.10 driver is installed on your Windows 95, 98, NT, or 2000 computer, you must remove this driver before you can install a more recent driver. Refer to the “[Uninstalling the 6.10 Driver](#)” section on page 8-14 for instructions.



## Upgrading the Driver

Follow the instructions in this section to upgrade your client adapter's driver to a more recent version. Use [Table 8-1](#) to quickly locate the instructions to upgrade the driver for your specific operating system.

**Table 8-1 Updating the Driver Instructions**

Operating System	Page Number
Windows 95	<a href="#">8-9</a>
Windows 98	<a href="#">8-9</a>
Windows NT	<a href="#">8-10</a>
Windows 2000	<a href="#">8-11</a>
Windows Millennium Edition (Me)	<a href="#">8-12</a>
Windows XP	<a href="#">8-13</a>

### Upgrading the Driver for Windows 95 and 98



**Note**

Windows 95 is supported only by 2.4-GHz client adapters. Therefore, a Windows 95 driver is not available for the 5-GHz client adapters.

**Step 1** Use your computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

**Step 2** Click the link for Cisco Aironet Wireless LAN Client Adapters.

**Step 3** Perform one of the following:

- If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as 340 or 350 series). Select the latest bundled file for your computer's operating system and your specific client adapter type (such as PCMCIA or MPI).
- If you want to select the client adapter's software files individually, find the section for Windows drivers and click the link for your computer's operating system. Select the driver file with the greatest version number for your specific client adapter type (such as PCMCIA or MPI).



**Note**

The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, the drivers for mini PCI cards are labeled *MPI*, and the drivers for PC-Cardbus cards are labeled *CB*.

**Step 4** Read and accept the terms and conditions of the Software License Agreement.

**Step 5** Select the file again to download it.

**Step 6** Save the file to a floppy disk or to your computer's hard drive.

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

**Step 8** Make sure your client adapter is installed in your computer.

**Step 9** Double-click **My Computer**, **Control Panel**, and **System**.

**Step 10** Click the **Device Manager** tab.

- Step 11** Double-click **Network Adapters**.
- Step 12** Select the Cisco Systems Wireless LAN Adapter.
- Step 13** Click **Properties**, the **Driver** tab, and the **Change Driver** or **Update Driver** button.
- Step 14** The Update Device Driver Wizard window appears. Click **Next**.
- Step 15** Select **Search for a better driver than the one your device is using now (Recommended)** and click **Next**.
- Step 16** Select the location of the new driver (floppy disk drive or specify a location), deselect the other options, enter the full path to the extracted driver files, and click **Next**.
- Step 17** A message appears indicating that the system is ready to install the new driver. Click **Next** and **Finish**. The driver upgrade is complete, and the old driver is overwritten by the new one.
- 

## Upgrading the Driver for Windows NT



**Note** Windows NT is supported only by 2.4-GHz client adapters. Therefore, a Windows NT driver is not available for the 5-GHz client adapters

---

- Step 1** Use your computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
- Step 2** Click the link for Cisco Aironet Wireless LAN Client Adapters.
- Step 3** Perform one of the following:
- If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as 340 or 350 series). Select the latest bundled file for Windows NT and your specific client adapter type (such as PCMCIA or MPI).
  - If you want to select the client adapter's software files individually, find the section for Windows drivers and click the link for Windows NT. Select the driver file with the greatest version number for your specific client adapter type (such as PCMCIA or MPI).



**Note** The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, and the drivers for mini PCI cards are labeled *MPI*.

---

- Step 4** Read and accept the terms and conditions of the Software License Agreement.
- Step 5** Select the file again to download it.
- Step 6** Save the file to a floppy disk or to your computer's hard drive.
- Step 7** Find the file using Windows Explorer, double-click it, and extract its files to a folder.
- Step 8** Make sure your client adapter is installed in your computer.
- Step 9** Double-click **My Computer**, **Control Panel**, **Network**, and **Adapters**.
- Step 10** Select the Cisco Systems Wireless LAN Adapter.
- Step 11** Click the **Update** button.

- Step 12** In the Windows NT Setup window, enter the path to the extracted driver files and click **Continue**.
- Step 13** Follow the instructions on the screen to complete the upgrade process.
- 

## Upgrading the Driver for Windows 2000

---

- Step 1** Use your computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
- Step 2** Click the link for Cisco Aironet Wireless LAN Client Adapters.
- Step 3** Perform one of the following:
- If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as CB20A or 350 series). Select the latest bundled file for Windows 2000 and your specific client adapter type (such as CB or MPI).
  - If you want to select the client adapter's software files individually, find the section for Windows drivers and click the link for Windows 2000. Select the driver file with the greatest version number for your specific client adapter type (such as CB or MPI).



**Note** The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, the drivers for mini PCI cards are labeled *MPI*, and the drivers for PC-Cardbus cards are labeled *CB*.

---

- Step 4** Read and accept the terms and conditions of the Software License Agreement.
- Step 5** Select the file again to download it.
- Step 6** Save the file to a floppy disk or to your computer's hard drive.
- Step 7** Find the file using Windows Explorer, double-click it, and extract its files to a folder.
- Step 8** Make sure your client adapter is installed in your computer.
- Step 9** Double-click **My Computer**, **Control Panel**, and **System**.
- Step 10** Click the **Hardware** tab and **Device Manager**.
- Step 11** Double-click **Network Adapters** and the Cisco Systems Wireless LAN Adapter.
- Step 12** Click the **Driver** tab.
- Step 13** Click the **Update Driver** button.
- Step 14** The Update Device Driver Wizard window appears. Click **Next**.
- Step 15** Select **Display a list of the known drivers for this device so that I can choose a specific driver** and click **Next**.
- Step 16** Click **Have Disk**.
- Step 17** Enter or browse to the path where the extracted driver files are and click **OK**.
- Step 18** A message appears indicating that the system is ready to install the new driver. Click **Next** and **Finish**. The driver upgrade is complete, and the old driver is overwritten by the new one.
-

## Upgrading the Driver for Windows Me

- 
- Step 1** Use your computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
- Step 2** Click the link for Cisco Aironet Wireless LAN Client Adapters.
- Step 3** Perform one of the following:
- If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as CB20A or 350 series). Select the latest bundled file for Windows Me and your specific client adapter type (such as CB or MPI).
  - If you want to select the client adapter's software files individually, find the section for Windows drivers and click the link for Windows Me. Select the driver file with the greatest version number for your specific client adapter type (such as CB or MPI).




---

**Note** The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, the drivers for mini PCI cards are labeled *MPI*, and the drivers for PC-Cardbus cards are labeled *CB*.

---

- Step 4** Read and accept the terms and conditions of the Software License Agreement.
- Step 5** Select the file again to download it.
- Step 6** Save the file to a floppy disk or to your computer's hard drive.
- Step 7** Find the file using Windows Explorer, double-click it, and extract its files to a folder.
- Step 8** Make sure your client adapter is installed in your computer.
- Step 9** Double-click **My Computer**, **Control Panel**, and **System**.
- Step 10** Click the **Device Manager** tab.
- Step 11** Double-click **Network Adapters**.
- Step 12** Select the Cisco Systems Wireless LAN Adapter.
- Step 13** Click **Properties**, the **Driver** tab, and the **Update Driver** button. The Update Device Driver Wizard window appears.
- Step 14** Select **Specify the location of the driver (Advanced)** and click **Next**.
- Step 15** Select **Search for a better driver than the one your device is using now (Recommended)**.
- Step 16** Select the **Specify a location** check box, deselect the other options, enter the path to the extracted driver files, and click **Next**.
- Step 17** A message appears indicating that Windows has found an updated driver. Select **The updated driver (Recommended)** and click **Next**.
- Step 18** A message appears indicating that the system is ready to install the new driver. Click **Next** and **Finish**.
- Step 19** If you are prompted to restart your computer, click **Yes**.
- The driver upgrade is complete, and the old driver is overwritten by the new one.
-

## Upgrading the Driver for Windows XP



---

**Note** These instructions assume you are using Windows XP's classic view rather than its category view.

---

- Step 1** Use your computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
- Step 2** Click the link for Cisco Aironet Wireless LAN Client Adapters.
- Step 3** Perform one of the following:
- If you want to ensure compatibility among all three pieces of client adapter software and download the software files from a single location, click the bundle that corresponds to your client adapter's model number (such as CB20A or 350 series). Select the latest bundled file for Windows XP and your specific client adapter type (such as CB or MPI).
  - If you want to select the client adapter's software files individually, find the section for Windows drivers and click the link for Windows XP. Select the driver file with the greatest version number for your specific client adapter type (such as CB or MPI).



---

**Note** The drivers for PC, LM, and PCI cards are labeled *PCMCIA-LMC-PCI*, the drivers for mini PCI cards are labeled *MPI*, and the drivers for PC-Cardbus cards are labeled *CB*.

---

- Step 4** Read and accept the terms and conditions of the Software License Agreement.
- Step 5** Select the file again to download it.
- Step 6** Save the file to a floppy disk or to your computer's hard drive.
- Step 7** Find the file using Windows Explorer, double-click it, and extract its files to a folder.
- Step 8** Make sure your client adapter is installed in your computer.
- Step 9** Double-click **My Computer**, **Control Panel**, and **System**.
- Step 10** Click the **Hardware** tab and **Device Manager**.
- Step 11** Double-click **Network Adapters** and the Cisco Systems Wireless LAN Adapter.
- Step 12** Click the **Driver** tab and the **Update Driver** button. The Welcome to the Hardware Update Wizard screen appears.
- Step 13** Select the **Install from a list or specific location (Advanced)** option and click **Next**.
- Step 14** When prompted to choose your search and installation options, select **Don't search. I will choose the driver to install** and click **Next**.
- Step 15** When prompted to select a network adapter to install, click the **Have Disk** button. The Install From Disk screen appears.
- Step 16** Click the **Browse** button, browse to the location of the extracted driver files, and click **Open**. The installation wizard finds the driver file. Click **OK** on the Install From Disk screen.

- Step 17** The Select Network Adapter screen reappears. Select the Cisco Systems Wireless LAN Adapter and click **Next**.
- Step 18** The installation wizard copies the driver files from the floppy disk or computer's hard drive. When the installation is complete, click **Finish**.

The driver upgrade is complete, and the old driver is overwritten by the new one.

## Uninstalling the Driver

This section provides instructions for uninstalling a client adapter driver from your computer. Two examples of when you may need to uninstall a driver are listed below:

- If you are running Windows 95, 98, NT, or 2000 and a Cisco Aironet client adapter was previously installed on your computer with the 6.10 driver, you must uninstall this driver before you can install a more recent driver, such as the one provided on the CD that shipped with your client adapter.
- If you experience difficulty while installing the driver for your computer's operating system, you may want to abort the installation procedure and start over. However, before you attempt to install the driver again, you must first uninstall any part of the driver that you may have already installed.

Table 8-2 enables you to quickly locate the instructions for uninstalling a driver for your specific operating system.

**Table 8-2** Locating Driver Uninstall Instructions

Operating System	6.10 Driver	Driver Other Than 6.10
Windows 95	<a href="#">page 8-14</a>	<a href="#">page 8-17</a>
Windows 98	<a href="#">page 8-14</a>	<a href="#">page 8-17</a>
Windows NT	<a href="#">page 8-15</a>	<a href="#">page 8-18</a>
Windows 2000	<a href="#">page 8-16</a>	<a href="#">page 8-18</a>
Windows Millennium (Me)	Not applicable	<a href="#">page 8-17</a>
Windows XP	Not applicable	<a href="#">page 8-19</a>

## Uninstalling the 6.10 Driver

To uninstall the 6.10 driver, follow the instructions that apply to your computer's operating system.

### Uninstalling the 6.10 Driver for Windows 95 and 98

- Step 1** Make sure the client adapter is in your computer and the computer is booted up.
- Step 2** Right-click the **WepStat** icon in the system tray on your desktop. This icon looks like two connected computers.
- Step 3** Click **Terminate**.
- Step 4** Insert the CD that contains the 6.10 driver into your computer's CD-ROM drive.
- Step 5** Open **Windows Explorer** and find the \Utilities\RmWep directory on your computer's CD-ROM drive.

- Step 6** Double-click the **RmWep.exe** file.
- Step 7** Minimize **Windows Explorer**.
- Step 8** Double-click **My Computer**, **Control Panel**, and **Network**.
- Step 9** In the Network window, select the Cisco Systems Wireless LAN Adapter.
- Step 10** Click **Remove** and **OK**.
- Step 11** When prompted to restart your computer, click **No**.
- Step 12** Maximize **Windows Explorer**.
- Step 13** Click **View**, **Options** or **Folder Options**, and **View**. Under Hidden files, make sure **Show all files** is selected, make sure the **Hide file extensions for known file types** check box is deselected, and click **OK**.
- Step 14** Find your computer's operating system in the following table, go to the path listed, and delete the file indicated.

Operating System	Location of File	File to be Deleted
Windows 95	C:\Windows\Inf	pc4800.inf
Windows 98	C:\Windows\Inf or C:\Windows\Inf\Other	pc4800.inf or aironetnetx500.inf

- Step 15** Remove the CD from your computer's CD-ROM drive.
- Step 16** Shut down your computer.
- Step 17** Remove the client adapter.

### Uninstalling the 6.10 Driver for Windows NT

- Step 1** Make sure the client adapter is in your computer and the computer is booted up.
- Step 2** Right-click the **WepStat** icon in the system tray on your desktop. This icon looks like two connected computers.
- Step 3** Click **Terminate**.
- Step 4** Insert the CD that contains the 6.10 driver into your computer's CD-ROM drive.
- Step 5** Open **Windows Explorer** and find the \Utilities\RmWep directory on your computer's CD-ROM drive.
- Step 6** Double-click the **RmWep.exe** file.
- Step 7** Close **Windows Explorer**.
- Step 8** Double-click **My Computer**, **Control Panel**, and **Network**.
- Step 9** In the Network window, click the **Adapters** tab.
- Step 10** Select the Cisco Systems Wireless LAN Adapter.
- Step 11** Click **Remove**.
- Step 12** When asked if you wish to continue, click **Yes** and **Close**.

- Step 13** When prompted to restart your computer, click **No**.
  - Step 14** Remove the CD from your computer's CD-ROM drive.
  - Step 15** Shut down your computer.
  - Step 16** Remove the client adapter.
- 

### Uninstalling the 6.10 Driver for Windows 2000

---

- Step 1** Make sure the client adapter is in your computer and the computer is booted up.
  - Step 2** Right-click the **WepStat** icon in the system tray on your desktop. This icon looks like two connected computers.
  - Step 3** Click **Terminate**.
  - Step 4** Insert the CD that contains the 6.10 driver into your computer's CD-ROM drive.
  - Step 5** Open **Windows Explorer**.
  - Step 6** Click **Tools, Folder Options, and View**.
  - Step 7** Under Hidden files and folders, make sure **Show hidden files and folders** is selected, make sure the **Hide file extensions for known file types** check box is deselected, and click **OK**.
  - Step 8** Find the \Utilities\RmWep directory on your computer's CD-ROM drive.
  - Step 9** Double-click the **RmWep.exe** file.
  - Step 10** Go to C:\Windows\Inf and double-click the oemx.inf and oemx.pnf files, where *x* equals a numeral, to open them.
  - Step 11** Delete the oemx.inf and oemx.pnf files that are labeled *Aironet* and are for a wireless LAN adapter.
  - Step 12** Remove the CD from your computer's CD-ROM drive.
  - Step 13** If you are prompted to restart your computer, click **Yes**.
  - Step 14** When the computer restarts, double-click **My Computer, Control Panel, and Add/Remove Hardware**.
  - Step 15** In the Add/Remove Hardware Wizard window, click **Next**.
  - Step 16** Click **Uninstall/Unplug a device**. Click **Next**.
  - Step 17** Click **Uninstall a device**. Click **Next**.
  - Step 18** From the Devices list, select the Cisco Systems Wireless LAN Adapter. Click **Next**.
  - Step 19** Click **Yes, I want to uninstall this device**. Click **Next**.
  - Step 20** Click **Finish**.
  - Step 21** Shut down your computer.
  - Step 22** Remove the client adapter.
-



## Uninstalling a Driver Other Than the 6.10 Driver

To uninstall a driver other than the 6.10 driver, follow the instructions that apply to your computer's operating system.



**Note** When you uninstall the driver, any saved profiles are lost.

### Uninstalling the Driver for Windows 95, 98, and Me



**Note** This procedure does not uninstall the driver that was bundled with Windows Me. It uninstalls only drivers to which you have upgraded. When you follow the steps below to uninstall an upgraded driver and then eject and reinsert the card, Windows Me finds the original driver and reinstalls it automatically.

- Step 1** Double-click **My Computer**, **Control Panel**, and **Network**.
- Step 2** In the Network window, select the Cisco Systems Wireless LAN Adapter.
- Step 3** Click **Remove** and **OK**.
- Step 4** When prompted to restart your computer, click **No**.
- Step 5** Open **Windows Explorer**.
- Step 6** If your computer's operating system is Windows 95 or 98, click **View**, **Options** or **Folder Options**, and **View**. Under Hidden files, make sure **Show all files** is selected and click **OK**.
- Step 7** Find your computer's operating system in the following table, go to the path listed, and delete the file indicated.

Operating System	Location of File	File to be Deleted
Windows 98	C:\Windows\Inf or C:\Windows\Inf\Other	pc4800.inf, aironetnetx500.inf, cisonetx500.inf, or CisonetA504.inf
Windows Me	C:\Windows\Inf\Other	aironetnetx500.inf, cisonetx500.inf, or CisonetA504.inf

- Step 8** Find your computer's operating system in the following table and delete any pcx50\*.sys files from the path indicated.

Operating System	Location of pcx50*.sys Files
Windows 95	C:\Windows\System\pcx50*.sys
Windows 98	C:\Windows\System\pcx50*.sys
Windows Me	C:\Windows\System32\Drivers\pcx50*.sys

- Step 9** Restart your computer.

## Uninstalling the Driver for Windows NT

---

- Step 1** Double-click **My Computer**, **Control Panel**, and **Network**.
  - Step 2** In the Network window, click the **Adapters** tab.
  - Step 3** Select the Cisco Systems Wireless LAN Adapter.
  - Step 4** Click **Remove**.
  - Step 5** When asked if you wish to continue, click **Yes** and **Close**.
  - Step 6** When prompted to restart your computer, click **Yes**.
- 

## Uninstalling the Driver for Windows 2000

---

- Step 1** Make sure the client adapter is installed in your computer. Otherwise, Windows cannot find the adapter to remove it.
  - Step 2** Double-click **My Computer**, **Control Panel**, and **Add/Remove Hardware**.
  - Step 3** In the Add/Remove Hardware Wizard window, click **Next**.
  - Step 4** Click **Uninstall/Unplug a device**. Click **Next**.
  - Step 5** Click **Uninstall a device**. Click **Next**.
  - Step 6** From the Devices list, select the Cisco Systems Wireless LAN Adapter. Click **Next**.
  - Step 7** Click **Yes, I want to uninstall this device**. Click **Next**.
  - Step 8** Click **Finish**.
  - Step 9** Open **Windows Explorer**.
  - Step 10** Click **Tools**, **Folder Options**, and **View**.
  - Step 11** Under Hidden files and folders, make sure **Show hidden files and folders** is selected. Click **OK**.
  - Step 12** Go to C:\Windows\Inf and double-click the oemx.inf and oemx.pnf files, where *x* equals a numeral, to open them.
  - Step 13** Delete the oemx.inf and oemx.pnf files that are labeled *Cisco* and are for a wireless LAN adapter.
  - Step 14** Go to C:\Windows\System32\Drivers and delete any pcx50\*.sys files.
  - Step 15** Shut down your computer.
  - Step 16** Remove the client adapter.
  - Step 17** Turn your computer back on.
-

## Uninstalling the Driver for Windows XP

**Note**

This procedure does not uninstall the driver that was bundled with Windows XP. It uninstalls only drivers to which you have upgraded. When you follow the steps below to uninstall an upgraded driver and then eject and reinsert the card, Windows finds the original driver and reinstalls it automatically.

**Note**

These instructions assume you are using Windows XP's classic view rather than its category view.

- 
- Step 1** Double-click **My Computer**, **Control Panel**, and **System**.
- Step 2** Click the **Hardware** tab and **Device Manager**.
- Step 3** Double-click **Network Adapters** and the Cisco Systems Wireless LAN Adapter.
- Step 4** Click the **Driver** tab and the **Uninstall** button.
- Step 5** A warning appears indicating that you are about to uninstall the client adapter from your system. Click **OK**.
- 

## ACU Procedures

This section provides instructions for the following procedures:

- Opening ACU, see below
- Exiting ACU, see [page 8-20](#)
- Modifying ACU installation settings, see [page 8-20](#)
- Determining the version of ACU, see [page 8-23](#)
- Upgrading ACU, see [page 8-24](#)
- Uninstalling ACU, see [page 8-27](#)
- Deleting the ACU icon from the desktop, see [page 8-28](#)

## Opening ACU

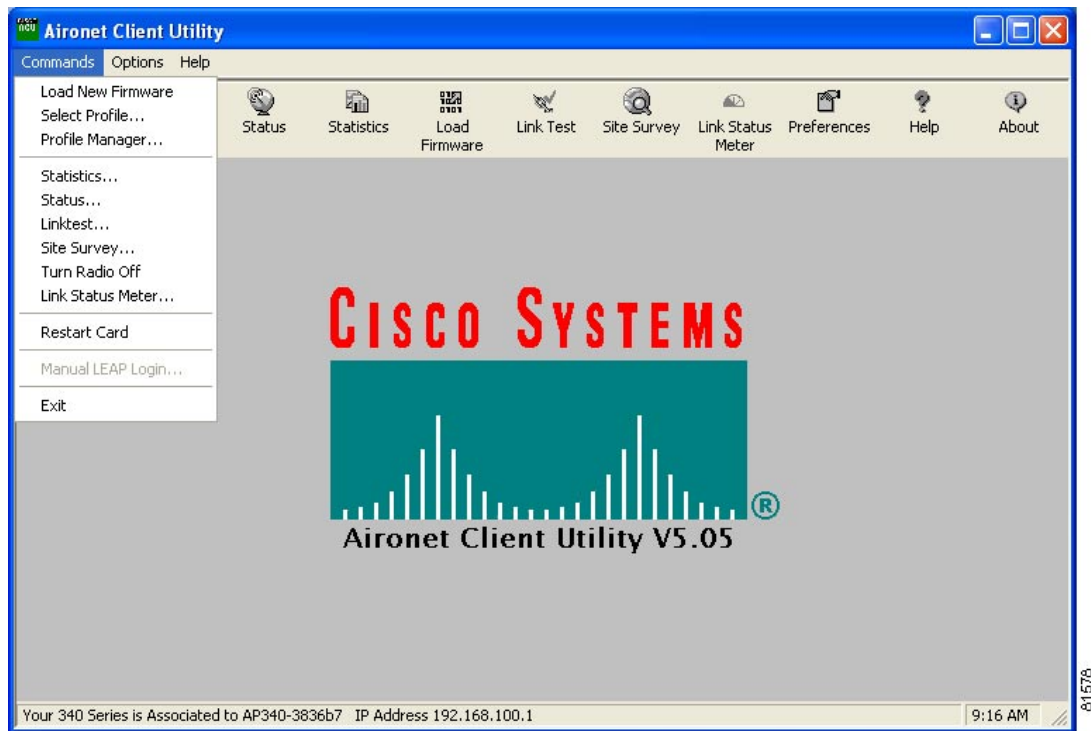
To open ACU, perform one of the following:

- Double-click the **Aironet Client Utility (ACU)** icon on your desktop.
- Select **Aironet Client Utility (ACU)** from the folder in the Windows Start Menu that you chose during installation [the default location is **Start > Program Files > Cisco Aironet > Aironet Client Utility (ACU)**].
- Double-click **My Computer > Control Panel > Aironet Client Utility**.

