

Intel(R) PRO/Wireless 2915ABG Network Connection User 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.

Your Intel(R) PROSet/Wireless 2915ABG Network Connection adapter is compatible with 802.11a, 802.11b or 802.11g wireless standards. Operating at 5 GHz or 2.4 GHz frequency at speeds of up to 54 Mbps you can now connect your computer to existing high-speed networks using multiple access points within large or small environments. Your wireless adapter maintains automatic data rate control according to access point location to achieve the fastest possible connection. provide enhanced security measures using 802.1x network authentication. All of your wireless networks connections can be easily managed by Intel PROSet/Wireless. Intel(R) PRO/Wireless profiles provide enhanced security measures using 802.1x network authentication.



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

Table of Contents

- [Using Intel PROSet/Wireless](#)
- [Using Profiles](#)
- [Setting up Security](#)
- [Security Overview](#)
- [Introduction to Wireless Networking](#)
- [Connecting to a Network](#)
- [Specifications](#)
- [Troubleshooting](#)
- [Glossary](#)
- [Customer Support](#)
- [Safety and Regulatory Information](#)
- [Warranty](#)
- [Adapter Registration](#)

Information in this document is subject to change without notice.

© 2000–2004 Intel Corporation. All rights reserved. Intel Corporation, 5200 N.E. Elam Young Parkway, Hillsboro, OR 97124-6497 USA

The copying or reproducing of any material in this document in any manner whatsoever without the written permission of Intel Corporation is strictly forbidden. Intel(R) is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries. 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. Intel disclaims any proprietary interest in trademarks and trade names other than its own. *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation.

*Other names and brands may be claimed as the property of others.

Intel Corporation assumes no responsibility for errors or omissions in this document. Nor does Intel make any commitment to update the information contained herein.

June 2004

[Back to Contents](#)

Using Intel PROSet/Wireless Software: Intel(R) PRO/Wireless 2915ABG Network Connection User Guide

- [Using Intel\(R\) PROSet/Wireless as your Wireless Manager](#)
 - [Starting Intel PROSet/Wireless](#)
 - [Launch Intel PROSet/Wireless from the task tray](#)
 - [Task Tray Menu Options](#)
 - [Tool Tips and Balloon Message Prompts](#)
 - [Intel PROSet/Wireless Main Window](#)
 - [Connection Status Icons](#)
 - [Connection Details](#)
 - [Profile List](#)
 - [Available Networks](#)
 - [Menus \(Tools and Profile menus\)](#)
 - **Tools Menu**
 - [Application Settings](#)
 - [Adapter Settings](#)
 - [Use Microsoft Client](#)
 - [Advanced Statistics](#)
 - [Intel Wireless Troubleshooter](#)
 - [Administrator Tool](#)
 - **Profiles Menu**
 - [Import/Export](#)
 - [Manage Exclusions](#)
 - [Enabling and Disabling the Radio](#)
 - [Installing and Uninstalling the Software](#)
 - [Installing and Uninstalling Single Sign On Feature](#)
-

Using Intel(R) PROSet/Wireless as your Wireless Manager

Intel PROSet/Wireless can be used to setup, 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 as your wireless manager, you can disable it from the Wireless Network tab. To disable Windows XP as your wireless manager:

1. Double-click the Intel PROSet/Wireless icon in the desktop task tray or click **Start** à **Settings** à **Control Panel** and double-click on **Network Connections**.
2. Right-click **Wireless Network Connection** and click **Properties**.
3. Click on **Wireless Networks** tab on the Wireless Network Connection Properties.
4. Verify that the **Use Windows to configure my wireless network settings** box is not selected. If it is, deselect it.
5. Click **OK**. This confirms that the Intel PROSet/Wireless utility is configured to manage your network profiles.



NOTE: Check that the [Application Settings](#) option **Notify me when another application is using the wireless device** is selected. This option prompts you when Windows XP starts to manage your network profiles.

Starting Intel PROSet/Wireless

Launch Intel PROSet/Wireless either from the task tray icon, the Windows Start button, or from the Windows Control Panel icon.

To launch Intel PROSet/Wireless use either of the following methods:

- Click **Start > Programs > Intel 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**.

Exit Intel PROSet/Wireless:

- To exit Intel PROSet/Wireless and close the task tray icon, click **Exit** from the from the task tray menu or click the **Close** button on the Intel PROSet/Wireless main window.
-

Launch Intel PROSet/Wireless from the task tray

To launch Intel PROSet/Wireless, double-click the task tray icon located in the lower right corner of your Windows desktop or right-click the task tray icon and click **Open Intel PROSet/Wireless**.

Exit Intel PROSet/Wireless

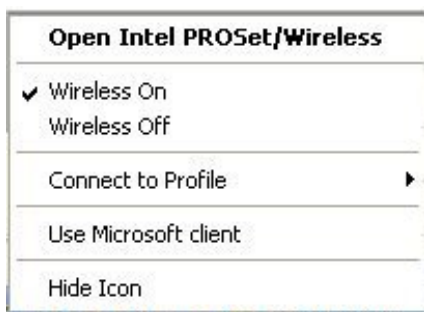
To exit Intel PROSet/Wireless and hide the task tray icon, right-click the task tray icon and click **Hide Icon** on the task tray menu.

- To show the task tray icon after the Intel PROSet/Wireless is launched, select "Show application icon in the taskbar" in the Application Settings options.

Close Intel PROSet/Wireless

- Click **Close** to close the Intel PROSet Wireless main window. To open the main window, right-click the task tray icon and click **Open Intel PROSet/Wireless**.
-

Task Tray Menu Options



The Intel PROSet/Wireless icon displays in the task tray located in the lower right corner of your Windows desktop. Right-click the status icon to display the menu options. Intel PROSet/Wireless can support multiple adapters. These wireless adapters are displayed in the task tray menu options.

Menu Item	Comments
Open Intel PROSet/ Wireless	Double-click this option to launch Intel PROSet/Wireless.
Wireless On	Turn the wireless radio on.
Wireless Off	Toggles the radio off.
Connect to Profile	Displays the current profiles shown in the Profile List. A profile can also be activated.
Use Microsoft client	Toggles between the Intel PROSet/Wireless and Windows XP Wireless Zero Configuration Service. When you use the Microsoft client you cannot use your Intel profiles
Open Intel PROSet/ Wireless	
Hide Icon	Remove Intel PROSet/Wireless icon from the task tray. 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.

Icon	Description
	Wireless off: The wireless adapter is off. The wireless device does not transmit or receive while it is off. Click Wireless on/off to enable the adapter. The icon is white and static.
	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 periodically scans for available networks. If you want to force a scan, double-click the icon to launch Intel PROSet/Wireless and click Refresh . Red icon.
	Wireless network found: An available wireless network is found. Double-click the icon to display the Available Networks listing, select the network, and click Configure . 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.

The green icon with waves reflects 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. It does not reflect connection status. You can still click the icon to open the task tray menu.

Tool Tips and Balloon Message Prompts

The Tool Tips and Balloon message prompts provide feedback and interaction. To display Tool tips, move your mouse pointer over the icon. Balloon messages prompts are displayed when your wireless network changes state. For example, if you are out of range of any wireless networks, when you come into range a balloon prompt is 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.

Tool Tip:

"Connected to a wireless network"

Wireless Network Name: Mynetwork

Speed: 54Mbps

Signal Strength: Very Good



Balloon Prompts

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

Balloon Prompt

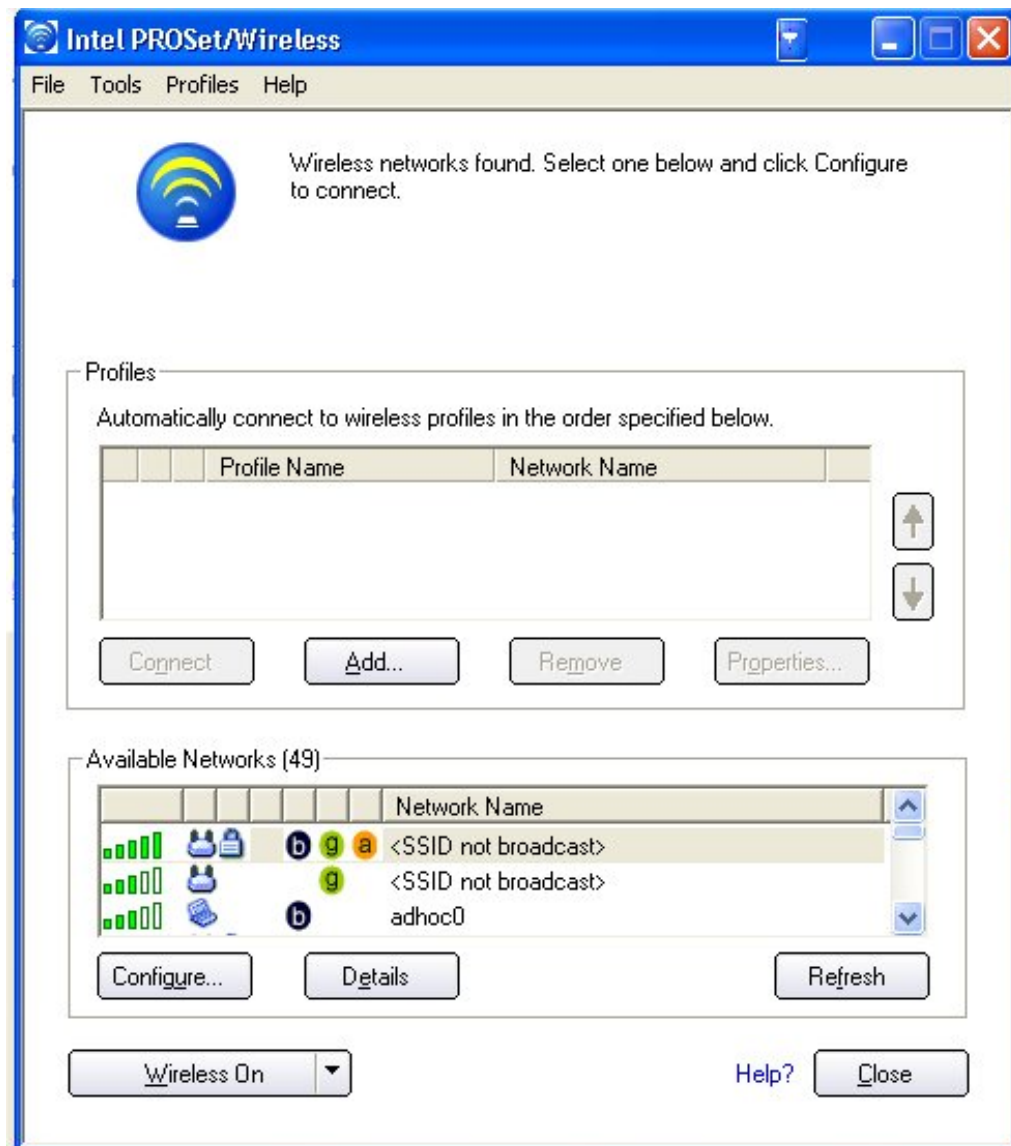
"Wireless network found"

Action: Double-click the Balloon Prompt to connect to the available network.



Intel PROSet/Wireless Main Window

The Intel PROSet/Wireless main window provides basic information about your connection. If you are associated to a network it will contain information such as SSID, profile name, speed, AP settings such as 802.11 band, channel and security mode. The signal quality section of the main windows provides information about the quality of the wireless signal. Click [Details](#) to view detailed parameters of the access point and network adapter.










Use the Intel PROSet/Wireless to:


- View the current connection status (signal quality, speed and current network name)
- Scan for available wireless networks
- Manage profiles
- Auto-connect profiles to available networks in a specific order defined in the Profile list
- Connect to infrastructure and ad hoc networks
- Configure adapter power settings

Connection Status Icons

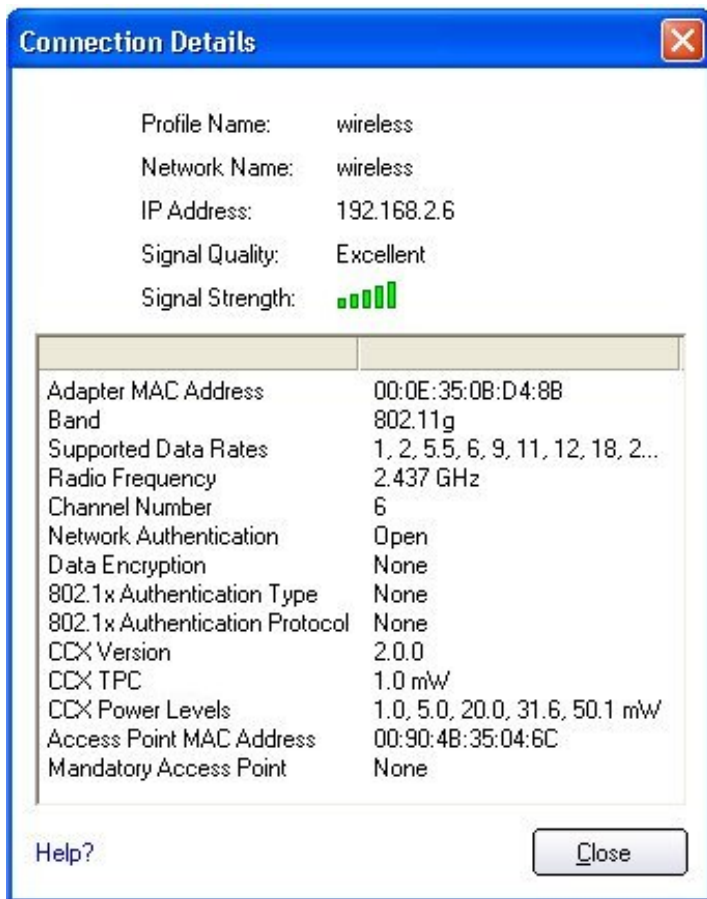
The Intel PROSet/Wireless main window displays connection status icons which indicate the current connection status of your wireless adapter. The task tray icon also indicates the current connection status. Refer to [Task Tray Icons](#) for more information.

Main Window Connection Status Description

Icon	Description
	Wireless turned off: The wireless adapter is not associated to a network. Click the Turn wireless on 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 the Details button 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): <ul style="list-style-type: none">• 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 peer-to-peer mode. The number of vertical green bars indicate the strength of the transmit and receive signals. <p>The signal quality ranges from excellent to out of range. The following factors affect signal quality:</p> <ul style="list-style-type: none">• 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. See Connection Details for information.
Turn wireless off/on	Toggle the radio off and on. Refer to Turn radio On/Off for more information.
Help?	Displays the help information for this page.
Close	Close the Intel PROSet/Wireless main window.
X	Close the Intel PROSet/Wireless main window.

Connection Details



The Connection Details displays the current network connection information.

Network Connection Details page 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	<p>A radio frequency (RF) signal can be assessed by basically two component:</p> <ul style="list-style-type: none"> • strength (quantity) of the signal • the quality of the signal. <p>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 equipments. 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.</p>

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, 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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	Displays the frequency of the current wireless connection. <ul style="list-style-type: none"> • 5.260 Ghz • 2.457 GHz
Channel Number	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	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" if not enabled. If enabled, 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	Close page.
Help?	Displays the help information for this page.

Profile List

A profile is a saved group of network settings. Profiles are useful when moving from one wireless network to another. Different profile can be configured for each wireless network. Profile settings can include, the network name (SSID), operating mode, and security settings.

The Profiles List displays the current user and administrator profiles in the order that they are to be applied. Use the up and down arrows to arrange profiles in a specific order to automatically connect to a wireless network. The [Configuration Service](#) also uses the profiles priority list to connect to wireless networks.








NOTE: [Prelogon/Common](#) or [Persistent](#) profiles are displayed at the top of the Profiles list. These profiles have priority over user based profiles. Prelogon/Common 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.








NOTE: Use the Enable Auto-Import feature to import profiles into the Profile List. Refer to [Automatic Profile Distribution](#) for more information.

Profiles

Name	Description
Profile Name	Profiles are network settings that allow your wireless adapter to connect to a network access point (Infrastructure mode) or computer (peer-to-peer ad hoc mode) which does not use an access point. Refer to Set 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 WEP encryption or 802.1x authentication is enabled.	
	The wireless adapter is associated with an access point or computer (Ad hoc mode). If a profile has 802.1x settings enabled, this indicates that the adapter is associated and authenticated.
	Infrastructure operating mode.
	Ad hoc operating mode.
	The network is using Security encryption.
	The band frequency being used by the wireless network.
Network Name	Name of the wireless network (SSID) or computer.
Arrows	Use the arrows to position profiles in a preferred order for auto-connection. <ul style="list-style-type: none"> • 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	Activate the selected profile and connect to the wireless network.
Add	Create a new profile using the Profile Wizard. Refer to Profile Wizard Overview for more information.
Remove	Delete a selected profile from the Profile List. Not all profiles can be removed from the list, one profile must remain in the list. Refer to Removing a Profile for more information.
Properties	Edit the contents of an existing profile. You can also double-click a profile in the Profile List to edit the profile. Refer to Editing an Existing Profile for more information.

Available Networks

The Available Networks list displays a list of wireless networks within range of the adapter. Click **Connect** 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	Connect to the selected available Network Name.
Properties	The Networks Properties displays the current network connection status for the wireless adapter. Refer to Network Properties for information.
Refresh	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.

Network Properties

This page displays the current connection status for the wireless adapter.

Network Connection Details dialog description

Name	Description
Network Name	Displays the wireless network name.
Band	<p>Band (Frequency): Current band and frequency being used. Displays Out of Range if no band and frequency is displayed. Displays:</p> <ul style="list-style-type: none"> • 802.11b, 802.11g • 802.11a • 802.11b • 802.11g
Operation Mode	Displays the current operating mode, Infrastructure [AP] (default) or Ad hoc.

