

Intel(R) PRO / Wireless 3945ABG 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 with a wireless network in your home or office. This wireless local area network (WLAN) 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) PRO/Wireless 3945ABG Network Connection adapter is compatible with 802.11a, 802.11b and 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 that use 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. All of your wireless network connections are easily managed by Intel(R) PROSet/Wireless software. Profiles that are set up through the Intel PROSet/Wireless software provide enhanced security measures with 802.1x network authentication.

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

Table of Contents

- [Use Intel PROSet/Wireless Software](#)
- [Connect to a Network](#)
- [Use Profiles](#)
- [Set up Security](#)
- [Troubleshooting](#)
- [Administrator Tool](#)

- [Glossary](#)
 - [Wireless Network Overview](#)
 - [Security Overview](#)
 - [Specifications](#)
 - [Customer Support](#)
 - [Safety and Regulatory Information](#)
 - [Warranty](#)
 - [Adapter Registration](#)
-

Information in this document is subject to change without notice.

© 2004–2005 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.

"Important Notice FOR ALL USERS OR DISTRIBUTORS!!!!

Intel wireless LAN adapters are engineered, manufactured, tested, and quality checked to ensure that they meet all necessary local and governmental regulatory agency requirements for the regions that they are designated and/or marked to ship into. Since wireless LANs

are generally unlicensed devices that share spectrum with radars, satellites, and other licensed and unlicensed devices, it is sometimes necessary to dynamically detect, avoid, and limit usage to avoid interference with these devices. In many instances Intel is required to provide test data to prove regional and local compliance to regional and governmental regulations before certification or approval to use the product is granted. Intel's wireless LAN's EEPROM, firmware, and software driver are designed to carefully control parameters that affect radio operation and to ensure electromagnetic compliance (EMC). These parameters include, without limitation, RF power, spectrum usage, channel scanning, and human exposure.

For these reasons Intel cannot permit any manipulation by third parties of the software provided in binary format with the wireless WLAN adapters (e.g., the EEPROM and firmware). Furthermore, if you use any patches, utilities, or code with the Intel wireless LAN adapters that have been manipulated by an unauthorized party (i.e., patches, utilities, or code (including open source code modifications) which have not been validated by Intel), (i) you will be solely responsible for ensuring the regulatory compliance of the products, (ii) Intel will bear no liability, under any theory of liability for any issues associated with the modified products, including without limitation, claims under the warranty and/or issues arising from regulatory non-compliance, and (iii) Intel will not provide or be required to assist in providing support to any third parties for such modified products.

Note: Many regulatory agencies consider Wireless LAN adapters to be "modules", and accordingly, condition system-level regulatory approval upon receipt and review of test data documenting that the antennas and system configuration do not cause the EMC and radio operation to be non-compliant."

Use Intel(R) PROSet/Wireless Software: Intel(R) PRO/Wireless 3945ABG Network Connection User Guide

- [Use Intel PROSet/Wireless as your Wireless Manager](#)
 - [Start Intel PROSet/Wireless](#)
 - [Start Intel PROSet/Wireless from the Taskbar](#)
 - [Taskbar Icons](#)
 - [Tool Tips and Desktop Alerts](#)
 - [Intel PROSet/Wireless Main Window](#)
 - [Wireless Networks List](#)
 - [Connection Status Icons](#)
 - [Network Properties](#)
 - [Connection Details](#)
 - [Profiles List](#)
 - [Intel PROSet/Wireless Menus](#)
 - **Tools Menu**
 - [Application Settings](#)
 - [Intel Wireless Troubleshooter](#)
 - [Administrator Tool](#)
 - **Advanced Menu**
 - [Adapter Settings](#)
 - [Advanced Statistics](#)
 - [Use Windows to manage Wi-Fi](#)
 - **Profiles Menu**
 - [Manage Profiles](#)
 - [Import/Export](#)
 - [Manage Exclusions](#)
 - [Enable and Disable the Radio](#)
 - [Install and Uninstall the Software](#)
-

Use Intel PROSet/Wireless as your Wireless Manager

Intel(R) PROSet/Wireless is 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 use Microsoft(R) Windows(R) XP Wireless Zero Configuration as your wireless manager, you can disable it from the Microsoft Windows Wireless Network tab.

To disable Microsoft Windows XP Wireless Zero Configuration as your wireless manager:

1. Double-click the Intel PROSet/Wireless icon in the desktop task tray or click **Start > Settings > Control Panel**.
2. Double-click **Network Connections**.
3. Right-click **Wireless Network Connection**.
4. Click **Properties**.

5. Click **Wireless Networks**.
6. Verify that the **Use Windows to configure my wireless network settings** is not selected. If it is, clear it.
7. 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 when another application uses the wireless adapter** is selected. This option prompts you when Microsoft Windows XP Wireless Zero Configuration starts to manage your network profiles.

Start Intel PROSet/Wireless

To start Intel PROSet/Wireless use one of the following methods:

- Click **Start > Programs > Intel PROSet Wireless > Intel PROSet Wireless**.
- Right-click the [Taskbar icon](#) located in the lower right corner of your Windows Desktop. Click **Open Intel PROSet/Wireless**.
- Double-click the Taskbar icon to open Intel PROSet/Wireless.

Exit Intel PROSet/Wireless:

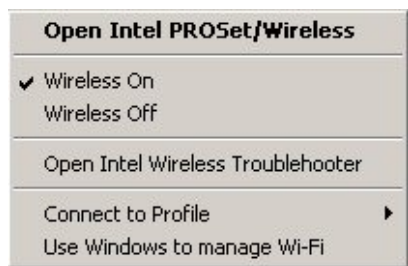
To close Intel PROSet/Wireless from the main window use one of the following:

- Select **File > Exit** from the main window.
- Click **Close**.
- Click the **Close** button (X) at the top right corner of the window.

Start Intel PROSet/Wireless from the Taskbar

To start Intel(R)PROSet/Wireless, double-click the Taskbar icon  located in the lower right corner of your Windows desktop or right-click the Taskbar icon and click **Open Intel PROSet/Wireless**.

Taskbar Menu Options



The Intel PROSet/Wireless icon displays on the Taskbar located in the lower right corner of your Windows desktop. Right-click the status icon to display the menu options.

Menu Item	Comments

Open Intel PROSet/Wireless	Click to start Intel PROSet/Wireless when Intel PROSet/Wireless is your wireless manager. If you select Use Windows to manage Wi-Fi from the Taskbar menu, the menu option changes to Open Wireless Zero Configuration and Microsoft Windows XP Wireless Zero Configuration Service is used as your wireless manager. When you use Microsoft Windows, you cannot use your Intel profiles.
Open Wireless Zero Configuration	
Wireless On	If you have Intel PROSet/Wireless installed, the current state of the radio displays in the Intel PROSet/Wireless main window and on the Taskbar. Select Wireless On to turn the radio on. Select Wireless Off to turn the radio off.
Wireless Off	If your computer has an external switch installed, use it to switch the radio on or off. Refer to your computer manufacturer's documentation for more information about this switch.
802.11a Radio Off	This option is available only for wireless adapters that support 802.11a, 802.11b, and 802.11g. Select to turn off the 802.11a radio. NOTE: This setting is unavailable unless it is set in the Administrator Tool or if your adapter is an Intel(R) PRO/Wireless 2200BG Network Connection.
Open Intel Wireless Troubleshooter	Opens an application that can assist you to resolve wireless network connection issues. When a connection issue is detected, a desktop alert appears at the bottom right corner of your desktop. See Intel Wireless Troubleshooter for more information.
Connect to Profile	Displays the current profiles in the Profile list. Used also to connect to a profile.
Use Windows to manage Wi-Fi	Toggles between the Intel PROSet/Wireless and Microsoft Windows XP Wireless Zero Configuration Service. When you use Microsoft Windows, you cannot use your Intel profiles.
Use Intel PROSet/Wireless to manage Wi-Fi	

Taskbar Icons

The Taskbar icon provides visual indication of the current wireless connection state. The connection status icon is located on the lower right corner of your Windows desktop. The Taskbar can be set to visible or not visible on the [Application Settings](#) Tools menu.

Icon	Description
	Wireless Off: The wireless adapter is off. The wireless device does not transmit or receive while it is off. Click Wireless On to enable the adapter. The icon is white and static.

 2:48 PM	Searching for wireless networks: The wireless adapter searches for any available wireless networks. The icon is white with animation.
 2:48 PM	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 . The icon is red.
 2:48 PM	Wireless network found: An available wireless network is found. Double-click the icon to display the Wireless Networks list. Select the network. Click Connect . The icon is yellow.
 2:48 PM	Authentication failed. Unable to authenticate with wireless network. The icon is green with a yellow warning triangle.
 2:48 PM	Connecting to a wireless network. Flashes while an IP address is being obtained or an error occurs.
 2:48 PM	Connected to a wireless network: Connected to a wireless network. A Tool Tip displays network name, speed, signal quality and IP address. The icon is green with waves that reflect signal quality. The more waves, the better the signal quality.

Tool Tips and Desktop Alerts

The Tool Tips and Desktop Alerts provide feedback and interaction. To display Tool Tips, move your mouse pointer over the icon. Desktop alerts are displayed when your wireless network changes state. For example, if you are out of range of any wireless networks, a desktop alert is displayed when you come into range.

Select **Show Information Notifications** in the [Application Settings](#) to enable desktop alerts.

Tool Tips

Tool tips display when the mouse pointer rolls over the icon. The tool tips display text for each of the connection states.



Desktop Alerts

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

Tool Tip:

Intel PROSet/Wireless

Connected to a wireless network
Wireless Network Name: Wireless
Speed: 54.0 Mbps
Signal Quality: Excellent
IP Address: 192.168.1.103



Wireless networks found

Action: Click the desktop alert to connect to the available network.



Desktop alerts are also used to indicate if there is a connection problem. Click the alert to open the [Intel Wireless Troubleshooter](#).



Intel PROSet/Wireless Main Window

The Intel PROSet/Wireless Main Window allows you 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 Device to Device (ad hoc) networks.
- Configure [adapter settings](#).
- [Troubleshoot](#) wireless connection problems.



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 Profiles 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 Taskbar icon also indicates the current connection status. Refer to [Taskbar Icons](#) for more information.

Main Window Connection Status Description

The icons are used to designate connection status. The icons are used to designate connection status.

The icons are used to designate the connection status.

Icon	Description
	Wireless Off: The radio is not associated to a network. Click the Wireless On button to enable the radio.
	The authentication process to connect to the network has not been started.
	Searching for wireless networks: The wireless adapter is scanning for any available wireless networks. Animated Icons: 
	No wireless networks found: The adapter does not find any wireless networks.
	Wireless network found: An available wireless network is found. You can choose to connect to available networks displayed in the Wireless Networks list.
	Connecting to a wireless network. You are connecting to a wireless network. The crescent shaped curves switch between green and white until an IP Address is obtained or a connection error occurs.
	Connected to a wireless network: You are connected to a wireless network. The network name, speed, signal quality, and IP address display the current connection status. Click the Details button to display details of the current network connection.
Network Name	Network Name (SSID): This is 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.
Signal Quality 	The signal quality icon bars indicate the quality of the transmit and receive signals between your wireless adapter and the nearest access point or computer in Device to Device (ad hoc) mode. The number of vertical green bars indicates the strength of the transmit and receive signals. The signal quality ranges from excellent to out of range. The following factors affect signal quality: • Signal quality decreases with distance and is affected by metal and concrete barriers. • Metal objects can reflect signals and cause interference. • Other electrical devices can cause interference.
Properties	Provides adapter connection status information. See Properties Button for information.
Wireless On (Off)	Switch the radio off and on. Refer to Turn Wireless On or Off for more information.
Help?	Provides help information for this page.
Close	Closes the Intel PROSet/Wireless main window.

Wireless Networks

The Wireless Networks list displays a list of wireless networks within range of the adapter.

Name	Description
	The signal strength of the wireless network access point or computer (Device to Device [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 (Device to Device [ad hoc] mode).
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.
Status	Notification that the adapter is connecting to the wireless network. Once connected, the status is changed to Connected .
	Profiles: Identifies a network in the Wireless Networks list that is connected and has a profile in the profiles list.
	The wireless network uses Network (infrastructure) mode.
	The wireless network uses Device to Device (ad hoc) mode.
	The wireless network uses Security encryption.
	The band frequency being used by the wireless network (802.11a, 802.11b, 802.11g).
	The wireless network is on the exclusion list. Connection to a network or an access point that is on this list is not automatic.
Connect (Disconnect)	Click to connect to a wireless network. Once connected, the button changes to Disconnect .
Properties	Provides detailed information about the connected network and its access points. See Network Properties for information.
Refresh	Refreshes the list of available networks. If any new networks are available within the adapter range, the list is updated to show the new network name.
Wireless On (Wireless Off)	Switch the radio off and on. Refer to Wireless Off (On) for more information.
Close	Closes the Intel PROSet/Wireless main window.
Help?	Provides help information for this page.

Network Properties

Click the **Properties** button on the Intel PROSet/Wireless main window to display the security settings for the wireless adapter. You can also add profiles to be excluded from automatic connection. If network exclusion is enabled (see [Application Settings](#)) then the Network Properties also indicates if the network is excluded from automatic connection.

Network Properties details

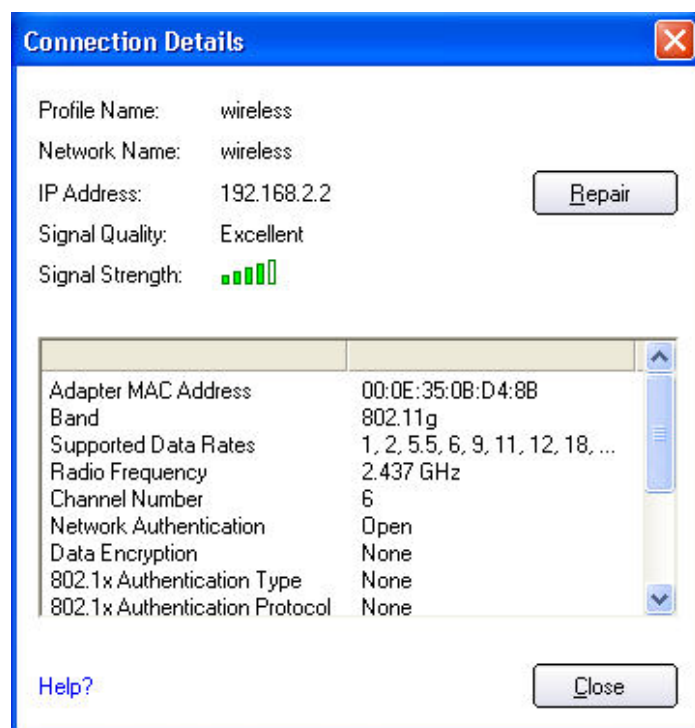
Name	Description
------	-------------

Network Name	Displays the wireless network name.
Band	Current band and frequency being used. Displays Out of Range if no band and frequency is displayed. The following bands are listed: • 802.11a • 802.11b • 802.11g
Operation Mode	Displays the current operating mode: • Network (Infrastructure) 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. • Device to Device (ad hoc) A communication configuration in which every computer has the same capabilities, and any computer can initiate a communication session. Also known as a peer-to-peer network or a computer-to-computer network.
Authentication Level	Displays the current authentication security mode for the profile being used. The following network authentication levels are listed: • None: No encryption used. • Open • Shared • WPA-Enterprise • WPA2-Enterprise • WPA-Personal • WPA2-Personal • Unknown Displays the 802.11 authentication used by the currently used profile. Refer to Security Settings for more information.
Data Encryption	The following Data Encryption settings are listed: • None • WEP • TKIP • CKIP • AES-CCMP Refer to Security Settings for more information.

Access Points in this Network (0-50)	• Signal Strength: The Signal strength icon bars indicate the strength of the transmit and receive signals in percent values between your wireless adapter and the nearest access point. Indicates how well the wireless adapter communicates with an access point or another wireless computer in Device to Device (ad hoc) mode. Signal Quality ranges from Excellent to Out of Range. • Displays 802.11a, 802.11b, or 802.11g. 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 of the selected network.
Manage Exclusions	Refer to Manage Exclusions for more information.
Close	Closes the Network Properties.
Help?	Provides help information for this page.

Connection Details

When you are connected to a network, you can click the **Details** button on the Intel PROSet/Wireless main window to display the Connection Details.



Connection Details description

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

Profile Name	Name of the profile.
Network Name	Network Name (SSID) of the current connection.
IP Address	Internet Protocol (IP) address for the current connection.
Signal Quality	A radio frequency (RF) signal can be assessed by two components: • signal strength (quantity) • signal quality The quality of the signal is determined by a combination of factors. Primarily it is composed of signal strength and the ratio of the RF noise present. RF noise occurs both naturally and artificially by electrical equipment. If the amount of the RF noise is high, 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 difficult for the radio receiver to discern the data information contained in the signal from the noise itself.
Signal Strength	While adequate signal strength is required for good data communications, even more important is the quality of the signal. A strong signal of poor quality results in poor data communications. If the signal quality is low, investigate sources of noise nearby, such as interference from other wireless LANs, other RF transmitters, electric motors or compressors. Also reflections of the signal by metallic or other objects in the area can result in poor signal quality.
Adapter MAC Address	Media Access Control (MAC) address for the wireless adapter.
Band	Indicates the wireless band of the current connection. • 802.11a • 802.11b • 802.11g
Supported Data Rates	Rates at which the wireless adapter can send and receive data. Displays the speed in Mbps for the frequency being used. • 802.11g - 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 • 802.11b - 1, 2, 5.5, and 11 • 802.11a - 6, 9, 11, 12, 18, 24, 36, 48, and 54
Radio Frequency	Displays the frequency of the current wireless connection. • 5.280 GHz • 2.437 GHz
Channel Number	Displays the transmit and receive channel.
Network Authentication	Displays Open, Shared, WPA-Personal and WPA2-Personal modes, WPA-Enterprise, and WPA2-Enterprise. Displays the 802.11 authentication used by the currently used profile. Refer to Security Overview for more information.
Data Encryption	Displays None, WEP, TKIP or AES-CCMP. Refer to Security Overview for more information.
802.1x Authentication Type	Displays None, MD5, EAP-SIM, TLS, TTLS, PEAP, LEAP, or EAP-FAST. Refer to Security Settings for more information.

802.1x Authentication Protocol	Displays None, GTC, MS-CHAP-V2 or TLS. Refer to Security Settings for more information.
CCX Version	Version of the Cisco Compatible Extensions on this wireless connection.
Current TX Power	Cisco Compatible Extensions Power Levels.
Supported Power Levels	1.0, 5.0, 20.0, 31.6, 50.1 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, from the Mandatory Access Point setting , the access point MAC address is displayed. This option directs the wireless adapter to connect to an access point that uses a specific MAC address (48-bit 12 hexadecimal digits, for example, 00:06:25:0E:9D:84).
Repair	Renews the IP Address. If you have trouble accessing the network, verify if the IP address is valid. If it is 0.0.0.0 or 169.x.x.x, then it is probably not valid. If your network is setup for automatic network address assignment, then click Repair and request a new IP address.
Close	Closes the page.
Help?	Provides help information for this page.

Profile Management

The Profiles List displays the current user 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.

Use the **Connect** button to connect to a wireless network. Once connected, a profile is created in the Profiles list. You can also add, edit, and remove profiles from the Profiles 'list.

Different profiles can be configured for each wireless network. Profile settings can include, the network name (SSID), operating mode, and security settings. See [Profile Management](#) for more information.

Profiles list

Name	Description
Profile Name	Network settings that allow your wireless adapter to connect to a network access point (infrastructure mode) or computer (Device to Device [ad hoc]) mode which does not use an access point. Refer to 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 whether network security is being used.	
	Blue circle: The wireless adapter is associated with an access point or computer (Device to Device [ad hoc] mode). If a profile has 802.1x security enabled, this indicates that the wireless adapter is associated and authenticated.

	Indicates infrastructure mode.
	Indicates Device to Device (ad hoc) mode.
	Indicates an Administrator profile.
	The wireless network uses Security encryption.
Arrows  	Position profiles in a preferred order for auto-connection. • Up-arrow: Move the position of a selected profile up in the Profiles list. • Down-arrow: Move the position of a selected profile down in the Profiles list.
Connect	Connect the selected profile for the wireless network.
Add	Use the Profile Wizard to create a new profile. Refer to Create a New Profile for more information.
Remove	Removes a selected profile from the Profile list. Refer to Delete a Profile for more information.
Properties	Used to edit the contents of an existing profile. You can also double-click a profile in the Profile list to edit the profile. Refer to Edit an Existing Profile for more information.
	Export/Import: Imports and exports user-based profiles to and from the Profile list. Wireless profiles can be automatically imported into the Profile list. See Import and Export Profiles for more information.
Close	Closes the profile management window.

