

A simplified description of 802.1x authentication is:

- A client sends a "request to access" message to an access point. The access point requests the identity of the client.
 - The client replies with its identity packet which is passed along to the authentication server.
 - The authentication server sends an "accept" packet to the access point.
 - 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:
 - EAP TLS Authentication Protocol - RFC 2716 and RFC 2246
 - EAP Tunneled TLS (TTLS)
 - PEAP
 - Supports Microsoft Windows XP and Windows 2000
-

WPA or WPA2

Wi-Fi Protected Access (WPA or 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 Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements that include a per-packet key mixing function, a message integrity check (MIC) called Michael an extended initialization vector (IV) with sequencing rules, and a rekeying mechanism. With 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.

Enterprise Mode: Enterprise Mode verifies network users through a RADIUS or other authentication server. WPA utilizes 128-bit encryption keys and dynamic session keys to ensure your wireless network's privacy and enterprise security. Enterprise Mode is targeted to corporate or government environments.

Personal Mode: Personal Mode requires manual configuration of a pre-shared key (PSK) on the access point and clients. PSK authenticates users via a password, or identifying code, on both the client station and the access point. No authentication server is needed. Personal Mode is targeted to home and small business environments.

WPA-Enterprise and WPA2-Enterprise: Provide this level of security on enterprise networks with an 802.1x RADIUS server. An authentication type is selected to match the authentication protocol of the 802.1x server.

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

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

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

NOTE: Some security solutions may not be supported by

your computer's operating system and may require additional software or hardware as well as wireless LAN infrastructure support. Check with your computer manufacturer for details.

TKIP (Temporal Key Integrity Protocol) is an enhancement to WEP (Wired Equivalent Privacy) security. TKIP provides per-packet key mixing, a message integrity check and a rekeying mechanism, which fixes the flaws of WEP.

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. The TLS protocol is intended to secure and authenticate communications across a public network through data encryption. The TLS Handshake Protocol allows the server and client to provide mutual authentication and to negotiate an encryption algorithm and cryptographic keys before data is transmitted.

TTLS

These settings define the protocol and the credentials used to authenticate a user. In TTLS (Tunneled Transport Layer Security), 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, as MD5 Challenge over this encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel. TTLS implementations today support all methods defined by EAP, as well as several older methods ([PAP](#), [CHAP](#), [MS-CHAP](#) and MS-CHAPv2). TTLS can easily be extended to work with new protocols by defining new attributes to support new protocols.

Authentication Protocols

- **PAP:** Password Authentication Protocol is a two way handshake protocol designed for use with PPP. Authentication Protocol Password Authentication Protocol is a plain text password used on older SLIP systems. It is not secure.
- **CHAP:** Challenge Handshake Authentication Protocol is a three way handshake protocol which is considered more secure than PAP (Password Authentication Protocol).
- **MS-CHAP (MD4):** Uses a Microsoft version of RSA Message Digest 4 challenge and reply protocol. This only works on Microsoft systems and enables data encryption. This authentication method causes all data to be encrypted.

PEAP

PEAP is a new Extensible Authentication Protocol (EAP) IEEE 802.1x authentication type designed to take advantage of server-side EAP-Transport Layer Security (EAP-TLS) and to support various authentication methods, including users' passwords and one-time passwords, and Generic Token Cards.

Cisco Features

Cisco LEAP

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

Cisco Rogue Access Point Security Feature

The Cisco Rogue Access Point feature provides security protection from an introduction of a rogue access point that could mimic a legitimate access point on a network in order to extract information about user

credentials and authentication protocols that could compromise security. This feature only works with Cisco's LEAP authentication. Standard 802.11 technology does not protect a network from the introduction of a rogue access point. Refer to [LEAP Authentication](#) for more information.

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 Sequence Number

802.11b and 802.11g Mixed Environment Protection Protocol

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

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 is able 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 are 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 is 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-Cell 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 use standard mode, send all messages unencrypted. These access points broadcast that the network does not use encryption, but allows clients that use WEP mode to join . When Mixed-Cell is enabled in a profile, it allows you to connect to access points that are configured for "optional encryption."

Radio Management

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

[Back to Top](#)

[Back to Contents](#)

[Trademarks and Disclaimers](#)

Glossary of Terms: Intel(R) PRO / Wireless 3945ABG Network Connection User Guide

Glossary

[Numerical](#) [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [L](#) [M](#) [N](#) [O](#)
[P](#) [R](#) [S](#) [T](#) [W](#)

Term	Definition
802.11	The 802.11 standard refers to a family of specifications developed by the IEEE for wireless LAN technology. The 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
802.11a	The 802.11a standard specifies a maximum data transfer rate of 54 Mbps and an operating frequency of 5 GHz. The 802.11a standard uses the Orthogonal Frequency Division Multiplexing (OFDM) transmission method. Additionally, the 802.11a standard supports 802.11 features such as WEP encryption for security.
802.11b	802.11b is an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. Throughput data rate 5+ Mbps in the 2.4 GHz band.

802.11g	The 802.11g standard specifies a maximum data transfer rate of 54 Mbps, an operating frequency of 2.4GHz, and WEP encryption for security. 802.11g networks are also referred to as Wi-Fi networks.
802.1x	802.1x is the IEEE Standard for Port-Based Network Access Control. This is used in conjunction with EAP methods to provide access control to wired and wireless networks.
AAA Server	Authentication, Authorization and Accounting Server. A system to control access to computer resources and track user activity.
Access Point	Access point (AP). A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer and to connect to the Internet.
ad hoc network	A communication configuration in which every computer has the same capabilities, and any computer can initiate a communication session. Also known as a peer-to-peer network or a computer-to-computer network.
AES-CCMP	Advanced Encryption Standard - Counter CBC-MAC Protocol is the new method for privacy protection of wireless transmissions specified in the IEEE 802.11i standard. AES-CCMP provides a stronger encryption method than TKIP.
Authentication	Verifies the identity of a user logging onto a network. Passwords, digital certificates, smart cards and biometrics are used to prove the identity of the client to the network. Passwords and digital certificates are also used to identify the network to the client.
BER	Bit error rate. The ratio of errors to the total number of bits being sent in a data transmission from one location to another.
Bit Rate	The total number of bits (ones and zeros) per second that a network connection can support. Note that this bit rate will vary, under software control, with different signal path conditions.

Broadcast SSID	Used to allow an access point to respond to clients on a wireless network by sending probes.
BSSID	A unique identifier for each wireless client on a wireless network. The Basic Service Set Identifier (BSSID) is the Ethernet MAC address of each adapter on the network.
CA (certificate authority)	A corporate certification authority implemented on a server. In addition, Internet Explorer's certificate can import a certificate from a file. A trusted CA certificate is stored in the root store.
CCX	Cisco Compatible eXtension. Cisco Compatible Extensions Program ensures that devices used on Cisco wireless LAN infrastructure meet the security, management and roaming requirements.
Certificate	Used for client authentication. A certificate is registered on the authentication server (i.e., RADIUS server) and used by the authenticator.
CKIP	Cisco Key Integrity Protocol (CKIP) is a Cisco proprietary security protocol for encryption in 802.11 media. CKIP uses a key message integrity check and message sequence number to improve 802.11 security in infrastructure mode. CKIP is Cisco's version of TKIP.
Client computer	The computer that gets its Internet connection by sharing either the host computer's connection or the Access Point's connection.
DSSS	Direct Sequence Spread Spectrum. Technology used in radio transmission. Incompatible with FHSS.
EAP	Short for Extensible Authentication Protocol, EAP sits inside of Point-to-Point Protocol's (PPP) authentication protocol and provides a generalized framework for several different authentication methods. EAP is supposed to head off proprietary authentication systems and let everything from passwords to challenge-response tokens and public-key infrastructure certificates all work smoothly.

EAP-FAST	EAP-FAST, like EAP-TTLS and PEAP, uses tunneling to protect traffic. The main difference is that EAP-FAST does not use certificates to authenticate.
EAP-GTC	The EAP-GTC (Generic Token Card) is similar to the EAP-OTP except with hardware token cards. The request contains a displayable message, and the response contains the string read from the hardware token card.
EAP-OTP	EAP-OTP (One-Time Password) is similar to MD5, except it uses the OTP as the response. The request contains a displayable message. The OTP method is defined in RFC 2289. The OTP mechanism is employed extensively in VPN and PPP scenarios but not in the wireless world
EAP-SIM	Extensible Authentication Protocol-Subscriber Identity Module (EAP-SIM) authentication can be used with: • Network Authentication types: Open, Shared, and WPA2-Enterprise. • Data Encryption types: None, WEP and CKIP. A SIM card is a special smart card that is used by GSM-based digital cellular networks. The SIM card is used to validate your credentials with the network
EAP-TLS	A type of authentication method using EAP and a security protocol called the Transport Layer Security (TLS). EAP-TLS uses certificates that use passwords. EAP-TLS authentication supports dynamic WEP key management.
EAP-TTLS	A type of authentication method using EAP and Tunneled Transport Layer Security (TTLS). EAP-TTLS uses a combination of certificates and another security method such as passwords.
Encryption	Scrambling data so that only the authorized recipient can read it. Usually a key is needed to interpret the data.

FHSS	Frequency-Hop Spread Spectrum. Technology used in radio transmission. Incompatible with DSSS.
File and printer sharing	A capability that allows a number of people to view, modify, and print the same file(s) from different computers.
Fragmentation threshold	The threshold at which the wireless adapter breaks the packet into multiple frames. This determines the packet size and affects the throughput of the transmission.
GHz	Gigahertz. A unit of frequency equal to 1,000,000,000 cycles per second.
Host computer	The computer that is directly connected to the Internet via a modem or network adapter.
Infrastructure Network	A wireless network centered around an access point. In this environment, the access point not only provides communication with the wired network, but also mediates wireless network traffic in the immediate neighborhood.
IEEE	Institute of Electrical and Electronics Engineers (IEEE) is an organization involved in defining computing and communications standards.
Internet Protocol (IP) address	The address of a computer that is attached to a network. Part of the address designates which network the computer is on, and the other part represents the host identification.
LAN	Local area network. A high-speed, low-error data network covering a relatively small geographic area.
LEAP	Light Extensible Authentication Protocol. A version of Extensible Authentication Protocol (EAP). LEAP is a proprietary extensible authentication protocol developed by Cisco, which provides a challenge-response authentication mechanism and dynamic key assignment.
MAC	A hardwired address applied at the factory. It uniquely identifies network hardware, such as a wireless adapter, on a LAN or WAN.

Mbps	Megabits-per-second. Transmission speed of 1,000,000 bits per second.
MHz	Megahertz. A unit of frequency equal to 1,000,000 cycles per second.
MIC (Michael)	Message integrity check (commonly called Michael).
MS-CHAP	An EAP mechanism used by the client. Microsoft Challenge Authentication Protocol (MSCHAP) Version 2, is used over an encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel.
ns	Nanosecond. 1 billionth (1/1,000,000,000) of a second.
OFDM	Orthogonal Frequency Division Multiplexing.
PEAP	Protected Extensible Authentication Protocol (PEAP) is an Internet Engineering Task Force (IETF) draft protocol sponsored by Microsoft, Cisco, and RSA Security. PEAP creates an encrypted tunnel similar to the tunnel used in secure web pages (SSL). Inside the encrypted tunnel, a number of other EAP authentication methods can be used to perform client authentication. PEAP requires a TLS certificate on the RADIUS server, but unlike EAP-TLS there is no requirement to have a certificate on the client. PEAP has not been ratified by the IETF. The IETF is currently comparing PEAP and TTLS (Tunneled TLS) to determine an authentication standard for 802.1X authentication in 802.11 wireless systems. PEAP is an authentication type designed to take advantage of server-side EAP-Transport Layer Security (EAP-TLS) and to support various authentication methods, including user's passwords and one-time passwords, and Generic Token Cards.
Peer-to-Peer Mode	A wireless network structure that allows wireless clients to communicate with each other without using an access point.

Power Save mode	The state in which the radio is periodically powered down to conserve power. When the notebook is in Power Save mode, receive packets are stored in the access point until the wireless adapter wakes up.
Preferred network	One of the networks that has been configured. Such networks are listed under Preferred networks on the Wireless Networks tab of the Wireless Configuration Utility (Windows 2000 environment) or Wireless Network Connection Properties (Windows XP environment).
RADIUS	Remote Authentication Dial-In User Service (RADIUS) is an authentication and accounting system that verifies users credentials and grants access to requested resources.
RF	Radio Frequency. The international unit for measuring frequency is Hertz (Hz), which is equivalent to the older unit of cycles per second. One Mega-Hertz (MHz) is one million Hertz. One Giga-Hertz (GHz) is one billion Hertz. For reference: the standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 0.55 -1.6 MHz, the FM broadcast radio frequency band is 88-108 MHz, and microwave ovens typically operate at 2.45 GHz.
Roaming	Movement of a wireless node between two micro cells. Roaming usually occurs in infrastructure networks built around multiple access points.
RTS threshold	The number of frames in the data packet at or above which an RTS/CTS (request to send/clear to send) handshake is turned on before the packet is sent. The default value is 2347.
Shared Key	An encryption key known only to the receiver and sender of data.
SIM	Subscriber Identity Module card is used to validate credentials with the network. A SIM card is a special smart card that is used by GSM-based digital cellular networks.

Silent Mode	Silent Mode Access Points or Wireless Routers have been configured to not broadcast the SSID for the wireless network. This makes it necessary to know the SSID in order to configure the wireless profile to connect to the access point or wireless router.
Single Sign On	Single Sign On feature set allows the 802.1x credentials to match your Windows log on user name and password credentials for wireless network connections.
SSID	Service Set Identifier. A value that controls access to a wireless network. The SSID for your wireless network card must match the SSID for any access point that you want to connect with. If the value does not match, you are not granted access to the network. You can have up to three SSIDs. Each SSID can be up to 32 characters long and is case-sensitive.
TKIP	Temporal Key Integrity protocol improves data encryption. Wi-Fi Protected Access utilizes its TKIP. TKIP provides important data encryption enhancements including a re-keying method. TKIP is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP.
TLS	Transport Layer Security. A type of authentication method using the Extensible Authentication Protocol (EAP) and a security protocol called the Transport Layer Security (TLS). EAP-TLS uses certificates which use passwords. EAP-TLS authentication supports dynamic WEP key management. The TLS protocol is intended to secure and authenticate communications across a public network through data encryption. The TLS Handshake Protocol allows the server and client to provide mutual authentication and to negotiate an encryption algorithm and cryptographic keys before data is transmitted.

TTLS	Tunneled Transport Layer Security. These settings define the protocol and the credentials used to authenticate a user. In TTLS, the client uses EAP-TLS to validate the server and create a TLS-encrypted channel between the client and server. The client can use another authentication protocol, typically password-based protocols, such as MD5 Challenge over this encrypted channel to enable server validation. The challenge and response packets are sent over a non-exposed TLS encrypted channel. TTLS implementations today support all methods defined by EAP, as well as several older methods (CHAP, PAP, MS-CHAP and MS-CHAPv2). TTLS can easily be extended to work with new protocols by defining new attributes to support new protocols.
WEP	Wired Equivalent Privacy. Wired Equivalent Privacy, 64- and 128-bit (64-bit is sometimes referred to as 40-bit). This is a low-level encryption technique designed to give the user about the same amount of privacy that he would expect from a LAN. WEP is a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by data over radio waves so that it is protected as it is transmitted from one end point to another.
WEP Key	Either a pass phrase or hexadecimal key. The pass phrase must be 5 ASCII characters for 64-bit WEP or 13 ASCII characters for 128-bit WEP. For pass phrases, 0-9, a-z, A-Z, and ~!@#\$%^&*()_+ `- = { } [] \ : " ; ' < > ? , . / are all valid characters. The hex key must be 10 hexadecimal characters (0-9, A-F) for 64-bit WEP or 26 hexadecimal characters (0-9, A-F) for 128-bit WEP.
Wi-Fi	Wireless Fidelity. Is meant to be used generically when referring of any type to 802.11 network, whether 802.11b, 802.11a, or dual-band.

