Intel(R) PROSet/Wireless 2915ABG Network Connection User Guide

---

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

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

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

Table of Contents

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

Information in this document is subject to change without notice.
© 2000–2004 Intel Corporation. All rights reserved. Intel Corporation, 5200 N.E. Elam Young Parkway, Hillsboro, OR 97124-6497 USA

The copying or reproducing of any material in this document in any manner whatsoever without the written permission of Intel Corporation is strictly forbidden. Intel(R) is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Intel disclaims any proprietary interest in trademarks and trade names other than its own. *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation.

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

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

June 2004

Using Intel PROSetWireless: Intel(R) PROSetWireless 2915ABG Network Connection User Guide

- Using Intel(R) PROSetWireless as your Wireless Manager
- Starting Intel PROSetWireless
- Intel PROSetWireless Main Window
- Tool Tips and Balloon Message Popups
- Connection Status Icons
- Connection Details
- Profile List
- Profile Wizard
- Network Connection Profile Setup:
  - Profile Name
  - Application Settings
  - Network Settings
  - Security Settings
  - Advanced Settings
  - Set Auto Transferable Profile
  - Set Auto Connect
- Profile Menu
  - Import Profiles
  - Manage Exclusions
- Network Connection Status
- Diagnosing and Correcting the Problem
- Viewing and Controlling the Radio

Using Intel(R) PROSetWireless as your Wireless Manager

Intel(R) PROSetWireless can be used to simply add and manage wireless profiles (connection to a network). It also includes advanced features to configure and control the wireless radio and to diagnose wireless connection problems.

If you are using Microsoft* as your wireless manager, you can disable it from the Wireless Network tab. To disable Microsoft* as your wireless manager:

1. Right-click on the Intel PROSetWireless icon in the system tray and select **Disable Microsoft Wireless Manager**.
2. Right-click on the Intel PROSetWireless icon in the system tray and select **Exit**.

Starting Intel PROSetWireless

Intel PROSetWireless can be started from the Windows Start button, or from the Windows Control Panel.

To launch Intel PROSetWireless use either of the following methods:

- Click **Start > Programs > Intel PROSetWireless > Intel PROSetWireless**.
- Double-click the Intel PROSetWireless icon in the Windows Control Panel. Depending on the view, select **Open Intel PROSetWireless**.

Intel PROSetWireless Main Window

- To exit Intel PROSetWireless select **Exit**.
- To exit Intel PROSetWireless and close the task tray icon, click **Exit** from the from the task tray menu or click **Close** button in the Intel PROSetWireless main window.

Launch Intel PROSetWireless from the task tray

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

Tool Tips and Balloon Message Popups

The tool Tips and Balloon message popups provide feedback and information. To display Tool tips, move your mouse over the icon. To display balloon message popups, right-click the icon and select the appropriate popup. Balloon popups can be enabled or disabled in the Application Settings.

Tool Tips

Tool tips display when the mouse pointer rolls over the icon. The tool tip displays the tool tip of the connection status.

Tool Tip

Connected to a wireless network

Wireless Network Name
Signal Strength: Very Good

Connected to a wireless network
Wireless Network Name
Signal Strength: Very Good

Balloon Popups

When your cursor is hovered in wireless message control displays, if you click the pop-up, that an appropriate action occurs. For example when wireless network is found, the following balloon popup displays:

Balloon Popup

Wireless network found
Click here to connect to this network

Intel PROSetWireless Main Window

Use the main Intel PROSetWireless to:

- View the current connection status (signal quality, speed and current network).
- Create and manage profiles.
- Configure application and network settings.
- Diagnose connection and radio problems.
- Control the radio and view its status.

Connection Status Icons

The Intel PROSetWireless icon will change connection status icons which indicate the current connection status. Hover your mouse over the icon to display a tool tip with connection status information. Click the **Tool Tips** icons for more information.

Wireless Connection Status Icon Descriptions

	Description
	Disabled radio. The wireless adapter is not associated to a network. Click the **Tool Tips** icon for more information.
	Searching for wireless networks. The wireless adapter is scanning for any available wireless networks.
	Associated icon.
	No wireless networks found. Unable to associate to a wireless network. Check the wireless network configuration.
	Connected to a wireless network. Connected to a wireless network. The network name, speed, and signal strength are displayed in the tool tip. Click the **Tool Tips** icon for more information.
	Wireless network found. An available wireless network is found. Click the icon to connect to the network.

Signal Quality

The signal quality icon helps indicate the quality of the transmit and receive signals between your wireless adapter and the network. Hover your mouse over the icon to display a tool tip with the signal quality information. Click the **Tool Tips** icon for more information. Signal quality is displayed as a percent and as a number of bars.

Speed	The signal quality icon helps indicate the quality of the transmit and receive signals between your wireless adapter and the network. Hover your mouse over the icon to display a tool tip with the signal quality information. Click the **Tool Tips** icon for more information. Signal quality is displayed as a percent and as a number of bars.
	54 Mb, 11 Mb, 5.5 Mb, 2 Mb, 1 Mb
	54 Mb, 11 Mb, 5.5 Mb, 2 Mb, 1 Mb
	54 Mb, 11 Mb, 5.5 Mb, 2 Mb, 1 Mb
	54 Mb, 11 Mb, 5.5 Mb, 2 Mb, 1 Mb
	54 Mb, 11 Mb, 5.5 Mb, 2 Mb, 1 Mb
Signal Strength	Provides adapter connection status information. See Connection Details for information.
Signal Quality	Provides adapter connection status information. See Connection Details for information.
Speed	Displays the link information for the adapter.
Network Name	Displays the Network Name (SSID) of the connection.
Channel Number	Displays the channel and receiver channel.
Receiver Channel Number	Displays the receiver channel. Only displays if the receiver channel differs from the transmit channel.
Receiver Signal Quality	Displays the receiver signal quality. Only displays if the receiver signal quality differs from the transmit signal quality.
Receiver Signal Strength	Displays the receiver signal strength. Only displays if the receiver signal strength differs from the transmit signal strength.
Receiver Speed	Displays the receiver link information for the adapter. Only displays if the receiver link information differs from the transmit link information.
Receiver Network Name	Displays the receiver network name (SSID). Only displays if the receiver network name differs from the transmit network name

Ad-Hoc Channel	Choose from a list of the available channels.
Enable Ad-Hoc QoS	Enable Select this option to enable throughput enhancements.
Wireless Mode	**Disable** - Select this option to disable throughput enhancements. Use this option to select whether to allow the 11a/b/g mixed environment. Use 802.11b/g only if you have 802.11b/g devices in your network. Use 802.11a only if you have 802.11a devices in your network. Use 802.11a/b/g if you have 802.11a, 802.11b and 802.11g devices in your network. **Power Management** - Allows you to select a balance between power consumption and performance. Select Max Perf if you want to maximize performance. Select Max Power if you want to maximize battery life. **Out-Default value (Default)** - Power settings based on the computer's power source. **802.11a** - Only 802.11a devices can connect to the Ad-Hoc network. Use this setting if you have 802.11a devices in your network. **802.11b** - Only 802.11b devices can connect to the Ad-Hoc network. Use this setting if you have 802.11b devices in your network. **802.11b and 802.11g only** - Connect the wireless adapter to 802.11b and 802.11g devices only. **802.11a and 802.11b and 802.11g** - Connect the wireless adapter to 802.11a and 802.11b and 802.11g devices. **802.11a and 802.11b and 802.11g (Default)** - Connect the wireless adapter to 802.11a and 802.11b and 802.11g devices.
Preferred Band	Select the preferred band. Select the wireless band(s) that the wireless adapter attempts to connect to before connecting to the Ad-Hoc network. Select the operating band. The selections are: • 802.11a • 802.11b • 802.11g • Any available band
Wireless Mode	**802.11a only, 802.11b only, and 802.11g only** - Connect the wireless adapter to 802.11a, 802.11b, or 802.11g devices only. **802.11a and 802.11b and 802.11g** - Connect the wireless adapter to 802.11a and 802.11b and 802.11g devices. **802.11a and 802.11b and 802.11g (Default)** - Connect the wireless adapter to 802.11a and 802.11b and 802.11g devices.
OK	Save settings and close the dialog box.
Cancel	Cancel settings and close the dialog box.
Help?	Displays the help information for this dialog.

Use Microsoft Client (Tools menu)

Intel(R) PROSet/Wireless Tools
Intel(R) PROSet/Wireless Tools
Intel(R) PROSet/Wireless Tools

Back to Contents

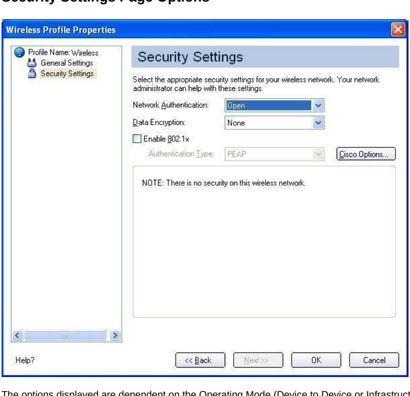
Setting up Security: Intel PRO/Wireless 2915ABG Network Connection User Guide

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

From the Security Settings page you can enter the required security settings for the selected wireless network. See the Profile Wizard Overview for a description of when the Profile Wizard is launched.

