802.11n 2T3R Wireless PCI Adapter

USER MANUAL 1.0.0

© 2009

Table of Contents

1 Overview

Thank you for purchasing this product. Read this chapter to know about your 802.11n 2T3R Wireless PCI Adapter.

Unpacking information

Before getting started, please verify that your package includes the following items:

1.One 802.11n 2T3R Wireless PCI Adapter.

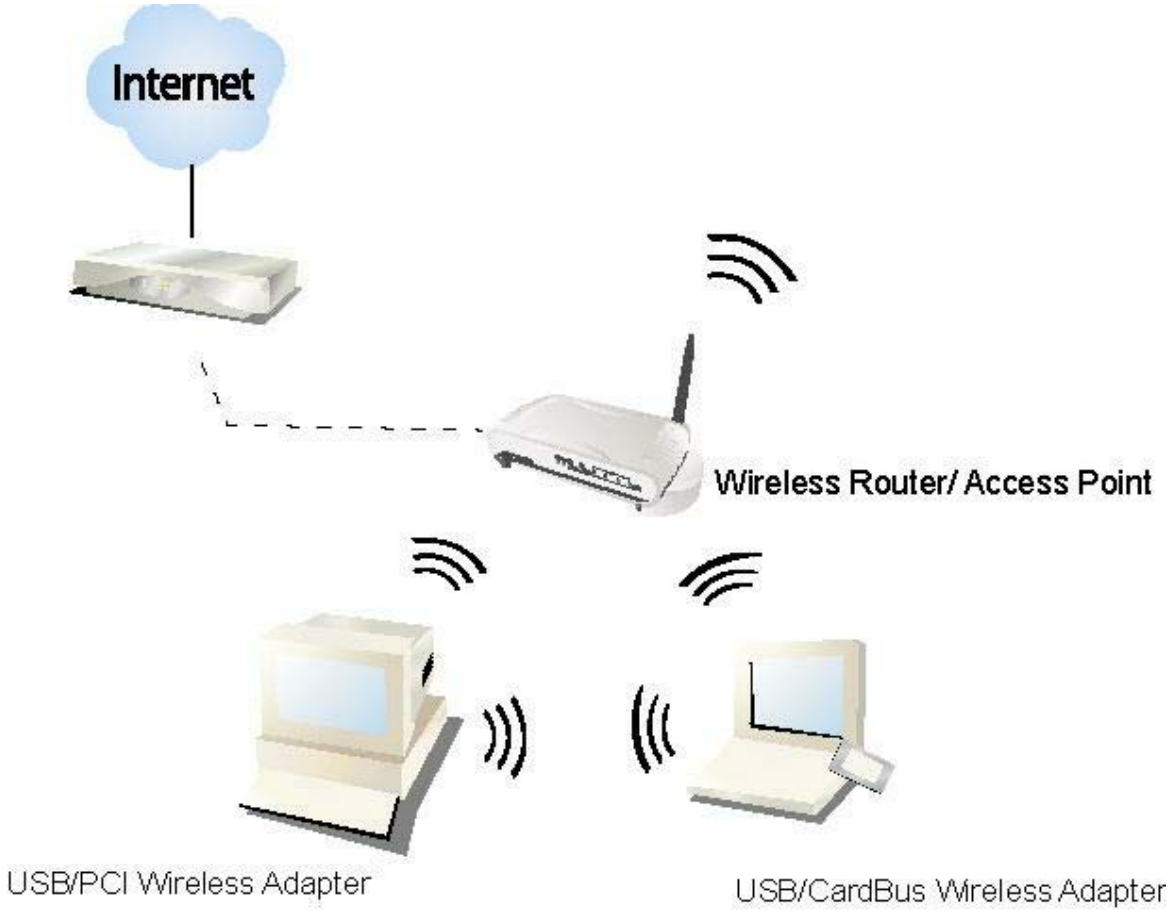
2.One Utility/ Manual CD.

3.Three 2 dbi Antenna

2 Introduction the 2T3R Wireless PCI Adapter

PCI Adapter

The 802.11n 2T3R Wireless PCI adapter provides users to launch 802.11n 2T3R wireless network at 300 Mbps in the 2.4GHz band, which is also compatible with 802.11b/g wireless devices at 11/54 Mbps. You can configure this adapter with ad-hoc mode to connect to other 2.4GHz wireless computers, or with Infrastructure mode to connect to a wireless AP or router for accessing to Internet. This adapter includes a convenient Utility for scanning available networks and saving preferred networks that users usually connected with. Security encryption can also be configured by this utility.



