

Intel PROSet/Wireless 2915ABG Network Connection User's Guide

With your wireless network card, you can access wireless networks, share files or printers, or even share your Internet connection. All of these features can be explored using a wireless network in your home or office. This wireless LAN solution is designed for both home and business use. Additional users and features can be added as your networking needs grow and change.

 **NOTE:** This software is compatible with the Intel® PROSet/Wireless 2915ABG Network Connection and the Intel® PROSet/Wireless 2200BG Network Connection.

[Making a Basic Network Connection in Windows XP](#)

[Making a Basic Network Connection in Windows 2000](#)

[Using the Intel PROSet for Wireless Utility](#)

[Using Intel PROSet/WirelessProfiles](#)

[Security Overview](#)

[Configuring Advanced Network Security Settings in Windows XP](#)

[Configuring Advanced Network Security Settings in Windows 2000](#)

[Specifications](#)

[Regulatory Information](#)

[Troubleshooting](#)

[Glossary](#)

Information in this document is subject to change without notice.

© 2000–2004 Dell Inc. All rights reserved.

The copying or reproducing of any material in this document in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden. The trademarks *Dell*, *Latitude*, *Inspiron*, the *DELL* logo, and *TrueMobile* are trademarks of Dell Inc. *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the

entities claiming the marks and names or their products. Dell disclaims any proprietary interest in trademarks and trade names other than its own.

August 2004

[Back to Contents](#)

Making a Basic Network Connection in Windows XP: Intel® PRO/Wireless 2915ABG Network Connection User's Guide

[Connecting to a Network in Windows XP](#)

[Viewing the Status of Your Wireless Connection](#)

Connecting to a Network in Windows XP

The information in this User's Guide assumes that your wireless card and the software are already installed in your system. If you did not receive your wireless card as part of a system, refer to the Setup Guide that came with your wireless card for hardware and software installation instructions. You can check your system to verify that the wireless card is installed.

To see if you have a wireless card installed:

1. From your Windows desktop, right-click **My Computer** and select **Properties**.
2. From the Hardware tab, click **Device Manager**.
3. Double-click **Network adapters**.

If the wireless card is installed you will see **Intel® PRO/Wireless 2915ABG Network Connection**. If the wireless card is not installed this name will not be displayed.

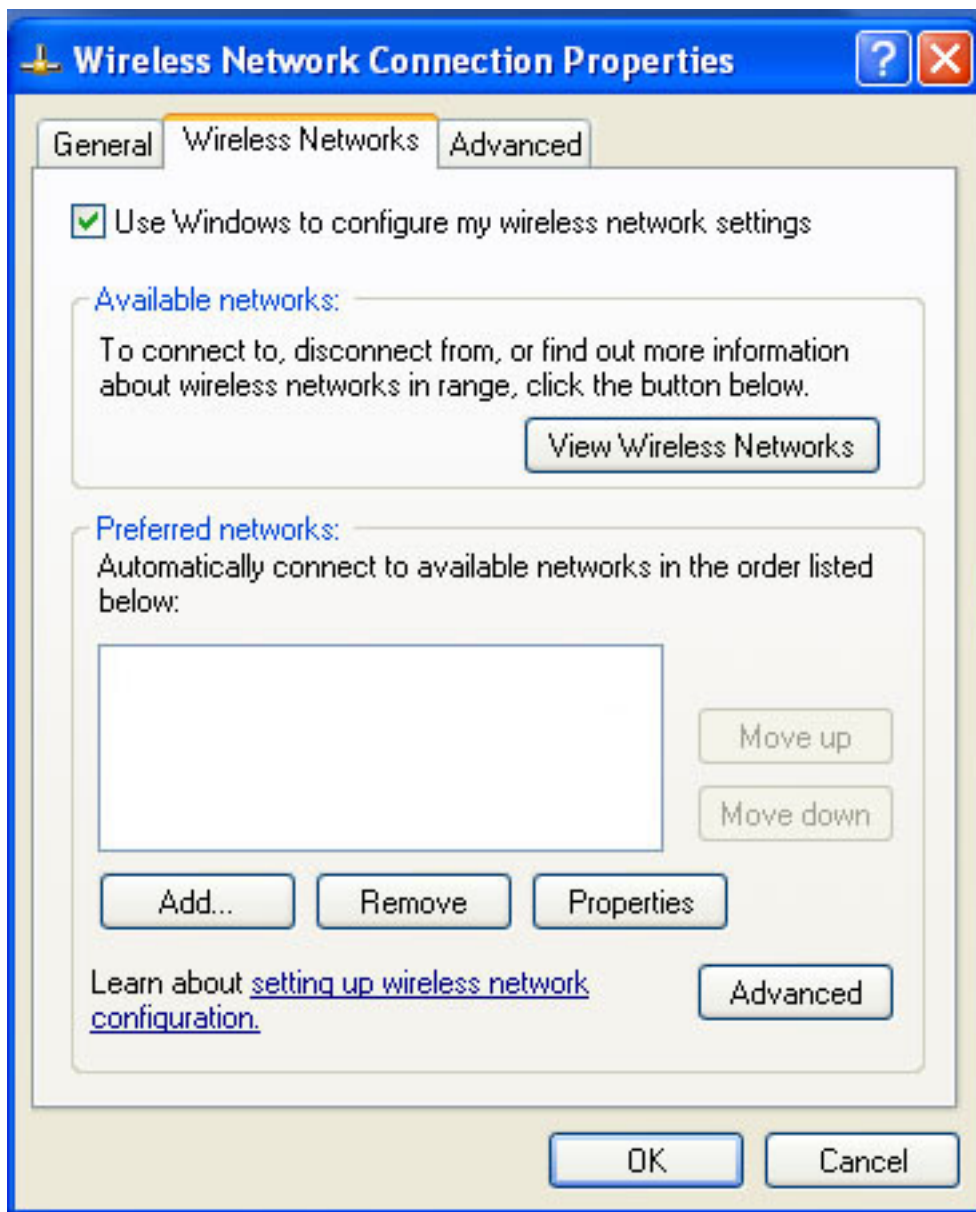
If you are using Windows XP, it is recommended that you follow the steps below to configure your wireless network connection. You can also choose to use Intel® PROSet/Wireless to configure your wireless card. This is discussed in the [Making a Basic Network Connection in Windows 2000](#) section.

 **NOTE:** If you are using Windows XP (Service Pack 2) Category View some of the dialogs shown in the following examples may appear different from those on your screen. To switch from Category View to Classic view, click **Start** à **Control Panel** and on the navigation bar click **Switch to Classic View**.

Connecting to a Network

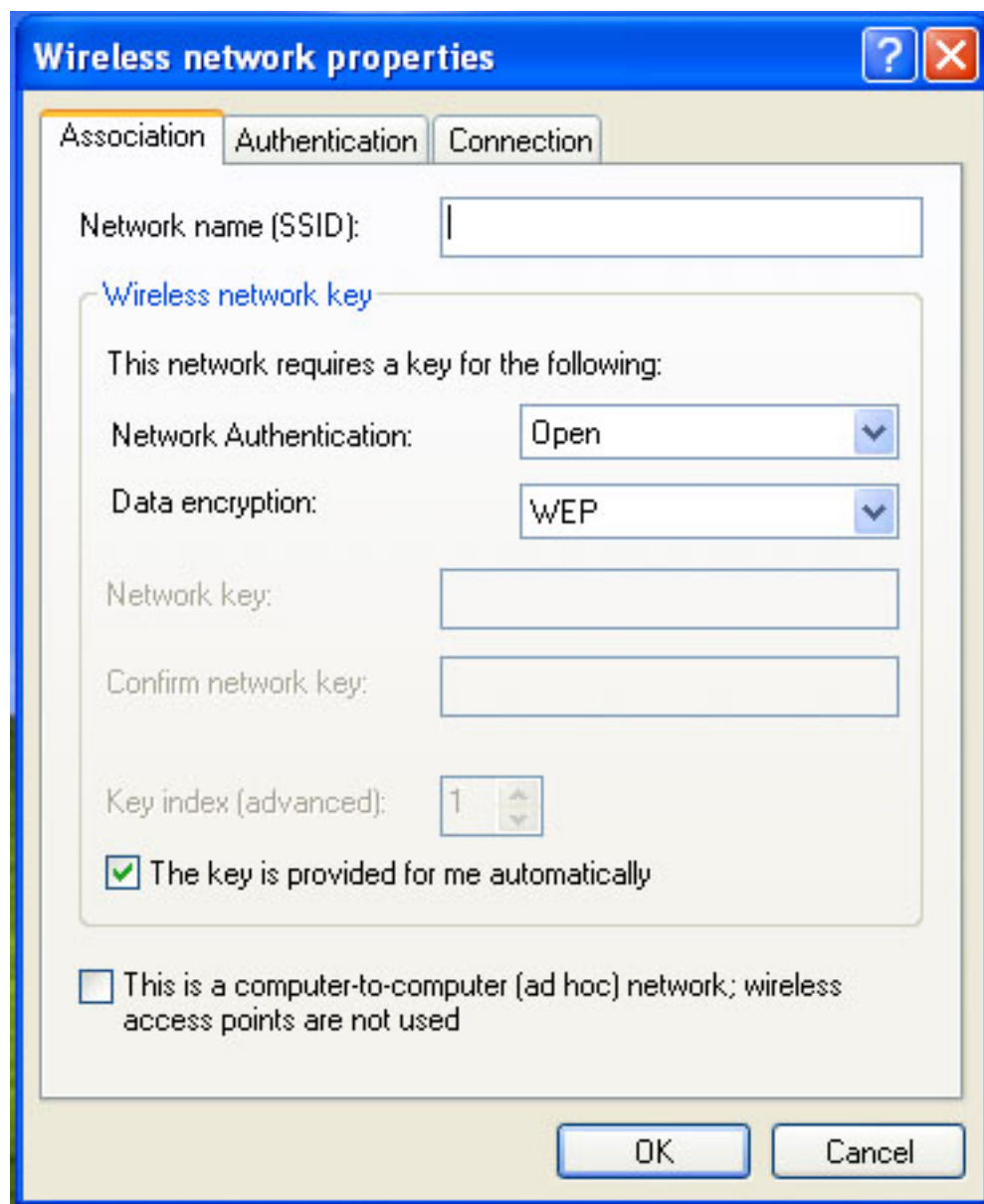
Before attempting to connect to your network, make sure that your [access point](#) or [wireless router](#) is connected correctly. Please consult your access point or wireless router documentation to configure your access point or wireless router. You should now choose the type of security for your wireless network. Most home networks use either no security or Wired Equivalent Privacy ([WEP](#)) encryption. Additional security settings are also available that are typically used in corporate environments or for advanced users who require higher levels of security.

1. Right-click the **Intel® PROSet/Wireless icon** on the task tray and click **Open Microsoft client**. The Wireless Network Connection Properties dialog opens:



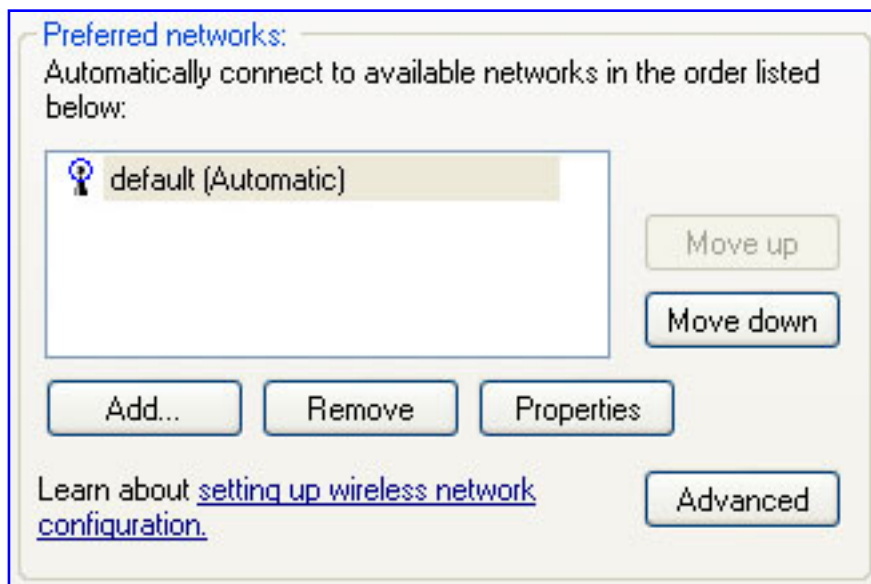
 **NOTE:** The names of wireless networks your computer can see are shown under **Preferred networks**. The name of your network is usually shown here.

2. On the **Wireless Networks** tab, under Preferred networks, click **Add**. The **Wireless network properties** dialog opens:

The image shows a Windows XP dialog box titled "Wireless network properties". It has three tabs: "Association", "Authentication", and "Connection". The "Association" tab is selected. Inside the dialog, there is a text field for "Network name (SSID)". Below it is a section titled "Wireless network key" which contains the text "This network requires a key for the following:". Under this text are two dropdown menus: "Network Authentication" set to "Open" and "Data encryption" set to "WEP". Below these are two text fields for "Network key" and "Confirm network key". There is also a "Key index (advanced)" spinner box set to "1". A checkbox labeled "The key is provided for me automatically" is checked. At the bottom, there is an unchecked checkbox labeled "This is a computer-to-computer (ad hoc) network; wireless access points are not used". At the very bottom of the dialog are "OK" and "Cancel" buttons.

 **NOTE:** The names of wireless networks your computer can see are shown under **Available Networks**. For Windows XP SP2, it is necessary to Click on **View Wireless Networks** to see a list of available networks. The name of your network is usually shown here. If a blank network name (SSID) is received from a [silent mode](#) wireless router, there will be no entry for that network in the available networks list. To associate with a "silent mode" wireless router, a new profile must first be created before connection. After connection, the associated SSID can be viewed in the available networks list and in the preferred networks list.

3. Enter the name of your network in the **Network name (SSID)** field.
4. Click **OK**. The new network name appears in the **Preferred networks** list:



Adding an infrastructure network

Network security must now be configured. For a home wireless network, you can choose not to have security, or you can configure your network for WEP security. If there is no network security, anyone can access your wireless network. WEP security provides some level of security for your wireless network. Additional advanced security settings are also available that are typically used in corporate environments or for advanced users who require higher security levels. You must ensure that the security settings on the access point exactly match those chosen for the wireless connection. Choose the appropriate link below for the security type you want to use.

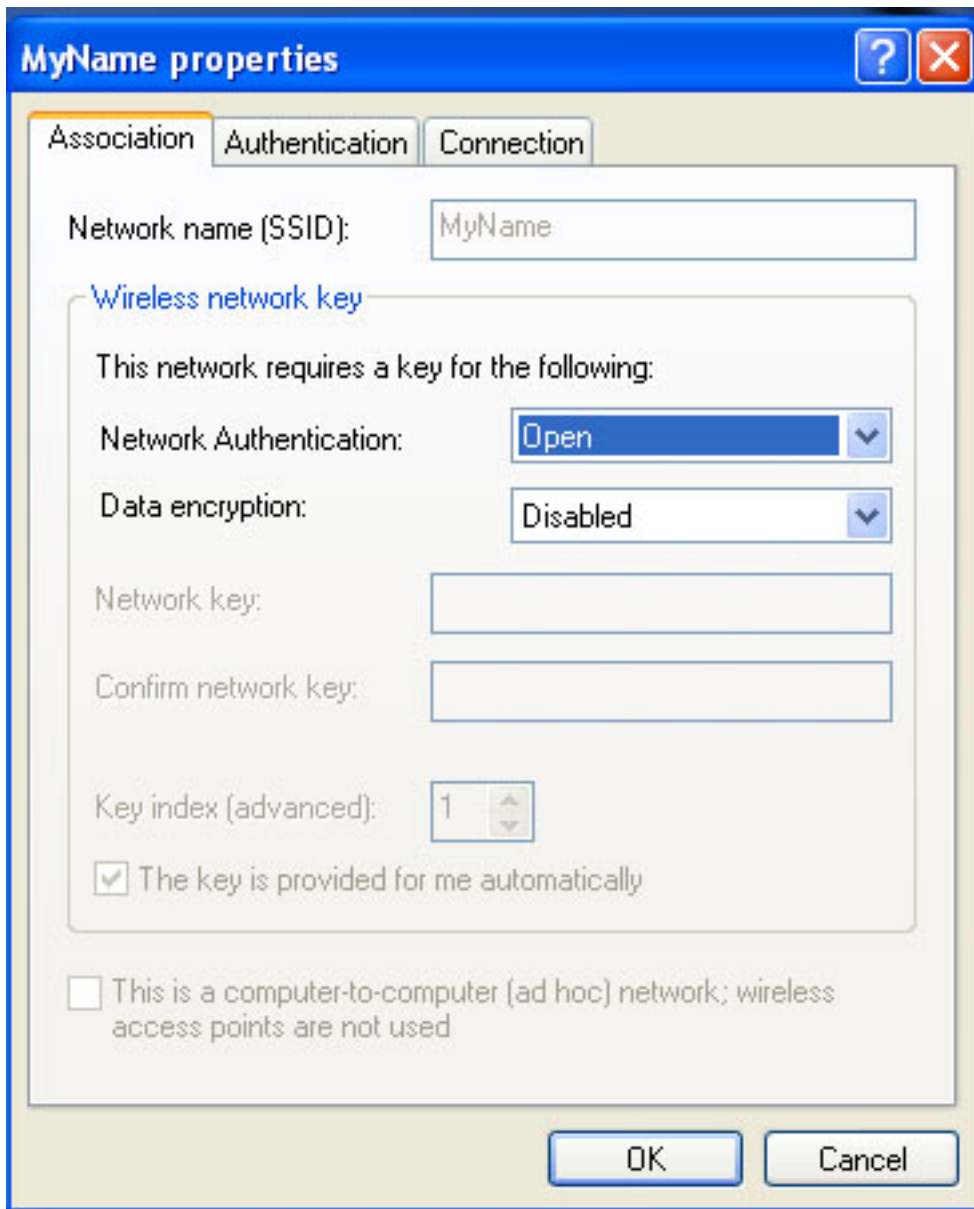
- [Configuring your Infrastructure Network with No Security](#)
- [Configuring your Infrastructure Network with WEP Security](#)
- [Configuring Advanced Network Security Settings in Windows XP](#)
- [Configuring Advanced Network Security Settings Using Intel® PROSet for Wireless](#)

Configuring your Infrastructure Network with No Security

1. Right-click the Intel® PROSet/Wireless Network icon on the task tray and click **Open Microsoft client**. The Wireless Network connection Properties dialog opens (see [Connecting to a Network](#)).
2. On the Wireless Network Connection Properties dialog (see [Connecting to a](#)

[Network](#)), click to select your wireless network in the **Preferred networks** section.

3. Click **Properties**. The **your wireless network Properties** dialog opens:



4. From the **Network Authentication** drop-down menu, click to select **Open**.



NOTE: Earlier versions of Windows XP software may not contain these drop-down menus. If you are using one of these earlier versions, click to deselect the **Data encryption (WEP enabled)** checkbox and skip to step 5.

5. From the **Data encryption** drop-down menu, click to select **Disabled**.
6. To save your settings on this dialog, click **OK**.

7. To close the Wireless Network Connection Properties dialog, click **OK**.

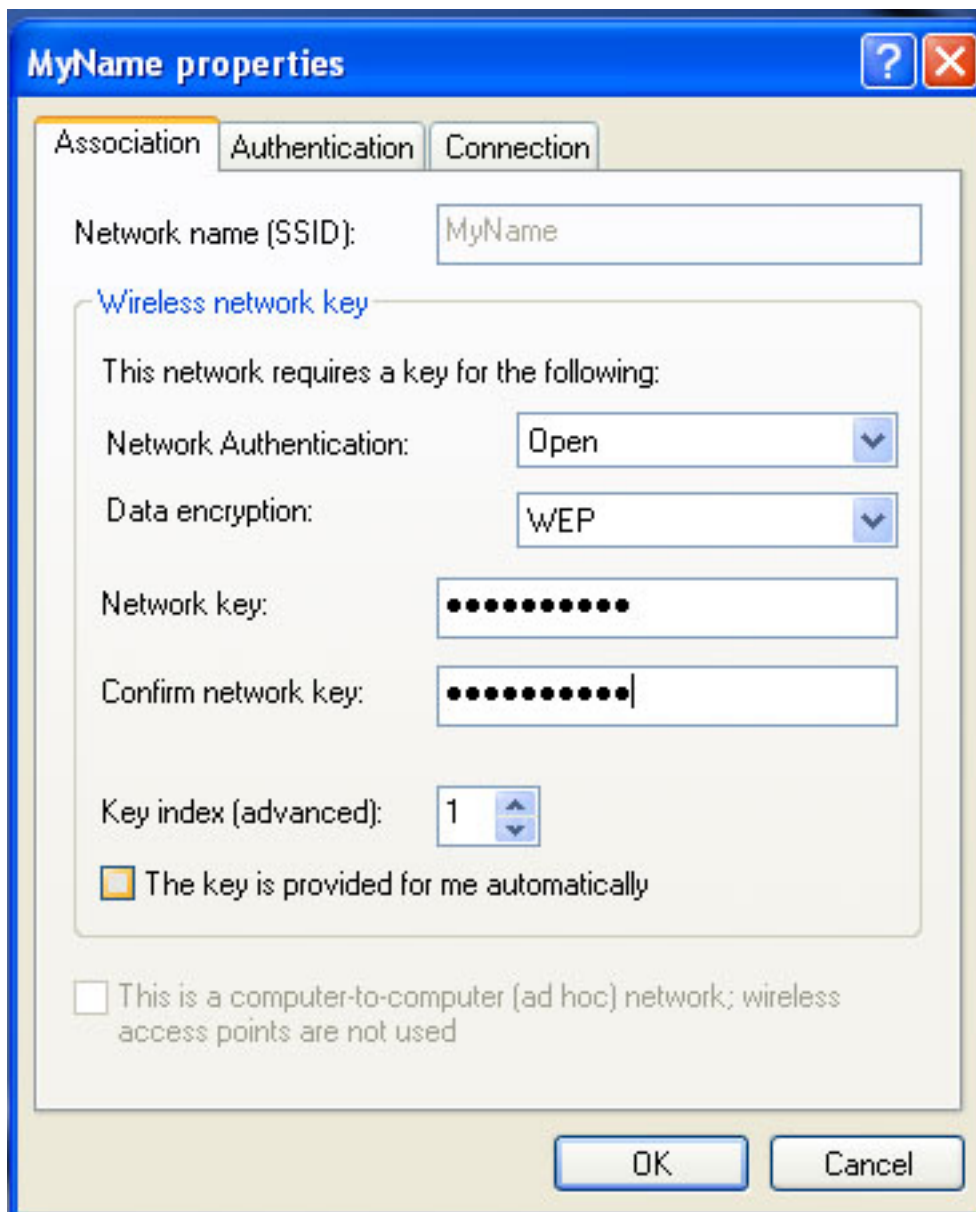
Your network configuration is now complete. Continue to [Viewing the Status of your Wireless Connection](#).

Configuring your Infrastructure Network with WEP Security

1. On the Wireless Network Connection Properties dialog (see [Connecting to a Network](#)), click to select your wireless network in the **Preferred networks** section.
2. Click **Properties**. The **Wireless Network Properties** dialog opens.
3. From the **Network Authentication** drop-down menu, select **Open**.

 **NOTE:** Earlier versions of Windows XP software may not contain these drop-down menus. If you are using one of these earlier versions, click to select the **Data encryption (WEP enabled)** checkbox and skip to step 5.

4. From the **Data encryption** drop-down menu, select **WEP**.
5. Click the checkbox to deselect **The key is provided for me automatically**.
6. Type the WEP network key in the **Network key** field. Your **Network key** must exactly match the access point's network key. Your Network key will be either 5 or 13 ASCII (text) characters, or 10 or 26 hexadecimal (0-9, A-F) characters. The person who configured your access point is the only one who knows your network key.
7. Type this key again in the **Confirm network key** field. The settings are shown in the following illustration:



8. To save your settings, click **OK**.
9. To close the Wireless Network Connection Properties dialog, click **OK**.

Your network configuration is now complete. Continue to [Viewing the Status of your Wireless Connection](#).

Viewing the Status of your Wireless Connection

The quality of your wireless connection is affected by:

- The strength of your wireless networking signal

- The level of noise created by other devices in your home or office
- The location and environment in your home or office

The quality of your wireless network is indicated by the Wireless Network Connection icon, located in the lower right corner of your Windows desktop. Point to this icon for a description of your signal quality.

NOTE **NOTE:** It is also possible to view the current status of your wireless connection from the Intel® PROSet/Wireless main screen. To open PROSet/Wireless, double-click the PROSet icon located in the lower right corner of your Windows desktop.

[Back to Top](#)

[Back to Contents](#)

[Back to Contents](#)

Making a Basic Network Connection in Windows 2000: Intel® PRO/Wireless 2915ABG Network Connection User's Guide

[Connect to a Network in Windows 2000](#)

[Viewing the Status of your Wireless Connection](#)

Connecting to a Network using Windows 2000

This document assumes that your wireless card is already installed in your system and the software has been installed. If you did not receive your wireless card as part of a system, refer to the Setup Guide that came with your wireless card for hardware and software installation instructions.

To see if you have a wireless card installed:

1. From your Windows desktop, right-click **My Computer** and select **Properties**.
2. From the Hardware tab, select the **Device Manager** button.
3. Double-click **Network adapters**.
4. If a supported wireless card is installed, you will see either **Intel® PROSet/Wireless 2200BG Network Connection** or **Intel) PRO/Wireless 2915ABG Network Connection**. If a supported wireless card is not installed this name will not be displayed.

If you are using Windows 2000, you must use Intel® PROSet/Wireless to configure your wireless card. This procedure is discussed in this section.

 **NOTE: USING WINDOWS XP:** It is recommended that you use Windows XP to configure profiles for your network connections. However, you can also use Intel® PROSet/Wireless to create your profiles. If you need to configure profiles using Cisco specific settings such as [LEAP](#) you will also need to use Intel® PROSet/Wireless. Refer to [Making a Basic Network Connection in Windows XP](#) for information about configuring your wireless network profiles.

Configuring a Network Profile in Infrastructure Mode using Windows 2000

To connect to a wireless network, you must first configure a network profile for that network on your computer using Intel® PROSet/Wireless. Refer to [Using Intel® PROSet/Wireless](#) for instructions about how to launch Intel® PROSet/Wireless.

You can connect to a network by first creating a new profile using the Profile Wizard, and then selecting that profile to connect to the network access point using the Connect button. Refer to [Creating a profile](#) for more information.

Follow the applicable instruction set below, based on whether the network requires network security key information (check with your network administrator or access point installer to see if network key information is required).

- [Configuring your Infrastructure Network with no security](#)
- [Configuring your Infrastructure Network with WEP Security](#)

Configuring your Infrastructure Network with No Security

To configure a new profile with no security:

1. Double-click the **Intel® PROSet/Wireless** icon in the desktop task tray, or click **Start** à **Programs** à **Intel® PROSet/Wireless** à **Intel® PROSet/Wireless**. (Be sure you are using Intel® PROSet/Wireless and not Microsoft Client to configure a new profile.)
2. From the Intel® PROSet/Wireless dialog, under Profiles, click **Add**. The General Settings dialog opens:

Create Wireless Profile

Profile Name: Wireless

General Settings

Security Settings

General Settings

Profile Name: Wireless

Wireless Network Name (SSID): Wireless

Operating Mode:

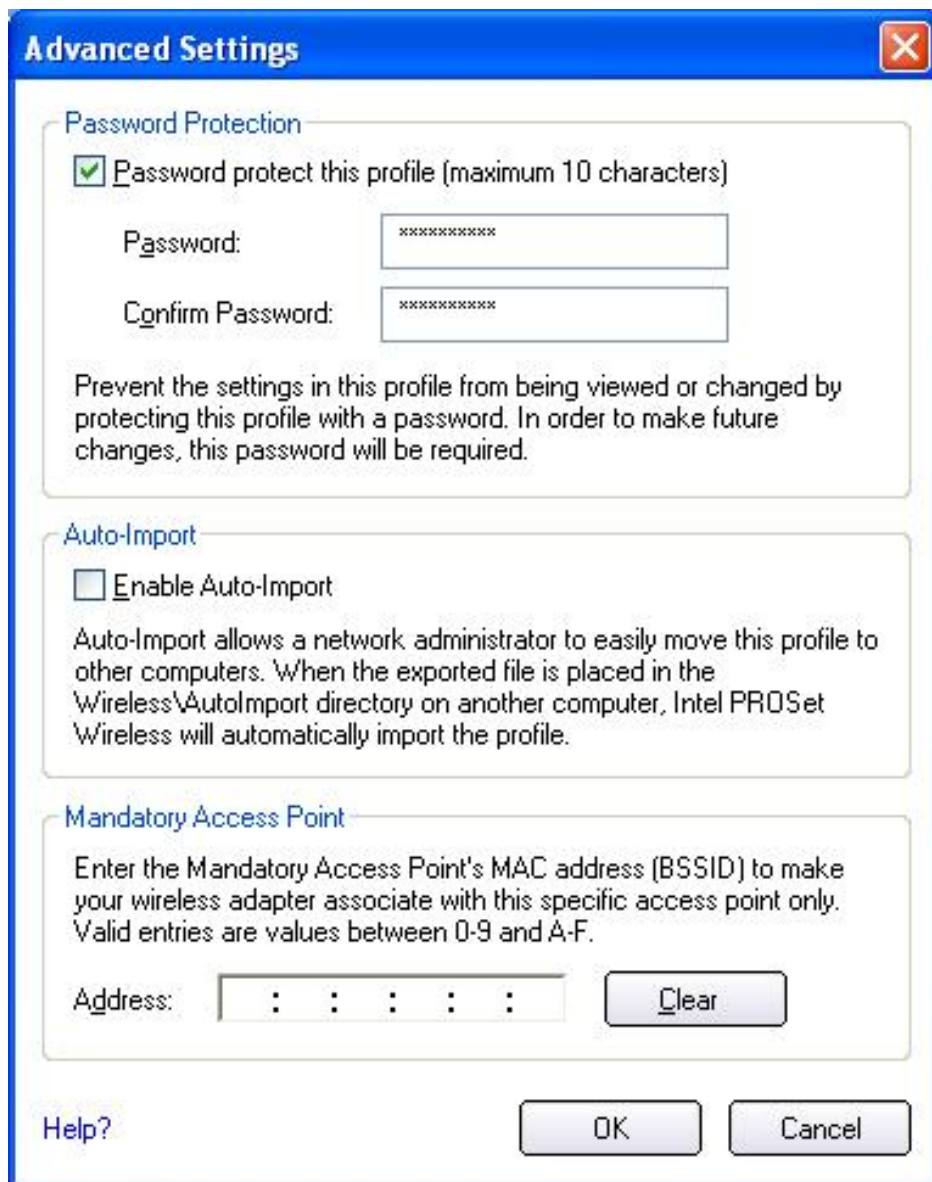
☒ Network (Infrastructure) - Connect to wireless networks and/or the internet.

☐ Device to device (Ad hoc) - Connect directly to other computers.

Advanced...

