Intel(R) Wireless WiFi Link 4965AGN User Guide

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

Your Intel(R) Wireless WiFi Link 4965AGN adapter is compatible with 802.11a, 802.11b 802.11g and 802.11n wireless standards. Operating at 5 GHz or 2.4 GHz frequency at speeds of up to 54 Mbps you can now connect your computer to existing high-speed networks that use multiple access points within large or small environments. Your wireless adapter maintains automatic data rate control according to access point location to achieve the fastest possible connection. All of your wireless network connections are easily managed by Intel(R) PROSet/Wireless software. Profiles that are set up through the Intel PROSet/Wireless software provide enhanced security measures with 802.1x network authentication.

> **NOTE:** The software is compatible with the Intel(R) Wireless WiFi Link 4965AGN, Intel(R) Wireless WiFi Link 4965AG_, Intel(R) PRO/Wireless 3965ABG Network Connection, Intel(R) PRO/Wireless 3945ABG Network Connection, Intel(R) PRO/Wireless 3945BG Network Connection, Intel(R) PRO/Wireless 2915ABG Network Connection and the Intel(R) PRO/Wireless 2200BG Network Connection.

Table of Contents

Use Intel PROSet/Wireless Software
Connect to a Network
Use Profiles
Set up Security
Troubleshooting
Administrator Tool
Glossary
Wireless Network Overview
Security Overview
Specifications
Customer Support
Safety and Regulatory Information
Warranty
Adapter Registration

Information in this document is subject to change without notice.
© 2004–2006 Intel Corporation. All rights reserved. Intel Corporation, 5200 N.E. Elam Young Parkway, Hillsboro, OR 97124-6497 USA

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

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

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

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

Intel wireless LAN adapters are engineered, manufactured, tested, and quality checked to ensure that they meet all necessary local and governmental regulatory agency requirements for the regions that they are designated and/or marked to ship into. Since wireless LANs are generally unlicensed devices that share spectrum with radars, satellites, and other licensed and unlicensed devices, it is sometimes necessary to dynamically detect, avoid, and limit usage to avoid interference with these devices. In many instances Intel is required to provide test data to prove regional and local compliance to regional and governmental regulations before certification or approval to use the product is granted. Intel's wireless LAN's EEPROM, firmware, and software driver are designed to carefully control parameters that affect radio operation and to ensure electromagnetic compliance (EMC). These parameters include, without limitation, RF power, spectrum usage, channel scanning, and human exposure.

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

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

October 2006

Back to Contents

Use Intel(R) PROSet/Wireless Software

Use Intel PROSet/Wireless on your Wireless Manager
Use Intel PROSet/Wireless
Start Intel PROSet/Wireless from the Taskbar
Taskbar Icon
Tool Tips and Desktop Alerts
Intel PROSet/Wireless Main Window
Wireless Networks List
Connection Status
Network Profile Properties
Advanced Settings
Wireless Network Properties
Profiles List
Profile Management
Menus

Use Intel PROSet/Wireless on your Wireless Manager

Intel(R) Wireless Manager is a powerful, easy-to-use manager software platform for Intel(R) Wireless. It also includes Intel(R) PROSet/Wireless Software, which provides advanced configuration options for Intel(R) Wireless.

Intel(R) Wireless Manager and Intel(R) PROSet/Wireless Software can be configured on your wireless manager, use Intel(R) PROSet/Wireless Software to configure Intel(R) Wireless.

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

1. Click **Start** > **Settings** > **Control Panel**.
2. Double-click **Network Connections**.
3. Right-click **Wireless Network Connection**.
4. Select **Properties**.
5. Clear the **Use Windows to configure my wireless network settings** check box (selected) in the **Wireless Networks** tab. Click **OK** to save the change and close the dialog box.

NOTE: Clicking the **Advanced** button opens **Ready done another application** when the wireless network is configured. Clear the check box (selected) in the **Wireless Networks** tab to prevent this dialog.

Start Intel PROSet/Wireless

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

- Click **Start** > **Programs** > **Intel PROSet/Wireless** > **Intel PROSet/Wireless**.
- Double-click the Intel PROSet/Wireless icon in the Windows* Taskbar Notification Area to open the Taskbar Icon. Select **Open Intel PROSet/Wireless**.
- Right-click the Intel PROSet/Wireless icon in the Windows* Taskbar Notification Area.

To open Intel PROSet/Wireless from the Taskbar, select one of the following options:

- Select **Disc Mode** from the menu.
- Select **Open Intel PROSet/Wireless**.
- Select **Exit** to close the icon from the right corner of the screen.

Start Intel PROSet/Wireless from the Taskbar

To start Intel PROSet/Wireless, double-click the **Taskbar** icon in the Windows* Taskbar Notification Area. Alternatively, right-click the **Taskbar** icon and select **Open Intel PROSet/Wireless**.

Taskbar Menu Options

The Taskbar Menu provides the following options:

Menu Item	Description
Open Intel PROSet/Wireless	Opens the Intel PROSet/Wireless Software.
Open Wireless Zero Configuration	Opens the Microsoft Windows* Wireless Zero Configuration.
Disc Mode	Opens the Disc Mode dialog box. Disc Mode allows the Intel(R) Wireless Software to be uninstalled without the Intel(R) Wireless Software causing the Windows* Wireless Zero Configuration to be enabled.
Profiles	Lists the available profiles. Select a profile to activate it.
Disable Radio	Disables the Intel(R) Wireless Radio.
Open Intel Wireless Troubleshooter	Opens the Intel Wireless Troubleshooter.
Open Intel PROSet Configuration	Opens the Intel PROSet/Wireless Software.
Open Intel PROSet Monitor	Opens the Intel PROSet Monitor.
Exit Wireless Zero Configuration	Exits the Microsoft Windows* Wireless Zero Configuration.
Exit Intel PROSet/Wireless	Exits the Intel PROSet/Wireless Software.

Taskbar Icons

	Connected to a wireless network The signal strength is indicated by the number of bars.
	Connected to a wireless network The signal strength is indicated by the number of bars. Data is being transmitted or received.
	Connected to a wireless network The signal strength is indicated by the number of bars. Security is enabled for the wireless network.
	Connected to a wireless network The signal strength is indicated by the number of bars. Data is being transmitted or received. Security is enabled for the wireless network.
	Connected to a wireless network The signal strength is indicated by the number of bars. Security is enabled for the wireless network.
	Connected to a wireless network The signal strength is indicated by the number of bars. Data is being transmitted or received.
	Connected to a wireless network The signal strength is indicated by the number of bars.
	Connected to a wireless network The signal strength is indicated by the number of bars. Data is being transmitted or received.
	Connected to a wireless network The signal strength is indicated by the number of bars. Security is enabled for the wireless network.
	Connected to a wireless network The signal strength is indicated by the number of bars. Data is being transmitted or received. Security is enabled for the wireless network.

Tool Tips and Desktop Alerts

The Tool Tips and Desktop Alerts provide information. It displays Tool Tips, Desktop Alerts and Desktop pop-ups when the mouse pointer is over the Taskbar Icon. Tool Tips and Desktop Alerts can be enabled or disabled in the Taskbar Icon Preferences.

Tool Tips

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

Desktop Alerts

Alerts are used to respond to wireless event changes. A pop-up alert displays when an appropriate action is taken. For example, when a connection is made to a wireless network.

Action Click on an alert to open the Intel PROSet/Wireless Software.

Clicking connection alerts displays the wireless network that you are connected to. The speed of the connection, signal strength and security.

Clicking alerts will also open to Intel PROSet/Wireless Software. Click the alert to open the Intel PROSet/Wireless Software.

Intel PROSet/Wireless Main Window

The Intel PROSet/Wireless Main Window allows you to:

- View the current connection status.
- View the wireless networks list.
- Manage profiles.
- Configure advanced options.
- View the Intel PROSet/Wireless Software version information.

Connection Status Icon

The Connection Status Icon displays the current status of your wireless adapter. The connection status uses Windows* Wireless Zero Configuration. Intel PROSet/Wireless Software provides additional information in the Connection Status.

Main Window Connection Status Description

The main page connection status displays the following information:

	Description
	Connected Indicates that the adapter is associated to a network. Click the **Wireless Icon** to access the wireless network.
	Disconnected Indicates a wireless connection is not established.
	Operating for wireless access The wireless adapter is operating for any available wireless network.
	Disabled The wireless adapter is disabled.
	No wireless networks found The adapter does not find any wireless network. The connection manager will continue to search for a wireless network. Click **Refresh** to force a search for wireless networks.
	Connection to a wireless network Indicates that a connection to a wireless network. The connection manager is attempting to connect to a wireless network. Click **Refresh** to force a search for wireless networks.
Network Name	**Name (Profile Name or SSID)** The name of the network that the adapter is associated to. If the **Profile Name** is enabled in the Advanced Settings, the Profile Name displays. Otherwise the SSID displays. If the network is a mixed mode network, the network name displays with a (mixed) suffix. If the network is a 802.11a network, the network name displays with a (a) suffix. If the network is a 802.11b network, the network name displays with a (b) suffix. If the network is a 802.11g network, the network name displays with a (g) suffix.
Speed	Displays the speed of the connection. Speed is a function of signal strength. Speed is also a function of the number of stations associated to the same access point. Speed is also a function of the number of stations associated to the same access point. Speed is also a function of the number of stations associated to the same access point

Security	Security allows consumers to a network with the defined WEP, WPA and WPA2 security options. Consumers can select the security type and enter the key.
Key	Shared secret key used in the selected mode
Key Index	Shared secret key index (1-4)
Save	Save changes and apply

Intel Wireless Toolbox(Vista Version)

Available Nets
2Wireless - Intel Centrino Duo Platform
Connected
Disconnect
Refresh
Show Tray
Show Connection Status
Show Signal Strength
Show Link Quality
Show Channel
Show Network Name
Show Network Type
Show Security Type
Show Data Rate
Show Tx Power
Show Channel Frequency
Show Station Name
Show Network Mode
Show Adapter Name
Show Adapter Type
Show Driver Version
Show Firmware Version
Show Hardware Version
Show Driver Date
Show Firmware Date
Show Hardware Date
Show Adapter Index
Show Adapter Description
Show Adapter Manufacturer
Show Adapter Hardware Address
Show Adapter Network Address
Show Adapter Network Mask
Show Adapter Gateway
Show Adapter DHCP Server
Show Adapter DHCP Lease Obtained
Show Adapter DHCP Lease Expiration
Show Adapter Primary DNS Server
Show Adapter Secondary DNS Server
Show Adapter WINS Server
Show Adapter Primary WINS Server
Show Adapter Secondary WINS Server
Show Adapter Number of Bytes Received
Show Adapter Number of Bytes Sent
Show Adapter Number of Bytes Received and Sent
Show Adapter Number of Bytes Received Per Second
Show Adapter Number of Bytes Sent Per Second
Show Adapter Number of Bytes Received and Sent Per Second
Show Adapter Number of Bytes Received Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received and Sent Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second Per Second
Show Adapter Number of Bytes Received Per Second

Back to Contents

Connect to a Network

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 **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

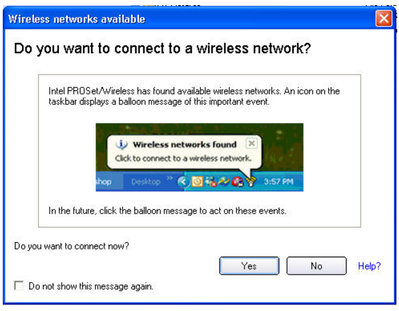
Intel PROSet/Wireless automatically detects wireless networks that are within range of your wireless adapter. When a network is found, a desktop alert notification displays: **Wireless networks found**. See Taskbar Icons for more information.

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 **Create Wireless Profile General Settings** 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. **Wireless Network Name (SSID):** Contains the network identifier name.
4. Click **Next**. The **Security Settings** attempts to detect the network settings of this network.
   - If a pre-shared key (PSK) or WEP password are required, you are prompted to enter this information prior to connection. Click **Advanced** to change or edit the PSK or other security settings. For information on key and passwords, see Network Keys.
   - If you need to add security settings, click **Next** to add the required security settings. Refer to Security Overview 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 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 to manage Wi-Fi** from the Taskbar menu.

From Intel PROSet/Wireless:

From the Advanced 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 or click **Use Intel PROSet/Wireless to manage Wi-Fi** 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

Back to Contents

Profile Management

What is a Profile?
Profiles List
Profiles List icons
Connect to a Profile
Create a New Profile
Edit an Existing Profile
Remove a Profile
Set a Profile Password
Export and Import Profiles

What is a Profile?

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

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

1. Select a Network Name from the **Wireless Networks** list.
2. Enter the network key.
3. If the wireless network requires a WEP password or encryption key, you are prompted to enter this information. Depending on the type of encryption and the security options, click **Advanced** to open the **Create Wireless Profile** dialog box.
4. Click **OK** to connect. A profile is created and added to the Profiles list.

The Create Wireless Profile manager guides you through the settings required to connect with the wireless network. Depending on the network you are connecting to, and the security options the wireless network is configured to send, the user may be prompted with a wide range of the wireless settings.