## Exiting ACU

To exit ACU, select **Exit** from the Commands drop-down menu (see [Figure 8-4](#)).

**Figure 8-4** Commands Drop-Down Menu



## Modifying ACU Installation Settings

Follow the steps below if you need to change any of the settings selected during ACU installation (for example, selecting LEAP or the location of the ACU program files).

- 
- Step 1** Close any Windows programs that are running.
  - Step 2** Select **Start > Run**, enter or browse to the path where the ACU files are installed (the default location is C:\Program Files\Cisco Aironet\setup.exe), and click **OK**. The Welcome screen for the Aironet Client Utility setup maintenance program appears.
  - Step 3** Select **Modify** and click **Next**. The installation goes through the same sequence of screens that appeared during the initial installation to allow you to select or deselect various options. The following steps walk you through the remaining screens.

**Step 4** In the Select Options screen, select as many of the following options as desired and click **Next**:

Option	Description
LEAP	<p>Enables you to create a profile in ACU that uses LEAP authentication. If this option is not selected now and you later want to use LEAP, you must run this installation program again, select <b>Modify</b>, and select this option.</p> <p><b>Note</b> Refer to <a href="#">Chapter 5</a> for information on using LEAP.</p> <p><b>Note</b> If you select LEAP on a Windows 95, 98, or 98 SE device, Microsoft hot fixes are installed during ACU installation to fix two problems related to the use of LEAP. Refer to <a href="#">Chapter 9</a> for more information on the hot fixes.</p> <p><b>Note</b> If you select LEAP on a Windows XP device, you cannot use Windows XP's fast user switching feature.</p>
Allow Saved LEAP User Name and Password	<p>Enables you to create a profile in ACU that uses a saved (rather than temporary) username and password for LEAP authentication. When such a profile is used, the saved username and password are used to start the LEAP authentication process, and you are not prompted to enter them.</p> <p><b>Note</b> This option is available only if the LEAP option is selected.</p>
PEAP	<p>Installs the PEAP supplicant, which enables the client to support PEAP authentication. If this option is not selected now and you later want to use PEAP, you must run this installation program again, select <b>Modify</b>, and select this option.</p> <p><b>Default:</b> Selected</p> <p><b>Note</b> Refer to <a href="#">Chapter 5</a> for information on using PEAP.</p> <p><b>Note</b> PC-Cardbus cards do not support PEAP authentication.</p> <p><b>Note</b> This option appears for all operating systems except Windows 95; however, your client adapter can authenticate using PEAP only if your computer's operating system is Windows 2000 (with Service Pack 3 or greater and the Windows 2000 Wireless 802.1X hot fix) or Windows XP.</p> <p><b>Note</b> Service Pack 1 for Windows XP includes Microsoft's PEAP supplicant, which supports a Windows username and password only and does not interoperate with Cisco's PEAP supplicant. To use Cisco's PEAP supplicant, install ACU version 5.05 or greater after Service Pack 1 for Windows XP. Otherwise, it will be overwritten by Microsoft's PEAP supplicant.</p>

Option	Description
EAP-SIM	<p>Installs the EAP-SIM supplicant, which enables the client to support EAP-SIM authentication. If this option is not selected now and you later want to use EAP-SIM, you must run this installation program again, select <b>Modify</b>, and select this option.</p> <p><b>Default:</b> Deselected</p> <p><b>Note</b> Refer to <a href="#">Chapter 5</a> for information on using EAP-SIM.</p> <p><b>Note</b> PC-Cardbus cards do not support EAP-SIM authentication.</p> <p><b>Note</b> This option appears for all operating systems except Windows 95; however, your client adapter can authenticate using EAP-SIM only if your computer's operating system is Windows 2000 (with Service Pack 3 or greater and the Windows 2000 Wireless 802.1X hot fix) or Windows XP.</p>
Create ACU Icon on your Desktop	Causes the installation program to add an ACU icon to your computer's desktop to provide quick access to the utility.
Allow Non-Administrator Users to save profiles to the registry	<p>Enables users without administrative rights to modify profiles in ACU and save them to the registry on computers running Windows NT, 2000, or XP.</p> <p><b>Note</b> This option is not available for Windows 95, 98, and Me because these versions of Windows do not support different classes of users.</p>

**Step 5** In the Choose Destination Location screen, perform one of the following:

- If you want the ACU program files to be installed in the default location (C:\Program Files, if C:\Program Files is the default Windows program file folder), click **Next**.
- If you want to specify a different destination location for the ACU program files, click **Browse**, select a location, and click **Next**.

**Step 6** In the Select Program Folder screen, specify a program folder name for ACU by selecting from the list of existing folders (the default name is Cisco Aironet) or typing in a new folder name; then click **Next**. A status screen displays the progress of the installation. Then the Setup Complete screen appears.

**Step 7** If your computer needs to be rebooted, select **Yes, I want to restart my computer now** or **No, I will restart my computer later** and click **Finish**.



**Note** If you are prompted to reboot your computer, Cisco recommends that you select the **Yes, I want to restart my computer now** option.

The client utility installation has been modified.

## Determining the Version of ACU

Follow the instructions in this section to determine if you need to upgrade ACU.

- Step 1** To determine the version of ACU that your client adapter is currently using, open ACU; then click the **About** icon or select the **About Aironet Client Utility** option from the Help drop-down menu. The About Aironet Client Utility screen appears (see [Figure 8-5](#)).

**Figure 8-5 About Aironet Client Utility Screen**



- Step 2** To determine the latest version of ACU available on Cisco.com, follow the steps below:



**Note** This step enables you to determine the version numbers of individual ACU files on Cisco.com. If you downloaded a bundled file from Cisco.com, find the folders that were extracted from the bundle. Look at the ACU folder. The version number is included in the folder name.

- a. Use your computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
- b. Click the link for Cisco Aironet Wireless LAN Client Adapters.
- c. Click the link for the Windows utility.
- d. Find the ACU file with the greatest version number. This is the latest available version on Cisco.com.

- Step 3** If the version of ACU available from Cisco.com has a higher number than the version currently being used by your client adapter, follow the instructions in the “[Upgrading ACU](#)” section on [page 8-24](#) to upgrade ACU.



**Note** If a version of ACU prior to 4.13 is installed on your computer, you must uninstall it before you can upgrade to a more recent version. Refer to the “[Uninstalling ACU Versions Prior to 4.13](#)” section on [page 8-27](#) for instructions.

## Upgrading ACU

Follow the instructions in this section to upgrade ACU to a more recent version.



---

**Note** If you create profiles using ACU version 5.0 (or greater), these profiles are saved if you upgrade to a more recent version of ACU.

---

**Step 1** Close any Windows programs that are running.

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

- If you are installing ACU from a bundled file on Cisco.com, follow the steps below:
  - a. Using Windows Explorer, find the folders that were extracted from the bundle and double-click the ACU folder.
  - b. Go to [Step 3](#).
- If you are installing ACU from an individual file on Cisco.com, follow the steps below:
  - a. Use the computer's web browser to access the following URL:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>
  - b. Click the link for Cisco Aironet Wireless LAN Client Adapters.
  - c. Click the link for the Windows utility.
  - d. Select the latest ACU file.
  - e. Read and accept the terms and conditions of the Software License Agreement.
  - f. Select the ACU file again to download it.
  - g. Save the file to your computer's hard drive.
  - h. Find the file using Windows Explorer, double-click it, and extract its files to a folder.
  - i. Go to [Step 3](#).

**Step 3** Select **Start > Run**, enter or browse to the path where you extracted the files (for example, C:\temp\setup.exe), and click **OK**. The Aironet Client Utility Setup screen and the InstallShield Wizard appear.

**Step 4** When the Welcome screen appears, click **Next**.



**Step 5** In the Select Options screen, select as many of the following options as desired and click **Next**:

Option	Description
LEAP	<p>Enables you to create a profile in ACU that uses LEAP authentication. If this option is not selected now and you later want to use LEAP, you must run this installation program again, select <b>Modify</b>, and select this option.</p> <p><b>Note</b> Refer to <a href="#">Chapter 5</a> for information on using LEAP.</p> <p><b>Note</b> If you select LEAP on a Windows 95, 98, or 98 SE device, Microsoft hot fixes are installed during ACU installation to fix two problems related to the use of LEAP. Refer to <a href="#">Chapter 9</a> for more information on the hot fixes.</p> <p><b>Note</b> If you select LEAP on a Windows XP device, you cannot use Windows XP's fast user switching feature.</p>
Allow Saved LEAP User Name and Password	<p>Enables you to create a profile in ACU that uses a saved (rather than temporary) username and password for LEAP authentication. When such a profile is used, the saved username and password are used to start the LEAP authentication process, and you are not prompted to enter them.</p> <p><b>Note</b> This option is available only if the LEAP option is selected.</p>
PEAP	<p>Installs the PEAP supplicant, which enables the client to support PEAP authentication. If this option is not selected now and you later want to use PEAP, you must run this installation program again, select <b>Modify</b>, and select this option.</p> <p><b>Default:</b> Selected</p> <p><b>Note</b> Refer to <a href="#">Chapter 5</a> for information on using PEAP.</p> <p><b>Note</b> PC-Cardbus cards do not support PEAP authentication.</p> <p><b>Note</b> This option appears for all operating systems except Windows 95; however, your client adapter can authenticate using PEAP only if your computer's operating system is Windows 2000 (with Service Pack 3 or greater and the Windows 2000 Wireless 802.1X hot fix) or Windows XP.</p> <p><b>Note</b> Service Pack 1 for Windows XP includes Microsoft's PEAP supplicant, which supports a Windows username and password only and does not interoperate with Cisco's PEAP supplicant. To use Cisco's PEAP supplicant, install ACU version 5.05 or greater after Service Pack 1 for Windows XP. Otherwise, it will be overwritten by Microsoft's PEAP supplicant.</p>

Option	Description
EAP-SIM	<p>Installs the EAP-SIM supplicant, which enables the client to support EAP-SIM authentication. If this option is not selected now and you later want to use EAP-SIM, you must run this installation program again, select <b>Modify</b>, and select this option.</p> <p><b>Default:</b> Deselected</p> <p><b>Note</b> Refer to <a href="#">Chapter 5</a> for information on using EAP-SIM.</p> <p><b>Note</b> PC-Cardbus cards do not support EAP-SIM authentication.</p> <p><b>Note</b> This option appears for all operating systems except Windows 95; however, your client adapter can authenticate using EAP-SIM only if your computer's operating system is Windows 2000 (with Service Pack 3 or greater and the Windows 2000 Wireless 802.1X hot fix) or Windows XP.</p>
Create ACU Icon on your Desktop	Causes the installation program to add an ACU icon to your computer's desktop to provide quick access to the utility.
Allow Non-Administrator Users to save profiles to the registry	<p>Enables users without administrative rights to modify profiles in ACU and save them to the registry on computers running Windows NT, 2000, or XP.</p> <p><b>Note</b> This option is not available for Windows 95, 98, and Me because these versions of Windows do not support different classes of users.</p>

**Step 6** In the Choose Destination Location screen, perform one of the following:

- If you want the ACU program files to be installed in the default location (C:\Program Files, if C:\Program Files is the default Windows program file folder), click **Next**.
- If you want to specify a different destination location for the ACU program files, click **Browse**, select a location, and click **Next**.

**Step 7** In the Select Program Folder screen, specify a program folder name for ACU by selecting from the list of existing folders (the default name is Cisco Aironet) or typing in a new folder name; then click **Next**.

A status screen displays the progress of the installation. Then one of two Setup Complete screens appears, depending on whether Windows needs to be restarted to complete the installation.

**Step 8** Perform one of the following:

- If your computer does not need to be rebooted, select either of the following options and click **Finish**:

Option	Description
View the README.TXT file	Opens a read-me file containing information about ACU.
Launch the Aironet Client Utility	Opens ACU so you can configure your client adapter.

- If your computer needs to be rebooted, select **Yes, I want to restart my computer now** or **No, I will restart my computer later** and click **Finish**.



**Note** If you are prompted to reboot your computer, Cisco recommends that you select the **Yes, I want to restart my computer now** option.

The ACU upgrade is complete.

## Uninstalling ACU

The procedure for uninstalling ACU varies based on the software's version number. Follow the instructions in one of the sections below to uninstall ACU.

### Uninstalling ACU Versions Prior to 4.13

If a version of ACU earlier than 4.13 is installed on your computer, Cisco recommends that you uninstall it before installing ACU version 5.0 or greater. Follow the steps below to uninstall a version of ACU prior to 4.13.

- Step 1** Double-click **My Computer**, **Control Panel**, and **Add/Remove Programs**.
- Step 2** Select the **Aironet Client Utility (ACU)**.
- Step 3** Click **Add/Remove** or **Change/Remove**.
- Step 4** When prompted to confirm your decision, click **Yes**. ACU is uninstalled.

### Uninstalling ACU Version 4.13 or Greater

Follow the steps below if you ever need to uninstall ACU version 4.13 or greater and its setup program.



**Note** Cisco does not recommend uninstalling ACU version 4.13 or greater before installing the latest version of ACU.

- Step 1** Close any Windows programs that are running.
- Step 2** Select **Start > Run**, enter the path to the installed ACU files (the default location is C:\Program Files\Cisco Aironet\setup.exe), and click **OK**. The Welcome screen for the Aironet Client Utility setup maintenance program appears.
- Step 3** Select **Remove** and click **Next**.
- Step 4** When asked if you want to completely remove the selected application and all of its components, click **OK**. The Setup Complete screen appears.

- Step 5** If your computer needs to be rebooted, select **Yes, I want to restart my computer now** or **No, I will restart my computer later**.



**Note** If you are prompted to reboot your computer, Cisco recommends that you select the **Yes, I want to restart my computer now** option. If you choose to restart your computer later, a warning appears indicating that the installed software might not work properly if you do not restart Windows, especially before installing ACU again.

- Step 6** Click **Finish**. ACU is uninstalled.

## Deleting the ACU Icon from the Desktop

An ACU icon is automatically added to the desktop when you install ACU, provided you selected this option during installation. If you wish to remove this icon from your desktop, right-click the icon, click **Delete**, and click **Yes** to confirm your decision.

## Restarting the Client Adapter

ACU enables you to re-initialize (or restart) the client adapter without having to reboot your computer or eject and reinsert the adapter. For instance, 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 reassociates to an access point with a stronger signal.



**Note** Restarting the client adapter may cause you to lose your wireless network connection.

Follow the steps below to restart the client adapter.

- Step 1** Open ACU.
- Step 2** Select the **Restart Card** option from the Commands drop-down menu (see [Figure 8-4](#)).
- Step 3** When prompted to confirm your decision, click **Yes**. The driver stops the client adapter's radio, writes the configuration (although no parameter settings have been changed), and restarts the radio. The status bar at the bottom of the ACU screen shows the client adapter losing association and then reassociating.

# Turning Your Client Adapter's Radio On or Off

Your client adapter's radio can be turned on or off. Turning the radio off prevents the adapter from transmitting RF energy. You might want to turn off the client adapter's radio in the following situations:

- You are not transmitting data and want to conserve battery power.
- You have EAP-SIM authentication set up to occur transparently (the SIM card is left in the reader and the PIN is stored in the computer), and you do not want to be billed for air time upon entering an area that enables the client to authenticate.
- You are using a laptop on an airplane and want to prevent the adapter's transmissions from potentially interfering with the operation of certain devices.

When the radio is on, it periodically sends out beacons even if it is not associated to an access point, as required by the 802.11 specification. Therefore, it is important to turn it off around devices that are susceptible to RF interference.



**Note**


---

Your client adapter is not associated while the radio is off.

---

You can turn the client adapter's radio on or off from the Windows system tray (if you installed the EAP-SIM supplicant) or from ACU. Follow the instructions on the next page.

## From the Windows System Tray

In the Windows system tray, move the cursor over the Aironet Client Monitor icon. 

A message appears indicating whether the client adapter's radio is on or off. Also, a red X appears on the icon when the radio is off.

If the radio is on, double-click the icon to turn the radio off or right-click the icon and select **Turn Radio Off**.

If the radio is off, double-click the icon to turn the radio on or right-click the icon and select **Turn Radio On**.

## From ACU

If your client adapter's radio is on, open ACU and select **Radio Off** from the Commands drop-down menu (see [Figure 8-4](#)) to turn the radio off. The status bar at the bottom of the ACU screen indicates that the radio is turned off.

If your client adapter's radio is off, open ACU and select **Radio On** from the Commands drop-down menu (see [Figure 8-4](#)) to turn the radio on.

## Uninstalling Microsoft Hot Fixes

When LEAP is selected during ACU installation on a Windows 95, 98, or 98 SE device, Microsoft hot fixes are also installed to fix two problems related to the use of LEAP. If you ever need to uninstall the hot fixes, select **Start > Run**, enter `C:\Windows\Inf\Qfe\W98.se\241052un.inf`, and click **OK**.





## Troubleshooting

---

This chapter provides information for diagnosing and correcting common problems 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 9-9](#)
- [Getting Help, page 9-25](#)

# 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 at <http://www.cisco.com/public/support/tac/home.shtml>. Select **Wireless Technologies** under Top Issues.

## Interpreting the Indicator LEDs


**Note**

Mini PCI cards do not have 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	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
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, 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 in ACU.



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

Green LED	Amber LED	Condition
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 if you encounter problems with your client adapter.

### Problems Installing the Driver

If you experience problems during driver installation, you may want to restart the installation process. Go to the [“Uninstalling the Driver”](#) section on page 8-14 to start with a clean install.

### Problems Installing ACU

If your attempt to install ACU failed, follow the steps below to repair the installation.

- 
- Step 1** Close any Windows programs that are running.
  - Step 2** Select **Start > Run**, enter the path to the installed ACU files (the default location is C:\Program Files\Cisco Aironet\setup.exe), and click **OK**. The Welcome screen for the Aironet Client Utility setup maintenance program appears.
  - Step 3** Select **Repair** and click **Next**. The Setup Complete screen appears.
  - Step 4** If your computer needs to be rebooted, select **Yes, I want to restart my computer now** or **No, I will restart my computer later**.




---

**Note** If you are prompted to reboot your computer, Cisco recommends that you select the **Yes, I want to restart my computer now** option.

---

- Step 5** Click **Finish**. The repair is complete. All of the selections you made during the previous installation are maintained.
-

## Client Adapter Recognition Problems



**Note** This section does not apply to mini PCI cards.

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



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

## Resolving Resource Conflicts



**Note** This section does not apply to the mini PCI cards.

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

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

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

## Resolving Resource Conflicts in Windows 95, 98, and Me

- 
- Step 1** Double-click **My Computer**, **Control Panel**, and **System**.
  - Step 2** Click the **Device Manager** tab.
  - Step 3** Double-click **Network Adapters**.
  - Step 4** Select the Cisco Systems Wireless LAN Adapter.
  - Step 5** Click the **Properties** button.
  - Step 6** In the General screen, the Device Status field indicates if a resource problem exists. If a problem is indicated, click the **Resources** tab.
  - Step 7** Deselect the **Use automatic settings** check box.
  - Step 8** Under Resource Settings or Resource Type, click **Input/Output Range**.
  - Step 9** Look in the Conflicting Device list at the bottom of the screen. If it indicates that the range is being used by another device, click the **Change Setting** button.
  - Step 10** Scroll through the ranges in the Value dialog box and select one that does not conflict with another device. The Conflict Information window at the bottom of the screen indicates if the range is already being used.

- Step 11** Click **OK**.
  - Step 12** Under Resource Settings or Resource Type, click **Interrupt Request**.
  - Step 13** Look in the Conflicting Device list at the bottom of the screen. If it indicates that the IRQ is being used by another device, click the **Change Setting** button.
  - Step 14** Scroll through the IRQs in the Value dialog box and select one that does not conflict with another device. The Conflict Information window at the bottom of the screen indicates if the IRQ is already being used.
  - Step 15** Click **OK**.
  - Step 16** Reboot your computer.
- 

## Resolving Resource Conflicts in Windows NT

---

- Step 1** Select **Start > Programs > Administrative Tools > Windows NT Diagnostics**.
  - Step 2** Click the **Resources** tab.
  - Step 3** Click the **IRQ** button.
  - Step 4** The used IRQs are listed in numerical order along the left side of the Resources window. Write down the number of an IRQ that is not being used; you will need it for Step 11.
  - Step 5** Click the **I/O Port** button.
  - Step 6** The used I/O ranges are listed in numerical order along the left side of the Resources window under Address. Write down an I/O range that is not being used (for example, if range 0100-013F is followed by 0170-0177 in the list, then 0140-0169 is an available range); you will need it for Step 13.
  - Step 7** Double-click **My Computer, Control Panel, and Network**.
  - Step 8** Click the **Adapters** tab and select the Cisco Aironet Wireless LAN Adapter.
  - Step 9** Click **Properties**.
  - Step 10** Select **Interrupt** under Property.
  - Step 11** Select the number of the unused interrupt from Step 4 in the Value drop-down box.
  - Step 12** Select **IO Base Address** under Property.
  - Step 13** Select a value that is within the unused range you determined in Step 6. For example, if your unused range is 0140-0169, you could select 150.
  - Step 14** Click **OK**.
- 

## Resolving Resource Conflicts in Windows 2000

---

- Step 1** Double-click **My Computer, Control Panel, and System**.
- Step 2** Click the **Hardware** tab and **Device Manager**.
- Step 3** Double-click **Network Adapters** and the Cisco Systems Wireless LAN Adapter.
- Step 4** In the General screen, the Device Status field indicates if a resource problem exists. If a problem is indicated, click the **Resources** tab.
- Step 5** Deselect the **Use automatic settings** check box.