Authentication Level	<p>Displays the current authentication security mode for the profile being used.</p> <p>Displays:</p> <ul style="list-style-type: none"> • None: No encryption used. • Shared • WPA-Enterprise • WPA-Personal • Unknown
Data Encryption	<p>Displays the 802.11 authentication used by the currently used profile. Displays the 802.1x authentication algorithm; MD5, LEAP, TLS, TTLS and PEAP. Refer to Security Settings for more information.</p> <p>Displays: Yes, Normal (open or shared modes), WPA and WPA-PSK. Refer to Security Settings for more information.</p>
Access Points in this Network <0-50>	<ul style="list-style-type: none"> • Signal Strength: The Signal Quality icon bars indicate the strength of the transmit and receive signals in percent values between your wireless adapter and the nearest access point. <p>Indicates how well the wireless adapter is communicating with an access point or another wireless computer in peer-to-peer mode. Signal Quality ranges from Excellent to Out of Range.</p> <ul style="list-style-type: none"> • Displays a, b, or g. This icon indicates the band being used. • Channel: Displays the current transmit and receive channel being used for a particular wireless network. • BSSID (Infrastructure operating mode): Displays the twelve digit MAC address of the access points in the selected network.
Manage Exclusions	Refer to Manage Exclusions for more information.
Close	Close page.
Help?	Displays the help information for this page..

Menus

Use the **File**, **Tools**, **Profiles** and **Help** menu options to configure your network settings.

Name	Description
File	<p>Exit: Close the Intel PROSet/Wireless main window.</p> <p>To launch Intel PROSet/Wireless:</p> <ul style="list-style-type: none"> • 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: Provide system wide connection preferences. Use **Ctrl+P** from your keyboard as an alternative to using your mouse to access this feature. Refer to [Application Settings](#) for information.

Adapter Settings: Displays Adapter Settings corresponding to the settings made in Windows Device Manager, Use **Ctrl+A** from your keyboard as an alternative to using your mouse to access this feature. Refer to [Adapter Settings](#) for information.

Use Microsoft* client: Enable Windows XP as the wireless manager. Use **F10** from your keyboard as an alternative to using your mouse to access this feature. Refer to Use Microsoft client for more information.

Advanced Statistics: This information pertains to how the adapter is communicating with an access point. Use **Ctrl+S** from your keyboard as an alternative to using your mouse to access this feature. Refer to [Advanced Statistics](#) for more information.

Intel Wireless Troubleshooter The Troubleshooter is an application that can assist you in resolving wireless network connection issues. Use **Ctrl+W** from your keyboard as an alternative to using your mouse to access this feature. Refer to [Intel Wireless Troubleshooter](#) for information.

Administrator Tool: The Administrator tool is for 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. Use **Ctrl+T** from your keyboard as an alternative to using your mouse to access this feature. Refer to [Administrator Tool](#) for more information.

Profiles

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.

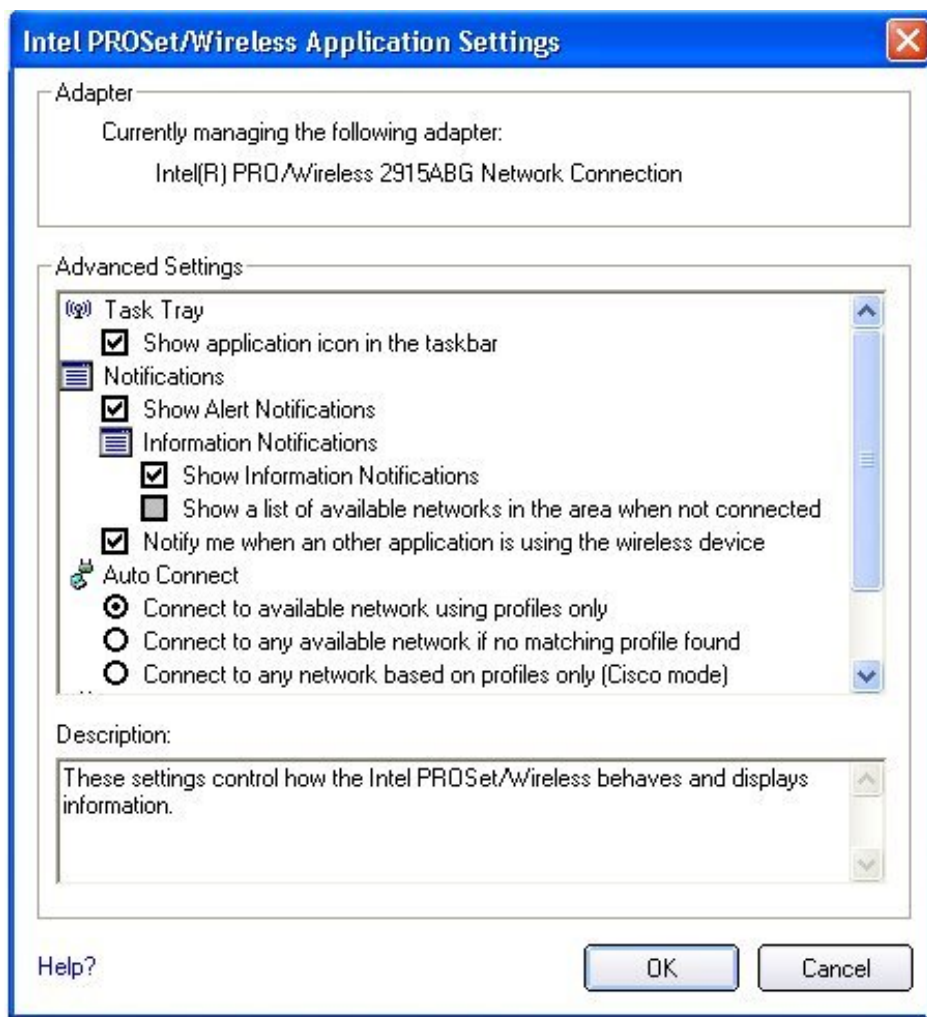
Manage Exclusions: Include or exclude specific access points. Refer to [Manage Exclusions](#) for information. Use **Ctrl+M** from your keyboard as an alternative to using your mouse to access this feature. Refer to [Exclude List](#) for information.

Help

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

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

Application Settings (Tools menu)



The Application Settings control how the 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	<p>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.</p> <p>The Task Tray Status Icon provides several functions:</p> <ul style="list-style-type: none"> • 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 dialog box 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 (coffee shop, airport terminal). To take advantage of the Intel PROSet/Wireless features you want to disable this software when you leave the hotspot.

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 specifies that the user knows 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

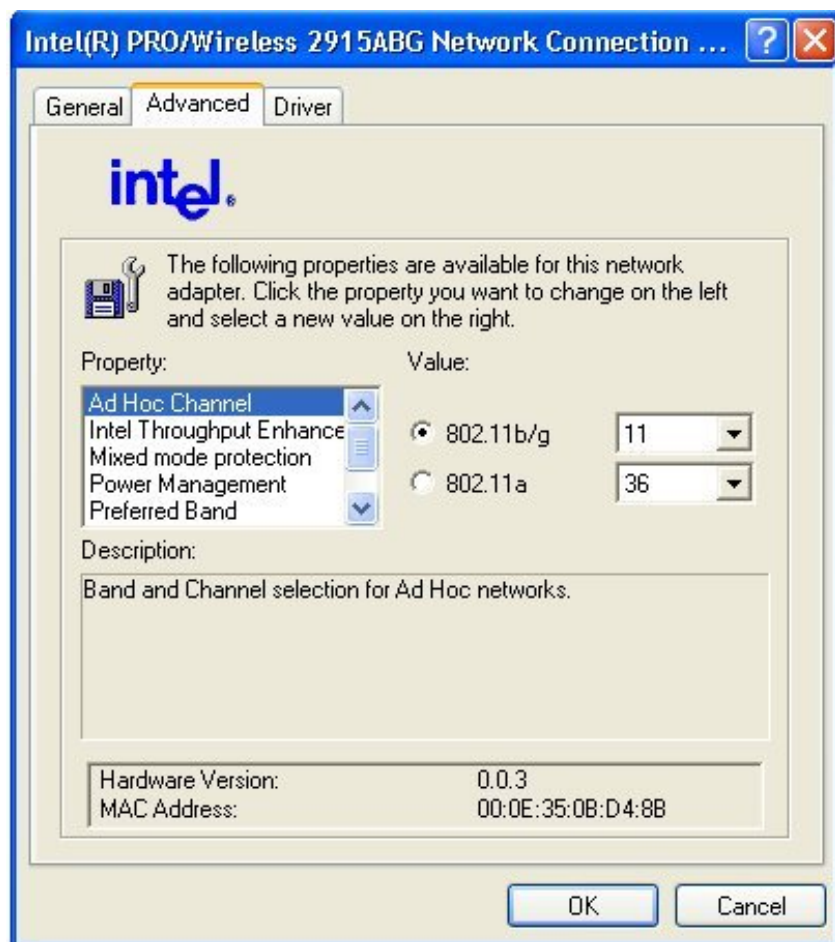
Save settings and return to the previous page.

Cancel

Close the page and cancel changes.

Help?

Displays the help information for this page.

Adapter Settings (Tools menu)

Adapter Settings displays the Device Properties for the Intel® PRO/Wireless 2915ABG Network Connection.

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.

Ad Hoc 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 takes effect when using either Infrastructure or ad hoc mode. Change the value of the Packet Burst Control.

Intel Throughput Enhancement

Enable: Select this option to enable throughput enhancement.

Disable: (Default) - Select this option to disable throughput enhancement.

Mixed mode protection

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

Power Management

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: (Default) - Power settings based on the computer's power source.

Manual: Adjust the slider for the desired setting. Use the lowest setting for maximum battery life. Use the highest setting for maximum performance.

Note: Power consumption savings vary based on infrastructure settings.

Preferred Band

Select the operating band. The selections are:

- **802.11g**
- **802.11a**
- **802.11b**

Wireless Mode

802.11a, 802.11b, and 802.11g: (Default) - Connect the either 802.11a, 802.11b or 802.11g wireless networks.

802.11g only: Connect the wireless adapter to 802.11g networks only.

802.11a and 802.11g only: Connect the wireless adapter to 802.11a and 802.11g networks only.

802.11b and 802.11g only: Connect 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

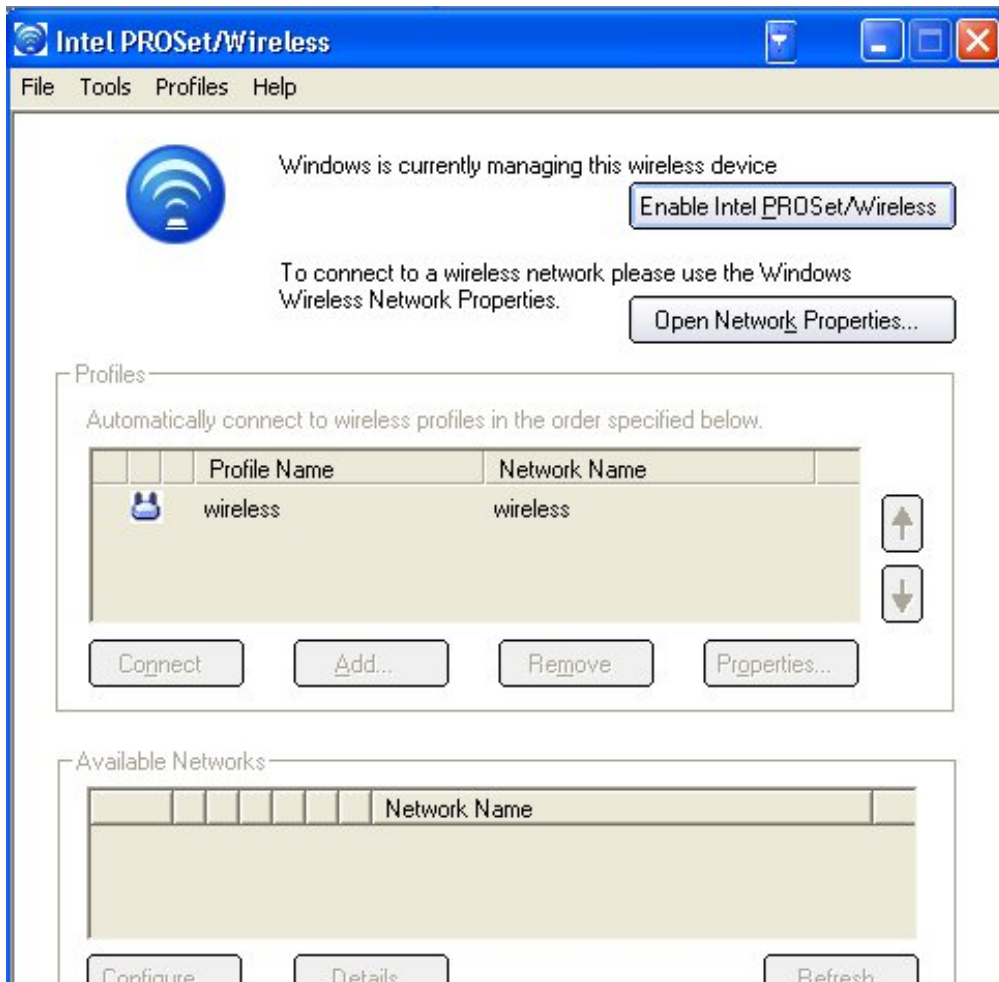
Save settings and return to the previous page.

Cancel

Close the page and cancel any changes made.

Help?

Displays the help information for this dialog.

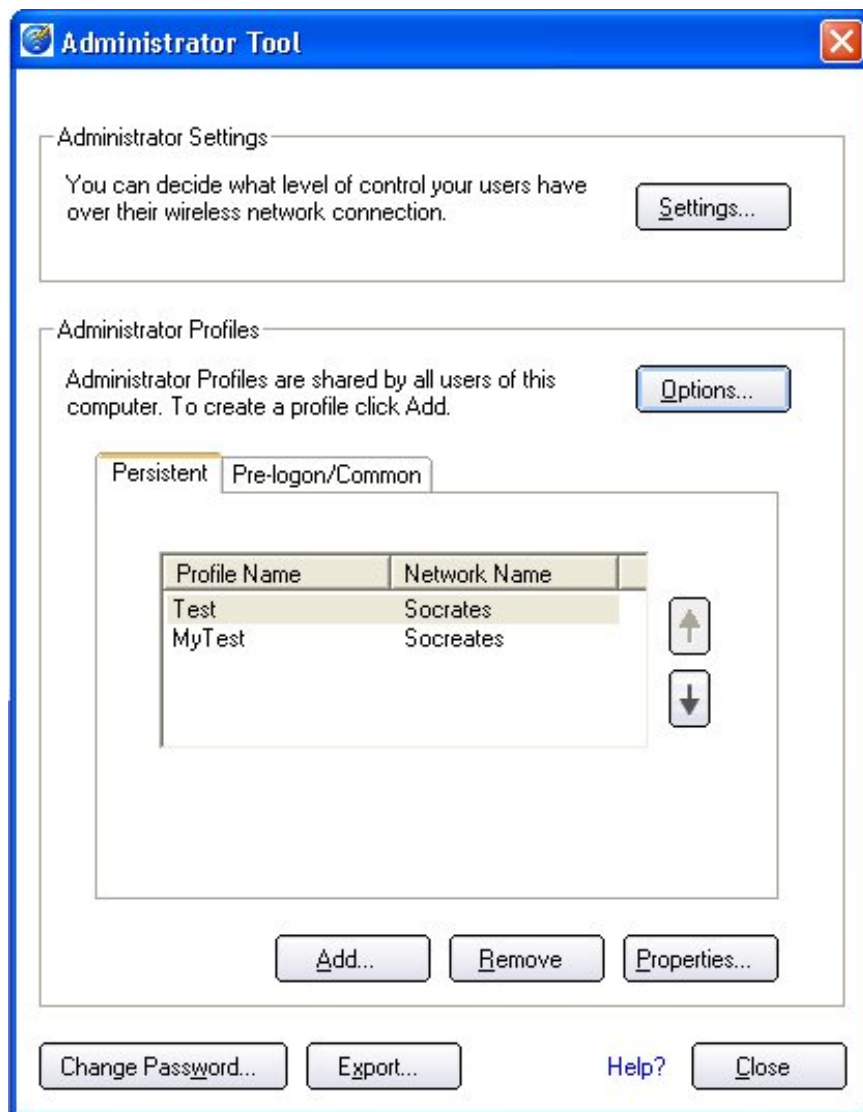
Use Microsoft Client *(Tools menu)



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.

Refer to [Intel PROSet/Wireless Configuration Service](#) for information on re-enabling Intel PROSet/Wireless.

Administrator Tool (Tools menu)



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

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

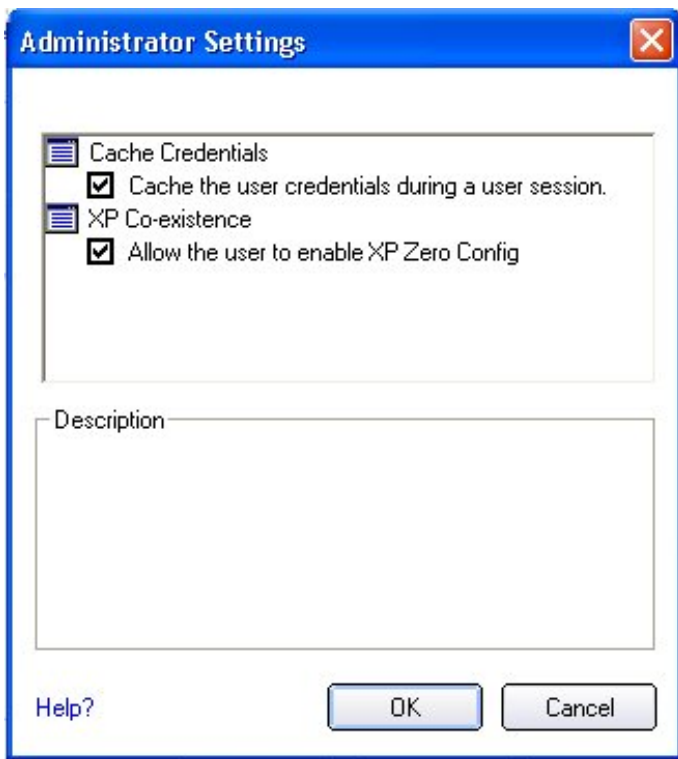
wireless connections.