Key Features

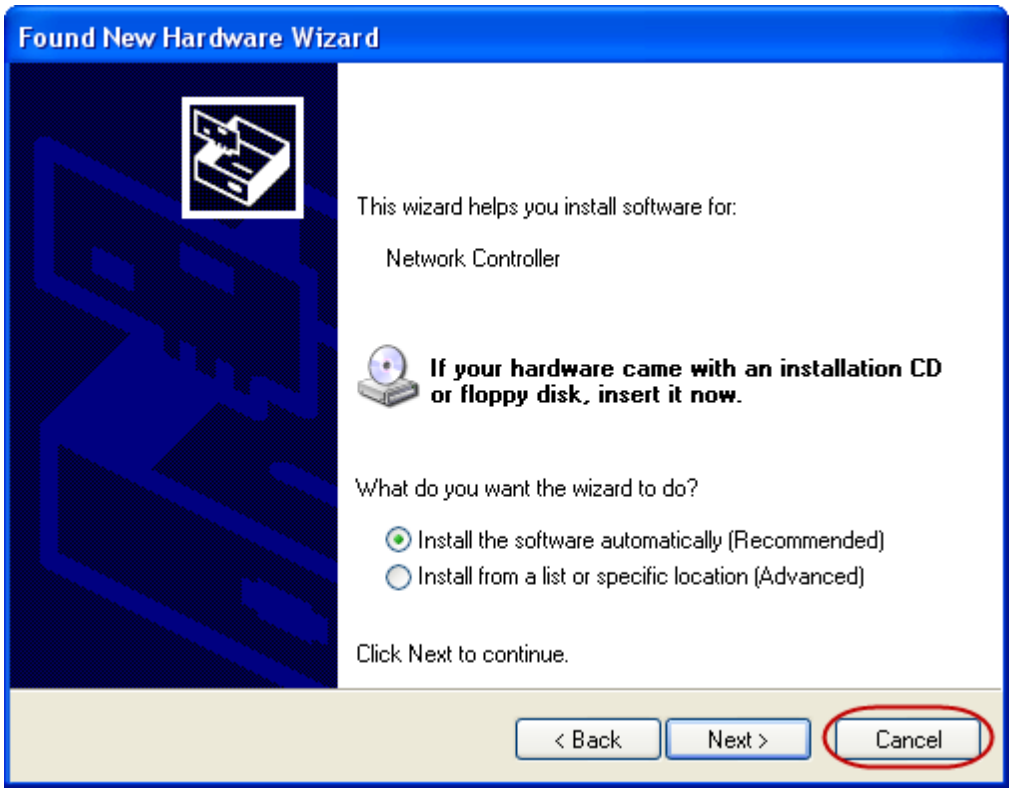
- Complies with IEEE 802.11n/b/g wireless standard
- Supports driver for Windows® 2000, XP and Vista.
- 2.4GHz Frequency band, MIMO 2T3R
- Supports QoS: WMM, WMM-PS
- Complies with PCI 2.3 or Mini PCI type III
- Support wireless data encryption with 64/128-bit WEP, WPA, WPA2
- High Speed transfer data rate up to 300 Mbps
- Supports Multiple BSSID
- Supports auto-installation and diagnostic utilities.

3 Installation Guide

3.1 Software Installation

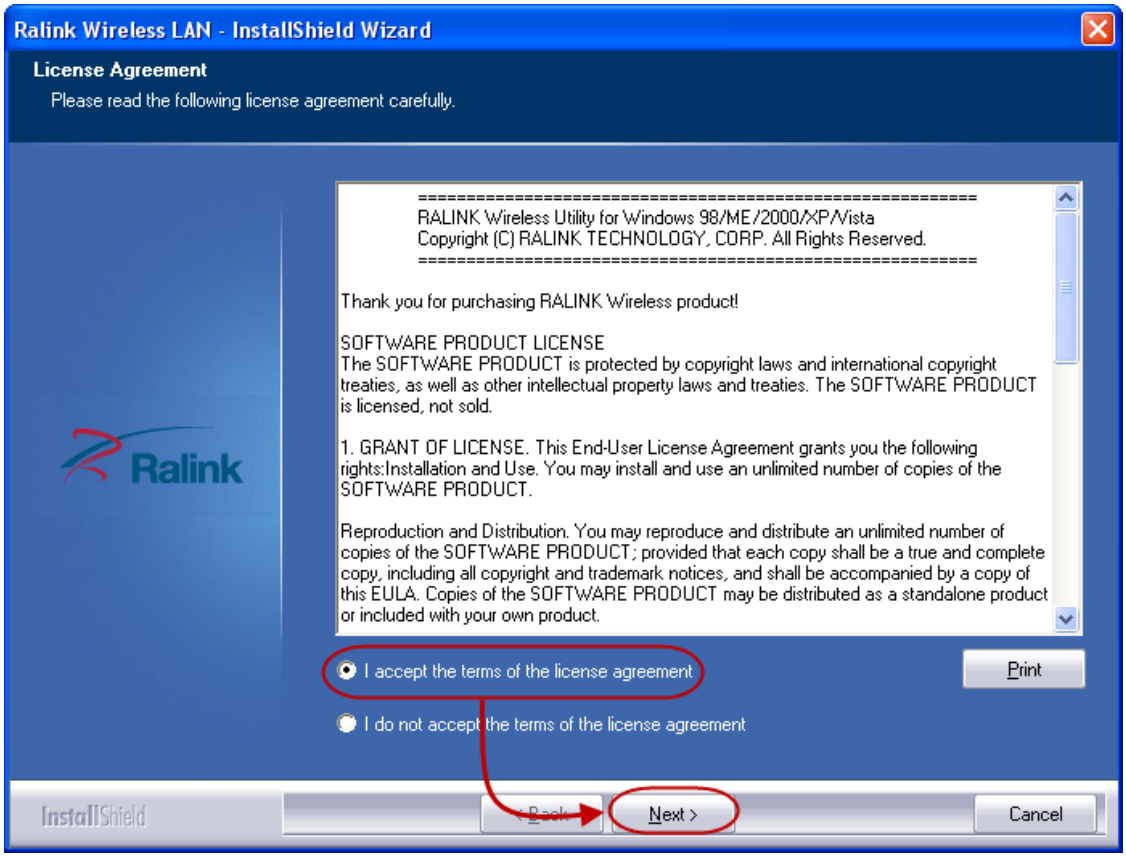
Note: The following driver installation guide uses Windows® XP as the presumed operation system. The procedures and screens in Windows® 2000 and Vista are familiar with Windows® XP.

