802.11a/b/g/n Dual Band

WELL WCU450AN Dual

User's Manual

WEEE Directive & Product Disposal

At the end of its serviceable life,
this product should not be treated as household or general waste.
It should be handed over to the applicable collection point for
the recycling of electrical and electronics equipment,
or returned to the supplier for disposal.

Table of Contents

Welcome

Thank you for purchasing the IEEE 802.11n Wireless USB Adapter. In addition, Wireless USB Adapter is backward compatible with 802.11a/b/g. When Wireless USB Adapter is connecting to the standard 802.11a,802.11b, 802.11g or 802.11n APs or routers, it can perform much better than other standard stations.
Wireless USB Adapter supports higher data throughput than the IEEE802.11n standard (up to 450Mbps).
For the security of WLAN, Wireless USB Adapter supports 64/128-bit WEP data encryption which protects your wireless network from eavesdropping.
It also supports WPA/WPA2 which combines IEEE802.1x and TKIP technologies. Client users are required to authorize before accessing to APs or routers, and the data transmitted on the network is encrypted and decrypted by a dynamically changed secret key. Wireless USB Adapter supports WPA2 function which provides a stronger encryption through AES which is the most advanced WLAN solution for IEEE802.11i. Besides, Wireless USB Adapter supports WPS function which provides a stronger encryption and easier configuration through WPA2 which is the most advanced WLAN solution for IEEE802.11i.

Package Contents

The Wireless USB Adapter package includes the following.

1. Wireless USB Adapter
2. Quick Installation Guide
3. AUTORUN CD

Wireless USB Adapter Overview

Wireless USB Adapter has the USB interface, LED and WPS button below.

Interface

USB Interface: Connect the USB Interface to a USB slot on your computer.

LED Description

Label	Color	On	Flash	Off
WiFi	Green	Ready	Transmit / Receive Data	WLAN Off
WPS	Green	device connected to encrypted WLAN network	Start WPS pairing within 2 minutes	device connected to unencrypted WLAN network

WPS Button

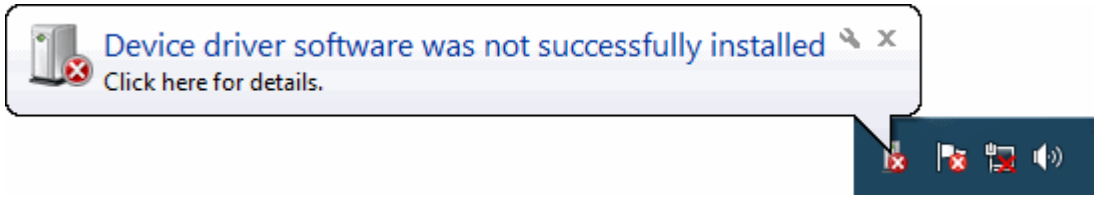
WPS Button: Press this button for 3 seconds to do WPS with AP.

Wireless USB Adapter Installation

The following instructions will guide you to through the process of installing the Wireless USB Adapter.

Windows 7

Step 1:
Once USB Adapter connected to computer and the following will appear on screen.



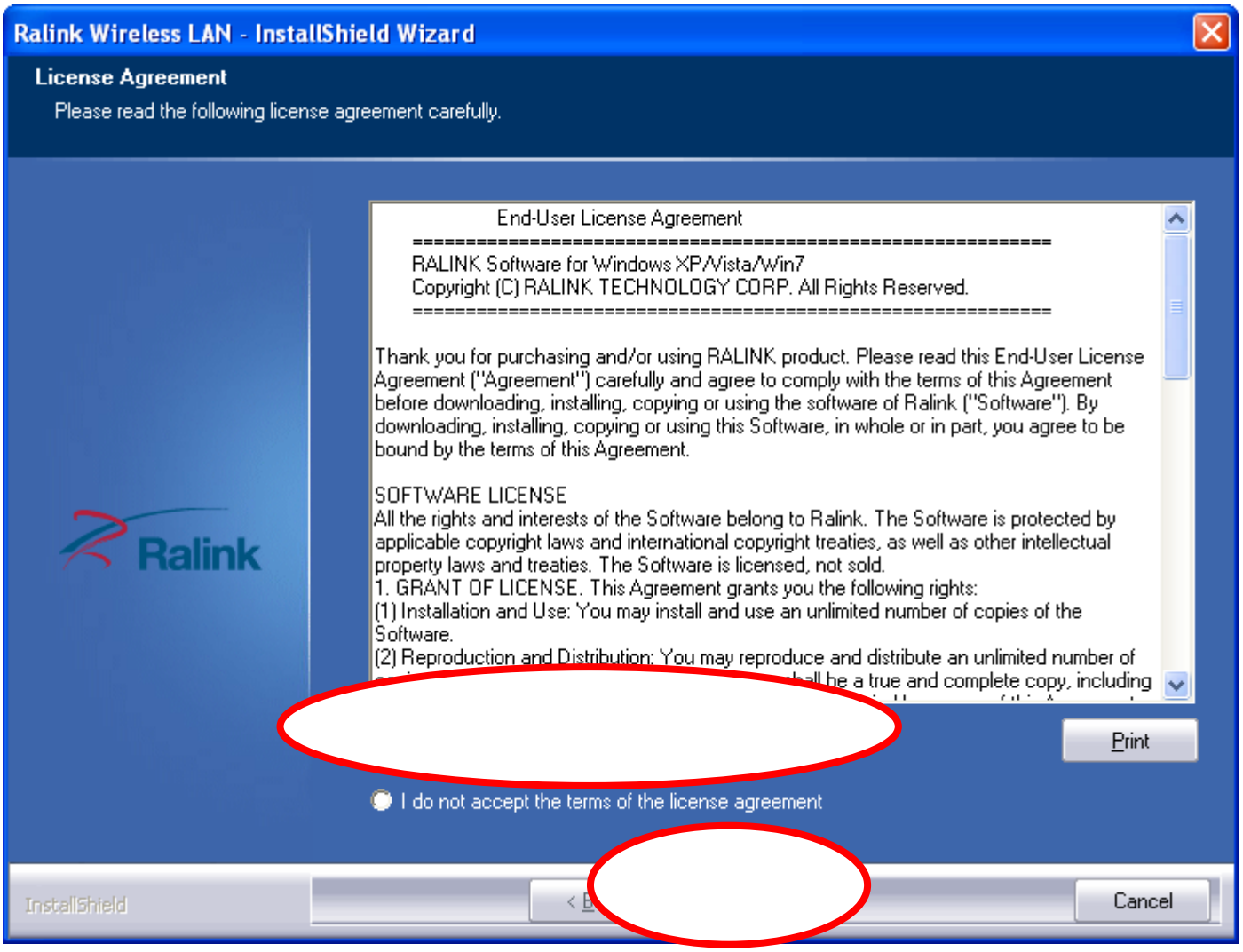
Step 2:
Please insert the AUTORUN CD into your CD-ROM drive.
The CD should auto-start, displaying the following window. If it does not start, click on **Start – Run** and type in **CD: \autorun.exe** (where CD is the drive letter of your CD-ROM drive.) Click **" Driver Installation "**.

Step 3:

For Security reasons Windows 7 requires the installer program to have administrator privileges so the new policy called **" User Account Control "** has been introduced in Windows 7. If UAC is enabled Windows pops up a window **" User Account Control "** Windows need your permission to continue. User needs to Click **" Yes "** to proceed with the installation.

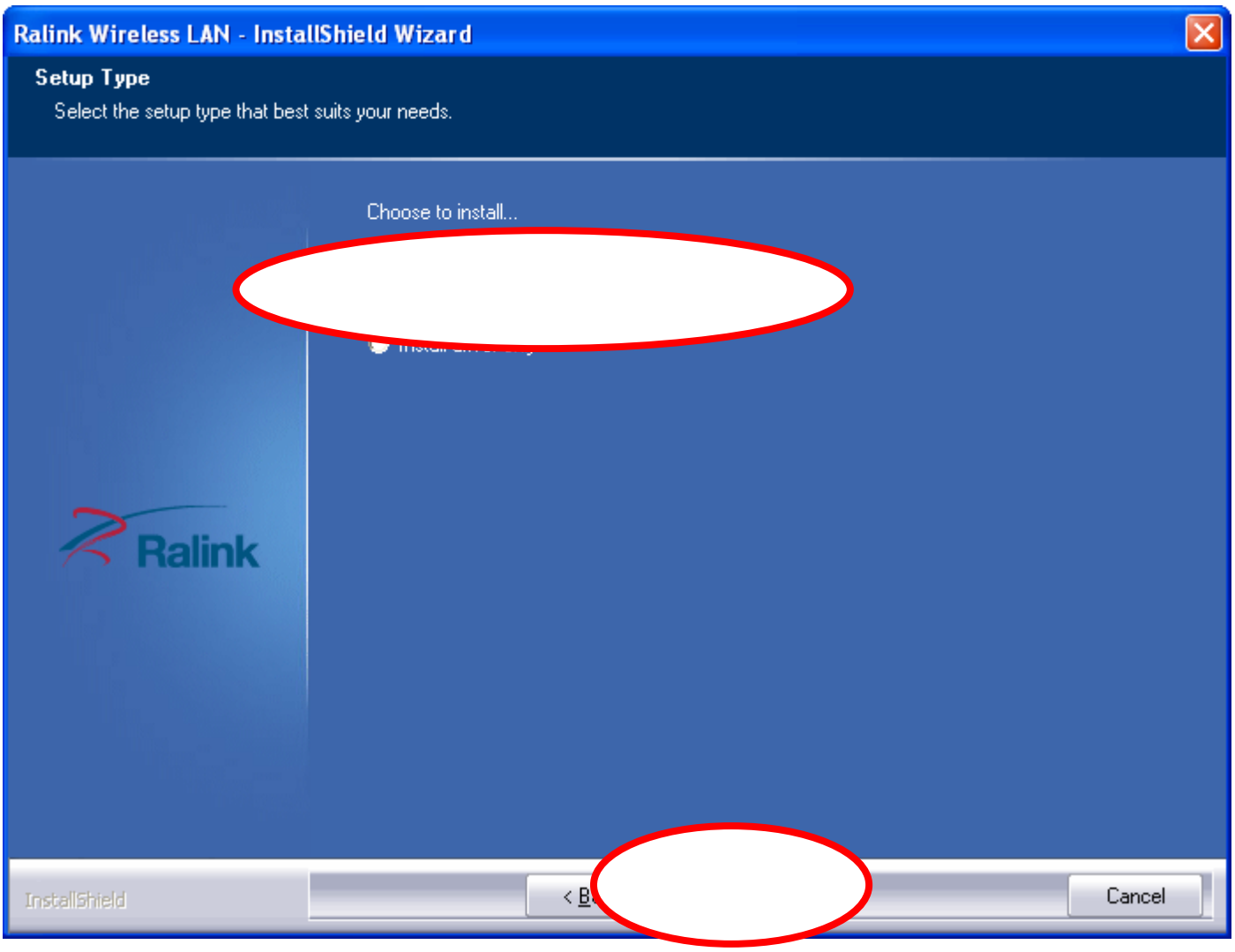
Step 4:

Click **" I accept the terms of the license agreement "** and then click **" Next "**



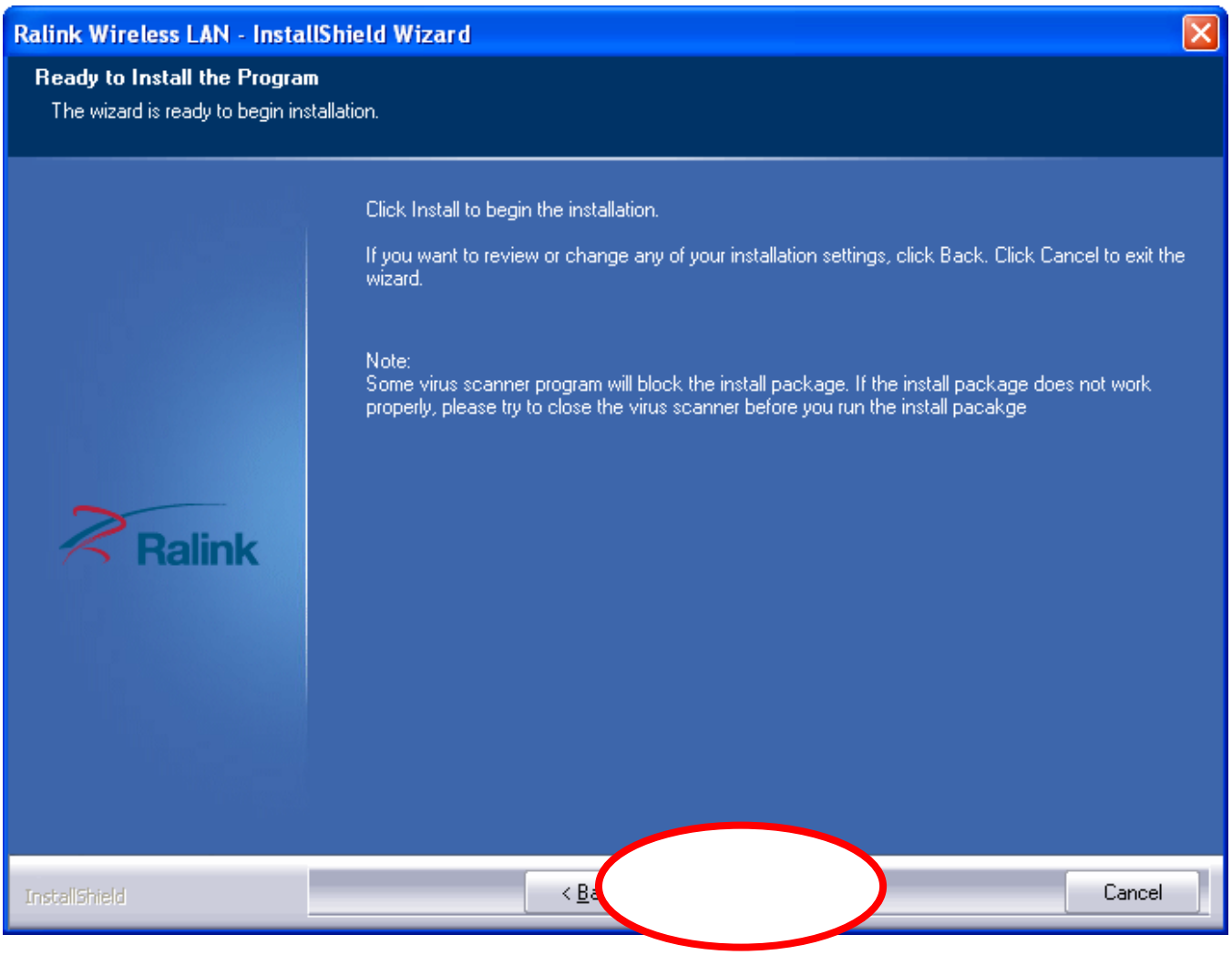
Step 5:

Click **" Install driver and Ralink WLAN Utility "** and then click **" Next "**



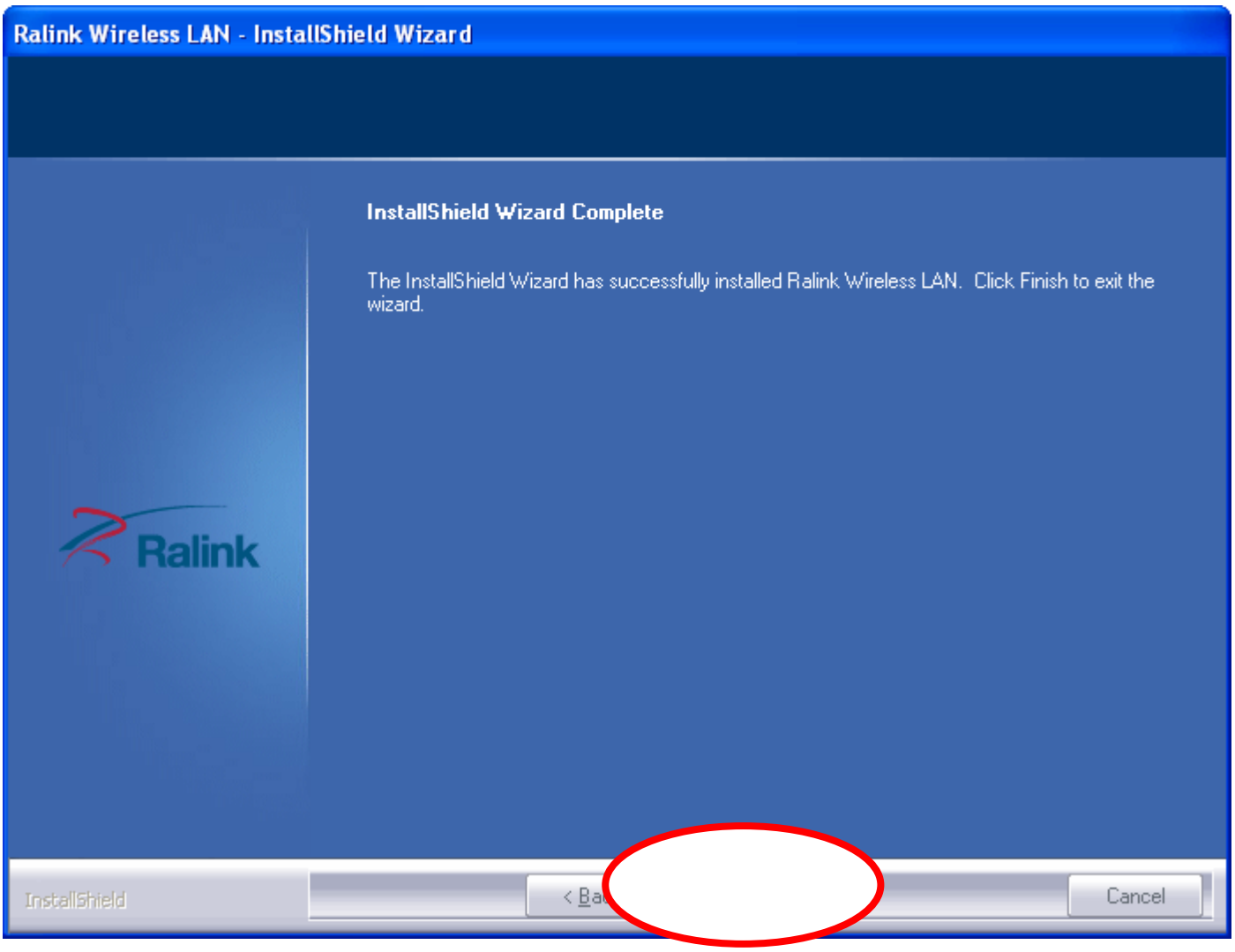
Step 6:

Click **" Install "**.



Step 7:

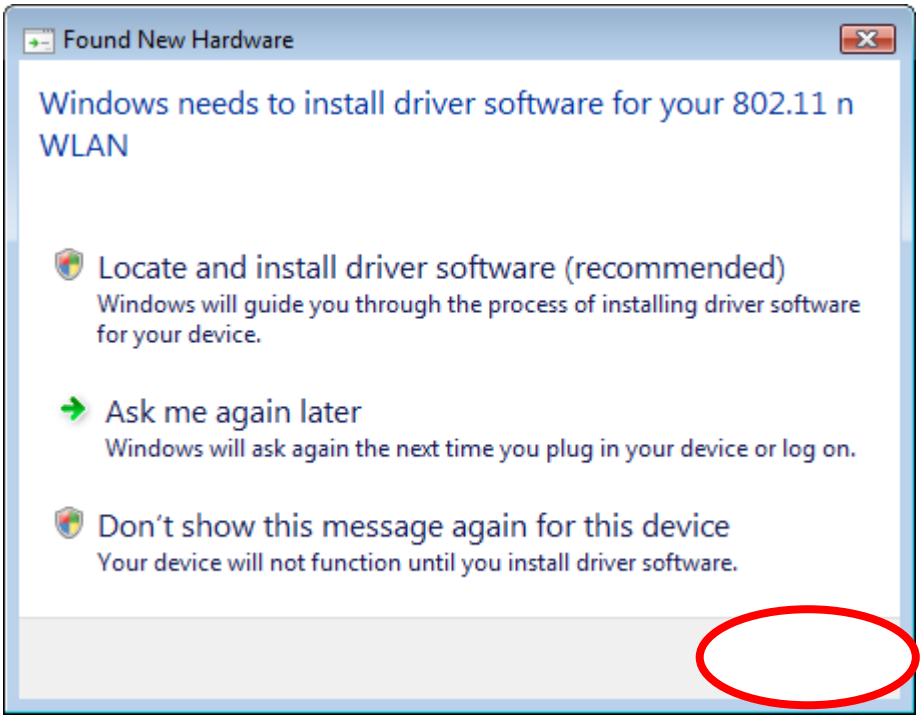
Click **" Finish "**.



Windows Vista

Step 1:

As Windows starts it will detect that new hardware has been added, and start the **" Found New Hardware Wizard "**. Click on **" Cancel "**.



Step 2:

Please insert the AUTORUN CD into your CD-ROM drive.

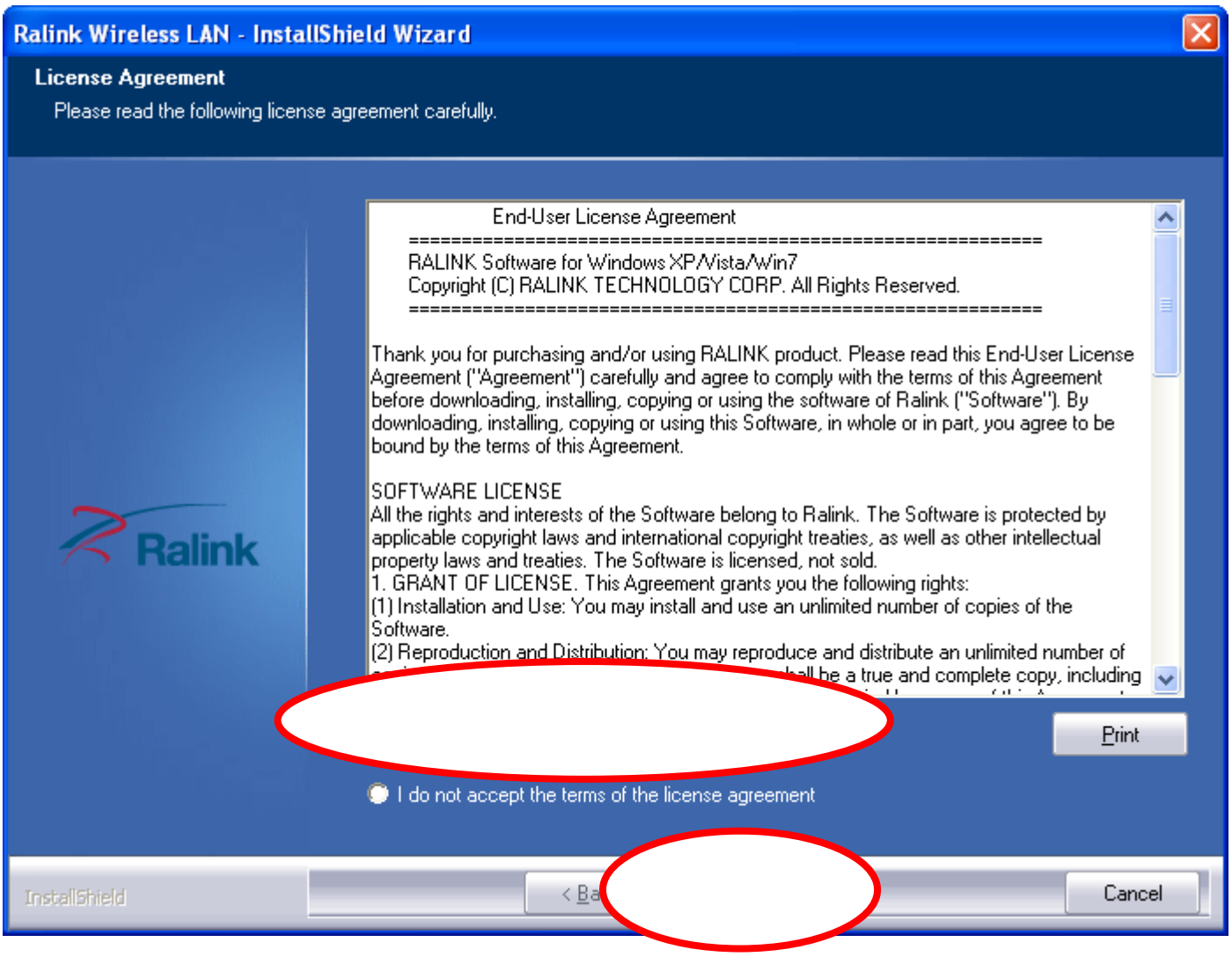
The CD should auto-start, displaying the following window. If it does not start, click on **Start – Run** and type in **CD: \autorun.exe** (where CD is the drive letter of your CD-ROM drive.) Click **" Driver Installation "**.

Step 3:

For Security reasons VISTA requires the installer program to have administrator privileges so the new policy called **" User Account Control "** has been introduced in Windows VISTA. If UAC is enabled Windows pops up a window **" User Account Control "** Windows need your permission to continue. User needs to Click **" Allow "** to proceed with the installation.

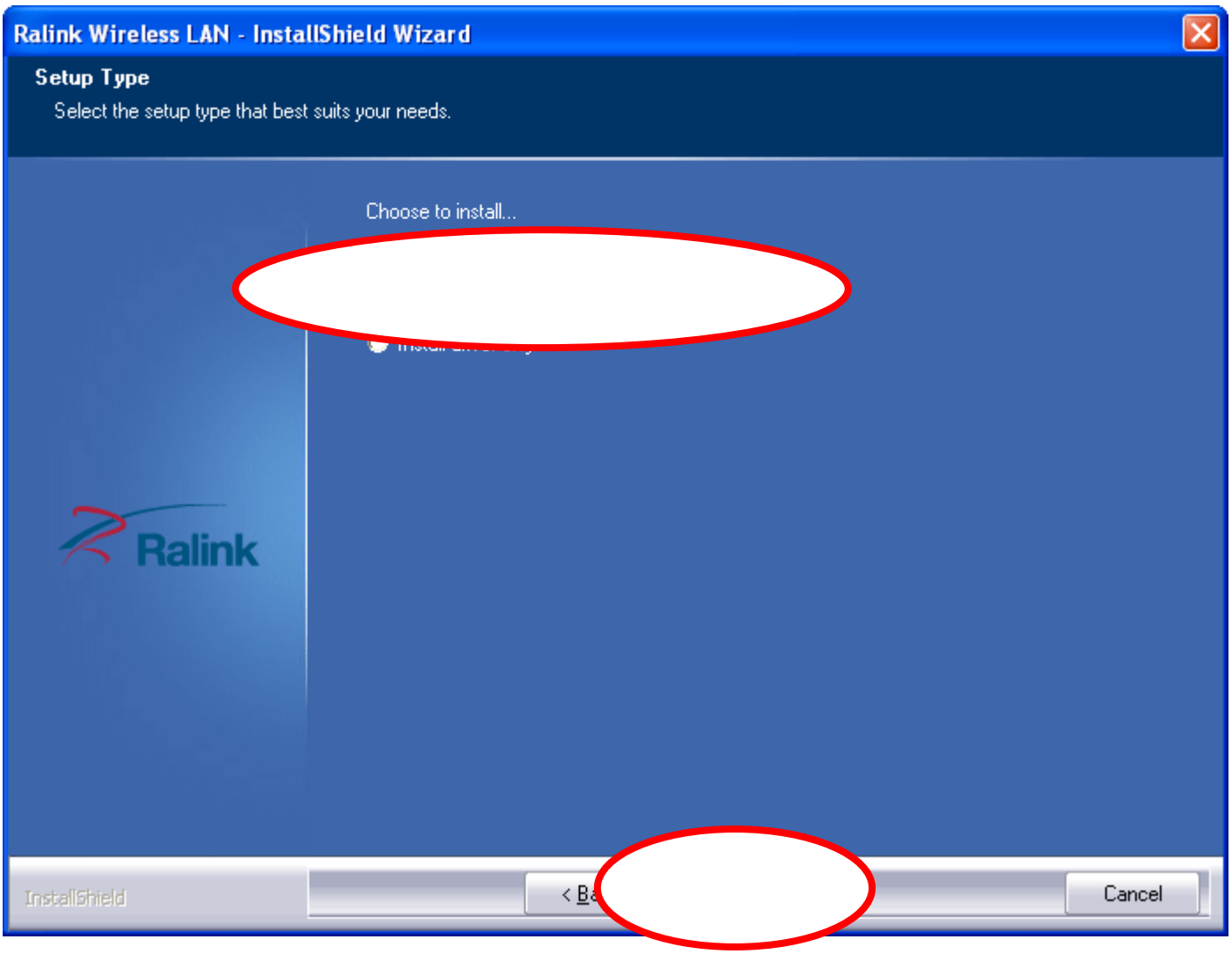
Step 4:

Click **" I accept the terms of the license agreement "** and then click **" Next "**



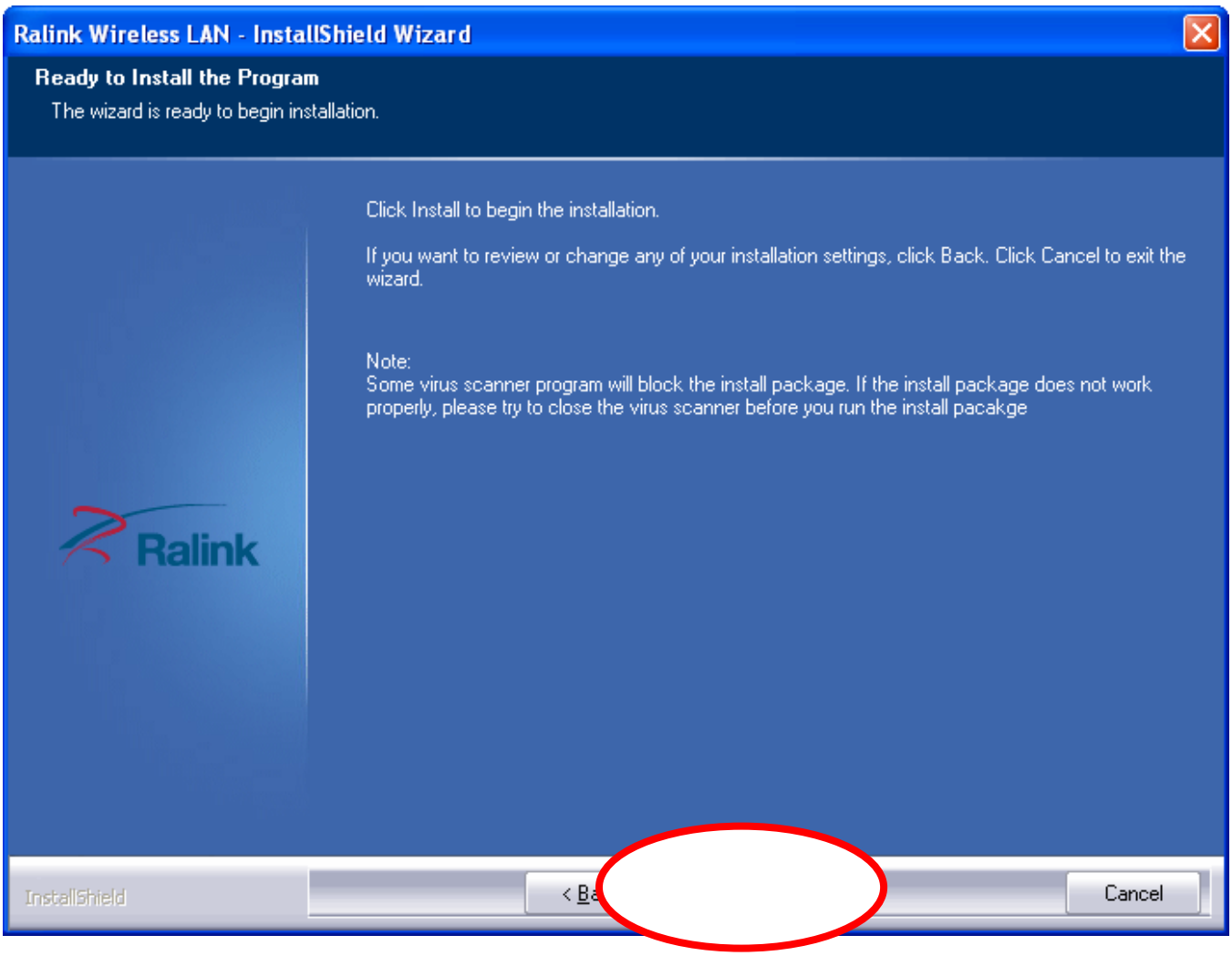
Step 5:

Click **" Install driver and Ralink WLAN Utility "** and then click **" Next "**



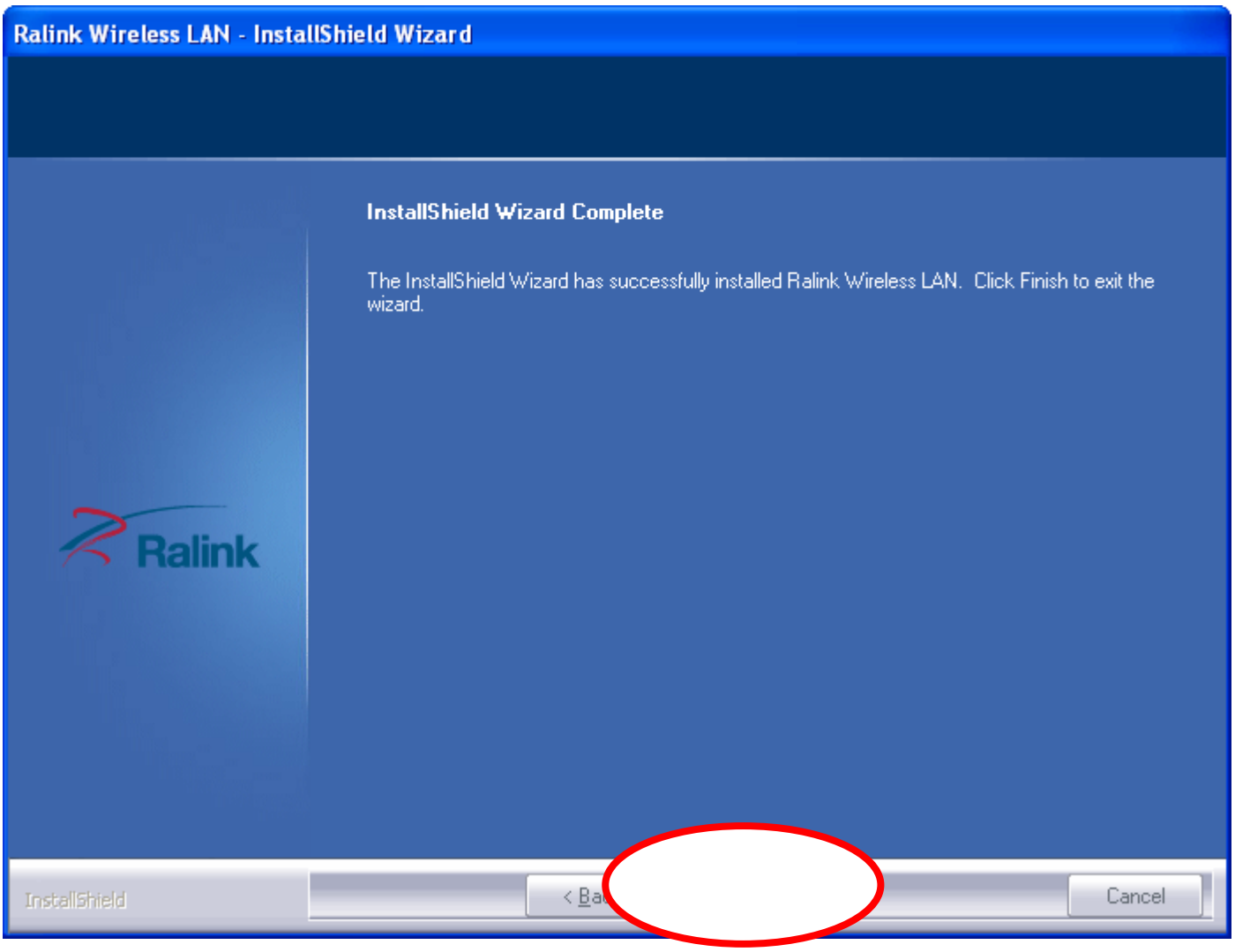
Step 6:

Click **" Install "**.