Users cannot modify Administrator settings or profiles unless they have the password for this tool. A password should be chosen that is secure and not easily guessed.

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

Name	Description
Administrator Settings	Settings: Set the user control over their wireless network connections.
Administrator Profiles	Options: 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. Since they 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 profiles.
	Add: Launch the Profile Wizard to create a profile.
	Remove: Remove a selected profile from the profiles list.
	Properties: Edit the selected profile contents.
Change Password	Change the password for the Administrator Tool. See Change Password for more information.
Export	Export the settings and profiles as one package to other computers on your network.
Close	Close the page.
Help?	Displays the help information for this page.

Administrator Settings



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

Name	Description
Cache Credentials	<p>Cache Credentials:</p> <ul style="list-style-type: none"> • Cache the user credentials during a user session: <ul style="list-style-type: none"> • 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	<p>Allow the user to enable XP Zero Configuration:</p> <ul style="list-style-type: none"> • Allow the user to enable XP Zero Configuration: <ul style="list-style-type: none"> • 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: <p style="margin-left: 40px;">Do you wish to disable Windows XP management and let Intel(R) PROSet manage your wireless network?</p> <ul style="list-style-type: none"> • Select Yes, if you want Intel(R) PROSet for 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 notified in the event that Windows XP Zero Configuration wireless manager is enabled.

OK	Save settings and close the page.
Cancel	Cancel settings and close the page.
Help?	Displays the help information for this page.

Administrator Profile Options

These settings provide advanced profile connection options. Allows the Administrator to enable or disable Persistent and or Pre-Logon profiles on the computer.

Name	Description
Persistent Connection	Persistent Connection: A Persistent profile is active during boot time and when no user is logged onto the computer.
Pre-Logon/Common Connection	Pre-Logon/Common Connection: A Pre-Logon profile is active once a user logs onto the computer. These profiles appear at the top of the profile list. They cannot be modified by the end user without a password.
OK	Save settings and close the page.
Cancel	Cancel settings and close the page.
Help?	Displays the help information for this page.

Change Password

The Administrator Tool can be password protected. The default setting is no password. When a password is assigned, the Administrator Settings and Profiles can only be accessed if the assigned password is entered. Administrator profiles that are displayed in the Profiles list can be viewed using the Properties button.

To create a password:

1. Click **Administrator Tool** from the **Tools** menu.
2. Click **Change Password**.
3. Enter a password in the **New Password** text box.
4. Enter the new password again in the **Confirm Password** text box. The entered password characters display as asterisks.
5. Click **OK** to save the new password and close the page.

To change or unlock the existing password:

1. Click **Administrator Tool** from the **Tools** menu.
 2. Click **Change Password**.
 3. Enter the existing password in the **Old Password** text box.
 4. Enter the new password in the **New Password** text box.
 5. Enter the new password again in the **Confirm Password** text box.
 6. Click **OK** to save the new password and close the page.
-

Advanced Statistics (Tools menu)

Provides current adapter connection information. The following describes information for the **Advanced Statistics** page.

Name	Description
Statistics	<p data-bbox="537 304 1601 380">Advanced Statistics - This information pertains to how the adapter is communicating with an access point.</p> <p data-bbox="537 422 1601 497">Association - If the adapter finds an access point to communicate with, the value is In range. Otherwise, the value is Out of range.</p> <ul data-bbox="670 533 1601 831" style="list-style-type: none"> <li data-bbox="670 533 1601 609">● AP MAC Address: The twelve digit MAC address (00:40:96:31:1C:05) of the AP. <li data-bbox="670 611 1601 686">● Number of associations: The number of times the access point has found the adapter. <li data-bbox="670 688 1601 764">● AP count: The number of available access points within range of the wireless adapter. <li data-bbox="670 766 1601 831">● Number of full scans: The number of times the adapter has scanned all channels for receiving information. <p data-bbox="537 873 1601 1020">Roaming - This information contains counters that are related to reasons for the adapter roaming. Roaming occurs when an adapter communicates with one access point and then communicates with another for better signal strength.</p> <ul data-bbox="670 1062 1601 1839" style="list-style-type: none"> <li data-bbox="670 1062 1601 1096">● Roaming Count: The number of times that roaming occurred. <li data-bbox="670 1098 1601 1205">● AP did not transmit: The adapter did not receive radio transmission from the access point. You may need to reset the access point. <li data-bbox="670 1207 1601 1354">● 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. <li data-bbox="670 1356 1601 1503">● 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. <li data-bbox="670 1505 1601 1652">● 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. <li data-bbox="670 1654 1601 1730">● Poor channel quality: The quality of the channel is low and caused the adapter to look for another access point. <li data-bbox="670 1732 1601 1839">● 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. <p data-bbox="537 1881 1601 1986">Miscellaneous - Use this information to determine if an association with a different access point increases performance and helps maintain the highest possible data rate.</p>

- **Received Beacons:** Number 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.

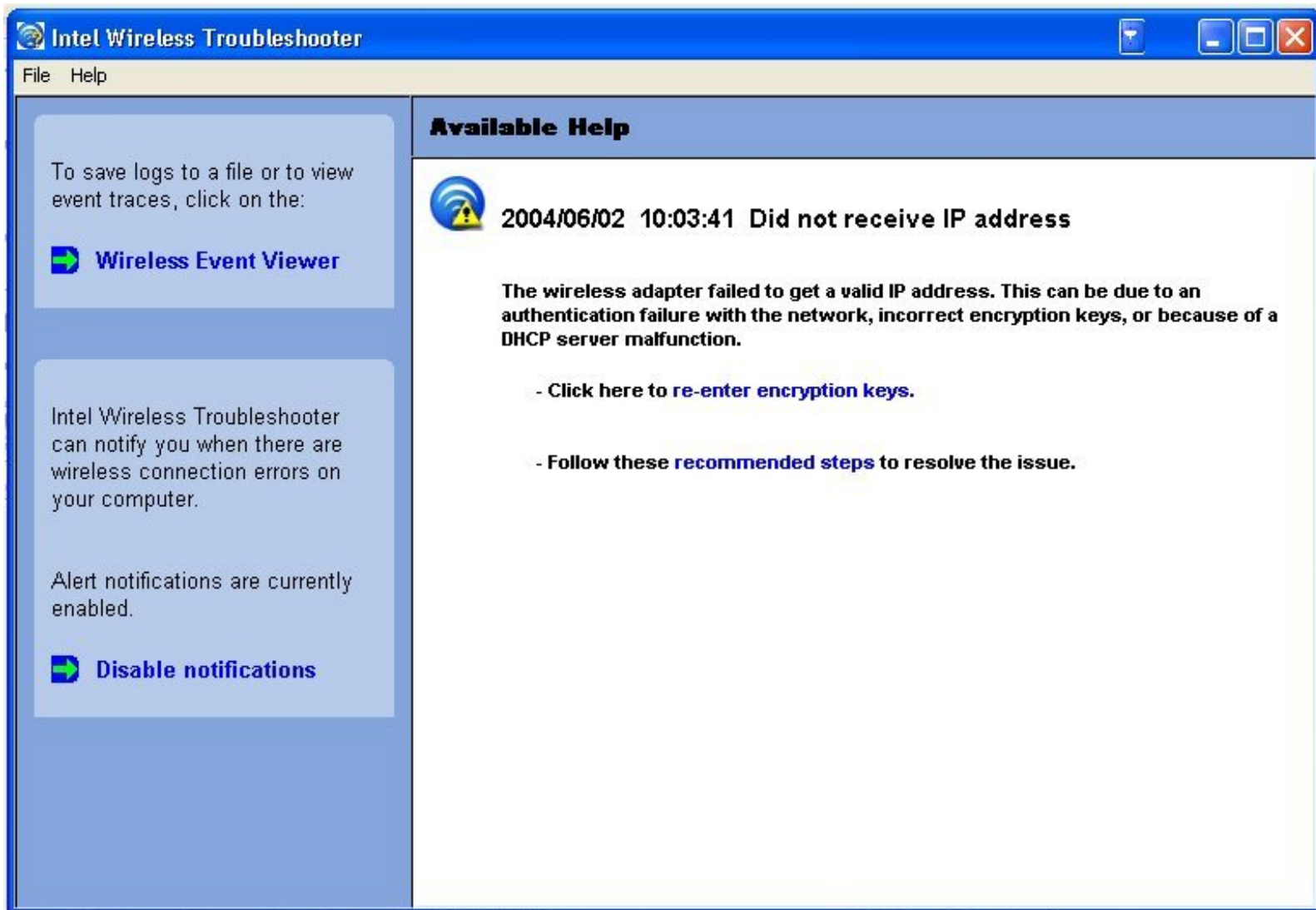
Close

Close the dialog and return to the main window.

Help?

Displays the help information for this page.

Intel Wireless Troubleshooter (Tools menu)



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. Once you click on the balloon tip, a diagnostic message displays the recommended steps to resolve the occurred connection issue. For example, if a connection issue occurred because of an invalid password, the Profile Wizard application is launched when you click on a displayed hyperlink. You can also launch [Wireless Event Viewer](#) from this page and enable or disable alert notifications. The Intel Wireless Troubleshooter is supported under Windows XP and 2000.

Intel Wireless Troubleshooter Description

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 parts. The error message and time stamp are preceded by an icon. The hint text part contains description about available utilities and help for resolving the associated connection issue. If you click on a help text link, the help text is displayed in a pop-up window. If you click on the associated issue resolver link, a program is launched to resolve the connection issue. You can launch [Wireless Event Viewer](#) or enable or disable from the last pane.

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

Help Intel(R) 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 below.
- Link to recommended steps to resolve error

Import/Export Profiles (Profiles menu)



Allows you to import and export user based profiles to and from the Profiles List. Wireless Profile can be automatically imported into the Profiles List. See [Import and Export Profiles](#) for more information.

To export Administrator profiles refer to [Administrator Export Properties](#) for more information.

Importing Profiles into the Profile 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 profile files. Only profiles that have been enabled **Enable Auto-Import** in [Advanced Settings](#) can be automatically imported. If a profile of the same name already exists in the Profiles List a dialog is displayed allowing you to either reject the imported profile, or accept it, in which case the existing profile is replaced. All imported user based profiles are placed at the bottom of the Profiles List, and the profile file is immediately deleted after it is the imported, whether the import was successful or not. Refer to [Automatic Profile Distribution](#) for more information.

Password Protected Profiles

Password protected user based profiles can be imported and exported automatically to remote systems. If a profile is password protected, before it can be edited, the assigned password must be entered. Refer to [Set a Password Protect](#) for more information.

Import/Export Description

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

Export profiles	<p>Select the profiles you want to export:</p> <p>Select individual or multiple profiles from the list. The profile mode icon indicates either infrastructure or ad hoc mode is being used, and if security is being used.</p> <p>Browse: Browse your hard disk for the destination directory. The directory path displays in the destination directory window.</p> <p>Export: Start exporting your profiles.</p>
Import profiles	<p>Imports profiles into the Profile List.</p> <p>Import: Browse your laptop hard disk for profiles to import.</p>
OK	Save settings and return to the previous page.
Cancel	Close the page and cancel any changes made.
Help?	Displays the help information for this page.

Manage Exclusions (Profiles menu)

The Exclude List management dialog is displayed when you select this menu option from the Profiles menu.

IMPORTANT: You are not automatically connected to a network or an Access Point that is in this list.

This dialog allows you to exclude entire wireless networks (SSID) or for networks with more than one access point, you may exclude an individual wireless access point (BSSID).

Name	Description
Exclude List Management	<p>Network Name: Name (SSID) of the wireless network.</p> <p>BSSID: MAC address for the selected access point.</p> <p>Reason: Indicates the reason that this entry was excluded from automatic connection.</p> <p>Note: Entries that are colored gray are excluded rouge access points. These entries cannot be removed from the list.</p>
Add	Add an access point to the list.
Remove	Remove an access point from the list.
Reset list	Clear the list.
Close	Close page and save settings.
Help?	Displays the help information for this page.

Turn Wireless Off/On

The wireless radio can be switched off and on using either the optional hardware radio switch on your computer,

from Intel PROSet/Wireless, or by disabling the device in Windows.



NOTE: When your computer is switched on, the radio is constantly transmitting signals. In certain situations, such as in a plane, signals from the radio may cause interference. Use the following methods if you need to disable the radio and use your laptop without emitting radio signals.

Using the optional computer radio off/on switch

If your computer has an external switch installed, it can be used to switch the radio on or off. Refer to the computer manufacturer for more information about this switch. If you have Intel PROSet/Wireless installed, the current state of the radio displays in the Intel PROSet/Wireless main window and in the [Task Tray](#).

Using Intel PROSet/Wireless to switch the radio off/on

From Intel PROSet/Wireless, the radio can be switched on or off. The status icon in the Intel PROSet/Wireless displays the current state of the radio.

From the Intel PROSet/Wireless main Window, click **Wireless off/on** and toggle the radio off and on.

Switching the radio off or on from the Task Tray Icon

To switch the radio off or on, click the [Task Tray icon](#) and select **Wireless Off (On)**.

How to Disable the Radio using Device Manager

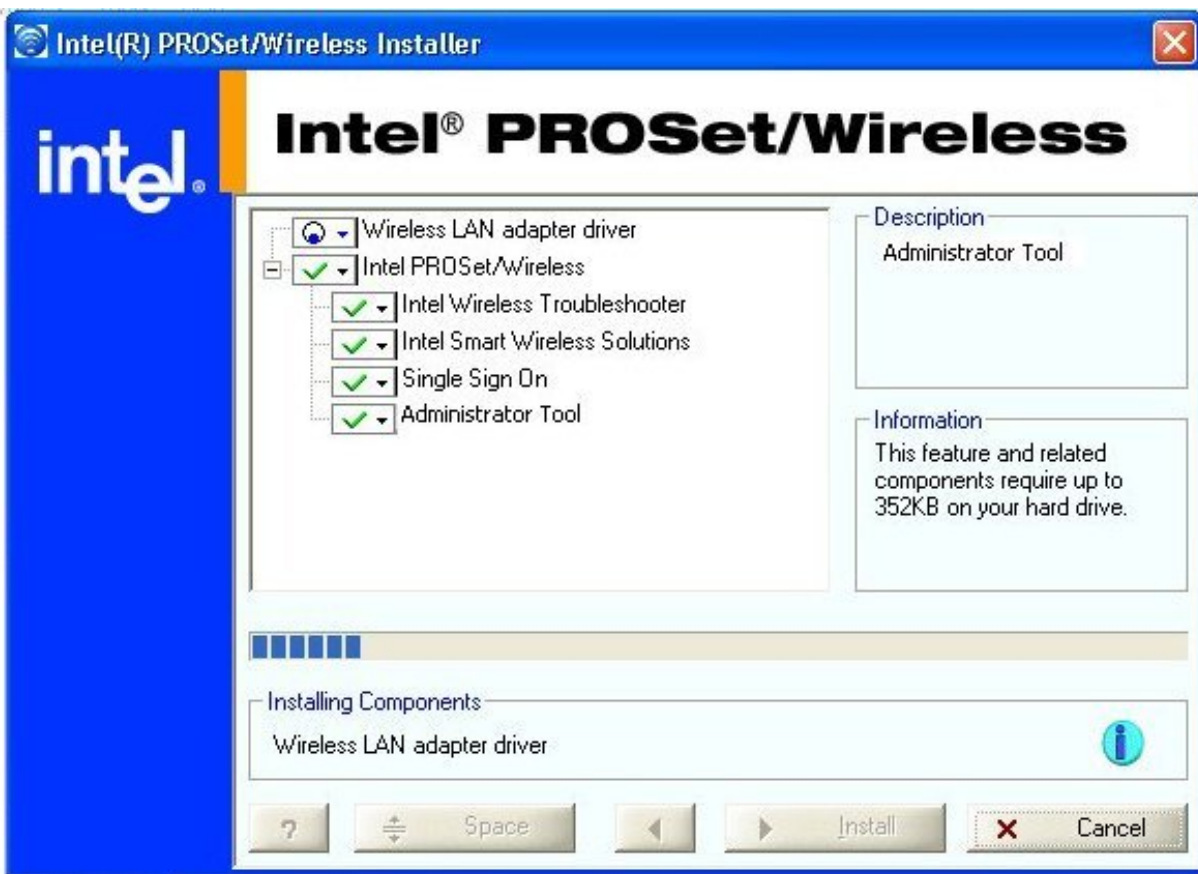
The radio can be disabled (made non-functional) via the Windows operating system using Device Manager.

Windows XP and 2000

1. From your desktop, right-click **My Computer** and click **Properties**.
2. Click the **Hardware** tab.
3. Click **Device Manager**.
4. Double-click **Network adapters**.
5. Right-click the installed wireless adapter in use.
6. Choose **Disable** from the pop-up menu.
7. Click **OK**.

Install and Uninstall the Software

[Intel Wireless Troubleshooter](#), Intel Smart Wireless Solutions, the Single Sign On feature and [Administrator Tool](#) are not installed during the **Typical** installation process. To install these features, use the **Custom** option during the installation process. The [Single Sign On Feature](#) can also be installed or uninstalled after Intel PROSet/Wireless has been installed. Refer to [Installing and Uninstalling Single Sign On Feature](#) for instructions.