Intel PROSet/Wireless Menus

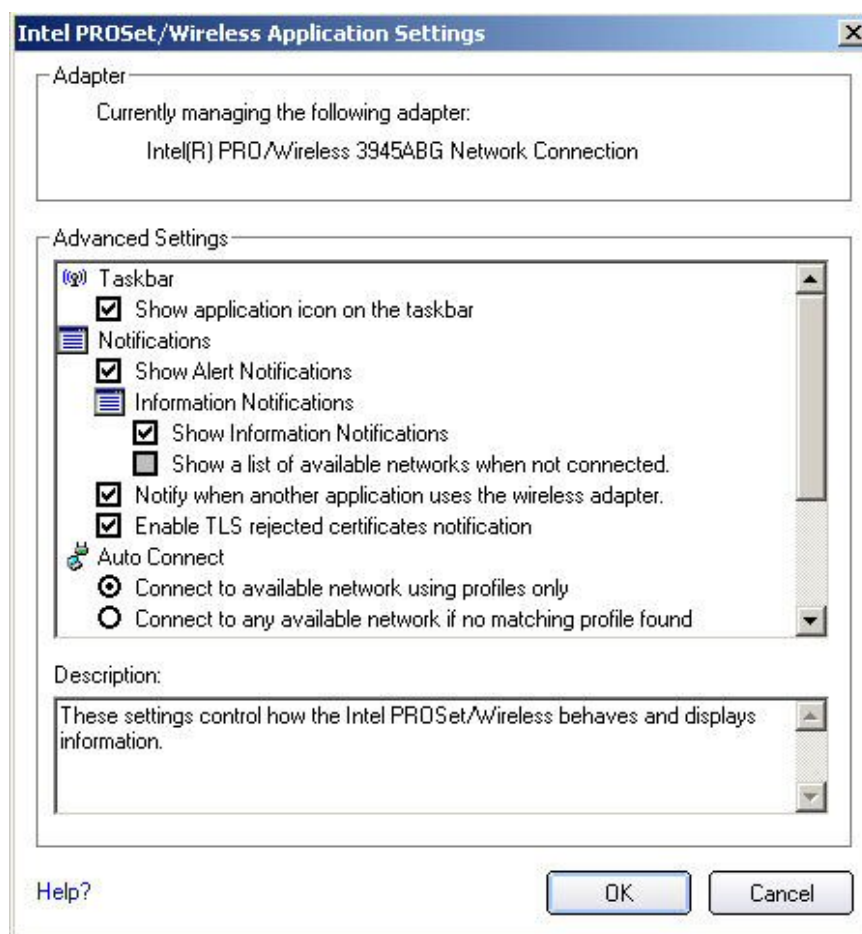
Use the **File**, **Tools**, **Advanced**, **Profiles** and **Help** menus to configure your network settings.

Name	Description
File	Exit: Close the Intel PROSet/Wireless main window. Use one of these options to start the Intel PROSet/Wireless Software: • Click Start > Programs > Intel PROSet Wireless > Intel PROSet Wireless. • Right-click the Taskbar icon located in the lower right corner of your Windows Desktop, and click Open Intel PROSet/Wireless. • Double-click the Taskbar icon to open Intel PROSet/Wireless.

Tools	Application Settings: Use to set system wide connection preferences. Refer to Application Settings for information. Use Ctrl+P from your keyboard as an alternative to access this feature. Intel Wireless Troubleshooter: Use to resolve wireless network connection problems. Use Ctrl+W from your keyboard as an alternative to access this feature. Refer to Intel Wireless Troubleshooter for more information. Administrator Tool: Used by administrators or the person who has administrator privileges on this computer to configure shared profiles (Pre-logon, Persistent and Voice over IP (VoIP)). Refer to Administrator Tool for more information. Use Ctrl+T from your keyboard as an alternative to access this feature. NOTE: The Administrator Tool is available only if it installed during a custom installation of the Intel PROSet/Wireless software. Refer to Install or Uninstall the Software for more information on custom installation.
Advanced	Adapter Settings: Displays Adapter Settings which correlates to the settings in the Microsoft Windows Advanced settings. Refer to Adapter Settings for information. Use Ctrl+A from your keyboard as an alternative to access this feature. To access Adapter Settings from Microsoft Windows: • Select Network Connections from the Windows Control Panel • Right-click the Wireless Network Connection. • Select Properties from the menu. • Click Configure to display the Advanced settings for the adapter. Advanced Statistics: Select to determine how the adapter communicates with an access point. Use Ctrl+S from your keyboard as an alternative to access this feature. Refer to Advanced Statistics for more information. Use Windows to manage Wi-Fi: Select to enable Microsoft Windows XP Wireless Zero Configuration as the wireless manager. Use F10 from your keyboard as an alternative to access this feature. Refer to Switch to Microsoft Windows XP Wireless Zero Configuration for more information.
Profiles	Manage Profiles: Select to create or edit profiles. Use Ctrl+R from your keyboard as an alternative to access this feature. Manage Exclusions: Select to exclude networks from automatic connection. Refer to Manage Exclusions for more information. Use Ctrl+M from your keyboard as an alternative to access this feature.

Help	Intel PROSet/Wireless Help: Starts the online help. Use F1 from your keyboard as an alternative to access this feature. To navigate the help window: • Press F6 to toggle between the left and right pane. Use the up and down arrow as an alternative on your keyboard to move up and down within the pane. • To view information, click Contents in the left-side pane or use Alt+C on your keyboard as an alternative to access this feature. • Double-click on a book icon to open a Contents' topic. Use the up and down arrows to select a topic and press Enter as an alternative to open the sub-topics. • Click Index or Search to look for a specific term. Use Alt+S on your keyboard as an alternative to access the Search feature. About: Displays version information for the currently installed application components.
-------------	--

Application Settings (Tools menu)



The settings on this page control the behavior of the Intel PROSet/Wireless software.

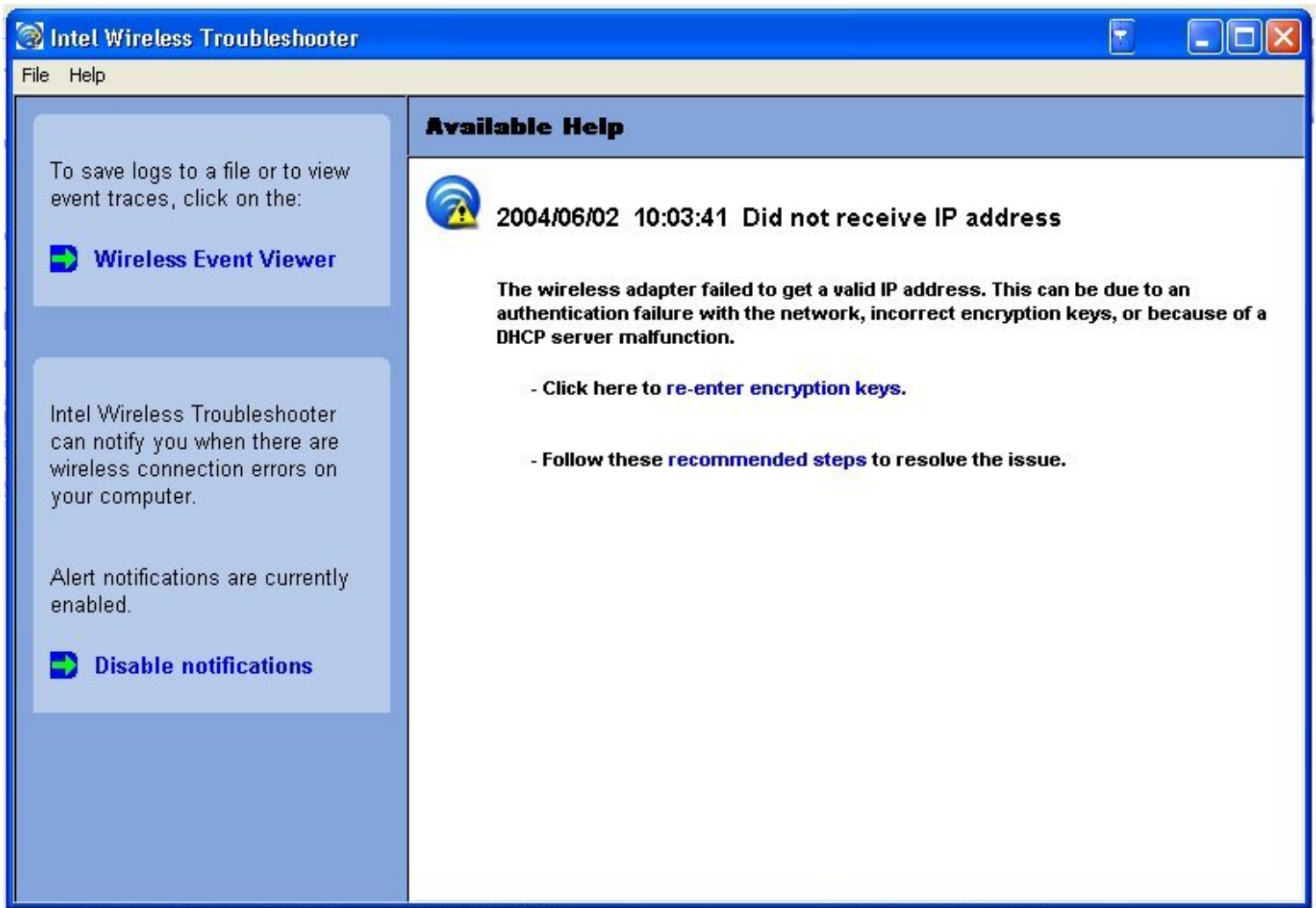
Application Settings description

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

Adapter	Lists the network adapter that are currently available. It may be either an Intel(R) PRO/Wireless 3945ABG Network Connection, an Intel(R) PRO/Wireless 2915ABG Network Connection or, an Intel(R) PRO/Wireless 2200BG Network Connection.
Advanced Settings: The following settings control how Intel PROSet/Wireless behaves and displays information.	
Taskbar	Show application icon on the taskbar: Select to display the Taskbar status icon. This icon resides on the Windows Taskbar (Notification Area). This icon provides the status of your wireless connection. Clear to not display the Taskbar status icon. The Taskbar Status Icon provides several functions: • Visual feedback for the connection state and wireless activity of your wireless network. The icon changes color and animation for different wireless activity. See Taskbar Icons for more information. • Menu: A menu is displayed when you right click the icon. From this menu you perform tasks such as turn on or off the radio or launch the Intel PROSet/Wireless application. See Taskbar Menu Options for more information. • Tool tips and desktop alerts. See: Tool Tips and Desktop Alerts for more information.
Notifications	Show Alert Notifications: Select to display desktop alerts next to the taskbar icon. When your action is required, a message displays. Only events of high importance trigger a desktop alert. If the desktop alert is selected, then the appropriate action is taken. Clear to not display desktop alerts. Refer to Tool Tips and Desktop Alerts for more information. Select one of the following options: Information Notifications: These desktop alerts are of lower importance. They do not require your interaction but can greatly improve the wireless experience. • Show Information Notifications: Selected by default. All informational desktop alerts are displayed next to the taskbar status icon. These desktop alerts improve your wireless experience with notifications 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 Desktop Alerts for more information. • Show a list of available networks in the area when not connected: When Show Information Notifications is cleared, you can select this item. When the desktop alerts are disabled, this option allows you to continue to be notified of available networks when the wireless adapter is not connected. Notify when another application uses the wireless adapter: When selected, a message is displayed when other applications are trying to manage your wireless adapter. This is helpful if you use software provided by a hotspot location (coffee shop, airport terminal). To take advantage of the Intel PROSet/Wireless features, disable this software when you leave the hotspot.

	Enable TLS rejected certificates notification: Select if you want a warning issued when a PEAP-TLS certificate is rejected by the authentication server. See Enterprise Security and Set up the Client for TLS authentication for more information.
Auto Connect	Use profiles only to connect to available networks: (Default) Connect the wireless adapter to an available network with a matching profile from the Profiles List. If no matching profile is found, you are notified (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: Select to connect to a network automatically if you have not configured a profile and are at a location that has an open, unsecured wireless 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.
Manage Exclusions	Enable automatic exclude list feature: Select 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 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.
Wireless Networks List	Show column sort headers: Select to display the column names in the Wireless Networks list. Click on a column header to sort the column in either ascending or descending order.
OK	Save settings and return to the previous page.
Cancel	Closes and cancels changes.
Help?	Provides help information for this page.

Intel Wireless Troubleshooter (Tools menu)



Intel Wireless Troubleshooter is an application that can help you resolve wireless network connection issues. When a connection issue is detected, a desktop alert appears at the bottom right corner of your desktop. Once you click the desktop alert, a diagnostic message displays the recommended steps to resolve the connection problem. For example, if a connection problem occurred because of an invalid password, the Profile Wizard application is launched when you click a displayed hyperlink. You can also launch [Wireless Event Viewer](#) and enable or disable alert notifications. The Intel Wireless Troubleshooter is supported under Microsoft Windows XP and Microsoft Windows 2000

The Intel Wireless Troubleshooter page contains two panes. Use your left mouse button on the left pane to display a list of available tools. The right pane displays the current connection issue in a section. Each section has two parts: the error message and the recommended action. The recommended action contains descriptions about available utilities and helps to resolve the associated connection issue. If you click a help link, the help text is displayed in a window. If you click the associated issue resolution link, a program is launched to resolve the connection issue.

Refer to the [Troubleshooting](#) section for information on resolving errors.

Name	Description
File	Exit: Exits 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	Launches Wireless Event Viewer .
Disable Notification	Select to disable the alert notifications.
Enable Notification	Select to enable the alert notifications.
Available Help	Date Time error message: • Description of error. • Link to resolve error (if available). See Resolve Errors for more information. • Link to recommended steps to resolve error.

Administrator Tool (Tools menu)

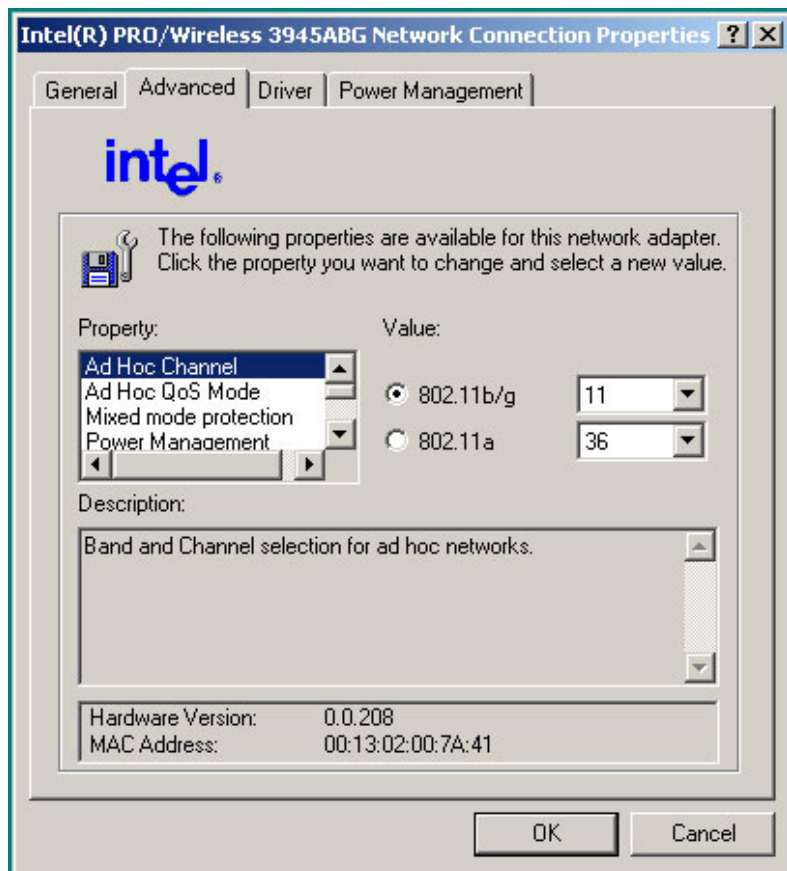
The Administrator tool is for administrators or the person who has administrator privileges on this computer. This tool allows the administrator to restrict what level of control the users of this computer have over their wireless connections. This tool is used also to configure common (shared) profiles.

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. For more information, refer to the [Administrator Tool](#) section.

Name	Description
Administrator Settings	An administrator can select which level of control that users have over their wireless network connections. Refer to Administrator Tool
Administrator Profiles	Enable or disable Persistent, Pre-Logon and Voice over IP (VoIP) profiles on the computer. Refer to Administrator Tool .
Adapter Settings	An administrator can select which level of control that users have over their wireless network connections. Refer to Adapter Settings .
Software	Select which of the Intel PROSet/Wireless applications are installed on a user's computers. Refer to Administrator Tool .
Administrator packages	The Administrator Packages are used to save administrative profiles and other settings. You can copy or send this self-extracting executable to clients on your network. When it is run, the contents are installed and configured on the destination computer. Refer to Administrator Tool .
Change Password	Change the password for the Administrator Tool. See Change Password for more information.
Close	Closes the page.
Help?	Provides help information for this page.

Adapter Settings (Advanced menu)



The Adapter Settings displays the device properties for the wireless adapter installed on your computer. It may be either an Intel(R) PRO/Wireless 3945ABG Network Connection, an Intel(R) PRO/Wireless 2915ABG Network Connection or, an Intel(R) PRO/Wireless 2200BG Network Connection.

Adapter Settings description

Name	Description
Ad Hoc Channel	Unless the other computers in the ad hoc network use a different channel from the default channel, there is no need to change the channel. Value: Select the allowed operating channel from the list. • 802.11b/g: Select this option when 802.11b and 802.11g (2.4 GHz) ad hoc band frequency is used. • 802.11a: Select this option when 802.11a (5 GHz) ad hoc band frequency is used.

Ad Hoc Power Management	Set power saving features for Device to Device (ad hoc) networks. • Disable: Select when connecting to ad hoc networks that contain stations that do not support ad hoc power management • Maximum Power Savings: Select to optimize battery life. • Noisy Environment: Select to optimize performance or connecting with multiple clients. NOTE: This setting is unavailable if the adapter is an Intel PRO/Wireless 2915ABG Network Connection or an Intel PRO/Wireless 2200BG Network Connection.
Ad Hoc QoS Mode	Quality of Service (QoS) control in ad hoc networks. QoS provides prioritization of traffic from the access point over a wireless LAN based on traffic classification. WMM (Wifi MultiMedia) is the QoS certification of the Wi-Fi Alliance (WFA). When WMM is enabled, the adapter uses WMM to support priority tagging and queuing capabilities for Wi-Fi networks. • WMM Enabled.(Default) • WMM Disabled
Mixed mode protection	Use to avoid data collisions in a mixed 802.11b and 802.11g environment. Request to Send/Clear to Send (RTS/CTS) should be used in an environment where clients may not hear each other. CTS-to-self can be used to gain more throughput in an environment where clients are in close proximity and can hear each other.
Power Management	Allows you to select a balance between power consumption and adapter performance. The wireless adapter power settings slider sets a balance between the computer's power source and the battery. • Use default value: (Default) Power settings are 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.
Preamble Mode	Changes the preamble length setting received by the access point during an initial connection. Always use a long preamble length to connect to an access point. Auto Tx Preamble allows automatic preamble detection. If supported, short preamble should be used. If not, use long preamble (Long Tx Preamble).
Preferred Band	Select the operating band. The selections are: • 802.11g • 802.11a • 802.11b NOTE: This setting is available only for an Intel(R) PRO/Wireless 2200BG Network Connection.

