



Installation and User Guide

Wireless LAN Client Adapter

Airgo Networks, Inc.
900 Arastradero Road
Palo Alto, CA 94304
P: 650-475-1900
F: 650-475-1708
www.airgonetworks.com

Part Number: 640-00069-00
Published: July 2004

Copyright © 2003 by Airgo Networks. All Rights Reserved.

No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Airgo Networks unless such copying is expressly permitted by U.S. copyright law.

Overview	1
Connecting the Wireless LAN Client Adapter	2
Installing the Wireless LAN Client Adapter Driver and Client Utility	4
Uninstalling the Client Utility and Drivers	8
Overview of Wireless Networking	11
Service Set Identifiers	12
Wireless Bands and Channels	12
Client Utility	12
Accessing the Client Utility	14
Navigating the User Interface	14
Configuration Overview	20
Scanning for Available Networks	20
Working with Profiles	21
Profile Window	23
Wireless Security	24

Preface

This guide explains how to install and configure the Wireless LAN Client Adapter, which provides PC laptop and desktop users with access to 802.11 access points. The guide is intended for business and consumer users who want to install and configure the Wireless LAN Client Adapter quickly and easily. It is also intended for users who are interested in advanced configuration and troubleshooting.

The Wireless LAN Client Adapter products include the following device options:

- PC Card adapter for use in laptop and notebook computers
- PCI adapter for use in desktop system PCI expansion slots
- Mini PCI adapter for use in laptop computer mini-PCI expansion slots

The Client Utility, a software tool designed to provide basic configuration options for the device, is shipped with each unit along with the device drivers.

Organization of this Guide

This guide consists of the following chapters:

- **Chapter 1, “Installation Overview,”** describes the features of the Wireless LAN Client Adapter and explains how to install it.
- **Chapter 2, “Introduction to the Client Utility,”** provides an overview of the Client Utility.
- **Chapter 3, “Configuration,”** describes the configuration settings of the Client Utility.
- **Appendix A, “Individual Driver and Client Utility Installation Procedures,”** explains how to install the driver and Client Utility as separate tasks.
- **Glossary** defines terms that apply to wireless and networking technology in general and Airgo products.

Conventions Used in this Guide

This guide uses the following conventions for instructions and information.

Notes, Cautions, and Warnings

Notes, cautions, and time-saving tips use the following conventions and symbols.



NOTE: Notes contain helpful suggestions or information that are important to the task at hand.



CAUTION: Caution indicates that there is a risk of equipment damage or loss of data when certain actions are performed.



WARNING: Warnings are intended to alert you to situations that could result in injury (such as exposure to electric current, for example).

Related Documentation

The following documentation related to the Airgo Networks wireless networking product line is available via CD-ROM and also on the company website, <http://www.airgonetworks.com>.

- **Access Point Installation and Configuration Guide** — Describes how to install and configure the Access Point.
- **NMS Pro Installation and Configuration Guide** — Explains how to install and use the enterprise network management application.
- **Command Line Interface (CLI) Reference Manual** — Provides a listing of all the commands available for the Access Point, usable through console access and command line interface; this manual is intended for advanced users and system administrators.

1 Installation Overview

This chapter explains how to install the Wireless LAN Client Adapter, adapter driver, and Client Utility. It includes the following topics:

- **Overview**
- **Connecting the Wireless LAN Client Adapter**
- **Installing the Wireless LAN Client Adapter Driver and Client Utility**
- **Uninstalling the Client Utility and Drivers**

Overview

The Wireless LAN Client Adapter provides the communication link between your laptop or desktop PC and other devices in a wireless network. The adapter operates in the 2.4 GHz radio frequency band and can communicate with any device that meets the IEEE 802.11b or 802.11g wireless network standards.

When used with Access Points as part of a wireless network installation, the Wireless LAN Client Adapter offers the following special features:

- Enhanced Data Rates
- Extended Range
- Multi Mode and Multi-band Operation
- Interference Handling

The Client Utility, shipped with each Wireless LAN Client Adapter, includes tools for setting the basic configuration.

Device Types

The Wireless LAN Client Adapter is currently offered in three device types:

- **PC Card** — Extended Type II PCMCIA CardBus (32-bit interface) for use in laptop and notebook computers
- **PCI Card** — PCI adapter for use in desktop computer expansion slots
- **Mini PCI** — Mini PCI adapter for use in laptop computer mini-PCI expansion slots

Shipping Package Contents

The Wireless LAN Client Adapter shipping package contains the following items:

- Wireless LAN Client Adapter PC or PCI Card
- CD containing the device driver and Client Utility

System Requirements

Your PC must meet the following minimum requirements:

- Windows XP or Windows 2000
- 96 MB memory

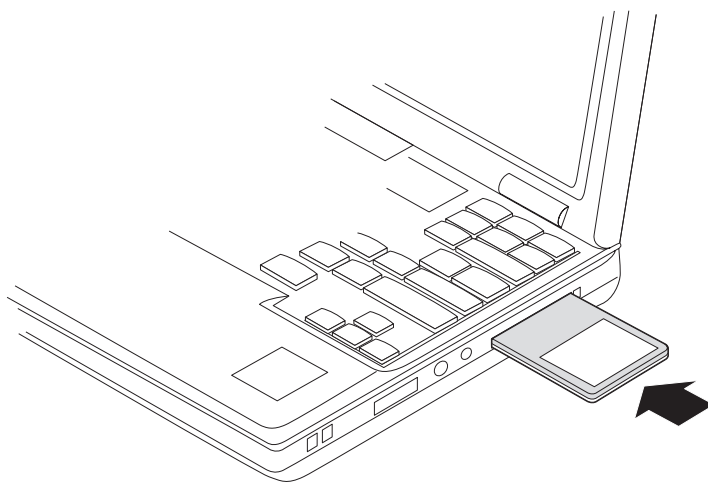
- CPU 1.0 GHz or greater
- At least 10 MB disk capacity available for the driver and Client Utility software.
- Type II or Type III cardbus slot for notebooks and laptops

Connecting the Wireless LAN Client Adapter

To install the PC card:

- With the computer powered on or off, slide the PC card firmly into an available CardBus slot (Figure 1).

Figure 1: PC Card Installation



LB48016

To safely remove the PC card while the computer is powered up:

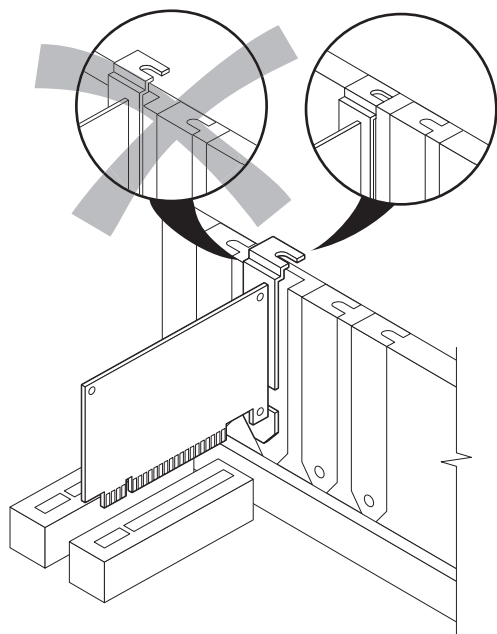
- 1 Right-click the system tray icon entitled **Safely Remove Hardware** or **Eject or Stop Hardware**.
The system prompts you to select the device to stop.
- 2 Select **Airgo Networks Wireless LAN NIC**, and click **Stop**.
- 3 Click **OK** when asked to confirm.
- 4 Press the CardBus eject button on the side of your computer to release the slot locking mechanism and slide the PC card out.

To install the PCI card adapter (Figure 2):

- 1 Power down your PC.
- 2 Remove the cover that provides access to the PCI expansion slot.
- 3 Insert the PCI card into an available PCI slot.
- 4 Replace the cover.
- 5 Attach the antenna to the external connector on the PCI card.

You are now ready to install the Wireless LAN Client Adapter driver software.

Figure 2: PCI Card Installation



Checking Adapter Activity

The LEDs on the PC card and PCI card indicate the state of current communications:

- **Solid green** — The adapter is associated (connected) to the network.
- **Slow blinking green** — The adapter is not associated to the network.
- **Fast blinking green** — The adapter is transmitting or receiving data.

Installing the Wireless LAN Client Adapter Driver and Client Utility

i **NOTE:** Before installing the Wireless LAN Client Adapter or any other wireless adapter, you must make sure that your system has the latest Microsoft patches to support wireless networking. You can find information and patches at

http://www.microsoft.com/hardware/broadbandnetworking/10_concept_wireless_security.msp.

Follow the steps in this section to install the software needed to support your Wireless LAN Client Adapter. The software includes:

- Wireless LAN Client Adapter driver
- Client Utility

Installation Steps

1 If you are using the PCI card, make sure that it is physically installed (page 3). If you are using the PC card, slide it into the CardBus slot on your computer.