To install the software:

1. Insert the Installation CD in your CD drive.
2. Click **Install Software** on the Intel(R) PRO Network screen.
3. On the License Agreement screen, after reading the license agreement. Select **I accept the terms in the license agreement** and click **Next**.
4. Click **Custom**.
5. Select from the list of features to install:

Intel PROSet/Wireless: The Intel(R) PROSet/Wireless application software.

- **Install:** Click **Intel PROSet Wireless**. Select **Install this feature and all subfeatures**. Proceed to step 5.
- **Not install:** Click **Do not install this feature**. A red x displays next to the option indicating that it will not be installed.

Intel Smart Wireless Solutions: Provides an easy configuration wizard for connecting to a wireless router.

- **Install:** Click Intel Smart Wireless Solutions. Select **Install this feature and all subfeatures**. Proceed to step 5.
- **Not Install:** Click **Do not install this feature**. A red x displays next to the option indicating that it will not be installed.

Single Sign On: Provides administrator control of Pre-Logon and Persistent connections.

- **Install:** Click **Single Sign On**. Select **Install this feature and all subfeatures**. Click **Next** and proceed to step 5. **Note:** Windows XP Fast Switching and the Welcome screen are disabled when the Single


Sign On feature is installed.

- **Uninstall:** Click Single Sign On. Select **Do not install this feature**. A red x displays next to the option indicating that it will not be installed.

Administrator Tool: Provides administrator control over what level of control each user has over their wireless network connections.

- **Install:** Click **Single Sign On**. Select **Install this feature and all subfeatures**. Click **Next** and proceed to step 5. **Note:** Windows XP Fast Switching and the Welcome screen are disabled when the Single Sign On feature is installed.
- **Not Install:** Click **Do not install this feature**. A red x displays next to the option indicating that it will not be installed.

5. Click **Install**.
6. After the software is installed on your computer, the installed components are listed.
7. Click **OK**.

 **NOTE:** If the Single Sign On feature was installed, you must reboot the system.

8. Click **Yes** to reboot.

Installing and Uninstalling the Single Sign On Feature

The Single Sign On feature, includes Pre-Logon Connect and Persistent Connect features. By default they are not installed during the initial software installation process unless you choose to make a Custom install. These features can also be installed or uninstalled after Intel PROSet Wireless has been installed.

To install the Single Sign On features after Intel PROSet/Wireless has been installed:

1. Click **Start > Settings > Control Panel > Add or Remove Programs > Intel PROSet Wireless**.
2. Select **Change**.
3. Select **Modify** on the Program Maintenance screen
4. Click **Next**.
5. 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 is installed.
6. Click **Modify**.
7. After the software is installed on your computer, the component is listed as "Installed."
8. Click **OK**.

To remove the Single Sign On feature:

1. Click **Start > Settings > Control Panel > Add or Remove Programs > Intel PROSet Wireless**.
2. Select **Change**.
3. Select **Modify** on the Program Maintenance screen
4. Click **Next**.
5. Click **Single Sign On**. Select **Do not install this feature**. A red x displays next to the option.
6. Click **Modify**.
7. After the software is installed on your computer, the component is listed as "Not Present."
8. Click **OK**.

[Back to Contents](#)

Setting up Security: Intel PRO/Wireless 2915ABG Network Connection User Guide

- [Security Settings Page Options](#)
 - [Network Authentication: Device to Device](#)
 - [Network Authentication \(Infrastructure\): Enable 802.1x Authentication](#)
-

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

See the [Profile Wizard Overview](#) for a description of when the Profile Wizard is launched.

See [Security Overview](#) for more information the different security options for wireless networks.

Security Settings Page Options



The options displayed are dependent on the Operating Mode (Device to Device or Infrastructure) selected on the General Settings page.

Name	Setting
-------------	----------------

Network Authentication

[Open](#)

[Shared](#)

[WPA-Enterprise](#)

[WPA2-Enterprise](#)

[WPA-Personal](#)

[WPA2-Personal](#)

Data Encryption

None

[WEP](#)

[CXIP](#)

Enable 802.1x (Authentication Type)

[MD5 Open](#)

[MD5 WEP Key](#)

[EAP-SIM](#)

[TLS](#)

[TTLS](#)

[PEAP](#)

[LEAP](#)

[EAP-FAST](#)

Cisco Options

Click to view the [Cisco Compatible Extensions](#) Options page.

Note: Cisco Compatible Extensions are automatically enabled for CKIP, LEAP or 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.

Network Authentication: Device to Device

Open/None authentication/WEP encryption

This ad hoc 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	None: No data encryption used. 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 (64-bit): Enter 5 alphanumeric characters, 0-9, a-z or A-Z. Hex key (64-bit): Enter 10 alphanumeric hexadecimal characters, 0-9, A-F. Pass phrase (128-bit): Enter 13 alphanumeric characters, 0-9, a-z or A-Z. Hex key (128-bit): Enter 26 alphanumeric hexadecimal characters, 0-9, A-F.

Network Authentication (Infrastructure): Enable 802.1x Authentication

Open authentication, no encryption

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

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

Network Authentication

Open: 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.

Open authentication, WEP encryption

This network uses no network authentication with WEP data encryption.

Name	Description
Network Authentication	<p>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.</p>
Data Encryption	<p>WEP: WEP data encryption can be configured using 64-bit or 128-bit. WEP settings can be used with all Network Authentication protocols.</p> <p>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.</p>
Encryption Level	<p>Unchecked.</p>
Key Index	<p>1,2,3,4: Up to four passwords may be specified by changing the Key Index.</p>
Wireless Security Password (WEP Key)	<p>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.</p> <p>Pass phrase and hex key options are:</p> <p>Pass phrase (64-bit): Enter 5 alphanumeric characters, 0-9, a-z or A-Z. Hex key (64-bit): Enter 10 alphanumeric hexadecimal characters, 0-9, A-F.</p> <p>Pass phrase (128-bit): Enter 13 alphanumeric characters, 0-9, a-z or A-Z. Hex key (128-bit): Enter 26 alphanumeric hexadecimal characters, 0-9, A-F.</p>

Shared authentication

Name	Description
Network Authentication	<p>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).</p> <p>Refer to Security Overview - Open and Shared Key authentication for more information</p>
Data Encryption	<p>None: No data encryption used.</p> <p>WEP: WEP data encryption can be configured using 64-bit or 128-bit.</p> <p>CKIP: Cisco Key Integrity Protocol (CKIP) is a Cisco proprietary security protocol for data encryption in 802.11 media.</p>
Enable 802.1x	Disabled.
Encryption Level	64-bit or 128-bit: When switching between 64-bit and 128-bit encryption, the previous settings are erased and a new key must be entered.
Key Index	1,2,3,4: Up to four passwords may be specified by changing the Key Index.
Wireless Security Password (WEP Key)	<p>Enter 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.</p> <p>Pass phrase (64-bit): Enter 5 alphanumeric characters, 0-9, a-z or A-Z.</p> <p>Hex key (64-bit): Enter 10 alphanumeric hexadecimal characters, 0-9, A-F.</p> <p>Pass phrase (128-bit): Enter 13 alphanumeric characters, 0-9, a-z or A-Z.</p> <p>Hex key (128-bit): Enter 26 alphanumeric hexadecimal characters, 0-9, A-F.</p>

WPA - Enterprise or WPA2 - Enterprise

Obtain and install a client certificate, refer to [Setting up the Client for TLS authentication](#) or consult your system administrator.



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-2 Enterprise requires an authentication server.

Name	Description
Network Authentication	WPA-Enterprise
Data Encryption	Refer to Security Overview - Open and Shared Key authentication for more information
Enable 802.1x	AES-CCMP Checked..
Authentication Type	TLS. Refer to TLS Authentication.

WPA - Personal or WPA2 - Personal

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 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 a also re-keying mechanism. Using these improvement enhancements, TKIP protects against WEP's known weaknesses.

Name	Description
Network Authentication	WPA-Personal: See Security Overview
	WPA2-Personal: See Security Overview
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.
	CKIP: Cisco Key Integrity Protocol (CKIP) is a Cisco proprietary security protocol for encryption in 802.11 media. Refer to Security Overview for more information. Note: CKIP is enabled only when the checkbox

for Cisco Client eXtentions is selected.

TKIP: To improve data encryption, Wi-Fi Protected Access utilizes its Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a re-keying method. Refer to [Security Overview](#) for more information. **Note:** TKIP is enabled only when the checkbox for Cisco Client eXtentions is selected.

Default is unchecked (Disabled). Select this option to enable Cisco-Client Options. Refer to [Cisco Compatible Extensions Options](#) for details. From the Cisco Compatible Extensions Options page you can enable Radio Management support and [Mixed Cells mode](#).

Check this box to enable **CKIP** and **TKIP** data encryption and 802.1x **LEAP** authentication on the [Security Settings](#) page.

Enter your network key (wireless security password) for your wireless network in the Network key field. Make sure that the network key used matches the Windows network key.

Password:

- Enter a text phrase with at least 8 up to 63 characters in the pass phrase field.

WPA-Personal uses Wi-Fi Protected Access authentication. Pre Shared Key (WPA-PSK) mode does not use an authentication server. WPA-PSK requires configuration of a pre-shared key (PSK). The data encryption key is derived from the PSK.

Cisco-Client eXtentions

WPA Key

802.1x MD5 - Open/None

MD5 authentication is a one-way authentication method that uses user names and passwords. This method does not support key management, but does require a pre-configured key if data encryption is used.

MD5 Settings

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

Network Authentication

Open: No authentication used. Refer to [Open and Shared Key authentication](#) for more information.

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

Checked.

Authentication Type

MD5: A one-way authentication method that uses user names and passwords.

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.

Prompt for the user name and password

Prompts for a user name and password before you connect the wireless network. The user name and password must be first set in the authentication server by the administrator.

Use the following user name and password

The user name and password must be first set in the authentication server by the administrator.

User Name: This user name must match the user name that is set in the authentication server.

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.

802.1x MD5 – WEP Key

MD5 authentication is a one-way authentication method that uses user names and passwords. This method does not support key management, but does require a pre-configured key if data encryption is used.

MD5 Settings for Shared/None, Open/WEP, Open/CKIP.**Name****Description****Network Authentication**

Open: No authentication used. Refer to [Open and Shared Key authentication](#) for more information.

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.

CKIP: Cisco Key Integrity Protocol (CKIP) is a Cisco proprietary security protocol for encryption in 802.11 media. Refer to [Security Overview](#) for more information.

Checked.

64-bit: 64-bit or 128-bit encryption.

1,2,3,4: Up to four passwords may be specified by changing the Key Index.

Wireless Security Password (WEP Key) Enter 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 alphanumeric characters, 0-9, a-z or A-Z.

Hex key (64-bit): Enter 10 alphanumeric hexadecimal characters, 0-9, A-F.

Pass phrase (128-bit): Enter 13 alphanumeric characters, 0-9, a-z or A-Z.

Hex key (128-bit): Enter 26 alphanumeric hexadecimal characters, 0-9, A-F.

Step 2 of 2: MD5 User

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.

Prompt for the user name and password: Prompts for a user name and password before you connect the wireless network. The user name and password must be first set in the authentication server by the system 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.

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.

EAP-SIM Authentication

Your Subscriber Identity Module (SIM) card is used to validate your credentials with the network. A SIM card is a special smart card that is used by GSM based digital cellular networks.

EAP-SIM authentication can be used with:

- **Network Authentication types:** Open, Shared, WPA-Enterprise and WPA2-Enterprise
- **Data Encryption types:** None, WEP and CKIP

Name	Description
EAP-SIM User	<p>Specify user name (identity): Select this option to specify the user name.</p> <ul style="list-style-type: none"> • User Name: The user name assigned to the SIM card.

TLS Authentication

These settings define the protocol and the credentials used to authenticate a user. TLS authentication is a two-way authentication method that exclusively uses digital certificates to verify the identity of a client and a server.

Name	Description
Step 1 of 2: TLS User	
Use my smart card or certificate	<p>Smart card: Click this option if the certificate resides on a smart card.</p>
	<p>Certificate: Click this option if the certificate resides on this computer</p>
User Name	<p>User Name: This user name must match the user name that is set in the authentication server by the administrator prior to client's authentication. The user name is case-sensitive.</p>
Client Certificate	<p>Select: TLS requires a Client Certificate from the Personal Certificate store of the Windows logged-in user. This certificate identifies you as the user. This certificate is used for client authentication. Click Select to choose a client certificate</p>
Step 2 of 2: TLS Server	

Certificate Issuer

Certificate Issuer: The server certificate received during TLS message exchange must have been issued by this certificate authority. Trusted intermediate certificate authorities and root authorities whose certificates exist in the system store are available for selection in the drop-down list box. If Any Trusted CA is selected, any CA in the list is 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.

Specify 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, based 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 fully qualified 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.

Server 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.

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.

Name	Description
Step 1 of 2: TTLS User Authentication Protocol	<p>This parameter specifies the authentication protocol operating over the TTLS tunnel. The protocols are: PAP, CHAP, MD5, MS-CHAP and MS-CHAP-V2.</p> <p>Using PAP, CHAP, MD5, MS-CHAP, and MS-CHAP-V2 protocols:</p> <ul style="list-style-type: none">● 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.● 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 administrator.● Use the following user name and password: The user name and password are securely (encrypted) saved in the profile<ul style="list-style-type: none">● User Name: This user name must match the user name that is set in the authentication server.● 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 Client Certificate	<p>Select: A client certificate from the Personal certificate store of the Windows logged-in user, this certificate is used for client authentication.</p>
Roaming Identity	<p>When using 802.1x MS RADIUS as an authentication server, the authentication server authenticates the device by using the "Roaming Identity" username from Inte. PROSet/Wireless 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).</p>
Step 2 of 2: TTLS Server	

Certificate Issuer

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

Specify Server/Certificate Name

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

- **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.

PEAP Authentication**Name****Description**

Step 1 of 2: PEAP User

Authentication Protocol

This parameter specifies the authentication protocol operating over the PEAP tunnel. The protocols are: MS-CHAP-V2, GTC, and TLS.

Using MS-CHAP-V2 and GTC protocols:

- **Use the Windows logon user name and password:** If this feature is selected the credentials are retrieved from the Windows Logon process.
- **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.
 - **For GTC protocol:** 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.
 - **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 Intel PROSet/Wireless 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 system 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:** Choose a client certificate from the Personal certificate store of the Windows logged-in user. This certificate is used for client authentication.

Step 2 of 2: PEAP Server Certificate Issuer

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

Specify Server/Certificate Name

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

- **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.

LEAP Authentication

Name	Description
Use the Windows logon user name and password	Selecting this feature, the user credentials are retrieved from the Windows Logon process.
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 system administrator.

Use the following user name and password:

The user name and password must be first set in the authentication server by the system administrator.

User Name: This user name must match the user name that is set in the authentication server.

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.

EAP-FAST Authentication

EAP-FAST is an improvement on LEAP. Refer to [Cisco Features](#) for more information.

Name	Description
Use the Windows logon user name and password	The user credentials are retrieved from the Windows Logon process.
Prompt for the user name and password	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 administrator.
Use the following user name and password:	The user name and password must be first set in the authentication server by the administrator.
	User Name: This user name must match the user name that is set in the authentication server.
	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 automatic provisioning of Protected Access Credentials (PAC):

EAP-FAST uses a Protected Access Credentials key to protect the user credentials that are exchanged.

- Click “Allow automatic provisioning” if you want to obtain the PAC from the server.
- If a PAC has already been obtained, uncheck “Allow automatic provisioning”, and click **Select** to choose an existing PAC on your computer.

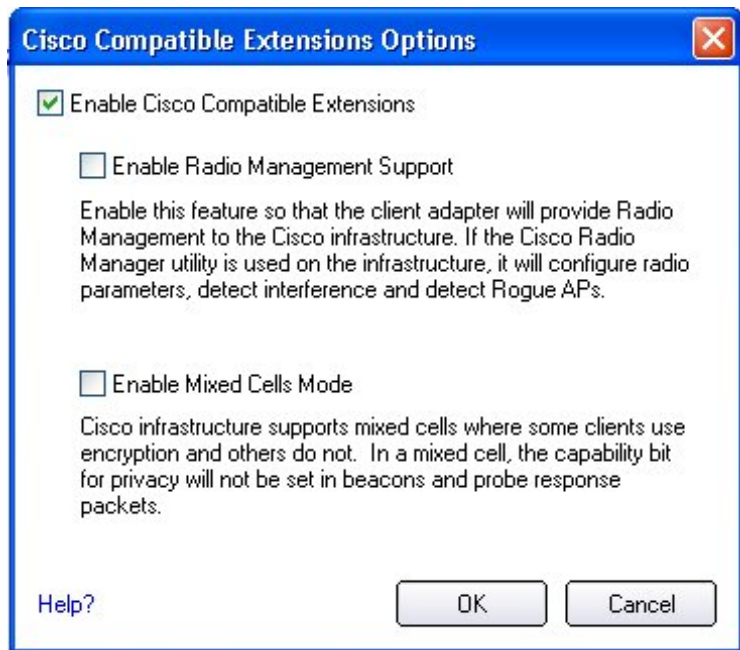
Allow Fast Roaming (CCKM)

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.

Cisco Compatible Extensions Options

Cisco Options: Select this feature to enable Cisco Compatible Extensions for this wireless connection profile. From this dialog you can enable/disable Radio Management and Mixed Cells Mode.



NOTE: Cisco Compatible Extensions are automatically enabled for CKIP, LEAP or EAP-FAST profiles. You may override this behavior by checking or un-checking options.

Name	Description
Enable Cisco Compatible Options:	Select this feature to enable Cisco Compatible Extensions for this wireless connection profile.
Radio Management:	Enable Radio Management Support: Click to choose that your wireless adapter provides radio management to the Cisco infrastructure. If the Cisco Radio Management utility is used on the infrastructure, it configures radio parameters, detect interference and Rogue access points. Default setting is checked.
Mixed Cells Mode:	Enable Mixed Cells Mode: Click to allow the wireless LAN adapter to communicate with mixed cells. A mixed cell is a wireless network in which some devices use WEP and some do not. Refer to Mixed Cells Mode for more information. Default setting is unchecked.