Roaming Aggressiveness	This setting allows you to define how aggressively your wireless client roams to improve connection to an access point. • Default: Balanced setting between not roaming and performance. • Lowest: Your wireless client will not roam. Only significant link quality degradation causes it to roam to another access point. NOTE: This setting is unavailable if the adapter is an Intel(R) PRO/Wireless 2915ABG Network Connection or an Intel(R) PRO/Wireless 2200BG Network Connection.
Throughput Enhancement	Changes the value of the Packet Burst Control. • Enable: Select to enable throughput enhancement. • Disable: (Default) Select to disable throughput enhancement.
Transmit Power	Default Setting: Highest power setting Lowest Minimum Coverage: Set the adapter to a lowest transmit power. Enable you to expand the number of coverage areas or confine a coverage area. Reduce the coverage area in high traffic areas to improve overall transmission quality and avoid congestion and interference with other devices. Highest Maximum Coverage: Set the adapter to a maximum transmit power level. Select for maximum performance and range in environments with limited additional radio devices. NOTE: The optimal setting is for a user to always set the transmit power at the lowest possible level still compatible with the quality of their communication. This allows the maximum number of wireless devices to operate in dense areas and reduce interference with other devices that this radio shares radio spectrum with. NOTE: This setting takes effect when either Infrastructure or Ad hoc mode is used.
Wireless Mode	Select which band to use for connection to a wireless network: • 802.11a only: Connect the wireless adapter to 802.11a networks only • 802.11b only: Connect the wireless adapter to 802.11b networks only • 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 • 802.11a, 802.11b, and 802.11g: (Default) - Connect to either 802.11a, 802.11b or 802.11g wireless networks. NOTE: These wireless modes (Modulation type) determine the discovered access points displayed in the Wireless Networks list.

OK	Saves settings and returns to the previous page.
Cancel	Closes and cancels any changes.
Help?	Provides help information for this page.

Advanced Statistics (Advanced menu)

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

Name	Description
Statistics	Advanced Statistics: This information pertains to how the adapter communicates with an access point. Association: If the adapter finds an access point to communicate with, the value is in range. Otherwise, the value is out of range. • AP MAC Address: The twelve digit MAC address (00:40:96:31:1C:05) of the AP. • Number of associations: The number of times the access point has found the adapter. • AP count: The number of available access points within range of the wireless adapter. • Number of full scans: The number of times the adapter has scanned all channels for receiving information. • Number of partial scans: The number of scans that have been terminated. 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. • Roaming Count: The number of times that roaming occurred. • AP did not transmit: The adapter did not receive radio transmission from the access point. You may need to reset the access point. • Poor beacon quality: The signal quality is too low to sustain communication with the access point. You have moved the adapter outside the coverage area of the access point or the access point's device address information has been changed. • AP load balancing: The access point ended its association with the adapter based on the access point's inability to maintain communication with all its associated adapters. Too many adapters are trying to communicate with one access point. • AP RSSI too low: The Receive Signal Strength Indicator (RSSI) is too low to maintain an association with the adapter. You may have moved outside the coverage area of the access point or the

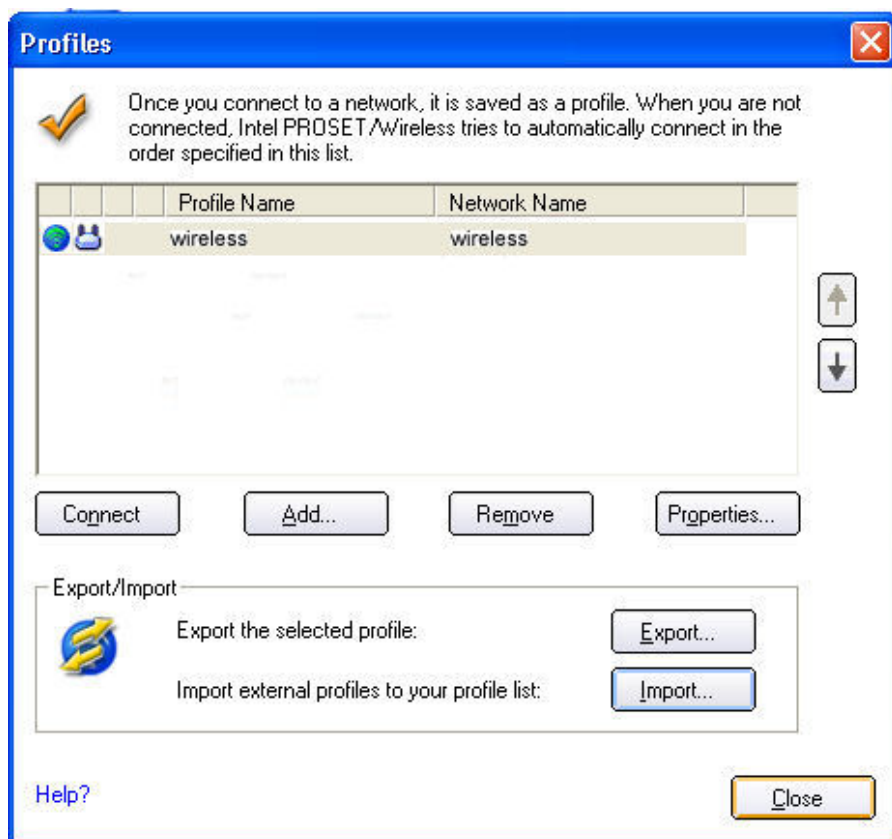
	access point could have increased its data rate. • Poor channel quality: The quality of the channel is low and caused the adapter to look for another access point. • AP dropped mobile unit: The access point dropped a computer from the list of recognizable mobile devices. The computer must re-associate with an access point. Miscellaneous: Use this information to determine if an association with a different access point increases performance and helps maintain the highest possible data rate. • Received Beacons: Number beacons received by the adapter. • Percent missed Beacons: Percent value for missed beacons. • Percent transmit errors: The percentage of data transmissions that had errors. • Signal Strength: Signal strength of the access point which the adapter communicates with.
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 taking new data measurements.
Close	Closes and returns to the main window.
Help?	Provides help information for this page.

Use Windows to manage Wi-Fi (Advanced menu)



The Microsoft Windows XP Wireless Zero Configuration feature provides a built-in wireless configuration utility. This feature can be enabled and disabled within Intel PROSet/Wireless or click **Use Windows to manage Wi-Fi** on the [Tools](#) menu or the [Taskbar](#) menu. If Windows XP Wireless Zero Configuration is enabled, the features in Intel(R) PROSet/Wireless are disabled.

Import or Export Profiles (Profiles menu)



Import Profiles into the Profile List

Import wireless profiles automatically into the Profiles List. This is accomplished by Intel (R) PROSet/Wireless monitoring the import folder on your hard disk for new profile files. Only profiles that have been enabled through **Enable Auto-Import** in the [Advanced Settings](#) are automatically imported. If a profile of the same name already exists in the Profiles List, you are notified to either reject the imported profile, or accept it. If accepted, 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 from your hard disk after it is the imported, whether the import was successful or not.

Password Protected Profiles

Import and export password protected user-based profiles 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	Step 1: Select one or more profiles to export from your profile list below: 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. Step 2: Export the selected profile: Click Export to save your profiles to a selected directory. Step 3: Select the destination folder. Click Browse to search your hard disk for the destination directory. The C:\ drive is the default directory. Select the drive and directory. Click OK. Click OK to return to the Profiles page. 
Import profiles	Select individual or multiple profiles to imports Profiles list. 1. Click Import to search your hard disk for profiles to import. 2. Select the profile from the selected drive or directory 3. Click Import. You are notified when the selected profile as been successfully imported. 4. Click OK to return to the Profiles page. Click Cancel to close and cancel any changes.
OK	Saves settings and returns to the previous page.
Help?	Provides help information for this page.

Manage Exclusions (Profiles menu)

Exclude List Management is available when you either select Manage Exclusions from the Profiles menu or click the [Properties](#) button on the Wireless Networks list.

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

Use Exclude List Management to exclude entire wireless networks (SSID). For networks with more than one access point, you may exclude an individual wireless access point (BSSID).

Name	Description

Exclude List Management	• Network Name: Name (SSID) of the wireless network. • Radio: Displays the band if there is a DHCP error. • MAC Address: The Ethernet MAC address of the device. • Reason: Explains why this entry was excluded from automatic connection. • Details: Provides specific information on how the access point was excluded and how to remove it from exclusion. This network has been excluded from automatic connection for the following reasons. -User has excluded this network manually. To make this network (or access points) eligible for automatic connection again, select it and click the Remove button. Note: - The Reset button removes all entries except rogue access points from the list. - Rogue access points are removed from the list when a connection is made to this access point using valid credentials. - All excluded access points in a network (other than rogue) are removed from the list when a profile for that network is applied manually NOTE: Entries that are dimmed are excluded rouge access points. A rogue access point is any access point unsanctioned by network administrators. These entries cannot be removed from the list.
Add	Add a network name (SSID) to the list.
Remove	Remove an entry from the list. 1. Select the entry from the list. 2. Click Remove. 3. You are asked: Do you want to remove the selected item from the Exclude List? 4. Click Yes to remove the profile from the list.
Reset list	Removes all of the networks and access points from the Exclude List.
Close	Closes page and saves settings.
Help?	Provides help information for this page.

Turn Wireless Off/On

To switch the wireless radio on or off, use one of the following:

- The optional hardware radio switch on your computer
- Intel PROSet/Wireless software
- Microsoft Windows

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

Use the optional computer radio on or off switch

If your computer has an external switch installed, use it 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 on the [Taskbar](#).

Use Intel PROSet/Wireless to switch the radio on or off

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

From the Intel PROSet/Wireless main Window, click **Wireless On or Wireless Off** to toggle the radio on or off.

Switch the radio on or off from the Task Tray Icon

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

How to use the Device Manager to disable the radio

The radio can be disabled (made non-functional) from the Microsoft Windows Device Manager.

NOTE: If you disabled the radio from Microsoft Windows, then you must use Microsoft Windows to turn the radio on. You cannot use a hardware switch or Intel PROSet/Wireless to enable the radio again.

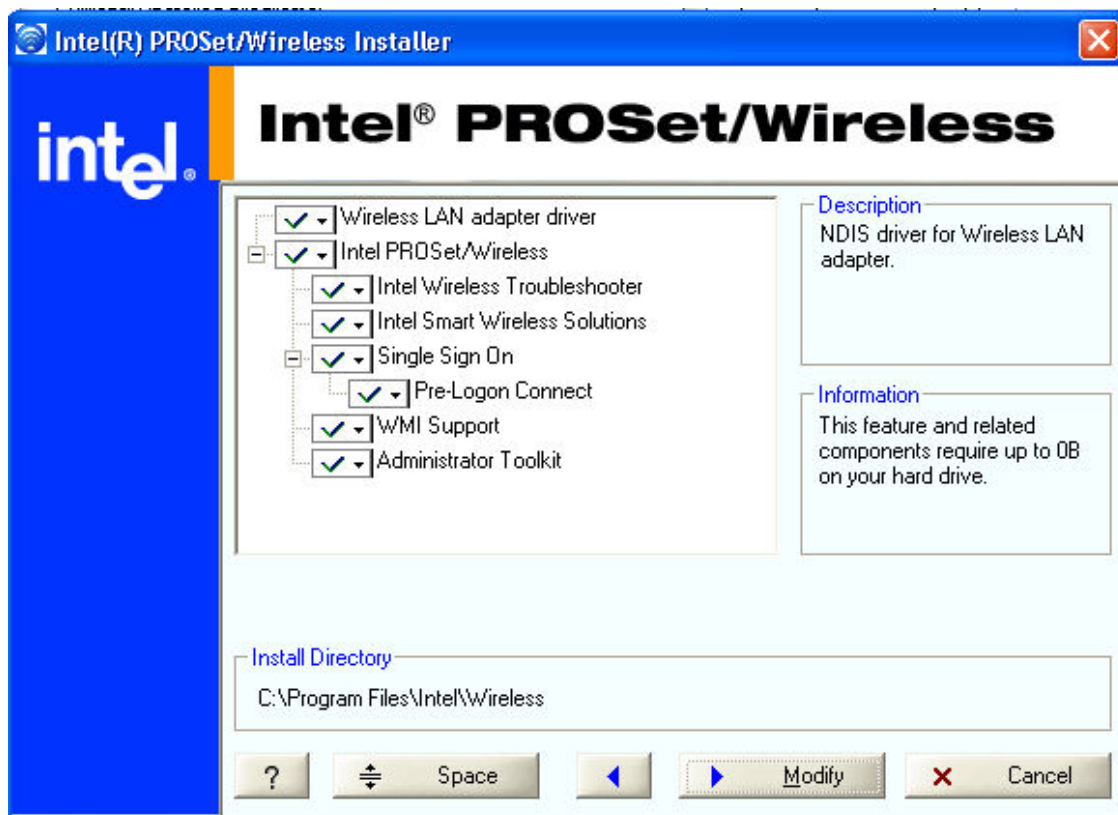
Microsoft Windows XP

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

Install and Uninstall the Software

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.

A Typical install includes the Wireless LAN adapter driver, the Intel PROSet/Wireless software and the [Intel Wireless Troubleshooter](#).



To install the software:

1. Insert the Installation CD in your CD drive.
2. Click **Install Software** on the Intel PROSet/Wireless Network screen.
3. Read the license agreement.
4. Select **I accept the terms in the license agreement**.
5. Click **Next**.
6. Click **Custom**.
7. Select from the list of features to install:

Intel PROSet/Wireless: The Intel PROSet Wireless application software.

- **Install:** Click **Intel PROSet Wireless**. Select **Install this feature and all subfeatures**. Proceed to step 8.
- **Not install:** Click **This feature will not be available**. A red x displays next to the option indicates that it is not to be installed.

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

- **Install:** Click **Intel Smart Wireless Solutions**. Select **Install this feature and all subfeatures**. Proceed to step 8.
- **Not Install:** Select **This feature will not be available**. A red x displays next to the option indicates that it is not to be installed.

Intel Wireless Troubleshooter: Helps you resolve wireless connection issues.

- **Install:** Click **Intel Wireless Troubleshooter**. Select **Install this feature and all subfeatures**. Click **Next** and proceed to step 8.
- **Not Install:** Select **This feature will not be available**. A red x displays next to the option indicates that it is not to be installed.

WMI Support: Wireless Management Instrumentation functionality allows administrators who do not have Intel PROSet/Wireless installed to manage remotely clients that do have Intel PROSet/Wireless installed.

- **Install:** Click **WMI Support**. Select **Install this feature and all subfeatures**. Proceed to step 8.
- **Not install:** Click **This feature will not be available**. A red x displays next to the option indicates that it is not be installed.

Administrator Toolkit: Installs the Administrator Tool to the Tools menu. This tool is used to configure common (shared) profiles. The Administrator Tool is also used by an Information Technology department to enable or disable features within the Intel PROSet/Wireless software.

- **Install:** Click **Administrator Toolkit** . Select **Install this feature and all subfeatures**. Click **Next** and proceed to step 5.
- **Not Install:** Select **This feature will not be available**. A red x displays next to the option indicates that it is not to be installed.

Single Sign On: Installs the Single Sign On features. This tool is used to configure common (shared) profiles with the Administrator Tool.

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

Single Sign On 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 use Microsoft Windows XP Home Edition. It is targeted for the home user; Fast User Switching is also available on Microsoft Windows XP Professional if you install it on a stand alone or workgroup-connected computer. If a computer running Microsoft Windows XP Professional is added to a domain, then Fast User Switching option is not available.

Pre-Logon Connect: A Pre-Logon profile is active once a user logs onto the computer.

- **Install:** Click **Single Sign On**. Select **Install this feature and all subfeatures**. Click **Next** and proceed to step 8.
- **Not Install:** Select **This feature will not be available**. A red x displays next to the option indicates that it is not to be installed.

8. Click **Install**.
9. The installed components are listed after the software is installed on your computer.
10. Click **OK**.

NOTE: When Pre-Logon is installed, you are asked to reboot after installation of the software.

To uninstall Intel PROSet/Wireless:

1. Click **Start > Settings > Control Panel > Add or Remove Programs**.
2. Click **Intel PROSet/Wireless Software** .
3. Click **Remove**.
4. Click **Next**.

5. You are asked what you would like to do with your current profiles and settings:

You have chosen to completely remove the Intel PROSet/Wireless software.

Select what to do with your current profiles and settings.

- **Do not save my profiles and settings.** Select to completely remove all of your current profiles and settings. If you reinstall the software, the profiles and settings are no longer available.
- **Save my profiles and settings in the current format (Intel PROSet/Wireless 10.x).** Select to save your current profiles and settings. If you reinstall the software, your current profiles and settings are available.
- **Convert and save my profiles and settings in Intel PROSet/Wireless 9.x format.** If you need to revert to a previous version of Intel PROSet/Wireless software, select to save your settings. After you have reinstalled the software, your current profiles and settings are available. **NOTE:** Only settings applicable to the prior version of the software are available.

6. Make a selection and click **OK**.

7. Click **Yes** to restart your computer.

[Back to Top](#)

[Back to Contents](#)

[Trademarks and Disclaimers](#)

Profile Management: Intel(R) PRO/Wireless 3945ABG Network Connection User Guide

- [What is a Profile](#)
 - [Profiles List](#)
 - [Profiles List icons](#)
 - [Connect to a Profile](#)
 - [Create a New Profile](#)
 - [Edit an Existing Profile](#)
 - [Remove a Profile](#)
 - [Set a Profile Password](#)
 - [Import and Export Profiles](#)
-

What is a Profile?

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

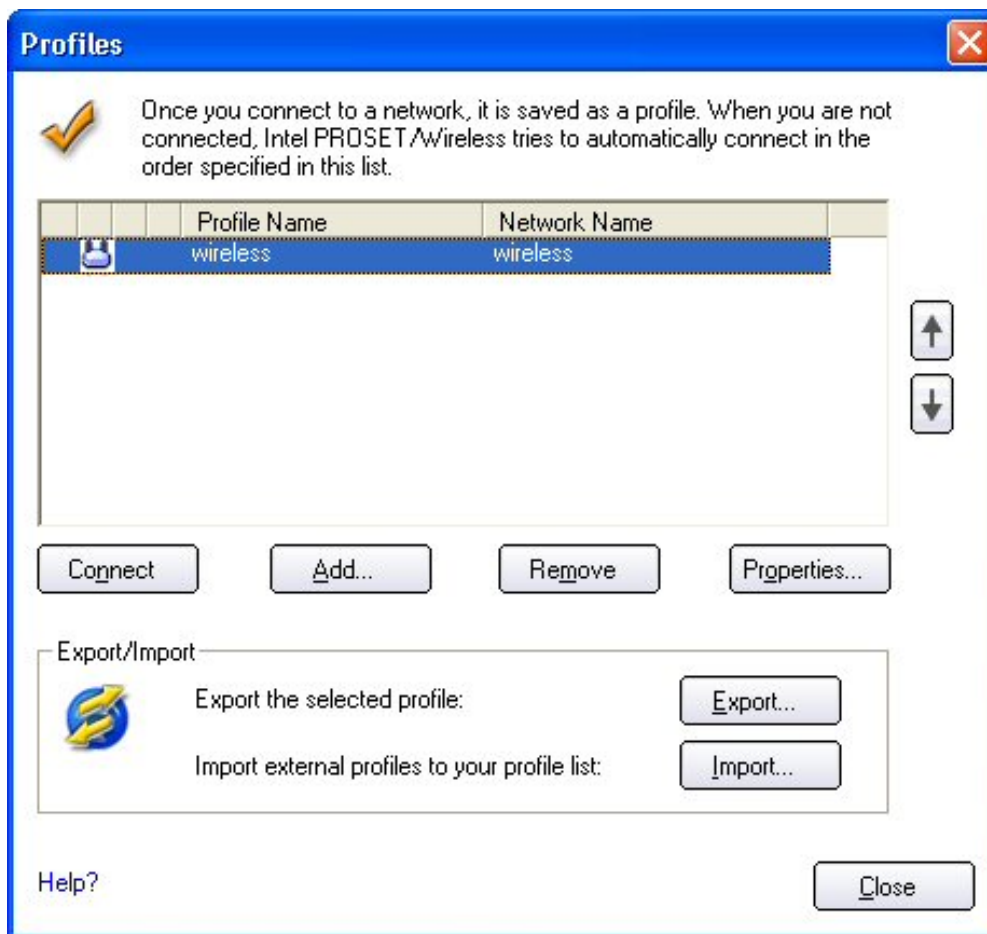
A profile is created when you connect to a wireless network.

1. Select a network from the **Wireless Networks** list.
2. Click **Connect**.
3. If the wireless network requires a WEP password or encryption key, enter the password. To change the security options, click **Advanced** to open the Profile Wizard Security Settings.
4. Click **OK** to connect. A profile is created and added to the Profiles list.

The Profile Management Wizard guides you through the settings required to connect with the wireless network. At completion, the profile is saved and added to the Profiles list. Since these wireless settings are saved, the next time you are in range of this wireless network you are automatically connected.