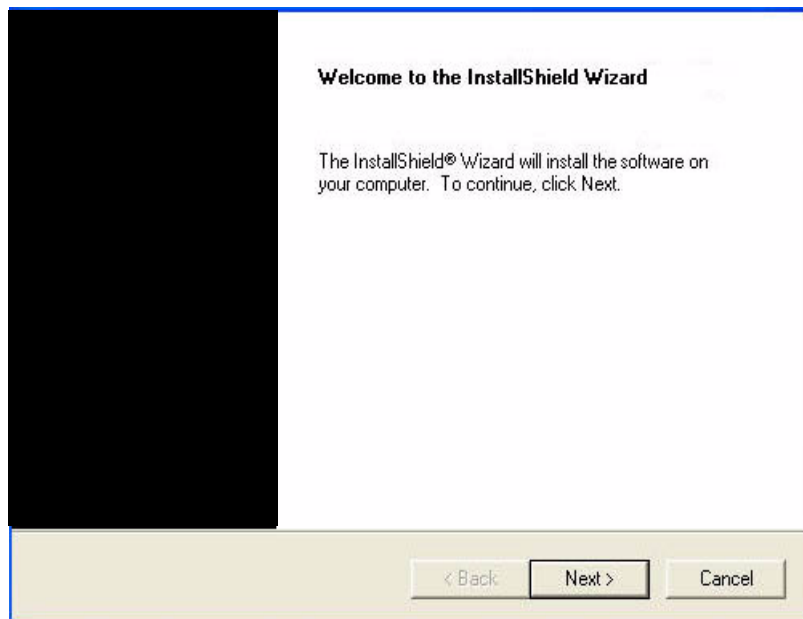
2 Power up your computer.

i **NOTE:** If the Microsoft Found New Hardware Wizard opens, click **Cancel** to close the wizard.

3 Insert the Wireless LAN Client Adapter distribution CD.
The CD menu opens.

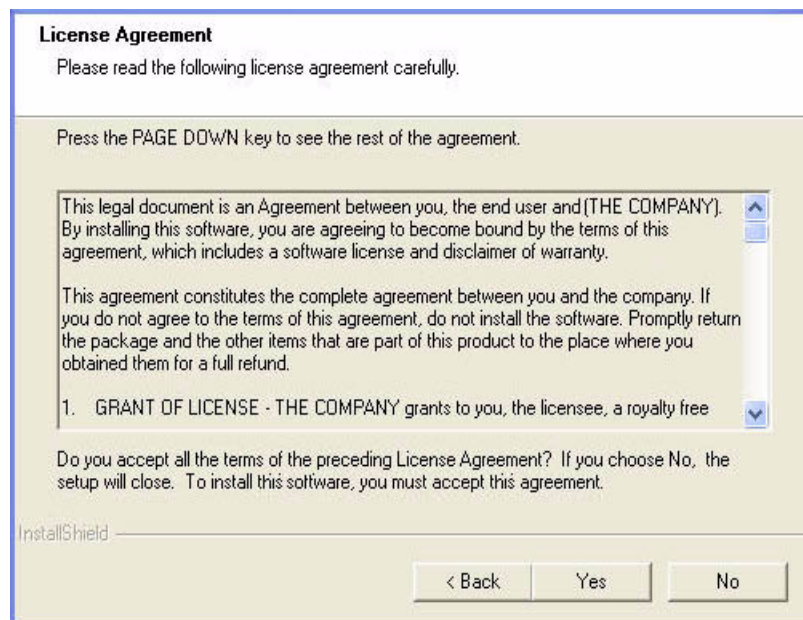


4 Currently, both the Network Card Drivers and Client Utility are selected and this selection cannot be modified. Click **Install Software** and the Installation Wizard opens.



5 Click Next.

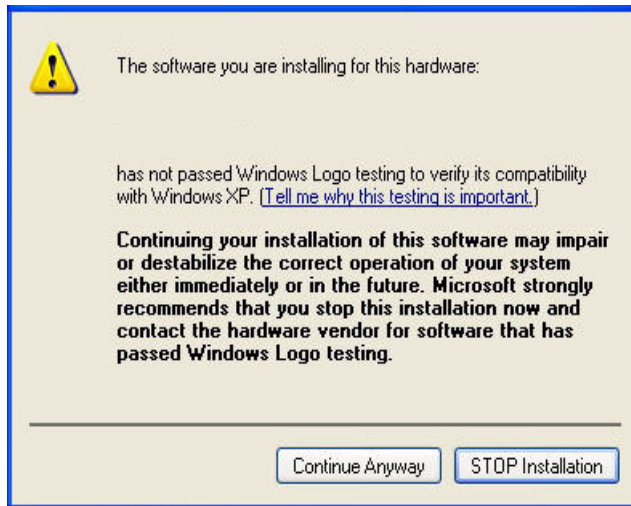
The License agreement window opens.



6 Review the license agreement, and then click Yes.

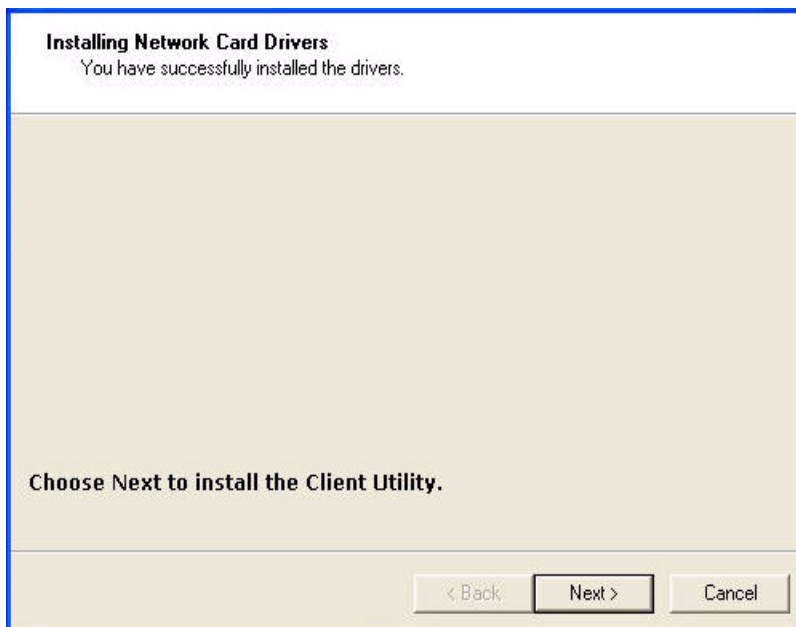
7 Click **OK**.¹

You may see a warning regarding Windows logo testing.



8 Click **Continue Anyway**.

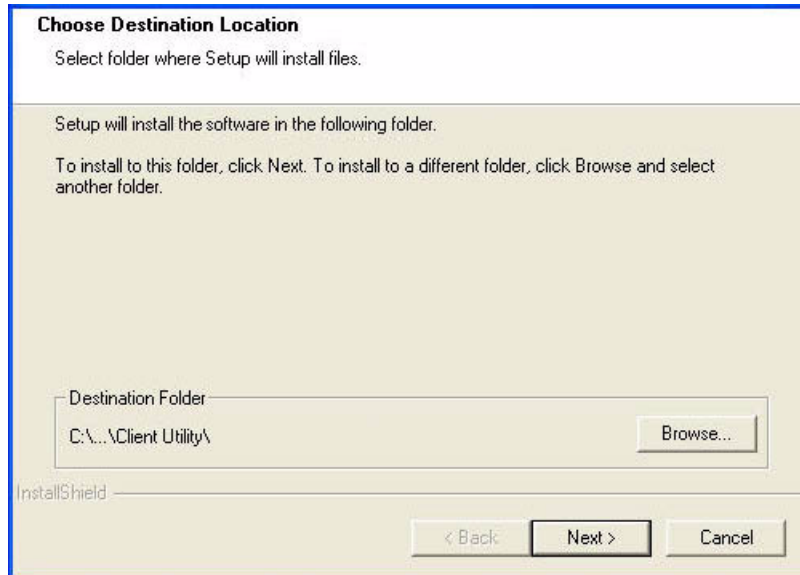
The installation wizard installs the adapter driver. The next screen indicates that the installation was successful and prompts you to continue with Client Utility installation.



9 Click **Next**.

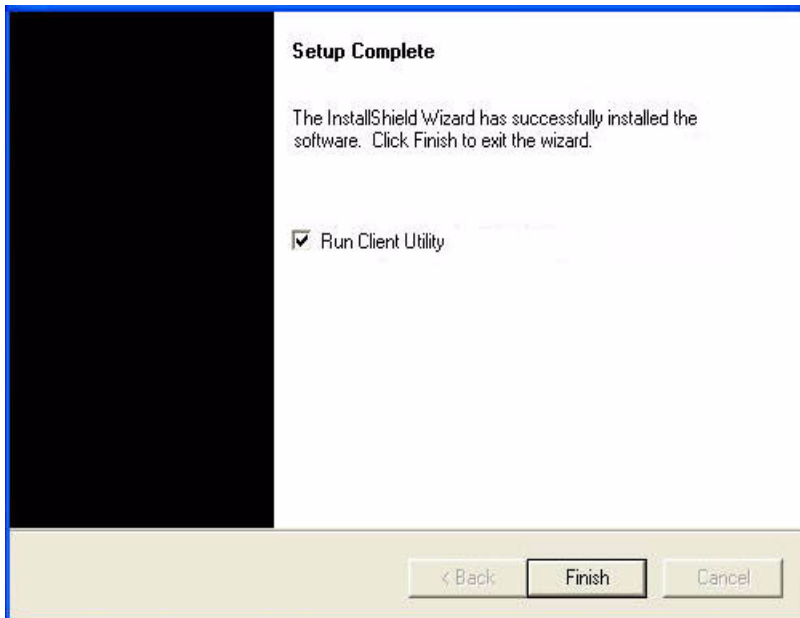
¹ If your PC Card adapter is not yet physically installed, the installation, the wizard prompts you to do so.