[Back to Contents](#)

[Trademarks and Disclaimers](#)

Using Profiles: Intel(R) PRO/Wireless 2915ABG Network Connection User Guide

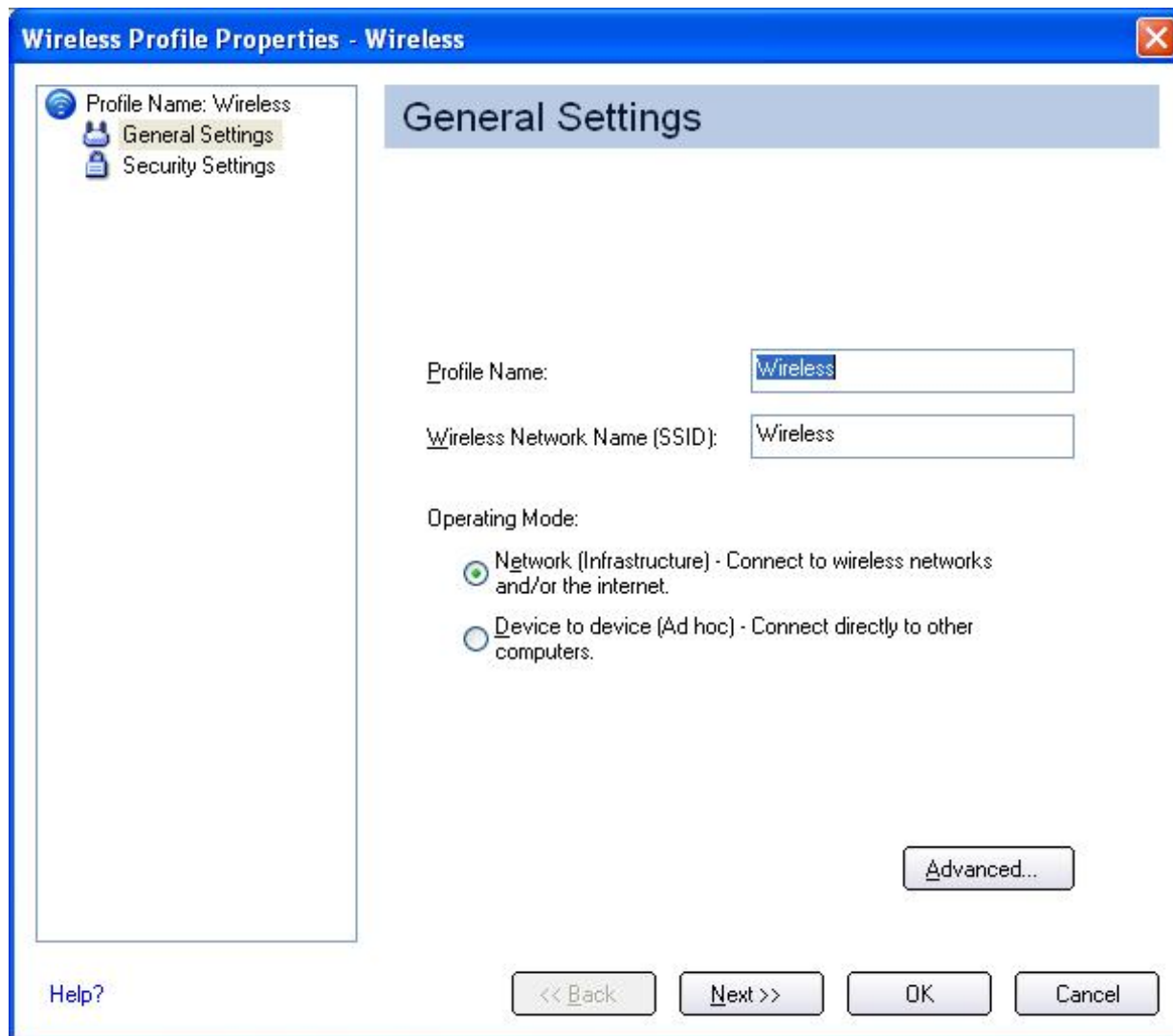
- [Profile Wizard Overview](#)
 - [Creating a New Profile](#)
 - [Editing an Existing Profile](#)
 - [Removing a Profile](#)
 - [Importing and Exporting Profiles](#)
 - [Setting a Profile Password](#)
 - [Administrator Profiles](#)
 - [Automatic Profile Distribution](#)
 - [Single Sign On Support and Windows XP Welcome Screen and Fast User Switching](#)
-

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 to another wireless network, the “**Connect to wireless network**” page is displayed. From Intel PROSet/Wireless, select a network from the Available Network list, and click **Configure**.

1. The [General Settings](#) page is displayed with 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.



2. Click **Next** to display the Profile Wizard Security Settings page. This starts the access point query process to determine the highest level of security required for the selected network. Refer to [Setting up Security](#) for more information on security options.
3. After the required security is determined, click **Next**.
4. 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 system administrator.

Creating a New Profile

Use the Profile Wizard to create a new profile.

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 is launched and the General Settings page is displayed.

The screenshot shows a dialog box titled "Wireless Profile Properties - Wireless". On the left, there is a sidebar with three items: "Profile Name: Wireless" (with a wireless icon), "General Settings" (with a gear icon and highlighted), and "Security Settings" (with a lock icon). 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.
- Navigation buttons at the bottom: **<< Back**, **Next >>**, **OK**, and **Cancel**.
- A **Help?** link in the bottom left corner.

2. Enter a profile name in the **Profile Name** text box.
3. Enter the **Wireless Network Name (SSID)** in the text box.
4. Select the Operating Mode: **Network** or **Device to Device**.
5. Click **Advanced** for the following options:

Advanced Settings

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:

Help?

- [Password protect the profile](#). Click **Password protect this profile**. Type the password in the text box, then re-enter it in the **Confirm Password** text box.
- [Auto-Import](#) this profile (for network administrators only).
- [Mandatory Access Point](#). This option makes the wireless adapter associate with a specific access point.

6. From the General Settings page, Click **Next**. The Security Settings page is displayed



6. The Security Settings page displays the current security status for the network access point. Click **Next** to set Network Authentication and Data Encryption options.

7. 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.
 8. Click **OK** when you have completed the profile settings. The Profile Wizard ends and you are returned to Intel PROSet/Wireless main window. To change or verify the profile settings, click the **Back** button.
 9. If you are not currently connected to a network, Intel PROSet/Wireless detects that a new profile has been added and automatically attempts to connect to this new profile.
 10. If you want to manually connect to this profile, click **Connect** to use this wireless network. The [connection icon](#) displays the current connection status. The network name, transmit and receive speed, and signal quality are also displayed.
-

Editing an Existing Profile

To edit an existing profile:

1. Select the profile to edit from the Profiles List.
 2. Click **Properties**. The General Settings and Security Settings pages display all of the profile settings and parameters that can be modified.
 3. Click **Next** and **Back** to navigate through the General and Security Setting settings.
 - **General Settings**. Refer to [General Settings](#) for more information.
 - **Security Settings**. Refer to [Security Settings](#) for more information.
-

Removing a Profile

To remove a profile:

1. Select the profile to be removed from the Profiles List.
2. Click **Remove** to delete the profile.



NOTE: You cannot delete all profiles from the Profiles List. There must always be one profile displayed in the list.

Importing and Exporting Profiles



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.

Export Profiles

To export profiles from your profile list:

1. From the Intel PROSet/Wireless main window, click **Import/Export** on the Profiles menu.
2. Select the profile or profiles from the list,
3. Specify the destination folder on your hard drive. You can use the Browse button to navigate to a folder.
4. Click **OK** after the profiles have been successfully exported.
5. Click **Close** to close Intel PROSet/Wireless main window.

Import profiles

To add profiles to your profile list:

1. From the Intel PROSet/Wireless main window, click **Import/Export** on the Profiles menu.
2. Click **Import**.
3. Locate the profile to import on your computer or enter the profile name in the file name field. The profile extension is either **.profiles** or **.p50**. The profiles to import can be located in any directory you choose on your computer.
4. Click **Import** to import the profile into the profile list.
5. Click **Close** to return to the Intel PROSet/Wireless main window. The imported profile is displayed in the profile list and is ready to use.

Setting a Profile Password



Note: A password protected profile can be imported and exported; however, before editing the profile, the password must be entered.

To set a password for an existing profile:

1. From the Intel PROSet/Wireless main window, click **Properties**. The General Settings page is displayed.
2. Click [Advanced](#).
3. Click **Password protect this profile**.
4. **Password:** Type the password.
5. **Confirm Password:** Re-type the password.
6. Click **OK** to save the setting and return to the General Settings page.
7. Click **OK**. The Intel PROSet/Wireless main window is displayed.

Administrator Profiles

Administrator Profiles are created using the Administrator Tool.

Administrator Profiles are profiles or shared profiles that are 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 from the Administrator Tool which is password protected.

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

Persistent Connection

Persistent profiles are applied at boot time or whenever no one is logged on the computer. After a user logs off, a Persistent profile maintains a wireless connection either until the computer is turned off or a different user logs on.

Pre-Logon/Common Profiles

Pre-logon/Common profiles are applied once a user logs on. If Single Sign On (“Use Windows username and password”) 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 once the user session is active. Pre-logon/Common profiles always appear at the top of a user’s profile list. A user can still prioritize their own profiles that 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.

Pre-Logon Connect Status

When the [Single Sign On](#) component is installed, you have Pre-Logon/Common support.

During the Windows log on sequence, a Pre-logon Status page is displayed. This page displays the progress of the network connection. After the wireless adapter is associated with the network access point, the Status page closes.

Administrator Export Properties

Use the Administrator Settings and Administrator Profiles options to configure shared profiles for exporting. Exported profiles and settings can be pushed to any Intel PROSet/ Wireless 'auto import' folder. They are exported as one package.

Administrator Export Preferences dialog

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

Export Administrator Preferences**Step 1: Select which preferences you want to export:**

- **Administrator Settings:** Export all the settings. These include control of Cache Credentials and XP Co-existence.
- **Administrator Profiles:** Export all the Persistent and Pre-logon/Common Profiles.

Step 2: Select the destination file:

- **Browse button:** Select the destination path and directory. The export destination file has a .sso extension. The directory path displays in the destination directory window.

Step 3: Export the selected preferences:

- **Export button:** Start exporting your profiles to the assigned destination folder.

Close

Close page.

Help?

Displays the help information for this page.

Automatic Profile Distribution

The Enable Auto-Import feature allows a network administrator to distribute a profile automatically to computers connected to a network. These profiles can be automatically imported from the \Programs Files\Intel\Wireless\AutoImport directory on the client computer. Enable Auto-Import option is located on the the [Advanced Settings](#) page. Click **Advanced** on the Profile Wizard General Settings page to access the Advanced Settings.

The profile must 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 is automatically available from the Profiles List. If an attempt is made to edit a distributed profile that is password protected, a password prompt appears.

Automatically importing 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 can be automatically imported. If a profile of the same name already exists in the Profiles List, a dialog is displayed from which you can either reject the import, or accept in which case the existing profile is replaced. All imported profiles are placed at the bottom of the Profiles List, and the profile file is immediately deleted after the import whether the import was successful or not.

To import a profile into the Profiles List:

1. Select the profile from the Profiles List, and click the **Properties** button.
2. Click the **Advanced** button.
3. Select **Enable Auto-import**.
4. Click **OK** to save the setting and exit.
5. Click **OK** to close the General Settings page.
6. Export the profile from the Profiles List. Refer to [Importing and Exporting Profiles](#) for details.

7. Copy the exported profile from its directory to the **Programs Files\Intel\Wireless\AutoImport** directory. The profile is now ready to distribute to other computers.

Single Sign On Support 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 ("Use Windows user name and password") is targeted to the enterprise environment where users logon 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 Fast User Switching option is not available.

[Back to Contents](#)

[Trademarks and Disclaimers](#)

[Back to Contents](#)

Security Overview: Intel(R) PRO/Wireless 2915ABG Network Connection User Guide

- [WEP encryption](#)
 - [802.1x Authentication](#)
 - [WPA/WPA2](#)
 - [Cisco Features](#)
-

WEP encryption

Using the 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.

Wired Equivalent Privacy (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

802.11 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 AP 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 passed a challenge based authentication.

802.1x Authentication

[How 802.1x authentication works](#)

[802.1x features](#)

Overview

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).

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 server (RADIUS)). 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 networks 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

Refer to [Security Settings](#) for more information.

WPA/WPS2

Wi-Fi Protected Access (WPA/WPA2) 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 a also re-keying mechanism. Using these improvement enhancements, TKIP protects against WEP's known weaknesses.

The second generation of WPA that complies with the IEEE TG1 specification is known as WPA2.

WPA/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/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 (WPA-PSK) 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 network 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.” Refer to [Cisco Compatible Extensions Options](#) for more information.

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 on the infrastructure, it configures radio parameters, detects interference and Rogue access points.

[Back to Contents](#)

Connecting to a Network: Intel(R) PRO/Wireless 2915ABG Network Connection User Guide

- [Connecting to a wireless network](#)
 - [Connect to a wireless network without security](#)
 - [Connect to a wireless network with WEP security](#)
 - [Connect to a wireless network using a profile](#)
 - [Scan for available networks](#)
 - [Configure a Linksys \(EOU\) Access Point](#)
 - [Intel\(R\) PROSet/Wireless Configuration Service](#)
-

Connecting to a wireless network

You can connect to a wireless network using any one of the following ways.

- **Automatic Connection:** Automatically connect to an available network using an existing profile as specified in the order of the Profiles List.
 - **Activate Profile:** Select a profile from the Profiles List and click Connect. If a connection is made, a [balloon prompt](#) is displayed at the task tray.
 - **Manually Connect:** Select a network from the list of available networks and click **Configure** to launch the Profile Wizard. You can then create a profile.
-

Connect to a wireless network without security

To connect to a wireless network without security:

1. Click **Refresh**. The available wireless networks display in the Available network list.



NOTE: If your wireless adapter receives a blank network name (SSID) from a stealth access point, both the blank SSID and <no profile> display in the Available networks list. After connection both the blank SSID and the associated SSID display in the Available networks list and the Profiles List.

2. Select a wireless network from the list of available networks click **Configure**.
 3. The Connect one-time to: <name of network> page is displayed.
 4. The Profile Wizard General Settings page displays. The Wireless Network Name (SSID) displays. The profile name uses the same name as the wireless network name (SSID). To use a different profile name, enter the new name in the Profile Name text box.
 5. Click **Next**. The Security Settings page displays.
 6. Click **Yes, I want to connect to this network, I know it is open**.
 7. The next Security Settings page displays the current security status for the network access point. Click **Skip** or **OK** to save the settings and close the Security Settings page.
 8. The profile displays in the Profiles List and is positioned at the bottom of the list. Use the Profiles 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.
 9. Select the profile and click **Activate** to connect to the selected 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.
-

Connect to a wireless network with WEP security

To connect to a wireless network with WEP security:

1. Click **Refresh**. The available wireless networks display in the Available network list.



NOTE: If your wireless adapter receives a blank network name (SSID) from a stealth access point, both the blank SSID and <no profile> display in the Available networks list. After connection both the blank SSID and the associated SSID display in the Available networks list and the Profiles List.

2. Select a wireless network from the list of available networks and double-click the network name or click **Connect**. The Profile Wizard General Settings page displays. The Wireless Network Name (SSID) displays. The profile name uses the same name as the wireless network name (SSID). To use a different profile name, enter the new name in the Profile Name text box.
 3. Click **Next**. Intel(R) PROSet/Wireless determines the required security settings for the selected network.
 4. The Security Settings page displays the network security settings. Enter the required WEP security key information and click **OK** to save the settings and close the Security Settings page.
 5. The profile displays in the Profiles List and is positioned at the bottom of the list. Use the Profiles List arrows to position the profile in the list. If the profile is positioned at the top of the list, it automatically is connected to the network the next time the wireless network is detected.
 6. Select the profile and click **Activate** to connect to the selected 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.
-

Connect to a wireless network using a profile

To connect to a wireless network using a profile:

1. Select the profile from the Profiles List.
2. 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. Click the Details button to display details of the current network connection.



NOTE: For a list of available access points on a particular wireless network, click the **Properties** button on the main window. Refer to [Network Properties](#) for details.

Scan for available networks

Use the Refresh button to detect any available network within the range of your wireless adapter. When an available network is found, select the network name from the Available Networks list. If the adapter is currently connected to a network access point, the current wireless connection is still maintained while scanning for available networks.

- If the wireless adapter receives a blank network name (SSID) from a stealth access point, both the blank SSID and <no profile> display in the available networks list. To associate with a stealth access point, a new profile must first be created. Click the **Connect** button to launch the Profile Wizard, then create a profile for the selected wireless network. After connection both the blank SSID and the associated SSID can be viewed in the Profiles List.

Setting up a Linksys Access Point

[Configure a Linksys \(EOU\) Access Point](#)

The Intel(R)Smart Wireless Solutions feature Linksys(R) access point with the Ease of Use (EOU) feature enables you to configure a secure wireless connection from your Intel(R) Centrino(TM) wireless laptop computer. The feature automatically launches the **Intel(R) Wireless Network Configuration Wizard** on your Intel Centrino wireless laptop when a Linksys (EOU) access point is within range of your wireless adapter. The Configuration Wizard guides you through setting up a secure wireless network using Wi-Fi Protected Access (WPA). You can also assign a unique name to your wireless network.

Linksys (EOU) features

- Setup a secure wireless network using WPA
- Setup your wireless network with a new network name and no security (Anyone can access my network).

The Linksys Access Point is setup with factory defaults, which include no security (open authentication) and **linksys-g** as the network name (SSID). In this state, your wireless network is not secure and allows others to easily monitor any data transfer over the wireless link.