Wireless Router	A stand-alone wireless hub that allows any computer that has a wireless network adapter to communicate with another computer and to connect to the Internet. Also known as an access point.
WLAN	Wireless Local-Area Network. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.
WPA	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 is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion. WPA consists of RC4 and TKIP and provides support for BSS (Infrastructure) mode only. (Not compatible with WPA2.)
WPA2	Wi-Fi Protected Access 2 (WPA2). This is the second generation of WPA that complies with the IEEE TGi specification. WPA2 consists of AES encryption, pre-authentication and PMKID caching. It provides support for BSS (Infrastructure) mode and IBSS (Ad hoc) mode. (Not compatible with WPA.)
WPA-Enterprise	Wi-Fi Protected Access-Enterprise applies to corporate users. A new standards-based, interoperable security technology for wireless LAN (subset of IEEE 802.11i draft standard) that encrypts data sent over radio waves. WPA is a Wi-Fi standard that was designed to improve upon the security features of WEP as follows: • Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys have not been tampered with. • User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is

	relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network. WPA is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion.
WPA-Personal	Wi-Fi Protected Access-Personal provides a level of security in the small network or home environment.
WPA-PSK	Wi-Fi Protected Access-Pre-Shared Key (WPA-PSK) mode does not use an authentication server. It can be used with the data encryption types WEP or TKIP. WPA-PSK requires configuration of a pre-shared key (PSK). You must enter a pass phrase or 64 hex characters for a Pre-Shared Key of length 256-bits. The data encryption key is derived from the PSK.

[Back to Top](#)

[Back to Contents](#)

[Trademarks and Disclaimers](#)

Administrator Tool: Intel(R) PRO / Wireless 3945ABG Network Connection User Guide

- [Set Administrator Password](#)
 - [Administrator Packages](#)
 - [Administrator Profiles](#)
 - [Persistent](#)
 - [Pre-Logon](#)
 - [Voice over IP \(VoIP\)](#)
 - [Administrator Tool Settings](#)
 - [Administrator Settings](#)
 - [Adapter Settings](#)
 - [Software](#)
 - [Administrator Tasks](#)
-

The Administrator Tool is used by the person who has administrator privileges on this computer. This tool is used to configure common (shared) profiles, pre-logon profiles, and persistent connection profiles. The Administrator Tool can also be used by an Information Technology department to configure user settings within the Intel(R) PROSet/Wireless software and to create custom install [packages](#) to export to other systems.

The Administrator Tool is located on the Tools menu. It must be selected during installation of the Intel PROSet/Wireless software or the feature is not displayed in the Tools menu.

Set Administrator Password

Users cannot modify Administrator settings or profiles unless they have the password for this tool. When you first access the Administrator Tool, you are required to enter a password. The password must not exceed 100 characters. Null passwords are not allowed.

1. **Enter password:** Create a password (maximum 100 characters).
2. **Confirm Password:** Reenter the password.
3. Click **OK**. The [Open Administrator Package](#) displays.

To change the existing password:

1. Click **Administrator Tool** from the Tools menu.
 2. Click **Change Password** on the password entry form.
 3. **Old Password:** Enter the existing password.
 4. **New Password:** Enter the new password.
 5. **Confirm Password:** Reenter the new password again.
 6. Click **OK** to save the new password and enter the Administrator Tool.
-

Administrator Packages

The Administrator Packages are used to save administrative profiles and other settings. You can copy or send this self-extracting executable to clients on your network. When the executable runs, the contents are installed and configured on the destination computer.

To create a new package:

1. On the Tools menu, click **Administrator Tool**.
2. Enter your password to the Administrator Tool.
3. **Administrator Package:** Click **Create a new package**.
4. Click **OK**.
5. Select **Include Settings** on the [Profiles](#), [Settings](#), [Adapter Settings](#), or [Software](#) pages to configure the options to be included in the package.
6. Click **Close**.
7. You are notified: **The current package is changed. Would you like to save the changes?**
8. Click **Yes**. Save the executable file to a directory on the local disk drive.
9. Click **Save**. The file is created. **NOTE:** This process may take several minutes.
10. Click **Finished** to view the package contents.
 - Click **Apply this file to this computer** if you want to use the package configuration on the Administrator's computer.
 - Copy the executable file to any user's computer to install the configuration that has been saved in the package.
11. Click **Enable Intel PROSet/Wireless**. This procedure selects Intel(R) PROSet/Wireless to manage your network profiles.

NOTE: You can also select **Save Package** on the Administrator Tool File Menu to save the package.

To edit a package:

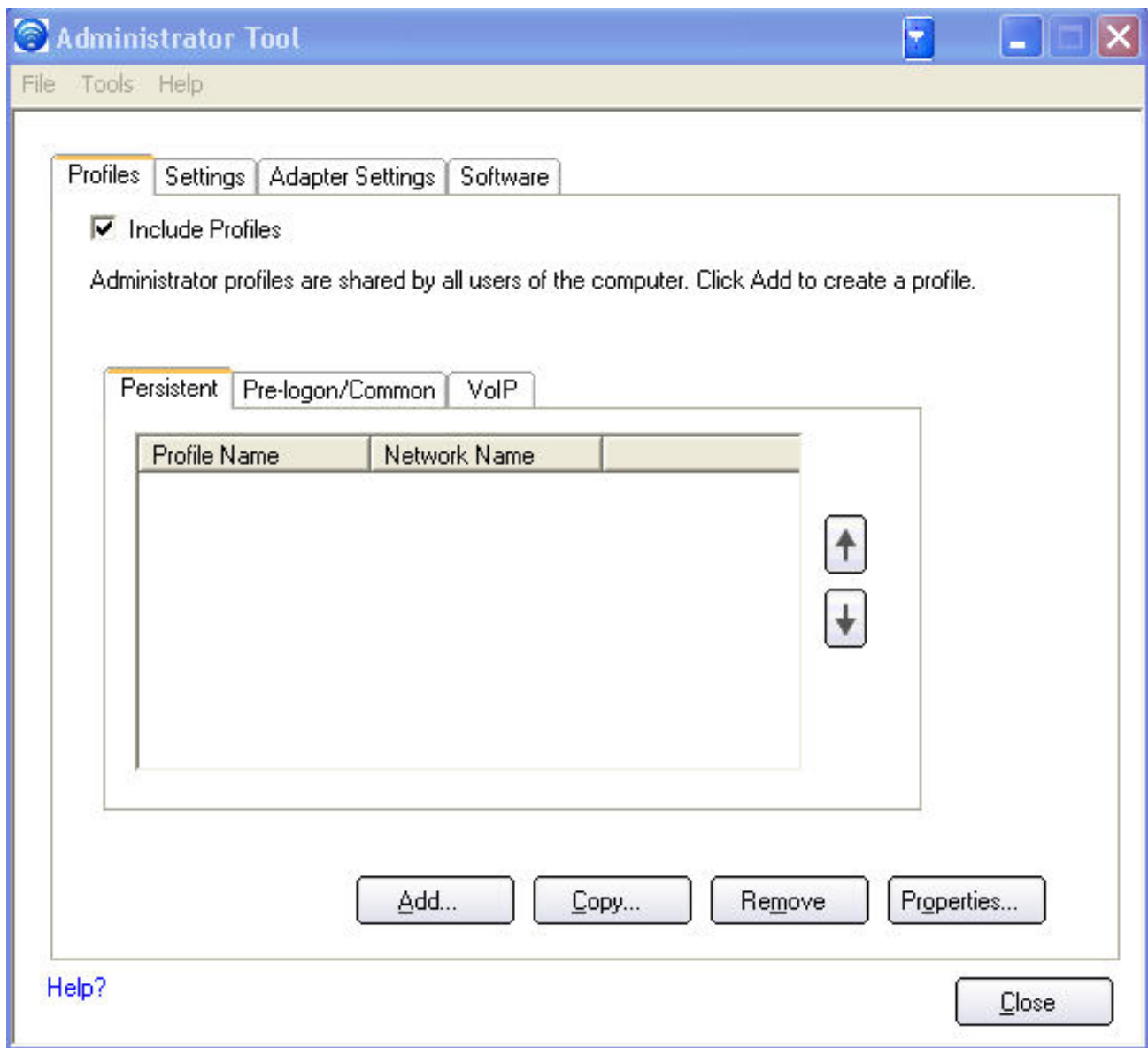
1. Access the Administrator Tool.
2. On the Open Administrator Package page, click **Open** to edit an existing package.
3. Click **Browse**. Locate the package's executable file.
4. Click **Open**. Make your updates.
5. Click **Close**.
6. You are notified: **The current package is changed. Would you like to save the changes?**
7. Click **Yes**. Save the executable file to a directory on the local disk drive.

NOTE: You can also select **Open Package** on the Administrator Tool File menu to edit an Administrator Package.

Administrator Profiles

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

There are three types of Administrator Profiles: **Persistent**, **Pre-login/Common** and **Voice over IP (VoIP)**.



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.

Persistent Connect key points:

- The following types of profiles can be created as Persistent profiles:
 - All profiles that do not require 802.1x authentication (for example, Open authentication with WEP encryption, Open authentication with no encryption).
 - All profiles with 802.1x authentication that have the credentials saved: [MD5](#), [LEAP](#), [EAP-FAST](#).
 - Profiles with security settings that include the "Use the following user name and password" option.

- Profiles that use the machine certificate to authenticate.

NOTE: Intel PROSet/Wireless supports machine certificates. However, they are not displayed in the certificate listings.

- WPA-Enterprise profiles that do not use a user certificate.
- WPA-Personal profiles.
- Persistent profiles are applied at system power up and after a user logs off.

To create a Persistent Profile:

1. Click **Include Profiles**.
2. Click **Persistent**.
3. Click **Add** to open the General Settings.
4. **Wireless Network Name (SSID):** Enter the network identifier.
5. **Profile Name:** Enter a descriptive profile name.
6. **Operating Mode: Infrastructure** is selected.
7. **Administrator Profile Type: Persistent: Active when no users are logged on** is selected.
8. Click **Next**.
9. Click **Enterprise Security** to open the Security Settings. See [Enterprise Settings](#) for 802.1x security configuration information.
10. Click **OK**.

Pre-Logon Connection

Pre-Logon/Common profiles are applied prior to a user log on. If Single Sign On support is installed, the profile is applied and connection is made prior to the the Windows log on sequence (pre-logon).

If Single Sign On support is not installed, the profile is applied once the user session is active.

Pre-logon/Common profiles always appear at the top of a the Profiles list. A user can still prioritize their own profiles that they have created but they cannot reprioritize Pre-logon/Common Profiles. Since these profiles appear at the top of the profiles list, Intel PROSet/Wireless automatically attempts to connect to the Administrator profiles first before any user created profiles.

NOTE: Only administrators can create or export Pre-Logon/Common profiles.

Pre-Logon Connect key points are:

- Pre-Logon Connect is active only at the Windows log on.
- The following types of profiles can be created as Pre-Logon profiles:
 - 802.1x [MD5](#), [LEAP](#), [EAP-FAST](#) profiles that use either the "Use the Windows logon user name and password" or "Use the following user name and password" credentials when configuring the profile's security settings.
 - 802.1x [PEAP](#) or [TTLS](#) profiles with user or machine certificates (the user must have administrative rights to use machine certificates).
 - [TLS](#) profiles that use digital certificates to verify the identity of a client and a server.
 - [EAP-SIM](#) profiles that use a Subscriber Identity Module (SIM) card to validate your credentials with the network.
 - All non-802.1x (Open and WEP) Common or User Based profiles.
- A Pre-Logon profile is applied at Windows user log-on time.

Pre-Logon/Common Connection Status

Pre-Logon support is installed during a **Custom** install of the Intel PROSet/Wireless software. Refer to [Install and Uninstall the Software](#) for more information.

NOTE: If the Single Sign On or Pre-Logon Connect features are not installed, an administrator is still able to create Pre-Logon/Common profiles for export to a user's computer.

The following describes how the Pre-Logon Connect feature functions from system power-up. The assumption is that there is a saved profile with valid security settings marked with "Use Windows Logon user name and password" that are applied at the time of Windows log on.

1. After a system power-up, enter your Windows log on domain, user name, and password.
2. Click **OK**. The Pre-Logon profile Status page displays the progress of the network connection. After the wireless adapter is connected to the network access point, the Status page closes and the Windows user logs on.
 - If the corresponding access point rejects your credentials during the Pre-Logon connect, the profile credentials prompts you for your user credentials.
 - Enter your credentials.
 - Click **OK**. The profile is applied and the Status page displays the progress of the connection status until you are logged onto Windows.
 - Click **Cancel** on the Credentials page to select another profile.

When a user logs off, any wireless connection is disconnected and a persistent profile (if one is available) is applied. Under certain circumstances it is desirable to maintain the current connection (for example, if user specific data needs to be uploaded to the server post-log off or when roaming profiles are used).

Create a profile which is marked as both pre-logon and persistent to achieve this functionality. If such a profile is active when the user logs off, the connection is maintained.

To create a Pre-Logon/Common Profile:

1. Click **Include Profiles**.
2. Click **Pre-Logon/Common**.
3. Click **Add** to open the General Settings.
4. **Wireless Network Name (SSID)**: Enter the network identifier.
5. **Profile Name**: Enter a descriptive profile name.
6. **Operating Mode: Infrastructure** is selected.
7. **Administrator Profile Type: Pre-logon/Common: Active when a user is logged on. This profile is shared by all users.** This profile type is already selected.
8. Click **Next**.
9. Click **Advanced** to open the Advanced Settings. Use the Advanced Settings to set the following:
 - [Auto-Connect](#): Select to automatically or manually connect to a profile.
 - [Auto-Import](#) this profile (for network administrators only).
 - [Mandatory Access Point](#): Select to associate the wireless adapter with a specific access point.
 - [Password protect the profile](#): Select to password protect a profile.
 - [Start application](#): Specify a program to be started when a wireless connection is made.
 - **User Name Format**:

An administrator can select the user name format for the authentication server.

The choices are:

- user (default)
- user@domain
- user@domain.com
- DOMAIN\user

10. Click **OK** to close the Advanced Settings.

11. Click **Enterprise Security** to open the Security Settings. See [Enterprise Security](#) for 802.1x security configuration information.
12. Click **OK** to save the profile and add it to the Administrator profiles list.

NOTE: If a Persistent connection was already established, a Pre-Login/Common profile is ignored if the profile is configured with both Pre-Login/Common and Persistent connection options.

Voice over IP (VoIP) Profiles

Intel PROSet/Wireless software supports VoIP third-party soft-phone applications.