The wizard prompts you to choose an installation location.



- 10** Click **Next** to accept the default location, or click **Browse** to select a different location before clicking **Next**.

The wizard completes the installation.



- 11** Click **Finish** to complete the installation and start the Client Utility.

The installation is now complete. If you encounter any difficulties, refer to “Confirming the Installation” on page 33 for additional information.

Uninstalling the Client Utility and Drivers

This section explains how to remove the Client Utility software from your system, which may be necessary if you are upgrading to a newer version of the utility.

 **NOTE:** Use the Windows System control panel if you need to uninstall only the Wireless LAN Client Adapter driver.

Follow these steps to uninstall the Client Utility software and adapter driver:

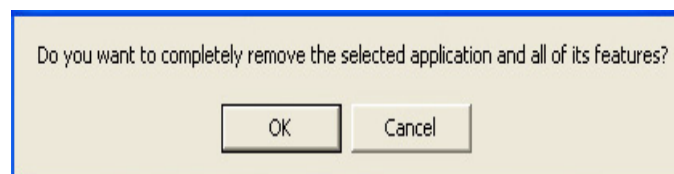
- 1 From the Start menu, choose **Programs > Airgo Networks > Uninstall Airgo Networks Software**.

The Uninstall Wizard prompts you to choose the type of maintenance to perform.



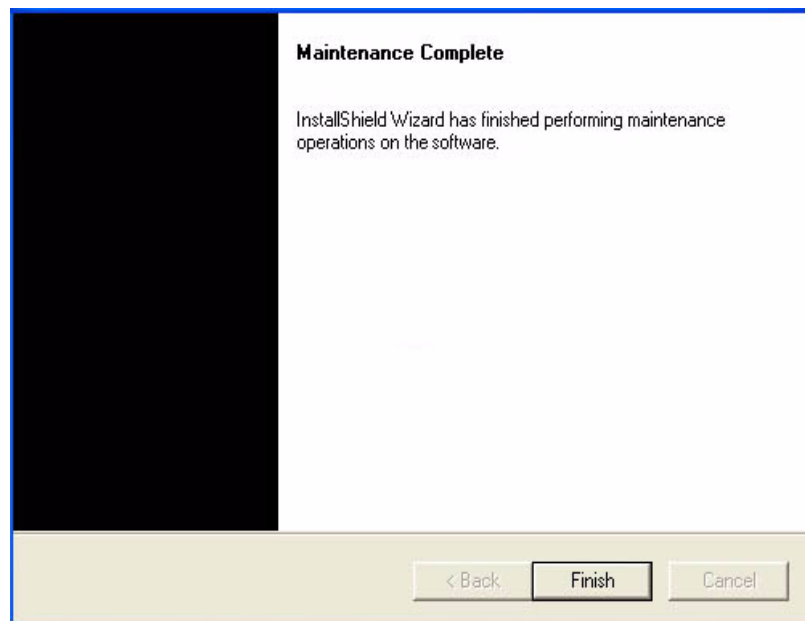
- 2 Select **Remove** and click **Next**.

The wizard prompts you to confirm.



- 3 Click **OK** to continue.

When the uninstall process is complete, the wizard presents a Finish window.



4 Click **Finish.**

The Uninstall process is now complete.

2 Introduction to the Client Utility

The chapter provides an overview of wireless networking and explains how to access the Client Utility to configure your Wireless LAN Client Adapter. It includes the following topics:

- **Overview of Wireless Networking**
- **Client Utility**
- **Navigating the User Interface**

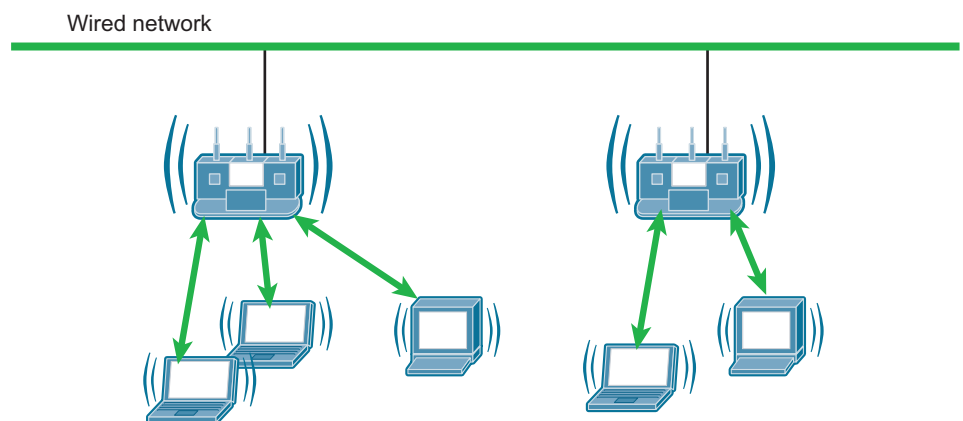
Overview of Wireless Networking

The Wireless LAN Client Adapter connects your PC to a wireless local area network (wireless LAN) by way of radio signals. An *access point* is the device that forwards data from the wired network to your PC by way of radio signals and connects you with other wireless users. The IEEE 802.11 standard identifies two types of wireless networking modes:

- In an infrastructure network, an access point links the wireless LAN to a wired network. By attaching to an existing network infrastructure, you can gain access to other resources on the wired network, other wireless LANs, or the Internet. This is the mode to use when setting up a home network or accessing an office network (Figure 3).
- In an ad-hoc wireless network, you establish communications between your PC and a small number of other wireless users without using an access point (Figure 4).

NOTE: The Wireless LAN Client Adapter installed on your PC can communicate with any access point that supports the industry standard IEEE 802.11 wireless communications protocol. It is recommended that you use the Wireless LAN Client Adapter with Access Points in order to take advantage of their advanced range, high data rates, and other features.

Figure 3: Infrastructure Network



A0017

Figure 4: Ad-Hoc Network



A0018

Service Set Identifiers

The Service Set Identifier (SSID) is a name that uniquely identifies a wireless local area network. Each device in the wireless network must have the same SSID configured in order to participate in the network. The SSID can be up to 32 alphanumeric characters in length and is also known as the wireless network name.

The 802.11 standard specifies two types of network service sets identified by SSID:

- **Basic Service Set (BSS)** — collection of wireless devices operating with an access point in infrastructure mode (Basic Service Set - BSS) or without an access point in ad-hoc mode (Independent Basic Service Set - IBSS).
- **Extended Service Set (ESS)** — collection of BSSs with wireless devices that can roam from one BSS to another while staying connected to wireless network resources.

Wireless Bands and Channels

Wireless Bands and Channels

The IEEE 802.11 b/g specification addresses wireless devices that operate in the 2.4 GHz radio frequency band. Within the band (range of radio frequencies) individual channels carry a separate radio signal. Automatic and manual band and channel selection are provided, along with monitoring and analysis capabilities to assess the status of radio coverage and signal quality.

Client Utility

If you followed the installation instructions in Chapter 1, the Client Utility is already installed on your PC. The Client Utility enables you to perform all these functions:

- Obtain a view of your wireless network, including the type of network, the access point with which you are associated, and information about the radio signals currently being transmitted and received.
- Scan and connect to wireless networks within radio range of your PC.
- Create or select a profile, which stores the specifics of the network connection, security selections, and power level for your Wireless LAN Client Adapter. The Client Utility supports multiple profiles, enabling you to connect to different networks, whether at home, at work, or at wireless hotspot locations.

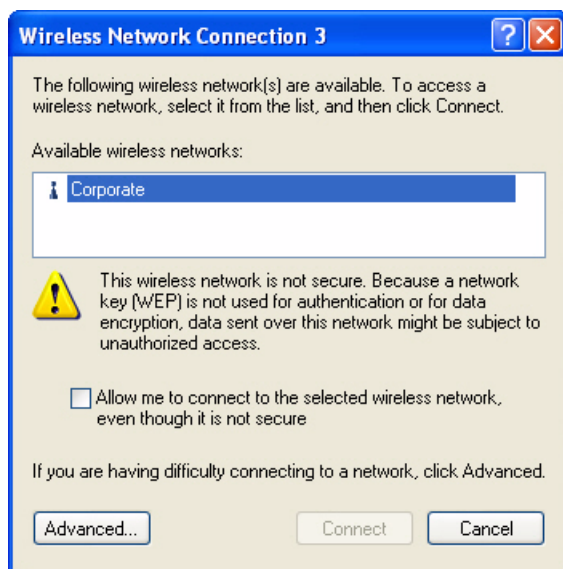
Using the Client Utility With Windows XP

To use the profile features of the Client Utility on Windows XP, you must specify that Windows XP will not be managing the wireless adapter.