Help? << Back Next >> OK Cancel

3. Enter the Profile Name and Wireless Network Name (SSID) in the appropriate fields.
4. Select **Network [Infrastructure]**. If you want to assign a password for this profile, click **Advanced**. The Advanced Settings dialog opens:

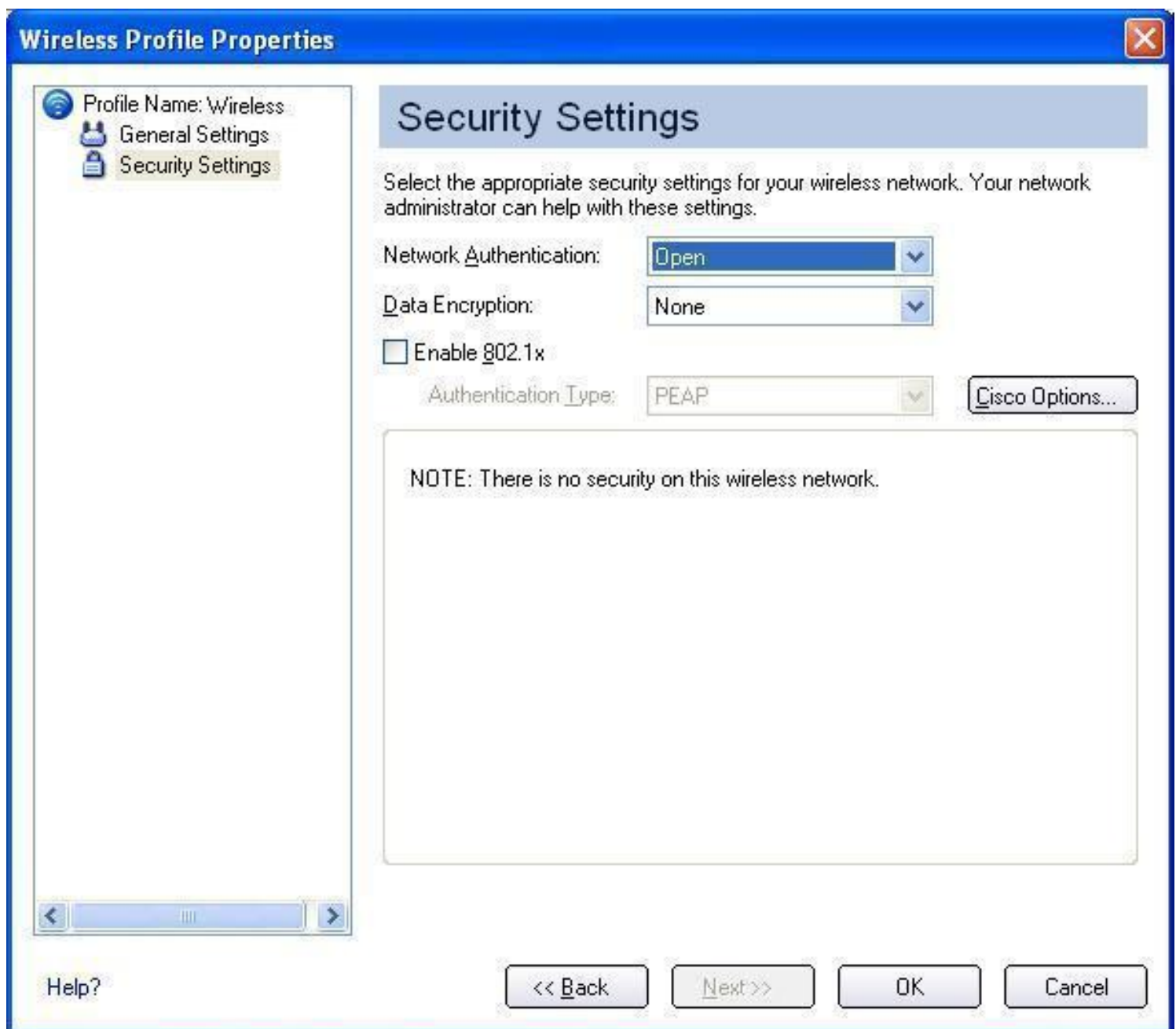


The image shows a Windows-style dialog box titled "Advanced Settings" with a blue header bar and a red close button in the top right corner. The dialog is divided into three sections, each with a blue header:

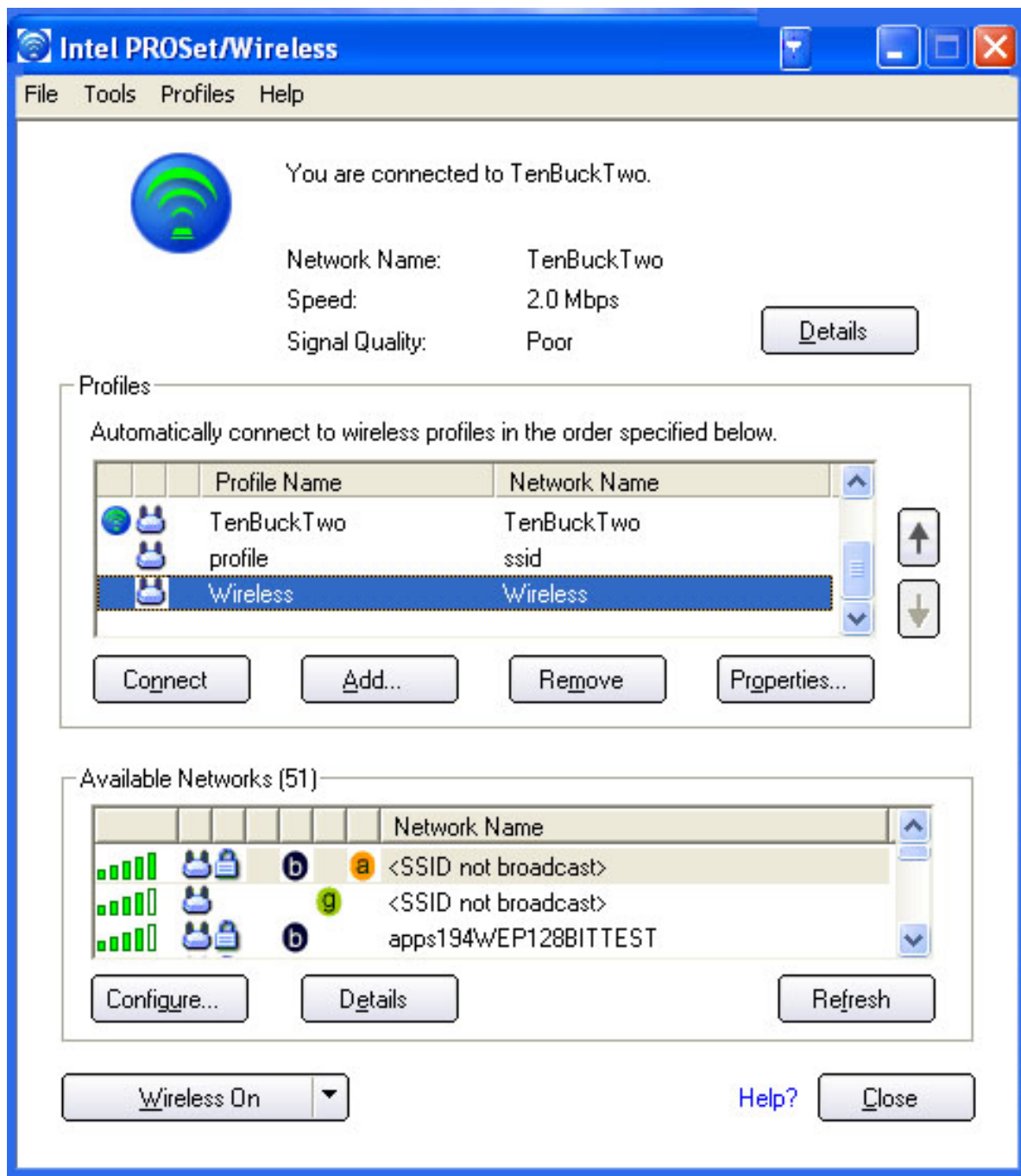
- Password Protection:** This section contains a checked checkbox labeled "Password protect this profile (maximum 10 characters)". Below this are two text input fields: "Password:" and "Confirm Password:", both containing ten asterisks (XXXXXXXXXX). A paragraph of text below the fields reads: "Prevent the settings in this profile from being viewed or changed by protecting this profile with a password. In order to make future changes, this password will be required."
- Auto-Import:** This section contains an unchecked checkbox labeled "Enable Auto-Import". Below it is a paragraph: "Auto-Import allows a network administrator to easily move this profile to other computers. When the exported file is placed in the Wireless\AutoImport directory on another computer, Intel PROSet Wireless will automatically import the profile."
- Mandatory Access Point:** This section contains a paragraph: "Enter the Mandatory Access Point's MAC address (BSSID) to make your wireless adapter associate with this specific access point only. Valid entries are values between 0-9 and A-F." Below this is a text input field for the "Address:" with a placeholder showing five colons (: : : : :) and a "Clear" button to its right.

At the bottom of the dialog, there is a "Help?" link on the left and two buttons, "OK" and "Cancel", on the right.

5. Select **Password protect this profile** (maximum 10 characters).
6. Enter the password, then re-enter it in the **Confirm Password** box.
7. To close the dialog, click **OK**. The previous Create Wireless Profile dialog reopens:



8. Click **Next**.
9. For Network Authentication, select **Open** (recommended).
10. Select **None** as the Data Encryption.
11. To save your settings and close the Security Settings page, click **OK**. The Intel® PROSet/Wireless dialog reopens.



12. The new profile is positioned at the bottom of the Profiles list. Use the up and down arrows to position it at the top of the list.
13. To connect to the wireless network, select it and click **Connect**.
14. To verify the status of your wireless connection, refer to [Viewing the Status of your Wireless Connection](#).

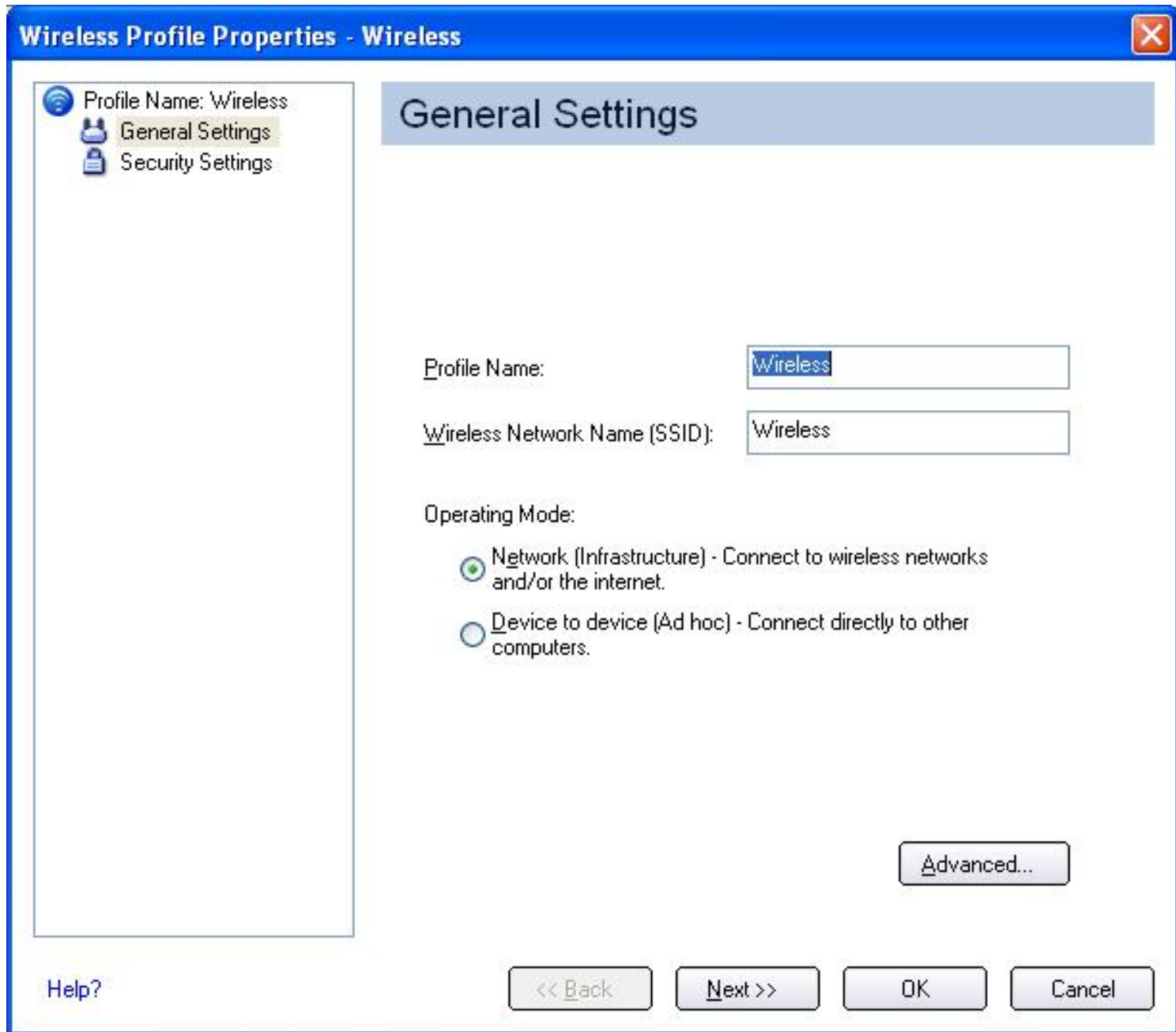
Configuring your Infrastructure Network with WEP security

The following describes how to edit an existing profile and apply Wired Equivalent Privacy (WEP) encryption.

 **NOTE:** Before starting, have the security network key available for the access point (for home use). If the access point is installed in a corporate environment, contact your system administrator for the network key.

To configure a profile with WEP security:

1. Double-click the **Intel® PROSet/Wireless** icon in the desktop task tray, or click **Start** à **Programs** à **Intel® PROSet/Wireless** à **Intel® PROSet/Wireless**.
2. From the Intel® PROSet/Wireless dialog, select the profile from the Profiles list and click **Properties**. The General Settings dialog opens:



The image shows the 'Wireless Profile Properties - Wireless' dialog box. On the left is a sidebar with a tree view containing 'Profile Name: Wireless', 'General Settings' (selected), and 'Security Settings'. The main area is titled 'General Settings' and contains the following fields and options:

- Profile Name:** A text box containing 'Wireless'.
- Wireless Network Name (SSID):** A text box containing 'Wireless'.
- Operating Mode:** Two radio button options:
 - ☒ **Network (Infrastructure)** - Connect to wireless networks and/or the internet.
 - ☐ **Device to device (Ad hoc)** - Connect directly to other computers.
- Advanced...** button.
- At the bottom are four buttons: **Help?**, **<< Back**, **Next >>**, **OK**, and **Cancel**.

3. Click **Next**. The Security Settings dialog opens:

Wireless Profile Properties - Wireless

Profile Name: Wireless

General Settings

Security Settings

WEP Key

Security Settings

Select the appropriate security settings for your wireless network. Your network administrator can help with these settings.

Network Authentication: Open

Data Encryption: WEP

☐ Enable 802.1x

Authentication Type: None

Cisco Options...

WEP Key

Encryption Level: 128-bit

Key Index: 1

Wireless Security Password (WEP Key):

(HINT: Passphrase - 13 characters OR Hex - 26 hexadecimal values)

The Security Password is the same value used by the Wireless Access Point.

(Advanced: Up to four passwords (keys) may be specified by changing the Key Index.)

Help? << Back Next >> OK Cancel

4. For Network Authentication, select **Open** (recommended).
5. Select **WEP** as the Data Encryption.
6. For the Encryption Level, select **64-bit** or **128-bit**.
7. Select a key index number **1, 2, 3, or 4**. Key selection must correspond to the network key on the access point.
8. Enter the password characters in the **Wireless Security Password (WEP Key)** text box. Select either of the following:
 - **Use ASCII characters:** Click **Use ASCII characters** to enable. Enter a text phrase, five (using 64-bit) or 13 (using 128-bit) alphanumeric characters (0-9, a-z or A-Z), in the pass phrase field.
 - **Use hex Key:** Click **Use hex Key** to enable. Enter ten (using 64-bit) alphanumeric characters, 0-9, A-F, or twenty-six (using 128-bit)

alphanumeric characters (0-9, A-F) in the hex key field.

 **NOTE:** Both the network name and the network key information are case-sensitive.

- 9. To save the settings and close the Security Settings page, click **OK**.
- 10. The profile is positioned at the bottom of the Profiles list. Use the up and down arrows to position it at the top of the list.
- 11. To connect to the wireless network, click **Connect**.
- 12. To verify the status of your wireless connection, refer to [Viewing the Status of your Wireless Connection](#).

Your basic configuration is now complete. If your network required advanced security options, click on the appropriate link below for advanced configuration instructions.

[Configuring Advanced Network Security Settings in Windows XP](#): Using Windows XP Support.

[Configuring Advanced Network Security Settings in Windows 2000](#): Using Intel® PROSet/Wireless.

Viewing the Status of Your Wireless Connection

The wireless network connection icon in the bottom right corner of the windows desktop indicates the current status of your wireless connection. There is also a signal quality icon on the Intel® PROSet/Wireless main windows that provides the current status of your wireless connection. The signal can vary from poor to excellent depending on the surroundings and quality of the signal from the access point or computer (ad hoc mode). The following table shows how the signal quality icon indicates the status of your wireless connection, and the suggested actions for low signals.

Connection Icon	Connection Status	Bars/Color	Suggested Action
	Excellent	5 green bars	No action required
	Very Good	4 green bars	No action required
	Good	3 green bars	No action required

	Low	2 green bars	Move closer to the access point
	Very Low	1 yellow bar	Move closer to the access point
	No connection	no colored bars	Computer is still trying to establish initial connection or you have moved out of the range of your access point.

[Back to Top](#)

[Back to Contents](#)

[Back to Contents](#)

Using Intel® PROSet/Wireless: Intel PROSet/Wireless 2915ABG Network Connection User's Guide

[Using Intel PROSet/Wireless as Your Wireless Manager](#)

[Enabling/Disabling the Wireless Radio](#)

[Intel PROSet/Wireless Main Window](#)

[Intel PROSet/Wireless Menus](#)

[Administrator Tool](#)

[Single Sign On Feature](#)

[Installing and Uninstalling the Software](#)

[Installing and Uninstalling the Single Sign On Feature](#)

[Window XP Zero Configuration](#)

Using Intel PROSet/Wireless as Your Wireless Manager

The following information is for Windows XP users. If you are using Windows 2000 refer to [Making a Basic Network Connection in Windows 2000](#).

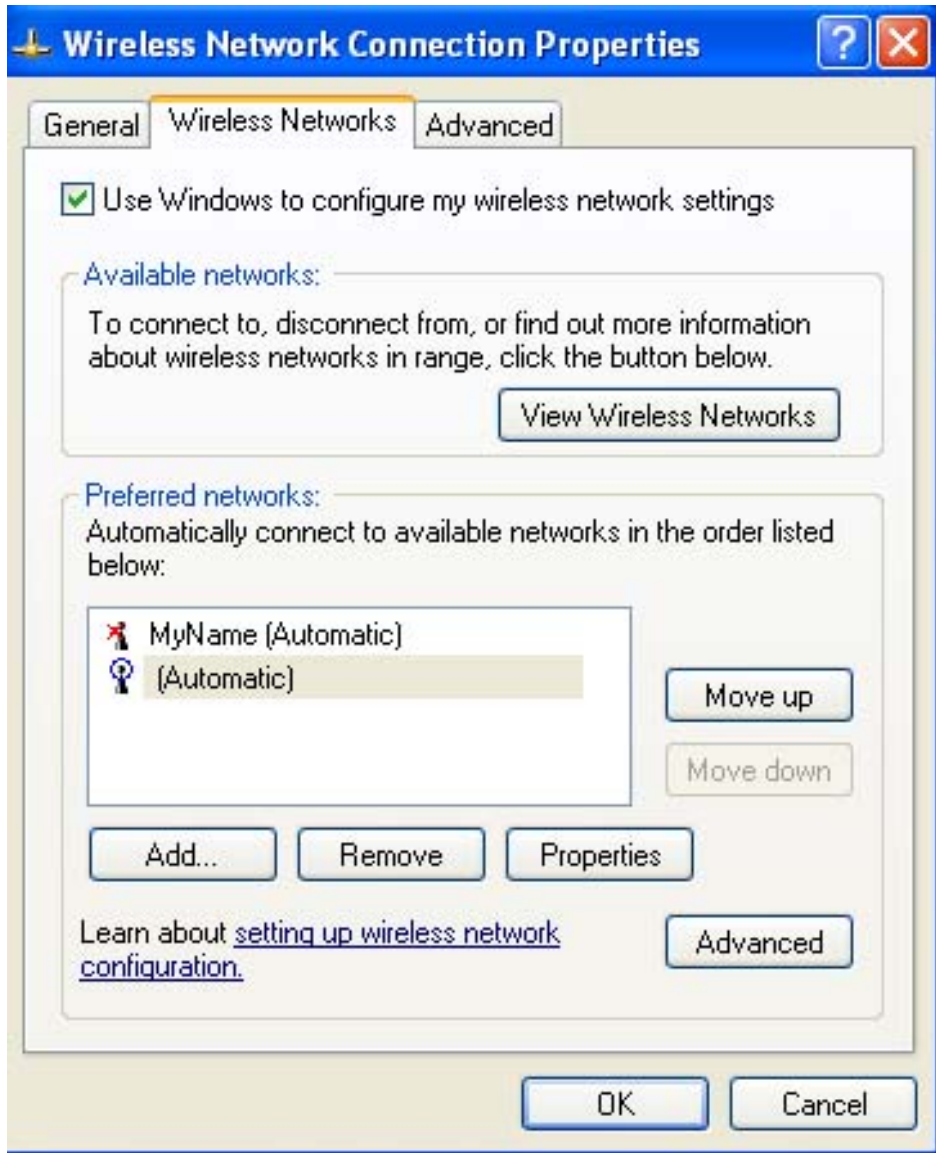
Intel PROSet/Wireless can be used to set up, edit, and manage network profiles to connect to a network. It also includes advanced settings such as power management and channel selection for setting up ad hoc networks. If you are using Windows XP, it is recommended that you use Windows XP to manage your network profiles. However, if your network requires [LEAP](#) authentication, you will need to use Intel® PROSet/Wireless to configure your LEAP profiles.

Disabling Windows XP Wireless Manager from the Windows Operating System

To disable Windows XP as your wireless manager from Windows:

1. Click **Start** à **Settings** à **Control Panel**.

2. Double-click **Network Adapters**.
3. Right-click Wireless Network Connection, and then click **Properties**. The Wireless Network Connection Properties page opens:



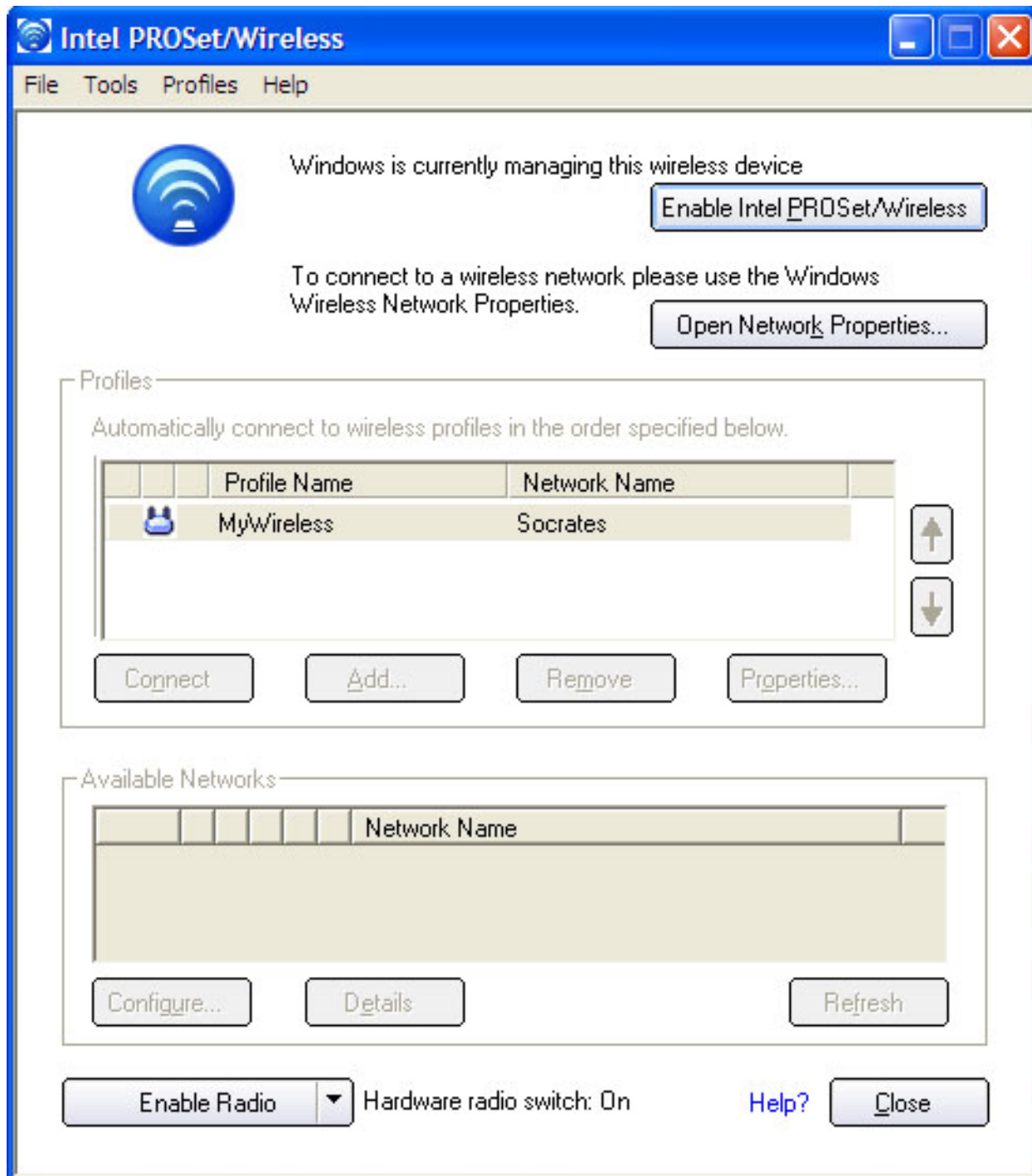
2. On the Wireless Networks tab, click to clear the **Use Windows to configure my wireless network settings** checkbox.
 3. To save your settings, click **OK**.
- This procedure configures Intel® PROSet/Wireless to manage your network profiles.

Disabling Windows XP from Intel® PROSet/Wireless

If Windows XP is enabled, the Intel® PROSet/Wireless main window is disabled. However, you can still open the Intel® PROSet/Wireless window from the Start menu and disable Windows XP.

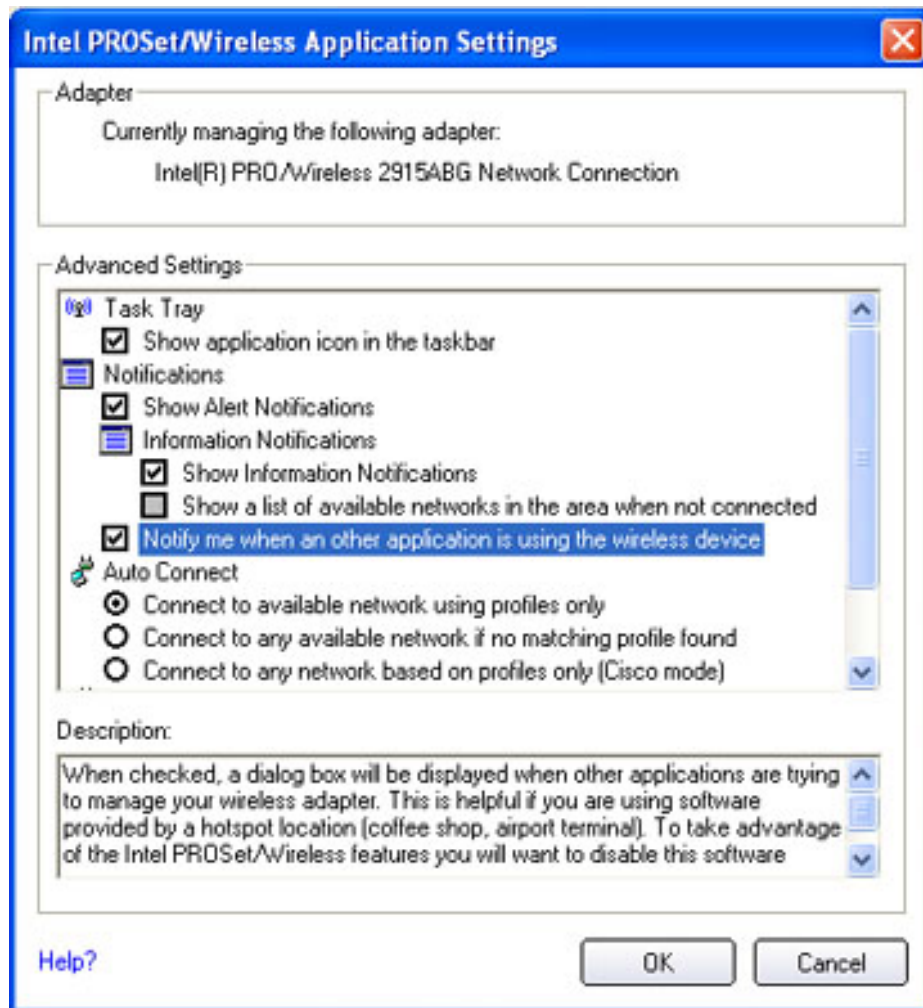
To disable Windows XP from the Intel PROSet/Wireless window:

1. Click **Start** à **Programs** à **Intel PROSet/Wireless**. The Intel PROSet/Wireless window opens.



2. Click **Enable Intel PROSet/Wireless**. This procedure configures Intel PROSet/Wireless to manage your network profiles.

NOTE: To be notified when Windows XP or any other wireless manager starts to manage your network profiles, select **Applications Settings** under the Tools menu on the Intel PROSet/Wireless window box. Next, select **Notify when another application is using the wireless device** checkbox, as shown in the following illustration:



Enabling/Disabling the Wireless Radio

The wireless radio can be enabled/disabled from a hardware radio switch on your computer, in conjunction with either the Intel PROSet/Wireless or with Windows.

NOTE: When your computer is switched on and the radio is enabled, the radio is capable of constantly transmitting signals. In certain situations, such as in a plane, signals from the radio may cause interference. The following methods describe how to disable the radio and use your laptop without emitting radio signals.

Using the Fn + F2 radio off/on switch

To enable/disable the radio:

1. Press **Fn + F2** to switch the radio on or off. This is known as the hardware switch. If you have Intel PROSet/Wireless installed, the current state of the radio is displayed in the Intel PROSet/Wireless [main window](#) and in the [task tray](#). The hardware radio switch **must** be turned on before you can enable the radio using the Intel PROSet/Wireless or Windows Device Manager:

Radio icon status: Using Fn + F2 displays a large wireless icon indicating that the radio is enabled or disabled, as shown in the following illustration:

**Radio Enabled using
Fn + F2**



**Radio Disabled
using Fn + F2**



Using Intel PROSet/Wireless to enable/disable the radio

The radio can be enabled/disabled from Intel PROSet/Wireless. The status icon on the Intel PROSet/Wireless main window displays the current state of the radio.

When the radio is on, an attempt is made to associate the network access point using the last profile. If the adapter cannot connect to the access point, the Configuration Service attempts to find an available network.

To enable/disable the radio using **Intel PROSet/Wireless**:

- To enable/disable the radio from the **Intel PROSet/Wireless main window**:

- Open the Intel PROSet/Wireless main window.
 - To toggle the radio off and on, click **Enable/Disable Radio**.
- To enable/disable the radio off/on from the **task tray**:

- Right-click the task tray icon .
- From the menu that opens, select **Enable Radio** or **Disable Radio**.

When the radio is disabled, the task try shows the icon with a red X: .
The icon is located in the lower right corner of Windows desktop.

Using Device Manager to enable/disable the radio

The radio can be enabled/disabled using Device Manager on the Windows operating system. The wireless icon on the task tray will display the current state of the radio.

To enable/disable the radio from the **Windows Device Manager**:

1. From the Windows desktop, right-click **My Computer** and then click **Properties**.
2. Click the Hardware tab, and then click **Device Manager**.
3. Double-click **Network adapters**.
4. Right-click the installed wireless adapter in use.
5. From the pop-up menu, choose **Enable/Disable** (depending on whether the radio is currently on or off).
6. When prompted, click **Yes**.

 **NOTE::** Make sure the radio is enabled on both the software and the hardware. If it is not enabled on the hardware, you will receive this message when you try to connect:

The Intel® PRO/Wireless 2915ABG (or the Intel PROSet/Wireless 2200BG) network connection is still disabled.
Press Fn + F2 to enable it.