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

## Resolving Resource Conflicts in Windows XP



### Note

These instructions assume you are using Windows XP's classic view, not its category view.

---

- Step 1** Double-click **My Computer**, **Control Panel**, and **System**.
- Step 2** Click the **Hardware** tab and **Device Manager**.
- Step 3** Under Network Adapters, double-click the Cisco Systems Wireless LAN Adapter.
- Step 4** In the General screen, the Device Status field indicates if a resource problem exists. If a problem is indicated, click the **Resources** tab.
- Step 5** Deselect the **Use automatic settings** check box.
- Step 6** Under Resource Settings, click **I/O Range**.
- Step 7** Look in the Conflicting Device list at the bottom of the screen. If it indicates that the range is being used by another device, click the **Change Setting** button.
- Step 8** Scroll through the ranges in the Value dialog box and select one that does not conflict with another device. The Conflict Information window at the bottom of the screen indicates if the range is already being used.
- Step 9** Click **OK**.
- Step 10** Under Resource Settings, click **IRQ**.
- Step 11** Look in the Conflicting Device list at the bottom of the screen. If it indicates that the IRQ is being used by another device, click the **Change Setting** button.

- Step 12** Scroll through the IRQs in the Value dialog box and select one that does not conflict with another device. The Conflict Information window at the bottom of the screen indicates if the IRQ is already being used.
- Step 13** Click **OK**.
- Step 14** Reboot your computer.
- 

## Problems Associating to an Access Point

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

- If possible, move your workstation a few feet closer to an access point and try again.
- Make sure that the client adapter is securely inserted in your computer's client adapter slot.
- If you are using a PCI client adapter, make sure that the antenna is securely attached.
- Make sure that the access point is turned on and operating.
- Check that all parameters are set properly for both the client adapter and the access point. These include the SSID, EAP authentication, WEP activation, network type, channel, etc.
- Follow the instructions in the previous section to resolve any resource conflicts. If you are using Windows NT, you may also want to try disabling the Ethernet port.
- 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 LEAP or EAP 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, network protocols, and further authentication information might be needed to connect to the network.

## Losing Association Upon Resuming from Suspend Mode (Windows NT and Mini PCI Card Only)

Because Windows NT does not support resuming of mini PCI cards, your client adapter loses its association to an access point upon resuming from suspend mode. If this occurs, restart your client adapter to reassociate.

## Parameters Missing from ACU Properties Screens

If some parameters are grayed out on the ACU Properties screens, your system administrator may have used an auto installer to deactivate these parameters. In this case, these parameters are not available for you to set.

## LEAP Login Screen Appears Before Windows Login Screen

If you are using Windows 95, 98, or Me and your client adapter is configured to use LEAP authentication with an automatically prompted login, the LEAP login screen should appear before the Windows screen after you reboot. If the Windows screen appears first, follow the steps below.

- 
- Step 1** On the Windows desktop, right-click the **My Network Places** icon.
  - Step 2** Click **Properties**.
  - Step 3** On the Network - Configuration screen, click the arrow on the right side of the Primary Network Logon box.
  - Step 4** Select **Cisco Aironet Wireless Logon** and click **OK**.
  - Step 5** When prompted to restart your computer, click **Yes**.
- 

## Microsoft Hot Fixes

When LEAP is selected during ACU installation on a Windows 95, 98, or 98 SE device, Microsoft hot fixes are also installed to fix two problems related to the use of LEAP. You can obtain descriptions of these hot fixes and the problems they resolve at the following Microsoft URLs:

- <http://support.microsoft.com/support/kb/articles/Q247/8/05.asp> (for Windows 95, 98, and 98 SE)
- <http://support.microsoft.com/support/kb/articles/Q165/4/02.asp> (for Windows 95 only)

**Note**

Only the English version of the hot fixes are installed. Foreign language versions of these operating systems require hot fixes specific to those languages. Contact Microsoft Product Support Services to obtain the hot fixes for languages other than English. Without the hot fixes installed, you may be prompted to enter your credentials at the Windows login prompt twice. To work around this problem, enter your login credentials again.

---

# 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 four sections (general, LEAP authentication, PEAP authentication, and EAP-SIM 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="#">9-9</a>
LEAP authentication	<a href="#">9-12</a>
PEAP authentication	<a href="#">9-15</a>
EAP-SIM authentication	<a href="#">9-20</a>

## General Error Messages

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

**Error Message** Bad Firmware Image File (*filename*)

**Explanation** The selected firmware file is corrupt and will not be sent to the client adapter.

**Recommended Action** Select a different firmware file and try to load it.

**Error Message** Card Removed at *xx:xx*

**Explanation** The client adapter was ejected from the computer.

**Recommended Action** Reinsert the client adapter if you wish to resume wireless communications.

**Error Message** Error Reading *filename*

**Explanation** A problem occurred while the computer was reading the firmware file from the disk.

**Recommended Action** Re-copy the firmware file to a floppy disk or to your computer's hard drive and try to load it again or select a different firmware file and try to load it.

**Error Message** Error Writing to Flash Memory

**Explanation** A problem occurred while the firmware was being flashed.

**Recommended Action** Eject the client adapter and reinsert it. If the client adapter functions properly, the firmware was flashed successfully. If the client adapter does not function or functions improperly, your client adapter may need to be returned for service. Refer to the [“Technical Assistance Center”](#) section in the Preface for information on contacting TAC.

**Error Message** Firmware Incompatible with Hardware

**Explanation** The selected firmware file does not work with the client adapter.

**Recommended Action** Select a different firmware file and try to load it.

**Error Message** Firmware Upgrade Failed

**Explanation** A problem occurred while the firmware was being flashed.

**Recommended Action** Eject the client adapter and reinsert it. If the client adapter functions properly, the firmware was flashed successfully. If the client adapter does not function or functions improperly, your client adapter may need to be returned for service. Refer to the [“Technical Assistance Center”](#) section in the Preface for information on contacting TAC.

**Error Message** Maximum Power Save Mode Will Be Temporarily Disabled While You Are Running This Application!

**Explanation** The client adapter cannot be run in Max PSP mode while ACU is running.

**Recommended Action** No user action is required. The client adapter automatically runs in Fast PSP mode while ACU is running.

**Error Message** No Wireless LAN Adapters Found

**Explanation** A client adapter is not inserted in the computer.

**Recommended Action** Insert a client adapter if you wish to start wireless communications.

**Error Message** No Wireless LAN Adapters Installed!

**Explanation** An attempt was made to start ACU without a client adapter being inserted in the computer. ACU cannot execute if a client adapter is not inserted because it needs to be able to read from and write to the adapter.

**Recommended Action** Insert a client adapter and start ACU.



**Error Message** Software installed might not work properly if you choose not to restart Windows. Please make sure to restart Windows before installing/using Aironet Client Utility.

**Explanation** The No, I will restart my computer later option was selected on the Setup Complete screen during an uninstall or install of ACU.

**Recommended Action** Restart your computer before installing or using ACU again.

**Error Message** Unable to Open *filename*

**Explanation** The selected firmware file cannot be found.

**Recommended Action** Re-copy the firmware file to a floppy disk or to your computer's hard drive and try to load it again or select a different firmware file and try to load it.

**Error Message** Wireless Connection Unavailable. (Windows XP only)

**Explanation** ACU was used to configure the client adapter on Windows XP, but the Use Windows to configure my wireless network settings check box in Windows XP is selected. This message appears even if the client adapter is associated to an access point.

**Recommended Action** Deselect the **Use Windows to configure my wireless network settings** check box in Windows XP to force Windows to display the correct status.

**Error Message** You cannot run a linktest because the radio in your Wireless LAN Adapter is not on!

**Explanation** An attempt was made to run a link test while the client adapter's radio was off.

**Recommended Action** Turn on the client adapter's radio by selecting **Radio On** from the Commands drop-down menu; then run the link test.

**Error Message** You cannot run a linktest because your Cisco Wireless LAN Adapter is not associated!

**Explanation** An attempt was made to run a link test while the client adapter was not associated to an access point or other wireless device.

**Recommended Action** Run the link test after the client adapter is associated to an access point or another wireless device.

**Error Message** You must specify an IP address before running a linktest!

**Explanation** An attempt was made to run a link test although the IP address of the access point or other wireless device with which to test the RF link was not specified.

**Recommended Action** In the Linktest screen's IP Address of Access Point field, enter the IP address of the access point or other wireless device with which you want to test the RF link.

**Error Message** You need to be an administrator or a user with administrative rights to install Aironet Client Utility. Please log on as a different user and try again.

**Explanation** A non-administrative user attempted to install ACU. The ACU installation process terminates.

**Recommended Action** Logon as a different user and attempt the installation process again.

**Error Message** Your Wireless LAN Adapter is not inserted!

**Explanation** One of two conditions is present: 1) a client adapter is not inserted in your computer or 2) ACU was started with one variety of client adapter inserted (such as a PCM342), it was subsequently ejected, and another variety was inserted (such as a PCM352).

**Recommended Action** Perform one of the following: 1) insert a client adapter into your computer if one is not present or 2) shut down ACU and restart it.

## LEAP Authentication Error Messages

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

**Error Message** Cannot find a wireless adapter that supports LEAP. Please make sure that you have installed the correct client adapter and updated your firmware.

**Explanation** LEAP authentication failed because the client adapter's firmware does not support LEAP.

**Recommended Action** Follow the instructions in the [“Upgrading the Firmware”](#) section on page 8-5 to install the latest client adapter firmware.

**Error Message** Cannot find a wireless adapter that supports WEP. Please make sure that you have installed the correct client adapter and purchased WEP support.

**Explanation** LEAP authentication failed because the client adapter does not support WEP.

**Recommended Action** Make sure that you have installed the correct client adapter or upgrade the adapter for WEP support.

**Error Message** The combination of domain name and user name exceeds maximum number of characters (32) that LEAP supports. Please uncheck Include Windows Logon Domain with User Name in ACU or log on to a local computer, or use shorter names.

**Explanation** The combination of characters entered for the username and domain name in the Windows login screen or the LEAP login screen exceed the maximum number supported by LEAP, which is 32.

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

- Deselect the **Include Windows Logon Domain With User Name** check box in the LEAP Settings screen of ACU.
- Log on to a local computer, which does not use a domain name, and try to authenticate again.
- Enter a set of credentials (username, password, and domain name) with fewer characters.

**Error Message** The current active profile is not configured for LEAP.

**Explanation** The Manual LEAP Login option was selected in ACU, but the active profile is not configured for LEAP. The LEAP authentication process aborts.

**Recommended Action** If you want the client adapter to LEAP authenticate, select a profile that is configured for LEAP.

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

**Explanation** The username and password for your current profile have expired or are no longer valid. When the LEAP login screen appeared, prompting you to enter your new username and password, you selected Cancel.

**Recommended Action** Click **No**, enter your new username and password when the LEAP login screen reappears, and click **OK**. The client adapter should authenticate using your new credentials. If the profile uses saved credentials, edit the profile in ACU by changing the username and password on the LEAP Settings screen and save your changes. (If you select **Yes**, the profile is disabled until you reboot your system or eject and reinsert the card.)

**Error Message** A recently installed program has disabled the Welcome screen and Fast User Switching. To restore these features, you must uninstall the program. The following file name might help you identify the program that made the change: cswGina.dll. (Windows XP only)

**Explanation** LEAP was selected during ACU installation on a Windows XP computer; then the Change the way users log on or off option was selected under Windows XP's User Accounts.

**Recommended Action** If LEAP is selected during ACU installation, you cannot use Windows XP's fast user switching feature. If you want to use fast user switching and do not want to use LEAP, you must run the ACU installation program again, select **Modify**, and deselect **LEAP**.

**Error Message** To run LEAP successfully, you will have to apply Microsoft Q241052 Update for the language version of your operating system as documented on <http://support.microsoft.com/support/kb/articles/Q247/8/05.asp>. Please contact Microsoft Product Support Services to obtain the fix.

**Explanation** When LEAP is selected during ACU installation on a Windows 95, 98, or 98 SE device, Microsoft hot fixes are also installed to fix two problems related to the use of LEAP. However, only the English version of the hot fixes are installed. Foreign language versions of these operating systems require hot fixes specific to those languages.

**Recommended Action** Contact Microsoft Product Support Services to obtain the hot fixes for languages other than English. Without the hot fixes installed, you may be prompted to enter your credentials at the Windows login prompt twice. To work around this problem, enter your login credentials again.

**Error Message** Unable to authenticate wireless user. Please make sure you have entered the right user name and password and try again.

**Explanation** LEAP authentication failed.

**Recommended Action** Re-enter the LEAP user name and password or cancel the LEAP authentication. To start another LEAP authentication process, log off and log in again or select **Manual LEAP Login** from the Commands drop-down menu.

**Error Message** The user name and password entered for profile 'xxx' are no longer valid and have failed the LEAP authentication. Please enter a new user name and password.

**Explanation** The username and password for your current profile have expired or are no longer valid; therefore, your client adapter is unable to LEAP authenticate.

**Recommended Action** When the LEAP login screen appears, enter your new username and password and click **OK**. The client adapter should authenticate using your new credentials.

**Error Message** The user name and password entered for saved profile 'xxx' are no longer valid and have failed the LEAP authentication. Please enter a new user name and password. Please also remember to change them permanently in the saved profile using the ACU Profile Manager.

**Explanation** The username and password for your current profile, which uses saved credentials, have expired or are no longer valid; therefore, your client adapter is unable to LEAP authenticate.

**Recommended Action** When the LEAP login screen appears, enter your new username and password and click **OK**. The client adapter should authenticate using your new credentials. Then edit the profile in ACU by changing the username and password on the LEAP Settings screen and save your changes.

## PEAP Authentication Error Messages

This section lists error messages that may occur during PEAP authentication. The messages are divided into six subsections based on the type of database that is used with PEAP. Use [Table 9-4](#) to quickly locate the error messages for your database.

**Table 9-4 Locating PEAP Authentication Error Messages**

Error Message Category	Page Number
All PEAP-supported databases	<a href="#">9-15</a>
Windows NT or 2000 domain databases	<a href="#">9-15</a>
All OTP databases	<a href="#">9-16</a>
OTP databases using SofToken version 1.3	<a href="#">9-17</a>
OTP databases using SofToken II version 2.0	<a href="#">9-18</a>
OTP databases using RSA SecurID version 2.5	<a href="#">9-19</a>

### For All PEAP-Supported Databases

**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.

### For Windows NT or 2000 Domain Databases

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

**Explanation** You entered different values in the New Password and Confirm New Password fields on the Change Password screen. They must be identical.

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

**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 screen does not match the password that was used previously.

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

**Error Message** Your domain password has been successfully changed on the server. To synchronize any Windows password that might be locally cached, you must also manually change the password in Windows.

**Explanation** You have successfully changed your domain password using the Static Password screen. However, if you also have a locally cached Windows password, you must manually change it to synchronize it with your domain password.

**Recommended Action** Press **Ctrl-Alt-Delete**, select **Change Password**, and enter your old password once and your new password twice.

## For All OTP Databases

**Error Message** Failed to change your PIN. Error code xxx. Run Software Token program to fix it.

**Explanation** Your attempt to change your PIN using the Change PIN screen failed due to a problem with the software token program.

**Recommended Action** Run the software token program and then try to change your PIN again.

**Error Message** Invalid PIN. Please try again.

**Explanation** The PIN that you entered is invalid.

**Recommended Action** Re-enter your PIN.

**Error Message** New PIN and Confirm New PIN do not match. Please try them again.

**Explanation** You entered different values in the New PIN and Confirm New PIN fields on the Change PIN screen. They must be identical.

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

**Error Message** New PIN is invalid. Please try it again.

**Explanation** The PIN that you entered in the New PIN field on the Change PIN screen is invalid.

**Recommended Action** Re-enter your new PIN.

**Error Message** The old PIN you supplied is invalid. Please try it again.

**Explanation** The old PIN that you entered on the Change PIN screen is invalid.

**Recommended Action** Re-enter your old PIN.

**Error Message** Please check either Support Hardware Token or Support Software Token. One of them must be selected.

**Explanation** While the client adapter was being configured for PEAP authentication, the One Time Password option was selected on the Generic Token Card Properties screen, but neither the Support Hardware Token nor the Support Software Token option was selected.

**Recommended Action** Select either the **Support Hardware Token** check box or the **Support Software Token** check box or both.

**Error Message** Your PIN has expired. Please change your PIN.

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

**Recommended Action** Follow the instructions in the [“After Your PIN Expires \(OTP Databases Only\)” section on page 6-16](#) to change your PIN.

## For OTP Databases Using Secure Computing Softoken Version 1.3

**Error Message** Could not find Softoken.exe in the program path specified. Please make sure Softoken is installed correctly and the correct program path is entered.

**Explanation** Softoken.exe is not located in the path you entered on the Generic Token Card Properties screen.

**Recommended Action** Make sure that Softoken is installed correctly; then re-enter the program path.

**Error Message** Error getting data from Softoken server. Please make sure Softoken is installed correctly and the correct program path is entered.

**Explanation** An error occurred while attempting to get data from the Softoken server.

**Recommended Action** Make sure that Softoken is installed correctly and the correct program path is entered.

**Error Message** Initialization of Softoken library failed. Please make sure Softoken is installed correctly and the correct program path is entered.

**Explanation** An error occurred with the Softoken program.

**Recommended Action** Make sure that Softoken is installed correctly and the correct program path is entered.

**Error Message** The program path entered exceeds the maximum length allowed (255).

**Explanation** The program path entered on the Generic Token Card Properties screen contains more characters than the field allows.

**Recommended Action** Re-enter the path using a maximum of 255 characters. If necessary, move Softoken.exe to a directory with a shorter path.

**Error Message** Program path must be specified for SofToken Version 1.3.

**Explanation** Secure Computing SofToken Version 1.3 was selected from the Supported Type drop-down box on the Generic Token Card Properties screen, but the SofToken program path was not entered.

**Recommended Action** Enter the path to the SofToken program in the SofToken Program Path field.

**Error Message** SofToken is not set up to allow processing from SofToken calls. Calls have been disabled from the SofToken Manager, the SofToken program does not have any valid users yet, or the last person to use SofToken was not initialized correctly.

**Explanation** The SofToken program is not set up to process SofToken API calls.

**Recommended Action** Make sure that SofToken is configured to enable SofToken calls and verify that you are set up as a valid user.

**Error Message** Unable to launch SofToken.exe. Please make sure SofToken is installed correctly and the correct program path is entered.

**Explanation** An error occurred with the SofToken program.

**Recommended Action** Make sure that SofToken is installed correctly and the correct program path is entered.

**Error Message** Unable to load SofToken library. Please make sure that SofToken is installed correctly.

**Explanation** An error occurred with the SofToken program.

**Recommended Action** Make sure that SofToken is installed correctly and the correct program path is entered.

## For OTP Databases Using Secure Computing SofToken II Version 2.0

**Error Message** Error getting the OTP password for the user. Run SofToken II to ensure the user is set up correctly.

**Explanation** An error occurred while attempting to obtain the OTP password for the user.

**Recommended Action** Run the SofToken II program to make sure that the user is set up properly.



**Error Message** Failed to load data from the OTP database for User ID: xxxx. Run SofToken II to ensure the user is set up correctly.

**Explanation** An error occurred while attempting to load data from the OTP database for the specified user.

**Recommended Action** Run the SofToken II program to make sure that the specified user is set up properly.

**Error Message** Here is the hint you entered when you created your PIN: xxxx.

**Explanation** You entered an invalid PIN.

**Recommended Action** Use the hint to help you remember your PIN; then re-enter it.

**Error Message** Unable to load SofToken II library. Please make sure that SofToken II is installed correctly.

**Explanation** An error occurred with the SofToken II program.

**Recommended Action** Make sure that SofToken II is installed correctly.

## For OTP Databases Using RSA SecurID Version 2.5

**Error Message** Error getting password from RSA SecurID Software Token.

**Explanation** An error occurred while attempting to obtain the user password from the RSA SecurID program.

**Recommended Action** Run the RSA SecurID program to make sure that the user is set up properly.

**Error Message** Unable to load RSA library. Please make sure that RSA SecurID Software Token is installed correctly.

**Explanation** An error occurred with the RSA SecurID program.

**Recommended Action** Make sure that RSA SecurID is installed correctly.

**Error Message** Unable to open RSA Token service.

**Explanation** An error occurred with the RSA SecurID program.

**Recommended Action** Make sure that RSA SecurID is installed correctly.

## EAP-SIM Authentication Error Messages

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

**Error Message** `Client_handleResponseIdentity` error.

**Explanation** When asked to perform an authentication, the supplicant encountered an error retrieving your network username from the SIM card. This error may occur if an invalid SIM card (such as one intended for mobile phone use) is inserted in the card reader or if Windows encountered a processing error.



**Note** The eight-digit hexadecimal error code in the message may assist technical support in troubleshooting your problem.

**Recommended Action** Make sure that you have a valid SIM card that was provided to you for wireless network access and that is inserted properly. If the problem occurs several times in a row, reboot your computer.

**Error Message** For the changes to take effect, please restart your WLAN card (or your computer) NOW.

**Explanation** The changes you made on the SIM Authentication Properties screen can take effect only if you perform a complete reauthentication. Otherwise, your wireless network connection may appear to be stuck in the “Validating identity” state.

**Recommended Action** Turn off your client adapter’s radio, wait a few seconds, and then turn the radio back on. Refer to the [“Turning Your Client Adapter’s Radio On or Off”](#) section on page 8-29 for instructions.