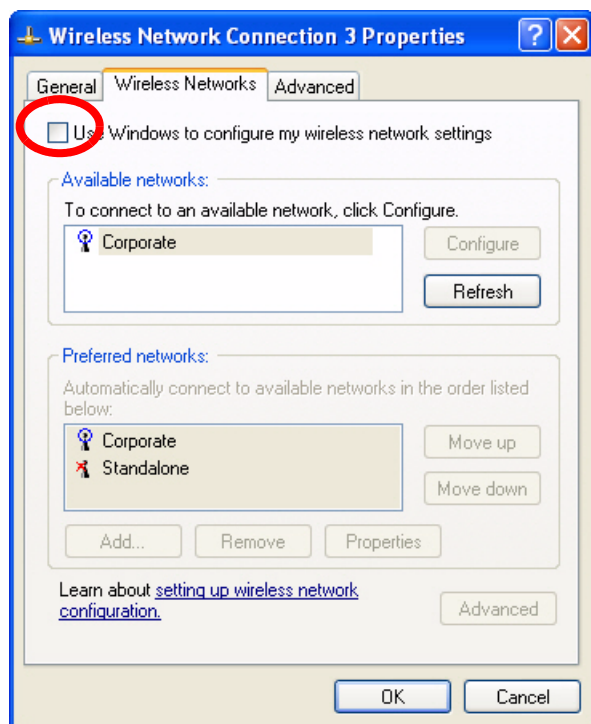
To specify that Windows will not be managing the wireless adapter:

- 1 Right-click the wireless icon on the system tray.
- 2 Select **View Available Wireless Networks**.

The window shows the list of available networks.



- 3 Click **Advanced** to open the Wireless Network Connection Properties window, Wireless Networks tab.



- 4 Clear the checkbox entitled Use Windows to configure my wireless network settings.
- 5 Click **OK**.

You can now use the Client Utility to manage your wireless connections.

Accessing the Client Utility

If you followed the instructions in Chapter 1, the Client Utility is installed on your PC.

To start the Client Utility:

- Choose **Start > Programs > Airgo Networks > Client Utility**.

The Client Utility application icon will appear in the system tray.

Using the Tray Icon

When you start the Client Utility, a small signal icon becomes visible in the system tray on the Windows toolbar (Figure 5). The color of the icon reflects the quality of the wireless connection: green for good, yellow for intermittent connection, red if there is no active connection, and a red X if the Wireless LAN Client Adapter radio is turned off. The tray icon provides access to the Client Utility menu.

Figure 5: Client Utility System Tray Icon



Application icon

To open the Client Utility window from the tray icon:

- Right-click and select **Launch Client Utility** or double-click on the icon.

To exit the Client Utility:

- Right-click and select **Exit**.

To access the help system:

- Right-click and select **Help**.

Disabling and Re-Enabling the Wireless LAN Client Adapter

You can easily enable or disable the Wireless LAN Client Adapter radio from the Client Utility.

To enable the radio:

- 1 Right-click the Client Utility icon in the system tray.
- 2 Select **Radio On**.

To disable the radio:

- 1 Right-click the Client Utility icon in the system tray.
- 2 Select **Radio Off**.

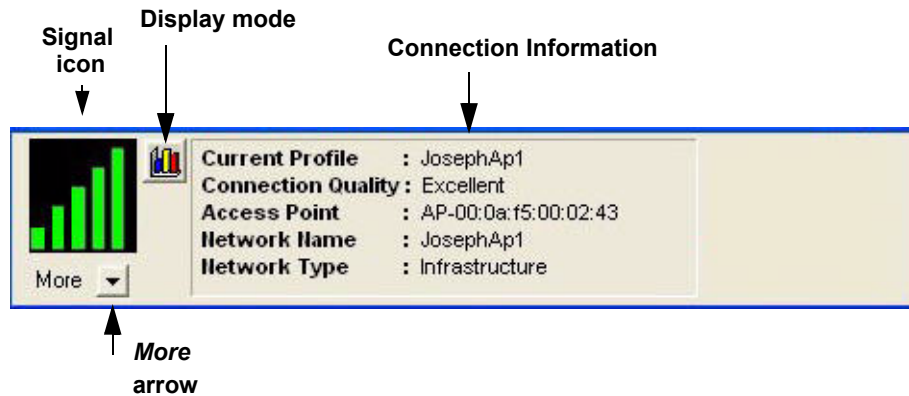
Navigating the User Interface

This section explains how to use the compact and expanded views of the Client Utility.

Using the Compact View

The compact view displays summary information about current communications between your PC and the access point. When you start the Client Utility, the compact view opens in text mode (Figure 6).

Figure 6: Client Utility Compact View, Text Mode

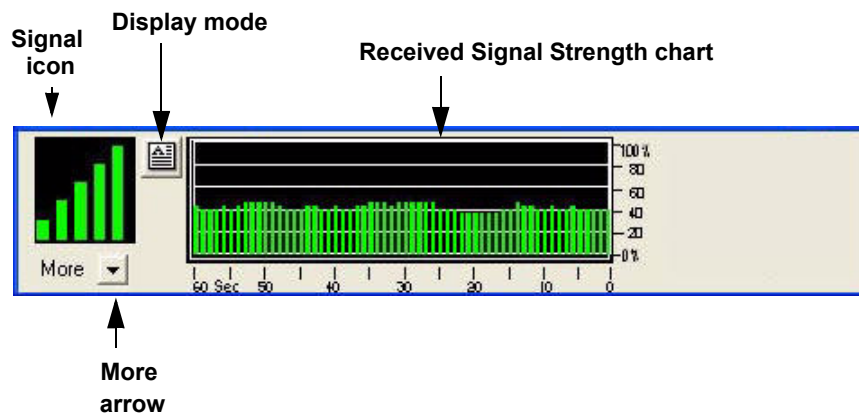


The Signal icon on the left changes color according to current received signal strength: green if signal strength is good, yellow if it is of lower quality, and red if there is no active signal. The Received Signal Strength bar chart displays a history of this information for the past 60 seconds.

Text mode lists the network profile currently in use, the name of the access point to which your Wireless LAN Client Adapter is connected, and the name of the wireless network. It also gives a text description of the current received signal strength: excellent, acceptable, or blank if there is no signal.

The compact view also has a graphical mode, which opens when you click the Display Mode icon (Figure 7).

Figure 7: Client Utility Compact View, Graphical Mode



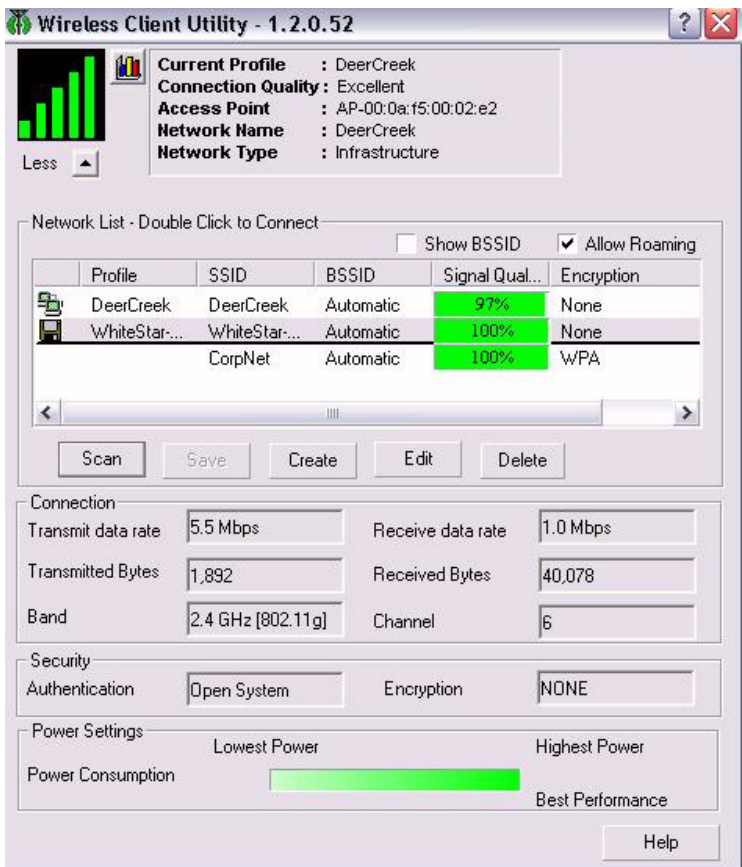
Use the graphical mode at any time to obtain a snapshot of the signal strength to your Wireless LAN Client Adapter.

The More arrow opens the expanded view. When the expanded view is open, the arrow is labeled Less. Click **Less** to return to the compact view.

Using the Expanded View

Click **More** to open the Client Utility to the expanded view (Figure 8).

Figure 8: Client Utility, Expanded View



The upper section of the expanded view lists all the networks and network profiles available to your PC. The following information and options are available:

Item	Description
Status icon	An icon is displayed if a profile has been saved for the entry or if the Wireless LAN Client Adapter is currently connected to that network:  Profile is saved  You are currently connected to this network A horizontal line separates the profiles at the top of the list (above the line) from the identified networks that do not have profiles defined (below the line).
Profile	Name of the profile, if a profile is defined
SSID	Name of the network
BSSID	MAC address of the access point if Show BSSID is checked, or automatic if show BSSID is not checked.
Signal quality	Quality of the radio signal established with the access point, as a percentage

Item (continued)	Description
Encryption	Type of data encryption enabled for this access point or profile
Network	Infrastructure or ad-hoc

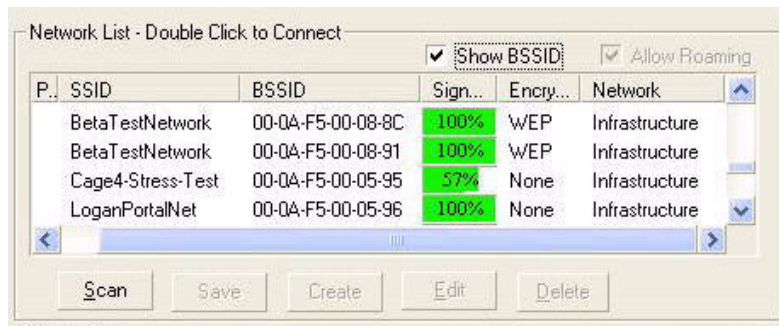
Use the horizontal scroll bar to view all the columns. You can resize each column by selecting and moving the column header dividers.