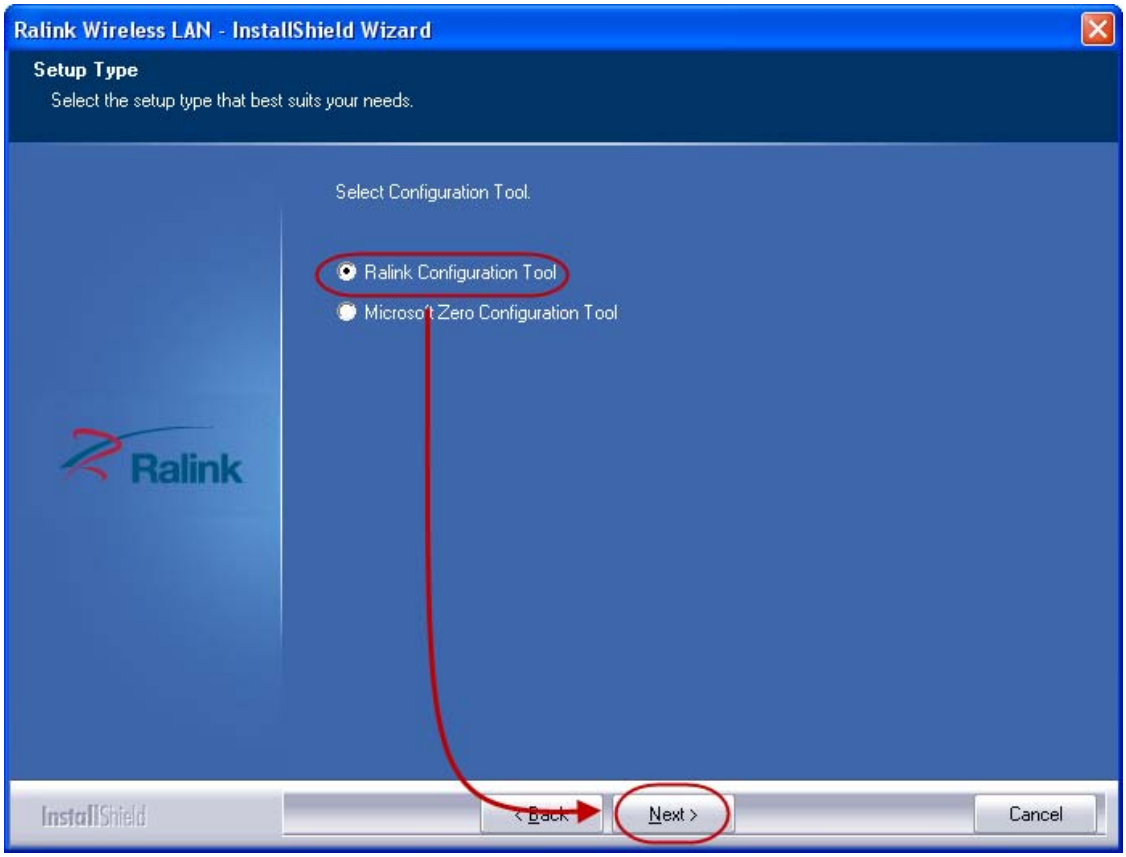
1. Insert this product to your computer. The system finds the newly installed device automatically. Click cancel to close this window.



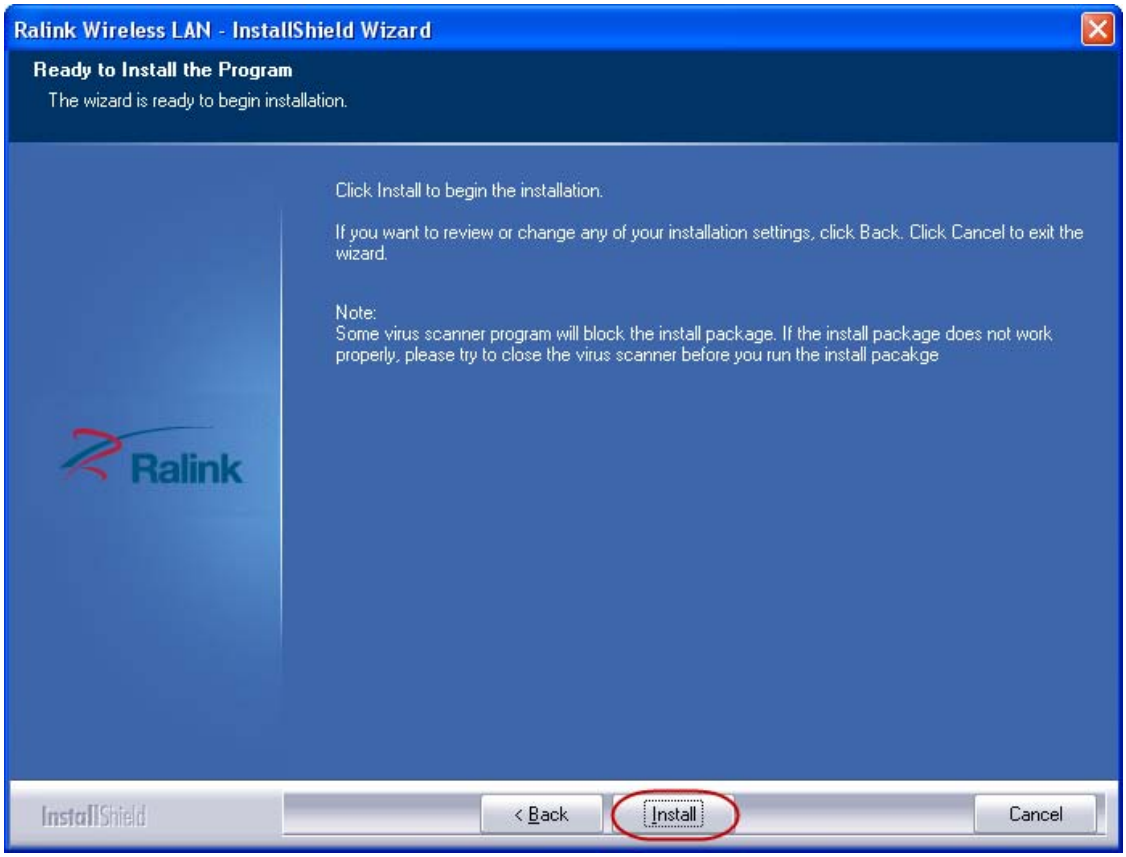
2. Insert the CD-Rom that came with this product to your CD-Rom drive. The menu window pops up automatically. Please click the "**Driver Installation**" button of this product.
   Note: If the CD-Rom fails to auto-run, please click on "**My Computer**" > **your CD-Rom Drive** > **Driver folder** then double-click the "**Setup**" icon to start this menu.