Profiles List

The Profiles List displays the list of existing profiles. When you come within range of a wireless network, Intel PROSetWireless automatically uses the Profile List to see if there is a match. If a match is found, you are automatically connected to the network.

Profile List Priority Arrows

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

Profiles List Icons

The network profile status icons indicate whether the adapter is associated with a network, the type of network, and the type of security that is configured or enabled. These icons display next to the profile name in the profile list.

Icon	Description
Profile Name	Displays the profile name in your name for this network. It can be anything that helps you identify this network. For example, My Home Network, Coffee Shop, Work Network.
Network Name	Displays the wireless network SSID or ESSID.
Connection Icons	The network profile status icons indicate the different connection states of the adapter. Hover over the icon to view a ToolTip of operating mode, level of network security, or being associated.
	Blue circle: The wireless adapter is associated with an access point or peer. Hover over the icon to view a ToolTip of the network name. Hover over the ellipsis that the wireless adapter is associated and authenticated.
	Indicates Network (Infrastructure) mode.
	Indicates Device to Device (ad hoc) mode.
	Indicates an Administrator profile.
	The wireless network keeps **Security** encryption.
Arrows	Use the arrows to position profiles in a preferred order for auto-connection.
	Up arrow: Moves the position of a selected profile up in the Profiles list.
	Down arrow: Moves the position of a selected profile down in the Profiles list.
Connect	Connect the selected profile to the wireless network.
Add	Opens the **Create Wireless Profile General Settings**, which is used to create a new profile. Refer to General Settings for more information.
Remove	Removes a selected profile from the Profile List. Refer to Remove a Profile for more information.
Properties	Used to edit the contents of an existing profile. You can also double-click a profile to open the Profile Properties. Refer to Edit an Existing Profile for more information.
	Export / Import: Imports and exports user-based profiles to and from the Profiles list. Refer to Export or Import Profiles for more information.
Close	Closes the profile management window.
Help?	Provides help information for this page.

Connect to a Profile

When you are in range of a wireless network that has a matching profile you are automatically connected to the network. Connect to a wireless network manually by selecting a profile from the Profiles list and clicking the **Connect** button. This is accessed from Intel PROSetWireless or from the Taskbar icon.

Manually connect to a profile from Intel PROSetWireless:

1. Double-click the **Taskbar** icon to open Intel PROSetWireless main window.
2. Select the profile from the Profiles list.
3. Select the profile from the Profile list.
4. Click **Connect**. The wireless adapter is only made if the wireless network is in range.

Manually connect to a profile from the **Taskbar**:

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

Create a New Profile

Select a network from the **Wireless Networks** list. Click **Connect**. The **Create Wireless Profile** manager guides you through the settings required to connect with the wireless network. Click **Advanced** button on the **Create Wireless Profile Settings** screen to select the appropriate security settings.

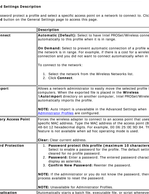
To create a new profile and connect to a wireless network:

1. Open the Intel PROSetWireless main window, click **Profiles**.
2. Select a network from the **Wireless Networks** list, click **Create Profile General Settings**.
3. **Profile Name**: Enter a descriptive profile name.
4. **Wireless Network Name (SSID)**: Enter the wireless network name.
5. Select the Operating Mode: **Network (Infrastructure)** or **Device to Device (ad hoc)**.

General Settings Description

Name	Description
Profile Name	Name of the wireless network profile.
	When you configure a wireless network that was selected from the Wireless Networks list, the Profile Name is the same as the Wireless Network Name (SSID). The same can be changed to a descriptive name. It is recommended for your personal use.
	Example: My Office Network, Bob's Home Network, ABC Company Network.
Wireless Network Name (SSID)	Name of the wireless network you want to add the wireless adapter for connection. The network name must match exactly the name of the wireless access point. It is case sensitive.
	When you configure a wireless network that was selected from the Wireless Network list, the Wireless Network Name (SSID) is the same as the Wireless Network Name (SSID) and should not change it.
	If an access point does not broadcast its network name (SSID) or the wireless adapter is configured to not broadcast its network name (SSID), the Wireless Network Name (SSID) is displayed as the Wireless Network Name. To associate with an hidden (not broadcast) network entry, a new profile must be created before connection. After connection, the network name (SSID) is displayed in the Wireless Network Name (SSID) and the profile is saved.
Operating Mode	**Network (Infrastructure)**: Connect to an access point. Be Network (Infrastructure) mode when connecting to a wireless access point. Network (Infrastructure) mode is the type of wireless network most commonly used. Wireless Network (Infrastructure) mode is required for access with an 802.1x authentication network entry, a less-secure profile that is created before connection. After connection, the network name (SSID) is displayed in the Wireless Network Name (SSID) and the profile is saved.
	Device to Device (ad hoc): Connect directly to other computers in an ad hoc wireless network. This type of connection is useful for connections between two or more computers in a small office or home network. Wireless Network (Infrastructure) mode is required for access to the Internet.
	Administrator: Select this profile type for Administrator. Use the Advanced Settings to set Maintain Connection, User Name Format, Auto Connect or Force import options. Select Administrator profile type when you want to create a profile that can be used to connect to the Intel Administrator Control Center.
Save	Saves the profile and closes the window.
OK	Closes window and saves changes with the current settings.
Cancel	Closes the Create Wireless Profile window and cancel any changes.
Help?	Provides help information for this page.

1. Click **Advanced** to open the following option:
   - Open **Other**:
   - **Auto Connect**: Select to automatically or manually connect to a profile.
   - **Auto Import**: Network administrator can export a profile on another computer.
   - **Mandatory Access Point**: Select to associate the wireless adapter with a specific access point.
   - **Maintain Connection**: Select to maintain connection.
   - **Start Application**: Specify a program to be started when a wireless connection is made.
   - **Maintain Connection**: Select to remain connected to a user profile after log off.

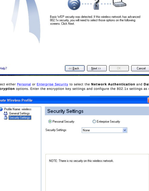


Advanced Settings Description

Use advanced settings to protect a profile and select a specific access point on a network to connect to. Click the **Advanced** button on the General Settings page to access this page.

Name	Description
Auto Connect	**Automatic (Default)**: Select to have Intel PROSetWireless connect automatically to this profile when it is in range.
	On Demand: Select to prevent automatic connection of a profile when in range. Use this option if you want to connect to a specific profile (for example, personal) and you do not want to connect automatically when in range.
	To connect to the network:
	1. Select the network from the Wireless Networks list.
	2. Click **Connect**.
Auto Import	Allows a network administrator to easily move the selected profile to other computers. Select one of the following options for Auto Import:
	Subnet Broadcast directory on another computer. Intel PROSetWireless automatically imports the profile.
	NOTE: Auto Import is unavailable in the Advanced Settings when Administrator profiles are selected.
Mandatory Access Point	Forces the wireless adapter to connect to an access point that uses a specified MAC address. Enter the MAC address of the access point in the text box. The MAC address is displayed in the format: 00-AA-00-BB-CC-DD. This feature is not available when ad hoc operating mode is used.
	Open: User current address.
Password Protection	1. **Password protect this profile (maximum 15 characters)**: Select to password protect the profile. The default setting is cleared for no profile password.
	2. **Password**: Enter a password. The entered password characters are displayed as asterisks.
	3. **Confirm New Password**: Reenter the password.
	NOTE: If the administrator or you do not know the password, there is no process available to reset the password.
Start Application	**NOTE:** Unavailable for Administrator Profiles.
	Allows a specified application to be started when a user proper password (per password) is the profile is changed, start a Microsoft Windows CMD prompt, session automatically. Whenever you connect to a wireless network.
	1. Enter **Grabbit Start Application**.
	2. Enter the name of the program that you want to start or click **Browse** to select the program. Enter the full path to the program.
	3. Enter **Grabbit Stop Application**.
	4. Enter the name of the program that you want to stop.
	NOTE: Unavailable for Administrator Profiles.
Maintain Connection	Select the **Maintain Connection** option to selected and a persistent profile series, the persistent profile will not be applied at logoff. It will be applied if and the connection with this profile is lost.
	NOTE: The option may be used with Novell VPN client when it is configured to use Novell Client.
OK	Saves and uses the settings.
Cancel	Closes and cancel any changes.
Help?	Opens information for this page.

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



2. Select either Personal or Enterprise Security to select the **Network Authentication** and **Data Encryption** options. Enter the encryption keys and configure the 802.1x settings as required.

3. Click **OK** when you have completed the profile settings. To change or verify the profile settings, click **Back**.
4. Click **Finish** to save the profile settings. Intel PROSetWireless automatically detects that a new profile has been added and automatically attempts to connect to this new profile.
5. If you want to manually connect to this profile, click **Connect**. The connection icon displays the connection status. The network name, connection and receive speeds, and signal quality are also displayed.

Edit an Existing Profile

To edit an existing profile:

1. Click **Profiles** on the Intel PROSetWireless main window.
2. Select the profile to edit in the Profiles list.
3. Click **Properties** to open the **Profile Properties General Settings**.
4. Click **Next** or **Back** to navigate through the Wireless Profile Properties General and Security Settings.
   - **General Settings**: Refer to General Settings for more information.
   - **Security Settings**: Refer to Security Settings for more information.
5. Click **OK** to save the current settings and exit. Click **Cancel** to exit without saving changes.

Remove a Profile

To remove a profile:

1. Click **Profiles** on the Intel PROSetWireless main window.
2. Select the profile to remove.
3. Click **Remove**. You are notified that **Selected profiles will be permanently removed. Do you want to continue?**
4. Click **Yes**. The profile is removed from the Profiles list.

If you are not connected to the network:

1. Click **Profiles** on the Intel PROSetWireless main window.
2. Select the profile from the list.
3. Click **Remove**. You are notified that **Selected profiles will be permanently removed. Do you want to continue?**
4. Click **Yes**. The profile is removed from the Profiles list. If **profile name is active and will be permanently removed. Do you want to continue?** Click **Yes**. The profile is removed from the Profiles list.

NOTE: If the profile is active, you are prompted, you cannot remove or edit the profile settings without entering the password. If the administrator or you do not know the password, there is no process available to reset the password.

Set a Profile Password

To password protect an existing profile:

1. Click **Profiles** on the Intel PROSetWireless main window.
2. Select the profile from the Profiles list.
3. Click **Properties** to open the Wireless Profile General Settings.
4. Click **Advanced** to open the Advanced Settings.
5. Click **Next** to navigate through the Wireless Profile Properties Settings.
6. Select **Password protect this profile (maximum 15 characters)**.
7. Enter the password in the **Password** and **Confirm New Password** fields.
8. **Confirm Password**: Reenter the password.
9. Click **OK** to return to the Intel PROSetWireless main window.

Export or Import Profiles

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

NOTE: To export Administrator profiles, refer to Administrator Packages for more information.

Export Profiles from the Profiles List

1. Select intended or multiple profiles from the list.
2. Select **Export** to export one or more profiles from the Profiles list.
3. Select the destination folder. Click **Browse** to search your hard disk for the destination directory. The C:\ drive is the default directory.

4. Click **OK** to export the selected profile. You are notified: **Successfully exported selected profiles to the destination folder: C:**.

To select multiple profiles:

1. Use your mouse to highlight a profile.
2. Click **Ctrl**.
3. Click the mouse on the next selected. Release the instructions from Step 2 above to export multiple profiles.

Import Profiles into the Profiles List

To import profiles manually:

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

Administrator profiles are automatically be imported automatically into the Profiles list. Intel PROSetWireless automatically imports the profiles that have been created through **Export** or through **Export Profiles** in the Advanced Settings are automatically imported. If a profile of the same name already exists, the user profiles are notified to either replace the imported profile or accept it. If accepted, the profile is replaced.

All imported user-based profiles are placed at the bottom of the Profiles list.

Password Protected Profiles

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

Back to Top
Back to Contents

Trademarks and Disclaimers

Back to Contents

Set Up Profile Security

Jump to: Personal Security Settings
Enterprise Security
Configure Profiles for Infrastructure Networks
Set up a Client with Personal Security
Set up a Client with WPA-Personal (TKIP) or WPA2-Personal (TKIP) Security Settings
Set up a Client with WPA-Personal (AES-CCMP) or WPA2-Personal (AES-CCMP)
Set up a Client with WPA-Enterprise (TKIP) or WPA2-Enterprise (TKIP)
Set up a Client with WPA-Enterprise (AES-CCMP) or WPA2-Enterprise (AES-CCMP)
Set up a Client with WPA2-Enterprise (AES-CCMP) Network Authentication
Set up a Client with WPA2-Enterprise (AES-CCMP) Network Authentication
Set up a Client with EAP-SIM Network Authentication
Set up a Client with EAP-AKA Network Authentication
Set up a Client with EAP-TTLS Network Authentication
Set up a Client with EAP-FAST Network Authentication
Set up a Client with EAP-PEAP Network Authentication
Set up a Client with EAP-TLS Network Authentication
Set up Data Encryption and Authentication
Set up a Client with Open Authentication and No Data Encryption
Set up a Client with Open Authentication and 64-bit Data Encryption
Set up a Client with Open Authentication and 128-bit Data Encryption
Set up a Client with Shared Key Authentication and 64-bit Data Encryption
Set up a Client with Shared Key Authentication and 128-bit Data Encryption
Set up a Client with Shared Key Authentication and WEP Data Encryption
Set up a Client with Open Authentication and WEP Data Encryption
Set up a Client with Open Authentication and Data Encryption
Set up a Client with Open Authentication

Use Intel(R) PROSet/Wireless Software to create profiles for Intel(R) Wireless adapters or set the required security settings for Intel(R) Wireless adapters in Windows Vista* Business Edition or Windows Vista* Ultimate Edition.