See Security Overview for more information the different security options for wireless networks.

Security Settings Page Options



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

Name	Setting
Network Authentication	**Open** **Shared** **WPA-Enterprise** **WPA2-Enterprise** **WPA-Personal** **WPA2-Personal**
Data Encryption	**None** **WEP** **CXIP**
Enable 802.1x (Authentication Type)	**MD5 Open** **MD5 WEP Key** **EAP-SIM** **TLS** **TTLS** **PEAP** **LEAP** **EAP-FAST**
Cisco Options	Click to view the Cisco Compatible Extensions Options page. **Note:** Cisco Compatible Extensions are automatically enabled for CKIP, LEAP or EAP-FAST profiles.
Back	View the prior page in the Profile Wizard.
Next	View the next page in the Profile Wizard. If more security information is required then the next Step of the Security page is displayed.
OK	Close the Profile Wizard and save the profile.
Cancel	Close the Profile Wizard and cancel any changes made.
Help?	Displays the help information for the current page.

Network Authentication: Device to Device

Open/None authentication/WEP encryption

This ad hoc network uses no network authentication with WEP data encryption.

Name	Description
Network Authentication	**Open:** No authentication used. Open authentication allows a wireless device access to the network without 802.11 authentication. The access point allows any request for authentication. If no encryption is enabled on the network, any wireless device with the correct network name (SSID) can associate with the access point and gain access to the network.
Data Encryption	**None:** No data encryption used. **WEP:** WEP data encryption can be configured using 64-bit or 128-bit. When WEP encryption is enabled on an access point, the WEP key provides a way to verify access to the network. If the wireless device does not have the correct WEP key, even though authentication is successful, the device is unable to transmit data through the access point or decrypt data received from the access point.
Encryption Level	**64-bit or 128-bit:** 64-bit or 128-bit encryption.
Key Index	**1,2,3,4:** Up to four passwords may be specified by changing the Key Index.
Wireless Security Password (WEP Key)	Type the wireless network Password (WEP Key) in the text box. The Password is the same value used by the Wireless Access Point or Router. Contact your wireless network administrator for this password. **Pass phrase (64-bit):** Enter 5 alphanumeric characters, 0-9, a-z or A-Z. **Hex key (64-bit):** Enter 10 alphanumeric hexadecimal characters, 0-9, A-F. **Pass phrase (128-bit):** Enter 13 alphanumeric characters, 0-9, a-z or A-Z. **Hex key (128-bit):** Enter 26 alphanumeric hexadecimal characters, 0-9, A-F.

Network Authentication (Infrastructure): Enable 802.1x Authentication

Open authentication, no encryption

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

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

Open authentication, WEP encryption

This network uses no network authentication with WEP data encryption.

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

Shared authentication

Name	Description
Network Authentication	**Shared:** Shared authentication is accomplished with a pre-configured WEP key. Use this mode for 802.11 Authentication. This mode can work with any 802.1x authentication protocol and with the following data encryption options; **None**, **WEP** (64-bit, or 128-bit) or **CKIP** (64-bit, or 128-bit). Refer to Security Overview - Open and Shared Key authentication for more information
Data Encryption	**None:** No data encryption used. **WEP:** WEP data encryption can be configured using 64-bit or 128-bit. **CKIP:** Cisco Key Integrity Protocol (CKIP) is a Cisco proprietary security protocol for data encryption in 802.11 media.
Enable 802.1x	Disabled.
Encryption Level	**64-bit or 128-bit:** When switching between 64-bit and 128-bit encryption, the previous settings are erased and a new key must be entered.
Key Index	**1,2,3,4**: Up to four passwords may be specified by changing the Key Index.
Wireless Security Password (WEP Key)	Enter the wireless network Password (WEP Key) in the text box. The Password is the same value used by the Wireless Access Point or Router. Contact your wireless network administrator for this password. **Pass phrase (64-bit):** Enter 5 alphanumeric characters, 0-9, a-z or A-Z. **Hex key (64-bit):** Enter 10 alphanumeric hexadecimal characters, 0-9, A-F. **Pass phrase (128-bit):** Enter 13 alphanumeric characters, 0-9, a-z or A-Z. **Hex key (128-bit):** Enter 26 alphanumeric hexadecimal characters, 0-9, A-F.

WPA - Enterprise or WPA2 - Enterprise

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

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

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

WPA - Personal or WPA2 - Personal

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

Name	Description
Network Authentication	**WPA-Personal:** See Security Overview **WPA2-Personal:** See Security Overview
Data Encryption	**WEP:** WEP data encryption can be configured using 64-bit or 128-bit. WEP settings can be used with all Network Authentication protocols. When WEP encryption is enabled on an access point, the WEP key provides a way to verify access to the network. If the wireless device does not have the correct WEP key, even though authentication is successful, the device is unable to transmit data through the access point or decrypt data received from the access point. **CKIP:** Cisco Key Integrity Protocol (CKIP) is a Cisco proprietary security protocol for encryption in 802.11 media. Refer to Security Overview for more information. **Note:** CKIP is enabled only when the checkbox for Cisco Client eXtentions is selected. **TKIP:** To improve data encryption, Wi-Fi Protected Access utilizes its Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a re-keying method. Refer to Security Overview for more information. **Note:** TKIP is enabled only when the checkbox for Cisco Client eXtentions is selected.
Cisco-Client eXtentions	Default is unchecked (Disabled). Select this option to enable Cisco-Client Options. Refer to Cisco Compatible Extensions Options for details. From the Cisco Compatible Extensions Options page you can enable Radio Management support and Mixed Cells mode. Check this box to enable **CKIP** and **TKIP** data encryption and 802.1x **LEAP** authentication on the Security Settings page.
WPA Key	Enter your network key (wireless security password) for your wireless network in the Network key field. Make sure that the network key used matches the Windows network key. **Password:** • Enter a text phrase with at least 8 up to 63 characters in the pass phrase field. WPA-Personal uses Wi-Fi Protected Access authentication. Pre Shared Key (WPA-PSK) mode does not use an authentication server. WPA-PSK requires configuration of a pre-shared key (PSK). The data encryption key is derived from the PSK.

802.1x MD5 - Open/None

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

MD5 Settings

Name	Description
Network Authentication	**Open:** No authentication used. Refer to Open and Shared Key authentication for more information. Open authentication allows a wireless device access to the network without 802.11 authentication. The access point allows any request for authentication. If no encryption is enabled on the network, any wireless device with the correct network name (SSID) can associate with the access point and gain access to the network.
Data Encryption	**None:** No data encryption used.
Enable 802.1x	Checked.
Authentication Type	**MD5:** A one-way authentication method that uses user names and passwords.
Use the Windows logon user name and password	If this feature is selected the user's credentials are retrieved from the user's Windows Logon process.
Prompt for the user name and password	Prompts for a user name and password before you connect the wireless network. The user name and password must be first set in the authentication server by the administrator.
Use the following user name and password	The user name and password must be first set in the authentication server by the administrator. **User Name:** This user name must match the user name that is set in the authentication server. **Password:** This password must match the password that is set in the authentication server. The entered password characters display as asterisks. **Confirm Password:** Re-enter the user password.

802.1x MD5 – WEP Key

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

MD5 Settings for Shared/None, Open/WEP, Open/CKIP.

Name	Description
Network Authentication	**Open:** No authentication used. Refer to Open and Shared Key authentication for more information. Open authentication allows a wireless device access to the network without 802.11 authentication. The access point allows any request for authentication. If no encryption is enabled on the network, any wireless device with the correct network name (SSID) can associate with the access point and gain access to the network. .
Data Encryption	**WEP:** WEP data encryption can be configured using 64-bit or 128-bit. WEP settings can be used with all Network Authentication protocols. When WEP encryption is enabled on an access point, the WEP key provides a way to verify access to the network. If the wireless device does not have the correct WEP key, even though authentication is successful, the device is unable to transmit data through the access point or decrypt data received from the access point. **CKIP:** Cisco Key Integrity Protocol (CKIP) is a Cisco proprietary security protocol for encryption in 802.11 media. Refer to Security Overview for more information.
Enable 802.1x	Checked.
Step 1 of 2: WEP Key	
Encryption Level	**64-bit:** 64-bit or 128-bit encryption.
Key Index	**1,2,3,4:** Up to four passwords may be specified by changing the Key Index.
Wireless Security Password (WEP Key)	Enter the wireless network Password (WEP Key) in the text box. The Password is the same value used by the Wireless Access Point or Router. Contact your wireless network administrator for this password. Pass phrase and hex key options are: **Pass phrase (64-bit):** Enter 5 alphanumeric characters, 0-9, a-z or A-Z. **Hex key (64-bit):** Enter 10 alphanumeric hexadecimal characters, 0-9, A-F. **Pass phrase (128-bit):** Enter 13 alphanumeric characters, 0-9, a-z or A-Z. **Hex key (128-bit):** Enter 26 alphanumeric hexadecimal characters, 0-9, A-F.
Step 2 of 2: MD5 User	
Use the Windows logon user name and password:	If this feature is selected the user's credentials are retrieved from the user's Windows Logon process.
Prompt for the user name and password:	Prompts for a user name and password before you connect the wireless network. The user name and password must be first set in the authentication server by the system administrator.
Use the following user name and password:	The user name and password must be first set in the authentication server by the IT administrator. **User Name:** This user name must match the user name that is set in the authentication server. **Password:** This password must match the password that is set in the authentication server. The entered password characters display as asterisks. **Confirm Password:** Re-enter the user password.