Step 7:

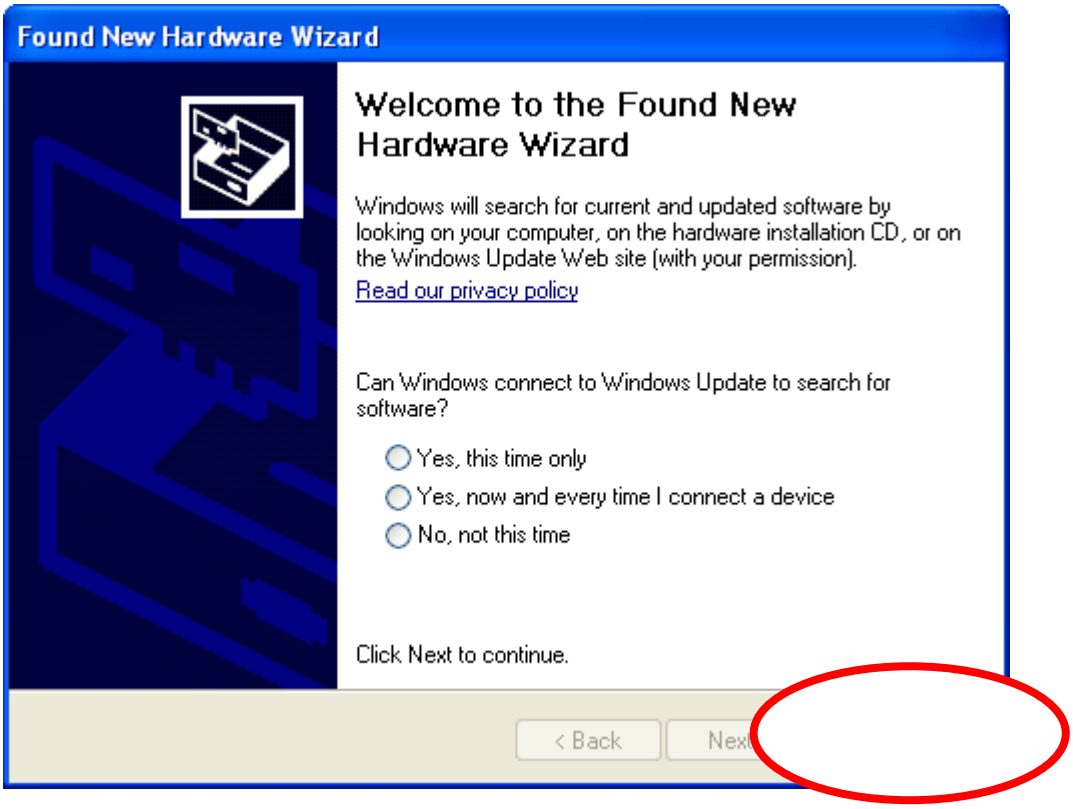
Click **" Finish "**.



Windows XP

Step 1:

As Windows starts it will detect that new hardware has been added, and start the **" Found New Hardware Wizard "**. Click on **" Cancel "**.



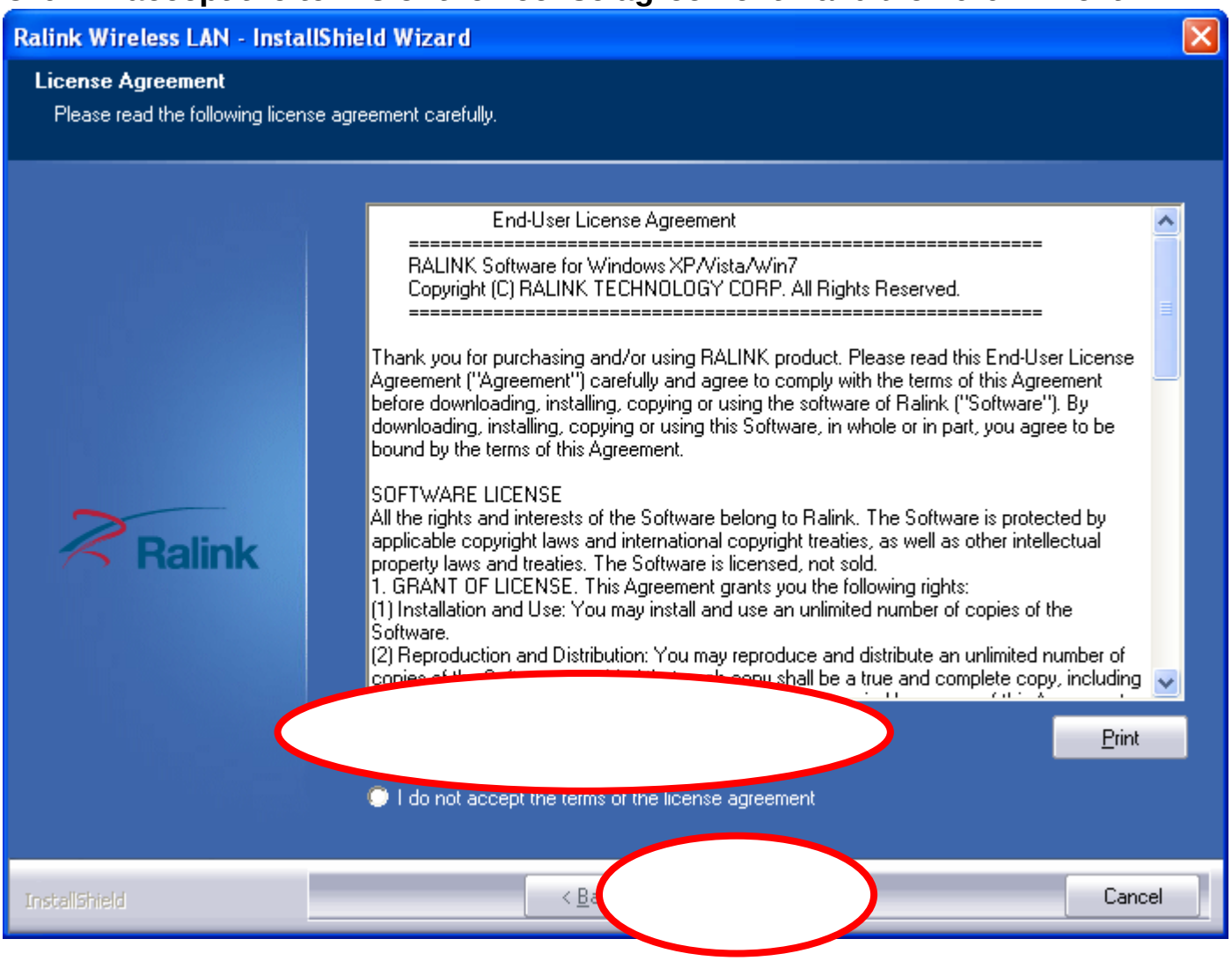
Step 2:

Please insert the AUTORUN CD into your CD-ROM drive.

The CD should auto-start, displaying the following window. If it does not start, click on **Start – Run** and type in **CD: \autorun.exe** (where CD is the drive letter of your CD-ROM drive.) Click **" Driver Installation "**.

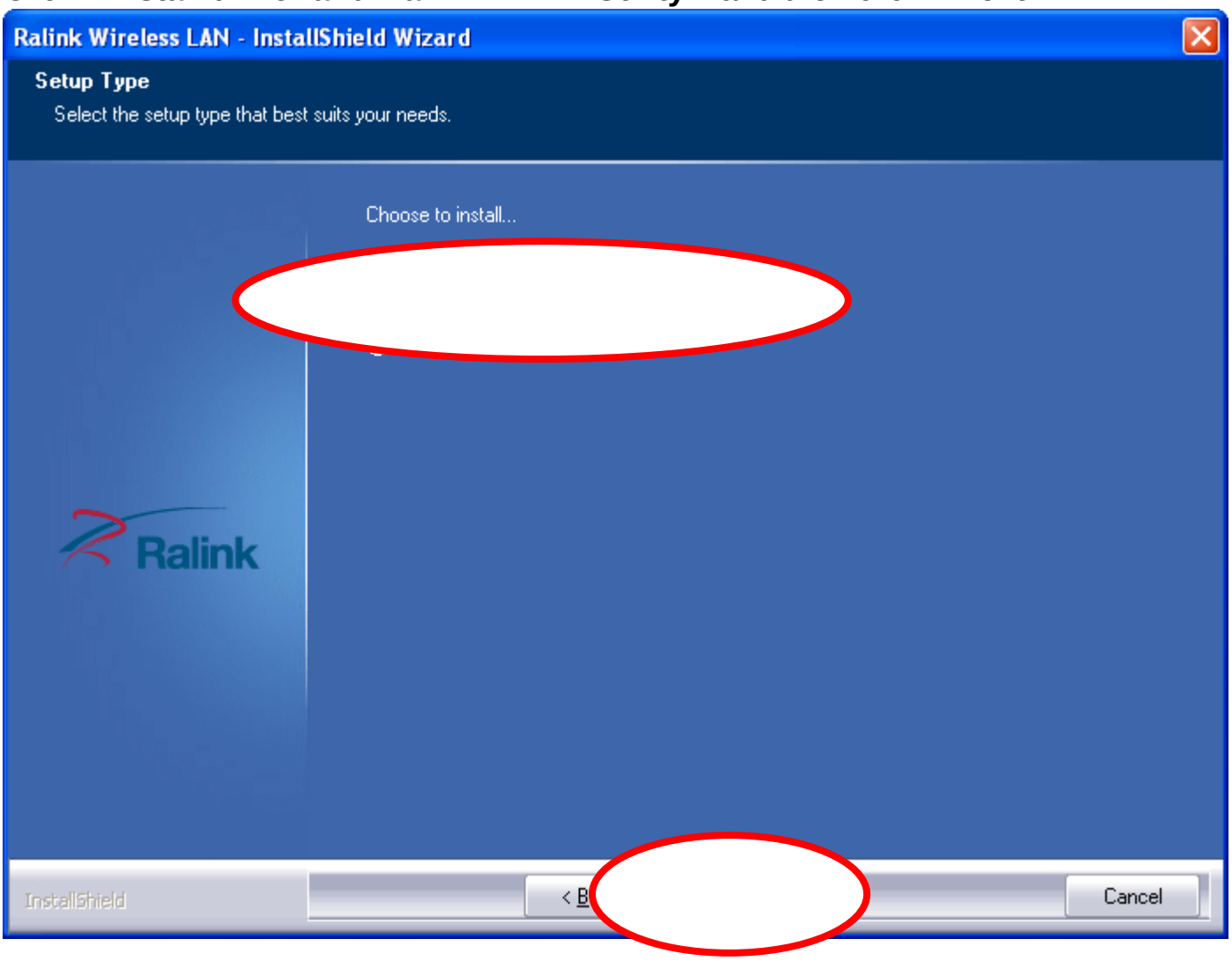
Step 3:

Click **" I accept the terms of the license agreement "** and then click **" Next "**



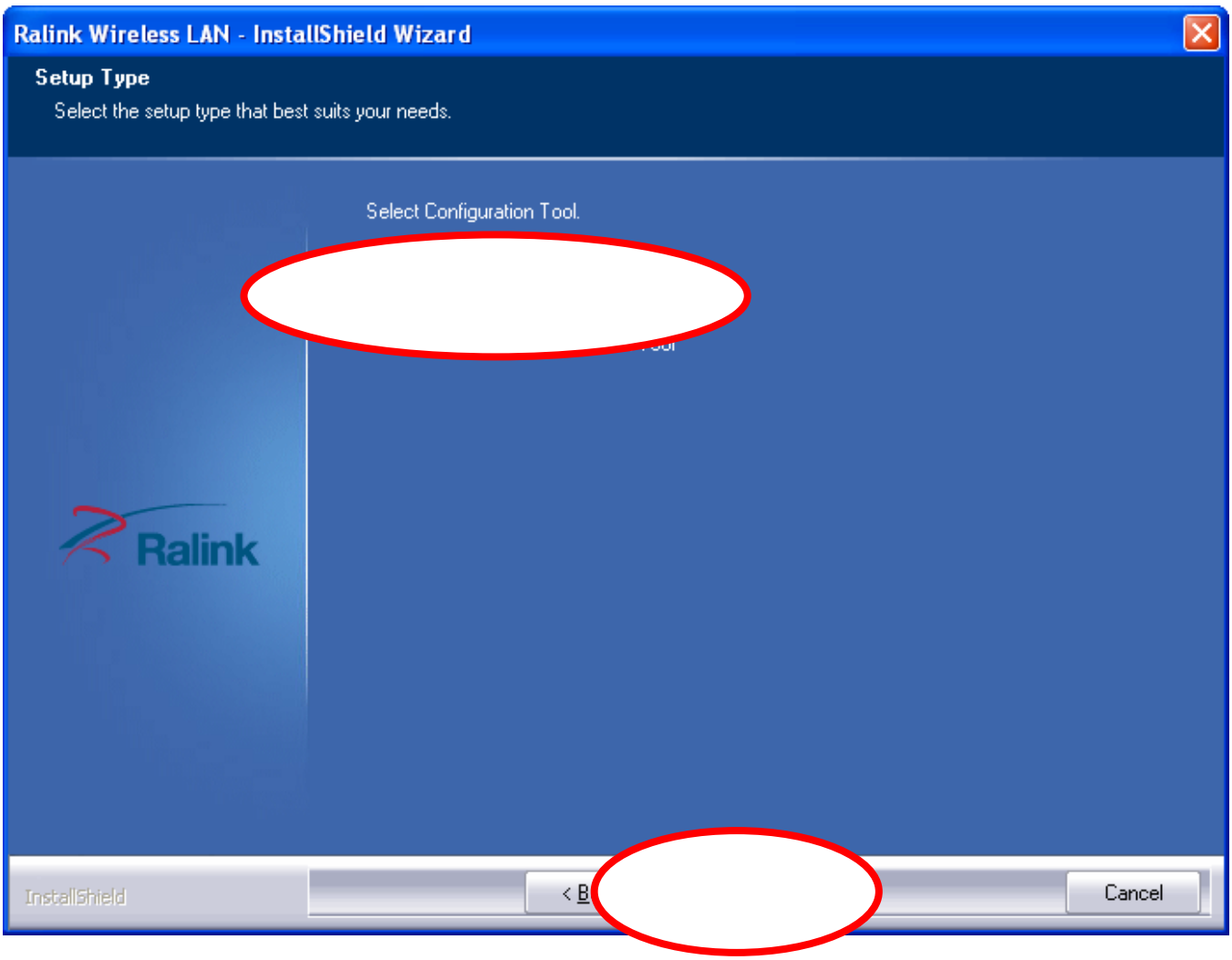
Step 4:

Click **" Install driver and Ralink WLAN Utility "** and then click **" Next "**



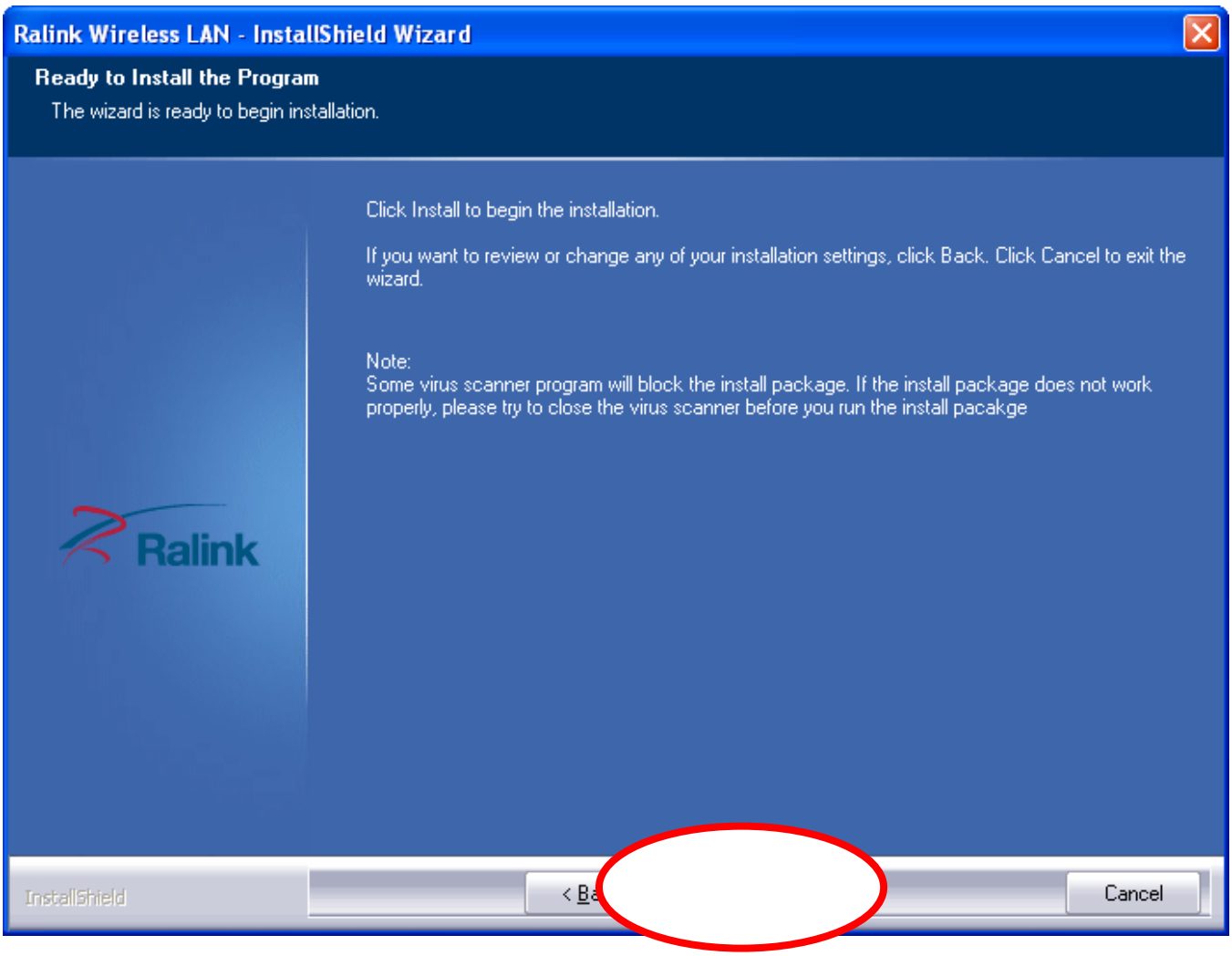
Step 5:

Click **" Ralink Configuration Tool "** and then click **" Next "**



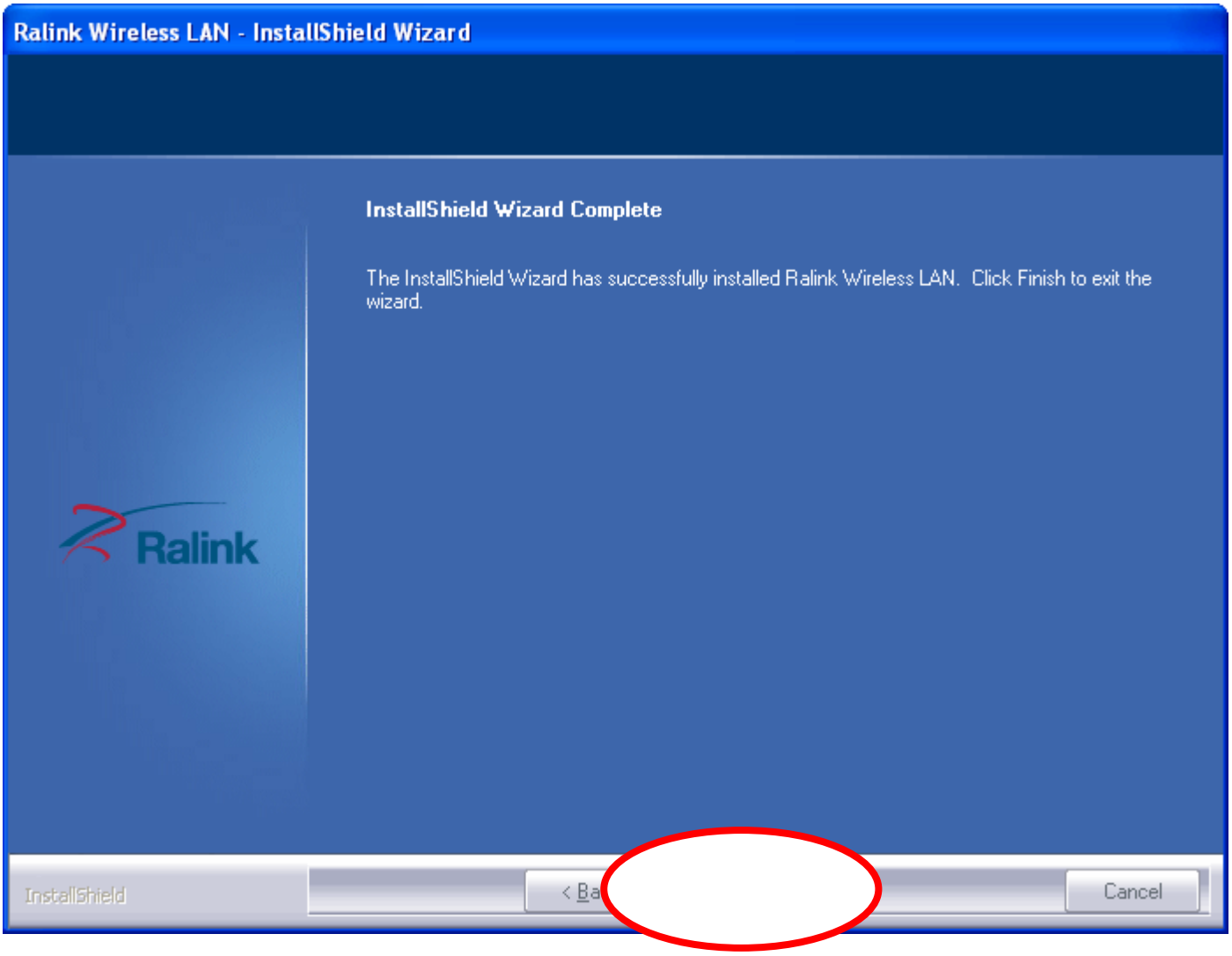
Step 6:

Click **" Install "**.



Step 7:

Click **" Finish "**.



Making a Basic Wireless Network Connection

For Windows XP/Vista/7 users, your native Windows XP/Vista/7 wireless support (Wireless Zero Configuration Service) has been disabled by default.

Infrastructure mode

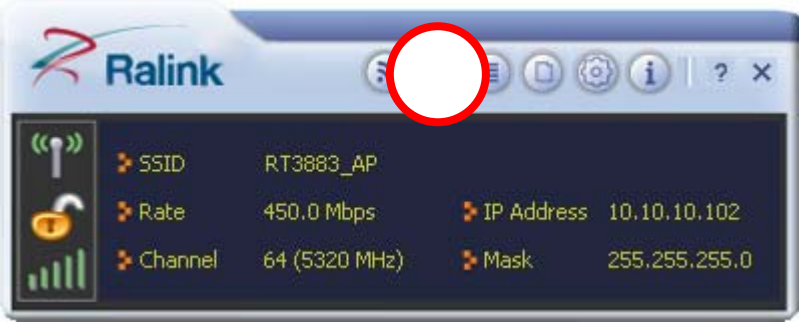
An Infrastructure Mode network contains at least one wireless client and one wireless AP or router. This client connects to Internet or intranet by communicating with this wireless AP or router.

Step 1:

Double click the  icon in the task bar to start the utility.

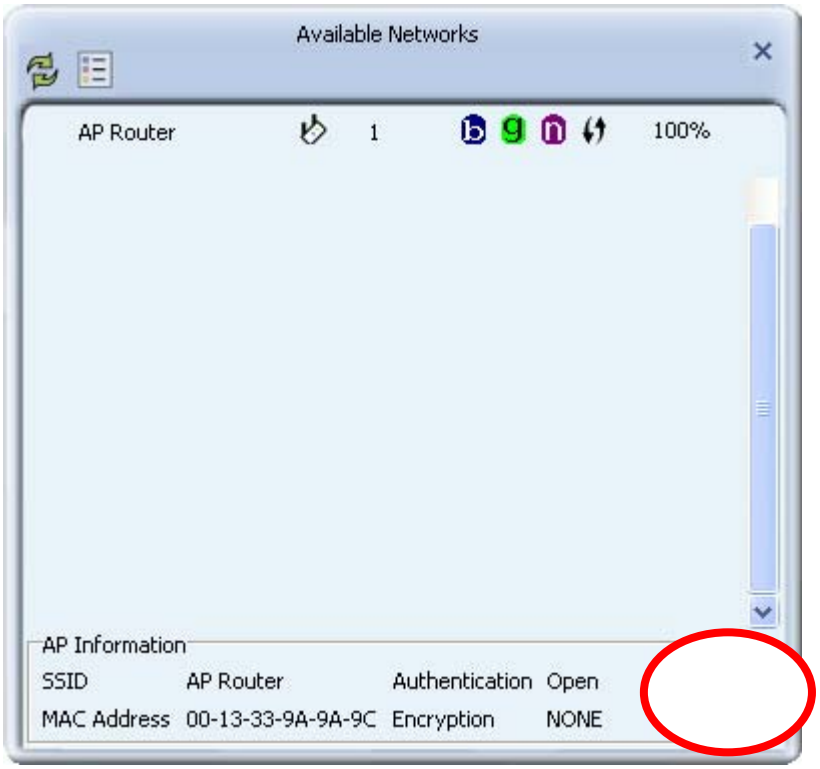
Step 2:
The Utility appears, by default connected to an available open wireless network. Check the name of the network to which you are connected. If this is the correct network, no further steps are required.

Step 3:
To connect to an alternative network, click the **Available Networks** button.



Step 4:

In the Available Networks window that appears, select the name of the network to which you are connecting. Then click the connect icon and wait several seconds while the Utility sets up a connection.

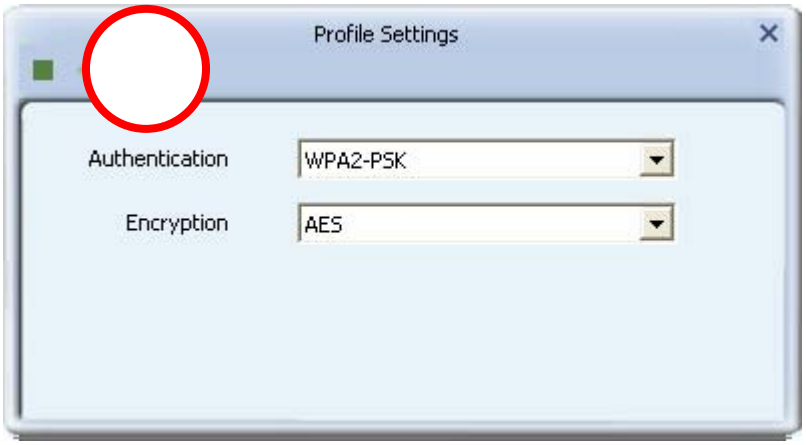


Step 5:

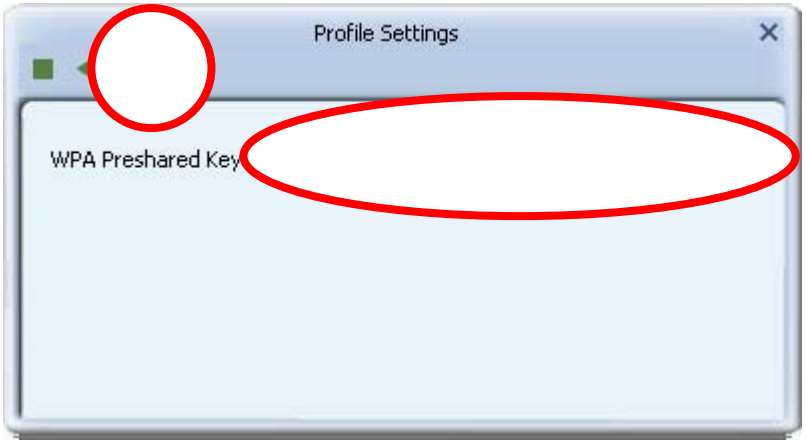
The Utility automatically detects and displays the security settings of the network to which you are connecting in the Profile Settings screens. For instructions on setting up security, click on the security method (WPA-PSK or WPA2-PSK, WEP, 802.1X, WPA, or WPA2 WAPI-PSK, WAPI-CA, No Security) detected for your network.

WPA-PSK or WPA2-PSK

a. If the Utility shows that WPA-PSK or WPA2-PSK security is detected, click the right arrow to save your settings.

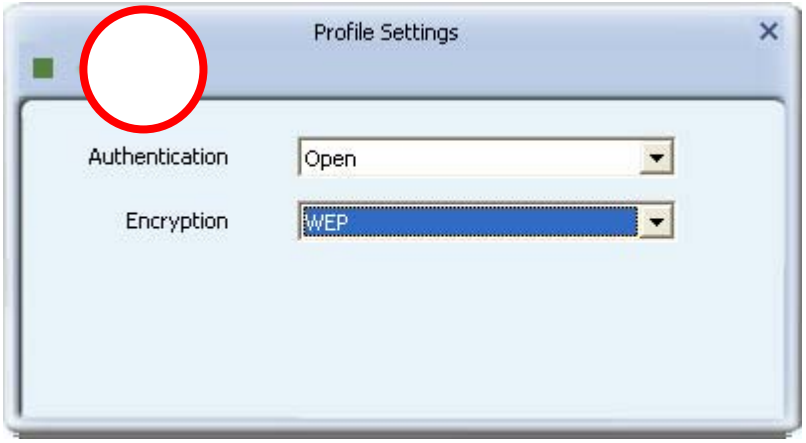


b. In the screen that displays, in the 'WPA Preshared Key' field, type a security key, the same as that used by the AP or wireless router to which you are connecting. Click the right arrow to save your settings and connect to the network.