Two checkboxes above the Network List influence the display and behavior of the network connections:

Option	Description
Show BSSID	If this checkbox is selected, the Network List includes an entry for each access point in a given SSID by MAC address.
Allow Roaming	If this checkbox is selected, you can move from one access point to another without changing the active network selection.

Figure 9 The next figure shows a Network List with the Show BSSID checkbox selected. The access points for the SSID are listed below, along with the BSSID.

Figure 9: Network List with Show BSSID Selected



The Scan, Save, Create, Edit, and Delete buttons below the Network List are used to detect available access points and work with profiles.

The remaining areas in the Expanded View display read-only information about the current connection and settings. The Connection section displays the following information:

- The current connection rate for data transmitted between your PC and the access point, in megabits per second. When there is no active data transmission, it shows the rate at which beacons are transmitted.
- The radio channel and band used for communications.
- The number of transmitted and received bytes of data since the wireless connection was initiated.

The Security section shows the authentication and data encryption currently used; and the Power section shows the level of power at which the Wireless LAN Client Adapter is operating.

[Chapter 3](#) explains how to scan and connect to a network and how to create and save profiles containing configuration information.

Background Operation and Exiting

While the Client Utility is running, its icon is always displayed on the Windows system tray. To close the Client Utility window while keeping it operating in the background, click **X** in the upper right corner of the utility window. To exit the utility, right-click the system tray icon, and select **Exit**.

3 Configuration

Configuration Overview

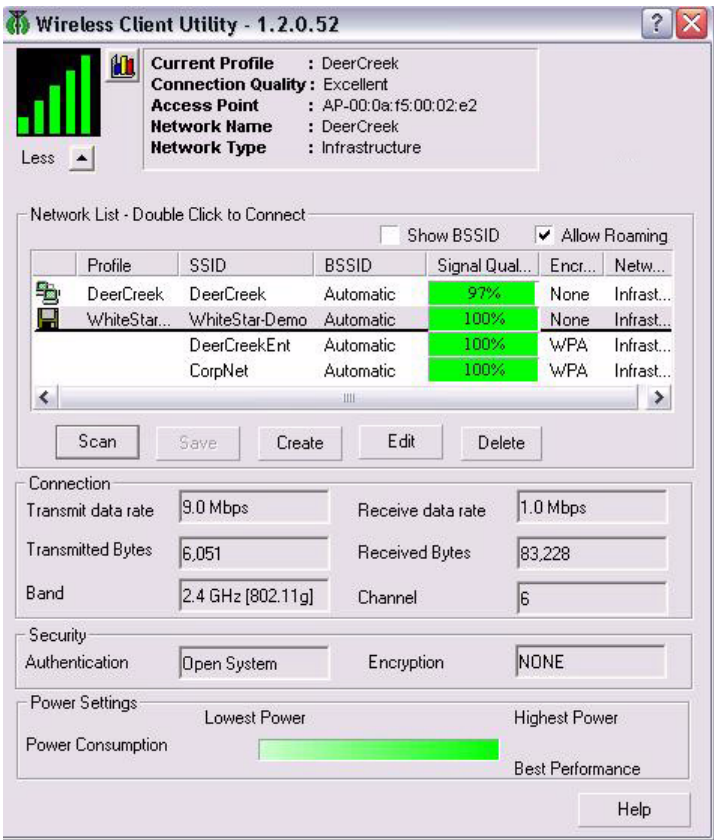
This chapter explains how to scan for and connect to wireless networks and how to set up a profile to store network configuration information. It includes the following topics:

- **Configuration Overview**
- **Scanning for Available Networks**
- **Working with Profiles**
- **Profile Window**
- **Wireless Security**

Configuration Overview

Figure 10 shows the Client Utility in Expanded View.

Figure 10: Client Utility, Expanded View



The Client Utility uses profiles to store information describing how your Wireless LAN Client Adapter connects to the wireless network. Each profile contains information about the type of network connection, security settings, and power settings.

To make it easy for you to connect to wireless networks at home, office, or wireless hotspot locations, Client Utility provides the ability to create multiple profiles, each containing information about a different network or a different set of configuration values. When you move from one location to another, your Wireless LAN Client Adapter automatically detects which network is currently available and applies the correct profile. The Network List includes all the saved profiles and newly identified networks.

If you travel to an area with a network not previously encountered or configured, your Wireless LAN Client Adapter attempts to connect to it. If successful, you can save the detected settings in your list of available profiles.

[The remainder of this chapter describes how to scan and connect to wireless networks, and how create and work with profiles.](#)

Scanning for Available Networks

Upon boot-up, the Wireless LAN Client Adapter scans for all access points within radio range and attempts to connect to one of them based on previously scanned profiles. It associates with the first

access point it finds for which it can establish radio communications. Association normally happens automatically; however, it is recommended that you start the Client Utility once you are connected. This enables you to verify the configuration and confirm that the access point to which you are connected is a trusted component of your network.

Whenever you open the Client Utility, the system performs an automatic scan. You can also scan for networks at any time, upon demand.

To scan for available networks:

- 1 Choose **Start > Programs > Airgo Networks > Client Utility**.
This displays the application icon in the system tray.
- 2 Click **More** to open the Expanded View.
- 3 Click **Scan**.

A scanning box opens (Figure 11) to show that the scan is taking place. When the scan is complete, the Network List area (Figure 10) displays all the discovered networks.

Figure 11: Scanning Icon



The results of the scan are presented near the top of the expanded Client Utility window (Figure 10). If a profile already exists for the discovered SSID, it appears in the network list with its name in the Profile column with a disk icon to the left. If a profile does not exist, the Profile column is blank.

Working with Profiles

[This section provides instructions on the tasks used in managing profiles:](#)

To create a new profile:

- 1 Click **Create** to open the Profile window.
- 2 Enter a new name in the Profile Name field.
- 3 Enter the SSID of the network. For more information, see “Service Set Identifiers” on page 12.
- 4 Drag the sliding bar to select an output power level.
- 5 Select a security level and details. For more information, see “Security Settings” on page 24.
- 6 Click **Save**. The Profile window closes and the newly created profile appears in the Network List in the Client Utility window.

To make an existing profile active (use the profile to control wireless communications from your PC):

- 1 Double-click on the entry in the Network List.
- 2 Click **Save & Activate**.

You can edit any profile in the list, including the active one. If you edit and save the active profile, the system temporarily drops the network connection while implementing the changes. When the configuration change is complete, the network connection is restored.

To edit a profile:

- 1 Highlight the profile name and click **Edit**.

If the profile is active, the system requests confirmation that you want to continue. Click **OK** to open the profile window. See “Profile Window” on page 23 for detailed information on the settings in the Profile window.

- 2 Confirm the network type and SSID.
- 3 Move the sliding power setting bar to the desired output power level.
- 4 Select the level of security (Low or No).
- 5 If low security is selected, choose the encryption and authentication options to match those of the access point or access points to which you are associating.
- 6 Click **Save**.

To delete a profile:

- 1 Highlight the profile name and click **Delete**.

Click **OK** when prompted to confirm.

Profile Window

Figure 13 shows the Profile window, which opens when you double-click on an entry in the network list or highlight a listed profile and click Edit. This section provides an overview of the information in the Profile window.

Profile Name

The top of the window contains an area for the name of the profile. When you create a profile, select a name that clearly identifies the network.¹ The default profile name is the SSID.

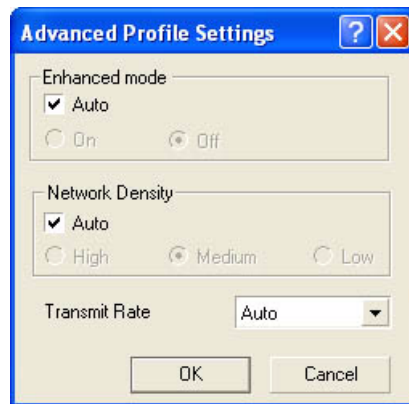
Figure 12: Profile Window

Advanced Settings

The Advanced button to the right of the Profile Name opens the Advanced Profile Settings window. (Figure 13). The settings in this window enable you to take advantage of the enhanced performance features of the Access Point. It is recommended to keep the default Auto settings, which provide compatibility with basic and enhanced data rates and network density.

¹ The Profile Name field is grayed out when you edit an existing profile.

Figure 13: Advanced Profile Settings



Network Settings

The Network section shows the type of network (infrastructure or ad-hoc) and contains an area to enter the SSID (service set identifier), a name that uniquely identifies the network.