Third party VoIP applications support Voice Codecs. Codecs are used to encode voice for transmission across IP networks. Codecs generally provide a compression capability to save network bandwidth.

Intel PROSet/Wireless software supports the following International Telecommunications Union (ITU) codec standards:

Codec	Algorithm	Data Rate (Kbps)	Comments
ITU G.711	PCM (Pulse Code Modulation)	64	G.711 with mu-law used in North America and Japan, while G.711 with A-law used in the rest of the world.
ITU G.722	SBADPCM (Sub-Band Adaptive Differential Pulse Code Modulation)	48, 56 and 64	
ITU G.723	Multi-rate Coder	5.3 and 6.4	
ITU G.726	ADPCM (Adaptive Differential Pulse Code Modulation)	16, 24, 32, and 40	
ITU G.727	Variable-Rate ADPCM	16-40	
ITU G.728	LD-CELP (Low-Delay Code Excited Linear Prediction)	16	

ITU G.729	CS-ACELP (Conjugate Structure Algebraic-Code Excited Linear Prediction)	8
-----------	---	---

An administrator can create profiles that use pre-existing VoIP profiles to configure various codec data rates and frame rates to improve voice quality in VoIP transmissions.

To create a VoIP profile:

NOTE: Ensure [Voice over IP](#) is not disabled in the Administrator Settings. It is enabled by default.

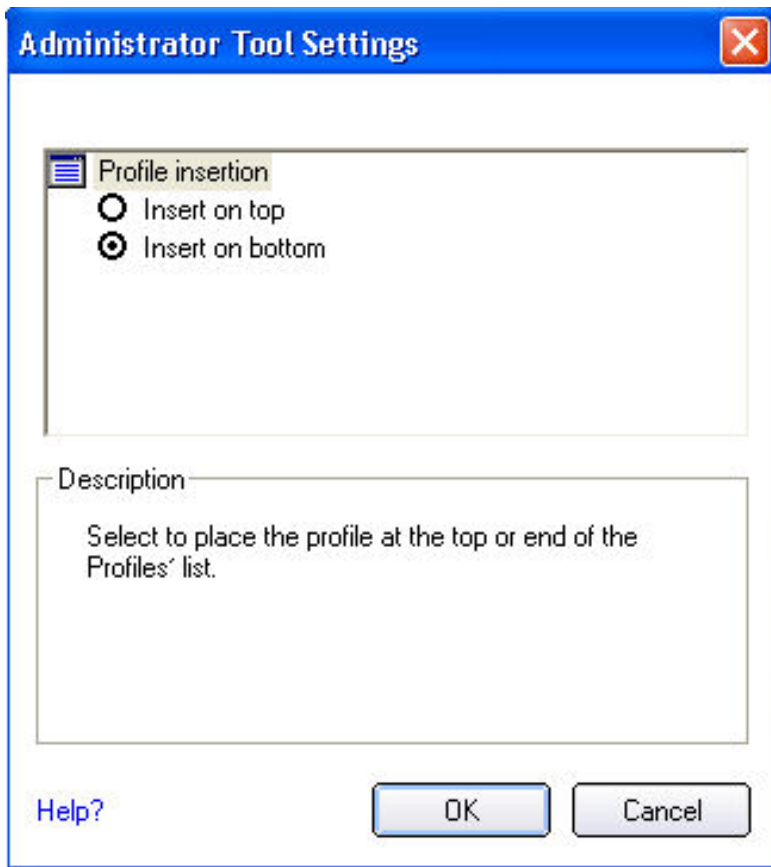
1. Click **Include Profiles**.
2. Select a profile from the list.
3. Click **Properties** to open the **Create VoIP Profiles** page.
4. Select the Codec bandwidth, application usage and Frame Rate.

Codec	Usage	Frame Rate
• G711_64 • G711_56 • G711_48 • G722_64 • G722_56 • G722_48 • G722_1_32 • G722_1_24 • G722_1_16 • G726_16 • G726_24, • G726_32 • G726_40 • G728_12_8 • G728_16 • G729_8 • G729a_8 • G729b_8 • G729ab_8 • G729d_6_4 • G729e_8 • G729e_11_8 • GIPS_iPCM_VARIABLE	• Interactive Voice • Audio Conference • Voice Data • Video • Streaming Audio	• 10 • 20 • 30

- | | | |
|--|--|--|
| <ul style="list-style-type: none">• G722_2_VARIABLE• SPEEX_VARIABLE | | |
|--|--|--|

5. Click **OK** to return to the Profiles list.
 6. Click **Close** to save the profile settings to a [package](#).
-

Administrator Tool Settings



An Administrator can determine where Administrator profiles are placed in a user's Profiles list.

1. Click the Administrator Tool **Tools** menu.
 2. Click **Settings** to open the **Administrator Tool Settings**
 3. Select **Insert on Top** to always place Administrator profiles at the top of a user's Profiles list.
 - Select **Insert on Bottom** to always place Administrator profiles at the bottom of a user's Profiles list.
 4. Click **OK** to close and return to the Administrator Tool.
-

Administrator Settings

An administrator can select which level of control that users have over their wireless network connections.

To configure Administrator Settings:

1. Click **Include settings**.
2. Enable or disable each setting listed in the table below.

Name	Description
802.11a Radio On/Off	Select Add 802.11a Radio On/Off Selection to allow a user to turn on or off the 802.11a radio on their computer. This adds the 802.11a Radio Off control to the Taskbar menu and the Intel PROSet/Wireless main window on a user's computer. NOTE: This option is available only for wireless adapters that support 802.11a, 802.11b and 802.11g. This setting is unavailable if the adapter is an Intel(R) PRO/Wireless 2200BG Network Connection.
802.1x Authentication	Enable a user to create or connect to profiles that support different 802.1x authentication EAP types. Select which 802.1x authentication EAP types you want enabled on a user's computer: MD5, EAP-SIM, LEAP, TLS, TTLS, PEAP, EAP-FAST.
Administrator Tool	Disable access to the Administrator Tool on a user's computer.
Application Auto Launch	Select to start a batch file, executable file, or script automatically when a specific profile connects to the network. For example, start a Virtual Private Network (VPN) session automatically whenever a user connects to a wireless network.
Application On Radio Toggle	Enables a third-party application to disable the Intel PROSet/Wireless Wireless On or Wireless Off switch.

Cache Credentials	Select to save credentials after a user logs on. If the wireless connection temporarily disconnects, the saved credentials are used upon reconnection. The credentials are cleared when the user logs off. NOTE: if cleared, The Prompt each time I connect option is unavailable when creating profiles
Cisco Compatible Extensions	Select to enable Cisco Compatible Extensions on a user's computer. Clear to disable.
Device to Device (ad hoc)	Enable or disable whether a user is able to either create ad hoc profiles or join ad hoc networks. Select one of the following to enable or disable whether the user can connect to device to device networks: • Enable device to device networking. • Enable secure device to device networking only. • Disable device to device networking. Select to either allow a user to configure profiles with device to device (ad hoc) settings or prevent configuration of device to device (ad hoc) profiles. • Show device to device application settings • Hide device to device application settings. To remove the Device to device (Ad hoc) operating mode from the Profile Wizard General Settings, select both Disable device to device networking and Hide device to device application settings. This prevents a user from creating profiles that support Device to device (Ad hoc) network.

Import and Export	Select to import to or export profiles from a user's computer. Enable permits auto import of user profiles when copied to an auto import folder.
Message On Radio Toggle	Enables a third-party application to notify a user that the Intel PROSet/Wireless radio is either on or off.
Pre-Logon Cisco Mode	Enable Cisco Mode during a pre-logon connection. Cisco access points have the capability to support multiple wireless network names (SSIDs) but only broadcast one. In order to connect to such an access point, an attempt is made to connect with each profile. This is referred to as Cisco Mode. NOTE: The pre-logon connection may take longer to connect.
Profile Connectivity	Select the profile connectivity level on a user's computer? Disable Intel Profile Switching. Users are only able to connect with the first Pre-Logon (Common) profile or connect with Pre-Logon profiles only. • Allow the user to connect to all administrator profiles. • Allow the user to only connect to the first administrator profile.
Security Level	Select the security level on a user's computer? Users are able to connect to profiles only with this security level. • Allow the user to connect to networks with Personal Security only. • Allow the user to connect to networks with Enterprise Security.

Single Sign On	Select which Administrator Profile types are enabled on a user computer? • Persistent Connection: Profiles are active during start up and when no user is logged onto the computer. • Pre-Logon Connection: Profiles are active immediately once a user logs onto the computer. Common profiles are enabled if Pre-Logon features are not installed on a user's computer. Common profiles are active after a user has logged on and the session becomes active. Persistent and Pre-Logon or Common profiles are placed at the top of the user's profiles list. They cannot be changed or deleted by a user.
Voice over IP	Enables a third-party software to use the VoIP application on a user's computer. The default setting enables this feature.
Wireless Zero Configuration	Select if you only want Intel PROSet/Wireless to manage a user's wireless connections. Disables Microsoft Windows XP Wireless Zero Configuration.
Close	Closes the Administrator Tool.
Help?	Provides help information for this page.

Adapter Settings

To configure Adapter Settings:

1. Click **Include settings**.
2. For each setting listed in the table below, select one of the following options:
 - **Use default value:** Resets the setting on the user machine to the default value.
 - **No change:** Maintains the user selected value. The administrator

decides not to enforce all the settings on a user's computer. The user can change the adapter setting values from the Intel PROSet/Wireless Advanced menu.

- **Select the value:** The administrator selects the value that is to be used on the user's computer.

Name	Description
Ad Hoc Channel	There is no need to change the channel unless the other computers in the ad hoc network use a different channel from the default channel. Value: Select the allowed operating channel from the list. ● 802.11b/g: Select this option when 802.11b and 802.11g (2.4 GHz) ad hoc band frequency is used. ● 802.11a: Select this option when 802.11a (5 GHz) ad hoc band frequency is used.
Ad Hoc Power Management	Set power saving features for Device to Device (ad hoc) networks. ● Disable: Select when connecting to ad hoc networks that contain stations that do not support ad hoc power management ● Maximum Power Savings: Select to optimize battery life. ● Noisy Environment: Select to optimize performance or connecting with multiple clients. NOTE: This setting is unavailable if the adapter is an Intel PRO/Wireless 2915ABG Network Connection or an Intel PRO/Wireless 2200BG Network Connection.

Ad Hoc QoS Mode	Quality of Service (QoS) control in ad hoc networks. QoS provides prioritization of traffic from the access point over a wireless LAN based on traffic classification. WMM (Wifi MultiMedia) is the QoS certification of the Wi-Fi Alliance (WFA). When WMM is enabled, the adapter uses WMM to support priority tagging and queuing capabilities for Wi-Fi networks. • WMM Enabled.(Default) • WMM Disabled
Mixed Mode Protection	Use to avoid data collisions in a mixed 802.11b and 802.11g environment. Request to Send/Clear to Send (RTS/CTS) should be used in an environment where clients may not hear each other. CTS-to-self can be used to gain more throughput in an environment where clients are in close proximity and can hear each other.
Power Management	Power Management: Allows you to select a balance between power consumption and adapter performance. The wireless adapter power settings slider sets a balance between the computer's power source and the battery. • Use default value: (Default) - Power settings are based on the computer's power source. • Manual: Adjust the slider for the desired setting. Use the lowest setting for maximum battery life. Use the highest setting for maximum performance. NOTE: Power consumption savings vary based on infrastructure settings.
Preamble Mode	Change the preamble length setting received by the access point during an initial connection. Always use a long preamble length to connect to an access point. Auto Transmit (Tx) Preamble allows automatic preamble detection. If supported, short preamble should be used. If not, use long preamble.

Roaming Aggressiveness	This setting allows you to define how aggressively your wireless client roams to improve connection to an access point. • Default: Balanced setting between not roaming and performance. • Lowest: Your wireless client will not roam. Only significant link quality degradation causes it to roam to another access point. NOTE: This setting is unavailable if the adapter is an Intel(R) PRO/Wireless 2915ABG Network Connection or an Intel(R) PRO/Wireless 2200BG Network Connection.
Throughput Enhancement	Change the value of the Packet Burst Control. • Enable: Select to enable throughput enhancement. • Disable: (Default) - Select to disable throughput enhancement.
Transmit Power	Default Setting: Highest power setting Lowest Minimum Coverage: Set the adapter to a lowest transmit power. Enable you to expand the number of coverage areas or confine a coverage area. Reduce the coverage area in high traffic areas to improve overall transmission quality and avoid congestion and interference with other devices. Highest Maximum Coverage: Set the adapter to a maximum transmit power level. Select for maximum performance and range in environments with limited additional radio devices. NOTE: The optimal setting is for a user to always set the transmit power at the lowest possible level still compatible with the quality of their communication. This allows the maximum number of wireless devices to operate in dense areas and reduce interference with other

	devices that this radio shares radio spectrum with. NOTE: This setting takes effect when either Infrastructure or Ad hoc mode is used.
Wireless Mode	Select which band to use for connection to a wireless network: • 802.11a only: Connect the wireless adapter to 802.11a networks only. • 802.11b only: Connect the wireless adapter to 802.11b networks only. • 802.11g only: Connect the wireless adapter to 802.11g networks only. • 802.11a and 802.11g only: Connect the wireless adapter to 802.11a and 802.11g networks only. • 802.11b and 802.11g only: Connect the wireless adapter to 802.11b and 802.11g networks only. • 802.11a, 802.11b, and 802.11g: (Default) - Connect to either 802.11a, 802.11b or 802.11g wireless networks. NOTE: These wireless modes (modulation types) determine the discovered access points displayed in the Wireless Networks list.
OK	Saves settings and return to the previous page.
Cancel	Closes the page and cancels any changes.
Help?	Provides help information for this page.

Software

Select which of the Intel PROSet/Wireless applications are installed on a user's computers.

1. Select **Include Software**.
2. Place the Intel PROSet/Wireless installation CD in the CD drive.
3. **Specify the Intel PROSet/Wireless Software Installation program:**
Click **Browse** to locate the Autorun.exe file.
4. Click **OK**.
5. **Specify which components you want to export:** Select which

applications to install on a user's computer.

- [Intel Wireless Troubleshooter](#): Helps you resolve wireless connection issues
 - **Administrator Tool**: Installs the Administrator Tool to the Tools menu.
 - **Intel Smart Wireless Solutions**: Provides an easy configuration wizard for connection to a wireless router.
 - **Single Sign On**: Installs the Single Sign On features. This tool is used to configure common (shared) profiles.
 - **Wireless Management Instrumentation**: Allows administrators who do not have Intel PROSet/Wireless installed to remotely manage clients that do have Intel PROSet/Wireless installed.
-

Administrator Tasks

How to Obtain a Client Certificate

If you do not have any certificates for EAP-TLS (TLS) or EAP-TTLS (TTLS) you must obtain a client certificate to allow authentication.

Certificates are managed from either Internet Explorer or the Microsoft Windows Control Panel.

Microsoft Windows XP and Microsoft Windows 2000: When a client certificate is obtained, do not enable strong private key protection. If you enable strong private key protection for a certificate, you need to enter an access password for the certificate every time this certificate is used. You must disable strong private key protection for the certificate if you configure the service for TLS or TTLS authentication. Otherwise, the 802.1x service fails authentication because there is no logged in user to provide the required password.