Profiles List

The profile list displays a list of existing profiles. When you come in range of a wireless network, Intel PROSet/Wireless scans the Profile List to see if there is a match. If a match is found, you are automatically connected to the network.



Profile List Priority Arrows

- Use the **up-arrow** to move the position of a selected profile up in the profiles list.
- Use the **down-arrow** to move the position of a selected profile down in the profiles list.

Profiles List Icons

The network profile status icons indicate if the adapter is associated with a network, the type of operating mode being used, and if security encryption is enabled. These icons display next to the profile name in the profile list.

Name	Description
Profile Name	Profiles are network settings that allow your wireless adapter to connect to a network access point (Infrastructure mode) or computer (device-to-device [Ad hoc] mode) which does not use an access point.
Network Name	Name of the wireless network (SSID) or computer.

Connection Icons - The network profile status icons indicate the different connection states of the adapter with a wireless network, the type of operating mode being used, and if network security is being used.	
	Blue circle: The wireless adapter is associated with an access point or computer (Ad hoc mode). If a profile has 802.1x security enabled, this indicates that the wireless adapter is associated and authenticated.
	Indicates Network (Infrastructure) mode.
	Indicates Device to Device (ad hoc) mode.
	Indicates an Administrator profile.
	The wireless network uses Security encryption.
Network Name	Name of the wireless network (SSID) or computer.
Arrows	Use the arrows to position profiles in a preferred order for auto-connection. • Up-arrow: Move the position of a selected profile up in the profile list. • Down-arrow: Move the position of a selected profile down in the profile list.
	
	
Connect	Connect the selected profile for the wireless network.
Add	Create a new profile using the Profile Wizard. Refer to Create a New Profile for more information.
Remove	Remove a selected profile from the Profile List. Refer to Remove 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 Edit an Existing Profile for more information.
	Export/Import: Import and export user-based profiles to and from the Profiles list. Wireless profiles can be automatically imported into the Profiles list. See Import and Export Profiles for more information.
Close	Closes the profile management window.

Connect to a Profile

When you are in range of a wireless network that has a matching profile you are automatically connected to that network. If a network with a lower priority profile is also in range you can force the connection to that lower profile. This is achieved from Intel PROSet/Wireless or from the Taskbar icon.

Manually connect to a profile from Intel PROSet/Wireless

1. Double-click the Taskbar icon to open the Intel PROSet/Wireless main window.
2. Click **Profiles** to open the Profiles list.
3. Select the profile from the Profile list.
4. Click **Connect**. Remember that the connection is only made if the wireless network is in range.

Manually connect to a profile from the Taskbar

1. Right-click the Intel PROSet/Wireless connection Taskbar icon.
2. Click **Connect to Profile**.
3. Select a profile.
4. Click to start the connection.

Create a New Profile

Select a network from the **Wireless Networks** list. Click **Connect**. The Create Wireless Profile Wizard guides you through the necessary steps to create a profile and connect to the network. During this process, the Wizard attempts to detect the appropriate security settings for you.

The screenshot shows the 'Create Wireless Profile' wizard window. The title bar is blue with the text 'Create Wireless Profile' and a close button. 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 padlock icon). The main area has a light blue header 'General Settings'. Below this, there are two text input fields: 'Wireless Network Name (SSID):' with the value 'wireless' and 'Profile Name:' with the value 'wireless'. A paragraph of text explains: 'The Wireless Network Name (SSID) is a unique identifier that differentiates one wireless network from another. The Profile Name is your name for the network. Example: Home or Office.' Below this, there is a section 'Operating Mode:' with two radio button options. The first option, 'Network (Infrastructure) - Connect to wireless networks and/or the Internet.', is selected. The second option is 'Device to device (Ad hoc) - Connect directly to other computers.' At the bottom, there are five buttons: 'Advanced...' (disabled), 'Help?' (blue text), '<< Back' (disabled), 'Next >>' (disabled), and 'OK' (disabled). The 'Cancel' button is also present.

Create Wireless Profile

Profile Name: wireless

General Settings

Security Settings

Wireless Network Name (SSID): wireless

Profile Name: wireless

The Wireless Network Name (SSID) is a unique identifier that differentiates one wireless network from another. The Profile Name is your name for the network. Example: Home or Office.

Operating Mode:

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

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

Advanced... Help? << Back Next >> OK Cancel



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

1. From the Intel PROSet/Wireless main window, click **Profiles**.
2. On the Profiles page, click **Add** to open the Profile Wizard General Settings.
3. Use the General Settings to add the [Profile Name](#), [Wireless Network Name](#), select the [Operating Mode](#), and access [Advanced Settings](#).

General Settings Description

Name	Description
Profile Name	Name of the wireless network profile. When you configure a wireless network that was selected from the Wireless Networks list, the profile name is the same as the Wireless Network Name (SSID). This name can be changed to be more descriptive or customized for your personal use. Examples: My Office Network, Bob's Home Network, ABC Company Network
Wireless Network Name (SSID)	Name of the wireless network access point used by the wireless adapter for connection. The SSID must match exactly the name of the wireless access point. It is case sensitive. When you configure a wireless network that was selected from the Wireless Networks list, the SSID is taken from the wireless network list. You cannot and should not change it. Blank SSID: If the wireless adapter receives a blank network name (SSID) from a stealth access point, <SSID not broadcast> is displayed in the Wireless Networks list. Provide the actual SSID for the access point. After connection both the blank SSID and the associated SSID can be viewed in the available networks list.

Operating Mode	Network (Infrastructure): Connect to an access point. An infrastructure network consists of one or more access points and one or more computers with wireless adapters. This connection is the type used in home networks, corporate networks, hotels, and other areas that provide access to the network and/or the internet. Device to Device (ad hoc): Connect directly to other computers in an ad hoc wireless network. This type of connection is useful for connections between two or more computers only. It does not provide access to network resources or the internet.
Advanced	Click Advanced to access the Advanced Settings . The Advanced Settings allows you to set auto-connect or auto-import options, launch an application, set a profile password or specify a certain access point address for adapter connection (Mandatory access point). Refer to Advanced Settings for more information.
Next	Proceeds to the Security Settings page.
OK	Finishes creation of the new profile with the current settings.
Cancel	Closes the Profile Wizard and cancel any changes.
Help?	Provides help information for this page.

4. Click [Advanced](#) for the following options:

- [Auto-Connect](#): Select to automatically or manually connect to a profile.
- [Auto-Import](#) this profile (for network administrators only).
- [Mandatory Access Point](#): Select to associate the wireless adapter with a specific access point.
- [Password protect the profile](#): Select to password protect a profile.
- [Start Application](#): Specify a program to be started when a wireless connection is made.

Advanced Settings

Settings:

- Auto Connect
- Auto Import
- Mandatory Access Point
- Password Protection**
- Start Application

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. To make future changes, this password is required.

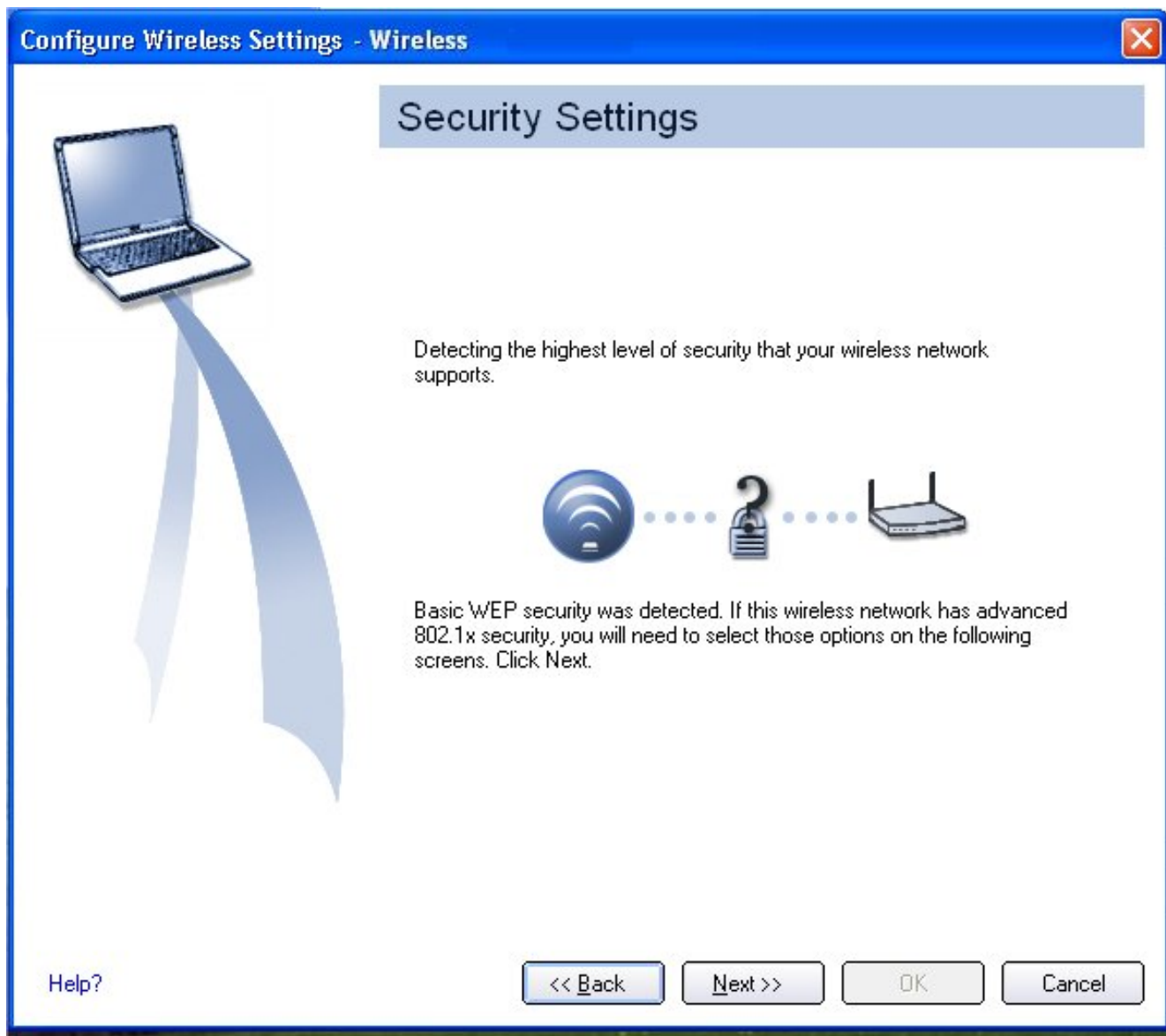
[Help?](#)

Advanced Settings Description

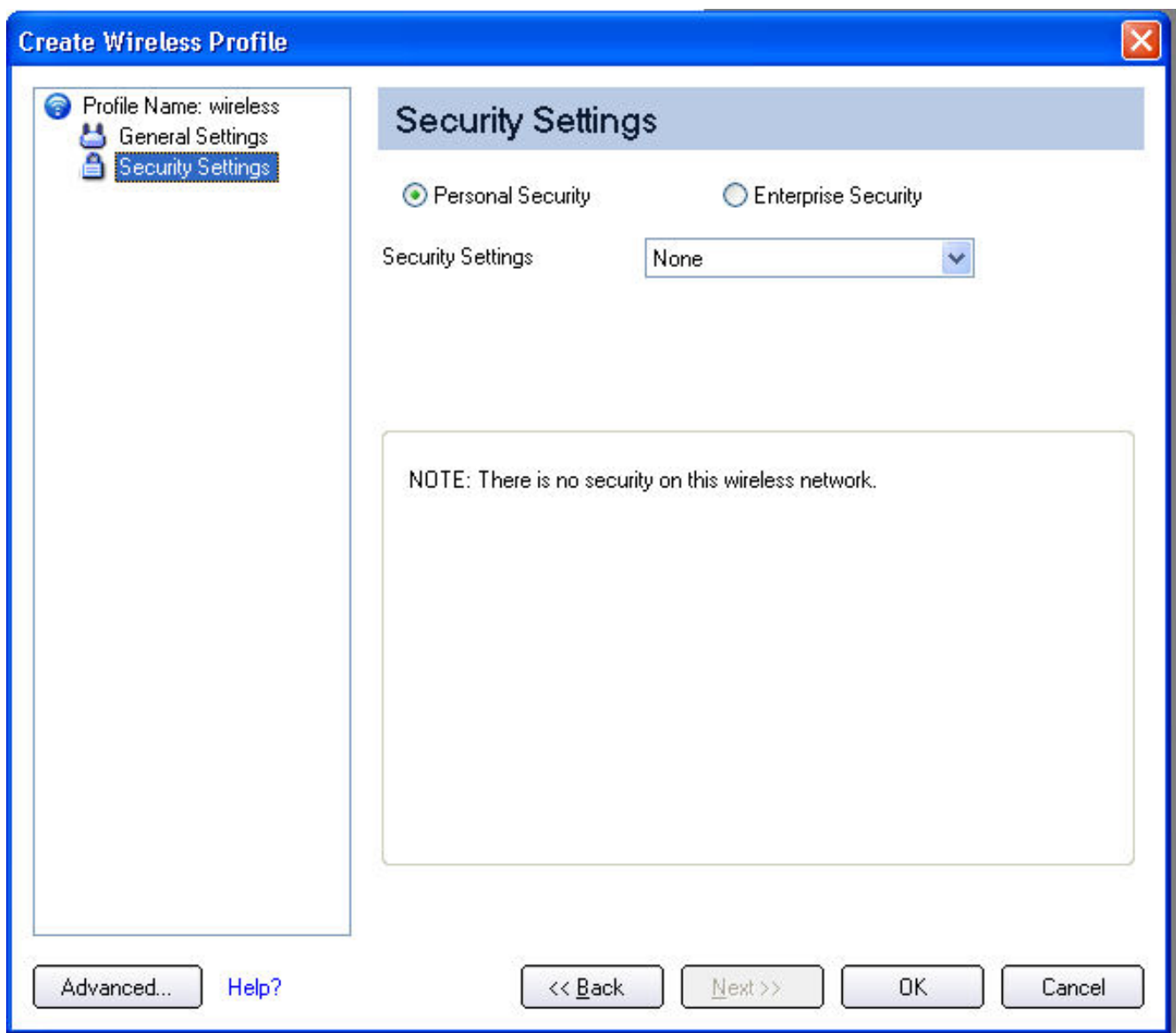
Name	Description
Auto Connect	Automatic: (Default) Select to have Intel PROSet/Wireless automatically connect to this profile when it is in range. On Demand: Select to prevent automatic connection of a profile when the network is in range. For example, if there is a cost for a wireless connection and you did not want to connect automatically when in range. To connect to the network: 1. Select the network from the Wireless Networks list 2. Click Connect.
Auto Import	Allows a network administrator to easily move the selected profile to other computers. When the exported file is placed in the Wireless\AutoImport directory on another computer, Intel PROSet/Wireless automatically imports the profile.

Mandatory Access Point	Mandatory Access Point: Forces the wireless adapter to connect to an access point that uses a specific MAC address. Type the MAC address of the access point (BSSID); 48-bit 12 hexadecimal digits. For example, 00:06:25:0E:9D:84. This feature is not available when ad hoc operating mode is used. Clear: Clear current address.
Password Protection	1. Password protect this profile (max. 10 characters): Select to enable a password for the profile. The default setting is cleared for no profile password. 2. Password: Enter a password. The entered password characters display as asterisks. 3. Confirm New Password: Reenter the password.
Start Application	Automatically starts a batch file, executable file, or script whenever you connect to the profile. For example, start a Virtual Private Network (VPN) session automatically whenever you connect to a wireless network. 1. Click Enable Start Application. 2. Enter the name of the program that you want to start or click Browse to locate the file on your hard disk. 3. Click OK to close the Advanced Settings.
OK	Close and save the settings.
Cancel	Close and cancel any changes.
Help?	Help information for this page.

5. From the General Settings, click **Next** to open the Security Settings.



6. 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.



7. Click **OK** when you have completed the profile settings. The Profile Wizard ends and you are returned to the Intel PROSet/Wireless main window. To change or verify the profile settings, click **Back**.
8. 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.
9. If you want to manually connect to this profile, click **Connect**. The [connection icon](#) displays the current connection status. The network name, transmit and receive speeds, and signal quality are also displayed.

Edit an Existing Profile

To edit an existing profile:

1. Click **Profiles** on the Intel PROSet/Wireless main window.
2. Select the profile to edit in the Profiles list.
3. Click **Properties** to open the General Settings.

4. Click **Next** and **Back** to navigate through the General and Security Settings:
 - **General Settings**. Refer to [General Settings](#) for more information.
 - **Security Settings**. Refer to [Security Settings](#) for more information.
 5. Click **OK** to save the current settings and exit. Click **Cancel** to exit without saving changes.
-

Remove a Profile

To delete a profile:

1. Click **Profiles** on the Intel PROSet/Wireless main window.
 2. Select the profile from the list.
 3. Click **Remove**.
 - If you are still connected to the network, you are notified that **This profile is active and will be permanently removed. Do you want to continue?**
 - If you are not connected, you are notified that the **Profile will be permanently removed. Do you want to continue?**
 4. Click **Yes**. The profile is removed from the Profiles list.
-

Set a Profile Password

To password protect an existing profile:

1. Click **Profiles** on the Intel PROSet/Wireless main window.
 2. Select the profile from the list.
 3. Click **Properties** to open the General Settings.
 4. Click [Advanced](#) to open the the Advanced Settings.
 5. Click **Password Protection** to open the Password Protection settings.
 6. Click **Password protect this profile (maximum 10 characters)**
 7. **Password:** Type the password
 8. **Confirm Password:** Reenter the password.
 9. Click **OK** to save the setting and return to the General Settings page.
 10. Click **OK** to return to the Intel PROSet/Wireless main window.
-

Import or Export Profiles

Allows you to import and export user-based profiles to and from the Profiles list. Wireless profiles can be automatically imported into the Profiles list.

NOTE: To export Administrator profiles, refer to [Administrator Packages](#) for more information.

Import Profiles into the Profile List

To import profiles manually:

1. Click **Import** on the Profiles page.
2. Select the profile files to import.
3. Click **Import**.
4. You are notified that the profile has been successfully imported.
5. Click **OK**.

An administrator can set profiles to be imported automatically into the Profile list. Intel PROSet/Wireless monitors the import folder on your hard disk for new profile files. Only profiles that have been enabled through **Enable Auto-Import** in the [Advanced Settings](#) are automatically imported. If a profile of the same name already exists in the Profile list, you are notified to either reject the imported profile or accept it. If accepted, the existing profile is replaced.

All imported user-based profiles are placed at the bottom of the Profile List, and the profile file is immediately deleted from your hard disk after it is imported, whether the import was successful or not.

Password Protected Profiles

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

Export Profiles from the Profiles List

1. Select individual or multiple profiles from the list.

To select multiple profiles:

- Use your mouse to highlight a profile.
 - Press **Ctrl**.
 - Click each profile that you want selected.
2. Select **Export** to export one or more profiles from the Profile list.
 3. Select the destination folder. Click **Browse** to search your hard disk for the destination directory. The C:\ drive is the default directory.
 4. Click **OK** to export the selected profile. You are notified: **Successfully exported selected profiles to the destination folder: C:\.**

[Back to Top](#)

[Back to Contents](#)

[Trademarks and Disclaimers](#)

Set Up Profile Security: Intel(R) PRO/Wireless 3945ABG Network Connection User Guide

[Use Intel\(R\) PROSet/Wireless Software](#)

[Personal Security](#)

[Personal Security Settings](#)

[Set up Data Encryption and Authentication](#)

- [Configure Profiles for Device to Device \(Ad Hoc\) Networks](#)
 - [Set up a Client with Open Authentication and No Data Encryption \(None\)](#)
 - [Set up a Client with WEP 64-bit or WEP 128-bit Data Encryption](#)
- [Configure Profiles for Infrastructure Networks](#)
 - [Set up a Client with No Data Encryption and No Network Authentication \(None\)](#)
 - [Set up a Client with WEP 64-bit or WEP 128-bit Data Encryption](#)
 - [Set up a Client with WPA-Personal \(TKIP\) or WPA2-Personal \(TKIP\) Security Settings](#)
 - [Set up a Client with WPA-Personal \(AES-CCMP\) or WPA2-Personal \(AES-CCMP\) Security Settings](#)

[Enterprise Security](#)

[Enterprise Security Settings](#)

- [Configure Profiles for Device to Device \(Ad Hoc\) Networks](#)
 - [Set up a Client with Open Network Authentication and No Data Encryption \(None\)](#)
 - [Set up a Client with Open Network Authentication and WEP Data Encryption](#)
- [Configure Profiles for Infrastructure Networks](#)
 - **Network Authentication**
 - [Set up a Client with Shared Network Authentication](#)
 - [Set up a Client with WPA-Personal or WPA2 Personal Network Authentication](#)
 - [Set up a Client with WPA-Enterprise or WPA2-Enterprise Network Authentication](#)
 - **802.1x Authentication Types**
 - [Set up a Client with WEP Data Encryption and MD5 Network Authentication](#)
 - [Set up a Client with WEP Data Encryption and EAP-SIM Network Authentication](#)
 - [Set up a Client with AES-CCMP Data Encryption and TLS Network Authentication](#)
 - [Set up a Client with AES-CCMP Data Encryption and TTLS Network Authentication](#)
 - [Set up a Client with AES-CCMP Data Encryption and PEAP Network Authentication](#)
 - [Set up a Client with AES-CCMP Data Encryption and LEAP Network Authentication](#)
 - [Set up a Client with AES-CCMP Data Encryption and EAP-FAST Network Authentication](#)

Use Intel(R) PROSet/Wireless Software

The following sections describe how to use Intel(R) PROSet/Wireless to set up the required security settings for your wireless adapter. Refer to [Personal Security](#).