- Select **SSID** to connect to an existing wireless network, usually with an interface to a wired network, for Internet and email access, file sharing, and print and other services.
- Select **Connect to Ad Hoc Network** to attach to a temporary wireless network that has been set up by another user.
- Select **Start Ad-Hoc Network** to create a temporary wireless network without using an access point

Ad-hoc networks are generally used to enable file and print sharing for short-term activities such as meetings or conferences. If you are creating a new ad-hoc network, use the default Auto-Channel option, unless it is necessary for you to use a specific radio channel. The auto-channel option automatically selects a channel to use for the ad-hoc network.

Power Setting

The Power Settings area contains a sliding bar to select output power between the lowest and highest available levels. Higher settings enable the highest performance. Lower settings draw less power from your PC and are advisable when you want to conserve PC battery life or you know that you are within close range of an access point.

Security Settings

The Security Settings area includes choices for configuring a secure connection between your PC and access point. The next section, [“Wireless Security,”](#) provides background on wireless security options and gives guidelines for security settings in the enterprise, small office, and home environments.

Wireless Security

Although security is important in any network, the characteristics of wireless networks can make them vulnerable to attack. Unlike wired networks, which require a physical connection that can be secured with lock and key, wireless networks require only a radio signal for communication, and physical barriers do not provide protection. A concern since the introduction of the IEEE 802.11

wireless communication standard, wireless security continues to evolve, as shortcomings of existing security solutions are uncovered and new solutions are adopted.

[Company Name - Short] products provide a complete state-of-the-art security solution for 802.11 wireless networks, using the native wireless support in Windows 2000 and Windows XP where appropriate.

Wireless security encompasses two major components: encryption and authentication. Encryption is the means by which data transferred across the wireless link are protected from eavesdropping. Authentication is the means by which the access point verifies the identity of your PC and your identity, and confirms that you have permission to use the network.

Encryption

Encryption protects wireless data from being intercepted and deciphered during transmission, and thereby assures the security of your data. Several encryption options are supported:

- AES (Advanced Encryption Standard) — excellent financial-grade security
- TKIP (Temporal Key Integrity Protocol) — good security, as an upgrade to legacy systems
- WEP (Wired Equivalent Privacy) — minimal protection security, acceptable only for non-critical data
- Open or no encryption — no protection, use only for non-critical communications or with other security protection such as https or VPN/IPsec for corporate communications

The latest and most effective encryption methods are part of the WPA (Wi-Fi Protected Access) cipher suite and are recommended for all environments in which security is an important consideration, whether in the enterprise, small office or home. WPA provides much more complete protection against discovery of encryption keys than do the earlier WEP standards. WPA itself has already spawned two generations of encryption technology, with AES being the latest and most effective standard. TKIP is the encryption protocol that was first introduced with WPA, but it provides less complete protection than does AES.

The original 802.11 wireless communication specification standard included WEP for wireless security. Although still widely used today, WEP security does not provide adequate protection against discovery of encryption keys, and may therefore be vulnerable to attack. Use WEP only in cases where the access point does not support higher level security and security is a consideration in your network design.

The WEP algorithm requires an encryption key, which is a code used in the encrypting and decrypting of data. Although all WEP methods are vulnerable, 128-bit keys are somewhat more difficult to decrypt than 64-bit keys. WEP provides the option of entering a key in ASCII (text) or hexadecimal (numeric) format. ASCII keys are useful as a text passphrase, while hexadecimal keys provide more protection and support for other devices. Key generation can be manual or automatic, with automatically generated keys providing more protection.

Authentication

Effective authentication methods rely on manual distribution of shared or pre-shared authentication keys or automatic generation of keys by use of a RADIUS (Remote Authentication Dial-In User Service) server.

A shared or pre-shared key is an authentication string entered at the access point and client PCs. Authentication takes place by matching the key stored in each PC with the key stored in the access point.

Automatic key-generation methods rely upon digital certificates, which contain encoded user and encryption information to verify the identity of a user and match it with a database of secure user records. A certificate authority is the network service that manages digital certificates and guarantees their integrity. The IEEE 802.1X standard specifies certificate-based authentication using EAP (Extensible Authentication Protocol). EAP, in turn, comes in numerous variations.

Most enterprises manage remote access to the certificate authority using a RADIUS (Remote Authentication Dial-In User Service) server. In this arrangement, client PC users install RADIUS client software on their local PCs to provide RADIUS server access. Funk Software and Microsoft are the major suppliers of RADIUS client software.

For home or small office networks, shared or pre-shared keys can provide adequate authentication without the burden of centralized management and control. A built-in RADIUS security portal is provided in the Access Point to extend the management and scalability features of centralized management to administrators in small-to-mid sized office environments.

Client Utility Security Options

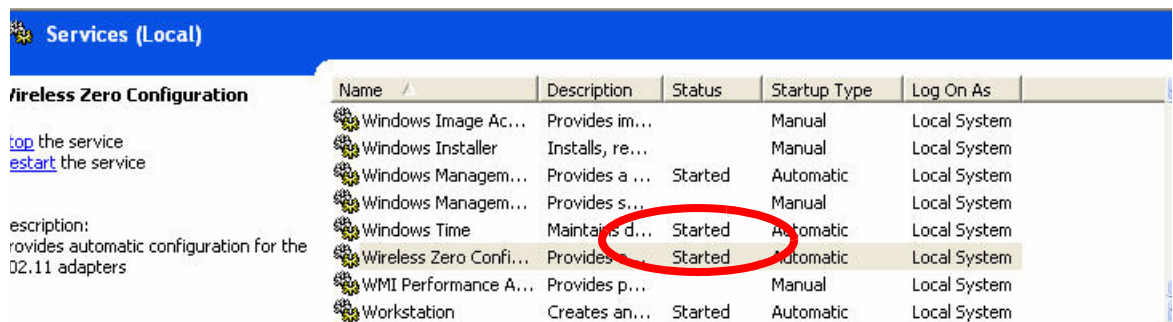
The network list in the Client Utility Expanded View displays the security required for each SSID and profile.

The Client Utility supports configuration of the WEP or Open security options. In the Profile window, you can select WEP or open security for the radio connection between your PC and the access point, and enter choices for encryption and authentication within the selected security framework. For instructions, see “Working with Profiles” on page 21.

Windows XP users can connect to networks that support WPA security. To do so, it is necessary to use the Wireless Zero Config (WZC) capability native to Windows XP. When WZC is enabled, the profile features of the Client Utility are automatically disabled; however, it is still recommended to use the Client Utility to view and scan for networks.

To use WZC to configure security settings, first confirm that the WZC service is enabled:

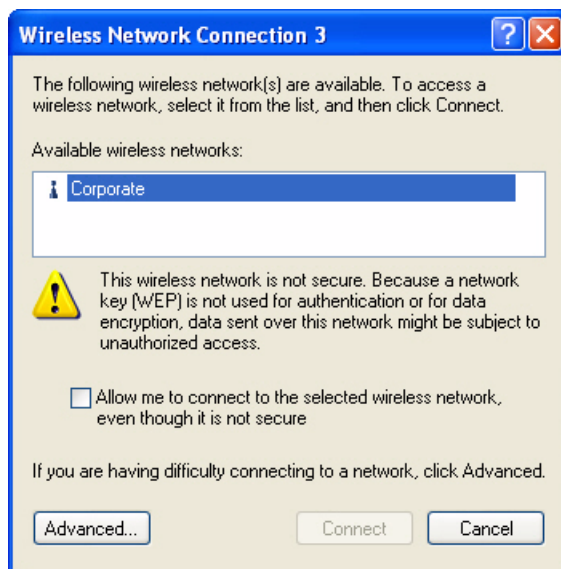
- 1 From the Start menu, choose **Control Panel > Administrative Tools > Services**.
- 2 Check whether the Status column displays “Started.”



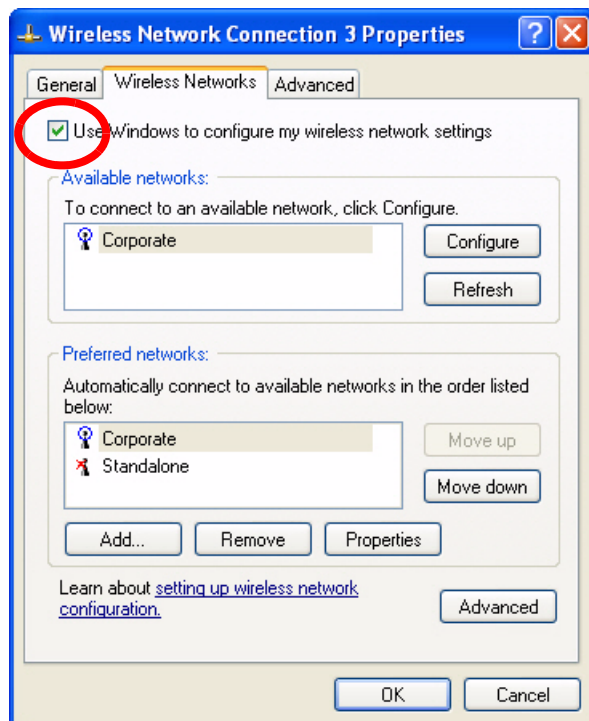
- 3 If Started is not the value in the Status column,
 - a Double-click the Wireless Zero Config entry to open the Wireless Zero Configuration Properties dialog box.
 - b Select **Automatic** from the Start-up Type pull-down list.
 - c Click **Start**.
 - d Click **OK**.