Configure a Linksys (EOU) Access Point

To configure a Linksys Access Point from your Intel Centrino laptop computer:

Wireless Network Configuration Wizard - Step 1

Welcome to Wireless Network Configuration

This dialog box displays when a Linksys (EOU) access point is within the range of your wireless adapter and starts the first step to establish a secure wireless connection with your Intel Centrino laptop computer.

- **Do not launch this Wizard again:** Click to postpone this process to a later time.



NOTE: You can re-enable this feature in the Intel PROSet/Wireless [Application Settings](#).

1. Click **Next** to continue.

Verify Ownership of your Linksys Access Point - Step 2

The ownership identification step prevents the wizard from trying to configure the wrong wireless device.

The character ownership key must be verified before your notebook can communicate with the access point.

2. Find the Ownership ID and Device ID key printed on the bottom of your Linksys Access Point or Wireless Router and enter it in the appropriate box.
 - **Ownership ID:** Enter the eight-character ownership identification key.
 - **Device ID:** Enter the eight-character device identification key



NOTE: A Linksys access point without an ownership identification key printed on it does not support the Intel(R) Smart Wireless Solutions feature and cannot be configured using the Configuration Wizard. Click **Cancel** to close the Configuration Wizard and refer to your Linksys User Guide.

3. Click **Next** to continue.

Enter New Configuration for Linksys Access Point - Step 3

4. To complete the configuration information, add the following network and security information.

Enter Network Name (SSID):

- **What is the Network Name:** Enter a network name (SSID) that identifies this wireless network. You can use a simple pass phrase such as Jerry's Wireless Network or OfficeWLAN or use a more secure stronger network name such as Main!<Office>\$WLAN.
- The Network Name can be up to 32 characters long. You may use upper- and lower-case letters, numbers, spaces, and most special characters. Avoid these characters - \ / : * ? < > | "

Securing your Network

Select one of the following options:

- **No security. Anyone can access my wireless network.**
- **WPA-Personal Security (8 to 63 alphanumeric characters).**

WPA is a security system that encrypts the data sent "over the air" on a wireless network so that only those users that know the Pass Phrase can access the network or interpret the transmitted data.

- **What is a Pass Phrase?** The Pass Phrase is used to create constantly changing keys that encrypt the data that is transmitted between wireless devices. The Pass Phrase that you enter here is used in the Linksys wireless device and this Intel Centrino laptop computer. If you have other WPA compliant wireless devices, the same Pass Phrase must be entered into each of them.

Enter a Pass Phrase

Choose a **simple** or **strong** pass phrase (password) that is easy to remember. Enter at least 10 alphanumeric characters or more (a-z, A-Z, 0-9) and one special character from (! \$ % ^ * () - _ = + [] : < . > ?)

Write the pass phrase down on a piece of paper or save it in a text file on your laptop computer in case you forget it. This password is used by other wireless devices to connect to this wireless network. If you do not specify a Pass Phrase, the default Pass Phrase is used. This Pass Phrase is used to encrypt and transmit data securely over the wireless link between your Intel Centrino laptop computer and the Linksys access point.

5. Click **Next**. A status dialog box displays while the Linksys Access Point is being configured.

Wireless Configuration Complete - Final Step

The Configuration Wizard has successfully completed setting up your Linksys access point. You can now establish a secure wireless connection from your Intel Centrino laptop computer.

6. **Configure my Broadband (DSL/Cable) Settings:** Click to launch a configuration web page after you click **Finish**. This web page provides advanced options such as Internet and Broadband settings.
7. Click **Finish** to close the Configuration Wizard.

Intel PROSet/Wireless Configuration Service

This page is displayed if an available wireless network access point or hotspot is detected within range of your computer, and there is no matching profiles found in the profile list. If balloon prompts are enabled, this page is shown when you click the [Task Tray Balloon message prompt](#).

Name	Description
Available Networks	The available Network Names and Icons display the type of available network. Note: If the wireless adapter receives a blank network name (SSID) from a stealth access point <SSID not broadcast> is displayed in the list. To associate with a stealth access point, a new profile must first be created. Click the Configure button to launch the Profile Wizard, then create a profile for the selected network. After connection both the blank SSID and the associated SSID can be viewed in the available networks list.
Do not show this again	Normally this checkbox is not shown. It is only displayed when the Display available networks when not associated setting is checked in Application Settings. If it is displayed you can check this box to stop the dialog box from displaying again.
Configure	Configure the selected wireless network.
Close	Close the Configuration Service page.
Help?	Displays the help information for this page.

Intel PROSet/Wireless Configuration Service Overview

[About the Configuration Service](#)

[Other Wireless Managers](#)

The Intel Wireless Network Configuration Service provides automatic wireless connection to available wireless networks using profiles created and prioritized in the Profiles list. This feature is constantly monitoring in the background the connection status of the wireless adapter. If no matching profiles are found in the Profiles list for an available network, a balloon prompt is displayed indicating that wireless networks are available. If you clicks the balloon prompt, the **Connect to a wireless network** dialog is displayed. From this dialog you can select an available network and click **Configure** to configure the wireless network for connection.

About the Configuration Service

- The Configuration Service is launched when you log on to your computer.
- Available networks are automatically connected when a matching profile is found in the Profile list.
- Once the adapter is connected to a wireless network, if a network with a higher priority profile becomes available, the current connection is not disconnected. You may manually connect to that higher profile by selecting the profile in Intel PROSet/Wireless and clicking **Connect**.
- The service is only available if the Intel PROSet/Wireless software is installed.
- If a connection to a wireless network cannot be made using any of the profiles in the Profiles List, then you are notified of available networks.
- If there are multiple profiles listed for an available network, you are prompted to choose which profile to connect.

Other Wireless Managers

If the Wireless Network Configuration Service detects another software application trying to communicate with the wireless device, you are notified of this behavior.

Windows XP Wireless Manager

To switch from Intel PROSet/Wireless to the Windows XP wireless manager use either of the following methods:

- **From the Task Tray Menu:**

Click **Use Microsoft client** to switch to using Windows XP Wireless Zero Configuration. Selecting this option disables Intel PROSet/Wireless as your current wireless manager. You can then configure your connection using Windows XP.

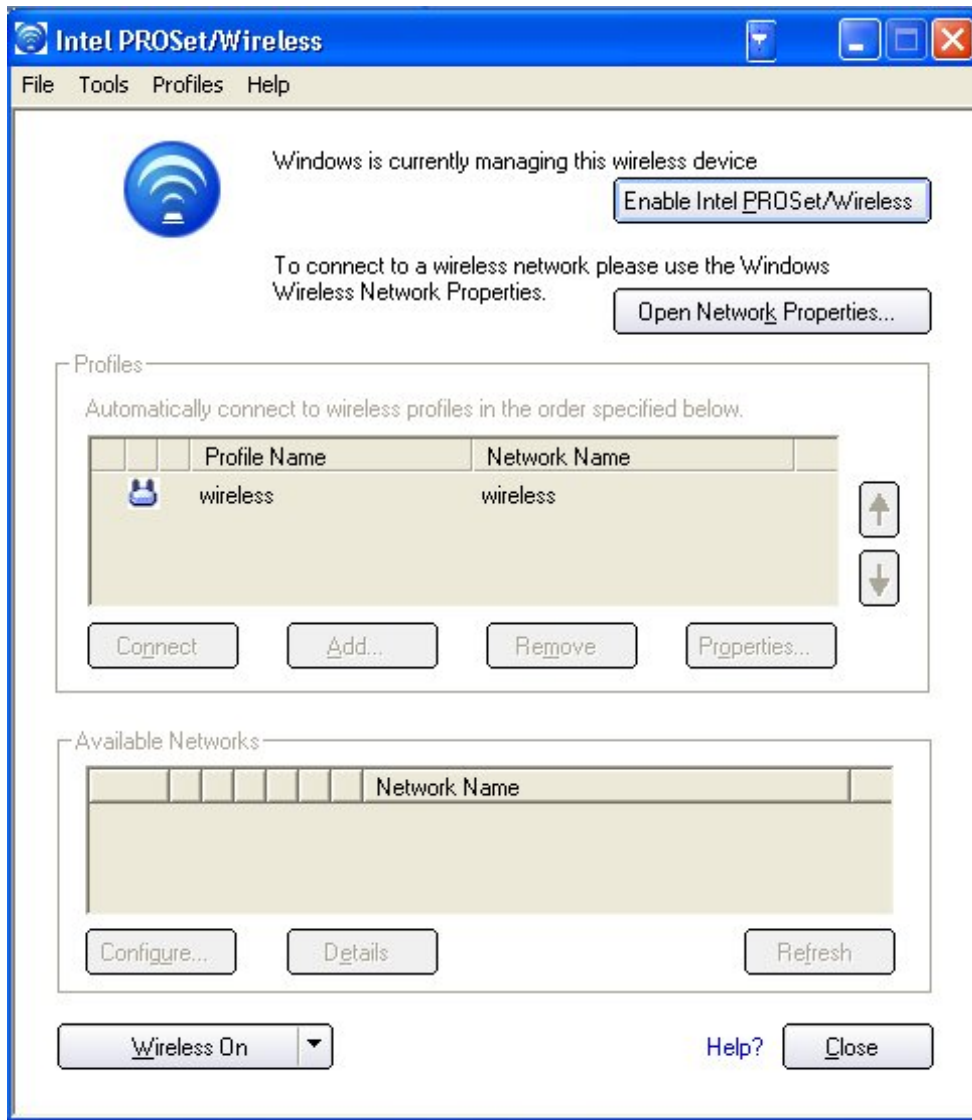


NOTE: Any wireless profiles created in Intel PROSet/Wireless are not visible by Windows XP Wireless Zero Configuration. If you want to use your Intel wireless profiles you need to switch back to using Intel PROSet/Wireless by selecting the **Use Intel/PROSet/Wireless** task tray menu option.

To enable Intel PROSet/Wireless as your wireless manager, click **Use Intel PROSet/Wireless** from the task tray options.

- **From Intel PROSet/Wireless:**

From, the Tools menu, click **Use Microsoft client** in the Intel PROSet/Wireless application. When you are finished using the Microsoft client, you can switch back by clicking **Enable Intel PROSet/Wireless**.



3rd Party Wireless Software

If you are using software provided by a hotspot location (coffee shop, airport terminal), the Configuration Service notifies you and then disables itself. It cannot manage the wireless device when another wireless manager is communicating with the wireless device. To take advantage of the Intel PROSet/Wireless features you want to disable or remove this software when you leave the hotspot.

When you are finished using the 3rd party wireless software, the Configuration Service is re-enabled automatically when you suspend or restart the computer. If you want to manually enable the Configuration Service, you can open Intel PROSet/Wireless and click **Enable Intel PROSet/Wireless**.

[Back to Contents](#)

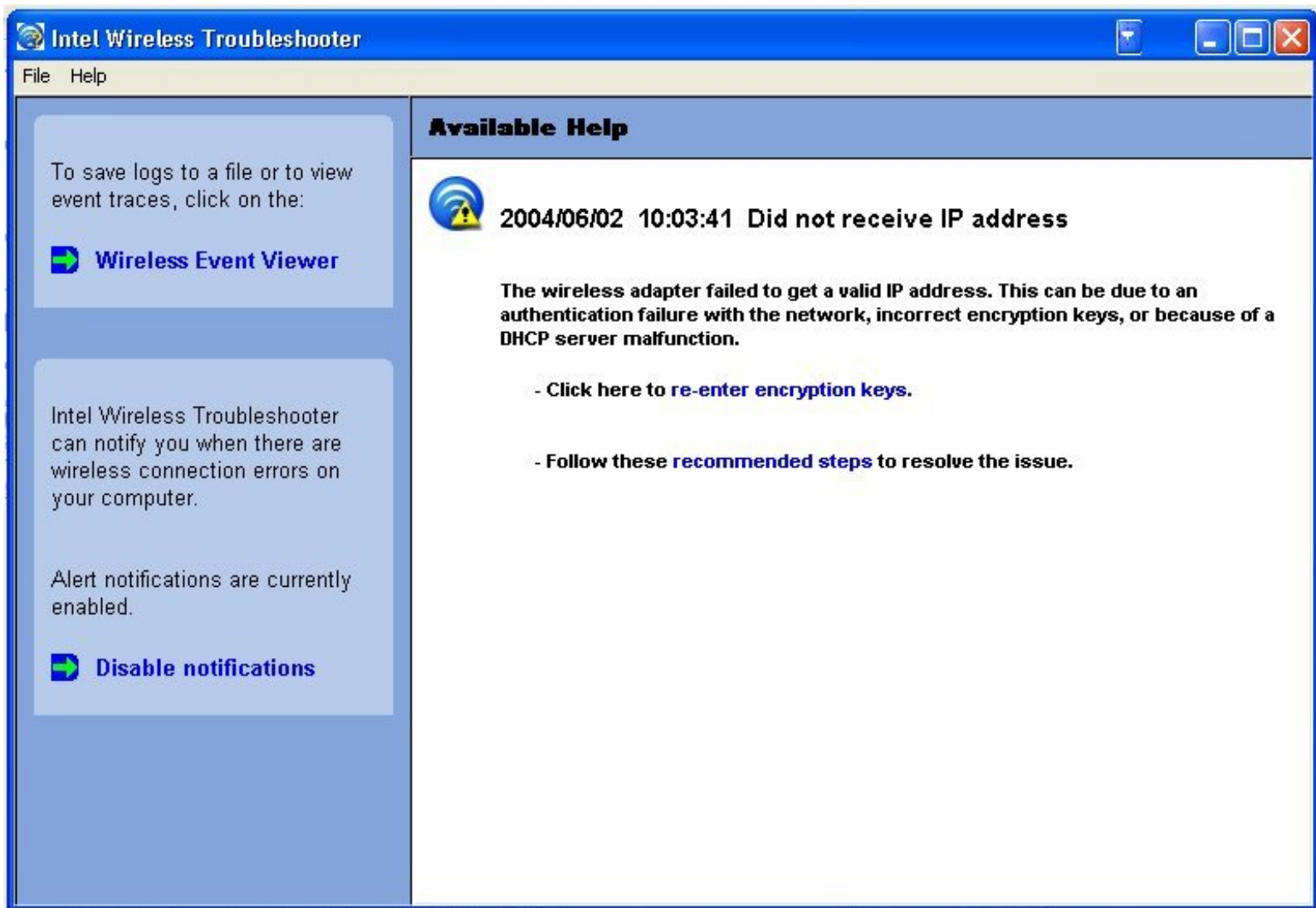
[Trademarks and Disclaimers](#)

[Back to Contents](#)

Troubleshooting: Intel PRO/Wireless 2915ABG Network Connection User Guide

- [Intel Wireless Troubleshooter](#)
- [Event Viewer](#)
- [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. Once you click on the balloon tip, a diagnostic message displays the recommended steps to resolve the occurred connection issue. For example, if a connection issue occurred because of an invalid password, the Profile Wizard application is launched when you click on a displayed hyperlink. You can also launch [Wireless Event Viewer](#) from this page and enable or disable alert notifications. The Intel Wireless Troubleshooter is supported under Windows XP and 2000.

Intel Wireless Troubleshooter Description

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 parts. The error message and time stamp are preceded by an icon. The hint text part contains description about available utilities and help for resolving the associated connection issue. If you click on a help text link, the help text is displayed in a pop-up window. If you click on the associated issue resolver link, a program is launched to resolve the connection issue. You can launch [Wireless Event Viewer](#) or enable or disable from the last pane.

File	Exit: Exit Intel Wireless Troubleshooter application.
Help	Intel(R) 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 <ul style="list-style-type: none"> • Description of error • Link to resolve error (if available). See Resolving Errors below. • Link to recommended steps to resolve error

Wireless Event Viewer

Level	Description	Date and Time
Information	Intel® Wireless Troubleshooter s...	2004/06/02 10:04:07
Error	Did not receive an IP address fro...	2004/06/02 10:03:41
Information	Profile MyProfile for Socrates bei...	2004/06/02 10:02:07
Information	Profile wireless for wireless being ...	2004/06/02 10:01:45
Information	Profile wireless for wireless being ...	2004/06/02 10:01:00
Information	AcStatusNoStatusChange	2004/06/02 10:00:36
Information	Profile wireless for wireless being ...	2004/06/02 10:00:36
Information	AcStatusNoStatusChange	2004/06/02 10:00:16
Information	Profile @direct@ for <No current ...	2004/06/02 10:00:16

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. In addition, you can email the binary format log file to an email address (pre-configured with a default email address) when network connection is available. Wireless Event Viewer is supported under Windows XP and 2000. To launch Wireless Event Viewer, click **Start > Programs > Intel PROset Wireless > > Intel PROset Wireless > Tools > Intel Wireless Troubleshooter > Wireless Event Viewer**.

Name	Description
File	<p>Preferences: Change the name of the log file by selecting the Preferences menu item. Click to display the Preference dialog.</p> <ul style="list-style-type: none"> • The available logs will be saved to the following file: The current file name is displays in the editable text box. The default location is the desktop. <p>Browse button: Specify a new fully qualified file name. OK button: Close the dialog and apply the new changes. Cancel button: Close the dialog without applying any changes.</p> <p>Exit: Exit Intel Wireless Troubleshooter.</p>
Level	<p>The severity level of the connection issue is indicated by an icon. The severity levels are:</p> <ul style="list-style-type: none"> • Information • Error • Warning
Description	Brief description of the connection issue.
Date and Time	Date and time of the detected connection issue. This field can be sorted in ascending or descending order. Click the column header to sort the displayed events.

Save As	Save the available logs to the pre-defined file name. Everything in the log shall be saved to the predefined file name. The default file name is: Product_Name_Month_Day_Year_HH_MM_SS.binary_file_ext The default file name format can be changed to another name.
Clear	Removes the information in the Wireless Event Viewer.
Help?	Displays the help information for this dialog.