**Error Message** `GetUserPin` returned error.

**Explanation** Windows encountered an error while prompting for or retrieving the PIN.



**Note** The eight-digit hexadecimal error code in the message may assist technical support in troubleshooting your problem.

**Recommended Action** Wait until the system tries to authenticate the client adapter again (approximately 30 to 60 seconds) and enter a valid PIN. Do not click Cancel or otherwise interfere with the normal operation of Windows. If the problem persists, reboot your computer.

**Error Message** Maximum length of PIN is 8 characters.

**Explanation** You tried to enter a PIN that is longer than eight characters. SIM card PINs are restricted to a maximum length of eight alphanumeric characters.

**Recommended Action** Delete one or more characters from the PIN field or delete all of the characters you entered and retype the complete PIN.

**Error Message** Network authentication aborted.

**Explanation** When you were asked to enter a PIN, you clicked the Cancel button and cancelled the authentication process. The supplicant will not attempt to authenticate to the network.



---

**Note** The system will try to authenticate automatically within 30 to 60 seconds.

---

**Recommended Action** If you want to authenticate to the network and establish a wireless network connection, enter the valid PIN for your SIM card. If you do not want to establish a connection, consider turning off or ejecting the client adapter; otherwise, the system will reprompt you every 30 to 60 seconds.

**Error Message** Network rejected user authentication.

**Explanation** The service provider's network has rejected your authentication attempt. This is most likely due to an expired or invalid SIM card or an invalidated account. However, it could also occur if the service provider at your current location does not allow access to the network for subscribers of your service provider.

**Recommended Action** Make sure that your account is in good standing and that you have a valid SIM card. Switch to a SIM card that is valid at the current location and try again.

**Error Message** Please check your smartcard reader and insert your SIM card.

**Explanation** When asked to perform an authentication, the supplicant could not get the smartcard reader to initialize within a reasonable time (that is, 90 seconds for the first try and 5 minutes for subsequent tries). Most likely, the reader is not plugged in correctly, or the computer no longer recognizes it.



---

**Note** The eight-digit hexadecimal error code in the message may assist technical support in troubleshooting your problem.

---

**Recommended Action** Follow the steps below.

- 
- Step 1** Install a smartcard reader if you have not done so.
  - Step 2** If a reader is installed, make sure that it is inserted completely into the PCMCIA slot (PCMCIA model) or that the connector cable is inserted properly into the serial or USB connector (serial/USB port model).
  - Step 3** Make sure that the system recognizes your reader. It should be listed under Smart card readers in Windows device manager. If your reader is not listed, eject and re-insert the reader (PCMCIA model) or disconnect and reconnect the cable (serial/USB port model).
  - Step 4** If the computer still does not recognize your reader, reboot the computer with the reader installed.
-

**Error Message** Please check your smartcard reader and SIM card, then try again.

**Explanation** The supplicant has detected a general smartcard-related error (that is, not one of the specific errors included in this section) and has aborted the authentication process.



**Note** The eight-digit hexadecimal error code in the title may assist technical support in troubleshooting your problem.

**Recommended Action** Follow the steps below.

- 
- Step 1** Make sure that your smartcard reader is installed properly and that your SIM card is inserted properly.
  - Step 2** Follow the Recommended Action instructions for the “Please check your smartcard reader and try again” error message below.
  - Step 3** Follow the Recommended Action instructions for the “Please insert your SIM card and try again” error message on [page 9-23](#).
  - Step 4** If you are sure that the reader and card are both inserted properly, wait until the system tries to authenticate again. This should occur within 30 to 60 seconds.



**Caution** Never remove your SIM card until the system has completed the authentication process.

- Step 5** If the problem persists, try restarting the client adapter or rebooting your computer.
- 

**Error Message** Please check your smartcard reader and try again.

**Explanation** Windows could not detect a smartcard reader in the system. You may not have installed a reader, or this may happen after resuming Windows from suspend or hibernation.

**Recommended Action** Follow the steps below.

- 
- Step 1** Install a smartcard reader if you have not done so.
  - Step 2** If a reader is installed, make sure that it is inserted completely into the PCMCIA slot (PCMCIA model) or that the connector cable is inserted properly into the serial or USB connector (serial/USB port model).
  - Step 3** Make sure that the system recognizes your reader. It should be listed under Smart card readers in Windows device manager. If your reader is not listed, eject and re-insert the reader (PCMCIA model) or disconnect and re-connect the cable (serial/USB port model).
  - Step 4** If the computer still does not recognize your reader, reboot the computer with the reader installed.
-

**Error Message** Please contact your service provider to unblock your card.

**Explanation** You have exceeded your SIM card's retry limit by entering too many incorrect PINs in a row.

**Recommended Action** Contact your service provider's customer service center to get the card unblocked. The phone number may be printed on your SIM card.

**Error Message** Please do not switch SIM cards after authenticating.

**Explanation** The supplicant has detected that the network username stored on the currently inserted SIM card differs from the username that was used in a previous authentication. Due to this mismatch, authentication may fail.

**Recommended Action** If the currently inserted SIM card is recognized by the network, authentication may succeed or fail, depending on the network configuration. If your client adapter is authenticated, you may ignore this message. Otherwise, replace the SIM card currently inserted with the SIM card that was used for your first authentication and wait until the system tries to authenticate your client adapter again (approximately 30 to 60 seconds). You may also restart the client adapter or reboot your computer with the new SIM card to try again.

**Error Message** Please enter a PIN (1 to 8 characters).

**Explanation** When you were prompted for a PIN, you clicked the OK button before entering the PIN.

**Recommended Action** Enter the PIN required to access your SIM card. If you do not want to authenticate at this time or do not have your PIN available, click the **Cancel** button instead.

**Error Message** Please insert your SIM card and try again.

**Explanation** The system could not detect a SIM card in the smartcard reader.

**Recommended Action** Make sure that your SIM card is inserted into the reader properly. It should be inserted into the reader all the way and not into the empty space in the PCMCIA slot. Try removing and re-inserting the card. You should feel it latch into place and notice a slight resistance when attempting to remove it.

**Error Message** SimOpenSession error.

**Explanation** When asked to retrieve your network username, the supplicant was unable to establish a connection to the SIM card. This can occur if a SIM card is not inserted in the reader, the SIM card is not inserted properly, or the wrong SIM card is inserted.

**Recommended Action** Make sure that you are using a valid SIM card (that is, the SIM card provided to you for wireless network access, not a SIM card intended for mobile phone use). If that does not correct the error, make sure that your SIM card is inserted into the reader properly. It should be inserted into the reader all the way and not into the empty space in the PCMCIA slot. Try removing and re-inserting the card. You should feel it latch into place and notice a slight resistance when attempting to remove it.

**Error Message** Time-out waiting for smartcard reader initialization.

**Explanation** When asked to perform an authentication, the supplicant could not get the smartcard reader to initialize within a reasonable time (90 seconds for the first try and 5 minutes for subsequent tries). Most likely, the reader is not plugged in correctly, or the computer no longer recognizes it.



**Note** The eight-digit hexadecimal error code in the message may assist technical support in troubleshooting your problem.

**Recommended Action** Follow the steps below.

- 
- Step 1** Install a smartcard reader if you have not done so.
  - Step 2** If a reader is installed, make sure that it is inserted completely into the PCMCIA slot (PCMCIA model) or that the connector cable is inserted properly into the serial or USB connector (serial/USB port model).
  - Step 3** Make sure that the system recognizes your reader. It should be listed under Smart card readers in Windows device manager. If your reader is not listed, eject and re-insert the reader (PCMCIA model) or disconnect and re-connect the cable (serial/USB port model).
  - Step 4** If the computer still does not recognize your reader, reboot the computer with the reader installed.
- 

**Error Message** Wrong PIN entered (*X* tries left).

**Explanation** The SIM card could not validate the PIN you have entered. You must have entered the wrong PIN.

**Recommended Action** Make sure that you enter the correct PIN. If your PIN contains letters, enter them in the correct case as the PIN is case sensitive. Check that the Caps Lock key has not inadvertently been pressed. Also, make sure that you have inserted the correct SIM card.



**Note** Most SIM cards limit the number of times in a row that you can enter an incorrect PIN. The error message indicates how many attempts you have left. Entering the correct PIN resets the limit to its original value. However, if the number of retries is exhausted, the SIM card locks up and becomes useless.

# Getting Help

To access information about ACU, open ACU; then click the **Help** icon or select **Contents** from the Help drop-down menu. An overview of ACU is displayed.

From the Overview of the Aironet Client Utility screen, you can access additional information.

- To access information on specific menu options, click **Contents**; double-click **Aironet Client Utility Commands**, the desired menu (such as Options Menu), and the desired topic (such as Preferences).
- To access information on specific parameters, click **Contents**; double-click **Configurable Parameters**, the client adapter, a parameter category (such as System Parameters), and the desired parameter (such as SSID).
- To access information on specific diagnostic topics, click **Contents**; double-click **Run Time Diagnostic Information**, a diagnostic category (such as Running a Linktest), and the desired topic (such as Packet Size).
- To search for a specific topic, click **Index**, select an index entry, and click **Display**.
- To search for a specific word or phrase, click **Contents** or **Index**, click the **Find** tab, and follow the instructions in the Find Setup Wizard window.







## Technical Specifications

---

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

The following topics are covered in this appendix:

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

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

**Note**

If a distinction is not made between radio or client adapter type, the specification applies to all Cisco Aironet Wireless LAN Client Adapters.

**Table A-1 Technical Specifications for Cisco Aironet Wireless LAN Client Adapters**

---

**Physical Specifications**


---

Size	
PC card and PC-Cardbus card	4.5 in. L x 2.1 in. W x 0.2 in. H (11.3 cm L x 5.4 cm W x 0.5 cm H)
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)
PCI card	5.8 in. L x 3.2 in. W x 0.5 in. H (14.7 cm L x 8.1 cm W x 1.3 cm H)
Mini PCI card	2.3 in. L x 2.0 in. W x 0.2 in. H (6.0 cm L x 5.1 cm W x 0.5 cm H)
Weight	
PC card and LM card	1.3 oz (0.037 kg)
PCI card	4.6 oz (0.13 kg)
Mini PCI card	0.5 oz (0.014 kg)
PC-Cardbus card	1.5 oz (0.043 kg)
Enclosure	
PC card and PC-Cardbus card	Extended Type II PC card
LM card	Standard Type II PC card with RF connectors
Connector	
PC card and LM card	68-pin PCMCIA
PCI card	PCI card edge
PC-Cardbus card	68-pin Cardbus
Status indicators	Green and amber LEDs (except mini PCI card); see <a href="#">Chapter 9</a>
Operating temperature	
340 series client adapters	32°F to 158°F (0°C to 70°C)
350 series client adapters	-22°F to 158°F (-30°C to 70°C)
5-GHz client adapters	-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
ESD	15 kV (human body model)

**Table A-1 Technical Specifications for Cisco Aironet Wireless LAN Client Adapters (continued)**

<b>Radio Specifications</b>	
Type	
2.4-GHz client adapters	Direct-sequence spread spectrum (DSSS) IEEE 802.11b compliant
5-GHz client adapters	Orthogonal frequency division multiplexing (OFDM) IEEE 802.11a compliant
Power output	
<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 340 or 350 series client adapter, your power level options may be different than those listed here.
340 series PC card	30 mW (15 dBm) 1 mW (0 dBm)
340 series LM card and PCI card	30 mW (15 dBm) 15 mW (12 dBm) 5 mW (7 dBm) 1 mW (0 dBm)
350 series client adapters	100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 5 mW (7 dBm) 1 mW (0 dBm)
PC-Cardbus card	20 mW (13 dBm) 10 mW (10 dBm) 5 mW (7 dBm)  <b>Note</b> These values are based on the FCC peak measurement method as defined in FCC 15.407(a)(4).
Operating frequency	
2.4-GHz client adapters	2.400 to 2.497 GHz (depending on the regulatory domain in which the client adapter is used)
5-GHz client adapters	5.15 to 5.25 GHz in the UNII 1 band* 5.25 to 5.35 GHz in the UNII 2 band* *Depending on the regulatory domain in which the client adapter is used
Usable channels	
2.4-GHz client adapters	2412 to 2484 MHz in 5-MHz increments
5-GHz client adapters	5170 to 5320 MHz in 20-MHz increments

**Table A-1 Technical Specifications for Cisco Aironet Wireless LAN Client Adapters (continued)**

Interference rejection	
2.4-GHz client adapters	35 dB adjacent channel rejection
5-GHz client adapters	16 dB @ 6 Mbps adjacent channel rejection 15 dB @ 9 Mbps adjacent channel rejection 13 dB @ 12 Mbps adjacent channel rejection 11 dB @ 18 Mbps adjacent channel rejection 8 dB @ 24 Mbps adjacent channel rejection 4 dB @ 36 Mbps adjacent channel rejection 0 dB @ 48 Mbps adjacent channel rejection -1 dB @ 54 Mbps adjacent channel rejection
Data rates	
2.4-GHz client adapters	1, 2, 5.5, and 11 Mbps
5-GHz client adapters	6, 9, 12, 18, 24, 36, 48, and 54 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 Orthogonal frequency division multiplexing (OFDM) - 6 to 54 Mbps
Receiver sensitivity	
340 series client adapters	-90 dBm @ 1 Mbps -88 dBm @ 2 Mbps -87 dBm @ 5.5 Mbps -83 dBm @ 11 Mbps
350 series client adapters	-94 dBm @ 1 Mbps -91 dBm @ 2 Mbps -89 dBm @ 5.5 Mbps -85 dBm @ 11 Mbps
5-GHz client adapters	-85 dBm @ 6 Mbps -84 dBm @ 9 Mbps -82 dBm @ 12 Mbps -80 dBm @ 18 Mbps -77 dBm @ 24 Mbps -73 dBm @ 36 Mbps -69 dBm @ 48 Mbps -68 dBm @ 54 Mbps
Receiver delay spread (multipath)	
2.4-GHz client adapters	500 ns @ 1 Mbps 400 ns @ 2 Mbps 300 ns @ 5.5 Mbps 140 ns @ 11 Mbps (350 series client adapters) 70 ns @ 11 Mbps (340 series client adapters)

**Table A-1 Technical Specifications for Cisco Aironet Wireless LAN Client Adapters (continued)**

Range	
340 series client adapters	<p><b>Outdoor</b> 1500 ft (457.2 m) @ 1 Mbps 1200 ft (365.8 m) @ 2 Mbps 800 ft (243.8 m) @ 5.5 Mbps 400 ft (121.9 m) @ 11 Mbps</p> <p><b>Indoor</b> 300 ft (91.4 m) @ 1 Mbps 225 ft (68.6 m) @ 2 Mbps 150 ft (45.7 m) @ 5.5 Mbps 100 ft (30.5 m) @ 11 Mbps</p> <p><b>Note</b> The above range numbers assume the use of a snap-on antenna with the LM card.</p>
350 series client adapters	<p><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</p> <p><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</p> <p><b>Note</b> The above range numbers assume the use of a snap-on antenna with the LM card.</p>
5-GHz client adapters	<p><b>Outdoor</b> 1200 ft (365.8 m) @ 6 Mbps 700 ft (213.4 m) @ 18 Mbps 120 ft (36.6 m) @ 54 Mbps</p> <p><b>Indoor</b> 200 ft (61.0 m) @ 6 Mbps 150 ft (45.7 m) @ 18 Mbps 70 ft (21.3 m) @ 54 Mbps</p> <p><b>Note</b> The above range numbers assume that the client adapter is being used with a Cisco Aironet 1200 Series Access Point with a patch antenna. Different range characteristics are likely when using the client adapter with a non-Cisco access point or a Cisco Aironet 1200 Series Access Point with an omni-directional antenna.</p>
Antenna	
PC card	Integrated diversity antenna
LM card	Two MMCX antenna connectors
PCI card	RP-TNC connector
Mini PCI card	Ultra-miniature SMT U.FL antenna connectors
PC-Cardbus card	Integrated patch antenna

**Table A-1 Technical Specifications for Cisco Aironet Wireless LAN Client Adapters (continued)**

<b>Power Specifications</b>	
Operational voltage	
PC, LM, and PCI card	5.0 V ( $\pm 0.25$ V)
Mini PCI card	3.0 to 3.6 V
PC-Cardbus card	3.3 V ( $\pm 0.33$ V)
Receive current steady state	
PC card and LM card	Typically 250 mA
PCI card	Typically 350 mA
Mini PCI card	Typically 330 mA
PC-Cardbus card	Typically 580 mA
Transmit current steady state	
340 series PC card and LM card	Typically 350 mA @ 15 dBm
340 series PCI card	Typically 450 mA @ 15 dBm
350 series PC card and LM card	Typically 450 mA @ 20 dBm
350 series PCI card	Typically 550 mA @ 20 dBm
350 series mini PCI card	Typically 570 mA @ 20 dBm
PC-Cardbus card	Typically 520 mA
Sleep mode steady state	
340 series PC card and LM card	Typically 15 mA
340 series PCI card	Typically 110 mA
350 series PC card, LM card, and mini PCI card	Typically 15 mA
350 series PCI card	Typically 115 mA
PC-Cardbus card	Typically 20 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>

**Table A-1 Technical Specifications for Cisco Aironet Wireless LAN Client Adapters (continued)**

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 EN 301.489-1 and EN-301.489-17
Radio approvals	FCC Part 15.247 (2.4-GHz client adapters) FCC Part 15.407 (5-GHz client adapters) Canada RSS-139-1 (2.4-GHz client adapters), RSS-210 Japan Telec 33B (2.4-GHz client adapters) Japan ARIB STD-T71 (5-GHz client adapters) EN 300.328 (2.4-GHz client adapters) EN 301.893 (5-GHz client adapters)
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](#)
- [Dipole 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 tändhattar eller i en explosiv miljö om inte enheten modifierats för att kunna användas i sådana sammanhang.**

# Dipole Antenna Installation Warning

**Warning**

In order to comply with FCC radio frequency (RF) exposure limits, dipole 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 dipoolantennes zich minstens 20 cm of meer van de lichamen van alle personen bevinden.

**Varoitus**

FCC:n antamien radiotaajuuksille altistumista koskevien rajoitusten mukaan dipoliantennien 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 dipôles 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 Dipolantennen 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 dipolo devono stare ad una distanza minima di 20 cm dal corpo di ogni persona.

**Advarsel**

I henhold til eksponeringsgrensene for radiofrekvenser (RF), skal dipole 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 dipolo 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 dipolo 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 dipolsantenner 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 pitkäaikaistenlähetys- 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-adaptorns 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.
-

■ Warning for Laptop Users



## Declarations of Conformity and Regulatory Information

---

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 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-6](#)

# Manufacturer's Federal Communication Commission Declaration of Conformity Statement



**Models:** AIR-PCM341, AIR-PCM342, AIR-LMC341, AIR-LMC342, AIR-PCI341, AIR-PCI342, AIR-PCM351, AIR-PCM352, AIR-LMC351, AIR-LMC352, AIR-PCI351, AIR-PCI352, AIR-PCM350-A-K9, AIR-PCM350-40-A-K9, AIR-LMC350-A-K9, AIR-LMC350-40-A-K9, AIR-PCI350-A-K9, AIR-PCI350-10-A-K9, AIR-MPI350-xx-A-K9 (where *xx* is the OEM code), AIR-CB20A-A-K9, AIR-CB20A-A-K9-4

**FCC Certification Number:** LDK102038 (AIR-PCM34x),  
 LDK102035 (AIR-LMC34x and AIR-PCI34x),  
 LDK102040 (AIR-xxx35x),  
 LDK102042 (AIR-MPI350),  
 LDK102044 (AIR-CB20A)

**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.



**Caution**

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

**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-ANT4941	Dipole	2.2
AIR-ANT5959	Omni-directional	2.0

**Note**

AIR-ANT3338 is approved for use only with LM cards.

# Department of Communications – Canada

## Canadian Compliance Statement

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

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

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

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

Cisco Aironet 11-Mbps 2.4-GHz client adapters are certified to the requirements of RSS-139-1 and RSS-210 for 2.4-GHz spread spectrum devices, and Cisco Aironet 54-Mbps 5-GHz client adapters are certified to the requirements of RSS-210 for 5-GHz devices. The use of these devices in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

## European Community, Switzerland, Norway, Iceland, and Liechtenstein

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

English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Deutsch:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Dansk:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Español:	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/EC.
Έλληνας:	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 related to this product can be found at the following URL:  
<http://www.cisconfax.com>.

## 2.4-GHz Client Adapters

For the 340 series, the following standards were applied:

- Radio: ETS 300.328
- EMC: ETS 300.826
- Safety: EN 60950

The following CE mark is affixed to the 340 series equipment:



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 (except for the 350 series mini PCI card, or AIR-MPI350):



The above CE mark is required as of April 8, 2000 but might change in the future.

The following CE mark is affixed to the 350 series mini PCI card (AIR-MPI350):

**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**

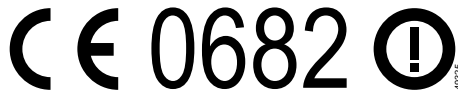
Combinations of power levels and antennas resulting in a radiated power level above 100 mW equivalent isotropic radiated power (EIRP) are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and other countries that have adopted the 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-4.

## 5-GHz Client Adapters

For the 5-GHz client adapters, the following standards were applied:

- Radio: EN 301.893
- EMC: EN 301.489-1, EN 301.489-17
- Safety: EN 60950

The following CE mark is affixed to the 5-GHz equipment:



## 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





## Channels, Power Levels, and Antenna Gains

---

This appendix lists the IEEE 802.11a and 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-4](#)

# Channels

## For IEEE 802.11a

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

**Table D-1 Channels for IEEE 802.11a**

Channel Identifier	Frequency	Regulatory Domains			
		Americas (-A)	Japan (-J)	Singapore (-S)	Taiwan (-T)
34	5170 MHz	-	X	-	-
36	5180 MHz	X	-	X	-
38	5190 MHz	-	X	-	-
40	5200 MHz	X	-	X	-
42	5210 MHz	-	X	-	-
44	5220 MHz	X	-	X	-
46	5230 MHz	-	X	-	-
48	5240 MHz	X	-	X	-
52	5260 MHz	X	-	-	X
56	5280 MHz	X	-	-	X
60	5300 MHz	X	-	-	X
64	5320 MHz	X	-	-	X
149	5745 MHz	-	-	-	-
153	5765 MHz	-	-	-	-
157	5785 MHz	-	-	-	-
161	5805 MHz	-	-	-	-



**Note**

All channel sets are restricted to indoor usage except the Americas (-A), which allows for indoor and outdoor use on channels 52 through 64 in the United States.



