ThinkVantage Access Connections 4.1

User's Guide

ThinkVantage Access Connections 4.1

User's Guide

Note: Before using this information and the product it supports, read the general information in Appendix D, “Notices,” on page 81.

First Edition (January 2006)

Contents

Figures

About this book

This book provides information about using ThinkVantage® Access Connections v.4.1.

How this book is organized

Chapter 1, “Introducing Access Connections,” on page 1 contains an overview of the Access Connections application and its features.

Chapter 2, “Using location profiles,” on page 3 contains instructions for creating profiles and making a network connection.

Chapter 3, “Configuration options,” on page 55 contains instructions for configuring various options.

Chapter 4, “Using a wireless WAN connection,” on page 63 contains instructions for using a wireless WAN connection.

Chapter 5, “Introducing a peer-to-peer connection,” on page 65 contains instructions for using a peer-to-peer connection.

Appendix A, “Frequently asked questions,” on page 73 contains answers to frequently asked questions about Access Connections.

Appendix B, “Command line interface,” on page 77 contains a list of commands that can be entered from the command line.

Appendix C, “Getting help and technical assistance,” on page 79 contains information about accessing ThinkVantage Support Web sites for help and technical assistance.

Appendix D, “Notices,” on page 81 contains product notices and trademarks.

Notices used in this book

This book contains the following notices designed to highlight key information:

- **Notes:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenience or difficulty.
- **Attention:** These notices warn of possible damage to programs, devices, or data. An attention notice is placed just before an instruction or situation that might lead to damage.

Syntax conventions that are used in this book

The syntax in this book adheres to the following conventions:

- Commands are shown in lowercase letters.
- Variables are shown in italics and explained immediately afterward.
- Optional commands or variables are enclosed in brackets.
- Where you must type one of two or more parameters, the parameters are separated by vertical bars.

- Default values are underlined.
- Repeatable parameters are enclosed in braces.

ThinkVantage Access Connections resources on the World Wide Web

The following Web pages provide resources for understanding, using, and troubleshooting Access Connections and other systems-management tools.

ThinkVantage Access Connections home page
http://www.pc.ibm.com/us/think/thinkvantagetech/accessconnections.html

Go to this Web page to download the latest Access Connections software and documentation.

ThinkVantage Personal Computing Support - ThinkVantage Technologies page
http://www.pc.ibm.com/us/think/thinkvantagetech.html

Consult this Web page for information about ThinkVantage Technologies.

ThinkVantage Personal Computing Support page
http://www.lenovo.com/think/support

Go to this Web page for access to the ThinkVantage Personal Computing Support Web site.

Chapter 1. Introducing Access Connections

Access Connections is a connectivity assistant program for your ThinkPad® computer that enables you to create and manage location profiles. Each location profile stores all of the network and Internet configuration settings that are needed to connect to a network infrastructure from a specific location such as home or work. The location profile also enables users to specify different default printers, default home pages for Internet Explorer and the Firefox Browser, security settings for specific locations, and to start different applications automatically in different locations.

By switching between location profiles, when moving their computers from place to place, users can quickly and easily connect to a network without having to manually reconfigure settings or restart the computer each time. Access Connections also enables the user to view and connect to Bluetooth devices, and to set Bluetooth security options. It enables users to switch network and Internet settings quickly by selecting a location profile.

The network connection can be made using a modem, a wired network adapter (Ethernet), a broadband device (Digital Subscriber Line (DSL), cable modem, or Integrated Services Digital Network (ISDN), satellite connection devices, a wireless LAN or a wireless WAN adapter. Virtual Private Networking (VPN) connections are also supported.

System requirements

Before installing Access Connections, you must consider where it will be installed and what network profiles you will want to create. The following is a list of system considerations and limitations that must be considered before installing Access Connections.

Supported operating systems

Operating systems supported:

- Windows 2000
- Windows XP

Access Connections is language-independent, that is can be used with any language operating system.

New features in Access Connections v.4.1

Access Connections v.4.1 includes the following new features and improvements:

- Peer-to-peer connection
- Support for Sierra Wireless 1xEV-DO Network Adapter for Verizon Wireless WAN service
- Support for Vodafone HSDPA/WCDMA Communication Manager software.

  Note: For WAN connection service, Access Connections provides an integration with WAN communication software developed by Vodafone. You can specify in the WAN profile that this application software is to be launched.
- Support for Firefox Internet browser
- New Mini-PCI cards supported

– Intel Pro/Wireless 3945 ABG Wireless LAN adapter
– Broadcomm 4318/4311 Wireless LAN Adapter

  Notes on use of Access Connections when using Broadcomm 4318/4311 Wireless LAN adapter:

  1. Limited support is offered on Windows XP. For access to it, enable Windows Zero Configuration Service.
  2. Find Wireless Network and Peer to Peer Community features are not supported.
  3. To configure wireless connection go to the Windows XP wireless network setup menu.
  4. Access Connections v.4.1 supports only wireless radio control and signal status display.

• Updated easy-to-use graphic user interface

Updating Access Connections

Access Connections can check whether a version later than the one you have is offered on the support web site. If updated version is available, Access Connections will download and install it automatically. To enable this feature, go to the main tool bar and select **Help**. On the pop-up menu click **Check for Updates**.

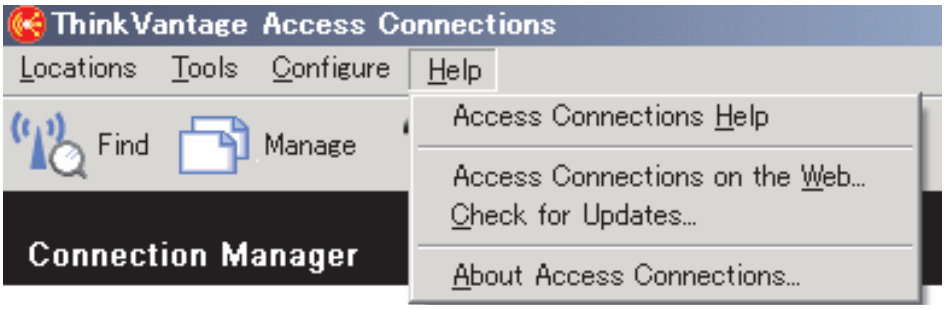

Figure 1. Updating Access Connections

Chapter 2. Using location profiles

ThinkVantage Access Connections is a software utility that manages your network connectivity at multiple locations through location profiles. A location profile stores the network configuration required to connect to a desired network, along with location-specific settings such as your browser home page, proxy configuration, firewall status, file and printer sharing, and default printer. By switching between location profiles as you move your computer from place to place, Access Connections can quickly and easily connect to a network with no need for you to reconfigure network settings manually.

Creating a location profile

A location profile defines all of the settings required to establish a connection to a given network, along with other settings that are location-specific, such as the default printer and the browser settings. Access Connections provides a profile wizard that helps you create location profiles for networks of different types.

To create a new location profile, do the following:

1. Start Access Connections. If this is your first time to access Access Connections, the Welcome to Access Connections window is displayed.

Figure 2. Welcome to Access Connections window

To display more details about the copyright statement, press **More Information**.

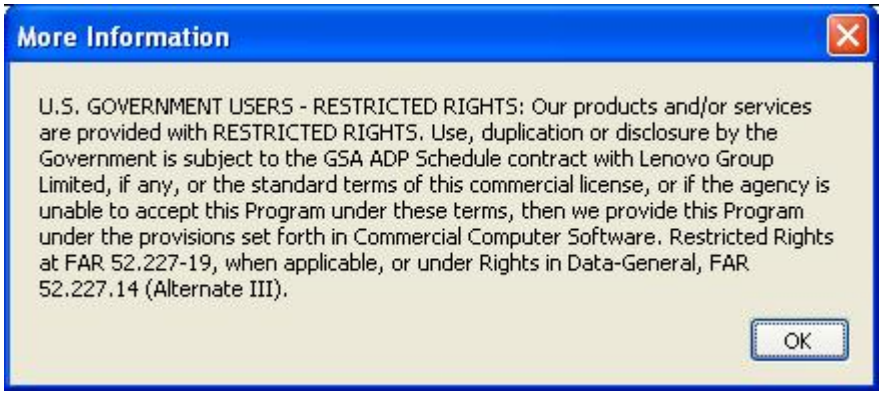

Figure 3. More Information window

2. Press **OK**. The main window opens.

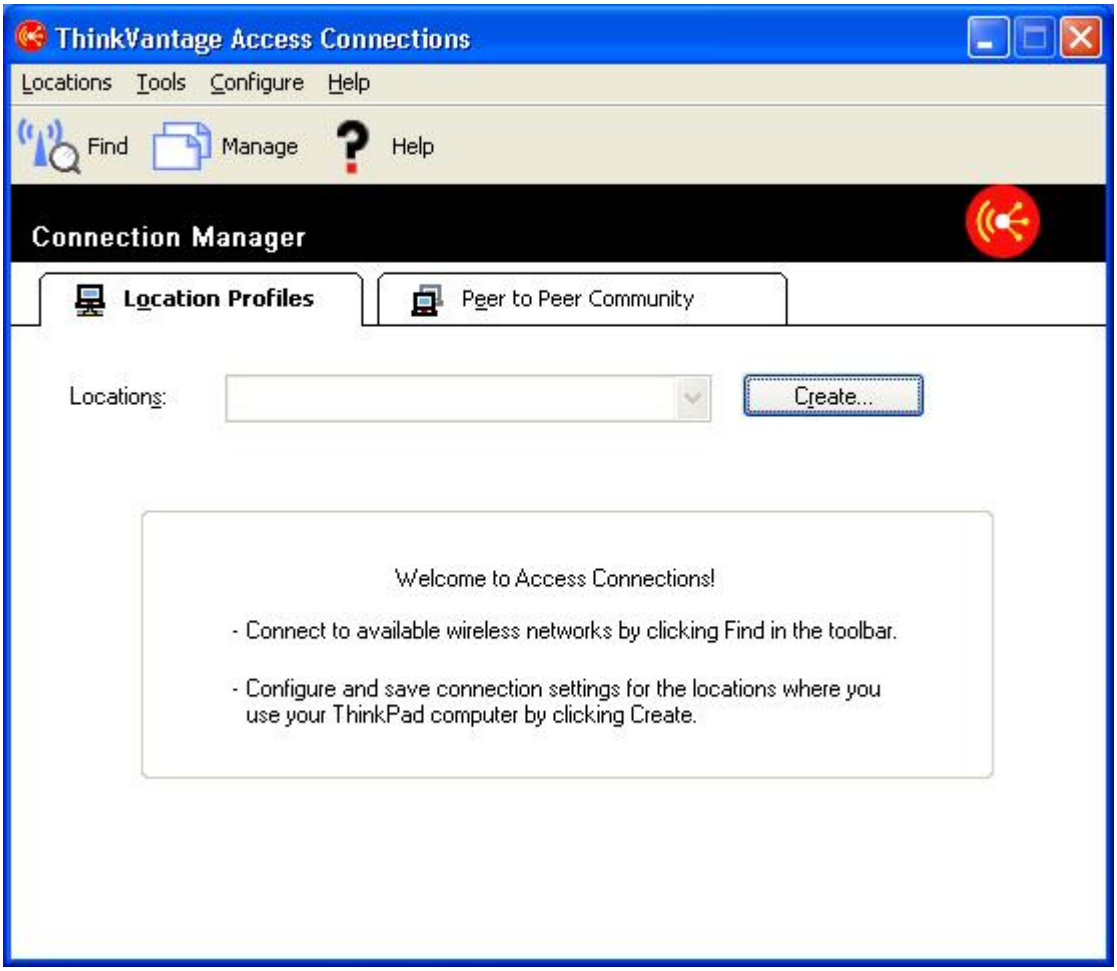

Figure 4. Access Connections main window—main menu

3. On the toolbar, click **Locations**.

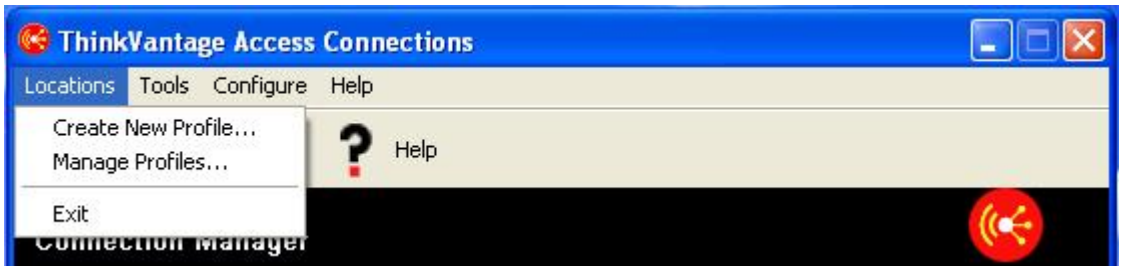

Figure 5. Main menu—Locations

On the popup, click **Create New Profile**. The profile wizard starts.

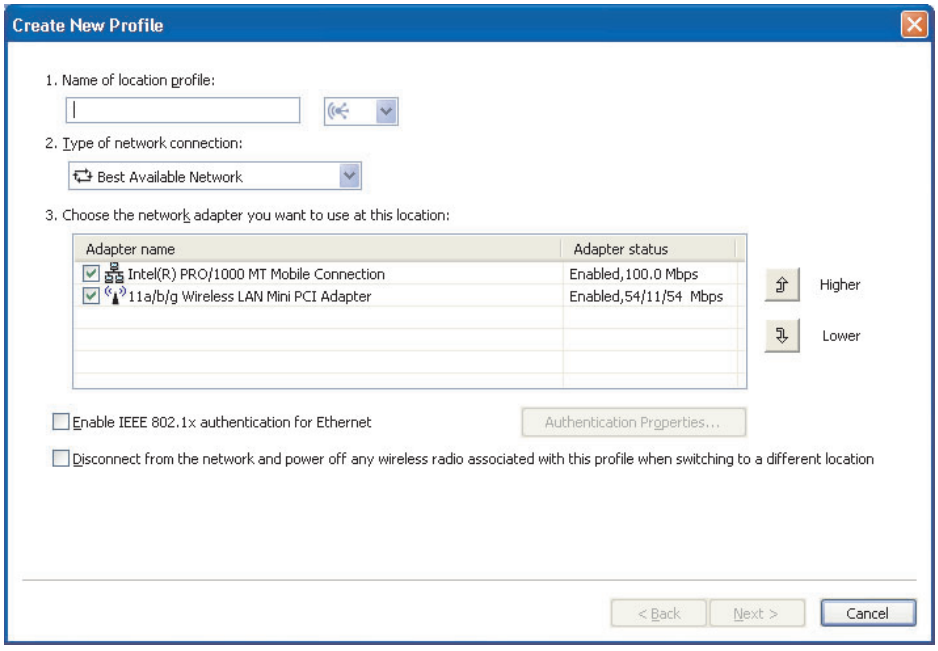

Figure 6. Profile wizard window

4. Insert the profile name. It may be the physical location of the network or any other easily recognizable name.

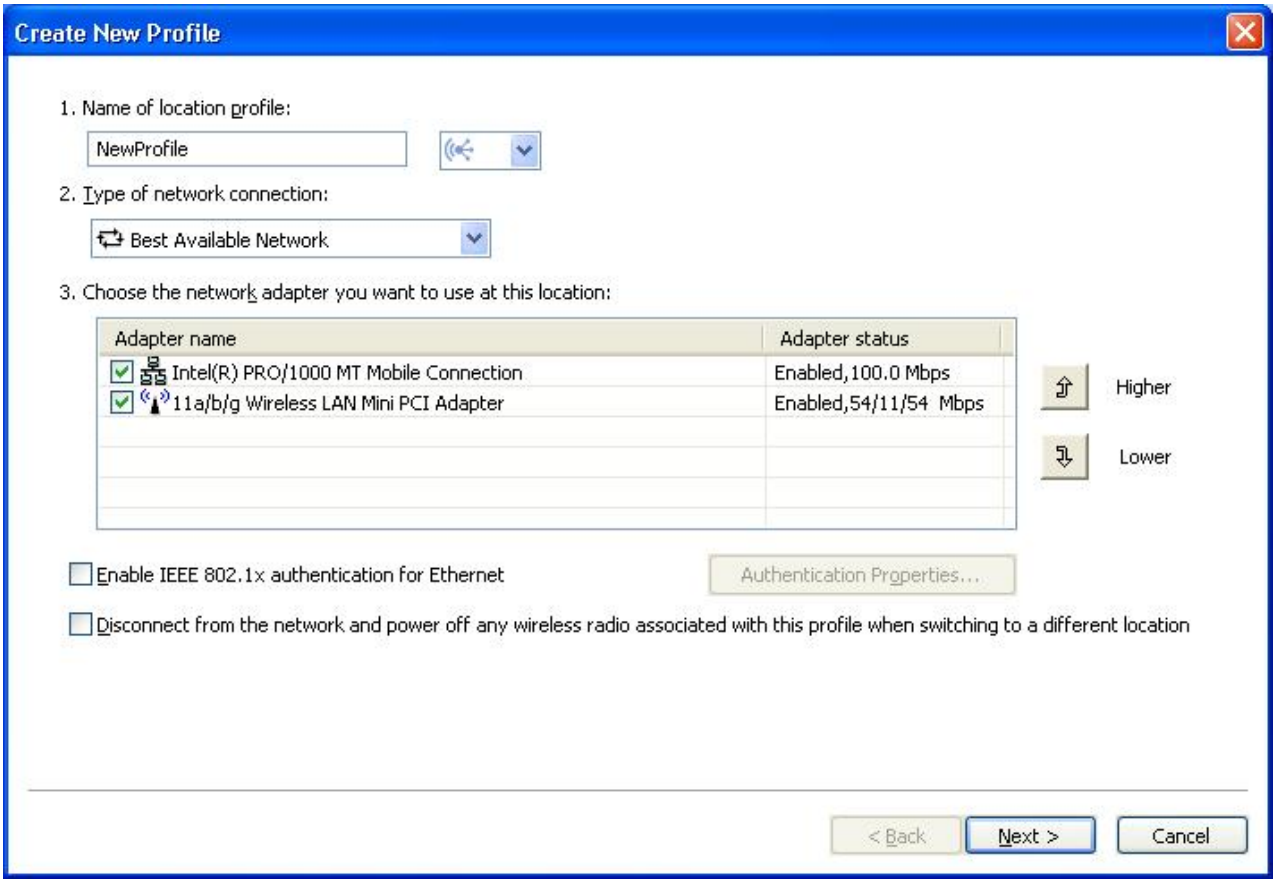

Figure 7. Profile wizard—Insert Profile Name

For any profile created, you can also select one of the location icons that Access Connections provides for home, office, airport, hotspot, hotel , train, or meeting area.

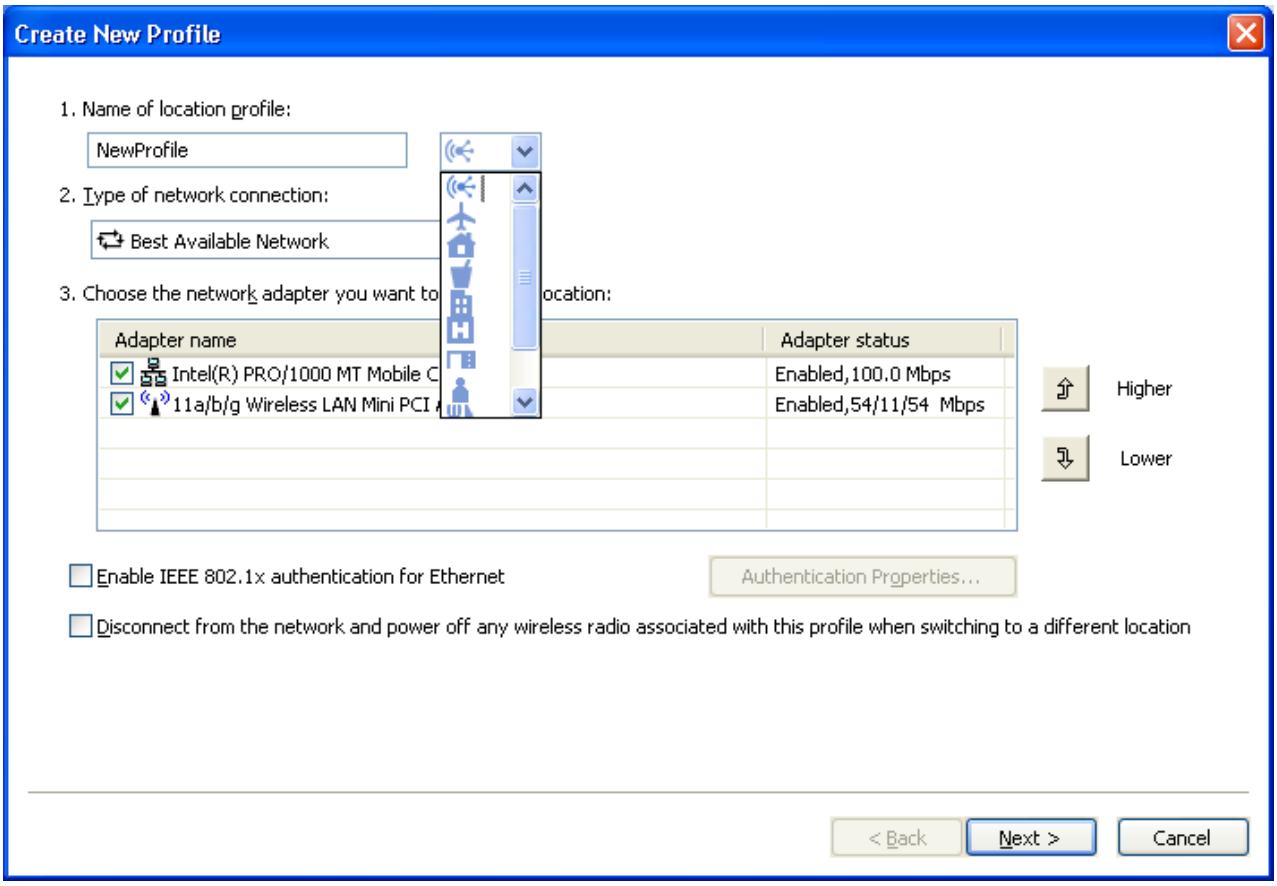

Figure 8. Pull-down menu for Location icon

5. Select the type of network connection. You can select any of the types listed on the screen below:

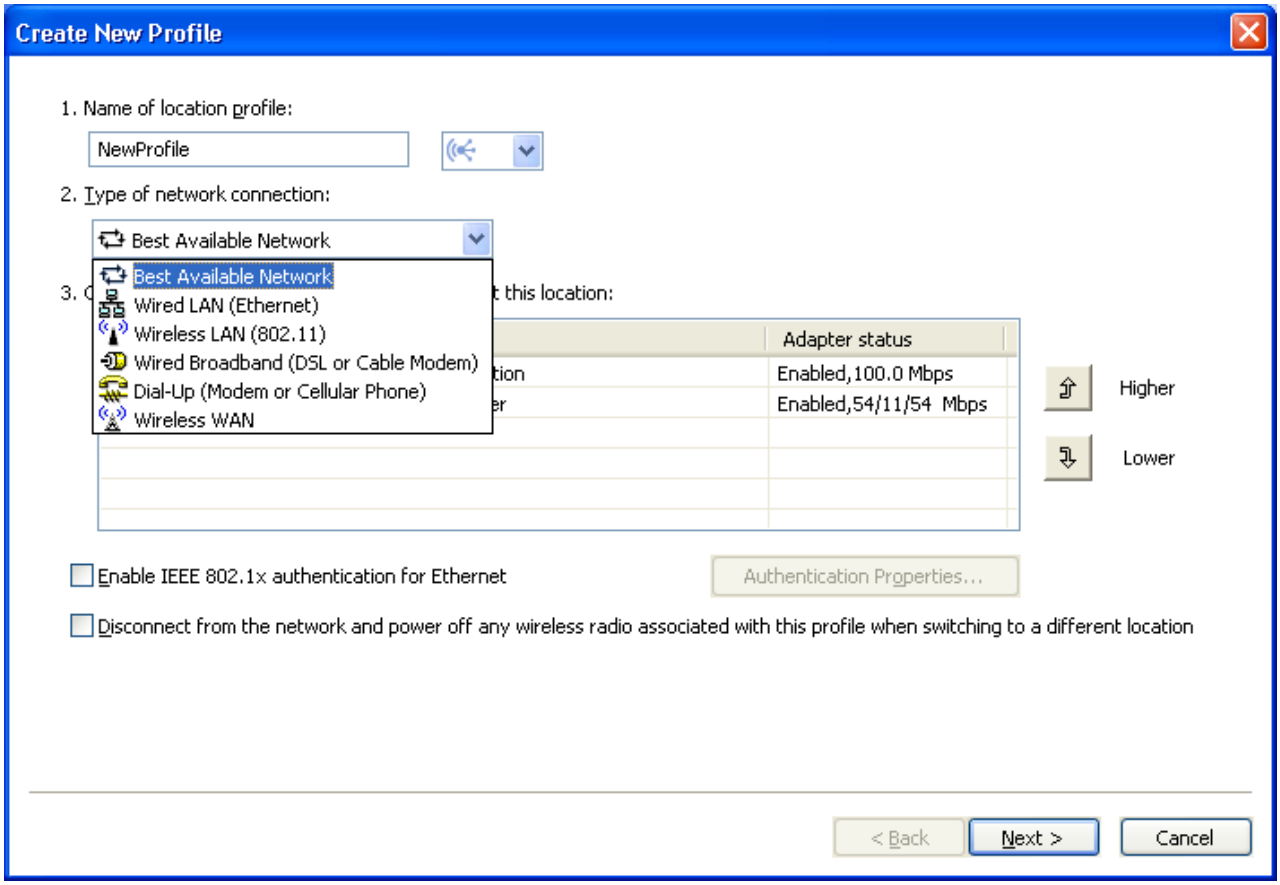

Figure 9. Pull-down menu for the type of network connection

Best Available Network

Choose this type of network connection to create a profile that will automatically select either a wired Ethernet network or a wireless 802.11 networks at the same location. This capability is useful when you move frequently within a location - for instance, between a wired connection at your desk and a wireless LAN connection elsewhere in the same building. Access Connections will automatically determine which adapters in your computer support this type of network connection, and show them in the table. Choose all of the adapters you want to use. When more than one network adapter has access to a network at this location, Access Connections will attempt to connect, using the adapter highest in the list first. To change the priorities for connections, select an adapter from the table and then click **Higher** or **Lower**.