Now use WZC to configure security settings:

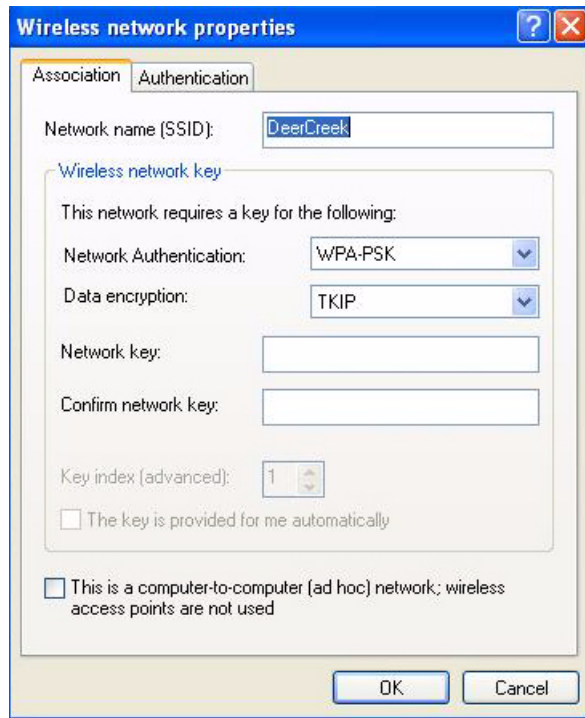
- 1 Right-click the wireless icon on the system tray.
- 2 Select **View Available Wireless Networks**.
- 3 The window shows the list of available networks.



- 4 Select your network, and click **Advanced** to open the Wireless Network Connection Properties window, Wireless Networks tab.
- 5 Confirm that **Use Windows to configure my wireless network settings** is selected.



- 6 Select the network, and click **Configure**.
- 7 Confirm the authentication and encryption selections exactly match those of the access point to which you are connecting. Enter a network key, if required.



- 8 If you selected AES for data encryption, open the Authentication tab and select the EAP type appropriate to your network.
- 9 Click **OK** as needed to close the WZC windows.

Glossary

This glossary defines terms that apply to wireless and networking technology in general and [Company Name - Short] products in particular.

802.1x

Standard for port-based authentication in LANs. Identifies each users and allows connectivity based on policies in a centrally managed server.

802.11

Refers to the set of WLAN standards developed by IEEE. The three commonly in use today are 802.11a, 802.11b, and 802.11g, sometimes referred to collectively as Dot11.

Access Control List (ACL)

A list of services used for security of programs and operating systems. Lists users and groups together with the access awarded for each.

Access Point (AP)

An inter-networking device that connects wired and wireless networks together. Also, an 802.11x capable device that may support one or more 802.11 network interfaces in it and co-ordinates clients stations in establishing an Extended Service Set 802.11 network

Advanced Encryption Standard (AES)

An encryption algorithm developed for use by U.S. Government agencies and now incorporated into encryption standards for commercial transactions.

Client Utility (ACU)

Application that executes on a client station and provides management and diagnostics functionality for the 802.11 network interfaces.

Ad-Hoc network

A group of nodes or systems communicating with each other without an intervening Access Point. Many wireless network cards support ad-hoc networking modes.

Authentication Server

A central resources that verifies the identity of prospective network users and grants access based on pre-defined policies.

Authentication Zone

A administrative grouping of resources for user authentication.

Backhaul

The process of getting data from a source and sending it for distribution over the main backbone network. Wireless backhaul refers to the process of delivering data from a node on the wireless network back to the wired network. Also referred to a WDS.x.

Basic Service Set (BSS)

The set of all wireless client stations controlled by a single access point. The BSSID, or identifier, for the basic service set can be assigned or default to the MAC address of the access point.

Bridge

A connection between two (or more) LANs using the same protocol. Virtual bridges are used as a means of defining layer 2 domains for broadcast messages. Each virtual bridge uniquely defines a virtual local area network (VLAN).

Class of Service (COS)

A method of specifying and grouping applications into various QoS groups or categories.

Differentiated Services Code Point (DSCP)

A system of assigning Quality of Service “Class of Service” tags.

Domain Name Service (DNS)

A standard methodology for converting alphanumeric Internet domain names to IP addresses.

Dynamic Host Configuration Protocol (DHCP)

A communications protocol enabling IP address assignments to be managed both dynamically and centrally. With DHCP enabled on a node (a system, device, network card, or Access Point), when it boots or is connected to a network, an address is automatically assigned. Each assigned address is considered to be “leased” to a specific node; when the lease expires, a new IP can be requested and/or automatically reassigned. Without DHCP, IP addresses would need to be entered manually for each and every device on the network.

Dynamic Frequency Selection (DFS)

A method for selecting the least intrusive and noisy available frequency for operation, part of the 802.11 specification.

Dynamic IP Address

A TCP/IP network address assigned temporarily (or dynamically) by a central server, also known as a DHCP server. A node set to accept dynamic IPs is said to be a “DHCP client.”

Extensible Authentication Protocol (EAP)

Standard that specifies the method of communication between an authentication server and the client, or supplicant, requesting access to the network. EAP supports a variety of authentication methods.

Extensible Authentication Protocol Over LAN (EAPOL)

Protocol used for 802.1x authentication.

EAP-TLS

EAP using Transport Layer Security. EAP-based authentication method based on X.509 certificates, which provides mutual, secure authentication. Certificates must be maintained in the authentication server and supplicant.

EAP-PEAP

Protected EAP-based authentication method based on X.509 certificates. Uses a two-phase approach in which the server is first authenticated to the supplicant.

This establishes a secure channel over which the supplicant can be authenticated to the server.

Extended Service Set (ESS)

A set of multiple connected BSSs. From the perspective of network clients, the ESS functions as one wireless network, with clients able to roam between the BSSs within the ESS.

ESSID

Name or identifier of the ESS used in network configuration.

hostname

The unique, fully qualified name assigned to a network computer, providing an alternative to the IP address as a way to identify the computer for networking purposes.

Hypertext Transfer Protocol (HTTP)

Protocol governing the transfer of data on the World Wide Web between servers and browser (and browser enabled software applications).

Hypertext Transfer Protocol over SSL (HTTPS)

A variant of HTTP that uses SSL (Secure Sockets Layer) encryption to secure data transmissions. HTTPS uses port 443, as opposed to HTTP which uses port 80.

Independent Basic Service Set (IBSS)

A set of clients communicating with each other or a network via an Access Point.

Internet Protocol (IP)

The network layer protocol for routing packets through the Internet.

IP address

32-bit number, usually presented as a period-separated (dotted decimal) list of three-digit numbers, which identifies an entity on the Internet according to the Internet Protocol standard.

Local Area Network (LAN)

A group of computers, servers, printers, and other devices connected to one another, with the ability to share data between them.

Maskbits

Number of bits in the subnet prefix for an IP address, (provides the same information as subnet mask). Each triplet of digits in an IP address consists of 8 bits. To specify the subnet in maskbits, count the number of bits in the prefix. To specify using a subnet mask, indicate the masked bits as an IP address. Example: subnet mask 255.255.255.0 is equivalent to 24 maskbits, which is the total number of bits in the 255.255.255 prefix.

Media Access Control (MAC) Address

A unique hardware-based equipment identifier, set during device manufacture. The MAC address uniquely identifies each node of a network. Access Points can be configured with MAC access lists, allowing only certain specific devices to connect with the LAN through them, or to allow certain MAC-identified network cards or devices access only to certain resources.

MAC address authentication

Method of authenticating clients by using the MAC address of the client station as opposed to the user.

Network Address Translation (NAT)

The translation of one IP address used within a network to another address used elsewhere. One frequent use of NAT is the translation of IPs used *inside* a company, versus the IP addresses visible to the outside world. This feature helps increase network security to a small degree, because when the address is translated, this provides an opportunity to authenticate the request and/or to match it to known, authorized types of requests. NAT is also used sometimes to map multiple nodes to a single outwardly visible IP address.

Network Interface Card (NIC)

Generic term for network interface hardware that includes wired and wireless LAN adapter cards, PC Cardbus PCMCIA cards, and USB-to-LAN adapters.

Network Management System (NMS)

Software application that controls a network of multiple access points and clients.

Node

Generic term for a network entity. Includes a access point, network adapter (wireless or wired), or network appliance (such as a print server or other non-computer device)

Network Time Protocol (NTP)

NTP servers are used to synchronize clocks on computers and other devices. APs have the capability to connect automatically to NTP servers to set their own clocks on a regular basis.

Ping Packet INternet Groper (ping)

A utility which determines whether a specific IP address is accessible, and the amount of network time (measured in milliseconds) for response. Ping is used primarily to troubleshoot Internet connections.

Policy-based Networking

The management of a network with rules (or policies), governing the priority and availability of bandwidth and resources, based both on the type of data being transmitted, as well as the privileges assigned to a given user or group of users. This allows network administrators to control how the network is used, to help maximize efficiency.

Power Over Ethernet (PoE)

Power supplied to a device by way of the Ethernet network data cable instead of a electrical power cord.

Preamble Type

The preamble defines the length of the cyclic redundancy check (CRC) block for communication between the Access Point and a roaming network adapter. All nodes on a given network should use the same preamble type.