EAP-SIM Authentication

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

EAP-SIM authentication can be used with:

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

Name	Description
EAP-SIM User	**Specify user name (identity):** Select this option to specify the user name. • **User Name:** The user name assigned to the SIM card.

TLS Authentication

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

Name	Description
Step 1 of 2: TLS User	
Use my smart card or certificate	**Smart card:** Click this option if the certificate resides on a smart card. **Certificate:** Click this option if the certificate resides on this computer
User Name	**User Name:** This user name must match the user name that is set in the authentication server by the administrator prior to client's authentication. The user name is case-sensitive.
Client Certificate	**Select:** TLS requires a Client Certificate from the Personal Certificate store of the Windows logged-in user. This certificate identifies you as the user. This certificate is used for client authentication. Click **Select** to choose a client certificate
Step 2 of 2: TLS Server	
Certificate Issuer	**Certificate Issuer:** The server certificate received during TLS message exchange must have been issued by this certificate authority. Trusted intermediate certificate authorities and root authorities whose certificates exist in the system store are available for selection in the drop-down list box. If Any Trusted CA is selected, any CA in the list is acceptable. • **Allow intermediate certificates:** The server certificate received during negotiation may have been issued directly by the certificate authority indicated in the "Certificate issuer" field, or additionally by one of its intermediate certificate authorities. Check this box to allow a number of unspecified certificates to be in the server certificate chain between the server certificate and the specified CA. If unchecked, then the specified CA must have directly issued the server certificate.
Specify Server/Certificate Name	Check this option if you want to specify your server/certificate name. The server name, or a domain to which the server belongs, based on which of the two options below has been selected. • **Server name must match exactly:** When selected, the server name entered must match exactly the server name found on the certificate. The server name should include the fully qualified domain name (e.g., Servername.Domain name) in this field. • **Domain name must end in specified name:** When selected, the server name field identifies a domain and the certificate must have a server name belonging to this domain or to one of its sub-domains (e.g., zeelans.com, where the server is blueberry.zeelans.com). **Note:** These parameters should be obtained from the system administrator.
Server Name	The server name, or a domain to which the server belongs, depending on which of the two options below has been selected. • **Server name must match exactly:** When selected, the server name entered must match exactly the server name found on the certificate. The server name should include the complete domain name (e.g., Servername.Domain name) in this field. • **Domain name must end in specified name:** When selected, the server name field identifies a domain and the certificate must have a server name belonging to this domain or to one of its sub-domains (e.g., zeelans.com, where the server is blueberry.zeelans.com). **Note:** These parameters should be obtained from the system administrator.

TTLS Authentication

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

Name	Description
Step 1 of 2: TTLS User	

Authentication Protocol	This parameter specifies the authentication protocol operating over the TTLS tunnel. The protocols are: PAP, CHAP, MD5, MS-CHAP and MS-CHAP-V2.
	
	Using PAP, CHAP, MD5, MS-CHAP, and MS-CHAP-V2 protocols:
	• **Use the Windows logon user name and password:** If this feature is selected the user's credentials are retrieved from the user's Windows Logon process.
	• **Prompt for the user name and password:** Selecting this feature prompts for user name and password before you connect to the wireless network. The user name and password must be first set in the authentication server by the administrator.
	• **Use the following user name and password:** The user name and password are securely (encrypted) saved in the profile
	  ◦ **User Name:** This user name must match the user name that is set in the authentication server.
	  ◦ **Password:** This password must match the password that is set in the authentication server. The entered password characters display as asterisks.
	  ◦ **Confirm Password:** Re-enter the user password.

Use Client Certificate	**Select:** A client certificate from the Personal certificate store of the Windows logged-in user, this certificate is used for client authentication.
Roaming Identity	When using 802.1x MS RADIUS as an authentication server, the authentication server authenticates the device by using the "Roaming Identity" username from Inte. PROSet/Wireless and ignores the "Authentication Protocol MS-CHAP-V2" User Name. This feature is the 802.1x identity supplied to the authenticator. Microsoft IAS RADIUS accepts only a valid username (dotNet user) for EAP clients. Enter a valid username when using 802.1x MS RADIUS. For all other servers, this is an optional field, therefore, it is recommended that this field not contain a true identity, but instead the desired realm (e.g., anonymous@myrealm).
Step 2 of 2: TTLS Server	
Certificate Issuer	The server certificate received during the PEAP message exchange must have been issued by this certificate authority. Trusted intermediate certificate authorities and root authorities whose certificates exist in the system store are available for selection in the list box. If Any Trusted CA is selected, any CA in the list is acceptable. • **Allow intermediate certificates:** The server certificate received during negotiation may have been issued directly by the certificate authority indicated in the "Certificate issuer" field, or additionally by one of its intermediate certificate authorities. Check this box to allow a number of unspecified certificates to be in the server certificate chain between the server certificate and the specified CA. If unchecked, then the specified CA must have directly issued the server certificate.
Specify Server/Certificate Name	The server name, or a domain to which the server belongs, depending on which of the two fields below has been checked. • **Server name must match exactly:** When selected, the server name entered must match exactly the server name found on the certificate. The server name should include the complete domain name (e.g., Servername.Domain name) in this field. • **Domain name must end in specified name:** When selected, the server name field identifies a domain and the certificate must have a server name belonging to this domain or to one of its sub-domains (e.g., zeelans.com, where the server is blueberry.zeelans.com) **Note:** These parameters should be obtained from the system administrator.

PEAP Authentication

Name	Description
Step 1 of 2: PEAP User	

Authentication Protocol	This parameter specifies the authentication protocol operating over the PEAP tunnel. The protocols are: MS-CHAP-V2, GTC, and TLS.
	
	Using MS-CHAP-V2 and GTC protocols:
	• **Use the Windows logon user name and password:** If this feature is selected the credentials are retrieved from the Windows Logon process.
	• **Prompt for the user name and password:** Selecting this feature prompts for user name and password before you connect to the wireless network. The user name and password must be first set in the authentication server by the IT administrator.
	  ◦ **For GTC protocol:** Select whether you want to use a static password or a one-time password.
	• **Use the following user name and password:** The user name and password are securely (encrypted) saved in the profile
	  ◦ **User Name:** This user name must match the user name that is set in the authentication server.
	  ◦ **Password:** This password must match the password that is set in the authentication server. The entered password characters display as asterisks.
	  ◦ **Confirm Password:** Re-enter the user password.
	• **Use a client certificate:** You may optionally select a client certificate from the Personal certificate store of the Windows logged-in user, this certificate is used for client authentication.
	• **Roaming Identity**: When using 802.1x MS RADIUS as an authentication server, the authentication server authenticates the device by using the "Roaming Identity" username from Intel PROSet/Wireless and ignores the "Authentication Protocol MS-CHAP-V2" User Name. This feature is the 802.1x identity supplied to the authenticator. Microsoft IAS RADIUS accepts only a valid username (dotNet user) for EAP clients. Enter a valid username when using 802.1x MS RADIUS. For all other servers, this is an optional field, therefore, it is recommended that this field not contain a true identity, but instead the desired realm (e.g., anonymous@myrealm).
	
	Using TLS protocol:
	• **Use my smart card or certificate:** Select smart card if the certificate resides on a smart card. Select certificate if the certificate resides on the computer.
	• **User Name:** This user name must match the user name that is set in the authentication server by the system administrator prior to client's authentication. The user name is case-sensitive. This name specifies the identity supplied to the authenticator by the authentication protocol operating over the TLS tunnel. This user's identity is securely transmitted to the server only after an encrypted channel has been verified and established.
	• **Select:** Choose a client certificate from the Personal certificate store of the Windows logged-in user. This certificate is used for client authentication.

Step 2 of 2: PEAP Server	
Certificate Issuer	The server certificate received during the PEAP message exchange must have been issued by this certificate authority. Trusted intermediate certificate authorities and root authorities whose certificates exist in the system store are available for selection in the list box. If Any Trusted CA is selected, any CA in the list is acceptable. • **Allow intermediate certificates:** The server certificate received during negotiation may have been issued directly by the certificate authority indicated in the "Certificate issuer" field, or additionally by one of its intermediate certificate authorities. Check this box to allow a number of unspecified certificates to be in the server certificate chain between the server certificate and the specified CA. If unchecked, then the specified CA must have directly issued the server certificate.
Specify Server/Certificate Name	Click this option if you want to specify your server/certificate name. • **Server name must match exactly:** When selected, the server name entered must match exactly the server name found on the certificate. The server name should include the complete domain name (e.g., Servername.Domain name) in this field. • **Domain name must end in specified name:** When selected, the server name field identifies a domain and the certificate must have a server name belonging to this domain or to one of its sub-domains (e.g. zeelans.com, where the server is blueberry.zeelans.com) **Note:** These parameters should be obtained from the system administrator.