A data profile information entry has to configure advanced security settings for one wireless adapter. The Intel(R) Wireless adapter can have multiple data profile information entries. Each data profile information entry can have different security settings.

For general information about security settings, refer to Security Overview.

Personal Security

Personal Security is a set of security settings that enable and use only a pre-shared security key. Personal Security is a security mode that is used in home and small office networks. Personal Security supports the following security modes: Open Authentication, Shared Key Authentication, WPA-Personal, WPA2-Personal, and WPA-Auto-Personal.

Personal Security Settings

Personal Security Settings Screenshot

Security Mode:	Select Personal Security Mode. The Personal security mode uses a pre-shared security key for authentication and data encryption.
Security Type:	Select Security Type. The Security Type drop-down menu displays the following Personal Security Types: **Device to Device (ad hoc):** It is used to device-device, peer-peer or ad hoc networks. Open Authentication and Shared Key Authentication are supported. Data encryption is optional. Open Authentication and Shared Key Authentication are supported. Data encryption is optional. **WPA-Personal:** WPA-Personal is a security mode that uses a pre-shared key for authentication and data encryption. WPA-Personal is a security mode that uses a pre-shared key for authentication and data encryption. **NOTE:** Device to Device (ad hoc) connections are identified with a network name (SSID). **WPA2-Personal:** WPA2-Personal is a security mode that uses a pre-shared key for authentication and data encryption. WPA2-Personal is a security mode that uses a pre-shared key for authentication and data encryption. **Personal (infrastructure):** Networks are identified with an access point name (SSID). Open Authentication, Shared Key Authentication, WPA-Personal, and WPA2-Personal are supported. Data encryption is optional. Open Authentication, Shared Key Authentication, WPA-Personal, and WPA2-Personal are supported. Data encryption is optional. **NOTE:** Personal (infrastructure) networks are identified with an access point name (SSID). Open Authentication, Shared Key Authentication, WPA-Personal, and WPA2-Personal are supported. Data encryption is optional.
Encryption:	Select Encryption. The Encryption drop-down menu displays the following data encryption settings: • **Disabled** • **WEP** • **TKIP** • **AES-CCMP** If you configure a profile for an infrastructure network, select: • **Disabled** - Data encryption is not required. Data encryption is not required. • **WEP-Shared Key** - Data encryption is required. Data encryption is required. • **WPA-Personal TKIP** or **WPA2-Personal TKIP**. WPA-Personal enables the TKIP encryption. WPA2-Personal enables the TKIP encryption. • **WPA-Personal AES-CCMP** or **WPA2-Personal AES-CCMP**. WPA-Personal enables the AES-CCMP encryption. WPA2-Personal enables the AES-CCMP encryption.
Pre-Shared Key:	Enter the Pre-Shared Key. Enter the Pre-Shared Key.
Show characters	Select Show characters. Select Show characters.

Set up Data Encryption and Authentication

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and No Data Encryption

Open Authentication and No Data Encryption

Open Authentication and No Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and 64-bit Data Encryption

Open Authentication and 64-bit Data Encryption

Open Authentication and 64-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and 128-bit Data Encryption

Open Authentication and 128-bit Data Encryption

Open Authentication and 128-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and 64-bit Data Encryption

Shared Key Authentication and 64-bit Data Encryption

Shared Key Authentication and 64-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and 128-bit Data Encryption

Shared Key Authentication and 128-bit Data Encryption

Shared Key Authentication and 128-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and WEP Data Encryption

Shared Key Authentication and WEP Data Encryption

Shared Key Authentication and WEP Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and WEP Data Encryption

Open Authentication and WEP Data Encryption

Open Authentication and WEP Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and Data Encryption

Open Authentication and Data Encryption

Open Authentication and Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication

Open Authentication

Open Authentication

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Enterprise Security

Enterprise Security is a set of security settings that enable and use only a pre-shared security key. Enterprise Security is a security mode that is used in home and small office networks. Enterprise Security supports the following security modes: Open Authentication, Shared Key Authentication, WPA-Enterprise, WPA2-Enterprise, and WPA-Auto-Enterprise.

Enterprise Security Settings

Enterprise Security Settings Screenshot

Security Mode:	Select Enterprise Security Mode. The Enterprise security mode uses a pre-shared security key for authentication and data encryption.
Security Type:	Select Security Type. The Security Type drop-down menu displays the following Enterprise Security Types: **WPA-Enterprise:** WPA-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption. WPA-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption. **WPA2-Enterprise:** WPA2-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption. WPA2-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption.
Encryption:	Select Encryption. The Encryption drop-down menu displays the following data encryption settings: • **Disabled** • **WEP** • **TKIP** • **AES-CCMP**
Pre-Shared Key:	Enter the Pre-Shared Key. Enter the Pre-Shared Key.
Show characters	Select Show characters. Select Show characters.

Configure Profiles for Infrastructure Networks

Use the Intel(R) PROSet/Wireless Software to create profiles for Intel(R) Wireless adapters or set the required security settings for Intel(R) Wireless adapters in Windows Vista* Business Edition or Windows Vista* Ultimate Edition.

A data profile information entry has to configure advanced security settings for one wireless adapter. The Intel(R) Wireless adapter can have multiple data profile information entries. Each data profile information entry can have different security settings.

For general information about security settings, refer to Security Overview.

Set up a Client with Personal Security

WPA-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption. WPA-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption.

WPA2-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption. WPA2-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption.

Personal (infrastructure): Networks are identified with an access point name (SSID). Open Authentication, Shared Key Authentication, WPA-Personal, and WPA2-Personal are supported. Data encryption is optional. Open Authentication, Shared Key Authentication, WPA-Personal, and WPA2-Personal are supported. Data encryption is optional.

NOTE: Personal (infrastructure) networks are identified with an access point name (SSID). Open Authentication, Shared Key Authentication, WPA-Personal, and WPA2-Personal are supported. Data encryption is optional. Open Authentication, Shared Key Authentication, WPA-Personal, and WPA2-Personal are supported. Data encryption is optional.

Set up Data Encryption and Authentication

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and No Data Encryption

Open Authentication and No Data Encryption

Open Authentication and No Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and 64-bit Data Encryption

Open Authentication and 64-bit Data Encryption

Open Authentication and 64-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and 128-bit Data Encryption

Open Authentication and 128-bit Data Encryption

Open Authentication and 128-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and 64-bit Data Encryption

Shared Key Authentication and 64-bit Data Encryption

Shared Key Authentication and 64-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and 128-bit Data Encryption

Shared Key Authentication and 128-bit Data Encryption

Shared Key Authentication and 128-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and WEP Data Encryption

Shared Key Authentication and WEP Data Encryption

Shared Key Authentication and WEP Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and WEP Data Encryption

Open Authentication and WEP Data Encryption

Open Authentication and WEP Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and Data Encryption

Open Authentication and Data Encryption

Open Authentication and Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication

Open Authentication

Open Authentication

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Personal Security

Personal Security Settings

Personal Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

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

WPA-Personal Security Settings

WPA-Personal Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

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

WPA-Personal Security Settings

WPA-Personal Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with WPA-Enterprise (TKIP) or WPA2-Enterprise (TKIP)

WPA-Enterprise Security Settings

WPA-Enterprise Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with WPA-Enterprise (AES-CCMP) or WPA2-Enterprise (AES-CCMP)

WPA-Enterprise Security Settings

WPA-Enterprise Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with WPA2-Enterprise (AES-CCMP) Network Authentication

WPA2-Enterprise Security Settings

WPA2-Enterprise Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with WPA2-Enterprise (AES-CCMP) Network Authentication

WPA2-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption. WPA2-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption.

WPA-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption. WPA-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption.

Enterprise (infrastructure): Networks are identified with an access point name (SSID). Open Authentication, Shared Key Authentication, WPA-Enterprise, and WPA2-Enterprise are supported. Data encryption is optional. Open Authentication, Shared Key Authentication, WPA-Enterprise, and WPA2-Enterprise are supported. Data encryption is optional.

NOTE: Enterprise (infrastructure) networks are identified with an access point name (SSID). Open Authentication, Shared Key Authentication, WPA-Enterprise, and WPA2-Enterprise are supported. Data encryption is optional. Open Authentication, Shared Key Authentication, WPA-Enterprise, and WPA2-Enterprise are supported. Data encryption is optional.

Set up Data Encryption and Authentication

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and No Data Encryption

Open Authentication and No Data Encryption

Open Authentication and No Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and 64-bit Data Encryption

Open Authentication and 64-bit Data Encryption

Open Authentication and 64-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and 128-bit Data Encryption

Open Authentication and 128-bit Data Encryption

Open Authentication and 128-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and 64-bit Data Encryption

Shared Key Authentication and 64-bit Data Encryption

Shared Key Authentication and 64-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and 128-bit Data Encryption

Shared Key Authentication and 128-bit Data Encryption

Shared Key Authentication and 128-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and WEP Data Encryption

Shared Key Authentication and WEP Data Encryption

Shared Key Authentication and WEP Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and WEP Data Encryption

Open Authentication and WEP Data Encryption

Open Authentication and WEP Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and Data Encryption

Open Authentication and Data Encryption

Open Authentication and Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication

Open Authentication

Open Authentication

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Enterprise Security

Enterprise Security Settings

Enterprise Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with WPA-Enterprise (TKIP) or WPA2-Enterprise (TKIP)

WPA-Enterprise Security Settings

WPA-Enterprise Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with WPA-Enterprise (AES-CCMP) or WPA2-Enterprise (AES-CCMP)

WPA-Enterprise Security Settings

WPA-Enterprise Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with WPA2-Enterprise (AES-CCMP) Network Authentication

WPA2-Enterprise Security Settings

WPA2-Enterprise Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with WPA2-Enterprise (AES-CCMP) Network Authentication

WPA2-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption. WPA2-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption.

WPA-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption. WPA-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption.

Enterprise (infrastructure): Networks are identified with an access point name (SSID). Open Authentication, Shared Key Authentication, WPA-Enterprise, and WPA2-Enterprise are supported. Data encryption is optional. Open Authentication, Shared Key Authentication, WPA-Enterprise, and WPA2-Enterprise are supported. Data encryption is optional.

NOTE: Enterprise (infrastructure) networks are identified with an access point name (SSID). Open Authentication, Shared Key Authentication, WPA-Enterprise, and WPA2-Enterprise are supported. Data encryption is optional. Open Authentication, Shared Key Authentication, WPA-Enterprise, and WPA2-Enterprise are supported. Data encryption is optional.

Set up Data Encryption and Authentication

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and No Data Encryption

Open Authentication and No Data Encryption

Open Authentication and No Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and 64-bit Data Encryption

Open Authentication and 64-bit Data Encryption

Open Authentication and 64-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and 128-bit Data Encryption

Open Authentication and 128-bit Data Encryption

Open Authentication and 128-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and 64-bit Data Encryption

Shared Key Authentication and 64-bit Data Encryption

Shared Key Authentication and 64-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and 128-bit Data Encryption

Shared Key Authentication and 128-bit Data Encryption

Shared Key Authentication and 128-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and WEP Data Encryption

Shared Key Authentication and WEP Data Encryption

Shared Key Authentication and WEP Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and WEP Data Encryption

Open Authentication and WEP Data Encryption

Open Authentication and WEP Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and Data Encryption

Open Authentication and Data Encryption

Open Authentication and Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication

Open Authentication

Open Authentication

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Enterprise Security

Enterprise Security Settings

Enterprise Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with WPA-Enterprise (TKIP) or WPA2-Enterprise (TKIP)

WPA-Enterprise Security Settings

WPA-Enterprise Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with WPA-Enterprise (AES-CCMP) or WPA2-Enterprise (AES-CCMP)

WPA-Enterprise Security Settings

WPA-Enterprise Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with WPA2-Enterprise (AES-CCMP) Network Authentication

WPA2-Enterprise Security Settings

WPA2-Enterprise Security Settings

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with WPA2-Enterprise (AES-CCMP) Network Authentication

WPA2-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption. WPA2-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption.

WPA-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption. WPA-Enterprise is a security mode that uses a pre-shared key for authentication and data encryption.

Enterprise (infrastructure): Networks are identified with an access point name (SSID). Open Authentication, Shared Key Authentication, WPA-Enterprise, and WPA2-Enterprise are supported. Data encryption is optional. Open Authentication, Shared Key Authentication, WPA-Enterprise, and WPA2-Enterprise are supported. Data encryption is optional.