## For IEEE 802.11b

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

**Table D-2 Channels for IEEE 802.11b**

Channel Identifier	Frequency	Regulatory Domains				
		Americas (-A)	EMEA (-E)	Israel (-I)	China (-C)	Japan (-J)
1	2412 MHz	X	X	-	X	X
2	2417 MHz	X	X	-	X	X
3	2422 MHz	X	X	X	X	X
4	2427 MHz	X	X	X	X	X
5	2432 MHz	X	X	X	X	X
6	2437 MHz	X	X	X	X	X
7	2442 MHz	X	X	X	X	X
8	2447 MHz	X	X	X	X	X
9	2452 MHz	X	X	X	X	X
10	2457 MHz	X	X	-	X	X
11	2462 MHz	X	X	-	X	X
12	2467 MHz	-	X	-	-	X
13	2472 MHz	-	X	-	-	X
14	2484 MHz	-	-	-	-	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.



**Note**

France is included in the EMEA regulatory domain; however, only channels 10 through 13 can be used in France. Users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of France.

# Maximum Power Levels and Antenna Gains

## For IEEE 802.11a

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

**Table D-3** Maximum Power Levels Per Antenna Gain for IEEE 802.11a

Regulatory Domain	Maximum Power Level (mW) with 6-dBi Antenna Gain
Americas (-A) (160 mW EIRP maximum on channels 34-48, 800 mW EIRP maximum on channels 52-64)	20
Japan (-J) (10 mW/MHz EIRP maximum)	20
Singapore (-S) (100 mW EIRP maximum)	20
Taiwan (-T) (800 mW EIRP maximum)	20

## For IEEE 802.11b

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

**Table D-4** Maximum Power Levels Per Antenna Gain for IEEE 802.11b

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
Americas (-A) (4 watts EIRP maximum)	0	100
	2.2	100
	5.2	100
	6	100
	8.5	100
	12	100
	13.5	100
	21	20

**Table D-4** Maximum Power Levels Per Antenna Gain for IEEE 802.11b (continued)

Regulatory Domain	Antenna Gain (dBi)	Maximum Power Level (mW)
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
China (-C) (10 mW EIRP maximum)	0	5
	2.2	5
	5.2	n/a
	6	n/a
	8.5	n/a
	12	n/a
	13.5	n/a
	21	n/a
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 XP

---

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

The following topics are covered in this appendix:

- [Overview, page E-2](#)
- [Configuring the Client Adapter, page E-5](#)
- [Using Windows XP to Associate to an Access Point, page E-18](#)
- [Viewing the Current Status of Your Client Adapter, page E-19](#)

# Overview

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

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

**Note**

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

## Overview of Security Features

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

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

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

### Static WEP Keys

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

Static WEP keys are write-only and temporary; therefore, they cannot be read back from the client adapter and they are lost when power to the adapter is removed or the Windows device is rebooted. Although the keys are temporary, you do not need to re-enter them each time the client adapter is inserted or the Windows device is rebooted. This is because the keys are stored (in an encrypted format for security reasons) in the registry of the Windows device. When the driver loads and reads the client adapter’s registry parameters, it also finds the static WEP keys, unencrypts them, and stores them in volatile memory on the adapter.

### EAP (with Static or Dynamic WEP Keys)

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.

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

- **EAP-TLS**—This authentication type is enabled 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.

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



---

**Note** EAP-TLS requires the use of a certificate. Refer to Microsoft's documentation for information on downloading and installing the certificate.

---

- **EAP-MD5**—This authentication type is enabled through the operating system and uses static WEP to encrypt data. EAP-MD5 requires you to enter a separate EAP username and password (in addition to your standard Windows network login) in order to start the EAP authentication process and gain access to the network.



---

**Note** If you want to authenticate without encrypting the data that is transmitted over your network, you can use EAP-MD5 without static WEP.

---

RADIUS servers that support EAP-MD5 include Cisco Secure ACS version 3.0 or greater and Cisco Access Registrar version 1.8 or greater.

- **Protected EAP (or PEAP)**—PEAP authentication is designed to support One-Time Password (OTP), Windows NT or 2000 domain, and LDAP user databases over a wireless LAN. It is based on EAP-TLS authentication but uses a password or PIN instead of a client certificate for authentication. PEAP 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. If your network uses an OTP user database, PEAP requires you to enter either a hardware token password or a software token PIN to start the EAP authentication process and gain access to the network. If your network uses a Windows NT or 2000 domain user database or an LDAP user database (such as NDS), PEAP requires you to enter your username, password, and domain name in order to start the authentication process.

RADIUS servers that support PEAP authentication include Cisco Secure ACS version 3.1 or greater.



---

**Note** To use PEAP authentication, you must install the PEAP supplicant during ACU installation or Service Pack 1 for Windows XP. This Service Pack includes Microsoft's PEAP supplicant, which supports a Windows username and password only and does not interoperate with Cisco's PEAP supplicant. To use Cisco's PEAP supplicant, install ACU version 5.05 or greater after Service Pack 1 for Windows XP. Otherwise, it will be overwritten by Microsoft's PEAP supplicant.

---



---

**Note** PC-Cardbus cards do not support PEAP authentication.

---

- **EAP-SIM**—EAP-SIM authentication is designed for use in public wireless LANs with clients containing Gemplus SIM+ smartcards in PCSC-compliant smartcard readers. EAP-SIM 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-SIM requires you to enter a user verification code, or *PIN*, for communication with the SIM card. You can choose to have the PIN stored in your computer or to be prompted to enter it only after a reboot or prior to every authentication attempt.

RADIUS servers that support EAP-SIM include Cisco Access Registrar version 3.0 or greater.




---

**Note** To use EAP-SIM authentication, you must install the EAP-SIM supplicant during ACU installation.

---




---

**Note** PC-Cardbus cards do not support EAP-SIM authentication.

---

When you enable Require EAP on your access point and configure your client adapter for EAP-TLS, EAP-MD5, PEAP, or EAP-SIM using Windows XP, authentication to the network occurs in the following sequence:

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




---

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

---

2. Communicating through the access point, the client and RADIUS server complete the authentication process, with the password (EAP-MD5 and PEAP), certificate (EAP-TLS), or internal key stored on the SIM card and in the service provider's Authentication Center (EAP-SIM) being the shared secret for authentication. The password, certificate, or internal key is never transmitted during the process.




---

**Note** The authentication process is now complete for EAP-MD5. For EAP-TLS, PEAP, and EAP-SIM, the process continues.

---

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)

---



# Configuring the Client Adapter

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



**Note**

If you installed ACU but intend to use Windows XP to configure the client adapter, open ACU and make sure the **Use Another Application To Configure My Wireless Settings** option is selected on the Profile Manager screen.

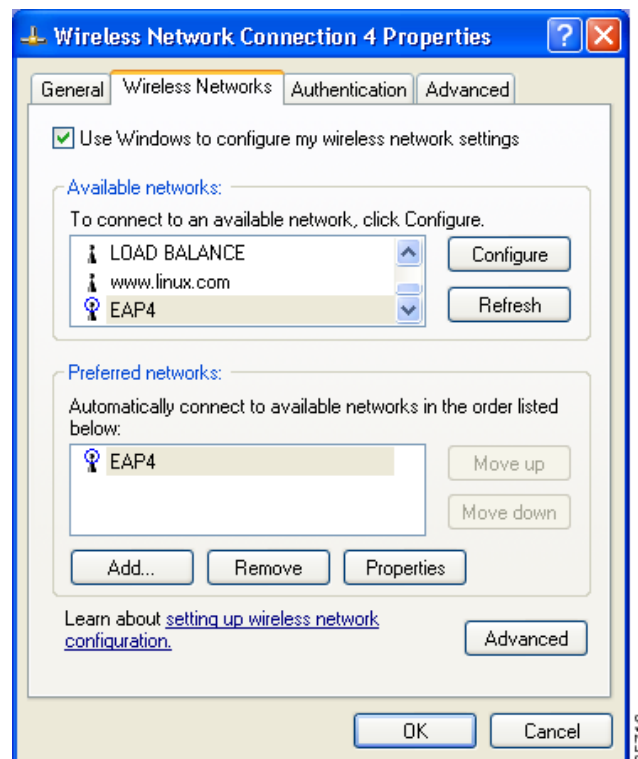


**Note**

These instructions assume you are using Windows XP's classic view rather than its category view.

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

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



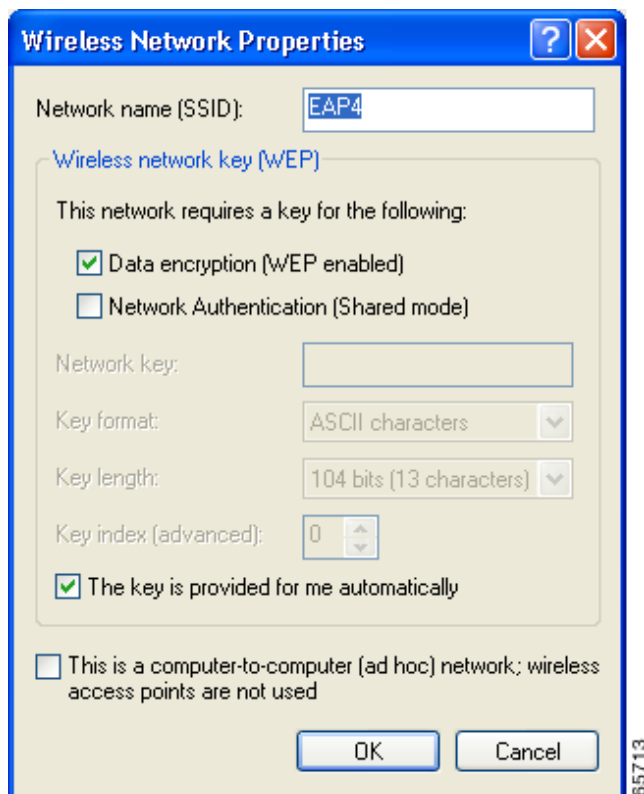
- Step 6** Make sure that the **Use Windows to configure my wireless network settings** check box is selected.
- Step 7** Select the SSID of the access point to which you want the client adapter to associate from the list of available networks and click **Configure**. If the SSID of the access point you want to use is not listed or you are planning to operate the client adapter in an *ad hoc network* (a computer-to-computer network without access points), click **Add**.



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

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

**Figure E-2** *Wireless Network Properties Screen*



- Step 8** Perform one of the following:
- If you selected an SSID from the list of available networks, make sure the SSID appears in the Network name (SSID) field.
  - If you clicked Add, enter the case-sensitive SSID of the access point to which you want the client adapter to associate or the name of the ad hoc network in the Network name (SSID) field.
- Step 9** Select the **Data encryption (WEP enabled)** check box if you are planning to use static or dynamic WEP.

- Step 10** Select the **Network Authentication (Shared mode)** check box if you want to use shared key, rather than open, authentication with the access point.

*Open authentication* allows your client adapter, regardless of its WEP settings, to authenticate and attempt to communicate with an access point.

*Shared key authentication* allows 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** If you are planning to use EAP-TLS authentication, do not select this check box. 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.

---

- Step 11** Follow the steps below to enter up to four WEP keys, if you are planning to use static WEP.



---

**Note** If you are planning to use EAP-TLS authentication, which uses dynamic WEP, go to [Step 12](#).

---

- a. Obtain the WEP key for the access point (in an infrastructure network) or other clients (in an ad hoc network) from your system administrator and enter it in the Network key field. In order to communicate, the client adapter must use the same WEP key as the access point or other clients.
- b. Select one of the following WEP key formats:
  - **ASCII characters**—Specifies that the WEP key will be entered in ASCII text, which includes alpha characters, numbers, and punctuation marks.
  - **Hexadecimal digits**—Specifies that the WEP key will be entered in hexadecimal characters, which include 0-9, A-F, and a-f.



---

**Note** ASCII text WEP keys are not supported on the Cisco Aironet 1200 Series Access Points, so you must select the Hexadecimal digits option if you are planning to use your client adapter with these access points.

---

- c. Select one of the following WEP key lengths:
  - **104 bits (13 characters/26 digits)**—You can select this option (or the 40 bits option) if your client adapter supports 128-bit WEP.
  - **40 bits (5 characters/10 digits)**—You must select this option if your client adapter supports only 40-bit WEP.
- d. In the Key index (advanced) field, select the number of the WEP key you are creating (**0, 1, 2, or 3**).



---

**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).

---

- e. Repeat the previous steps if you want to enter another WEP key.

- Step 12** Select the **The key is provided for me automatically** check box if you are planning to use EAP-TLS, which uses dynamic WEP keys.
- Step 13** Select the **This is a computer-to-computer (ad hoc mode) network; wireless access points are not used** check box if you are planning to operate the client adapter in an ad hoc network.
- Step 14** Click **OK** to save your settings and to add this SSID to the list of preferred networks (see [Figure E-1](#)). The client adapter automatically attempts to associate to the network(s) in the order in which they are listed.
- Step 15** Perform one of the following if you are planning to use EAP authentication:
- If you are planning to use EAP-TLS authentication, follow the instructions in the “[Enabling EAP-TLS Authentication](#)” section below.
  - If you are planning to use EAP-MD5 authentication, follow the instructions in the “[Enabling EAP-MD5 Authentication](#)” section on page E-11.
  - If you are planning to use PEAP authentication, follow the instructions in the “[Enabling PEAP Authentication](#)” section on page E-13.
  - If you are planning to use EAP-SIM authentication, follow the instructions in the “[Enabling EAP-SIM Authentication](#)” section on page E-16.
- 

## Enabling EAP-TLS Authentication

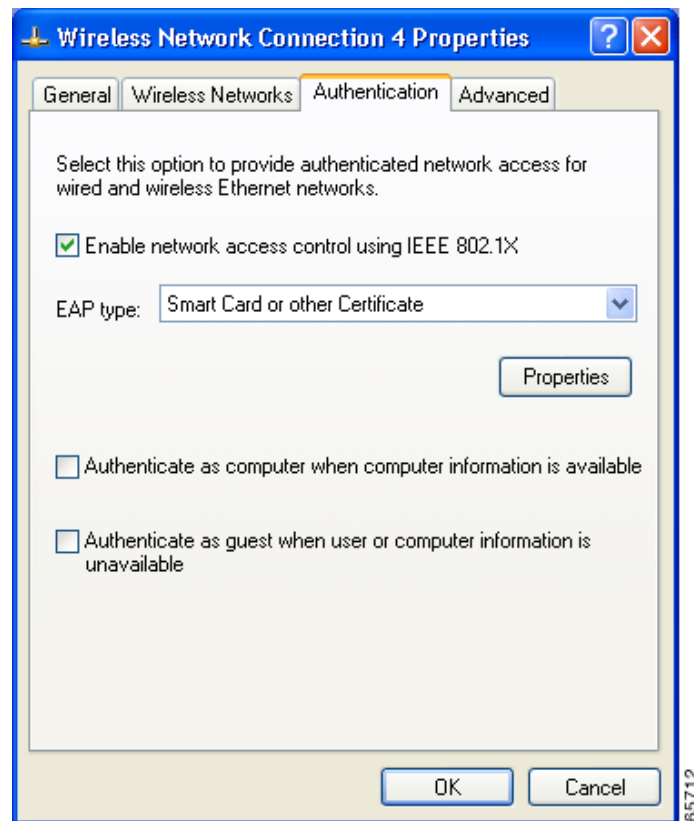
Follow the steps below to prepare the client adapter to use EAP-TLS authentication, provided you have completed the initial configuration.

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



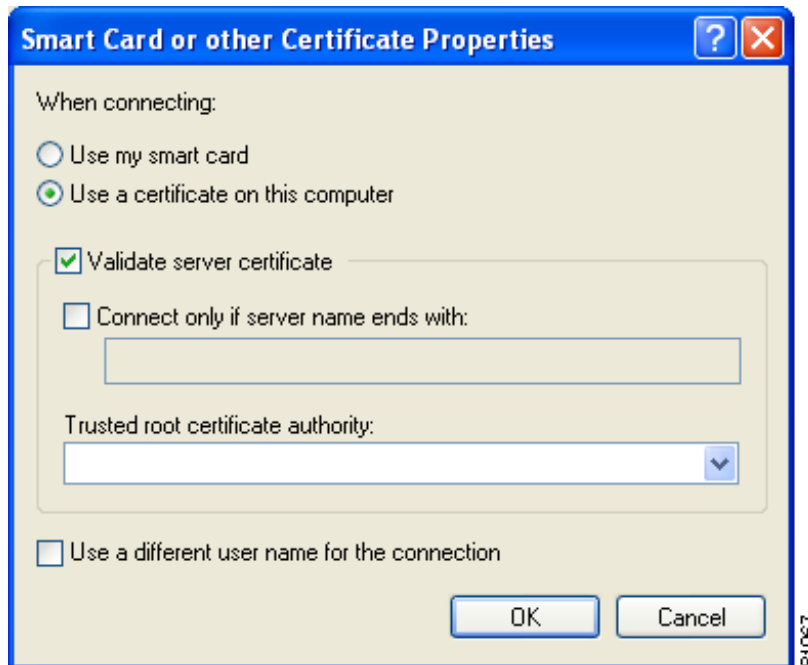
**Note** When Service Pack 1 for Windows XP is released, the Authentication tab may move from its current location. To access it, click the **Wireless Networks** tab, select the network that you are configuring in the Preferred network list, and click **Properties**.

---

**Figure E-3** Wireless Network Connection Properties Screen (Authentication Tab)

- Step 2** Select the **Enable network access control using IEEE 802.1X** check box.
- Step 3** For EAP type, select **Smart Card or other Certificate**.
- Step 4** Click **Properties**. The Smart Card or other Certificate Properties screen appears (see [Figure E-4](#)).

Figure E-4 Smart Card or other Certificate Properties Screen



- Step 5** Select the **Use a certificate on this computer** option.
- Step 6** Select the **Validate server certificate** check box.
- Step 7** Make sure that the name of the certificate authority from which the EAP-TLS certificate was downloaded appears in the Trusted root certificate authority field.



**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** Click **OK** to save your settings. The configuration is complete.
- Step 9** If a pop-up message appears above the system tray informing you that you need to accept a certificate to begin the EAP authentication process, click the message and follow the instructions provided to accept the certificate.



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

- Step 10** If a message appears indicating the root certification authority for the server's certificate, and it is the correct certification authority, click **OK** to accept the connection. Otherwise, click **Cancel**.

- Step 11** If a message appears indicating the server to which your client adapter is connected, and it is the correct server to connect to, click **OK** to accept the connection. Otherwise, click **Cancel**.

The client adapter should now EAP authenticate.



---

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

---

- Step 12** To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. Click **View** and **Refresh** to obtain the current status. If the client adapter is authenticated, the status reads, “Authentication succeeded.”
- 

## Enabling EAP-MD5 Authentication

Follow the steps below to prepare the client adapter to use EAP-MD5 authentication, provided you have completed the initial configuration.

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

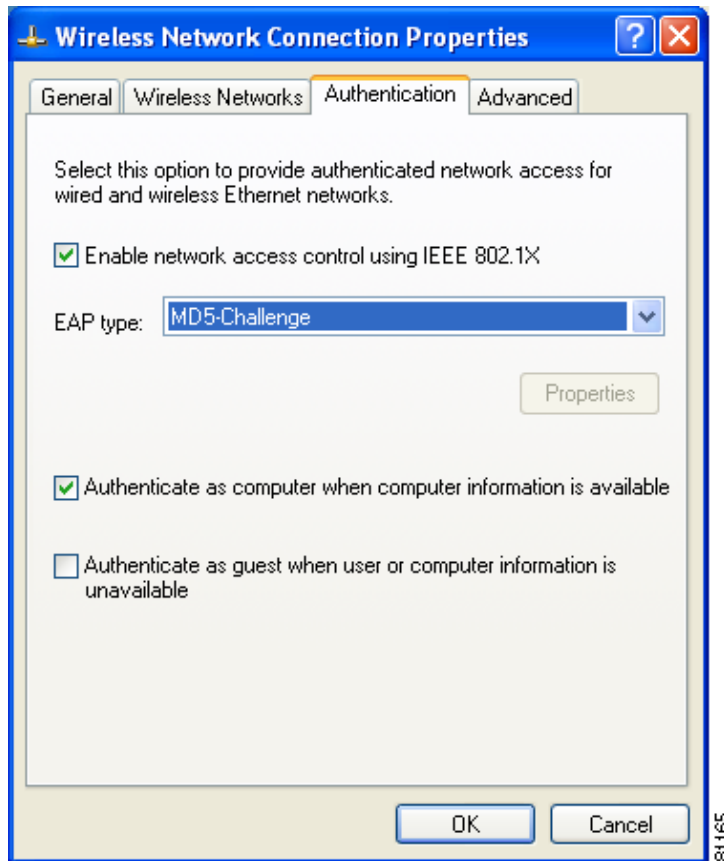


---

**Note** When Service Pack 1 for Windows XP is released, the Authentication tab may move from its current location. To access it, click the **Wireless Networks** tab, select the network that you are configuring in the Preferred network list, and click **Properties**.

---

Figure E-5 Wireless Network Connection Properties Screen (Authentication Tab)



- Step 2** Select the **Enable network access control using IEEE 802.1X** check box.
- Step 3** For EAP type, select **MD5-Challenge**.
- Step 4** Click **OK** to save your settings. The configuration is complete, and the client adapter should attempt to associate and EAP authenticate using MD5.
- Step 5** When a pop-up message appears above the system tray informing you that you need to enter your credentials to access the network, click the message. The Wireless Network Connection screen appears.
- Step 6** Enter your EAP-MD5 authentication username, password, and optional domain name (which are registered with the RADIUS server) and click **OK**. The client adapter should now EAP authenticate.



**Note** Whenever the computer reboots and you enter your Windows username and password, the pop-up message appears, and you must re-enter your EAP-MD5 credentials in order to EAP authenticate.

- Step 7** To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. Click **View** and **Refresh** to obtain the current status. If the client adapter is authenticated, the status reads, "Authentication succeeded."