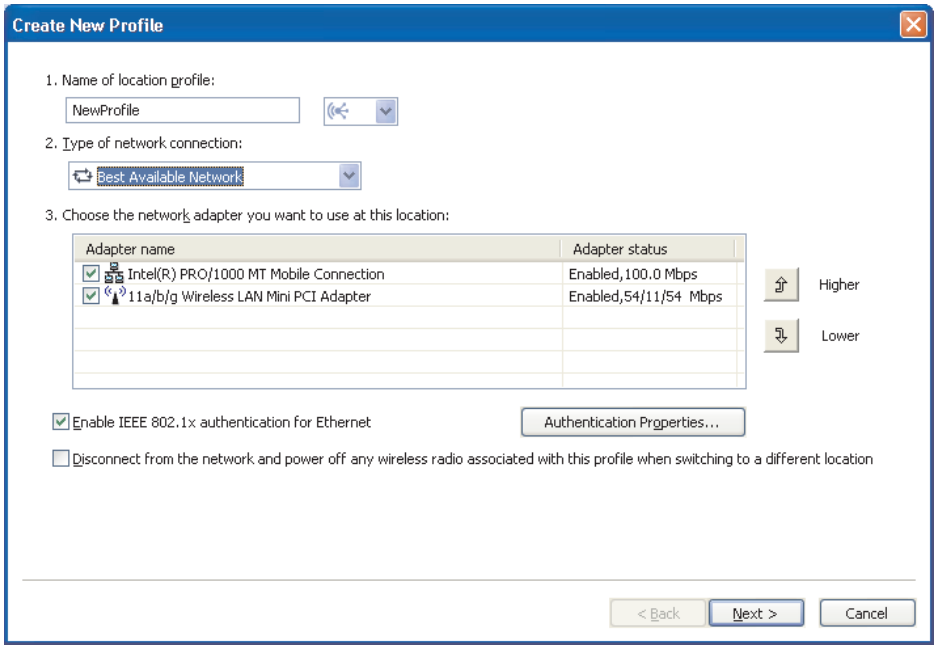

Figure 10. Create New Profile - Best Available Network

Wired LAN (Ethernet)

Choose this type of network connection if the profile will be used only to connect to a Wired LAN (Ethernet). Access Connections will automatically determine which adapters in your computer support this type of network connection, and show them in the table.

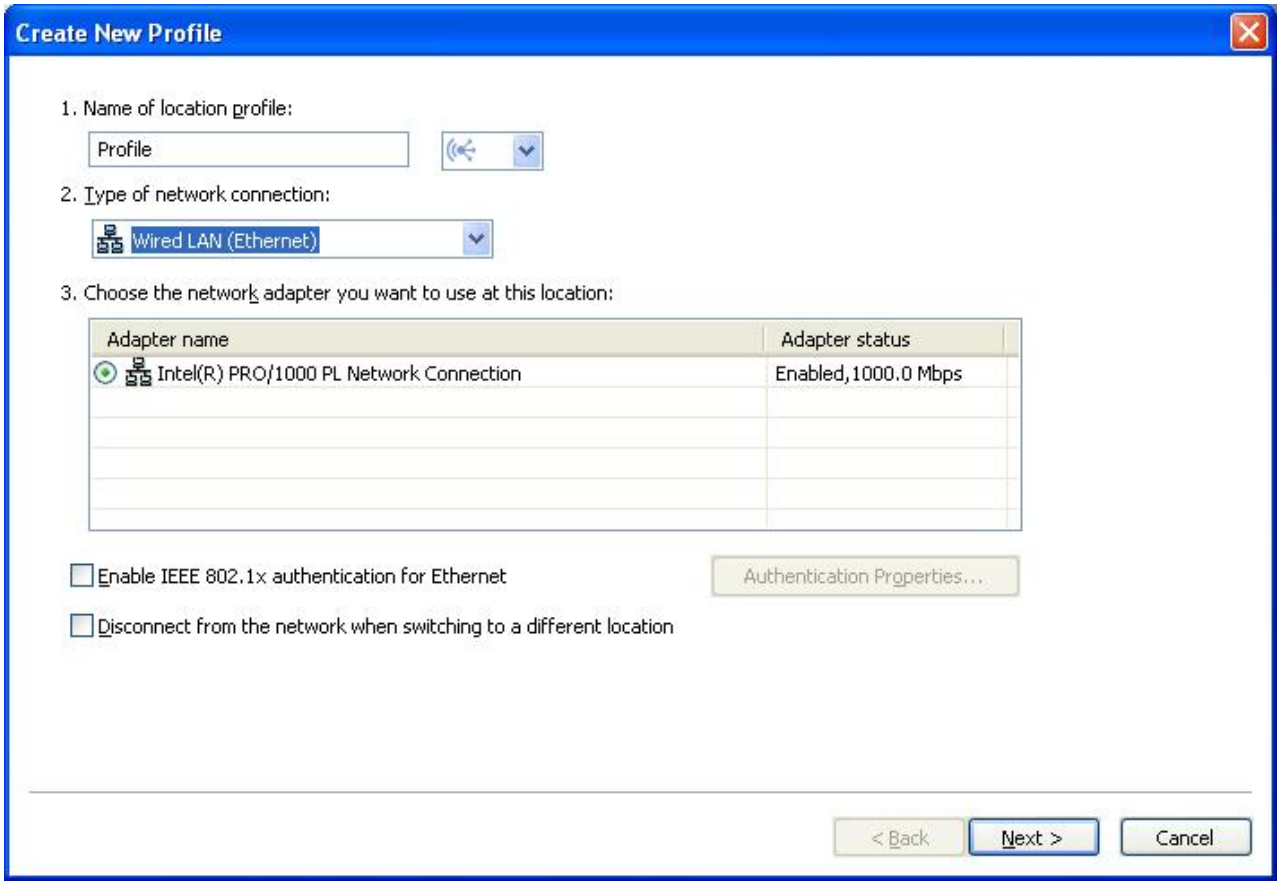

Figure 11. Create New Profile—Wired LAN (Ethernet)

Wireless LAN (802.11)

Choose this type of network connection if the profile will be used to connect to an 802.11 a, b, or g wireless LAN only. Access Connections will automatically determine which adapters in your computer support this type of network connection, and show them in the table. You can configure the settings for authentication and encryption.

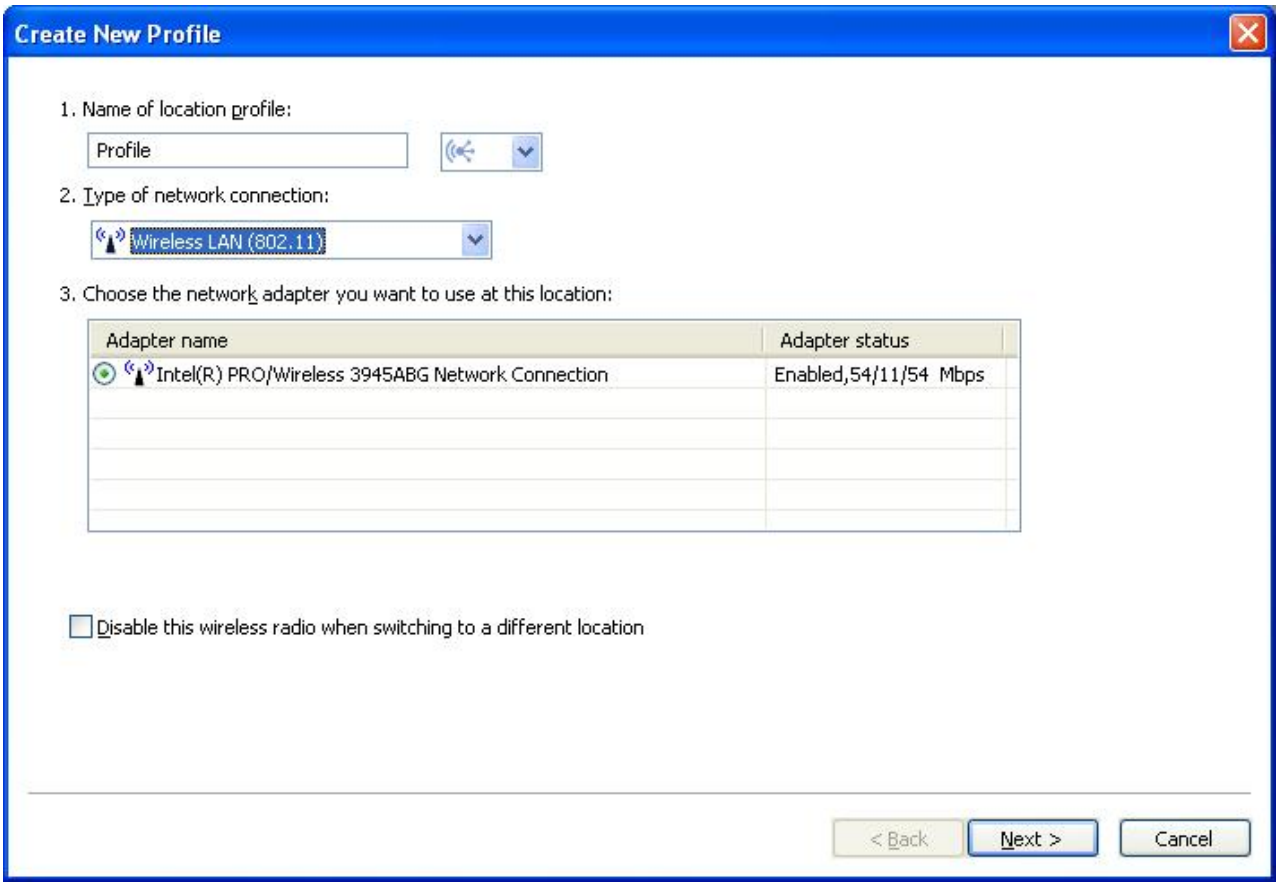

Figure 12. Create New Profile—Wireless LAN (802.11)

Wired Broadband (DSL or Cable Modem)

Choose this type of network connection if the profile will be used only to connect to wired broadband. The broadband connections are DSL, cable modem, and ISDN. Typically, your computer will connect to the broadband network through an Ethernet adapter. Access Connections will automatically determine which adapters in your computer support this type of network connection, and show them in the table. Choose the one you want to use. If your broadband connection is DSL, you also must select **Configure my DSL settings**.

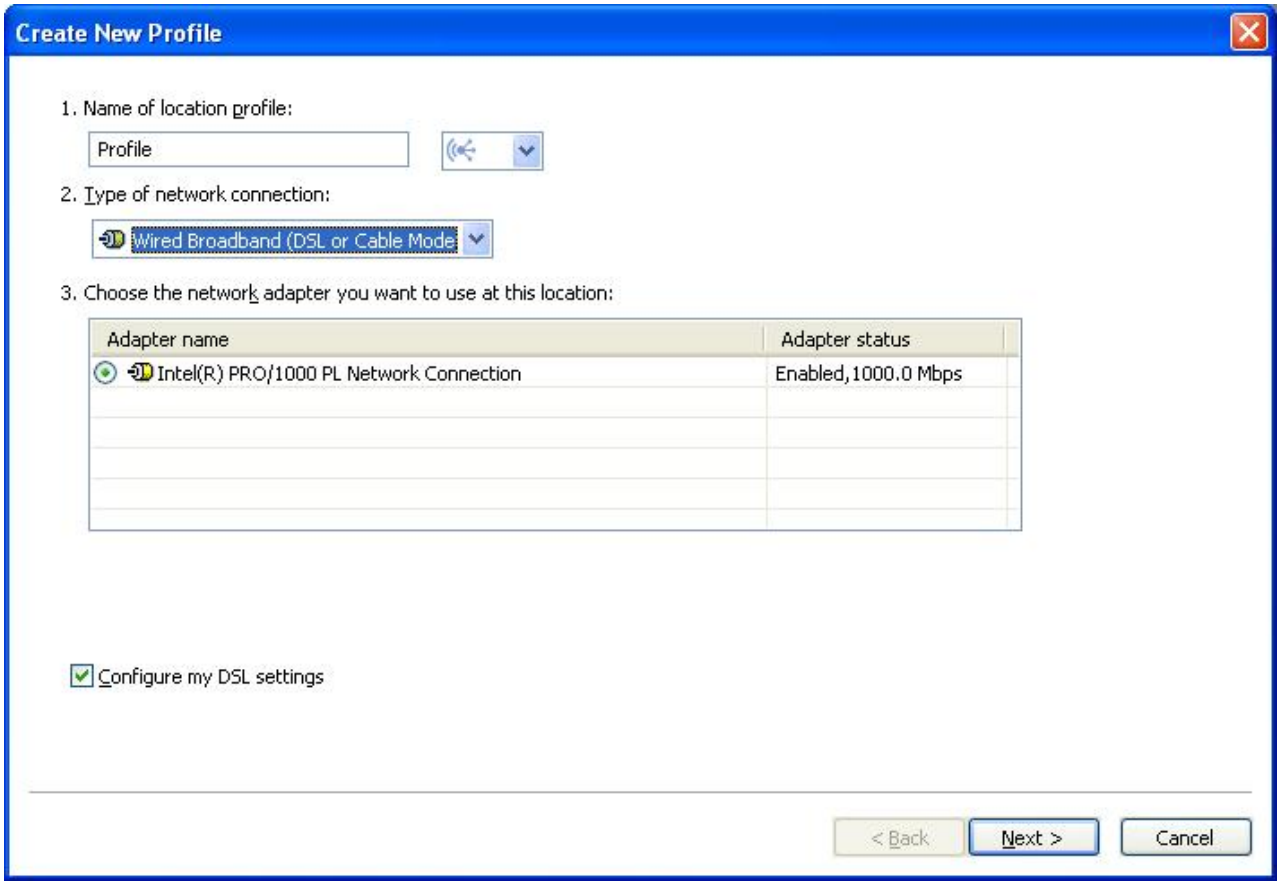

Figure 13. Create New Profile—Wired Broadband (DSL or Cable Modem)

Dial-up (modem or cellular phone)

Choose this type of network connection if the profile will be used only to connect to dial-up. Examples of dial-up connections are a standard modem attached to a telephone line, and a Bluetooth modem wirelessly connected to a cellular phone. Access Connections will automatically determine which adapters in your computer support this type of network connection, and show them in the table.

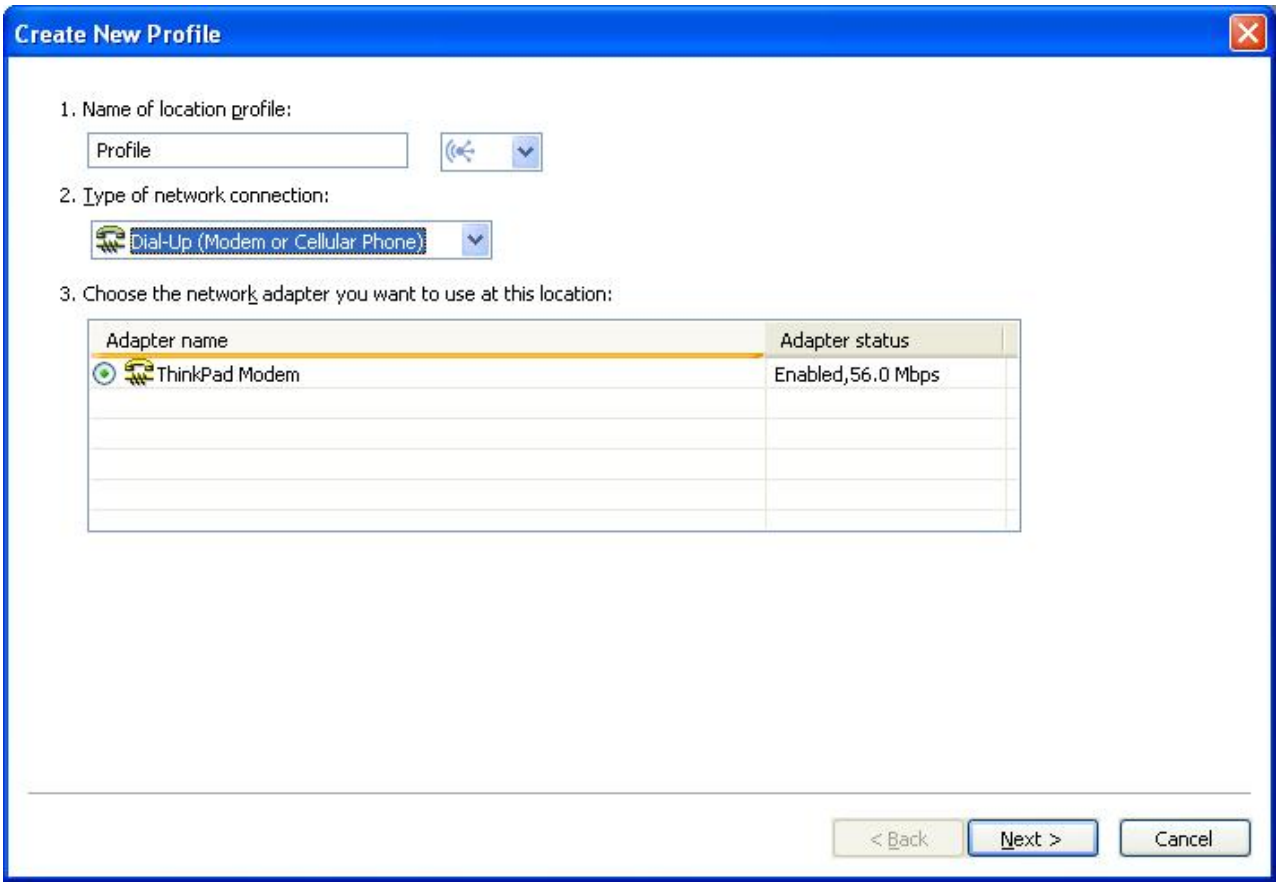

Figure 14. Creating New Profile—Dial-up (modem or cellular phone)

Wireless WAN

Choose this type of network connection if the profile will be used only to connect to a wireless WAN (wide area network). Wireless WAN connections require a service subscription to connect successfully. Access Connections will automatically determine which adapters in your computer support this type of network connection, and show them in the table. Choose the one you want to use.

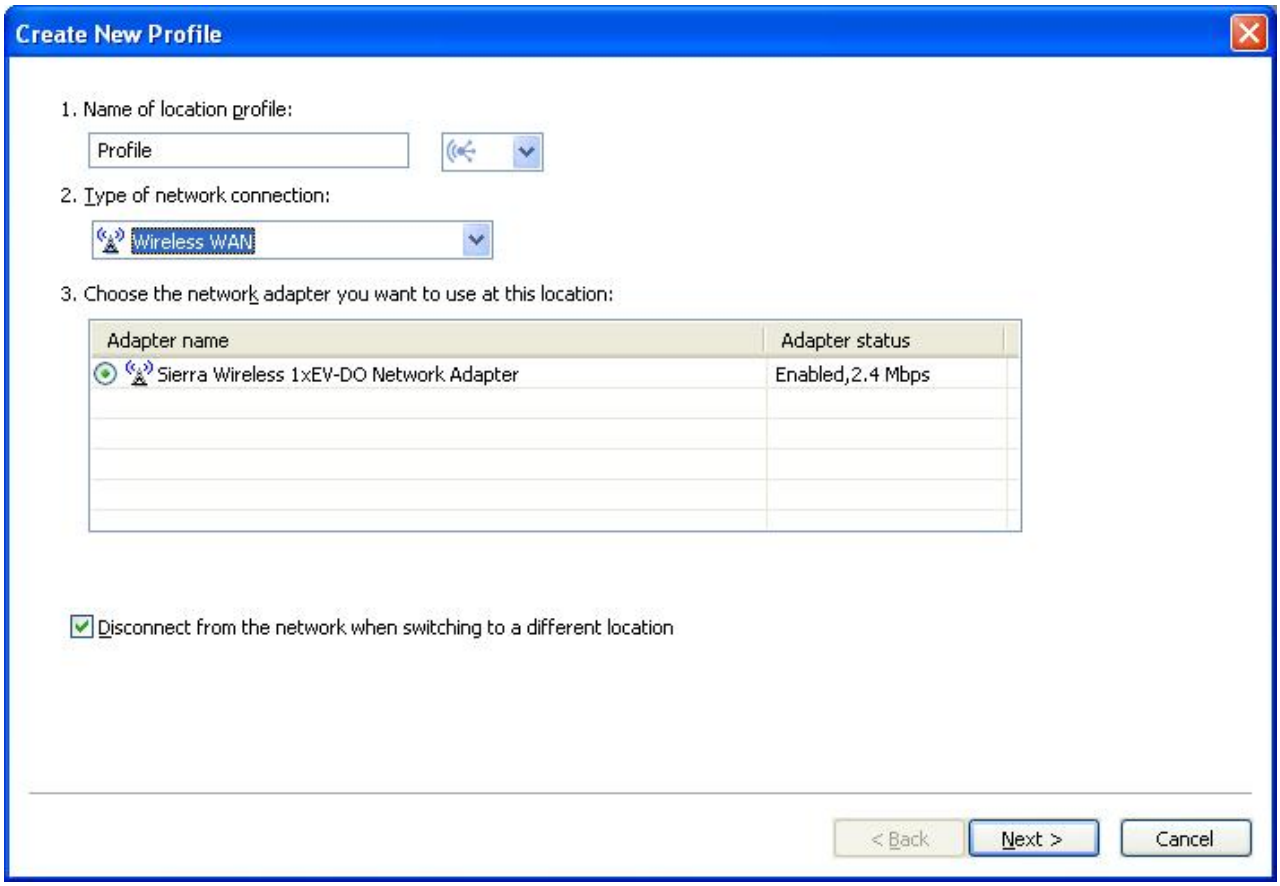

Figure 15. Creating New Profile—Wireless WAN

6. If you selected **Best Available Network** in step 5 on page 8, you can enable optional IEEE 802.1x authentication (EAP over LAN). Do as follows:
   a. Select **Enable IEEE 802.1x authentication for Ethernet**.

b. Click **Authentication Properties**; then enter the authentication settings provided by your network administrator.