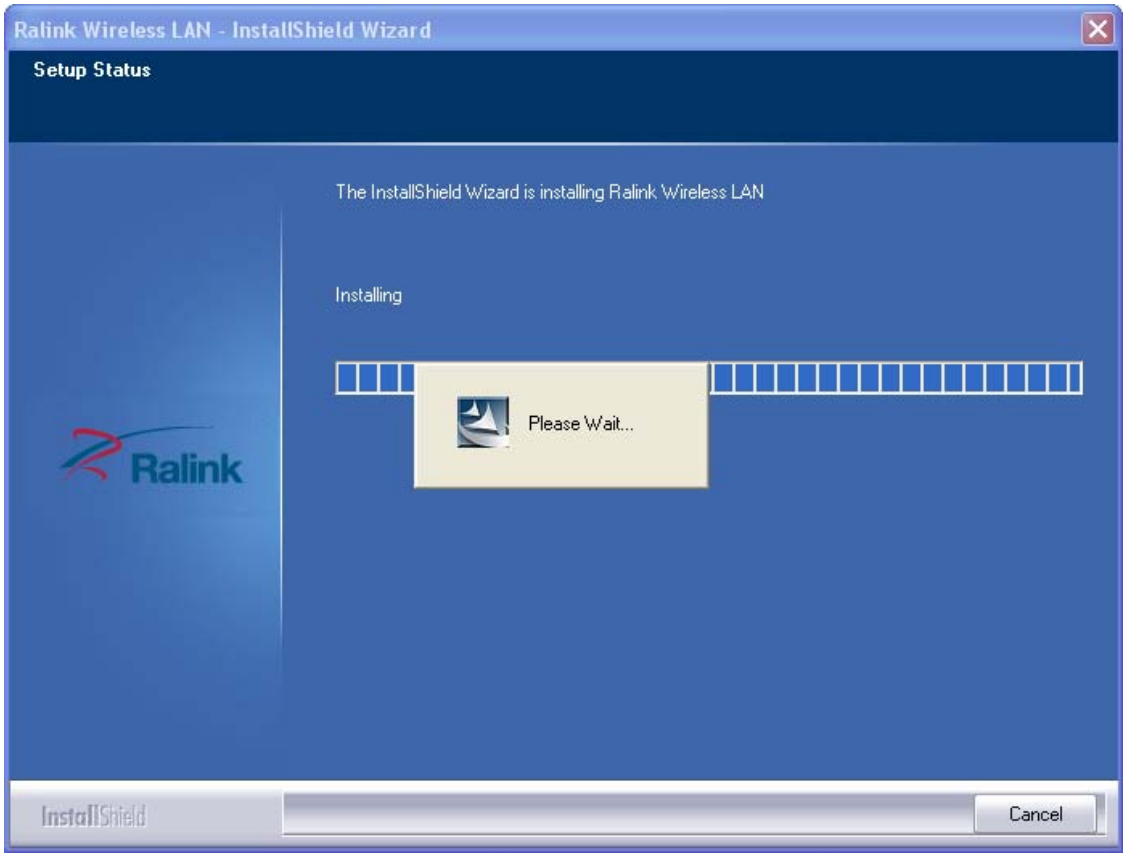
3. Select if you are going to configure your wireless network with this device or with Microsoft Zero Configuration tool.
   Note: This can be changed after installing this software.


Ralink Wireless LAN - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
RALINK Wireless Utility for Windows 98/ME/2000/XP/Vista
Copyright (C) RALINK TECHNOLOGY, CORP. All Rights Reserved.
Thank you for purchasing RALINK Wireless product!
SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.
1. GRANT OF LICENSE. This End-User License Agreement grants you the following rights:Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.
Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
Ralink
InstallShield
< Back
Next >
Cancel