## Enabling PEAP Authentication

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



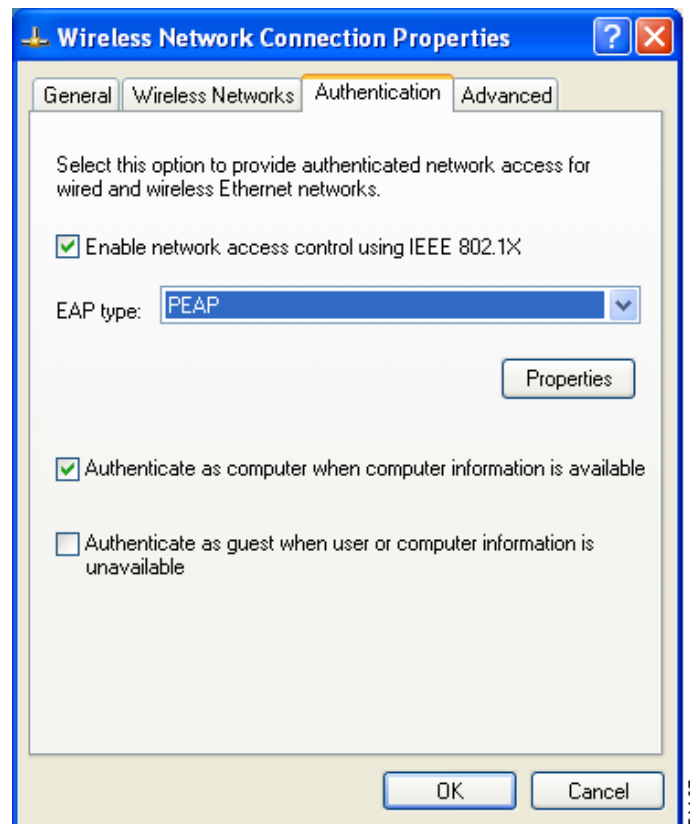
**Note** PC-Cardbus cards do not support PEAP authentication.

**Step 1** Click the **Authentication** tab on the Wireless Network Connection Properties screen. The following screen appears (see [Figure E-6](#)).



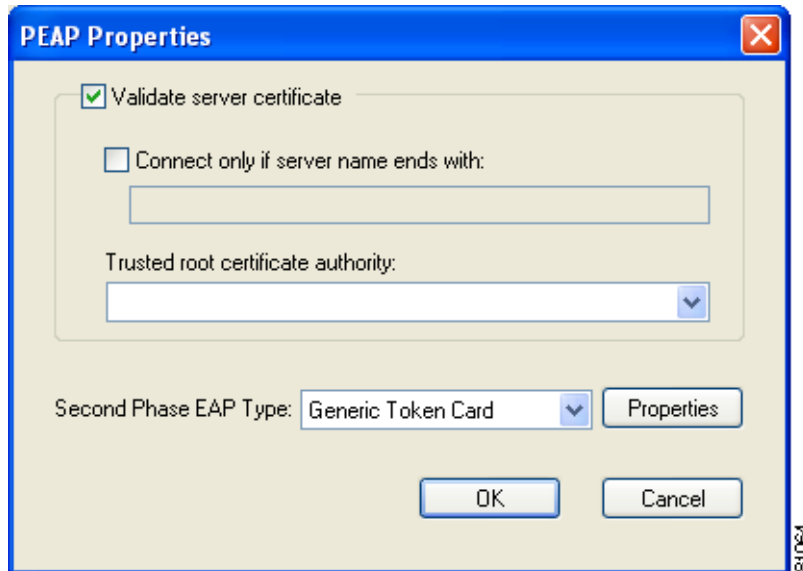
**Note** When Service Pack 1 for Windows XP is released, the Authentication tab may move from its current location. To access it, click the **Wireless Networks** tab, select the network that you are configuring in the Preferred network list, and click **Properties**.

**Figure E-6** Wireless Network Connection Properties Screen (Authentication Tab)



- Step 2** Select the **Enable network access control using IEEE 802.1X** check box.
- Step 3** For EAP type, select **PEAP**. Click **Properties**. The PEAP Properties screen appears (see [Figure E-7](#)).

**Figure E-7 PEAP Properties Screen**



- Step 4** Select the **Validate server certificate** check box if server certificate validation is required (recommended).
- Step 5** Select the **Connect only if server name ends with** 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.

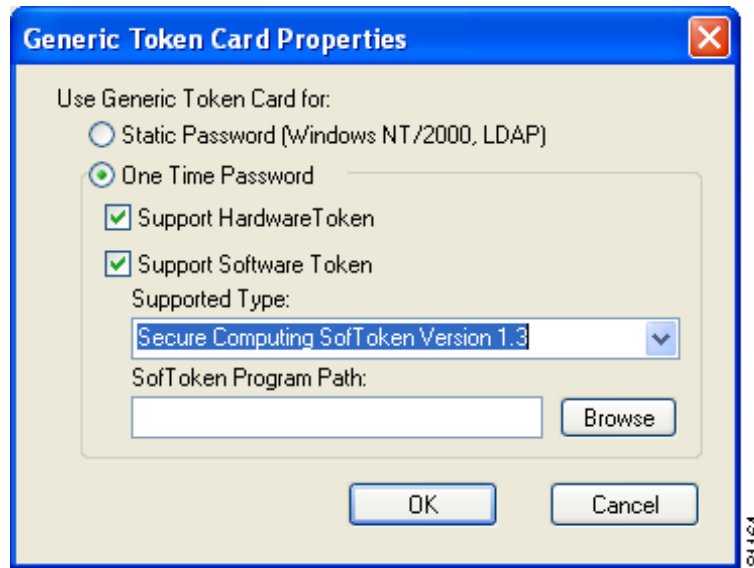
- Step 6** Make sure that the name of the certificate authority from which the server certificate was downloaded appears in the Trusted root certificate authority field.



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

- Step 7** Currently Generic Token Card is the only second phase EAP type available. Click **Properties**. The Generic Token Card Properties screen appears (see [Figure E-8](#)).

Figure E-8 Generic Token Card Properties Screen



**Step 8** Select either the **Static Password (Windows NT/2000, LDAP)** or the **One Time Password** option, depending on your user database.

**Step 9** Perform one of the following:

- If you selected the **Static Password (Windows NT/2000, LDAP)** option in [Step 8](#), go to [Step 10](#).
- If you selected the **One Time Password** option in [Step 8](#), select one or both of the following check boxes to specify the type of tokens that will be supported for one-time passwords:
  - **Support Hardware Token**—A hardware token device obtains the one-time password. You must use your hardware token device to obtain the one-time password and enter the password when prompted for your user credentials.
  - **Support Software Token**—The PEAP supplicant works with a software token program to retrieve the one-time password. You have to enter only the PIN, not the one-time password. If you select this check box, you must also select from the Supported Type drop-down box the software token software that is installed on the client (such as Secure Computing SofToken Version 1.3, Secure Computing SofToken II 2.0, or RSA SecurID Software Token v 2.5), and if Secure Computing SofToken Version 1.3 is selected, you must find the software program path using the Browse button.



**Note** The SofToken Program Path field is unavailable if a software token program other than Secure Computing SofToken Version 1.3 is selected.

**Step 10** Click **OK** to save your settings. The configuration is complete.

**Step 11** Refer to the [“Using PEAP”](#) section on [page 6-13](#) for instructions on authenticating using PEAP.

## Enabling EAP-SIM Authentication

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



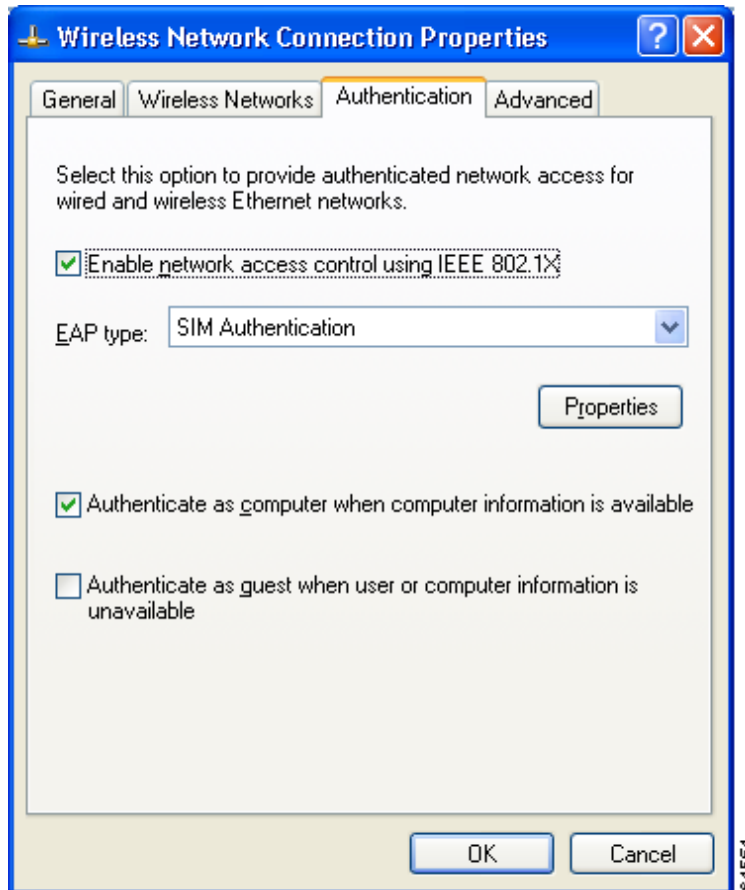
**Note** PC-Cardbus cards do not support EAP-SIM authentication.

**Step 1** Click the **Authentication** tab on the Wireless Network Connection Properties screen. The following screen appears (see [Figure E-9](#)).



**Note** When Service Pack 1 for Windows XP is released, the Authentication tab may move from its current location. To access it, click the **Wireless Networks** tab, select the network that you are configuring in the Preferred network list, and click **Properties**.

**Figure E-9** Wireless Network Connection Properties Screen (Authentication Tab)

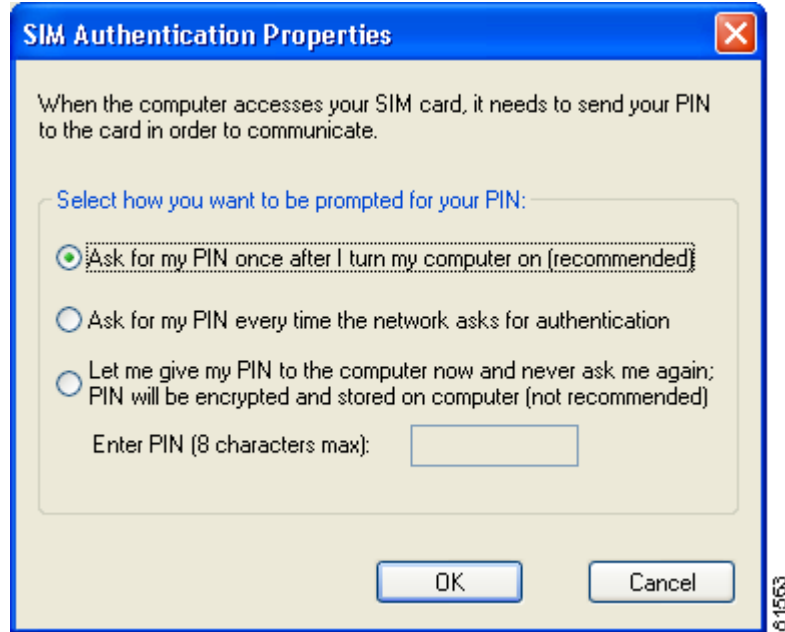


**Step 2** Select the **Enable network access control using IEEE 802.1X** check box.

**Step 3** For EAP type, select **SIM Authentication**.

**Step 4** Click **Properties**. The SIM Authentication Properties screen appears (see [Figure E-10](#)).

Figure E-10 SIM Authentication Properties Screen



**Step 5** To access any resources (data or commands) on the SIM, the EAP-SIM supplicant must provide a valid PIN to the SIM card, which must match the PIN stored on the SIM. Select one of the following options to specify how the EAP-SIM supplicant should handle the SIM card's PIN:

- **Ask for my PIN once after I turn my computer on (recommended)**—The software does not permanently store the PIN. It prompts you for the PIN once, on the first authentication of every session, where a *session* is defined as the time between power-up and shutdown or reboot.
- **Ask for my PIN every time the network asks for authentication**—The software never stores the PIN; it prompts you for the PIN every time an EAP-SIM authentication is performed. This option is not recommended if your client will be roaming between access points or if session timeouts are implemented (such as for accounting and security purposes).
- **Let me give my PIN to the computer now and never ask me again; PIN will be encrypted and stored on computer (not recommended)**—You need to enter the PIN only once, in the Enter PIN edit box below this option. The software stores the PIN in the registry and retrieves it from there when required. If you select this option, you must enter the PIN now. The PIN is validated when an authentication attempt is made.



**Note** This option is not recommended because it enables others to use the SIM without knowing the PIN.

**Step 6** Click **OK** to save your settings. The configuration is complete.

If you chose to store the PIN in the computer's registry, the EAP authentication process begins automatically, and the client adapter should EAP authenticate and use the saved PIN to access the SIM card.



---

**Note** If the stored PIN is wrong and therefore rejected by the SIM, the EAP-SIM supplicant temporarily changes the prompt mode to the default setting (Ask for my PIN once after I turn my computer on) in order to prevent the SIM from locking up. Unless changed manually, this setting stays in effect until your computer is powered off. Change your stored PIN on the SIM Authentication Properties screen.

---

If you chose to be prompted for the PIN after a power-up or reboot or at every authentication request, a pop-up message appears above the Windows system tray informing you that you need to enter your credentials to access the network. Click the message, enter your PIN, and click **OK**. The client adapter should now EAP authenticate.

**Step 7** To verify authentication, double-click **My Computer**, **Control Panel**, and **Network Connections**. The status appears to the right of your Wireless Network Connection. Click **View** and **Refresh** to obtain the current status. If the client adapter is authenticated, the status reads, "Authentication succeeded."



---

**Note** ACU and the Windows Network Connection icon on the Windows XP taskbar may indicate a connection status when authentication is still in the pending state or the authentication server fails to respond.

---

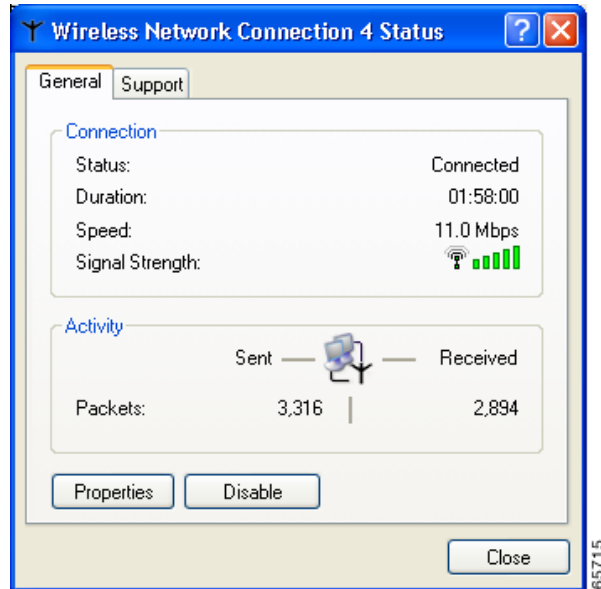
## Using Windows XP to Associate to an Access Point

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

## Viewing the Current Status of Your Client Adapter

To view the status of your client adapter, click the icon of the two connected computers in the Windows system tray. The Wireless Network Connection Status screen appears (see [Figure E-11](#)).

**Figure E-11** Wireless Network Connection Status Screen



■ Viewing the Current Status of Your Client Adapter





## Performing a Site Survey

---

This appendix explains how ACU's site survey tool can be used when conducting a site survey.

The following topics are covered in this appendix:

- [Overview, page F-2](#)
- [Specifying Signal Strength Units, page F-3](#)
- [Using Passive Mode, page F-3](#)
- [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-3](#) 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.

## Specifying Signal Strength Units

Follow the steps below to specify how signal strength units are displayed on the site survey screens.

- 
- Step 1** Double-click the **Aironet Client Utility (ACU)** icon on your desktop to open ACU.
- Step 2** Click the **Preferences** icon or select **Preferences** from the Options drop-down menu. The Aironet Client Utility Preferences screen appears.
- Step 3** Under Signal Strength Display Units, select one of the following options:
- **Percent**—Displays the signal strength as a percentage.
  - **dBm**—Displays the signal strength in decibels with respect to milliwatts.

**Note**

dBm can be selected only if your client adapter is using PCM/LMC/PCI card firmware version 3.92 or greater, mini PCI card firmware version 5.0 or greater, or PC-Cardbus card firmware version 4.99 or greater.

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

## Using Passive Mode

- 
- Step 1** Open ACU; then click the **Site Survey** icon or select **Site Survey** from the Commands drop-down menu. The Site Survey - Passive Mode screen appears, provided a client adapter is installed in the Windows device and is running.

[Figure F-1](#) shows the Site Survey - Passive Mode screen with the signal strength values displayed as percentages, and [Figure F-2](#) shows the top of the same screen with the signal strength values displayed in dBm.

**Note**

The name of the current profile appears in parentheses at the top of the screen.

Figure F-1 Site Survey - Passive Mode Screen (with Signal Strength as a Percentage)

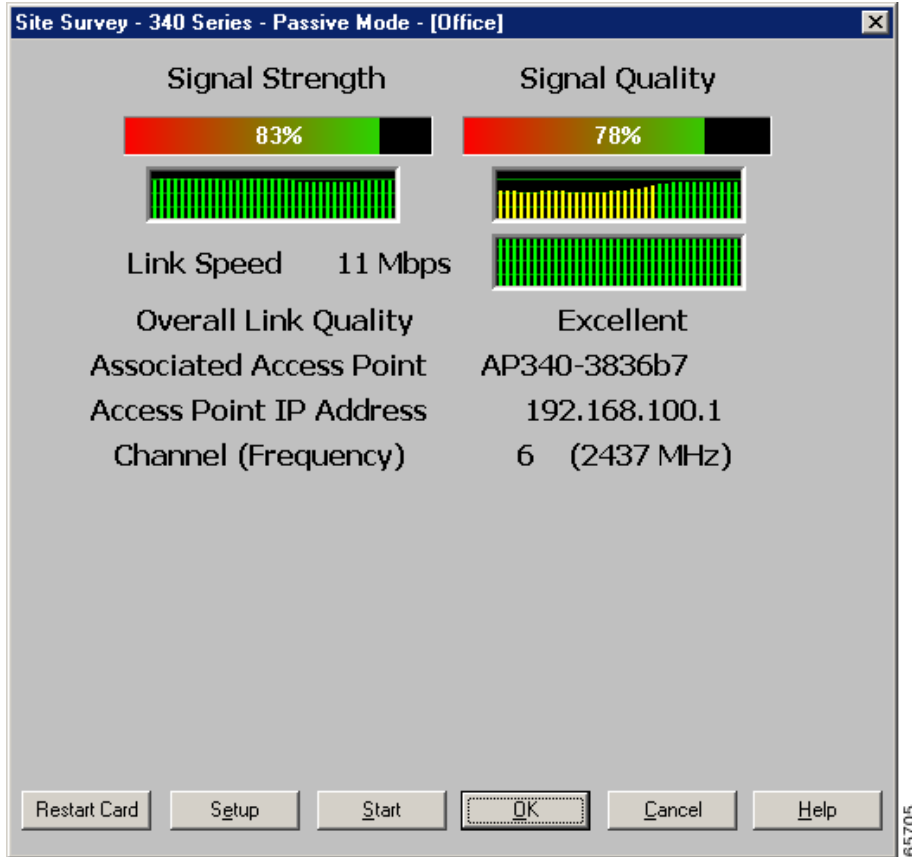


Figure F-2 Top of Site Survey - Passive Mode Screen (with Signal Strength in dBm)

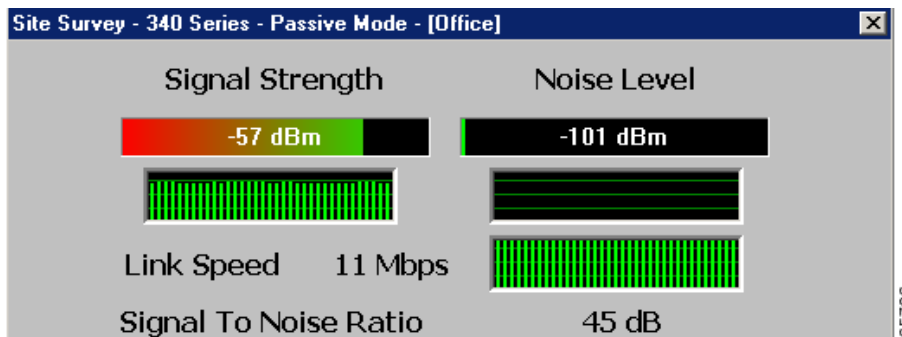


Table F-1 interprets the information that is displayed on the Site Survey - Passive Mode screen.