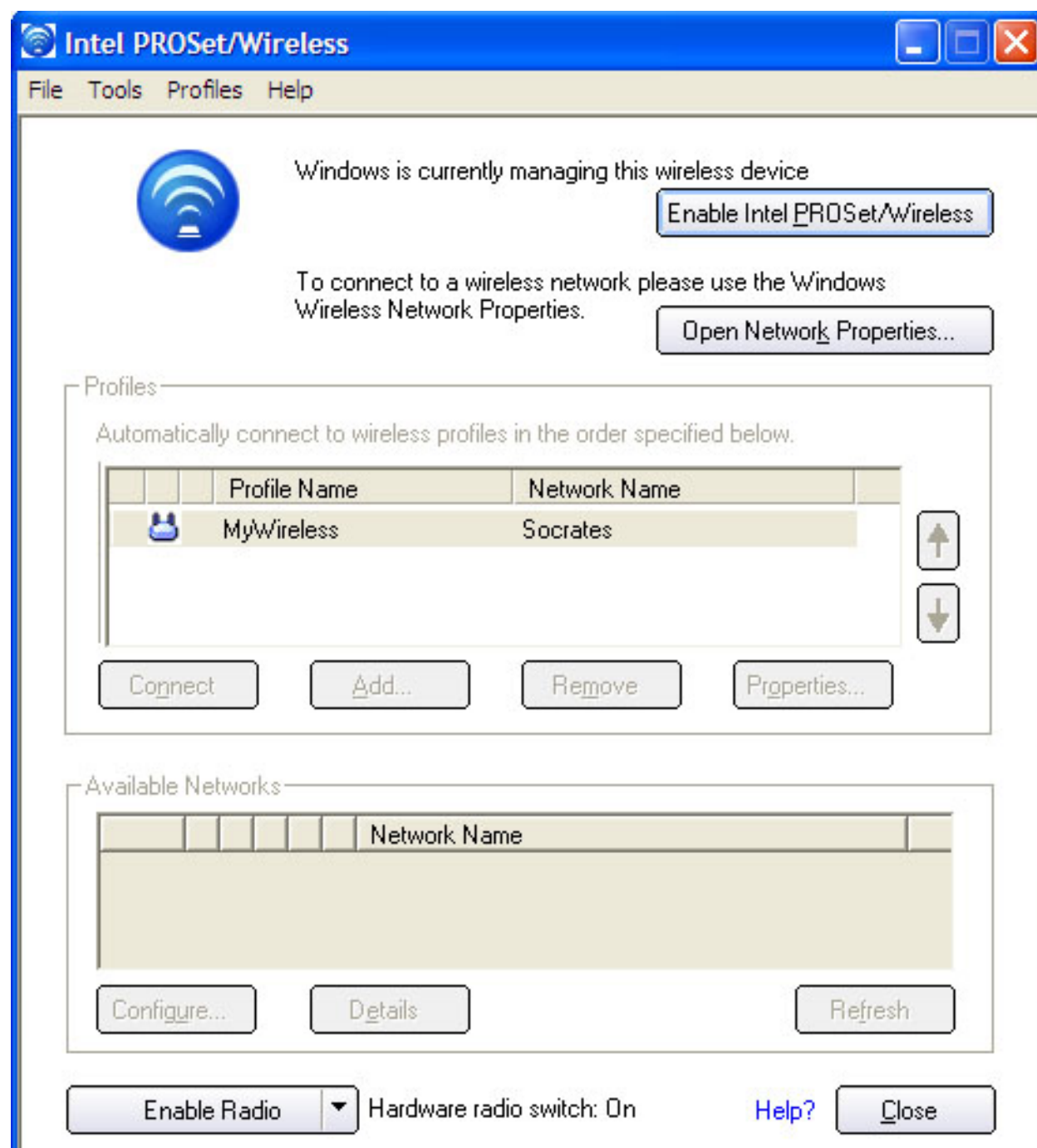
A red **X** indicates the radio is disabled.

Intel PROSet/Wireless Main Window

The main window contains basic information about your connection. If you are associated to a network, it will contain information such as SSID, profile name, and speed, and AP settings such as 802.11 band, channel, and security mode. The Signal Quality icon provides visual information about the quality of the wireless signal. It varies from poor to excellent, depending on the surroundings and quality of the signal from the access point. Refer to [Viewing the Status of your Wireless Connection](#) for more information.

The current status of the radio is also displayed in the Intel PROSet/Wireless main screen. Refer to [enabling the radio](#) for more information about how to enable/disable the wireless radio.

Intel PROSet/Wireless Main Window:

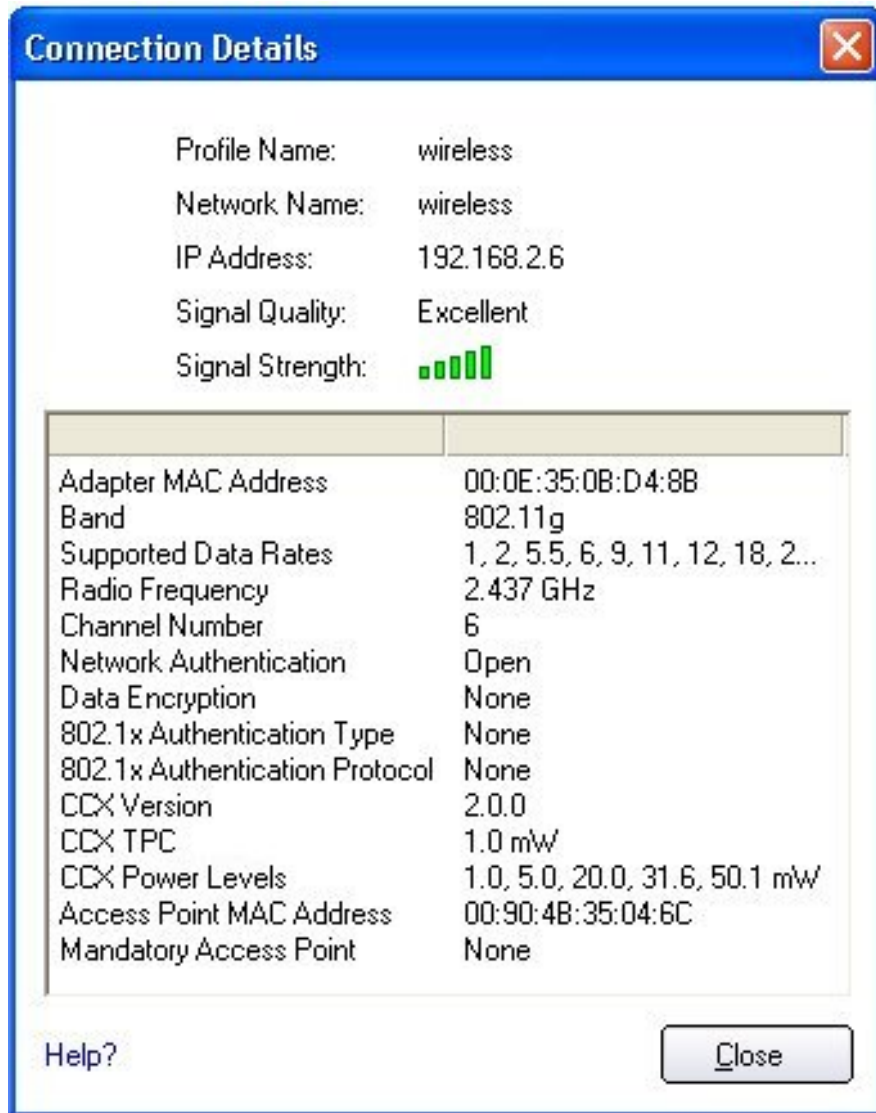


Enable Radio

Hardware radio switch: On

[Help?](#)[Close](#)

- To view detailed parameters of the access point and network adapter, as shown in the following illustration, click **Details**.



The Connection Details window displays the current network connection information.

Connection Details description

Name	Description
Profile Name	Name of the profile. If this is a one-time connection then <no active profile> is displayed.
Network Name	Network Name (SSID) of the current connection.
IP address	Internet Protocol (IP) address for the current connection.

Signal Quality	A radio frequency (RF) signal can be assessed by basically two components: • strength (quantity) of the signal • the quality of the signal The quality of the signal is determined by a combination of factors - but primarily is composed of signal strength and the ratio of the RF noise present. RF noise occurs both naturally in nature and artificially by electrical equipment. If the amount of the RF noise is high, and/or the signal strength is low, it results in a lower signal to noise ratio which causes poorer signal quality. With a low signal to noise ratio it is more difficult for the radio receiver to discern the data information contained in the signal from the noise itself.
Signal Strength	While adequate signal strength is required for good data communications, even more important is the quality of the signal. A strong signal of poor quality results in poor data communications. If the signal quality is low, investigate sources of noise nearby, such as interference from other wireless LANs, other RF transmitters, electric motors or compressors. Also reflections of the signal by metallic or other objects in the area can result in poor signal quality.
Adapter MAC Address	The Media Access Control (MAC) address for the wireless adapter.
Band	Indicates the wireless band of the current connection. • 802.11a • 802.11b • 802.11g
Supported Data rates	Rates at which the wireless adapter can send and receive data. Displays the speed in Mbps for the frequency being used. • 802.11g - 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 • 802.11b - 1, 2, 5.5, and 11 • 802.11a - 6, 9, 11, 12, 18, 24, 36, 48, and 54
Radio Frequency Channel Number	Displays the channel frequency of the current wireless connection. Displays the transmit and receive channel.

Network Authentication	Displays Open, Shared, WPA-Enterprise, WPA-Personal, WPA2-Enterprise and WPA2-Personal modes. Displays the 802.11 authentication used by the currently used profile. Refer to Security Settings for more information.
Data Encryption	Displays None, WEP, CKIP, TKIP or AES-CCMP. Refer to Security Settings for more information.
CCX Version	Version of the Cisco Compatible Extensions on this wireless connection.
CCX TPC Power	Cisco Compatible Extensions Power Levels.
CCX Power Levels	0.2, 0.4, 1.0, 6.3, 100.0 mW
Access Point MAC Address	The Media Access Control (MAC) address for the associated access point.
Mandatory Access Point	Displays "None" is not enabled. If enabled from the Mandatory AP setting, the access point MAC address is displayed. This option directs the wireless adapter to connect to an access point using a specific MAC address (48-bit 12 hexadecimal digits, e.g., 00:06:25:0E:9D:84).
Close	Closes the page.
Help?	Displays the help information for this page.

Main Window Connection Status Icons

Icon	Description
	Radio Disabled: The wireless adapter is not associated to a network. Click the Enable Radio button to enable the adapter.
	Searching for wireless networks: The wireless adapter is scanning for any available wireless networks.
Animated Icons:	
	
	No wireless networks found: There are no available wireless networks found.



Wireless network found: An available wireless network is found. You can choose to connect to available networks displayed in the Available Networks list.



Connected to a wireless network: Connected to a wireless network. The network name, speed, and signal quality display the current connection status. Click **Details** to display details of the current network connection.



Not connected to a wireless network: Not connected to a wireless network.

Network Name

Network Name (SSID): The name of the network that the adapter is connected to. The Network Name SSID must be the same as the SSID of the access point, using infrastructure mode (also called BSSID, ESSID, or Net ID) or other computers in an ad hoc network (also called IBSSID).

Speed

Displays the current data transfer rate in mega-bits-per-second (Mbps):

- 802.11g - 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54
- 802.11b - 1, 2, 5.5, or 11
- 802.11a - 54, 48, 36, 24, 18, 12, 9, 6

Signal Quality



The signal quality icon bars indicate the quality of the transmit and receive signals between your wireless adapter and the nearest access point or computer in device-to-device mode. The number of vertical green bars indicate the strength of the transmit and receive signals.

The signal quality ranges from excellent to out of range. The following factors affect signal quality:

- Signal quality decreases with distance and is affected by metal and concrete barriers.
- Metal objects can reflect signals and cause interference.
- Other electrical devices can cause interference.

Details

Provides adapter connection status information.

Enable/Disable Radio

Switch the radio off and on. Refer to [Enabling/Disabling Wireless the Radio](#) for more information.

Help?

Displays the help information for this window. Drag **Help?** to the item of interest to display help information.

Close	Close the Intel PROSet/Wireless main window.
X	Close the Intel PROSet/Wireless main window.

Profiles list (on the main window)

Name	Description
Profile Name	Profiles are network settings that allow your wireless adapter to connect to a network access point (Infrastructure mode) or computer (device-to-device ad hoc mode) which does not use an access point. Refer to Setting up Profiles for more information.
Network Name	Name of the wireless network (SSID) or computer.
Connection Icons	The network profile status icons indicate the different connection states of the adapter with a wireless network, the type of operating mode being used, and if network security is being used. Blue circle: The wireless adapter is associated with an access point or computer (Ad hoc mode). If a profile has 802.1x security enabled, this indicates that the wireless adapter is associated and authenticated.  Infrastructure operating mode.  Ad hoc operating mode.  The network is using Security encryption.  Wireless network band frequency being used.
Network Name	Name of the wireless network (SSID) or computer.
Arrows	Use the arrows to position profiles in a preferred order for auto-connection. • Up-arrow: Move the position of a selected profile up in the profile list. • Down-arrow: Move the position of a selected profile down in the profile list.
Connect button	Connect the selected profile to the wireless network.
Add button	Create a new profile using the Profile Wizard.
Remove button	Remove a selected profile from the Profile List. All profiles cannot be removed from the list, one profile must remain in the list.
Properties button	Edit the contents of an existing profile. You can also double-click a profile in the Profile List to edit the profile.

Available networks (on the main window)

The Available Networks list displays a list of wireless networks within range of the adapter. Use the Connect button to launch the Profile Wizard to create a profile for the selected wireless network.

Name	Description
	The signal strength of the wireless network access point or computer (Ad hoc mode). The signal strength icon bars indicate that the wireless network or computer is available for connection but is still not associated with an access point or computer (Ad hoc mode).
	The wireless network is using Infrastructure operating mode.
	The wireless network is using Ad hoc operating mode.
	The wireless network is using Security encryption.
	The band frequency being used by the wireless network.
Network Name	Name of the wireless network (SSID) or computer.
Configure button	Configures the selected available Network Name.
Properties button	The Networks Properties displays the current network connection status for the wireless adapter. Refer to Network Properties for information.
Details button	Provides detailed information about the selected network and its access points.
Refresh button	Refresh the list of available networks. If any new networks are available with range of the adapter, the list is updated to show the new network name.

Intel PROSet/Wireless Menus

You can use the following menu options to configure your network settings:

- **File**
- [Tools](#)
- [Profiles](#)
- **Help**

- [Task Tray](#)

Wireless Menu Descriptions

Name	Description
File	Exit: Close the Intel PROSet/Wireless main window. To launch Intel PROSet/Wireless: • Click Start > Programs > Intel PROSet/Wireless > Intel PROSet/Wireless. • Right-click the task tray icon located in the lower right corner of your Windows Desktop, and click the menu option Open Intel PROSet/Wireless. • Double-click the task tray icon to open Intel PROSet/Wireless.
Tools	Application Settings: Provides system wide connection preferences. Refer to Application Settings for information. Use Ctrl+P from your keyboard as an alternative to using your mouse to access this feature. Adapter Settings: Displays Adapter Settings that correspond to the settings made in the Windows Advanced Settings. Refer to Adapter Settings for information. Use Ctrl+A from your keyboard as an alternative to using your mouse to access this feature. Use Microsoft client): Enables Windows XP as the wireless manager. Use F10 on your keyboard as an alternative to using your mouse to access this feature. Refer to Switching to Windows XP wireless manager for more information. Advanced Statistics: Provides detailed information about the network connection. Intel Wireless Troubleshooter: Self diagnostics utility. Use Ctrl+D from your keyboard as an alternative to using your mouse to access this feature. Administrator Tool: If installed, the Administrator tool is for

Profiles

administrators or the person who has administrator privileges on this computer. This option is used to configure shared profiles using Pre-logon and Persistent profiles. Refer to Administrator Tool for more information. Use **Ctrl+T** from your keyboard as an alternative to using your mouse to access this feature.

Import/Export: Import and export profiles to and from the profile list. Refer to Import/Export Profiles for information. Use **Ctrl+I** from your keyboard as an alternative to using your mouse to access this feature.

Manage Exclusions: Include or exclude specific access points. Refer to Manage Exclusions for information. Use **Ctrl+M** from your keyboard as an alternative to using your mouse to access this feature.

Help

Intel PROSet/Wireless Help: Launch the online help (F1).

About: Displays version information for the currently installed application components.

Tools Menu

The following options are available from the Tools menu.

Application Settings (Tools menu)

Application Settings control how Intel PROSet/Wireless behaves and displays information.

Name	Description
Adapter	Displays the name of the installed adapter currently being managed by Intel PROSet/Wireless

Task Tray

Show application icon in the taskbar: Select this option to display the task tray status icon. This icon resides in the Windows Task bar (Notification area). Clear the box to not display the task tray status icon. Selecting **Hide Icon** from the task tray menu also clears this check box.

The Task Tray Status Icon provides several functions:

- Visual feedback for the connection state and wireless activity of your wireless network. The icon changes color and animation for different wireless activity. See [Task Tray Icons](#) for more information.
- Menu – A menu is displayed when you click the icon. From this menu you perform tasks such as turning on/off the radio or launching the Intel PROSet/Wireless application. See: [Task Tray Menu Options](#) for more information.
- Tool tips and balloon prompts. See: [Tool Tip and Balloon Prompts](#) for more information.

Notifications

Show Alert Notifications: Select this option to display balloon windows next to the task tray icon. When your action is required, a message prompt displays. Only high importance events (alerts) trigger a balloon window. If the balloon window is checked, then the appropriate action is taken. Clear the box to not display balloon message prompts displayed. Refer to [Tool Tip and Balloon Prompts](#) for more information.

Select one of the following options:

- **Information Notifications:** These balloons are of lower importance. They do not require your interaction but can greatly improve the wireless experience.
- **Show Information Notifications:** This checkbox is checked by default. All informational balloon windows are displayed next to the task tray status icon. These balloons improve your wireless experience by notifying you when available wireless networks are in range. They also inform you when a wireless connection has been made or has been lost. Refer to [Tool Tip and Balloon Prompts](#) for more information.

- **Show a list of available networks in the area when not connected:** When the **Show Information Notifications** checkbox is not checked, you can check this item. Since the informational balloon windows are disabled this option allows you to still be notified of available networks when the wireless adapter is not connected.
- **Notify me when another application is using the wireless device:** When checked, a window is displayed when other applications are trying to manage your wireless adapter. This is helpful if you are using software provided by a hotspot location (such as a coffee shop or airport terminal. To take advantage of the Intel PROSet/Wireless features you may want to disable the hotspot software when you leave.

For more information about using the options above, refer to [Configuration Service](#).

Auto Connect

Connect to available network using profiles only: (Default)

Connect the wireless adapter to an available network using a matching profile from the [Profiles List](#). If no matching profile is found you are notified by a notification (see [Notifications](#)). The wireless device remains disconnected until a matching profile is found or you configure a new matching profile.

Connect to any available network if no matching profile found:

If the wireless adapter is disconnected and wireless networks are found, the Intel PROSet/Wireless Configuration service attempts to match a profile from the [Profiles List](#) and if a match is found, connect. If no matches are found and one of the available networks is open (unsecured), this option allows the Intel Configuration Service to connect to that open network. **Note:** Open networks have no security. You would need to provide your own security for this wireless connection. One way to secure an open wireless connection is with Virtual Private Networking (VPN) software.

Connect to any network based on profiles only (Cisco mode):

This mode supports multiple and blank network names (SSIDs) for access points that support Cisco Compatible Extensions. Select this option to try every profile in preferred order. This requires that users know they are in the vicinity of an access point which has more than one SSID but only advertises one.

Manage Exclusions	Enable automatic exclude list feature: Select this checkbox to enable the automatic exclude list feature. This feature provides a way to exclude access points from automatic connection. Refer to Manage Exclusions for more information. Enable manual exclude list feature: Select this checkbox to enable the manual exclude list feature. This feature provides a way to exclude networks from automatic connection. Refer to Manage Exclusions for more information.
OK	Save settings and return to the previous window.
Cancel	Close the page and cancel changes.
Help?	Displays the help information for this window.

Adapter Settings (Tools menu)

The Advanced tab on the Intel® PRO/Wireless 2915ABG Network Connection and Intel® PRO/Wireless 2200BG Network Connection window provides global settings for the wireless adapter. To access this window, click **Tools > Adapter Settings**. The Advanced tab is the default setting.

Advanced Tab Description

Name	Description
Ad Hoc Channel	Value: 802.11b/g: Select this option when using 802.11b and 802.11g (2.4 GHz) ad hoc band frequency. - Select the allowed operating channel from the list. 802.11a: Select this option when using 802.11a (5 GHz) ad hoc band frequency. - Select the allowed operating channel from the list.

Intel Throughput Enhancement

Changes the value of the Packet Burst control.

Enable: Enables throughput enhancement.

Disable: (default setting) Disables throughput enhancement.

Mixed mode protection

Use this option to avoid collision in the 11b/11g mixed environment. Use RTS/CTS where clients may not hear each other. Use CTS-to-self to gain more throughput where clients are physically close to and can hear each other.

Power Management

Allows you to select a balance between power consumption and adapter performance. The wireless adapter power settings slider sets a balance between the computer's power source and the battery.

Use default value: Power settings are based on the computer's power source (Default).

Manual: Allows you to adjust the slider for the desired setting. Use the lowest setting for maximum battery life.* Use the highest setting for maximum performance.

* Power consumption savings will vary based on infrastructure settings.

Preamble Mode

The preamble property allows you to change the preamble length setting received by the access point during initial connection.

Auto Tx Preamble: (Default) Allows automatic detection of the preamble setting received from the access point to enable the appropriate preamble option. Short preamble is used if this option is supported; if not, long preamble is used.

Long Tx Preamble: Always use a long preamble length to connect to an access point.

Preferred Band

If there is a wireless network that supports more than one band of operation, this setting will determine which band to connect with. For example, if 802.11a is selected for this Preferred Band setting, but an 802.11a network is unavailable, then the wireless adapter will still connect to an available 802.11b or 802.11g network. The selections are:

- 802.11g
- 802.11a
- 802.11b

Transmit Power

Decreasing the transmit power level reduces the radio coverage.

Default setting: Highest power setting.

- **Lowest:** Minimum coverage. Setting the transmission power level enables you to expand or confine a coverage area in respect to other wireless devices that could be operating nearby. Reducing a coverage area in high traffic areas improves transmission quality by reducing the number of missed beacons and noise in that coverage area.
- **Highest Maximum coverage.** Set the adapter to a maximum transmit power level. Select this setting when operating in highly reflective environments and areas where other devices could be operating nearby, and when attempting to communicate with mobile computers at the outer edge of a coverage area.

Note: This setting will take effect when using either Infrastructure or ad hoc mode.

Data Rate

Select the data transfer rate in megabits-per-second (Mbps).

Best Rate: (Default) Use the fastest rate detected.

Manually select: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54.

Wireless Mode	802.11a, 802.11b and 802.11g (Default): Connects to 802.11a, 802.11b, or 802.11g wireless networks. • 802.11g only: Connects the wireless adapter to 802.11g networks only. • 802.11a and 802.11g only: Connects the wireless adapter to 802.11a and 802.11g networks only. • 802.11b and 802.11g only: Connects the wireless adapter to 802.11b and 802.11g networks only. Note: These wireless mode (Modulation type) options determine the discovered access points displayed in the Available networks list.
OK	Save settings and return to the previous window.
Cancel	Cancel changes and return to the previous window.
Help	Displays the help for this window.

Windows Advanced Options (Adapter Settings)

To access the Windows XP/2000 Advanced options:

1. Start Windows and log on with administrative privileges.
2. From your desktop, right-click **My Computer** and click **Properties**.
3. Click the **Hardware** tab.
4. Click **Device Manager**.
5. Double-click **Network adapters**.
6. Right-click the name of the installed wireless adapter in use, and then click **Properties**.
7. Select the **Advanced** tab.
8. Select the **Property** you want (e.g., Mixed mode protection, Power Management, etc.).
9. To deselect the checkbox, click **Use default value**.
10. Select the new value (**Disable** or **Enable**) from the drop-down box.
11. To save your settings and exit the window, click **OK**.

To access the Windows 98SE/Me Advanced options:

1. Start Windows and log on with administrative privileges.
2. From your desktop, right-click **My Computer** and then click **Properties**.
3. Click the **Device Manager** tab.
4. Double-click **Network adapters**.
5. Right-click the name of the installed wireless adapter in use, and then click

Properties.

6. Select the **Advanced** tab.
7. Select the **Property** you want (e.g., Mixed mode protection, Power Management, etc.).
8. To deselect the checkbox, click **Use default value**.
9. Select the new value (**Disable** or **Enable**) from the drop-down box.
10. To save your settings and exit the window, click **OK**.

To access the Windows NT4.0 Advanced options:

1. Start Windows and log on with administrative privileges.
2. From your desktop, right-click **My Computer** and click **Properties**.
3. Click the **Hardware** tab.
4. Click the **Device Manager** button.
5. Double-click **Network adapters**.
6. Right-click the name of the installed wireless adapter in use, and then click **Properties**.
7. Select the **Advanced** tab.
8. Select the **Property** you want (e.g., Mixed mode protection, Power Management, etc.).
9. To deselect the checkbox, click **Use default value**.
10. Select the new value (**Disable** or **Enable**) from the drop-down box.
11. To save your settings and exit the window, click **OK**.

Advanced Statistics (Tools menu)

Provides current adapter connection information. The following describes information for the **Statistics Details** window.

Name	Description
Statistics Details	Advanced Statistics - This information pertains to how the adapter is communicating with an access point. Association - If the adapter finds an access point to communicate with, the value is In range. Otherwise, the value is Out of range. • AP MAC Address: The twelve digit MAC address (e.g., 00:40:96:31:1C:05) of the AP. • Number of associations: The number of times

the access point has found the adapter.

- **AP count:** The number of available access points within range of the wireless adapter.
- **Number of full scans:** The number of times the adapter has scanned all channels for receiving information.

Roaming - Roaming information indicates reasons for adapter roaming. Roaming occurs when an adapter communicates with one access point and then communicates with another for better signal strength.

- **Roaming Count:** The number of times that roaming occurred.
- **AP did not transmit:** The adapter did not receive radio transmission from the access point. You may need to reset the access point.
- **Poor beacon quality:** The signal quality is too low to sustain communication with the access point. You have moved the adapter outside the coverage area of the access point or the access point's device address information has been changed.
- **AP load balancing:** The access point ended its association with the adapter based on the access point's inability to maintain communication with all its associated adapters. Too many adapters are trying to communicate with one access point.
- **AP RSSI too low:** The Receive Signal Strength Indicator (RSSI) is too low to maintain an association with the adapter. You may have moved outside the coverage area of the access point or the access point could have increased its data rate.
- **Poor channel quality:** The quality of the channel is low and caused the adapter to look for another access point.
- **AP dropped mobile unit:** The access point dropped a computer from the list of recognizable mobile devices. The computer must re-associate with an access point.

Miscellaneous - Use this information to determine if an association with a different access point increases performance and helps maintain the highest possible data rate.

- **Received Beacons:** Number of beacons received by the adapter.
- **Percent missed Beacons:** Percent value for missed beacons.
- **Percent transmit errors:** The percentage of data transmissions that had errors.
- **RSSI:** Signal strength of the access point with which the adapter is communicating.

Transmit/Receive (Tx/Rx) Statistics

Displays percent values for non-directed, and directed packets.

Total host packets: The sum total number of directed and non-directed packets counts.

- Transmit - (Mbps)
- Receive - (Mbps)

Non-directed packets: The number of received packets broadcast to the wireless network.

Directed packets: The number of received packets sent specifically to the wireless adapter.

Total Bytes: The total number of bytes for packets received and sent by the wireless adapter.

Reset Statistics

Resets the adapter statistical counters back to zero and begins making new data measurements.

Close Help?

Close the window and return to the main window.

Displays the help information for this window.

Intel Wireless Troubleshooter (Tools menu)

Name	Description
------	-------------

File	Exit: Exit Intel Wireless Troubleshooter application.
Help	Intel® Wireless Troubleshooter Help: Displays online help on the Intel Wireless Troubleshooter.
	About: Displays version information for the Intel Wireless Troubleshooter.
Wireless Event Viewer	Launch Wireless Event Viewer .
Disable Notification	Click to disable the alert notifications.
Enable Notification	Click to enable the alert notifications if an error is detected.
Available Help	Date Time error message: • Description of error. • Link to resolve error (if available). See Resolving Errors. • Link to recommended steps to resolve error.

Administrator Tool (Tools menu)

Name	Description
Administrator Settings	Settings button: Set the user's control over their wireless network connections.
Administrator Profiles	Options button: Enable or disable Persistent and Pre-Logon profiles on the computer. Persistent Connection: A Persistent profile is active during boot time and when no user is logged onto the computer. Pre-Logon/Common Connection: A Pre-Logon profile is active once a user logs onto the computer. When Single Sign On support is installed, this type of profile uses your Windows log on user name and password. Pre-logon/Common are placed at the top of the Profiles list. Because these profiles are at the top of the list, when available they are connected first.

Disable Intel Profile Switching. Users will only be able to connect with the first Pre-Logon profile: Disable Profile Switching only applies to Pre-logon/Common profiles.

Add: Launches the Profile Wizard to create a profile.

Remove: Removes a selected profile from the profiles list.

Properties: Allows users to edit the selected profile contents.

Change Password

Allows users to change the Administrator Tool password.

Export

Allows users to export settings and profiles as one package to other computers on the network.

Close

Closes the window.

Help?

Displays the help for this window.

Profiles Menu

The following options are available from the Profiles menu

Import/Export (Profiles menu)

This option allows you to import and export profiles.

Import/Export Description

Name	Description
Export profiles	Select the profiles you want to export: Select individual or multiple profiles from the list. The profile mode icon indicates either infrastructure or ad hoc mode is being used and whether security is being used. Browse: Browse your hard disk for the destination directory. The directory path is shown in the destination directory window. Export: Start exporting profiles.

Import profiles	Imports profiles in to the Profiles list.
OK	Import: Browse your hard disk for files to import. Saves settings and returns to the previous window.
Cancel	Closes the window and cancels any changes.
Help?	Displays help information for this window.

For information about importing/exporting user-created profiles, refer to [Importing/Exporting Profiles](#).

For information about exporting Administrator profiles, refer to [Administrator Export Preferences](#).

Manage Exclusions (Profiles menu)

The Exclude List management window is displayed when you select this menu option from the Profiles menu. This option allows you to exclude or include specific access points.

This window allows you to see which networks (SSID) or individual access points (BSSID) have been excluded.

Manage Exclusions Description

Name	Description
Exclude List Management	Network Name: Name (SSID) of the wireless network. Radio: Displays band frequency of the wireless adaptor: 2.457 GHz for 802.11b and 802.11g; 5.2 GHz for 802.11a. BSSID: MAC address for the selected access point. Reason: Describes why the profile was excluded. There are two kinds of exclude entries: User added or Faulty access point exclusions. These are dynamically entered in the list because of DHCP, 802.1x, or Rogue access point failure.

	Details: Explanation of the exclusion and suggestions for fixing the exclusion.
	Note: Entries that are colored gray are excluded rogue access points. These entries cannot be removed from the list.
Add	Adds an access point to the list.
Remove	Removes an access point from the list.
Reset list	Refreshes the list.
Close	Closes window and save settings.
Help?	Displays the help information for this window.

Task Tray Icon Menu Options

The Intel PROSet/Wireless icon  is displayed in the task tray located in the lower right corner of your Windows desktop. Right-click the status icon to display the menu options.

Task Tray Icon Menu Description

Menu Item	Sub-menu Item	Comments
Open Intel PROSet/Wireless	none	Click this option to launch Intel PROSet/Wireless. If the Microsoft client is managing the wireless adapter, this menu option will read: Open Microsoft client. To switch back to Intel PROSet/Wireless, select Use Intel PROSet/Wireless from the menu.

Open Microsoft client	none	Launches Windows XP wireless manager. A list of available networks will be displayed. This option is displayed if Use Intel PROSet/Wireless is selected.
Enable Radio	none	Turns the radio on.
Disable Radio	none	Turns the radio off.
Connect to Profile	List of profiles is displayed	Displays the current profiles in the Profile List. Select a profile to activate it.
Use Microsoft client	None	Toggles between Intel PROSet/Wireless and Windows XP Wireless Zero Configuration Service. When you use Microsoft client, you will not be able to use the Intel PROSet/Wireless profiles.
Use Intel PROSet/Wireless		

Hide Icon	None	Removes Intel PROSet/Wireless icon from the task tray. The icon for the current session will no longer be displayed. Refer to Application Settings to display or hide the task tray icon.
-----------	------	---

Task Tray Icons

The task tray icon  provides visual indication of the current wireless connection state. The connection status icon is located in the lower right corner of your Windows desktop. The task tray can be set to visible or not visible in the Application Settings Tools menu selection.

Task Tray Icon Description

Icon	Description
	Disable Radio: The wireless adapter is off. The wireless device does not transmit or receive while it is off. Click Enable Radio to enable the adapter. The icon is white with a red X .
	Searching for wireless networks: The wireless adapter is searching for any available wireless networks. White icon with animation.
	No wireless networks found: There are no available wireless networks found. Intel PROSet/Wireless will periodically scan for available networks. If you want to force a scan, double-click the icon to launch Intel PROSet/Wireless and click the Refresh button. Red icon.



Wireless network found: An available wireless network is found. Double-click the icon to display the Available Networks window, select the network, and click the **Configure** button.

Yellow icon.



Authentication failed. Not able to authenticate with wireless network.

Green icon with a yellow warning triangle.



Connected to a wireless network: Connected to a wireless network. Tool tip display network name, speed, and signal quality.

Green icon with waves that reflect signal quality. More waves mean better signal quality.

 **NOTE:** If you are using Windows XP as your wireless manager, the task tray icon is white, and it will not reflect connection status. You can still click it to display the task tray menu.

Tool Tips and Balloon Message Prompts

The Tool Tips and Balloon message prompts provide feedback and interaction for your wireless adapter. To display Tool tips move your mouse pointer over the icon. Balloon message prompts will be displayed when your wireless network changes state. For instance if you are out of range of any wireless networks, when you come in range a balloon prompt will be displayed. Balloon prompts can be enabled or disabled in the Application Settings.

Tool Tips

Tool tips display when the mouse pointer rolls over the icon. The tool tips display text for each of the connection states. For example when you are connected to a wireless network, the text shown below will be displayed in the tool tip:

Tool Tip Description

Tool Tip	Description
----------	-------------



Wireless Network Name: Intel

Speed: 54Mbps

Signal Quality: Excellent

Balloon Prompts

When user action is required, a balloon message prompt is displayed. If you click the prompt, an appropriate action is taken. For example, when wireless networks are found, the following balloon prompt appears:

Balloon Prompt description

Balloon Prompt



Description

Wireless Network found.