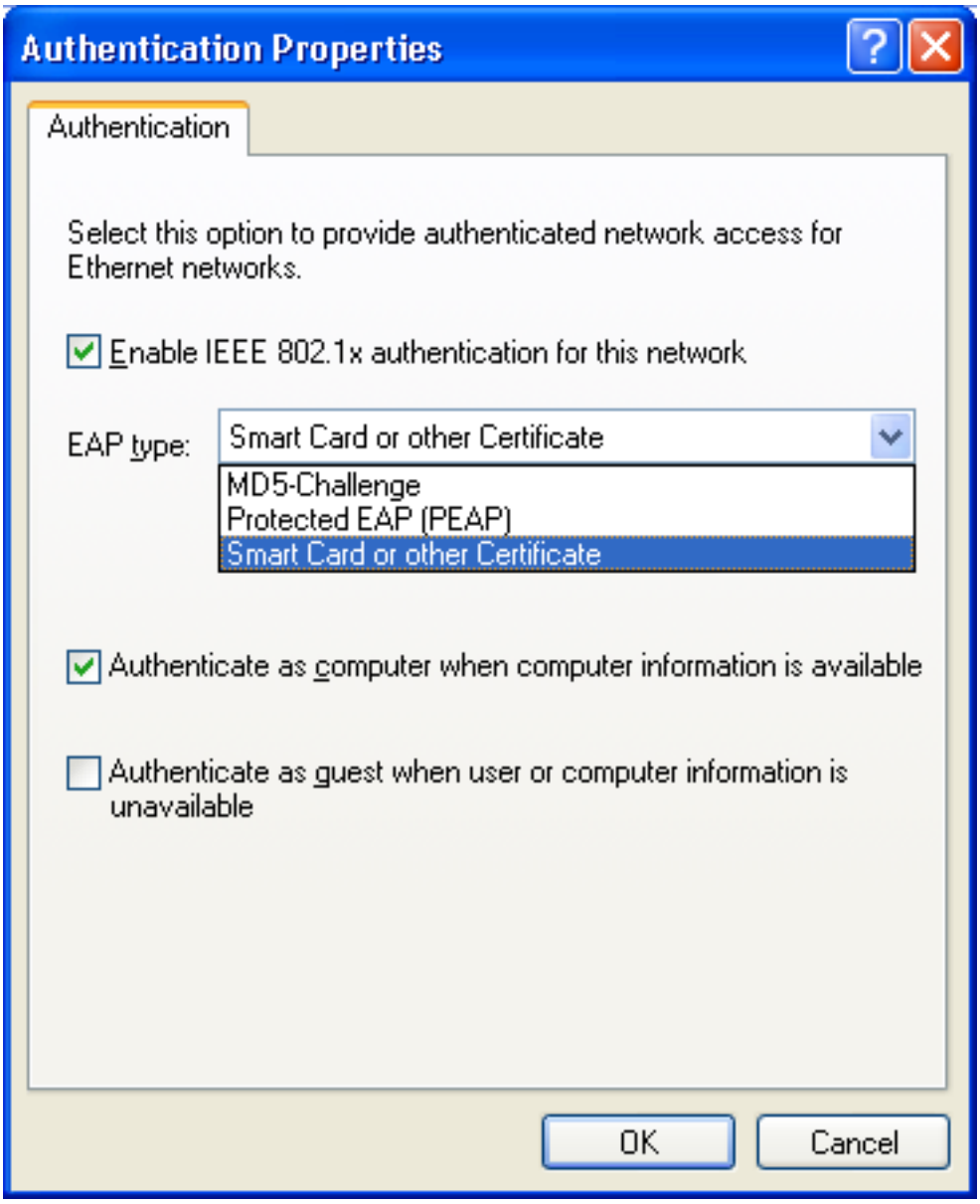

Figure 16. Authentication Properties window

c. Click **OK**.

7. You can prevent multiple simultaneous connections, and thus conserve battery life, by selecting **Disconnect from the network and power off any wireless radio associated with this profile when switching to a different location**.
8. Click **Next**.
9. Enter your wireless network configuration; then click **Next**.
10. Go to step 38 on page 25.
11. If you selected **Wired LAN (Ethernet)** in step 5 on page 8, you can enable IEEE 802.1x authentication for the wired network (EAPoL). Do as follows:
    a. Select **Enable IEEE 802.1x authentication for Ethernet**.

b. Click **Authentication Properties**; then enter the authentication settings provided by your network administrator.

c. Click **OK**.

12. To disconnect from the network when you switch to a different location profile, select **Disconnect from the network when switching to a different location**.
13. Click **Next**.
14. Go to step 38 on page 25.
15. If you selected **Wireless LAN (802.11)** in step 5 on page 8, you can conserve battery life by preventing multiple simultaneous connections. To do this, select **Disable this wireless radio when switching to a different location**.
16. Click **Next**. The wireless network configuration window appears.

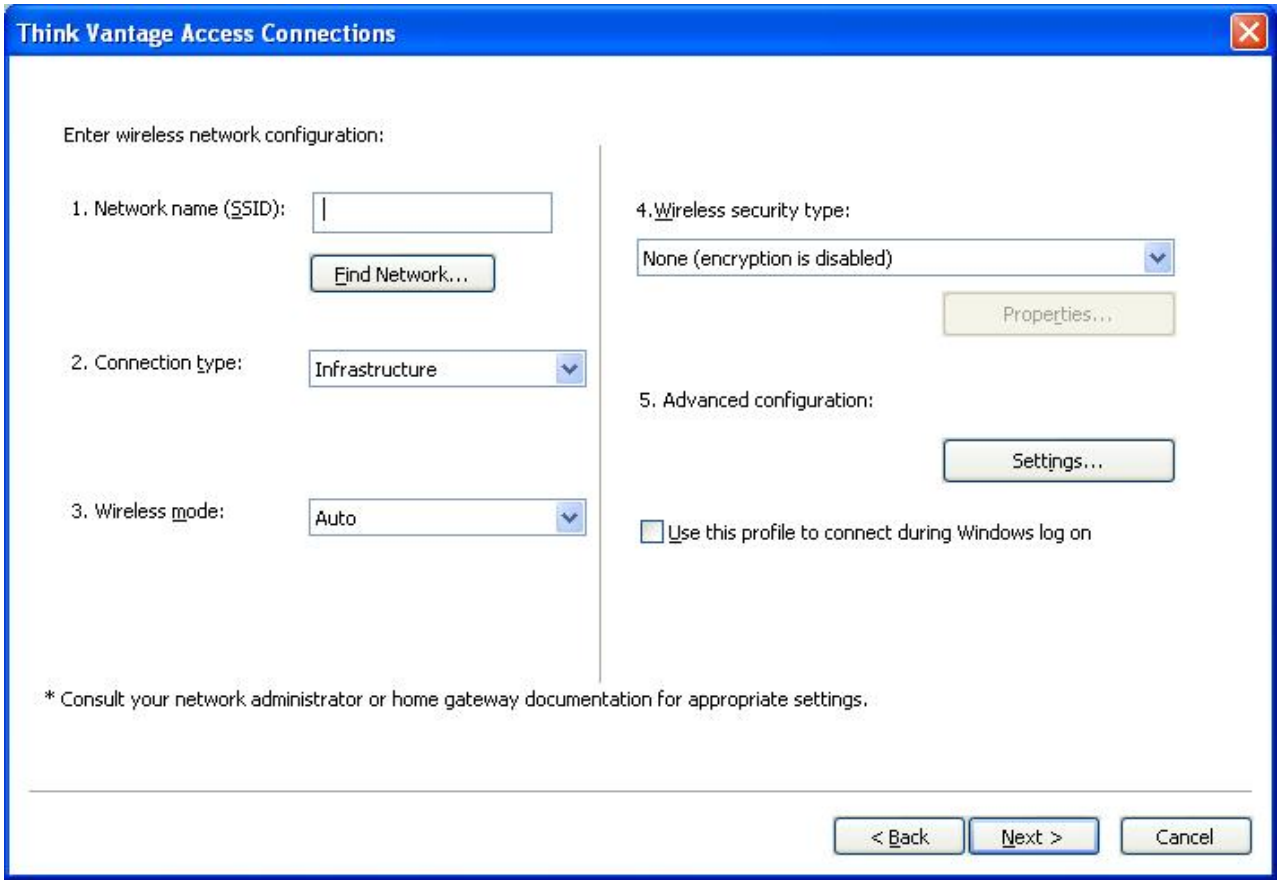

Figure 17. Wireless network configuration window

17. Enter the name of the wireless network to which you are attempting to connect. (The network name is also known as the SSID.) To scan for wireless networks within range of your computer and display the names of those being broadcasted by access points, click **Find Network**. To connect to any available non-secured (open) wireless network that is in range, leave the SSID field blank. For more information about connecting to a wireless network, see “Connecting to a wireless network” on page 45.

18. Next, select the connection type. Two types are available:

    Infrastructure
    Use this connection type when your computer will be communicating with wireless access points.

    Adhoc
    Use this connection type to communicate directly with another computer without connecting to a wireless access point first.

19. Select either **Auto**, **802.11b**, **802.11g** or **802.11a** for **Wireless Mode**. This setting is available only if the installed adapter is compatible with different standards. If you select **Auto**, the adapter will automatically run in the mode that is compatible with in-range access points. If you set the same mode as on the in-range access point, the connection will be established faster.

20. Select one of the wireless security types, listed in the figure:

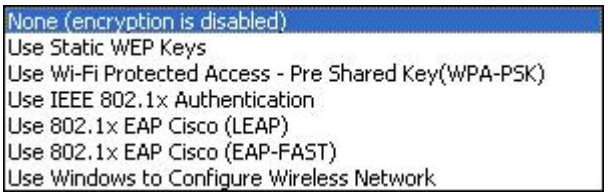

Figure 18. Wireless security types

None (encryption is disabled)
Select this option when connecting to non-secured (open) wireless networks such as public hotspots. Optionally, you can establish a wireless LAN connection before logging on to Windows. To do so, select **Use this profile to connect during Windows logon**.

Use Static WEP Keys
A wireless network that implements this type of security uses predefined alphanumeric or hexadecimal strings (keys) in encrypting and decrypting data that is transmitted and received through the wireless network. Usually, you enter these keys only once. They are then automatically associated with your wireless adapter each time the adapter is inserted or your computer is started. Optionally, if you want to use this profile to establish a wireless LAN connection before logging on to Windows, select **Use this profile to connect during Windows logon**.

Use Wi-Fi Protected Access - Pre-Shared Key (WPA-PSK)
Wireless networks that implement this type of security require users to authenticate with a Pre-Shared Key. Data transmitted and received through the wireless network can be encrypted and decrypted by use of WEP or TKIP data encryption. Optionally, if you want to establish a wireless LAN connection before logging on to Windows, select **Use this profile to connect during Windows logon**.

Use IEEEE 802.1x Authentication
Wireless networks that implement IEEE 802.1x Extensible Authentication Protocol (EAP) security require each user to authenticate his or her identity with a username and password or a certificate credential before being allowed to connect. Data is encrypted and decrypted by use of either static or dynamic WEP keys. Dynamic keys are session-based and are generated each time an authentication attempt is made.

Use 802.1x - EAP Cisco (LEAP)

This version of EAP is available only when a Cisco or Cisco-compatible wireless adapter is installed in your system. It uses authentication and dynamic encryption keys to secure the wireless network.

Use 802.1x - EAP Cisco (EAP-FAST)

This version of EAP is available only when a Cisco or Cisco-compatible wireless adapter is installed in your system. It is an improved version of 802.1x EAP Cisco (LEAP). It uses Protected Access Credentials (PAC) and users' credentials to secure the wireless network.

Use Windows to configure wireless network

Choose this option to have the Windows Zero configuration service manage this wireless connection. The settings for configuring security for this wireless connection will be managed by Windows, and cannot be exported by Access Connections.

For more information about each of the wireless security types, see “Wireless security settings” on page 28.

21. Click **Properties**; then enter the additional settings for your selected security type. These settings are usually provided by your network administrator.
22. To configure radio power management, quality of service, transmitting power level, 802.11b preamble, and preferred access points, click **Settings** in the Advanced Configuration section. This invokes the Advanced Wireless Settings window.

Figure 19. Advanced Wireless Settings window

The following settings are available:

Transmit Power Level
Choose a transmitting power level, from the minimum 10%, to the maximum, 100%. Use it to transmit at the lower level. The value is set automatically in response to a notice from the access point.

802.11b Preamble
The default setting is **Short&long**. This setting is included for compatibility with the old access points, which do not accept a long preamble.

Enable QoS
Select this check box if you need to set the priority when transmitting data such as video stream.

Power save mode
You can adjust the power saving mode in three stages. The mode can be set for each location profile.

Preferred Access Point MAC Addresses
If you specify a MAC address for the access point, the connection will be made only to that address. If you do not specify a MAC address, the system will find an SSID automatically and connect to that SSID.

Contact your network administrator for the appropriate settings.

23. Click **Next**.
24. Go to step 38 on page 25.
25. If you selected **Wired Broadband (DSL or Cable Modem)** in step 5 on page 8, and your broadband connection is DSL, you must also select **Configure my DSL settings**.

26. Click **Next**. The phonebook settings page is displayed.

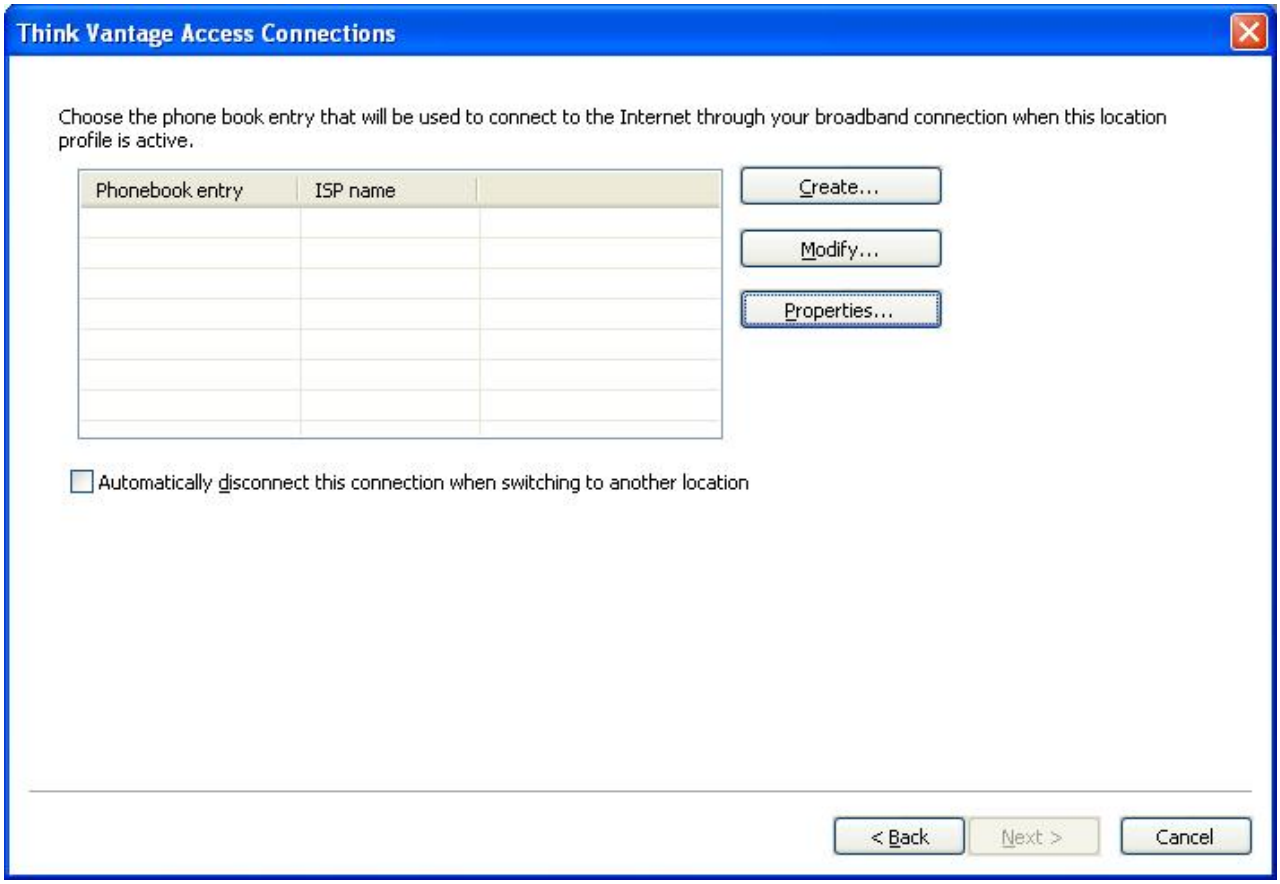

Figure 20. Phonebook settings window

27. Choose or create a phonebook entry. To enter the details of the DSL account, click **Properties**.

28. The Enter Your DSL Account Details window is displayed.

Figure 21. Enter Your DSL Account Details window

Enter the necessary information; then click **OK**.

29. Click **Next**.
30. Go to step 38 on page 25.
31. If you selected **Dial-up (Modem or Cellular Phone)** in step 5 on page 8, click **Next**.
32. For a dial-up connection, a dialer program is required.

To use a dialer application provided by your service provider, select **Find my dialer program**.

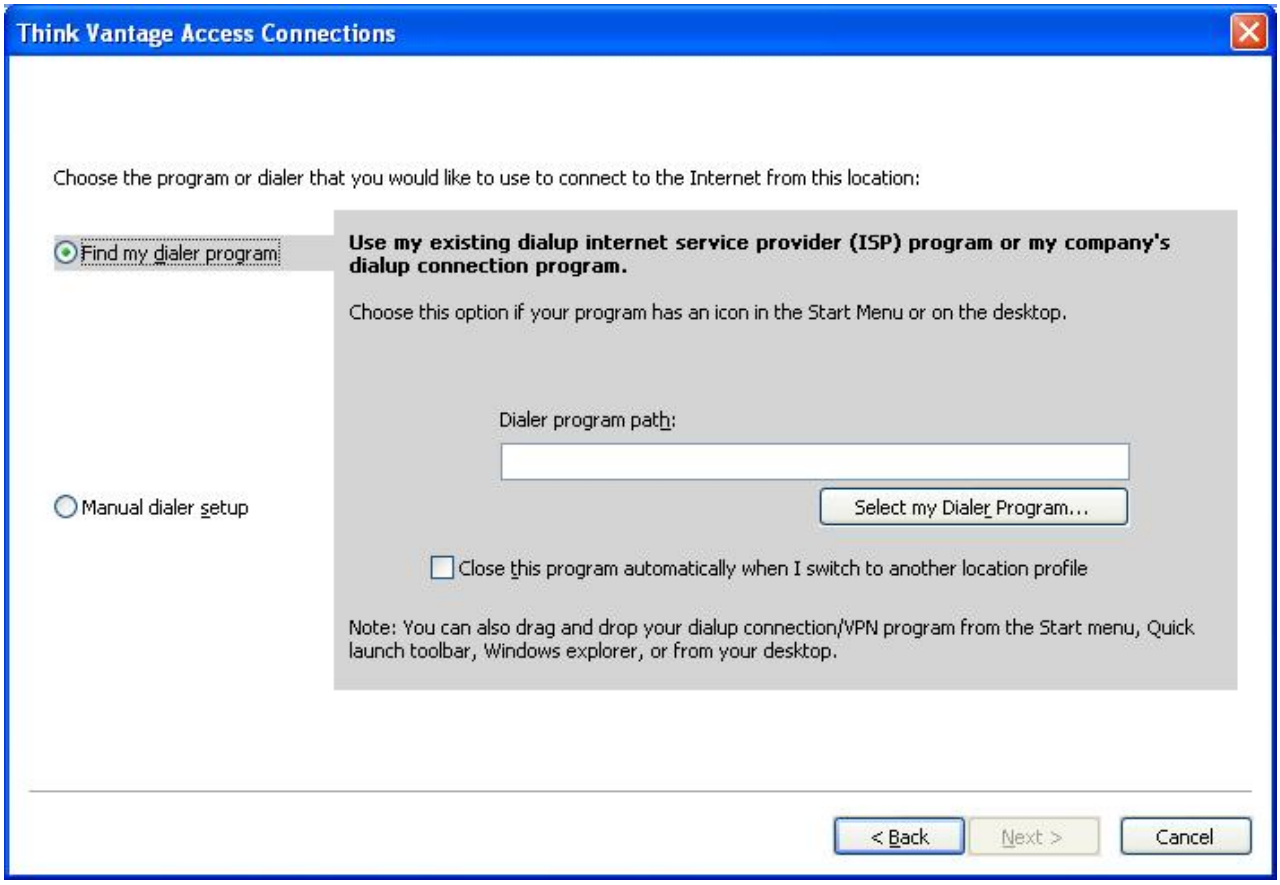

Figure 22. Find my dialer program window

Enter the path by clicking **Select my Dialer Program**.

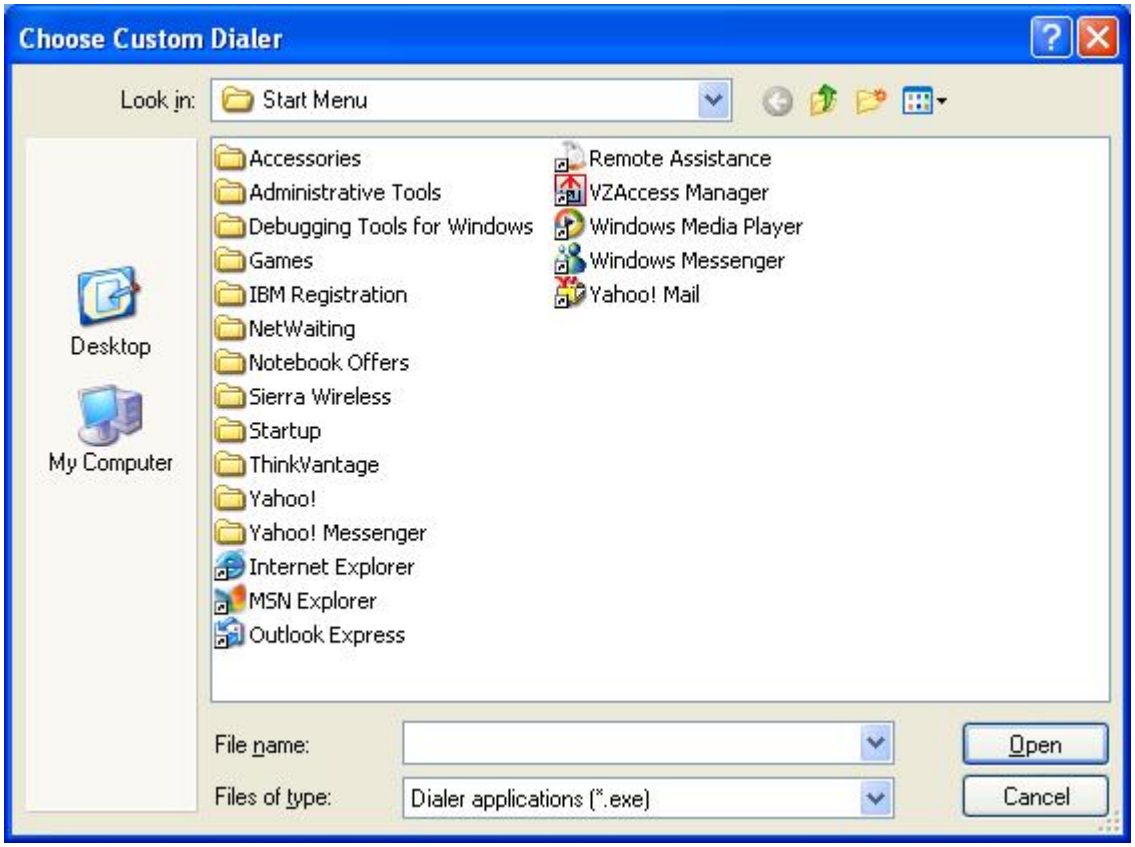

Figure 23. Choose Custom Dialer window

To use the dialer application provided by Windows, select **Manual dialer setup**. Then either select an existing phonebook entry or add a new one.

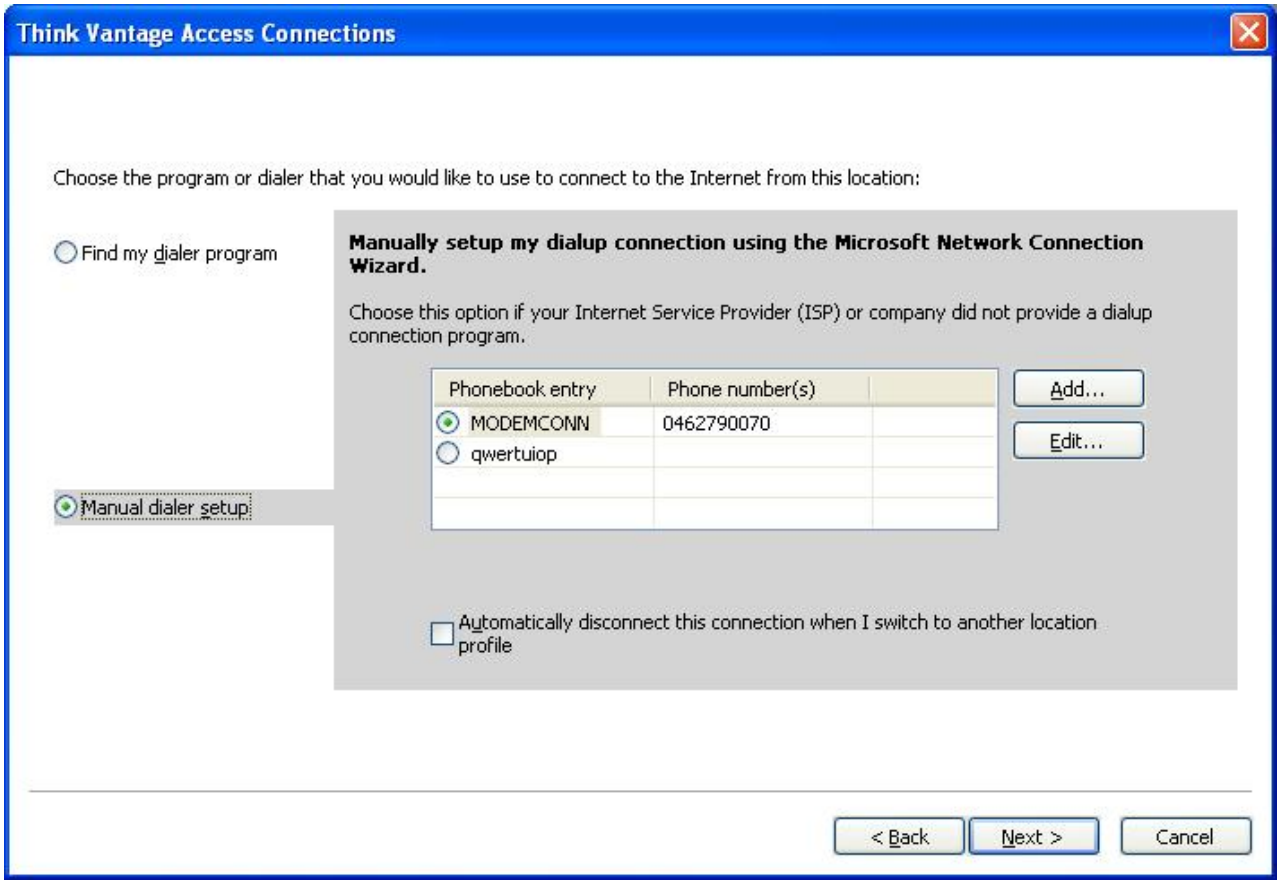

Figure 24. Manual dialer setup window

33. Click **Next**.
34. Go to step 38 on page 25.
35. If you selected **Wireless WAN** in step 5 on page 8, select the adapter from the list; then click **Next**.
36. Configure connection settings by selecting either the **Using Access Connections** option or the **Using wireless WAN client utility** option.