**Table F-1 Site Survey Passive Mode Statistics**

<b>Statistic</b>	<b>Description</b>
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 (2.4-GHz client adapters)	<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 for 2.4-GHz client adapters and only if you selected signal strength to be displayed as a percentage. See the <a href="#">“Specifying Signal Strength Units” section on page F-3</a> for information.</p>
Noise Level (2.4-GHz client adapters)	<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 for 2.4-GHz client adapters and only if you selected signal strength to be displayed in dBm. See the <a href="#">“Specifying Signal Strength Units” section on page F-3</a> for information.</p>
Beacons Received (5-GHz client adapters)	<p>The percentage of beacon packets received versus those expected to be received. The higher the value and the more green the bar graph is, the clearer the signal.</p> <p><b>Example:</b> The access point sends out 10 beacons per second, so you would expect the client adapter to receive 50 beacon packets in 5 seconds. If it receives only 40 packets, the percentage of beacons received would be 80%.</p> <p><b>Range:</b> 0 to 100%</p> <p><b>Note</b> This setting appears only for 5-GHz client adapters.</p>

**Table F-1 Site Survey Passive Mode Statistics (continued)**

Statistic	Description
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>The Link Speed histogram provides a visual interpretation of the current rate at which your client adapter is transmitting packets. Differences in link speed are indicated by the following colors: green (fastest), yellow (middle of the range), and red (slowest).</p> <p><b>Value:</b> 1, 2, 5.5, or 11 Mbps (2.4-GHz client adapters); 6, 9, 12, 18, 24, 36, 48, or 54 Mbps (5-GHz client adapters)</p>
Overall Link 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 for 2.4-GHz client adapters (but only if you selected signal strength to be displayed as a percentage) and for 5-GHz client adapters. See the <a href="#">“Specifying Signal Strength Units”</a> section on page F-3 for information.</p>
Signal To Noise Ratio (2.4-GHz client adapters)	<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 for 2.4-GHz client adapters and only if you selected signal strength to be displayed in dBm. See the <a href="#">“Specifying Signal Strength Units”</a> section on page F-3 for information.</p>
Associated Access Point	<p>The access point to which your client adapter is associated. It is shown only if the access point was configured with a name and your client adapter is in infrastructure mode.</p>
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 access point was configured with an IP address and your client adapter is in infrastructure mode.</p>
Channel (Frequency)	<p>The frequency that your client adapter is currently using as the channel for communications.</p> <p><b>Value:</b> Dependent on client adapter radio and regulatory domain</p>

**Step 2** If you want to activate the site survey active mode, go to the [“Using Active Mode”](#) section on page F-7. Otherwise, click **OK** or **Cancel** to exit the site survey application.

## Using Active Mode

Follow the steps below 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 Mode screen (see [Figure F-1](#)), click the **Setup** button. The Site Survey Active Mode Setup screen appears (see [Figure F-3](#)).

**Figure F-3 Site Survey Active Mode Setup Screen**

[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 are 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>						
Continuous Link Test	<p>Selecting this check box causes the test to run until you click <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> Deselected</p>						
Destination Is Another Cisco/Aironet Device	<p>Selecting 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 screen.</p> <p>If the device specified in the Destination MAC Address field is not a Cisco Aironet device, do not select 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> Selected</p>						
Number of Packets	<p>The number of packets that are sent during the test.</p> <p><b>Range:</b> 1 to 999</p> <p><b>Default:</b> 100</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>						
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 border="1"> <thead> <tr> <th>Retry Value</th> <th>Description</th> </tr> </thead> <tbody> <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 for 2.4-GHz client adapters; 32 for 5-GHz client adapters) will be used.</td> </tr> </tbody> </table>	Retry Value	Description	None	No retries will occur.	Default Retries	The firmware's default value for retries (16 for 2.4-GHz client adapters; 32 for 5-GHz client adapters) will be used.
Retry Value	Description						
None	No retries will occur.						
Default Retries	The firmware's default value for retries (16 for 2.4-GHz client adapters; 32 for 5-GHz client adapters) will be used.						



**Table F-2 Site Survey Active Mode Parameters (continued)**

Parameter	Description						
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 (2.4-GHz client adapters); 6, 9, 12, 18, 24, 36, 48, or 54 Mbps (5-GHz client adapters)</p> <p><b>Default:</b> 11 Mbps (2.4-GHz client adapters); 54 Mbps (5-GHz client adapters)</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> 50 ms</p>						
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>						
Packet Tx Type	<p>The packet type that is transmitted during the test.</p> <p><b>Default:</b> Unicast</p> <table border="1"> <thead> <tr> <th>Packet Type</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </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, click **OK** to save the settings. The Site Survey - Passive Mode screen appears (see [Figure F-1](#)).
- Step 3** Click the **Start** button to run the site survey test. The Site Survey - Active Mode screen appears. [Figure F-4](#) shows the Site Survey - Active Mode screen with the signal strength values displayed as percentages, and [Figure F-5](#) shows the top of the same screen with the signal strength values displayed in dBm.

Figure F-4 Site Survey - Active Mode Screen (with Signal Strength as a Percentage)

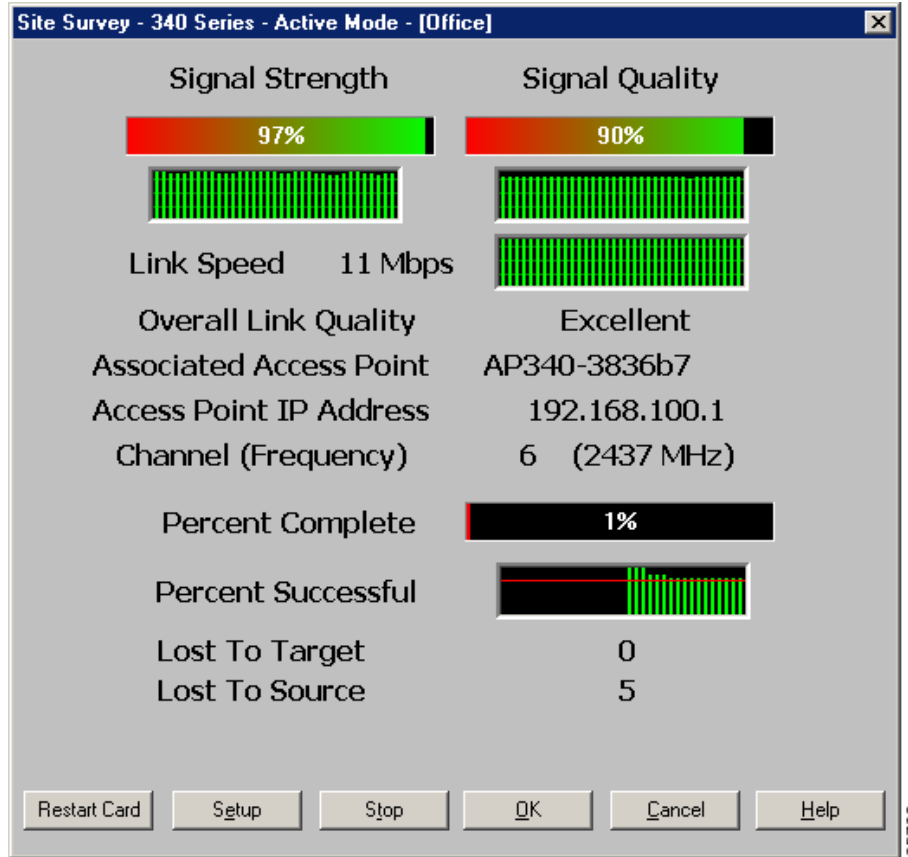


Figure F-5 Top of Site Survey - Active Mode Screen (with Signal Strength in dBm)

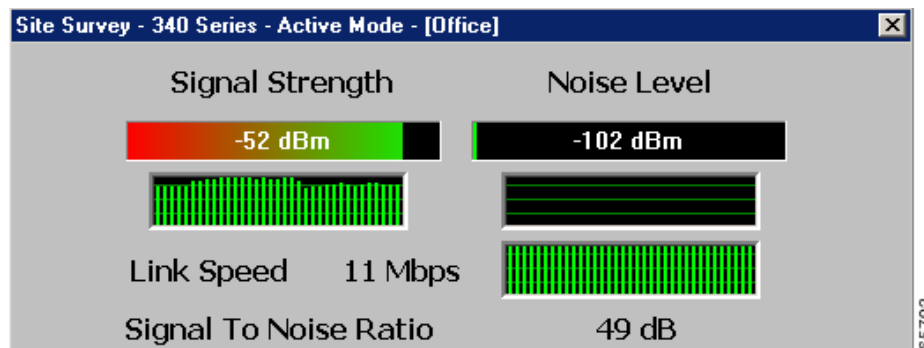


Table F-3 interprets the information that is displayed on the Site Survey - Active Mode screen while the site survey test is running.

**Table F-3 Site Survey Active Mode Statistics**

<b>Statistic</b>	<b>Description</b>
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 (2.4-GHz client adapters)	<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 for 2.4-GHz client adapters and only if you selected signal strength to be displayed as a percentage. See the <a href="#">“Specifying Signal Strength Units” section on page F-3</a> for information.</p>
Noise Level (2.4-GHz client adapters)	<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 for 2.4-GHz client adapters and only if you selected signal strength to be displayed in dBm. See the <a href="#">“Specifying Signal Strength Units” section on page F-3</a> for information.</p>
Beacons Received (5-GHz client adapters)	<p>The percentage of beacon packets received versus those expected to be received. The higher the value and the more green the bar graph is, the clearer the signal.</p> <p><b>Example:</b> The access point sends out 10 beacons per second, so you would expect the client adapter to receive 50 beacon packets in 5 seconds. If it receives only 40 packets, the percentage of beacons received would be 80%.</p> <p><b>Range:</b> 0 to 100%</p> <p><b>Note</b> This setting appears only for 5-GHz client adapters.</p>

**Table F-3 Site Survey Active Mode Statistics (continued)**

Statistic	Description
Link Speed	<p>The rate at which your client adapter is transmitting packets to or from its associated access point.</p> <p>The Link Speed histogram provides a visual interpretation of the current rate at which your client adapter is transmitting packets. Differences in link speed are indicated by the following colors: green (fastest), yellow (middle of the range), and red (slowest).</p> <p><b>Value:</b> 1, 2, 5.5, or 11 Mbps (2.4-GHz client adapters); 6, 9, 12, 18, 24, 36, 48, or 54 Mbps (5-GHz client adapters)</p>
Overall Link 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 for 2.4-GHz client adapters (but only if you selected signal strength to be displayed as a percentage) and for 5-GHz client adapters. See the <a href="#">"Specifying Signal Strength Units"</a> section on page F-3 for information.</p>
Signal To Noise Ratio (2.4-GHz client adapters)	<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 for 2.4-GHz client adapters and only if you selected signal strength to be displayed in dBm. See the <a href="#">"Specifying Signal Strength Units"</a> section on page F-3 for information.</p>
Associated Access Point	<p>The access point to which your client adapter is associated. It is shown only if the access point was configured with a name and the client adapter is in infrastructure mode.</p>
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 access point was configured with an IP address and the client adapter is in infrastructure mode.</p>
Channel (Frequency)	<p>The frequency that your client adapter is currently using as the channel for communications.</p> <p><b>Value:</b> Dependent on client adapter radio and regulatory domain</p>
Percent Complete	<p>The percentage of packets that have been transmitted based on the number specified in the Number of Packets field.</p>

**Table F-3 Site Survey Active Mode Statistics (continued)**

Statistic	Description
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.

- Step 4** When you click the **Stop** button or when the Percent Complete reaches 100%, the active mode changes back to the passive mode.
- Step 5** Click **OK** or **Cancel** to exit the site survey application.

## 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.



### Note

Restarting the client adapter may cause you to lose your wireless network connection.

Follow the steps below to attempt to force the client adapter to disassociate from its current access point and reassociate to another during a site survey.

- Step 1** Click the **Restart Card** button on the bottom of the Site Survey screen.
- Step 2** When prompted to confirm your decision, click **Yes**. The driver stops the client adapter's radio, writes the configuration (although no parameter settings have been changed), and restarts the radio.





## 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.
- 802.11a** The IEEE standard that governs the deployment of 5-GHz OFDM systems. It specifies the implementation of the physical layer for wireless UNII bands (see [UNII](#), [UNII 1](#), and [UNII 2](#)) and provides four channels per 100 MHz of bandwidth.
- 802.11b** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps 2.4-GHz wireless LANs.

---

### A

- Access Point** A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.
- Ad Hoc Network** A wireless network composed of stations without access points.
- 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 or EAP-TLS 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>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>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>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.
<b>Full Duplex</b>	A means of communication whereby each node receives and transmits simultaneously (two-way). See also <a href="#">Half Duplex</a> .

---

**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>Half Duplex</b>	A means of communication whereby each node receives and transmits in turn (one-way). See also <a href="#">Full Duplex</a> .
<b>Hexadecimal</b>	A set of characters consisting of ten numbers and six letters (0-9, A-F, and a-f).

---

**I**

<b>IEEE</b>	Institute of Electrical and Electronics Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.
<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**

**LEAP** LEAP, or *EAP-Cisco Wireless*, is the 802.1X authentication type that is available for use with operating systems that do not have EAP support. 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**

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

**MIC** Message integrity check. MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The client adapter's driver must support MIC functionality, and MIC must be enabled on the access point.

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

**Multicast Packets** Packets transmitted to multiple stations.

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

---

**O**

**OFDM** Orthogonal frequency division multiplexing. A multicarrier modulation method for broadband wireless communications.

**Overrun Packets** Packets that were discarded because the access point had a temporary overload of packets to handle.

---

**P**

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

---

**Q**

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

---

<b>R</b>	
<b>Radio Channel</b>	The frequency at which a radio operates.
<b>Range</b>	A linear measure of the distance that a transmitter can send a signal.
<b>Receiver Sensitivity</b>	A measurement of the weakest signal a receiver can receive and still correctly translate it into data.
<b>RF</b>	Radio frequency. A generic term for radio-based technology.
<b>Roaming</b>	A feature of some access points that allows users to move through a facility while maintaining an unbroken connection to the LAN.
<b>RP-TNC</b>	A connector type unique to Cisco Aironet radios and antennas. Part 15.203 of the FCC rules covering spread spectrum devices limits the types of antennas that may be used with transmission equipment. In compliance with this rule, Cisco Aironet, like all other wireless LAN providers, equips its radios and antennas with a unique connector to prevent attachment of non-approved antennas to radios.
<b>RTS Threshold</b>	The packet size at which an access point issues a request to send (RTS) before sending the packet.

---

<b>S</b>	
<b>Spread Spectrum</b>	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.
<b>SSID</b>	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.

---

<b>T</b>	
<b>TKIP</b>	Temporal Key Integrity Protocol. Also referred to as <i>WEP key hashing</i> . 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.
<b>Transmit Power</b>	The power level of radio transmission.

---

<b>U</b>	
<b>Unicast Packets</b>	Packets transmitted in point-to-point communication.
<b>UNII</b>	Unlicensed National Information Infrastructure. An FCC regulatory domain for 5-GHz wireless devices. UNII bands are 100 MHz wide and divided into four channels when using 802.11a OFDM modulation.

- UNII 1** A UNII band dedicated to in-building wireless LAN applications. UNII 1 is located at 5.15 to 5.25 GHz and allows for a maximum transmit power of 40 mW (or 16 dBm) with an antenna up to 6 dBi. UNII 1 regulations require a nonremovable, integrated antenna.
- UNII 2** A UNII band dedicated to in-building wireless LAN applications. UNII 2 is located at 5.25 to 5.35 GHz and allows for a maximum transmit power of 200 mW (or 23 dBm) with an antenna up to 6 dBi. UNII 2 regulations allow for an auxiliary, user-installable antenna.

---

## W

- WEP** Wired Equivalent Privacy. An optional security mechanism defined within the 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable.
- Workstation** A computing device with an installed client adapter.



---

## Numerics

### 802.1X

authentication types

in ACU [5-22](#)

in Windows XP [E-3](#)

defined [5-22, E-2](#)

---

## A

About Aironet Client Utility [8-23](#)

About icon [8-23](#)

access point

currently associated to [7-10](#)

in wireless infrastructure [1-9](#)

IP address

current [7-10](#)

in link test [7-19](#)

in site survey active mode [F-12](#)

in site survey passive mode [F-6](#)

MAC address

current [7-10](#)

in link test [7-21](#)

in site survey active mode [F-8](#)

specifying [5-16](#)

mismatches [7-14](#)

name

current [7-10](#)

in link test [7-21](#)

in site survey active mode [F-12](#)

in site survey passive mode [F-6](#)

problems

associating to [9-7](#)

authenticating to [9-7](#)

role in wireless network [1-7](#)

security settings [5-26 to 5-28](#)

Access Point Authentication parameter [5-29](#)

Ack packets

number received [7-16](#)

number transmitted [7-15](#)

ACU

See Aironet Client Utility (ACU)

ad hoc network

defined [E-6](#)

parameters [5-17 to 5-20](#)

selecting in ACU [5-6](#)

selecting in Windows XP [E-8](#)

wireless LAN configuration [1-8](#)

Advanced (Ad Hoc) screen [5-17](#)

Advanced (Infrastructure) screen [5-14](#)

advanced ad hoc parameters

described [5-2, 5-17](#)

setting [5-17 to 5-20](#)

advanced infrastructure parameters

described [5-2, 5-13](#)

setting [5-13 to 5-16](#)

aged packets [7-14, 7-16](#)

Aironet Client Monitor icon, using to turn radio on or off [8-29](#)

Aironet Client Utility (ACU)

About icon [8-23](#)

accessing help [9-25](#)

compatibility with driver and firmware [3-20](#)

described [1-5 to 1-7](#)

- determining latest version [3-2](#)
  - determining version of [8-23](#)
  - exiting [8-20](#)
  - feature comparison to Windows XP [3-19](#)
  - icon
    - adding to desktop [3-22](#)
    - deleting from desktop [8-28](#)
    - using to open ACU [3-24, 4-2, 8-19](#)
  - installation program settings, modifying [8-20 to 8-22](#)
  - installing [3-20 to 3-23, 9-3](#)
  - opening [4-2, 8-19](#)
  - overview [1-6](#)
  - Properties screens
    - overview [5-2](#)
    - parameters missing [9-8](#)
  - screens, buttons described [1-7](#)
  - selecting between two installed client adapters [3-24](#)
  - uninstalling [8-27](#)
  - upgrading [8-24 to 8-27](#)
  - verifying installation [3-23](#)
  - Aironet Client Utility Preferences screen [4-9, 7-3](#)
  - Aironet Client Utility screen [1-6](#)
  - Allow Association To Mixed Cells parameter [5-21](#)
  - Allow Non-Administrator Users to use ACU to modify profiles parameter
    - in ACU [4-9](#)
    - in ACU installation program [3-22, 8-22, 8-26](#)
  - Allow Saved LEAP User Name and Password parameter, in ACU installation program [3-21, 8-21, 8-25](#)
  - antenna
    - described [1-4](#)
    - gains [D-4 to D-5](#)
    - mode currently being used [7-8](#)
    - placement [F-2](#)
    - specifications [A-5](#)
  - Antenna Mode (Receive) parameter
    - ad hoc mode [5-18](#)
    - infrastructure mode [5-15](#)
  - Antenna Mode (Transmit) parameter
    - ad hoc mode [5-18](#)
    - infrastructure mode [5-15](#)
  - Apply button, function [1-7](#)
  - association
    - rejections [7-14](#)
    - timeouts [7-14](#)
  - audience of document [xii](#)
  - authentication
    - process [5-24, E-4](#)
    - rejections [7-14](#)
    - timeouts [7-14](#)
    - type, status of [7-8](#)
  - Automatically Prompt for LEAP User Name and Password option [5-33](#)
  - auto profile selection, using [4-5](#)
- 
- B**
- beacon packets
    - number received [7-13](#)
    - number transmitted [7-15](#)
  - beacon period, status of [7-10](#)
  - Beacon Period parameter [5-20](#)
  - beacons received
    - current [7-11, 7-22, F-5, F-11](#)
    - in site survey passive mode [F-5, F-6, F-11, F-12](#)
  - boot block firmware, current version of [7-6](#)
  - broadcast key rotation
    - described [5-26](#)
    - setting on client and access point [5-28](#)
  - broadcast packets
    - number received [7-13](#)
    - number transmitted [7-15](#)
  - broadcast SSIDs [5-4, E-6](#)
  - bytes
    - number received [7-13](#)
    - number transmitted [7-15](#)

**C**

## CAM

See Constantly Awake Mode (CAM)

Canadian compliance statement [C-3](#)

Cancel button, function [1-7](#)

Card and Socket Services [2-4](#)

carrier/correlation (Car/Cor) [5-12](#)

caution, defined [xiii](#)

Change Password screen - Windows XP [6-16](#)

Change PIN screen - Windows 2000 [6-17](#)

## channel

current [7-10](#)

determining if clear [5-12](#)

in site survey active mode [F-12](#)

in site survey passive mode [F-6](#)

Channel parameter [5-10](#)

channels, supported by regulatory domains [D-2, D-3](#)

channel set, for which client adapter is configured [7-9](#)

Cisco.com, obtaining technical assistance [xvi to xvii](#)

Clear Channel Assessment parameter [5-12](#)

client name [7-9](#)

Client Name parameter [5-4](#)

## client utility

See Aironet Client Utility (ACU)

clock, setting to display seconds [1-6](#)

collisions, multiple/single [7-15](#)

Commands drop-down menu [6-9](#)

## configuring client adapter

deciding between ACU and Windows XP [3-18](#)

in ACU [5-1 to 5-42](#)

in Windows XP [E-5 to E-12](#)

Constantly Awake Mode (CAM) [5-5](#)

Contents ACU menu option [9-25](#)

## Continuous Link Test parameter

in RF link test [7-19](#)

in site survey active mode [F-8](#)

conventions of document [xiii to xiv](#)

## CRC error

in packet [7-13](#)

in PLCP header [7-13](#)

Create ACU Icon on your Desktop parameter, in ACU installation program [3-22, 8-22, 8-26](#)

## CTS packets

number received [7-16](#)

number transmitted [7-15](#)

**D**

## data rate

for which client adapter is configured [7-9](#)

mismatches [7-14](#)

specifications [A-4](#)

when performing a site survey [F-2](#)

## Data Rate parameter

in RF network [5-8](#)

in site survey active mode [F-9](#)

## Data Retries parameter

in RF network [5-13](#)

in site survey active mode [F-8](#)

## dBm

signal strength units in site survey [F-3](#)

signal strength units on Status and Linktest screens [7-4](#)

## declarations of conformity

European community, Switzerland, Norway, Iceland, and Liechtenstein [C-4 to C-5](#)

FCC [C-2](#)

RF exposure [C-6](#)

Defaults button, function [1-7](#)

default values, displaying [1-7](#)

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 to 7-4](#)  
 using [7-4 to 7-22](#)

dipole antenna [1-4, B-3](#)

Display Seconds on Clock parameter [1-6](#)

diversity antenna [1-4](#)

diversity mode [5-15, 5-18](#)

document  
 audience [xii](#)  
 conventions [xiii to xiv](#)  
 organization [xii to xiii](#)  
 purpose [xii](#)

documentation  
 CD-ROM [xv](#)  
 feedback [xvi](#)  
 obtaining [xv to xvi](#)  
 ordering [xvi](#)

domain name  
 including in Windows login [5-33](#)  
 specifying for saved user name and password [5-33](#)

driver  
 compatibility with ACU and firmware [3-20](#)  
 current version of [7-6](#)  
 described [1-5](#)  
 determining latest version [3-2](#)  
 determining version of [8-8](#)  
 installation overview [3-4](#)  
 installing [3-3 to 3-19](#)  
 uninstalling [8-14 to 8-19](#)  
 upgrading [8-9 to 8-14](#)  
 verifying installation [3-23](#)

duplicate packets, number received [7-13](#)

dynamic WEP keys, overview [5-22 to 5-25, E-2 to E-4](#)