Click to connect to a wireless network.

Launching Intel PROSet/Wireless from the Task Tray

To launch Intel PROSet/Wireless, use one of the following options:

- Click the task tray icon located in the lower right corner of your Windows desktop.
- Right-click the task tray icon and then click Open Intel PROSet/Wireless.

Administrator Tool

The Administrator Tool is used for administrators or the person who has administrator privileges on this computer. This tool is used to configure shared (common) profiles.

This tool also allows the administrator to restrict what level of control the users of this computer have over their wireless connections.

Users cannot modify administrator settings or profiles unless they have the password for this tool. A password should be chosen that is secure.

You can export these settings and profiles as one package to other computers on your network.

Name	Description
Administrator Settings	Settings button: Set the user's control over their wireless network connections.
Administrator Profiles	Options button: Enable or disable Persistent and Pre-Logon profiles on the computer. Persistent Connection: A Persistent profile is active during boot time and when no user is logged onto the computer. Pre-Logon/Common Connection: A Pre-Logon profile is active once a user logs onto the computer. When Single Sign On support is installed, this type of profile uses your Windows logon user name and password. Pre-logon/Common are placed at the top of the Profiles list. Because these profiles are at the top of the list, when available they are connected first. Disable Intel Profile Switching. Users will only be able to connect with the first Pre-Logon/Common profile: Disable Profile Switching only applies to Pre-logon profiles. Add: Launches the Profile Wizard to create a profile. Remove: Removes a selected profile from the profiles list. Properties: Allows users to edit the selected profile contents.
Change Password	Allows users to change the Administrator Tool password.
Export	Allows users to export settings and profiles as one package to other computers on the network.
Close	Closes the window.
Help?	Displays the help for this window.

Administrator Export Preferences

Use the Administrator Settings and Profiles options to configure shared profiles for exporting. Exported profiles can be pushed to any Intel PROSet/Wireless user's 'auto import' folder.

IT Export Preferences window

Name	Description
Export Administrator Preferences	Step 1: Select one or both types you want to export: • Administrator Settings: Export all settings. These include control of Cache Credentials and or XP Co-existence options. • Administrator Profiles: Export all the Persistent and Pre-Logon/Common Profiles. Step 2: Select the destination file: • Browse button: Select the profile destination path and directory. The export destination file has an .sso extension. The directory path appears in the destination directory window. Step 3: Export the selected preferences: • Export button: Start exporting your profiles to the assigned destination folder.
Close	Closes the window.
Help?	Displays the help for this window.

Administrator Profile Options

These settings provide advanced profile connection options and allow the administrator to enable or disable Persistent and or Pre-Logon/Common profiles on the computer.

Name	Description
Persistent Connection	A Persistent profile is active during boot time and when no user is logged onto the computer.

Pre-Logon/Common Connection

A Pre-Logon/Common profile is active once a user logs onto the computer. These profiles appear at the top of a user's profiles list. They cannot be modified by the user without a password. Users can still prioritize the profiles they have created but they cannot re-prioritize Pre-logon/Common Profiles. Since these profiles appear at the top of the profile list, Intel PROSet/Wireless automatically attempts to connect to the Administrator profiles first before any user-created profiles.

OK

Saves settings and close the window.

Cancel

Cancels settings and close the window.

Help?

Displays the help for this window.

Administrator Settings Window

These settings allow the administrator to control how users of this computer use their wireless connection.

Name	Description
------	-------------

Cache Credentials	Cache the user credentials during a user session:
--------------------------	--

- **Click checkbox:** Cache user credentials in memory so that you are only prompted the first time before connection instead of each time you connect or disconnect to the network during the Windows log on session.
- **Clear checkbox:** Prompt for credentials each time wireless connectivity (authentication, re-authentication) is established using 802.1x profiles with either the Use Windows Logon credentials or the Prompt for Credentials on Connection option.

XP Co-existence Allow the user to enable XP Zero Configuration:

- **Click checkbox:** Displays a prompt, **Windows XP is managing your profiles**, indicating that Windows XP Zero Configuration is enabled and is managing your wireless adapter. You are prompted to answer the following question:

Do you wish to disable Windows XP management and let Intel® PROSet manage your wireless network?

- Select **Yes**, if you want Intel® PROSet/ Wireless to manage your wireless adapter.
- Select **No**, if you want Windows XP to manage your wireless adapter.
- **Clear checkbox:** If the box is cleared, when Intel® PROSet/Wireless launches, you are not be notified in the event that Windows XP Zero Configuration wireless manager is enabled.

OK	Saves settings and close the window.
Cancel	Cancels settings and close the window.
Help?	Displays the help information for this window.

Creating Administrator Profiles with the Administrator Tool

Administrator Profiles are created using the Administrator Tool. User profiles are created from the Intel® PROSet/Wireless main window.

Administrator Profiles are user-based or shared profiles owned and managed by the network administrator or the administrator of this computer. These profiles are common/shared by all users on this computer. However, end users cannot modify these profiles; they can only be modified using the Administrator Tool, which is password protected.

There are two types of Administrator profiles: **Persistent and Pre-logon/Common**.

Administrator Profiles are:

- **Persistent Connection:** This profile is applied at boot time or whenever no one is logged on to the computer. A Persistent profile maintains a wireless connection either

until the computer is turned off or a different user logs on.

- **Pre-Logon Common Connection:** This profile is applied when a user logs on. If Single Sign On support is installed, the connection is made as part of the Windows log-on sequence (pre-logon). If Single Sign On support is not installed on the computer, the profile is applied when the user session becomes active. Pre-logon/common profiles always appear at the top of the user's Profiles list. Users can still prioritize their profiles (the ones they created), but they cannot change the priority of Pre-logon/Common Profiles. Because pre-logon/common profiles appears at the top of the Profiles list, Intel® PROSet/Wireless automatically attempts to connect to the Administrator-created profiles before any user-created profiles.

Pre-Logon Connection Status Window

When the Single Sign On component is installed, the user has Pre-logon support. During the Windows log-on sequence, a Pre-logon Status window opens. This window displays the progress of the network connection. After the wireless adapter is associated with the network access point, the Status window closes.

1. After a system restart or power-up, the Windows Log On window opens, prompting you to enter your Windows Log On domain, user name, and password.
2. Click **OK**. The PreLogon profile Status window displays the progress of the network connection. After the wireless adapter is associated with the network access point, the status window closes and the Windows user log on window is displayed.

Single Sign On and Windows XP Welcome Screen and Fast User Switching

The Fast User Switching and the Windows XP Welcome Screen are disabled when Single Sign On support is installed.

Single Sign On is targeted to the environment where users log on to their computer with a user name, password, and typically a domain. Fast User Switching does not support domain log on.

 **NOTE:** Windows Fast User Switching is enabled by default if you are using Windows XP Home Edition. It is targeted for the home user. Fast User Switching is also available on Windows XP Professional if you install it on a stand-alone or workgroup-connected computer. If a computer running Windows XP Professional is added to a domain, then the Fast User Switching option is not available.

Modifying and Uninstalling the Software

The Single Sign On Pre-Logon Connection feature is not installed during the Typical installation process. To install this feature, use the **Custom** option during the installation process.

Installing and Uninstalling the Single Sign On Feature

The Single Sign On Pre-Logon Connect feature is not installed during the initial software installation process. This feature can be installed or uninstalled after Intel® PROSet/Wireless has been installed.

To install the Single Sign On the Pre-Logon Connect feature after Intel® PROSet/Wireless has been installed:

1. Click **Start** à **Settings** à **Control Panel** à **Add or Remove Programs** à **Intel PROSet/Wireless**.
2. Select **Change/Remove**.
3. On the Program Maintenance screen select **Modify** and then click **Next**.
4. Click **Single Sign On**. Select **Install this feature and all subfeatures**. **Note:** Windows XP Fast Switching and the Welcome screen are disabled when the Single Sign On feature options are installed.
5. Click **Modify**. After the software is installed on your computer, the component is listed as **Installed**.
6. Click **OK**.

To remove the Single Sign On Pre-Logon Connect feature:

1. Click **Start** à **Settings** à **Control Panel** à **Add or Remove Programs** à **Intel PROSet/Wireless**.
2. Select **Change/Remove**.
3. On the Program Maintenance screen select **Modify** and then click **Next**.
4. Click **Pre-Logon connect** subfeature of **Single Sign On**. Select **Do not install this feature**. A red **X** appears next to the option.
5. Click **Modify**. After the feature is uninstalled on your computer, the component is listed as Not Present.

6. Click **OK**.
-

Uninstalling Intel PROSet/Wireless

The Intel PROSet/Wireless software can be uninstalled.

To remove Intel PROSet/Wireless:

1. Click **Start > Settings > Control Panel > Add or Remove Programs > Intel PROSet/Wireless**.
 2. Select **Change/Remove**.
 3. Select **Modify** on the Program Maintenance screen
 4. Click **Next**.
 5. Click **OK**. After the software is uninstalled on your computer, the component is listed as **Not Present**.
 6. Click **OK**.
-

Windows XP Wireless Zero Configuration Feature

The Windows XP Wireless Zero Configuration feature provides a built-in wireless configuration utility. This feature can be enabled and disabled in Windows XP or by clicking Use Microsoft Client on the Tools menu. If XP Zero Configuration is enabled the features in Intel® PROSet/Wireless are disabled.

[Back to Top](#)

[Back to Contents](#)

[Back to Contents](#)

Using Intel® PROSet/Wireless Profiles

[What Is a Profile?](#)[Profile Types](#)[Administrator Profiles](#)[Profiles List](#)[Loading a Profile from the Task Tray](#)[Creating a New Profile Using the Profile Wizard](#)[Configuring Multiple Profiles](#)[Editing a Profile](#)[Adding WEP Encryption to a Profile](#)[Creating an Ad Hoc Connection with an Existing Profile](#)[Deleting a Profile](#)[Setting a Profile Password](#)[Importing and Exporting Profiles](#)[Automatic Profile Distribution](#)[Connecting to a Network without a Profile](#)[Connecting to a Network with a Blank SSID](#)[Profile Connection Preferences](#)

-

What Is a Profile?

A profile is a saved group of network settings. Profiles are useful when moving from one wireless network to another. Different profiles can be configured for each wireless network. Profile settings must include the network name (SSID), operating mode, and security settings. From the Intel PROSet/Wireless main window, you can add, edit, and remove profiles.

A profile is created when you connect to a wireless network. When you select a network from the **Available networks** list and click **Configure**, the Profile Wizard is launched. The Profile Wizard guides you through the settings required to connect to a wireless network. When the profile is complete, you can save it, and it is added to the Intel PROSet/Wireless main window Profiles list. Because these are saved settings, the next time you are in range of this wireless network, you are automatically connected. For more information, refer to [Profile Wizard Overview](#).

Profile Types

There are two types of profiles that can be used to connect to a wireless network. The profile types are:

- **User Profiles:** These profiles are created by the user. If there is more than one user on a computer network, the other users will need to create their own profiles. User-created wireless profiles are not accessible by other network users.
 - **Administrator Profiles:** If one or more profiles need to be shared among users on a network, you need to install the **Administrator Tool** and create Administrator profiles. For more information, refer to [Administrator Profiles](#).
-

Administrator Profiles

Administrator Profiles are created using the Administrator Tool. User profiles are created from the Intel PROSet/Wireless main window.

Administrator Profiles are user-based or shared profiles owned and managed by the network administrator or the administrator of this computer. These profiles are common/shared by all users on this computer. However, end users cannot modify these profiles; they can only be modified using the Administrator Tool, which is password protected.

There are two types of Administrator profiles: **Persistent and Pre-logon/Common**.

Administrator Profiles are:

- **Persistent Connection:** This profile is applied at boot time or whenever no one is logged on the computer. A Persistent profile maintains a wireless connection either until the computer is turned off or a different user logs on.
- **Pre-Logon Common Connection:** This profile is applied when a user logs on. If Single Sign On support is installed, the connection is made as part of the Windows log-on sequence (pre-logon). If Single Sign On support is not installed on the computer, the profile is applied when the user session becomes active. Pre-logon/common profiles always appear at the top of the user's Profiles list. Users can still prioritize their profiles (the ones they created), but they cannot change the priority of Pre-logon/Common Profiles. Because pre-logon/common profiles appears at the top of the Profiles list, Intel PROSet/Wireless automatically attempts to connect to the Administrator profiles before any user-created profiles.

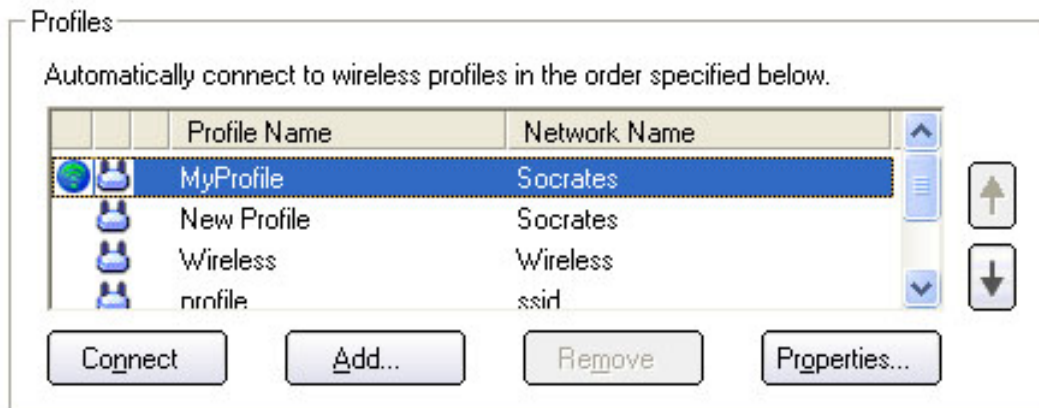
For more information about these profiles, see [Creating Administrator Profiles with the Administrator Tool](#).

Profiles List

The Profiles list displays a list of existing profiles. When you are in range of a wireless network, Intel PROSet/Wireless scans the Profiles list to see if there is a match. If a match is found, you are automatically connected to the network. For more information, see Configuration Service.

The priority order of the Profiles list is the same as the priority used by Intel PROSet/Wireless to find a match.

The Profiles List, found on the [Intel PROSet/Wireless main window](#):



- Use the up and down arrows to arrange profiles in a specific order to automatically connect to a wireless network.

Profiles can be arranged in a specific order of connection: 1 is the highest priority. The Configuration Service also uses the profiles priority list to connect to wireless networks. The Profiles list displays the available user-based and shared profiles. User-based profiles can be arranged in order of network connection priority. Administrator (shared) profiles will always take precedence over user-based profiles. You can connect to one network, using the first profile in the Profiles list, and then automatically connect to another network using the next profile. This allows you to stay connected while roaming freely from one wireless network to another. Although you can assign multiple profiles to a single network, you can only use one profile per connection. To add a new profile, use the Profile Wizard sequence of windows to configure the profile contents. The following sections discuss how to set up and configure a profile to connect to a network.

NOTE: Administrator (shared) Pre-Logon or Persistent profiles are displayed at the top of the Profiles list. These profiles have priority over user-based profiles. Shared profiles in the Profiles list cannot be modified only viewed.

- Use the **Connect** button to connect a profile to the selected wireless network. You can also add, edit, and remove profiles from the main window.

Profile Icons

The network profile status icons indicate whether the adapter is associated with a network, the type of operating mode being used, and whether security encryption is enabled. These icons are shown next to the profile name in the profile list. Refer to [Profiles](#) for details.

Connecting to a Profile

When you are in range of a wireless network that has a matching profile, you will be automatically connected to that network. If a network with a lower priority profile is also in range, you can force the connection to that lower profile. This can be accomplished using Intel PROSet/Wireless or from the task tray icon.

Manually connecting to a profile from Intel PROSet/Wireless

1. To open Intel PROSet/Wireless, double-click the **task tray icon**.
2. From the Profiles list, select an existing **profile**.
3. Click **Connect**. Remember: The connection will only be made if the wireless network is in range.

Manually connecting to a profile from the task tray icon

1. Right-click the **Intel PROSet/Wireless icon** on the task tray.
 2. Select **Connect to Profile**, and then click the desired profile.
-

Loading a Profile from the Task Tray

To load a profile from the Task Tray:

1. Right-click the **Intel PROSet/Wireless** connection icon in the task tray.
 2. Make sure that the **Intel PROSet/Wireless connection manager** is selected (not Microsoft client).
 3. Click **Connect to Profile** and select the profile to be launched.
-

Profile Wizard Overview

Use the Profile Wizard to create a network profile for connection to a specific wireless network.

When the Intel Configuration Service detects an available network and the adapter is not associated with another wireless network, the **Connect to wireless network** window is displayed. From Intel PROSet/Wireless, select a network from the Available Networks list and click **Configure**. The Profile Wizard guides you through the wireless network configuration process.

- **Security Detection:** After you select a wireless network from the Available Networks list, the General Settings page opens to display the network name and operating mode for the selected network. The identified Wireless Network Name (SSID) cannot be modified, but you can change the Profile name. Click **Next** to display the second Profile wizard Security progress page. This starts the access point query process to determine the highest level of security required for the selected network. After the required security is determined, the Security settings page displays the required information that must be entered to connect to that particular network. For example, if an Infrastructure WEP network is selected, WEP encryption and key index information is displayed, but only the WEP Network Key needs to be entered. If you do not know the required network settings, contact your administrator.

Profiles

To add profiles or to edit an existing profile:

- **Add (Create a new profile):** Click **Add** to open the Profile wizard and create a new profile. In this mode all of the General and Security page settings are blank and require that you enter adapter and wireless network information. Before creating a new profile, contact your administrator for the required network settings, or have the necessary network information ready to enter.
- **Properties (Edit a profile):** Click **Properties** to open the Profile Wizard and edit the profile contents. The General Settings and Security Settings pages display all of the profile settings and parameters that can be modified.

For more information, refer to [Creating a New Profile Using Profile Wizard](#) or [Configuring Multiple Profiles Using Profile Wizard](#).

Creating a New Profile Using the Profile Wizard

The Profile Wizard allows you to create a new profile, configure the profile contents, and connect to a wireless network. If you select a network from the **Available Networks** list and click **Configure**, the Profile Wizard guides you through the necessary steps to create a profile and connect to the network. During this process, the Profile Wizard attempts to detect the appropriate security settings for you.

To create a new profile and connect to a wireless network:

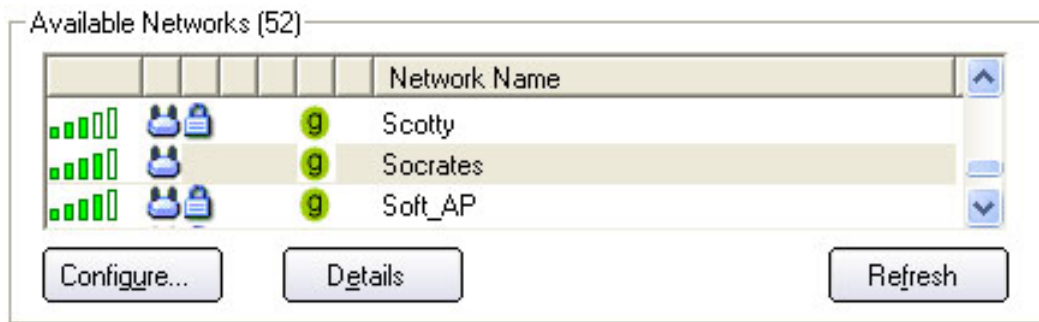
1. From the Intel PROSet/Wireless main window, click **Add**. The Profile Wizard launches, and the [General Settings](#) window opens.
 2. In the Profile Name text box, enter a **profile name**.
 3. In the Wireless Network Name (SSID) text box, enter the **Wireless Network Name**.
 4. Select the Operating Mode you want to use, **Infrastructure** or **Ad Hoc**.
 5. For the following options, click **Advanced**:
 - Password protect the profile: Select the Password protect this profile checkbox. Enter the password in the text box, and then re-enter it in the Confirm Password text box.
 - Auto-Import: Allows automatic import of this profile. For network administrators only.
 - Mandatory Access Point: Makes the wireless adapter associate with a specific access point.
 6. To save your settings and return to the General Settings page, click **OK**.
 7. Click **Next**. The [Security Settings](#) window opens.
 8. Select the Network Authentication and Data Encryption options. Enter the encryption key settings and configure the 802.1x settings as required. Refer to security settings for more information.
 9. When you complete the profile settings, click **OK** to return to the Intel PROSet/Wireless window. (To change or verify the profile settings, select the profile and click **Properties**.)
 10. From the Profiles list, select the new profile name.
 11. To connect to the wireless network, click **Connect**. The network name, transmit and receive speed, and signal quality are displayed.
 12. To close the window, click **Close**.
-

Configuring Multiple Profiles Using Profile Wizard

Typically, one profile is assigned for a particular network connection. If there are multiple profiles assigned to one wireless network name (SSID), before connection to the network, Intel PROSet/Wireless configuration Service displays a window showing the multiple profile names for that particular network. One profile must be selected to connect to the network.

To configure a profile to a network for which a wireless profile already exists.

1. Open the Intel PROSet/Wireless window.
2. From the Available Networks list, select the network to which you want to configure a profile:



3. Click **Configure**. The connect or configure a New Profile window opens:



4. Click **Configure**. The Configure Wireless Settings window opens, indicating you need to designate settings for the new profile:



5. Click **Next**. The General Settings window opens:

Configure Wireless Settings - Socrates

General Settings



Specify the Profile Name. You can keep the default or personalize the name.
Example: ABC Corporate Network

Profile Name:

Wireless Network Name (SSID): Socrates

Operating Mode: Network (Infrastructure)

Network (Infrastructure) - Connect to wireless networks and/or the internet.

[Advanced...](#)

[Help?](#)

<< [Back](#) [Next](#) >> [OK](#) [Cancel](#)

6. In the Profile Name text box, enter a name for the profile and then click **Next**. The Security Settings window opens:



7. Enter the Wireless Security Password (WEP Key) and click **Next**.
8. When the next window opens, showing you are done, click **OK**. You are returned to the Intel PROSet/Wireless main window.

 **NOTE:** If the Network requires a password, a password window will open, prompting you to enter the password.

General Settings Window

The **General Settings** window is the first page in the Profile Wizard. From this page you can specify the profile name, the wireless network name (SSID) and choose the operating mode.

While configuring the profile, you can use the left pane to navigate to the General and Security Settings pages. The Back and Next button located at the bottom of the Profile Wizard can also be used for the same functions.

General Settings window description

Name	Description
Profile Name	Name of the wireless network profile. Examples: My Office Network, Bob's Home Network, ABC Company Network, etc.
Wireless Network Name (SSID)	Name of the wireless network access point used by the wireless adapter for connection. The SSID must match exactly the name of the wireless access point. It is case sensitive. When you are configuring a wireless network that was selected from the Available Networks list, the SSID is taken from the available network list. You cannot and should not change it. Blank SSID: If the wireless adapter receives a blank network name (SSID) from a stealth access point, <SSID not broadcast> is displayed in the available networks list. Provide the actual SSID for the access point. After connection both the blank SSID and the associated SSID can be viewed in the available networks list.
Operating Mode	Network (Infrastructure): Connect to an access point. An infrastructure network consists of one or more access points and one or more computers with wireless adapters. This connection is the type used in home networks, corporate networks, hotels and others to provide access to the network and/or the internet. Device to device (Ad hoc): Connect directly to other computers in an ad hoc wireless network. This type of connection is useful for connections between 2 or more computers only. It will not provide access to network resources or the Internet.
Advanced	Advanced Settings allows you to set a profile password, specify a certain access point address for adapter connection (Mandatory AP), or allow the profile to be Auto-Imported on another computer.

Administrator Profiles

If you are creating or editing an Administrator profile from the Administrator Tool you have the following options:

Persistent Connection: This is active when no user is logged on. It is used to maintain a wireless connection when no users are logged on.

Pre-Logon/Common: This is active when a user is logged on. This profile is shared by all users. It is useful when you want all users of a computer to use a specific profile. This profile appears at the top of the profile list in PROSet/Wireless.

Users cannot edit/modify Administrator profiles. They can only be edited from the Administrator Tool.

NOTE: The Administrator Tool is only available if it has been installed.

- Next
- Cancel
- Help?

Opens Security Settings page.
Closes the Profile Wizard and cancels any changes.
Displays the help for this window.

Security Settings Window

From the Security Settings page you can enter the required security settings for the selected wireless network.

 **NOTE:** The options displayed are dependent on the Operating Mode selected on the General Settings page.

Security Settings Description

Name	Setting
Network Authentication	Open Shared WPA-Enterprise WPA2-Enterprise WPA-Personal WPA2-Personal

Data Encryption	None WEP CKIP TKIP AES-CCMP
Enable 802.1x (Authentication Type)	MD5 EAP-SIM TLS TTLS PEAP LEAP EAP-FAST
Cisco Options	Click to view the Cisco Compatible Extensions Options window. NOTE: Cisco Compatible Extensions are automatically enabled for CKIP, LEAP and EAP-FAST profiles.
Back	View the prior page in the Profile Wizard.
Next	View the next page in the Profile Wizard. If more security information is required then the next Step of the Security page is displayed.
OK	Close the Profile Wizard and save the profile.
Cancel	Close the Profile Wizard and cancel any changes made.
Help?	Displays the help information for the current page.

Advanced Settings Description

From this window you can password protect a profile, enable the Auto-Import feature, and select a specific access point on a network to connect to. Use the Advanced button on the General Settings page to access this window.

Advanced Settings Description

Name	Description
------	-------------

Password Protection	Password: Password can be up to 10 characters. The entered password characters display as asterisks. Confirm New Password: Type the same password as entered in the Password field.
Auto-Import	Enable Auto-Import: Check to allow the profile to be imported and exported to other computers. This option allows a network administrator to distribute this profile automatically to computers connected to a network. Refer to Automatic File Distribution for more information.
Mandatory Access Point	Mandatory Access Point: Forces the wireless adapter to connect to an access point using a specific MAC address. Type the MAC address of the access point (BSSID) 48-bit 12 hexadecimal digits, e.g., 00:06:25:0E:9D:84. This feature is not available when using ad hoc operating mode. Clear button: Clear current address.
OK	Close the window and save the settings.
Cancel	Close the window and cancel any changes.
Help?	Displays the help information for this window.

Editing a Profile

To edit an existing profile:

1. From the Profiles list, select the profile you want to edit.
2. Click **Properties**. The General Settings window opens.
3. In the left pane of the General Settings window, click General Settings or Security Settings.
4. Edit the settings are required:
 - General Settings: Refer to General Settings for more information.
 - Security Settings: Refer to Security Settings for more information.
5. When you finish editing the settings, click **OK** to return to the main window.
6. From the Profile list, select the edited profile name and click **Connect**. The connection status, network name, transmit and receive speed, and signal quality are displayed.

Adding WEP Encryption to a Profile

NOTE: Before starting, you must obtain a user name and password on the RADIUS server from your system administrator.

To add WEP with no authentication to a new profile:

1. From Intel PROSet/Wireless window, click **Properties** from the Profile list. The General Settings window opens.
2. Click **Next** (or select Security Settings from the left pane). The Security Settings window opens.
3. For the Network Authentication, select **Open** (recommended).
4. For Data Encryption, select **WEP**.
5. For the Encryption Level, select either **64-bit** or **128-bit**.
6. Select the **key index 1, 2, 3, or 4** (1 is the default setting). When using the WEP key index, each wireless station must use the same key index number to access the wireless network.
7. In the Wireless Security Password (WEP Key) text box, enter the **Wireless Security Password (WEP Key)**:
 - **64-bit:** Enter a text phrase, up to 5 alphanumeric characters (0-9, a-z, or A-Z), in the pass phrase field or enter a hexadecimal value up to 10 alphanumeric characters (0-9, A-F) in the Network Key field.
 - **128-bit:** Enter a text phrase, up to 13 alphanumeric characters (0-9, a-z, or A-Z), or enter a hexadecimal value up to 26 alphanumeric characters (0-9, A-F) in the Network key field.
8. To save the profile settings, click **OK**.

Creating an Ad Hoc Connection with an Existing Profile

To create an ad hoc connection:

1. From the Intel PROSet/Wireless main window, select the profile you want from the profile list and click **Properties**.
2. When the General Settings window opens, click **Device to device (Ad hoc) - connect directly to other computers**.
3. Click **Next**.
4. For Data Encryption, select **WEP**.
5. For the Encryption Level, select **64-** or **128-bit**. The 128-bit level offers stronger encryption.
6. For the Key Index, select **1**. When using WEP Key Index, each wireless station must use the same key index number to access the wireless network.
7. Enter the **Wireless Security Password (WEP Key)**:
 - **64-bit:** Enter a text phrase, up to 5 alphanumeric characters (0-9, a-z, or A-Z), in the pass phrase field or enter a hexadecimal value up to 10 alphanumeric characters (0-9, A-F) in the

Network Key field.

- **128-bit:** Enter a text phrase, up to 13 alphanumeric characters (0-9, a-z, or A-Z), or enter a hexadecimal value up to 26 alphanumeric characters (0-9, A-F) in the Network key field.

7. To save the profile settings, click **OK**.

Deleting a Profile

To delete a profile:

1. Open the Intel ProSet/Wireless window.
2. From the Profiles List, click the profile to be deleted and click **Remove**.
3. When prompted to be sure you want to permanently delete the profile, click **Yes**.

 **NOTE:** You cannot delete all profiles from the Profiles List. There must always be one profile displayed in the list. If you are a restricted user the Delete button is disabled if you select a Common profile. Common profiles can only be edited and deleted if you have administrator privileges.

Setting a Profile Password

To password protect an existing profile:

1. From the Intel PROSet/Wireless main window, select a profile from the Profiles list and then click **Properties**. The General Settings page opens.
 2. Click the Advanced button.
 3. Click **Password protect this profile**.
 4. In the Password text box, type a password.
 5. In the Confirm Password text box, re-type the password.
 6. To save the setting and return to the General Settings page, click **OK**.
 7. On the General Settings page, click **OK**.
 8. To close the main window, click **Close**.
-

Connecting to a Network without a Profile

To connect to an available network without a profile using Windows:

1. Right-click the wireless client icon on the task tray and click **Open Microsoft client**.
2. Under Available Networks, click **View Wireless Networks**. A list of available networks

opens.

3. Select the network you want and click **Connect**. When you open the Microsoft client, the network you selected will appear in the Preferred Networks list.
4. To check the connection status, right-click the **Wireless Network icon** on the task tray.

To connect to an available network without a profile using Intel PROSet/Wireless:

1. Open the Intel PROSet/Wireless window.
 2. Under Available Networks, select the network you want to connect to.
 3. Click **Configure**. A connection window opens.
 4. Select Connect one time and click **OK**. The Wireless connection icon on the task tray indicates that you are now connected to the selected network.
-

Connecting to a Network with a Blank SSID

If the wireless adapter receives a blank network name (SSID) from a stealth access point, <SSID not broadcast> is displayed in the available networks list. To associate with a stealth access point, a new profile must first be created before connection. After connection both the blank SSID and the associated SSID can be viewed in the available networks list.

To connect to an access point that transmits a blank network name (SSID) in the Available Networks list:

1. On the Intel PROSet/Wireless window, click the **Refresh** button.
 2. Select the network name with a blank SSID and <no profile> shown in the Available Networks list.
 3. Click **Configure**.
 4. The Profile Wizard window opens. Enter a profile name and Network Name (SSID) and security settings if required.
 5. Click **Next** until settings are complete.
 6. To save the profile settings and return to the Wireless Networks tab, click **OK**.
 7. Select the new profile from the Profiles List and click **Connect**.
-

Profile Connection Preferences

To access the profile connection preference option:

1. From the Intel PROSet/Wireless main window, click **Application Settings** on the **Tools** menu.
2. Under **Auto Connect**, select one of the following options:

- **Connect to available network using profiles only:** (Default setting) Use the profiles in the Profiles List to connect to any available network.
 - Connect to any available network without using a profile from the Profile List.
 - **Connect to any network based on profiles only (Cisco mode):** Tries every profile in preferred order. This assumes the user knows they are in the vicinity of an access point which has more than one SSID. It advertises only one wireless profile which allows you to get connected easily to a network.
4. To save the setting, click **OK**.
 5. To close the main window, click **Close**.
-

Importing and Exporting Profiles (Profiles menu)

You can import and export user-based profiles to and from the Profiles list. Wireless profiles can be automatically imported into the Profiles list. This is accomplished by Intel PROSet/Wireless monitoring the import folder on your hard disk for new profiles. Only profiles that have been enabled (Enable Auto-Import) on the Profiles Import/Export window can be automatically imported. If a profile of the same name already exists in the Profiles list, a window prompts you to reject or accept the imported profile. If you accept it, the existing profile is replaced. All imported user-based profiles are placed at the bottom of the Profiles list, and it is immediately deleted from the import folder on your hard disk after import, whether the import was successful or not. For more information, refer to [Automatic Profile Distribution](#).