It also provides information about how to configure advanced security settings for your wireless adapter. This requires information from a systems administrator (corporate environment) or advanced security settings on your access point (for home users). Refer to [Enterprise Security](#).

For general information about security settings, refer to [Security Overview](#).

Personal Security

Use Personal Security if you are a home or small business user who can use a variety of simple security procedures to protect your wireless connection. Select from the list of security settings that do not require extensive infrastructure setup for your wireless network. A [RADIUS](#) or [AAA](#) server is not required.

- Review the [Set up Data Encryption and Authentication](#) information to learn about the different security types.
 - To add or change the required security settings, click [Security Settings](#) for information to set security for the selected wireless network.
 - See [Profile Management](#) for a description of when to use the Profile Wizard.
 - See [Security Overview](#) for more information about the different security options for wireless networks.
 - If you want to verify the security settings, select a wireless network in the Wireless Networks list. Click [Details](#) to review the operating mode, authentication level and data encryption.
 - See [Enterprise Security](#) to set 802.1x authentication security.
-

Personal Security Settings

Personal Security Settings Description

None WEP CKIP TKIP AES-CCMP	
Name	Setting
Personal Security	Select to open the Personal Security settings. The security settings that are available are dependent on the Operating Mode selected in the Profile Wizard : Device to Device (ad hoc) or Network (Infrastructure) .

Data Encryption	If you configure a profile for a Device to Device (ad hoc) network, select • None: No authentication required. • WEP-64 bit or WEP-128 bit: A network key or password is used for encryption. If you configure an profile for an Infrastructure network, select: • None: No authentication required. • WEP-64 bit or WEP-128 bit: A network key or password is used for encryption. • WPA-Personal (TKIP) or WPA2-Personal (TKIP): WPA-Personal utilizes the Temporal Key Integrity Protocol (TKIP) for data encryption. • WPA-Personal (AES-CCMP) or WPA2-Personal (AES-CCMP): WPA-Personal utilizes a new method for privacy protection of wireless transmissions specified in the IEEE 802.11i standard, AES-CCMP
Advanced	Select to access the Advanced Settings to configure the following options: • Auto-Connect: Select to automatically or manually connect to a profile. • Auto-Import this profile (for network administrators only). • Password protect the profile: Select to password protect a profile. • Mandatory Access Point: Select to associate the wireless adapter with a specific access point. • Start application: Specify a program to be started when a wireless connection is made.
Back	View the prior page in the Profile Wizard.
OK	Closes the Profile Wizard and saves the profile.
Cancel	Closes the Profile Wizard and cancels any changes made.
Help?	Provides the help information for the current page.

Set up Data Encryption and Authentication

In a home wireless network, you can use a variety of simple security procedures to protect your wireless connection. These include:

- Enable Wi-Fi Protected Access (WPA)
- Change your password
- Change the network name (SSID)

Wi-Fi Protected Access (WPA) encryption provides protection for your data on the network. WPA uses an encryption key called a Pre-Shared Key (PSK) to encrypt data before

transmission. Enter the same password in all of the computers and access points in your home or small business network. Only devices that use the same encryption key can access the network or decrypt the encrypted data transmitted by other computers. The password automatically initiates the Temporal Key Integrity Protocol (TKIP) for the data encryption process.

Network Keys

WEP encryption provides two levels of security:

- 64-bit key (sometimes referred to as 40-bit)
- 128-bit key (also known as 104-bit)

For improved security, use a 128-bit key. If you use encryption, all wireless devices on your wireless network must use the same encryption keys.

You can create the key yourself and specify the key length (64- or 128-bit) and key index (the location that a specific key is stored). The greater the key length, the more secure the key.

Key Length: 64-bit

Pass phrase (64-bit): Enter five (5) alphanumeric characters, 0-9, a-z or A-Z.

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

Key Length: 128-bit

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

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

With 802.11, a wireless station can be configured with up to four keys (the key index values are 1, 2, 3, and 4). When an access point or a wireless station transmits an encrypted message that uses a key stored in a specific key index, the transmitted message indicates the key index that was used to encrypt the message body. The receiving access point or wireless station can then retrieve the key that is stored at the key index and use it to decode the encrypted message body.

Personal Security: Configure Profiles for Device to Device (Ad Hoc) Networks

Set up a Client with Open Authentication and No Data Encryption (None)

In device to device mode, also called ad hoc mode, wireless computers send information directly to other wireless computers. You can use ad hoc mode to network multiple computers in a home or small office, or to set up a temporary wireless network for a meeting.

On the Intel(R)PROSet/Wireless main window, select one of the following methods to connect to a device to device network:

- Double-click a ad hoc network in the Wireless Networks list.
- Select a network in the Wireless Networks list. Click **Connect**. The Intel PROSet/Wireless software automatically detects the security settings for the wireless adapter.
- Create a device to device (ad hoc) network profile as described below.

NOTE: Device to Device (ad hoc) networks are identified with a notebook image () in the Wireless Networks and Profiles list.

To create a profile for a wireless network connection with no encryption:

1. Click **Profiles** on the Intel PROSet/Wireless main window.
2. On the Profile page, click **Add** to open the Create Wireless Profile General Settings.
3. **Profile Name:** Enter a descriptive profile name.
4. **Wireless Network Name (SSID):** Enter the network identifier.
5. **Operating Mode:** Click **Device to Device (ad hoc)**.
6. Click **Next**.
7. Click **Personal Security** to open the Security Settings.
8. **Data Encryption:** The default setting is **None**, which indicates that there is no security on this wireless network.
9. Click **OK**. The profile is added to the Profiles list and connects to the wireless network.

Set up a Client with WEP 64-bit or WEP 128-bit Data Encryption

When WEP data encryption is enabled, a network key or password is used for encryption.

You must enter the key and specify the length (64- or 128-bit) and key index (the location that a specific key is stored). The more complex the key (mixed letters and numbers), the more secure the key.

To add a network key to a device to device network connection:

1. On the Intel PROSet/Wireless main window, double-click a Device to Device (ad hoc) network in the Wireless Networks list or select the network and click **Connect**. When connected, a profile is added to the Profiles list.

NOTE: Device to Device (ad hoc) networks are identified with a notebook image () in the Wireless Networks and Profiles list.

2. Click **Profiles** to access the Profiles list. Select the network that you connected to in Step 1.
3. Click **Properties** to open the Wireless Profile Properties' General Settings. The Profile name and Wireless Network Name (SSID) display. Device to Device (ad hoc) should be selected as the Operating Mode.
4. Click **Next** to access the Security Settings.
5. Click **Personal Security**.
6. **Security Settings:** The default setting is **None**, which indicates that there is no security on this wireless network.

To add a password or network key:

1. **Security Settings:** Select either **WEP 64-bit** or **WEP 128-bit** to configure WEP data encryption with a 64- or 128-bit key.

When WEP encryption is enabled on a device, the WEP key is used 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.

2. **Password:** Enter the Wireless Security Password (Encryption Key).
 - **Pass phrase (64-bit):** Enter five (5) alphanumeric characters, 0-9, a-z or A-Z.
 - **WEP key (64-bit):** Enter 10 hexadecimal characters, 0-9, A-F.
 - **Pass phrase (128-bit):** Enter 13 alphanumeric characters, 0-9, a-z or A-Z.
 - **WEP key (128-bit):** Enter 26 hexadecimal characters, 0-9, A-F.
 3. **Key Index:** Up to four passwords may be specified by changing the Key Index.
 4. To add more than one password:
 - Select the Key Index number: **1, 2, 3, or 4.**
 - Enter the Wireless Security Password.
 - Select another Key Index number.
 - Enter another Wireless Security Password.
 5. Click **OK** to return to the Profiles list.
-

Personal Security: Configure Profiles for Infrastructure Networks

An infrastructure network consists of one or more access points and one or more computers with wireless adapters installed. Each access point must have a wired connection to a wireless network. For home users, this is usually a broadband or cable network.

Set up a Client with No (None) Data Encryption

On the Intel(R)PROSet/Wireless main window, select one of the following methods to connect to an Infrastructure network:

- Double-click an Infrastructure network in the Wireless Networks list
- Select an Infrastructure network in the Wireless Networks list. Click **Connect**. The Intel PROSet/Wireless software automatically detects the security settings for the wireless adapter.

NOTE: Infrastructure networks are identified with an access point image () in the Wireless Networks and Profiles list.

Set up a Client with WEP 64-bit or WEP 128-bit Data Encryption

When WEP data encryption is enabled, a network key or password is used for encryption.

A network key is provided for you automatically (for example, it might be provided by your wireless network adapter manufacturer), or you can enter it yourself and specify the key length (64- or 128-bit), key format (ASCII characters or hexadecimal digits), and key index

(the location where a specific key is stored). The greater the key length, the more secure the key.

To add a network key for an Infrastructure network connection:

1. On the Intel PROSet/Wireless main window, double-click an Infrastructure network in the Wireless Networks list or select the network and click **Connect**.

NOTE: Infrastructure networks are identified with an access point image () in the Wireless Networks and Profiles list.

2. Click **Profiles** to access the Profiles list.
3. Click **Properties** to open the Wireless Profile Properties' General Settings. The Profile name and Wireless Network Name (SSID) display. Network (Infrastructure) should be selected as the Operating Mode.
4. Click **Next** to access the Security Settings.
5. **Security Settings:** The default setting is **None**, which indicates that there is no security on this wireless network.

To add a password or network key:

1. **Security Settings:** Select either **WEP 64-bit** or **WEP 128-bit** to configure WEP data encryption with a 64- or 128-bit key.

When WEP encryption is enabled on an access point, the WEP key is used 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.

2. **Password:** Enter the Wireless Security Password (Pass phrase) or Encryption Key (WEP key).
 - **Pass phrase (64-bit):** Enter five (5) alphanumeric characters, 0-9, a-z or A-Z.
 - **WEP key (64-bit):** Enter 10 hexadecimal characters, 0-9, A-F.
 - **Pass phrase (128-bit):** Enter 13 alphanumeric characters, 0-9, a-z or A-Z.
 - **WEP key (128-bit):** Enter 26 hexadecimal characters, 0-9, A-F.
3. **Key Index:** Change the Key Index to set up to four passwords.

To add more than one password:

- Select the Key Index number: **1, 2, 3, or 4**.
 - Enter the Wireless Security Password.
 - Select another Key Index number.
 - Enter another Wireless Security Password.
4. Click **OK** to return to the Profiles list.

Set up a Client with WPA-Personal (TKIP) or WPA2-Personal (TKIP) Security Settings

WPA Personal Mode requires manual configuration of a pre-shared key (PSK) on the access point and clients. This PSK authenticates users a password or identifying code, on both the

client station and the access point. An authentication server is not needed. WPA Personal Mode is targeted to home and small business environments.

WPA2 is the second generation of WPA security that provides enterprise and consumer wireless users with a high level of assurance that only authorized users can access their wireless networks. WPA2 provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some corporate and government users.

To configure a profile with WPA-Personal network authentication and TKIP data encryption:

1. On the Intel PROSet/Wireless main window, double-click an Infrastructure network in the Wireless Networks list or select the network and click **Connect**.

NOTE: Infrastructure networks are identified with an access point image () in the Wireless Networks and Profiles list.

2. Click **Profiles** to access the Profiles list.
3. Click **Properties** to open the Wireless Profile Properties' General Settings. The Profile name and Wireless Network Name (SSID) display. Network (Infrastructure) should be selected as the Operating Mode.
4. Click **Next** to access the Security Settings.
5. **Security Settings:** Select **WPA-Personal (TKIP)** to provide security to a small business network or home environment. A password, called a pre-shared key (PSK), is used. The longer the password, the stronger the security of the wireless network.

If your wireless access point or router supports WPA2-Personal then you should enable it on the access point and provide a long, strong password. The longer the password, the stronger the security of the wireless network. The same password entered in the access point needs to be used on this computer and all other wireless devices that access the wireless network.

NOTE: WPA-Personal and WPA2-Personal are not interoperable.

6. **Wireless Security Password (Encryption Key):** Enter a text phrase with eight to 63 characters. Verify that the network key matches the password in the wireless access point.
7. Click **OK** to return to the Profiles list.

Set up a Client with WPA-Personal (AES-CCMP) or WPA2-Personal (AES-CCMP) Security Settings

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. For a home user or small business, WPA-Personal utilizes either Advanced Encryption Standard - Counter CBC-MAC Protocol (AES-CCMP) or Temporal Key Integrity Protocol (TKIP).

To configure a profile with WPA2-Personal network authentication and AES-CCMP data encryption:

1. On the Profile page, select a profile.
2. Click **Properties** to open the Wireless Profile Properties' General Settings. The Profile name and Wireless Network Name (SSID) display. Network (Infrastructure) should be selected as the Operating Mode.
3. Click **Next**. The Security Settings page opens.
4. **Security Settings:** Select **WPA-Personal (AES-CCMP)** to provide this level of security in the small network or home environment. It uses a password also called a pre-shared key (PSK). The longer the password, the stronger the security of the wireless network.

AES-CCMP (Advanced Encryption Standard - Counter CBC-MAC Protocol) is the new method for privacy protection of wireless transmissions specified in the IEEE 802.11i standard. AES-CCMP provides a stronger encryption method than TKIP. Choose AES-CCMP as the data encryption method whenever strong data protection is important.

If your Wireless access point or router supports WPA2-Personal then you should enable it on the access point and provide a long, strong password. The same password entered into access point needs to be used on this computer and all other wireless devices that access the wireless network.

NOTE: WPA-Personal and WPA2-Personal are not interoperable.

Some security solutions may not be supported by your computer's operating system. You may require additional software or hardware as well as wireless LAN infrastructure support. Contact your computer manufacturer for details.

Set Password

1. **Wireless Security Password (Encryption Key).** Enter a text phrase (length is between eight and 63 characters). Verify that the network key used matches the wireless access point key.
2. Click **OK** to return to the Profiles list.

[Back to Top](#)

[Back to Contents](#)

Enterprise Security

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

Use Enterprise Security if your network environment requires 802.1x authentication.

- 802.1x authentication methods, include passwords, certificates and [smart cards](#).
- 802.1x authentication types are: [MD5](#), [EAP-SIM](#), [LEAP](#), [TLS](#), [TTLS](#), [PEAP](#), [EAP-FAST](#).
- See [Profile Management](#) for a description of when the Profile Wizard is launched.
- See [Security Overview](#) for more information on the different security options for wireless networks.

- See [Personal Security](#) to set basic WEP or WPA security in a non-enterprise environment (home, small business).

Enterprise Security Settings

Enterprise Security Settings Description

Name	Setting
Enterprise Security	Select to open the Enterprise Security settings. The security settings that are available are dependent on the Operating Mode selected: Device to Device (ad hoc) or Network (Infrastructure) .
Network Authentication	If you configure a Device to Device (ad hoc) profile, the default is Open authentication. If you configure an Infrastructure profile, select: • Open authentication: Any wireless station can request authentication. • Shared authentication: Uses an encryption key known only to the receiver and sender of data. • WPA-Personal or WPA2 Personal: Uses a password also called a pre-shared key (PSK). • WPA-Enterprise or WPA2-Enterprise: Use on enterprise networks with an 802.1x RADIUS server.
Data Encryption	• None: No encryption. • WEP • CKIP • TKIP • AES-CCMP
Enable 802.1x (Authentication Type)	Click to open the following 802.11x authentication types: • MD5 • EAP-SIM • TLS • TTLS • PEAP • LEAP • EAP-FAST

Cisco Options	Click to view the Cisco Compatible Extensions . NOTE: Cisco Compatible Extensions are automatically enabled for CKIP and LEAP profiles.
Advanced button	Select to access the Advanced Settings to configure the following options: • Auto-Connect: Select to automatically or manually connect to a profile. • Auto-Import this profile (for network administrators only). • Mandatory Access Point: Select to associate the wireless adapter with a specific access point. • Password Protection: Select to password protect a profile. • Start application: Specify a program to be started when a wireless connection is made.
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	Closes the Profile Wizard and saves the profile.
Cancel	Closes the Profile Wizard and cancels any changes made.
Help?	Provides the help information for the current page.

Enterprise Security: Configure Profiles for Device to Device (Ad Hoc) Networks

Set up a Client with Open Network Authentication and No (None) Data Encryption

When **Open** authentication is used, 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 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 can gain access to the network.

In Device to Device (ad hoc) mode, wireless computers send information directly to other wireless computers. You can use ad hoc mode to network multiple computers in a home or small office, or to set up a temporary wireless network for a meeting.

1. On the Intel(R)PROSet/Wireless main window, select one of the following methods to connect to a device to device network:
 - Double-click a Device to Device (ad hoc) network in the Wireless Networks list.

- Select a Device to Device (ad hoc) network in the Wireless Networks list. Click **Connect**. The Intel PROSet/Wireless software automatically detects the security settings for the wireless adapter.

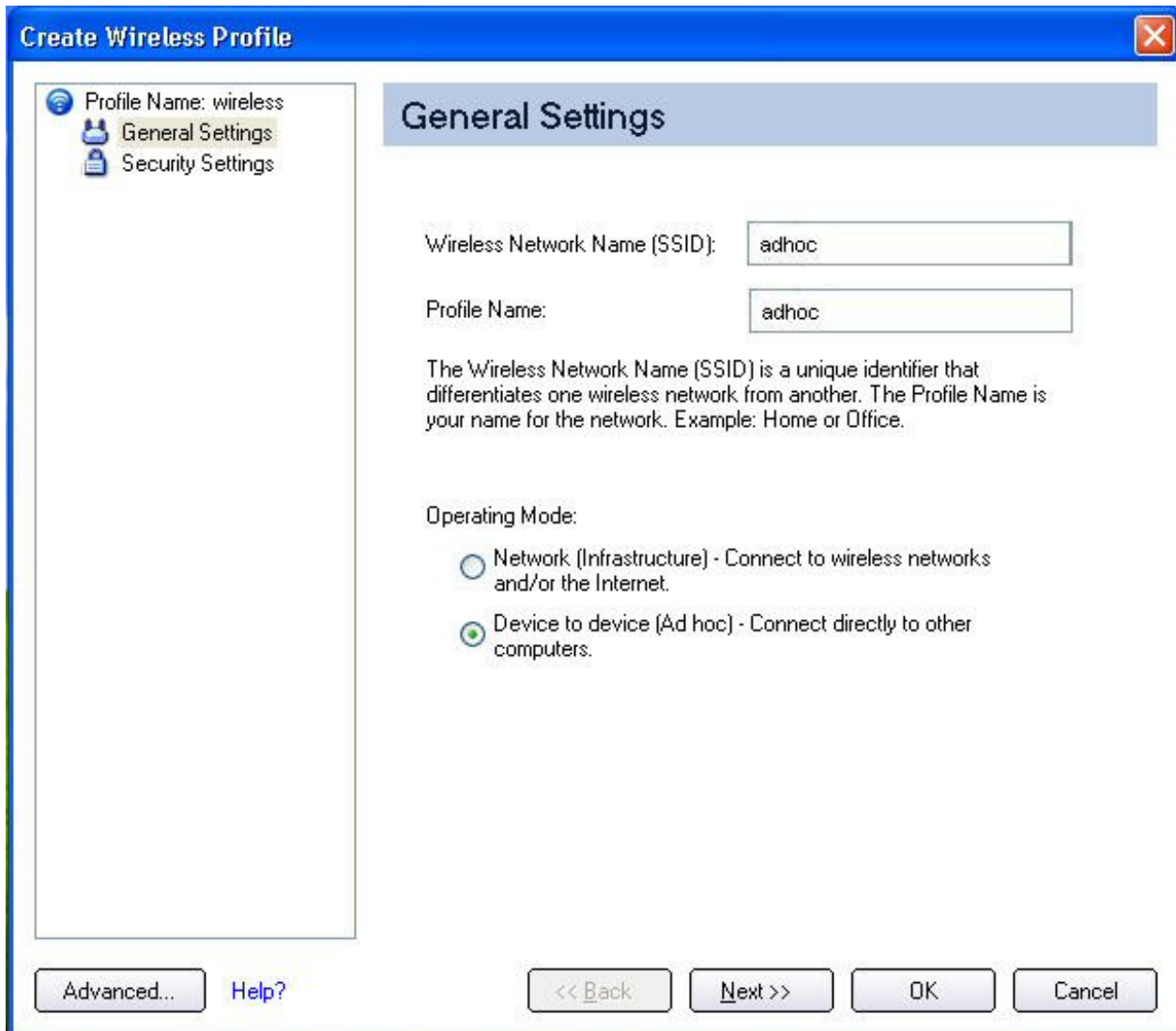
NOTE: Device to Device (ad hoc) networks are identified with a notebook image () in the Wireless Networks and Profiles list.