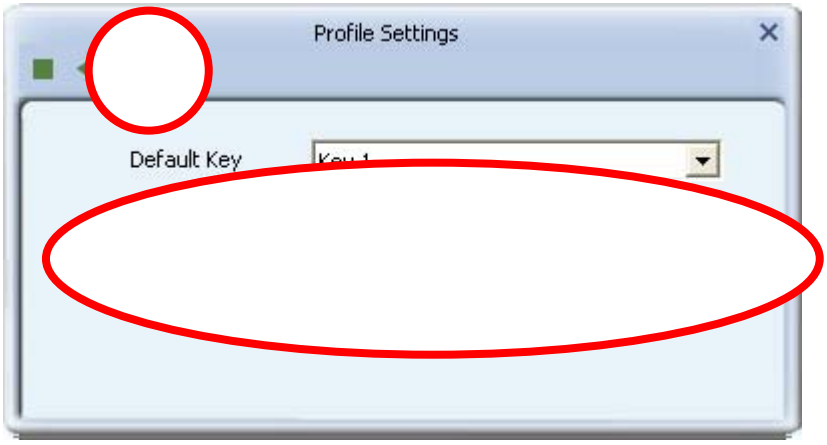


WEP

a. If the Utility shows that WEP security is detected, click the right arrow to save your settings.

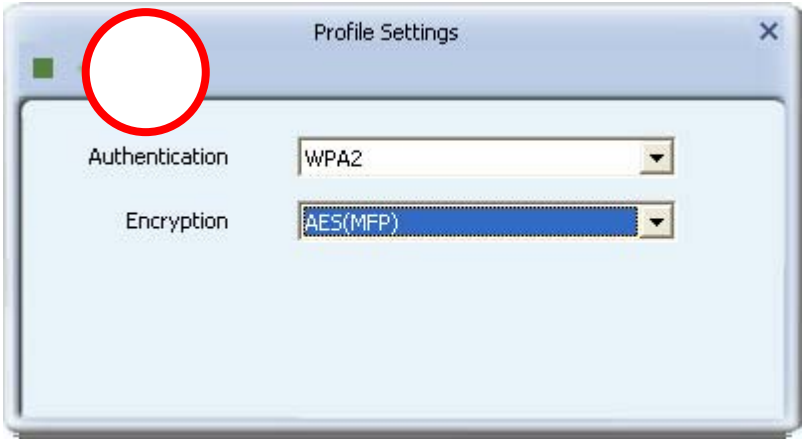


b. In the 'WEP Key' field, type the same WEP key as that configured on the AP or wireless router to which you are connecting, and ensure that 'Default Tx Key' and 'Key Format' settings are also the same. Click the right arrow to save your settings and connect to the network.

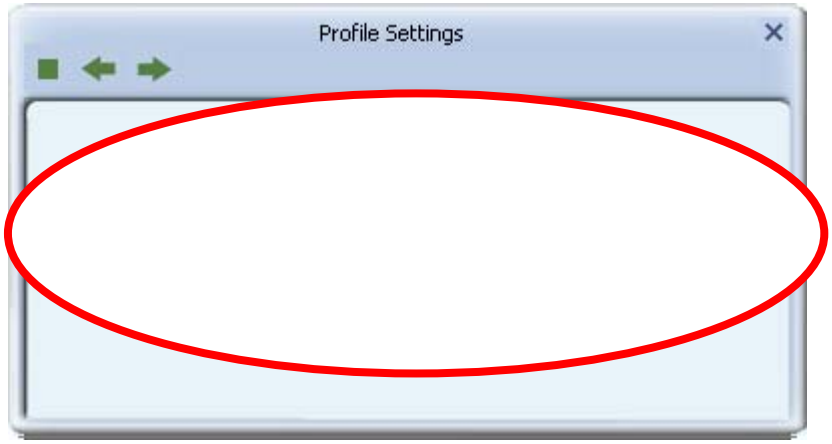


802.1X, WPA, or WPA2

a. If the Utility shows that 802.1x, WPA, or WPA2 security is detected, click the right arrow to save your settings.

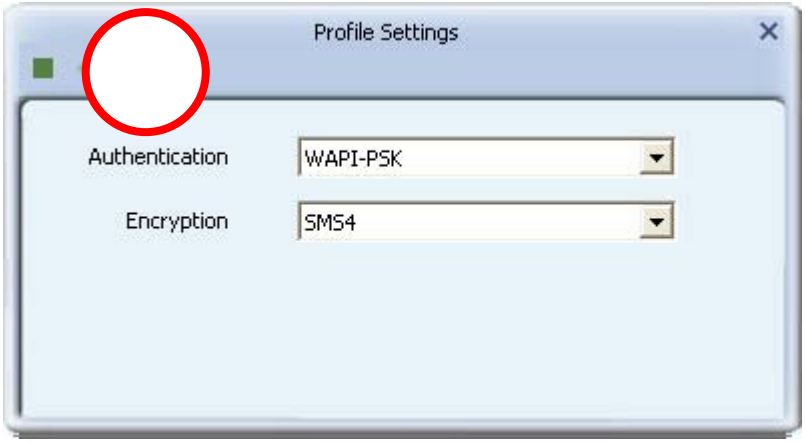


b. Select the EAP Method (Extensible Authentication Protocol) and Tunnel Authentication method, and if required, the Tunnel ID method and Tunnel Mode, and enter the user name and password, using the settings provided by your organization's network administrator. For more information on settings for these fields and for those in the screens that follow, see Setting Up Enterprise Security. Click the right arrow to save your settings.

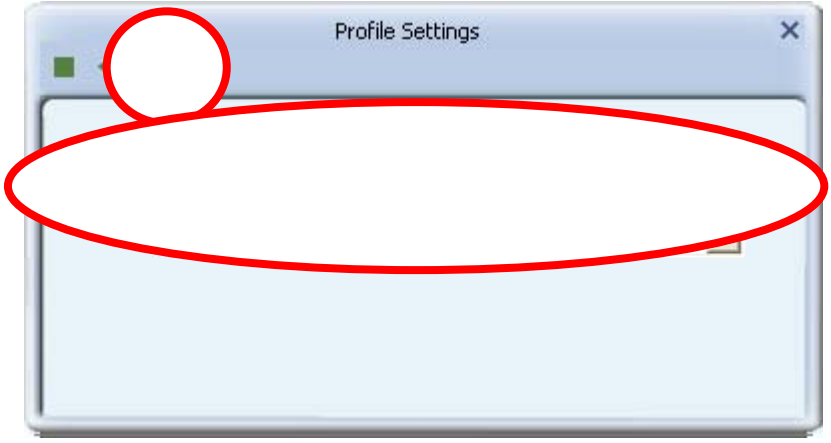


WAPI-PSK

a. If the Utility shows that WAPI-PSK security is detected, click the right arrow to save your settings.

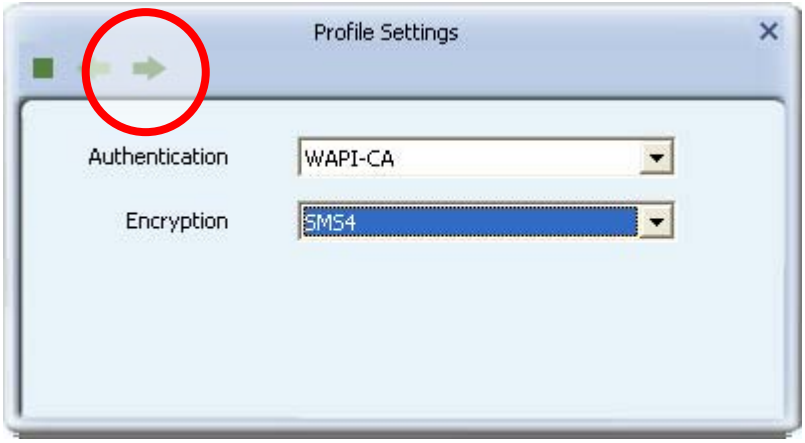


b. In the 'WPA Preshared Key' field, type a security key, and select a Key Format setting, the same as that used by the AP or wireless router to which you are connecting. Click the right arrow to save your settings and connect to the network.

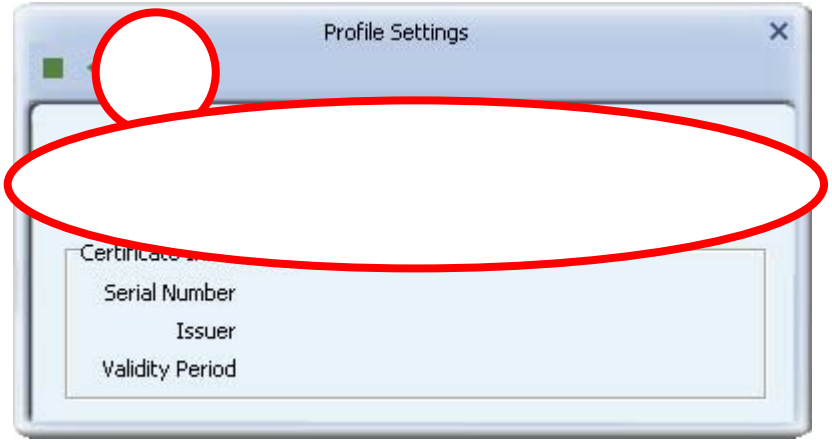


WAPI-CA

a. If the Utility shows that WAPI-CA security is detected, click the right arrow to save your settings.

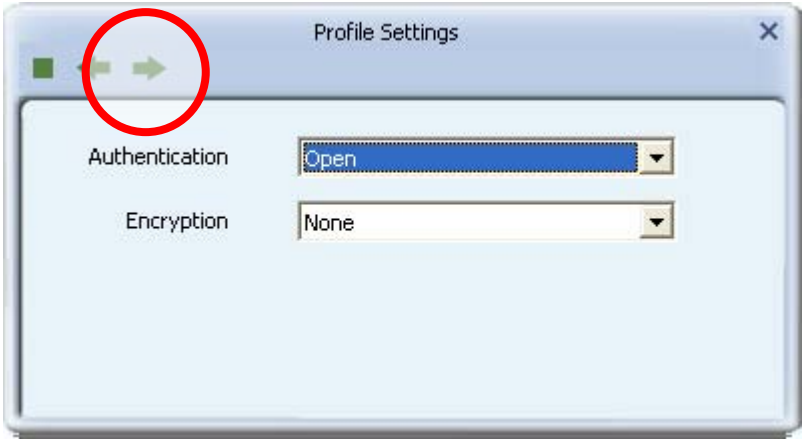


b. If you have a WAPI certificate already installed, in the Select Mode field, select Auto and click the right arrow to save your settings and connect to the network. Otherwise, if there is no WAPI certificate in your system, go to Setting Up Enterprise Wireless Security: Setting Up WAPI-CA for information on installing a WAPI certificate.



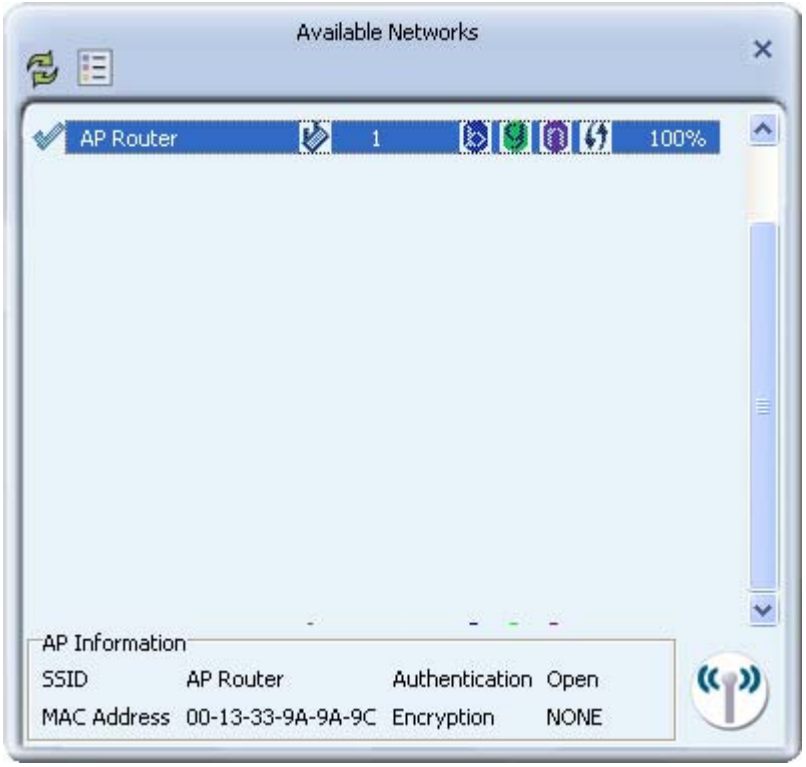
No Security

If your network has no security (not recommended), no further settings are required. Click the right arrow to save your settings and connect to the network.



Step 6:

Now you are ready to use the Wireless Network to Internet or intranet.



Connecting to a Wireless Network Using WPS

WPS (Wi-Fi Protected Setup) is the simplest and most secure way to connect to a wireless network. WPS is a wireless security method aimed at combining strong WPA or WPA2 security with a simple setup procedure. If the AP or wireless router to which you are connecting shows the WPS logo (shown below), you can set up a wireless connection simply and securely using WPS.

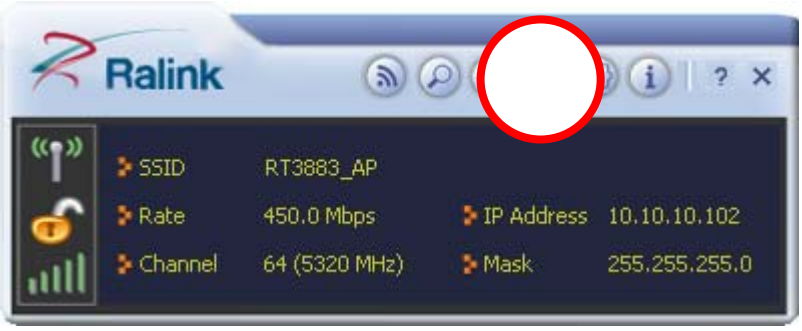
You can apply WPS in two ways.
The Push-Button (PBC) method: (Recommended) The device to which you are connecting must have a WPS button available on its external casing or as part of its software interface.
The PIN (personal identification number) method: Use this method if the device to which you are connecting has no WPS button.

Instructions

Follow these instructions to set up a WPS connection using either a push-button or a PIN.

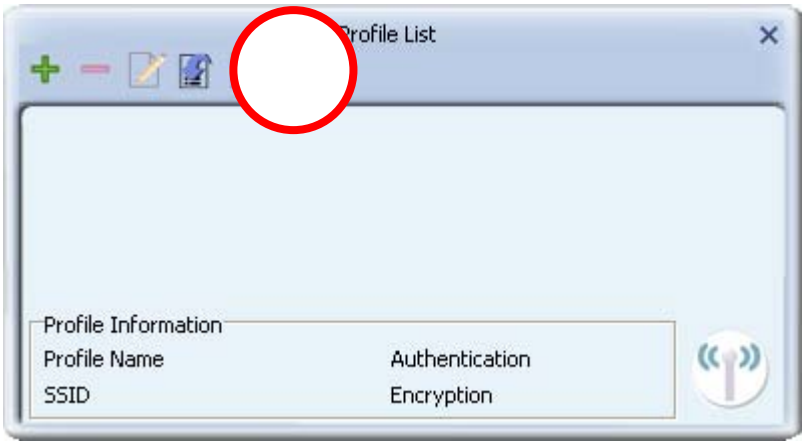
Step 1:

Click the Profile Settings button in the Ralink Utility.



Step 2:

The Profile List screen displays. In this screen, click the WPS button .



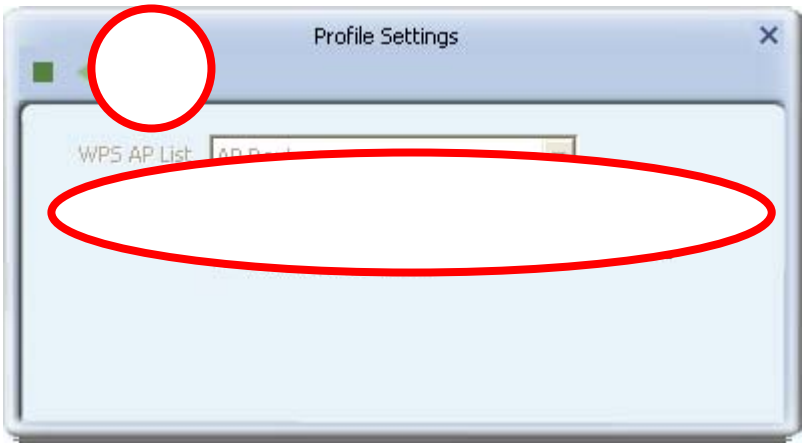
Step 3:
Select your WPS method.

a. If the device to which you are connecting has a WPS push button, either on the casing or in the device's software interface, follow the instructions for the PBC method.

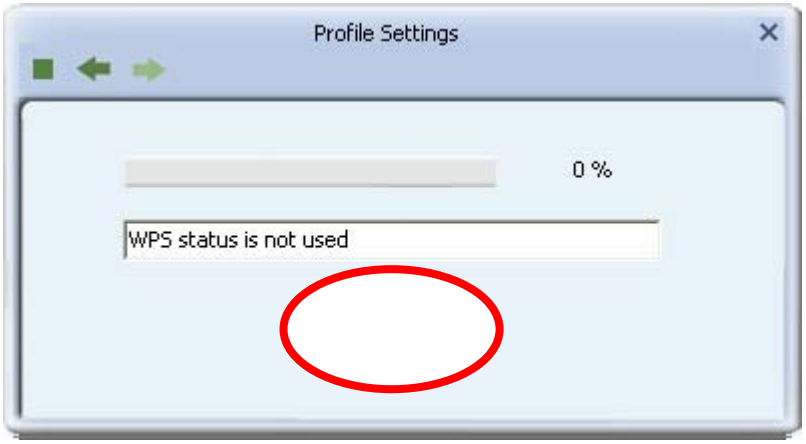
b. If the device to which you are connecting has no WPS push button, follow the instructions for the PIN method.

The PBC Methods

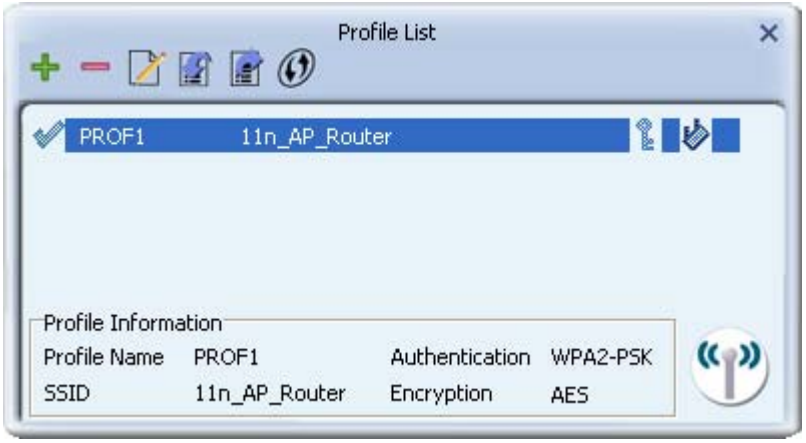
a. To use the PBC method, select **Push-Button Configuration(PBC)**. Click the right arrow to save your settings.



b. Click **Start PBC**. At the same time (within 120 seconds) click the WPS button on the device to which you are connecting.

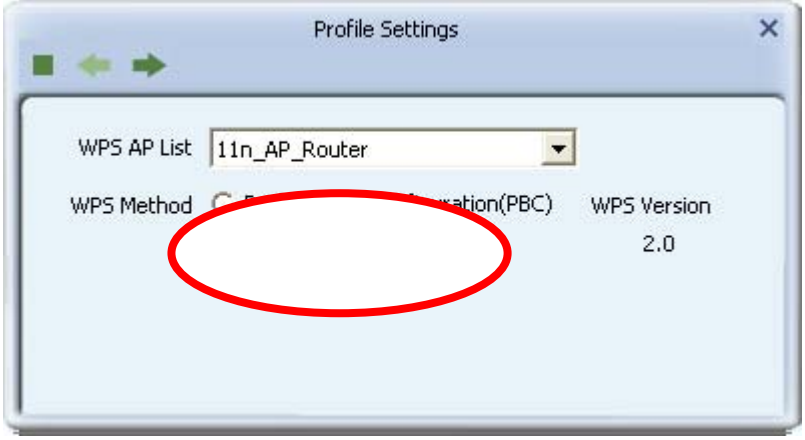


c. Once connected, your WPS profile appears in the Profile List screen.



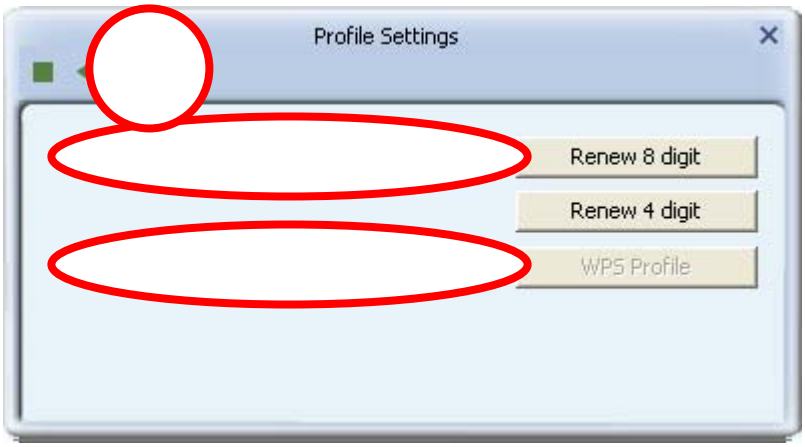
The PIN Method

a. To use the PIN method, select **PIN / numeric code** and, in the **WPS AP List** field, select the name of the network to which you connecting. Click the right arrow to save your settings.



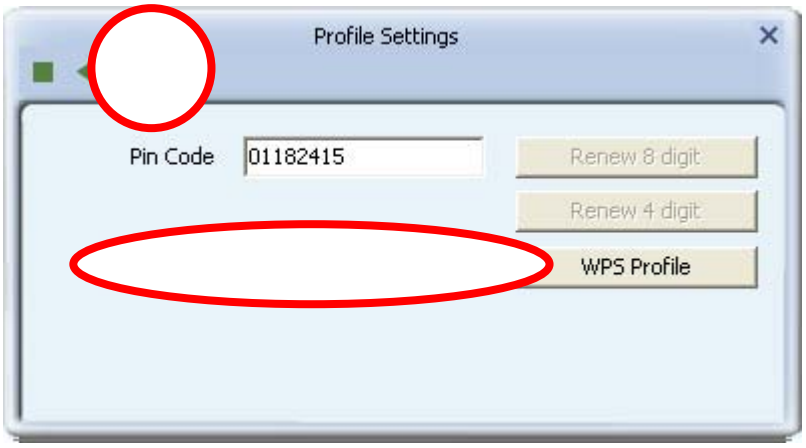
b. You can use either the PIN provided by the Ralink Utility or the PIN provided by the device to which you are connecting.

PIN provided by the Ralink Utility.
If the device to which you are connecting requires a PIN, in the **Config Mode** field, from the drop-down list, select **Enrollee**. Your PIN is displayed in the **Pin Code** field on your Utility. Then in the corresponding WPS interface on the device to which you are connecting, enter your PIN in its PIN entry field. Click the right arrow to save your settings.

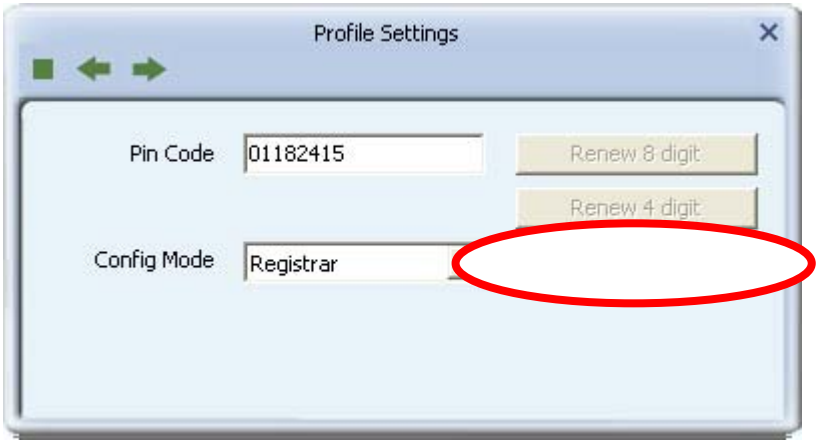


PIN provided by the device to which you connecting.

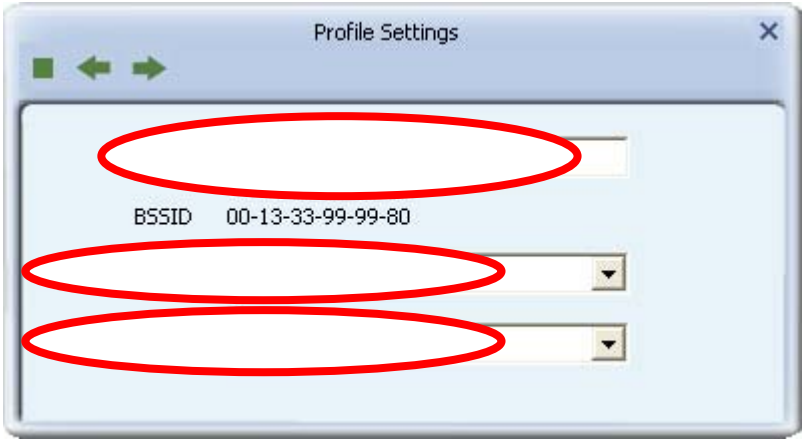
If the device to which you are connecting provides a PIN (e.g. on the device casing), in the **Config Mode** field, select **Registrar**. In the **PIN Code** field, type the PIN provided by the device to which you are connecting. Click the right arrow to save your settings.



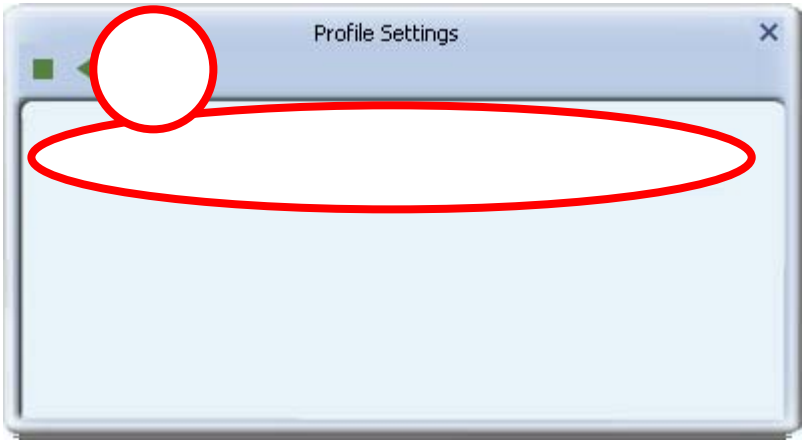
To optionally configure the connection name and security type on your WPS connection, click the **WPS Profile** button. Otherwise leave settings at their default and click the right arrow to save your settings.



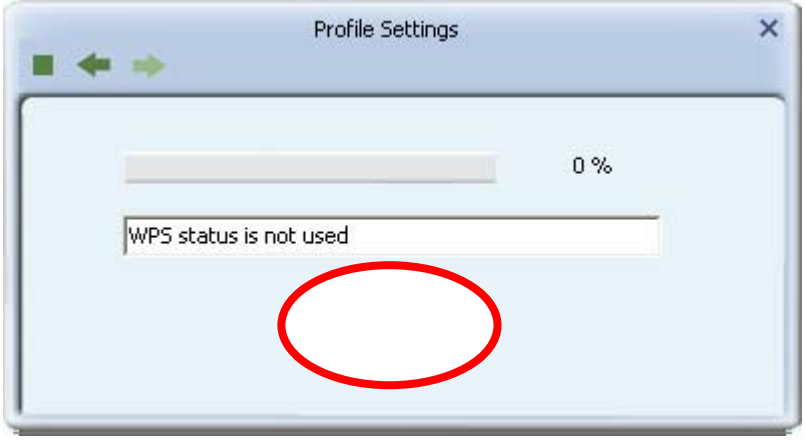
If you click on the **WPS Profile** button, the following screen appears, allowing you to configure the name of your network connection and security method. In **SSID** type a name for your WPS connection, and select an Authentication and Encryption method.



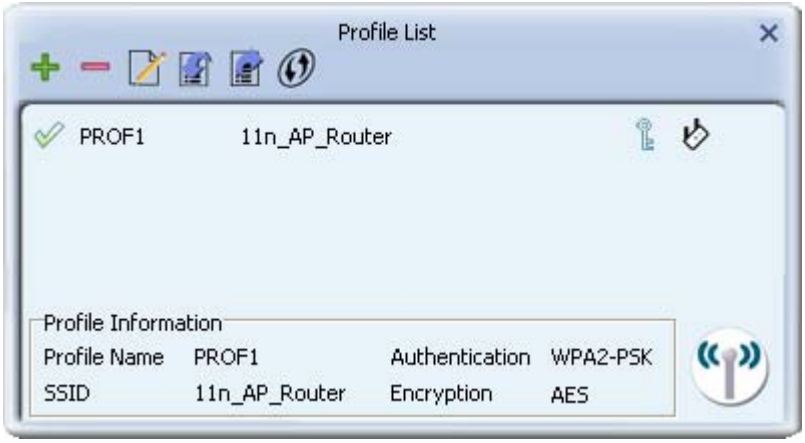
In the **WPA Preshared Key** field, type a passphrase 8-63 characters long made up of characters **0**-**9**, **a**-**z**, **A**-**Z**, keyboard symbols and spaces. Click the right arrow to save your settings.



c. For both PIN methods, the following screen displays. Click the **Start PIN** button. At the same time (within 120 seconds) activate the corresponding WPS PIN connection function on the device to which you are connecting.



d. Once connected, your WPS profile appears in the Profile List screen.



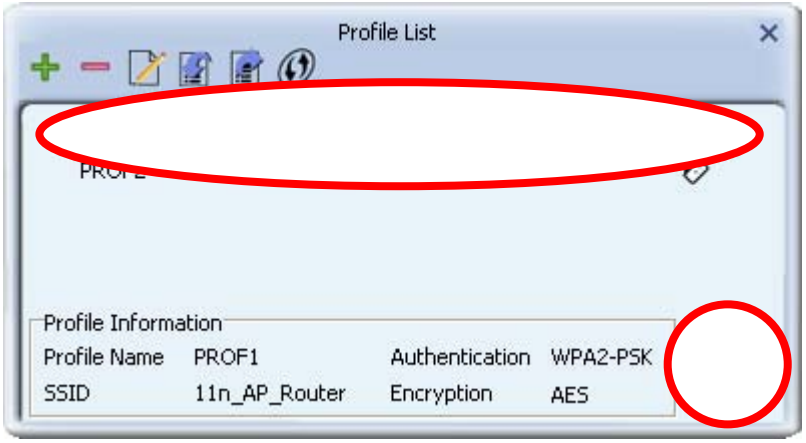
Connecting Using a Profile

You can also use a profile to connect to frequently used wireless networks. To do this you need to already have set up a profile as shown in Setting Up a Wireless Network Profile.

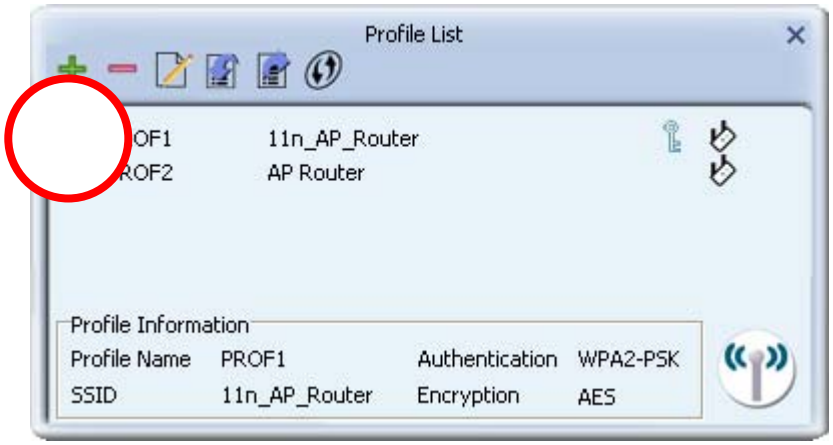
Instructions

Step 1:
In the Profile screen, select the profile for the network to which you are connecting.

Click the Connect button .