 **NOTE:** A password protected profile can be imported and exported; however, before editing the profile, the password must be entered. Refer to [Setting a Profile Password](#) for more information. To export Administrator profiles, refer to [Administrator Export Properties](#) for more information.

Import/Export Window Description

Name	Description
------	-------------

Export profiles	Select the profiles you want to export: Select individual or multiple profiles from the list. The profile mode icon indicates either infrastructure or ad hoc mode is being used and whether security is being used. Browse: Browse your hard disk for the destination directory. The directory path is shown in the destination directory window. Export: Start exporting profiles.
Import profiles	Imports profiles in to the Profiles list. Import: Browse your hard disk for files to import.
OK	Saves settings and returns to the previous window.
Cancel	Closes the window and cancels any changes.
Help?	Displays help information for this window.

To import profiles:

1. Open the Intel PROSet/Wireless window.
2. On the menu bar, point to **Profiles** and then click **Import/Export**.
3. When the Import/Export Profiles window opens, click **Import**.
4. Select the profile you want to import and click **Import**. (The profiles extension is either **.profiles** or **.p50**. The profiles to import can be located in any directory you choose on your computer.)
5. When the Import Successful window appears, click **OK**.
6. To return to the main window, click **Close**.

To export profiles:

1. Open the Intel PROSet/Wireless window.
 2. On the menu bar, point to **Profiles** and then click **Import/Export**.
 3. When the Import/Export Profiles window opens, select the profile you want to export from the Profiles list.
 4. To select the destination folder, click **Browse**.
 5. Select the destination folder and click **Open**.
 6. Click **Export**.
 7. When the Export Successful window appears, click **OK**.
 8. To return to the main window, click **Close**.
-

Automatic Profile Distribution

The **Enable Auto-Import** feature allows a network administrator to distribute profiles automatically to computers connected to a network. The **Enable Auto-Import** option is located on the [Advanced Settings](#) window. Use the Advanced button on the General settings page to access the Advanced Settings.

Importing Profiles

To distribute a profile automatically, the Enable Auto-Import must be selected, and then the profile can be copied to a specific directory on the host computer. From there it can be distributed to multiple computers. Once the profile is received by the remote computer it will automatically be available for use on the Profiles list. If a profile is password protected when sent, the user will be prompted for the password before the profile can be used.

Automatically importing wireless network profiles is accomplished by monitoring the import folder on your hard disk for new profile files. Only profiles that have the **Enable Auto-Import** box checked on the Profile Wizard Advanced page window can be automatically imported. If a profile of the same name already exists in the Profiles List, a window is displayed from which you can either reject the import, or accept in which case the existing profile will be replaced. All imported profiles will be placed at the bottom of the Profiles List, and the profile file will be immediately deleted from the import folder on your hard disk after the import whether the import was successful or not.

To import a profile into the Profiles List:

Step 1: Enable the enable Auto-Import feature:

- a. From the Intel PROSet/Wireless window, select a profile to be edited from the Profiles List in the Networks page, and click **Properties** (or click **Add** to create a new profile using the Profile Wizard). The General Settings window opens.
- b. Click **Advanced**. The Advanced Settings window opens.
- c. Click the **Enable Auto-Import** check box.
- d. To save the setting and close the window, click **OK** (Edit a profile) or **Finish** (Add a profile). You are returned to the General Settings window.
- e. Click **OK**. You are returned to the Intel PROSet/Wireless main window.

Step 2: Export the profile from the Profiles list to a folder on your hard disk. Refer to [Importing and Exporting Profiles](#) for details.

Step 3: Copy the exported profile (.50/.profile extension) from its folder to the directory: Program Files\Intel\Wireless\AutoImport. The profile is now ready to distribute to other computers.

Step 4: Using a network copy utility such as SMS, you can distribute the profiles to each of

the remote computers on the network. The profiles must be copied into the following directory on the remote computer: **Program files/Intel/Wireless/AutoImport**. The profile is displayed in the Profiles list of the remote computer.

 **NOTE:** If a profile is sent with password protection, the user is prompted for the password before the profile can be used.

[Back to Contents](#)

Security Overview

[WEP encryption](#)

[802.1x Authentication](#)

[WPA/WPA2](#)

[Cisco Features](#)

This section describes the types of security used in connecting to wireless networks.

WEP encryption

Using IEEE 802.11 Wired Equivalent Privacy ([WEP](#)) encryption can prevent unauthorized reception of wireless data. WEP encryption provides two levels of security, using a 64-bit key (sometimes referred to as 40-bit) or a 128-bit key (also known as 104-bit). For better security, use a 128-bit key. If you use encryption, all wireless devices on your wireless network must use the same encryption keys.

WEP encryption and shared authentication provides protection for your data on the network. WEP uses an encryption key to encrypt data before transmitting it. Only computers using the same encryption key can access the network or decrypt the encrypted data transmitted by other computers. Authentication provides an additional validation process from the adapter to the access point.

The WEP encryption algorithm is vulnerable to passive and active network attacks. [TKIP](#) and [CKIP](#) algorithms include enhancements to the WEP protocol that mitigate existing network attacks and address its shortcomings

Open and Shared Key authentication

The 802.11 authentication supports two types of network authentication methods: Open System and Shared Key.

- Using **Open** authentication, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an

authentication management frame that contains the identity of the sending station. The receiving station, or Access Point, grants any request for authentication. Open authentication allows any device network access. If no encryption is enabled on the network, any device that knows the SSID of the access point can gain access to the network.

- Using **Shared Key** authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel. Shared key authentication requires that the client configure a static WEP key. The client access is granted only if it passes a challenge-based authentication.

802.1x Authentication

The 802.1x authentication is independent of the 802.11 authentication process. The 802.1x standard provides a framework for various authentication and key-management protocols. There are different 802.1x authentication types, each providing a different approach to authentication but all employing the same 802.1x protocol and framework for communication between a client and an access point. In most protocols, upon the completion of the 802.1x authentication process, the supplicant receives a key that it uses for data encryption. Refer to [How 802.1x authentication works](#) for more information. With 802.1x authentication, an authentication method is used between the client and a Remote Authentication Dial-In User Service (RADIUS) server connected to the access point. The authentication process uses credentials, such as a user's password that are not transmitted over the wireless network. Most 802.1x types support dynamic per-user, per-session keys to strengthen the static key security. 802.1x benefits from the use of an existing authentication protocol known as the Extensible Authentication Protocol (EAP).

The 802.1x authentication for wireless LANs has three main components: The authenticator (the access point), the supplicant (the client software), and the authentication server (a Remote Authentication Dial-In User Service [[RADIUS](#)] server). The 802.1x authentication security initiates an authorization request from the wireless client to the access point, which authenticates the client to an Extensible Authentication Protocol ([EAP](#)) compliant RADIUS server. This RADIUS server may authenticate either the user (via passwords or certificates) or the system (by [MAC](#) address). In theory, the wireless client is not allowed to join the network until the transaction is complete. There are several authentication algorithms used for 802.1x. Some examples are; MD5-Challenge, [EAP-TLS](#), [EAP-TTLS](#), Protected EAP ([PEAP](#)), and EAP Cisco Wireless Light

Extensible Authentication Protocol (LEAP). These are all methods for the wireless client to identify itself to the RADIUS server. With RADIUS authentication, user identities are checked against databases. RADIUS constitutes a set of standards addressing Authentication, Authorization and Accounting (AAA). Radius includes a proxy process to validate clients in a multi-server environment. The IEEE 802.1x standard is for controlling and authenticating access to port-based 802.11 wireless and wired Ethernet networks. Port-based network access control is similar to a switched local area network (LAN) infrastructure that authenticates devices that are attached to a LAN port and prevent access to that port if the authentication process fails.

What is a RADIUS?

RADIUS is the Remote Access Dial-In User Service, an Authorization, Authentication, and Accounting (AAA) client-server protocol, which is used when a AAA dial-up client logs in or out of a Network Access Server. Typically, a RADIUS server is used by Internet Service Providers (ISP) to perform AAA tasks. AAA phases are described as follows:

- **Authentication phase:** Verifies a user name and password against a local database. After the credentials are verified, the authorization process begins.
- **Authorization phase:** Determines whether a request is allowed access to a resource. An IP address is assigned for the Dial-Up client.
- **Accounting phase:** Collects information on resource usage for the purpose of trend analysis, auditing, session time billing, or cost allocation.

How 802.1x authentication works

A simplified description of the 802.1x authentication is:

1. A client sends a "request to access" message to an access point. The access point requests the identity of the client.
 2. The client replies with its identity packet which is passed along to the authentication server.
 3. The authentication server sends an "accept" packet to the access point.
 4. The access point places the client port in the authorized state and data traffic is allowed to proceed.
-

802.1x features

- 802.1x supplicant protocol support
 - Support for the Extensible Authentication Protocol (EAP) - RFC 2284
 - Supported Authentication Methods:
 - MD5 - RFC 2284
 - EAP TLS Authentication Protocol - RFC 2716 and RFC 2246
 - EAP Tunneled TLS (TTLS)
 - Cisco LEAP
 - EAP-FAST
 - EAP-SIM
 - PEAP
 - Supports Windows XP, 2000
-

WPA and WPS2

Wi-Fi Protected Access (WPA) is a security enhancement that strongly increases the level of data protection and access control to a wireless network. WPA enforces 802.1x authentication and key-exchange and only works with dynamic encryption keys. To strengthen data encryption, WPA utilizes its Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements that include a per-packet key-mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and also a re-keying mechanism. Using these improvement enhancements, TKIP protects against WEP's known weaknesses.

The second generation of WPA that complies with the IEEE TGi specification is known as WPA2.

WPA-Enterprise and WPA2- Enterprise: Provides this level of security on enterprise networks with a 802.1x RADIUS server. An Authentication Type is selected to match the authentication protocol of the 802.1x server.

WPA-Personal and WPA2-Personal: Provides this level of security in the small network or home environment. It uses a password also called a pre-shared key (PSK). The longer this password the stronger the security of the wireless network. If your Wireless Access Point or Router supports WPA/WPA2 Personal, then you should enable it on the access point and provide a long, strong password. The same password entered into access point needs to be used on this computer and all other wireless devices that access the

wireless network.

Cisco Features

Cisco LEAP

Cisco LEAP (Cisco Light EAP) is a server and client 802.1x authentication via a user-supplied logon password. When a wireless access point communicates with a Cisco LEAP-enabled RADIUS (Cisco Secure Access Control Server (ACS) server), Cisco LEAP provides access control through mutual authentication between client wireless adapters and the wireless network and provides dynamic, individual user encryption keys to help protect the privacy of transmitted data.

Fast Roaming (CCKM)

When a wireless LAN is configured for fast reconnection, a LEAP enabled client device can roam from one access point to another without involving the main server. Using Cisco Centralized Key Management (CCKM), an access point configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client without perceptible delay in voice or other time-sensitive applications.

CKIP

Cisco Key Integrity Protocol (CKIP) is Cisco proprietary security protocol for encryption in 802.11 media. CKIP uses the following features to improve 802.11 security in infrastructure mode:

- Key Permutation (KP)
- Message Integrity Check (MIC)
- Message Sequence Number

EAP-FAST

EAP-FAST, like EAP-TTLS and PEAP, uses tunneling to protect traffic. The main difference is that EAP-FAST does not use certificates to authenticate.

Provisioning in EAP-FAST is negotiated solely by the client as the first communication exchange when EAP-FAST is requested from the server. If the client does not have a pre-shared secret Protected Access Credential (PAC), it can request to initiate a provisioning EAP-FAST exchange to dynamically obtain one from the server.

EAP-FAST documents two methods to deliver the PAC: manual delivery through an out-of-band secure mechanism, and automatic provisioning.

- Manual delivery mechanisms can be any delivery mechanism that the administrator of the network feels is sufficiently secure for their network.
- Automatic provisioning establishes an encrypted tunnel to protect the authentication of the client and the delivery of the PAC to the client. This mechanism, while not as secure as a manual method may be, is more secure than the authentication method used in LEAP.

The EAP-FAST method can be divided into two parts: provisioning, and authentication. The provisioning phase involves the initial delivery of the PAC to the client. This phase only needs to be performed once per client and user.

Mixed Cells Mode

Some access points, for example Cisco 350 or Cisco 1200, support environments in which not all client stations support WEP encryption, this is called Mixed-Cell Mode. When these wireless networks operate in “optional encryption” mode, client stations that join in WEP mode send all messages encrypted, and stations that join in using standard mode send all messages unencrypted. These APs broadcast that the network is not using encryption, but allow clients to join using WEP mode. When “Mixed-Cell” is enabled in a profile, it allows you to connect to access points that are configured for “optional encryption.”

Radio Management

When this feature is enabled your wireless adapter provides radio management information to the Cisco infrastructure. If the Cisco Radio Management utility is used in the infrastructure, it configures radio parameters, detects interference and rogue access points.

[Back to Top](#)

[Back to Contents](#)

[Back to Contents](#)

Configuring Advanced Network Security Settings in Windows XP: Intel® PROSet/Wireless 2915ABG Network Connection User's Guide

[Configuring an Ad Hoc Network with No Security](#)

[Configuring an Ad Hoc Network with WEP Security](#)

[Configuring a WPA-PSK Client with AES or TKIP Encryption](#)

[Configuring a WPA-PSK Client with AES or TKIP Encryption and TLS or TTLS Authentication](#)

[Configuring a WPA Client with AES or TKIP Encryption and PEAP Authentication](#)

[Configuring a Client for TLS/TTLS Authentication](#)

If you are using Windows 2000, click [Configuring Advanced Network Security Settings in Windows 2000](#) for instructions on how to configure advanced security settings for your wireless adapter.

This section contains instructions about how to configure advanced security settings for your wireless adapter. This requires information about advanced security settings on your access point (for home users) or from a system administrator (corporate environment). Refer to [Making a Basic Network Connection in Windows XP](#) for basic setup instructions.

 **NOTE:** If you cannot view your network in the list of **Available Networks**, it may be because your network does not broadcast or is in [silent mode](#). Click **Add** and enter the name of the SSID of the network you are trying to associate with to add it to the list of **Preferred Networks**. For further configuration, select the added network and click **Configure** to edit security settings. Refer to the [Troubleshooting](#) section for further instructions on how to configure networks with silent SSID's.

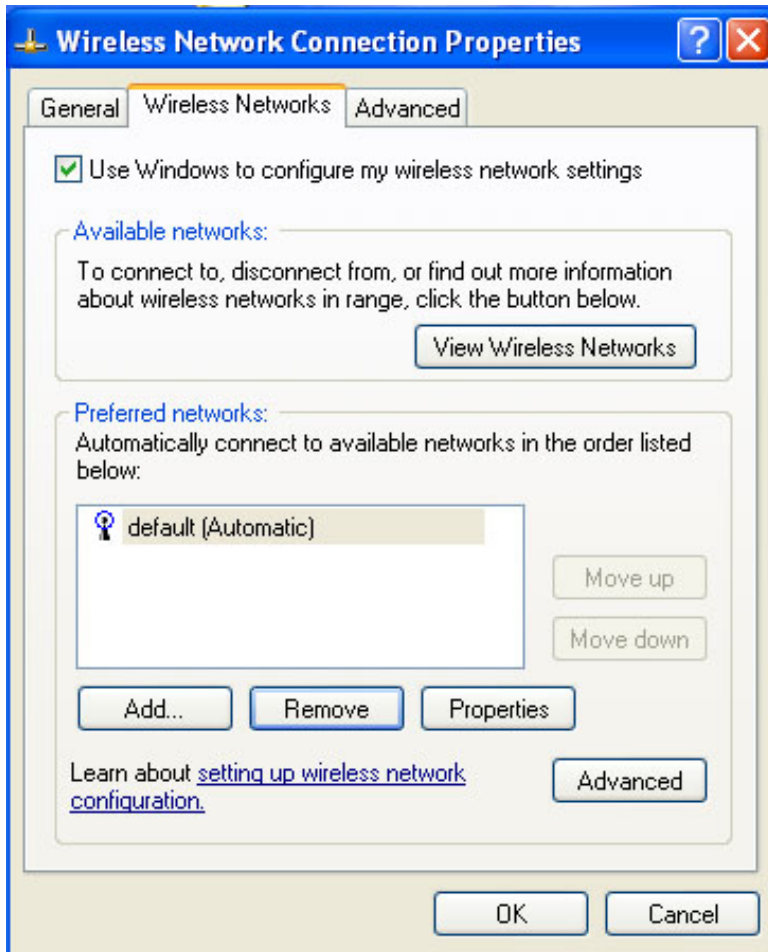
If you are using Windows XP (Service Pack 2) Category View some of the windows shown in the following examples may appear different from those on your screen. To switch from Category View to Classic view, click **Start** à **Control Panel** and on the navigation bar click **Switch to Classic View**.

Configuring an Ad hoc Network with No Security

In peer-to-peer (ad hoc) mode, you can send and receive information to other computers without using an access point. Each computer in a peer-to-peer network is called a peer. Creating an ad hoc network requires more than one computer with a wireless adapter. All systems on the ad hoc network must be configured identically. You can use peer-to-peer mode to network computers in a home or small office, or to set up a temporary wireless network for a meeting.

To configure an ad hoc network connection with no security:

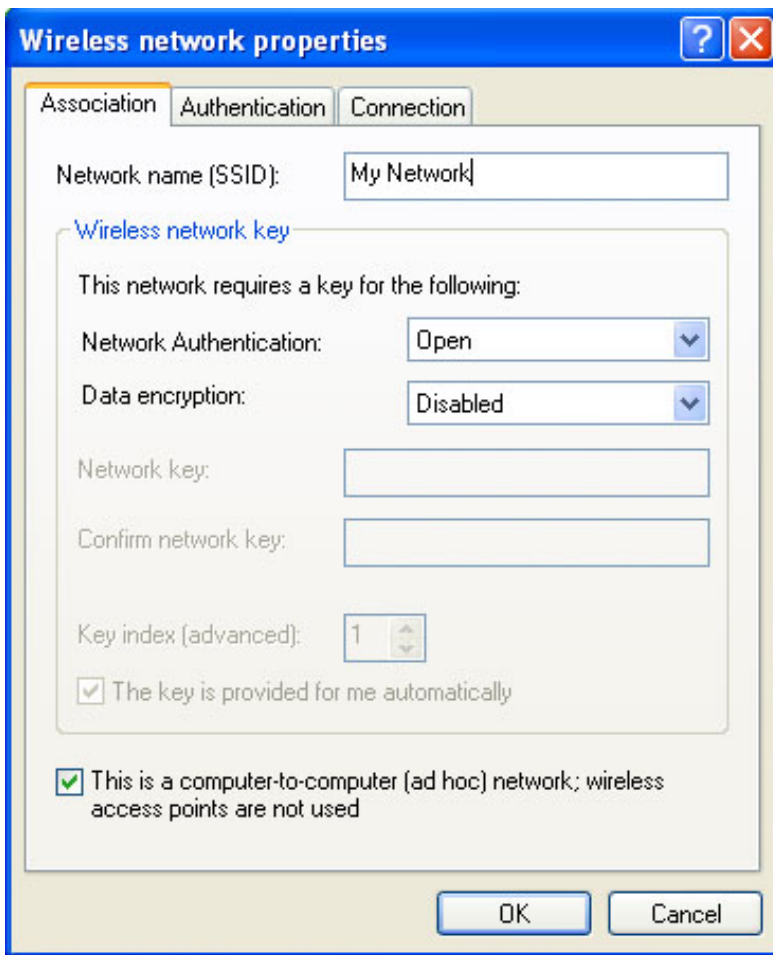
1. Click **Start** à **Settings** à **Control Panel** and double-click **Network Connections**.
2. Right-click **Wireless Network Connection** and click **Properties**.
3. On the Wireless Network Connection Properties window, select the **Wireless Networks** tab.
4. Verify that the **Use Windows to configure my wireless network settings** box is selected. If it is not, select it. The correct setting is shown in the following illustration:



5. Click **Add**. The **Wireless Network Connection Properties** window opens.

NOTE: The names of wireless networks your computer can see are shown under **Available Networks**. The name of the network is usually shown here.

6. In the **Network name (SSID)** text box, enter the name of the network you want to add.
7. For Network Authentication, select **Open** (default setting).
8. For Data encryption, select **Disabled**.
9. Select the **This is a computer-to-computer (ad hoc) network; wireless Access Points are not used** checkbox. These settings are shown in the following illustration:



10. Click **OK**. You are returned to the Wireless Network tab, and the new network name appears in the **Preferred networks** list.

 **NOTE:** Internet connection and firewall settings under Windows XP (Service Pack 2) may affect the ability to connect to an ad hoc network.

Your network configuration is now complete. Continue to [Viewing the Status of your Wireless Network Connection](#).

Ad hoc connection options

Name	Description
Network Authentication	Open: No authentication used. Open authentication allows a wireless device access to the network without 802.11 authentication. The access point allows any request for authentication. If no encryption is enabled on the network, any wireless device with the correct network name (SSID) can associate with the access point and gain access to the network. Shared: Shared authentication is accomplished with a pre-configured WEP key. Use this mode for 802.11 Authentication. This mode can work with any 802.1x authentication protocol and with the following data encryption options; None, WEP (64-bit, or 128-bit) or CKIP (64-bit, or 128-bit).

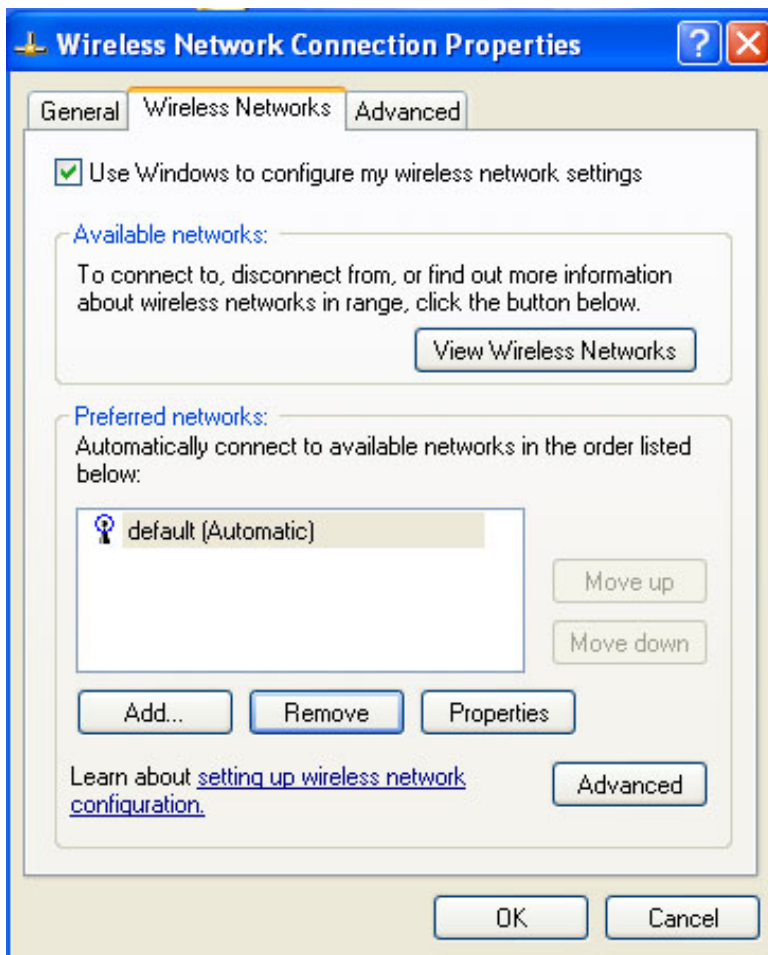
	WPA-None: No authentication used on a Wi-Fi Protected Access (WPA) client. This works with TKIP and AES data encryption in an ad hoc connection.
Data Encryption	Disabled: No data encryption is used. WEP: WEP data encryption can be configured using 64-bit or 128-bit. WEP settings can be used with all Network Authentication protocols. When WEP encryption is enabled on an access point, the WEP key provides a way to verify access to the network. If the wireless device does not have the correct WEP key, even though authentication is successful, the device is unable to transmit data through the access point or decrypt data received from the access point.
Encryption Level	64-bit or 128-bit: 64-bit or 128-bit encryption.
Key Index	1,2,3,4: Up to four passwords may be specified by changing the Key Index.
Wireless Security Password (WEP Key)	Type the wireless network Password (WEP Key) in the text box. The Password is the same value used by the wireless access point or router. Contact your wireless network administrator for this password. Pass phrase (64-bit): Enter 5 ASCII characters (can use any characters, including spaces). Hex key (64-bit): Enter 10 alphanumeric hexadecimal characters, 0-9, A-F. Pass phrase (128-bit): Enter 13 ASCII characters (can use any characters, including spaces). Hex key (128-bit): Enter 26 alphanumeric hexadecimal characters, 0-9, A-F.

Configuring an Ad hoc Network with WEP Security

One configuration option for your ad hoc network is to set it up with no security (data encryption disabled), but this allows anyone to access your wireless network. Another option is to use [WEP](#) encryption. Using WEP encryption provides some level of security for your wireless network.

To use configure your ad hoc network with WEP security:

1. Click **Start** à **Settings** à **Control Panel** and double-click **Network Connections**.
2. Right-click **Wireless Network Connection** and click **Properties**. The Wireless Network Connection Properties window opens.
3. On the Wireless Network Connection Properties window, click the **Wireless Networks** tab as shown in the following illustration:



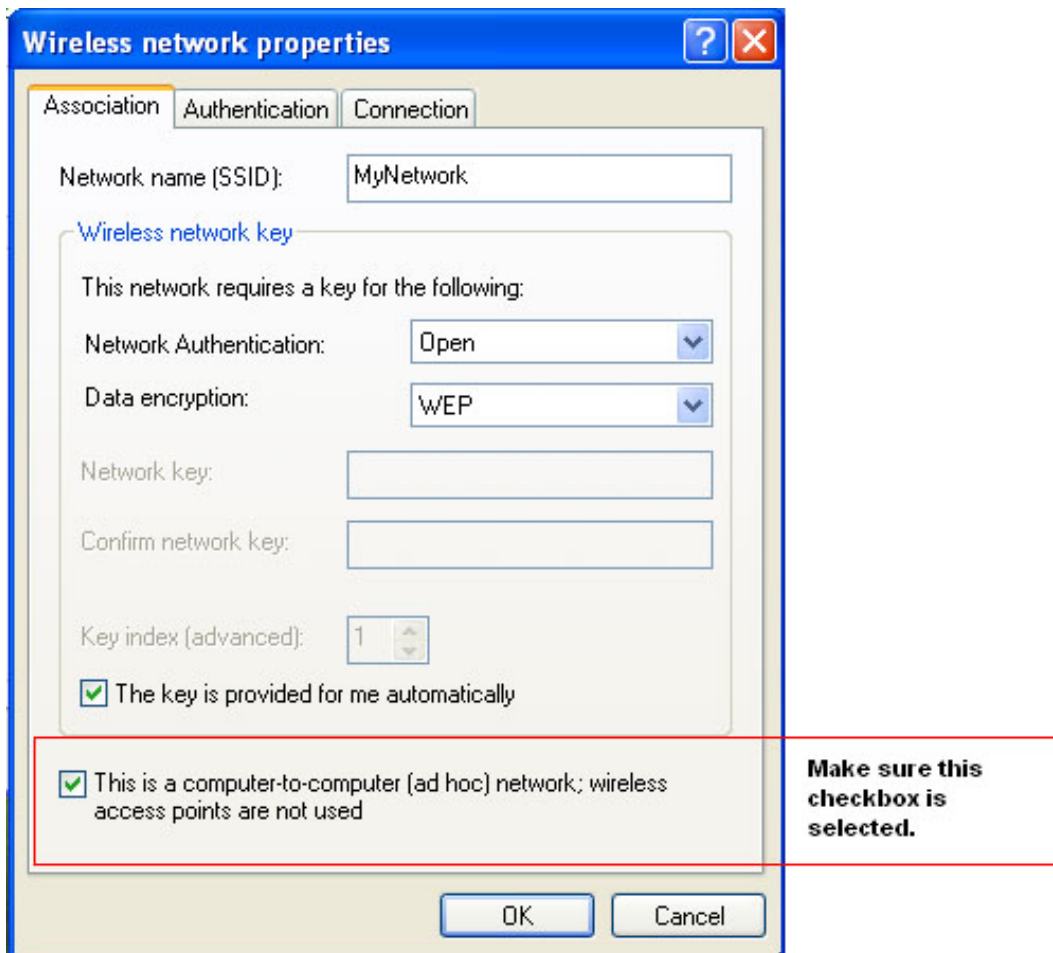
4. From the list of Preferred Networks, select the network and click **Properties**. The Network properties window opens.

Note: Make sure that **This is a computer-to-computer (ad hoc) network; wireless access points are not used** is selected.

5. On the Association tab, from the Network Authentication drop-down menu, select **Open**.

NOTE: Earlier versions of Windows XP software may not contain these drop-down menus. If you are using one of these earlier versions, click to select the **Data encryption (WEP enabled)** checkbox and continue with the next step.

6. From the Data Encryption drop-down menu, click **WEP**. These settings are shown in the following illustration:



NOTE: If the wireless network does not require a network key (password), skip to step 10.

7. If you need to provide a network key, click to deselect **The key is provided for me automatically**.
8. In the Network key text box, type the **WEP network key**. Your Network key must exactly match the password (network key) used by other computers in the ad hoc network. Your Network key will be either 5 or 13 ASCII (text) characters, or 10 or 26 hexadecimal (0-9, A-F) characters.
9. In the Confirm network key text box, type this key again.
10. To save your settings, click **OK**.
11. To close the Wireless Network Connection Properties window, click **OK**.

Your network configuration is now complete. For more information about the status of your connection, refer to [Viewing the Status of your Wireless Network Connection](#).

Ad hoc network connection using no network authentication (Open) with WEP data encryption

Name	Description
Network Authentication	Open: No authentication used. Open authentication allows a wireless device access to the network without 802.11 authentication. The access point allows any request for authentication. If no encryption is enabled on the network, any wireless device with the correct network name (SSID) can associate with the access point and gain access to the network.

Data Encryption	WEP: WEP data encryption can be configured using 64-bit or 128-bit. WEP settings can be used with all Network Authentication protocols. When WEP encryption is enabled on an access point, the WEP key provides a way to verify access to the network. If the wireless device does not have the correct WEP key, even though authentication is successful, the device is unable to transmit data through the access point or decrypt data received from the access point.
Encryption Level	64-bit or 128-bit: 64-bit or 128-bit encryption.
Key Index	1,2,3,4: Up to four passwords may be specified by changing the Key Index.
Wireless Security Password (WEP Key)	Type the wireless network Password (WEP Key) in the text box. The Password is the same value used by the wireless access point or router. Contact your wireless network administrator for this password. Pass phrase and hex key options are: Pass phrase (64-bit): Enter 5 ASCII characters (can use any characters, including spaces). Hex key (64-bit): Enter 10 hexadecimal characters, 0-9, A-F. Pass phrase (128-bit): Enter 13 ASCII characters (can include any characters, including spaces). Hex key (128-bit): Enter 26 alphanumeric hexadecimal characters, 0-9, A-F.

Configuring a WPA-PSK Client with AES or TKIP Encryption

This security level is available for Infrastructure networks. To configure a WPA-PSK client:

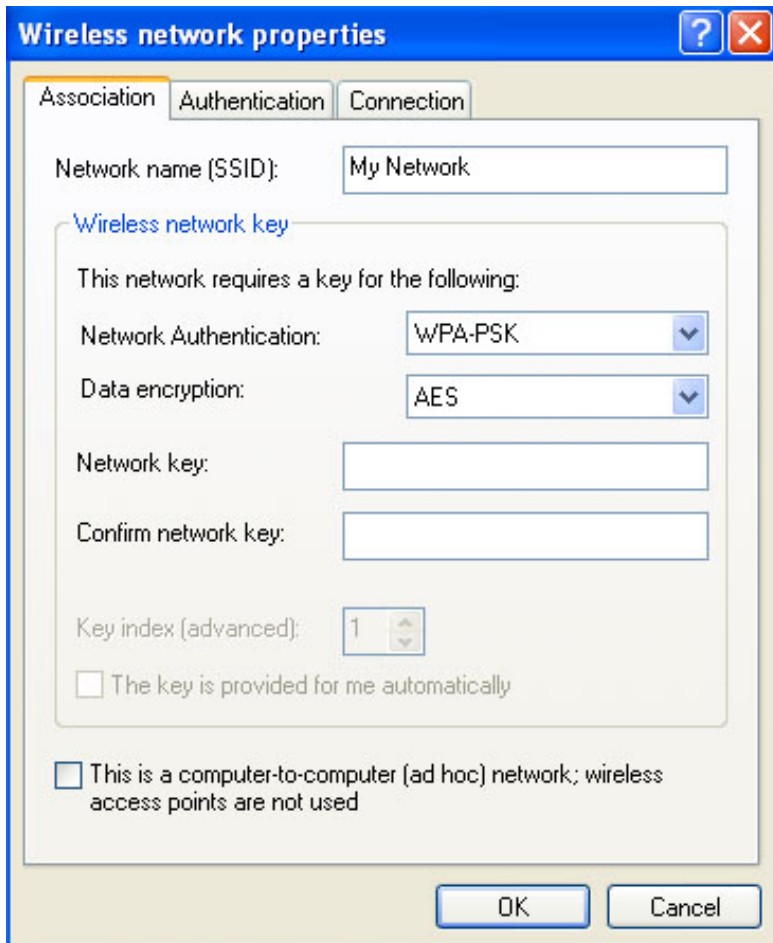
1. Click **Start** à **Settings** à **Control Panel** and then double-click **Network Connections**.
2. Right-click **Wireless Network Connection** and click **Properties**.
3. On the Wireless Network Connection Properties window, select the **Wireless Networks** tab.
4. Verify that the **Use Windows to configure my wireless network settings** box is selected. If it is not, select it.
5. From the Preferred Networks list, select the network you want and click **Properties**.