- Authentication:
 - If no authentication is required, the network connects without a prompt to enter any log-on credentials. Any wireless device with the correct network name (SSID) is able to associate with the network devices.
 - If Data Encryption is required, select WEP. You are asked to select either a 64-bit or 128-bit encryption level Security Password (Encryption Key) and a Key Index. These values must match the various devices in your ad hoc network, or data is not transferred.

NOTE: If you need to edit or change the wireless network settings, refer to [Profile Management](#) for more information.

To create a profile for a wireless network connection with no encryption:

1. Click **Profiles** on the Intel PROSet/Wireless main window.
2. On the Profile page, click **Add** to open the Create Wireless Profile General Settings.



The screenshot shows the 'Create Wireless Profile' dialog box with the 'General Settings' tab selected. The left sidebar shows 'Profile Name: wireless', 'General Settings' (selected), and 'Security Settings'. The main area contains the following fields and options:

- Wireless Network Name (SSID):** Text box containing 'adhoc'.
- Profile Name:** Text box containing 'adhoc'.
- Operating Mode:**
 - ☐ Network (Infrastructure) - Connect to wireless networks and/or the Internet.
 - ☒ Device to device (Ad hoc) - Connect directly to other computers.

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

Advanced... Help? << Back Next >> OK Cancel

3. **Wireless Network Name (SSID):** Enter the network identifier.
4. **Profile Name:** Enter a descriptive profile name.
5. **Operating Mode:** Click **Device to Device (ad hoc)**.
6. Click **Next**

Create Wireless Profile

Profile Name: ad hoc

General Settings

Security Settings

Security Settings

☐ Personal Security ☒ Enterprise Security

Network Authentication: Open

Data Encryption: None

☐ Enable 802.1x

Authentication Type: None Cisco Options...

NOTE: There is no security on this wireless network.

Advanced... Help? << Back Next >> OK Cancel

7. Click **Enterprise Security** to open the Security Settings.
8. **Network Authentication: Open** (Selected).

When **Open** authentication is used, 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 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 can gain access to the network. Device to Device (ad hoc) networks always operate with **Open** authentication.

9. **Data Encryption:** None is the default.
10. Click **OK**. The profile is added to the Profiles list and connects to the wireless network.

Set up a Client with Open Network Authentication and WEP Data Encryption

On the Intel PROSet/Wireless main window, select one of the following methods to connect to a device to device network:

1. Double-click a Device to Device (ad hoc) network in the Wireless Networks list.
2. Select a Device to Device (ad hoc) network in the Wireless Networks list. Click **Connect**. The Intel PROSet/Wireless software automatically detects the security settings for the wireless adapter.

NOTE: Device to Device (ad hoc) networks are identified with a notebook image (



) in the Wireless Networks and Profiles list.

3. If Data Encryption is required, you may select WEP. You are asked to select either a 64-bit or 128-bit encryption level Security Password (Encryption Key) and a Key Index. These values must match the various devices in your device to device (ad hoc) network, or data is not transferred.

NOTE: If you need to edit or change the wireless network settings, refer to [Profile Management](#) for more information.

To create a profile for a wireless network connection with WEP encryption:

1. Click **Profiles** on the Intel PROSet/Wireless main window.
2. On the Profile page, click **Add** to open the Create Wireless Profile Wizard's General Settings.
3. **Wireless Network Name (SSID):** Enter the network identifier.
4. **Profile Name:** Enter a descriptive profile name.
5. **Operating Mode:** Click **Device to Device (ad hoc)**.
6. Click **Next**.
7. Click **Enterprise Security** to open the Security Settings.
8. **Network Authentication:** **Open** is selected (Default). Ad hoc networks only use Open authentication.
9. **Data Encryption:** Select **WEP**. WEP data encryption can be configured with 64- or 128-bit key. If the wireless device does not have the correct WEP key, the device is unable to transmit or decrypt data.
10. **Encryption Level:** Select **64-** or **128-bit**.
11. **Wireless Security Password (Encryption Key):** Enter the wireless network Password (WEP Key). The Password is the same value used by the wireless access point or router. Contact your administrator for this password.
 - **Pass phrase (64-bit):** Enter five (5) alphanumeric characters, 0-9, a-z, or A-Z.
 - **Hex key (64-bit):** Enter 10 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 hexadecimal characters, 0-9, A-F.
12. **Key Index:** Select **1**, **2**, **3**, or **4**. Up to four passwords may be specified by changing the Key Index.

To change the security settings:

1. Click **Profiles** on the Intel PROSet/Wireless main window. The network that you just connected to is listed in the Profiles list.
 2. Select the wireless network.
 3. Click **Properties** to open the Wireless Profile Properties General Settings. The **Wireless Network Name (SSID)** and **Profile Name** are already defined. **Device to Device (ad hoc)** is selected as the operating mode.
 4. Click **Next** to access the Security Settings.
 5. Click **Enterprise Security**.
 6. **Network Authentication:** Open is the default. No authentication is used.
 7. **Data Encryption:** WEP is selected. You can change the WEP key, key index or encryption level.
 8. Click **OK** to return to the Profiles list after you have completed your changes.
-

Enterprise Security: Configure Profiles for Infrastructure Networks

An infrastructure network consists of one or more access points and one or more computers with wireless adapters installed. Each access point must have a wired connection to a wireless network.

Set up a Client with No Authentication or Data Encryption (None)

On the Intel(R)PROSet/Wireless main page, select one of the following methods to connect to an Infrastructure network:

- Double-click an Infrastructure network in the Wireless Networks list.
- Select an Infrastructure network in the Wireless Networks list. Click **Connect**. The Intel PROSet/Wireless software automatically detects the security settings for the wireless adapter.

If there is no authentication required, the network connects without a prompt to enter any log-on credentials. Any wireless device with the correct network name (SSID) is able to associate with other devices in the network.

To create a profile for a wireless network connection with no encryption:

1. Click **Profiles** on the Intel PROSet/Wireless main window.
2. On the Profile page, click **Add** to open the Create Wireless Profile General Settings.
3. **Profile Name:** Enter a descriptive profile name.
4. **Wireless Network Name (SSID):** Enter the network identifier.
5. **Operating Mode:** Click **Network (Infrastructure)**
6. Click **Next**.
7. Click **Enterprise Security** to open the Security Settings.
8. **Network Authentication: Open** (Selected).

Open authentication allows a wireless device access to the network without 802.11 authentication. If no encryption is enabled on the network, any wireless device with

the correct network name (SSID) can associate with an access point and gain access to the network.

9. **Data Encryption:** None is the default.
 10. Click **OK**. The profile is added to the Profiles list and connects to the wireless network .
-

Set up a Client with Shared Network Authentication

When **Shared Key** authentication is used, 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 or CKIP key. The client access is granted only if it passes a challenge-based authentication. CKIP provides stronger data encryption than WEP, but not all operating systems and access points support it.

NOTE: While shared key would appear to be the better option for a higher level of security, a known weakness is created by the clear text transmission of the challenge string to the client. Once an invader finds the challenge string, the shared authentication key can be easily reverse engineered. Therefore, open authentication is actually, and counter intuitively, more secure. To create a profile with shared authentication:

1. Click **Profiles** on the Intel PROSet/Wireless main window.
 2. On the Profile Page, click **Add** to open the Create Wireless Profile General Settings.
 3. **Profile Name:** Enter a descriptive profile name.
 4. **Wireless Network Name (SSID):** Enter the network identifier.
 5. **Operating Mode:** Click **Network (Infrastructure)**.
 6. Click **Next** to access the Security Settings.
 7. Click **Enterprise Security**.
 8. **Network Authentication:** Select **Shared**. Shared authentication is accomplished with a pre-configured WEP key.
 9. **Data Encryption:** Select None, WEP (64- or 128-bit), or [CKIP](#) (64- or 128-bit).
 10. **Enable 802.1x:** Disabled.
 11. **Encryption Level: 64- or 128-bit:** When switching between 64- and 128-bit encryption, the previous settings are erased and a new key must be entered.
 12. **Key Index:** Select **1, 2, 3, or 4**. Change the Key Index to specify up to four passwords.
 13. **Wireless Security Password (Encryption Key):** Enter the wireless network password (WEP Encryption Key). This password is the same value used by the wireless AP or router. Contact your administrator for this password.
 - **Pass phrase (64-bit):** Enter five (5) alphanumeric characters, 0-9, a-z or A-Z.
 - **Hex key (64-bit):** Enter 10 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 hexadecimal characters, 0-9, A-F.
-

Set up a Client with WPA-Personal or WPA2-Personal Network Authentication

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 key-exchange and only works with dynamic encryption keys. If your wireless AP or router supports WPA-Personal and WPA2-Personal then you should enable it on the AP and provide a long, strong password. For personal or home networks without a RADIUS or AAA server, use Wi-Fi Protected Access Personal.

- **WPA-Personal:** A wireless security method that provides strong data protection and prevents unauthorized network access for small networks. It uses Temporal Key Integrity Protocol (TKIP) encryption or [AES-CCMP](#) and protects against unauthorized network access through the use of a pre-shared key (PSK).
- **WPA2-Personal:** A follow-on wireless security method to WPA that provides stronger data protection and prevents unauthorized network access for small networks.

NOTE: WPA-Personal or WPA2 Personal are not interoperable.

Some security solutions may not be supported by your computer's operating system and may require additional software or certain hardware as well as wireless LAN infrastructure support. Check with your computer manufacturer for details.

To add a profile with WPA-Personal or WPA2-Personal network authentication:

1. Click **Profiles** on the Intel PROSet/Wireless main window.
2. On the Profile page, click **Add** to open the Profile Wizard's General Settings.
3. **Profile Name:** Enter a descriptive profile name.
4. **Wireless Network Name (SSID):** Enter the network identifier.
5. **Operating Mode:** Click **Network (Infrastructure)**.
6. Click **Next** to access the Security Settings.
7. Click **Enterprise Security**.
8. **Network Authentication:** Select **WPA-Personal or WPA2-Personal**. See [Security Overview](#).
9. **Data Encryption:** Select one of the following:
 - **TKIP** provides per-packet key mixing, a message integrity check and a rekeying mechanism.
 - **AES-CCMP** (Advanced Encryption Standard - Counter CBC-MAC Protocol) is used as the data encryption method whenever strong data protection is important.
10. **Password:** Enter a text phrase from 8 to 63 characters. The longer the password, the stronger the security of the wireless network. The same password entered into an access points needs to be used on this computer and all other wireless devices that access the wireless network.

Set up a Client with WPA-Enterprise or WPA2-Enterprise Network Authentication

WPA2-Enterprise requires an authentication server.

- **WPA-Enterprise:** A wireless security method that provides strong data protection for multiple users and large managed networks. It uses the 802.1X authentication framework with TKIP encryption and prevents unauthorized network access by verifying network users through an authentication server.
- **WPA2-Enterprise:** The follow-on wireless security method to WPA that provides

stronger data protection for multiple users and large managed networks. It prevents unauthorized network access by verifying network users through an authentication server.

NOTE: WPA-Enterprise and WPA2-Enterprise are not interoperable.

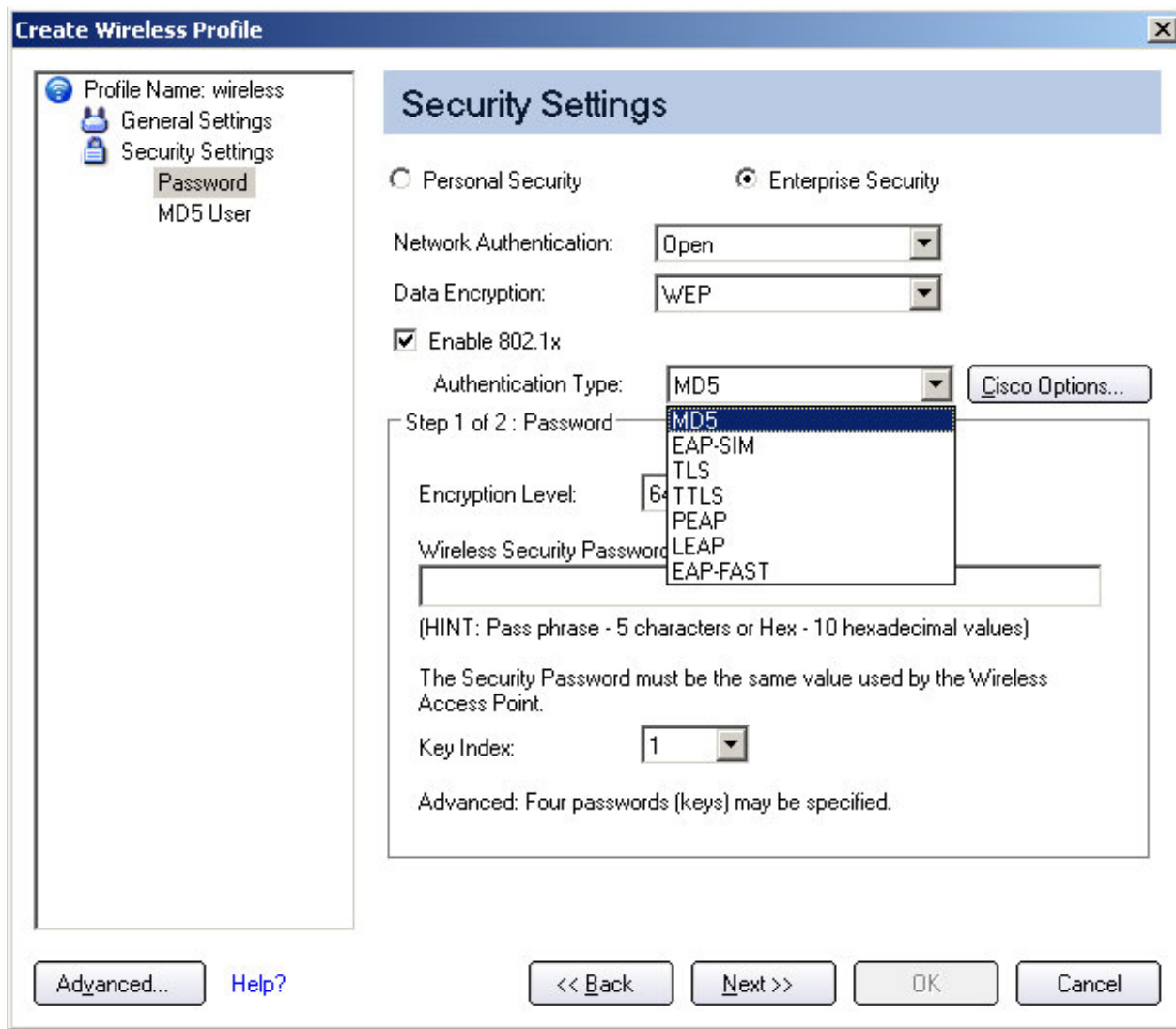
To add a profile that uses WPA - Enterprise or WPA2 - Enterprise authentication:

1. Obtain a user name and password on the RADIUS server from your administrator.
2. Certain Authentication Types require that obtain and install a client certificate. Refer to [Setting up the Client for TLS authentication](#) or consult your administrator.
3. Click **Profiles** on the Intel PROSet/Wireless main window.
4. On the Profile page, click **Add** to open the Profile Wizard's General Settings.
5. **Profile Name:** Enter a descriptive profile name.
6. **Wireless Network Name (SSID):** Enter the network identifier.
7. **Operating Mode:** Click **Network (Infrastructure)**.
8. Click **Next**.
9. Click **Enterprise Security**.
10. **Network Authentication:** Select **WPA-Enterprise** or **WPA2-Enterprise**.
11. **Data Encryption:** Select one of the following:
 - **TKIP** provides per-packet key mixing, a message integrity check and a rekeying mechanism.
 - **AES-CCMP** (Advanced Encryption Standard - Counter CBC-MAC Protocol) is used as the data encryption method whenever strong data protection is important. [AES-CCMP](#) is recommended.
12. **Enable 802.1x:** Selected.
13. **Authentication Type:** Select one of the following: [MD5](#), [EAP-SIM](#), [LEAP](#), [TLS](#), [TTLS](#), [PEAP](#), [EAP-FAST](#).

Set up a Client with WEP Data Encryption and MD5 Network Authentication

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. To add WEP and MD5 authentication to a new profile:

NOTE: Before you begin, you need to know the user name and password on the RADIUS server that grants access to the network.



1. Click **Profiles** on the Intel PROSet/Wireless main window.
2. On the Profile page, click **Add** to open the Profile Wizard's General Settings.
3. **Profile Name:** Enter a descriptive profile name.
4. **Wireless Network Name (SSID):** Enter the network identifier.
5. **Operating Mode:** Click **Network (Infrastructure)**.
6. Click **Next**.
7. Click **Enterprise Security**.
8. **Network Authentication:** Select **Open** (Recommended).
9. **Data Encryption:** Select **WEP**.
10. Click **802.1x Enabled**.
11. **Authentication type:** Select MD5.

Step 1 of 2: Password

1. **Encryption Level:** Select either **64-** or **128-bit**.
2. **Wireless Security Password (Encryption Key):** Enter your network key (wireless security password) for your wireless network. Verify that the network key matches the wireless AP.
 - o **Use pass phrase:** Enter a text phrase, up to 5 (64-bit) or 13 (128-bit) alphanumeric characters (0-9, a-z or A-Z).
 - o **Use hex key:** Enter up to 10 alphanumeric characters (64-bit, 0-9, A-F) or 26 alphanumeric characters (128-bit, 0-9, A-F).

3. **Key Index:** Select **1, 2, 3** or **4**. (Default key is 1.)
4. Click **Next**.

The screenshot shows the 'Create Wireless Profile' dialog box with the 'Security Settings' tab selected. On the left, a tree view shows 'Profile Name: wireless', 'General Settings', 'Security Settings', 'Password', and 'MD5 User'. The 'Security Settings' section has two radio buttons: 'Personal Security' (unselected) and 'Enterprise Security' (selected). Below these are dropdown menus for 'Network Authentication' (set to 'Open') and 'Data Encryption' (set to 'WEP'). A checkbox 'Enable 802.1x' is checked. Below it, 'Authentication Type' is set to 'MD5', with a 'Cisco Options...' button to its right. A sub-section titled 'Step 2 of 2: MD5 User' contains three radio buttons: 'Use the Windows logon user name and password' (unselected), 'Prompt for the user name and password' (unselected), and 'Use the following user name and password:' (selected). Below this are four text fields: 'User Name' (containing 'User Name'), 'Domain' (containing 'Domain Name'), 'Password' (masked with 'xxxxxxxx'), and 'Confirm Password' (masked with 'xxxxxxxx'). At the bottom are buttons for 'Advanced...', 'Help?', '<< Back', 'Next >>', 'OK', and 'Cancel'.

Step 2 of 2: MD5 User

1. Select one of the following credential methods:
 - **Use Windows logon user name and password:** The 802.1x credentials match your Windows user name and password. Before connection, you are prompted for your Windows logon credentials.