    If you select the **Using Access Connections** option, which is available for integrated cards, you can then choose the connection that you want to attempt, and then select advanced settings to configure your network or roaming preferences.

    If you select **Using wireless WAN client utility**, you can then browse for the utility provided by the service provider. Launch the client utility to manage the wireless WAN connection whenever you apply the profile.
37. Click **Next**.

38. The Additional settings window appears.

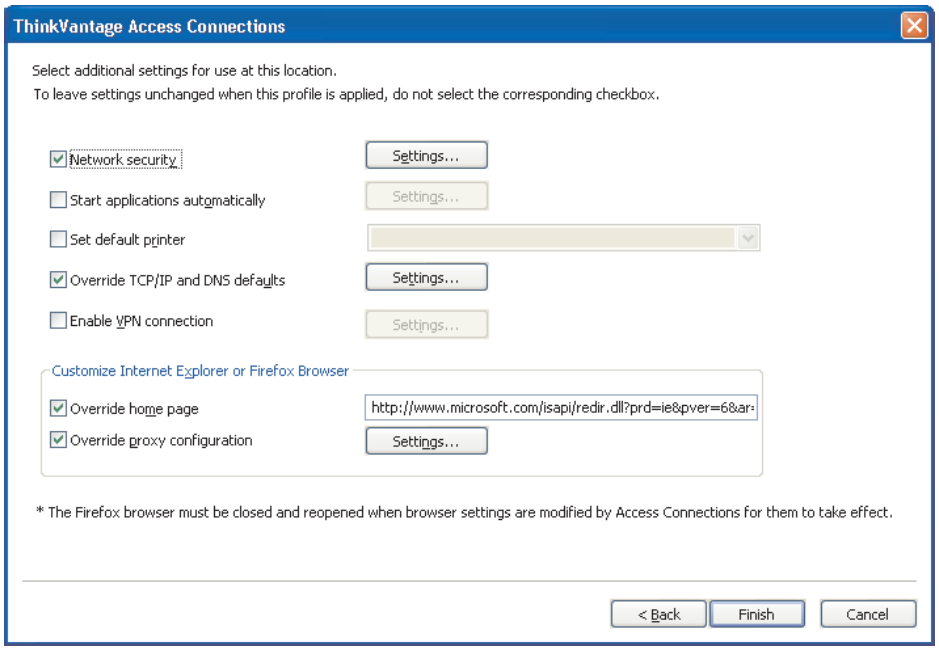

Figure 25. Additional settings window

Change the additional settings as appropriate.

39. Click **Finish**. The confirmation panel appears.
40. Click **Save**.
41. To add the newly created profile to a list of the automatically switched profiles, select **Add this location profile to the Automatic Location Switching list**. You can skip this when the profile is used for a temporary connection, such as a wireless LAN connection to the hotspot.

Additional settings

To apply additional categories of settings while the profile is active, select the category and then click the corresponding **Settings** button, or enter a value into the corresponding text field. To leave the settings for a category unchanged while this profile is active, do not select the corresponding check box.

Network Security

On the Security Settings window, select one or more of the following options:

Disable file and printer sharing
Prevents other computers on a Microsoft-based network from accessing your files and printers. This option is available only in Windows XP.

Disable Internet Connection Sharing
Prevents other computers on the local network from using your computer as a bridge to access network resources through your Internet connection.

Enable Windows firewall

Prevents unauthorized access to your computer from the network. This option is available only in Windows XP. For Windows XP Service Pack 2, this setting is selected by default. To disable the default OS setting, clear this check box. You cannot establish the VPN connection when this setting is enabled; to use the VPN connection, clear this check box.

Figure 26. Security Settings window

Start Applications Automatically

You can select programs that should be launched automatically. You can specify whether the program is to execute before or after the network connection of the profile becomes active.

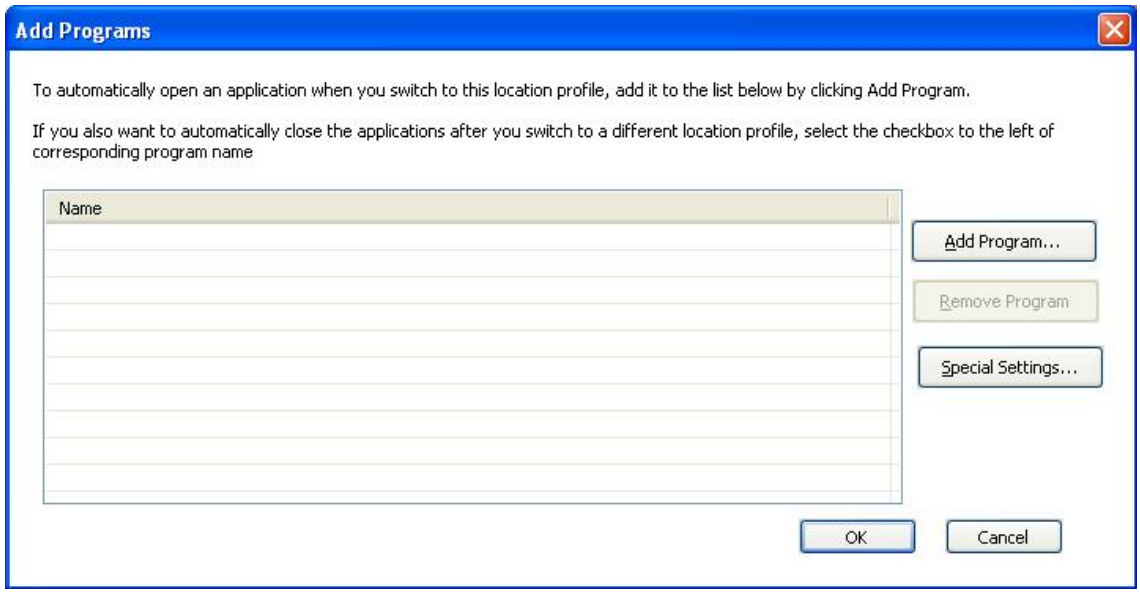

Figure 27. Add Programs window

To close the program automatically when you switch to another profile, select the check box to the left of the registered program.

To close the program automatically before connecting to a network, enter the name of this application on the Special settings panel. Your computer will connect to the network only after this program is closed.

Set Default Printer

Choose the printer that will be used by default. All print jobs will be sent to this printer unless otherwise specified. This way you can print out without having to switch the printer manually each time you switch locations.

Override TCP/IP and DNS Defaults

Choose whether TCP/IP and DNS settings should be obtained automatically from a DHCP network server or defined locally, by use of static addresses.

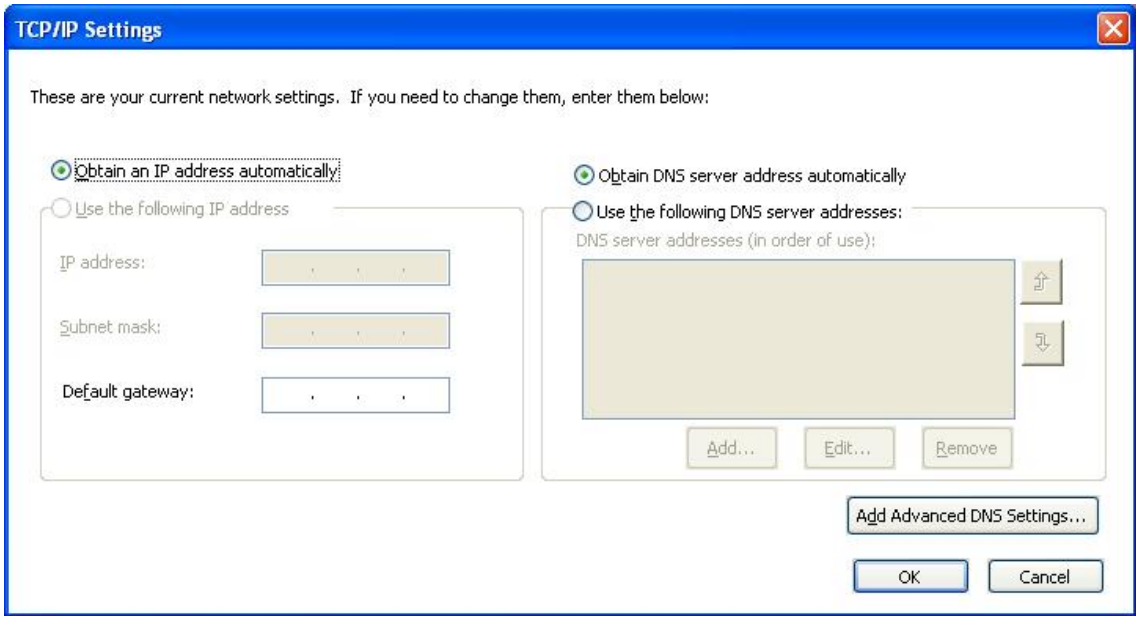

Figure 28. TCP/IP Settings

Enable VPN Connection

Choose whether to use a virtual private network (VPN) to connect to the Internet. For more information about setting a VPN connection, see “Editing VPN settings” on page 40.

Override Home Page

Choose whether to set a home page in Internet Explorer or Firefox browser.

Override Proxy Configuration

Choose whether to define proxy servers for use at this location.

Wireless security settings

Using static WEP key

If you selected **Use Static WEP keys** for the wireless security type, the Static WEP Settings window opens.

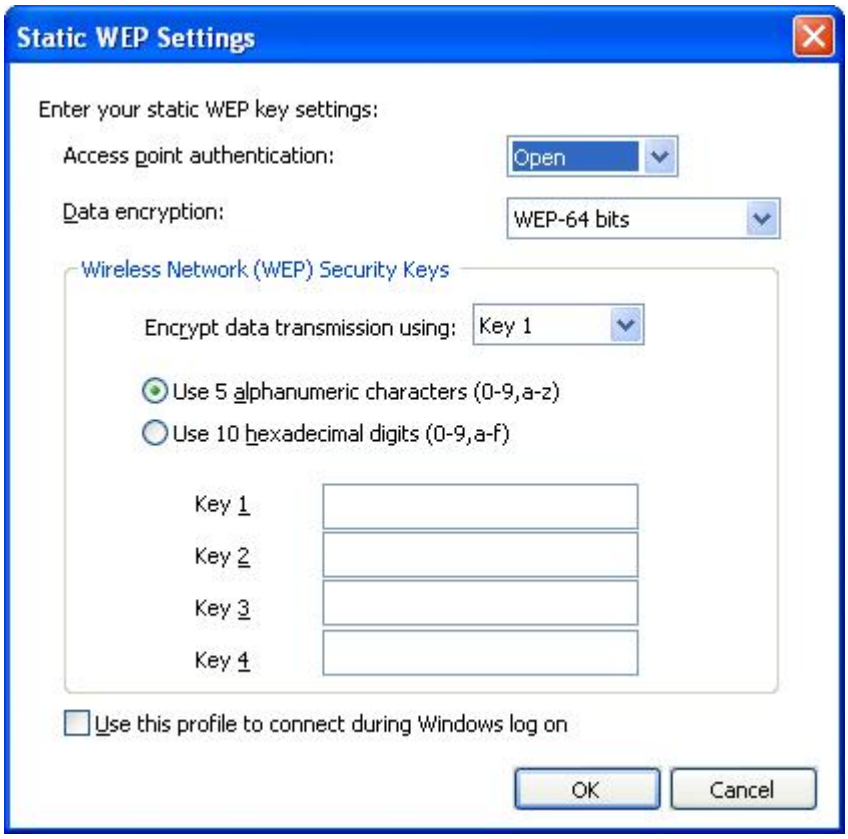

Figure 29. Static WEP Settings window

Here you must configure the following settings:

Data encryption

Select **64bit (WEP-64 bits)** or **128bit (WEP-128bits)** for the WEP key length.

To determine the actual length of the key, subtract the initial vector (24 bits) from the specified value. That is, 40 bits, or 5 alphanumeric characters, are available for a 64-bit key, and 104 bits, or 13 alphanumeric characters, are available for a 128-bit key.

Encrypt data transmission using

Select one of the four keys defined below. The selected key is used for encrypting the actual data transmission.

The key can be entered in either alphanumeric or hexadecimal characters. For the number of characters, see “Data encryption.”

Use this profile to connect during Windows logon

Select this check box if you want to connect to the network by use of this profile when you first power on your computer, without logging on to Windows.

Using Wi-Fi Protected Access - Pre-Shared Key (WPA-PSK)

If you selected **Use WPA-PSK key** as the wireless security type, the WPA-PSK Settings window opens.

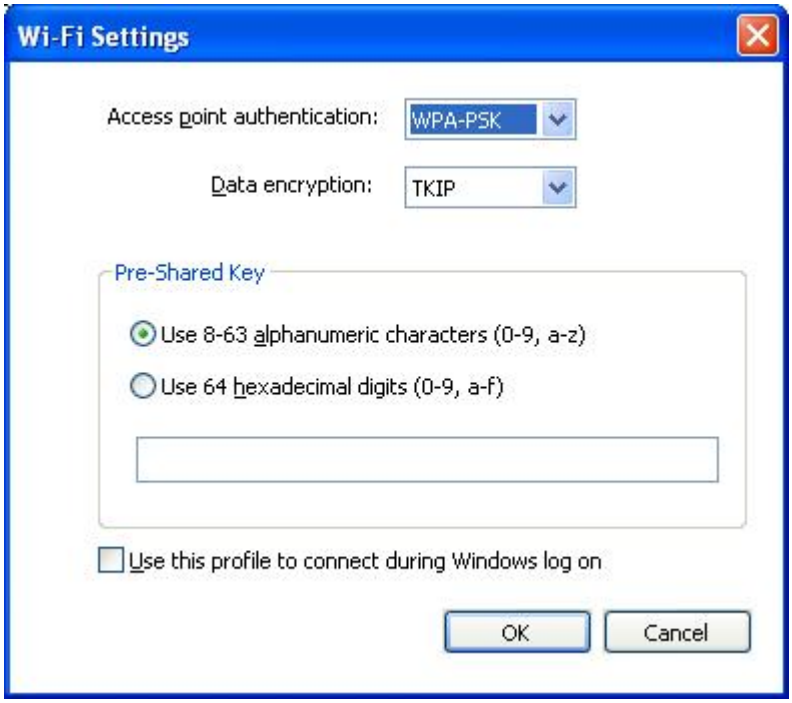

Figure 30. Wi-Fi Settings window

You can configure the following settings:

Data encryption

The popup lists the data encryption modes available for the wireless LAN card that is installed on your system. Select the data encryption mode, such as WEP, TKIP, or AES. The mode should match the settings of the access point. Consult your network administrator for the appropriate settings.

Pre-Shared Key

The key entered here will be used for encrypting the actual transmission. Enter the same key as the one set on the access point. You can use either alphanumeric or hexadecimal characters; if you use hexadecimal, be sure to enter all 64 digits correctly.

Use this profile to connect during Windows logon

Select this check box if you want to connect to the network by use of this profile when you first power on your computer, without logging on to Windows.

Using Windows standard features to configure 802.1x

If your computer is running Windows XP, you can configure 802.1x, including WPA, by selecting either Windows standard functions or Access Connections. A profile configured by use of Access Connections can be distributed as a package. For more information about distributing location profiles, see Appendix A, “Frequently asked questions,” on page 73, question 9 on page 73 and question 10 on page 74.

If you select this mode, Access Connections will not handle the configuration of wireless LAN. Select this mode to configure adapters that cannot be directly configured by use of Access Connections. When you use this mode, make note that:

- Depending on the wireless LAN adapter installed on your computer, reconnecting to the access point or 802.1x authentication when your computer returns from suspend mode may take longer.
- If you have other location profiles configured by use of Access Connections, switching to a location profile configured by use of Windows standard features may take time.
- If the location profile configured by use of Access Connections is no longer valid—for example, if you have moved to a different location—you can switch to a different location profile. For a Windows-configured location profile, however, you will need to logon to Windows again. Automatic location switching that involves domain logon is not supported.

To configure 802.1x by use of Windows standard functions, select **Use Windows to Configure Wireless Network** as the wireless security type. The 802.1x Settings windows opens; click **Authentication Properties**.

Figure 31. 802.1x Settings window

The Windows Authentication Properties window is displayed.

Configure the settings as follows:

- **Association** tab

  SSID The SSID entered here must match the one entered previously, in step 17 on page 16.

  Data encryption
  If data encryption is necessary, select **Key is provided**, and make sure that no other options are selected.

- **Authentication** tab

  Enable 802.1x on this network
  Select this check box.

Authenticate as computer when computer information is available
Select this check box if you are using machine authentication.

Properties
Click this button, and configure the settings that depend on the authentication you use. You must also enter the **Certificate issuer** setting.

Note: If you configure the wireless network settings by use of Windows standard functions, certain functions that are available on the wireless LAN card, such as authentication type and encryption type, may not activate properly. In this case, choose **Use IEEE 802.1x authentication** for the security type.

If you selected **Use Windows to configure wireless network** for the security mode, Windows XP will configure the wireless connection.

Using IEEE802.1x Authentication

To use functions of Access Connections in configuring the settings for authenticating Wireless LAN 802.1x, select **Use IEEE 802.1x authentication**. The 802.1x Settings window opens.

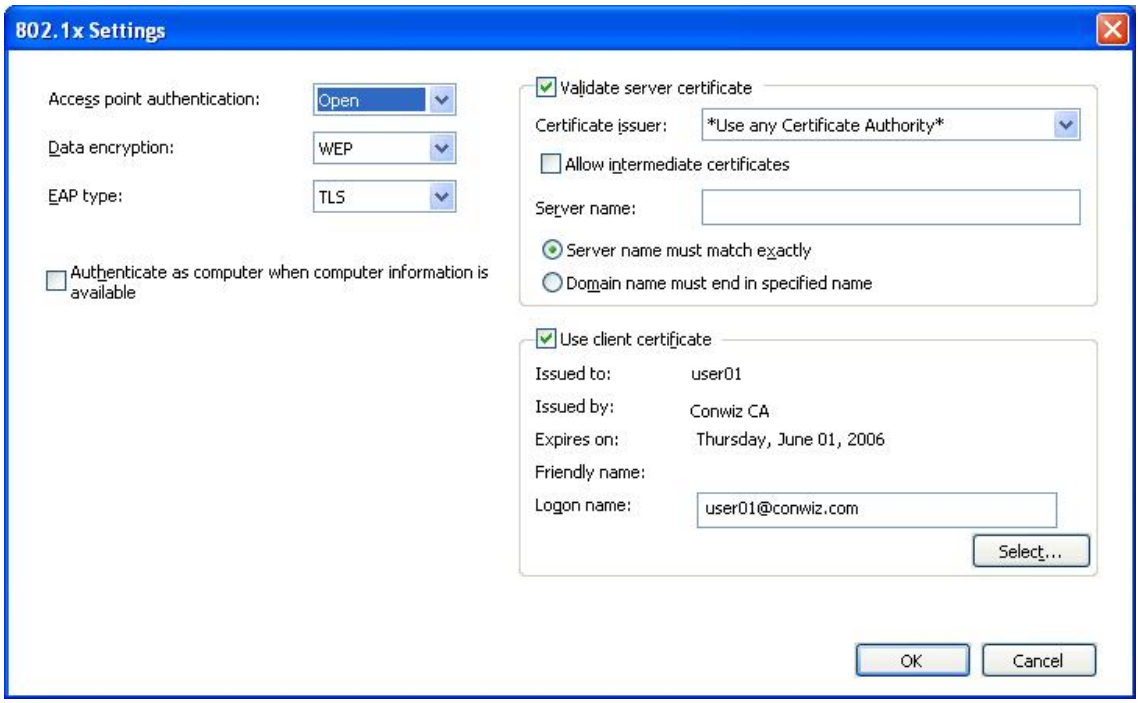

Figure 32. 802.1x Settings—Access Connections window

You can configure the following settings:

Access point authentication
You can select one of the following types:
- Open/common
- WPA
- WPA2

Data encryption
Select the value appropriate for your network. If you select **WPA** as the

Access point authentication setting, **Data encryption** must be set to either **TKIP** or **AES**. If you select **WPA2**, **AES** is selected by default.

Validate server authentication

You may have to enter the subdomain name of the Radius server (ibm.com etc.).

Use client certificate

Click **Select**. The Select Certificate window opens.

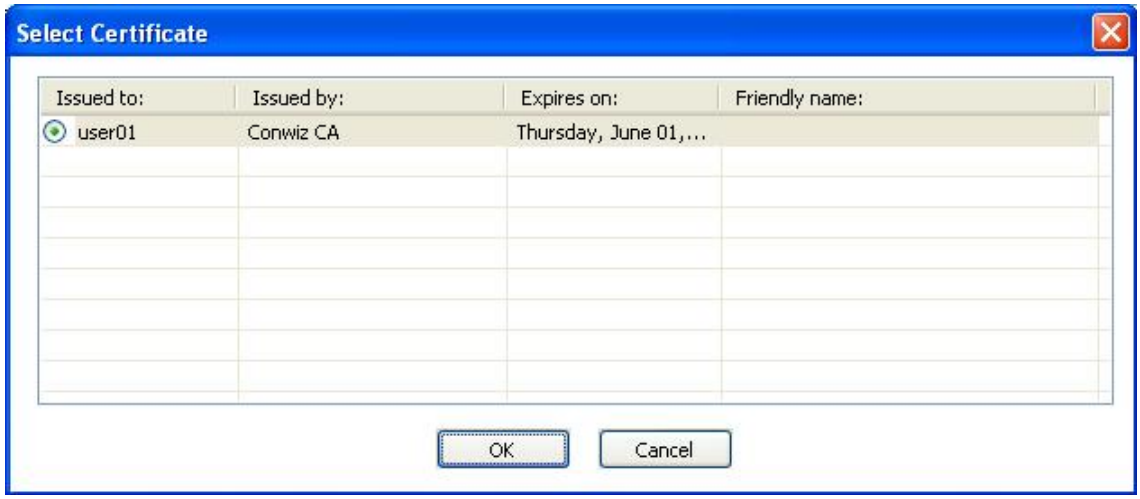

Figure 33. Select Certificate window

Select the certificate to be used for this profile.

EAP type

Select one of the following types:

- EAP-TLS
- EAP-TTLS
- PEAP-MSCHAP-V2
- PEAP-GTC

The type of EAP authentication depends on the authentication server. For more information, consult your network administrator.

When EAP authentication is set to TLS:

Validate server certificate

If the server certificate has to be verified, select the **Validate server certificate** check box, and specify the certificate of a reliable route certificate issuer. If the server name is in the specific domain, specify the domain name in the server name field.

If the server certificate does not need to be verified, leave the **Validate server certificate** check box blank. In this case, the application will not check the reliability of the server, and the connection will not be a tightly secured one.

Client certificate

The use of a client certificate is required. To specify a particular certificate, press the **Select** button, and select the certificate from the list. If you select the wrong certificate or one that has expired, the connection will not be

established. If the selected certificate is valid, the logon ID that appears on the certificate is entered automatically in the **Logon name** field.