 **NOTE:** If the wireless network access point is in silent mode ([blank network name SSID](#)) the network name will not be displayed. You must first add the network name (SSID), then it will appear in the list of available networks.

6. For Network Authentication, select [WPA-PSK](#) (Wi-Fi Protected Access Pre-shared Key).

NOTE: Earlier versions of Windows XP did not support encryption modes such as WPA and WPA-PSK. If you cannot view these options in the dropdown menu, please update Windows XP to the latest service pack. If WPA is required the Microsoft WPA supplicant must also be installed.

7. For Data Encryption, select **AES** or **TKIP**. These settings are shown in the following illustration:



8. If you need to provide a network key, click to deselect **The key is provided for me automatically**.
9. Enter the network key in the **Network Key** and the **Confirm Network Key** box. The network key must be a text phrase from 8 to 63 characters long or, a Hex key (0-9, A-F) 64 characters long.

NOTE: Refer to your access point/router settings (for home users) or, contact your system administrator for the data encryption type and network key (enterprise users.)

10. To save your settings, click **OK**.
11. To close the Wireless Network Connection Properties window, click **OK**.

For more information about connection status, refer to [Viewing the Status of your Wireless Network Connection](#).

For more information about PEAP authentication, refer to [Security Overview](#).

Configuring a WPA-PSK Client with AES or TKIP Encryption and TLS or TTLS

Authentication

Transport Layer Security TLS and Tunnelled Transport Layer Security (TTLS) settings define the protocol and the credentials used to authenticate a user. TLS is a type of authentication method using Extensible Authentication Protocol (EAP) and a security protocol called Transport Layer Security. EAP-TLS uses certificates that require passwords. EAP-TLS authentication supports dynamic WEP key management. The TLS protocol is intended to secure and authenticate communications across a public network through data encryption. The TLS Handshake Protocol allows the server and client to provide mutual authentication and to negotiate an encryption algorithm and cryptographic keys before data is transmitted. In TTLS, the client uses EAP-TLS to validate the server and create a TLS-encrypted channel between the client and server. The client can use another authentication protocol, typically password-based protocols, such as MD5 Challenge over this encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel. TTLS implementations today support all methods defined by EAP, as well as several older methods (CHAP, PAP, MS-CHAP and MS-CHAPv2). TTLS can easily be extended to work with new protocols by defining new attributes to support new protocols.

To configure this infrastructure network:

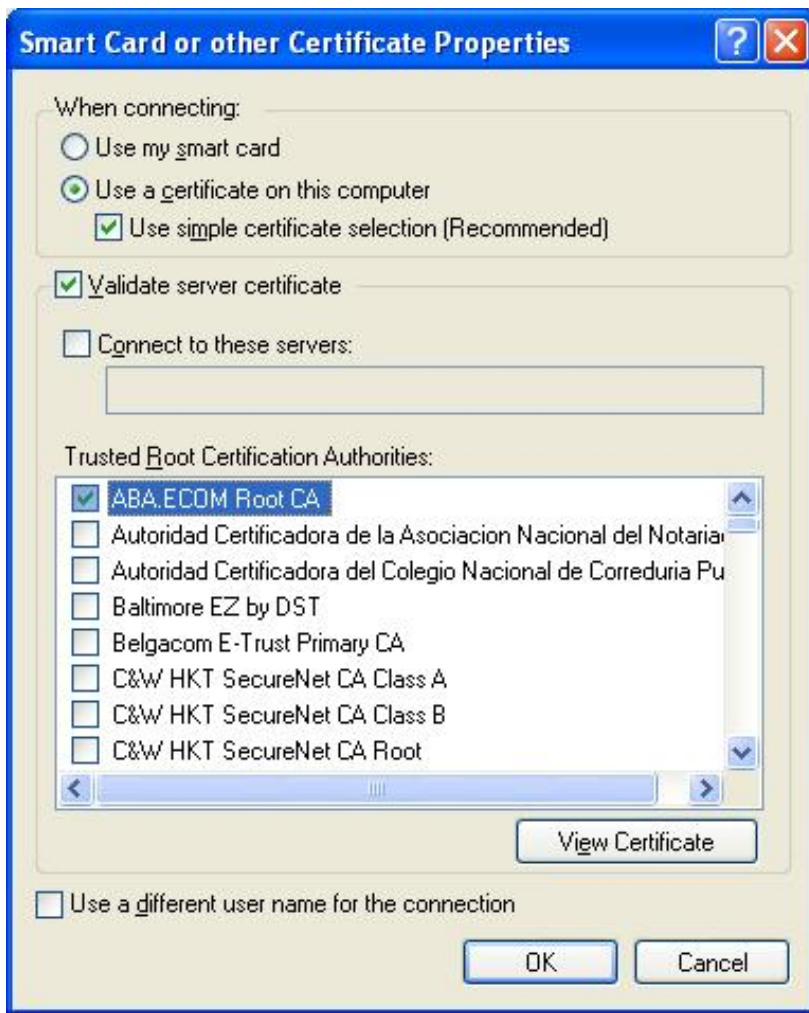
1. Click **Start** à **Settings** à **Control Panel** and double-click **Network Connections**.
2. Right-click **Wireless Network Connection Properties** and click **Properties**.
3. When the Wireless Network Properties window opens, click the **Wireless Networks** tab.
4. Verify that the **Use Windows to configure my wireless network settings** box is selected. If it is not, select it.
5. From the Preferred Networks list, select the network you want and click **Properties**. The network properties window opens.
6. For Network Authentication, select [WPA-PSK](#) (Wi-Fi Protected Access).

 **NOTE:** Earlier versions of Windows XP did not support encryption modes such as WPA and WPA-PSK. If you cannot view these options in the dropdown menu, please update Windows XP to the latest service pack.

7. For Data Encryption (depending on your network encryption), select [AES](#) or [TKIP](#). If you are not sure which data encryption type to use, contact your network administrator.
8. Click the **Authentication** tab and then select **Smart Card or other certificate** for EAP Type, as shown in the following illustration:



9. Click **Properties** and then select **Use a certificate on this computer**:



10. Select the appropriate certificate(s) from the Trusted Root Certification Authorities. Contact your network administrator if you cannot find the appropriate certificate or do not know which one to use.
11. To close the Smart Card or other Certificate Properties window, click **OK**.
12. To close the Wireless network properties box, Click **OK**.

To verify that your network connection has been made, refer to [Viewing the Status of your Wireless Network Connection](#).

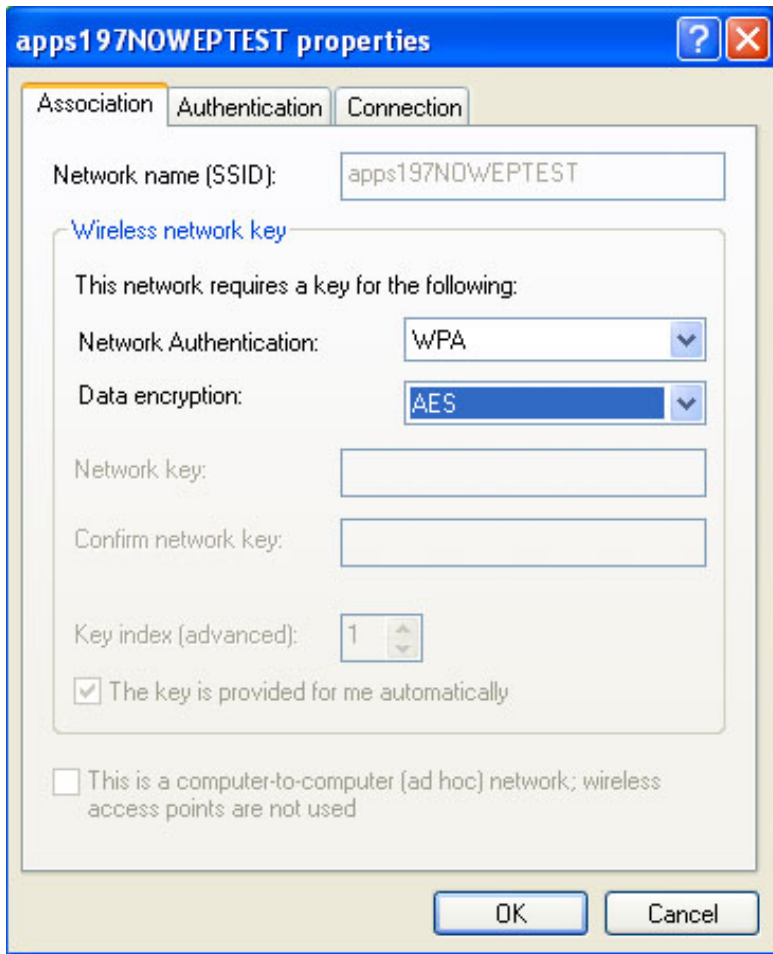
For information about how to obtain a client certificate for TLS or TTLS authentication, contact your network administrator or, refer to [Setting up a client for TLS/TTLS authentication](#).

Configuring a WPA Client with AES or TKIP Encryption and PEAP Authentication

Protected Extensible Authentication Protocol (PEAP) is an Internet Engineering Task Force (IETF) draft protocol sponsored by Microsoft, Cisco, and RSA Security. PEAP is designed to take advantage of server-side Extensible Authentication Protocol (EAP)-Transport Layer Security (TLS) and to support various authentication methods, including user passwords, one-time passwords, and Generic Token Cards.

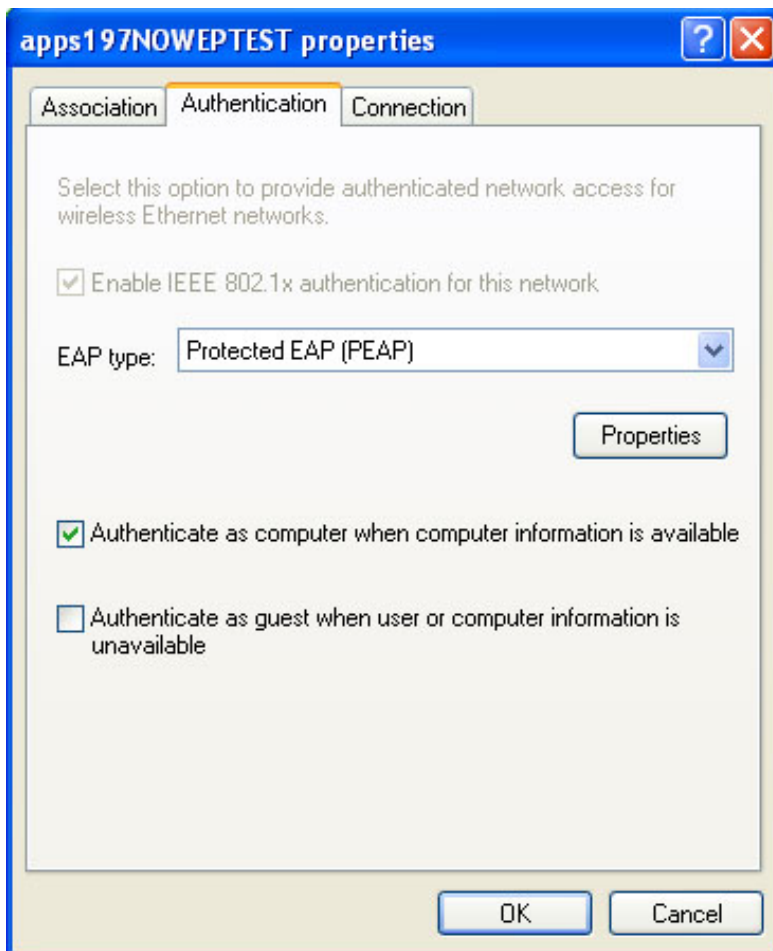
To configure this infrastructure network with PEAP authentication:

1. Click **Start** à **Settings** à **Control Panel** and then double-click **Network Connections**.
2. Right-click **Wireless Network Connection** and click **Properties**.
3. On the Wireless Network Connection Properties window, select the **Wireless Networks** tab.
4. Verify that the **Use Windows to configure my wireless network settings** box is selected. If it is not, select it.
5. From the Preferred Networks list, select the network you want and click **Properties**. The network properties window opens.
6. For Network Authentication, select **WPA**.
7. For Data encryption, select **AES** or **TKIP**. These settings are shown in the following illustration.

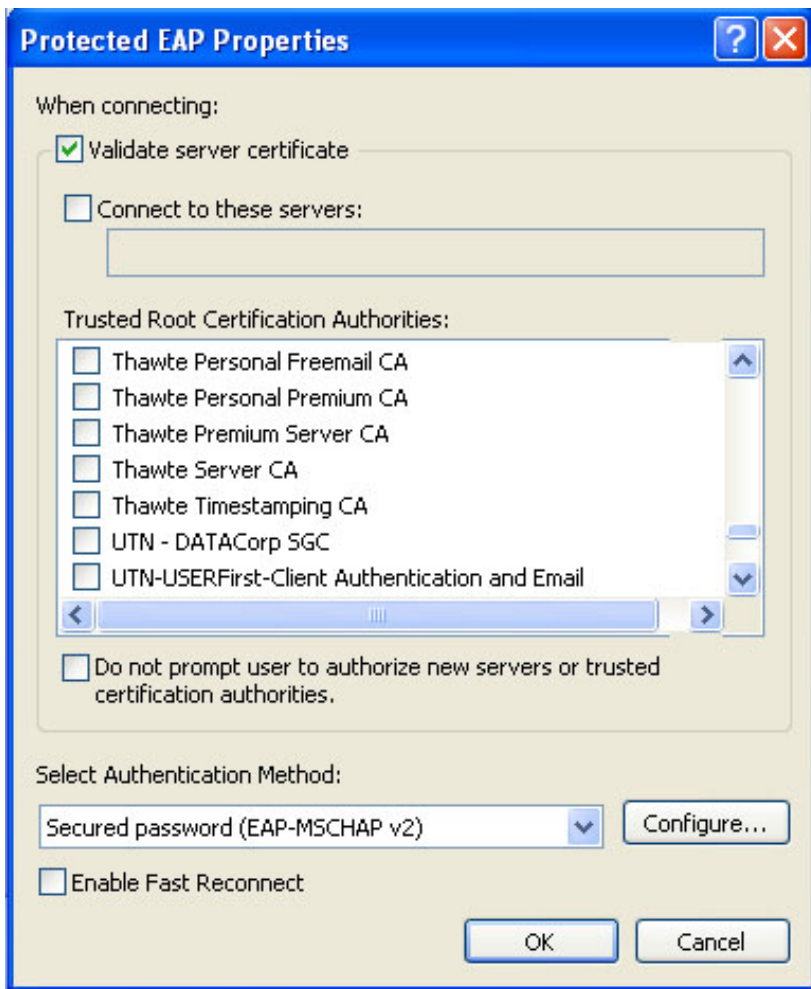


NOTE: Earlier versions of Microsoft Windows XP did not support encryption modes such as WPA and WPA-PSK. If you cannot view these options in the dropdown menu, please update Windows XP to the latest service pack.

8. Click the **Authentication** tab and for EAP type, select **Protected EAP (PEAP)**.



9. Click **Properties**.
10. When the Protected EAP Properties window opens, select **Validate server certificate**.
11. Select the appropriate **Trusted Root Certification Authority** from the list.
12. For the authentication method, select **Secured password (EAP-MSCHAP v2)**. These settings are shown in the following illustration:



13. Click **Configure**. The following properties window opens.



14. Make sure **Automatically use my Windows logon name and password** is checked.

15. To return to the previous window, click **OK**.

16. To save your settings on the Protected AP Properties window, click **OK**.

17. To save your settings on the Authentication tab, click **OK**.

18. To close the Wireless Network Connection Properties window, click **OK**.

To verify that your network connection has been made, refer to [Viewing the Status of your Wireless Network Connection](#).

For more information about PEAP authentication, refer to [Security Overview](#).

Configuring a Client for TLS/TTLS Authentication

The information in this section is intended for enterprise system administrators. For enterprise customers, contact your system administrator to obtain a client certificate for TLS/TTLS authentication. While obtaining a certificate for TLS/TTLS authentication, ensure strong private key protection is disabled. This is required for 802.1x authentication. EAP-TLS and EAP-TTLS authentication require client certificates in the local repository for the logged in users account and a trusted CA certificate in the root store. Certificates can be obtained from a corporate certificate authority located on a Windows 2000 Server or using Internet Explorer's certificate import wizard.

Obtaining a certificate from Windows 2000 Server

1. Launch Internet Explorer and browse to the Certificate Authority (CA) HTTP Service.
2. Logon to the CA Authority with the username and password of the user account created on the authentication server. This username and password are not necessarily the same as your Windows username and password.
3. On the Welcome page, select **request a certificate** task and submit the form.
4. On the Choose request page, select **Advanced request** and click **Next**.
5. On the Advanced Requests page, select **Submit a certificate request to this CA** using a form and click next.
6. On the Advanced Requests page, choose the **user certificate** template. Select **Mark keys as exportable** and click next.
7. On the Certificate Issued page, select **Install this certificate**. If this is the first certificate you have installed, you will prompted install a trusted CA certificate in the root store. Click **Yes** as you will need this certificate for TLS and TTLS authentication.
8. If you certificate was correctly installed, you will see the message: **Your new certificate has been successfully installed**.
9. To verify the installation, click à **Tools** à **Internet Options** à **Content** à **Certificates**. The new certificate should be installed in the personal folder.

Obtaining a certificate from a file

1. Right click on Internet Explorer icon on desktop, and select **Properties**.
 2. Select the **Content** tab, click the **Certificates** button. This displays a list of installed certificates.
 3. Select the import button under the list of certificates. This starts the Certification Import Wizard.
 4. Select the certificate file and click the password page.
 5. Enter the password for the file and ensure **strong private key protection option** is **not** selected.
 6. On the certification store page, select **automatically select certificate store based on the type of certificate**.
 7. Proceed to **complete the certificate import** and click **Finish**.
-

[Back to Top](#)

[Back to Contents](#)

[Back to Contents](#)

Configuring Advanced Network Security Settings in Windows 2000: Intel® PROSet/Wireless 2915ABG Network Connection User's Guide

[Using Intel PROSet/Wireless](#)

[Ad Hoc Network Overview](#)

[Configuring an Ad Hoc Network with WEP Security or without Security](#)

[Configuring a WEP Client with WEP and MD5 Authentication](#)

[Configuring a WPA2-Enterprise Client with WEP, TKIP or AES-CCMP authentication](#)

[Configuring a WPA Client with TKIP Encryption and TTLS or PEAP Authentication](#)

[Configuring a CCX Client with CKIP Encryption and LEAP Authentication](#)

[System Administrator Tasks \(Obtain a Certificate\)](#)

Using Intel® PROSet/Wireless

The following sections describe how to set up peer-to-peer networking using Intel® PROSet/Wireless.

It also provides information about how to configure advanced security settings for your wireless adapter. This requires information from a system administrator (corporate environment) or advanced security settings on your access point (for home users). If you are using Windows XP, refer to [Making a Basic Network Connection in Windows XP](#) to configure basic profiles. For advanced security settings, refer to [Configuring Advanced Network Security Settings in Windows XP](#). If you are using Windows 2000, click [Making a Basic Network Connection in Windows 2000](#) for basic setup instructions.

 **NOTE:** The software is compatible with the Intel® PRO/Wireless 2915ABG Network Connection and Intel® PRO/Wireless 2200BG Network Connection.

Ad Hoc Network Overview

In peer-to-peer (ad hoc) mode, you can send information to and receive it from other computers without using an access point. Each computer in a peer-to-peer network is called a peer. Creating an ad hoc network requires more than one computer with a wireless adapter. All systems on the

ad hoc network must be configured identically.

To join an ad hoc network, you must know the ad hoc network key to connect to other computers in the ad hoc network. If you create the ad hoc network from your computer, other computers can connect using the network key (SSID) that you created. Once a network connection is established and after permission rights are given by other computers in the ad hoc network, you can freely share files. All wireless clients in the ad hoc network must use the same network name (SSID) and channel number. For a list of allowed 802.11b ad hoc channels, refer to the [Adapter Settings](#) for more information.

[Configuring an Ad Hoc Network with WEP Security or without Security](#)

Configuring an Ad Hoc Network with WEP Security or without Security

The following examples illustrate how to create a new ad hoc profile using the Profile Wizard and connect to an ad hoc network with or without WEP security. For more information about authentication and encryption settings, refer to [Security Overview](#).

To configure a new ad hoc profile with no security:

1. Double-click the **Intel PROSet Wireless** icon in the desktop task tray or click **Start** à **Programs** à **Intel PROSet Wireless** à **Intel PROSet Wireless**.
2. From the Intel PROSet/Wireless main window click **Add**. The General Settings window opens:

Create Wireless Profile

Profile Name: Ad Hoc

General Settings

Security Settings

General Settings

Profile Name: Ad Hoc

Wireless Network Name (SSID): Ad Hoc

Operating Mode:

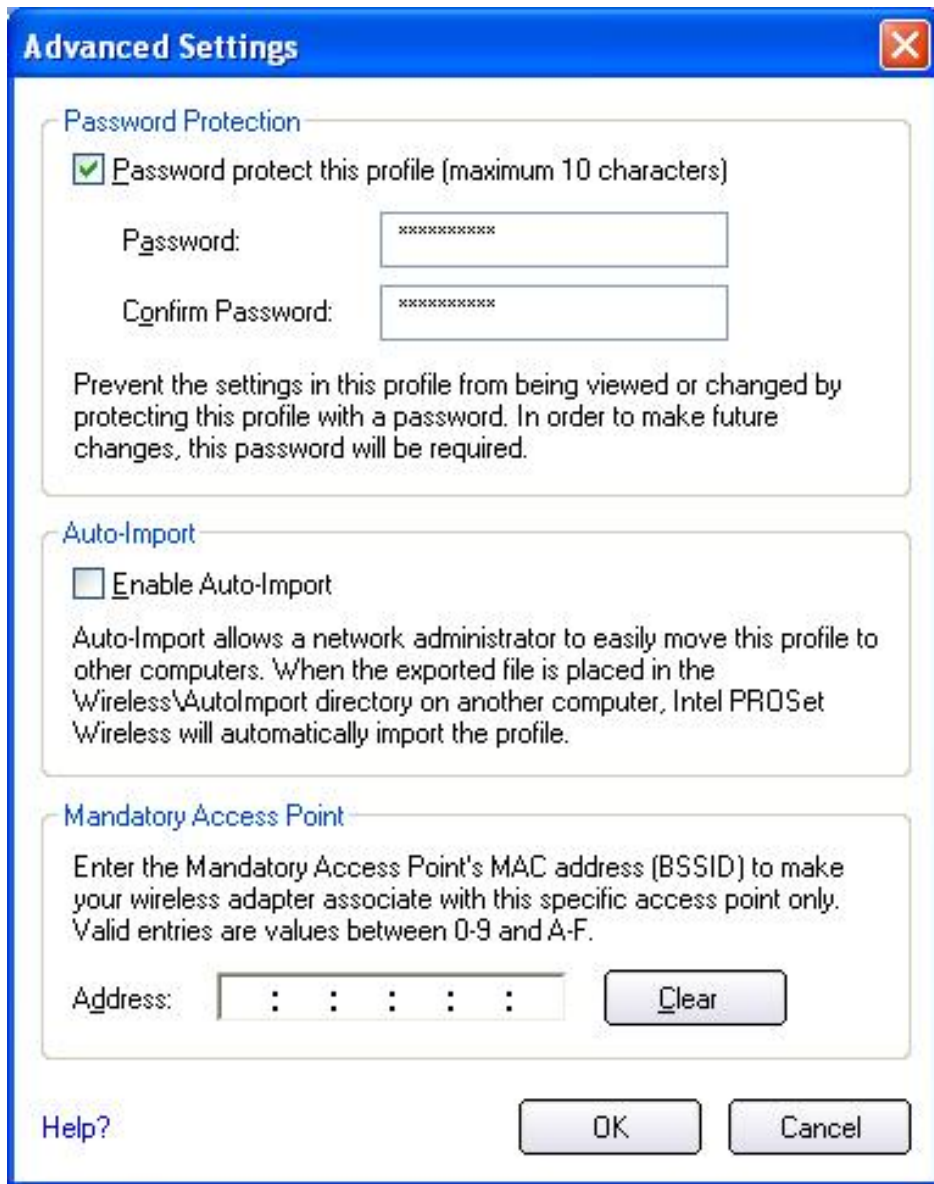
☐ Network (Infrastructure) - Connect to wireless networks and/or the internet.

☒ Device to device (Ad hoc) - Connect directly to other computers.

Advanced...

Help? << Back Next >> OK Cancel

3. Enter the **Profile Name** and **Wireless Network Name (SSID)**.
4. Select **Device to device [Ad hoc]**.
5. If you want to assign a password for this profile, click **Advanced**. The Advanced Settings window opens.



The image shows a Windows 2000 dialog box titled "Advanced Settings" with a blue title bar and a close button (X) in the top right corner. The dialog is divided into three sections: "Password Protection", "Auto-Import", and "Mandatory Access Point".

Password Protection

☒ Password protect this profile (maximum 10 characters)

Password:

Confirm Password:

Prevent the settings in this profile from being viewed or changed by protecting this profile with a password. In order to make future changes, this password will be required.

Auto-Import

☐ Enable Auto-Import

Auto-Import allows a network administrator to easily move this profile to other computers. When the exported file is placed in the Wireless\AutoImport directory on another computer, Intel PROSet Wireless will automatically import the profile.

Mandatory Access Point

Enter the Mandatory Access Point's MAC address (BSSID) to make your wireless adapter associate with this specific access point only. Valid entries are values between 0-9 and A-F.

Address:

At the bottom left is a "Help?" link. At the bottom right are "OK" and "Cancel" buttons.

6. Select **Password protect this profile (maximum 10 characters)**.
7. Enter the password, and then enter it again in the Confirm Password box.
8. To save your settings and close the window, click **OK**. You are returned to the General Settings window.
9. Click **Next**. The Security Settings window opens:

Create Wireless Profile

Profile Name: Ad Hoc

General Settings

Security Settings

WEP Key

Security Settings

Select the appropriate security settings for your wireless network. Your network administrator can help with these settings.

Network Authentication: Open

Data Encryption: WEP

☐ Enable 802.1x

Authentication Type: None Cisco Options...

WEP Key

Encryption Level: 64-bit Key Index: 1

Wireless Security Password (WEP Key):

(HINT: Passphrase - 5 characters OR Hex - 10 hexadecimal values)

The Security Password is the same value used by the Wireless Access Point.

(Advanced: Up to four passwords (keys) may be specified by changing the Key Index.)

Help? << Back Next >> OK Cancel

10. In the Network Authentication text box, select **Open** (default setting).
11. In the Data Encryption text box:
 - No security: Select **None** and proceed to step 15.
 - WEP security: Select **WEP** and continue to step 12.
12. For the Encryption Level, select **64-bit** or **128-bit**.
13. For Key Index, select a key index number **1, 2, 3, or 4**. Key selection must correspond to the network key on the access point.
14. In the **Wireless Security Password (WEP Key)** text box, enter the password characters. Select either of the following:
 - **Use ASCII characters:** Click **Use ASCII characters** to enable. Enter a

text phrase, five (using 64-bit) or 13 (using 128-bit) ASCII characters (can use all characters, including space), in the pass phrase field.

- **Use hex Key:** Click **Use hex Key** to enable. Enter ten (using 64-bit) alphanumeric characters, 0-9, A-F, or 26 (using 128-bit) alphanumeric characters (0-9, A-F) in the hex key field.

 **NOTE:** Both the network name and the network key information are case-sensitive.

15. To save the settings and close the Security Settings window, click **OK**. The profile is positioned at the bottom of the Profiles list. Use the up and down arrows to position it elsewhere on the list.
16. To connect to the wireless network, click **Connect**.

To verify the status of your wireless connection, refer to [Viewing the Status of your Wireless Connection](#).

 **NOTE:** Unless other computers in the ad hoc network use a different channel from the default channel, there is no need to change the default channel. If you want to change the default channel, select **Adapter Settings** under the Tools menu, choose the operating band, and then select a channel.

Security Settings: Open authentication, no encryption

There is no network authentication or data encryption used on this network.

Name	Description
Network Authentication	Open: No authentication used. Open authentication allows a wireless device access to the network without 802.11 authentication. The access point allows any request for authentication. If no encryption is enabled on the network, any wireless device with the correct network name (SSID) can associate with the access point and gain access to the network.
Data Encryption	None: No data encryption used.
Enable 802.1x	Unchecked.

Security Settings: Open Authentication, WEP Encryption

This network uses no network authentication with WEP data encryption.

Name	Description
------	-------------

Network Authentication	Open: No authentication used. Open authentication allows a wireless device access to the network without 802.11 authentication. The access point allows any request for authentication. If no encryption is enabled on the network, any wireless device with the correct network name (SSID) can associate with the access point and gain access to the network.
Data Encryption	WEP: WEP data encryption can be configured using 64-bit or 128-bit. When WEP encryption is enabled on an access point, the WEP key provides a way to verify access to the network. If the wireless device does not have the correct WEP key, even though authentication is successful, the device is unable to transmit data through the access point or decrypt data received from the access point.
Encryption Level	64-bit or 128-bit: 64-bit or 128-bit encryption.
Key Index	1,2,3,4: Up to four passwords may be specified by changing the Key Index.
Wireless Security Password (WEP Key)	Type the wireless network Password (WEP Key) in the text box. The Password is the same value used by the Wireless Access Point or Router. Contact your wireless network administrator for this password. Pass phrase and hex key options are: Pass phrase (64-bit): Enter 5 aASCII characters (can include any characters, including spaces). Hex key (64-bit): Enter 10 hexadecimal characters, 0-9, A-F. Pass phrase (128-bit): Enter 13 alphanumeric characters (can use any characters, including spaces). Hex key (128-bit): Enter 26 alphanumeric hexadecimal characters, 0-9, A-F.

Configuring a WEP Client with WEP and MD5 Authentication

Note: Before starting, you must obtain a user name and password on the RADIUS server from your system administrator.

To add WEP and MD5 authentication to a new profile:

1. From Intel PROSet/Wireless main window, under the Profile list click **Add**. The General Settings window opens.
2. Enter the profile and network (SSID) name.

3. For the operating mode, select **Infrastructure**.
4. If you want to assign a profile password, click **Advanced** and enter the password information; then click **OK** to return to the General Settings window.
5. On the General Settings window, click **Next**. The Security Settings window opens.

The screenshot shows the 'Create Wireless Profile' dialog box with the 'Security Settings' tab selected. On the left, a tree view shows 'Profile Name: wep', 'General Settings', 'Security Settings' (selected), 'WEP Key', and 'MD5 User'. The main area is titled 'Security Settings' and contains the following fields and options:

- Network Authentication:** A dropdown menu set to 'Open'.
- Data Encryption:** A dropdown menu set to 'WEP'.
- Enable 802.1x:** A checked checkbox.
- Authentication Type:** A dropdown menu set to 'MD5'. A list box is open showing options: MD5, EAP-SIM, TLS, TTLS, PEAP, LEAP, and EAP-FAST.
- Step 1 of 2: WEP Key:** A label for the current step.
- Encryption Level:** A dropdown menu set to '128'.
- Wireless Security Password:** A text box with a hint: '(HINT: Passphrase - 13 characters OR Hex - 26 hexadecimal values)'. Below it, a note states: 'The Security Password is the same value used by the Wireless Access Point. (Advanced: Up to four passwords (keys) may be specified by changing the Key Index.)'
- Cisco Options...:** A button.

At the bottom, there are four buttons: 'Help?', '<< Back', 'Next >>', 'OK', and 'Cancel'.

6. For Network Authentication, select **Open** (recommended).
7. For Data Encryption, select **WEP**.
8. Click the **Enable 802.1x** checkbox.
9. For Authentication Type, select **MD5** as the 802.1x.
10. For the Encryption Level, select either **64-bit** or **128-bit**.
11. Select the **key index 1, 2, 3 or 4**. Key 1 is the default setting.
12. In the Wireless Security Password (WEP Key) text box, enter the required **pass phrase** or

hex key.