LEAP Authentication

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

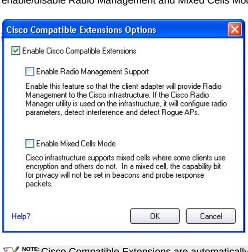
EAP-FAST Authentication

EAP-FAST is an improvement on LEAP. Refer to Cisco Features for more information.

Name	Description
Use the Windows logon user name and password	The user credentials are retrieved from the Windows Logon process.
Prompt for the user name and password	Prompts for user name and password before you connect to the wireless network. The user name and password must be first set in the authentication server by the administrator.
Use the following user name and password:	The user name and password must be first set in the authentication server by the administrator. **User Name:** This user name must match the user name that is set in the authentication server. **Password:** This password must match the password that is set in the authentication server. The entered password characters display as asterisks. **Confirm Password:** Re-enter the user password.
Allow automatic provisioning of Protected Access Credentials (PAC):	EAP-FAST uses a Protected Access Credentials key to protect the user credentials that are exchanged. • Click "Allow automatic provisioning" if you want to obtain the PAC from the server. • If a PAC has already been obtained, uncheck "Allow automatic provisioning", and click **Select** to choose an existing PAC on your computer.
Allow Fast Roaming (CCKM)	Click **Allow Fast Roaming** (Cisco Centralized Key Management (CCKM)) to enable the client wireless adapter for fast secure roaming. When a wireless LAN is configured for fast reconnection, a LEAP enabled client device can roam from one access point to another without involving the main server. Using Cisco Centralized Key Management (CCKM), an access point configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client without perceptible delay in voice or other time-sensitive applications.

Cisco Compatible Extensions Options

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



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

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

Back to Contents

Trademarks and Disclaimers

Back to Contents

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

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

Profile Wizard Overview

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

When the Intel Configuration Service detects an available network and the adapter is not associated to another wireless network, the "Connect to wireless network" page is displayed. From Intel PROSet/Wireless, select a network from the Available Network list, and click Configure.

1. The General Settings page is displayed with the network name and operating mode for the selected network. The identified Wireless Network Name (SSID) cannot be modified, but you can change the Profile Name.

2. Click Next to display the Profile Wizard Security Settings page. This starts the access point query process to determine the highest level of security required for the selected network. Refer to Setting up Security for more information on security options.
3. After the required security is determined, click **Next**.
4. The Security Settings page displays the required information that must be entered to connect to that particular network. For example, if an Infrastructure WEP network is selected, WEP encryption and key index information is displayed, but only the WEP Network Key needs to be entered. If you do not know the required network settings, contact your system administrator.

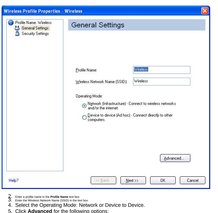
Creating a New Profile

Use the Profile Wizard to create a new profile.

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

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

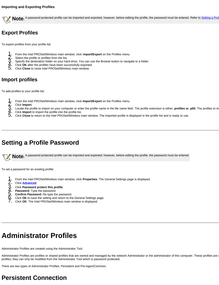
1. From the Intel PROSet/Wireless main window click tools. The Profile Wizard is launched and the General Settings page is displayed.



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

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

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



6. The Security Settings page displays the current security status for the network access point. Click **Next** to set Network Authentication and Data Encryption options.
7. Select the Network Authentication and Data Encryption options. Enter the encryption key settings and configure the 802.1x settings as required. Refer to Security Settings for more information.
8. Click OK when you have completed the profile settings. The Profile Wizard ends and you are returned to Intel PROSet/Wireless main window. To change or verify the profile settings, click the **Back** button.
9. If you are not currently connected to a network, Intel PROSet/Wireless detects that a new profile has been added and automatically attempts to connect to this new profile.
10. If you want to manually connect to this profile, click Connect to use this wireless network. The connection icon displays the current connection status. The network name, transmit and receive speed, and signal quality are also displayed.

Editing an Existing Profile

To edit an existing profile:

1. Select the profile to edit from the Profiles List.
2. Click **Properties**. The General Settings and Security Settings pages display all the profile settings and parameters that can be modified.
3. Click **Next** and **Back** to navigate through the General and Security Setting settings.

- **General Settings**, Refer to General Settings for more information.
- **Security Settings**, Refer to Security Settings for more information.

Removing a Profile

To remove a profile:

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

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

Importing and Exporting Profiles

Note. A password protected profile can be imported and exported, however, before editing the profile, the password must be entered. Refer to Setting a Profile Password for more information.

Export Profiles

To export profiles from your profile list:

1. From the Intel PROSet/Wireless main window, click **Import/Export** on the Profiles menu.
2. Select the profile to export from the list.
3. Specify the destination folder on your hard drive. You can use the Browse button to navigate to a folder.
4. Enter a file name for the exported profile in the text box.
5. Click **Close** to close Intel PROSet/Wireless main window.

Import profiles

To add profiles to your profile list:

1. From the Intel PROSet/Wireless main window, click **Import/Export** on the Profiles menu.
2. Click **Import**.
3. Use the Browse button to select an your computer or enter the profile name in in the name text box. The profile extensions is either **.profiles** or **.pfl**. The profiles to import can be located in any directory you choose on your computer.
4. Click **Import** to import the profile into the profiles list.
5. Click **Close** to return to the Intel PROSet/Wireless main window. The imported profile is displayed in the profile list and is ready to use.

Setting a Profile Password

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

To set a password for an existing profile:

1. From the Intel PROSet/Wireless main window, click **Properties**. The General Settings page is displayed.
2. Click **Advanced**.
3. Type **Password protect this profile**.
4. Type the password in the **Password** box.
5. Type **Confirm Password**. Re-type the password.
6. Click **Next** to navigate through the General and Security Setting pages.
7. Click **OK**. The Intel PROSet/Wireless main window is displayed.

Administrator Profiles

Administrator Profiles are created using the Administrator Tool.

Administrator Profiles are profiles in shared profiles that are owned and managed by the network Administrator or the administrator of this computer. These profiles are common/shared by all users on this computer. However end users cannot modify these profiles. Only the administrator can modify these administrator profiles.

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

Persistent Connection

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

Pre-Logon/Common Profiles

Pre-logon/Common profiles are applied once a user logs on. If Single Sign On (Cisco Wireless username and password if support is installed) the connection is made as part of the Windows log on sequence (pre-logon). If Single Sign On support is not installed or the Cisco Wireless username and password are not the same as the Windows log on, the connection is made after the Windows log on sequence is completed. Pre-logon/Common profiles are common/shared by all users on this computer. Pre-logon/Common profiles. Since these profiles appear at the top of the profile list, Intel PROSet/Wireless automatically attempts to connect to the Administrator profiles first before any user created profiles.

Pre-Logon Connect Status

When the Single Sign On component is installed, you have Pre-Logon/Connect support.

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

Administrator Export Properties

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

Administrator Export Preferences dialog

Name	Description
Export Administrator Preferences	**Step 1: Select which preferences you want to export:** • Administrator Settings: Export all the settings. These include control of Cache Credentials and XP Co-existence. • Administrator Profiles: Export all the Persistent and Pre-logon/Common Profiles. **Step 2: Select the destination file:** • Browse button: Select the destination path and directory. The export destination file has a .sso extension. The directory path displays in the destination directory window. **Step 3: Export the selected preferences:** • Export button: Start exporting your profiles to the assigned destination folder.
Close	Close page.
Help?	Displays the help information for this page.

Automatic Profile Distribution

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

The profile must be copied to a specific directory on the host computer. From there it can be distributed to multiple computers. Once the profile is received by the remote computer it is automatically available from the Profiles List. If an attempt is made to edit a distributed profile that is password protected a password prompt appears.

Automatically importing profiles is accomplished by monitoring the import folder on your hard disk for new profile files. Only profiles that have the **Enable Auto-Import** box checked can be automatically imported. If a profile of the same name already exists in the profiles list, the imported profile is not added to the list, and an error dialog is shown. A unique id is stored in the existing profile to backpack. An imported profile will be placed at the bottom of the Profiles List, and the profile file is immediately deleted after the import whether the import was successful or not.

To import a profile into the Profiles List:

1. Select the profile from the Profiles List, and click the **Properties** button.
2. Click the **Advanced** button.
3. Check **Enable Auto-Import**.
4. Click **OK** to close the Advanced Settings page.
5. Click **OK** to close the General Settings page.
6. Click **Close** to return to the Intel PROSet/Wireless main window.
7. Copy the exported profile from the directory to the **Programs Files\Intel\Wireless\Autoimport** directory. The profile is now ready to distribute to other computers.

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

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

Single Sign On (Cisco Wireless user name and password) is supported in the enterprise environment where users logon to their computer with a user name, password and typically a domain. Fast User Switching does not support domain log on.