Authenticate as computer when computer information is available

If you are using an IBM wireless adapter, you can use machine certification for the authentication. To do this, select the **Authenticate as computer when computer information is available** check box; then proceed with configuring the settings without specifying the client certificate. Save the configured profile. The connection will be based entirely on the information in the computer certificate.

If you specify the client certification and also select the A**uthenticate as computer when computer information is available** check box, both the computer certificate and the client certificate will be authenticated.

You can use computer certification to log on to the network domain.

When EAP authentication is set to TTLS:

Validate server certificate

If the server certificate must be verified, select the check box for **Validate server certificate**, and specify the certificate of a reliable route certificate issuer. If the server name belongs to a specific domain, specify the domain name in the server name field.

If the server certificate does not need to be verified, leave the **Validate server certificate** check box blank. The application will not check the reliability of the server, and the connection will not be tightly secured.

Roaming type

In the **Roaming type** field, enter the user account name that is already registered on Func Software Odyssey Server. This should be the name specified in the user ID field of the **Tunnel authentication** setting.

Tunnel authentication

MS-CHAP-V2 is the protocol available for the Tunnel authentication.

The following settings can be configured by the user (for the user name, enter the same name as the one specified in the **Roaming type** field).

Use Windows logon name and password

The user ID and password used for Windows logon will be used for tunnel authentication as well. This setting is valid for activating the Single sign-on function, which authenticates EAP-TTLS by use of the user ID and password for Windows logon. To enable this setting, go to Option, and select the check box for Use Windows logon user name and password to authenticate the wireless network. Tunnel authentication and logon to the domain server will be processed simultaneously.

For Thinkpad computers that support the use of fingerprint reader to log on to Windows, the wireless network authentication will be processed automatically.

Use temporary user ID and password

If you select this setting, a message will be displayed when you deploy this location profile, asking you to enter the user ID and password for tunnel authentication. After you enter the necessary information, the authentication will start. This option is used to connect to the wireless network manually.

Use saved user ID and password

The user ID and password for the tunnel authentication are set in advance.

If using the Windows logon user name and password for wireless network authentication is enabled, the available user ID and password will be used for tunnel authentication at Windows logon, and the computer will log on to the Windows domain server. To enable this setting, go to **Option**, and select the check box for **Use Windows logon user name and password to authenticate the wireless network**.

When EAP authentication is set to PEAP:

Validate server certificate

If the server certificate must be verified, select the **Validate server certificate** check box, and specify the certificate of a reliable route certificate issuer. If the server name belongs to a specific domain, specify the domain name in the server name field.

If the server certificate does not have to be verified, leave the **Validate server certificate** check box blank. The application will not check the reliability of the server, and the connection will not be tightly secured.

Roaming type

In the **Roaming type** field, enter the name of the user account that has been registered on the Radius Server. This name should be the one specified in the user ID field of the **Tunnel authentication** setting.

Tunnel authentication

The following protocols are supported for tunnel authentication:

- MS-CHAP-V2
- GTC (Generic Token Card)

When tunnel authentication is set to MS-CHAP-V2, you can configure the following settings (enter the name specified for the **Roaming type** field).

Use Windows logon name and password

The user ID and password that are used for Windows logon will be used for tunnel authentication as well. This setting is valid for activating the Single sign-on function, which authenticates EAP-PEAP by use of the user ID and password for Windows logon. To enable this setting, go to **Option**, and select the check box for **Use Windows logon user name and password to authenticate the wireless network**. Tunnel authentication and logon to the domain server will be processed simultaneously.

For Thinkpad computers that support logging on to Windows by use of a fingerprint reader, the wireless network authentication will be processed automatically.

Use temporary user ID and password

If you select this setting, a message will be displayed when you deploy this location profile, asking you to enter the user ID and password for tunnel authentication. After you enter the necessary information, the authentication will start. This option is used to connect to the wireless network manually.

Use saved user ID and password

The user ID and password for tunnel authentication are set in advance.

If the use of the Windows logon user name and password for wireless network authentication is enabled, the available user ID and password will be used for tunnel authentication at Windows logon, and the computer will

log on to the Windows domain server. To enable this setting, go to **Option**, and select the check box for **Use Windows logon user name and password to authenticate the wireless network**.

When tunnel authentication is set to GTC, you can configure the following settings.

Use one-time token

Under GTC tunnel authentication, the connection is established after a temporary password for tunnel authentication, called a token, specified by RSA security is entered. To apply this setting, select this check box. Then, whenever you deploy the location profile, a message asking you to input the token number and ID is displayed.

Use temporary user ID and password

If you select this setting, a message will be displayed when you deploy this location profile, asking you to enter the user ID and password for tunnel authentication. After you enter the necessary information, the authentication will start. This option is used to connect to the wireless network manually.

Use saved user ID and password

The user ID and password for the tunnel authentication are set in advance.

If the use of the Windows logon user name and password for wireless network authentication is enabled, the available user ID and password will be used for tunnel authentication at Windows logon, and the computer will log on to the Windows domain server. To enable this setting, go to **Option**, and select the check box for **Use Windows logon user name and password to authenticate the wireless network**.

Using 802.1x - EAP Cisco (LEAP)

If you have selected EAP Cisco (LEAP) mode, you can configure the settings for user ID and password necessary for use of Cisco LEAP. The LEAP Settings window is displayed:

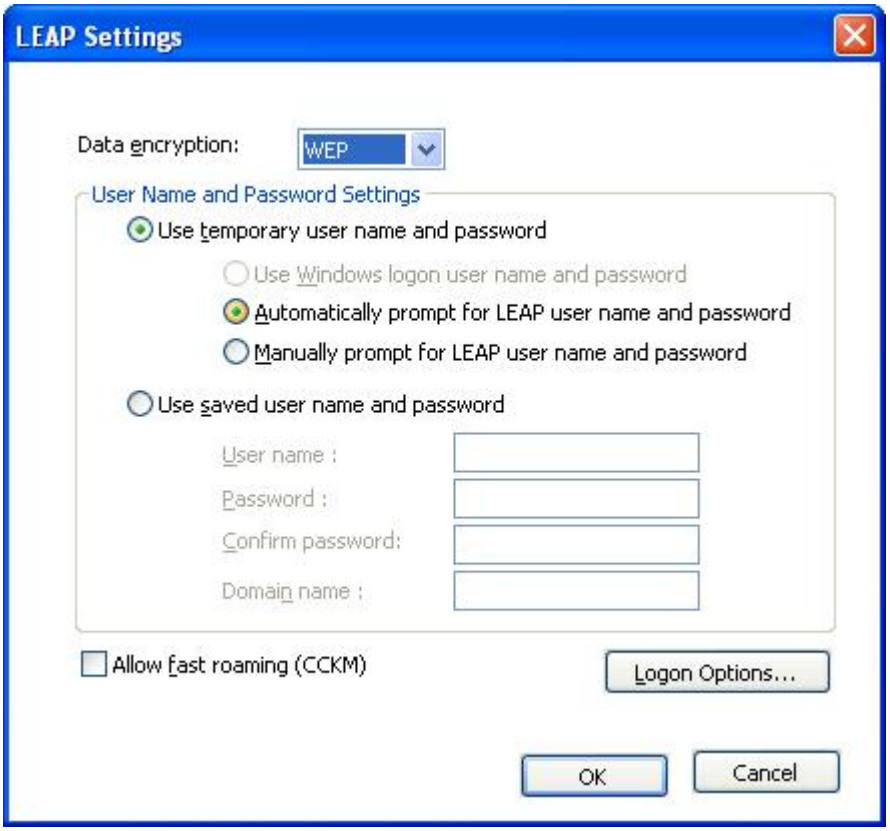

Figure 34. LEAP Settings window

Configure the following settings.

Data encryption

Select one of the following options:

- WEP
- CKIP
- TKIP
- AES

Configure the user name and password as follows:

Use Windows logon name and password

The user ID and password used for Windows logon are also used for LEAP authentication. This setting is valid for activating the Single sign-on function, which processes LEAP authentication by use of the user ID and password for logon to Windows. To enable this setting, go to **Option**, and select the check box for **Use Windows logon user name and password to authenticate the wireless network**. Tunnel authentication and logon to the domain server will be processed simultaneously.

For Thinkpad computers that support logging on to Windows by use of a fingerprint reader, the wireless network authentication will be processed automatically.

Automatically display user name and password prompt for LEAP

To display the prompt asking you to enter the user name and password that are to be displayed when the location profile is deployed (if they have not already been entered), choose this setting. After you enter the user name and password, the authentication process starts. Once entered, the authentication information is saved by the computer, and the prompt does not appear again unless you log off or restart your computer; then it is cleared, and will have to be entered again the next time you log on. The prompt appears only if the user name and password used for previous LEAP authentication are not found.

Manually display user name and password prompt for LEAP

A prompt asking you to enter the user name and password is displayed every time you deploy the location profile. After you enter the user name and password, the authentication process starts.

Use saved user ID and password

The user ID and password for LEAP authentication are set in advance.

If using the Windows logon user name and password for wireless network authentication is enabled, the available user ID and password will be used for LEAP authentication at Windows logon, and the computer will log on to the Windows domain server. To enable this setting, go to **Option**, and select the check box for **Use Windows logon user name and password to authenticate the wireless network**.

Include Windows logon domain with user name

Select this check box if the network contains multiple domains. Then both the user name and the domain name are verified by the access point during LEAP authentication.

Do not connect to network when user is not logged on

To disconnect from the network when the user logs off, select this option. Otherwise, the computer will maintain the connection even after the user has logged off.

LEAP authentication timeout value

If LEAP authentication takes longer that usual, change this setting to increase the time before the connection is timed out. The default setting is 60 seconds. For some wireless LAN adapters, this setting cannot be changed.

Enable fast roaming (CCKM)

Select this option to enable switching between different Cisco access points when you move your computer; this is the fast roaming feature. You will then be able to roam quickly between access points with no need to reauthenticate.

Using 802.1- Cisco (EAP-FAST)

If you have selected EAP Cisco (EAP-FAST) mode, you can set a user ID and password for use of this security mode. The EAP-FAST Settings window is displayed as follows:

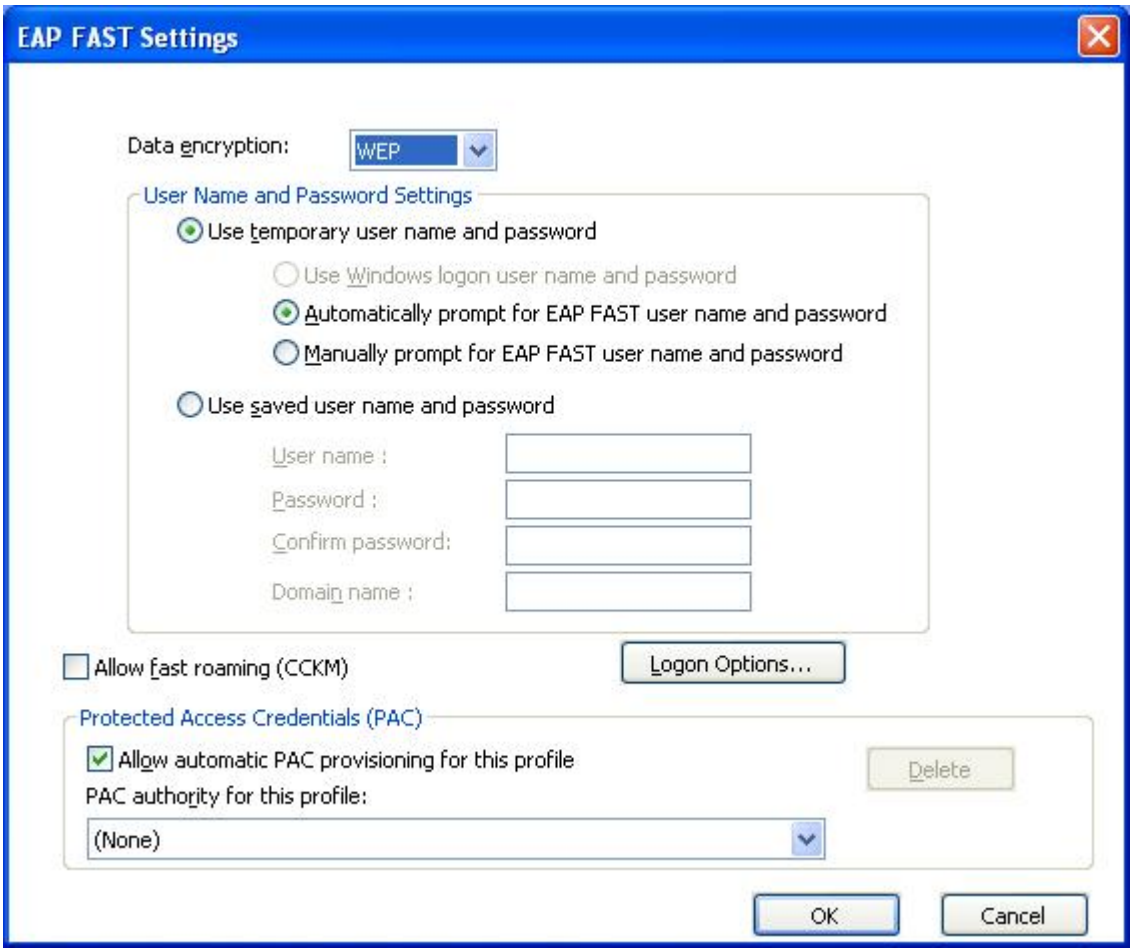

Figure 35. EAP-FAST Settings window

Configure the following settings:

Data encryption

Select one of the following options:

- WEP
- CKIP
- TKIP
- AES

Configure the user name and password as follows:

Use Windows logon name and password

The user ID and password for Windows logon will also be used for EAP-FAST authentication. This setting is valid for activating the Single sign-on function, which processes the EAP-FAST authentication by use of the user ID and password for Windows logon. To enable this setting, go to **Option**, and select the check box for **Use Windows logon user name and password to authenticate the wireless network**. Tunnel authentication and logon to the domain server will be processed simultaneously.

For Thinkpad computers that support the use of a fingerprint reader to log on to Windows, the wireless network authentication will be processed automatically.

Automatically display user name and password prompt for EAP-FAST
To display the prompt asking you to enter the user name and password displayed when the location profile is deployed (if they have not already been entered), choose this setting. The authentication starts as soon as you enter the user name and password. The authentication information is saved by the computer, and the prompt does not appear again unless you log off or restart your computer; then it is cleared, and will need to be input again the next time you log on.

Manually display user name and password prompt for EAP-FAST
A prompt asking you to enter the user name and password is displayed every time you deploy the location profile. After you enter the user name and password, the authentication process starts.

Use saved user ID and password
The user ID and password for the EAP-FAST authentication are set in advance.

If using the Windows logon user name and password for wireless network authentication is enabled, the available user ID and password will be used for EAP-FAST authentication at Windows logon, and the computer will log on to the Windows domain server. To enable this setting, go to **Option**, and select the check box for **Use Windows logon user name and password to authenticate the wireless network**.

Protected Access Credential (PAC): Allow automatic PAC provisioning for this profile
To process EAP-FAST authentication by automatically receiving a PAC file from Cisco ACS server, select this check box. Automatic PAC provisioning is useful if you want to use the EAP-FAST authentication to log on to the Windows server domain.

If you are using a Cisco 802.11b wireless adapter or an IBM wireless adapter, you can use the saved PAC file for EAP-FAST authentication by selecting the PAC file from the list. These adapters support the importing of a PAC file. To import the PAC file, click the **Import** button.

You can also configure the following settings by use of the **Logon option** button.

Append Windows logon domain to user name
Select this check box if the network contains multiple domains. Then both the user name and the domain name are verified by the access point during LEAP authentication.

Do not connect to network when user is not logged on
Select this check box to disconnect from network when the user logs off. Otherwise, the computer will maintain the connection.

EAP-FAST authentication time out
If EAP-FAST authentication takes longer than usual, change this setting to increase the time before the connection is timed out. The default setting is 60 seconds. For some wireless LAN adapters, this setting cannot be changed.

Enable fast roaming (CCKM)
Select this check box to enable switching between different Cisco access

points when you move your computer; this is the fast roaming feature. You will then be able to roam quickly between access points without having to authenticate repeatedly.

Editing VPN settings

If you selected the optional setting **Enable Virtual Private Network (VPN) connection** in the process of creating a profile, the VPN settings window is displayed.

Select the VPN program to use for connecting to a network. To use the VPN program provided by your company, select **I use an application provided by my company** and then click **Select my VPN program**. You also can configure Access Connections to launch the VPN application automatically when you switch to this location profile, and to close it automatically when you switch to a different one.

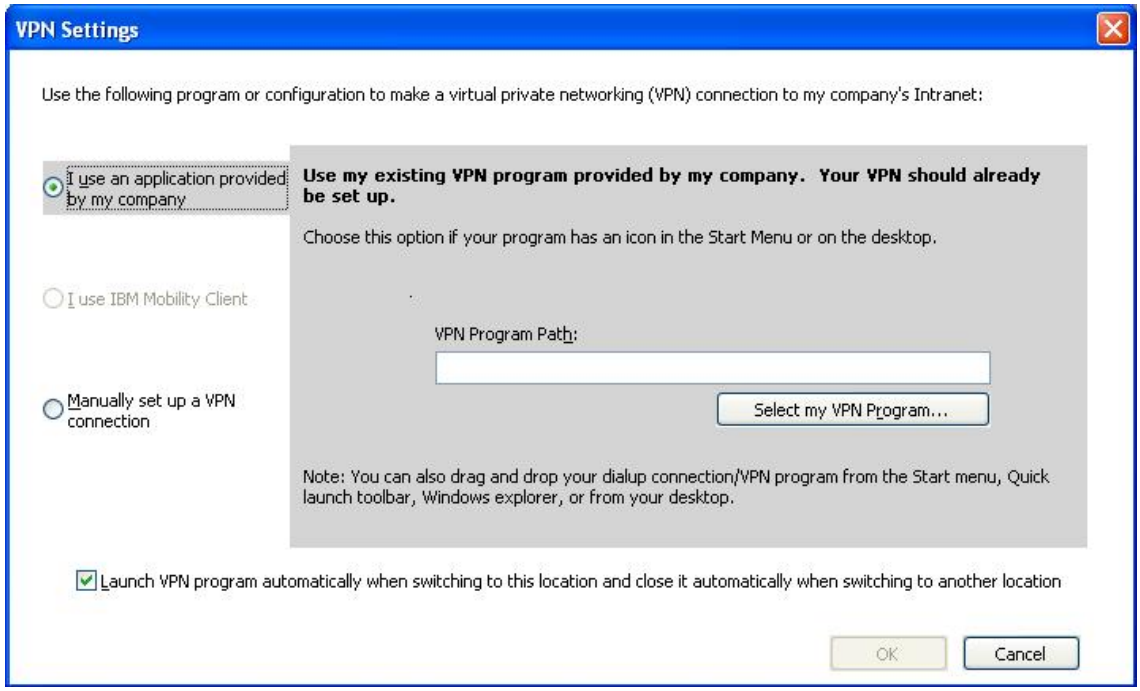

Figure 36. VPN settings—using an application provided by my company window

If you select **Use my existing VPN program provided by my company**, Access Connections starts this program.

To use the IBM Mobility Client, select **I use IBM Mobility Client** and then click **Select Mobility Client Profile**. You can configure Access Connections so that IBM Mobility Client is launched automatically when you switch to this location profile.

To use the VPN program provided by Windows, select **Manually set up a VPN connection**, and then either select an existing phonebook entry or add a new one.

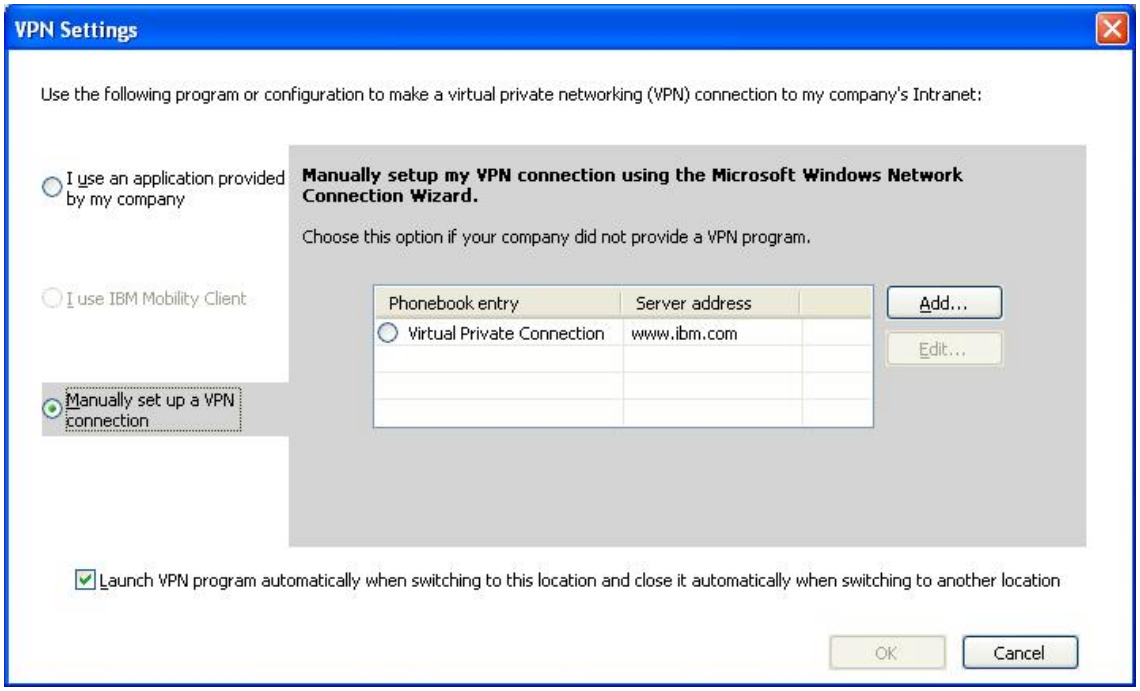

Figure 37. VPN settings—Manually set up a VPN connection window

If you select **Manually set up my VPN connection using Microsoft Windows network connection Wizard**, proceed to create the VPN connection by clicking the **Add** button.

To disconnect the VPN connection automatically when you switch to another profile, select the check box for **Launch VPN program automatically when switching to this location and close it automatically when switching to another location** button. (For some VPN programs, this command may not work.)

Managing location profiles

To create or delete a location profile, or edit the settings for an existing profile, go to **Locations** on the main toolbar, and press **Manage Profiles** on the pull-down menu. The Manage Location Profiles panel, with a list of available profiles, is displayed.

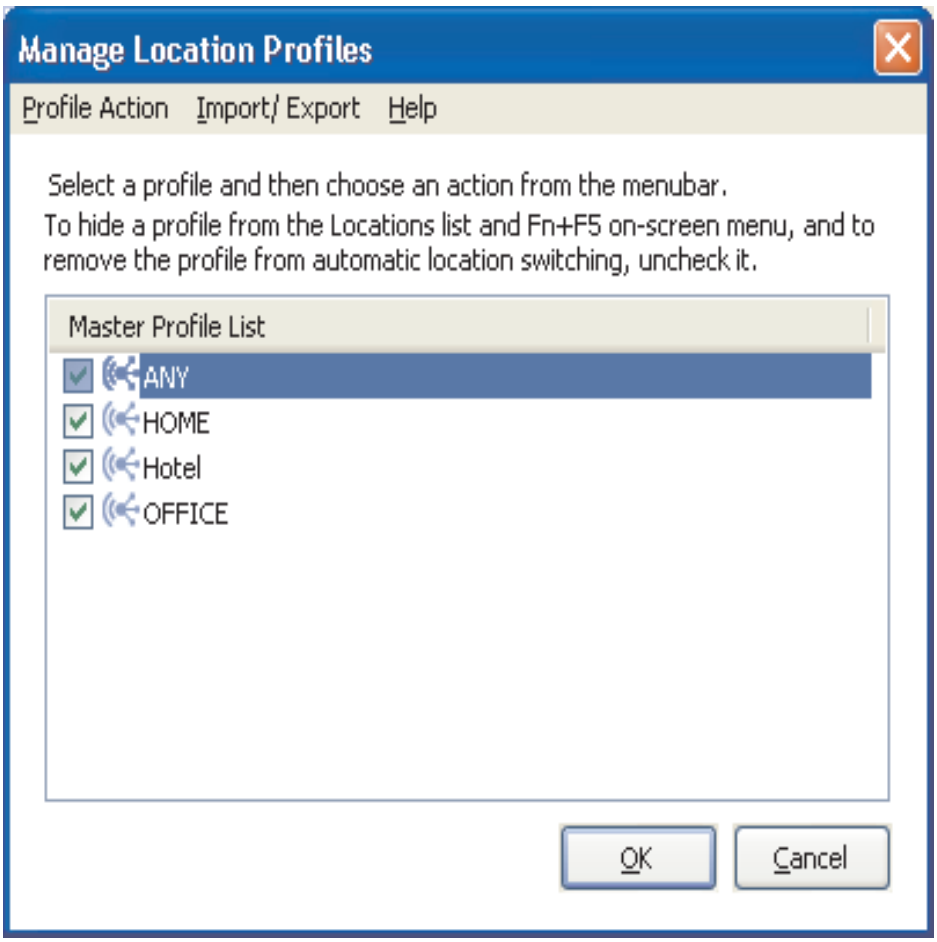

Figure 38. Manage Location Profiles window

Select a profile and perform one of the following actions found under **Profile Action**:

Create:
Create a new location profile.