---

**E**

EAP authentication  
 overview [5-22 to 5-25, 6-2, E-2 to E-4](#)  
 using [6-1 to 6-19](#)

EAP-Cisco Wireless  
 See LEAP authentication

EAP-MD5 authentication  
 authenticating after profile selection/card  
 insertion/reboot/logoff [6-13](#)  
 described [5-23 to 5-25, E-3, E-4](#)  
 disabling [5-41](#)  
 enabling  
 in Windows XP [E-11 to E-12](#)  
 through ACU [5-34 to 5-37](#)  
 RADIUS servers supported [5-23, 5-24, E-3](#)  
 setting on client and access point [5-27](#)

EAP-SIM authentication  
 authenticating if the PIN is stored on the computer [6-19](#)  
 authenticating if you are prompted for the PIN [6-17](#)  
 described [5-24 to 5-25, E-4, E-4](#)  
 enabling  
 in Windows XP [E-16 to E-18](#)  
 through ACU [5-40 to 5-41](#)  
 error messages [9-20 to 9-24](#)  
 RADIUS servers supported [5-24, E-4](#)  
 setting on client and access point [5-28](#)

EAP SIM screen [6-18](#)

EAP-TLS authentication  
 authenticating after a reboot/logoff [6-12](#)  
 authenticating after profile selection/card  
 insertion [6-12](#)  
 described [5-23 to 5-25, E-3, E-4](#)  
 disabling [5-41](#)  
 enabling  
 in Windows XP [E-8 to E-11](#)  
 through ACU [5-34 to 5-37](#)  
 RADIUS servers supported [5-23, E-3](#)  
 setting on client and access point [5-27](#)



EIRP, maximum [1-4, D-4 to D-5](#)

energy detect (ED) [5-12](#)

error messages [9-9 to 9-24](#)

errors

MAC CRC [7-13](#)

overrun [7-13](#)

PLCP [7-13](#)

---

## F

Fast PSP [5-5](#)

FCC

declaration of conformity statement [C-2](#)

safety compliance statement [2-2](#)

firmware

802.1x draft standards [5-31, 8-5](#)

compatibility with ACU and driver [3-20](#)

current version of [7-6](#)

described [1-5](#)

determining version of [8-5](#)

upgrading [8-5 to 8-7](#)

forcing client adapter to reassociate [F-13](#)

fragmented packets [5-13](#)

Fragment Threshold parameter [5-13](#)

frequencies [D-2, D-3](#)

frequency [5-10](#)

currently being used [7-10](#)

in site survey active mode [F-12](#)

in site survey passive mode [F-6](#)

---

## G

Generic Token Card Properties screen - Windows  
XP [5-39, E-15](#)

---

## H

hardware components of client adapter [1-3 to 1-4](#)

Help

button, function [1-7](#)

drop-down menu [9-25](#)

icon [9-25](#)

help, ACU [9-25](#)

history of RF performance, displayed [7-4](#)

host-based EAP

described [5-23 to 5-25](#)

disabling [5-41](#)

enabling [5-34 to 5-41](#)

Host Based EAP option [5-34](#)

host devices [2-4](#)

---

## I

I/O range [9-4](#)

Include Profile in Auto Profile Selection parameter [4-3](#)

Include Windows Login Domain With User Name  
parameter [5-33](#)

infrastructure device, defined [1-3](#)

infrastructure network

parameters [5-13 to 5-16](#)

selecting in ACU [5-6](#)

wireless LAN configuration [1-9](#)

inserting client adapter [8-2 to 8-4](#)

interference [2-5](#)

interrupt request (IRQ) [9-4](#)

introduction to client adapters [1-2 to 1-3](#)

IP address

of access point in link test [7-19](#)

of access point in site survey active mode [F-12](#)

of access point in site survey passive mode [F-6](#)

of associated access point [7-10](#)

of client adapter [7-9](#)

**J**

Japan, guidelines for operating client adapters **C-6**

**L**

## LEAP authentication

authenticating after a reboot/logoff

with automatically prompted login **6-6**

with manually prompted login **6-9 to 6-10**

with saved username and password **6-11**

with Windows username and password **6-3 to 6-4**

authenticating after profile selection/card insertion

with automatically prompted login **6-5 to 6-6**

with manually prompted login **6-8**

with saved username and password **6-11**

with Windows username and password **6-3**

authenticating after your LEAP credentials expire

with automatically prompted login **6-7**

with manually prompted login **6-10**

with saved username and password **6-11**

with Windows username and password **6-4**

described **5-22 to 5-23, 5-24**

disabling **5-41**

enabling **5-31 to 5-34**

error messages **9-12 to 9-14**

RADIUS servers supported **5-22**

setting on client and access point **5-26**

stages of **6-2**

supported software **5-31**

LEAP Authentication Timeout Value parameter **5-33**

## LEAP login screen

appearing before Windows login screen **9-8**

displayed **6-5, 6-6, 6-8, 6-10**

LEAP option **5-31**

LEAP parameter, in ACU installation program **3-21, 8-21, 8-25**

LEAP Settings screen **5-32**

## LEDs

described **1-4**

interpreting **9-2 to 9-3**

## link quality

in link test **7-22**

in site survey active mode **F-12**

in site survey passive mode **F-6**

overall **7-11**

## link speed

currently being used **7-9**

in link test **7-21**

in site survey active mode **F-12**

in site survey passive mode **F-6**

## Link Status Meter

ACU menu option **7-16**

icon **7-16**

screen **7-17**

link status meter, viewing **7-16 to 7-17**

## Linktest

ACU menu option **7-18**

screen **7-19, 7-20**

linktest, statistics **7-21**

Link Test icon **7-18**

## LM card

antenna **1-4, 5-15, 5-18**

described **1-2**

Load Firmware icon **8-7**

Load New Firmware ACU menu option **8-7**

long radio headers, using **5-9**

**M**

## MAC address

of access point, specifying **5-16**

of access point in link test **7-21**

of access point in site survey active mode **F-8**

of associated access point **7-10**

of client adapter **7-9**

MAC CRC errors [7-13](#)

Manually Prompt for LEAP User Name and Password  
option [5-33](#)

Max Power Savings  
See Max PSP

Max PSP [5-5](#)

message integrity check (MIC)  
described [5-25, 7-7](#)  
setting on client and access point [5-28](#)  
statistics [7-14 to 7-15](#)  
status of [7-7](#)

microcellular network [1-9](#)

Microsoft hot fixes  
described [9-8](#)  
uninstalling [8-29](#)

mini PCI card  
antenna [1-4, 5-15, 5-18](#)  
described [1-2](#)  
losing association upon resuming from suspend  
mode [9-7](#)

multicast packets  
in site survey active mode [F-9](#)  
number received [7-13](#)  
number transmitted [7-15](#)

---

## N

network  
configurations [1-7 to 1-9](#)  
problems connecting to [9-7](#)  
security parameters  
described [5-2, 5-20](#)  
setting [5-20 to 5-42](#)  
type, current [7-10](#)

network login screen [6-7](#)

Network Security screen [5-20](#)

Network Security Type parameter [5-28, 5-31, 5-34, 5-41](#)

Network Type parameter [5-6](#)

noise level  
current [7-11](#)  
in link test [7-21](#)  
in site survey active mode [F-11](#)  
in site survey passive mode [F-5](#)

No Network Connection Unless User is Logged In  
parameter [5-33](#)

note, defined [xiii](#)

Number of Packets parameter  
in link test [7-19](#)  
in site survey active mode [F-8](#)

---

## O

OK button, function [1-7](#)

One Time Password screen - Windows XP [6-15](#)

open authentication [5-29, E-7](#)

Open window [8-7](#)

Options drop-down menu [1-6, 4-8, 7-2, F-3](#)

organization of document [xii to xiii](#)

overrun errors [7-13](#)

---

## P

package contents [2-3](#)

packets  
Ack [7-15](#)  
aged [7-14, 7-16](#)  
beacon [5-20, 7-10, 7-13, 7-15](#)  
broadcast [7-13, 7-15](#)  
CTS [7-15, 7-16](#)  
duplicate [7-13](#)  
fragmented [5-13](#)  
linktest statistics [7-21](#)  
multicast [7-13, 7-15, F-9](#)  
RTS [5-16, 5-19, 7-15](#)  
site survey active mode statistics [F-11 to F-13](#)  
site survey passive mode statistics [F-5 to F-6](#)  
statistics [7-13 to 7-16](#)

- unicast [7-13, 7-15](#)
- with MIC [7-14 to 7-15](#)
- Packet Size parameter [7-19, F-8](#)
- Packet Tx Type parameter [F-9](#)
- PC card
  - antenna [1-4, 5-15, 5-18](#)
  - described [1-2](#)
  - inserting [8-2 to 8-3](#)
  - removing [8-4](#)
- PC-Cardbus card
  - antenna [1-4](#)
  - described [1-2](#)
  - inserting [8-2 to 8-3](#)
  - removing [8-4](#)
- PCI card
  - antenna [1-4, 5-15, 5-18](#)
  - described [1-2](#)
  - inserting [8-3 to 8-4](#)
  - removing [8-4](#)
- PEAP authentication
  - authenticating after profile selection/card insertion/reboot/logoff [6-13 to 6-15](#)
  - authenticating after your password expires (Windows NT or 2000 domain databases) [6-16](#)
  - authenticating after your PIN expires (OTP databases) [6-16 to 6-17](#)
  - described [5-24 to 5-25, E-3, E-4](#)
  - enabling
    - in Windows XP [E-13 to E-15](#)
    - through ACU [5-38 to 5-39](#)
  - error messages [9-15 to 9-19](#)
  - RADIUS servers supported [5-24, E-3](#)
  - setting on client and access point [5-27](#)
- PEAP Properties screen - Windows XP [5-38, E-14](#)
- peer-to-peer network [1-8, 5-6](#)
- percent
  - signal strength units in site survey [F-3](#)
  - signal strength units on Status and Linktest screens [7-4](#)
- Percent Successful histogram, in site survey active mode [F-9, F-13](#)
- Percent Success Threshold parameter [F-9](#)
- Periodically Scan For A Better Access Point parameter [5-9](#)
- physical specifications [A-2](#)
- PLCP
  - CRC errors [7-13](#)
  - format errors [7-13](#)
  - length errors [7-13](#)
- power level
  - current [7-9](#)
  - maximum [D-4 to D-5](#)
- power levels, available [7-9](#)
- power save mode, currently being used [7-10](#)
- Power Save Mode parameter [5-5](#)
- power specifications [A-6](#)
- Preferences
  - ACU menu option [1-6, 4-8, 7-2, F-3](#)
  - icon [1-6, 4-8, 7-2, F-3](#)
- product model numbers [1-3](#)
- profile
  - current [7-7](#)
  - default [7-6](#)
- Profile Manager
  - ACU menu option [4-2](#)
  - icon [4-2](#)
  - screen [4-2, 4-6, 4-7, 4-8](#)
- profile manager
  - creating a new profile [4-3](#)
  - deleting a profile [4-7](#)
  - denying access to non-administrative users [4-8](#)
  - editing a profile [4-6](#)
  - exporting a profile [4-8](#)
  - importing a profile [4-7](#)
  - opening [4-2 to 4-3](#)
  - overview [4-2](#)
  - permitting non-administrator use [3-22](#)
  - renaming a profile [4-7](#)
  - selecting the active profile [4-4](#)
  - setting a profile to default values [4-6](#)

## Protected EAP

See PEAP authentication

purpose of document [xii](#)

---

**R**

## radio

described [1-3](#)

specifications [A-3 to A-5](#)

turning on or off [8-29](#)

Radio Off ACU menu option [8-29](#)

Radio On ACU menu option [8-29](#)

## RADIUS servers

additional information [5-25, E-4](#)

defined [5-22, E-2](#)

supported [5-22 to 5-24, E-3, E-4](#)

range [5-8, 5-11](#)

receive statistics [7-13 to 7-15](#)

## regulatory

domains [5-10, 7-9, D-2, D-3](#)

information [C-2 to C-7](#)

specifications [A-6](#)

related publications [xv](#)

removing client adapter [8-4](#)

Reset button [7-12, 7-15](#)

## resource conflicts, resolving

in Windows 2000 [9-5](#)

in Windows 95, 98, and Me [9-4 to 9-5](#)

in Windows NT [9-5](#)

in Windows XP [9-6 to 9-7](#)

## Restart Card

ACU menu option [8-28](#)

button, in site survey [F-13](#)

restarting client adapter [8-28, F-13](#)

## RF link test

prerequisites [7-18](#)

running [7-18 to 7-22](#)

stopping [7-22](#)

## RF network parameters

described [5-2, 5-6](#)

setting [5-6 to 5-13](#)

RF Network screen [5-7](#)

RF obstructions [2-5, F-3](#)

roaming [1-9](#)

## RTS packets

advanced ad hoc parameters [5-19](#)

advanced infrastructure parameters [5-16](#)

number retransmitted [7-16](#)

number transmitted [7-15](#)

## RTS Retry Limit parameter

ad hoc mode [5-19](#)

infrastructure mode [5-16](#)

## RTS Threshold parameter

ad hoc mode [5-19](#)

infrastructure mode [5-16](#)

---

**S**

## safety

information [2-2 to 2-3](#)

specifications [A-6](#)

## saved username and password

described [5-32](#)

entering [5-33](#)

Screen Update Timer parameter [7-4](#)

seamless roaming [1-9](#)

## security features

overview [5-21 to 5-26](#)

synchronizing [5-26 to 5-28](#)

Select A Wireless LAN Adapter Card screen [3-24](#)

sensitivity [A-4, F-2](#)

server-based authentication, status of [7-8](#)

Setup button, in site survey [F-7](#)

shared key authentication [5-29, E-7](#)

- short radio headers
  - status of [7-7](#)
  - using [5-9](#)
- Show History parameter [7-4](#)
- signal quality
  - current [7-11](#)
  - in link test [7-21](#)
  - in site survey active mode [F-11](#)
  - in site survey passive mode [F-5](#)
  - on Link Status Meter screen [7-17](#)
- signal strength
  - as a percentage [7-4, F-3](#)
  - current [7-10](#)
  - in dBm [7-4, F-3](#)
  - in link test [7-21](#)
  - in site survey active mode [F-11](#)
  - in site survey passive mode [F-5](#)
  - on Link Status Meter screen [7-17](#)
- Signal Strength Display Units parameter [7-4](#)
- signal to noise ratio
  - current [7-11](#)
  - in link test [7-22](#)
  - in site survey active mode [F-12](#)
  - in site survey passive mode [F-6](#)
- SIM Authentication Properties screen - Windows XP [5-40, E-17](#)
- site requirements
  - for client devices [2-5](#)
  - for infrastructure devices [2-5](#)
- Site Survey
  - Active Mode screen [F-10](#)
  - Active Mode Setup screen [F-7](#)
  - ACU menu option [F-3](#)
  - icon [F-3](#)
  - Passive Mode screen [F-4](#)
- site survey
  - active mode
    - overview [F-2](#)
    - setting parameters [F-8 to F-9](#)
    - starting [F-9](#)
    - statistics [F-11 to F-13](#)
    - using [F-7 to F-13](#)
  - exiting [F-6, F-13](#)
  - guidelines [F-2](#)
  - passive mode
    - overview [F-2](#)
    - statistics [F-5 to F-6](#)
    - using [F-3 to F-6](#)
  - specifying signal strength units [F-3](#)
- Smart Card or other Certificate Properties screen - Windows XP [5-37, E-10](#)
- software components of client adapter [1-5 to 1-7](#)
- specifications
  - physical [A-2](#)
  - power [A-6](#)
  - radio [A-3 to A-5](#)
  - regulatory compliance [A-6](#)
  - safety [A-6](#)
- Specified Access Point 1- 4 parameters [5-16](#)
- spread spectrum [1-3](#)
- SSID
  - current [7-10](#)
  - mismatches [7-13](#)
- SSID1 parameter [5-4](#)
- SSID2 parameter [5-4](#)
- SSID3 parameter [5-4](#)
- Start button
  - function [1-7](#)
  - in RF link test [7-20](#)
  - in site survey [F-9](#)
- Static Password screen - Windows XP [6-14](#)
- static WEP
  - disabling [5-30](#)
  - procedures [5-28 to 5-30](#)

- with open authentication, setting on client and access point [5-26](#)
- with shared key authentication, setting on client and access point [5-26](#)

static WEP keys

- entering [5-28 to 5-30](#)
- guidelines for entering
  - in ACU [5-29](#)
  - in Windows XP [E-7](#)
- overview [5-22 to 5-23, E-2 to E-3](#)
- overwriting [5-30](#)
- selecting transmit key [5-30](#)
- size of [5-29](#)

Statistics

- icon [7-12](#)
- screen [7-12](#)

statistics

- client adapter, viewing [7-12 to 7-16](#)
- link test [7-21](#)
- receive [7-13 to 7-15](#)
- site survey
  - active mode [F-11 to F-13](#)
  - passive mode [F-5 to F-6](#)
- transmit [7-15 to 7-16](#)

Status

- ACU menu option [7-4, 8-5, 8-8](#)
- icon [7-4, 8-5, 8-8](#)
- screen [7-5](#)

status of client adapter

- in link test [7-21](#)
- viewing
  - in ACU status bar [1-6](#)
  - in ACU Status screen [7-4 to 7-11](#)
  - in Windows XP [E-19](#)

Stop button

- function [1-7](#)
- in site survey active mode [F-13](#)

- system parameters
  - described [5-2, 5-3](#)
  - setting [5-3 to 5-6](#)
- System Parameters screen [5-3](#)
- system requirements [2-4](#)

---

## T

- technical assistance, obtaining [xvi to xviii](#)
- Technical Assistance Center, contacting [xvii to xviii](#)
- Temporal Key Integrity Protocol (TKIP)
  - described [5-26](#)
  - setting on client and access point [5-28](#)
- temporary username and password
  - automatically prompt for [5-33](#)
  - described [5-32](#)
  - manually prompt for [5-33](#)
  - selecting options [5-33](#)
  - using Windows credentials [5-33](#)
- throughput [5-5, 5-8, 5-9, 5-13](#)
- transmit key [5-30](#)
- Transmit Power parameter [5-11](#)
- transmit statistics [7-15 to 7-16](#)
- troubleshooting information [9-2 to 9-25](#)

---

## U

- unicast packets
  - in site survey active mode [F-9](#)
  - number received [7-13](#)
  - number transmitted [7-15](#)
- unpacking the client adapter [2-3](#)
- up time
  - statistic [7-15](#)
  - status of [7-10](#)
- Use Auto Profile Selection option [4-5](#)
- Use Saved User Name and Password option [5-32](#)
- Use Selected Profile option [4-5](#)

- Use Short Radio Headers parameter [5-9](#)
- Use Temporary User Name and Password option [5-32](#)
- Use Windows to configure my wireless network settings parameter - Windows XP [E-6](#)
- Use Windows User Name and Password option [5-33](#)

---

## W

- Wake Duration parameter [5-19](#)
- warning
  - defined [xiii to xiv](#)
  - dipole antenna [B-3](#)
  - explosive device proximity [2-3, B-2](#)
  - laptop users [2-3, B-4 to B-5](#)
- WEP
  - designation in product model numbers [1-3](#)
  - keys
    - additional security features [5-25 to 5-26](#)
    - defined [5-21, E-2](#)
    - size of [5-22, E-2](#)
    - types of [5-21, E-2](#)
  - parameter [5-28](#)
  - status of [7-8](#)
- WEP Key Entry Method parameter [5-29](#)
- WEP key hashing [5-26](#)
- Windows 2000
  - installing driver [3-13 to 3-14](#)
  - uninstalling 6.10 driver [8-16](#)
  - uninstalling driver other than 6.10 [8-18](#)
  - upgrading driver [8-11](#)
- Windows 95
  - determining version [3-4](#)
  - installing driver [3-4 to 3-8](#)
  - uninstalling 6.10 driver [8-14 to 8-15](#)
  - uninstalling driver other than 6.10 [8-17](#)
  - upgrading driver [8-9](#)
- Windows 98
  - installing driver [3-8 to 3-10](#)
  - uninstalling 6.10 driver [8-14 to 8-15](#)
  - uninstalling driver other than 6.10 [8-17](#)
  - upgrading driver [8-9](#)
- Windows login screen [6-3, 6-4](#)
- Windows Me
  - installing driver [3-15 to 3-16](#)
  - uninstalling driver [8-17](#)
  - upgrading driver [8-12](#)
- Windows NT
  - installing driver [3-11 to 3-12](#)
  - uninstalling 6.10 driver [8-15](#)
  - uninstalling driver other than 6.10 [8-18](#)
  - upgrading driver [8-10](#)
- Windows system tray, using Aironet Client Monitor icon [8-29](#)
- Windows XP
  - configuring client adapter through [E-5 to E-12](#)
  - enabling EAP-MD5 authentication [E-11 to E-12](#)
  - enabling EAP-SIM authentication [E-16 to E-18](#)
  - enabling EAP-TLS authentication [E-8 to E-11](#)
  - enabling PEAP authentication [E-13 to E-15](#)
  - feature comparison to ACU [3-19](#)
  - inability to use fast user switching [3-21](#)
  - installing driver [3-17 to 3-19](#)
  - making a configuration decision [3-18](#)
  - security features [E-2 to E-4](#)
  - uninstalling driver [8-19](#)
  - upgrading driver [8-13](#)
  - using to associate to an access point [E-18](#)
  - viewing status of client adapter [E-19](#)
- wireless infrastructure [1-9](#)
- Wireless Network Connection Properties screen (Authentication Tab) - Windows XP [5-36, E-9, E-12, E-13, E-16](#)
- Wireless Network Connection Properties screen (Wireless Networks Tab) - Windows XP [E-5](#)
- Wireless Network Connection Status screen - Windows XP [E-19](#)



Wireless Network Properties screen - Windows XP [E-6](#)

workstation

defined [1-3](#)

in wireless infrastructure [1-9](#)

World Mode parameter [5-9](#)