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

Back to Contents

Trademark and Disclaimers

Back to Contents

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

- WEP encryption
- 802.1x Authentication
- WPA/WPA2
- Cisco Features

WEP encryption

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

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

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

Open and Shared Key authentication

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

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

802.1x Authentication

How 802.1x authentication works
802.1x features

Overview

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

802.1x authentication for wireless LANs has three main components: The authenticator (the access point), the supplicant (the client software), and the authentication server (a Remote Authentication Dial-In User Service server (RADIUS)). 802.1x authentication security initiates an authorization request from the wireless client to the access point, which authenticates the client to an Extensible Authentication Protocol (EAP) compliant RADIUS server. This RADIUS server may authenticate either the user (via passwords or certificates) or the system (by MAC address). In theory, the wireless client is not allowed to join the networks until the transaction is complete. There are several authentication algorithms used for 802.1x. Some examples are: MD5-Challenge, EAP-TLS, EAP-TTLS, Protected EAP (PEAP), and EAP-Cisco Wireless Light Extensible Authentication Protocol (LEAP). These are all methods for the wireless client to identify itself to the RADIUS server. With RADIUS authentication, user identities are checked against databases. RADIUS constitutes a set of standards addressing Authentication, Authorization and Accounting (AAA). Radius includes a proxy process to validate clients in a multi-server environment. The IEEE 802.1x standard is for controlling and authenticating access to port-based 802.11 wireless and wired Ethernet networks. Port-based network access control is similar to a switched local area network (LAN) infrastructure that authenticates devices that are attached to a LAN port and prevent access to that port if the authentication process fails.

What is a RADIUS?

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

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

How 802.1x authentication works

A simplified description of the 802.1x authentication is:

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

802.1x features

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

Refer to Security_Settings for more information.

WPA/WPS2

Wi-Fi Protected Access (WPA/WPA2) is a security enhancement that strongly increases the level of data protection and access control to a wireless network. WPA enforces 802.1x authentication and key-exchange and only works with dynamic encryption keys. To strengthen data encryption, WPA utilizes its Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements that include a per-packet key mixing function, a message integrity check (MIC) named Michael an extended initialization vector (IV) with sequencing rules, and a also re-keying mechanism. Using these improvement enhancements, TKIP protects against WEP's known weaknesses.

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

WPA/WPA2 – Enterprise provides this level of security on enterprise networks with a 802.1x RADIUS server. An Authentication Type is selected to match the authentication protocol of the 802.1x server.

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

Cisco Features

Cisco LEAP

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

Fast Roaming (CCKM)

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

CKIP

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

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

EAP-FAST

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

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

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

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

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

Mixed Cells Mode

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

Radio Management

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

Back to Contents

Back to Contents

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

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

Connecting to a wireless network

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

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

Connect to a wireless network without security

To connect to a wireless network without security:

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

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

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

Connect to a wireless network with WEP security

To connect to a wireless network with WEP security:

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

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

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

Connect to a wireless network using a profile

To connect to a wireless network using a profile:

1. Select the profile from the Profiles List.
2. Click **Connect**. The connection icon indicates that you are connected to the network. The network name, speed, and signal quality display the current connection status. Click the Details button to display details of the current network connection.

NOTE: For a list of available access ports on a particular wireless network, click the **Properties** button on the main window. Refer to Network Properties for details.

Scan for available networks

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

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

Setting up a Linksys Access Point

Configure a Linksys (EOU) Access Point

Configure a Linksys (EOU) Access Point

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

Linksys (EOU) features:

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

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

Configure a Linksys (EOU) Access Point

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

Wireless Network Configuration Wizard - Step 1

Welcome to Wireless Network Configuration

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

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

NOTE: You can re-enable this feature in the Intel PROSet/Wireless Application Settings.

1. Click **Next** to continue.

Verify Ownership of your Linksys Access Point - Step 2

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

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

2. Find the Ownership ID and Device ID key printed on the bottom of your Linksys Access Point or Wireless Router and enter it in the appropriate box.

- **Ownership ID:** Enter the eight-character ownership identification key.
- **Device ID:** Enter the eight-character device identification key.

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

3. Click **Next** to continue.

Enter New Configuration for Linksys Access Point - Step 3

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

Enter Network Name (SSID)

- **What is the Network Name**: Enter a network name (SSID) that identifies this wireless network. You can use a simple pass-phrase such as Jerry's Wireless Network or ORoomMLAN or use a more secure stronger network name such as 1Ge4Ty9Ma.
- The Network Name can be up to 32 characters long. You may use upper- and lower-case letters, numbers, spaces, and most special characters. Avoid these characters: ! , ? " * + / \ ^

Securing your Network

Select one of the following options:

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

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

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

Enter a Pass Phrase

Choose a **simple** or **strong** pass phrase (password) that is easy to remember. Enter at least 32 alphanumeric characters or more (a-z, A-Z, 0-9) and one special character from (! @ % *) ( ) _ + = [ ] { } ~ ^ ?

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

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

Wireless Configuration Complete - Final Step

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

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

Intel PROSet/Wireless Configuration Service

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

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

Intel PROSet/Wireless Configuration Service Overview

About the Configuration Service
Other Wireless Managers

The Intel Wireless Network Configuration Service provides automatic wireless connection to available wireless networks using profiles created and prioritized in the Profiles List. This feature is constantly monitoring in the background the connection status of the wireless adapter. If a matching profiles are found in the Profiles list for an available network, a balloon prompt is displayed indicating that wireless networks are available. If you click the balloon prompt, the **Connect to a wireless network** dialog is displayed. From this dialog you can select an available network and click **Configure** to configure the wireless network for connection.

About the Configuration Service

- The Configuration Service is launched when you log on to your computer.
- Available networks are automatically connected when a matching profile is found in the list.
- If a matching profile is found for multiple wireless networks, if a network with a higher priority profile becomes available, the current connection is not disconnected. You may manually connect to that higher profile by selecting the profile in Intel PROSet/Wireless and clicking **Connect**.
- The service is only available if the Intel PROSet/Wireless software is installed.
- If no matching profiles are found for an available network, you are prompted to create a profile in the Profiles List. Then you are notified of available networks.
- If there are multiple profiles found for an available network, you are prompted to choose which profile to connect.

Other Wireless Managers

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

Windows XP Wireless Manager

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

- **From the Task Tray Menu:**

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

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

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

- **From Intel PROSet/Wireless:**

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

3rd Party Wireless Software

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

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

Back to Contents

Trademarks and Disclaimers

Back to Contents

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

- Intel Wireless Troubleshooter
- Event Viewer
- Resolving Errors

Intel Wireless Troubleshooter

Name	About. Displays version information for the Intel Wireless Troubleshooter
File	Exit. Exit Intel Wireless Troubleshooter
Help	**Intel(R) Wireless Troubleshooter Help:** Displays online help on the Intel Wireless Troubleshooter

Wireless Event Viewer	Click to open the Wireless Event Viewer
Disable Notification	Click to disable the alert notifications
Enable Notification	Click to enable the alert notifications if an error is detected.
Available Help	Date Time error message: • Description of error • Click here for a more detailed description of the error. • Link to recommended steps to resolve error

Wireless Event Viewer

The Wireless Event Viewer program displays a list of error log records. You can save all available log records in a binary format file for sending to customer support. In addition you can select the binary format log file to an email recipient. Wireless Event Viewer can also display the contents of a previously saved binary log file. The binary log file format is supported under Windows XP SP2 and SP3. To launch Event Viewer, click **Start > Programs > Intel PRO/Set Wireless > > Intel PROset Wireless >Tools > Intel Wireless Troubleshooter > Wireless Event Viewer**.

Name	**Description:** **Preferences: Change the name of the log file by selecting the Preferences menu item. Click on display the Preference dialog.** • **The available logs will be saved to the following file:** The current file name is displays in the Preference dialog. Click on Browse to change the name. **Screen Buffer:** Specify a new fully qualified file name. **OK:** Close the page and apply the new changes. **Cancel:** Close the page without applying the changes. **Exit:** Exit Wireless Troubleshooter.
Level	The severity level of the connection issue is indicated by an icon. The severity levels are: • Information • Error • Warning
Description:	Brief description of the connection issue.
Date and Time	Date and time of the connection issue. This field can be sorted in ascending or descending order. Click the column header to sort the displayed records.
Save As	Save the available logs to the pre-defined file name. Everything in the log shall be saved to the pre-defined file name. Click on Save As to change the name.
Clear	Protocol, Name, SRVR, Dest, Time, Info, LVL, Seq, Ex
	The default file name format can be changed in another name. Removes the information in the Wireless Event Viewer.
Help?	Displays the help information for this dialog.

Resolving Errors

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

Authentication failed due to invalid user credentials
Authentication failed due to invalid password
Authentication failed due to invalid user password
Authentication failed due to invalid server identity
Authentication failed due to invalid server certificate
Authentication failed due to an invalid user certificate
Authentication failed due to timeout
Authentication failed because the AAA server is unavailable
The wireless adapter failed to get a valid IP address
Wireless Adapter Not Associated
Short Card was unexpectedly removed
Disconnection from an Access Point
The Wireless Adapter Is Not Present Or Has Unexpectedly Removed
The Link Server Rejected the EAP Method
An Administrative Profile Failed to Authenticate
An Administrative Profile Failed to Obtain an IP Address from the DHCP Server

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

This authentication error can be caused by invalid user credentials when using either a TTLS or PEAP profile.