NOTE: Enterprise (infrastructure) networks are identified with an access point name (SSID). Open Authentication, Shared Key Authentication, WPA-Enterprise, and WPA2-Enterprise are supported. Data encryption is optional. Open Authentication, Shared Key Authentication, WPA-Enterprise, and WPA2-Enterprise are supported. Data encryption is optional.

Set up Data Encryption and Authentication

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and No Data Encryption

Open Authentication and No Data Encryption

Open Authentication and No Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and 64-bit Data Encryption

Open Authentication and 64-bit Data Encryption

Open Authentication and 64-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and 128-bit Data Encryption

Open Authentication and 128-bit Data Encryption

Open Authentication and 128-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and 64-bit Data Encryption

Shared Key Authentication and 64-bit Data Encryption

Shared Key Authentication and 64-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and 128-bit Data Encryption

Shared Key Authentication and 128-bit Data Encryption

Shared Key Authentication and 128-bit Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Shared Key Authentication and WEP Data Encryption

Shared Key Authentication and WEP Data Encryption

Shared Key Authentication and WEP Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and WEP Data Encryption

Open Authentication and WEP Data Encryption

Open Authentication and WEP Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication and Data Encryption

Open Authentication and Data Encryption

Open Authentication and Data Encryption

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Set up a Client with Open Authentication

Open Authentication

Open Authentication

Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

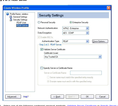
Open Authentication and Shared Key Authentication are supported. Data encryption is optional.

Authentication Protocols: The protocols specified for authentication protocol selection over the PEAP tunnel. The client and AAA server negotiate the authentication protocol to be used. The client and AAA server support the following authentication protocols: EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, EAP-SIM, EAP-AKA, EAP-FAST, EAP-TTLS, and EAP-PEAP.

Authentication Protocols: The protocols specified for authentication protocol selection over the PEAP tunnel

To configure a cisco router, present:

- **Authentication Protocol**: Select **IKE** (Internet Key Exchange)
- **Key Management**: Select **Pre-Shared and CRL** (Internet Key Exchange and Certificate Revocation List)
- **Data Encryption**: Select **DES** (Data Encryption Standard)



- Click **OK**

MS-CHAP v2: The parameter specifies the authentication protocol operating over the PPP tunnel.

- Select one of the following options: Use Windows logon Username and password, Use a certificate, Prompt for username and password

Click **Next** to open the **EAP Setup** window.

EAP: The parameter specifies the extensible authentication protocol that exclusively uses digital certificates.

- Where said field is not available, refer to Step 2a-2b Phase 2a-2b Authentication in section part 1 of this document.
- Select one of the following options: Use Windows logon Username and password, Use the certificate installed on the computer, or Use a smart card.

Click **Next** to open the **Finish** window.

Step 1 of 2: EAP Server

- Click **Save**
- Click **Save** to open the **Windows logon** or the Security Settings page and also set the **Extended Authentication (XAUTH)** to **Windows logon** or **Authentication Method List** to **Windows logon**
- Click **OK** to save the **Security Settings**

PEAP Set Certificate Auth Attributes

In the Netasistant Settings, select **Install Windows Wireless Non-Broadcast Network Keying**, then **Install Certificate Auth Attributes**. Select the **Authentication Protocol** and **Authentication Method** to be used for the Certificate Authentication Attributes. Select the **Certificate Authority** and **Certificate Name** to be used for the Certificate Authentication Attributes.

Attribute	Description
Authentication Protocol	Specifies the authentication protocol used for the Certificate Authentication Attributes.
Authentication Method (only available if the Authentication Protocol is set to EAP)	Specifies the authentication method that the Access Control Server (ACS) uses to authenticate the client. Valid values are: **Any**, **Any Secure**, **Any Secure Fast**, **Any Secure Fast Cryptobinding**, **Any Fast**, **Any Fast Cryptobinding**, **Any Cryptobinding**, **Any Secure Cryptobinding**, **Any Secure Fast Cryptobinding**.
Certificate Authority	Specifies the certificate authority that issues certificates to the client. Select **Any** to allow any certificate authority to issue the client certificate.
Certificate Name	Specifies the certificate name that the client presents. Select **Any** to allow any certificate to be presented. **Please enter the name to be used** allows you to specify a certificate name. Enter the certificate name in the text box.

Click **Save** to save the Certificate Attributes.

Set up a Client with EAP Network Authentication

Install EAP Client Authentication Environment (EAPCE). Select **Start** > **Programs** > **Netasistant Settings**, then **Install Wireless Non-Broadcast Network Keying**, then **Install Client Authentication Attributes**.

- Click **Security Level**
- Select **Secure**
- Click **Security Type**
- Select **Network Authentication**
- Click **Network Authentication**
- Select **EAP**
- Click **Save**
- Click **Save** to open the **Security Settings**

EAP Setup

- Select one of the following authentication methods: Use Windows logon user name and password, Use a certificate, Use the certificate installed on the computer, or Use a smart card
- Click **Save** to open the **Security Settings**

Cisco Compatible Extensions Options

Cisco Options can be enabled for Cisco Compatible Extensions and Broad Cisco Wireless or Cisco Non-Broadcast Keying.

NOTE: Cisco Compatible Extensions are automatically enabled for WEP, and if set WEP Dynamic Key Exchange is enabled, Cisco Compatible Extensions are also enabled.

Cisco Compatible Extensions version 1.0 - or Version 2.0 - Cisco Compatible Extensions version 1.0 allows a client with it configured for Net authentication and WEP Dynamic Key Exchange to roam between Cisco Aironet access points. Cisco Compatible Extensions version 2.0 allows a client with it configured for Net authentication and WEP Dynamic Key Exchange to roam between Cisco Aironet access points and Cisco Aironet access points with Broadcast Key Rotation enabled.

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

Broadcast Key Rotation: Broadcast Key Rotation is a feature that allows the access point to broadcast the WEP key to the Cisco Aironet client. The Broadcast Key Rotation option is only available if the Cisco Compatible Extensions version 2.0 is selected. Broadcast Key Rotation allows the access point to broadcast the WEP key to the Cisco Aironet client. The Broadcast Key Rotation option is only available if the Cisco Compatible Extensions version 2.0 is selected. Broadcast Key Rotation allows the access point to broadcast the WEP key to the Cisco Aironet client.

- **Enable Cisco Compatible Options**: Select to enable Cisco Compatible Extensions for the wireless connection
- **Broadcast Key Rotation**: Broadcast Key Rotation is a feature that allows the access point to broadcast the WEP key to the Cisco Aironet client. The Broadcast Key Rotation option is only available if the Cisco Compatible Extensions version 2.0 is selected. Broadcast Key Rotation allows the access point to broadcast the WEP key to the Cisco Aironet client. The Broadcast Key Rotation option is only available if the Cisco Compatible Extensions version 2.0 is selected. Broadcast Key Rotation allows the access point to broadcast the WEP key to the Cisco Aironet client.
- **Enable EAP**: Select to enable EAP
- **Enable Cisco Options**: Select to enable Cisco Options
- **Cisco Options**: Select **Broadcast Key Rotation** or **Cisco Non-Broadcast Keying**

Set up a Client with EAP-PEAP Network Authentication

In Cisco Compatible Extensions Version 1.0/2.0, Only allows support for EAP-PEAP (Protected Extensible Authentication Protocol) Version 0 and Version 1 with Cisco Compatible Extensions version 1.0/2.0 and Cisco Compatible Extensions version 1.0/2.0 Version 1 only.

Cisco Compatible Extensions version 1.0/2.0 Version 1 implements the processing mechanism for intermediate security and cryptographic binding between the EAP-PEAP and the EAP-Cisco Wireless (LEAP) authentication.

Cisco Compatible Extensions, Version 1.0/2.0:

To set up a client with EAP-PEAP authentication with Cisco Compatible Extensions, version 1.0/2.0:

- Select **Secure**
- Click **Security Type**
- Select **Network Authentication**
- Click **Network Authentication**
- Select **EAP**
- Click **Save**
- Click **Save** to open the **Security Settings**

EAP Setup

- Select one of the following authentication methods: Use Windows logon user name and password, Use a certificate, Use the certificate installed on the computer, or Use a smart card
- Click **Save** to open the **Security Settings**

Cisco Compatible Extensions, Version 2.0/EAP:

To set up a client with EAP-PEAP authentication with Cisco Compatible Extensions, version 2.0/EAP:

- Select **Secure**
- Click **Security Type**
- Select **Network Authentication**
- Click **Network Authentication**
- Select **EAP**
- Click **Save**
- Click **Save** to open the **Security Settings**

EAP Setup

- Select one of the following authentication methods: Use Windows logon user name and password, Use a certificate, Use the certificate installed on the computer, or Use a smart card
- Click **Save** to open the **Security Settings**

Cisco Compatible Extensions, Version 2.0/EAP:

To set up a client with EAP-PEAP authentication with Cisco Compatible Extensions, version 2.0/EAP:

- Select **Secure**
- Click **Security Type**
- Select **Network Authentication**
- Click **Network Authentication**
- Select **EAP**
- Click **Save**
- Click **Save** to open the **Security Settings**

EAP Setup

Troubleshooting

Installing Windows Troubleshooter
Network Connection Problems
Manual Diagnostics Tool
Manual Configuration Tool

Intel Wireless Troubleshooter

Intel(R) Wireless Troubleshooter
Enabled Now
To turn on Tap the Wi-Fi Hotspot icon in the Notification Area.
Wireless Hotspot Client
Intel(R) Wireless Troubleshooter is a tool that helps you to diagnose and resolve wireless connection problems.
Intel(R) Wireless Troubleshooter
Disabled Now
To turn off Tap the Wi-Fi Hotspot icon in the Notification Area.
Wireless Hotspot Client
Intel(R) Wireless Troubleshooter is a tool that helps you to diagnose and resolve wireless connection problems.
Intel(R) Wireless Troubleshooter
Enabled Now
Wireless Hotspot Client
Intel(R) Wireless Troubleshooter is a tool that helps you to diagnose and resolve wireless connection problems.
Intel(R) Wireless Troubleshooter
Disabled Now

Transcribe this Document

Administrator Tool

Site Administrator Password
Administrator Tool Settings
Administrator Profiles
Administrator Profiles
- Processes
- Pre-Logon Connection Connection
- Outside Networks
- Application Settings

Application Settings
- Application Settings
- Application Settings
- Application Settings
- Application Settings

The Administrator Tool is used by the site Administrator to configure the Connection Manager environment for their site. The Administrator Tool is installed on the Administrator's computer and is accessed through the Windows Start menu. The Administrator Tool is also used to create and deploy the Connection Manager Profiles. Connection Manager Profiles are created using the Microsoft Windows Administration Kit (Microsoft Windows Server 2003 Administration Tools Pack).

The Administrator Tool is installed from the Server Setup. It must be installed during the initial installation of the Connection Manager Server. Subsequent installations of the Administrator Tool can be made from the Server Setup or from the Administrator Tool Installer.

Set Administrator Password

The Administrator Tool is password protected and prompts users every time the Administrator tool is accessed. The password is set during the initial installation of the Connection Manager Server. The password can be changed using the Administrator Tool.

NOTE: If you do not know the original password, there is no process available to reset the password.

To change the existing password:

1. Select **Administrator Tool** from the Tools menu.
2. Enter the current password in the **Administrator Password** field.
3. Select **Set Administrator Password** from the Tools menu.
4. Enter the new password in the **New Password** field.
5. **Confirm Password**: Reenter the new password.
6. Select **OK** to save the new password.

To change the existing password:

1. Select **Administrator Tool** from the Tools menu.
2. Enter the current password in the **Administrator Password** field.
3. Select **Administrator Tool Settings** from the Tools menu.
4. Enter the new password in the **Administrator Password** field.
5. **Confirm Password**: Reenter the new password.
6. Select **OK** to save the new password.

Administrator Tool Settings

As Administrator, set Administrator and Profile Administrator profiles are placed in the Profile Directory. Perform the following:

1. Select **Administrator Tool** from the Tools menu.
2. Enter the current password in the **Administrator Password** field.
3. Select **Administrator Tool Settings** from the Tools menu.
4. **Administrator Password**: Enter the current password.
5. **Confirm Password**: Reenter the current password.
6. **Profile Directory**: Enter the Profile Directory path.
7. **Profile Name Prefix**: Enter the Profile Name Prefix.
8. **Profile Name Suffix**: Enter the Profile Name Suffix.
9. Select **OK** to save the Administrator Tool Settings.

Administrator Packages

Administrator Packages are used to create and deploy Administrator profiles and settings. The site Administrator creates the Administrator Profiles using the Microsoft Windows Administration Kit. Profiles can be created and configured using the Administrator Tool.

To create an Administrator Package:

1. Select **Administrator Tool** from the Tools menu.
2. Enter the current password in the **Administrator Password** field.
3. Select **Administrator Tool Settings** from the Tools menu.
4. Enter the current password in the **Administrator Password** field.
5. **Profile Directory**: Enter the Profile Directory path.
6. **Profile Name Prefix**: Enter the Profile Name Prefix.
7. **Profile Name Suffix**: Enter the Profile Name Suffix.
8. Select **OK** to save the Administrator Tool Settings.