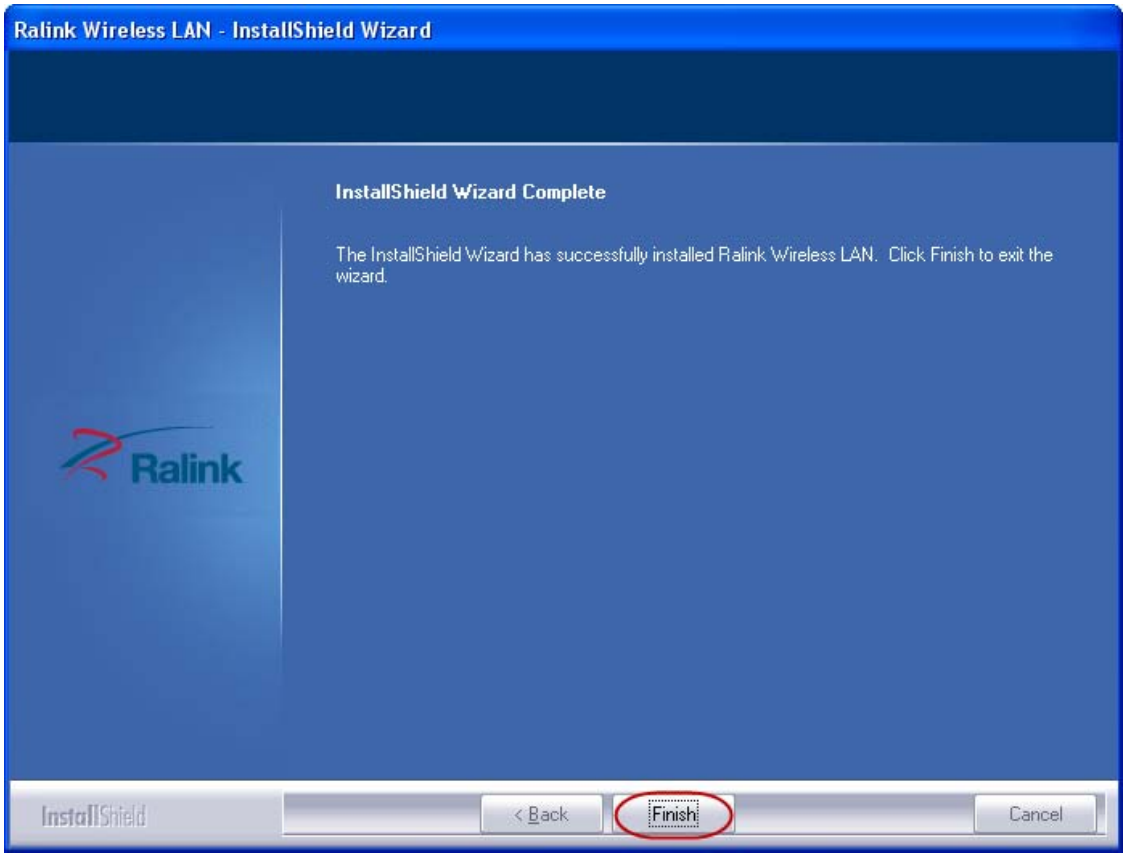


4. Click the "**Install**" button to start installing.


Ralink Wireless LAN - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Note:
Some virus scanner program will block the install package. If the install package does not work properly, please try to close the virus scanner before you run the install pacakge
Ralink
InstallShield
< Back
Install
Cancel



5. Click the "**Finish**" button to complete installation.



4 Management Guide

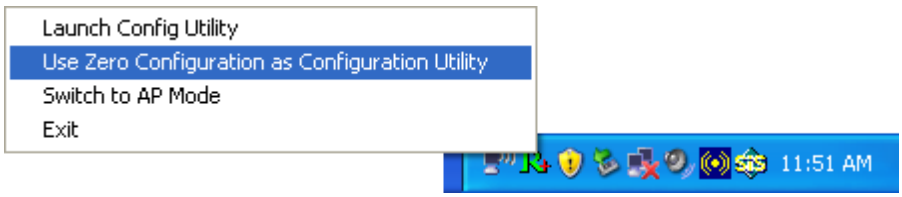
Read this chapter to understand the management interface of the device and how to manage the device.

4.1 Making a Basic Network Connection

4.1.1 Select a configuration tool

In the following instruction for making a network connection, we use the utility we provide to configure your wireless network settings.

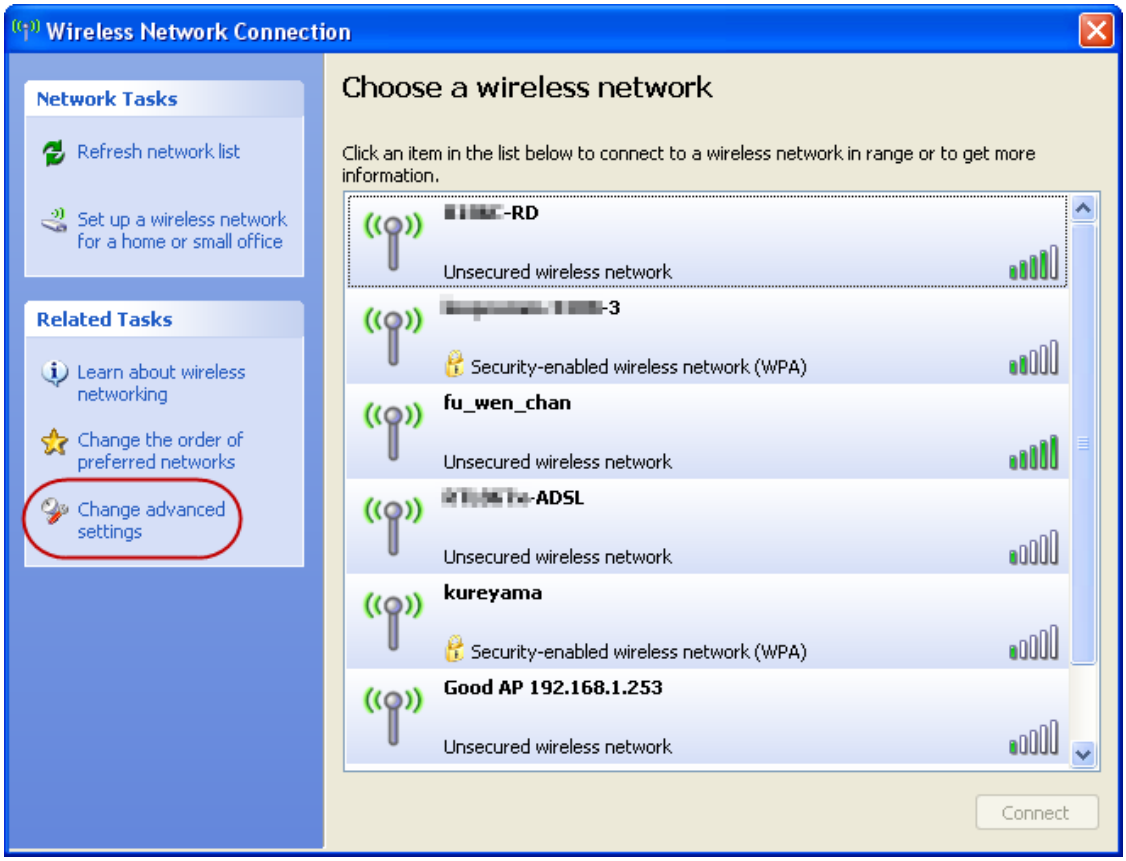
Note:
You could use either the software we provide or Microsoft Zero Configuration tool to configure this adapter. To switch between the two configuration tools, please right click on the icon on system tray to select.