13. In the left side panel, click **MD5 User** to display the MD5 setting. The following window opens:

The screenshot shows the 'Create Wireless Profile' window with the 'Security Settings' tab selected. The left sidebar shows the navigation tree with 'MD5 User' highlighted. The main area displays the 'Security Settings' for the 'MD5 User' profile. The 'Network Authentication' is set to 'Open' and 'Data Encryption' is set to 'WEP'. The 'Enable 802.1x' checkbox is checked. The 'Authentication Type' is set to 'MD5'. A 'Cisco Options...' button is visible. The 'Step 2 of 2 : MD5 User' section contains three radio button options: 'Use the Windows logon user name and password', 'Prompt for the user name and password', and 'Use the following user name and password:'. The third option is selected. Below this, there are four text input fields: 'User Name' (containing 'User Name'), 'Domain' (containing 'Domain Name'), 'Password' (empty), and 'Confirm Password' (empty). At the bottom, there are buttons for '<< Back', 'Next >>', 'OK', and 'Cancel', along with a 'Help?' link.

14. Select one of the following options:

- **Use the Windows logon user name and password:** Select this option to use your Windows log on user name for a Windows session. Note: this option is only available if you have the single sign On Pre-Login Connection component installed.
- **Prompt for the user name and password:** Select this option to prompt for user credentials when you log on to a Windows session.
- **Use the following user name and password:**

- **User Name:** This user name must match the user name that is set in the authentication server. Note: The user name and password do not have to be the same as the name of your current Windows user login.
- **Domain:** Optionally enter the domain name.
- **Password:** This password must match the password that is set in the authentication server. The entered password characters display as asterisks. Note: The user name and password do not have to be the same as the password of your current Windows user login.
- **Confirm Password:** Re-enter the user password.

15. To save the settings and close the Security Settings page, click **OK**.

Configuring a WPA/WPA2-Enterprise Client with WEP, TKIP, or AES-CCMP Authentication

 **Note:** (1) Before starting, you must obtain a user name and password on the RADIUS server from your system administrator. (2) For personal/home networks use Wi-Fi Protected Access Personal (WPA/WPA2 Personal) mode. WPA/WPA2-Enterprise requires an authentication server.

To add WPA/WPA-2 Enterprise authentication to a new profile:

1. Obtain and install a client certificate. For more information refer to [Setting up the Client for TLS authentication](#) or consult your system administrator.
2. From Intel PROSet/Wireless main window, click **Add** from the Profiles list. The General Settings window opens.
3. Enter the profile and network (SSID) name.
4. Select **Infrastructure** for the operating mode.
5. To assign a profile password, click **Advanced** and enter the password information; then click **OK** to return to the General Settings window.
6. On the General Settings window, click **Next**. The Security Settings window opens.
7. For Network Authentication, select WPA-Enterprise or [WPA2-Enterprise](#).
8. For Data Encryption, select WEP, TKIP, or [AES-CCMP](#).
9. Click the **Enable 802.1x** checkbox.
10. For the 802.1x Authentication Type, select [TLS](#). The Security settings are shown in the following illustration:

Create Wireless Profile

Profile Name: wep

General Settings

Security Settings

TLS User

TLS Server

Security Settings

Select the appropriate security settings for your wireless network. Your network administrator can help with these settings.

Network Authentication: WPA2 - Enterprise

Data Encryption: AES - CCMP

☒ Enable 802.1x

Authentication Type: TLS [Cisco Options...](#)

Step 1 of 2: TLS User

☐ Use my smart card

☒ Use a certificate on this computer

User Name:

Issued To:

Issued By:

Expires On:

Friendly Name:

Choose a certificate by clicking the Select button. [Select...](#)

[Help?](#) [<< Back](#) [Next >>](#) [OK](#) [Cancel](#)

11. Under TLS user, select either:

- **Use my smart card.** Insert your Smart Card when you log on to your computer using this profile.
- **Use a certificate on this computer:** Your user name should be displayed in the User Name text box. Click the **Select** button to open a list of installed certificates. Select a certificate from the list. This option selects a client certificate from the Personal certificate store of the Windows logged-in user. This certificate will be used for client authentication. Click the **Select** button to open a list of installed certificates. Click **OK** to close the window.

12. In the left side panel to display the TLS setting, click **TLS Server**. Choose a certificate from the list or use the default certificate 'Any Trusted CA' and select the required Server/Certificate Name.

13. Click **OK** to save the settings and close the Security Settings page.
14. Refer to [Viewing the Status of your Wireless Connection](#) to verify if your network connection has been made.

 **NOTE:** Refer to your access point/router settings (for home users) or, contact your system administrator for the data encryption type and network key (corporate users.)

Configuring a WPA/WPA2-Enterprise Client with TKIP Encryption and TTLS or PEAP Authentication

Using TTLS authentication: These settings define the protocol and the credentials used to authenticate a user. In TTLS, the client uses EAP-TLS to validate the server and create a TLS-encrypted channel between the client and server. The client can use another authentication protocol, typically password-based protocols, such as MD5 Challenge, over this encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel.

Using PEAP authentication: PEAP settings are required for the authentication of the client to the authentication server. In PEAP, the client uses EAP-TLS to validate the server and create a TLS-encrypted channel between client and server. The client can use another EAP mechanism, such as Microsoft Challenge Authentication Protocol (MSCHAP) Version 2, over this encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel.

 **Note:** Before starting, you must obtain a user name and password on the RADIUS server from your system administrator.

To set up a new profile:

1. Obtain and install a client certificate, refer to [Setting up the Client for TLS authentication](#) or consult your system administrator.
2. From Intel PROSet/Wireless main window, click **Add** under the Profiles List. The General Settings window opens.
3. Enter the profile and network (SSID) name.
4. For the operating mode, select **Infrastructure**.
5. To assign a profile password, click **Advanced** and enter the password information; then click **OK** to return to the General Settings window.
6. On the General Settings window, click **Next**.
7. For Network Authentication, select **WPA2-Enterprise**.
8. For Data Encryption, select [TKIP](#).

9. Click the **Enable 802.1x** checkbox.
10. For the 802.1x Authentication Type, select **PEAP**. The Security settings are shown in the following illustration:

Wireless Profile Properties - wep

Profile Name: wep

General Settings

Security Settings

PEAP User

PEAP Server

Security Settings

Select the appropriate security settings for your wireless network. Your network administrator can help with these settings.

Network Authentication: WPA - Enterprise

Data Encryption: TKIP

☒ Enable 802.1x

Authentication Type: PEAP Cisco Options...

Step 1 of 2: PEAP User

Authentication Protocol: MS-CHAP-V2

User Credentials: Prompt each time I connect

User Name:

Domain:

Password:

Confirm Password:

☐ Use a Client Certificate on this wireless network Select...

Roaming Identity:

[Help?](#) << Back Next >> OK Cancel

11. For authentication Protocol:

- Using MS-CHAP-V2 and GTC protocols:
 - **Use the Windows logon user name and password:** If this feature is selected the user's credentials are retrieved from the user's Windows Logon process. **Note:** This option is only available if you have the Single Sign On Pre-Login Connection component installed.

- **Prompt for the user name and password:** Selecting this feature will show a window which will prompt for user name and password before you connect to the wireless network. The user name and password must be first set in the authentication server by the IT administrator.
 - **For GTC protocol:** You may select whether you want to use a static password or a one-time password.
- **Use the following user name and password:** The user name and password are securely (encrypted) saved in the profile.
 - **User Name:** This user name must match the user name that is set in the authentication server.
 - **Domain:** Optionally enter the domain name.
 - **Password:** This password must match the password that is set in the authentication server. The entered password characters display as asterisks.
 - **Confirm Password:** Re-enter the user password.
- **Use a client certificate:** You may optionally select a client certificate from the Personal certificate store of the Windows logged-in user; this certificate is used for client authentication.
- **Roaming Identity:** When using 802.1x MS RADIUS as an authentication server, the authentication server authenticates the device by using the "Roaming Identity" username from PROSet and ignores the "Authentication Protocol MS-CHAP-V2" User Name. This feature is the 802.1x identity supplied to the authenticator. Microsoft IAS RADIUS accepts only a valid username (dotNet user) for EAP clients. Enter a valid username when using 802.1x MS RADIUS. For all other servers, this is an optional field, therefore, it is recommended that this field not contain a true identity, but instead the desired realm ([e.g., anonymous@myrealm](#)).

- **Using TLS protocol:**

- **Use my smart card or certificate:** Select smart card if the certificate resides on a smart card. Select certificate if the certificate resides on the computer.
- **User Name:** This user name must match the user name that is set in the authentication server by the IT administrator prior to client's authentication. The user name is case-sensitive. This name specifies the identity supplied to the authenticator by the authentication protocol operating over the TLS tunnel. This user's identity is securely transmitted to the server only after an encrypted channel has been verified and established.
- **Select button:** Select a client certificate from the Personal certificate store of the Windows logged-in user; this certificate will be used for client authentication.

12. For User Credentials, select **Use Windows logon**, **Prompt each time I connect**, or **Use the following**. If you select **Use the following**, you need to enter user name, domain, and password information.
13. To select a Client Certificate, click **Use a Client Certificate on this wireless network**, and then click **Select**.
14. When the Select Certificate window opens, select the certificate you want:

PEAP or TTLS: Server/Certificate Authority

Certificate Issuer

The server certificate received during the PEAP or TTLS message exchange must have been issued by this certificate authority. Trusted intermediate certificate authorities and root authorities whose certificates exist in the system store will be available for selection in the drop-down list box. If Any Trusted CA is selected, any CA in the list will be acceptable.

- **Allow intermediate certificates:** The server certificate received during negotiation may have been issued directly by the certificate authority indicated in the "Certificate issuer" field, or additionally by one of its intermediate certificate authorities. Check this box to allow a number of unspecified certificates to be in the server certificate chain between the server certificate and the specified CA. If unchecked, then the specified CA must have directly issued the server certificate.

Server/Certificate Name

Check this option if you want to specify your server/certificate name.

The server name, or a domain to which the server belongs, depending on which of the two options below has been selected.

- **Server name must match exactly:** When selected, the server name entered must match exactly the server name found on the certificate. The server name should include the complete domain name (e.g., Servername.Domain name) in this field.
- **Domain name must end in specified name:** When selected, the server name field identifies a domain, and the certificate must have a server name belonging to this domain or to one of its sub-domains (e.g., zeelans.com, where the server is blueberry.zeelans.com)

Note: These parameters should be obtained from the system

administrator.

15. To save your settings, click **OK**.

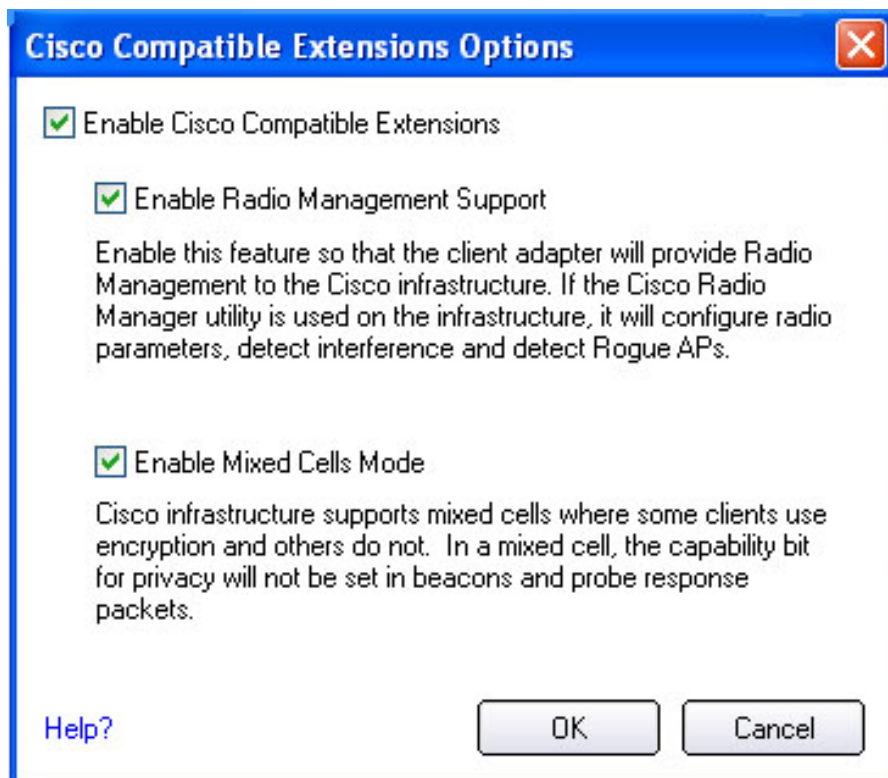
Configuring a CCX Client with CKIP Encryption and LEAP Authentication

Configuring [LEAP](#) using Intel PROSet/Wireless Assistant

An Intel PROSet Wireless CCX (v2.0) profile must be configured to connect to a specific ESS or Wireless LAN network. The profiles settings include LEAP and CKIP with automatic Rogue AP detection.

To configure a profile for CCX security settings:

1. On the Intel PROSet/Wireless main window, click **Add**. The General Settings window opens.
2. Enter the profile and network (SSID) name.
3. For the operating mode, select **Network [Infrastructure]**.
4. Click **Next**. The Security Settings window opens.
5. For Network Authentication, select **Open**.
6. For Data Encryption, select **CKIP**.
7. Click **Enable 802.1x**.
8. For Authentication Type, select **LEAP**.
9. Click **CCX Options**. The Cisco Compatible Extensions Options window opens.



10. Select the following options:

- Click the **Cisco Compatible Extensions** check box to enable CCX security.
- Click **Enable Radio Management Support**: Select this option for Cisco access point compatibility.
- Click **Mixed Cells**: Use this option to avoid collision in the 11b/11g mixed environment.

11. Click **OK**.

Under **LEAP User**, your user name is displayed in the User Name text box. The domain name is also displayed in the Domain text box (default setting).

12. In the Password text box, enter your **Windows login password**.

13. In the Confirm Password text box, re-enter the **password**. This password is your user account created on the authentication server. The user name and password do not have to be the same as name and password of your current Windows user login. **NOTE:** You can also select **Prompt for the user name and password**, which will allow you to enter your user name when you connect to the network.

14. Click **Allow for fast roaming (CCKM)** to enable this feature. The Security settings are shown in the following illustration:

Create Wireless Profile

Profile Name: FFF

General Settings

Security Settings

LEAP User

Security Settings

Select the appropriate security settings for your wireless network. Your network administrator can help with these settings.

Network Authentication: Open

Data Encryption: CKIP

☒ Enable 802.1x

Authentication Type: LEAP Cisco Options...

LEAP User

☐ Prompt for the user name and password

☒ Use the following user name and password:

User Name: Tony Lukyn

Domain: TL

Password:

Confirm Password:

☒ Allow Fast Roaming (CCKM)

[Help?](#) << Back Next >> OK Cancel

15. To save the settings and close the Security Settings page, click **OK**. The Intel PROSet/Wireless main window opens to display the profile at the bottom of the Profiles list. Use the profile list arrows to position the profile in the list. If the profile is positioned at the top of the list, it will automatically be connected to the network the next time the wireless network is detected.
16. To connect to the appropriate CCX enabled wireless network access point using the CCX Profile, select the profile and click **Connect**. The connection icon indicates that you are connected to the network. The network name, speed, and signal quality display the current connection status.
17. To display information about the current network connection, click **Details**.

For more information about connection status, refer to [Viewing the Status of Your Wireless Connection](#).

Security Settings for LEAP

Name	Description
Use the Windows logon user name and password	Selecting this feature, the user credentials are retrieved from the Windows Logon process. Note: This option is only available if you have the Single sign On Pre-Login Connection component installed.
Prompt for the user name and password	Selecting this feature, prompts for user name and password before you connect to the wireless network. The user name and password must be first set in the authentication server by the IT administrator.
Use the following user name and password:	The user name and password must be first set in the authentication server by the IT administrator. User Name: This user name must match the user name that is set in the authentication server. Domain: Optionally enter the name of the domain. Password: This password must match the password that is set in the authentication server. The entered password characters display as asterisks. Confirm Password: Re-enter the user password.
Allow Fast Roaming (CCKM)	Click Allow Fast Roaming (Cisco Centralized Key Management (CCKM)) to enable the client wireless adapter for fast secure roaming. When a wireless LAN is configured for fast reconnection, a LEAP enabled client device can roam from one access point to another without involving the main server. Using Cisco Centralized Key Management (CCKM), an access point configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client without perceptible delay in voice or other time-sensitive applications.

CCX Access Point and Client Configurations

The access point provides settings to select different authentication types depending on the wireless network environment. The client sends an Authentication algorithm field during the 802.11 authentication handshake that takes place between the client and the AP during connection establishment. The Authentication algorithm values recognized by a CCX enabled AP is different for the different authentication types. For instance "Network-EAP" which denotes LEAP has a value of 0x80 while "Open" which is the 802.11 specified Open authentication and

“Required EAP” which requires an EAP handshake exchange have values of 0x0.

Network-EAP only

AP: For CCX enabled networks using LEAP authentication only the authentication type is set with “Network-EAP” checkbox selected, and “Open” and “Required EAP” boxes unchecked. The AP is then configured to allow LEAP clients ONLY to authenticate and connect. In this case, the AP expects the 802.11 authentication algorithm to be set to 0x80 (LEAP), and rejects clients that attempt authentication with an Authentication algorithm value 0x0.

Client: In this case the client needs to send out an authentication algorithm value of 0x80 else the 802.11 authentication handshake would fail. During boot, when the Wireless LAN driver is already loaded, but the Intel PROSet Wireless supplicant is still unloaded, the client sends 802.11 authentication with an Authentication algorithm value of 0x0. Once the Intel PROSet Wireless supplicant loads, and engages the LEAP profile, it sends 802.11 authentication with an Authentication algorithm value of 0x80. However, the supplicant sends out 0x80 only if the Rogue AP box is checked.

Network-EAP, Open and Required EAP

AP: If Network-EAP, Open and Required EAP boxes are checked then it would accept both types of 802.11 authentication algorithm values 0x0 and 0x80. However, once the client is associated and authenticated the AP expects an EAP handshake to take place. For any reason if the EAP handshake does not take place quickly, the AP would not respond to the client for about 60 seconds.

Client: Here the client could send out an authentication algorithm value of 0x80 or 0x0. Both values are acceptable and the 802.11 authentication handshake would succeed. During boot, when the Wireless LAN driver is already loaded and the client sends 802.11 authentication with an Authentication algorithm value of 0x0. This is sufficient to get authenticated but the corresponding EAP or LEAP credentials need to be communicated to the AP to establish a connection.

Open and Required EAP only

AP: In the case where the AP is configured with Network-EAP unchecked, but Open and Required EAP checked, the AP will reject any client attempting to 802.11 authenticate using an authentication algorithm value of 0x80. The AP would accept any client using an authentication algorithm value of 0x0, and expects EAP handshake to commence soon after. In this case, the client uses MD5, TLS, LEAP or any other appropriate EAP method suitable for the specific network configuration.

Client: The client in this case is required to send out an authentication algorithm value of 0x0. As mentioned before the sequence involves a repeat of the initial 802.11 authentication handshake.

First, the Wireless LAN driver initiates authentication with a value of 0x0 and later the supplicant would repeat the process. However, the authentication algorithm value used by the supplicant depends on the status of the Rogue AP checkbox. **When the Rogue AP box is unchecked**, the client sends an 802.11 authentication with **Authentication algorithm value of 0x0** even after the supplicant loads and engages the LEAP profile.

Some non-Intel clients, for example, when set to LEAP, cannot authenticate in this case. However, the Intel Wireless LAN client can authenticate, if the Rogue AP is unchecked.

Rogue AP Checkbox configuration

When the checkbox is checked it ensures that the client implements the Rogue AP feature as required by CCX. The client makes note of APs that it failed to authenticate with and sends this information to the AP that allows it to authenticate and connect. Also, the supplicant sets the Authentication algorithm type to 0x80 when the Rogue AP box is checked. There may be some network configurations implementing and [Open and Required EAP only](#) as described above. For this setup to work, the client must use an Authentication Algorithm value of 0x0, as opposed to the need to use 0x80 for [Network-EAP only](#) described above. Therefore, the Rogue AP checkbox also enables the client to support Network-EAP only and Open and Required EAP only.

Note: Please refer to Cisco Client extensions version 2.0 document available at www.cisco.com for more details.

System Administrator Tasks (Obtain a Certificate)

Important: The following information is intended for system administrators.

How to Obtain a Client Certificate

If you do not have any certificates for EAP-TLS, or EAP-TTLS you must get a client certificate to allow authentication. For Enterprise customers, typically you need to consult your system network administrator for instructions about how to obtain a certificate on your network. Certificates can be managed from Internet Settings, accessed from either Internet Explorer or the Windows Control Panel. Use the "Content" page of "Internet Settings."

Windows XP and 2000 - When obtaining a client certificate, do not enable strong private key protection. If you enable strong private key protection for a certificate, you will need to enter an access password for the certificate each time this certificate is used. You must disable strong private key protection for the certificate if you are configuring the service for TLS/TTLS authentication. Otherwise the 802.1x service will fail authentication because there is no logged on

user to whom it can display the prompt window.

Notes about Smart Cards

After installing a Smart Card, the certificate is automatically installed on your computer and can be select from the personal certificate store and root certificate store.

Setting up the Client for TLS and TTLS authentication

The information in this section is intended for system administrators. For enterprise customers, contact your system administrator to obtain a client certificate for TLS/TTLS authentication. While obtaining a certificate for TLS/TTLS authentication, ensure strong private key protection is disabled. This is required for 802.1x authentication. EAP-TLS and EAP-TTLS authentication require client certificates in the local repository for the logged in users account and a trusted CA certificate in the root store. Certificates can be obtained from a corporate certificate authority located on a Windows 2000 Server, or, using Internet Explorer's certificate import wizard.

Step 1: Obtain a certificate from a Windows 2000 Server

1. Launch Internet Explorer and browse to the Certificate Authority (CA) HTTP Service. (Use a URL such as <http://myCA.myDomain.com/certsrv>).
2. Logon to the CA Authority with the username and password of the user account created on the authentication server. This username and password are not necessarily the same as your Windows username and password.
3. On the Welcome page, select **request a certificate task** and submit the form.
4. On the Choose request page, select **Advanced** request and click Next.
5. On the Advanced Requests page, select **Submit a certificate request to this CA using a form** and click **Next**.
6. On the Advanced Requests page, choose the **user certificate template**. Select **Mark keys** as exportable and click **Next**.
7. On the Certificate Issued page, select **Install this certificate**. If this is the first certificate you have installed, you will prompted install a trusted CA certificate in the root store. Click **Yes** as you will need this certificate for TLS and TTLS authentication.
8. If you certificate was correctly installed, you will see the message: Your new certificate has been successfully installed.
9. To verify the installation, click **Internet explorer > Tools > Internet Options > Content > Certificates**. The new certificate should be installed in the personal folder.

Importing a certificate from a file

1. Open **Internet Properties** (right-click on the Internet Explorer icon on the desktop and select Properties).
2. Click the **Certificates** button on the Content page. This will open the list of installed

certificates.

3. Click the **Import** button under the list of certificates. This will start the Certificate Import Wizard. (**Note:** Steps 1 through 3 may also be accomplished by double-clicking the icon for the certificate).
4. Select the file and proceed to the Password page.
5. On the Password page specify your access password for the file. Clear the **Enable strong private key protection** option.
6. On the Certificate store page select **Automatically select certificate store based on the type of certificate** (the certificate must be in the User accounts Personal store to be accessible in the Configure window of the Client; this will happen if 'automatic' is selected).
7. Proceed to 'Completing the Certificate Import' and click **Finish**.

Step 2: Specifying the certificate used by Intel PROSet Wireless

To create a profile using Shared Network authentication, WEP encryption, and TLS 802.1x authentication:

1. Obtain and install a client certificate, refer to **Step 1 Obtain a Certificate** or consult your system administrator.
2. Click the **Add** button.

General Settings

3. Enter the profile and network (SSID) name.
4. Select Network [Infrastructure] for the operating mode.
5. Click **Next**.

Security Settings

6. Select **Shared** in the Network Authentication options.
7. Select **WEP** as the Data encryption.
8. Click the **Enable 802.1x** checkbox to enable the 802.1x security option.
9. Select **TLS** as the 802.1x Authentication Type.

Step 1 of 3: WEP Key

10. Select either **64-bit** or **128-bit** for the Encryption Level.
11. Select the encryption Key index **1, 2, 3** or **4**.
12. Enter the Wireless Security Password (WEP Key):
 - **Use pass phrase:** Click Use Pass Phrase to enable. Enter a text phrase using 8-63 alphanumeric characters (0-9, a-z or A-Z), in the pass phrase field.
 - **Use hex Key:** Click Use hex Key to enable. Enter up to 64 alphanumeric characters,

0-9, A-F in the hex key field.

13. Click **TLS User** in the left side panel to display the TLS user settings.

Step 2 of 3: TLS User

14. Select either:

- **Use my smart card.** Insert your Smart Card when you log on to your computer using this profile.
- **Use a certificate on this computer:** Your user name should be displayed in the User Name text box. Click the **Select** button to open a list of installed certificates. Select a certificate from the list. This option selects a client certificate from the Personal certificate store of the Windows logged-in user. This certificate will be used for client authentication. Click the **Select** button to open a list of installed certificates. Click **OK** to close the window.

Note about Certificates: The specified identity should match the field "Issued to" in the certificate and should be registered on the authentication server (i.e., RADIUS server) that is used by the authenticator. Your certificate must be "valid" with respect to the authentication server. This requirement depends on the authentication server and generally means that the authentication server must know the issuer of your certificate as a Certificate Authority. You should be logged in using the same username you used when the certificate was installed. See [Step 1](#) for more information.

15. Click **TLS Server** in the left side panel to display the TLS server settings.

Step 3 of 3: TLS Server

16. Select from the Certificate Issuer list **Any Trusted CA** as the default.
17. Select the **Allow intermediate certificates** checkbox to allow a number of unspecified certificates to be in the server certificate chain between the server certificate and the specified CA. If unchecked, then the specified CA must have directly issued the server certificate
18. **Enter the Server/Certificate name.** If you know the server name enter this name. Select the appropriate option to match the server name exactly or specify the domain name. The options are **Server Name must match exactly** or **Domain name must end in the specified name**.
19. Click **OK** to save the settings and close the Security Settings page.
20. The profile displays in the profile list and is positioned at the bottom of the list. Use the profile list arrows to position the profile in the list. If the profile is positioned at the top of the list, it will automatically be connected to the network the next time the wireless network is detected.

21. Select the profile and click **Connect** to connect to the wireless network. The connection icon indicates that you are connected to the network. The network name, speed, and signal quality display the current connection status. Click the **Details** button to display details of the current network connection.
-

[Back to Top](#)

[Back to Contents](#)

[Back to Contents](#)

Specifications: Intel PROSet/Wireless Network Connection

Specifications: Intel PROSet/Wireless 2915ABG Network Connection

Form Factor	Mini PCI Type 3A	
Dimensions	Width 2.85 in x Length 1.75 in x Height 0.20 in (59.75 mm x 50.95 mm x 5 mm)	
Weight	0.7 oz. (12.90 g.)	
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066	
Dual Diversity Antenna	On-board dual diversity switching	
Connector Interface	124-pin SO-DIMM edge connector	
Voltage	3.3 Volt	
Operating Temperature	0 to +70 degrees Celsius	
Humidity	50 to 85% non-condensing	
Frequency Modulation	5 GHz (802.11a)	2.4 GHz (802.11b/g)
Frequency band	5.15 GHz to 5.85 GHz	2.400 - 2.472 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Medium	5 GHz UNII: Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz ISM: Orthogonal Frequency Division Multiplexing (OFDM)

Channels	4 to 12 non-overlapping, dependent on country	Channel 1-11 (US only) Channel 1-13 (Japan, Europe)
Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	11, 5.5, 2, 1 Mbps
General		
Operating Systems	Windows XP, Windows 2000	
Wi-Fi® Alliance certification	Wi-Fi® certification for 802.11b, 802.11g, 802.11a	
WLAN Standard	IEEE 802.11g, 802.11b, 802.11a	
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes	
Security	WPA, WPA-Enterprise, AES 128-bit, WEP 128-bit and 64-bit.Cisco Compatible Extensions v2.0, 802.1x: LEAP, PEAP, TKIP, EAP-TLS, EAP-TTLS, MD5	
Product Safety	UL, C-UL, CB (IEC 60590)	

Specifications: Intel PROSet/Wireless 2200BG Network Connection

Form Factor	Mini PCI Type 3A
Dimensions	Width 2.85 in x Length 1.75 in x Height 0.20 in (59.75 mm x 50.95 mm x 5 mm)
Weight	0.7 oz. (12.90 g.)
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066
Dual Diversity Antenna	On-board dual diversity switching
Connector Interface	124-pin SO-DIMM edge connector
Voltage	3.3 Volt
Operating Temperature	0 to +80 degrees Celsius

Humidity	50 to 85% non-condensing	
2.4 GHz Band (802.11b/g	Most of the World (United States)	Rest of World (Europe, Japan)
Frequency ranges	2.412 - 2.462 GHz	2.412 - 2.472 GHz
Channels	1 - 11 (active scan)	1 - 13 (active scan)
Modulation	CCK, DQPSK, DBPSK, BPSK, QPSK, 16 QAM, 64 QAM	
Wireless Medium	2.4 GHz ISM: Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM)	
Data Rates	54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbps	
General		
Operating Systems	Windows XP, 2000	
Wi-Fi® Alliance certification	Wi-Fi® certification for 802.11b, 802.11g, 802.11a	
WLAN Standard	IEEE 802.11g, 802.11b, 802.11a	
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes	
Security	WPA, WPA-Enterprise, AES 128-bit, WEP 128-bit and 64-bit.Cisco Compatible Extensions v2.0, 802.1x	
Product Safety	UL, C-UL, CB (IEC 60590)	

[Back to Top](#)

[Back to Contents](#)

[Back to Contents](#)

Regulatory Information: Intel PRO/Wireless 2915ABG Network Connection User's Guide

[Information For the User](#)
[Regulatory Information](#)

Information for the user

Safety Notices

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. The Intel PRO/Wireless 2915ABG Adapter meets the Human Exposure limits found in OET Bulletin 65, 2001, and ANSI/IEEE C95.1, 1992. Proper operation of this radio according to the instructions found in this manual will result in exposure substantially below the FCC's recommended limits.

The following safety precautions should be observed:

- Do not touch or move antenna while the unit is transmitting or receiving.
- Do not hold any component containing the radio such that the antenna is very close or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; if not, the radio may be damaged.
- Use in specific environments:
 - The use of wireless devices in hazardous locations is limited by the constraints posed by the safety directors of such environments.
 - The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).
 - The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.

- Explosive Device Proximity Warning (see below)
- Antenna Warning (see below)
- Use on Aircraft Caution (see below)
- Other Wireless Devices (see below)
- Power Supply (Access Point) (see below)

Explosive Device Proximity Warning

 **Warning:** Do not operate a portable transmitter (such as a wireless network device) near unshielded blasting caps or in an explosive environment unless the device has been modified to be qualified for such use.

Antenna Warnings

 **Warning:** To comply with the FCC and ANSI C95.1 RF exposure limits, it is recommended for the Intel PRO/Wireless 2915ABG Adapter installed in a desktop or portable computer, that the antenna for this device be installed so as to provide a separation distance of at least 20 cm (8 inches) from all persons and that the antenna must not be co-located or operating in conjunction with any other antenna or radio transmitter. It is recommended that the user limit exposure time if the antenna is positioned closer than 20 cm (8 inches).

 **Warning:** The Intel PRO/Wireless 2915ABG Adapter product is not designed for use with high-gain directional antennas. Use of such antennas with these products is illegal.

Use On Aircraft Caution

 **Caution:** Regulations of the FCC and FAA prohibit airborne operation of radio-frequency wireless devices because their signals could interfere with critical aircraft instruments.

Local Restrictions on 802.11b Radio Usage

 **Caution:** Because the frequency used by 802.11b wireless LAN devices may not yet be harmonized in all countries, 802.11b products are designed for use only in specific countries and are not allowed to be operated in countries other than those so designated. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are

configured with the correct selection of frequency and channel for the country of use. Any deviation from the permissible settings for the country of use is an infringement of national law and may be punished as such.

For country-specific information, please see the additional compliance information supplied with this product.

Wireless interoperability

The Intel PRO/Wireless 2915ABG Adapter is designed to be interoperable with any wireless LAN product that is based on direct sequence spread spectrum (DSSS) radio technology and to comply with the following standards:

- IEEE Std. 802.11b-1999. Standard on Wireless LAN.
- IEEE Std. 802.11g compliant. Standard on Wireless LAN.
- Wireless Fidelity (WiFi(R)) certification, as defined by the WECA (Wireless Ethernet Compatibility Alliance).