Edit: Modify the settings used in the selected profile.

Copy:
Copy the selected profile.

View: Show a summary of the settings used in the selected profile.

Rename:
Change the name of the selected location profile.

Desktop Shortcuts:
Create a desktop shortcut for the selected location profile. You can create a shortcut to connect (apply) a profile or disconnect.

Delete:
Permanently remove the selected location profile.

Location Switching:
Switch location profiles automatically.

By default, all existing location profiles are shown in the Manage Location Profiles window. To hide a profile from the Locations list and the Fn+F5 on-screen menu, and to remove the profile from automatic location switching, clear the check box to the left of the name of that profile.

Using shortcut icons

You can create a shortcut icon on your desktop for each of the profiles you use most often. Then you will be able to switch on a location profile by clicking the shortcut icon for it. To create a shortcut icon, open the Manage Location Profile panel, select the profile, and right-click it. From the pull-down menu, select either **Create Shortcut – Connect** or **Create Shortcut - Disconnect**.

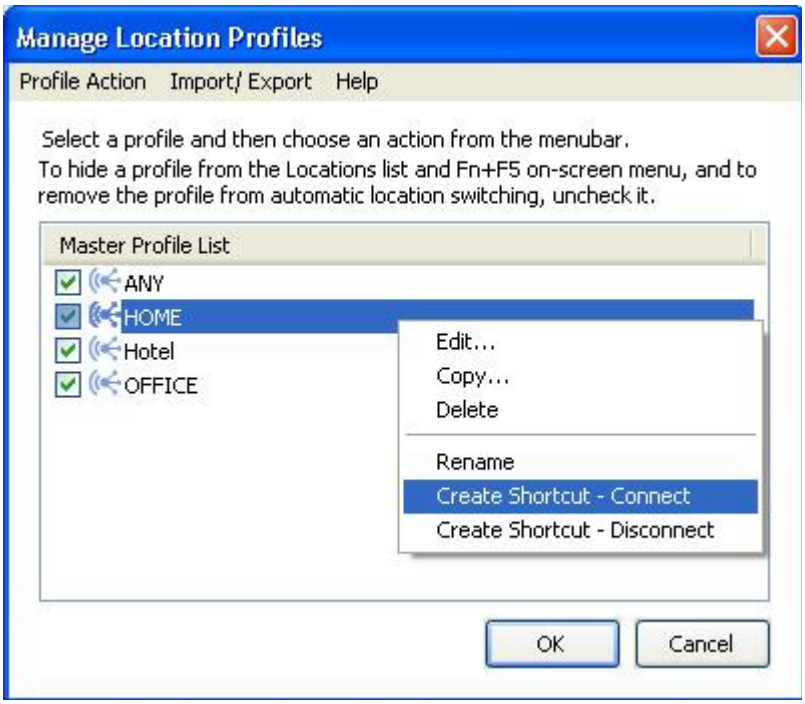

Figure 39. Manage Location Profiles window—Create Shortcut

You can switch to a different profile by entering a command from the command prompt:

```
<path>\qctray.exe /set [ Location profile name ]
```

It is not necessary to start up the Access Connections beforehand. To disconnect, use the following command:

```
<path>\qctray.exe /reset [Location profile name]
```

Connecting to a network

To connect to a network, choose and apply its location profile. You can connect or switch between existing location profiles from the main window, the on-screen menu that is displayed after pressing Fn+F5, or the system tray icon.

To connect from the main window, select the location profile, that matches where you are from the **Locations** pull-down menu, and then click **Connect**.

To connect from the on-screen menu, do the following:

1. Press and hold the Fn key on your keyboard, and then press F5. Release both keys.
2. The on-screen menu is displayed.

Figure 40. On-screen window

Click the **Location Profiles** tab.

3. Select the location profile that matches where you are.

To connect from the system tray icon, click the Access Connections icon in the system tray; then select the location profile that matches where you are.

Connecting to a wireless network

To find the wireless network available at your location, on the main menu click **Tools**, and then select **Find wireless networks** from the pull-down list. The list of available access points is displayed.

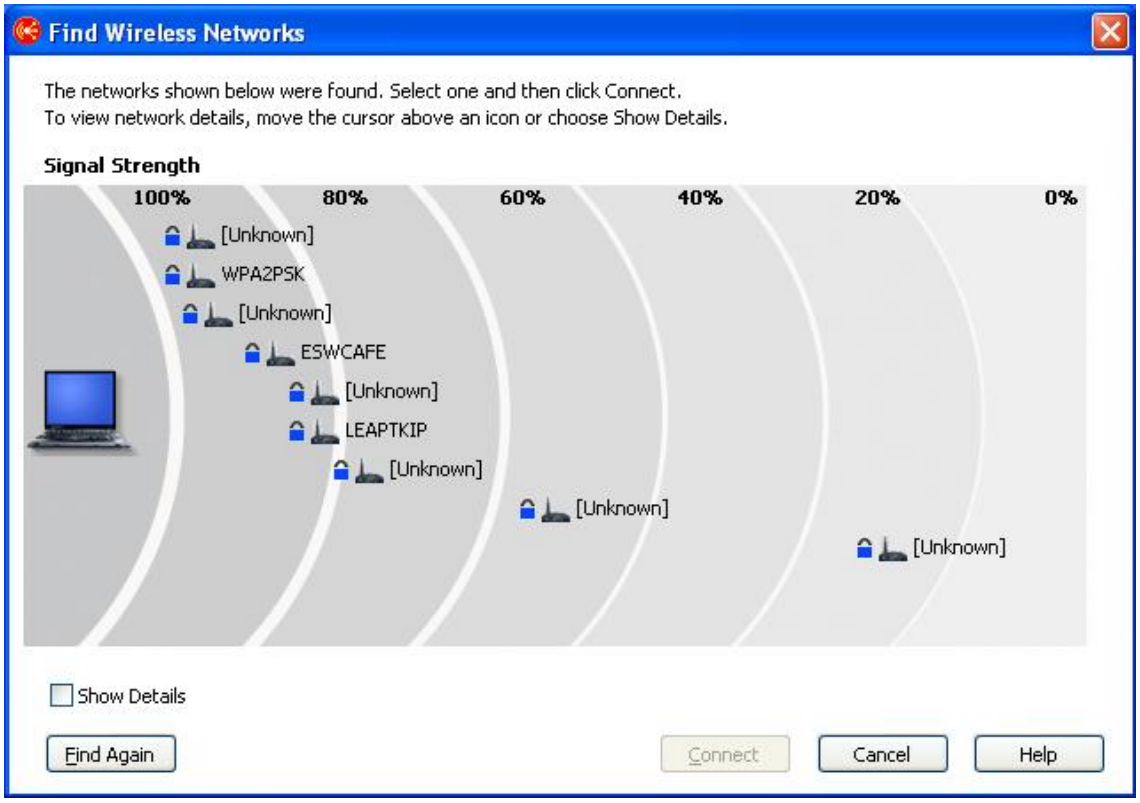

Figure 41. Find Wireless Networks window

An access point for an available network is indicated as follows: 

The following four icons indicate the type of wireless connection:

- Secured wireless LAN network

  

- Non-secured (open) wireless LAN network

  

- Secured peer-to-peer network

  

- Non-secured (open) peer-to-peer network

  

To display the access point list in the AC3.x format, select the **Show Details** check box.

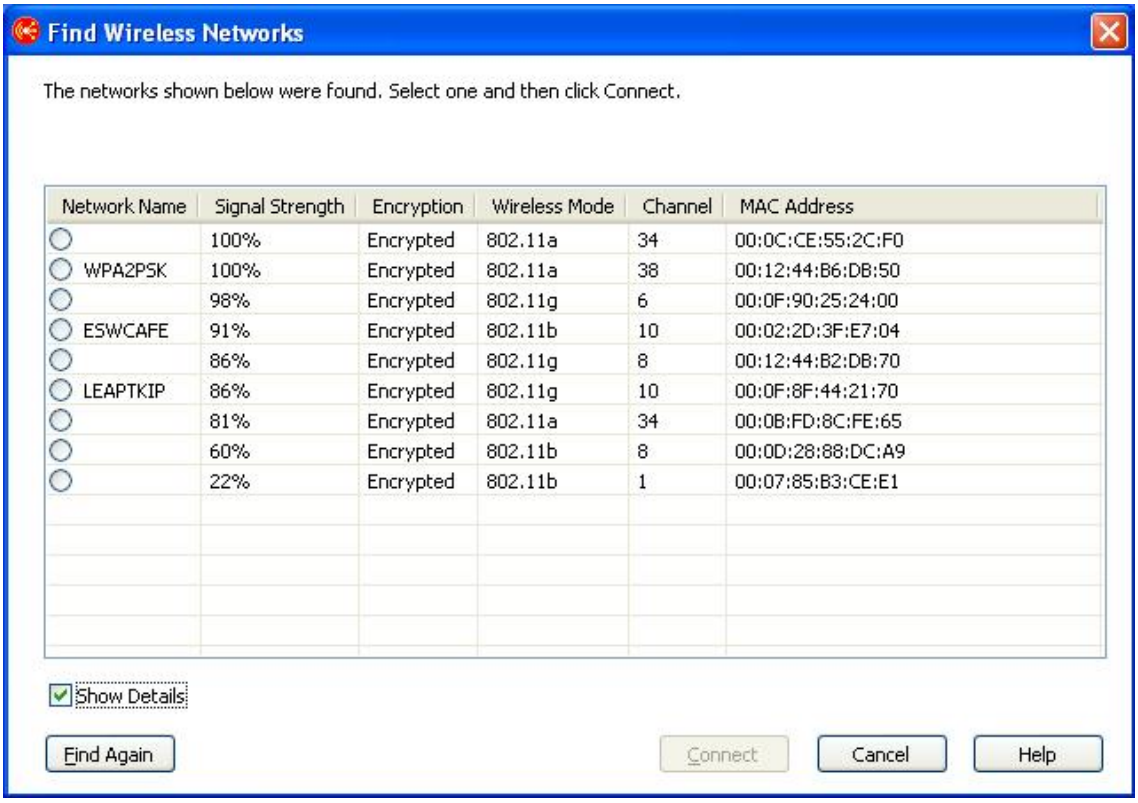

Figure 42. Find Wireless Networks window—detailed view

If the access point found is currently associated with your ThinkPad, its antenna is marked with a red circle. If it is encrypted, it is marked with a blue security icon.

To connect to any of the found networks, select the network and click **Connect**. If the network is a newly found one, either the location profile can be created automatically, or a temporary connection can be established without saving a location profile. In both cases you can only connect to an unencrypted access point. To connect to an encrypted access point, use the profile with the correct encryption key. If you are using Windows XP, and if the profile is created automatically, by default the setting for sharing files and printers is disabled, and the firewall is enabled. Turn the wireless LAN adapter on before you start searching for wireless networks.

Switching location profiles automatically

As you move your computer from place to place, Access Connections can automatically detect available wireless LAN (802.11) and Ethernet networks and apply the location profile of one of them for you.

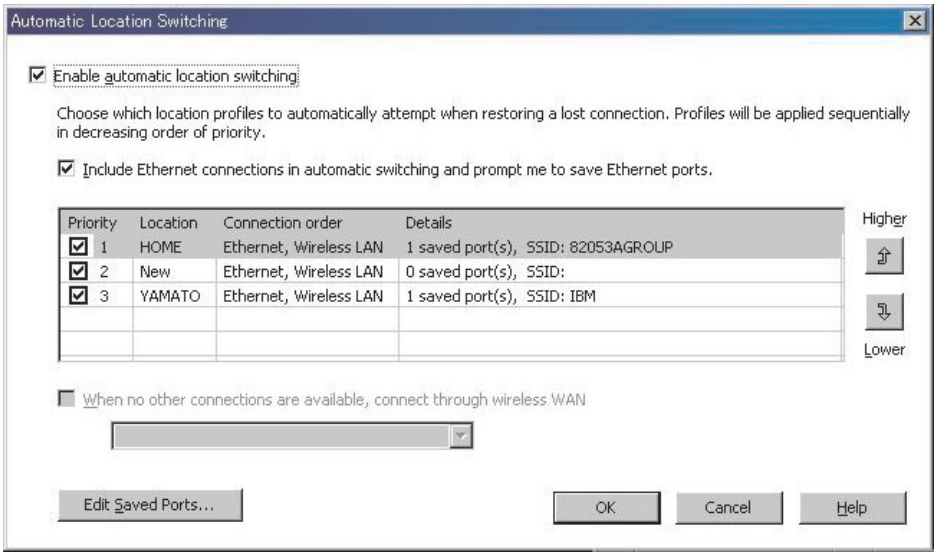

Figure 43. Automatic Location Switching window

To configure automatic switching between location profiles, do as follows:

1. On the menu bar of the main window of Access Connections, click **Configure**.
2. Select **Location Switching**.
3. To enable automatic location profile switching select **Enable automatic location switching**. Then, if an active connection is lost, Access Connections will search the list of profiles, in the order in which they are listed in the table, for one that matches an available wireless LAN network. When it finds such profile, it applies that profile to restore connectivity. You can change the order of the profiles by selecting a profile and then clicking **Higher** or **Lower**.
4. If you want Access Connections to check for available wired networks (in addition to wireless LAN networks) when switching automatically, select **Include Ethernet connections in automatic switching and prompt me to save Ethernet ports**.

   If this option is enabled, Access Connections will automatically obtain identifying information (a MAC address) for each new Ethernet port to which you connect, and then prompt you to associate that port with the location profile of your choice. When you later connect to the same Ethernet port, Access Connections will apply the profile you selected.

   To view or delete the MAC addresses of Ethernet ports that have been associated with location profiles, click **Edit Saved Ports**.
5. If your computer supports wireless WAN connections, you can select **When no other connections are available, connect through Wireless WAN** and select an appropriate wireless WAN location profile if one exists.
6. Click **OK**.

Viewing the connection status

You can use Access Connections to monitor the status of your network connections. For more information, click one of the following:

AC main window

When Access Connections is launched, the **Location Profiles** tab of the main window is selected by default. The window associated with this tab graphically depicts the status for the location profile selected in the **Locations** pull-down menu. For more details, hold the mouse over any graphic. Examples of graphics shown in this window as they typically appear from left to right are as follows:

- Computer connected to the network

- Computer disconnected from the network

- Firewall on

- (blank) Firewall off

- Open (non-secured) wired network communication in progress

- Connected to DSL network device

- Connected to DSL network device with VPN enabled

- Secured (encrypted) wired network communication in progress

- Open (non-secured) wireless network communication in progress

- Secured (encrypted) wireless network communication in progress

- Disconnected from DSL network device

- Connected to wireless access point

- Connected to wireless access point with VPN enabled

- Disconnected from wireless access point

- Connected to Ethernet network

- Connected to Ethernet network with VPN enabled

- Disconnected from Ethernet network

- Connected to wireless WAN network

- Connected to wireless WAN network with VPN enabled

- Disconnected from wireless WAN network

- Connected to remote device or network through a modem

- Connected to remote device or network using a modem with VPN enabled

- Disconnected from modem

Task tray icons

Access Connections provides two task tray icons. One is for general connection status; the other is for either wireless LAN or wireless WAN detailed status.

Icons for the status of Access Connections

- No location profile is active, or none exists.

- The current location profile is disconnected.

- The current location profile is connected.

- Peer to Peer Community is active.

Icons for status of wireless LAN

- Power to the wireless radio is off.

- Power to the wireless radio is on. The signal strength of the wireless connection is excellent.

- Power to the wireless radio is on. The signal strength of the wireless connection is marginal.

- Power to the wireless radio is on. The signal strength of the wireless connection is poor. To improve signal strength, move your system closer to the wireless access point.

Icons for status of wireless WAN

- Power to the WAN radio is off.

- No association

- No signal

- Signal level 1

- Signal level 2

- Signal level 3

Diagnostics

Access Connections provides a set of tools to check status of a network connection and solve any problems found. Click **Tools** on the main toolbar, and select **Diagnostics** from the pull-down menu. The Diagnostic Tools window is displayed.

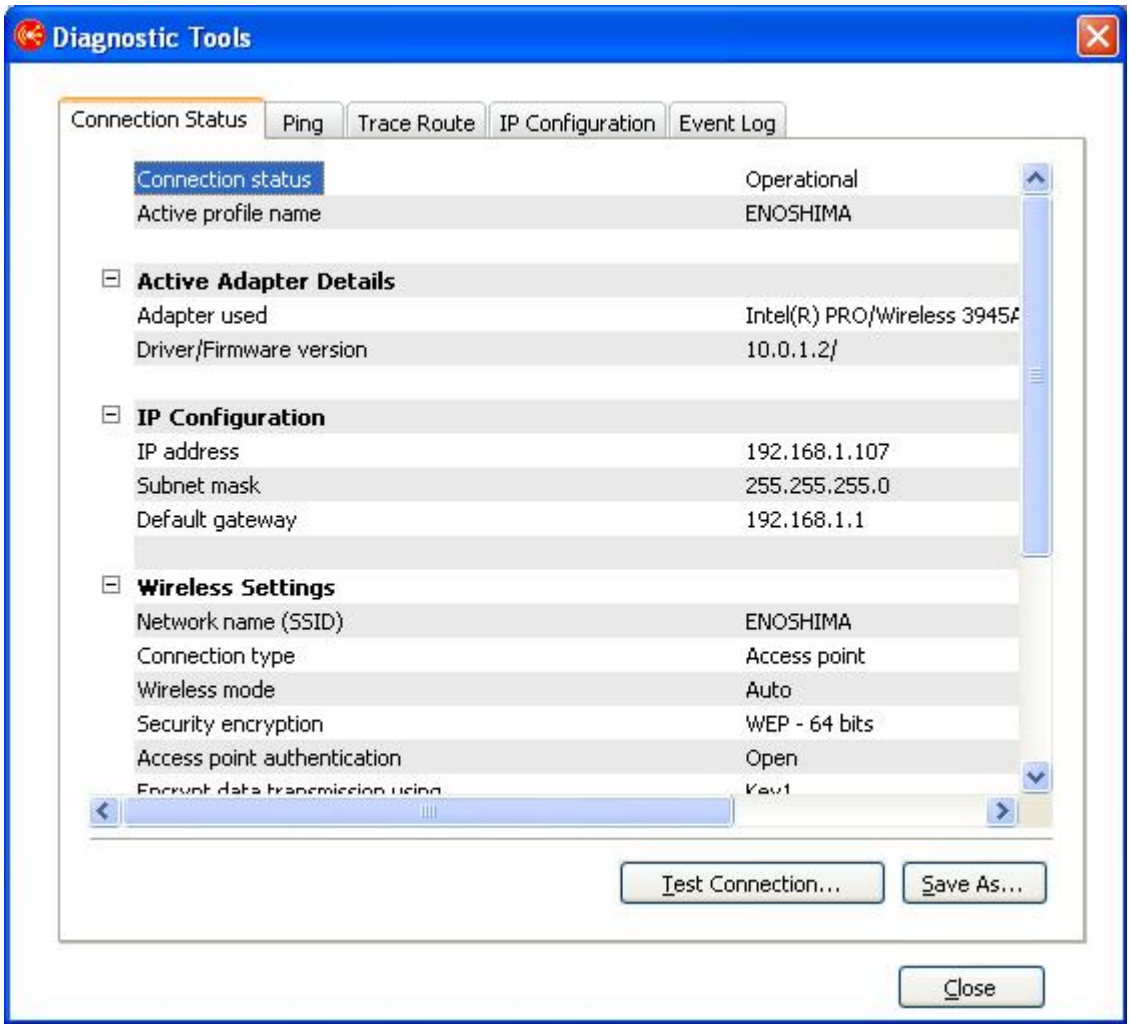

Figure 44. Diagnostic Tools

Click one of the following tabs to check the status of a connection and the network settings:

- **Connection status**
- **Ping**
- **Trace Route**
- **IP Configuration**

The **Event Log** tab is provided for use in solving problems with network connections, and can be used by a support center to investigate the causes.

To display the Diagnostic Tools panel from the main Access Connections panel, click **Properties**. You can also reach that panel from the window that appears when the connection to a network fails. To save the data, press **Save as** on the

Diagnostic Tools panel; the displayed information is saved as a text file that can be used by a support center to diagnose a problem.

When an attempt to connect to a network fails, the causes of problems, and possible solutions for them, are displayed, along with the current settings of the network.

Chapter 3. Configuration options

Access Connections enables each user to configure global settings and user preferences. Preferences apply only to the current user; global settings apply to all users of the computer. The following options and preferences can be configured:

- Network global settings
- Notification global settings
- User preferences
- Toolbar options
- Peer-to-peer options

Network global settings

To configure network global settings, do the following:

1. On the menu bar of the main window of Access Connections, select **Configure**.
2. Select **Global Settings**.
3. Click the **Network** tab.

The following window opens:

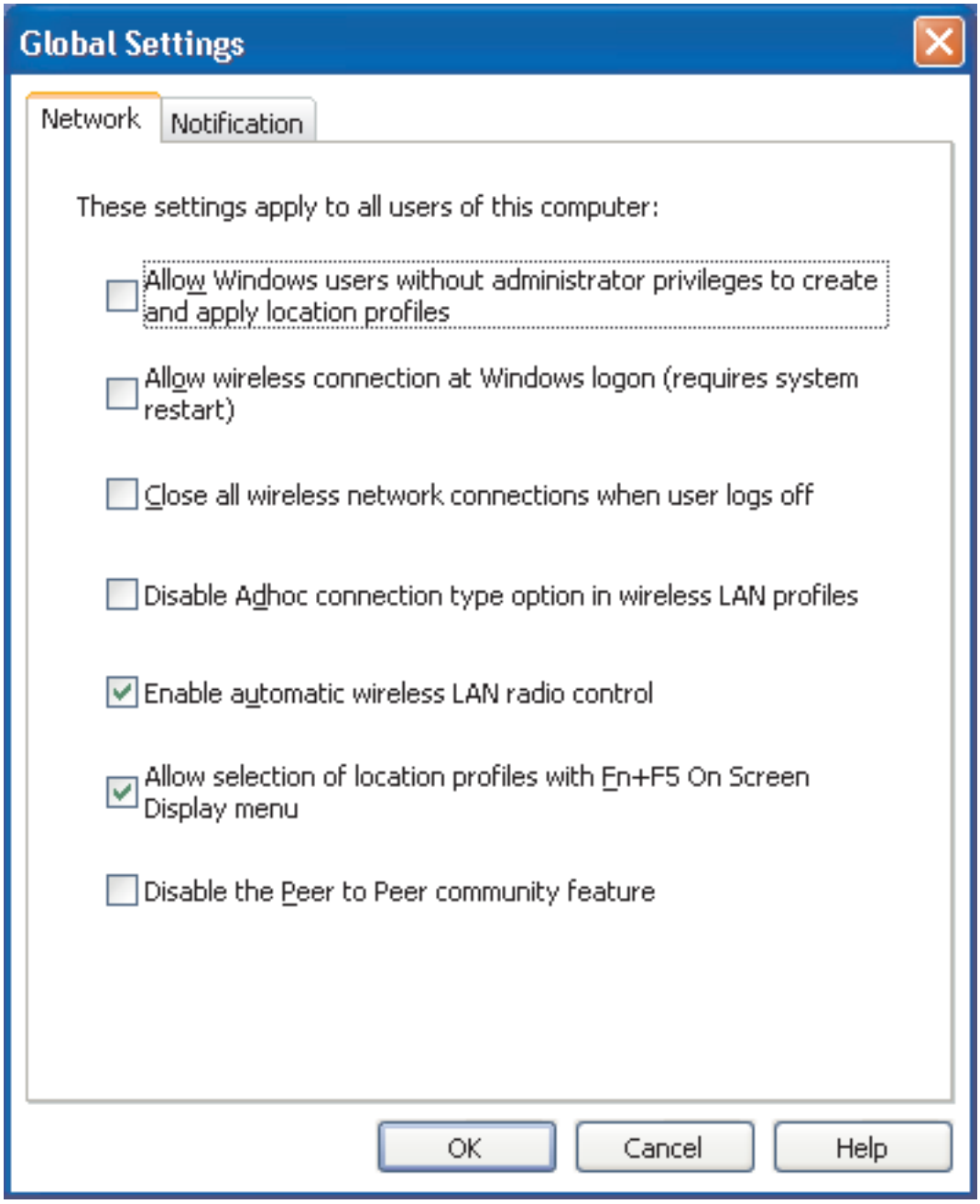

Figure 45. Global Settings—Network tab

4. Make the necessary changes, and click **OK**.

Network global settings apply to all users of this computer. The following network global settings can be configured:

Allow Windows users without administrator privileges to create and apply location profiles

Select this option to enable users to create and apply location profiles regardless of the windows logon privilege they have—administrator or limited user. Only a user who has logged on with administrator privileges

can enable this option. Even if this option is selected, Windows security protection by default does not allow a limited user to modify or create TCP/IP settings, security settings for the local drive sharing, or firewall settings.