Profile Name	Enter **Profile Name**.
Profile Description	Enter **Profile Description**.
Profile Directory	Enter **Profile Directory** for **Site package**.
Profile Name Prefix	Enter **Profile Name Prefix** for **Site package**.
Profile Name Suffix	Enter **Profile Name Suffix** for **Site package**.
Network Settings	Select **Network Settings** for **Site package**.
Dial-up Settings	Select **Dial-up Settings** for **Site package**.
Dial-up Settings for Site Package	Enter **Dial-up Settings** for **Site package**.
Site Package	Enter **Site Package** name.
Site Package Description	Enter **Site Package Description**.
Site Package Directory	Enter **Site Package Directory**.
Site Package Name	Enter **Site Package Name**

Name	Description
Set Cc Unique Mode	Specifies the Cc unique mode. Valid values are: 0 = Off, 1 = Warn, 2 = Block. The default value is 0.
Set Cc Warn	**Note:** This setting is available only if the value of the Set Cc Unique Mode parameter is 1 (Warn). The default value is false.
Set Cc Warn Message	Specifies the custom warning message that is displayed when the Cc unique mode is set to Warn. The default value is blank.
Set Domain	Specifies the domain name that is used when SMTP authentication is required. The default value is blank. **Note:** Set this parameter only if the Set Domain Required parameter is true.
Set Domain Required	Specifies whether a domain name is required. The default value is false. **Note:** Set this parameter only if the Set Domain parameter is blank.
Set Force Authentication	Specifies whether SMTP authentication is required. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Microsoft Proxy Settings**: Select to optimize performance when connecting to a Microsoft Exchange Server and authenticating using Kerberos.
Set Ssl Auth Mode	Specifies the Secure Sockets Layer (SSL) authentication mode. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Client Certificate**: Select to use a client certificate to authenticate. **Client Credentials**: Select to use the SSL client credentials to authenticate. **Client Credentials and Client Certificate**: Select to use both the SSL client credentials and a client certificate to authenticate. **Server Credentials**: Select to use the SSL server credentials to authenticate. **Server Credentials and Client Certificate**: Select to use the SSL server credentials and a client certificate to authenticate.
Set Ssl Client	Specifies the client certificate. Valid values are: **Subject Distinguished Name**: Select to specify the client certificate by its subject distinguished name. **Subject Common Name**: Select to specify the client certificate by its subject common name.
Set Ssl Client Subject	Specifies the client certificate subject. The default value is blank. **Note:** Set this parameter only if the Set Ssl Client parameter is Subject Common Name or Subject Distinguished Name.
Set Ssl Client Subject Distinguished Name	Specifies the client certificate subject distinguished name. The default value is blank. **Note:** Set this parameter only if the Set Ssl Client parameter is Subject Distinguished Name.
Set Ssl Client Subject Common Name	Specifies the client certificate subject common name. The default value is blank. **Note:** Set this parameter only if the Set Ssl Client parameter is Subject Common Name.
Set Ssl Ignore Errors	Specifies whether to ignore SSL errors. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to ignore all SSL errors.
Set Ssl Server	Specifies the server certificate. Valid values are: **Subject Distinguished Name**: Select to specify the server certificate by its subject distinguished name. **Subject Common Name**: Select to specify the server certificate by its subject common name.
Set Ssl Server Subject	Specifies the server certificate subject. The default value is blank. **Note:** Set this parameter only if the Set Ssl Server parameter is Subject Common Name or Subject Distinguished Name.
Set Ssl Server Subject Distinguished Name	Specifies the server certificate subject distinguished name. The default value is blank. **Note:** Set this parameter only if the Set Ssl Server parameter is Subject Distinguished Name.
Set Ssl Server Subject Common Name	Specifies the server certificate subject common name. The default value is blank. **Note:** Set this parameter only if the Set Ssl Server parameter is Subject Common Name.
Set Ssl Verify Mode	Specifies the SSL verification mode. Valid values are: **Disabled**: Select to disable SSL verification. **Enabled**: Select to enable SSL verification.
Set Ssl Verify Root Ca	Specifies the root certificate authority. The default value is blank. **Note:** Set this parameter only if the Set Ssl Verify Mode parameter is Enabled.
Set Ssl Verify Subject	Specifies the SSL verification subject. The default value is blank. **Note:** Set this parameter only if the Set Ssl Verify Mode parameter is Enabled.
Set Ssl Verify Subject Distinguished Name	Specifies the SSL verification subject distinguished name. The default value is blank. **Note:** Set this parameter only if the Set Ssl Verify Mode parameter is Enabled.
Set Ssl Verify Subject Common Name	Specifies the SSL verification subject common name. The default value is blank. **Note:** Set this parameter only if the Set Ssl Verify Mode parameter is Enabled.
Set Tls Mode	Specifies the TLS mode. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to use TLS.
Set Tls Version	Specifies the TLS version. Valid values are: **TLS 1.0**: Select to use TLS version 1.0. **TLS 1.1**: Select to use TLS version 1.1. **TLS 1.2**: Select to use TLS version 1.2.
Set Use Ssl	Specifies whether to use SSL. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to use SSL.
Set Use Ssl Proxy	Specifies whether to use SSL proxy. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to use SSL proxy.
Set Use Tls	Specifies whether to use TLS. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to use TLS.
Smtp Authentication	Specifies the SMTP authentication method. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Microsoft Proxy Settings**: Select to optimize performance when connecting to a Microsoft Exchange Server and authenticating using Kerberos.
Smtp Domain	Specifies the domain name that is used when SMTP authentication is required. The default value is blank. **Note:** Set this parameter only if the Smtp Domain Required parameter is true.
Smtp Domain Required	Specifies whether a domain name is required. The default value is false. **Note:** Set this parameter only if the Smtp Domain parameter is blank.
Smtp Force Authentication	Specifies whether SMTP authentication is required. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Microsoft Proxy Settings**: Select to optimize performance when connecting to a Microsoft Exchange Server and authenticating using Kerberos.
Smtp Ssl Auth Mode	Specifies the Secure Sockets Layer (SSL) authentication mode. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Client Certificate**: Select to use a client certificate to authenticate. **Client Credentials**: Select to use the SSL client credentials to authenticate. **Client Credentials and Client Certificate**: Select to use both the SSL client credentials and a client certificate to authenticate. **Server Credentials**: Select to use the SSL server credentials to authenticate. **Server Credentials and Client Certificate**: Select to use the SSL server credentials and a client certificate to authenticate.
Smtp Ssl Client	Specifies the client certificate. Valid values are: **Subject Distinguished Name**: Select to specify the client certificate by its subject distinguished name. **Subject Common Name**: Select to specify the client certificate by its subject common name.
Smtp Ssl Client Subject	Specifies the client certificate subject. The default value is blank. **Note:** Set this parameter only if the Smtp Ssl Client parameter is Subject Common Name or Subject Distinguished Name.
Smtp Ssl Client Subject Distinguished Name	Specifies the client certificate subject distinguished name. The default value is blank. **Note:** Set this parameter only if the Smtp Ssl Client parameter is Subject Distinguished Name.
Smtp Ssl Client Subject Common Name	Specifies the client certificate subject common name. The default value is blank. **Note:** Set this parameter only if the Smtp Ssl Client parameter is Subject Common Name.
Smtp Ssl Ignore Errors	Specifies whether to ignore SSL errors. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to ignore all SSL errors.
Smtp Ssl Server	Specifies the server certificate. Valid values are: **Subject Distinguished Name**: Select to specify the server certificate by its subject distinguished name. **Subject Common Name**: Select to specify the server certificate by its subject common name.
Smtp Ssl Server Subject	Specifies the server certificate subject. The default value is blank. **Note:** Set this parameter only if the Smtp Ssl Server parameter is Subject Common Name or Subject Distinguished Name.
Smtp Ssl Server Subject Distinguished Name	Specifies the server certificate subject distinguished name. The default value is blank. **Note:** Set this parameter only if the Smtp Ssl Server parameter is Subject Distinguished Name.
Smtp Ssl Server Subject Common Name	Specifies the server certificate subject common name. The default value is blank. **Note:** Set this parameter only if the Smtp Ssl Server parameter is Subject Common Name.
Smtp Ssl Verify Mode	Specifies the SSL verification mode. Valid values are: **Disabled**: Select to disable SSL verification. **Enabled**: Select to enable SSL verification.
Smtp Ssl Verify Root Ca	Specifies the root certificate authority. The default value is blank. **Note:** Set this parameter only if the Smtp Ssl Verify Mode parameter is Enabled.
Smtp Ssl Verify Subject	Specifies the SSL verification subject. The default value is blank. **Note:** Set this parameter only if the Smtp Ssl Verify Mode parameter is Enabled.
Smtp Ssl Verify Subject Distinguished Name	Specifies the SSL verification subject distinguished name. The default value is blank. **Note:** Set this parameter only if the Smtp Ssl Verify Mode parameter is Enabled.
Smtp Ssl Verify Subject Common Name	Specifies the SSL verification subject common name. The default value is blank. **Note:** Set this parameter only if the Smtp Ssl Verify Mode parameter is Enabled.
Smtp Tls Mode	Specifies the TLS mode. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to use TLS.
Smtp Tls Version	Specifies the TLS version. Valid values are: **TLS 1.0**: Select to use TLS version 1.0. **TLS 1.1**: Select to use TLS version 1.1. **TLS 1.2**: Select to use TLS version 1.2.
Smtp Use Ssl	Specifies whether to use SSL. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to use SSL.
Smtp Use Ssl Proxy	Specifies whether to use SSL proxy. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to use SSL proxy.
Smtp Use Tls	Specifies whether to use TLS. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to use TLS.
Tcp	Specifies the TCP port. The default value is 25.
Use Ssl	Specifies whether to use SSL. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to use SSL.
Use Ssl Proxy	Specifies whether to use SSL proxy. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to use SSL proxy.
Use Tls	Specifies whether to use TLS. Valid values are: **Disabled**: Select when connecting to an internal SMTP server that does not require authentication. **Enabled**: Select to use TLS.

To delete the Email Notification Profile, in the Administration Manager:

1. Stop the Celestixis Helpdesk Front end. Cmd:"PHPWebSrvMgr.exe/stop-c:c:\cmd\domain.cfg" where domain.cfg is the configuration file for the Celestixis Helpdesk Front end.
2. Stop the Celestixis Helpdesk Back end. Cmd:"PHPWebSrvMgr.exe/stop-c:c:\cmd\domain.cfg" where domain.cfg is the configuration file for the Celestixis Helpdesk Back end.
3. Delete the Email Notification Profile.
4. Start the Celestixis Helpdesk Front end. Cmd:"PHPWebSrvMgr.exe/start-c:c:\cmd\domain.cfg" where domain.cfg is the configuration file for the Celestixis Helpdesk Front end.
5. Start the Celestixis Helpdesk Back end. Cmd:"PHPWebSrvMgr.exe/start-c:c:\cmd\domain.cfg" where domain.cfg is the configuration file for the Celestixis Helpdesk Back end.

Software

Select which Vista Mitigation Software software components are installed on a user's computer.

Name	Description
Vista Software Install	Specifies the software to install. Valid values are: **Vista Mitigation Software**: Select to install the Vista Mitigation Software.
Vista Mitigation Software Installation Directory	Specifies the Vista Mitigation Software installation directory. The default value is blank.
Vista Mitigation Software Install Mode	Specifies the Vista Mitigation Software installation mode. Valid values are: **Silent**: Select to install the Vista Mitigation Software silently.
Vista Mitigation Software Install Log	Specifies the Vista Mitigation Software installation log. The default value is blank.
Vista Mitigation Software Uninstall Mode	Specifies the Vista Mitigation Software uninstall mode. Valid values are: **Silent**: Select to uninstall the Vista Mitigation Software silently.
Vista Mitigation Software Uninstall Log	Specifies the Vista Mitigation Software uninstall log. The default value is blank.
Vista Mitigation Software Uninstall Force	Specifies whether to force the Vista Mitigation Software uninstall. Valid values are: **Disabled**: Select to disable forced uninstall. **Enabled**: Select to force uninstall.
Vista Mitigation Software Uninstall Force Timeout	Specifies the Vista Mitigation Software uninstall force timeout. The default value is blank. **Note:** Set this parameter only if the Vista Mitigation Software Uninstall Force parameter is Enabled.
Vista Mitigation Software Uninstall Force Message	Specifies the Vista Mitigation Software uninstall force message. The default value is blank. **Note:** Set this parameter only if the Vista Mitigation Software Uninstall Force parameter is Enabled.
Vista Mitigation Software Uninstall Force Message Timeout	Specifies the Vista Mitigation Software uninstall force message timeout. The default value is blank. **Note:** Set this parameter only if the Vista Mitigation Software Uninstall Force parameter is Enabled.
Vista Mitigation Software Uninstall Force Message Text	Specifies the Vista Mitigation Software uninstall force message text. The default value is blank. **Note:** Set this parameter only if the Vista Mitigation Software Uninstall Force parameter is Enabled.