Notes about Smart Cards

After a Smart Card is installed, the certificate is automatically installed on your computer and is chosen from the personal certificate store and root certificate store.

Set up the Client for TLS authentication

Step 1: Obtain a certificate

To allow TLS authentication, you need a valid client certificate in the local

repository for the logged-in user's account. You also need a trusted CA certificate in the root store.

The following information provides two methods for obtaining a certificate:

- From a corporate certification authority (CA) implemented on a Windows 2000 server.
- Import a certificate from a file with Internet Explorer's certificate import wizard.

If you do not know how to obtain a user certificate from the CA, consult your administrator for the procedure.

To install the CA on the local machine:

1. Obtain the CA and store it on your local drive.
2. Click **Import**. The Certificate Import Wizard opens.
3. Click **Next**.
4. Click **Browse** to locate the certificate on your local drive.
5. Click the exported certificate.
6. Click **Open**.
7. Click **Next**.
8. Click **Place all certificates in the following store**.
9. Click **Browse** to open the **Select Certificate Store**.
10. Click **Show physical stores**.
11. Click **OK**.
12. From the list of stores, scroll up and expand **Trusted Root Certificate Authorities**.
13. Click **Local Computer**.
14. Click **OK**.
15. Click **Next**.
16. Click **Finish** to complete the process.
17. Reboot after a certificate is installed.

Use Microsoft Management Console (MMC) to verify that the CA is installed in the machine store.

1. In the Start menu, click **Run**.
2. Enter **MMC**.
3. Click **OK** to open The Microsoft Management Console.
4. Click **File**.
5. Click **Add/Remove Snap-in**.
6. Click **Add** to open the Add Standalone Snap-in page.
7. Click **Certificates**.
8. Click **Add**.

9. Click **Computer account**.
10. Click **Next**.
11. Click **Finish**.
12. Click **Close**.
13. Click **OK**.
14. In the console, click **Certificates (Local Computer)**.
15. Click **Trusted Root Certificate Authorities**.
16. Click **Certificates**.
17. Verify that the CA you just installed is listed.
18. Click **File**.
19. Click **Exit** to close the console.

Obtain a certificate from a Microsoft Windows 2000 CA:

1. Start Internet Explorer and browse to the Certificate Authority HTTP Service (use an URL such as `http://yourdomainserver.yourdomain/certsrv` with `certsrv` being the command that brings you to the certificate authority. You can also use the IP address of the server machine. For example, "192.0.2.12/certsrv."
2. Logon to the CA with the name and password of the user account you created on the authentication server. The name and password do not have to be the same as the Windows log on name and password of the current user.
3. On the Welcome page of the CA, select **Request a certificate task and submit the form**.
4. **Choose Request Type:** Select **Advanced request**.
5. Click **Next**.
6. **Advanced Certificate Requests:** Select **Submit a certificate request to this CA using a form**.
7. Click **Submit**.
8. **Advanced Certificate Request:** Select **User certificate template**.
9. Click **Mark keys as exportable**.
10. Click **Next**. Use the provided defaults.
11. **Certificate Issued:** Click **Install this certificate**.

NOTE: If this is the first certificate you have obtained, the CA first asks you if it should install a trusted CA certificate in the root store. This is not a trusted CA certificate. The name on the certificate is that of the host of the CA. Click **Yes**. You need this certificate for both TLS and TTLS.

12. If your certificate was successfully installed, you see the message, "Your new certificate has been successfully installed."
13. To verify the installation, click **Internet Explorer > Tools > Internet Options > Content > Certificates**. The new certificate should be

installed in the Personal folder.

Import a Certificate from a File

1. Open Internet Properties (right-click on the Internet Explorer icon on the desktop).
2. Select **Properties**.
3. **Content:** Click **Certificates**. The list of installed certificates appears.
4. Click **Import** to open the Certificate Import Wizard.
5. Select the file.
6. Specify your access password for the file. Clear **Enable strong private key protection**.
7. **Certificate store:** Click **Automatically select certificate store based on the type of certificate** (the certificate must be in the user accounts personal store to be accessible).
8. Proceed to **Completing the Certificate Import** and click **Finish**.

To configure a profile with WPA authentication with WEP or TKIP encryption that uses TLS authentication:

NOTE: Obtain and install a client certificate, refer to Step 1 or consult your administrator.

Specify the certificate used by Intel PROSet/Wireless

1. On the General page, click **Networks**.
2. Click **Add**.
3. **Profile Name:** Enter a profile name
4. **Network Name (SSID):** Enter the network identifier.
5. **Operating Mode:** Click **Infrastructure**.
6. Click **Next** to open the Security Settings.
7. **Network Authentication:** Select **WPA-Enterprise** or **WPA2-Enterprise**.
8. **Data Encryption:** Select **AES-CCMP**
9. **802.1x Enabled:** Selected.
10. **Authentication Type:** Select **TLS**.

Step 1 of 2: TLS User

1. Obtain and install a client certificate.
2. Select one of the following to obtain a certificate:
 - **Use my smart card:** Select if the certificate resides on a smart card.
 - **Use the certificate issued to this computer:** Click **Select** to

choose a certificate that resides in the machine store.

- **Use a user certificate on this computer.** Click **Select** to choose a certificate that resides on this computer.

3. Click **Next**.

Step 2 of 2: TLS Server

Select one of the following:

1. **Validate Server Certificate:**

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

2. **Specify Server or Certificate Name:** Select if you want to specify your server or certificate name.

The server name or domain to which the server belongs, is 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 (for example, Servername.Domain name).
- **Domain name must end in specified name:** When selected, the server name identifies a domain and the certificate must have a server name belonging to this domain or to one of its sub-domains (for example, zeelans.com, where the server is blueberry.zeelans.com).

NOTE: These parameters should be obtained from the administrator.

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

[Back to Top](#)

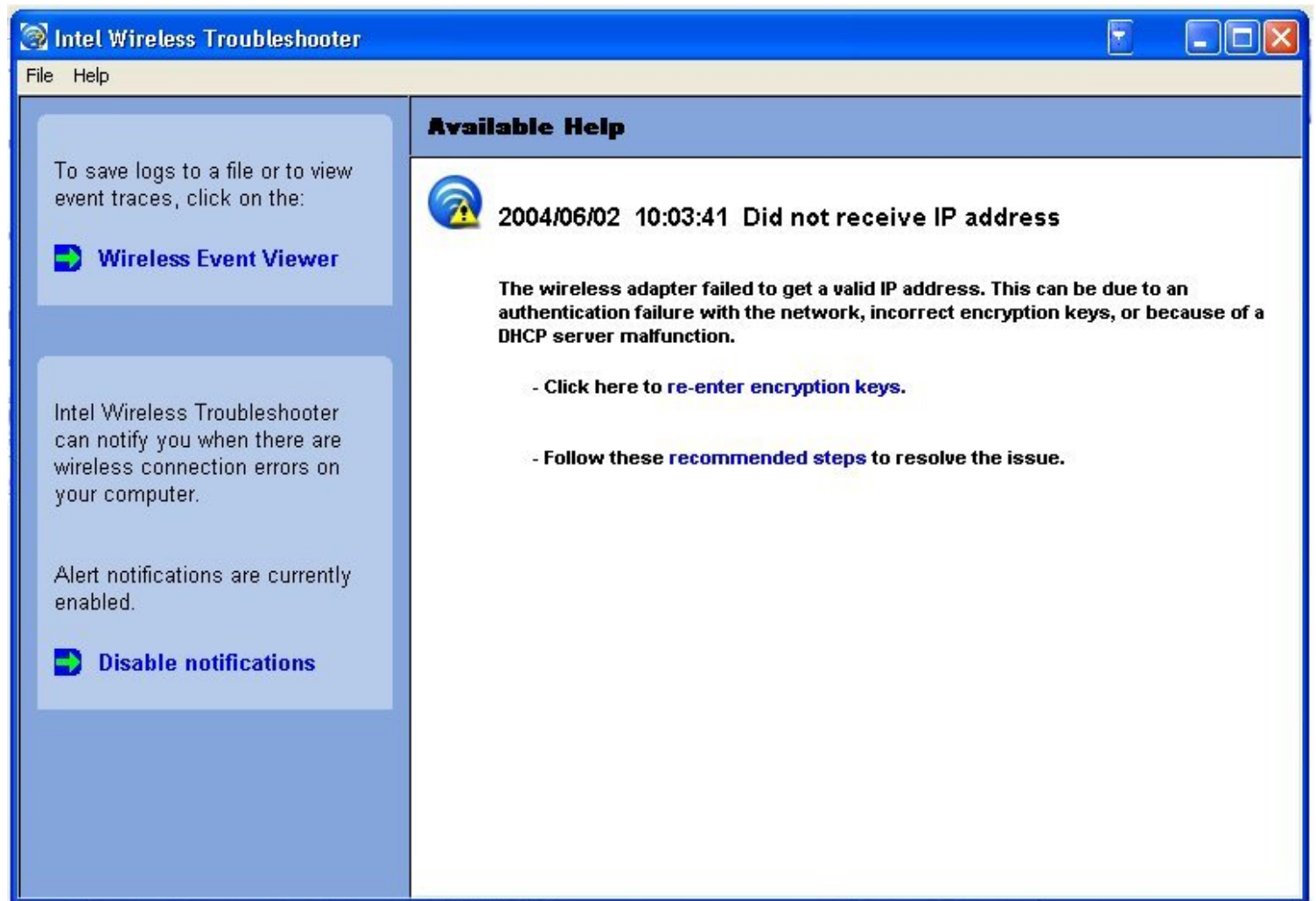
[Back to Contents](#)

[Trademarks and Disclaimers](#)

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

- [Intel\(R\) Wireless Troubleshooter](#)
 - [Wireless Event Viewer](#)
 - [Resolve Errors](#)
-

Intel Wireless Troubleshooter



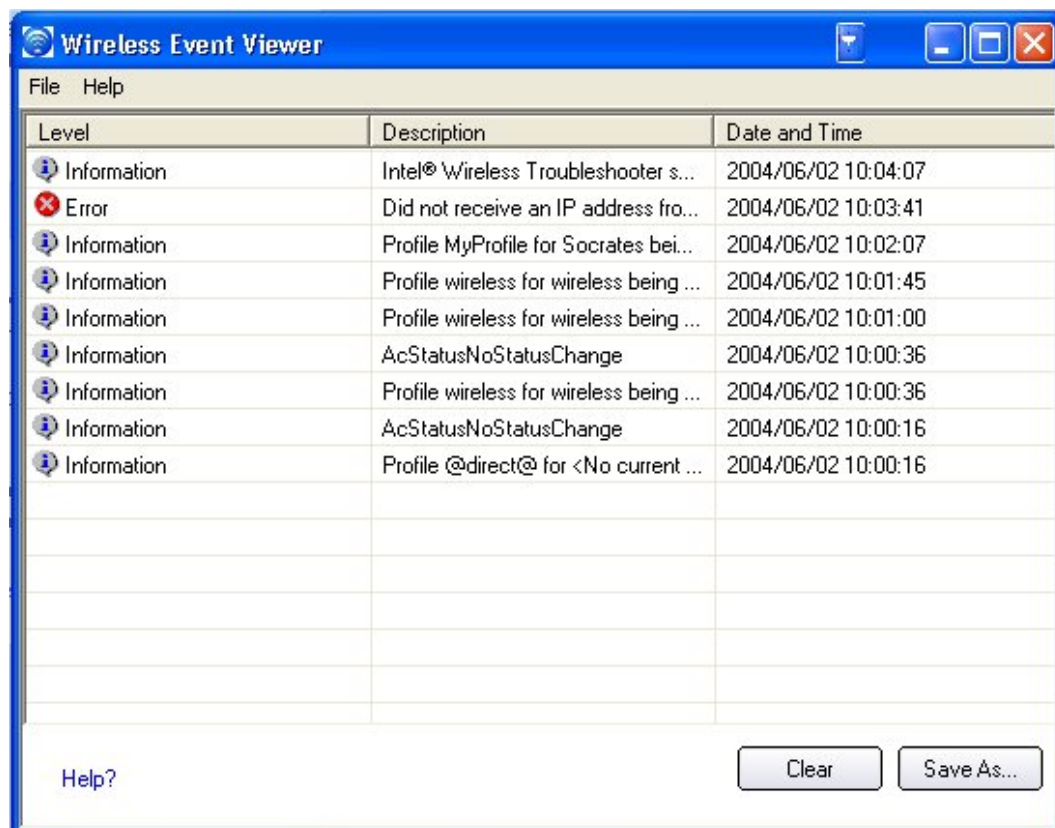
The Intel Wireless Troubleshooter is an application that can help you resolve wireless network connection issues. When a connection issue is detected, a desktop alert appears at the bottom right corner of your desktop screen. Once you click on the desktop alert, a diagnostic message displays the steps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

Intel Wireless Troubleshooter Description

The Intel Wireless Troubleshooter contains two panes. The left pane displays a list of available tools. The right pane displays the current connection issue. This pane is divided into two sections: the error message and the recommended action. The recommended action contains descriptions about available utilities and helps to resolve the associated connection issue. If you click on a help link, the help text is displayed in a window. If you click on the associated issue resolution link, a program is launched to resolve the connection issue.

Name	Description
File	Exit: Click to exit the Intel Wireless Troubleshooter application.
Help	Intel(R) Wireless Troubleshooter Help: Displays online help on the Intel Wireless Troubleshooter. About: Displays version information for the Intel Wireless Troubleshooter.
Wireless Event Viewer	Launch Wireless Event Viewer .
Disable Notification	Select to disable the alert notifications.
Enable Notification	Select to enable the alert notifications.
Available Help	Date Time error message • Description of error • Link to resolve error (if available). • 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 to a binary format file for sending to customer support. To launch Wireless Event Viewer, from the Tools menu, click [Intel Wireless Troubleshooter](#). Click **Wireless Event Viewer**.

Wireless Event Viewer

Name	Description
File	Settings: Wireless Event Viewer Settings: Select to change the storage location of the log file. • Specify the default folder for saved log files: The current folder is displayed. The default location is the desktop. Browse: Specify a new folder location. OK: Close and apply the new changes. Cancel: Close without applying any changes. Exit: Close the Intel Wireless Troubleshooter application.
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 detected connection issue. This column can be sorted in ascending or descending order. Click the column header to sort the displayed events.
Save As	Saves the available log. Use the suggested name or change it.
Clear	Removes the information in the Wireless Event Viewer.
Help?	Provides help information for this page. About: Displays version information for the Intel Wireless Troubleshooter.

Resolve 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 user name](#)

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

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

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

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

[Incorrect PIN for retrieving certificate](#)

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

[The wireless adapter failed to get a valid IP address](#)
[Authentication failed because timer expired](#)
[Smart Card was unexpectedly removed](#)
[Disconnection from an Access Point](#)
[GSM adapter was unexpectedly removed](#)
[The AAA Server Rejected the EAP Method](#)

Authentication failed due to invalid user credentials: Reenter credentials

This authentication error can be caused by invalid user credentials (could be user name, password or other form of user credentials).