Allow wireless connection at Windows logon (requires system restart)
Select this option to use the user name and password applied at Windows logon as the credentials for connecting to a wireless network. To enable the change to this setting, restart your computer.

Close all wireless network connections when user logs off
Select this option to disconnect from all wireless networks when you log off.

Disable Adhoc connection type option in wireless LAN profiles
Select this option to disable the Adhoc connection.

Enable automatic wireless LAN radio control
Select this option to enable automatic control of power on and off for the wireless LAN radio.

Allow selection of location profiles with Fn+F5 On Screen Display menu
If you select this option, pressing Fn+F5 will display a current list of location profiles on the Fn+F5 on-screen menu. You can use that menu to switch from one location profile to another and to power wireless radio on and off.

Disable the Peer to Peer community feature
Select this option to disable the peer-to-peer community feature.

Notification global settings

To configure notification global settings, do the following:

1. On the menu bar of the main window of Access Connections, click **Configure**.
2. Select **Global Settings**.
3. Click the **Notification** tab.

The following window opens:

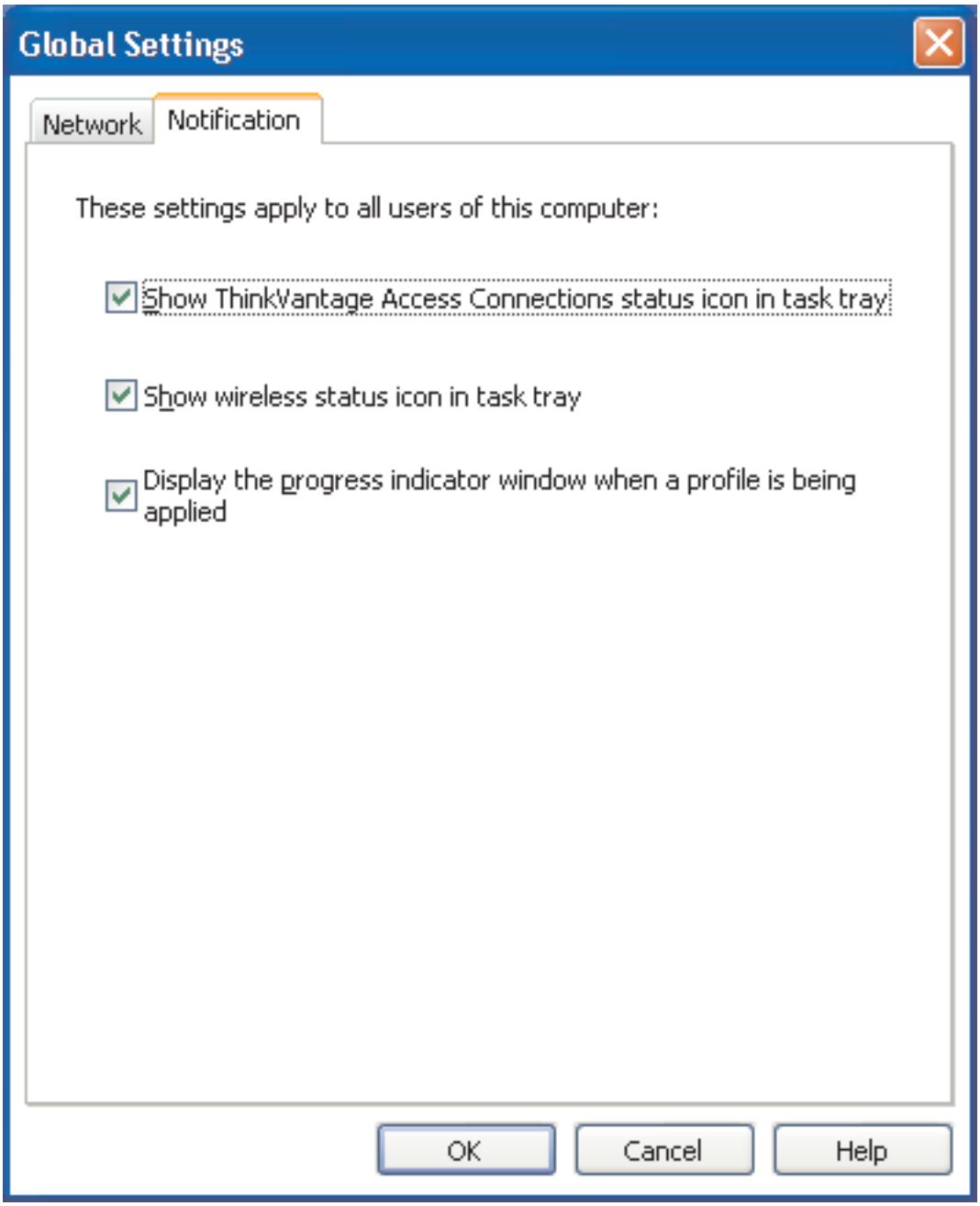

Figure 46. Global Settings—Notification tab

4. Make the necessary changes, and click **OK**.

Notification global settings apply to all users of this computer. The following global settings can be configured:

Show Access Connections status icon in task tray
If you select this option, the Windows task tray will show an icon that displays the status of Access Connections.

Show wireless status icon in task tray
If you select this option, the Windows task tray will show an icon that displays the status of your wireless network connection.

Display the progress indicator window when a profile is being applied
Select this option to display the progress indicator window while a profile is being applied.

User preferences

To configure the user preferences, do the following:

1. On the menu bar of the main window of Access Connections, click **Configure**.
2. Select **User Preferences**. The window opens.

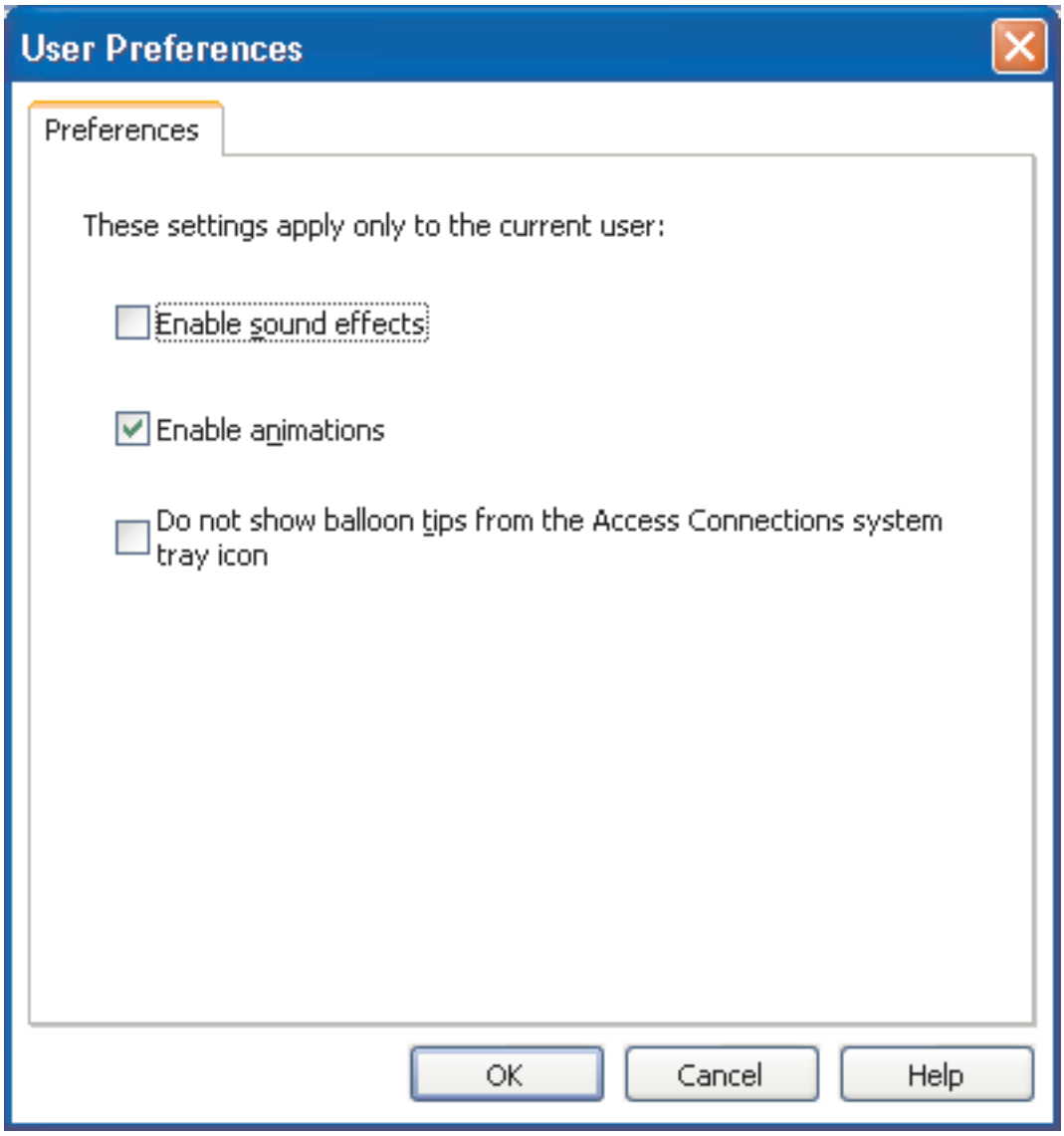

Figure 47. User preferences

3. Make the necessary changes, and click **OK**.

Preferences apply only for the current user. The following preferences can be configured for Access Connections:

Enable sound effects
Select this option to turn on sound effects in Access Connections when the status of a connection changes.

Enable animations
Select this option to turn on animation of graphics in Access Connections.

Do not show balloon tips from the Access Connections system tray icon
Select this option to turn off balloon tip information coming from the Access Connections system tray icon.

Toolbar options

By default, the main application window of Access Connections displays a toolbar that gives a quick access to frequently used functions. You can change the size of the icons in the toolbar and choose which features to include.

To customize the toolbar, do the following:

1. On the menu bar of the main window of Access Connections, click **Configure**.
2. Click **Toolbar Options**. The following window opens:

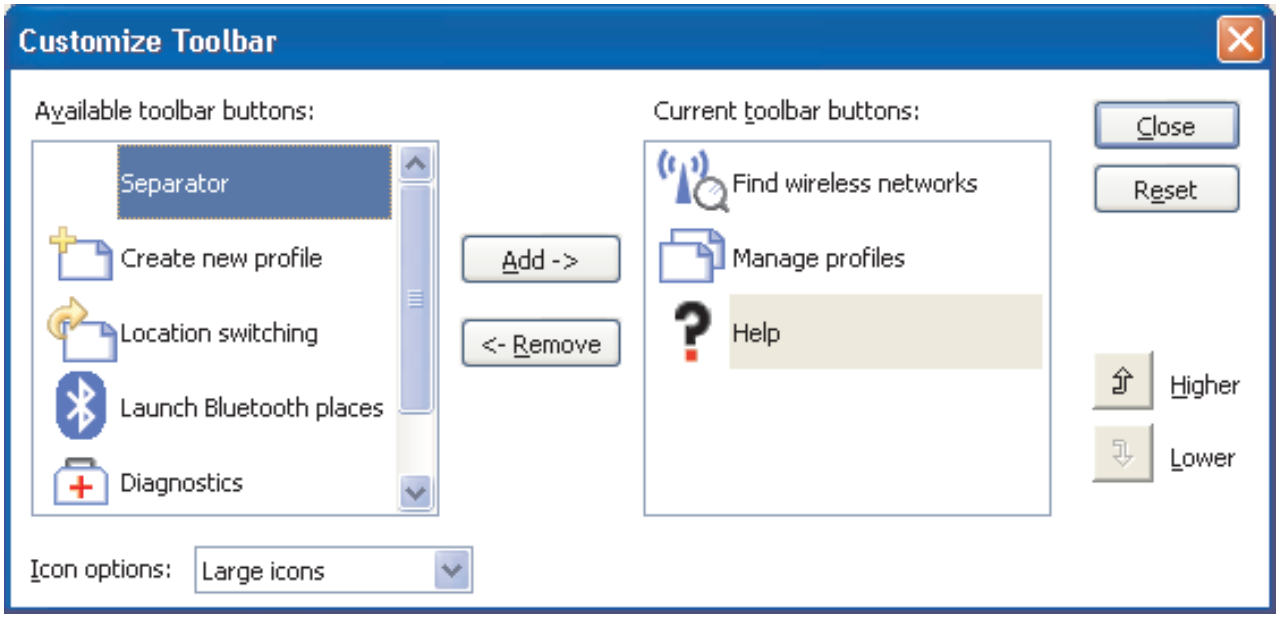

Figure 48. Customized toolbar

3. To add the icon for the function to the toolbar, choose it from the list of available toolbar buttons shown at the left of the panel, and click **Add**. To remove the icon for the function from the toolbar, choose it from the list of current toolbar buttons at the right of the panel, and click **Remove**.

   Note: Only three default buttons—**Find wireless networks**, **Manage profiles**, and **Help**—will appear with text captions in the toolbar of the main window.

4. To change the order of buttons on the toolbar, select a button from the list of current toolbar buttons, and click **Higher** to move it to the left for higher priority, or **Lower** to move it to the right for lower priority.
5. To change the size of the toolbar buttons, go to the **Icon options** menu, and select either **Large icons** or **Small icons**.
6. Click **Close**.

To reset the toolbar to default settings, do the following:

1. On the menu bar of the main window of Access Connections, click **Configure**.
2. Click **Toolbar Options**.
3. Click **Reset**.
4. Click **Close**.

Peer-to-peer options

To configure the peer-to-peer options, do the following:

1. On the menu bar of the main window of Access Connections, click **Configure**.
2. Select **Peer to Peer Options**. The window opens:

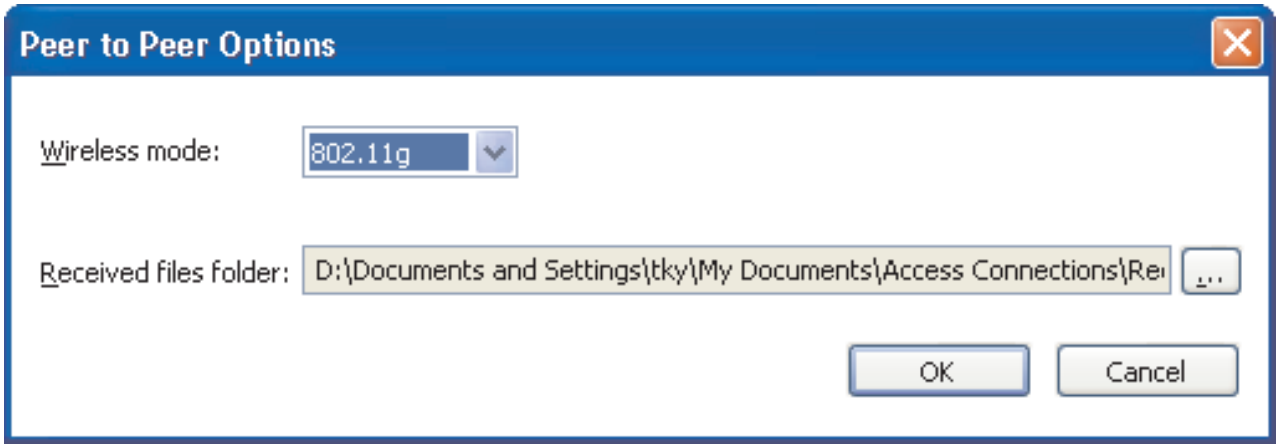

Figure 49. Peer to Peer Options window

3. Make the necessary changes, and click **OK**.

Peer-to-peer options apply to all users of this computer. The following peer-to-peer options can be configured:

Wireless mode
Select 802.11b, 802.11g, or 802.11a for **Wireless mode**.

Received files folder
Enter the file path for the **Received files folder**. Received files sent by Send File are stored in this folder.

Chapter 4. Using a wireless WAN connection

Access Connections v.4.1 supports wireless WAN mini-PCI Express devices for network connections.

To start a wireless WAN connection, you must first activate the integrated wireless WAN card in your computer. You can do that from the main Access Connections panel, as follows:

1. Click **Tools** on the main toolbar.
2. Select **Wireless Wide Area Network (WAN)** from the pull-down menu.
3. Click **Activate WAN card**. The Sierra Wireless Activation Wizard opens.

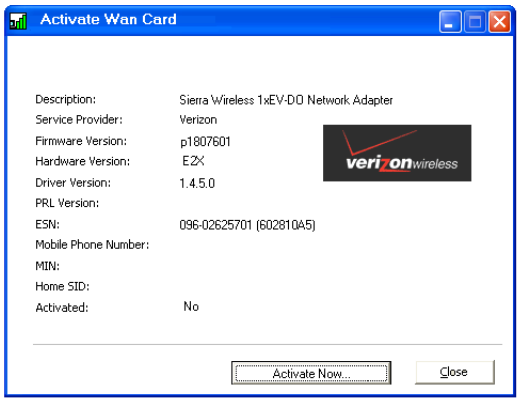

Figure 50. Activation process wizard

Creating and applying a wireless WAN profile

You can use the Access Connections profile wizard to create a profile for a wireless WAN. The first time you select a WAN device for connection to a network, Access Connections detects that the device is not configured, and automatically launches the Sierra Wireless Activation Wizard.

The wizard provides an option for the user to launch Verizon custom dialer. When Verizon custom dialer is launched, all connection and status control is displayed by the custom dialer. In this case, Access Connections main window shows minimum information (IP address, send/receive byte counts).

Note: When a wireless WAN client manager, such as VzAccess Manager, or Vodafone Mobile Connect, is running, the Fn+F5 on-screen window does not show the status of the wireless WAN adapter radio and the button for controlling the wireless radio.

When the user creates and applies a WAN location profile, Access Connections starts a process to activate wireless WAN radio, open a connection (in EvDO mode, CDMA1x mode or CDMA mode, depending on the service available at the location), and wait for an IP address to be assigned. As soon as the connection is established, details on the status of the profile are displayed, either in the main window of Access Connections or in the task tray if the related icon is clicked.

The detailed information contains the following data specific to the WAN connection:

Wireless signal condition
Strength of the signal, presented graphically.

Transmit /Receive Byte counts
The counts of bytes transmitted and received during a connection are displayed on the main window in real time. The duration of the connection is also displayed in real time, both in the main window and in the WAN status information window on the task tray.

Link to logged data
This is the connection history, which includes the date and time at which the user made the connection, and the number of bytes transmitted and received during each previous connection.

Link to Verizon Wireless web site
This is the Web link for getting information about updates.

If your computer does not have an integrated wireless WAN card, you can install a supported wireless WAN PCMCIA card. When you use a non-integrated card, your WAN connection will be managed by the wireless WAN client utility provided by your service provider. The instructions for activation come with the PCMCIA card.

Using Short Message Service (SMS) interface

Sierra Wireless Short Message Service (SMS) is a utility for sending text files. To send a message, go to the user interface window for SMS and do as follows:

1. On the main menu bar, click **Tools**.
2. Select **Wireless Wide Area Network (WAN)**.

   Note: The Wireless WAN menu in Access Connections is enabled only if an integrated wireless WAN card is used.
3. Select **Start Text Messaging**. The SMS message window opens.
4. Click **New**.
5. Enter the recipient's phone number and the message.
6. Click **Send**.

To view a received message, do as follows:

1. On the main menu bar, click **Tools**.
2. Select **Wireless Wide Area Network (WAN)**.
3. Select **Start Text Messaging**. The SMS message window opens.
4. Select the **Inbox** tab. A list of the received messages is displayed.

You can access the wireless WAN service provider to perform signup and activation tasks, view billing information, or receive customer support. Do as follows:

1. On the main menu bar, click **Tools**.
2. Select **Wireless Wide Area Network (WAN)**.
3. Select **Link to Service Provider**.

Chapter 5. Introducing a peer-to-peer connection

Access Connections v.4.1 provides a new, task-oriented way of connecting that is not based on using a location profile. This is a quick peer-to-peer connection established between users, or peers, by creating the temporary work group by use of wireless LAN device with secure file transfer feature.

Preparing the peer-to-peer connection

If you have enabled an Internet firewall, a peer-to-peer connection cannot be established unless a user with administrator privilege has created an exception rule. If you do not have this privilege, ask the computer administrator to change the firewall settings for you.

Windows Firewall (for a computer running Windows XP SP2)

1. From the **Control Panel** open the Security Center.

Figure 51. Windows Security

2. Click **Windows Firewall**.

The Windows Firewall window opens.

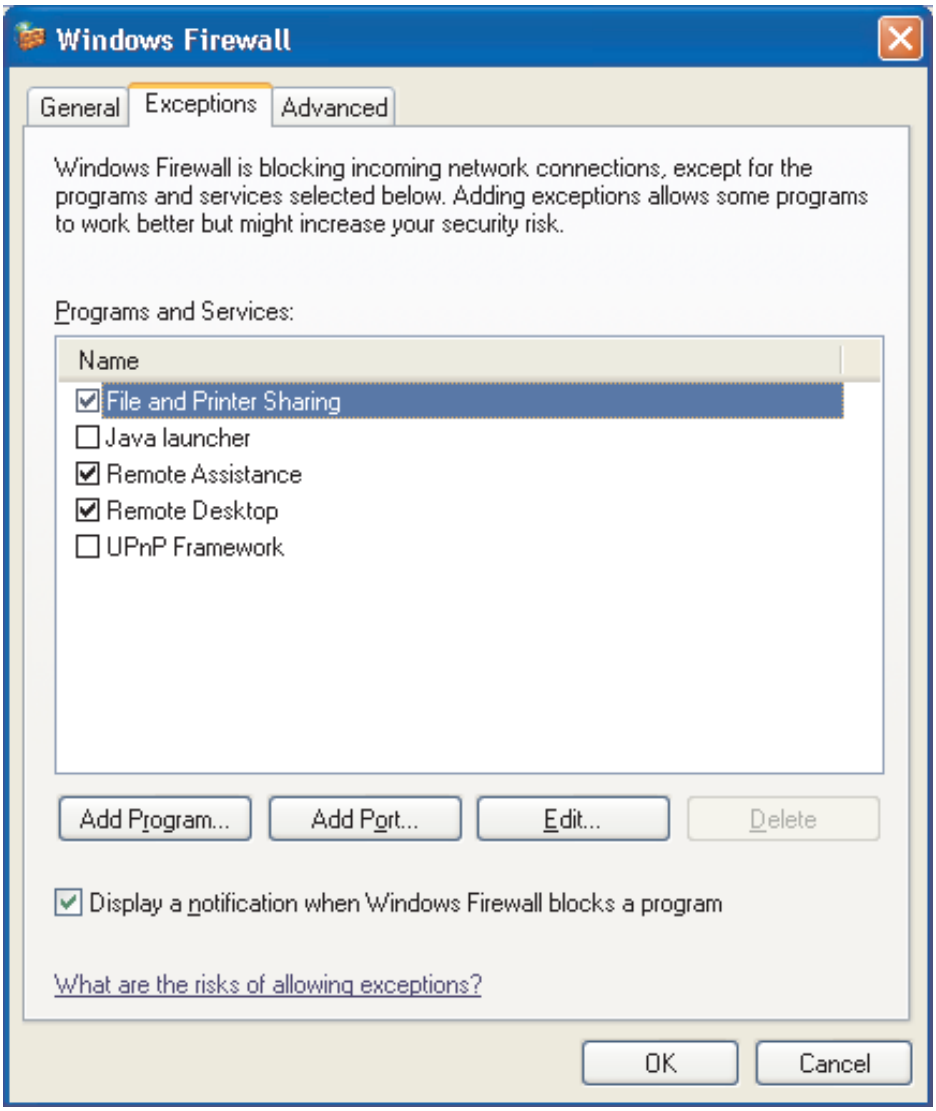

Figure 52. Windows Firewall window

3. Select the **Exception** tab, and click the **Add Program** button.

4. From the list, select **Access Connections**; then click **OK**.

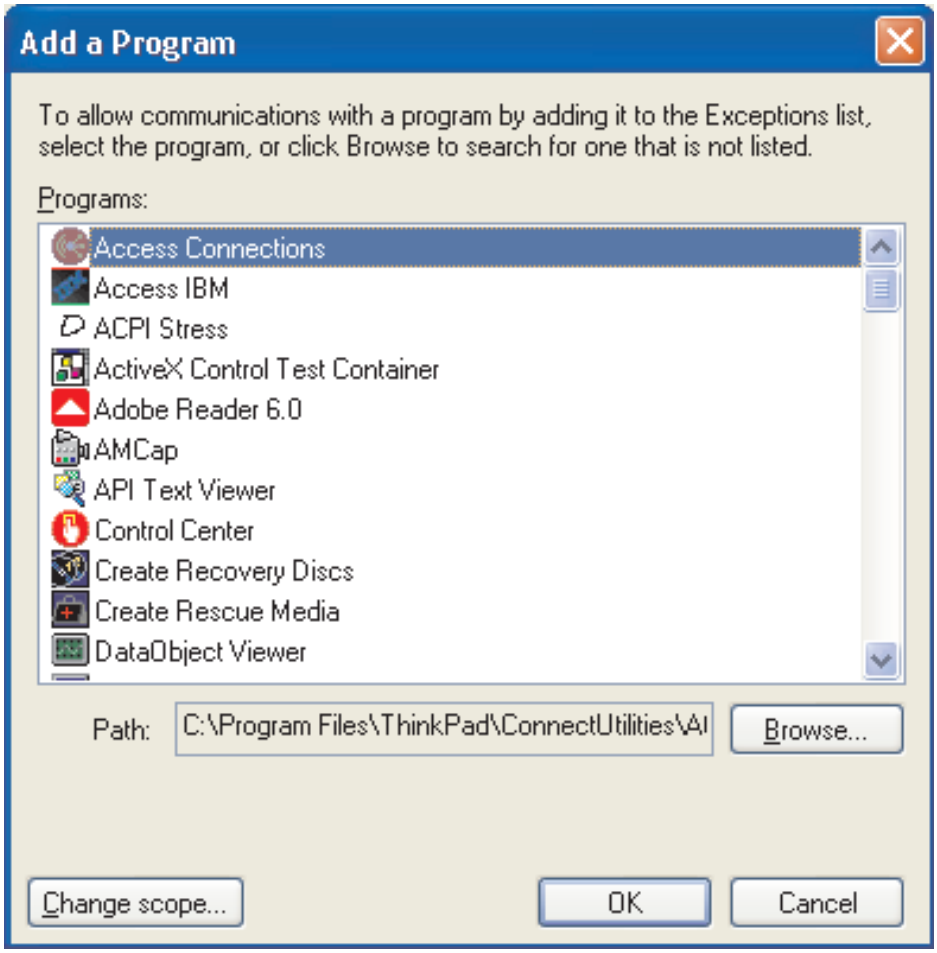

Figure 53. Add a Program window

5. The **Exception** tab opens. There, push the **Add Program** button again.
6. Click the **Browse** button, choose C:\Program Files\NetMeeting\conf.exe, and click **Open**.
7. On the Add a Program window, click **OK**. On the Windows Firewall dialog box, click **OK** again.
8. Close the Security Center.