Name	Description
Microsoft Update Service	Specifies the Microsoft Update Service. Valid values are: **Windows Update**: Select to use Windows Update. **Microsoft Update**: Select to use Microsoft Update. **Windows Server Update Services**: Select to use Windows Server Update Services.
Microsoft Update Service Location	Specifies the Microsoft Update Service location. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service parameter is Windows Server Update Services.
Microsoft Update Service Statistics Location	Specifies the Microsoft Update Service statistics location. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service parameter is Windows Server Update Services.
Microsoft Update Service Target Group	Specifies the Microsoft Update Service target group. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service parameter is Windows Server Update Services.
Microsoft Update Service Target Group Name	Specifies the Microsoft Update Service target group name. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service parameter is Windows Server Update Services.
Microsoft Update Service Update Source	Specifies the Microsoft Update Service update source. Valid values are: **Windows Update**: Select to use Windows Update. **Microsoft Update**: Select to use Microsoft Update. **Windows Server Update Services**: Select to use Windows Server Update Services.
Microsoft Update Service Update Source Location	Specifies the Microsoft Update Service update source location. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service Update Source parameter is Windows Server Update Services.
Microsoft Update Service Update Source Statistics Location	Specifies the Microsoft Update Service update source statistics location. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service Update Source parameter is Windows Server Update Services.
Microsoft Update Service Update Source Target Group	Specifies the Microsoft Update Service update source target group. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service Update Source parameter is Windows Server Update Services.
Microsoft Update Service Update Source Target Group Name	Specifies the Microsoft Update Service update source target group name. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service Update Source parameter is Windows Server Update Services.
Microsoft Update Service Update Source Proxy	Specifies the Microsoft Update Service update source proxy. Valid values are: **Disabled**: Select to disable proxy. **Enabled**: Select to enable proxy.
Microsoft Update Service Update Source Proxy Bypass	Specifies the Microsoft Update Service update source proxy bypass. Valid values are: **Disabled**: Select to disable proxy bypass. **Enabled**: Select to enable proxy bypass.
Microsoft Update Service Update Source Proxy Bypass Local	Specifies the Microsoft Update Service update source proxy bypass local. Valid values are: **Disabled**: Select to disable proxy bypass local. **Enabled**: Select to enable proxy bypass local.
Microsoft Update Service Update Source Proxy Bypass Proxy Server	Specifies the Microsoft Update Service update source proxy bypass proxy server. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service Update Source Proxy Bypass parameter is Enabled.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Port	Specifies the Microsoft Update Service update source proxy bypass proxy server port. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service Update Source Proxy Bypass parameter is Enabled.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Protocol	Specifies the Microsoft Update Service update source proxy bypass proxy server protocol. Valid values are: **HTTP**: Select to use HTTP. **HTTPS**: Select to use HTTPS.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Protocol Version	Specifies the Microsoft Update Service update source proxy bypass proxy server protocol version. Valid values are: **1.0**: Select to use version 1.0. **1.1**: Select to use version 1.1.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local. Valid values are: **Disabled**: Select to disable proxy bypass local. **Enabled**: Select to enable proxy bypass local.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local exceptions. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local parameter is Enabled.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Delimiter	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local exceptions delimiter. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions parameter is Enabled.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Delimiter Type	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local exceptions delimiter type. Valid values are: **Comma**: Select to use a comma. **Semicolon**: Select to use a semicolon. **Space**: Select to use a space.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local exceptions bypass proxy server local addresses. Valid values are: **Disabled**: Select to disable bypass proxy server local addresses. **Enabled**: Select to enable bypass proxy server local addresses.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses Delimiter	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local exceptions bypass proxy server local addresses delimiter. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses parameter is Enabled.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses Delimiter Type	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local exceptions bypass proxy server local addresses delimiter type. Valid values are: **Comma**: Select to use a comma. **Semicolon**: Select to use a semicolon. **Space**: Select to use a space.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses Bypass Proxy Server Local Addresses	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local exceptions bypass proxy server local addresses. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses parameter is Enabled.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses Bypass Proxy Server Local Addresses Delimiter	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local exceptions bypass proxy server local addresses delimiter. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses parameter is Enabled.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses Bypass Proxy Server Local Addresses Delimiter Type	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local exceptions bypass proxy server local addresses delimiter type. Valid values are: **Comma**: Select to use a comma. **Semicolon**: Select to use a semicolon. **Space**: Select to use a space.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses Bypass Proxy Server Local Addresses Bypass Proxy Server Local Addresses	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local exceptions bypass proxy server local addresses bypass proxy server local addresses. Valid values are: **Disabled**: Select to disable bypass proxy server local addresses. **Enabled**: Select to enable bypass proxy server local addresses.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses Bypass Proxy Server Local Addresses Bypass Proxy Server Local Addresses Delimiter	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local exceptions bypass proxy server local addresses bypass proxy server local addresses delimiter. The default value is blank. **Note:** Set this parameter only if the Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses Bypass Proxy Server Local Addresses parameter is Enabled.
Microsoft Update Service Update Source Proxy Bypass Proxy Server Proxy Bypass Local Exceptions Bypass Proxy Server Local Addresses Bypass Proxy Server Local Addresses Bypass Proxy Server Local Addresses Delimiter Type	Specifies the Microsoft Update Service update source proxy bypass proxy server proxy bypass local exceptions bypass proxy server local addresses bypass proxy server local addresses delimiter type. Valid values are: **Comma**: Select to use a comma. **Semicolon**: Select to use a semicolon. **Space**: Select to use a space.

Administrator Tasks

How to Delete a Client Certificate

If you do not have any workstations for SAP GUI (SSL) or SAP PCA (TLS) you have added a client certificate, you can delete it.

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

Windows XP and Windows 2003: Since a client certificate is identified, by its subject name, the easiest way to find the certificate you want to delete is to open the Internet Explorer Control Panel and view the certificates by issuer name. Then, you can delete the certificate issued to the Celestixis Helpdesk Front end. Alternatively, you can delete all certificates issued by the Celestixis Helpdesk Front end to prevent any future problems.

Windows Vista/Windows 2008: Since a client certificate is identified, by its subject name, the easiest way to find the certificate you want to delete is to open the Internet Explorer Control Panel and view the certificates by issuer name. Then, you can delete the certificate issued to the Celestixis Helpdesk Front end. Alternatively, you can delete all certificates issued by the Celestixis Helpdesk Front end to prevent any future problems.

Note: Client Certificates are stored in the Windows Certificate Store. Deleting a client certificate from the Internet Explorer Control Panel will remove it from the Windows Certificate Store. Deleting a client certificate from the Windows Control Panel will remove it from the Internet Explorer Control Panel.

To delete the client certificate:

1. In the Start menu, click **Run**.
2. Type **mmc**.
3. Click **OK**. The Microsoft Management Console.
4. Click **File**.
5. Click **Add/Remove Snap-in**.
6. Click **Add**. The Add Standalone Snap-in page.
7. Click **Certificates**.
8. Click **Add**.
9. Click **Close**.
10. Click **OK**.
11. Click **Console Root**.
12. Click **Certificates (Local Computer)**.
13. Click **Trusted Root Certificates**.
14. Click **Certificates**.
15. Click **Celestixis**.
16. Click **Delete**.
17. Click **Yes**.
18. Click **Exit**.

Obtain a certificate from a Microsoft Windows 2000 CA

Microsoft Windows 2000 Server provides a web based interface to its HTTP Server (port 80 TCP) which allows users to request certificates from the Microsoft Windows 2000 Certificate Authority. Microsoft Windows 2000 Server provides a web based interface to its HTTP Server (port 80 TCP) which allows users to request certificates from the Microsoft Windows 2000 Certificate Authority. Microsoft Windows 2000 Server provides a web based interface to its HTTP Server (port 80 TCP) which allows users to request certificates from the Microsoft Windows 2000 Certificate Authority.

1. Log on to the Windows 2000 Server as an administrator.
2. Open the Internet Explorer and browse to the Windows 2000 Server.
3. Click **Certificate Services**.
4. Click **Request a certificate**.
5. Click **Advanced request**.
6. Click **Create and submit a request to this CA**.
7. Fill in the form. Scroll up and submit **Trusted Root Certificate Authorities**.
8. Click **Submit**.

Set up client certificates

To SAP PCA authentication, you need a valid client certificate in the trust repository for the Celestixis Front end server. You can create a self signed certificate or use a CA signed certificate.

The following instructions provide step wisedide for obtaining a certificate.

Note: Client certificates are stored in the Windows Certificate Store. Deleting a client certificate from the Internet Explorer Control Panel will remove it from the Windows Certificate Store.

If you do not have time to obtain a client certificate from the CA, contact your administrator to obtain a certificate.

To install the CA on the client machine:

1. Open the IE and type in your copy URL.
2. Click **Certificate Services**.
3. Click **Retrieve the CA certificate and certificate revocation list**.
4. Click **Install this CA certificate chain**.
5. Click **Open**.
6. Click **Install certificate**.
7. Click **Next**.
8. Click **Place all certificates in the following store**.
9. Click **Browse** and select **Trusted Root Certificate Authorities**.
10. Click **Next**.
11. Click **Finish**.
12. Click **Yes**.
13. Click **OK**.
14. Click **OK**.

Microsoft Management Console (MMC) is verify that the CA is installed in the trusted root.

1. In the Start menu, click **Run**.
2. Type **mmc**.
3. Click **OK**. The Microsoft Management Console.
4. Click **File**.
5. Click **Add/Remove Snap-in**.
6. Click **Add**. The Add Standalone Snap-in page.
7. Click **Certificates**.
8. Click **Add**.
9. Click **Close**.
10. Click **OK**.
11. Click **Console Root**.
12. Click **Certificates (Local Computer)**.
13. Click **Trusted Root Certificates**.
14. Click **Certificates**.
15. Verify that the CA is installed in trust.
16. Click **Exit**.

Obtain a certificate from a Microsoft Windows 2000 CA.

Microsoft Windows 2000 Server provides a web based interface to its HTTP Server (port 80 TCP) which allows users to request certificates from the Microsoft Windows 2000 Certificate Authority. Microsoft Windows 2000 Server provides a web based interface to its HTTP Server (port 80 TCP) which allows users to request certificates from the Microsoft Windows 2000 Certificate Authority. Microsoft Windows 2000 Server provides a web based interface to its HTTP Server (port 80 TCP) which allows users to request certificates from the Microsoft Windows 2000 Certificate Authority.

1. Log on to the Windows 2000 Server as an administrator.
2. Open the Internet Explorer and browse to the Windows 2000 Server.
3. Click **Certificate Services**.
4. Click **Request a certificate**.
5. Click **Advanced request**.
6. Click **Create and submit a request to this CA**.
7. Fill in the form. Scroll up and submit **Trusted Root Certificate Authorities**.
8. Click **Submit**.

Note: SAP PCA (TLS) requires a certificate issued to the Celestixis Front end server. The certificate must be issued to the Celestixis Front end server. The certificate must be issued to the Celestixis Front end server.

1. Open Internet Explorer.
2. Type the URL of the Celestixis Front end server.
3. Click **Tools**.
4. Click **Internet Options**.
5. Click **Advanced**.
6. Scroll down to **Security**.
7. Select **Check for server certificate revocation**.
8. Click **OK**.
9. Click **Yes**.
10. Click **OK**.
11. Click **Yes**.
12. Click **OK**.

Set up SAP PCA Server

1. Open your client's proxy configuration.
2. Add the Celestixis Front end server.
3. Save the configuration.
4. Restart your client.

Name	Description
Root Password	Encryption, root, the root password.
Root Password Confirm	Encryption, root, the root password confirm.
Root Password Encrypted	Encryption, root, the root password encrypted.

1. Click **Next**.

Step 4 of 4: Tid Server

1. Select one of the following material: Internal server, Celestixis Server Certificate or Celestixis Server Certificate Chain.
2. Click **Next**.
3. Enter the Tid Server Port. The default value is 5555. The port on which Tid listens for Tid Client connections.
4. Click **Generate** to create a Tid Server certificate, request.