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](#)
- [The wireless adapter failed to get a valid IP address](#)
- [Authentication failed because timer expired](#)
- [Smart Card was unexpectedly removed](#)
- [Disconnection from an Access Point](#)
- [Error Occurred Because the GSM Adapter Was Unexpectedly Removed](#)
- [The AAA Server Rejected the EAP Method](#)
- [An Administrator Profile Failed to Authenticate](#)
- [An 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. Select a TTLS or PEAP profile from the profiles list.
2. Click **Properties**.
3. Click **Next**.
4. Select **TTLS** or **PEAP** for the 802.1x Authentication Type.
5. Select the **Use the following** option for User Credentials.

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.

7. Click the **OK** button to save the settings.

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 the **Use the following** option 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.
- For LEAP profiles: Select the **Use the following user name and password** option 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. Click the **OK** button to save the settings.

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.
 - Verify the 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.
- For LEAP profiles: Select the **Use the following user name and password** option and verify the password information. 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. Click the **OK** button to save the settings.

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, then click the **Select** button and select another certificate from the list of installed certificates and click **OK**.
 - For TLS profiles: Click the **Select** button and select another certificate from the list of installed certificates and 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. Click the **OK** button to save the settings.

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 the **Use the following** option 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.
 - For LEAP profiles: Select the **Use the following user name and password** option and verify the Domain information. If **Use Windows logon user name and password** or **Prompt for user name and password** is selected make sure that the correct Domain information is used when you connect to the wireless network.
 5. Click the **OK** button to save the settings.
-

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. Click **OK** to save the settings.
-

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, then click the **Select** button and select another certificate from the list of installed certificates and click **OK**.
 - For TLS profiles: Click the **Select** button and select another certificate from the list of installed certificates and 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. Click **OK** to save the settings.

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 a response from the authentication server.

Recommended action:

Select the profile and click **Connect** and try to associate with the network and authenticate with the server.

The 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.

Use the following steps to resolve this error:

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

Authentication failed because timer expired

Authentication failed because timer expires while this mobile station authenticating against a possible rogue AP. The Rogue AP timed out, possibly because of a problem with the RADIUS server.

Recommended action:

1. To prevent the wireless adapter from connecting with this possible Rogue AP, consider adding this Rogue AP to the [excluded access point list](#).
 2. Select the profile and click the **Connect** button 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 and click **Connect** to try to associate with the network.
-

Disconnection from an Access Point

The following error messages display when the wireless adapter is disconnected from the network access point.

Disconnect from access point due to failed associations.

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).

Error Occurred Because the GSM Adapter Was Unexpectedly Removed

This error occurs when the GSM adapter is not fully inserted or 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 **Connect**. The profile is now re-applied. Intel PROSet/Wireless attempts to connect to the wireless network.
-

The 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(R) 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.

Use the following steps to help resolve this error:

1. Double click on Intel PROSet/Wireless icon at the bottom right of the screen.
 2. From the Tools menu, select **Administrator Tool**.
 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.
-

An Administrator 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 **Administrator Tool**.
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(R) PROSet/Wireless attempts to connect to the wireless network.

[Back to Contents](#)

[Trademarks and Disclaimers](#)

[Back to Contents](#)

Wireless Network Overview: Intel(R) PRO/Wireless 2915ABG Network Connection User Guide

About Wireless Network Technology

- [Choosing a Wireless Network](#)
- [Configuring a Wireless Network](#)
- [Identifying a Wireless Network](#)

A wireless network connects computers without using network cables. Computers use radio communications to send data between each other. You can communicate directly with other wireless computers, or connect to an existing network through a wireless access point. When you set up your wireless adapter, you select the operating mode for the kind of wireless network you want. You can use your Intel® PRO/Wireless Network Connections adapter to connect to other similar wireless devices that comply with the 802.11 standard for wireless networking.<

Choosing a Wireless Network Mode

Wireless networks can operate with or without access points, depending on the number of users in the network. Infrastructure mode uses access points to allow wireless computers to send and receive information. Wireless computers transmit to the access point, the access point receives the information and rebroadcasts it to other computers. The access point can also connect to a wired network or to the Internet. Multiple access points can work together to provide coverage over a wide area.



Device-to-Device mode, also called Ad Hoc mode, works without access points and allows wireless computers to send information directly to other wireless computers. 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.



Configuring a Wireless Network

There are three basic components that must be configured for an 802.11 wireless network to operate properly:

- **Network Name**—Each wireless network uses a unique Network Name to identify the network. This name is called the Service Set Identifier (SSID). When you set up your wireless adapter, you specify the SSID. If you want to connect to an existing network, you must use the name for that network. If you are setting up your own network you can make up your own name and use it on each computer. The name can be up to 32 characters long and contain letters and numbers.
- **Profiles**—When you set up your computer to access a wireless network, Intel(R)PROSet/Wireless creates a profile for the wireless settings that you specify. If you want to connect to another network, you can scan for existing networks and make a temporary connection, or create a new profile for that network. After you create profiles, your computer will automatically connect when you change locations.
- **Security**—The 802.11b wireless networks use encryption to help protect your data. Wired equivalent privacy (WEP) uses a 64-bit or 128-bit shared encryption key to scramble data. Before a computer transmits data, it scrambles the data using the secret encryption key. The receiving computer uses this same key to unscramble the data. If you are connecting to an existing network, use the encryption key provided by the administrator of the wireless network. If you are setting up your own network you can make up your own key and use it on each computer.

Identifying a Wireless Network

Depending on the size and components of a wireless network, there are many ways to identify a wireless network:

- **The Network Name or Service Set Identifier (SSID)**—Identifies a wireless network. All wireless devices on the network must use the same SSID.
 - **>Extended Service Set Identifier (ESSID)**—A special case of SSID used to identify a wireless network that includes access points.
 - **Independent Basic Service Set Identifier (IBSSID)**—A special case of SSID used to identify a network of wireless computers configured to communicate directly with one another without using an access point.
 - **Basic Service Set Identifier (BSSID)**—A unique identifier for each wireless device. The BSSID is the Ethernet MAC address of the device.
 - **Broadcast SSID**—An access point can respond to computers sending probe packets with the broadcast SSID. If this feature is enabled on the access point, any wireless user can associate with the access point by using a blank (null) SSID.
-

[Back to Contents](#)

[Back to Contents](#)

Specifications: Intel PRO/Wireless 2915ABG Network Connection User Guide

- [Intel PROSet/Wireless 2915ABG Network Connection](#)
- [Intel PROSet/Wireless 2200BG 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 Contents](#)

[Trademarks and Disclaimers](#)

Glossary of Terms: Intel(R) PRO/Wireless 2915ABG Network Connection User Guide

Glossary

[Numerical](#) [A](#) [B](#) [D](#) [E](#) [F](#) [I](#) [K](#) [M](#) [O](#) [P](#) [R](#) [S](#) [T](#) [U](#) [W](#)

Numerical

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: The 802.11b standard specifies a maximum data transfer rate of 11Mbps, an operating frequency of 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.

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.

A

Access Point: A device that serves as a communications hub for wireless clients and provides a connection to a wired LAN.

Advanced Encryption Standard (AES): A federal information-processing standard, supporting 128-, 192-, and 256-bit keys.

B

Basic Service Set Identifier (BSSID): A unique identifier for each wireless client on a wireless network. The BSSID is the Ethernet MAC address of each adapter on the network.

Bit Rate: The total number of bits (ones and zeros) per second that a network connection can support. Note that this bit rate varies, under software control, with different signal path conditions.

Bluetooth: An incompatible, very short-range lower speed communications system (PAN), developed first in Europe as a “cable replacement” for printers and similar peripheral connections. Its usage has expanded to

include cordless earphones and similar devices. It uses the 2.4 GHz ISM band, and “co-exists” with 802.11b. Here the term, “co-exist” means that not all researchers agree on the amount of mutual interference generated when both systems operate in the same location.

Broadcast SSID: Used to allow an access point to respond to clients on a wireless network by sending probes.

D

Data Rate (Information Rate): Not all bits carry user information. Each group (packet) of bits contains headers, trailers, echo control, destination information, and other data required by the transmission protocol. It is important to understand the difference between bit rate and data rate, since the overhead information may consume more than 40% of the total transmission. This difference is common to many such data systems, including Ethernet.

Device-to-Device Mode: A wireless network structure that allows wireless clients to communicate with each other without using an access point.

Direct-Sequence Spread Spectrum (DSSS) and Frequency-Hop Spread Spectrum (FHSS): Two incompatible technologies used in radio transmission.

Dynamic IP Address: An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such as servers and printers, are usually assigned static IP addresses.

E

Extensible Authentication Protocol (EAP): An IETF standard that establishes an authentication protocol for network access. Many authentication methods, including passwords, certificates, and smart cards, work within this framework.

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 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.

EAP-TTLS: A type of authentication method using the Extensible Authentication Protocol (EAP) and Tunnelled Transport Layer Security (TTLS). EAP-TTLS uses a combination of certificates and another method, such as passwords. It is more secure than MD5 authentication, which uses passwords, and less secure than EAP-TLS authentication, which exclusively uses certificates. EAP-TTLS authentication supports dynamic WEP key management.

Encryption: Scrambling data so that only the authorized recipient can read it. Usually a key is needed to decrypt the data.

Extended Service Set Identifier (ESSID): A type of unique identifier applied to both the AP and the wireless PC Card that is attached to each packet. This allows the AP to recognize each wireless client and its traffic.

F

Firewall: A firewall is a set of related programs, located at a network gateway server, that protects the resources of a network from users from other networks.

Frequencies: Strike a piano key and you generate a tone. Pick up the tone with a microphone and your tone turns in to a “vibrating” or “cycling” electronic signal. The rate of vibration depends on the key struck. In electronics we refer to this rate of vibration as the number of “cycles per second.” The formal term for this value is Hertz. As we move up in rate, such as in the Broadcast Band, we can use KiloHertz (KHz) to represent 1,000 Hz, or Megahertz (MHz) to represent 1,000,000 Hz. Continuing much further upward, we finally reach 1,000,000,000 Hz, which we can fortunately shorten to a Gigahertz (GHz). These frequencies are the home of both 802.11a (5 GHz) and 802.11b (2.4 GHz).

I

Independent Basic Service Set Identifier (IBSSID): Used to identify a wireless network configured to allow each wireless client to communicate directly with each other without an access point.

Independent Network: A network that provides (usually temporarily) peer-to-peer connectivity without relying on a complete network infrastructure.

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.

Institute of Electrical and Electronics Engineers (IEEE): An organization involved in setting computing and communications standards.

ISM Bands: A series of frequency bands, set aside by the FCC for Industrial, Scientific and Medical applications. Users of these bands operate equipment on a shared basis, meaning that they must expect, and accept interference from other legal users. Products manufactured for ISM Band use must be approved by the FCC, but the user does not have to be licensed. In addition to WLAN, ISM bands support cordless phones, microwave ovens, baby monitors, toys, ham radio transceivers, and other wireless services.

K

Kerberos: An authentication system enabling protected communication over an open network using a unique key called a ticket.

M

Media Access Control (MAC) Address: A hardwired address applied at the factory. It uniquely identifies network hardware, such as a wireless PC Card, on a LAN or WAN.

Microcell: A bounded physical space in which a number of wireless devices can communicate. Because it is possible to have overlapping cells as well as isolated cells, the boundaries of the cell are established by some rule or convention.

Microwave: Technically, the term describes any frequency above 1.0 GHz.

Multipath: The signal variation caused when radio signals take multiple paths from transmitter to receiver.

O

Orthogonal Frequency Division Multiplexing (OFDM): A modulation technique for transmitting large amounts of digital data over radio waves. 802.11a and 802.11g use OFDM.

P

Personal Area Network (PAN): A personal area network, or PAN, is a networking scheme that enables computing devices such as PCs, laptop computers, handheld personal computers, printers and personal digital assistants (PDAs) to communicate with each other over short distances either with or without wires.

Preamble: A preliminary signal transmitted over a WLAN to control signal detection and clock synchronization.

R

Radio Frequency (RF) Terms (GHz, MHz, Hz): 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.

Range: The distance over which a given system can communicate.

RC4: An encryption algorithm designed at RSA Laboratories; specifically, a stream cipher of pseudo-random bytes that is used in WEP encryption.

Remote Authentication Dial-In User Service (RADIUS): An authentication and accounting system that verifies users' credentials and grants access to requested resources.

Roaming: Movement of a wireless node between two microcells. Roaming usually occurs in infrastructure networks built around multiple access points.

S

Service Set Identifier (SSID): Used to identify clients on a wireless network.

Shared key: An encryption key known only to the receiver and sender of data.

Static IP Address: A permanent IP address that is assigned to a node in a TCP/IP network.

T

Transmission Control Protocol (TCP): A method (protocol) used with the IP (Internet Protocol) to send data in the form of message units between network devices over a LAN or WAN. The IP carries the delivery of the data (routing), and TCP keeps track of the individual units of data (called packets) that a message is divided into for delivery over the network.

Transmission Control Protocol/Internet Protocol (TCP/IP): The basic communication language or set of protocols for communications over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols and not only TCP and IP.

Transceiver: A commonly used term that describes a combination transmitter and receiver. Both 802.11a and 802.11b devices would be properly described as data transceivers.

U

UNII Bands: Unlicensed National Information Infrastructure. In contrast to the ISM bands, these are a group of frequency bands set aside by the FCC for WLAN type communications only. Users must accept interference from other legal WLAN users, but the other sources of interference problems are, or legally should be, missing.

W

WEP64 and WEP128: Wired Equivalent Privacy, 64-bit 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. It is recommended to use the 128-bit option at all possible times. Remember that 802.11 devices transmit (broadcast) in all directions, and that it is possible, with very complex software, to copy and decode WEP transmissions. The task is not trivial, but it is possible. If your data is extremely sensitive, you should consider some form of secondary protection, such as strong passwords and an additional level of encryption. Suitable software packages are available from reputable suppliers. Although not intended by the original architects, WEP also helps prevent unauthorized access to your system by an outsider. Hackers have been known to access systems from outside a building, and to then to access the Web for a leisurely session, all at the system owner's expense.

Wide Area Network (WAN): A wide area network (WAN) is a voice, data, or video network that provides connections from one or more computers or networks within a business to one or more computers or networks that are external to such business.

Wireless: A microwave transceiver system.

Wireless Network: Wireless LAN is a type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. WLAN is a flexible data communication system used as an alternative to, or an extension of a wired LAN.

Wireless Node: A user computer with a wireless network interface card (adapter).

[Back to Contents](#)

[Back to Contents](#)

Customer Support: Intel(R) PRO/Wireless 2915ABG Network Connection User Guide

Customer Support

A banner image for Intel support. On the left, a hand holds a glowing sphere with an Intel processor chip inside. On the right, the text reads "welcome to support for Intel consumer products".

welcome to
support
for Intel consumer products

- **get technical help**
Select your product type at the left to find solutions, specifications, compatibility information and documentation.
- **download software, drivers and utilities**
- **search the support site**

Intel support is available online or by telephone. Available services include the most up-to-date product information, installation instructions about specific products, and troubleshooting tips.

Online Support

Technical Support: <http://support.intel.com>

Network Product Support: <http://www.intel.com/network>

Corporate Web Site: <http://www.intel.com>

[Back to Contents](#)

[Back to Contents](#)

Regulatory Information: Intel(R)PRO/Wireless 2915ABG Network Connection User Guide

Supported on the Intel(R) PRO/Wireless 2915ABG Network Connection and Intel(R) PRO/Wireless 2200BG Network Connection Hardware

[Intel\(R\) PRO/Wireless 2915ABG Network Connection](#)

[Information for the User](#)

[Regulatory Information](#)

[Intel\(R\) PRO/Wireless 2200BG Network Connection](#)

[Information for the User](#)

[Regulatory Information](#)

Intel(R) PRO/Wireless 2915ABG Network Connection

The information in this document applies to the following products:

Tri-mode wireless LAN adapters (802.11a/802.11b/802.11g)

Intel(R) PRO/Wireless 2915ABG Network Connection (model WM3B2915ABG)

Intel(R) PRO/Wireless 2915ABG Network Connection (model WM3A2915ABG)



NOTE: Due to the evolving state of regulations and standards in the wireless LAN field (IEEE 802.11 and similar standards), the information provided herein is subject to change. Intel Corporation assumes no responsibility for errors or omissions in this document. Nor does Intel make any commitment to update the information contained herein.

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(R) PRO/Wireless

2915ABG Network Connection 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.
- Antenna use:
 - In order to comply with FCC RF exposure limits, low gain integrated antennas should be located at a minimum distance of 20 cm (8 inches) or more from the body of all persons.
 - High-gain, wall-mount, or mast-mount antennas are designed to be professionally installed and should be located at a minimum distance of 30 cm (12 inches) or more from the body of all persons. Please contact your professional installer, VAR, or antenna manufacturer for proper installation requirements.
- 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(R) PRO/Wireless 2915ABG Network Connection 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:** Intel(R) PRO/Wireless LAN products are 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.

Other Wireless Devices

Safety Notices for Other Devices in the Wireless Network: Refer to the documentation supplied with wireless Ethernet adapters or other devices in the wireless network.

Local Restrictions on 802.11a and 802.11b Radio Usage

 **Caution:** Due to the fact that the frequencies used by 802.11a and 802.11b wireless LAN devices may not yet be harmonized in all countries, 802.11a and 802.11b products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. 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. The device transmit power control (TPC) interface is part of the Intel(R) PROSet/Wireless software. Operational restrictions for Equivalent Isotropic Radiated Power (EIRP) are provided by the system manufacturer. Any deviation from the permissible power and frequency settings for the country of use is an infringement of national law and may be punished as such.