Use the following steps to help resolve this error:

1. Select the TTLS or PEAP profile from the list.
2. Click **Properties**.
3. Click **Next**.
4. Select the **Use a PEAP** for the 802.1x Authentication Type.
5. Select the appropriate 802.1x Authentication Type.
   - For TTLS and PEAP profiles: Select the **Use the following** option for User Credentials.
     - Verify the User Name information.
     - **If Use Windows logon or Prompt each time** is selected: select make sure that the correct domain credentials information is used when you connect to the wireless network.
   - For LEAP profiles: Select the **Use the following user name and password** option and verify the user name and password. **If Use Windows logon or Prompt each time** is selected: select make sure that the **username** and **password** is selected make sure that the correct domain credentials information is used when you connect to the wireless network.
   - For TLS profiles: Select the **Use the following** option. Verify that the correct User Name is being used under **Specify user name (identity)**.
6. Click the **OK** button to save the settings.

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

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

Use the following steps to help resolve this error:

1. Select the appropriate profile from the profiles list.
2. Click **Properties**.
3. Click **Next**.
4. Select the appropriate 802.1x Authentication Type.
   - For TTLS and PEAP profiles: Select the **Use the following** option for User Credentials.
     - Verify the password information.
     - **If Use Windows logon** or **Prompt each time** is selected: make sure that the correct domain credentials information is used when you connect to the wireless network.
   - For LEAP profiles: Select the **Use the following user name and password** option and verify the user name and password. **If Use Windows logon or Prompt each time** is selected: select make sure that the **username** and **password** is selected make sure that the correct domain credentials information is used when you connect to the wireless network.
5. Click the **OK** button to save the settings.

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

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

Use the following steps to help resolve this error:

1. Select the appropriate profile from the profiles list.
2. Click **Properties**.
3. Click **Next**.
4. Select the appropriate 802.1x Authentication Type.
   - For TTLS and PEAP profiles: Verify that the correct Authentication Type is selected from the drop-down list. Click on the **Select** button and select another certificate from the list of installed certificates and click **OK**.
   - For TLS profiles: Click the **Select** button and select another certificate from the list of installed certificates and click **OK**.

Note about Certificates: The selected identity should match the field "Issued to" in the certificate and should be registered on the authentication server (i.e., RADIUS server) that is used by the authentication. Your authentication server may be configured to accept only certain certificates. Please contact your IT or network administrator for more information. Other reasons that cause the issue of an invalid server certificate are: You should be logged in using the same username you used when the certificate was installed.

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

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

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

Use the following steps to help resolve this error:

1. Select the appropriate profile from the profiles list.
2. Click **Properties**.
3. Click **Next**.
4. Select the appropriate 802.1x Authentication Type.
   - For TTLS and PEAP profiles: Verify that the correct Authentication Type is selected from the drop-down list. Click on the **Select** button and select another certificate from the list of installed certificates and click **OK**.
   - For TLS profiles: Click the **Select** button and select another certificate from the list of installed certificates and click **OK**.

Note about Certificates: The selected identity should match the field "Issued to" in the certificate and should be registered on the authentication server (i.e., RADIUS server) that is used by the authentication. Your authentication server may be configured to accept only certain certificates. Please contact your IT or network administrator for more information. Other reasons that cause the issue of an invalid server certificate are: You should be logged in using the same username you used when the certificate was installed.

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

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

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

Use the following steps to help resolve this error:

1. Select the appropriate profile from the profiles list.
2. Click **Properties**.
3. Click **Next**.
4. Select the appropriate 802.1x Authentication Type.
   - For TTLS and PEAP profiles: Verify that the Trusted Root Certificate Authority server name is correct.
5. Click **OK** to save the settings.

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

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

Use the following steps to help resolve this error:

1. Select the appropriate profile from the profiles list.
2. Click **Properties**.
3. Click **Next**.
4. Select the appropriate 802.1x Authentication Type.
   - For TTLS and PEAP profiles: Select the **Use the following** option for User Credentials.
     - Verify the Domain information.
     - **If Use Windows logon** or **Prompt each time** is selected: select make sure that the correct Domain credentials information is used when you connect to the wireless network.
   - For LEAP profiles: Select the **Use the following user name and password** option and verify the Domain information. **If Use Windows logon or Prompt each time** is selected: select make sure that the **Domain** and **password** is selected make sure that the correct domain credentials information is used when you connect to the wireless network.
   - For TLS profiles: Click the **Select** button and select another certificate from the list of installed certificates and click **OK**.

Note about Certificates: The selected identity should match the field "Issued to" in the certificate and should be registered on the authentication server (i.e., RADIUS server) that is used by the authentication. Your authentication server may be configured to accept only certain certificates. Please contact your IT or network administrator for more information. Other reasons that cause the issue of an invalid user certificate are: You should be logged in using the same username you used when the certificate was installed.

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

Authentication failed due to timeout

Recommended action:

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

Authentication failed because the AAA server is unavailable

The wireless adapter is associated to the access point, but the 802.1x authentication cannot be completed because of a response from the authentication server.

Recommended action:

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

The wireless adapter failed to get a valid IP address.

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

Use the following steps to resolve this error:

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

Authentication failed because timer expired

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

Recommended action:

1. To prevent the wireless adapter from connecting with this possible Rogue AP, consider adding this Rogue AP to the excluded access points.
2. Select the profile and click the **Connect** button and try to associate with the network and authenticate with the server.

Smart Card was unexpectedly removed

The error occurred because the Smart Card was unexpectedly removed.

Recommended action:

1. Insert the Smart Card.
2. Select the 802.1x EAP-SIM authentication profile and click **Connect** to try to associate with the network.

Disconnection from an Access Point

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

Disconnect from access point due to beacon loss.

Disconnect from access point due to authentication failures.

Disconnect from access point due to TKIP Message Check failure.

Disconnect from access point due to Cisco X-Frame Non-authentication failure.

Disconnect from access point due to 802.1x authentication failure.

Disconnect from access point due to association failure.

Disconnect from access point due to information element failure.

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

Disconnect from access point due to 802.1x authentication failure.

Recommended action:

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

Error Occurred Because the GSM Adapter Was Unexpectedly Removed

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

Use the following steps to help resolve this error:

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

The AAA Server Rejected the EAP Method

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

Use the following steps to help resolve this error:

1. Open Intel PROSet/Wireless by double clicking the task tray icon located at the bottom right of the screen.
2. Select the associated or last used profile from the profiles list.
3. Click **Properties**. The Wireless Profile Properties - General Settings page opens.
4. Click **Next**. The Wireless Profile Properties - Security Settings page opens.
5. Select the correct authentication type.
6. Click **Next** to see Step 2 of the Wireless Profile Properties - Security Settings page.
7. Select the correct EAP Method.
8. Click **OK**. The profile is now re-applied. Intel PROSet/Wireless attempts to connect to the wireless network.

An Administrator Failed to Obtain an IP Address from the DHCP Server

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

Use the following steps to help resolve this error:

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

Back to Contents

Copyright (c) 2004-2005 Intel Corporation. All rights reserved.

Back to Contents

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

---

About Wireless Network Technology

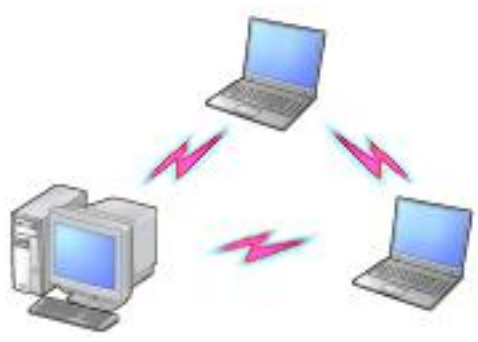
- Choosing a Wireless Network
- Configuring a Wireless Network
- Identifying a Wireless Network

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

Choosing a Wireless Network Mode

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

Device-to-Device mode, also called Ad Hoc mode, works without access points and allows wireless computers to send information directly to other wireless computers. You can use Peer-to-Peer mode to network computers in a home or small office or to set up a temporary wireless network for a meeting.