NOTE: This option is unavailable if Pre-Logon Connect is not selected during installation of the Intel PROSet/Wireless software. Refer to [Install or Uninstall the Single Sign On Feature](#).

- **Prompt for the user name and password:** Prompt for your user name and password every time you log onto the wireless network.
- **Use the following user name and password:** Use your saved credentials to log onto the network.
 - **User Name:** This user name must match the user name that is set in the authentication server by the administrator prior to client 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 identity is securely transmitted to the server only after an encrypted channel has been established.

- **Domain:** Name of the domain on the authentication server. The server name identifies a domain or one of its sub-domains (for example, zeelans.com, where the server is blueberry.zeelans.com). **NOTE:** Contact your administrator to obtain the domain name.
- **Password:** Specifies the user password. The password characters appear as asterisks. This password must match the password that is set in the authentication server.
- **Confirm Password:** Reenter the user password.

2. Click **OK** to save the credentials.
3. Click **Connect** to connect to the selected wireless network.

If you did not select **Use Windows logon** on the Security Settings page and also did not configure user credentials, an **Enter Credentials** message appears when you attempt to connect to this profile. Enter your user name and password. Click **Save User Credentials** to save the credentials for future use with this 802.1x profile.

4. Click **OK** to close Intel PROSet/Wireless.

Set up a Client with WEP Data Encryption and EAP-SIM Network Authentication

EAP-SIM uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. EAP-SIM requires you to enter a user verification code, or Personal Identification Number (PIN), for communication with the Subscriber Identity Module (SIM) card. A SIM card is a special smart card that is used by Global System for Mobile Communications (GSM) based digital cellular networks. To add a profile with EAP-SIM authentication:

1. On the Profile page, click **Add** to open General Settings.
2. **Profile Name:** Enter a profile name.
3. **Wireless Network Name (SSID):** Enter the network identifier.
4. **Operating Mode:** Click **Network (Infrastructure)**.
5. Click **Next** to access the Security Settings.
6. Click **Enterprise Security**.
7. **Network Authentication:** Select **Open** (Recommended).
8. **Data Encryption:** Select **WEP**.
9. Click **Enable 802.1x**.
10. **Authentication type:** Select EAP-SIM.

EAP-SIM authentication can be used with:

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

EAP-SIM User (optional)

1. **Specify user name (identity):** Click to specify the user name.

- **User Name:** Enter the user name assigned to the SIM card.

2. Click **OK**.

Set up a Client with AES-CCMP Data Encryption and TLS Network Authentication

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

To add a profile with TLS authentication:

1. Click **Profiles** on the Intel PROSet/Wireless main window.
2. On the Profile page, click **Add** to open the Profile Wizard's General Settings.
3. **Profile Name:** Enter a descriptive profile name.
4. **Wireless Network Name (SSID):** Type the network identifier.
5. **Operating Mode:** Click **Network (Infrastructure)**.
6. Click **Next** to access the Security Settings.
7. Click **Enterprise Security**.
8. **Network Authentication:** Select **WPA-Enterprise** or **WPA2-Enterprise**.
9. **Data Encryption:** Select **AES-CCMP** (Recommended).
10. **Enable 802.1x:** Selected.
11. **Authentication Type:** Select TLS to be used with this connection.

Create Wireless Profile

Profile Name: wireless

General Settings

Security Settings

TLS User

TLS Server

Security Settings

☐ Personal Security ☒ Enterprise Security

Network Authentication: WPA2 - Enterprise

Data Encryption: AES - CCMP

☒ Enable 802.1x

Authentication Type: TLS Cisco Options...

Step 1 of 2: TLS User

☐ Use my smart card

☒ Use the certificate issued to this computer

☐ Use a user certificate on this computer

Click the Select button to choose a certificate: Select...

Issued To:

User Name:

Advanced... Help? << Back Next >> OK Cancel

Step 1 of 2: TLS User

1. Obtain and install a client certificate, refer to [Set up the Client for TLS authentication](#) or consult your system administrator.
2. Select one of the following to obtain a certificate:
 - **Use my smart card:** Select if the certificate resides on a smart card.
 - **Use the certificate issued to this computer:** Click **Select** to choose a certificate that resides in the machine store.
 - **Use a user certificate on this computer.** Click **Select** to choose a certificate that resides on this computer.
3. Click **Next**.

Create Wireless Profile

Profile Name: wireless

General Settings

Security Settings

TLS User

TLS Server

Security Settings

☐ Personal Security ☒ Enterprise Security

Network Authentication: WPA2 - Enterprise

Data Encryption: AES - CCMP

☒ Enable 802.1x

Authentication Type: TLS Cisco Options...

Step 2 of 2: TLS Server

☒ Validate Server Certificate

Certificate Issuer: Any Trusted CA

☐ Allow Intermediate Certificates

☐ Specify Server or Certificate Name

Server or Certificate Name:

☐ Server name must match the specified entry exactly

☒ Domain name must end in with the specified entry

Advanced... Help? << Back Next >> OK Cancel

Step 2 of 2: TLS Server

Select one of the following:

1. Validate Server Certificate:

- **Certificate Issuer:** The server certificate received during TLS message exchange must be issued by this certificate authority (CA). Trusted intermediate certificate authorities and root authorities whose certificates exist in the system store are available for selection. 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 CA or additionally by one of its intermediate certificate authorities. Select to allow a number of unspecified certificates to be in the server certificate chain between the server certificate and the specified CA. If cleared, then the specified CA must have been directly issued by the server certificate.

2. Specify Server or Certificate Name:

Select if you want to specify your server or certificate name.

The server name or domain to which the server belongs, depends 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 (for example, Servername.Domain name).

- **Domain name must end in specified name:** When selected, the server name identifies a domain and the certificate must have a server name belonging to this domain or to one of its sub-domains (for example, zeelans.com, where the server is blueberry.zeelans.com). **NOTE:** These parameters should be obtained from the administrator.

3. Click **OK** to close the security settings.

Set up a Client with AES-CCMP Data Encryption and TTLS Network Authentication

TTLS authentication: These settings define the protocol and credentials used to authenticate a user. 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 (for example, MD5 Challenge over this encrypted channel to enable server validation). The challenge and response packets are sent over a non-exposed TLS encrypted channel. The following example describes how to use WPA with AES-CCMP encryption with TTLS authentication.

To set up a client with TTLS Network Authentication:

1. Click **Profiles** on the Intel PROSet/Wireless main window.
2. On the Profile page, click **Add** to open the Profile Wizard's General Settings.
3. **Profile Name:** Enter a descriptive profile name.
4. **Wireless Network Name (SSID):** Enter the network identifier.
5. **Operating Mode:** Click Network (Infrastructure).
6. **Click Next to access the Security Settings.**
7. Click **Enterprise Security**.
8. **Network Authentication:** Select **WPA-Enterprise** or **WPA2-Enterprise**.
9. **Data Encryption:** Select **TKIP** or **AES-CCMP** (Recommended).
10. **Enable 802.1x:** Selected.
11. **Authentication Type:** Select **TTLS** to be used with this connection.

Step 1 of 2: TTLS User

1. **Authentication Protocol:** This parameter specifies the authentication protocol operating over the TTLS tunnel. The protocols are: [PAP](#) (Default), [CHAP](#), MD5, [MS-CHAP](#) and MS-CHAP-V2. See [Security Overview](#) for more information.

For PAP, CHAP, MD5, MS-CHAP, and MS-CHAP-V2 protocols, select one of these authentication methods:

- **Use the Windows logon:** Select to retrieve the user's credentials from the user's Windows logon process.

NOTE: This option is unavailable if Pre-Logon Connect is not selected during installation of the Intel PROSet/Wireless software. Refer to [Install or Uninstall the Single Sign On Feature](#).

- **Prompt each time I connect:** Select to prompt for user name and password before you connect to the wireless network. The user name and password must be first set in the authentication server by the administrator.
 - **Use the following:** The user name and password are securely (encrypted) saved in the profile.
 - **User Name:** This user name must match the user name that is set in the authentication server.
 - **Domain:** Name of the domain on the authentication server. The server name identifies a domain or one of its subdomains (for example, zeelans.com, where the server is blueberry.zeelans.com). **NOTE:** Contact your administrator to obtain the domain name.
 - **Password:** This password must match the password that is set in the authentication server. The entered password characters display as asterisks.
 - **Confirm Password:** Reenter the user password.
2. **Roaming Identity:** If the Roaming Identity is cleared, %domain%\%username% is the default.

When 802.1x MS RADIUS is used as an authentication server, the server authenticates the device that uses the **Roaming Identity** user name from Intel PROSet/Wireless software, 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 user name (dotNet user) for EAP clients. When 802.1x MS RADIUS is used, enter a valid user name. For all other servers, this is optional. Therefore, it is recommended to use the desired realm (for example, anonymous@myrealm) instead of a true identity.

Step 2 of 2: TTLS Server

1. **Validate Server Certificate:** Selected.
2. **Certificate Issuer:** The server certificate received during the TTLS message exchange must have been issued by this certificate authority (CA). Trusted intermediate certificate authorities and root authorities whose certificates exist in the system store are available for selection. If Any Trusted CA is selected, any CA in the list is acceptable.
3. **Specify Server or Certificate Name:** The server name or domain to which the server belongs, whichever of the following 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 (for example, Servername.Domain name).
 - **Domain name must end in specified name:** When selected, the server name identifies a domain and the certificate must have a server name belonging to this domain or to one of its subdomains (for example, zeelans.com, where the server is blueberry.zeelans.com)

NOTE: These parameters should be obtained from the administrator.

Set up a Client with AES-CCMP Data Encryption and PEAP Network Authentication

PEAP authentication: PEAP settings are required for the authentication of the client to the

authentication server. The client uses EAP-TLS to validate the server and create a TLS-encrypted channel between client and server. The client can use another EAP mechanism (for example, Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2), over this encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel. The following example describes how to use WPA with AES-CCMP or TKIP encryption with PEAP authentication.

To set up a client with PEAP Authentication:

Obtain and install a client certificate. Refer to [Set up the Client for TLS authentication](#) or consult your administrator.

1. Click **Profiles** on the Intel PROSet/Wireless main window.
2. On the Profile page, click **Add** to open the Profile Wizard's General Settings.
3. **Profile Name:** Enter a descriptive profile name.
4. **Wireless Network Name (SSID):** Enter the network identifier.
5. **Operating Mode:** Click **Network (Infrastructure)**.
6. Click **Next** to access the Security Settings.
7. Click **Enterprise Security**.
8. **Network Authentication:** Select **WPA-Enterprise** or **WPA2-Enterprise**.
9. **Data Encryption:** Select **TKIP** or **AES-CCMP** (Recommended).
10. **Enable 802.1x:** Selected.
11. **Authentication Type:** Select **PEAP** to be used with this connection.

Step 1 of 2: PEAP User

PEAP relies on Transport Layer Security (TLS) to allow unencrypted authentication types (for example, EAP-Generic Token Card (GTC) and One-Time Password (OTP) support).

1. **Authentication Protocol:** Select either [GTC](#), [MS-CHAP-V2](#) (Default), or [TLS](#). Refer to [Authentication Protocols](#).
2. **User Credentials:** Select one of the following :
3. **Use Windows Logon:** Allows the 802.1x credentials to match your Windows user name and password. Before connection, you are prompted for your Windows logon credentials.
4. **Prompt each time I connect:** Prompts for user name and password every time you log onto the network.
5. **Use the following:** The user name and password are securely (encrypted) saved in the profile.
 - **User Name:** This user name must match the user name that is set in the authentication server.
 - **Domain:** Name of the domain on the authentication server. The server name identifies a domain or one of its subdomains (for example, zeelans.com, where the server is blueberry.zeelans.com). **NOTE:** Contact your administrator to obtain the domain name.
 - **Password:** This password must match the password that is set in the authentication server. The entered password characters display as asterisks.
 - **Confirm Password:** Reenter the user password.
6. **Roaming Identity:** If the Roaming Identity is cleared, %domain%\%username% is the default.

When 802.1x MS RADIUS is used as an authentication server, the authentication server authenticates the device with the **Roaming Identity**

user name from the Intel PROSet/Wireless utility 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 user name (dotNet user) for EAP clients. Enter a valid user name whenever 802.1x MS RADIUS is used. For all other servers, this is optional, therefore, it is recommended that you no use a true identity, but instead the desired realm (for example, anonymous@myrealm).

Configure Roaming Identity to support multiple users:

If you use a [Pre-Logon or Common](#) connection profile that requires the roaming identity to be based on the Windows logon credentials, the creator of the profile can add a roaming identity that uses %username% and %domain%. The roaming identity is parsed and the appropriate log on information is substituted for the keywords. This allows maximum flexibility in configuring the roaming identity while allowing multiple users to share the profile.

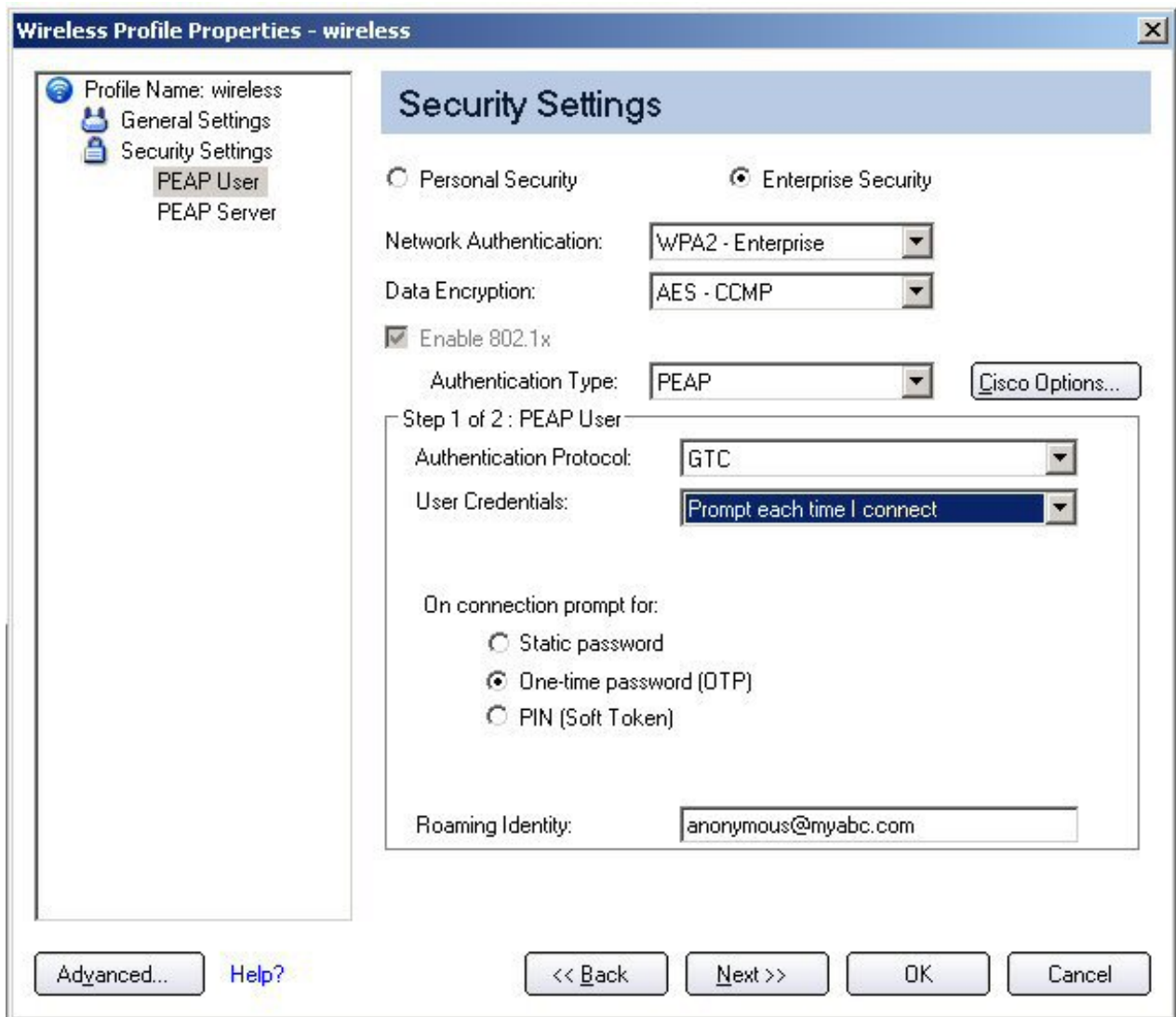
Please refer to your authentication server user guide for directions about how to format a suitable roaming identity. Possible formats are:

%domain%\%username%
%username%@%domain%
%username%@%domain%.com
%username%@mynetwork.com

If Roaming Identity is cleared, %domain%\%username% is the default.

Notes about the credentials: This user name and domain must match the user name that is set in the authentication server by the administrator prior to client 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 identity is securely transmitted to the server only after an encrypted channel has been verified and established.

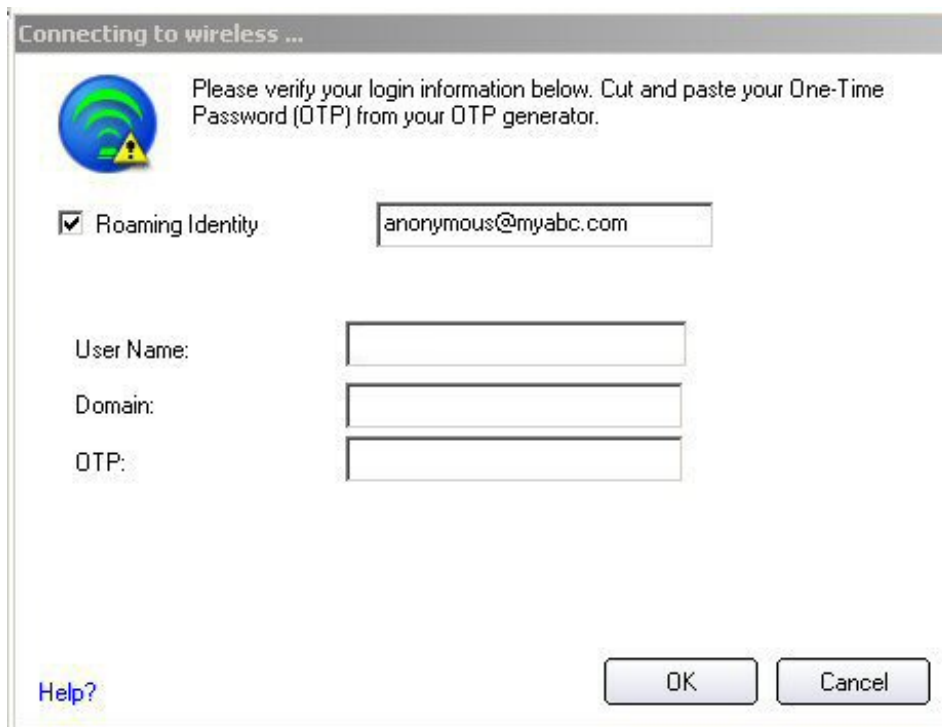
Authentication Protocols: These parameter specifies the authentication protocols that can operate over the TTLS tunnel. Below are instructions on how to configure a profile that uses PEAP authentication with [GTC](#), [MS-CHAP-V2](#) (Default), or [TLS](#) authentication protocols. **Generic Token Card (GTC)**



To configure a one-time password:

1. **Authentication Protocol:** Select **GTC** (Generic Token Card).
2. **User Credentials:** Select **Prompt each time I connect**
3. **On connection prompt for:** Select one of the following:
 - **Static password:** On connection, enter the user credentials.
 - **One-time password (OTP):** Obtain the password from a hardware token device.
 - **PIN (Soft Token):** Obtain the password from a soft token program.
4. Click **OK**.
5. Select the profile on the Wireless Networks list.
6. Click **Connect**. When prompted, enter the user name, domain and one-time password (OTP).
7. Click **OK**. You are asked to verify your log in information.

NOTE: The **Prompt each time I connect** option is unavailable if an Administrator has cleared the Cache Credentials setting in the the Administrator Tool. Refer to [Administrator Settings](#) for more information.



Connecting to wireless ...

Please verify your login information below. Cut and paste your One-Time Password (OTP) from your OTP generator.

☒ Roaming Identity

User Name:

Domain:

OTP:

[Help?](#)

MS-CHAP-V2. This parameter specifies the authentication protocol operating over the PEAP tunnel.