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

Wireless interoperability

The Intel(R) PRO/Wireless 2915ABG Network Connection adapter is designed to be interoperable with other wireless LAN products that are based on direct sequence spread spectrum (DSSS) radio technology and to comply with the following standards:

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

The Intel(R) PRO/Wireless 2915ABG Network Connection adapter and your health

The Intel(R) PRO/Wireless 2915ABG Network Connection 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(R) PRO/Wireless 2915ABG Network Connection 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(R)

PRO/Wireless 2915ABG Network Connection 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(R) PRO/Wireless 2915ABG Network Connection adapter equipment on board airplanes, or
- Using the Intel(R) PRO/Wireless 2915ABG Network Connection 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(R) PRO/Wireless 2915ABG Network Connection adapter wireless device before you turn it on.

Regulatory information

Information for the OEMs and Integrators:

The following statement must be included with all versions of this document supplied to an OEM or integrator, but should not be distributed to the end user.

- This device is intended for OEM integrators only.
- This device cannot be co-located with any other transmitter.
- Please refer to the full Grant of Equipment document for other restrictions.
- This device must be operated and used with a locally approved AP.

Information To Be Supplied to the End User by the OEM or Integrator

The following regulatory and safety notices must be published in documentation supplied to the end user of the product or system incorporating an Intel(R) PRO/Wireless 2915ABG Network Connection in compliance with local regulations.

The Intel(R) PRO/Wireless 2915ABG Network Connection 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](#). Intel Corporation is not responsible for any radio or television interference caused by unauthorized modification of the devices included with the Intel(R) PRO/Wireless 2915ABG Network Connection adapter kit, or the substitution or attachment of connecting cables and equipment other than that specified by Intel Corporation. The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user. Intel Corporation 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.

Local Restriction of 802.11a and 802.11b Radio Usage

The following statement on local restrictions must be published as part of the compliance documentation for all 802.11a and 802.11b products.

Caution: Due to the fact that the frequencies used by 802.11a and 802.11b wireless LAN devices may not yet be harmonized in all countries, 802.11a and 802.11b products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. 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 permissible settings and restrictions in the country of use could be an infringement of national law and may be punished as such.

FCC Radio Frequency Interference Requirements

This device is restricted to indoor use due to its operation in the 5.15 to 5.25 GHz frequency range. FCC requires this product to be used indoors for the frequency range 5.15 to 5.25 GHz to reduce the potential for harmful interference to co-channel Mobile Satellite systems. High power radars are allocated as primary users of the 5.25 to 5.35 GHz and 5.65 to 5.85 GHz bands. These radar stations can cause interference with and /or damage this device.

- This device is intended for OEM integrators only.
- This device cannot be co-located with any other transmitter.

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(R) PRO/Wireless 2915ABG Network Connection adapter wireless network device is far below the FCC radio frequency exposure limits. Nevertheless, the Intel(R) PRO/Wireless LAN wireless network 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.

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(R) PRO/Wireless 2915ABG Network Connection 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.

Canada—Industry Canada (IC)

This device complies with RSS210 of Industry Canada.

This Class B digital apparatus complies with Canadian ICES-003, Issue 2, and RSS-210, No 4 (Dec 2000) and No 5 (Nov 2001).

Cet appareil numérique de la classe B est conforme à la norme NMB-003, No. 2, et CNR-210, No 4 (Dec 2000) et No 5 (Nov 2001)..

"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 Frequency Bands

2.400 - 2.4835 GHz (Europe ETSI)

5.15 - 5.35 GHz and 5.47-5.725 GHz (Europe ETSI)

5.15-5.25 can be used outdoors and all other 5 GHz supported must be indoors

Low band 5.25 - 5.35 GHz is for indoor use only

5.47 - 5.725 GHz is not allowed in Austria, France and Switzerland

Declaration of Conformity

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

English	Hereby, Intel(R) Corporation, declares that this Intel(R) PRO/Wireless 2915ABG Network Connection is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	Intel(R) Corporation vakuuttaa täten että Intel(R) PRO/Wireless 2915ABG Network Connection tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart Intel(R) Corporation dat het toestel Intel(R) PRO/Wireless 2915ABG Network Connection in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
	Bij deze verklaart Intel(R) Corporation dat deze Intel(R) PRO/Wireless 2915ABG Network Connection voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la présente Intel(R) Corporation déclare que l'appareil Intel(R) PRO/Wireless 2915ABG Network Connection est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
	Par la présente, Intel(R) Corporation déclare que ce Intel(R) PRO/Wireless 2915ABG Network Connection est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables
Swedish	Härmed intygar Intel(R) Corporation att denna Intel(R) PRO/Wireless 2915ABG Network Connection står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	Undertegnede Intel(R) Corporation erklærer herved, at følgende udstyr Intel(R) PRO/Wireless 2915ABG Network Connection overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF

German	<p>Hiermit erklärt Intel(R) Corporation, dass sich dieser/diese/dieses Intel(R) PRO/Wireless 2915ABG Network Connection in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW i)</p> <p>Hiermit erklärt Intel(R) Corporation die Übereinstimmung des Gerätes Intel(R) PRO/Wireless 2915ABG Network Connection mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)</p>
Greek	<p>ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Intel(R) Corporation ΔΗΛΩΝΕΙ ΟΤΙ Intel(R) PRO/Wireless 2915ABG Network Connection ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ</p>
Italian	<p>Con la presente Intel(R) Corporation dichiara che questo Intel(R) PRO/Wireless 2915ABG Network Connection è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE</p>
Spanish	<p>Por medio de la presente Intel(R) Corporation declara que el Intel(R) PRO/Wireless 2915ABG Network Connection cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE</p>
Portuguese	<p>Intel(R) Corporation declara que este Intel(R) PRO/Wireless 2915ABG Network Connection está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.</p>
Malti	<p>Hawnhekk, Intel(R) Corporation, jiddikjara li dan Intel(R) PRO/Wireless 2915ABG Network Connection jikkonforma mal- ti•ijiet essenzjali u ma provvedimenti o rajn relevanti li hemm fid-Dirrettiva 1999/5/EC</p>

New Member States requirements of Declaration of Conformity

Estonian	Käesolevaga kinnitab Intel(R) Corporation seadme Intel(R) PRO/Wireless 2915ABG Network Connection vastavust direktiivi 1999/5/EÜ põhinoüetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Hungary	Alulírott, Intel(R) Corporation nyilatkozom, hogy a Intel(R) PRO/Wireless 2915ABG Network Connection megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak
Slovak	Intel(R) Corporation týmto vyhlasuje, že Intel(R) PRO/Wireless 2915ABG Network Connection spĺna základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Czech	Intel(R) Corporation tímto prohlašuje, že tento Intel(R) PRO/Wireless 2915ABG Network Connection je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES."
Slovenia	Šiuo Intel(R) Corporation deklaruoja, kad šis Intel(R) PRO/Wireless 2915ABG Network Connection atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Latvian	Ar šo Intel(R) Corporation deklarē, ka Intel(R) PRO/Wireless 2915ABG Network Connection atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem
Lithuanian	Intel(R) Corporation deklaruoja, kad Intel(R) Pro/Wireless 2915ABG Network Connection atitinka 1999/5/EC Direktyvos esminius reikalavimus ir kitas nuostatas".

Polish

Niniejszym, Intel(R) Corporation, deklaruje, że Intel(R) PRO/Wireless 2915ABG Network Connection spełnia wymagania zasadnicze oraz stosowne postanowienia zawarte Dyrektywie 1999/5/EC.

France

For Metropolitan departments

2.400 - 2.4835 GHz for indoor use

2.400 -2.454 GHz (channels 1 to 7) for outdoor use

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	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 Network Connection card in more areas within France. Please check with ART for the latest information (www.art-telecom.co.fr)

For Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte:

2.400 - 2.4835 GHz for indoor and outdoor use.

For Reunion, Guyane:

2.400 - 2.4835 GHz for indoor use.

2.420 - 2.4835 GHz for outdoor use (channels 5 to 13)



NOTE: Your Intel(R) PRO/Wireless 2915ABG Network Connection adapter transmits less than 100 mW, but more than 10 mW

Italia

A license is required for indoor use. Outdoor use is prohibited.



NOTE: E' necessaria la concessione ministeriale anche per l'uso interno. Verificare con i rivenditori la procedura da seguire. L'uso per installazione in esterni non e' permessa.

Japan Frequency Bands

2.400 - 2.497 GHz (Japan)

5.15 to 5.25 (offset Japanese channels) active scan

High Band Frequencies

5.725 to 5.825 active scan

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 in the manufacture OEM Regulatory Guidance document.

Underwriters Laboratories Inc. (UL) Regulatory Warning

For use in (or with) UL Listed personal computers or compatible.

Regulatory Information: Intel(R) PRO/Wireless 2200BG Network Connection

[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(R) PRO/Wireless 2200BG Network Connection 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(R) PRO/Wireless 2200BG Network Connection 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(R) PRO/Wireless 2200BG Network Connection 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:** Due to the fact that 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 of designated use. 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, see the additional compliance information supplied with the product.

Wireless interoperability

The Intel(R) PRO/Wireless 2200BG Network Connection 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(R) PRO/Wireless 2200BG Network Connection 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(R) PRO/Wireless 2200BG Network Connection 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(R) PRO/Wireless 2200BG Network Connection 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(R) PRO/Wireless 2200BG Network Connection adapter equipment on board airplanes, or
- Using the Intel(R) PRO/Wireless 2200BG Network Connection 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(R) PRO/Wireless 2200BG Network Connection adapter wireless device before you turn it on.

Regulatory information

The Intel(R) PRO/Wireless 2200BG Network Connection 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(R) PRO/Wireless 2200BG Network Connection 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(R) PRO/Wireless 2915ABG Network Connection 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(R) PROSet/Wireless 2915ABG Network Connection adapter wireless network device is far below the FCC radio frequency exposure limits. Nevertheless, the Intel(R) PROSet/Wireless LAN wireless network 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 2 cm between you (or any other person in the vicinity) and the antenna that is built into the computer.

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(R) PRO/Wireless 2200BG Network Connection 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)

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 apaitis ths koinotikhhs 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

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 (<http://www.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 in the manufacture OEM Regulatory Guidance document.

[Back to Contents](#)

Warranty: Intel(R) PRO/Wireless 2915ABG Network Connection User Guide

Product Warranty Information

One-Year Limited Hardware Warranty

Limited Warranty

Intel warrants to the purchaser of the Intel® PROSet/Wireless 2915ABG Network Connection PCI Card (the “Product”), and software delivered with or as part of the Product, including without limitation, the Intel Wireless Connect Technology, unmodified and in its original sealed packaging (“Original Purchaser”), that the Product, if properly used and installed, will be free from defects in material and workmanship and will substantially conform to Intel’s publicly available specifications for the Product for a period of one (1) year beginning on the date the Product was purchased in its original sealed packaging.

SOFTWARE OF ANY KIND DELIVERED WITH OR AS PART OF THE PRODUCT IS EXPRESSLY PROVIDED "AS IS", SPECIFICALLY EXCLUDING ALL OTHER WARRANTIES, EXPRESS, IMPLIED (INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE), provided however, that Intel warrants that the media on which the software is furnished will be free from defects for a period of ninety (90) days from the date of delivery. If such a defect appears within the warranty period, you may return the defective media to

Intel for replacement or alternative delivery of the software at Intel's discretion and without charge. Intel does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the software.

If the Product which is the subject of this Limited Warranty fails during the warranty period for reasons covered by this Limited Warranty, Intel, at its option, will:

- **REPAIR** the Product by means of hardware and/or software; OR
- **REPLACE** the Product with another product, OR, if Intel is unable to repair or replace the Product,
- **REFUND** the then-current Intel price for the Product at the time a claim for warranty service is made to Intel under this Limited Warranty.

THIS LIMITED WARRANTY, AND ANY IMPLIED WARRANTIES THAT MAY EXIST UNDER APPLICABLE STATE, NATIONAL, PROVINCIAL OR LOCAL LAW, APPLY ONLY TO YOU AS THE ORIGINAL PURCHASER OF THE PRODUCT.

Extent of Limited Warranty

Intel does not warrant that the Product, whether purchased stand-alone or integrated with other products, including without limitation, semi-conductor components, will be free from design defects or errors known as "errata." Current characterized errata are available upon request. Further, this Limited Warranty does NOT cover: (i) any costs associated with the replacement or repair of the Product, including labor, installation or other

costs incurred by you, and in particular, any costs relating to the removal or replacement of any Product soldered or otherwise permanently affixed to any printed circuit board or integrated with other products; (ii) damage to the Product due to external causes, including accident, problems with electrical power, abnormal, mechanical or environmental conditions, usage not in accordance with product instructions, misuse, neglect, accident, abuse, alteration, repair, improper or unauthorized installation or improper testing, or (iii) any Product which has been modified or operated outside of Intel's publicly available specifications or where the original product identification markings (trademark or serial number) has been removed, altered or obliterated from the Product; or (iv) issues resulting from incorporation of software products into a system, or (v) failure to apply Intel-supplied modifications or corrections to any software provided with or included in the Product.

How to Obtain Warranty Service

To obtain warranty service for the Product, you may contact your original place of purchase in accordance with its instructions or you may contact Intel. To request warranty service from Intel, you must contact the Intel Customer Support ("ICS") center in your region ([Click Here](#)) within the warranty period during normal business hours (local time), excluding holidays and return the Product to the designated ICS center. Please be prepared to provide: (1) your name, mailing address, email address, telephone numbers and, in the USA, valid credit card information; (2) proof of purchase; (3) model name and product identification number found on the Product; and (4) an explanation of the problem. The Customer Service Representative may need additional information from you depending on the nature of the problem. Upon ICS's verification that the Product is eligible for warranty service, you will be issued a Return Material Authorization ("RMA") number and provided with instructions for returning the Product to the designated ICS center. When you return the

Product to the ICS center, you must include the RMA number on the outside of the package. Intel will not accept any returned Product without an RMA number, or that has an invalid RMA number, on the package. You must deliver the returned Product to the designated ICS center in the original or equivalent packaging, with shipping charges pre-paid (within the USA), and assume the risk of damage or loss during shipment. Intel may elect to repair or replace the Product with either a new or reconditioned Product or components, as Intel deems appropriate. The repaired or replaced product will be shipped to you at the expense of Intel within a reasonable period of time after receipt of the returned Product by ICS. The returned Product shall become Intel's property on receipt by ICS. The replacement product is warranted under this written warranty and is subject to the same limitations of liability and exclusions for ninety (90) days or the remainder of the original warranty period, whichever is longer. If Intel replaces the Product, the Limited Warranty period for the replacement Product is not extended.

WARRANTY LIMITATIONS AND EXCLUSIONS

THIS WARRANTY REPLACES ALL OTHER WARRANTIES FOR THE PRODUCT AND INTEL DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, COURSE OF DEALING AND USAGE OF TRADE. **Some states (or jurisdictions) do not allow the exclusion of implied warranties so this limitation may not apply to you.** ALL EXPRESS AND IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THE LIMITED WARRANTY PERIOD. .NO WARRANTIES APPLY AFTER THAT PERIOD. **Some states (or jurisdictions) do not allow limitations on how long an implied warranty lasts, so this limitation may not apply to you.**

LIMITATIONS OF LIABILITY

INTEL'S RESPONSIBILITY UNDER THIS OR ANY OTHER WARRANTY, IMPLIED OR EXPRESS, IS LIMITED TO REPAIR, REPLACEMENT OR REFUND, AS SET FORTH ABOVE. THESE REMEDIES ARE THE SOLE AND EXCLUSIVE REMEDIES FOR ANY BREACH OF WARRANTY. TO THE MAXIMUM EXTENT PERMITTED BY LAW, INTEL IS NOT RESPONSIBLE FOR ANY DIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY OR UNDER ANY OTHER LEGAL THEORY (INCLUDING WITHOUT LIMITATION, LOST PROFITS, DOWNTIME, LOSS OF GOODWILL, DAMAGE TO OR REPLACEMENT OF EQUIPMENT AND PROPERTY, AND ANY COSTS OF RECOVERING, REPROGRAMMING, OR REPRODUCING ANY PROGRAM OR DATA STORED IN OR USED WITH A SYSTEM CONTAINING THE PRODUCT), EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. **Some states (or jurisdictions) do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you.** THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR JURISDICTION. ANY AND ALL DISPUTES ARISING UNDER OR RELATED TO THIS LIMITED WARRANTY SHALL BE ADJUDICATED IN THE FOLLOWING FORUMS AND GOVERNED BY THE FOLLOWING LAWS: FOR THE UNITED STATES OF AMERICA, CANADA, NORTH AMERICA AND SOUTH AMERICA, THE FORUM SHALL BE SANTA CLARA, CALIFORNIA, USA AND THE APPLICABLE LAW SHALL BE

THAT OF THE STATE OF DELAWARE. FOR THE ASIAPACIFIC REGION (EXCEPT FOR MAINLAND CHINA), THE FORUM SHALL BE

SINGAPORE AND THE APPLICABLE LAW SHALL BE THAT OF SINGAPORE. FOR EUROPE AND THE REST OF THE WORLD, THE FORUM SHALL BE LONDON AND THE APPLICABLE LAW SHALL BE THAT OF ENGLAND AND WALES IN THE EVENT OF ANY CONFLICT BETWEEN THE ENGLISH LANGUAGE VERSION AND ANY OTHER TRANSLATED VERSION(S) OF THIS LIMITED WARRANTY (WITH THE EXCEPTION OF THE SIMPLIFIED CHINESE VERSION), THE ENGLISH LANGUAGE VERSION SHALL CONTROL.

IMPORTANT! UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS SOLD HEREUNDER ARE NOT DESIGNED, OR INTENDED FOR USE IN ANY MEDICAL, LIFE SAVING OR LIFE SUSTAINING SYSTEMS, TRANSPORTATION SYSTEMS, NUCLEAR SYSTEMS, OR FOR ANY OTHER MISSION CRITICAL APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.