Use the following steps to resolve this error:

1. Select a TTLS, PEAP, LEAP or EAP-FAST profile from the Profiles list.
 2. Click **Properties** to open the General Settings.
 3. Click **Next** to open the Security Settings. **Enterprise Security** is selected.
 4. The 802.1x Authentication Type should be selected.
 5. Select **Use the following** for User Credentials.
 6. Verify the User Name, Domain, and password information.
 - If **Use Windows logon** or **Prompt each time I connect** is selected, verify that you use the correct user credentials information when you connect to the wireless network.
 7. Click **OK** to save the settings.
-

Authentication failed due to invalid user name: Reenter user name

This authentication error can be caused by an invalid user name.

Use the following steps to resolve this error:

1. Select the appropriate profile from the Profiles list.
 2. Click **Properties** to open the General Settings.
 3. Click **Next** to open the Security Settings. **Enterprise Security** is selected.
 4. Select the appropriate 802.1x Authentication Type.
 - For TTLS, PEAP, LEAP or EAP-FAST profiles: **Use the following** option should be selected.
 - Verify the User Name information.
 5. Click **OK** 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.

Use the following steps to resolve this error:

1. Select the appropriate profile from the Profiles list.
2. Click **Properties** to open the General Settings.
3. Click **Next** to open the Security Settings. **Enterprise Security** is selected.
4. The appropriate 802.1x Authentication Type is selected.
 - For TTLS and PEAP profiles: Verify that the correct Authentication Type is selected from the list, then click the **Select** button and select another certificate from the list of installed certificates and click **OK**.
 - For TLS profiles: Click **Select** and choose another certificate from the list of installed certificates and click **OK**.

Notes about certificates: The specified identity should match who the certificate is issued to and should be registered on the authentication server (for example, RADIUS server) that is used by the authenticator. Your certificate must be valid with respect to the authentication server. This requirement depends on the authentication server and generally means that the authentication server must know the issuer of your certificate as a Certificate Authority. You should be logged in with the same user name you used when the certificate was installed.

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

Authentication failed due to invalid server credentials: Reenter server credentials

This authentication error can be caused by an invalid server (domain) credential.

Use the following steps to resolve this error:

1. Select the appropriate profile from the Profiles list.
2. Click **Properties** to open the General Settings.
3. Click **Next** to open the Security Settings. **Enterprise Security** is selected.
4. Select the appropriate 802.1x Authentication Type.
 - For TTLS and PEAP profiles: Select **Use the following** for user credentials.
 - Verify the domain information.
 - If **Use Windows logon** or **Prompt each time I connect** is selected, verify that the correct domain credentials information is used when you connect to the wireless network.
5. Click **OK** to save the settings.

Authentication failed due to invalid server identity: Reenter server name

This authentication error can be caused by invalid server identity information.

Use the following steps to resolve this error:

1. Select the appropriate profile from the Profiles list.
2. Click **Properties** to open the General Settings.

3. Click **Next** to open the Security Settings. **Enterprise Security** is selected.
 4. Select the appropriate 802.1x Authentication Type.
 5. For TTLS and PEAP profiles: Verify that the Roaming Identity server name is correct.
 6. Click **OK** to save the settings.
-

Authentication failed due to an invalid user certificate: Reenter user credentials

This authentication error can be caused by invalid server (domain) credentials.

Use the following steps to resolve this error:

1. Select the appropriate profile from the Profiles list.
2. Click **Properties** to open the General Settings.
3. Click **Next** to open the Security Settings. **Enterprise Security** is selected.
4. Select the appropriate 802.1x Authentication Type.
5. For TTLS and PEAP profiles: Verify that the correct Authentication Type is selected.
6. Click **Select** and choose another certificate from the list of installed certificates.
7. Click **OK**.
8. For TLS profiles: Click **Select** and choose another certificate from the list of installed certificates.
9. Click **OK**.

Notes about Certificates: The specified identity should match who the certificate is issued to and should be registered on the authentication server (for example, RADIUS server) that is used by the authenticator. Your certificate must be valid with respect to the authentication server. This requirement depends on the authentication server and generally means that the authentication server must know the issuer of your certificate as a Certificate Authority. You should be logged in with the same user name you used when the certificate was installed.

9. Click **Close**.
 10. Click **OK** to save the settings.
-

Incorrect PIN for retrieving certificate: Reenter PIN

The certificate retrieval failed because of an incorrect PIN.

Recommended action: 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.

Use the following steps to resolve this error:

1. Select the profile
 2. Click **Connect** and attempt to associate with the network and authenticate with the server.
-

The wireless adapter failed to get a valid IP address

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

Use the following steps to resolve this error:

1. Select the appropriate profile from the Profiles list.
 2. Click **Properties** to open the General Settings.
 3. Click **Next** to open the Security Settings. **Enterprise Security** is selected.
 4. Enter the encryption key.
 5. Click **OK** to save the security settings for the profile.
-

Authentication failed because timer expired

Authentication failed because the authentication timer expired while this mobile station was authenticating. A rogue access point or a problem with the RADIUS server could have been the reason for the problem.

Recommended action:

- If a rogue access point is suspected, consider adding this access point to the [excluded access point list](#) to prevent the wireless adapter from connecting to this access point in the future.
 - If a rogue access point is not suspected, click the profile in the profile list. Click **Connect** to associate with the network and attempt to authenticate with the server.
-

Smart Card was unexpectedly removed

This error occurred because the Smart Card was unexpectedly removed.

Use the following a steps to resolve this error:

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

Disconnection from an Access Point

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

Disconnect from access point due to failed associations.

Disconnect from access point due to authentication failures.
Disconnect from access point due to TKIP Michael Integrity check failure.
Disconnect from access point due to Class 2 frame non-authentication failure.
Disconnect from access point due to Class 3 frame non-association failure.
Disconnect from access point due to reassociation failure.
Disconnect from access point due to Information Element failure.
Disconnect from access point due to EAPOL-Key protocol four-way handshake failure.
Disconnect from access point due to 802.1x authentication failure.

Recommended action: Select the profile. Click **Connect** and try to associate with the network.

GSM adapter was unexpectedly removed

See [Smart Card was unexpectedly removed](#)

The AAA Server Rejected the EAP Method

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

Use the following steps to resolve this error:

1. Double-click the Taskbar icon to open Intel PROSet/Wireless.
 2. Click **Profiles** on the Intel PROSet/Wireless main window.
 3. Select the associated or last-used profile from the Profiles list.
 4. Click **Properties** to open the General Settings.
 5. Click **Next** to open the Security Settings.
 6. Verify that **Enable 802.1x** is selected.
 7. Verify that the correct authentication type is selected.
 8. Enter the required security information.
 9. Click **OK**. The profile is now reapplied. Intel PROSet/Wireless attempts to connect to the wireless network.
-

[Back to Top](#)

[Back to Contents](#)

[Trademarks and Disclaimers](#)

Connect to a Network: Intel(R) PRO/Wireless 3945ABG Network Connection User Guide

- [Connect to a wireless network](#)
 - [First Time Connection](#)
 - [Other Wireless Managers](#)
-

Connect to a wireless network

You can connect to a wireless network with one of the following methods.

- **Automatic Connection:** If an existing profile matches an available network, you are automatically connected to that wireless network.
 - **Configure a new profile:** Select a wireless network from the list of wireless networks in the Intel PROSet/Wireless main window. Click **Connect**. If you successfully connect, a profile is created in the Profiles list for future use.
 - **Connect to a profile in the Profiles list:** You can select a profile from the Profiles list. To activate it, click **Profiles** on the Intel(R) PROSet/Wireless main window. Select the profile in the Profiles list. Click **Connect**. This allows you to connect to a network that is lower in the list (if it is available).
 - Right-click the [Taskbar icon](#) located in the lower right corner of your Windows Desktop. Right click **Connect to Profiles**. A list of previously configured profiles is listed. Select a profile.
-

First Time Connection

Intel PROSet/Wireless automatically detects wireless networks that are

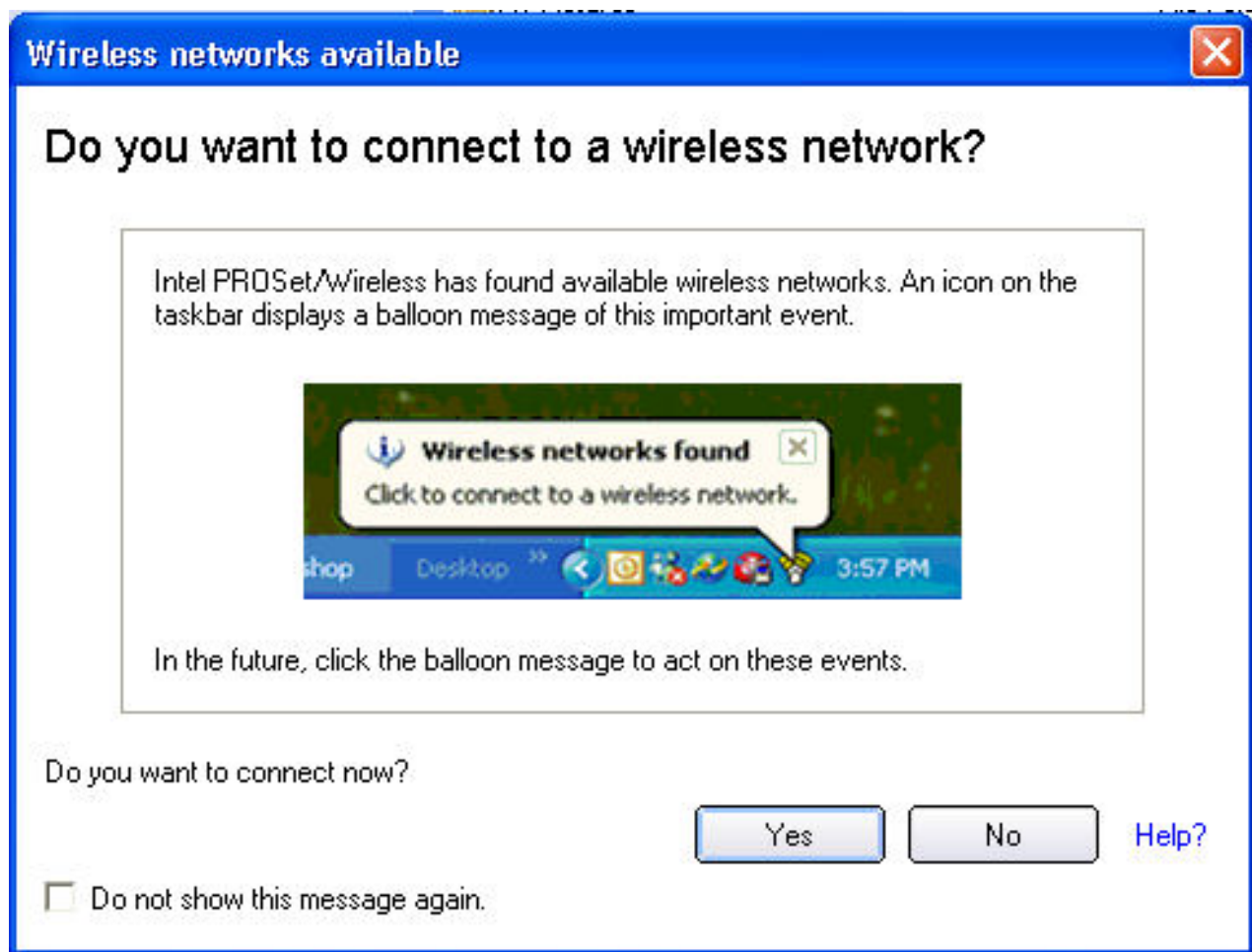
within range of your wireless adapter. When a network is found, a desktop alert notification displays: **Wireless networks found**. See [Taskbar Icons](#) for more information.

1. Double-click the desktop alert to open the Intel PROSet/Wireless main window.
2. Select a network from the wireless networks list.
3. Click **Connect**. If the network does not require security authentication, a desktop alert notifies you that you are connected to the network. Refer to [Intel PROSet/Wireless Main Window](#) and [Taskbar](#) for more information about the taskbar menu and icons.

If you need to add security authentication:

1. The Profile Wizard opens and guides you through the configuration process.
2. Specify a Profile Name. The Profile Name is your name for this network. It can be anything that helps you identify this network. For example, My Home Network, Coffee Shop on A Street.
3. Click **Next**. The Profile Wizard then attempts to detect the network settings of this network.
4. Continue through the Profile Wizard until completion. Refer to [Profile Management](#) and [Security Settings](#) for more information.
5. Click **OK** to connect to the wireless network.

If you ignore the **Wireless networks found** desktop alert, Intel PROSet/Wireless displays a message that prompts: **Do you want to connect to a wireless network?** Click **Yes**. The Intel PROSet/Wireless main window opens. Follow the instructions above to connect to a wireless network.



In addition to the Taskbar icon, Intel PROSet/Wireless also displays connection status and available networks. Refer to [Intel PROSet/Wireless Main Window](#) for more information.

Other Wireless Managers

If the Intel PROSet/Wireless detects another software application trying to communicate with the wireless device, you are notified of this behavior.

Microsoft Windows XP Wireless Zero Configuration

To switch from Intel PROSet/Wireless to the Microsoft Windows XP Wireless Zero Configuration, use either of the following methods:

- **From the Taskbar Menu:**

Click **Use Windows to manage Wi-Fi** to switch to Microsoft Windows XP Wireless Zero Configuration. Select this option to disable Intel PROSet/Wireless as your current wireless manager. You can then configure Microsoft Windows XP as your wireless manager.



NOTE: Any wireless profiles created in Intel PROSet/Wireless are not visible in Microsoft Windows XP Wireless Zero Configuration. If you want to use your Intel wireless profiles you need to select **Use Intel PROSet/Wireless** from the Taskbar menu.

- From Intel PROSet/Wireless:

From, the Tools menu, click **Use Windows to manage Wi-Fi** in the Intel PROSet/Wireless application. When you are finished using the Microsoft Windows XP Wireless Zero Configuration, you can switch back to Intel PROSet/Wireless. Click **Enable Intel PROSet/Wireless** on the Intel PROSet/Wireless main window.

To enable Intel PROSet/Wireless as your wireless manager, click **Use Intel PROSet/Wireless** from the Taskbar menu.



Third Party Wireless Software

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

[Back to Top](#)

[Back to Contents](#)

[Trademarks and Disclaimers](#)

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

About Wireless Network Technology

- [Select a Wireless Network](#)
- [Configure a Wireless Network](#)
- [Identify a Wireless Network](#)

A wireless network connects computers without network cables. Instead 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(R) PRO/Wireless Network Connections adapter to connect to other similar wireless devices that comply with the 802.11 standard for wireless networking.

Select 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 Device-to-Device mode to network computers in a home or small office or to set up a temporary wireless network for a meeting.



Configure 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 802.11 wireless networks use encryption to help protect your data. Wired equivalent privacy (WEP) uses a 64- or 128-bit shared encryption key to scramble data. Before a computer transmits data, it uses a secret encryption key to scramble the data. 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.