Quality of Service (QoS)

QoS is a term encompassing the management of network performance, based on the notion that transmission speed, signal integrity, and error rates can be managed,

measured, and improved. In a wireless network, QoS is commonly managed through the use of policies.

Remote Authentication Dial-In User Service (RADIUS)

A client/server protocol and software that enables remote access servers to communicate with a central server to authenticate users and authorize service or system access. RADIUS permits maintenance of user profiles in a central repository that all remote servers can share.

Radio Frequency (RF)

The electromagnetic wave frequency radio used for communications applications.

Roaming

Analogous to the way cellular phone roaming works, roaming in the wireless networking environment is the ability to move from one AP coverage area to another without interruption in service or loss in connectivity.

Rogue AP

An access point that connects to the wireless network without authorization.

Secure SHell (SSH)

Also known as the Secure Socket Shell, SSH is a UNIX-based command line interface for secure access to remote systems. Both ends of communication are secured and authenticated using a digital certificate, and any passwords exchanged are encrypted.

Service Set Identifier (SSID)

The SSID is a unique identifier attached to all packets sent over a wireless network, identifying one or more wireless network adapters as “belonging” to a common group. Some Access Points can support multiple SSIDs, allowing for varying privileges and capabilities, based on user roles.

Secure Sockets Layer (SSL)

A common protocol for message transmission security on the Internet. Existing as a program layer between Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers, SSL is a standard feature in Internet Explorer, Netscape, and most web server products.

Simple Mail Transfer Protocol (SMTP)

Protocol used to transfer email messages between email servers.

Simple Network Management Protocol (SNMP)

An efficient protocol for network management and device monitoring.

SNMP trap

A process that filters SNMP messages and saves or drops them, depending upon how the system is configured.

Spanning Tree Protocol (STP)

A protocol that prevents bridging loops from forming due to incorrectly configured networks.

Station (STA)

An 802.11 capable device that supports only one 802.11 network interface, capable of establishing a Basic Service Set 802.11 network (i.e., peer-to-peer network)

Static IP Address

A permanent IP address assigned to a node in a TCP/IP network.

Subnet

Portion of a network, designated by a particular set of IP addresses. Provides a hierarchy for addressing in LANs. Also called subnetwork.

Subnet Mask

A TCP/IP addressing method for dividing IP-based networks into subgroups or subnets (compare with maskbits). Each triplet of digits in an IP address consists of 8 bits. To specify using a subnet mask, indicate the masked bits as an IP address. To specify the subnet in maskbits, count the number of bits in the prefix. Example: subnet mask 255.255.255.0 is equivalent to 24 maskbits, which is the total number of bits in the 255.255.255 prefix.

Temporal Key Integrity Protocol (TKIP)

Part of the IEEE 802.11i encryption standard. TKIP provides improvements to WEP encryption, including per-packet key mixing, message integrity check and a re-keying mechanism.

Traffic Class Identifier (TCID)

Part of the standard 802.11 frame header. The 3-bit TCID is used for mapping to class-of-service values.

Transmission Control Protocol/Internet Protocol (TCP/IP)

One of the most commonly used communication protocols in modern networking. Addresses used in TCP/IP usually consist of four triplets of digits, plus a subnet mask (for example, 192.168.25.3, subnet 255.255.255.0).

Transport Layer Security (TLS)

Protocol that provides privacy protection for applications that communicate with each other and their users on the Internet. TLS is a successor to the Secure Sockets Layer (SSL).

Trunk

In telecommunications, a communications channel between two switching systems. In a wireless network, a trunk is a wireless connection from one access point to another.

Type of Service (ToS)

Sometimes also called IP Precedence, ToS is a system of applying QoS methodologies, based on headers placed into transmitted IP packets.

User Datagram Protocol (UDP)

A connectionless protocol similar to TCP/IP, but without the same level of error-checking. UDP is commonly used when some small degree of errors and packet-loss can be tolerated without losing program integrity, such as for online games.

Virtual LAN (VLAN)

A local area network with a definition that addresses network nodes on some basis other than physical location or even whether the systems are wired together or operating using the same local equipment. VLANs are, on average, much easier to manage than a physically implemented LAN. In other words, moving a user from one VLAN to another is a simple change in software, whereas on a regular LAN, the computer or device would need to be connected physically to a different switch

or router to accomplish the same thing. Network management software of some sort is used to configure and manage the VLANs on a given network.

Wi-Fi Protected Access (WPA)

Security mode for wireless networks that improves on the authentication and encryption features of WEP.

Wired Equivalent Privacy (WEP)

Security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. Uses dynamically or manually assigned keys for encryption and authentication, as dictated by the capabilities of the client station. The WEP algorithms are vulnerable to compromise; therefore, WEP security is only recommended for legacy clients that do not support the newer generation security standards.

Windows Internet Name Server (WINS)

The Windows implementation of DNS, which maps IP addresses to computer names (NetBIOS names). This allows users to access resources by computer name instead of by IP address.

Wi-Fi

A play on the term “HiFi,” Wi-Fi stands for Wireless Fidelity, which is a term for wireless networking technologies.

Wireless Local Area Network (WLAN)

An acronym for wireless local area network, employing radio frequencies to transmit data (usually encrypted for), much like LANs transmit data over wires and fiber optic cables.

Index

Numerics

128-bit WEP key 25
40-bit WEP key 25
802.11 11, 43
802.1x 43

A

access point (AP) 43
ACL 43
activating a profile 21
ad-hoc network 11, 43
Advanced Encryption Standard. See AES
AES 25, 43
allow roaming checkbox 17
ASCII encoding of WEP key 25
authentication 25
 server 43
authentication string 25
authentication zone 43
automatic scan 21

B

backhaul 43
bands 12
basic configuration 19
basic service set. See BSS
bridge 44
BSS 12, 44
BSSID 16, 44
 checkbox 17

C

channels 12
Client Utility 43
 compact view 14
 expanded view 15
Client Utility functions 12
compact view 14
connect to ad-hoc network 24
connecting the Wireless Client LAN Adapter 2
COS 44
creating a profile 21

D

deleting a profile 22
device types 1
DFS 44
DHCP 44
display mode 15
DNS 44
driver installation
 Windows 2000 31
 Windows XP 29
DSCP 44
dynamic IP address 44

E

EAP 44
EAP-PEAP 44
EAP-TLS 44
editing a profile 22
encryption 16, 25
ESS 12, 45
ESSID 45
extended service set. See ESS

F

features 1
Funk Software 26

G

graphical mode 15

H

hexidecimal encoding of WEP key 25
high security 26
home or small office 26
hostname 45
HTTP 45
HTTPS 45

I

IBSS 12, 45
icon in network list 16
IEEE 802.11 11
independent basic service set. See IBSS
IBSS
infrastructure network 11

infrastructure setting 24
installation 1
 confirming 33
 verifying Windows 2000 38
 verifying Windows XP 33
installing the driver and client utility 4
installing the Wireless Client LAN Adapter driver 29
introduction to the Client Utility 11
IP 45
IP address 45

L

LAN 45
LEDs 3
locations
 changing 20

M

MAC address 45
MAC address authentication 46
maskbits 45
Mini PCI adapter 1
moving from location to location 20

N

NAT 46
network
 ad-hoc 11
 infrastructure 11
network listing 20
network settings
 profile window 24
NIC 46
NMS 46
no security 26
node 46
NTP 46

O

open security 26

P

PC card 1
PCI card 1

- ping 46
- PoE 46
- policy-based networking 46
- power settings 24
- preamble type 46
- pre-shared key 25
- profile 16, 20
- profile name 23
- profile window 23
 - network settings 24
 - power settings 24
 - security settings 24
- profiles
 - activating 21
 - creating 21
 - deleting 22
 - editing 22

Q

- QoS 46

R

- RADIUS 47
- RADIUS server 26
- Remote Authentication Dial-In User Service. See RADIUS
- RF 47
- roaming 17, 47
- rogue AP 47

S

- scanning
 - for available networks 20
- security 24
 - authentication 24
 - encryption 24
- security options 26
- security settings 24
- service set identifier. See SSID
- show BSSID checkbox 17
- signal icon 15
- signal pattern 15
- signal quality 16
- SMTP 47
- SNMP 47
- SNMP trap 47
- software patches 4
- SSH 47
- SSID 12, 16, 47
- SSL 47
- STA 47
- start ad-hoc network 24
- starting the Client Utility 14

- station 47
- status icon 16
- STP 47
- subnet 48
- subnet mask 48
- system requirements 1

T

- TCID 48
- TCP/IP 48
- Temporal Key Integrity Protocol. See TKIP
- TKIP 25, 48
- TLS 48
- ToS 48
- tray icon 14
- trunk 48

U

- UDP 48
- uninstalling the Client Utility 8
- using the tray icon 14

V

- VLAN 48

W

- WEP 25, 26, 49
 - ASCII encoding 25
 - hexidecimal encoding 25
- Wi-Fi 49
- Wi-Fi Protected Access. See WPA
- Windows
 - managing wireless adapter 12
 - wireless software patches 4
 - Wireless Zero Config (WZC) 12
- WINS 49
- wireless adapter
 - and Windows 12
- wireless bands and channels 12
- Wireless Zero Config. See WZC
- WLAN 49
- WPA 25, 26, 49
- WZC 12
 - using to configure security 26