Configuring a Wireless Network

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

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

Identifying a Wireless Network

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

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

Back to Contents

Back to Contents

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

---

- Intel PROSet/Wireless 2915ABG Network Connection
- Intel PROSet/Wireless 2200BG Network Connection

Specifications: Intel PROSet/Wireless 2915ABG Network Connection

Form Factor	Mini PCI Type 3A	
Dimensions	Width 2.85 in x Length 1.75 in x Height 0.20 in (59.75 mm x 50.95 mm x 5 mm)	
Weight	0.7 oz. (12.90 g.)	
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066	
Dual Diversity Antenna	On-board dual diversity switching	
Connector Interface	124-pin SO-DIMM edge connector	
Voltage	3.3 Volt	
Operating Temperature	0 to +70 degrees Celsius	
Humidity	50 to 85% non-condensing	
Frequency Modulation	**5 GHz (802.11a)**	**2.4 GHz (802.11b/g)**
Frequency band	5.15 GHz to 5.85 GHz	2.400 - 2.472 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Medium	5 GHz UNII: Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz ISM: Orthogonal Frequency Division Multiplexing (OFDM)
Channels	4 to 12 non-overlapping, dependent on country	Channel 1-11 (US only) Channel 1-13 (Japan, Europe)
Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	11, 5.5, 2, 1 Mbps
General		
Operating Systems	Windows XP, Windows 2000	
Wi-Fi® Alliance certification	Wi-Fi® certification for 802.11b, 802.11g, 802.11a	
WLAN Standard	IEEE 802.11g, 802.11b, 802.11a	
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes	
Security	WPA, WPA-Enterprise, AES 128-bit, WEP 128-bit and 64-bit.Cisco Compatible Extensions v2.0, 802.1x: LEAP, PEAP, TKIP, EAP-TLS, EAP-TTLS, MD5	
Product Safety	UL, C-UL, CB (IEC 60590)	

Specifications: Intel PROSet/Wireless 2200BG Network Connection

Form Factor	Mini PCI Type 3A	
Dimensions	Width 2.85 in x Length 1.75 in x Height 0.20 in (59.75 mm x 50.95 mm x 5 mm)	
Weight	0.7 oz. (12.90 g.)	
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066	
Dual Diversity Antenna	On-board dual diversity switching	
Connector Interface	124-pin SO-DIMM edge connector	
Voltage	3.3 Volt	
Operating Temperature	0 to +80 degrees Celsius	
Humidity	50 to 85% non-condensing	
2.4 GHz Band (802.11b/g	**Most of the World (United States)**	**Rest of World (Europe, Japan)**
Frequency ranges	2.412 - 2.462 GHz	2.412 - 2.472 GHz
Channels	1 - 11 (active scan)	1 - 13 (active scan)
Modulation	CCK, DQPSK, DBPSK, BPSK, QPSK, 16 QAM, 64 QAM	
Wireless Medium	2.4 GHz ISM: Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM)	
Data Rates	54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 Mbps	
General		
Operating Systems	Windows XP, 2000	
Wi-Fi® Alliance certification	Wi-Fi® certification for 802.11b, 802.11g, 802.11a	
WLAN Standard	IEEE 802.11g, 802.11b, 802.11a	
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes	
Security	WPA, WPA-Enterprise, AES 128-bit, WEP 128-bit and 64-bit.Cisco Compatible Extensions v2.0, 802.1x	
Product Safety	UL, C-UL, CB (IEC 60590)	

Back to Contents

Trademarks and Disclaimers

Back to Contents

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

---

Numerical A B D E F I K M O P R S T U W

Numerical

802.11a: The 802.11a standard specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz. The 802.11a standard uses the Orthogonal Frequency Division Multiplexing (OFDM) transmission method. Additionally, the 802.11a standard supports 802.11 features such as WEP encryption for security.

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

802.11g: The 802.11g standard specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and WEP encryption for security. 802.11g networks are also referred to as Wi-Fi networks.

A

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

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

B

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

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

Bluetooth: An incompatible, very short-range lower speed communications system (PAN), developed first in Europe as a "cable replacement" for printers and similar peripheral connections. Its usage has expanded to include cordless earphones and similar devices. It uses the 2.4 GHz ISM band, and "co-exists" with 802.11b. Here the term, "co-exist" means that not all researchers agree on the amount of mutual interference generated when both systems operate in the same location.

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

D

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

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

Direct-Sequence Spread Spectrum (DSSS) and Frequency-Hop Spread Spectrum (FHSS): Two incompatible

technologies used in radio transmission.

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

E

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

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

EAP-TLS: A type of authentication method using the Extensible Authentication Protocol (EAP) and a security protocol called the Transport Layer Security (TLS). EAP-TLS uses certificates which use passwords. EAP-TLS authentication supports dynamic WEP key management.

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

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

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

F

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

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

I

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

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

Infrastructure Network: A wireless network centered around an access point. In this environment, the access point not only provides communication with the wired network but also mediates wireless network traffic in the immediate neighborhood.

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

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

K

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

M

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

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

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

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

O

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

P

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

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

R

Radio Frequency (RF) Terms (GHz, MHz, Hz): The international unit for measuring frequency is Hertz (Hz), which is equivalent to the older unit of cycles per second. One Mega-Hertz (MHz) is one million Hertz. One Giga-Hertz (GHz) is one billion Hertz. For reference: the standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 0.55 -1.6 MHz, the FM broadcast radio frequency band is 88-108 MHz, and microwave ovens typically operate at 2.45 GHz.

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

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

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

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

S

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

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

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

T

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

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

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

U

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

W

WEP64 and WEP128: Wired Equivalent Privacy, 64-bit and 128-bit (64-bit is sometimes referred to as 40-bit). This is a low-level encryption technique designed to give the user about the same amount of privacy that he would expect from a LAN. It is recommended to use the 128-bit option at all possible times. Remember that 802.11 devices transmit (broadcast) in all directions, and that it is possible, with very complex software, to copy and decode WEP transmissions. The task is not trivial, but it is possible. If your data is extremely sensitive, you should consider some form of secondary protection, such as strong passwords and an additional level of encryption. Suitable software packages are available from reputable suppliers. Although not intended by the original architects, WEP also helps prevents unauthorized access to your system by an outsider. Hackers have been known to access systems from outside a building, and to then to access the Web for a leisurely session, all at the system owner's expense.

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

Wireless: A microwave transceiver system.

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

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

Back to Contents

Back to Contents

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

---

Customer Support

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

Online Support

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

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

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

Back to Contents

Back to Contents

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

- Information For the User
- Regulatory Information

Products Covered

The information in this document applies to the following products:

Tri-mode wireless LAN adapters (802.11a/802.11b/802.11g)
Intel(R) PROSet/Wireless 2915ABG Network Connection (model WM3945ABG)
Intel(R) PROSet/Wireless 2915ABG Network Connection (model WM3945ABG)

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

Information for the user

Safety Notices

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. The Intel(R) PRO/Wireless 2915ABG Network Connection adapters meet the Human Exposure limits found in OET Bulletin 65, 2001, and Supplement B, 2001. These limits are consistent with the standards of the instructions found in Technical Manual will result in exposure substantially below the FCC's recommended limits.

The following safety precautions should be observed:

- Do not touch or move antenna while the unit is transmitting or receiving.
- Do not hold any component containing the radio such that the antenna is very close or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- Do not operate the radio or attempt to transmit data unless the antenna is connected; if not, the radio may be damaged.
- Use only the supplied or approved antenna.
  - The use of antenna devices other than antennas supplied or limited by the constraints posed by the safety directors of the FCC is prohibited.
  - The use of antenna devices on airplanes is governed by the Federal Aviation Administration (FAA).
  - The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.
- Antenna Placement
  - In order to comply with FCC RF exposure limits, low gain integrated antennas should be located at a minimum distance of 20 cm (8 inches) or more from the body of all persons.
  - High-gain, wall-mount, or mast-mount antennas are designed to be professionally installed and should be located at a minimum distance of 30 cm (12 inches) or more from the body of all persons. Installation by non-professional installer, SAR measurements are mandatory for proper installation requirements.
- Explosive Device Proximity Warning (see below)
- Antenna Warning (see below)
- Use on Aircraft Caution (see below)
- Other Wireless Devices (see below)
- Power Supply (Across Point) (see below)

Explosive Device Proximity Warning

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

Antenna Warnings

Warning: To comply with the FCC and ANSI C95.1 RF exposure limits, it is recommended for the Intel(R) PRO/Wireless2915ABG Network Connection adapter, when installed in a desktop computer, that the antenna for this device be installed to provide a separation distance of at least 20 cm (8 inches) from all persons and must not be co-located or operating in conjunction with any other antenna or radio transmitter. It is recommended that the user limit exposure time if the antenna is positioned closer than 20 cm (8 inches).

Warning: Intel(R) PRO/Wireless LAN products are not designed for use with high-gain directional antennas. Use of such antennas with these products is illegal.

Use On Aircraft Caution

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

Other Wireless Devices

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

Local Restrictions on 802.11a and 802.11b Radio Usage

Caution: Due to the fact that the frequencies used by 802.11a and 802.11b wireless LAN devices may not yet harmonized in all countries, 802.11a and 802.11b products are designed for use only in specific countries, and are not allowed to be operated in countries outside the specified regions. It is the duty of the user of the product to ensure that the product is operated only in the countries for which they were intended and for verifying that they are authorized for radio use in the country in question. Contact the country of use. The device transmitter power control (TPC) interface is part of the Intel(R) PRO/Wireless software. Operational restrictions for Equivalent Isotropic Radiated Power (EIRP) are controlled by the system manufacturer. Any deviation from the permissible power and antenna specifications of the country of use is an infringement of national law and may be punishable by fines.

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

Wireless Interoperability

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

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

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

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

- Using the Intel(R) PRO/Wireless 2915ABG Network Connection adapter equipment on board aircraft.
- Using the Intel(R) PRO/Wireless 2915ABG Network Connection adapter equipment in an environment where the risk of interference with other devices or services is perceived or deemed to be harmful.

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

Regulatory Information

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

Information for OEM integrators: Please refer to the full Grant of equipment document for other restrictions.