1. **User Credentials:** Select one of the following options:

- **Use Windows Logon:** Allows the 802.1x credentials to match your Windows user name and password. Before connection, you are prompted for your Windows logon credentials.
- **Prompt each time I connect:** Prompts for user name and password every time you log onto the network.
- **Use the following user name and password:** The user name and password are securely (encrypted) saved in the profile.
 - **User Name:** This user name must match the user name that is set in the authentication server.
 - **Domain:** Name of the domain on the authentication server. The server name identifies a domain or one of its subdomains (for example, zeelans.com, where the server is blueberry.zeelans.com). **NOTE:** Contact your administrator to obtain the domain name.
 - **Password:** This password must match the password that is set in the authentication server. The entered password characters display as asterisks.
 - **Confirm Password:** Reenter the user password.

NOTE: This option is unavailable if Pre-Logon Connect is not selected during installation of the Intel PROSet/Wireless software. Refer to [Install or Uninstall the Single Sign On Feature](#).

TLS: Transport Layer Security authentication is a two-way authentication method that exclusively uses digital certificates to verify the identity of a client and a server.

1. Obtain and install a client certificate, refer to [Set up the Client for TLS authentication](#) or consult your system administrator.
2. Select one of the following to obtain a certificate:
 - **Use my smart card:** Select if the certificate resides on a smart card.
 - **Use the certificate issued to this computer:** Click **Select** to choose a certificate that resides in the machine store.
 - **Use a user certificate on this computer.** Click **Select** to choose a certificate that resides on this computer.
3. Click **Next**.

Step 2 of 2: PEAP Server

Create Wireless Profile

Profile Name: wireless

General Settings

Security Settings

PEAP User

PEAP Server

Security Settings

☐ Personal Security ☒ Enterprise Security

Network Authentication: WPA2 - Enterprise

Data Encryption: AES - CCMP

☒ Enable 802.1x

Authentication Type: PEAP Cisco Options...

Step 2 of 2: PEAP Server

☒ Validate Server Certificate

Certificate Issuer: Any Trusted CA

☐ Allow Intermediate Certificates

☐ Specify Server or Certificate Name

Server or Certificate Name:

☐ Server name must match the specified entry exactly

☒ Domain name must end in with the specified entry

Advanced... Help? << Back Next >> OK Cancel

1. Select one of the following options:
 - **Certificate Issuer:** Click **Any Trusted CA** as the default.
 - Click **allow intermediate certificates** to allow a number of unspecified certificates to be in the server certificate chain between the server certificate and the specified CA. If cleared, then the specified CA must have directly issued the server certificate.
 - **Specify Server or Certificate Name:**
2. **Server or Certificate Name:** Enter the server name.
3. The server name or domain to which the server belongs, depends on which of the two options below has been selected.
 - **Server name must match the specified entry exactly:** When selected, the

server name must match exactly the server name found on the certificate. The server name should include the complete domain name (for example, Servername.Domain name).

- **Domain name must end with the specified entry:** When selected, the server name identifies a domain, and the certificate must have a server name that belongs to this domain or to one of its subdomains (for example, zeelans.com, where the server is blueberry.zeelans.com). **NOTE:** These parameters should be obtained from the administrator.

Notes about Certificates: The specified identity should match the **Issued to** identity in the certificate and should be registered on the authentication server (for example, 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. Use the same user name you used to log in when the certificate was installed.

4. Select the certificate from the list.
5. Click **OK**. The client certificate information appears under Client Certificate.
6. Click **Close**.
7. Click **Next**.
8. Click the new profile at the end of the Profiles list. Use the up and down arrows to change the priority of the new profile.
9. Click **Connect** to connect to the selected wireless network.

If you did not select **Use Windows logon** on the Security Settings page and also did not configure user credentials, no credentials are saved for this profile. Please enter your credentials to authenticate to the network.

10. Click **OK** to close Intel PROSet/Wireless.

PEAP-TLS Certificate Auto Enrollment

In the [Application Settings](#) (Advanced Settings), select **Intel(R) PROSet TLS Certificate Rejected Warning** if you want a warning issued when a PEAP-TLS certificate is rejected. When a certificate has an invalid field expiration date, you are notified that you must take one of the following actions: **A potential authentication problem for profile <profile name> has been detected. The expiration date in the associated certificate may be invalid. Choose one of the following options:**

Control	Description
Continue with current parameters.	Continue with the current certificate.
Update certificate manually.	The Select Certificate page opens for you to choose another certificate.

Update certificate automatically based on the certificates in the local store.	This option is enabled only when the local store holds one or more certificates for which the "issued to" and "issued by" fields match the current certificate and for which the "expiration date" has not expired. If you choose this option, the application selects the first valid certificate.
Log off to obtain certificate during log on process (this does not update the profile and only applies to certificates configured for auto enrollment).	Logs off the user, who must obtain a proper certificate during the next log on process. The profile must be updated to select the new certificate.
Auto enrollment	You are notified to: Please wait while the system is trying to obtain the certificate automatically. Click Cancel to end the certificate retrieval.
Do not show this message again.	A user is able to avoid this step in subsequent sessions. The choice selected is remembered for future sessions.

Set up a Client with AES-CCMP Data Encryption and LEAP Network Authentication

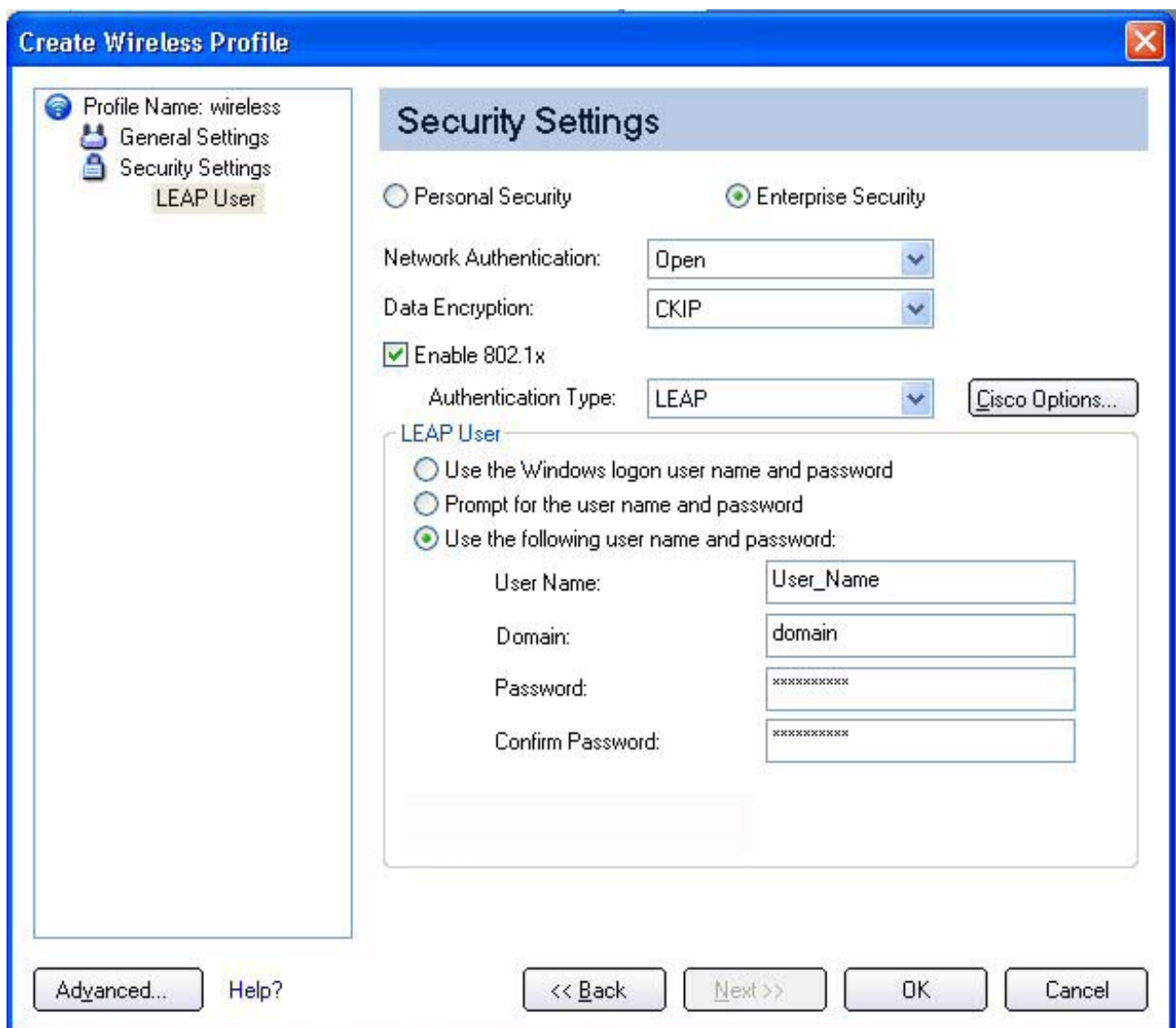
Cisco LEAP (Light Extensible Authentication Protocol) is an 802.1X authentication type that supports strong mutual authentication between the client and a RADIUS server. The LEAP profiles settings include LEAP, CKIP with Rogue AP detection integration. To set up a client with LEAP Authentication:

1. On the Profile page, Click **Add**. The General Settings page displays.
2. Click **Profiles** on the Intel PROSet/Wireless main window.
3. On the Profile page, click **Add** to open the Profile General Settings.
4. **Profile Name:** Enter a descriptive profile name.
5. **Wireless Network Name (SSID):** Enter the network identifier.
6. **Operating Mode:** Click Network (Infrastructure).
7. Click **Next** to access the Security Settings.
8. Click **Enterprise Security**.
9. **Network Authentication:** Select **WPA-Enterprise** or **WPA2-Enterprise**.
10. **Data Encryption:** Select **AES-CCMP** (Recommended).
11. **Enable 802.1x:** Selected.
12. **Authentication Type:** Select **LEAP** to be used with this connection.
13. Click **Cisco Options**.
14. Click **[Enable Cisco Compatible Extensions](#)** to enable Cisco Compatible Extensions (CCX) security (**[Allow Fast Roaming \(CCKM\)](#)**, **[Enable Radio Management Support](#)**, **[Enable Mixed Cells Mode](#)**.) .



15. Click **Enable Radio Management Support**. Use Radio Management to detect rogue access points.
16. Click **OK** to return to the Security Settings.

LEAP User:



1. Select one of the following authentication methods:

- **Use the Windows logon user name and password:** Allows the 802.1x credentials to match your Windows user name and password. The user's credentials are retrieved from the user's Windows log-on process. The credentials are only used if the user has no password defined in the Windows log-on credentials or if there is a problem capturing the Windows log-on credentials.

NOTE: This option is unavailable if Pre-Logon Connect is not selected during installation of the Intel PROSet/Wireless software. Refer to [Install or Uninstall the Single Sign On Feature](#).

- **Prompt for the user name and password:** Select to prompt for the 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:** Select to save your user name and password for future use when an 802.1x authentication profile is used.
 - **User Name:** This user name must match the user name that is set in the authentication server by the administrator prior to client authentication. The user name is case-sensitive. This name specifies the identity supplied to the authenticator by the authentication protocol. This user's identity is securely transmitted to the server only after an encrypted channel has been established.
 - **Domain:** Name of the domain on the authentication server. The server name identifies a domain or one of its sub-domains (for example, zeelans.com, where the server is blueberry.zeelans.com). **NOTE:** The domain name should be obtained from the administrator.
 - **Password:** Specifies the user password. The password characters are seen as asterisks. This password must match the password that is set in the authentication server.
 - **Confirm Password:** Reenter the user password.

2. Click **OK** to save the setting and close the page.

Cisco Compatible Extensions Options

Cisco Options: Use to enable or disable Radio Management and Mixed Cells Mode or Allow Fast Roaming (CCKM).

NOTE: Cisco Compatible Extensions are automatically enabled for CKIP, LEAP or EAP-FAST profiles. To override this behavior, select or clear options on this page.

- **Allow Fast Roaming (CCKM):** Select to enable the client wireless adapter for fast-secure roaming. When a wireless LAN is configured for fast reconnection, an [EAP-FAST](#), [EAP-TLS](#), [PEAP-GTC](#), [PEAP-MSCHAPv2](#) or [LEAP](#)-enabled client device can roam from one access point to another without involving the main server. Use Cisco Centralized Key Management (CCKM), an access point configured to provide Wireless Domain Services (WDS), to take the place of the RADIUS server and authenticate the client without perceptible delay in voice or other time-sensitive applications.

Enable Cisco Compatible Options: Select to enable Cisco Compatible Extensions for this wireless connection profile.

- **Enable Radio Management Support:** Select to have your wireless adapter provide radio management 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. Default setting is selected.
 - **Enable Mixed Cells Mode:** Select to allow the wireless adapter to communicate with mixed cells. A mixed cell is a wireless network in which there are both devices that use WEP and devices that do not. Refer to [Mixed Cells Mode](#) for more information. The default setting is cleared.
-

Set up a Client with AES-CCMP Data Encryption and EAP-FAST Network Authentication

EAP-FAST is an improvement on LEAP. Refer to [Cisco Features](#) for more information. To set up a client with EAP-FAST authentication:

1. Click **Profiles** on the Intel PROSet/Wireless main window.
2. On the Profile page, click **Add** to open the Profile Wizard's General Settings.
3. **Profile Name:** Enter a descriptive profile name.
4. **Wireless Network Name (SSID):** Enter the network identifier.
5. **Operating Mode:** Click **Network (Infrastructure)**.
6. Click **Next** to access the Security Settings.
7. Click **Enterprise Security**.
8. **Network Authentication:** Select **WPA2-Enterprise**.
9. **Data Encryption:** Select **AES-CCMP**.
10. **Enable 802.1x:** Selected.
11. **Authentication Type:** Select **EAP-FAST** to be used with this connection.
12. Click **Cisco Options** to select **Allow Fast Roaming (CCKM)** which enables the client wireless adapter for fast secure roaming.

Create Wireless Profile

Profile Name: wireless

General Settings

Security Settings

EAP-FAST User

Security Settings

☐ Personal Security ☒ Enterprise Security

Network Authentication: WPA2 - Enterprise

Data Encryption: AES - CCMP

☒ Enable 802.1x

Authentication Type: EAP-FAST Cisco Options...

EAP-FAST User

☐ Use the Windows logon user name and password

☐ Prompt for the user name and password

☒ Use the following user name and password:

User Name:

Domain:

Password:

Confirm Password:

☒ Allow automatic provisioning of Protected Access Credentials (PAC)

PACs... Authority ID (A-ID): None selected.

Advanced... Help? << Back Next >> OK Cancel

EAP-FAST User

1. Select the credentials retrieval method:

- **Use the Windows logon user name and password:** The user credentials are retrieved from the Windows log on process.

NOTE: This option is unavailable if Pre-Logon Connect is not selected during installation of the Intel PROSet/Wireless software. Refer to [Install or Uninstall the Single Sign On Feature](#).

- **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 first be 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.
 - **Domain:** Name of the domain on the authentication server. The server name identifies a domain or one of its sub-domains (for example, zeelans.com, where the server is blueberry.zeelans.com).

NOTE: Contact your administrator to obtain the domain name.

- **Password:** This password must match the password that is set in the authentication server. The entered password characters display as asterisks.
- **Confirm Password:** Reenter the user password.

2. **Allow automatic provisioning of Protected Access Credentials (PAC):**

EAP-FAST uses a PAC key to protect the user credentials that are exchanged. All EAP-FAST authenticators are identified by an Authority Identity (A-ID). The local authenticator sends its AID to an authenticating client, and the client checks its database for a matching AID. If the client does not recognize the AID, it requests a new PAC.

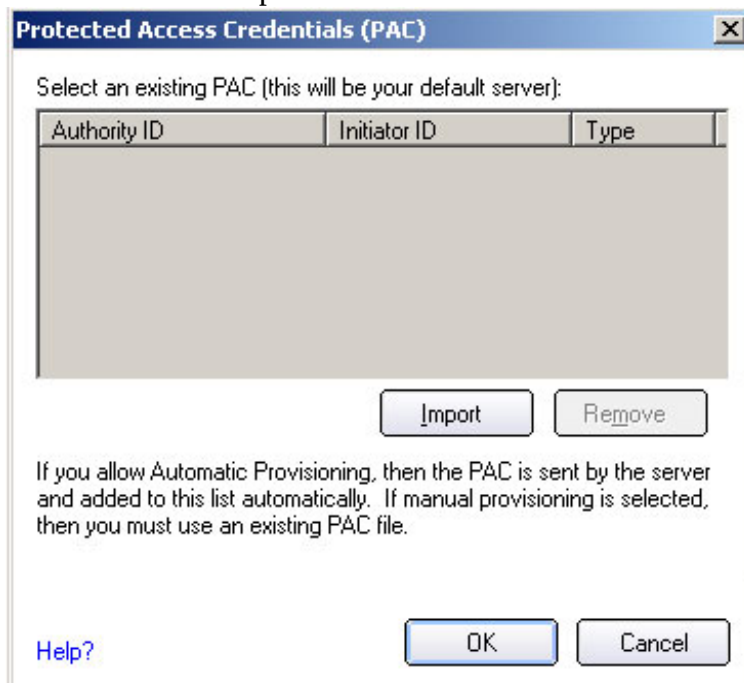
Click the **PACs** button to view any PACs that have already been provisioned and reside on this computer. A PAC must have already been obtained to clear **Allow automatic provisioning** on the Security Settings.

NOTE: If the provisioned Protected Access Credential (PAC) is valid, Intel(R) PROSet/Wireless does not prompt the user for acceptance of the PAC. If the PAC is invalid, Intel PROSet/Wireless fails the provisioning automatically. A status message is displayed in the [Wireless Event Viewer](#) that an administrator can review on the user's computer.

PAC distribution can also be completed manually (out-of-band). Manual provisioning enables you to create a PAC for a user on an ACS server and then import it into a user's computer. A PAC file can be protected with a password, which the user needs to enter during a PAC import.

To import a PAC:

1. Click **PACs** to open the **Protected Access Credentials (PAC)** list.



2. Click **Import** to import a PAC that resides on this computer or a server.
3. Select the PAC and click **Open**.

4. Enter the PAC password (optional).
 5. Click **OK** to close this page. The selected PAC is added to PAC list.
 6. Click **OK** to save the EAP-FAST settings and return to the Profiles list. The PAC is used for this wireless profile.
-

[Back to Top](#)

[Back to Contents](#)

- [Trademarks and Disclaimers](#)

Security Overview: Intel(R) PRO / Wireless 3945ABG Network Connection User Guide

- [WEP Encryption](#)
 - [Open and Shared Key authentication](#)
 - [802.1x Authentication](#)
 - [How 802.1x Authentication Works](#)
 - [802.1x Features](#)
 - [WPA/WPA2](#)
 - [Enterprise Mode](#)
 - [Personal Mode](#)
 - [WPA-Enterprise and WPA2-Enterprise](#)
 - [WPA-Personal and WPA2-Personal](#)
 - [AES-CCMP](#)
 - [TKIP](#)
 - [TLS](#)
 - [TTLS](#)
 - [PEAP](#)
 - [Cisco Features](#)
 - [Cisco LEAP](#)
 - [Cisco Rogue Access Point Security Feature](#)
 - [Fast Roaming \(CCKM\)](#)
 - [CKIP](#)
 - [802.11b and 802.11g Mixed Environment Protection Protocol](#)
 - [EAP-FAST](#)
 - [Mixed Cell Mode](#)
 - [Radio Management](#)
-

WEP Encryption

Use IEEE 802.11 Wired Equivalent Privacy (WEP) encryption to prevent unauthorized reception of wireless data. WEP encryption provides two levels of security: 64-bit key (sometimes referred to as 40-bit) or a 128-bit key (also known as 104-bit). For stronger 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 that use 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

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

- When **Open** authentication is used, any wireless station can request authentication. The station that needs to authenticate with another wireless station sends an authentication management request that contains the identity of the sending station. The receiving station or access point grants any request for authentication. Open authentication allows any device network access. If no encryption is enabled on the network, any device that knows the Service Set Identifier (SSID) of the access point can gain access to the network.
- When **Shared Key** authentication is used, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel. Shared key authentication requires that the client configure a static WEP key. The client access is granted

only if it passes a challenge-based authentication.

802.1x Authentication

[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 provides a different approach to authentication but all employ 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)
- 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: EAP-TLS, EAP-TTLS, and Protected EAP (PEAP). 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 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