4.1.2 To connect with Microsoft Zero Configuration tool

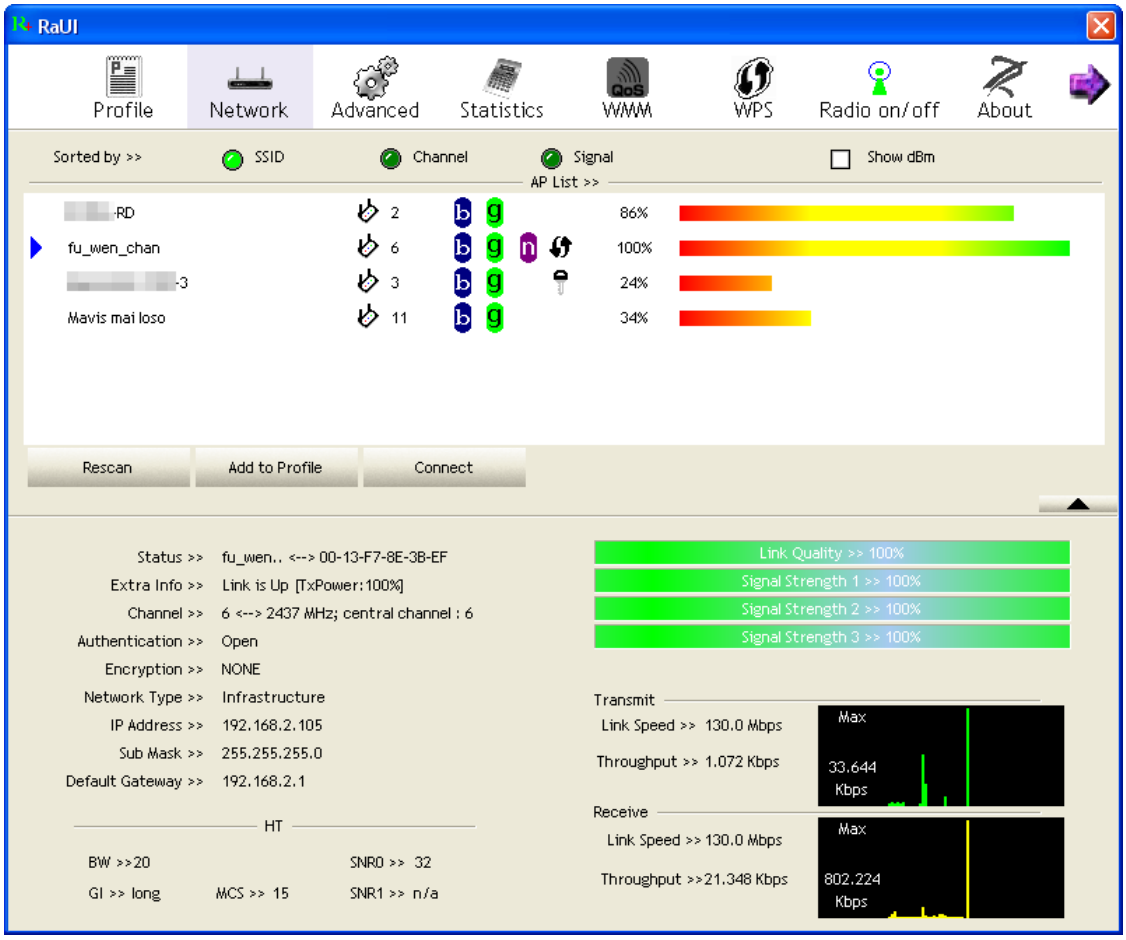
After specifying the Microsoft Zero Configuration tool to configure your wireless network, right click on the  icon on system tray. Select "**View available wireless Networks**" to specify your wireless network.

The tool shows the available wireless networks. Select your demanding network to connect with. To connect to a wireless network with more security settings, please click "**Change advanced settings** " to be compatible with your wireless network security settings.



4.1.3 To connect with 802.11n Wireless LAN Utility

We provide this utility for users to connect to a wireless network easily. It provides more information and configuration for this adapter. As default, the utility is started automatically upon starting your computer and connects to a connectable wireless network with best signal strength. Please refer to the following chapters to get information regarding to the functions of this utility.



4.2 Introduction to the 802.11n Wireless LAN Utility

Note: The Utility in Windows Vista is different from the following. For instructions on using the utility included in Windows Vista please refer to the instruction in **Appendix**.

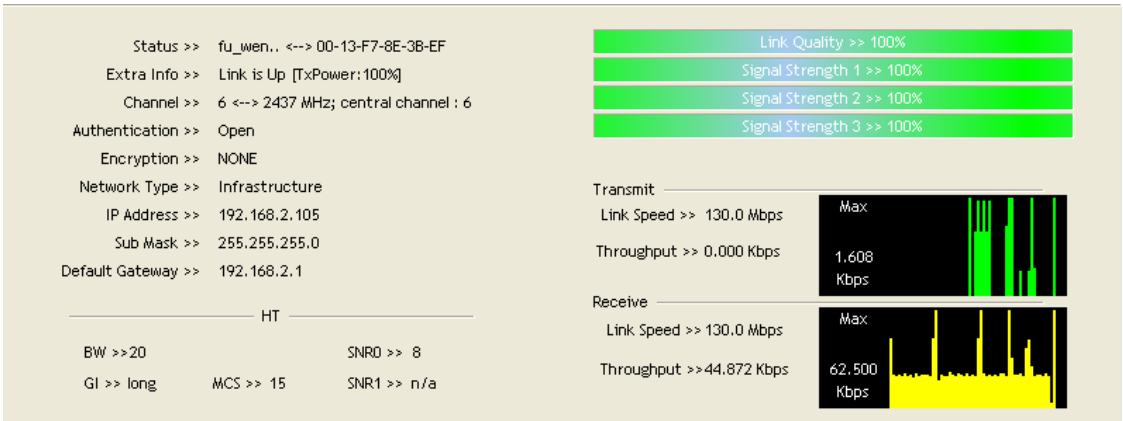
4.2.1 Interfaces

This Utility is basically consisted of three parts:

1. Functional buttons: on top of the window. You can click each button to access each configuration window.

2. Configuration column: Center of the utility window. Make your changes for each function in this part.
3. Status information: bottom of the utility window. Shows the connection status and system information.