The Intel(R) PRO/Wireless 2915ABG Network Connection adapter wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. For country-specific information, see the Intel(R) PRO/Wireless 2915ABG Compliance Addendum. Any units or television interference caused by unauthorized modification of the devices included with the Intel(R) PRO/Wireless 2915ABG Network Connection adapter kit, or the subsequent attachment of connecting cables and equipment other than those specified by the manufacturer, shall be corrected at the expense of the by such unauthorized modification, substitution or attachment is the responsibility of the user. Intel Corporation and its authorized resellers or distributors are not liable for any radio or television interference or violations of rules that arise from the user failing to comply with these guidelines.

NOTE Your Intel(R) PRO/Wireless 2915ABG Network Connection adapter transmits less than 100 mW, but more than 50 mW.

USA—Federal Communications Commission (FCC)

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

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

NOTE The radiated output power of the Intel(R) PRO/Wireless 2915ABG Network Connection adapter wireless network device is far below the FCC radio frequency exposure limits. Nevertheless, the Intel(R) PRO/Wireless LAN wireless network device may cause some local TV or radio interference or potential for human harm during normal operation that is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, you should keep a distance of at least 2 cm between you (or any other person in the vicinity) and the antenna that is built into the computer.

Interference statement

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

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

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

Canada—Industry Canada (IC)

This device complies with RSS210 of Industry Canada.

Europe Frequency Bands

2.400 - 2.4835 GHz (Europe ETS)

5.15 - 5.35 GHz and 5.47-5.725 GHz (Europe ETS)
5.15-5.25 can be used outdoors and other 5 GHz supported must be indoors.
Low band 5.25 - 5.35 GHz is for indoor use only.

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

Declaration of Conformity

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

English	Hereby, [Name of manufacturer] declares that this [radio equipment] is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	[Valmistaja = manufacturer] vakuuttaa täten että [tyyppinimi] [radiolaite] [tyypinnimi] täyttävät olennaiset ja muut tätä direktiivin 1999/5/EY direktiivin vaatimukset.ja sitä koskevien direktiivien muiden ehtojen mukaisesti.
Dutch	[Naam van de fabrikant] verklaart dat het toestel [type van toestel] in overeenstemming is met de essentiële eisen en de overige relevante bepalingen van richtlijn 1999/5/EC.
French	[Nom du fabricant] déclare que le [type de matériel] de [nom] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Swedish	[Tillverkarens namn] [Tillverkarens namn] [Beskrivning av produkten] [Identitetsbeteckning] med de väsentliga egenskaperna och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	[Navn på producent] [Navn på producent] [Produktbeskrivelse] [Produktnavn] [udstyrets typebetegnelse] overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
German	[Name des Herstellers] [Name des Herstellers] [Allgemeine Produktbeschreibung] [Produktbezeichnung] [Gerätetyp] in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG entsprechen.
Greek	[Όνομα κατασκευαστή] [Όνομα κατασκευαστή] [Περιγραφή προϊόντος] [Ονομασία προϊόντος] [Τύπος συσκευής] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣΤΙΘΕΜΕΝΩΝ ΟΥΣΙΩΔΩΝ ΑΠΑΙΤΗΣΕΩΝ ΚΑΙ ΤΩΝ ΛΟΙΠΩΝ ΣΧΕΤΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Italian	Con la presente [nome del costruttore] dichiara che questo [tipo di apparecchio] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente [nombre del fabricante] declara que el [clase de equipo] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Portuguese	[Nome do fabricante] declara que este [tipo de equipamento] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Malti	Hiwenhiek, [isem tal-fabrikatur], jiddikjara li dan [il-mudel tal-prodott] jikkonformaw mal-ħtiġiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Direttiva 1999/5/EC.

New Member States requirements of Declaration of Conformity

Estonian	Käesolevaga kinnitab [firma nimi = Name of manufacturer] [seadme liik = Description of equipment] vastavus direktiivi 1999/5/EÜ põhinõuetele ja nõuetele direktiivi kohaselevastavat lisatingimustele.
Hungary	Alulírott, [gyártó neve] nyilatkozom, hogy a [...-típusú] megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK direktíva egyéb ide vonatkozó rendelkezéseinek.
Slovak	Menej vyrobcu] týmto vyhlasuje, že [typ zariadenia] spĺňa základné požiadavky a ostatné príslušné ustanovenia Smernice 1999/5/ES.
Czech	[Jméno výrobce] tímto prohlašuje, že tento [typ zařízení] je ve shodě se základními požadavky a dalšími ustanoveními směrnice 1999/5/ES.
Slovenia	Tovo [ganmetny ponadlomeni] deklaracija, kot bo [ganmetny ponadlomeni] ustrelna komunikacijska oprema [ganmetny ponadlomeni] v skladu z osnovnimi zahtevami in drugimi ustreznimi predpisi Direktive 1999/5/EC.

France

For Metropolitan departments
2.400 - 2.483 GHz (Europe ETS)
2.400 - 2.454 GHz (Channels 1 to 7) for outdoor use.

For Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte:
2.400 - 2.483GHz (Ch1 for indoor and outdoor use)

For Reunion, Guyane:
2.400 - 2.483GHz (Ch1 for indoor use)
2.400 - 2.483GHz (Ch1 for outdoor use (channels 5 to 13)

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

Italia

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

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

Japan Frequency Bands

2.400 - 2.497 GHz (Japan)
5.15 to 5.25 (after Japanese channels) active scan.

High Band Frequencies

5.725 to 5.825 active scan.

Radio approvals

To determine whether you are allowed to use your wireless network device in a specific country, please check to see if the radio type within your wireless network device has received approval and is listed in the manufacture OEM Regulatory Guidance document.

Underwriters Laboratories Inc. (UL) Regulatory Warning

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

Back to Contents

Back to Contents

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

Product Warranty Information

One-Year Limited Hardware Warranty

Limited Warranty

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

SOFTWARE OF ANY KIND DELIVERED WITH OR AS PART OF THE PRODUCT IS EXPRESSLY PROVIDED "AS IS", SPECIFICALLY EXCLUDING ALL OTHER WARRANTIES, EXPRESS, IMPLIED (INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE), provided however, that Intel warrants that the media on which the software is furnished will be free from defects for a period of ninety (90) days from the date of delivery. If such a defect appears within the warranty period, you may return the defective media to Intel for replacement or alternative delivery of the software at Intel's discretion and without charge. Intel does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the software.

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

- **REPAIR** the Product by means of hardware and/or software; OR
- **REPLACE** the Product with another product, OR, if Intel is unable to repair or replace the Product,

- **REFUND** the then-current Intel price for the Product at the time a claim for warranty service is made to Intel under this Limited Warranty.

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

Extent of Limited Warranty

Intel does not warrant that the Product, whether purchased stand-alone or integrated with other products, including without limitation, semi-conductor components, will be free from design defects or errors known as "errata." Current characterized errata are available upon request. Further, this Limited Warranty does NOT cover: (i) any costs associated with the replacement or repair of the Product, including labor, installation or other costs incurred by you, and in particular, any costs relating to the removal or replacement of any Product soldered or otherwise permanently affixed to any printed circuit board or integrated with other products; (ii) damage to the Product due to external causes, including accident, problems with electrical power, abnormal, mechanical or environmental conditions, usage not in accordance with product instructions, misuse, neglect, accident, abuse, alteration, repair, improper or unauthorized installation or improper testing, or (iii) any Product which has been modified or operated outside of Intel's publicly available specifications or where the original product identification markings (trademark or serial number) has been removed, altered or obliterated from the Product; or (iv) issues resulting from incorporation of software products into a system, or (v) failure to apply Intel-supplied modifications or corrections to any software provided with or included in the Product.

How to Obtain Warranty Service

To obtain warranty service for the Product, you may contact your original place of purchase in accordance with its instructions or you may contact Intel. To request warranty service from Intel, you must contact the Intel Customer Support ("ICS") center in your region (Click Here) within the warranty period during normal business hours (local time), excluding holidays and return the Product to the designated ICS center. Please be prepared to provide: (1) your name, mailing address, email address, telephone numbers and, in the USA, valid credit card information; (2) proof of purchase; (3) model name and product identification number found on the Product; and (4) an explanation of the problem. The Customer Service Representative may need additional information from you depending on the nature of the problem. Upon ICS's verification that the Product is eligible for warranty service, you will be issued a Return Material Authorization ("RMA") number and provided with instructions for returning the Product to the designated ICS center. When you return the Product to the ICS center, you must include the RMA number on the outside of the package. Intel will not accept any returned Product without an RMA number, or that has an invalid RMA number, on the package. You must deliver the returned Product to the designated ICS center in the original or equivalent packaging, with shipping charges pre-paid (within the USA), and assume the risk of damage or loss during shipment. Intel may elect to repair or replace the Product with either a new or reconditioned Product or components, as Intel deems appropriate. The repaired or replaced product will be shipped to you at the expense of Intel within a reasonable period of time after receipt of the returned Product by ICS. The returned Product shall become Intel's property on receipt by ICS. The replacement product is warranted under this written warranty and is subject to the same limitations of liability and exclusions for ninety (90) days or the remainder of the original warranty period, whichever is longer. If Intel replaces the Product, the Limited Warranty period for the replacement Product is not extended.

WARRANTY LIMITATIONS AND EXCLUSIONS

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

LIMITATIONS OF LIABILITY

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

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

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