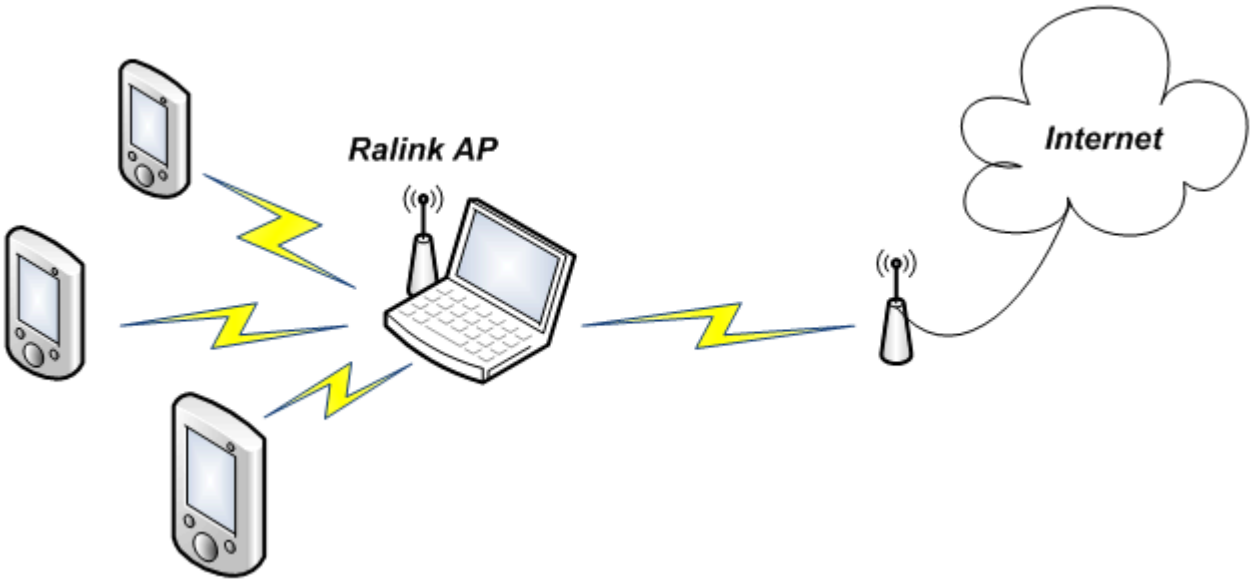
Step 2:
If the connection is successful, the tick icon appears .



Connecting your Network to the Internet

You can let computers and devices connected to the Ralink AP access the Internet, as shown in the diagram below. This is done by setting up a wireless connection between the Ralink AP and an AP connected to the Internet.

NOTE: This feature is only available in Windows 7 and above.

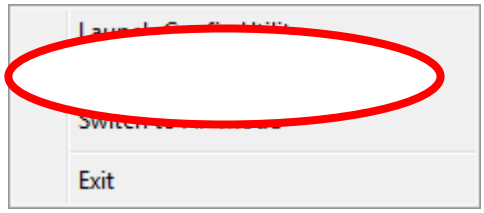


Instructions

Follow these instructions to let a device such as PDA access your network and use your Internet connection.

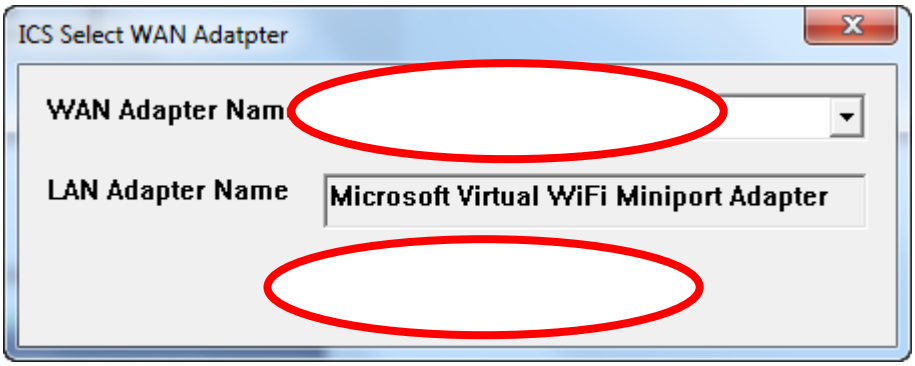
Step 1:
Right-click on the Ralink icon in the task bar in the bottom right hand corner of your screen.

Step 2:
In the menu that appears, click **Switch to Client + AP Mode**.



Step 3:

The following popup appears. In **WAN Adapter Name**, select the card you will use to access the Internet (or a network with Internet access). The adapter name given here is an example only, the name of your network card may differ.

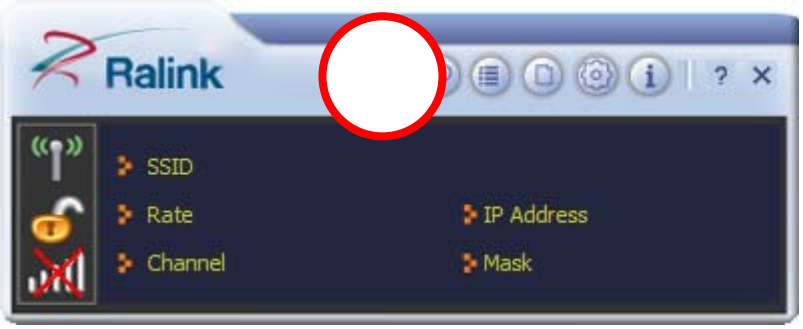


Step 4:

To connect your computer to an AP (or wireless router) with an Internet connection, follow the instructions for Connecting to a Wireless Network. Once properly configured, your computer should have access to the Internet.

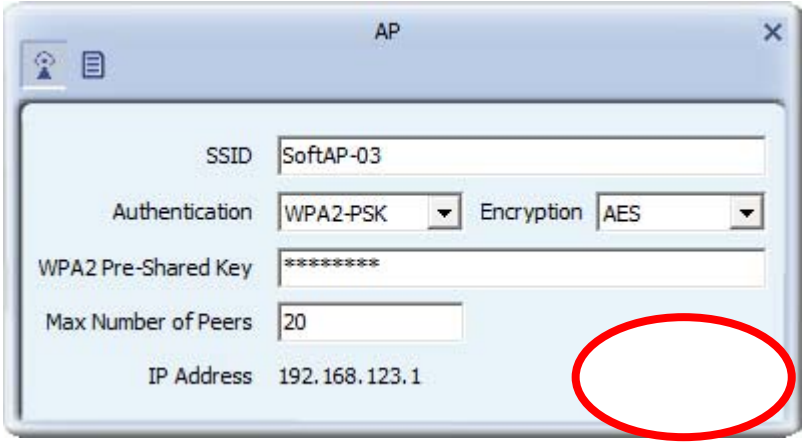
Step 5:

To set up a wireless network through which other devices access the Internet, click the 'AP' button  .



Step 6:

The AP screen appears. In the **SSID** field, type a name for your network. In the **Authentication** and **Encryption** fields, select the strongest security settings supported by devices joining your network. If required, type a security key and note this safely for use by devices joining your network. Click **Apply**.



Step 7:

Connect a device such as PDA to your network using the settings applied in the AP screen. Open a browser on the device to test its connection to the Internet.

Connecting Using Wi-Fi Direct

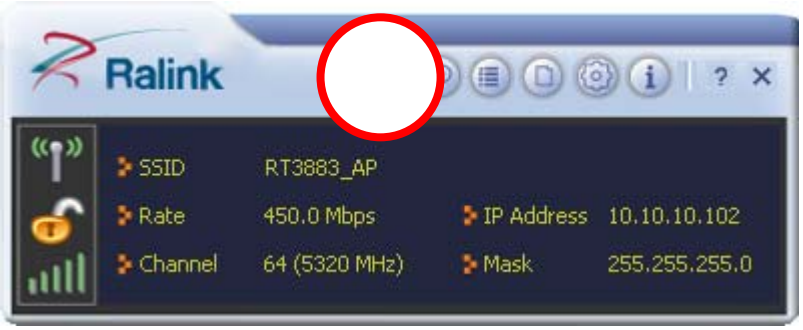
Use Wi-Fi Direct to connect directly to another computer or device that also supports Wi-Fi Direct. With Wi-Fi Direct connections there is no need for an AP or wireless router. In addition, Wi-Fi Direct supports WPS (Wi-Fi Protected Security) for quick setup of strong wireless security. In comparison to alternatives such as Bluetooth, Wi-Fi Direct offers faster speeds (up to 250 Mbps depending on your network environment), with a greater range (up to 219 yards/ 200 metres) with stronger security (WPA2-PSK with AES encryption).

Instructions

To connect one computer or device with another using Wi-Fi Direct, you need to make a Wi-Fi Direct connection request which the other computer or device accepts. For instructions on making and accepting a Wi-Fi Direct connection using the Ralink Utility, follow the steps given below.

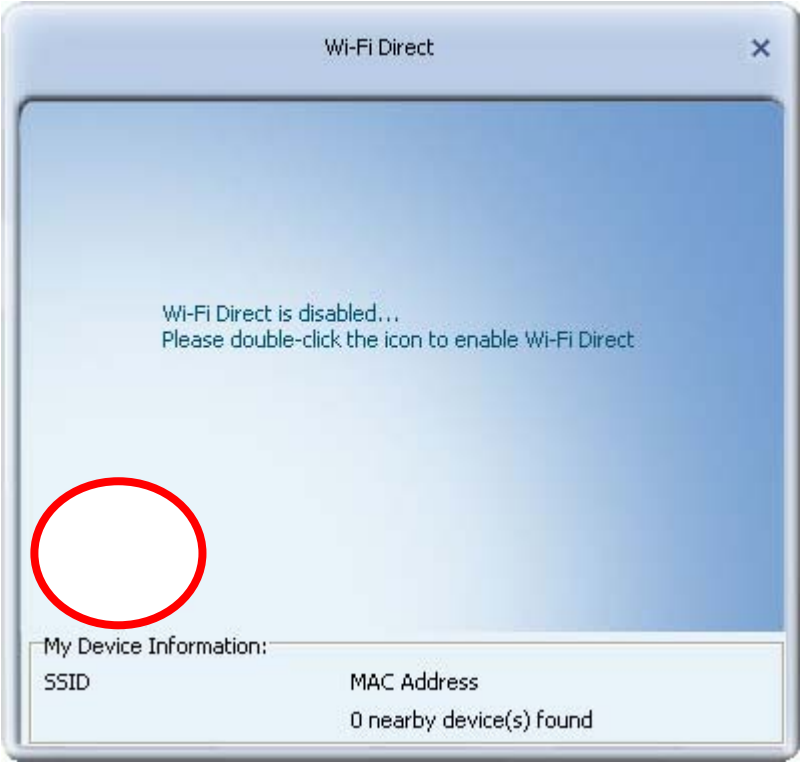
Step 1:

To access the Wi-Fi Direct screens, click the Wi-Fi Direct button  on the Ralink Utility.



Step 2:

The Wi-Fi Direct screen displays. To enable Wi-Fi Direct, double-click the notebook icon.

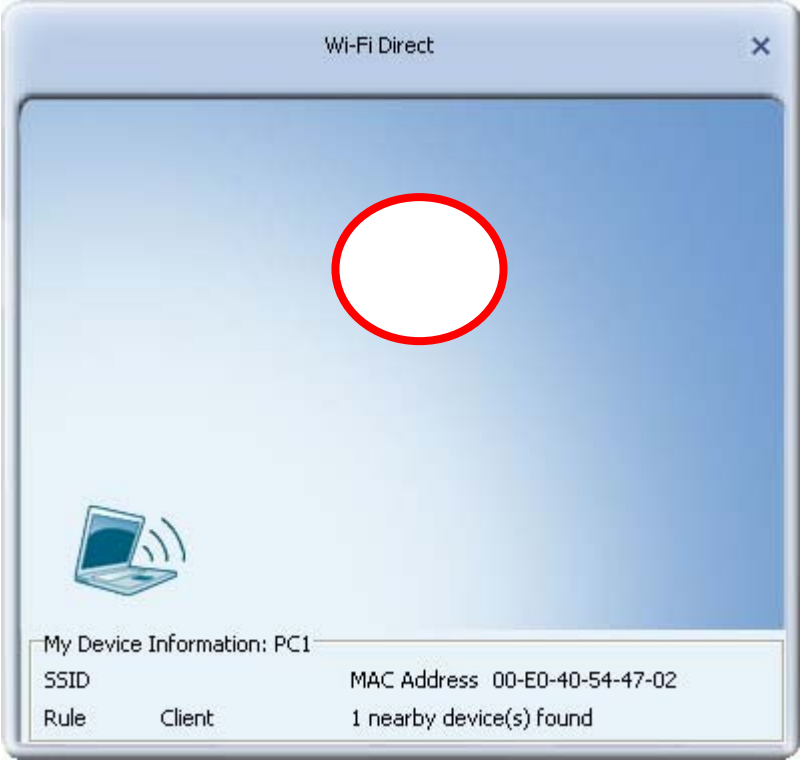


Step 3:

To identify your computer to other Wi-Fi Direct enabled devices, select **Use My Computer name** or **type a name**. Click the right arrow to save your settings.

Step 4:
The following screen displays available, Wi-Fi Direct enabled computers and devices. Wait several seconds until all available devices are detected, or right-click the notebook icon and select **Scan** to refresh this window.

To connect to a computer or device, double-click its icon in the screen.



Step 5:
The Wi-Fi Direct Settings screen appears, with options to configure WPS (Wi-Fi Protected Setup) on your Wi-Fi Direct connection.

a. If the device or computer to which you are connecting has a WPS push button, either on the device housing or in its software interface, follow the instructions for the Push Button Method.

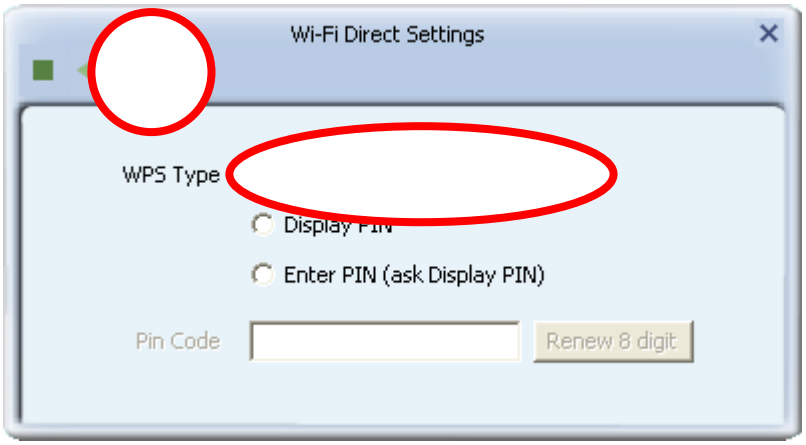
b. If the device or computer to which you are connecting has no WPS push button available, but can accept a WPS PIN, follow the instructions for the Display PIN Method.

c. If the device or computer to which you are connecting is providing a PIN, follow the instructions in the Enter PIN Method.

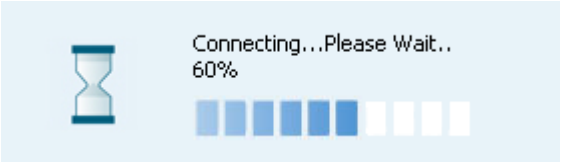
The Push Button Method

To use the WPS push button method, follow these steps.

For WPS Type, select **Push-Button Configuration(PBC)** and click the right arrow in this screen.

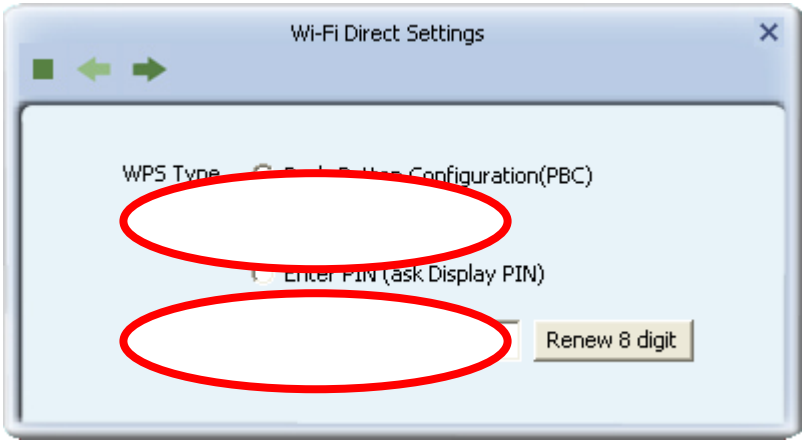


At the same time (within 30 seconds) activate the WPS push button method on the computer or device to which you are connecting. Wait several seconds while a Wi-Fi Direct connection is set up.

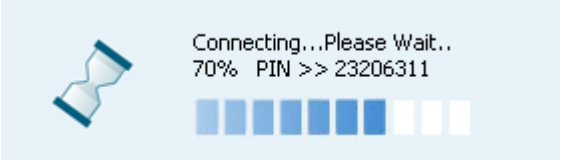


The Display PIN Method

To set up WPS security by providing a PIN, follow these steps.
For WPS Type, select **Display PIN**. Note the PIN displayed in the **PIN Code** field.
Click the right arrow.



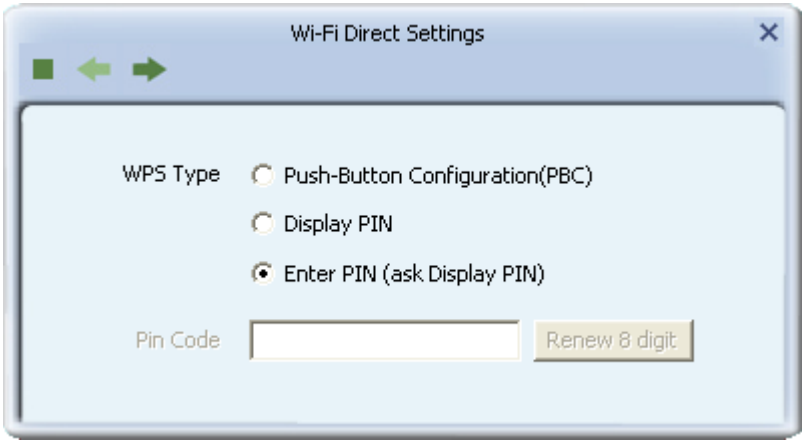
The WPS connection process begins. Within 120 seconds, enter the PIN shown in the Ralink Utility in the corresponding WPS PIN field on the interface of the device to which you are connecting.



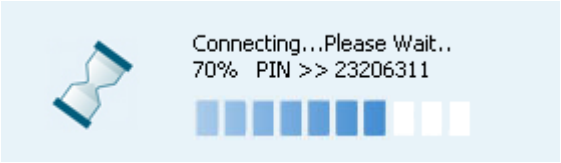
The Enter PIN Method

To set up WPS security using a PIN provided by the connecting device, follow these steps.

Once another computer or device makes a request to connect to your Ralink adapter, the following screen appears. Type the PIN made available from the computer or device making the connection request, and click the right arrow.

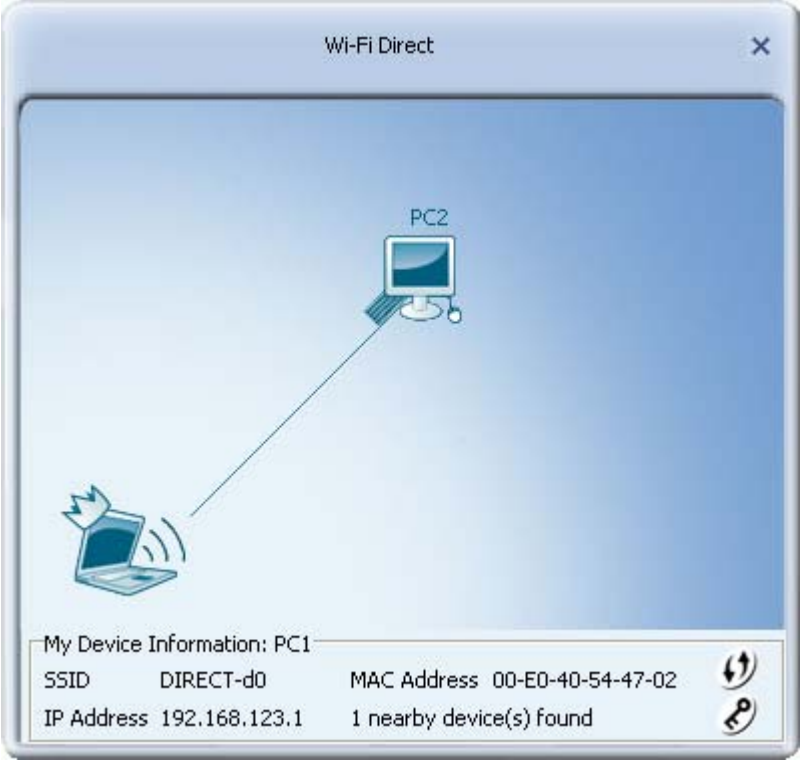


Wait several seconds while a Wi-Fi Direct connection is set up.



Step 6:

If your connection is successful, the connection details are shown in the screen that displays.



Sharing Files With Wi-Fi Direct

The Ralink Utility lets you share files using Wi-Fi Direct. You can use the Ralink Media Server to share media files such as music, video, and image files, or use Windows to share files.

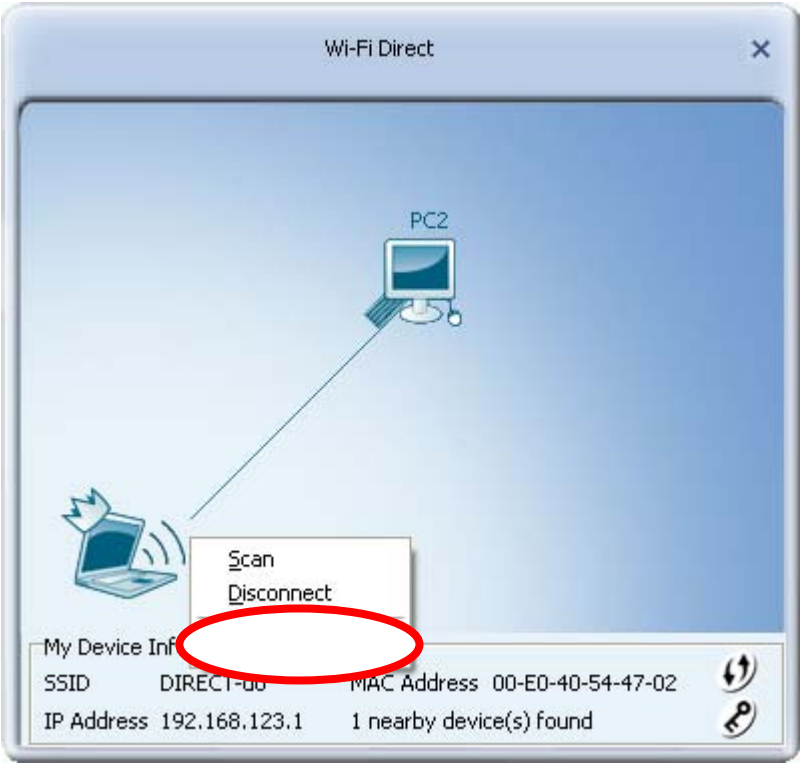
Instructions

Follow these instructions to share media files using the Ralink Media Server, or share all file types using Windows Vista/7 or Windows XP.

Sharing Media Files with the Ralink Media Server

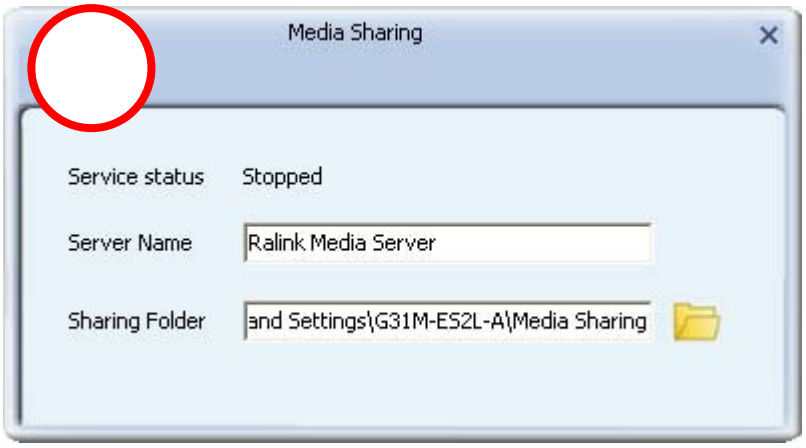
Step 1:
Ensure you have a Wi-Fi Direct connection set up. See Connecting Using Wi-Fi Direct for instructions on how to do this.

Step 2:
In the Wi-Fi Direct screen, right-click on the notebook icon and select Media Sharing.



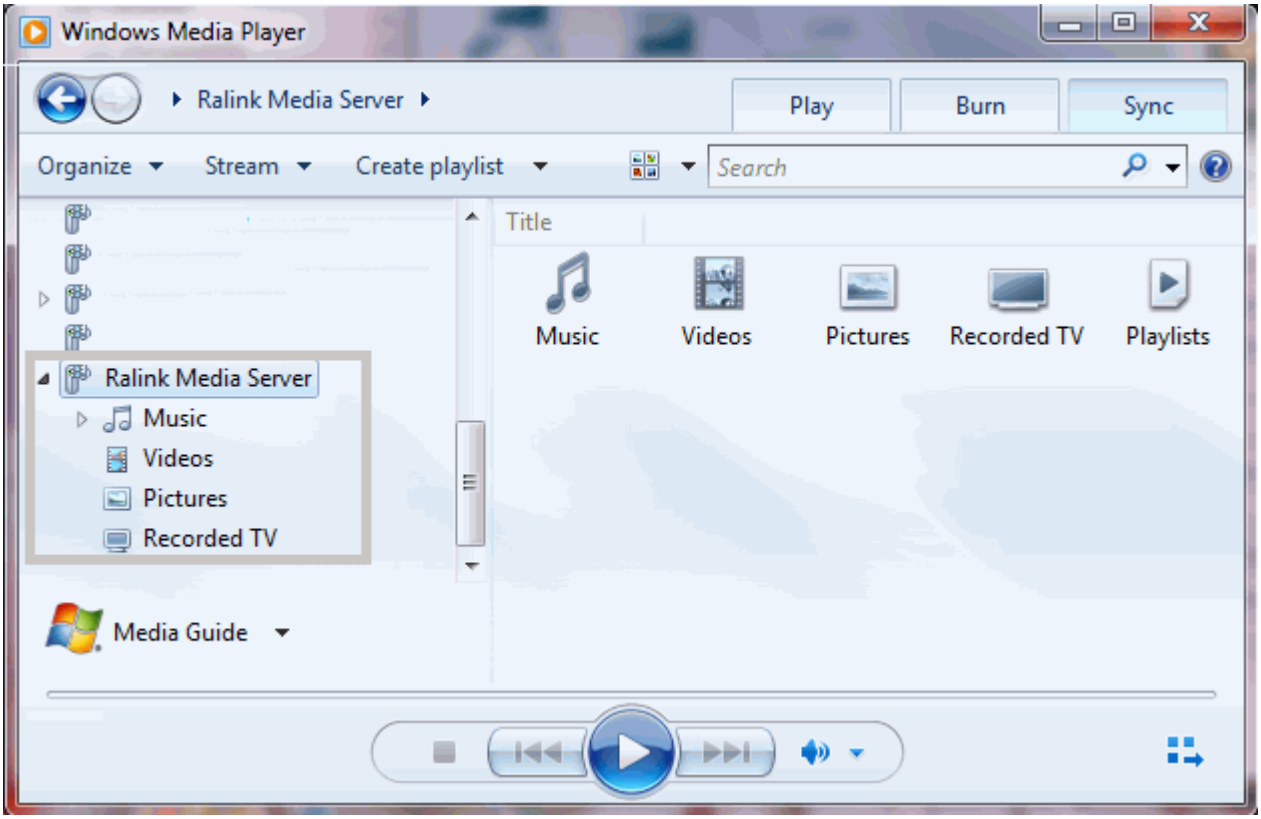
Step 3:

In the Media Sharing screen, click the right arrow to enable the server and begin sharing media files located in the Media Sharing folder.



Step 4:

The files shared by the media server can now be accessed on the connecting computer. Use a media player on the connecting computer to locate the server and the media files, and view them or begin playback.



Step 5:
To finish sharing using the Ralink Media Server, in the Media Sharing screen, press the stop button .

Setting Up a Wireless Network Profile

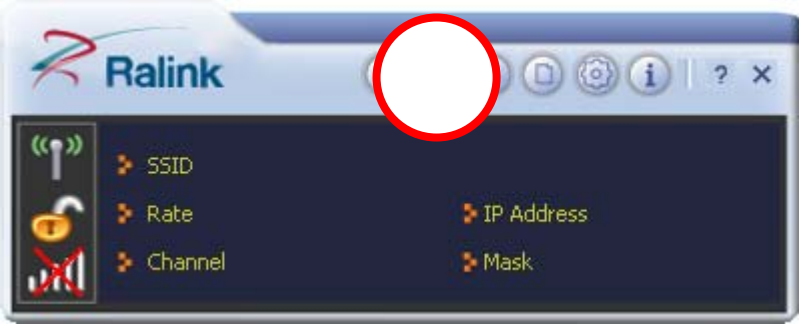
A profile is a group of settings which you can use to quickly set up a wireless connection. The Ralink Utility lets you set up profiles based on settings for a wireless network and for WPS (Wi-Fi Protected Setup) settings. To set up a WPS profile, follow the instructions provided for connecting using WPS with the PIN method. To set up a wireless network profile, follow the instructions below to set up a wireless network profile either by applying the settings of an available connection, or by configuring settings manually.

Instructions

Follow these instructions to set up a profile based on the settings of an available wireless network, or to manually add or edit profile settings.

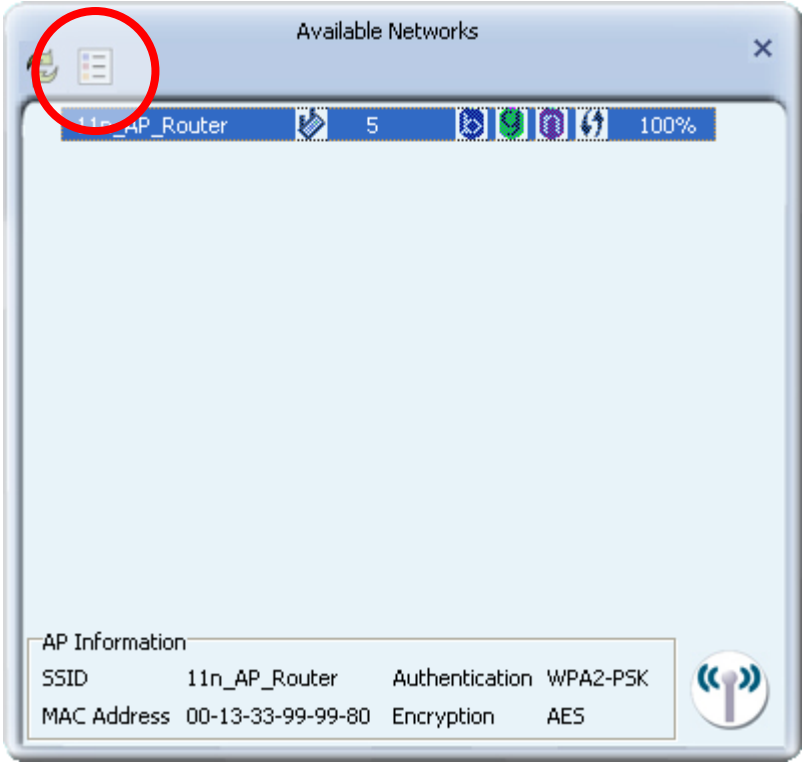
Setting Up a Profile Based on the Settings of an Available Network

Step 1:
To quickly set up a profile by using the settings of an available network, click the Available Networks button to display the Available Networks screen.



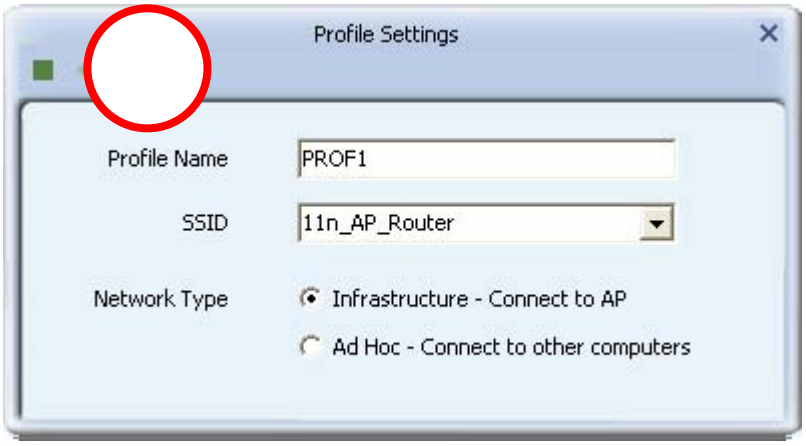
Step 2:

In this screen, select a network and click on the Add to Profile button .