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

Identify 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 Top](#)

[Back to Contents](#)

[Trademarks and Disclaimers](#)

Specifications: Intel PRO / Wireless 3945ABG Network Connection User Guide

- [Intel PRO/Wireless 3945ABG Network Connection](#)
 - [Intel PRO/Wireless 2915ABG Network Connection](#)
 - [Intel PRO/Wireless 2200BG Network Connection](#)
-

Intel PRO / Wireless 3945ABG Network Connection

Form Factor	PCI Express (TM) Mini Card	
Dimensions	Width 1.175 in x Length 2.039 in x Height 0.148 in (29.85 mm x 51.80 mm x 3.76 mm)	
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	53-pin Mini Card edge connector	
Voltage	3.3 V	
Operating Temperature	0 to +80 degrees Celsius	
Humidity	50 to 92% non-condensing (at temperatures of 25 °C to 55 °C)	
Frequency Modulation	5 GHz (802.11a)	2.4 GHz (802.11b / g)

Frequency band	5.25 - 5.35GHz 5.725 - 5.850GHz	2.400 - 2.4835 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	5280, 5300, 5320, 5745, 5765, 5785, 5805, 5825 MHz. (Taiwan DGT)	Channel 1-11 (US, DGT) 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	Microsoft Windows XP, Microsoft Windows 2000	
Wi-Fi(R) Alliance certification	Wi-Fi(R) certification for 802.11b, 802.11g, 802.11a, WPA, WPA2, WMM, EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, MD5	
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v4.0	
WLAN Standard	IEEE 802.11g, 802.11b, 802.11a	
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes	
Security	WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, AES-CCMP 128-bit, WEP 128-bit and 64-bit; 802.1x: EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, MD5	
Product Safety	UL, C-UL, CB (IEC 60590)	

Intel PRO / 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	Microsoft Windows XP, Microsoft Windows 2000	
Wi-Fi(R) Alliance certification	Wi-Fi(R) certification for 802.11b, 802.11g, 802.11a, WPA, WPA2, WMM, EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, MD5	
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v3.0	
WLAN Standard	IEEE 802.11g, 802.11b, 802.11a	
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes	
Security	WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, AES-CCMP 128-bit, WEP 128-bit and 64-bit. 802.1x: EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, MD5	
Product Safety	UL, C-UL, CB (IEC 60590)	

Intel PRO / Wireless 2200BG Network Connection

Form Factor	Mini PCI Type 3B

Dimensions	Width 2.34 in x Length 1.75 in x Height 0.20 in (59.45 mm x 44.45 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 mini PCI edge connector
Voltage	3.3 V
Operating Temperature	0 to +70 degrees Celsius
Humidity	50 to 85% non-condensing
Frequency Modulation	OFDM with BPSK, QPSK, 16QAM, 64QAM, DBPSK, DQPSK, CCK
Frequency band	2.400 - 2.472 GHz (US) 2.400 - 2.4835 GHz (Japan) 2.400 - 2.4835 GHz (Europe ETSI)
Modulation	OFDM with BPSK, QPSK, 16QAM, 64QAM, DBPSK, DQPSK, CCK
Channels	Full 14 channel support
Data Rates	1, 2, 5.5, 6, 9, 11, 12, 24, 36, 48 and 54 Mbps
General	
Operating Systems	Microsoft Windows XP, Microsoft Windows 2000

Wi-Fi(R) Alliance certification	Wi-Fi(R) certification for 802.11b, 802.11g, 802.11a, WPA, WPA2, WMM, EAP-SIM, LEAP, PEAP, TKIP, EAP-FAST, EAP-TLS, EAP-TTLS, MD5
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v2.0
WLAN Standard	IEEE 802.11g and 802.11b
Architecture	Infrastructure or ad hoc (peer-to-peer) operating modes
Security	WPA, LEAP, PEAP, TKIP, EAP-TLS, EAP-TTLS, AES (128-bit), WEP 128-bit and 64-bit.
Product Safety	UL, C-UL, CB (IEC 60590)

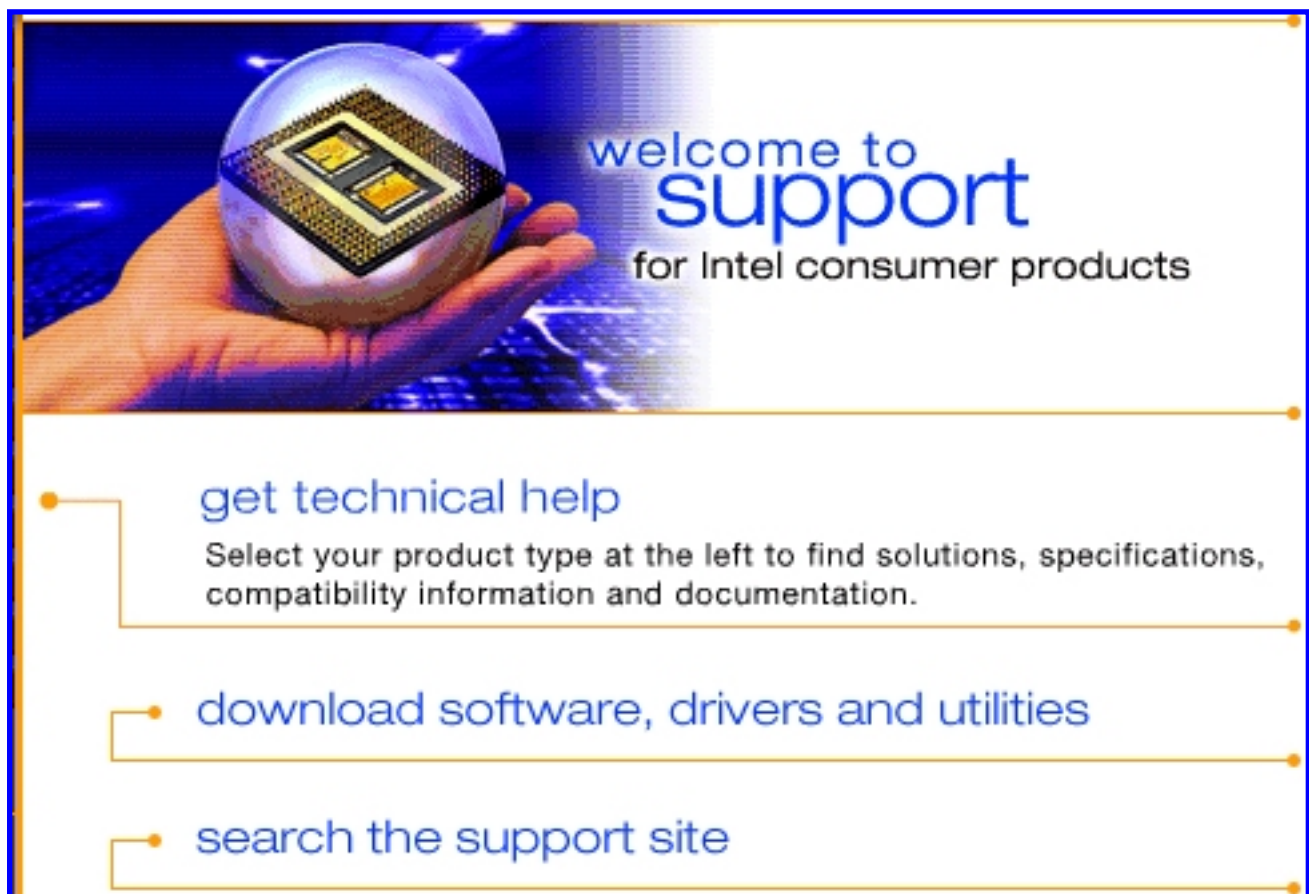
[Back to Top](#)

[Back to Contents](#)

[Trademarks and Disclaimers](#)

Customer Support: Intel(R) PRO/Wireless 3945ABG 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/support/go/wireless/wlan/pro3945abg.htm>

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

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

[Back to Contents](#)

Regulatory Information: Intel(R)PRO/ Wireless 3945ABG Network Connection User Guide

Supported on the Intel(R) PRO/ Wireless 3945ABG Network Connection, Intel(R) PRO/ Wireless 2915ABG Network Connection and Intel(R) PRO/ Wireless 2200BG Network Connection Hardware

[Intel\(R\) PRO/Wireless 3945ABG Network Connection](#)

- [Information for the User](#)
- [Regulatory Information](#)

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

- [Information for the User](#)
- [Regulatory Information](#)

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

- [Information for the User](#)
- [Regulatory Information](#)

Intel(R) PRO/ Wireless 3945ABG Network Connection

The information in this document applies to the following products:

Tri-mode wireless LAN adapters (802.11a/802.11b/802.11g)
Intel(R) PRO/Wireless 3945ABG Network Connection (model WM3945AGM1)
Intel(R) PRO/Wireless 3945ABG Network Connection (model WM3945AGM2)

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 3945ABG Network Connection adapter meets the Human Exposure limits found in OET Bulletin 65, supplement C, 2001, and ANSI/IEEE C95.1, 1992. Proper operation of this radio according to the instructions found in this manual will result in exposure substantially below the FCC's recommended limits.

The following safety precautions should be observed:

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

Explosive Device Proximity Warning

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

Antenna Warnings

 **Warning:** To comply with the FCC and ANSI C95.1 RF exposure limits, it is recommended for the Intel(R) PRO/Wireless 3945ABG Network Connection adapter installed in a desktop or portable computer, that the antenna for this device be installed so as to provide a separation distance of at least 20 cm (8 inches) from all persons and that the antenna must not be co-located or operating in conjunction with any other antenna or radio transmitter. It is recommended that the user limit exposure time if the antenna is positioned closer than 20 cm (8 inches).

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

Use On Aircraft Caution

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

Other Wireless Devices

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

Local Restrictions on 802.11a, 802.11b, and 802.11g Radio Usage

 **Caution:** Due to the fact that the frequencies used by 802.11a, 802.11b and 802.11g wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, and 802.11g products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. The device transmit power control (TPC) interface is part of the Intel(R) PROSet/Wireless software. Operational restrictions for Equivalent Isotropic Radiated Power (EIRP) are provided by the system manufacturer. Any deviation from the permissible power and frequency settings for the country of use is an

infringement of national law and may be punished as such.

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

Wireless interoperability

The Intel(R) PRO/Wireless 3945ABG 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 compliant Standard on Wireless LAN.
- IEEE Std. 802.11g compliant Standard on Wireless LAN.
- IEEE Std. 802.11a compliant Standard on Wireless LAN.
- Wireless Fidelity (WiFi) certification, as defined by the WECA (Wireless Ethernet Compatibility Alliance).

The Intel(R) PRO/Wireless 3945ABG Network Connection adapter and your health

The Intel(R) PRO/Wireless 3945ABG Network Connection adapter, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by this device, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The Intel(R) PRO/Wireless 3945ABG Network Connection adapter wireless device operates within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of the Intel(R) PRO/Wireless 3945ABG 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 3945ABG Network Connection adapter equipment on board airplanes, or
- Using the Intel(R) PRO/Wireless 3945ABG Network Connection adapter equipment in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful

If you are uncertain of the policy that applies to the use of wireless devices in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the Intel(R) PRO/Wireless 3945ABG Network Connection adapter wireless device before you turn it on.

Regulatory information

Information for the OEMs and Integrators:

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

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

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

The following regulatory and safety notices must be published in documentation supplied to the end user of the product or system incorporating an Intel(R) PRO/Wireless 3945ABG Network Connection in compliance with local regulations. Host system must be labeled with "Contains FCC ID: XXXXXXXX", FCC ID displayed on label.

The Intel(R) PRO/Wireless 3945ABG Network Connection adapter wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. For country-specific approvals, see [Radio approvals](#). Intel Corporation is not responsible for any radio or television interference caused by unauthorized modification of the devices included with the Intel(R) PRO/Wireless 3945ABG Network Connection adapter kit, or the substitution or attachment of connecting cables and equipment other than that specified by Intel Corporation. The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user. Intel Corporation and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from the user failing to comply with these guidelines.

Local Restriction of 802.11a 802.11b, and 802.11g Radio Usage

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

Caution: Due to the fact that the frequencies used by 802.11a, 802.11b, and 802.11g wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, and 802.11g products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. Any deviation from permissible settings and restrictions in the country of use could be an infringement of national law and may be punished as such.

FCC Radio Frequency Interference Requirements

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

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

USA—Federal Communications Commission (FCC)

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

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

NOTE: The radiated output power of the Intel(R) PRO/Wireless 3945ABG Network Connection adapter wireless network device is far below the FCC radio frequency exposure limits. Nevertheless, the Intel(R) PRO/Wireless LAN wireless network device should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, you should keep a distance of at least 20 cm between you (or any other person in the vicinity) and the antenna that is built into the computer.

Interference statement

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

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

NOTE:The Intel(R) PRO/Wireless 3945ABG Network Connection adapter wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Any other installation or use will violate FCC Part 15 regulations.

Canada—Industry Canada (IC)

This device complies with RSS210 of Industry Canada.

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

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

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

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

Europe Frequency Bands

2.400 - 2.4835 GHz (Europe ETSI)

5.15 - 5.35 GHz and 5.47-5.725 GHz (Europe ETSI)
Low band 5.25 - 5.35 GHz is for indoor use only

5.47 - 5.725 GHz is current not allowed in Czech Republic and France.

Declaration of Conformity

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

Czech	Intel(R) Corporation tímto prohlašuje, že tento Intel(R) PRO/Wireless 3945ABG Network Connection je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES."
Danish	Undertegnede Intel(R) Corporation erklærer herved, at følgende udstyr Intel(R) PRO/Wireless 3945ABG Network Connection overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Dutch	Hierbij verklaart Intel(R) Corporation dat het toestel Intel(R) PRO/Wireless 3945ABG Network Connection in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Bij deze verklaart Intel(R) Corporation dat deze Intel(R) PRO/Wireless 3945ABG Network Connection voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
English	Hereby, Intel(R) Corporation, declares that this Intel(R) PRO/Wireless 3945ABG Network Connection is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Estonian	Käesolevaga kinnitab Intel(R) Corporation seadme Intel(R) PRO/Wireless 3945ABG Network Connection vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish	Intel(R) Corporation vakuuttaa täten että Intel(R) PRO/Wireless 3945ABG Network Connection tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
French	Par la présente Intel(R) Corporation déclare que l'appareil Intel(R) PRO/Wireless 3945ABG Network Connection est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. Par la présente, Intel(R) Corporation déclare que ce Intel(R) PRO/Wireless 3945ABG Network Connection est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables.
German	Hiermit erklärt Intel(R) Corporation, dass sich dieser/diese/dieses Intel(R) PRO/Wireless 3945ABG Network Connection in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi) Hiermit erklärt Intel(R) Corporation die Übereinstimmung des Gerätes Intel(R) PRO/Wireless 3945ABG Network Connection mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Intel(R) Corporation ΔΗΛΩΝΕΙ ΟΤΙ Intel(R) PRO/Wireless 3945ABG Network Connection ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΞΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ
Hungary	Alulírott, Intel(R) Corporation nyilatkozom, hogy a Intel(R) PRO/Wireless 3945ABG Network Connection megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak
Icelandic	Intel lýsir her með yfir að thessi bunadur, Intel(R) PRO/Wireless 3945ABG Network Connection , uppfyllir allar grunnkröfur, sem gerðar eru í R&TTE tilskipun ESB nr 1999/5/EC
Italian	Con la presente Intel(R) Corporation dichiara che questo Intel(R) PRO/Wireless 3945ABG Network Connection è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latvian	Ar šo Intel(R) Corporation deklarē, ka Intel(R) PRO/Wireless 3945ABG Network Connection atbilst Direktīvas 1999/5/EK būtiskajām prasībām un cietim ar to saistītajiem noteikumiem
Lithuanian	Intel(R) Corporation deklaruoja, kad Intel(R) Pro/Wireless 3945ABG Network Connection atitinka 1999/5/EC Direktyvos esminius reikalavimus ir kitas nuostatas".
Malti	Hawnhekk, Intel(R) Corporation, jiddikjara li dan Intel(R) PRO/Wireless 3945ABG Network Connection jikkonforma mal- t -ijiet essenzjali u ma provvedimenti o r ajn rilevanti li hemm fid-Direttiva 1999/5/EC
Polish	Niniejszym, Intel(R) Corporation, deklaruje, że Intel(R) PRO/Wireless 3945ABG Network Connection spełnia wymagania zasadnicze oraz stosowne postanowienia zawarte Dyrektywie 1999/5/EC.
Portuguese	Intel(R) Corporation declara que este Intel(R) PRO/Wireless 3945ABG Network Connection está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovak	Intel(R) Corporation týmto vyhlasuje, že Intel(R) PRO/Wireless 3945ABG Network Connection spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Slovenia	Šiuo Intel(R) Corporation deklaruoja, kad šis Intel(R) PRO/Wireless 3945ABG Network Connection atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Spanish	Por medio de la presente Intel(R) Corporation declara que el Intel(R) PRO/Wireless 3945ABG Network Connection cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Swedish	Härmed intygar Intel(R) Corporation att denna Intel(R) PRO/Wireless 3945ABG Network Connection står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

France

Pour la France métropolitaine

2.400 - 2.4835 GHz (Canaux 1à 13) autorisé en usage intérieur
2.400 -2.454 GHz (canaux 1 à 7) autorisé en usage extérieur

Pour la Guyane et la Réunion

2.400 - 2.4835 GHz (Canaux 1à 13) autorisé en usage intérieur .
2.420 - 2.4835 GHz (canaux 5 à 13) autorisé en usage extérieur

Pour tout le territoire Fan-cais:

Seulement 5.15 -5.35 GHz autorisé pour le 802.11a

Belgium

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

In geval van privé-gebruik, buiten een gebouw, op een openbare plaats, is geen registratie nodig, wanneer de afstand minder dan 300m is. Voor een afstand groter dan 300m is een registratie bij BIPT vereist. Voor registraties en licenties, gelieve BIPT te contacteren.