The Intel(R) PRO/Wireless LAN 2200 3A Mini PCI adapter and your health

The Intel PRO/Wireless 2915ABG Adapter, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by this device, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The Intel PRO/Wireless 2915ABG Adapter wireless device operates within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of the Intel PRO/Wireless 2915ABG Adapter wireless device may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations include the following:

- Using the Intel PRO/Wireless 2915ABG Adapter equipment on board airplanes, or
- Using the Intel PRO/Wireless 2915ABG Adapter equipment in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful.

If you are uncertain of the policy that applies to the use of wireless devices in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the Intel PRO/Wireless 2915ABG Adapter wireless device before

you turn it on.

Regulatory information

The Intel PRO/Wireless 2915ABG Adapter wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. For country-specific approvals, see [Radio approvals](#). Dell Inc. is not responsible for any radio or television interference caused by unauthorized modification of the devices included with the Intel PRO/Wireless 2915ABG Adapter kit, or the substitution or attachment of connecting cables and equipment other than that specified by Dell Inc. The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user. Dell Inc. and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from the user failing to comply with these guidelines.

NOTE—Your Intel PRO/Wireless 2915ABG Adapter transmits less than 100 mW, but more than 10 mW.

USA—Federal Communications Commission (FCC)

This device complies with Part 15 of the FCC Rules. Operation of the device is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference that may cause undesired operation.

NOTE—The radiated output power of the Intel PRO/Wireless 2915ABG Adapter wireless network device is far below the FCC radio frequency exposure limits. Nevertheless, the Intel PRO/Wireless 2915ABG Adapter device should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, you should keep a distance of at least 20 cm between you (or any other person in the vicinity) and the antenna that is built into the computer. To determine the location of the antenna within your computer, check the information posted on the general Dell support site at <http://www.support.dell.com>.

Interference statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If the equipment is not installed and used in accordance with the instructions, the equipment may cause harmful interference to radio communications. There is no guarantee, however, that such interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception (which can be determined by turning the equipment off and on), the user is encouraged to try to correct the interference by taking one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

NOTE—The Intel PRO/Wireless 2915ABG Adapter wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Any other installation or use will violate FCC Part 15 regulations.

U.S. Frequency Bands

2.400 - 2.473 GHz

Canada—Industry Canada (IC)

This Class B digital apparatus complies with Canadian ICES-003, Issue 2, and RSS-210, Issue 4 (Dec. 2000).

Cet appareil numérique de la classe B est conforme à la norme NMB-003, No. 2, et CNR-210, No 4 (Dec 2000).

"To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing."

« Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé à l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence. »

Europe—EU Declaration of Conformity

Europe Frequency Bands

2.400 - 2.4835 GHz (Europe ETSI)

The lower band of 5.15 -- 5.25 GHz should be operated only outdoors.

This equipment complies with the essential requirements of the European Union directive 1999/5/EC.

Cet équipement est conforme aux principales exigences essentielles définies dans la Directive européenne RTTE 1999/5/CE.

Die Geräte erfüllen die grundlegenden Anforderungen der RTTE-Richtlinie 1999/5/EG.

Questa apparecchiatura è conforme ai requisiti essenziali della Direttiva Europea R&TTE 1999/5/CE.

Este equipo cumple los requisitos principales de la Directiva 1999/5/CE de la UE, "Equipos de Terminales de Radio y Telecomunicaciones".

Este equipamento cumpre os requisitos essenciais da Directiva 1999/5/CE do Parlamento Europeu e do Conselho (Directiva RTT).

O exoplismos autos plhroi tis basikes apaits ths koinotikhs odhgias EU R&TTE 1999/5/E.

Deze apparatuur voldoet aan de noodzakelijke vereisten van EU-richtlijn betreffende radioapparatuur en telecommunicatie-eindapparatuur 1999/5/EG.

Dette udstyr opfylder de Væsentlige krav i EU's direktiv 1999/5/EC om Radio- og teleterminaludstyr.

Dette utstyret er i overensstemmelse med hovedkravene i R&TTE-direktivet (1999/5/EC) fra EU.

Utrustningen uppfyller kraven för EU-direktivet 1999/5/EC om ansluten teleutrustning och ömsesidigt erkännande av utrustningens överensstämmelse (R&TTE).

Tämä laite vastaa EU:n radio- ja telepäätelaitedirektiivin (EU R&TTE Directive 1999/5/EC) vaatimuksia.

France

Some areas of France have a restricted frequency band. The worst case maximum authorized power indoors is:

- 10 mW for the entire 2.4 GHz band (2400 MHz–2483.5 MHz)
- 100 mW for frequencies between 2446.5 MHz and 2483.5 MHz (NOTE—Channels

10 through 13 inclusive operate in the band 2446.6 MHz to 2483.5 MHz)

There are few possibilities for outdoor use: On private property or on the private property of public persons, use is subject to a preliminary authorization procedure by the Ministry of Defense, with maximum authorized power of 100 mW in the 2446.5–2483.5 MHz band. Use outdoors on public property is not permitted. In the departments listed below, for the entire 2.4 GHz band:

- Maximum authorized power indoors is 100 mW
- Maximum authorized power outdoors is 10 mW

There is partial restriction of the 2.4 GHz band for outdoor/indoor in part of the 2.4 GHz band, according to the OEM Regulatory and Safety Notice Guidelines of CX2 2200BG (see page 12, concerning France).

Departments in which the use of the 2400–2483.5 MHz band is permitted with an EIRP of less than 100 mW indoors and less than 10 mW outdoors:

01 Ain Orientales	36 Indre	66 Pyrénées
02 Aisne	37 Indre et Loire	67 Bas Rhin
03 Allier	41 Loir et Cher	68 Haut Rhin
05 Hautes Alpes	42 Loire	70 Haute Saône
08 Ardennes	45 Loiret	71 Saône et Loire
09 Ariège	50 Manche	75 Paris
11 Aude	55 Meuse	82 Tarn et Garonne
12 Aveyron	58 Nièvre	84 Vaucluse
16 Charente	59 Nord	88 Vosges
24 Dordogne	60 Oise	89 Yonne
25 Doubs	61 Orne	90 Territoire de Belfort
26 Drôme	63 Puy du Dôme	94 Val de Marne
32 Gers	64 Pyrénées Atlantique	

This requirement is likely to change over time, allowing the use your wireless LAN card in more areas within France. Please check with ART for the latest information (www.art-telecom.co.fr)

Belgique

Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

Italia

For use in private premises: no restriction outdoor or indoor, 2.400 - 2.4835 Ghz

For use in public premises: no restriction outdoor or indoor, 2.400 - 2.4835 Ghz, but a general authorization has to be requested to the ministry of Post and telecommunications.

Japan Frequency Bands

2.400 - 2.497 GHz (Japan)

Radio approvals

To determine whether you are allowed to use your wireless network device in a specific country, please check to see if the radio type number that is printed on the identification label of your device is listed on the radio approval list posted on the general Dell support site at <http://support.dell.com>.

[Back to Top](#)

[Back to Contents](#)

[Back to Contents](#)

Intel Wireless Troubleshooter (Tools menu)

[Resolving Errors](#)

Intel Wireless Troubleshooter

Intel Wireless Troubleshooter is an application that can assist you in resolving wireless network connection issues. When a connection issue is detected, a balloon tip appears at the bottom right of your desktop screen. When you click the balloon tip, a diagnostic page displays the recommended steps to resolve the connection issue. For example, if a connection issue occurred because of an invalid password, the Profile Wizard application is launched when you click the displayed hyperlink. You can also launch [Wireless Event Viewer](#) from this page and enable or disable alert notifications.

Intel Wireless Troubleshooter Page Description

The Intel Wireless Troubleshooter page contains two panes. The left pane displays a list of available tools that can be started using your left mouse button. The right pane displays the current connection issue in a section. Each section has two parts: the error message and the hint text. The error message and time stamp are preceded by an icon. The hint text contains a description of available utilities and help for resolving the associated connection issue. If you click a help text link, the help text is displayed in a pop-up window. If you click the associated issue resolver link, a program is launched to resolve the connection issue. You can launch [Wireless Event Viewer](#) or enable or disable the error notification.

File **Exit:** Exit Intel Wireless Troubleshooter application.

Help **Intel Wireless Troubleshooter Help:**
Displays online help about the Intel Wireless Troubleshooter.

About: Displays version information for the Intel Wireless Troubleshooter.

Wireless Event Viewer Launch Wireless Event Viewer.

Disable Notification Click to disable the alert notifications.

Enable Notification Click to enable the alert notifications if an error is detected.

Available Help Date Time error message:

- Description of error.
- Link to resolve error (if available). See [Resolving Errors](#).
- Link to recommended steps to resolve error.

Resolving Errors

Use the following recommendations to resolve network connection issues detected by Intel Wireless Troubleshooter.

[Authentication failed due to invalid user credentials](#)

[Authentication failed due to invalid username](#)

[Authentication failed due to invalid user password](#)

[Authentication failed due to an invalid server certificate](#)

[Authentication failed due to invalid server credentials](#)

[Authentication failed due to invalid server identity](#)

[Authentication failed due to an invalid user certificate](#)

[Incorrect PIN for retrieving certificate](#)

[Authentication failed because the AAA server is unavailable](#)

[Wireless adapter failed to get a valid IP address](#)

[Authentication failed because timer expired](#)

[Smart Card was unexpectedly removed](#)

[Disconnection from an Access Point](#)

[AAA Server Rejected the EAP Method](#)

[Error Occurred Because the GSM Adapter Was Unexpectedly Removed](#)

[Administrator Profile Failed to Authenticate](#)

[IT Administrator Profile Failed to Obtain an IP Address from the DHCP Server](#)

Authentication failed due to invalid user credentials – Re-enter credentials

This authentication error can be caused by invalid user credentials when using either a [TTLS](#) or [PEAP](#) profile.

Use the following steps to help resolve this error:

1. From the profiles list, select a TTLS or PEAP profile.
2. Click **Properties**.
3. Click **Next**.

4. For the [802.1x](#) Authentication Type, select **TTLS** or **PEAP**.
 5. For User Credentials, select **Use the following**.
 6. Verify the User Name, Domain, and password information.
 - If **Use Windows logon** or **Prompt each time I connect** is selected, make sure that the correct user credentials information is used when you connect to the wireless network. **Note:** This option is only available if you have the Single Sign On Pre-Login Connection component installed.
 7. To save the settings, click **OK**.
-

Authentication failed due to invalid username – Re-enter username

This authentication error can be caused by an invalid user name when using either a [TTLS](#), [PEAP](#) or [LEAP](#) profile.

Use the following steps to help resolve this error:

1. Select the appropriate profile from the Profiles list.
 2. Click **Properties**.
 3. Click **Next**.
 4. Select the appropriate [802.1x](#) Authentication Type.
 - For TTLS and PEAP profiles: Select **Use the following** for User Credentials.
 - Verify the User Name information.
 - If **Use Windows logon** or **Prompt each time I connect** is selected, make sure that the correct user credentials information is used when you connect to the wireless network. **Note:** This option is only available if you have the Single Sign On Pre-Login Connection component installed.
 - For LEAP profiles: Select **Use the following user name and password** and verify the user name information. If **Use Windows logon user name and password** or **Prompt for user name and password** is selected, make sure that the correct user credentials information is used when you connect to the wireless network.
 - For [EAP-SIM](#) authentication type: Verify that the correct User Name is being used under **Specify user name (identity)**.
 5. To save the settings, click **OK**.
-

Authentication failed due to invalid user password – Re-enter Password

This authentication error can be caused by an invalid user password when using either a [TTLS](#), [PEAP](#) or [LEAP](#) profile.

Use the following steps to help resolve this error:

1. Select the appropriate profile from the profiles list.
 2. Click **Properties**.
 3. Click **Next**.
 4. Select the appropriate [802.1x](#) Authentication Type.
 - For TTLS and PEAP profiles: Select the **Use the following** option for User Credentials.
 - Re-enter the correct password.
 - If **Use Windows logon** or **Prompt each time I connect** is selected, make sure that the correct user credentials information is used when you connect to the wireless network. **Note:** This option is only available if you have the Single Sign On Pre-Login Connection component installed.
 - For LEAP profiles: Select **Use the following user name and password** and re-enter the correct password. If **Use Windows logon user name and password** or **Prompt for user name and password** is selected, make sure that the correct password information is used when you connect to the wireless network.
 5. To save the settings, click **OK**.
-

Authentication failed due to an invalid server certificate – Select another Certificate

This authentication error can be caused by an invalid server certificate when using either a [TLS](#), [TTLS](#), or [PEAP](#) profile.

Use the following steps to help resolve this error:

1. Select the appropriate profile from the profiles list.

2. Click **Properties**.
3. Click **Next**.
4. Select the appropriate [802.1x](#) Authentication Type.
 - For TTLS and PEAP profiles: Verify that the correct Authentication Type is selected from the drop-down list. Click **Use a Client Certificate on this wireless network** and click **Select**. Choose a valid certificate from the list of installed certificates, and then click **OK**.
 - For TLS profiles: Click **Use a Client Certificate on this wireless network** and click **Select**. Choose a valid certificate from the list of installed certificates, and then click **OK**.

Note About Certificates: The specified identity should match the "Issued to" field in the certificate and should be registered on the authentication server (i.e., RADIUS server) that is used by the authenticator. Your certificate must be "valid" with respect to the authentication server. This requirement depends on the authentication server and generally means that the authentication server must know the issuer of your certificate as a Certificate Authority. You should be logged in using the same user name you used when the certificate was installed.

5. Click **Close**.
6. to save the settings, click **OK**.

Authentication failed due to invalid server credentials – Re-enter server credentials

This authentication error can be caused by invalid server (Domain) credentials when using either a [TTLS](#), [PEAP](#), or [LEAP](#) profile.

Use the following steps to help resolve this error:

1. Select the appropriate profile from the profiles list.
2. Click **Properties**.
3. Click **Next**.
4. Select the appropriate [802.1x](#) Authentication Type.
 - For TTLS and PEAP profiles: Select **Use the following** for User Credentials.
 - Verify the Domain information.

- If **Use Windows logon** or **Prompt each time I connect** is selected, make sure that the correct Domain credentials information is used when you connect to the wireless network. **Note:** This option is only available if you have the Single Sign On Pre-Login Connection component installed.
 - For LEAP profiles: Select **Use the following user name and password** and verify the Domain is correct. If **Prompt for user name and password** is selected, make sure that the correct Domain and password information is entered when you connect to the wireless network. (Must match what appears on the Security settings window.)
5. To save the settings, click **OK**.
-

Authentication failed due to invalid server identity – Re-enter server name

This authentication error can be caused by invalid server identity information when using either a [TTLS](#) or [PEAP](#) profile.

Use the following steps to help resolve this error:

1. Select the appropriate profile from the profiles list.
 2. Click **Properties**.
 3. Click **Next**.
 4. Select the appropriate [802.1x](#) Authentication Type.
 5. For TTLS and PEAP profiles: Verify that the Roaming Identity server name is correct.
 6. To save the settings, click **OK**.
-

Authentication failed due to an invalid user certificate – Re-enter user credentials

This authentication error can be caused by an invalid user certificate when using either a [TLS](#), [TTLS](#), or [PEAP](#) profile.

Use the following steps to help resolve this error:

1. Select the appropriate profile from the profiles list.
2. Click **Properties**.
3. Click **Next**.
4. Select the appropriate [802.1x](#) Authentication Type.
 - For TTLS and PEAP profiles: Verify that the correct Authentication Type is selected from the drop-down list, click **Select**, choose a valid certificate from the list of installed certificates, and then click **OK**.
 - For TLS profiles: Click **Select**, choose a valid certificate from the list of installed certificates, and then click **OK**.

Note about Certificates: The specified identity should match the field "Issued to" in the certificate and should be registered on the authentication server (i.e., RADIUS server) that is used by the authenticator. Your certificate must be "valid" with respect to the authentication server. This requirement depends on the authentication server and generally means that the authentication server must know the issuer of your certificate as a Certificate Authority. You should be logged in using the same username you used when the certificate was installed.

5. Click **Close**.
6. To save the settings, click **OK**.

Incorrect PIN for retrieving certificate – Re-enter PIN

Recommended action:

The certificate retrieval failed because of an incorrect PIN. Re-enter the correct PIN.

Authentication failed because the AAA server is unavailable

The wireless adapter is associated to the [access point](#), but the [802.1x](#) authentication cannot be completed because of no response from the authentication server.

Recommended action:

On the Intel PROSet/Wireless main window, select the profile and click **Connect**. This procedure allows you to try to associate with the network and authenticate with the server.

Wireless adapter failed to get a valid IP address

This error can be due to an authentication failure with the network, incorrect encryption keys, or because of a DHCP server malfunction. Re-enter encryption keys.

If it is an encryption key mismatch, use the following steps to resolve this error:

1. Click **Properties**.
2. Click **Next**.
3. Enter the encryption key.
4. To save the security settings for the profile, click **OK**.

If it is a DHCP server issue:

- If using a wireless router, check the DHCP settings in that device.

Authentication failed because timer expired

Authentication failed because timer expires while trying to authenticate a possible rogue access point (AP). The rogue AP timed out, possibly because of a problem with the RADIUS server.

Recommended action:

- To prevent the wireless adapter from connecting with a possible rogue AP, consider adding this rogue AP to the [excluded access point list](#). Then the adapter will no longer try to connect with this AP.
- To try connecting again (if you don't think this is a rogue AP), on the Intel PROSet/Wireless main window, select the profile and click **Connect** and try to associate with the network and authenticate with the server.

Smart Card was unexpectedly removed

This error occurred because the Smart Card was unexpectedly removed.

Recommended action:

1. Insert the Smart Card.
 2. Select the [802.1x](#) EAP-SIM authentication profile.
 3. Click **Connect** and try to associate with the network.
-

Disconnection from an Access Point

The following error messages are displayed when the wireless adapter is disconnected from the network [access point](#).

Disconnect from access point due to failed association.

Disconnect from access point due to authentication failures.

Disconnect from access point due to TKIP [Michael](#) Integrity Check failure.

Disconnect from access point due to Class 2 frame non-authentication failure.

Disconnect from access point due to Class 3 frame non-association failure.

Disconnect from access point due to re-association failure.

Disconnect from access point due to Information Element failure.

Disconnect from access point due to EAPOL-Key protocol 4-way handshake failure.

Disconnect from access point due to [802.1x](#) authentication failure.

Recommended action:

To re-connect, remove the access point from the [exclude list](#) or manually connect (i.e., on the Intel PROSet/Wireless main window, select the profile and click **Connect**).

AAA Server Rejected the EAP Method

This error occurs when the AAA Server does not accept the configured authentication type.

Use the following steps to help resolve this error:

1. Open **Intel PROSet/Wireless** by double-clicking the task tray icon located at the bottom right of the screen.
2. Select the associated or last used profile from the Profiles list.
3. Click **Properties**. The Wireless Profile Properties – General Settings page opens.
4. Click **Next**. The Wireless Profile Properties – Security Settings page is opens.
5. Verify that **Enable [802.1x](#)** is checked.
6. Verify that the correct authentication type is selected.
7. Click **Next** to see Step 2 of the Wireless Profile Properties – Security Settings page.
8. Enter the required information.
9. Click **OK**. The profile is now re-applied. Intel PROSet/Wireless attempts to connect to the wireless network.

Error Occurred Because the GSM Adapter Was Unexpectedly Removed

This error occurs when the GSM adapter is not fully inserted or is unexpectedly removed from the mobile station.

Use the following steps to help resolve this error:

1. Re-insert the GSM adapter.
2. Double-click the **Intel PROSet/Wireless** icon at the bottom right of the screen.
3. Select the associated or last-used profile from the profiles list.
4. Click on **Connect**. The profile is now re-applied. Intel PROSet/Wireless attempts to connect to the wireless network.

An Administrator Profile Failed to Authenticate

This error occurs when the credentials in the profile are not accepted by the authenticator

such as [access point](#) or AAA server.

Note: The Administrator Tool may or may not be installed on your system. For more information about the Administrator Tool, refer to [Administrator Tool](#).

Use the following steps to help resolve this error:

1. Double-click the **Intel PROSet/Wireless** icon at the bottom right of the screen.
2. From the Tools menu, select **Administrator**.
3. Select the appropriate **Administrator Profile** from the profiles list.
4. Click **Properties**. The Wireless Profile Properties – General Settings page appears.
5. Click **Next**. The Wireless Profile Properties – Security Settings page opens.
6. Edit the credentials such as WEP keys and certificates.
7. Click **OK**. The profile is now re-applied. Intel PROSet/Wireless attempts to connect to the wireless network.

IT Administrator Profile Failed to Obtain an IP Address from the DHCP Server

This error can occur due to an authentication failure with the network, incorrect encryption keys, or because of a DHCP server malfunction.

Use the following steps to help resolve this error:

1. Double-click the **Intel PROSet/Wireless** icon at the bottom right of the screen.
2. From the Tools menu, click **IT Administration**.
3. Select the appropriate Administrator Profile from the profiles list.
4. Click **Properties**. The Wireless Profile Properties – General Settings page opens.
5. Click **Next**. The Wireless Profile Properties – Security Settings page is opens.
6. Edit the credentials such as WEP keys and certificates.
7. Click **OK**. The profile is now re-applied. Intel PROSet/Wireless attempts to connect to the wireless network.

Wireless Event Viewer

The Wireless Event Viewer program displays a list of error log records. You can save all

available log records to a binary format file for sending to customer support. To launch Wireless Event Viewer, from the Tools menu, click [Intel Wireless Troubleshooter](#), and then click **Wireless Event Viewer**.

Wireless Event Viewer

Name	Description
File	Preferences: Change the storage location of the log file by selecting Preferences from the File menu. Click to display the Preference page. • The available logs shall be saved to the following folder: The current folder is displayed in the text box. The default location is the desktop. Browse: Specify a new folder location. OK: Close the page and apply the new changes. Cancel: Close the page without applying any changes. Exit: Exit Intel Wireless Troubleshooter.
Level	The severity level of the connection event is indicated by an icon. The severity levels are: • Information • Error • Warning
Description	Brief description of the connection event.
Date and Time	Date and time of the detected connection event. This field can be sorted in ascending or descending order. Click the column header to sort the displayed events.
Save As	Save the available log. You can use the suggested name or change it.
Clear	Removes the information in the Wireless Event Viewer.
Help?	Displays the help information for this page.

Glossary: Intel PRO/Wireless 2915ABG Network Connection User's Guide

Term	Definition
802.11	The 802.11 standard refers to a family of specifications developed by the IEEE for wireless LAN technology. The 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
802.11a	The 802.11a standard specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz. The 802.11a standard uses the Orthogonal Frequency Division Multiplexing (OFDM) transmission method. Additionally, the 802.11a standard supports 802.11 features such as WEP encryption for security.
802.11b	802.11b is an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. Throughput data rate 5+ Mbps in the 2.4 GHz band.
802.11g	The 802.11g standard specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and WEP encryption for security. 802.11g networks are also referred to as Wi-Fi networks.
802.1x	802.1x is the IEEE Standard for Port-Based Network Access Control. This is used in conjunction with EAP methods to provide access control to wired and wireless networks.

Access Point	Access point (AP). A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer and to connect to the Internet.
Ad Hoc network	A communication configuration in which every computer has the same capabilities, and any computer can initiate a communication session. Also known as a peer-to-peer network or a computer-to-computer network.
AES	Advanced Encryption Standard. An additional replacement for WEP encryption.
Available network	One of the networks listed under Available networks on the Wireless Networks tab of the Wireless Configuration Utility (Windows 2000 environment) or Wireless Network Connection Properties (Windows XP environment). Any wireless network that is broadcasting and is within receiving range of the wireless adapter appears on the list.
BER	Bit error rate. The ratio of errors to the total number of bits being sent in a data transmission from one location to another.
Bit Rate	The total number of bits (ones and zeros) per second that a network connection can support. Note that this bit rate will vary, under software control, with different signal path conditions.
Broadcast SSID	Used to allow an access point to respond to clients on a wireless network by sending probes.
BSSID	A unique identifier for each wireless client on a wireless network. The Basic Service Set Identifier (BSSID) is the Ethernet MAC address of each adapter on the network.
CA (certificate authority)	A corporate certification authority implemented on a server. In addition, Internet Explorer's certificate can import a certificate from a file. A trusted CA certificate is stored in the root store.

CCX	Cisco Compatible eXtension. Cisco Compatible Extensions Program ensure that devices used on Cisco wireless LAN infrastructure meet the security, management and roaming requirements.
Certificate	Used for client authentication. A certificate is registered on the authentication server (i.e., RADIUS server) and used by the authenticator.
CKIP	Cisco Key Integrity Protocol (CKIP) is a Cisco proprietary security protocol for encryption in 802.11 media. CKIP uses a key message integrity check and message sequence number to improve 802.11 security in infrastructure mode. CKIP is Cisco's version of TKIP.
Client computer	The computer that gets its Internet connection by sharing either the host computer's connection or the Access Point's connection.
DSSS	Direct Sequence Spread Spectrum. Technology used in radio transmission. Incompatible with FHSS.
EAP	Short for Extensible Authentication Protocol, EAP sits inside of Point-to-Point Protocol's (PPP) authentication protocol and provides a generalized framework for several different authentication methods. EAP is supposed to head off proprietary authentication systems and let everything from passwords to challenge-response tokens and public-key infrastructure certificates all work smoothly.
EAP-FAST	EAP-FAST, like EAP-TTLS and PEAP, uses tunneling to protect traffic. The main difference is that EAP-FAST does not use certificates to authenticate.
EAP-TLS	A type of authentication method using EAP and a security protocol called the Transport Layer Security (TLS). EAP-TLS uses certificates that use passwords. EAP-TLS authentication supports dynamic WEP key management.

EAP-TTLS	A type of authentication method using EAP and Tunneled Transport Layer Security (TTLS). EAP-TTLS uses a combination of certificates and another security method such as passwords.
Encryption	Scrambling data so that only the authorized recipient can read it. Usually a key is needed to interpret the data.
FHSS	Frequency-Hop Spread Spectrum. Technology used in radio transmission. Incompatible with DSSS.
File and printer sharing	A capability that allows a number of people to view, modify, and print the same file(s) from different computers.
Fragmentation threshold	The threshold at which the wireless adapter breaks the packet into multiple frames. This determines the packet size and affects the throughput of the transmission.
GHz	Gigahertz. A unit of frequency equal to 1,000,000,000 cycles per second.
Host computer	The computer that is directly connected to the Internet via a modem or network adapter.
Infrastructure Network	A wireless network centered around an access point. In this environment, the access point not only provides communication with the wired network, but also mediates wireless network traffic in the immediate neighborhood.
IEEE	Institute of Electrical and Electronics Engineers (IEEE) is an organization involved in defining computing and communications standards.
Internet Protocol (IP) address	The address of a computer that is attached to a network. Part of the address designates which network the computer is on, and the other part represents the host identification.
LAN	Local area network. A high-speed, low-error data network covering a relatively small geographic area.

LEAP	Light Extensible Authentication Protocol. A version of Extensible Authentication Protocol (EAP). LEAP is an authentication implementation of 802.1x by Cisco, which provides a challenge-response authentication mechanism and dynamic WEP key assignment.
MAC	A hardwired address applied at the factory. It uniquely identifies network hardware, such as a wireless adapter, on a LAN or WAN.
Mbps	Megabits-per-second. Transmission speed of 1,000,000 bits per second.
MHz	Megahertz. A unit of frequency equal to 1,000,000 cycles per second.
MIC	Message integrity check (commonly called Michael).
MS-CHAP	An EAP mechanism used by the client. Microsoft Challenge Authentication Protocol (MSCHAP) Version 2, is used over an encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel.
ns	Nanosecond. 1 billionth (1/1,000,000,000) of a second.
OFDM	Orthogonal Frequency Division Multiplexing.
PEAP	Protected Extensible Authentication Protocol (PEAP) is an Internet Engineering Task Force (IETF) draft protocol sponsored by Microsoft, Cisco, and RSA Security. PEAP creates an encrypted tunnel similar to the tunnel used in secure web pages (SSL). Inside the encrypted tunnel, a number of other EAP authentication methods can be used to perform client authentication. PEAP requires a TLS certificate on the RADIUS server, but unlike EAP-TLS there is no requirement to have a certificate on the client. PEAP has not been ratified by the IETF. The IETF is currently comparing PEAP and TTLS (Tunneled TLS) to determine an authentication standard for 802.1X authentication in 802.11 wireless systems. PEAP is an authentication type designed to take advantage of

	server-side EAP-Transport Layer Security (EAP-TLS) and to support various authentication methods, including user's passwords and one-time passwords, and Generic Token Cards.
Peer-to-Peer Mode	A wireless network structure that allows wireless clients to communicate with each other without using an access point.
Power Save mode	The state in which the radio is periodically powered down to conserve power. When the notebook is in Power Save mode, receive packets are stored in the AP until the wireless adapter wakes up.
Preferred network	One of the networks that has been configured. Such networks are listed under Preferred networks on the Wireless Networks tab of the Wireless Configuration Utility (Windows 2000 environment) or Wireless Network Connection Properties (Windows XP environment).
RADIUS	Remote Authentication Dial-In User Service (RADIUS) is an authentication and accounting system that verifies users credentials and grants access to requested resources.
RF	Radio Frequency. The international unit for measuring frequency is Hertz (Hz), which is equivalent to the older unit of cycles per second. One Mega-Hertz (MHz) is one million Hertz. One Giga-Hertz (GHz) is one billion Hertz. For reference: the standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 0.55 -1.6 MHz, the FM broadcast radio frequency band is 88-108 MHz, and microwave ovens typically operate at 2.45 GHz.
Roaming	Movement of a wireless node between two micro cells. Roaming usually occurs in infrastructure networks built around multiple access points.
RTS threshold	The number of frames in the data packet at or above which an RTS/CTS (request to send/clear to send) handshake is turned on before the packet is sent. The default value is 2347.

Shared Key	An encryption key known only to the receiver and sender of data.
SIM	Subscriber Identity Module card is used to validate credentials with the network. A SIM card is a special smart card that is used by GSM-based digital cellular networks.
Silent Mode	Silent Mode Access Points or Wireless Routers have been configured to not broadcast the SSID for the wireless network. This makes it necessary to know the SSID in order to configure the wireless profile to connect to the access point or wireless router.
Single Sign On	Single Sign On feature set allows the 802.1x credentials to match your Windows log on user name and password credentials for wireless network connections.
SSID	Service Set Identifier. A value that controls access to a wireless network. The SSID for your wireless network card must match the SSID for any access point that you want to connect with. If the value does not match, you are not granted access to the network. You can have up to three SSIDs. Each SSID can be up to 32 characters long and is case-sensitive.
TKIP	Temporal Key Integrity protocol improves data encryption. Wi-Fi Protected Access utilizes its TKIP. TKIP provides important data encryption enhancements including a re-keying method. TKIP is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.

TLS	Transport Layer Security. A type of authentication method using the Extensible Authentication Protocol (EAP) and a security protocol called the Transport Layer Security (TLS). EAP-TLS uses certificates which use passwords. EAP-TLS authentication supports dynamic WEP key management. The TLS protocol is intended to secure and authenticate communications across a public network through data encryption. The TLS Handshake Protocol allows the server and client to provide mutual authentication and to negotiate an encryption algorithm and cryptographic keys before data is transmitted.
TTLS	Tunneled Transport Layer Security. These settings define the protocol and the credentials used to authenticate a user. In TTLS, the client uses EAP-TLS to validate the server and create a TLS-encrypted channel between the client and server. The client can use another authentication protocol, typically password-based protocols, such as MD5 Challenge over this encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel. TTLS implementations today support all methods defined by EAP, as well as several older methods (CHAP, PAP, MS-CHAP and MS-CHAPv2). TTLS can easily be extended to work with new protocols by defining new attributes to support new protocols.
WEP	Wired Equivalent Privacy. Wired Equivalent Privacy, 64- and 128-bit (64-bit is sometimes referred to as 40-bit). This is a low-level encryption technique designed to give the user about the same amount of privacy that he would expect from a LAN. WEP is a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by data over radio waves so that it is protected as it is transmitted from one end point to another.

Wi-Fi	Wireless Fidelity. Is meant to be used generically when referring of any type to 802.11 network, whether 802.11b, 802.11a, or dual-band.
Wireless Router	A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer and to connect to the Internet. Also known as an access point (AP).
WLAN	Wireless Local-Area Network. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.
WPA-Enterprise and WPA-Personal	Wi-Fi Protected Access. A new standards-based, interoperable security technology for wireless LAN (subset of IEEE 802.11i draft standard) that encrypts data sent over radio waves. WPA is a Wi-Fi standard that was designed to improve upon the security features of WEP which includes two improvements over WEP: 1. Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys have not been tampered with. 2. User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network. WPA is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion.

WPA-PSK

Wi-Fi Protected Access - Pre-Shared Key (WPA-PSK) mode does not use an authentication server. It can be used with the data encryption types: WEP or TKIP. WPA-PSK requires configuration of a pre-shared key (PSK). You must enter a pass phrase or 64 hex characters for a Pre-Shared Key of length 256-bits. The data encryption key is derived from the PSK.

[Back to Top](#)[Back to Contents](#)