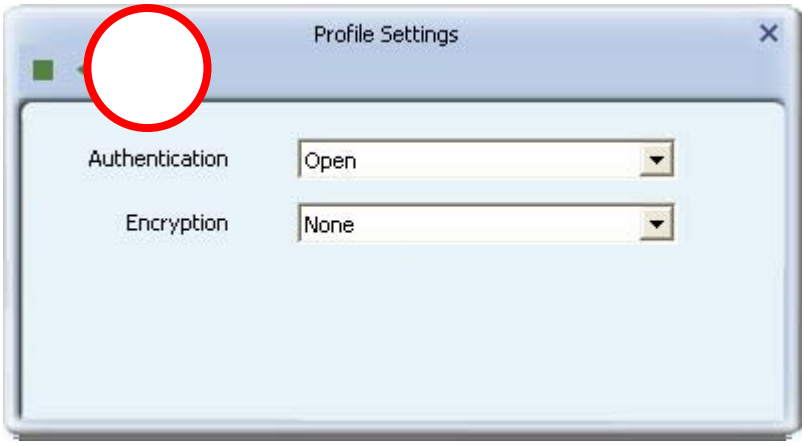
Step 3:

The settings of the network you selected in the Available Networks screen are automatically displayed in the Profile Settings screens. Click the right arrow in these screens to accept all settings.



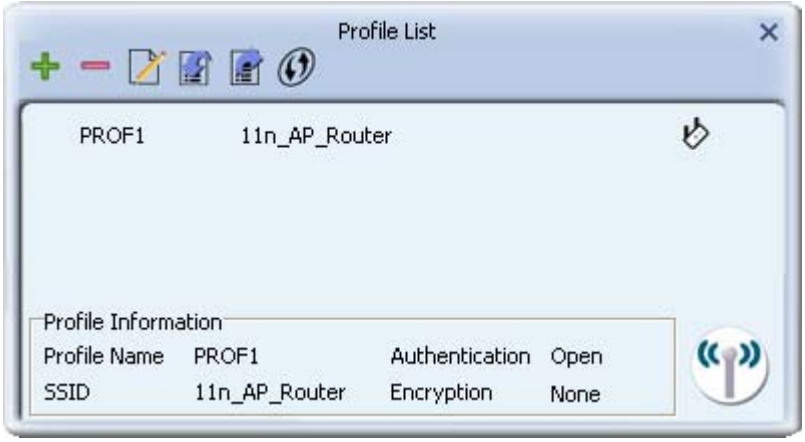
Step 4:

Click the right arrow in these screens to accept all settings. If required, enter security settings such as the security key for your network.



Step 5:

After you have set up a profile, it appears in the Profile List screen.



Setting Up Wireless Security for Home Networks

Overview

To make your wireless connection more secure, choose the strongest security settings supported by the AP or wireless router to which you are connected. For home and small business networks, WPA-PSK, WPA2-PSK, and WEP are common security methods, and WAPI-PSK is a possible alternative.

Supported Security Methods

The following table shows the authentication and encryption methods supported by the Ralink Utility.

Authentication Method	Encryption Method	Comments
WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key)	AES (Advanced Encryption Standard) TKIP (Temporal Key Integrity Protocol)	WPA2-PSK is a faster, more recent standard than WPA-PSK. AES is a stronger, more recent standard than TKIP.
Open Shared	WEP (Wireless Encrypted Privacy)	WEP is an older standard and is easily decrypted. If using WEP select Open as the authentication method for slightly stronger security.

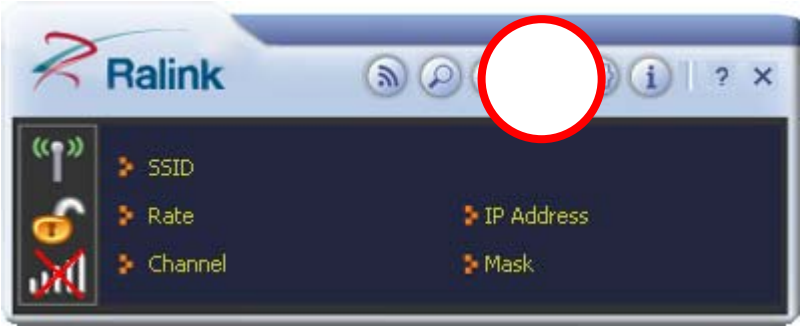
Note: WAPI-PSK authentication with SMS4 encryption is also available, however, at the time of writing, it is a new Chinese standard and has yet to be made an ISO standard.

Instructions

To configure security settings on your network connection, use the profile function in the Ralink Utility.

Step 1:

Click the Profile Settings button to display the Profile List screen.



Step 2:

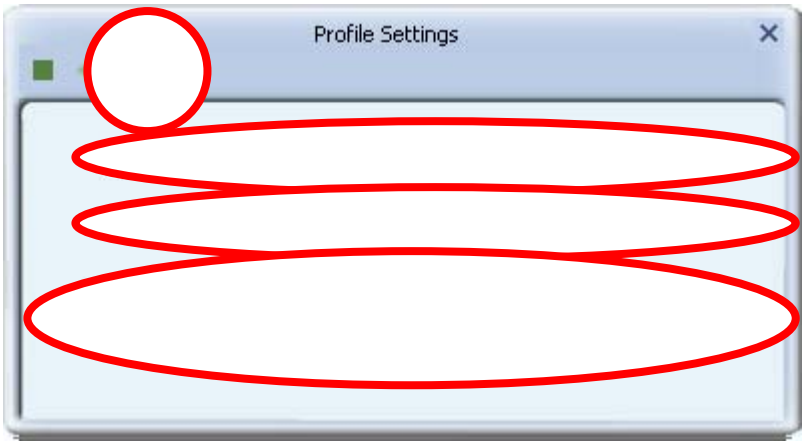
To configure a wireless security profile, click the Add button to add a new profile, or click the Edit button to edit an existing profile.

Step 3:

In the screen that displays, enter the following settings.

a. For 'Profile Name', type a name for the profile, or leave at its default value.
b. In the SSID field, type the name of the network for which you are configuring security settings, or select the name of the network from the drop-down list provided.
c. For 'Network Type', select whether your network is an infrastructure or ad hoc network. If uncertain, leave at its default setting (Infrastructure).

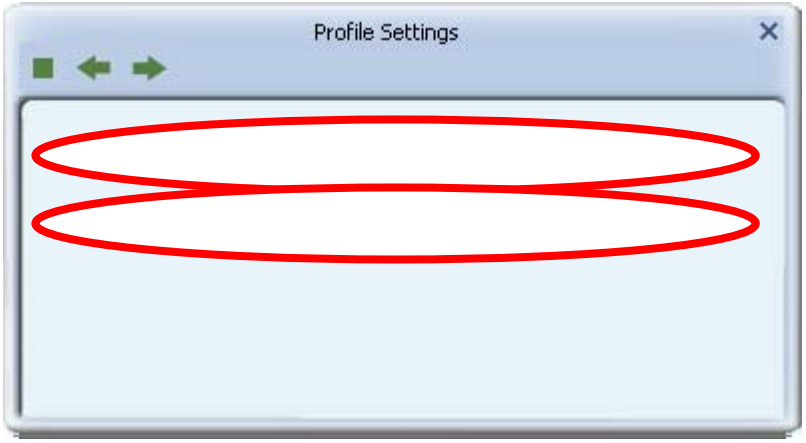
	Functions
Infrastructure	**Connect to AP** if you are connecting to a typical wireless network maintained by an AP or wireless router.
Ad Hoc	**Connect to other computers** if you are connecting to a distributed network with no AP or router.



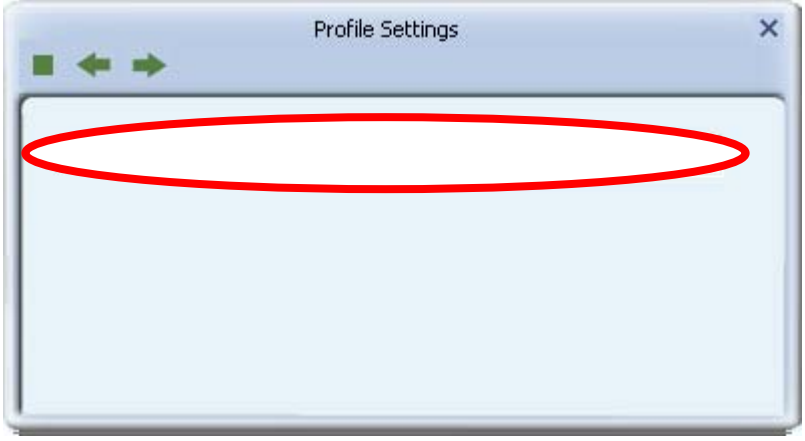
Step 4:
Click the right arrow to save your settings. For instructions on setting up a security method, click on the corresponding link.

Setting Up WPA-PSK or WPA2-PSK

For Authentication, select WPA-PSK or WPA2-PSK and for Encryption, select TKIP or AES. Click the right arrow to save your settings.

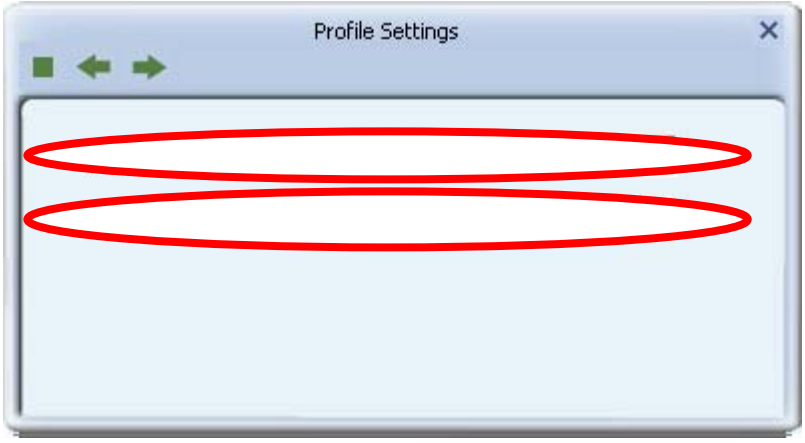


For **WPA Preshared Key**, type a passphrase 8-63 characters long made up of characters **0**-**9**, **a**-**z**, **A**-**Z**, keyboard symbols and spaces. Click the right arrow to save your settings and finish setting up WPA-PSK or WPA2-PSK security.



Setting Up WEP

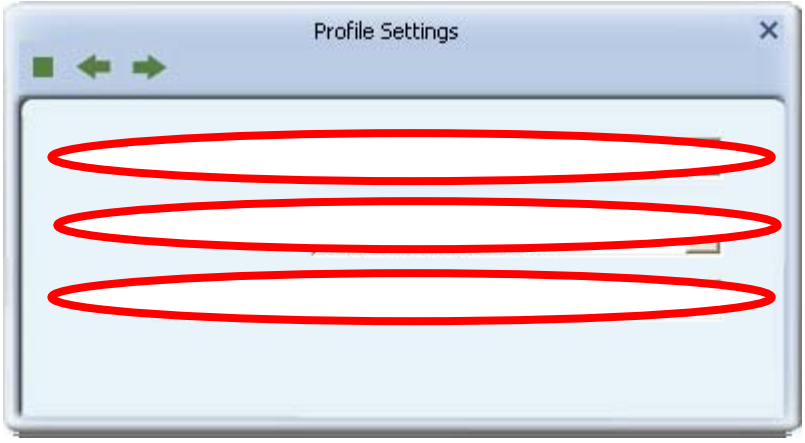
For Authentication, select Open or Shared, and for Encryption select WEP. Click the right arrow to save your settings.



In the screen that appears select a Key and Key Format setting supported by the wireless router or AP to which you are connecting.

a. If you select **Hex(10 or 26 hex digits)**, in the WEP Key field type a security key 10 or 26 characters long made up of digits **0-9** and letters **A-F**.

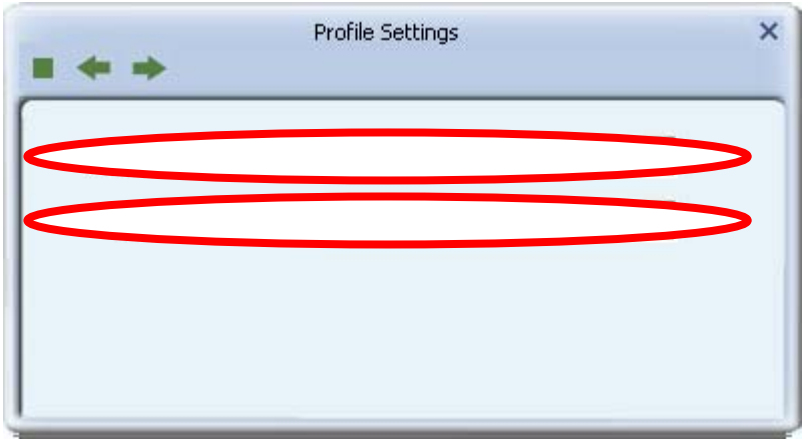
b. If you select **ASCII(5 or 13 ASCII characters)** in the WEP Key field, type a security key 5 or 13 characters long made up of digits **0-9** and letters **a-z** and **A-Z**.



Click the right arrow to save your settings and finish setting up WEP security.

Setting Up WAPI-PSK

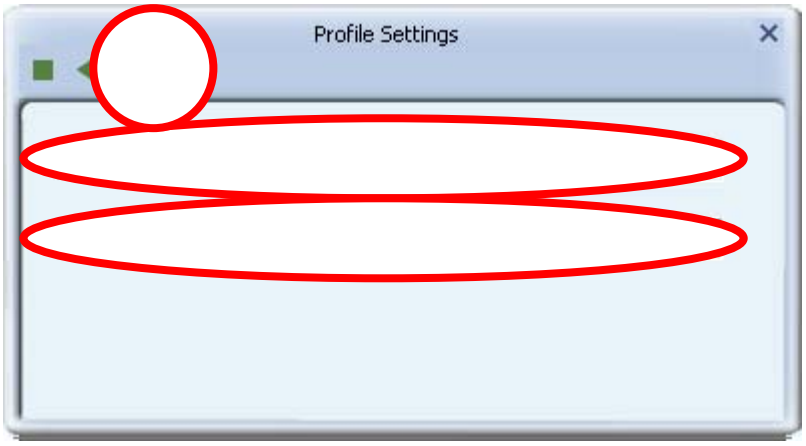
For Authentication, select WAPI-PSK and for Encryption, select SMS4. Click the right arrow to save your settings.



In the screen that appears select a Key and Key Format setting supported by the wireless router or AP to which you are connecting.

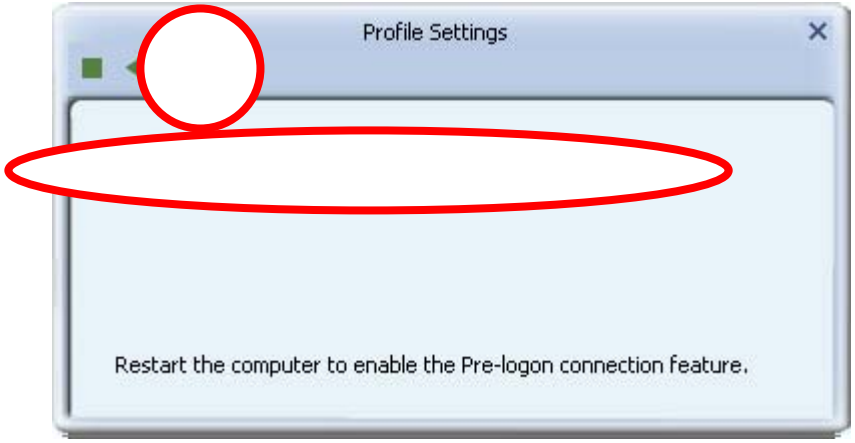
a. If, in the **Key Format** field, you select **Hex(8 ~ 64 hex digits)**, then in the **WPA Preshared Key** field type a security key 8-64 characters long made up of digits **0**-**9** and letters **A**-**F**.

b. If, in the **Key Format** field, you select **ASCII(8 ~ 64 ASCII characters)** in the **WPA Preshared Key** field, type a security key 8-64 characters long made up of digits **0**-**9** and letters **a**-**z** and **A**-**Z**.



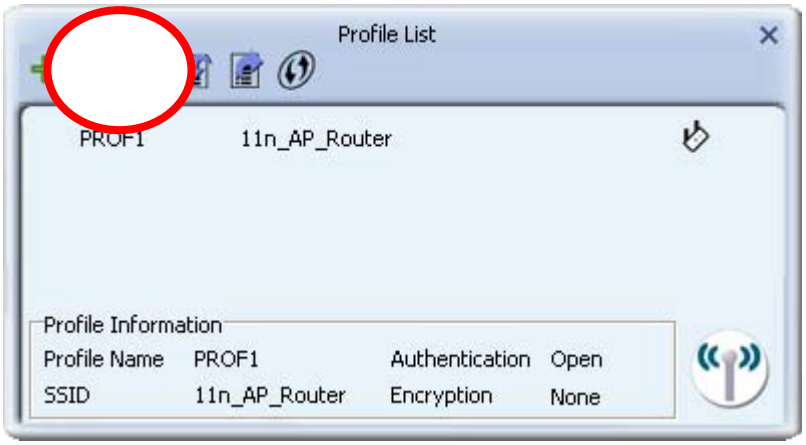
Click the right arrow to save your settings and finish setting up WAPI-PSK security.

Step 5:
With **WEP**, **WPA-PSK** or **WPA2-PSK** security, you can select Use **Pre-logon Connection** to automatically connect using the settings of this profile when logging in to Windows.



Step 6:

After you have set up security settings, it appears in the Profile Settings screen. To further edit settings, click the Edit button , or to delete settings, click the delete button .



Screen Descriptions

Operating Modes

The Utility has three modes; **client mode (Default)**, **access point mode**, and **client + AP Mode (Windows 7 only)**.

	Functions
client mode (Default setting)	Client mode allows you to use the Adapter as a wireless client, and to connect to an AP or wireless router and other clients in a wireless network.
access point mode	AP mode lets you use the Adapter as an access point and set up a wireless network, to which wireless clients can connect.
client + AP Mode (Windows 7 only)	Client and AP Mode lets you use the Adapter both as an AP and as a member of a wireless network at the same time (Windows 7 only).

Client Mode

Client mode is the default setting. To use client mode, leave settings at their defaults. Manually setting client mode is only required when switching from AP mode to client mode. Follow these steps to use manually set the Utility to client mode.

Step 1:

Right-click on the  icon in the task bar in the bottom right hand corner of your screen.

Step 2:

In the menu that appears, select **Switch to Client Mode**.

Step 3:
The Utility appears in compact mode showing the connection status of the Adapter.

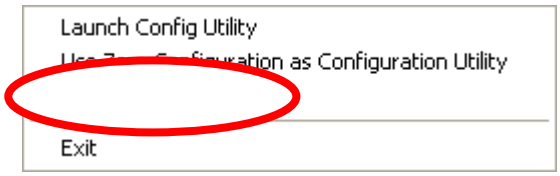
AP Mode

To set to the Utility to AP mode, follow these steps.

Step 1:

Right-click on the  icon in the task bar in the bottom right hand corner of your screen.

Step 2:
In the menu that appears, click **Switch to AP Mode**. Wait several seconds for the Utility to appear in AP mode.



Step 3:
The Utility appears in compact mode showing the connection status of the Adapter.

Client + AP Mode (Windows 7 only)

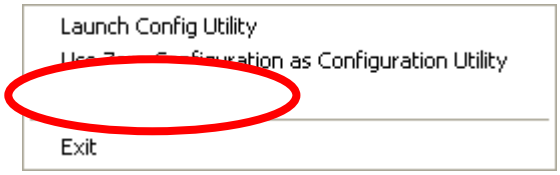
This mode is only available in Windows 7 or higher.

Step 1:

Right-click on the  icon in the task bar in the bottom right hand corner of your screen.

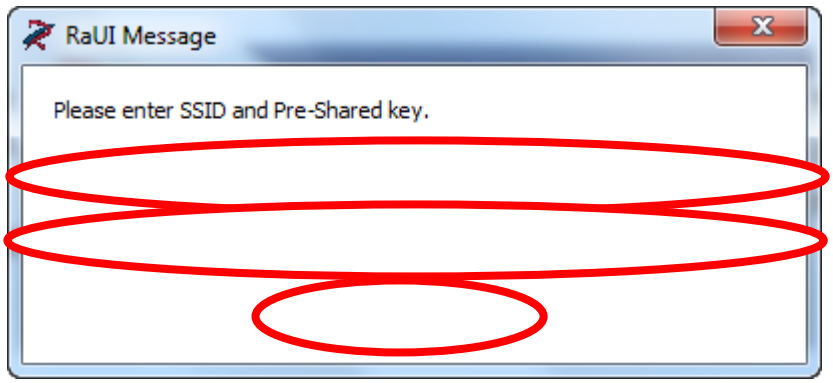
Step 2:

In the menu that appears, click **Switch to Client + AP Mode**.



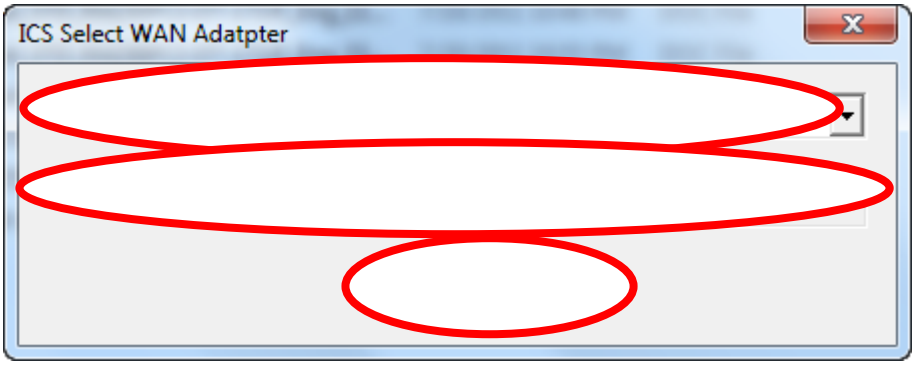
Step 3:

If configuring an AP for the first time, in the **SSID** field, type a name for your wireless network, and in the **WPA2 Pre-Shared Key** field, type a passphrase 8-63 characters long made up of characters **0**-**9**, **a**-**z**, **A**-**Z**, keyboard symbols and spaces. Click **OK**.



Step 4:

If multiple network interface cards (NICs) are available on your computer, in **WAN Adapter Name** select a NIC to connect to another network such as the Internet, and in **LAN Adapter Name**, select a NIC to connect to your AP's wireless network. Click **OK**. The following screenshot is an example only, your settings may differ.



The Compact Mode Screen

From the compact mode screen, use the Utility to connect to a wireless network, view connection status, set up profiles, and configure advanced networking features including connecting directly to another wireless-enabled computer or device.

The Utility in compact mode shows the connection status of the Adapter.

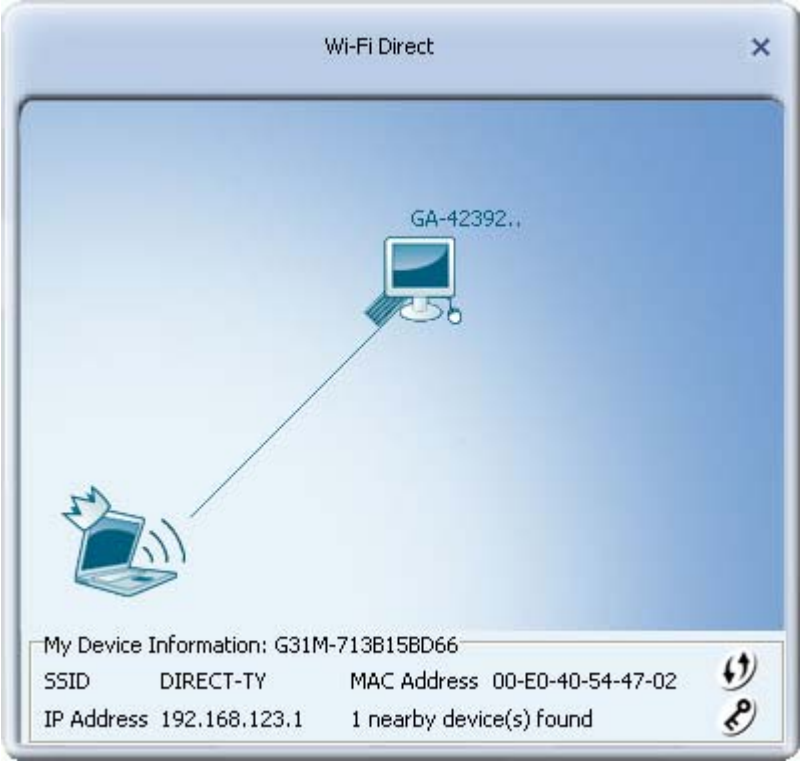
The Wi-Fi Direct Screens

Use these screens to connect directly to other Wi-Fi Direct enabled devices and to share media files such as music, images and videos.

Wi-Fi Direct Buttons	Functions
	Use the left and right arrows to work through the Profile screens.
	Click the Stop button to cancel setting up or editing a profile.

The Wi-Fi Direct Screen

Use this screen to find information about available Wi-Fi Direct-enabled devices and computers, and the status of your Wi-Fi Direct connection.



My Device Information: Displays the name configured for your Adapter for Wi-Fi Direct connections.

My Device Information	Functions
SSID	Displays the name of the Wi-Fi Direct connection.
IP Address	Displays the IP address of your Ralink Adapter on the Wi-Fi Direct network.
MAC Address	Displays the MAC address of your Ralink Adapter.
	Indicates the group owner (GO). The GO allocates IP addresses in a Wi-Fi Direct connection. By default GO status is assigned automatically but can be manually assigned by enabling autonomous GO on a device.
	Indicates the Group Owner is connected to one or more devices using Wi-Fi Direct.
	Displayed only in group owner mode. Click this to configure WPS settings for connections managed by the Ralink Utility in group owner mode.
	Displayed only in group owner mode. Click this to configure wireless security settings for connections managed by the Ralink Utility in group owner mode.

Right-click the notebook icon to display the following options.

	Functions
Scan	Select this option to refresh the list of available Wi-Fi Direct enabled devices.
Enable autonomous GO	Select this option to set your Adapter to act as group owner (GO) without requiring negotiation with other devices.
Media Sharing	Select this option to enable devices connected with Wi-Fi Direct to access media files on your computer.

The Wi-Fi Direct Screen

To display this screen, double-click on the notebook icon in the bottom left of the Wi-Fi Direct screen to enable Wi-Fi Direct.
Use this screen to identify your computer to other Wi-Fi Direct enabled devices.

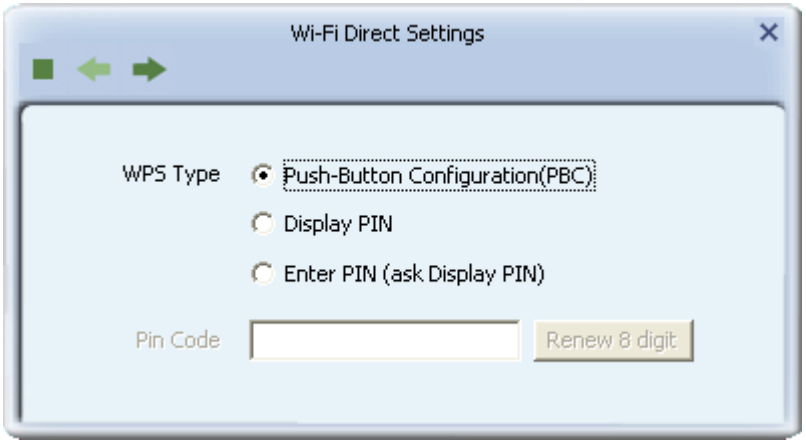
	Functions
Use My Computer name	Select this option to refresh the list of available Wi-Fi Direct enabled devices.
Manually Enter a name for Wi-Fi device	Select this option to manually enter a name to identify your computer to other Wi-Fi Direct enabled computers or devices.

The WPS Settings Screen

To display this screen, double-click on a device icon (not the notebook icon) in the Wi-Fi Direct screen to set up a Wi-Fi Direct connection with this device.

Use this screen to decide how Wi-Fi Protected Setup (WPS) is configured on your Wi-Fi Direct connection. WPS is a secure wireless connection method intended to simplify the process of configuring complicated security settings.

This screen also displays by clicking the WPS icon in the Wi-Fi Direct screen when Autonomous GO is enabled. These settings are applied to any Wi-Fi Direct connection made by the Utility when autonomous GO is enabled.

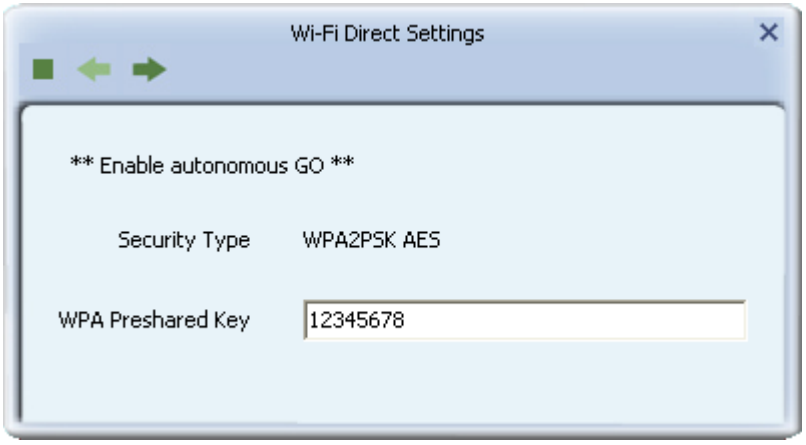


	Functions
Push-Button Configuration(PBC)	Select this option to securely connect two WPS enabled devices by manually pushing a physical or software WPS button.
Display PIN	Select this option and use the PIN displayed to configure WPS on the device to which you are connecting.
Enter PIN (ask Display PIN)	Select this option and enter the WPS PIN provided by the device to which you are connecting.
PIN Code	If **Display PIN** is selected, use the PIN displayed in this field to configure WPS on the device to which you are connecting. To obtain a new PIN, click **Renew 8 digit**. If **Enter PIN (ask Display PIN)** is selected, in this field type the 8-digit PIN provided by the device to which you are connecting.

The Autonomous GO Screen

Enable Autonomous GO to set the Adapter to automatically become group owner of any Wi-Fi Direct connection it has. This allows you to share a resource such as a network connection or access to media files to other computers or devices to which you are connected.

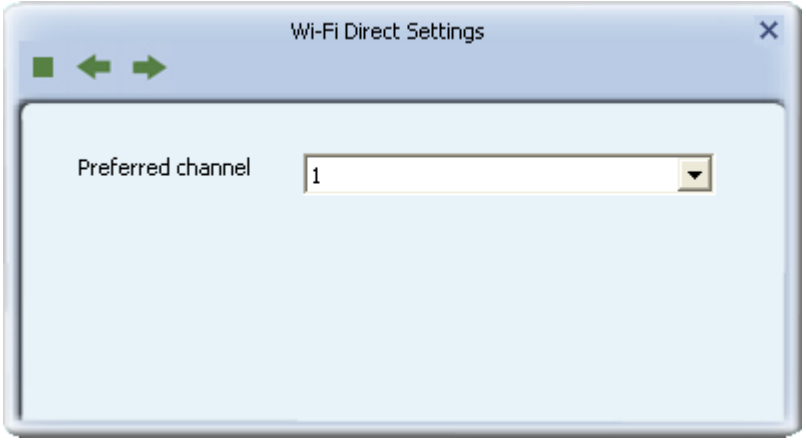
To display this screen, right-click on the own computer icon in the Wi-Fi direct screen and click **Enable autonomous GO**. To edit this setting later, click on the security icon in the Wi-Fi Direct screen.



WPA Preshared Key: In this field, type 8-63 alphanumeric characters.

The Channel Selection Screen

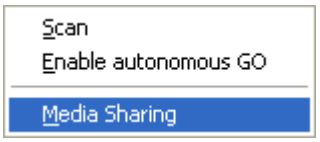
To display this screen, click the right arrow in the Autonomous GO screen. Use this screen to select the preferred operating channel and to save your settings to a profile.

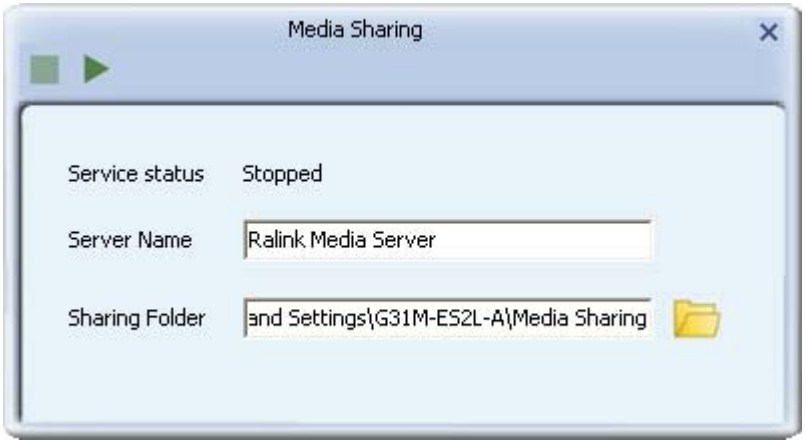


	Functions
Preferred channel	For reduced interference select the channel least used by nearby wireless networks.