Other firewalls

If you use a firewall other than the Windows firewall, consult your program manual to make rules covering exceptions. If your firewall does not support program control, open the ports listed in Table 1.

Table 1. Preparing the peer-to-peer connection

Application	Protocol	Port	Default Path
NetMeeting	TCP/UDP	522	C:\Program Files\NetMeeting\conf.exe
	TCP/UDP	1503	
	TCP/UDP	1720	
	TCP/UDP	1731	

Table 1. Preparing the peer-to-peer connection (continued)

Application	Protocol	Port	Default Path
Access Connections	UDP	5353	C:\Program Files\ThinkPad\ConnectUtilities\ ACMainGUI.exe
	UDP	49443	
IPSec (lsass.exe)	TCP/UDP	500	C:\Windows\system32\lsass.exe

Creating the peer-to-peer connection

To create a peer-to-peer connection, follow the steps below:

Note: Peer-to-peer connection may be blocked by a firewall. Temporarily disable the firewall program or add NetMeeting and Access Connections to exception rules. For details about configuring your computer for peer-to-peer connection, see “Preparing the peer-to-peer connection” on page 65.

1. Open the main AC window. The **Location Profiles** tab is displayed by default.

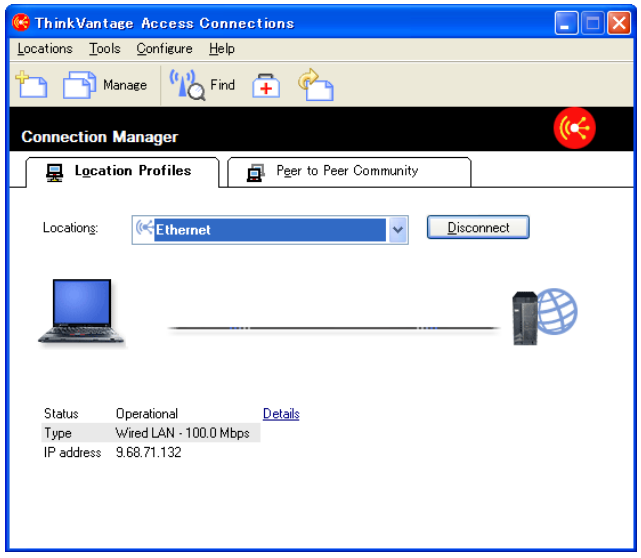

Figure 54. Main AC window—Location Profile tab

2. Click the **Peer to Peer Community** tab.

The ThinkPad Community starts, and the initial peer-to-peer window is displayed.

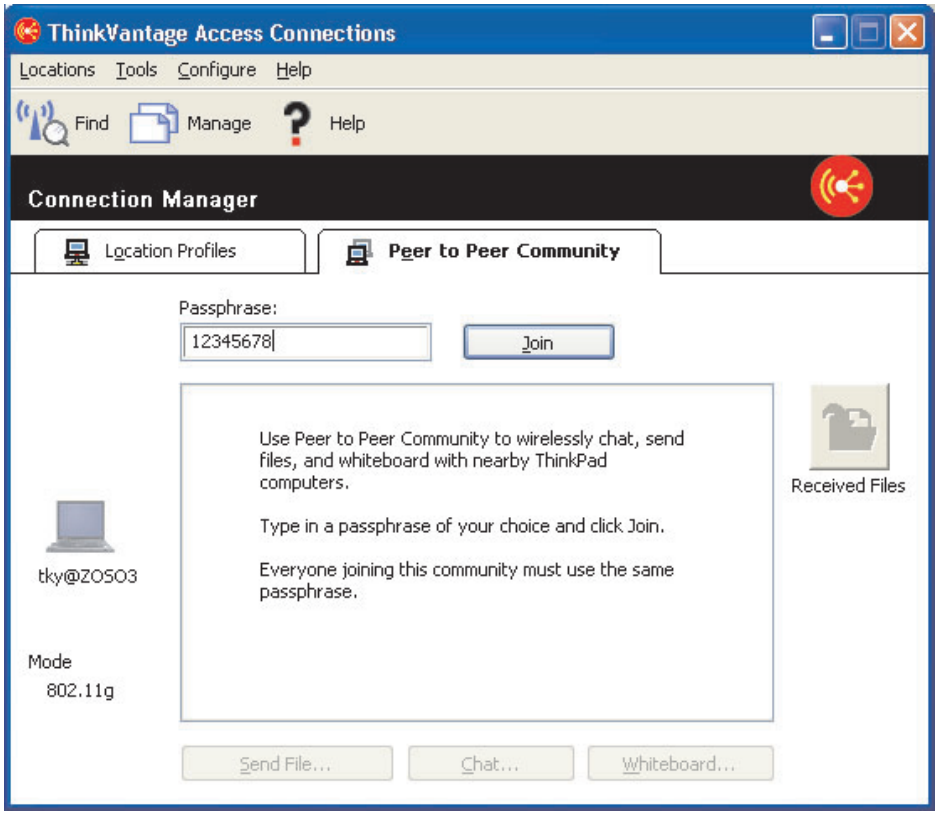

Figure 55. Peer to Peer Community tab—Join button

3. Enter a passphrase specific to the community being established. It must contain at least eight characters in UNICODE code, including quotation marks, spaces, and underscores. Each user must enter this passphrase to join the community. At start up, the Passphrase edit box is filled with the passphrase last used by the present user.

   A grayed-out ThinkPad icon, your user name, and the selected wireless mode are displayed at the left. To change the wireless mode, go to **Configure** menu. A short explanation of the use of the peer-to-peer capability is displayed in the list box at the center. The three application buttons at the bottom and the **Received Files** button at the right are disabled until the user is connected to a group.
4. Click the **Join** button.
5. ThinkPad Community starts setting up the wireless network. The following settings are configured automatically:
   - The wireless LAN adapter is automatically set to Adhoc mode (802.11 IBSS)
   - A temporary IP address is assigned.
   - Distributed DNS service is started.
   - A NetMeeting COM interface is initialized.

This process may take some time. During this process, a progress indicator is displayed. To stop applying the Adhoc setup, press the **Stop** button next to the progress indicator. ThinkPad Community restores the previous wireless adapter configurations.

Note: The **Close** button closes only the progress indicator dialog box. If this is the first use of Peer to Peer Community and NetMeeting, the NetMeeting initialization dialog appears.

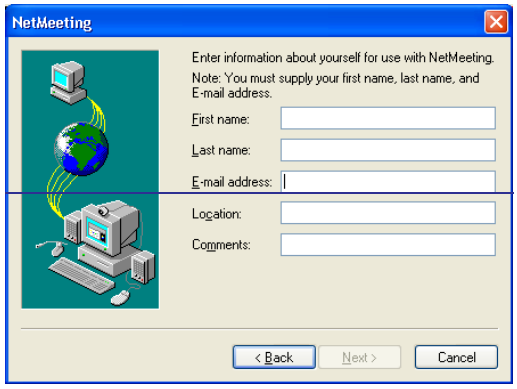

Figure 56. NetMeeting window

Enter at least your first and last name, and your e-mail address, and click **Next**.

6. When NetMeeting starts, the progress indicator dialog box disappears, and the color of the ThinkPad icon at the left changes. The application buttons remain disabled until another member is found in the neighborhood.

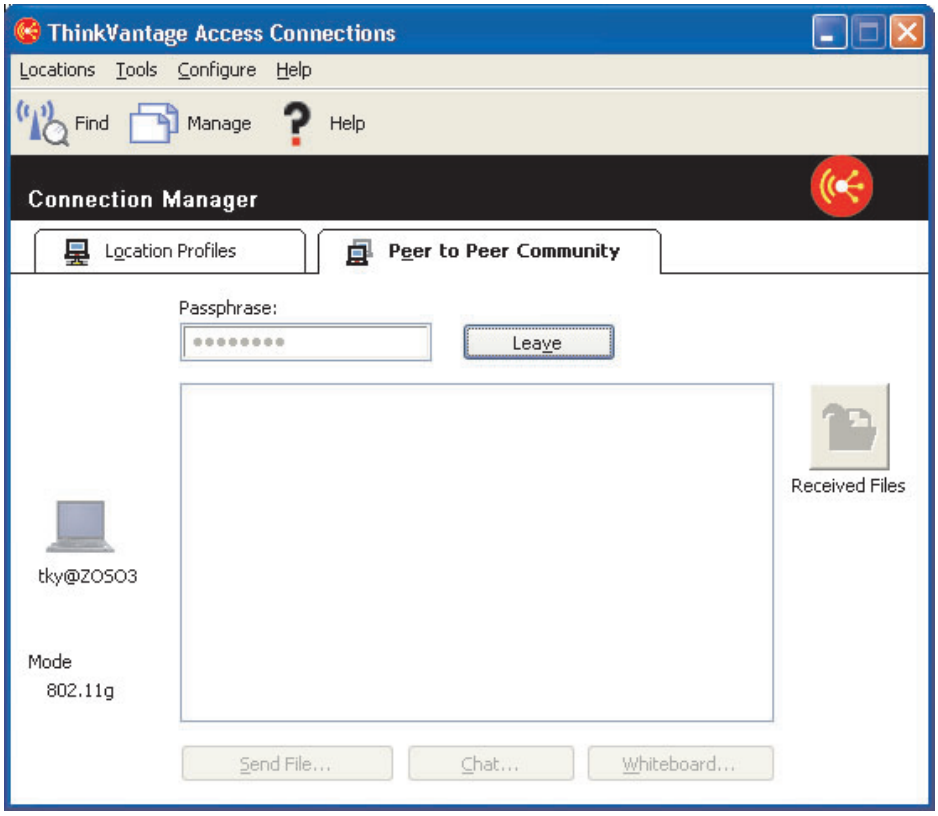

Figure 57. Peer to Peer community tab—Leave button

7. When members of the group are found, a ThinkPad icon for each of them is displayed, with the user name. The icon is grayed out until a NetMeeting connection with that member is established. When the first connection is established, the application buttons are enabled.

   For members using Windows 2000, establishing a connection may take longer.

Using peer-to-peer connection

After the peer-to-peer connection is established, you can do the following:

Send files

To send a file to other members, click the **Send File** button to start the File Transfer applet of NetMeeting. By default, the files a user receives are stored in the following folder in the user's document folder:

```
Access Connections\Received Files
```

To change the folder, go to the **Configure** menu.

Chat with members

Click the **Chat** button. The Chat applet of NetMeeting starts. A user can send a message to one or more members of the group, or to all of them.

Use Whiteboard

Click the **Whiteboard** button. The Whiteboard applet of NetMeeting starts.

The whiteboard is shared by all members.

For a detailed explanation of how to use these applets, see NetMeeting Help. To open it, click **Help** on the menu bar of each applet.

Change the configuration options

To change the following options, go to the **Configure** menu:

Note: After joining the group, you cannot change the settings.

Wireless mode (802.11 a/b/g)

For a wireless LAN adapter supporting multiple network types (for example, a, b, and g), you can switch between the modes used in Adhoc networking. The wireless adapter specifies the default mode.

Received Files folder path

You must have write access authorization to change this setting.

To enable IP security for secure mode connections...

To start a secure mode connection, enable IP security while connected. You must configure your computer first, and then enable IP security. The procedure is as follows:

- If your computer is running Windows XP with SP2 preloaded on it, install the Windows Support Tools (C:\Support\Tools). Open the C:\Support\Tools directory and double-click SETUP.EXE. Follow the instructions presented by the Setup Wizard. When you are asked to select the installation type, select **Complete**.
- If your computer is running Windows XP upgraded with SP2, go to the Microsoft Download Center (http://www.microsoft.com/downloads), and search for “Windows XP Service Pack 2 Support Tools.” Download the program into your temporary directory and execute it. Follow the instructions presented by the Setup Wizard. When you are asked to select the installation type, select Complete.
- If your machine is running Windows XP, and SP2 has not been installed, follow the installation procedure given for a computer running Windows XP with SP2 preloaded on it.
- If you have installed the OS yourself, insert the installation CD for Windows XP. If the setup program starts automatically, exit it and open the \Support\Tools directory using Windows Explorer. Then double-click SETUP.EXE, and follow the instructions presented by the Setup Wizard. When you are asked to select the installation type, select **Complete**.
- If your computer is running Windows 2000, go to the Windows 2000 Resource Kit Download page (http://www.microsoft.com/windows2000/techinfo/reskit/tools), and download “Ipsecpol.exe: Internet Protocol Security Policies Tool” to your temporary directory. You can then run that program to set up IPSecPol.exe.

Appendix A. Frequently asked questions

1. **How can I automatically connect to the network if I am using a wired connection at my desk, a wireless LAN connection in a meeting room, and a wireless LAN connection at my home?**

   Create an office location profile for both a wired LAN and a wireless LAN, using a **Best Available Network** for the type of network connection. Then, create a home location profile, using a wireless LAN network connection. Configure for automatic switching of location profiles, and select the office location profile and the home profile. The location profiles will now switch automatically.

2. **Can users without administrator privileges switch between location profiles?**

   A user who is not an administrator can switch the location profiles if the **Allow Windows users without administrator privileges to create and apply location profiles** option is selected in the network global settings.

3. **Can users without administrator privileges edit location profiles?**

   A user who is not an administrator can edit only a dial-up location profile. Such a user can create a profile if the **Allow Windows users without administrator privileges to create and apply location profiles** option has been selected in the global network settings.

4. **Can I capture the current network settings and use them in a location profile?**

   When you create a location profile, it will use the current network settings by default. If you want to use the current settings use them without change.

5. **Can I have a software application start automatically every time I connect with a particular location profile?**

   You can specify when the software should be started—before or after switching network connections—in the **Additional settings** of a location profile.

6. **How many location profiles can I create?**

   You can create as many as you need. There is no maximum.

7. **To use the latest Access Connections, which wireless LAN device drivers should I install on my computer?**

   Be sure to select the correct wireless LAN device driver. Access Connections uses new functions provided by the wireless LAN device driver, such as the 802.1x authentication type. For easy and safe installation of Access Connections, you can download the Access Connections plus wireless LAN driver pack. If you install this package, wireless LAN connections and all the necessary device drivers are detected and installed automatically.

8. **Does Access Connections have a silent install function?**

   If you add ″-s″ to the ″setup.exe″ installation command for Access Connections, silent or unattended installation starts. If a profile distribution file (*.loa) is in the same folder, it is automatically imported.

9. **If I am an administrator of Access Connections, what kind of functions can I use?**

   You can create a package to distribute your own location profiles to other computers. You can also include the settings in the package which is convenient if you use many computers in the same network environment. To become an administrator, go to http://www.pc.ibm.com/us/think/thinkvantagetech/accessconnections.html, and download and install the needed files on your ThinkPad computer.

10. **If I log on to Windows with a different user ID, are there any differences in the operations of Access Connections?**

    The differences are listed in the table:

Table 2. Differences in the operations of Access Connections when different user IDs are used

Abilities	Administrator	Power Users	Non-administrator
Be an administrator of Access Connections	Yes	No	No
Change the configurations [1]	Yes	Yes	Partially yes
Create, modify, or delete location profiles. [2]	Yes	Yes	Yes [3]
Change the configuration of automatic switching of location profiles.	Yes	Yes	No
Renew or release an IP address by use of diagnostic tools.	Yes	Yes	No
Export location profiles.	Yes	Yes	No
Search for a wireless network and connect to it.	Yes	Yes	Yes [3]
Switch from one location profile to another.	Yes	Yes	Yes [3]

[1]: You cannot change settings that have been imported from the distribution package and made subject to restrictions.

[2]: You cannot change settings that have been imported from the distribution package and made subject to restrictions. However, all users can create, modify, or delete a location profile for dial-up.

[3]: In the network global settings, you need to select the option Allow Windows users without administrator privileges to create and apply location profiles.

11. **I cannot switch location profiles in Windows 2000.**

    If Windows automatically configures network connections, disable the configuration as follows:

    a. Open **Control Panel**; then double-click **Administrative Tools**. Double-click **Services**, then **Wireless Configuration**.

    b. For **Startup Type**, select **Disabled**.

12. **Can the Fn+F5 key combination be used on all ThinkPad computers to enable or disable the wireless features?**

    You can use that key combination to enable or disable the wireless features only if ThinkPad Hotkey Features Version 1.03.0391 or later is installed on your computer. If it is installed, the wireless icon is printed on the F5 key.

13. **Why am I prompted to enter a comment when I am using an Ethernet connection?**

    You are prompted to type a comment because Access Connections has found a new network device for an automatic network connection. Access Connections recognizes this network as the most suitable one for the current location profile. The next time you connect to this network, this location profile is selected automatically.

14. **I cannot configure the fixed IP address.**

    If you select **Best Available Network** for the network connection type, you cannot configure a fixed IP address. Select wired LAN or wireless LAN only.

15. **Why is the Ethernet location profile not displayed in the automatic location switching list?**

    Ethernet location profiles with fixed IP addresses are excluded from the automatic switching list.

16. **If I am using a wireless LAN connection, I cannot log on to the domain.**

    The wireless LAN network connection is more vulnerable to an unauthorized access than the wired LAN network connection, because the wireless connection uses radio waves. If you try to connect to the wireless LAN network, the authentication process is required. Until the authentication process is completed, you cannot get access to the network. If it takes a long time to get access to the network after logging on to Windows, you may not be able to log on to the domain. Instead, your computer may try to get access to copies of the most recently requested network that have been stored in the cache of your computer. If the computer gets access to the copies locally, you cannot use some functions that are covered by logon script or logon policies. To make sure that you can log on to the domain, Access Connections starts the authentication immediately before the process of logging on to Windows is completed. If you use IEEE 802.1x Authentication, such as EAP-LEAP, EAP-PEAP, or EAP-TTLS, Access Connections changes the sequence for logging on, so that the authentication process is completed first. If you use Static WEP Keys or Wi-Fi Protected Access—Pre Shared Key (WPA-PSK), refer to the instructions in Wireless security settings section.

17. **When I am using peer-to-peer mode, I cannot select channels.**

    In peer-to-peer mode, because Access Connections searches for suitable channels for your SSID (network name), you do not need to select channels. For the wireless standard, IEEE 802.11a/b/g, Access Connection applies the default setting for the wireless adapter. To change this manually, click **Configure** menu in the main window of Access Connections, and select **Peer to Peer Options**. If you cannot connect with other members because of differences between wireless modes, leave the group and select a wireless mode that all members can use.

Appendix B. Command line interface

Access Connections can accept commands entered from the command line to switch between location profiles and to import or export location profiles. You can enter the following commands from a command prompt window, or you can create batch files for use by other users. Access Connections does not need to be running before these commands are executed.

Apply a location profile.

```
<path>\qctray.exe /set <location profile name>
```

Disconnect a location profile.

```
<path> \qctray.exe /reset <location profile name>
```

Delete a location profile.

```
<path> \qctray.exe /del <location profile name>
```

Import a location profile (valid only for files with .loc extension.)

```
<path> \qctray.exe /imp <location profile path>
```

Import a location profile by use of GUI (valid only for files with .loc extension.)

```
<path> \qctray.exe /GUIImp <location profile path>
```

Perform silent import of all profiles.

```
<path> \qctray.exe /importsilently
```

Import a signature file.

```
<path> \qctray.exe /importsignaturefile
```

Export a location profile (valid only for files with .loc extension.)

```
<path> \qctray.exe /exp <location profile path>
```

Migrate all location profiles.

```
<path> \qctray.exe /migratelocations
```

Apply dummy SSID profile for wireless cards (regardless of which profile was most recently active) and return immediately. Do not turn off the Wireless Radio.

```
<path> \qctray.exe /disconnectwl
```

Close AcMainGUI, AcTray, AcWlIcon modules.

```
<path> \qctray.exe /exit
```

Enter a special monitor mode in which all roaming is blocked, Ethernet as well as Wireless. Also when the third party application that has called this API is closed, reset the monitor mode.

```
<path> \qctray.exe /setmonitormode
```

Reset the monitor mode.

```
<path> \qctray.exe /resetmonitormode
```

Kill all Access Connections processes. Since this requires administrative privileges, the command will be routed through AcPrfMgrSvc to close all other Access Connections processes except for profile manager service.

```
<path> \qctray.exe /killac
```

Restart all Access Connections processes. Since this requires administrative privileges, the command will be routed through AcPrfMgrSvc.

```
<path> \qctray.exe /startac
```

Find Wireless networks.

```
<path> \qctray.exe /findwlnw
```

Display QCTRAY help information.

```
<path> \qctray.exe /help
```

Appendix C. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you. This appendix contains information about where to go for additional information about Lenovo and Lenovo products, what to do if you experience a problem, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the computer is turned on.
- Apply the suggestions for troubleshooting in the computer documentation.
- Use the diagnostic tools that come with your computer. Information about the diagnostic tools is in the *Hardware Maintenance Manual* and *Service and Troubleshooting Guide* for your computer.
- Go to the Support Web site at http://www.lenovo.com/think/support to check for technical information, hints, tips, and new device drivers or to submit a request for information.
- If your computer is equipped with the wireless radio switch, make sure that it is on.

You can solve many problems without outside assistance by following the troubleshooting procedures that are provided in the online help or in the publications that are provided with your computer and software. The information that comes with your computer also describes the diagnostic tests that you can perform. Most PC systems, operating systems, and programs come with information that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the information for the operating system or program.

Using the documentation

Information about your Lenovo system and preinstalled software, if any, is available in the documentation that comes with your system. That documentation includes printed books, online books, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. Lenovo maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.lenovo.com/think/support and follow the instructions.

Getting help and information from the World Wide Web

The Lenovo Web site has up-to-date information about Lenovo products, services, and support at http://www.lenovo.com/think/support

Appendix D. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
500 Park Offices Drive, Hwy. 54
Research Triangle Park, NC 27709
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO GROUP LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been

estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Appendix E. Trademarks

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Lenovo
ThinkPad
ThinkVantage

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM (used under license)
Approach
Lotus
Lotus Notes
Lotus Organizer
Freelance Graphics
SmartSuite
Word Pro
1-2-3

Microsoft, Windows, and Outlook are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, LANDesk, and Intel SpeedStep are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Index

Special characters

A

B

C

D

E

F

I

L

M