Back to Contents

Glossary of Terms

Numerical A B C D E F G H I L M N O P R S T U V 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 (AP)	A device that connects wireless devices to another network. For example, a wireless LAN, Internet modem or others.
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 than WEP/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 broadcasting its SSID.
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 Microsoft Windows, a certificate can import a certificate from a file. A trusted CA certificate is stored in the root store.
CCX	Cisco Compatible extensions. Cisco Compatible Extensions Program ensures that devices used on Cisco wireless LAN infrastructure meet 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 authentication.
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 multicast mode. CKIP is Cisco's version of KIP.
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 is everything from passwords to time-of-day-expiration 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 that comes 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 WPA-Enterprise, 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 Rivest, Shamir, Adleman (RSA) keys. 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 files from different computers.
Fragmentation threshold	The threshold at which the wireless adapter breaks the packet into smaller 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 extension to EAP initially 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-encrypted 802.11 encrypted channel.
ns	Nanosecond: 1 billionth (1/1,000,000,000) of a second
OFDM	Orthogonal Frequency Division Multiplexing.
Open Authentication	Allows any device network access. If encryption is not enabled on the network, any device that knows the Service Set Identifier (SSID) of the access point can gain access to the network.
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. PEAP 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, one-time-only 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 cached at 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 one hertz per second cycles per second. One Mega-Hertz (MHz) is one million Hertz. One Giga-Hertz (GHz) is one billion Hertz. For reference: the standard AC 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. Seamless network roaming is only supported in the same subnet of a network.
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 data 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 impossible 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 features let wireless 802.1x credentials to match your Windows log on user name and password credentials for wireless network access.
SSID	Service Set Identifier. SSID or network name is 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. Each SSID can be up to 32 alphanumeric characters long and is case-sensitive.
Stealth	A stealth access point is one that has the capability and is configured to not broadcast its SSID. This is the wireless network name that appears when a Wireless Configuration Utility (Windows 2000) or Windows XP Wireless Network Connection Properties (Windows XP) scans for available wireless networks. It is commonly considered a weak security feature, in that it does not readily disclose the presence of the wireless network. To connect to a stealth access point, a user must know the SSID and configure their DMU accordingly. The feature is not a part of the 802.11 specification, and is known by differing names by various vendors: closed mode, private network, SSID broadcasting.
TKIP	Temporal Key Integrity protocol improves data encryption. Wi-Fi Protected Access uses its TKIP. TKIP provides message data encryption enhancements including a re-keying method. TKIP is part of the IEEE 802.11i encryption standard for wireless networks. TKIP is the next generation of WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless networks. 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-CHAP2). TTLS can easily be extended to work with new protocols by defining new attributes to support new protocols.
WEP	Wired Equivalent Privacy. Wired Equivalency, 64- and 128-bit (64-bit is sometimes referred to as 40-bit). This is a low-level encryption scheme 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 (WLAN) 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 radio station 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, all 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. It 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 connect wirelessly to another computer within the same network and to connect to the Internet.
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 802.11i standard upon its completion. WPA consists of RC4 and TKIP and provides support for 802s (Infrastructure) mode in both Pre-Shared Key and 802.1X modes.
WPA2	Wi-Fi Protected Access 2 (WPA2). This is the second generation of WPA that complies with the IEEE 802 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, strong-security authentication 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 framework to ensure that only authorized network users can access the network. WPA is an interim standard that will be replaced with the IEEE 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

Back to Contents

Wireless Network Overview

About Wireless Network Technology
What do I need to setup a Wireless Network?
Wireless Networking Basics

- What is a wireless network management utility?
- Network Name
- Profiles
- Security
- Configure a Wireless Network
- Identify a Wireless Network
- Select a Wireless Network Mode

How do I turn my radio on and off?

About Wireless Network Technology

A Wireless Local Area Network (WLAN) connects computers without network cables. Instead computers use radio communications to send data between each other. In a WLAN, a radio communications device called an access point or wireless router connects network computers and provides Internet or network access. 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 Connection adapter to connect to other similar wireless devices that comply with the 802.11 standard for wireless networking.

What do I need to setup a Wireless Network?

To setup a wireless network, you need the following:

- Broadband internet service such as cable or DSL. This includes a broadband modem
- A wireless router
- A wireless network adapter (wireless card) for each computer that you want to connect to the wireless network.

Wireless Networking Basics

What is a wireless network manager or client utility?

The software application on your computer that is used to manage your wireless connections is commonly referred to as a wireless network manager or client utility. Your Dell portable computer ships with two client utilities installed: Intel PROSet/ Wireless and Microsoft Windows Zero Configuration. Intel PROSet is set by default as the utility which controls the management of your wireless connections.

You can select which utility is the managing utility based on your preference. However, it is important to understand that the wireless network connection settings (profiles) created by each utility are only applied when that utility is managing. It is a common error for users to inadvertently switch between the two utilities. This is a problem because network settings created in one utility are not applied if the other utility is managing the wireless connections. It is recommended that you choose one client utility to manage your wireless connections, and stay with it.

Refer to Connect to a Network for more information.

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 set 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

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

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 connect to an existing network, use the encryption key provided by the administrator of the wireless network. If you set up your own network, you can make up your own key and use it on each computer.

The 802.1x authentication is independent of the 802.11 authentication process. The 802.1x standard provides a framework for various authentication and key-management protocols. There are different 802.1x authentication types, each providing a different approach to authentication, but all employing the same 802.1x protocol and framework for communication between a client and an access point. The 802.1x authentication methods include passwords, certificates and smart cards (plastic cards that hold data). 802.1x authentication option can only be used with Infrastructure operation mode.

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-bit- 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

Refer to Get Connected

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.
- **Basic Service Set (BSS):** Consists of two or more wireless nodes, or stations, which have recognized each other and have established communications.
- **Independent Basic Service Set (IBSS):** A mode of operation in an 802.11 system that allows direct communication between 802.11 devices without the need to set up a communication session with an access point.

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.

How do I turn my radio on and off?

You can want to turn your wireless adapter's radio on and off to:

- Conserve your computer's battery when not connected
- Meet the requirement to turn off radios on airplanes to prevent interference

There are two methods to turn the radio on and off:

- The hardware switch
- The Enable/Disable button in Intel PROSet/Wireless software

A common cause for users not being able to connect to a wireless network is due to the radio being turned off. If you are unable to connect to a wireless network, verify that your radio is turned on by both the hardware switch and the software Enable/ Disable button. Verify that you have checked both methods.

Refer to Enable or Disable the Wireless Radio for more information.

Back to Top

Back to Contents

Trademarks and Disclaimers

Back to Contents

Security Overview

WEP Encryption

- Open and Shared Key authentication

802.1x Authentication

- How 802.1x Authentication Works
- 802.1X Features

WPA/WPA2
Enterprise Mode
Personal Mode
WPA-Enterprise and WPA2-Enterprise
WPA-Personal and WPA2-Personal
AES-CCMP
TKIP
TLS
TTLS

- Authentication Protocols

PEAP

- Authentication Protocols

Cisco Features

- Cisco LEAP
- Cisco Rogue Access Point Security Feature
- Fast Roaming (CCKM)
- CKIP
- 802.11b and 802.11g Mixed Environment Protection Protocol
- EAP-FAST
- Mixed Cell Mode
- Radio Management

WEP Encryption

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

Wired Equivalent Privacy (WEP) encryption and shared authentication provide protection for your data on the network. WEP uses an encryption key to encrypt data before transmitting it. Only computers that use the same encryption key can access the network or decrypt the encrypted data transmitted by other computers. Authentication prevents unauthorized access from the network to the access point.

The WEP encryption algorithm is vulnerable to passive and active network attacks. TKIP and CKIP algorithms include enhancements to the WEP protocol that mitigate existing network attack options in cryptanalysis.

Open and Shared Key Authentication

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

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

802.1x Authentication

Overview

The 802.1x authentication is independent of the 802.11 authentication process. The 802.1x standard provides a framework for various authentication and key management protocols. There are different 802.1x authentication types, each provides a different approach to authentication but all employ the same 802.1x protocol and framework for communication between a client and an access point. In Cisco Wireless LAN products, the 802.1x authentication is performed by a supplicant resident in the client and by the access point. Refer to 802.1x authentication works for more information. With 802.1x authentication, an authentication server (Cisco Secure ACS) authenticates each client Dial-In User Service (RADIUS) server connected to the access point. The authentication process uses information that is a user's password that are not transmitted over the wireless network. Most 802.1x types support dynamic per-user, per-session WEP to strengthen the static key security. 802.1x benefits from the use of an existing authentication protocol known as the Extensible Authentication Protocol (EAP).

802.1x authentication for wireless networks has three main components:

- The authenticator (the access point)
- The supplicant (the client software)
- The authentication server (RADIUS)

The 802.1x authentication process provides an authentication request from the wireless client to the access point, which authenticates the client to an Extensible Authentication Protocol-compatible authentication server. The RADIUS server then authenticates either the user (via passwords or certificates) or the system (by MAC address). In theory, the wireless client is not allowed to join the network until the transaction is complete.

There are two main authentication algorithms used for 802.1x. Some examples are: EAP-TLS, EAP-TTLS, and Protected EAP (PEAP). These are all methods for the wireless client to identify itself to the RADIUS server. With RADIUS authentication, user identities are checked against databases. RADIUS constitutes a set of standards that addresses network authentication, Authorization and Accounting (AAA). Radius includes a proxy process to validate clients in a multi-server environment. RADIUS is a client/server protocol. Authentication, authorization, and accounting-based 802.11 wireless and wired network networks. Port-based network access control (PNAC) is a wireless local area network (LAN) infrastructure that authenticates devices attached to a LAN port and prevent access to that port if the authentication process fails.

What is RADIUS?

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

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

How 802.1x Authentication Works

A simplified description of 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
- Extensible Authentication Protocol-Authentication Protocol (EAP) - RFC 2284
- Supported authentication Methods
  - EAP TLS Authentication Protocol - RFC 2716 and RFC 2246
  - EAP Tunneled TLS (TTLS)
  - PEAP
- Supports Windows XP and Windows 2000

NOTE: Intel PROSet/Wireless security features on Windows Vista support TTLS and EAP-SIM authentication only.

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 its Temporal Key Integrity Protocol (TKIP) and Message Integrity Code (MIC) functions. Authentication can first include a pre-shared key function, a message integrity check (MIC) called Michael an extended initialization vector (IV) with extended packet numbering, and a rekeying mechanism. With these 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 designed for 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 passphrase, that is manually entered on wireless devices. Personal Mode implementation over 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.

NOTE: WPA-Enterprise and WPA2-Enterprise are interoperable.

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 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) 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 security method whenever using 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 keys and TKIP. EAP-TLS is the most secure authentication method because it requires mutual authentication between the client and the data encryption. The Tunnel 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. TTLS (Tunneled Transport Layer Security), like EAP-TLS, uses EAP-TLS to validate the server and create a TLS-encrypted channel between the client and server. The client then uses this TLS-encrypted channel to exchange authentication information. Challenge over this encrypted channel to enable server authentication. TTLS is similar to a protocol and two non-exposed TLS encrypted channel. TTLS implementations support a variety of methods defined by EAP, as well as server only methods (PAP, CHAP, MS-CHAP and MS-CHAPv2). TTLS can easily be extended to work with new protocols, providing new attributes to support new protocols.

Authentication Protocols

- **MD5:** Message Digest 5 (MD5) is a one-way authentication method that uses user names and passwords. This method does not support key management, but does require a pre-configured key if data encryption is used. It can be safely deployed for wireless applications inside EAP tunnel methods.
- **PAP:** Password Authentication Protocol is a two way handshake protocol designed for use with PPP authentication. Password Authentication Protocol is a plain text protocol used with other protocols. It is not secure.
- **CHAP:** Challenge Handshake Authentication Protocol is a three-way handshake protocol that is considered more secure than MD5 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 requires administrators to select this authentication method unless all data are to be encrypted.
- **MS-CHAP-V2:** Introduces an additional feature not available with MSCHAPV1 or standard CHAP authentication, the changed password feature. This feature allows the client to change the account password if the RADIUS server reports that the password has expired.

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) security. PEAP authenticates wireless LAN clients, including users' passwords and one-time passwords, and Generic Token Cards.

Authentication Protocols

- **Generic Token Card (GTC):** Carries user specific token cards for authentication. The main feature in GTC is Digital Certificate/Token Card-based authentication. In addition, GTC includes the ability to bind a name identities until the TLS encrypted tunnel is established, which provides identity protection that user names are not being broadcasted during authentication.
- **MS-CHAP-V2:** Refer to MS-CHAP-V2 above.
- **TLS:** 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. Refer to TLS above.

Cisco Features

NOTE: Cisco Features are not supported on a Windows Vista platform.

Cisco LEAP

Cisco LEAP (Cisco Light EAP) is a server and client 802.1x authentication through a user supplied login password that allows 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 messages from wireless client security. This feature works with Cisco LEAP 802.1x authentication. Standard 802.11 technology does not protect a network from the presence 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 main server. This configuration allows 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 packets send all messages unencrypted. Mixed-Cell Mode provides a way to operate a network that does not support, 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 only 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 key, the server sends a Protected Access Credential (PAC) to the client as a provisioning EAP-FAST exchange is properly obtained over time for 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 deems secure enough for the specific network and the network.
- Automatic provisioning establishes an encrypted tunnel to the server for 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 delivers 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 networks operate in "optional encryption" mode, client stations that join in WEP mode, send all messages encrypted, and stations that use standard packets send all messages unencrypted. Mixed-Cell Mode provides a way to operate a 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 with the infrastructure, it configures radio parameters, detects interference and rogue access points.