The Media Sharing Screen

To display this screen, right-click on the own computer icon in the Wi-Fi direct screen and click **Media Sharing**.

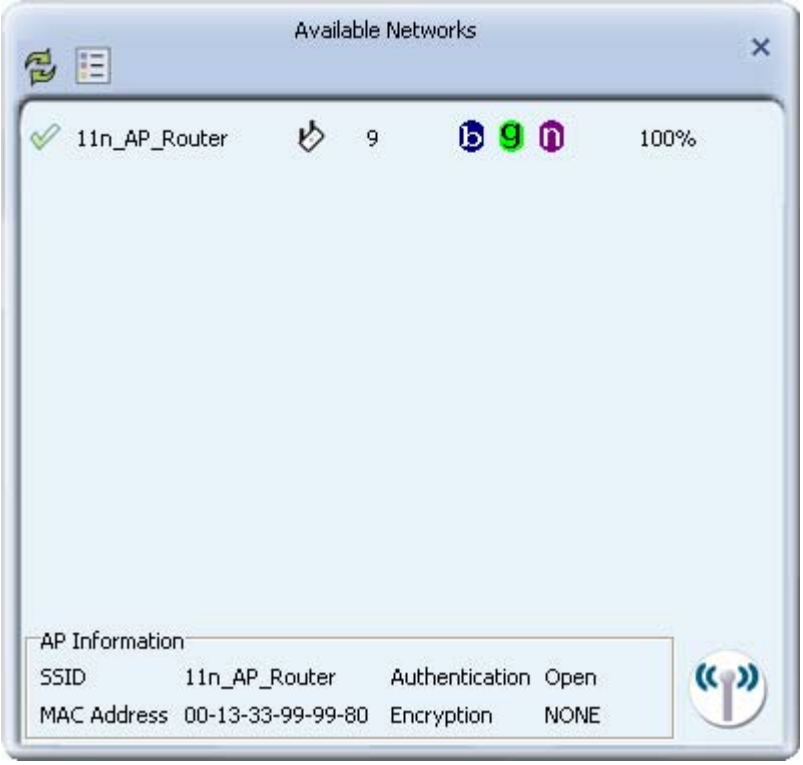




	Functions
Service Status	Indicates the status of the Ralink media server.
Server Name	Displays the name of the media server provided with the Utillity. Type an alternative name, or leave it at its default setting.
Sharing Folder	Click the browse icon to locate and load the folder to be shared.
	Click the right arrow to confirm settings and enable media sharing.
	Click the stop button to disable sharing.

The Available Networks Screen

The Available Networks screen provides information on available networks and their settings. Use this screen to connect to a network and add a profile.



Available Networks Buttons

The functions of the buttons in this screen are as follows.

	Functions
	Click the Rescan button to update the list of available wireless networks.
	Click the Add Profile button to add the connection settings of the selected wireless network to the Utility's list of profiles.
	Click the Connect button to connect to the selected wireless network.
✔ Sorted by SSID Sorted by Channel Sorted by Signal Strength	Right-click the Available Networks screen to display the Sort menu. This option sorts the list of available networks according to network name, channel number, or signal strength.

Available Networks Icons

Site Survey icons provide information on the network setting of a profile.

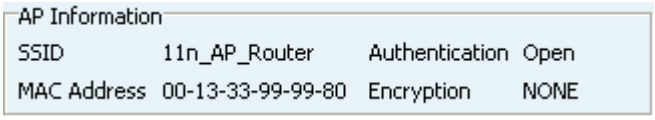
1 2 3 4 5 6 7

From left to right the icons are as follows.

	Functions
1. Connection status	- Successfully connected to the network.
2. SSID or Network Name	The name of the network to which you are connected.
3. The network mode	- Infrastructure mode: Indicates the network is maintained by an AP or wireless router. This is a typical wireless network. - Ad-hoc mode: Indicates the network is a distributed wireless network with no AP or router.
4. Channel number	For reduced interference select the channel least used by nearby wireless networks.
5. Wireless standards supported by the network	- IEEE 802.11b - IEEE 802.11g - IEEE 802.11n
6. The security status of the network	- Indicates that WPS is available on this network. - Indicates that a security method is configured on this network.
7. strength of the signal	The strength of the signal received from with the specified network.

AP Information

For more detailed information on an available network, select a network to display AP Information.



	Functions
SSID	The name of your network
MAC Address	A unique identifier of your Adapter, assigned by the manufacturer.
Authentication	Available authentication methods.
Encryption	Available encryption methods.

The Link Information Screens

Use these screens to find detailed information on network settings, connection quality, and packet statistics.

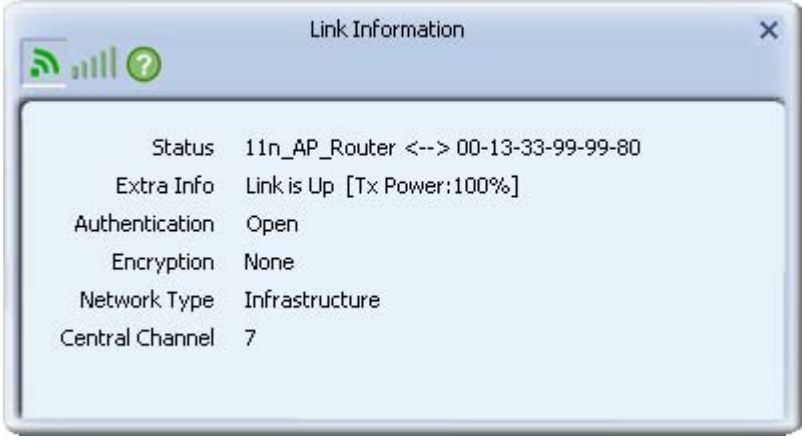
Link Information Buttons

Click the following buttons to access the Link Information screens.

	Functions
	Click this button to access the Link Status screen and find information on network settings.
	Click this button to access the Throughput screen and find information on connection quality.
	Click this button to access the Statistics screen and find information on packet statistics.

The Link Status Screen

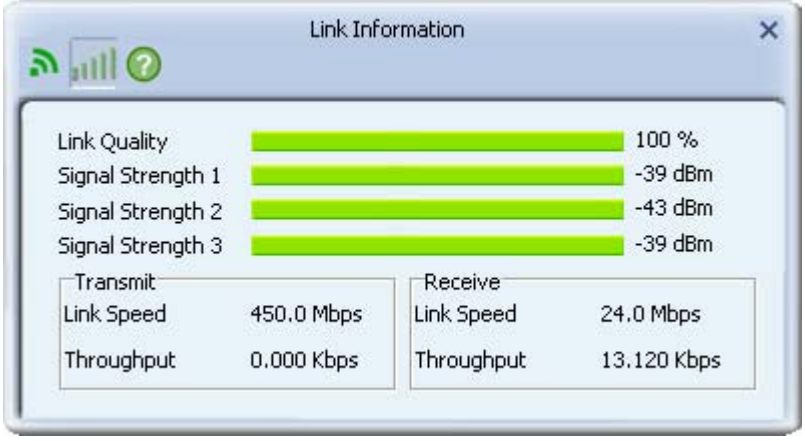
Use this screen to find information on your network settings.



	Functions
Status	This displays the name of your network and the MAC address of the access point (AP) to which you are connected. If there is no connection, **Disconnected** is displayed. If transmission is disabled (indicated by the radio button icon), **Turn off RF** is displayed.
Extra Info	If connected, **Link is Up** and signal strength is displayed. If disconnected, **Link is Down** is displayed.
Authentication	Displays the authentication method used by your connection. The Utility supports Open, Shared, WPA-PSK, WPA2-PSK, WPA, WPA2, 802.1X, CCKM, WAPI-PSK, and WAPI-CA.
Encryption	Displays the encryption method used by your connection. The Utility supports WEP, TKIP, AES, TKIP(MFP), AES(MFP), and SMS4.
Network Type	Displays the type of network to which you are connected. Infrastructure indicates a typical network with an AP or router, ad hoc indicates a distributed network without an AP or router.
Central Channel	This displays the channel used in this wireless connection. If multiple channels are used, for example, to increase the available bandwidth, this field displays the median channel number.

The Throughput Screen

Use this screen to find information on the quality of your connection.



	Functions
Link Quality	An indicator of the quality of the signal based on measurements of the strength of the received signal and the level of packet loss for both received and transmitted data.
Signal Strength 1	Indicates the signal strength for each antenna supported by your Adapter.
Transmit Link Speed	Shows the maximum transmission speed supported by your wireless connection given current network conditions.
Transmit Link Throughput	Shows the amount of data transmitted by the Adapter.
Receive Link Speed	Shows the maximum speed of signals received on your wireless connection given current network conditions.
Receive Link Throughput	Shows the amount of data received by the Adapter.

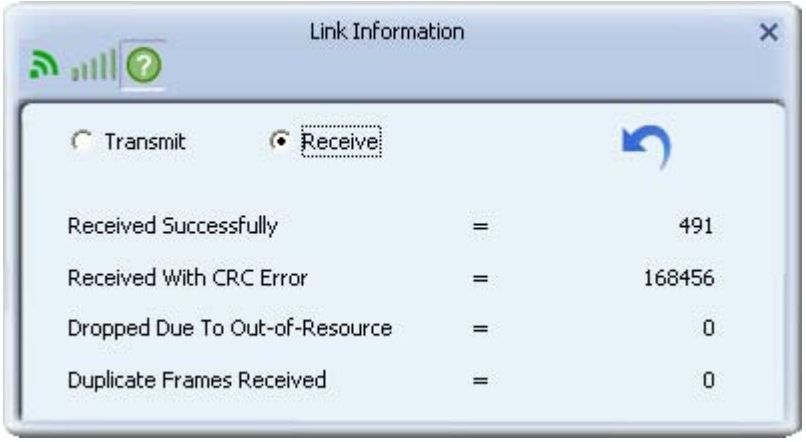
The Statistics Screens

Use these screens to find information on the packets transmitted and received by the Adapter.

The Transmit Screen

	Functions
Transmit	Select this option to find information on packets transmitted by the Adapter.
Receive	Select this option to find information on packets received by the Adapter.
Transmitted Successfully	Shows the number of successfully transmitted packets on the current wireless connection.
Retransmitted Successfully	Shows the number of successfully retransmitted packets on the current wireless connection. A high number may indicate interference on your network.
Fail to Receive ACK After All Retries	Shows the number of packets that were transmitted without an acknowledgement from a receiver. A high number may indicate interference on your network.
	Click this button to reset all packet statistics displayed in this screen to zero.

The Receive Screen



	Functions
Transmit	Select this option to find information on packets transmitted by the Adapter.
Receive	Select this option to find information on packets received by the Adapter.
Received Successfully	Shows the number of packets received on the current wireless connection.
Retransmitted Successfully	Shows the number of successfully retransmitted packets on the current wireless connection. A high number may indicate interference on your network.
Received With CRC Error	Shows the number of frames received with a CRC (Cyclical Redundancy Check) or checksum error. A number much higher than the number of packets successfully received indicates interference is a problem on your network.
Dropped Due To Out-Of-Resource	Shows the number of packets dropped due to an internal buffer overflow. An high number may indicate too much traffic on your network, or that your system is too slow to handle the current level of network traffic.
Duplicate Frames Received	Shows the number of duplicate frames received. A high number may indicate computers and devices on your network are not receiving acknowledgement of their transmission and so are resending their data. Interference may be a cause of this problem. This value is typically higher for an ad hoc network than for a infrastructure network.
	Click this button to reset all packet statistics displayed in this screen to zero.

The Profile Settings Screens

A profile is a set of network settings such as network name and security settings, which you can use to quickly set up a wireless connection instead of manually entering settings. Use these screens to configure a profile for a standard wireless connection or for a WPS-enabled network connection.

The Profile List Screen

The Profile List screen lets you add, edit and delete profiles, and find information on existing profiles. Use this screen to set up a profile and to configure WPS and wireless security for easy connection to frequently used wireless networks.

NOTE: When WZC is enabled, profile functions are unavailable.

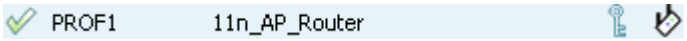
Profile List Buttons

The Profile List screen provides the following buttons.

	Functions
	Click the Add Profile button to add a new profile to the profile list.
	Click the Delete Profile button to remove a profile from the profile list.
	Click the Edit Profile button to change the details of the selected profile.
	Click the Import Profile button to import a profile in .prof file format.
	Click the Export Profile button to export the selected profile in .prof file format.
	Click the Add WPS Profile to set up a profile with Wireless Protected Setup (WPS) security settings.
	Click to connect using the network settings in the selected profile.

Profile Settings

The Profile List screen describes the following profile settings.



1 2 3 4 5

	Functions
1. Connection status	- Indicates if a connection made from the currently activated profile. - Indicates if the connection has failed on a currently activated profile.
2. Profile name	The name of this profile, default is PROF* (* indicating 1, 2, 3...).
3. Network name/SSID	The name of your network.
4. Security Status	- Security is enabled.
5. Network Type	- Infrastructure: Indicates that you are connecting to a typical wireless network maintained by an AP or wireless router. if uncertain, select this option. - Ad Hoc: Indicates that you are connecting to a distributed network with no AP or router.

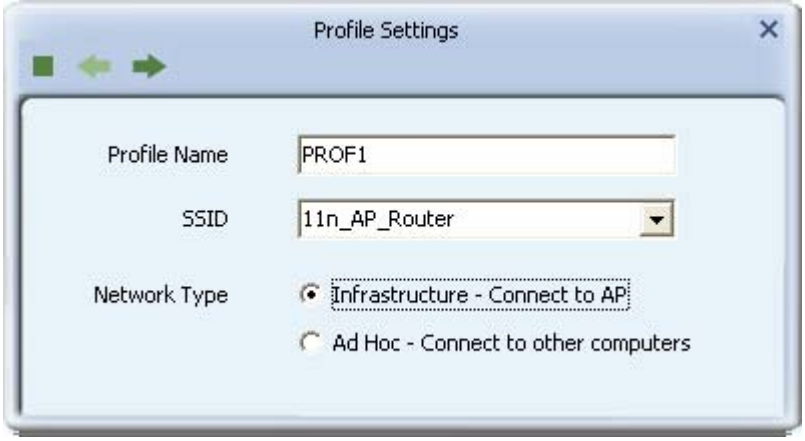
The Wireless Connection Profile Setting Screens

Use these screens to set up a profile or edit existing profile settings for a standard wireless connection.

Profile Buttons	Functions
	Use the left and right arrows to navigate through the Profile Setting screens.
	Click the Stop button to cancel setting up or editing a profile.

The Profile Details Screen

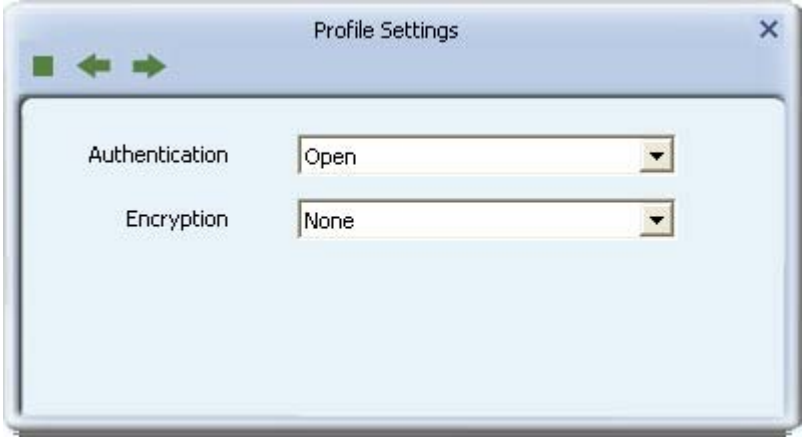
Use this screen to add or edit the name of the profile and its network name and type.



	Functions
Profile Name	Type a name for the profile, or leave at its default value: PROF*, where * is 1, 2, 3, and so on.
SSID	Type the name of the network to which you are connecting, or select an existing network name from the drop-down list provided.
Network Type	Infrastructure: Select this if you are connecting to a typical wireless network maintained by an AP or wireless router. If uncertain, select this option. Ad Hoc: Select this if you are connecting to a distributed network with no AP or router.

The Profile Security Settings Screen

Use these screens to configure authentication and encryption settings on your profile.



	Functions
Authentication	Select the strongest security method supported by your network. Options include Open, Shared, WPA, WPA-PSK, WPA2, WPA2-PSK, 802.1X, CCKM, WAPI-PSK, WAPI-CA.
Encryption	Select the strongest encryption supported by your network and the selected authentication method. Encryption method options for each authentication method are as shown.

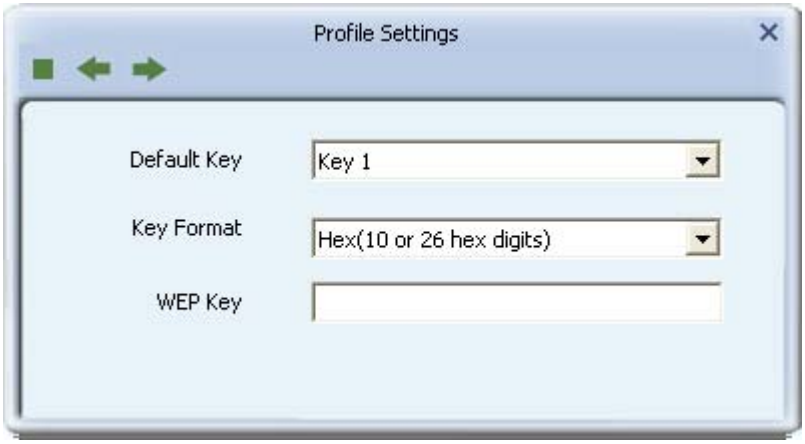
Security Protocol	Encryption Method	Comments
Open Shared	None WEP	Not secure. WEP is an older standard and is easily decrypted. If using WEP select Open a the authentication method for slightly stronger security.
WPA (Wi-Fi Protected Access)	TKIP (Temporal Key Integrity Protocol) AES (Advanced Encryption Standard)	Designed for large enterprises. Requires an authentication server. AES is a stronger, more recent standard than TKIP.
WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key)	TKIP, AES	Designed for home or small business wireless networks. AES is a stronger, more recent standard than TKIP.
WPA2 (Wi-Fi Protected Access 2)	TKIP, AES TKIP MFP (Temporal Key Integrity Protocol (Management Frame Protection)) AES MFP (Advanced Encryption Standard (Management Frame Protection))	Designed for large enterprises. Requires an authentication server. WPA2 is a stronger, more recent standard than WPA. AES is a stronger, more recent standard than TKIP. MFP (management frame protection) offers more security than no MFP.
WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key)	TKIP, AES	Designed for home or small business wireless networks. WPA2-PSK is a stronger, more recent standard than WPA-PSK. AES is a stronger, more recent standard than TKIP.

Security Protocol	Encryption Method	Comments
802.1X	WEP	Designed for large enterprises. Requires an authentication server. WPA and WPA2 are more recent standards.
CCKM (Windows Vista or 7 only)	WEP, TKIP, AES	CCKM allows secured roaming between APs with WDS (wireless domain services) enabled and access to the same RADIUS server.
WAPI-PSK (WLAN Authentication and Privacy Infrastructure - Pre-Shared Key)	SMS4	Designed for home or small business wireless networks. At the time of writing, this standard has not yet been accepted by ISO.
WAPI-CA (WLAN Authentication and Privacy Infrastructure - Certification Authority)	SMS4	Designed for large enterprises. Requires an authentication server. At the time of writing, this standard has not yet been accepted by ISO.

Following descriptions of the screens follow for each type of security.

The WEP Screen

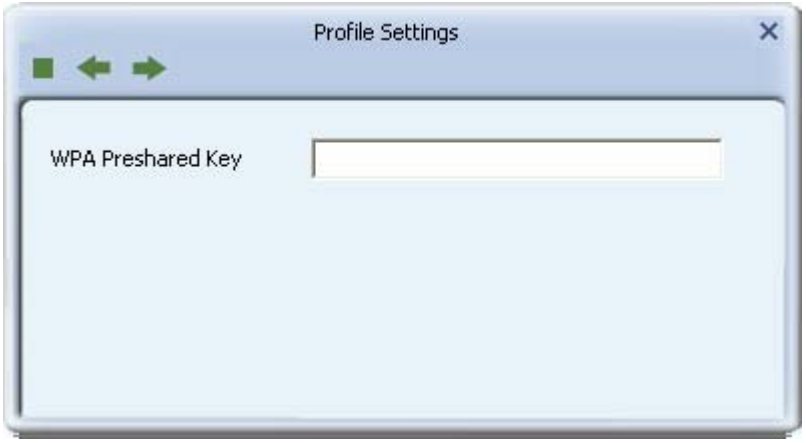
Use this screen to configure WEP security.



	Functions
Default Tx Key	Options are **Key 1** to **Key 4**. Select one of these options.
Key Format	Select a character format for your security passphrase. Options are **Hex(10 or 26 hex digits)** or **ASCII(5 or 13 ASCII characters)**.
WEP Key	Type a security passphrase according to the option you select in the Key Format field. If you select a key format of **Hex(10 or 26 hex digits)**, in the WEP Key field type a security key 10 or 26 characters long made up of digits **0**-**9** and letters **A**-**F**. If you select a key format of **ASCII(5 or 13 ASCII characters)** in the WEP Key field, type a security key 5 or 13 characters long made up of digits **0**-**9** and letters **a**-**z** and **A**-**Z**.

The WPA-PSK or WPA2-PSK Screen

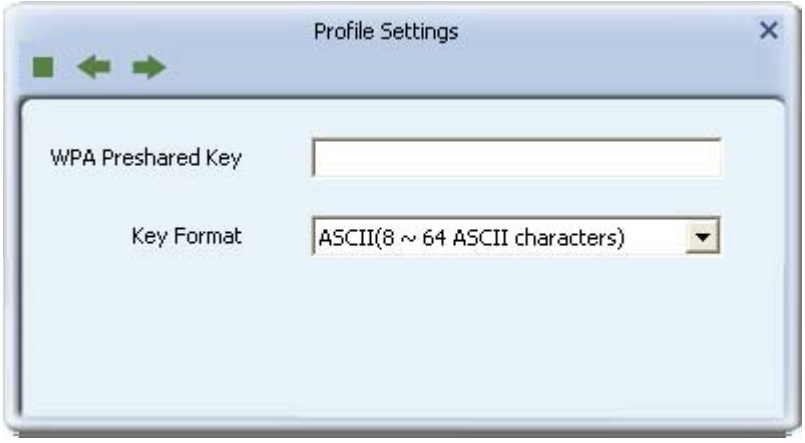
Use this screen to configure WPA-PSK or WPA2-PSK security.



	Functions
WPA Preshared Key	Type a passphrase 8-63 characters long made up of characters **0**-**9**, **a**-**z**, **A**-**Z**, keyboard symbols and spaces.

The WAPI-PSK Screen

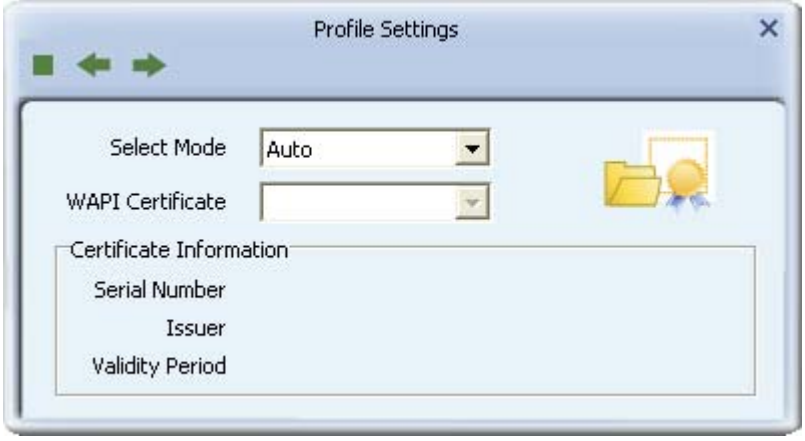
Use this screen to configure WAPI-PSK security.



	Functions
WPA Preshared Key	Type a security passphrase according to the option you select in the Key Format field. If you select a Key Format of **Hex(8~64 hex digits)**, in the **WPA Preshared Key** field type a security key 8-64 characters long made up of digits **0**-**9** and letters **A**-**F**. If you select a Key Format of **ASCII(8 or 64 ASCII characters)** in the **WPA Preshared** Key field, type a security key 8-64 characters long made up of digits **0**-**9** and letters **a**-**z** and **A**-**Z**.
Key Format	Options are **Hex(8~64 hex digits)** or **ASCII(8 or 64 ASCII characters)**.

The WAPI-CA Screen

Use this screen to configure WAPI-CA security.



	Functions
Select Mode	Options are **Auto** or **Manual**. Select **Auto** to automatically apply WAPI certificates installed on your system. Select **Manual** to manually select a WAPI certificate installed on your system from the drop-down list in the **WAPI Certificate** field.
WAPI Certificate	This option is available if **Auto** in **Select Mode** is selected. Select a WAPI certificate from the drop-down list for use in applying WAPI security
	Click this button to browse for WAPI certificates on your system.

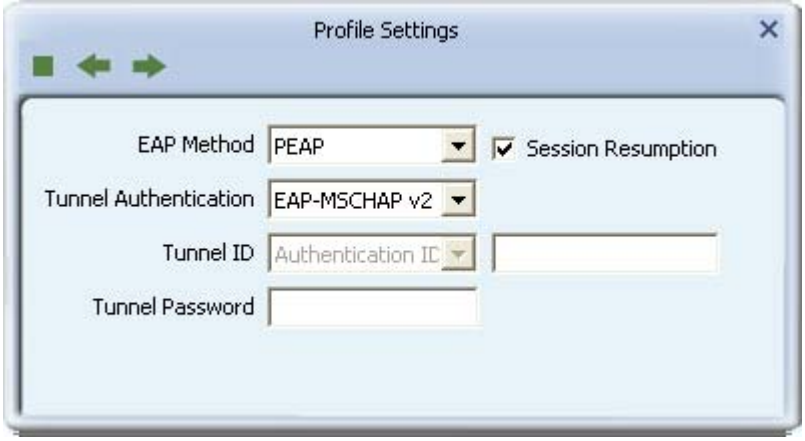
Certificate Information - This information is only available when a WAPI certificate is selected from the **WAPI Certificate** drop-down list.

	Functions
Serial Number	Shows the unique identifier of the WAPI certificate.
Issuer	Shows the organization that issued the WAPI certificate.
Valid Period	Shows the validity period of the certificate in month/day/year format.

The 802.1X, CCKM, WPA or WPA2 Screens

Use the following screens to configure authentication and tunnel methods required by 802.1X. CCKM, WPA and WPA2 security.

The EAP Method Screen



	Functions
EAP Method	Select an EAP (Extensible Authentication Protocol) Method. Options are PEAP, TLS/Smart Card, TTLS (XP only), EAP-FAST, MD5-Challenge (available only with 802.1X using Windows XP), and LEAP.
Session Resumption	Select this option to make use of the previous session's settings for faster re-authentication
Tunnel Authentication	Select a security method to use when accessing the authentication server. Options depend on the the EAP method selected.
Tunnel ID	Options are **Authentication ID** and **Machine ID**. If **Authentication ID** is selected, user-based credentials are required. If **Machine ID** is required, credentials are based on the computer requesting access to the authentication server.
Tunnel Password/Mode	**Tunnel Password** refers to the password set for the user or computer accessing the authentication server. 'Tunnel Mode' options may include **Static Password**, **Soft Token**, **Windows Logon** (Windows Vista/7 only), and **Prompt User**(Windows Vista/7 only). If tunnel mode is set to **Static Password**, the user authenticates once for the duration of the session. If tunnel mode is set to **Soft Token**, the user must authenticate, based on the time-out period of the soft token. If **Windows Logon** is selected, user credentials are based on the user's Windows account. If **Prompt User** is selected, user credentials are requested on connecting to the network.

The following table shows the options for this screen.

Authentication Method	Tunnel Authentication	Tunnel Mode	Tunnel ID	User Name/ Password Required
PEAP	EAP-MS-CHAP v2	n/a	n/a	Y/Y
	EAP-TLS/Smart Card	n/a	Authentication ID	Y/N (XP) N/N (Vista/7)
			Machine ID	N/N
	Generic Token Card	Static Password	n/a	Y/Y
		Soft Token		N/N
		Windows Logon (Vista/7)		N/N
		Prompt User (Vista/7)		N/N
TLS/Smart Card	n/a	n/a	Authentication ID	N/N
			Machine ID	N/N
TTLS (XP only)	CHAP, MS-CHAP, MS-CHAP v2, PAP, EAP-MD5	n/a	Authentication ID	N/Y
			Machine ID	N/Y
EAP-FAST	EAP-MSCHAP v2 (XP)	n/a	Authentication ID	N/Y
			Machine ID	N/Y
	EAP-TLS/Smart Card (XP)	n/a	Authentication ID	N/N
			Machine ID	N/N
	Generic Token Card (XP)	Static Password	Authentication ID	Y/Y
			Machine ID	N/Y
		Soft Token	Authentication ID	N/N
			Machine ID	N/N

Authentication Method	Tunnel Authentication	Tunnel Mode	Tunnel ID	User Name/ Password Required
MD5-Challenge (XP, 802.1X)	n/a	n/a	n/a	Y/Y
LEAP	n/a	Static Password (Vista/7)	n/a (Vista/7)	Y/Y
		Windows Logon (Vista/7)		N/N
		Prompt User (Vista/7)		N/N
		n/a (XP)	Authentication ID	N/Y
			Machine ID	N/Y

The screens that follow depend on certification method employed.

The Server Certification Screen

This screen appears for all PEAP and TTLS (XP only) methods.
Use this screen to configure access to server certificates.

	Functions
Use Server Certification	Select this to use certificates supplied by the authentication server. From the drop-down list, select the server that issues the certificate.
Allow intermediate certificates	(For Windows XP users only) Select this to allow the use of certificates supplied by a computer located in the certificate chain connecting the server certificate and the server specified in the 'Server Name' field.

The User Certification Screen

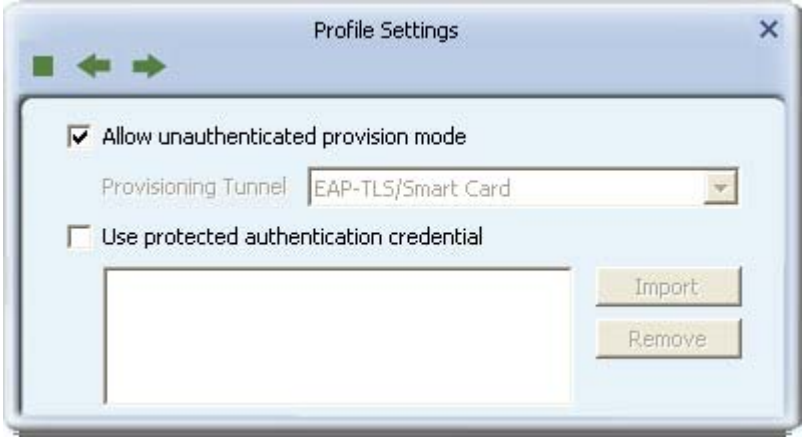
This screen appears for the following EAP and tunnel methods.
PEAP-EAP-TLS/Smart Card
TLS/Smart Card
All tunnel ID methods using TTLS (Windows XP only)

Use this screen to select a user certificate located on the user's computer.

	Functions
Use a certificate on this computer	Select this checkbox to set up security using a user certificate. This field may be grayed out with or without the checkbox selected, depending on whether you are using security which requires a user certificate or not. Otherwise the use of a user certificate is optional.
Issued to	This read-only field indicates the name of the user to whom the certificate was issued.
Issued by	This read-only field indicates the name of the authentication server which issued the certificate.
Expiration Date	This read-only field indicates the date on which the user certificate expires.
Friendly Name	This read-only field indicates the name assigned to the certificate for easy recognition.
Use my smart card	(Vista/Windows 7 only) Select this option to support smart card-based user authentication.