5 GHz interface is not allowed at this time.

Japan

5GHz 帯は室内でのみ使用のこと

Latvia

A license is required for outdoor use for operation in 2.4 GHz band.

Italia

A general authorization is requested for outdoor use in Italy

The use of these equipments is regulated by:

- D.L.gs 1.8.2003, n. 259, article 104 (activity subject to general authorization) for outdoor use and article 105 (free use) for indoor use, in both cases for private use.
- D.M. 28.5.03, for supply to public of RLAN access to networks and telecom services.

L'uso degli apparati è regolamentato da:

- D.L.gs 1.8.2003, n. 259, articoli 104 (attività soggette ad autorizzazione generale) se utilizzati al di fuori del proprio fondo e 105 (libero uso) se utilizzati entro il proprio fondo, in entrambi i casi per uso privato;
- D.M. 28.5.03, per la fornitura al pubblico dell'accesso R-LAN alle reti e ai servizi di telecomunicazioni.

Greece

A license is required for the outdoor use of band 5.470 – 5.725 GHz.

Belarus

2.4 GHz OFDM (802.11g) is not allowed at this time.

Indonesia

5 GHz interface is not allowed at this time.

Korea

당해 무선설비는 운용 중 전파혼신 가능성이 있음

Kuwait

5 GHz interface is not allowed at this time.

Oman

If the modules are less than 100 milliwatts they are unlicensed but if they are more than 100 milliwatts, the user is responsible for getting a license to operate from Telecommunications Regulatory Authority (TRA) in Sultanate of Oman.

Taiwan

第十二條

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Pakistan

Pakistan Telecommunication Authority (PTA) Approved

UAE

5 GHz interface is not allowed at this time.

Ukraine

5 GHz interface is not allowed at this time.

Radio approvals

To determine whether you are allowed to use your wireless network device in a specific country, please check to see if the radio type number that is printed on the identification label of your device is listed in the manufacture OEM Regulatory Guidance document.

Underwriters Laboratories Inc. (UL) Regulatory Warning

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

Intel(R) PRO / Wireless 2915ABG Network Connection

The information in this document applies to the following products:

Tri-mode wireless LAN adapters (802.11a/802.11b/802.11g)
Intel(R) PRO/Wireless 2915ABG Network Connection (model WM3B2915ABG)
Intel(R) PRO/Wireless 2915ABG Network Connection (model WM3A2915ABG)

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

Information for the user

Safety Notices

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

The following safety precautions should be observed:

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

Explosive Device Proximity Warning

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

Antenna Warnings

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

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

Use On Aircraft Caution

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

Other Wireless Devices

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

Local Restrictions on 802.11a, 802.11b, and 802.11g Radio Usage

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

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

Wireless interoperability

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

- IEEE Std. 802.1b compliant Standard on Wireless LAN.
- IEEE Std. 802.1g compliant Standard on Wireless LAN.
- IEEE Std. 802.1a compliant Standard on Wireless LAN.
- Wireless Fidelity (WiFi) certification, as defined by the WECA (Wireless Ethernet Compatibility Alliance).

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

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

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

If you are uncertain of the policy that applies to the use of wireless devices in a specific organization or environment (an airport, for example), you are encouraged to ask for

authorization to use the Intel(R) PRO/Wireless 2915ABG Network Connection adapter wireless device before you turn it on.

Regulatory information

Information for the OEMs and Integrators:

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

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

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

The following regulatory and safety notices must be published in documentation supplied to the end user of the product or system incorporating an Intel(R) PRO/Wireless 2915ABG Network Connection in compliance with local regulations. Host system must be labeled with "Contains FCC ID: XXXXXXXX", FCC ID displayed on label.

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

Local Restriction of 802.11a, 802.11b, and 802.11g Radio Usage

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

Caution: Due to the fact that the frequencies used by 802.11a, 802.11b, and 802.11g wireless LAN devices may not yet be harmonized in all countries, 802.11a, 802.11b, and 802.11g products are designed for use only in specific countries, and are not allowed to be operated in countries other than those of designated use. As a user of these products, you are responsible for ensuring that the products are used only in the countries for which they were intended and for verifying that they are configured with the correct selection of frequency and channel for the country of use. Any deviation from permissible settings and restrictions in the country of use could be an infringement of national law and may be punished as such.

FCC Radio Frequency Interference Requirements

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

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

USA—Federal Communications Commission (FCC)

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

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

NOTE: The radiated output power of the Intel(R) PRO/Wireless 2915ABG Network Connection adapter wireless network device is far below the FCC radio frequency exposure limits. Nevertheless, the Intel(R) PRO/Wireless LAN wireless network device should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, you should keep a distance of at least 20 cm between you (or any other person in the vicinity) and the antenna that is built into the computer.

Interference statement

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

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

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

Canada—Industry Canada (IC)

This device complies with RSS210 of Industry Canada.

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

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

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

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

Europe Frequency Bands

2.400 - 2.4835 GHz (Europe ETSI)

5.15 - 5.35 GHz and 5.47-5.725 GHz (Europe ETSI)
Low band 5.25 - 5.35 GHz is for indoor use only

5.47 - 5.725 GHz is current not allowed in Czech Republic and France.

Declaration of Conformity



Declaration of Conformity (1999/5/EC)

We, **INTEL CORPORATION SA**

Address: Branch Office; Veldkant 31; 2550 Kontich, Belgium

declare under our sole responsibility that the product:

- Name: **INTEL® PRO/Wireless 2915ABG Network Connection**
- Model: **WM3B2915ABG EU**

to which this declaration relates, is in compliance with all the applicable essential requirements, and other provisions of the European Council Directive:

1999/5/EC	Radio and Telecommunications Terminal Equipment Directive (R&TTE)
-----------	---

The conformity assessment procedure used for this declaration is Annex IV of this Directive

This product will bear the CE Mark label CE 0523 !

Product compliance has been demonstrated on the basis of:

- IEC 60950 (1999 3rd Edition with amendments 1, 2, 3, 4), and EN 60950 (2000) - 1995/519/EC, Council recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz)	For article 3.1(a) : Health and Safety of the User
- EN 301 489-1 v1.4.1, Aug. 2002 - EN 301 489-17 v1.2.1, Aug. 2002	For article 3.1(b) : Electromagnetic Compatibility
- Final Draft EN 300 328 v1.5.1, Mar 2004 - EN 301 893 v1.2.3, Aug 2003	For article 3.2 : Effective use of the spectrum allocated

The technical construction file is kept available at:

INTEL CORPORATION SA

Branch Office: Veldkant 31,
2550 Kontich, Belgium

Authorized Signature by

Date: July 19th 2004

Vincent Colin,
Worldwide Homologations Manager,
WPD Regulatory Department



Declaration of Conformity (1999/5/EC)

We, **INTEL CORPORATION SA**

Address: Branch Office; Veldkant 31; 2550 Kontich, Belgium

declare under our sole responsibility that the product:

- Name: **INTEL® PRO/Wireless 2915ABG Network Connection**
- Model: **WM3A2915ABG EU**

to which this declaration relates, is in compliance with all the applicable essential requirements, and other provisions of the European Council Directive:

1999/5/EC	Radio and Telecommunications Terminal Equipment Directive (R&TTE)
-----------	---

The conformity assessment procedure used for this declaration is Annex IV of this Directive

This product will bear the CE Mark label CE 0523 !

Product compliance has been demonstrated on the basis of:

- IEC 60950 (1999 3rd Edition with amendments 1, 2, 3, 4), and EN 60950 (2000) - 1995/519/EC, Council recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz)	For article 3.1(a) : Health and Safety of the User
- EN 301 489-1 v1.4.1, Aug. 2002 - EN 301 489-17 v1.2.1, Aug. 2002	For article 3.1(b) : Electromagnetic Compatibility
- Final Draft EN 300 328 v1.5.1, Mar 2004 - EN 301 893 v1.2.3, Aug 2003	For article 3.2 : Effective use of the spectrum allocated

The technical construction file is kept available at:

INTEL CORPORATION SA

Branch Office: Veldkant 31,
2550 Kontich, Belgium

Authorized Signature by

Date: July 19th 2004

Vincent Colin,
Worldwide Homologations Manager,
WPD Regulatory Department

Declaration of Conformity

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

Czech	Intel(R) Corporation tímto prohlašuje, že tento Intel(R) PRO/Wireless 2915ABG Network Connection je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Danish	Undertegnede Intel(R) Corporation erklærer herved, at følgende udstyr Intel(R) PRO/Wireless 2915ABG Network Connection overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF

Dutch	Hierbij verklaart Intel(R) Corporation dat het toestel Intel(R) PRO/Wireless 2915ABG Network Connection in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
	Bij deze verklaart Intel(R) Corporation dat deze Intel(R) PRO/Wireless 2915ABG Network Connection voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
English	Hereby, Intel(R) Corporation, declares that this Intel(R) PRO/Wireless 2915ABG Network Connection is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Estonian	Käesolevaga kinnitab Intel(R) Corporation seadme Intel(R) PRO/Wireless 2915ABG Network Connection vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish	Intel(R) Corporation vakuuttaa täten että Intel(R) PRO/Wireless 2915ABG Network Connection tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
French	Par la présente Intel(R) Corporation déclare que l'appareil Intel(R) PRO/Wireless 2915ABG Network Connection est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. Par la présente, Intel(R) Corporation déclare que ce Intel(R) PRO/Wireless 2915ABG Network Connection est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables.
German	Hiermit erklärt Intel(R) Corporation, dass sich dieser/diese/dieses Intel(R) PRO/Wireless 2915ABG Network Connection in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW <i>i</i>) Hiermit erklärt Intel(R) Corporation die Übereinstimmung des Gerätes Intel(R) PRO/Wireless 2915ABG Network Connection mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien).=
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Intel(R) Corporation ΔΗΛΩΝΕΙ ΟΤΙ Intel(R) PRO/Wireless 2915ABG Network Connection ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΑΟΙ ΠΙΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK.
Hungary	Alulírott, Intel(R) Corporation nyilatkozom, hogy a Intel(R) PRO/Wireless 2915ABG Network Connection megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Icelandic	<i>Intel</i> lýsir her með yfir að thessi bunadur, Intel(R) PRO/Wireless 2915ABG Network Connection , uppfyllir allar grunnkrofur, sem gerdar eru í R&TTE tilskipun ESB nr 1999/5/EC
Italian	Con la presente Intel(R) Corporation dichiara che questo Intel(R) PRO/Wireless 2915ABG Network Connection è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latvian	Ar šo Intel(R) Corporation deklarū*, ka Intel(R) PRO/Wireless 2915ABG Network Connection atbilst Direktīvas 1999/5/EK b*taskaj*m prasīb*m un citiem ar to saistītajiem noteikumiem.
Lithuanian	Intel(R) Corporation deklaruoja, kad Intel(R) Pro/Wireless 2915ABG Network Connection atitinka 1999/5/EC Direktyvos esminius reikalavimus ir kitas nuostatas".
Malti	Hawnhekk, Intel(R) Corporation, jiddikjara li dan Intel(R) PRO/Wireless 2915ABG Network Connection jikkonforma mal-•ti•ijiet essenzjali u ma provvedimenti o•rajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
Polish	Niniejszym, Intel(R) Corporation, deklaruje*, •e Intel(R) PRO/Wireless 2915ABG Network Connection spe•nia wymagania zasadnicze oraz stosowne postanowienia zawarte Dyrektywie 1999/5/EC.
Portuguese	Intel(R) Corporation declara que este Intel(R) PRO/Wireless 2915ABG Network Connection está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovak	Intel(R) Corporation týmto vyhlasuje, že Intel(R) PRO/Wireless 2915ABG Network Connection sp••a základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Slovenia	Šluo Intel(R) Corporation deklaruoja, kad šis Intel(R) PRO/Wireless 2915ABG Network Connection atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Spanish	Por medio de la presente Intel(R) Corporation declara que el Intel(R) PRO/Wireless 2915ABG Network Connection cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Swedish	Härmed intygar Intel(R) Corporation att denna Intel(R) PRO/Wireless 2915ABG Network Connection står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

France

Pour la France métropolitaine

2.400 - 2.4835 GHz (Canaux 1à 13) autorisé en usage intérieur
2.400 -2.454 GHz (canaux 1 à 7) autorisé en usage extérieur

Pour la Guyane et la Réunion

2.400 - 2.4835 GHz (Canaux 1à 13) autorisé en usage intérieur .
2.420 - 2.4835 GHz (canaux 5 à 13) autorisé en usage extérieur

Pour tout le territoire Fancais:

Seulement 5.15 -5.35 GHz autorisé pour le 802.11a

Belgium

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

In geval van privé-gebruik, buiten een gebouw, op een openbare plaats, is geen registratie nodig, wanneer de afstand minder dan 300m is. Voor een afstand groter dan 300m is een registratie bij BIPT vereist. Voor registraties en licenties, gelieve BIPT te contacteren.

Japan

5GHz 帯は室内でのみ使用のこと

Latvia

A license is required for outdoor use for operation in 2.4 GHz band. (Translation?)

Italia

A general authorization is requested for outdoor use in Italy

The use of these equipments is regulated by:

- D.L.gs 1.8.2003, n. 259, article 104 (activity subject to general authorization) for outdoor use and article 105 (free use) for indoor use, in both cases for private use.