Back to Top

Back to Contents

Trademarks and Disclaimers

Back to Contents

Specifications

Intel Wireless WiFi Link 4965AGN
Intel Wireless WiFi Link 4965AG
Intel PRO/Wireless 3965ABG Network Connection
Intel PRO/Wireless 3945ABG Network Connection
Intel PRO/Wireless 3945ABG Network Connection
Intel PRO/Wireless 2915ABG Network Connection
Intel PRO/Wireless 2200BG Network Connection

Intel Wireless WiFi Link 4965AGN

Form Factor	PCI Express (TM) Mini Card
Dimensions	Height 2.00 in x 1.18 in x 0.18 in (50.95 mm x 30.0 mm x 4.5 mm)
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066
Antenna Diversity	On-board diversity
Connector Interface	53-pin Mini Card edge connector
Voltage	3.3 V
Operating Temperature	0 to +80 degrees Celsius
Humidity	50% to 95% non-condensing (at temperatures of 25 °C to 35 °C)
Frequency Modulation	**5 GHz (802.11a/n/) 2.4 GHz (802.11b/g/ n)**
Frequency band	5.15 GHz - 5.85 GHz (dependent on country) 2.400 - 2.4835 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Modulation	5 GHz (OFDM) Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz (5M: Orthogonal Frequency Division Multiplexing (OFDM)
Channels	4 to 12 (dependent on country)	Channel 1-11 (US only) Channel 1-13 (Japan, Europe)
IEEE 802.11n	300, 270, 243, 240, 180, 150, 144, 135, 130, 120, 117, 115.5, 90, 86.667, 72.2, 65, 60, 57.8, 45, 43.3, 30, 28.9, 21.7, 15, 14.4, 7.2 Mbps
IEEE 802.11a Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps
IEEE 802.11g Data Rates	54, 48, 36, 24, 18, 12, 11, 9, 6 Mbps
IEEE 802.11b Data Rates	11, 5.5, 2, 1 Mbps
General	
Operating Systems	Microsoft Windows 2000. Microsoft Windows XP (32 and 64 bit). Windows Vista(TM) (32 and 64 bit)
Wi-Fi(R) Alliance certification	Wi-Fi(R) certification for 802.11b, 802.11g, 802.11a, WPA, WPA2, WMM, EAP-SIM
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v4.0
WLAN Standard	IEEE 802.11g, IEEE 802.11a, IEEE 802.11n
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 60950)

Intel Wireless WiFi Link 4965AG_

(version with Draft N capabilities disabled. Draft N refers to IEEE P802.11n(TM)/D1.0 Draft Amendment to STANDARD FOR Information Technology -Telecommunications and information exchange between systems-Local and Metropolitan networks-Specific requirements Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Enhancements for Higher Throughput)

Form Factor	PCI Express (TM) Mini Card
Dimensions	Height 2.00 in x 1.18 in x 0.18 in (50.95 mm x 30.0 mm x 4.5 mm)
Antenna Interface Connector	Hirose U.FL-R-SMT mates with cable connector U.FL-LP-066
Antenna Diversity	On-board diversity
Connector Interface	53-pin Mini Card edge connector
Voltage	3.3 V
Operating Temperature	0 to +80 degrees Celsius
Humidity	50% to 95% non-condensing (at temperatures of 25 °C to 35 °C)
Frequency Modulation	**5 GHz (802.11a/ n) 2.4 GHz (802.11b/g/ n)**
Frequency band	5.15 GHz - 5.85 GHz (dependent on country) 2.400 - 2.4835 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Modulation	5 GHz (OFDM) Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz (5M: Orthogonal Frequency Division Multiplexing (OFDM)
Channels	4 to 12 (dependent on country)	Channel 1-11 (US only) Channel 1-13 (Japan, Europe)
IEEE 802.11n	300, 270, 243, 240, 180, 150, 144, 135, 130, 120, 117, 115.5, 90, 86.667, 72.2, 65, 60, 57.8, 45, 43.3, 30, 28.9, 21.7, 15, 14.4, 7.2 Mbps
IEEE 802.11a Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps
IEEE 802.11g Data Rates	54, 48, 36, 24, 18, 12, 11, 9, 6 Mbps
IEEE 802.11b Data Rates	11, 5.5, 2, 1 Mbps
General	
Operating Systems	Microsoft Windows 2000. Microsoft Windows XP (32 and 64 bit). Windows Vista(TM) (32 and 64 bit)
Wi-Fi(R) Alliance certification	Wi-Fi(R) certification for 802.11b, 802.11g, 802.11a, WPA, WPA2, WMM, EAP-SIM
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v4.0
WLAN Standard	IEEE 802.11g, IEEE 802.11a, IEEE 802.11n
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 60950)

Intel PRO/Wireless 3965ABG Network Connection

Form Factor	PCI Express (TM) X1
Dimensions	Height 2.50 in x 2.77 in x 0.18 in (65.8 mm x 70.3 mm x 4.5 mm)
Antenna Interface Connector	Tyco connector
Connector Interface	36-pin PCI Express edge connector
Voltage	3.3 V
Operating Temperature	0 to +80 degrees Celsius
Humidity	50 to 95% non-condensing at temperature of 25 °C to 85 °C
Frequency Modulation	**5 GHz (802.11a) 2.4 GHz (802.11b/g)**
Frequency band	5.15 GHz - 5.85 GHz	2.400 - 2.4835 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Modulation	5 GHz (OFDM) Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz (5M Orthogonal Frequency Division Multiplexing (OFDM)
Channels	4 to 12 non-overlapping, dependent on SKU	Channel 1-11 (US only) Channel 1-13 (Japan)
Data Rates	54, 48, 36, 24, 18, 12, 9, 6 Mbps	11, 5.5, 2, 1 Mbps
General	
Operating Systems	Microsoft Windows 2000. Microsoft Windows XP (32 and 64 bit). Microsoft Windows Vista (32 and 64 bit)
Wi-Fi(R) Alliance certification	WPA™ - Enterprise, WPA™ - Personal, WPA2™ - Enterprise, WPA2™ - Personal Enhanced EAP: EAP-TLS, EAP-TTLS/EAP-MD5, EAP-TTLS/MSCHAPv2, PEAPv1/ EAP-GTC, MMH™, WMM-UAPSD (WSP)
Cisco Compatible Extensions certification	Cisco Compatible Extensions, v4
WLAN Standard	IEEE 802.11a, IEEE 802.11b IEEE 802.11g, IEEE 802.11e, IEEE 802.11h
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 3945ABG Network Connection

Form Factor	PCI Express (TM) Mini Card
Dimensions	Height 2.00 in x 1.18 in x 0.18 in (50.95 mm x 30.mm x 4.5 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	5.15 GHz - 5.85 GHz	2.400 - 2.4835 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Modulation	5 GHz (OFDM) Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz (5M 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, v4
WLAN Standard	IEEE 802.11g, 802.11a, 802.11e
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 3945ABG Network Connection

Form Factor	PCI Express (TM) Mini Card
Dimensions	Height 2.00 in x 1.18 in x 0.18 in (50.95 mm x 30.mm x 4.5 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	**2.4 GHz (802.11b/g)**
Frequency band	2.400 - 2.4835 GHz (dependent on country)
Modulation	CCK, DQPSK, DBPSK
Wireless Modulation	2.4 GHz (5M: Orthogonal Frequency Division Multiplexing (OFDM)
Channels	Channel 1-11 (US only) Channel 1-13 (Japan, Europe)
Data Rates	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
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 60950)

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 PCI-DINM 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 - 5.85 GHz	2.400 - 2.472 GHz (dependent on country)
Modulation	BPSK, QPSK, 16 QAM, 64 QAM	CCK, DQPSK, DBPSK
Wireless Modulation	5 GHz (OFDM) Orthogonal Frequency Division Multiplexing (OFDM)	2.4 GHz (5M 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 2.3x 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 - 2.4 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

Back to Contents

Customer Support

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

Online Support

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

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

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

Back to Contents

Back to Contents

Regulatory Information

Intel(R) Wireless WiFi Link 4965AGN
Intel(R) Wireless WiFi Link 4965AGX
Intel(R) PRO/Wireless 3945ABG Network Connection
Intel(R) PRO/Wireless 3945BG Network Connection
Intel(R) PRO/Wireless 2200BG Network Connection
Intel(R) PRO/Wireless 2200BG Network Connection

Intel(R) Wireless WiFi Link 4965AGN
Intel(R) Wireless WiFi Link 4965AGX

- Information for the user
- Regulatory information

Intel(R) PRO/Wireless 3945ABG Network Connection
Intel(R) PRO/Wireless 3945BG Network Connection

- Information for the user
- Regulatory information

Intel(R) PRO/Wireless 2200BG Network Connection

- Information for the user
- Regulatory information

Intel(R) Wireless WiFi Link 4965AGN and Intel(R) Wireless WiFi Link 4965AGX

The information in this document applies to the following products:

Intel(R) Wireless WiFi Link 4965AGN (Dual band 802.11a/b/g/n PCI-Express mini card)
Intel(R) Wireless WiFi Link 4965AGX (Dual band 802.11a/b/g/n PCI-Express mini card)

For details whether LAN adapter (802.11a/b/g/n PCI-E Mini Card) Intel(R) Wireless WiFi Link 4965AGN/4965AGX is installed in your system:

NOTE: Due to the ordering name of organizations and resellers is the combination of the Intel 4965 PCI-E Mini Card and Intel(R) Wireless Wireless Network Connection Software, the Intel(R) Wireless WiFi Link 4965AGN/4965AGX Wireless Network Connection Software is also called Intel(R) Wireless Wireless Network Connection Software.

Information for the user

Safety Notices

- Do not touch or move antenna while the unit is transmitting or receiving.
- Antenna should maintain at least a separation distance of 20 cm (8 inch) from all persons.
- Do not place or install near strong electromagnetic field generating equipment.
- Installation in the vicinity of medical equipment may cause interference.
- Installation in aircraft is prohibited.
- Use of wireless devices on aircraft is prohibited.
- Use of wireless devices on aircraft is prohibited. Operation of transmitters in aircraft is prohibited unless it is specifically permitted by the aircraft operator or is performed in accordance with instructions provided by the aircraft operator. Transmitter-equipped electronic devices should be switched off when on board an aircraft. Also, any other use of radio communication devices on board an aircraft may interfere with the aircraft's navigation system. Intentional interference with aircraft navigation systems is prohibited by law. Failure to observe these instructions may be considered a violation of law.
- Operation in the vicinity of medical equipment may cause interference. Switch off your wireless device when in hospital areas, except when operation is permitted by the Hospital Scientific Administrative Office. Switch off your wireless device when in the vicinity of medical equipment. Operation in the vicinity of medical equipment may cause interference. Switch off your wireless device when in the vicinity of medical equipment. Operation in the vicinity of medical equipment may cause interference. Switch off your wireless device when in the vicinity of medical equipment. Operation in the vicinity of medical equipment may cause interference. Switch off your wireless device when in the vicinity of medical equipment.
- Operation in the vicinity of other electronic devices may cause interference. Switch off your wireless device when in the vicinity of other electronic devices. Operation in the vicinity of other electronic devices may cause interference. Switch off your wireless device when in the vicinity of other electronic devices. Operation in the vicinity of other electronic devices may cause interference. Switch off your wireless device when in the vicinity of other electronic devices.
- Switch off your wireless device when in the vicinity of explosive devices.
- Switch off your wireless device when in the vicinity of explosive devices. Operation in the vicinity of explosive devices may cause interference. Switch off your wireless device when in the vicinity of explosive devices. Operation in the vicinity of explosive devices may cause interference.

Intel® Wireless-AC 9560 Intel® Dual Band Wireless-AC 8260 Intel® Dual Band Wireless-AC 3165 Intel® Dual Band Wireless-N 7265 Intel® Dual Band Wireless-N 7260 Intel® Dual Band Wireless-N 3160 Intel® Wireless-N 3165 Intel® Wireless-N 3160 Intel® Wireless-N 2230 Intel® Wireless-N 2200 Intel® Centrino® Wireless-N 1000 Intel® Centrino® Wireless-N 100 Intel® Centrino® Wireless-N 130 Intel® Centrino® Wireless-N 2200 Intel® Centrino® Wireless-N 135 Intel® Centrino® Wireless-N 105 Intel® Centrino® Advanced-N 6205 Intel® Centrino® Advanced-N 6235 Intel® Centrino® Wireless-N + WiMAX 6150 Intel® Centrino® Advanced-N + WiMAX 6250 Intel® Centrino® Ultimate-N 6300 Intel® Centrino® Advanced-N 6230 Intel® Centrino® Wireless-N 1030 Intel® Centrino® Wireless-N 2230 Intel® Centrino

intel.

CE0336①

Declaration of Conformity

We, **INTEL CORPORATION** 2200, Mission College Blvd.,Santa Clara, California, 95054, USA
declare under our sole responsibility that the product: **Intel® Wireless-AC 9560 rev.D, Intel® Wireless-AC 9560 rev.Q, 8260NGW, 8260D2W, 8260D2W2, 8260D2W2S, 8260D2W2XL, 8260D2W2XLS, 8260D2W2XLSL, 8260D2W2XLSLL, 8260D2W2XLSLLL, 8260D2W2XLSLLLL, 8260D2W2XLSLLLLL, 8260D2W2XLSLLLLLL, 8260D2W2XLSLLLLLLL, 8260D2W2XLSLLLLLLLL, 8260D2W2XLSLLLLLLLLL, 8260D2W2XLSLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL, 8260D2W2XLSL

Back to Contents

Warranty

Product Warranty Information

One-Year Limited Hardware Warranty

Limited Warranty

Intel warrants to the purchaser of the Intel(R) PRO/Wireless 3965ABG 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.