The PAC Screen

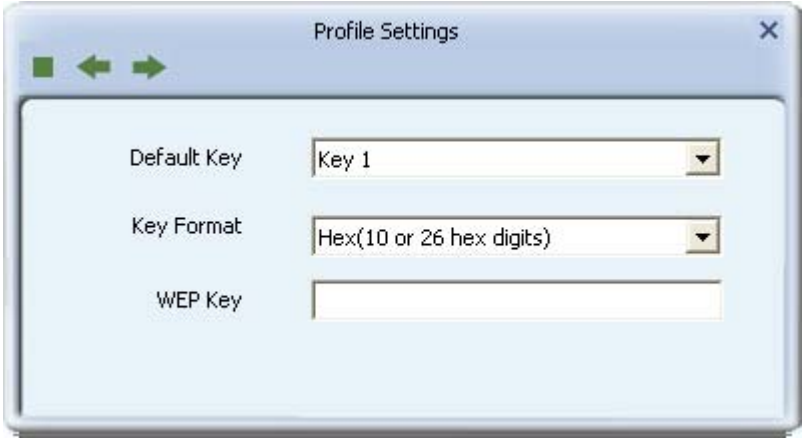
The PAC ScreenThis screen appears for EAP-FAST authentication (for Windows XP users only).



	Functions
Allow unauthenticated provision mode	Select this option to allow unauthenticated users to obtain a PAC (protected authentication credential) from the authentication server.
Provisioning Tunnel	This is the security method selected in the previous screen which is used to encrypt the PAC distribution procedure.
Use protected authentication credential	Select this option to allow the manual installation of a PAC.
Import	Click this button to locate and install a PAC.
Remove	Click this button to uninstall the selected PAC.

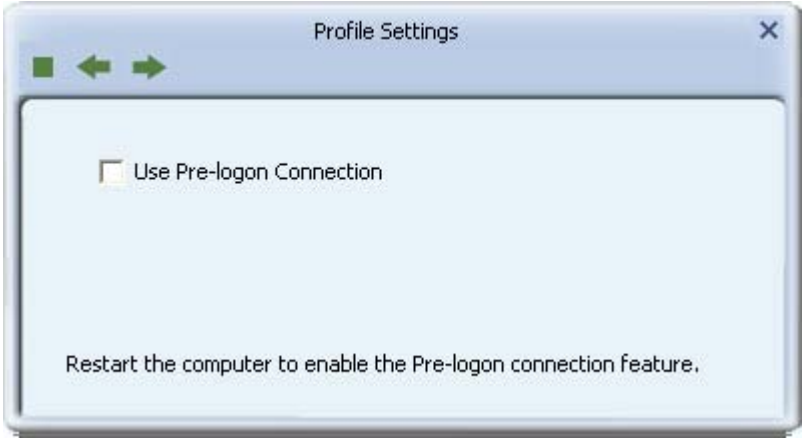
The WEP Screen

This screen appears for MD5-Challenge authentication (for Windows XP users only). See the WEP screen description above for details.



The Pre-Logon Screen

Use this screen to enable automatic connection using a profile upon starting Windows. This option is only available for profiles with WEP, WPA-PSK, WPA2-PSK, EAP-FAST, and EAP-LEAP configured.



	Functions
Use Pre-logon Connection	Select this option to enable automatic connection on system startup to a wireless network based on your profile settings.

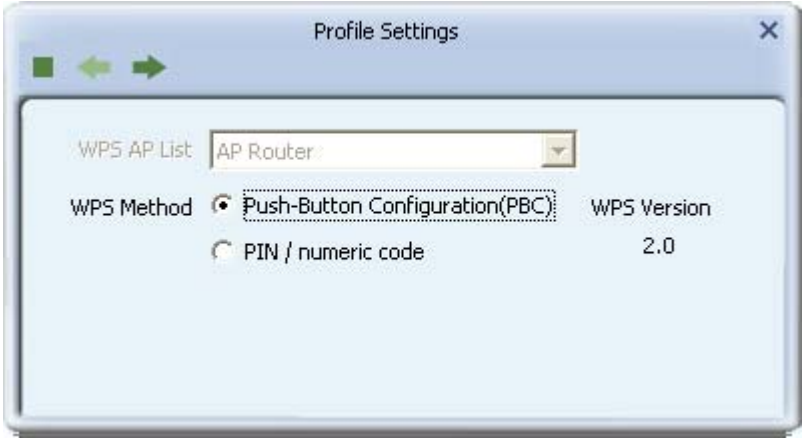
The WPS Profile Screens

Use these screens to configure a WPS profile.

WPS Profile Buttons

Profile Buttons	Functions
	Use the left and right arrows to navigate through the WPS profile screens.
	Click the Stop button to cancel setting up or editing a WPS profile.

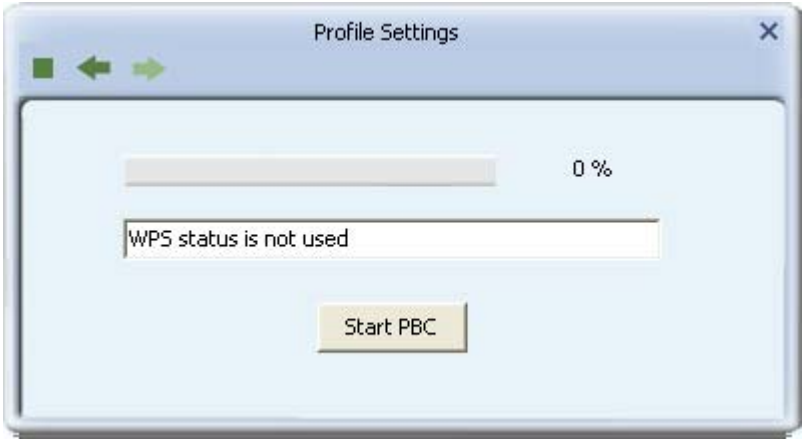
The WPS Profile Details Screen



Profile Buttons	Functions
WPS AP List	Displays a list of available WPS-enabled networks from a drop-down list.
WPS Method	**Push-Button Configuration(PBC):** This option allows you to use a push-button available on the external casing of your device or in its software interface to set up WPS. **PIN / numeric code:** This option allows you to manually transfer a PIN either from the device the device to which you are connecting to the Utility, or from the Utility to the device to which you are connecting.

The Push-Button Method Screen

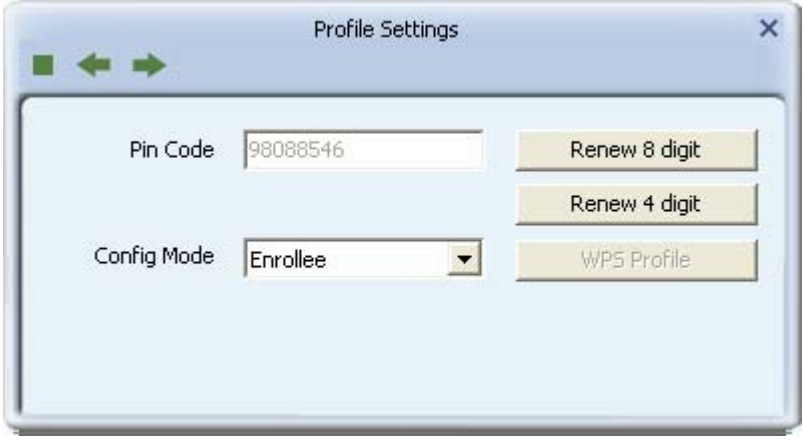
Use this screen to begin the WPS connection process using the push-button method.



Profile Buttons	Functions
Start PBC	Click this button to begin the WPS connection process. The corresponding WPS button available on the device to which you are connecting must be push within 120 seconds of this button.

The PIN Method Screen

Use this screen to set up a WPS connection using a PIN.



Profile Buttons	Functions
PIN Code	Displays the PIN used in this WPS connection. If **Enrollee** is selected in the **Config Mode** field, use this PIN to begin the WPS setup procedure on the device to which you are connecting. If **Registrar** is selected in the **Config Mode** field, locate the WPS PIN made available on the device to which you are connecting and type the PIN in this field.
Renew 8 digit	Click this button to display a new 8 digit PIN in the **PIN Code** field.
Renew 4 digit	Click this button to display a new 4 digit PIN in the **PIN Code** field.
Config Mode	From the drop-down list select **Enrollee** to use the PIN provided in the screen to set up a WPS connection, or select **Registrar** to use the PIN provided by the device to which you are connecting to set up a WPS connection.
WPS Profile	This option is only available when **Registrar** is selected in the **Config Mode** field. Click this button to configure the name of the WPS connection and its security settings. These settings may be left at their default.

The WPS Profile Screen

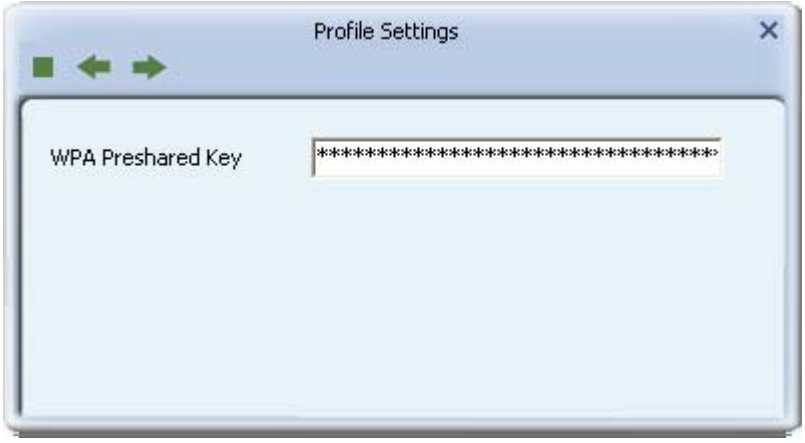
Use this screen to configure the name of your WPS connection and its security settings.

Profile Buttons	Functions
SSID	Type the name of your WPS connection. The name of this connection does not affect the name given for the entire network to which you are connecting.
BSSID	This is the MAC address of the Ralink adapter.
Authentication	Select the strongest security method supported by your network. Options include Open, Shared, WPA-PSK, or WPA2-PSK.
Encryption	Select the strongest encryption supported by your network and the selected authentication method. Options for each authentication method are as shown in the following table

Authentication Method	Encryption Method	Comments
WPA2-PSK (Wi-Fi Protected Access 2- Pre-Shared Key)	AES (Advanced Encryption Standard)	Select WPA2-PSK and AES for faster and stronger wireless security.
WPA-PSK/WPA2-PSK (Wi-Fi Protected Access - Pre-Shared Key/ Wi-Fi Protected Access 2 - Pre-Shared Key)	TKIP/AES (Temporal Key Integrity Protocol/ Advanced Encryption Standard)	Select WPA-PSK/WPA2-PSK and TKIP/AES if devices in your network do not support WPA2-PSK and AES.
Open	None	Not recommended.

The WPS WPA-PSK Screen

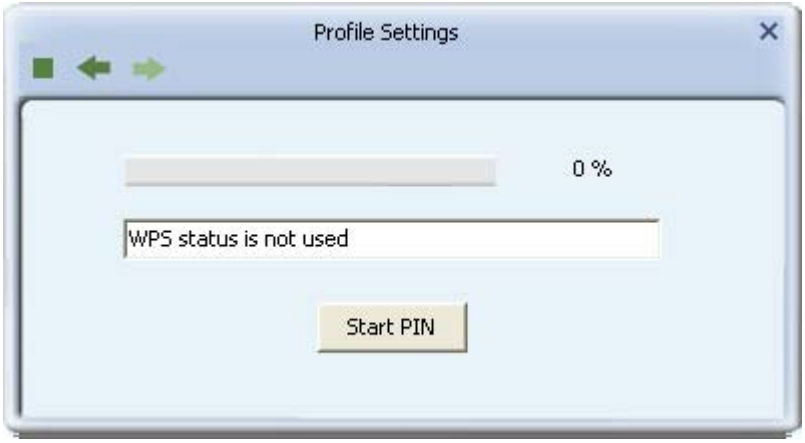
Use this screen to configure a passphrase for your WPS connection.



	Functions
WPA Preshared Key	Type a passphrase 8-63 characters long made up of characters **0**-**9**, **a**-**z**, **A**-**Z**, keyboard symbols and spaces.

The Start PIN Screen

Use this screen to start the WPS connection process using a PIN.



	Functions
Start PIN	This screen appears for both PIN methods. Click this button to begin the WPS connection process using a PIN. At the same time (within 120 seconds) activate the corresponding WPS PIN connection function on the device to which you are connecting.

The Advanced Screens

Use these screens to configure advanced settings including channel selection, wireless mode, certificate management, and ad hoc mode.

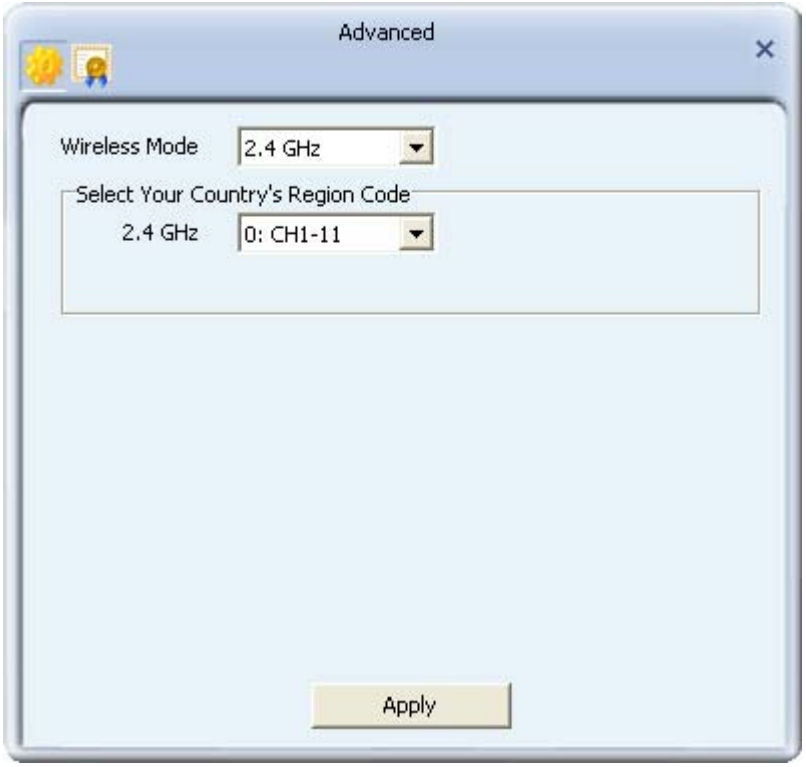
Advanced Buttons

Use the following buttons to navigate between the Advanced screens.

	Functions
	Click this button to access the Advanced screen and configure wireless mode settings.
	Click this button to access the Certificate Management screen to install and manage WAPI certificates.

The Advanced Screen

Use this screen to configure the wireless mode of your adapter.



NOTE: This screen shows options supported by an IEEE 802.11n adapter. Other adapters may support different options.

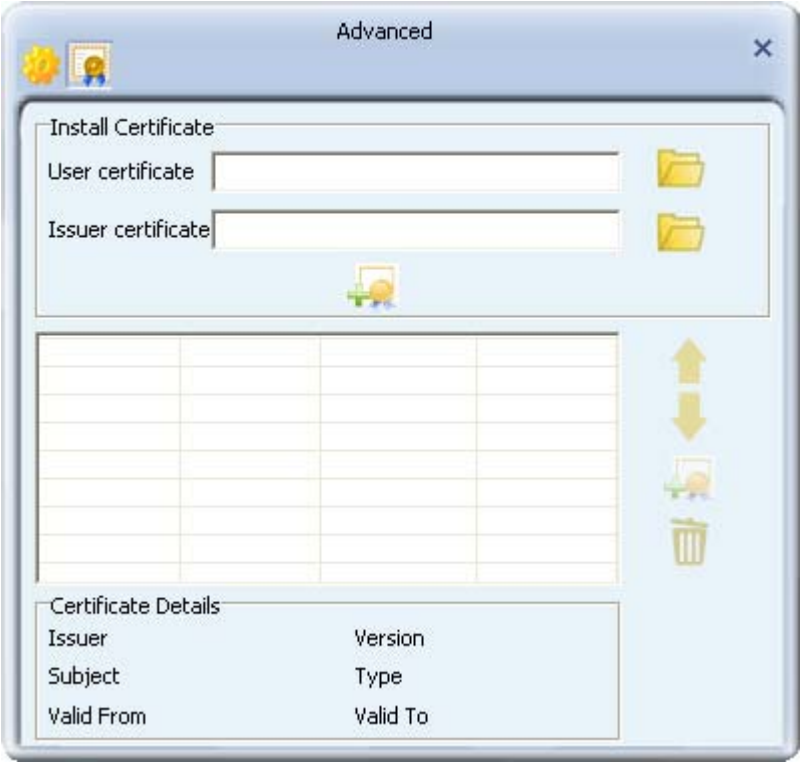
	Functions
Wireless Mode	Select the wireless mode that is compatible with the standards supported by the devices on your network. IEEE 802.11b/g/n all support 2.4 GHz. If uncertain, leave this setting at its default value.
Select Your Country Region Code	**2.4 GHz:** This field displays if IEEE 802.11b/g/n standards are supported. From the drop down list, select the appropriate code for your region. If uncertain, leave this setting at its default value.
Apply	Click Apply to save your changes.

The Certificate Management Screens

Use these screens to manage WAPI certificates for use in authenticating users and handling encryption. See Setting Up Enterprise Security: WAPI-CA for instructions on using certificates for user authentication.

The Certificate Management Screen

Use this screen to install WAPI user and issuer certificates.



	Functions
User certificate	Click on the browse icon to locate and load a WAPI user certificate. Only WAPI (.cer) certificates are supported.
Issuer certificate	Click on the browse icon to locate and load a WAPI issuer certificate. Only WAPI (.cer) certificates are supported.
	Click on the Install button to verify the user and issuer certificates. Once verified the authentication server unit (ASU) certificate is automatically downloaded and installed.
	If more than one ASU certificate is installed, click the Up and Down arrows to move the selected certificate up and down respectively. If the Ralink Utility is set to automatically detect a valid ASU, ASUs are examined in the order indicated in this screen. (See the Profile Settings: WAPI-CA security screen for instructions on setting automatic detection of valid ASUs.
	Click on the Delete button to remove the selected certificate from the certificate list.
	If the authentication server is located on a device external to the network's AP, click on the second Install button to install an ASU certificate.

Window field descriptions

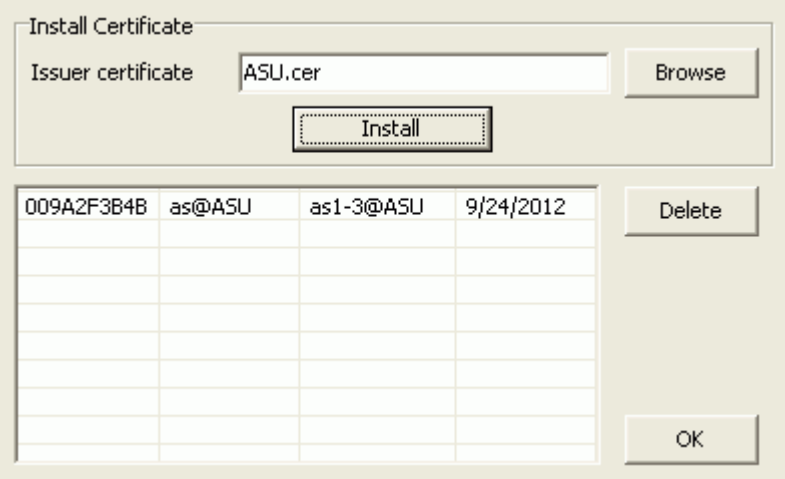
009A2F3B4B	as@ASU	as1-3@ASU	9/24/2012
1	2	3	4

	Functions
1	The ID number for the ASU
2	Issuer of the ASU.
3	Subject given for the ASU.
4	The date to which the ASU is valid.

Certificate Detail	Functions
Issuer	The issuer of the selected ASU.
Subject	Subject given for the ASU.
Valid From	The date from which the ASU is valid.
Version	The certificate version.
Type	This shows the type of the certificate.
Valid To	The date to which the ASU is valid.

The Install AS Screen

Use this screen to install a WAPI authentication server certificate.



	Functions
Issuer certificate	The authentication server unit (ASU) certificate.
Browse	Click this button to locate and select the ASU certificate to be installed.
Install	Click this to install the ASU certificate.
Delete	Click this to remove the ASU certificate from the list.
Type	This shows the type of the certificate.
OK	Click this to save your settings.

Window field descriptions

1	2	3	4
009A2F3B4B	as@ASU	as1-3@ASU	9/24/2012

	Functions
1	The serial number for the selected ASU certificate.
2	The issuer of the selected ASU certificate.
3	The given subject description for the selected ASU certificate.
4	The date to which the selected ASU certificate is valid.

The About Screen

Use this screen to find information on the Utility including version number and firmware.

	Functions
Utility	Shows the version number of the Utility. Wi-Fi Direct is supported by versions 4.1.3.0 and above.
Driver	Shows the driver version of this driver. Versions 3.2.4.0 and above support Wi-Fi Direct.
SDK	Shows the software development kit (SDK) provided for downstream developers.
Date	Shows the date of release for the utility version shown.
Date	Shows the date of release for the driver version shown.
Date	Shows the date of release for the SDK version shown

	Functions
MAC Address	The unique hexadecimal hardware identifier assigned to your Adapter.
Ralink	Click to connect to the Ralink web site.

The Compact Mode Screen (AP Mode)

From the compact mode screen in AP Mode, use the Utility to set up an access point (AP), control access to the AP based on MAC address.
The Utility in compact mode shows the AP status of the Adapter.

Click these buttons to open the following screens.

	Functions
	Use the AP Setup screen to set up a secure wireless network.
	Use the Advanced screen to configure advanced network settings.
	Use the Access Control List screen to configure an access policy for your network based on a client's MAC address.
	Use the Connected Devices screen to find information on clients currently connected to your network.
	Use the About screen to find information on specifications for the Utility.

The Utility also provides information and tools to manage your wireless connection.

	Functions
	Use the AP Setup screen to set up a secure wireless network.
	Indicates the security status of your connection.
	Indicates AP Mode is enabled.

Provides information on network settings.

	Functions
SSID	This displays the name of your wireless network
Mode	Indicates the mode and hence frequency supported by your wireless connection.
Channel	The channel assigned to your connection. Default is 6, options are 1-13.
IP	The IP address identifies your Adapter on your wireless network.
Mask	The subnet mask hides your IP address from outside your wireless network.

The AP Setup Screens

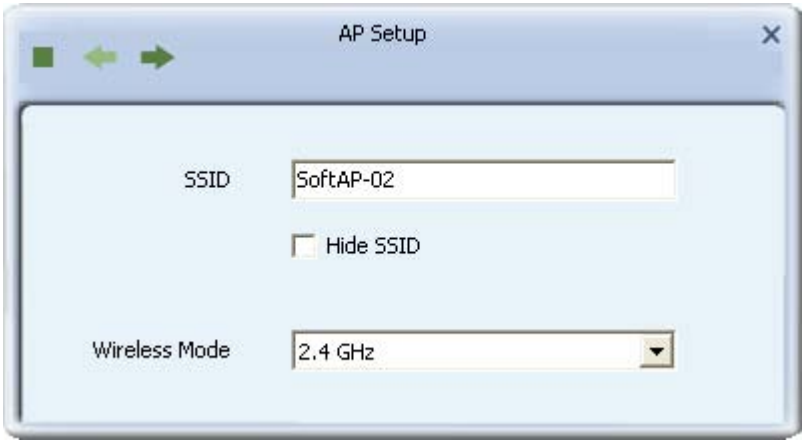
The AP Setup screens let you configure access point settings when the Utility is set to AP (access point) mode. Use these screens to set up a secure wireless network and manage access to the network.

The AP Setup Screens

The AP Setup screens let you configure access point settings when the Utility is

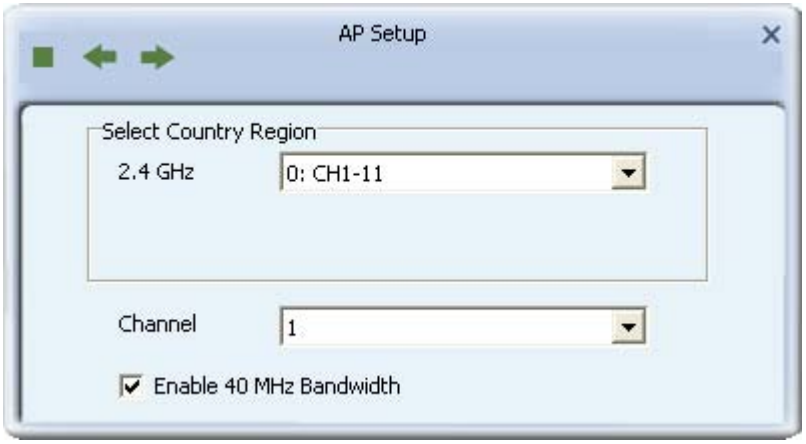
	Functions
	Use the left and right arrows to navigate through the AP Setup screens.
	Click the Stop button to cancel setting up your AP.

The Network Settings Screen



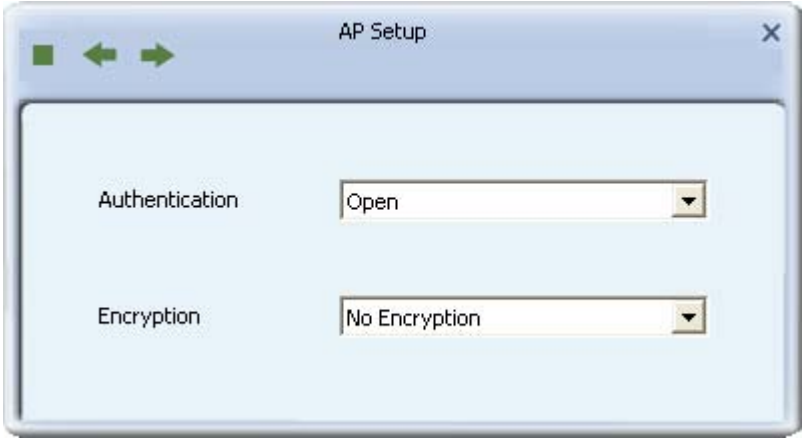
	Functions
SSID	This is the name of your network. Leave it at its default setting, or type a name for ease of use when accessing your network.
Hide SSID	Select this optional setting to hide the name of your network from unauthorized computers or devices.
Wireless Mode	Select the wireless mode that is compatible with the standards supported by the devices on your network. IEEE 802.11b/g/n all support 2.4 GHz and IEEE 802.11a/n all support 5 GHz. If uncertain, leave this setting at its default value.

The Channel Settings Screen



	Functions
Select Country Region: 2.4 GHz / 5 GHz	This indicates the **Wireless Mode** selected in the previous Network Settings screen. From the drop-down list, select the appropriate code for your region. For more information on the channels available for each region, see the Country Channel List.
Channel	Leave at its default value, or if interference is a problem on your network, choose a channel which experiences less interference. If you select **Enable 40 MHz Bandwidth**, choose a channel with minimal interference on the four channels adjacent to your selected channel.
Enable 40 MHz Bandwidth	Select this option to increase the bandwidth available for your wireless connection. This function works by incorporating the bandwidth available on the four channels adjacent to your selected channel. This option is only supported by IEEE 802.11n devices. If a computer or device connected to the AP does not support this function, bandwidth is reduced to its default level.

The Security Settings Screen



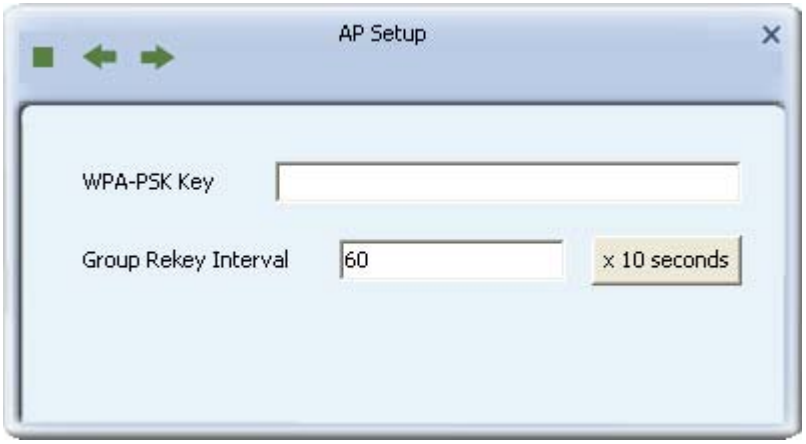
	Functions
Authentication	Select the strongest security method supported by your network. Options include Open, Shared, WPA-PSK, WPA2-PSK, or WPA-PSK/WPA2-PSK.
Encryption	Select the strongest encryption supported by your network and the selected authentication method. Options for each authentication method are as shown in the following table.

Authentication Method	Encryption Method	Comments
WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key) WPA-PSK/WPA2-PSK	AES (Advanced Encryption Standard) TKIP (Temporal Key Integrity Protocol) BOTH (WPA2-PSK only)	WPA2-PSK is a faster, more recent authenitcation standard than WPA-PSK. AES is a stronger, more recent encryption standard than TKIP. Selecting WPA-PSK/WPA2-PSK and BOTH allows the network to automatically adjust authentication and encryption methods to the strongest security supported by your network.

Authentication Method	Encryption Method	Comments
Open Shared	WEP (Wireless Encrypted Privacy)	WEP is an older standard and is easily decrypted. If using WEP select Open as the authentication method for slightly stronger security.

The WPA-PSK, WPA2-PSK or WPA-PSK/WPA2-PSK Security Screen

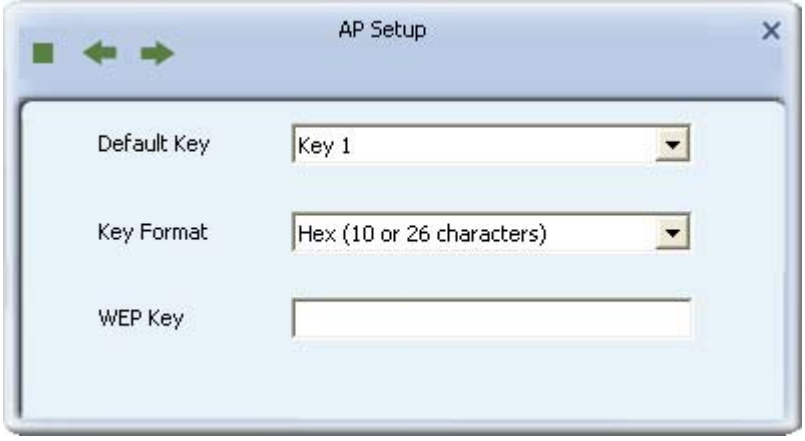
Use this screen to set up WPA-PSK, WPA2-PSK, or WPA-PSK/WPA2-PSK security on your network.



	Functions
WPA-PSK Key	Type a security key 8-63 characters long made up of characters **0**-**9**, **a**-**z**, **A**-**Z**, keyboard symbols and spaces.
Group Rekey Interval	The interval after which the AP resets the group key. This key supports wireless security on your network. If uncertain, leave at its default value.
x 10 seconds	Sets the unit for the 'Group Key Interval' to 10 seconds. After the specified period the group key is reset.
x 1000 packets	Sets the unit for the Group Key Interval to 1000 packets. After sending the specified number of packets the group key is reset.

The WEP Security Screen

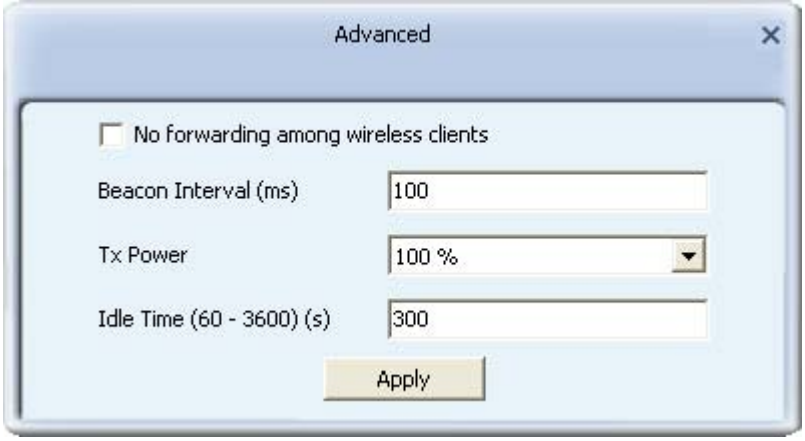
Use this screen to set up WEP security on your network.



	Functions
Default Tx Key	Options are **Key 1** to **Key 4**. Select one of these options.
Key Format	Select a character format for your security passphrase. Options are **Hex(10 or 26 hex digits)** or **ASCII(5 or 13 ASCII characters)**.
WEP Key	Type a security passphrase according to the option you select in the Key Format field. If you select a key format of **Hex(10 or 26 hex digits)**, in the WEP Key field type a security key 10 or 26 characters long made up of digits **0**-**9** and letters **A**-**F** If you select a key format of **ASCII(5 or 13 ASCII characters)** in the WEP Key field, type a security key 5 or 13 characters long made up of digits **0**-**9** and letters **a**-**z** and **A**-**Z**.