- D.M. 28.5.03, for supply to public of RLAN access to networks and telecom services.

L'uso degli apparati è regolamentato da:

- D.L.gs 1.8.2003, n. 259, articoli 104 (attività soggette ad autorizzazione generale) se utilizzati al di fuori del proprio fondo e 105 (libero uso) se utilizzati entro il proprio fondo, in entrambi i casi per uso privato ;

- D.M. 28.5.03, per la fornitura al pubblico dell'accesso R-LAN alle reti e ai servizi di telecomunicazioni.

Greece

A license is required for the outdoor use of band 5.470 – 5.725 GHz.

Belarus

2.4 GHz OFDM (802.11g) is not allowed at this time.

Indonesia

5 GHz interface is not allowed at this time.

Korea

당해 무선설비는 운용 중 전파혼신 가능성이 있음

Kuwait

5 GHz interface is not allowed at this time.

Oman

If the modules are less than 100 milliwatts they are unlicensed but if they are more than 100 milliwatts, the user is responsible for getting a license to operate from Telecommunications Regulatory Authority (TRA) in Sultanate of Oman.

Taiwan

第十二條

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

..

Pakistan

Pakistan Telecommunication Authority (PTA) Approved

UAE

5 GHz interface is not allowed at this time.

Ukraine

5 GHz interface is not allowed at this time.

Radio approvals

To determine whether you are allowed to use your wireless network device in a specific country, please check to see if the radio type number that is printed on the identification label of your device is listed in the manufacture OEM Regulatory Guidance document.

Underwriters Laboratories Inc. (UL) Regulatory Warning

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

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

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

Information for the user

Safety Notices

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. The Intel(R) PRO/Wireless 2200BG Network Connection meets the Human Exposure limits found in OET Bulletin 65, 2001, and ANSI/IEEE C95.1, 1992. Proper operation of this radio according to the instructions found in this manual will result in exposure substantially below the FCC's recommended limits.

The following safety precautions should be observed:

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

Explosive Device Proximity Warning

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

Antenna Warnings

Warning: To comply with the FCC and ANSI C95.1 RF exposure limits, it is recommended for the Intel(R) PRO/Wireless 2200BG Network Connection installed in a desktop or portable computer, that the antenna for this device be installed so as to provide a separation distance of at least 20 cm (8 inches) from all persons and that the antenna must not be co-located or operating in conjunction with any other antenna or radio transmitter. It is recommended that the user limit exposure time if the antenna is positioned closer than 20 cm (8 inches).

Warning: The Intel(R) PRO/Wireless 2200BG Network Connection product is not designed for use with high-gain directional antennas. Use of such antennas with these products is illegal.

Use On Aircraft Caution

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

Local Restrictions on 802.11b and 802.11g Radio Usage

All frequencies used by 802.11b and 802.11g are harmonized. Some countries though may not allow 802.11g.

Wireless interoperability

The Intel(R) PRO/Wireless 2200BG Network Connection adapter is designed to be interoperable with any wireless LAN product that is based on direct sequence spread spectrum (DSSS) radio technology and to comply with the following standards:

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

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

The Intel(R) PRO/Wireless 2200BG Network Connection adapter, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by this device, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The Intel(R) PRO/Wireless 2200BG Network Connection adapter wireless device operates within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of the Intel(R) PRO/Wireless 2200BG Network Connection adapter wireless device may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations include the following:

- Using the Intel(R) PRO/Wireless 2200BG Network Connection adapter equipment on board airplanes, or
- Using the Intel(R) PRO/Wireless 2200BG Network Connection adapter equipment in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful.

If you are uncertain of the policy that applies to the use of wireless devices in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the Intel(R) PRO/Wireless 2200BG Network Connection adapter wireless device before you turn it on.

Regulatory information

The Intel(R) PRO/Wireless 2200BG Network Connection adapter wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. For country-specific approvals, see [Radio approvals](#). Intel Corporation is not responsible for any radio or television interference caused by unauthorized modification of the devices included with the Intel(R) PRO/Wireless 2200BG Network Connection adapter kit, or the substitution or attachment of connecting cables and equipment other than that specified by Intel Corporation. The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user. Intel Corporation and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from the user failing to comply with these guidelines.

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 2200BG Network Connection adapter wireless network device is far below the FCC radio frequency exposure limits. Nevertheless, the Intel PROSet/Wireless LAN wireless network device should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, you should keep a distance of at least 2 cm between you (or any other person in the vicinity) and the antenna that is built into the computer.

Interference statement

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

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

NOTE: The Intel(R) PRO/Wireless 2200BG Network Connection adapter wireless network device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. Any other installation or use will violate FCC Part 15 regulations.

U.S. Frequency Bands

2.400 - 2.462 GHz

Canada—Industry Canada (IC)

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

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

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

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



C E0336 !

Declaration of Conformity

We, **INTEL CORPORATION SA** ; Branch Office; Veldkant 31; 2550 Kontich; Belgium
 Declare that the **INTEL® PRO/Wireless 2200BG Network Connection** with model name: **WM3A2200BG**
 is in conformance with the essential requirements of the European Council Directive:

1999/5/EC (R&TTE)	Radio and Telecommunications Terminal Equipment Directive (Following Annex IV of this Directive)
-------------------	---

The essential requirements being:

Health & Safety of the user (article 3.1.a)	Following directive 73/23/EEC & European Council Recommendation 1999 519 EC
Electromagnetic Compatibility (article 3.1.b)	Following directive 89/336/EEC
Effective use of the spectrum (article 3.2)	Following the Notified Body Opinion from TNO Certification B.V. with Notified Body number 0336

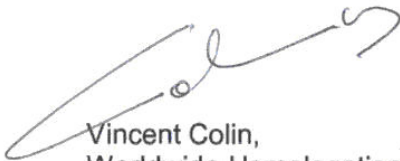
This declaration is based upon compliance to the following standards:

IEC 60950 (1999 3 rd Edition with amendments 1, 2, 3, 4) & EN 60950 (2000)	Safety Information Technology Equipment, Including Electrical Business Equipment. & Common modifications, special national conditions and National Deviation
EN 301 489-1 v1.4.1, Aug. 2002 EN 301 489-17 v1.2.1, Aug. 2002	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services: Part 1: Common technical requirements Part 17: Specific conditions for Wideband Data and Hiperlan equipment
EN 300 328-1 v1.4.1, Apr 2003	Electromagnetic compatibility and Radio Spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques. Part 2: Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
EN 50371	Generic standard to demonstrate the compliance of low power electronic and electrical apparatus with the basis restrictions related to human exposure to electromagnetic fields (10MHz - 300GHz) - General public

This declaration is made under our sole responsibility.

Authorized Signature by

Date: 01 December 2003



Vincent Colin,
Worldwide Homologations Manager,
WPD Regulatory Department



C E0336 !

Declaration of Conformity

We, **INTEL CORPORATION SA** ; Branch Office; Veldkant 31; 2550 Kontich; Belgium
Declare that the **INTEL® PRO/Wireless 2200BG Network Connection** with model name: **WM3A2200BG**
is in conformance with the essential requirements of the European Council Directive:

1999/5/EC (R&TTE)	Radio and Telecommunications Terminal Equipment Directive (Following Annex IV of this Directive)
-------------------	---

The essential requirements being:

Health & Safety of the user (article 3.1.a)	Following directive 73/23/EEC & European Council Recommendation 1999 519 EC
Electromagnetic Compatibility (article 3.1.b)	Following directive 89/336/EEC
Effective use of the spectrum (article 3.2)	Following the Notified Body Opinion from TNO Certification B.V. with Notified Body number 0336

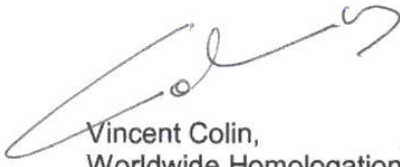
This declaration is based upon compliance to the following standards:

IEC 60950 (1999 3 rd Edition with amendments 1, 2, 3, 4) & EN 60950 (2000)	Safety Information Technology Equipment, Including Electrical Business Equipment. & Common modifications, special national conditions and National Deviation
EN 301 489-1 v1.4.1, Aug. 2002 EN 301 489-17 v1.2.1, Aug. 2002	Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services: Part 1: Common technical requirements Part 17: Specific conditions for Wideband Data and Hiperlan equipment
EN 300 328-1 v1.4.1, Apr 2003	Electromagnetic compatibility and Radio Spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques. Part 2: Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

	Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
EN 50371	Generic standard to demonstrate the compliance of low power electronic and electrical apparatus with the basis restrictions related to human exposure to electromagnetic fields (10MHz - 300GHz) - General public

This declaration is made under our sole responsibility.
Authorized Signature by

Date: 01 December 2003



Vincent Colin,
Worldwide Homologations Manager ,
WPD Regulatory Department

Declaration of Conformity

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

English	Hereby, Intel(R) Corporation, declares that this Intel(R) PRO/Wireless 2200BG Network Connection is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	Intel(R) Corporation vakuuttaa täten että Intel(R) PRO/Wireless 2200BG Network Connection tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart Intel(R) Corporation dat het toestel Intel(R) PRO/Wireless 2200BG Network Connection in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Bij deze verklaart Intel(R) Corporation dat deze Intel(R) PRO/Wireless 2200BG Network Connection voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la présente Intel(R) Corporation déclare que l'appareil Intel(R) PRO/Wireless 2200BG Network Connection est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. Par la présente, Intel(R) Corporation déclare que ce Intel(R) PRO/Wireless 2200BG Network Connection est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables.
Swedish	Härmed intygar Intel(R) Corporation att denna Intel(R) PRO/Wireless 2200BG Network Connection står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	Undertegnede Intel(R) Corporation erklærer herved, at følgende udstyr Intel(R) PRO/Wireless 2200BG Network Connection overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
German	Hiermit erklärt Intel(R) Corporation, dass sich dieser/diese/dieses Intel(R) PRO/Wireless 2200BG Network Connection in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW i) Hiermit erklährt Intel(R) Corporation die Übereinstimmung des Gerätes Intel(R) PRO/Wireless 2200BG Network Connection mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Intel(R) Corporation ΔΗΛΩΝΕΙ ΟΤΙ Intel(R) PRO/Wireless 2200BG Network Connection ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Icelandic	Intel lýsir her með yfir að thessi bunadur, Intel(R) PRO/Wireless 2200BG Network Connection , uppfyllir allar grunnkröfur, sem gerdar eru í R&TTE tilskipun ESB nr 1999/5/EC.
Italian	Con la presente Intel(R) Corporation dichiara che questo Intel(R) PRO/Wireless 2200BG Network Connection è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente Intel(R) Corporation declara que el Intel(R) PRO/Wireless 2200BG Network Connection cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Portuguese	Intel(R) Corporation declara que este Intel(R) PRO/Wireless 2200BG Network Connection está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Malti	Hawnhekk, Intel(R) Corporation, jiddikjara li dan Intel(R) PRO/Wireless 2200BG Network Connection jikkonforma mal-•ti•ijiet essenzjali u ma provvedimenti o•rajn rilevanti li hemm fid-Dirrettiva 1999/5/EC

New Member States requirements of Declaration of Conformity

Estonian	Käesolevaga kinnitab Intel(R) Corporation seadme Intel(R) PRO/Wireless 2200BG Network Connection vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Hungary	Alulírott, Intel(R) Corporation nyilatkozom, hogy a Intel(R) PRO/Wireless 2200BG Network Connection megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak
Slovak	Intel(R) Corporation týmto vyhlasuje, že Intel(R) PRO/Wireless 2200BG Network Connection sp••a základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Czech	Intel(R) Corporation tímto prohlašuje, že tento Intel(R) PRO/Wireless 2200BG Network Connection je ve shod• se základními požadavky a dalšími příslušnými ustanoveními sm•rnice 1999/5/ES."
Slovenia	Šiuo Intel(R) Corporation deklaruoja, kad šis Intel(R) PRO/Wireless 2200BGNetwork Connection atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Latvian	Ar šo Intel(R) Corporation deklar•, ka Intel(R) PRO/Wireless 2200BG Network Connection atbilst Direkt•vas 1999/5/EK b•tiskaj•m pras•b•m un citiem ar to saist•tajiem noteikumiem
Lithuanian	Intel(R) Corporation deklaruoja, kad Intel(R) Pro/Wireless 2200BG Network Connectionatitinka 1999/5/EC Direktyvos esminius reikalavimus ir kitas nuostatas".
Polish	Niniejszym, Intel(R) Corporation, deklaruje•, •e Intel(R) PRO/Wireless 2200BG Network Connection spe•nia wymagania zasadnicze oraz stosowne postanowienia zawarte Dyrektywie 1999/5/EC.

France

Pour la France métropolitaine

2.400 - 2.4835 GHz (Canaux 1à 13) autorisé en usage intérieur
2.400 -2.454 GHz (canaux 1 à 7) autorisé en usage extérieur

Pour la Guyane et la Réunion
2.400 - 2.4835 GHz (Canaux 1à 13) autorisé en usage intérieur
2.420 - 2.4835 GHz (canaux 5 à 13) autorisé en usage extérieur

Pour tout le territoire Fan cais:

Seulement 5.15 -5.35 GHz autorisé pour le 802.1

Belgique

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

In geval van privé-gebruik, buiten een gebouw, op een openbare plaats, is geen registratie nodig, wanneer de afstand minder dan 300m is. Voor een afstand groter dan 300m is een registratie bij BIPT vereist. Voor registraties en licenties, gelieve BIPT te contacteren.

Latvia

A license is required for outdoor use for operation in 2.4 GHz band.

Italia

The use of these equipments is regulated by:

- D.L.gs 1.8.2003, n. 259, article 104 (activity subject to general authorization) for outdoor use and article 105 (free use) for indoor use, in both cases for private use.
- D.M. 28.5.03, for supply to public of RLAN access to networks and telecom services.

L'uso degli apparati è regolamentato da:

- D.L.gs 1.8.2003, n. 259, articoli 104 (attività soggette ad autorizzazione generale) se utilizzati al di fuori del proprio fondo e 105 (libero uso) se utilizzati entro il proprio fondo, in entrambi i casi per uso privato;
- D.M. 28.5.03, per la fornitura al pubblico dell'accesso R-LAN alle reti e ai servizi di telecomunicazioni.

Belarus

2.4 GHz OFDM (802.11g) is not allowed at this time.

Korea

당해 무선설비는 운용 중 전파혼신 가능성이 있음

Taiwan

第十二條

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Pakistan

Pakistan Telecommunication Authority (PTA) Approved

Radio approvals

To determine whether you are allowed to use your wireless network device in a specific country, please check to see if the radio type number that is printed on the identification label of your device is listed in the manufacture OEM Regulatory Guidance document.

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

Product Warranty Information

One-Year Limited Hardware Warranty

Limited Warranty

Intel warrants to the purchaser of the Intel(R) PRO/Wireless 3945ABG Network Connection PCI Card (the “Product”), 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) have been removed, altered or obliterated from the Product; or (iv) issues resulting from modification (other than by Intel) of software products provided or included in the Product, (v) incorporation of software products, other than those software products provided or included in the Product by Intel, or (vi) 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 (<http://support.intel.com/support/notebook/centrino/sb/CS-009883.htm>) 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.