The Advanced Screen (AP Mode)

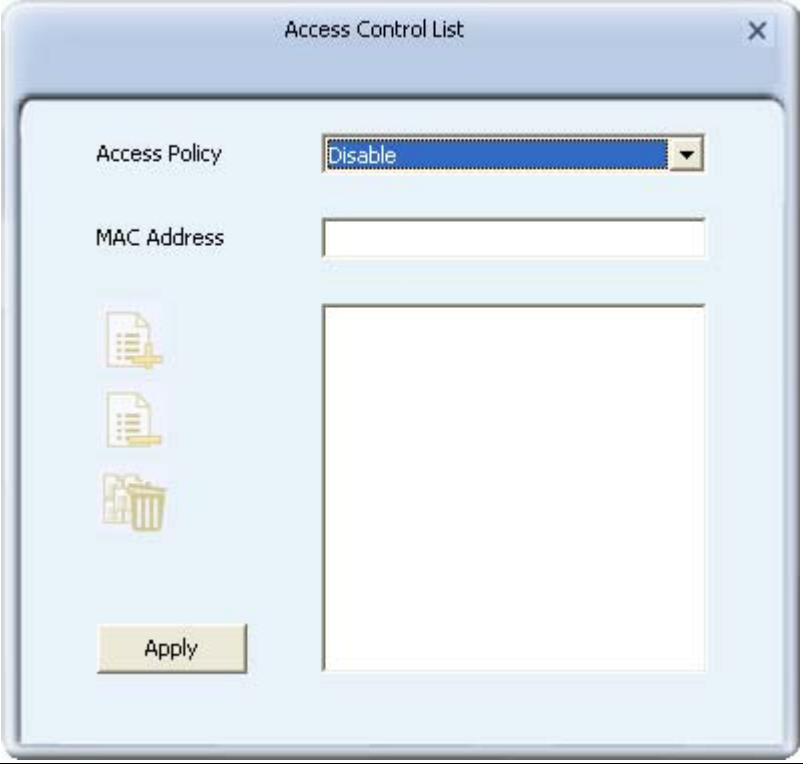
Use this screen to configure packet forwarding, the beacon interval, transmission power and idle time.



	Functions
No forwarding among wireless clients	If selected, this disables the forwarding of packets by the AP or router of packets sent by wireless clients to other wireless clients in the same network.
Beacon Interval (ms)	Default = 100 ms. The interval between beacon frames.
Tx Power	Default = 100%. The power of the transmitted signal as a percentage of maximum power. Options include 100%, 75%, 50%, 25%, and Low.
Idle time (60 - 3600) (s)	Default = 300s. The maximum time a connected computer or device can be idle before it is disconnected from the network.
Apply	Click Apply to save your changes.

The Access Control List Screen

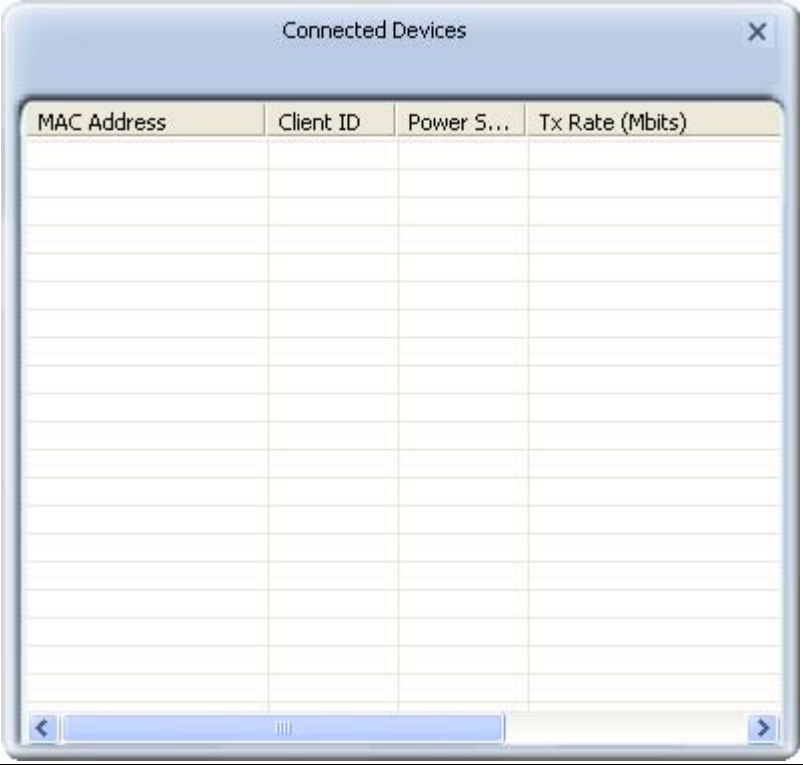
The Access Control List records the MAC addresses of clients for use when allowing or disallowing transmission on the network. Use the Access Control List to configure an access policy for your network based on a client's MAC address.



	Functions
Access Policy	Options include Disable (default), Reject All, and Allow All. **Disable:** Disables access control to your network based on MAC address. **Reject All:** All packets with a source MAC address matching those in the access control list cannot access your network. **Allow All:** All packets with a source MAC address matching those in the access control list have access to your network.
MAC Address	Type a MAC address in hexadecimal format without additional characters (e.g. colons or hyphens).
	Adds the MAC address in the MAC Address field to the MAC address control list.
	Removes the selected MAC address from the MAC address control list.
	Removes all MAC addresses from the MAC address control list.
Apply	Saves all changes made to the MAC address control list.

The Connected Devices Screen

The Connected Devices screen shows detailed information on current connections.



	Functions
MAC Address	The unique hexadecimal manufacturer-assigned identifier of a device connected to the AP.
Client ID	An ID number assigned to each device on your AP's network, starting at 2 with a maximum of 32.
Power Saving Mode	Indicates whether the connection with the associated device supports power-saving.
Tx Rate (Mbits)	Provides detailed information on factors affecting the data transfer rate. IEEE 802.11n specific information includes the MCS (modulation and coding scheme) index value applied in a connection, the BW (bandwidth), GI (guard interval), and the transmission rate of the current connection in megabits (Mbit).

The About Screen (AP Mode)

Use this screen to find information on specifications for the Utility

	Functions
Utility Version	Shows the version number of the Utility (different from the utility version in station mode).
Driver Version	Shows the version number of this driver (the same as that in station mode).
DLL Version	Displays the version number of the RaAPAPI.dll file, for use by downstream developers.
Date	Shows the date of release for the utility version shown.
Date	Shows the date of release for the driver version shown.
Date	Shows the date of release for the DLL version shown.
MAC Address	The unique hexadecimal identifier assigned to the Ralink Adapter.

Uninstall

Step 1:

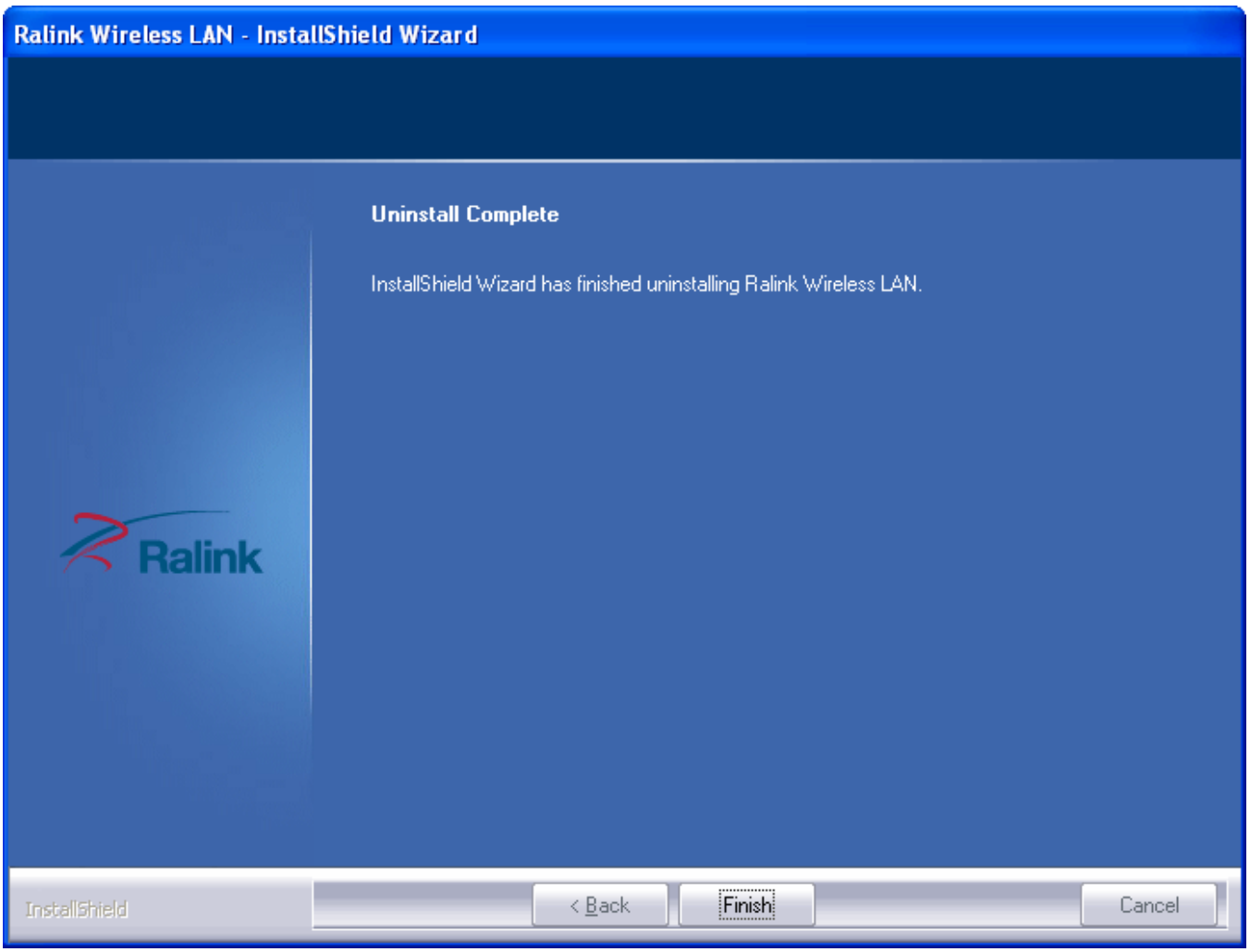
Click **" Start -> All Programs -> Ralink Wireless -> Uninstall - RT2860 "**.

Step 2:

Click **" Yes "**.

Step 3:

Click **" Finish "**.



Troubleshooting

The Troubleshooting section contains suggestions to problems using the Utility. Click on the following links to navigate to a problem area.

Not All Features are Available.

The Wi-Fi Direct button does not work.

If the transmitter icon displays as shown , click on it to enable transmission and to enable Wi-Fi Direct functionality.

The Profile button , the Advanced button , and the Connect button do not work.

The Utility is set to **Windows Zero Configuration mode** so these functions are unavailable while Windows manages the Adapter. To enable these features, right-click on the Utility icon in the bottom right corner of your screen. In the menu that displays, select **Use RaConfig as Configuration Utility** to enable these buttons.

The Profile button and the Advanced button do not work.

If you are logged on to Windows using a guest account, then these features are not available. Log out of Windows and log back in using an account with user or administrator permissions.

A warning message displays when I try to enable AP Mode and/or enable client mode.

Disable other non-Ralink wireless cards. In Windows go to Network Connections, right-click on all wireless connections displayed which do not use the Ralink Adapter, and select Disable.

Client mode or AP mode options are not available.
Ensure that you are not logged into Windows using the Guest account. When you are logged in to the Guest account in Windows XP or Vista, AP mode is not available. When you are logged in to the Guest account in Windows 7, neither client nor AP mode are available. To use these options, log out of Guest mode and log in as a user or administrator.

I Can't Connect to a Network.

I cannot find the name of my wireless network in the Available Networks screen.
a. If the Available Networks screen shows no available networks, check the Ralink icon in the bottom right of your screen. If the 'Ralink Wireless LAN Card Not exist' icon displays, ensure your Ralink adapter is correctly installed. Alternatively, check transmission is enabled as indicated by the transmission icon in the main screen .

b. Check the AP (access point) for your wireless network is turned on and is transmitting.

c. Click the Rescan button in the Available Networks screen.

d. Check the network name (SSID) settings on your AP. Check you have the correct SSID name and that broadcasting of the SSID is enabled.

I can see the name of my wireless network, but I can not connect to it. The Ralink icon displays as shown , indicating a disconnected status.
a. Check the network settings of your AP. You may be required to enter security settings.

b. Check you have entered the correct security settings.

c. Check the AP's MAC access policy has given you permission to access the AP.

d. Check the AP has DHCP enabled.

I can not remember my security settings (e.g. security key or password).
a. Check the security settings on your AP to find out its security settings.

b. Reset the AP to its default settings, and access the AP using the default security settings.

The Quality of My Connection is Bad.

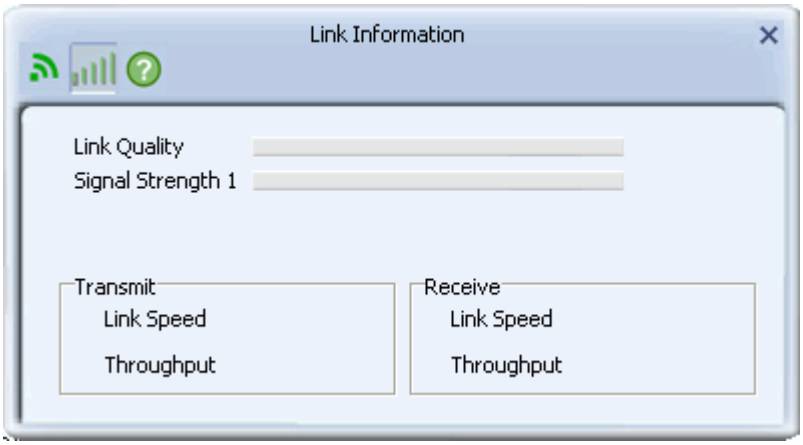
I am not sure whether signal quality is a problem.
Check the Ralink icon in the bottom right of your screen.

- Indicates a good connection and signal strength.

- Indicates a normal connection and signal strength.

- Indicates a weak connection and signal strength.

Alternatively, click on the Link Information button and then the Throughput button to check information on the link quality and signal strength.



The Ralink Utility indicates I have a weak connection. How can I increase the signal strength of my wireless connection?
a. Move the adapter closer to the AP. Avoid shielded locations, or locations experiencing interference.
b. Set your wireless connection to the least used network channel.
c. Upgrade your hardware to the latest wireless standards.

I Can't Use WPS.

When I start the WPS connection process, one of the following error messages displays.
No PBC AP available - Ensure you have started the WPS connection process on both devices, within 120 seconds of each other.
Too Many PBC APs available - There is more than one other device using WPS to connect to your device. Wait several minutes, then begin the WPS connection process on the two devices you are connecting.
WPS EAP process failed - You may have entered the wrong PIN. Repeat the WPS connection process, this time correctly, entering the PIN in the device to which you are connecting.
An inappropriate EAP-FAIL received - The device to which you were connecting was unable to process the WPS connection. Ensure it is turned on with WPS enabled.
Error PIN Code - Repeat the WPS connection process, this time correctly, entering the PIN in the device to which you are connecting.

I Can't Set Up a Wireless Network.

Other devices cannot see my AP.
Check the network name (SSID) settings on your AP. Check you have the correct SSID name and that transmission of the SSID is enabled.

Other devices cannot connect to my AP.
Check the network settings of the AP match those of devices you are connecting to. Check DHCP is enabled and that the MAC addresses of connecting devices have permission to access the AP.

Other devices cannot connect to the Internet through my AP.
Check you have correctly followed the instructions in Sharing Internet Access and have a working connection to the Internet from your AP.

I Can't Use Wi-Fi Direct.

I cannot see the Wi-Fi Direct button (Windows 7 only).

Due to Windows behavior, sometimes the Wi-Fi Direct function is disabled in Windows 7. To enable Wi-Fi Direct and make the Wi-Fi Direct button visible, in Windows 7, go to Control Panel\Network and Internet\Network Connections, right-click on a Network Connection such as Bluetooth, and select "Enable".

The Wi-Fi Direct button does not work.

If the transmitter icon displays as shown , click on it to enable transmission and to enable Wi-Fi Direct functionality.

I cannot see the computer or device to which I want to connect.

a. Right-click on the notebook icon, and click Scan.
b. Ensure Wi-Fi Direct is enabled on the device to which you connecting.
c. Ensure the computer or device to which you are connecting is within range and not shielded in any way.

I can see a device in the Wi-Fi Direct screen, but I cannot connect to it.

Check the GO (group owner) to which both devices belong (as indicated by the GO icon). If the devices belong to different GOs then their connection settings are different and they cannot connect. To connect these devices, they must connect to the same GO.

When I use WPS to set up a Wi-Fi Direct connection, I cannot enter the PIN in the 'PIN Code' field.

In this version of WPS, this field is graed out until the other WPS device begins the PIN connection process. Set the other WPS device to begin the PIN connection process. When the Ralink Utility receives a WPS connection attempt, you can then type the PIN in this field.

Error Messages

To understand a problem signified by an error message and to find suggested solutions, search for the error message in the following tables.

Error messages are organized into the following categories - **Security**, **Profile**, **Wi-Fi Direct**, **AP Mode**, and **miscellaneous** error messages.

Security Error Messages

ID	Error Message	Problem Description	Suggested Solution
1	The maximum number of PACs allowed is %d. Delete unneeded PACs before importing additional PAC files.	The maximum number of PAC that can be installed in the Utility is 150.	Delete any unneeded PACs before importing the PAC to be installed.
2	Invalid WPA-PSK key. Enter a key using 8-63 printable ASCII characters or 64 hexadecimal digits.	The WPS security passphrase entered is too short or too long.	Type a security passphrase in the WPA-PSK field which is between 8-63 ASCII characters or 8-64 hexadecimal characters.
3	Invalid WPA2-PSK. Enter a key using 8-63 printable ASCII characters or 64 hexadecimal digits.	The WPA2 security passphrase entered is too short or too long.	Type a security passphrase in the WPA2 Pre-Shared Key field which is between 8-63 ASCII characters or 8-64 hexadecimal characters.

ID	Error Message	Problem Description	Suggested Solution
4	Invalid WAPI key. Enter a key with an even length made up of 8-64 printable ASCII characters or hexadecimal digits.	The WAPI security passphrase entered is too short or too long.	Type a security passphrase in the WAPI PSK field which is between 8-64 keyboard characters.
5	Invalid WAPI key. An even number of hexadecimal digits is required.	If entering a WAPI security passphrase using hexadecimal characters, the total number of characters must be an even number.	Enter a security passphrase using an even number of hexadecimal characters.
6	Invalid WEP Key length. WEP key requires 10 or 26 hexadecimal characters.	If entering a WEP security passphrase using hexadecimal characters, the total number of characters must be 10 or 26 characters.	Enter a security passphrase using 10 or 26 hexadecimal characters.
7	Invalid WEP key length. WEP key requires 5 or 13 ASCII characters.	If entering a WEP security passphrase using ASCII characters, the total number of characters must be 5 or 13 characters.	Enter a security passphrase using 5 or 13 ASCII characters.
8	Please enter SSID	When attempting to connect to a wireless network which does not broadcast its network name (SSID), you need to enter the network name.	Enter the name of the network to which you are connecting.

ID	Error Message	Problem Description	Suggested Solution
9	Must input Identity	When setting up EAP security, for Tunnel ID you need to enter your user name.	In the Tunnel ID field, enter the user name assigned you by the network administrator.
10	Must input Password	When setting up EAP security, for Tunnel Password you need to enter the password associated with your user name.	In the Tunnel Password field, enter the password assigned you by the network administrator.
11	The network is configured with OPEN security. Do you want to connect?	The network to which you are connecting is open, and any data you send may be read or altered by others.	Click Yes to continue connecting to an unsecured network, or find a more secure network to which to connect.
12	No AP supported.	When setting up a WPS connection using the push button method, the Utility scans for APs that support WPS and reports an error message if none are found.	Check the AP to which you are connecting is turned on, with WPS enabled, and is in range.
13	Tunneled identity required for PEAP authentication!	The user name assigned you by the network administrator is required for PEAP authentication.	In the Tunnel ID field, type the user name assigned you by the network administrator.

ID	Error Message	Problem Description	Suggested Solution
14	Password required for MD5 authentication!	When setting up EAP-MD5, a password associated to your user name is required.	In the Tunnel Password field, type the password associated to your user name which was assigned you by the network administrator.
15	Please select a client certificate to use!	When setting up user certification on your EAP method, you need to select a user certificate.	When setting up an EAP method, in the certificate screen, select a user certificate.
16	The certificate's expiry date is invalid. Select a certificate with a valid expiry date.	The user certificate you selected is out of date.	Ask you network administrator for a new, valid user certificate.
17	Invalid User certificate	The WAPI user certificate was not accepted.	Check the expiry date of the certificate, a new certificate may be required. Alternatively, check the certificate is the correct one for the user.
18	Invalid Issuer certificate	The WAPI server certificate was not accepted.	Check the expiry date of the certificate, a new certificate may be required. Alternatively, check the certificate is the correct one for the authentication server.

ID	Error Message	Problem Description	Suggested Solution
19	Issuer and subject are not matched in Issuer certificate.	For WAPI certificates, the subject in a server certificate must match the issuer.	Check you have installed the server certificate and not the user certificate instead.
20	User certificate and Issuer certificate are not matched.	For WAPI server/user certificate pairs, the public key in both user and server certificates must match.	Manually examine the public key in server and user certificates to find matching pairs.
21	This setting already exists.	You are attempting to select a certificate that has already been selected.	You do not need to install this certificate. Continue settng up security.
22	The selected certificate is over the maximum length.	The certificate you have selected is too long.	Check you have selected the correct certificate. Alternatively, ask your network administrator for a new, valid certificate.
23	Issuer and subject are matched in Issuer certificate.	The issuer cannot issue a user certificate for itself.	Check you are connected to the correct authentication server. Alternatively, check you have installed the correct certificates.
24	Invalid Pin Code	When setting up a WPS connection, a PIN with a length not equal to either 4 or 8 is entered.	Type a PIN with the correct length. This is either a total of 4 or 8 digits.
25	Pin Code error	When setting up a WPS connection, a PIN with the correct length is entered, but with the wrong digits.	Re-enter the correct PIN.

ID	Error Message	Problem Description	Suggested Solution
26	This connected AP has been configured. You can select "YES" to try to reconfigure.	To set up a connection to an AP using a WPS profile, any existing WPS settings on the AP must be reset to those of your WPS profile.	Click YES to apply the settings of your WPS profile to the AP to which you are connecting. NOTE this feature is only available in WPS version 2.
27	The AP is already configured. Your profile settings can not be applied.	If the WPS settings of the WPS profile you are using to connect to an AP are different from those configured on the AP, then the connection will fail.	Reset either the WPS settings on the AP or those of the WPS profile you are using to connect to the AP, so that they are the same.
28	Your profile uses OPEN security to configure, and do you still want to configure?	You are attempting to set up a WPS connection using a WPS profile which has been configured with no security settings.	It is recommended that security is configured on any wireless connection used.
29	AP's uuid is empty, please press rescan button to scan again!	The Utility failed to detect all required settings on the AP to which you are using WPS to connect.	Restart the WPS connection process by clicking the "Start PIN" button. Alternatively, in the Site Survey screen, click the "Rescan" button to detect AP settings.

Profile Error Messages

ID	Error Message	Problem Description	Suggested Solution
1	Please enter profile's name	When setting up a profile, a name is required in the profile name field.	In the profile name field, type a name for the profile.
2	Profile name requires 1-32 characters.	When typing a name for the profile, the maximum size is 32 characters.	Type a name for the profile using no more than 32 characters.
3	A profile name consisting only of spaces is not allowed.	When typing a name for the profile, the spacebar can only used in conjunction with printable characters.	If using the spacebar while typing a name for your profile, ensure you have also typed printable characters.
4	The integer value following by "PROF" should not exceed 4294967294	When leaving the profile name to its default "PROF"+n+1, where n= number of profiles created, n may not exceed the stated maximum.	Enter an alternative profile name, for example, use hexadecimal to indicate high numbers of profiles.
5	Not accept profile whose security is WEP or WPA or TKIP for WPS verion2	When setting up a WPS profile, you configured non-AES security. However, WPS version 2 only accepts AES security.	To connect to a WPS version 2 enabled device, you need to configure a WPS profile with AES security. Alternatively, with a WPS profile configured with non-AES security, try connecting to a device with WPS version 1 enabled.

ID	Error Message	Problem Description	Suggested Solution
6	Failed to import! No profile in the file.	When importing a profile file, no profile settings were found in the file.	Try exporting a profile file, and use a text file editor to examine the settings. Any profile file you import should have similar settings.
7	Failed to import! More than one profile in the file.	When importing a profile file, conflicting profile settings were found in the file.	Use a text file editor such as Notepad to examine the profile file and delete conflicting entries.
8	Failed to import! This profile name already exists.	When importing a profile file, a profile with an identical profile name was found already configured.	Delete the existing profile with the matching name. Alternatively, using a text editor application such as Notepad, edit the name of the profile to be imported.
9	The profile to delete is currently in use.	You are currently connected to a network using the profile to be deleted.	Disconnect from the network to which you are currently connected, then delete the profile.
10	Please try again to save with another file name.	When exporting a profile which has the same name as an existing profile filename, and which is currently in use, the save will fail.	Rename the profile file you are exporting.
11	The maximum number of profiles allowed is 100.	You have reached the maximum number of profiles supported by the Utility.	To add additional profiles, delete existing profiles in the profile list.

Wi-Fi Direct Error Messages

ID	Error Message	Problem Description	Suggested Solution
1	Both devices are trying to become group owner.	When connecting using Wi-Fi Direct, both devices attempt to become group owner.	Disable Autonomous GO.
2	Channel dismatch: peer channel is %s	When setting up both a traditional wireless connection to an AP and a Wi-Fi Direct connection, the channels used need to match.	Manually configure the connections so that the channels used are the same.
3	PIN code error	When setting up WPS in Wi-Fi Direct, an incorrect PIN was entered.	Enter the correct PIN and repeat the Wi-Fi Direct WPS process.
4	The selected device is unavailable.	The Utility incorrectly shows a device is available for Wi-Fi Direct connection.	Check the device to which you are connecting is turned on and has Wi-Fi Direct enabled.
5	WPS method mismatch:Please use %s	When setting up WPS in Wi-Fi Direct, the device to which you are connecting uses the wrong WPS method.	Try again to set up WPS, this time using the correct WPS method.
6	The maximum number of users are connected to the Wi-Fi Direct network.	The maximum number of devices the Utility can connect to using Wi-Fi Direct is 32. After this number is reached any attempts to connect using Wi-Fi Direct will fail.	Disable unnecessary Wi-Fi Direct connections and reattempt to connect.

ID	Error Message	Problem Description	Suggested Solution
7	Reject by user	The device to which you are connecting using Wi-Fi Direct has rejected or failed to accept your connection request.	Reattempt the connection and if that fails, contact the owner of the device to which you are trying to connect.
8	Wi-Fi Direct group session is terminated due to channel conflict: peer channel is %s	When attempting to use Wi-Fi Direct to share your Internet connection by both connecting to an AP and to a device to which you are sharing the Internet, the channels of both connections must be the same.	Connect first to the AP, then to the device to which you are sharing the Internet. If the channels are still not the same, manually set the same channel settings on both connections.
9	Invite %s. Please set WPS settings from GO	When the Autonomous GO is enabled on the Utility, WPS settings must be configured before setting up a Wi-Fi Direct connection.	In the Wi-Fi Direct screen, when autonomous GO is enabled, click the WPS icon, and configure WPS settings.
10	Wi-Fi Direct does not support connections to members of an ad hoc network.	You are attempting to set up a Wi-Fi Direct connection to a device which is part of an ad hoc network.	Remove the device to which you are connecting using Wi-Fi Direct from the ad hoc network.
11	Conflict between 802.11N(20/40MHz) and 802.11BG mode: peer channel is %s %s will become number.	The device to which you are connecting supports a different Wi-Fi hardware standard from your device.	Wi-Fi Direct is an 802.11n standard. Set up a Wi-Fi Direct connection with an 802.11n device instead.

ID	Error Message	Problem Description	Suggested Solution
12	Please enter server friendly name	In the Media Sharing screen, type a name for the media server.	
13	Start Wi-Fi Direct concurrent GO Fail	When operating in "client + AP" mode, enabling the group owner setting failed.	Retry enabling the GO function.
14	Invalid Intent idex, Intent idex = 0~15	To decide the group owner in a Wi-Fi Direct connection, the intent index is used. The default for the Utility is 7 and within the valid range.	The default intent index value for the Ralink Utility is in the valid range. Check the intent index on the device to which you are connecting and reset it to an integer between 0 and 15.

AP Mode Error Messages

ID	Error Message	Problem Description	Suggested Solution
1	URL unavailable.	When clicking on the Ralink icon in the About screen, no connection to the Internet can be found.	Check you are connected to the Internet.
2	Invalid MAC address format. Use 8 hexadecimal digits.	When setting up the Access Control List, MAC addresses need to be entered using 8 characters "0"-"9" and "A"-"F", i.e. hexadecimal characters.	Ensure you have entered 8 hexadecimal characters.
3	Multicast MAC addresses are not accepted.	When entering MAC addresses in the Access Control screen, MAC addresses where the second character is odd are not accepted. Such a MAC address represents a group of devices, but the access control screen is intended to control individual access to the network.	Ensure the second character of the MAC address you are entering is not odd. This should not be an issue if you are entering the MAC address of a single device on your network.
4	Do not add the Ralink AP's MAC address.	As access to the network is required by the AP, you may not enter the AP's MAC address.	Do not attempt to add the MAC address of your AP to this list.
5	MAC address is already in the Access List.	The MAC address you are entering is already added to the access control list.	You do not need to add this MAC address.

ID	Error Message	Problem Description	Suggested Solution
6	MAC address required in Access List	When "Allow All" or "Reject All" is selected from the drop-down list in the Access Control screen, one or more MAC addresses must be added to the list.	Ensure that one or more MAC addresses are added to the access control list before selecting "Allow All" or "Reject All" in the Access Control screen.
7	The idle time should be between 60 - 3600 seconds.	In the Advanced screen, type an idle time between 60 and 3600 seconds.	
8	The beacon period should be between 20 - 1000 ms.	In the Advanced screen, type a beacon interval period between 20 and 1000 milliseconds.	
9	Invalid WPA-PSK security key. Use 8-63 printable ASCII characters or 64 hexadecimal	In the AP Setup screen, type a WPA-PSK security passphrase using either 8-63 ASCII characters ("a"-"z","A"-"Z", "0"-"9", plus keyboard symbols and the spacebar), or 8-64 hexadecimal characters ("0"-"9","A"-"F").	
10	Enter an integer value for the group rekey interval between 3 and 67108863.	In the AP Setup screen, if the "x 10 seconds" button displays, type a group rekey interval between 3-67108863 units of 10 seconds. If the "x 1000 packets" button displays, type a group rekey interval measured by the number of packets transmitted on the network between 3-67108863 x 1000 packets.	
11	Invalid WEP key length. WEP key %d requires 5 or 13 printable ASCII characters.	In the AP Setup screen, when setting up WEP security, when ASCII is selected, type a WEP security passphrase made up of 5 or 13 ASCII characters.	
12	Invalid WEP key length. WEP key %d requires 10 or 26 hexadecimal digits.	In the AP Setup screen, when setting up WEP security, when hexadecimal is selected, type a WEP security passphrase made up of 10 or 26 hexadecimal characters.	

ID	Error Message	Problem Description	Suggested Solution
13	Switch to client mode failed. Log out of other user accounts on your computer and retry.	When switching from AP mode to client mode, switching cannot complete if the Utility is running in another user account on the same computer.	Request the owner of the user account running the Utility to log in and close the Utility. Otherwise, try running the Utility as administrator.

Miscellaneous Error Messages

ID	Error Message	Problem Description	Suggested Solution
1	Switch radio failed!	The Adapter cannot be turned on or off, i.e. radio transmission cannot be enabled or disable.	Check whether you have permission by Windows to manage the Ralink Utility. Click "run as Administrator". Alternatively, reinsert the Adapter, or reinstall the Utility.
2	Before using SoftAP, please radio on...	When switching from client mode to AP mode, the radio transmission function has been disabled.	Click the radio (RF) icon in the main menu to enable radio transmission, then try again to switch to AP mode.
3	Please turn on AutoConfig service	When switching to AP mode, the Windows AutoConfig service has been disabled.	For information on enabling AutoConfig, visit the Microsoft support web site http://support.microsoft.com/.
4	Start failed!	You cannot start the Ralink Utility.	Check the Windows service AutoConfig is enabled. Alternatively, reboot your computer.
5	No selected item	When saving changes to a screen, user input is still required in fields such as radio buttons or combo boxes.	Check the screen to ensure that all required selections have been made before saving changes.
6	Please enter SSID	When configuring settings for connecting to an ad hoc network, an SSID or name of the network is required.	In the SSID field, type the name of the ad hoc network to which you are connecting.