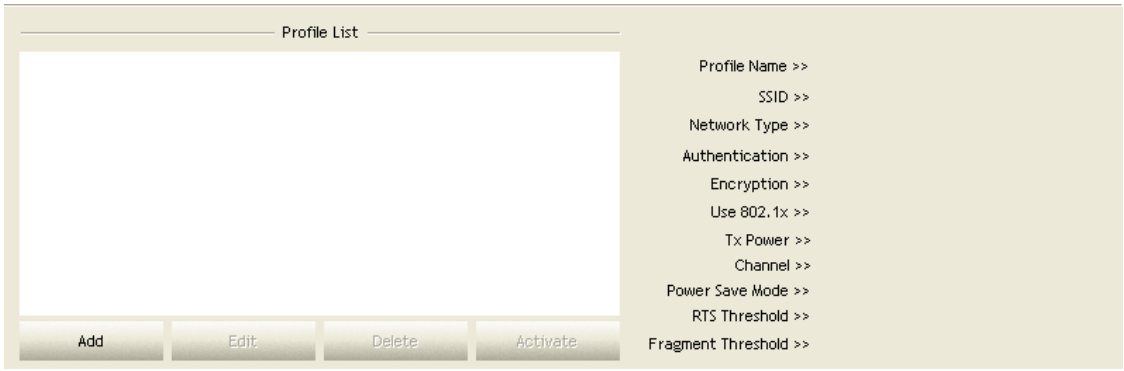
4.2.2 Information



Status	Shows the connecting status. Also shows the SSID while connecting to a valid network.
Extra Info	Display link status in use
Channel	Display current channel in use
Authentication	Authentication mode in use.
Encryption	Encryption type in use.
Network Type	Network type in use
IP Address	IP address of current connection
Sub Mask	Sub mask of current connection
Default Gateway	Default gateway of current connection
Link Speed	Show current transmit rate and receive rate
Throughput	Display transmit and receive throughput in Mbps
Link Quality	Display connection quality based on signal strength and TX/RX packet error rate.
Signal Strength 1	Receive signal strength 1, user can choose to display as percentage or dBm format.
Signal Strength 2	Receive signal strength 2, user can choose to display as percentage or dBm format.
Signal Strength 3	Receive signal strength 3, user can choose to display as percentage or dBm format.
Noise Strength	Display noise signal strength
HT	Display current HT status in use, containing BW, GI, MCS, SNR0, and SNR1 value.

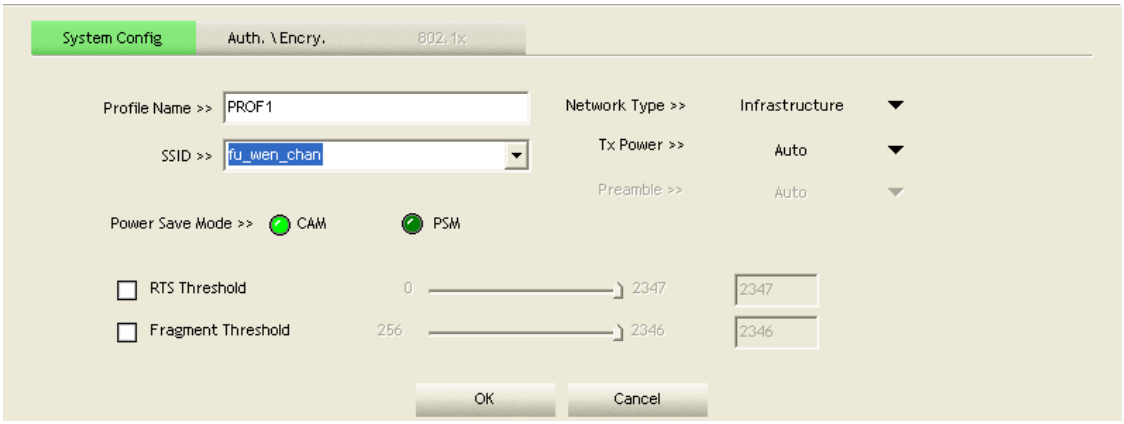
4.2.3 Profile

This profile page allows users to save different wireless settings, which helps users to get access to wireless networks at home, office or other wireless network environments quickly.



To add a new profile:

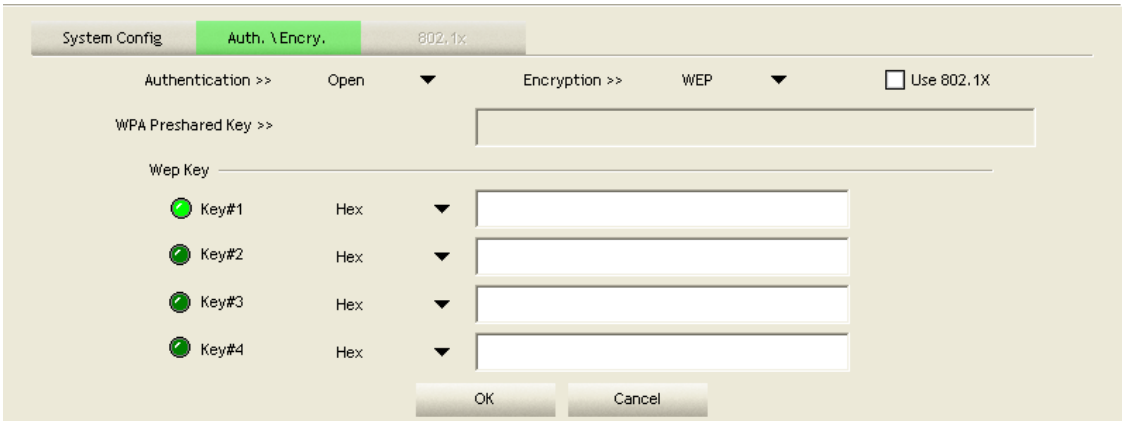
1. Click the "**Add**" button. The add profile window pops up.
   Note: you could also add a new profile quickly by selecting an available network in the "**Network**" function then press the "**Add to Profile**" button.
2. Fill in information for this profile in the system config section:



Profile Name	Choose a name for this profile, or use default name defined by system.
SSID	Fill in the intended SSID name or use the drop list to select from available Aps.
Power Save Mode	Choose from CAM (Constantly Awake Mode) or PSM (Power Saving Mode).
Network Type	There are two types, infrastructure and 802.11 Ad-hoc mode. Under Ad-hoc mode, you could also choose the preamble type; the available preamble type includes auto and long. In addition to that, the channel field will be available for setup in Ad-hoc mode.
RTS Threshold	For adjusting the RTS threshold number by sliding the bar or key in the value directly. The default value is 2347.
Fragment Threshold	Adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346.

3. Select an encryption type and fill in the corresponding wireless network

information:



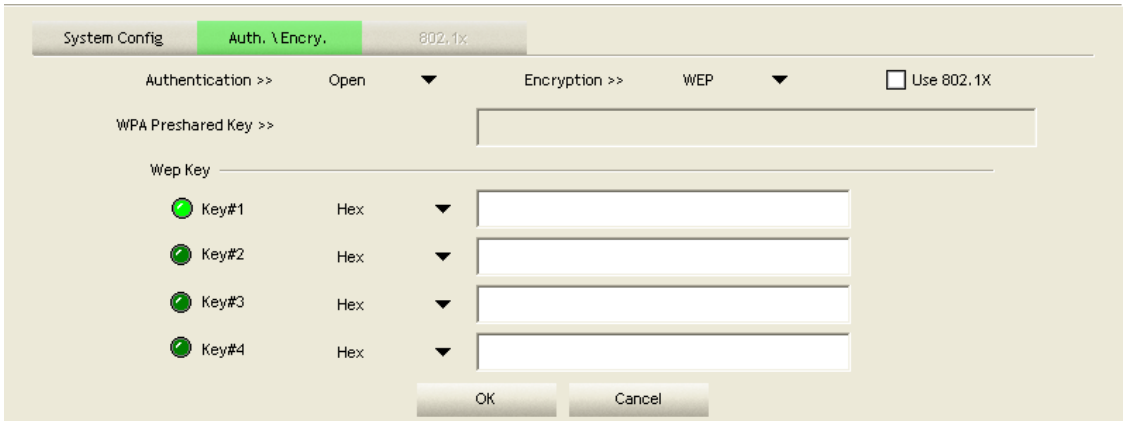
Authentication Type	There are 7 types of authentication modes supported by RaUI including open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK
Encryption Type	For open and shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.
802.1x	Use 802.1x to make WPA and WPA2 certification. This functions only works when connecting to a WPA and WPA2 supported device.
WPA Pre-shared Key	This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 32 length.
WEP Key	Only valid when using WEP encryption algorithm. The key must matched AP's key.

4. Specify the 802.1x information if you are using the 802.1X certification method. Users that don't use this function or connecting to an open-wireless network please skip this part.

EAP method:	To select an EAP method.
Tunnel Authentication:	Select a Tunnel authentication mode.

Session Resumption:	Select to enable this function or unmark it to disable.

ID \ PASSWORD



Authentication ID / Password: Identity, password and domain name for server. Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain name can be keyed in blank space.
Tunnel ID / Password: Identity and Password for server.

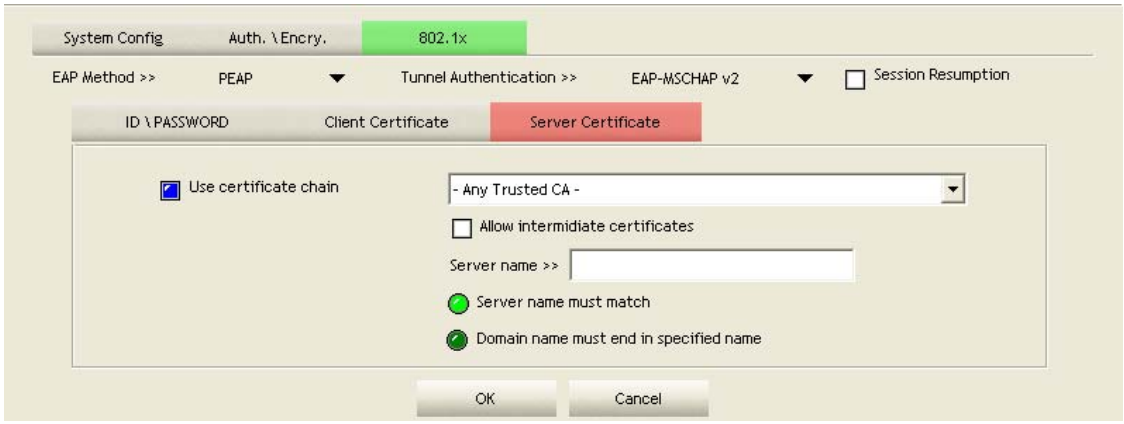
Client Certification

Use Client certificate: Client certificate for server authentication.

EAP Fast

Allow unauthenticated provision mode: Mark to enable unauthenticated provision mode.
Use protected authentication credential: Mark to use protected authentication credential.

Server Certification



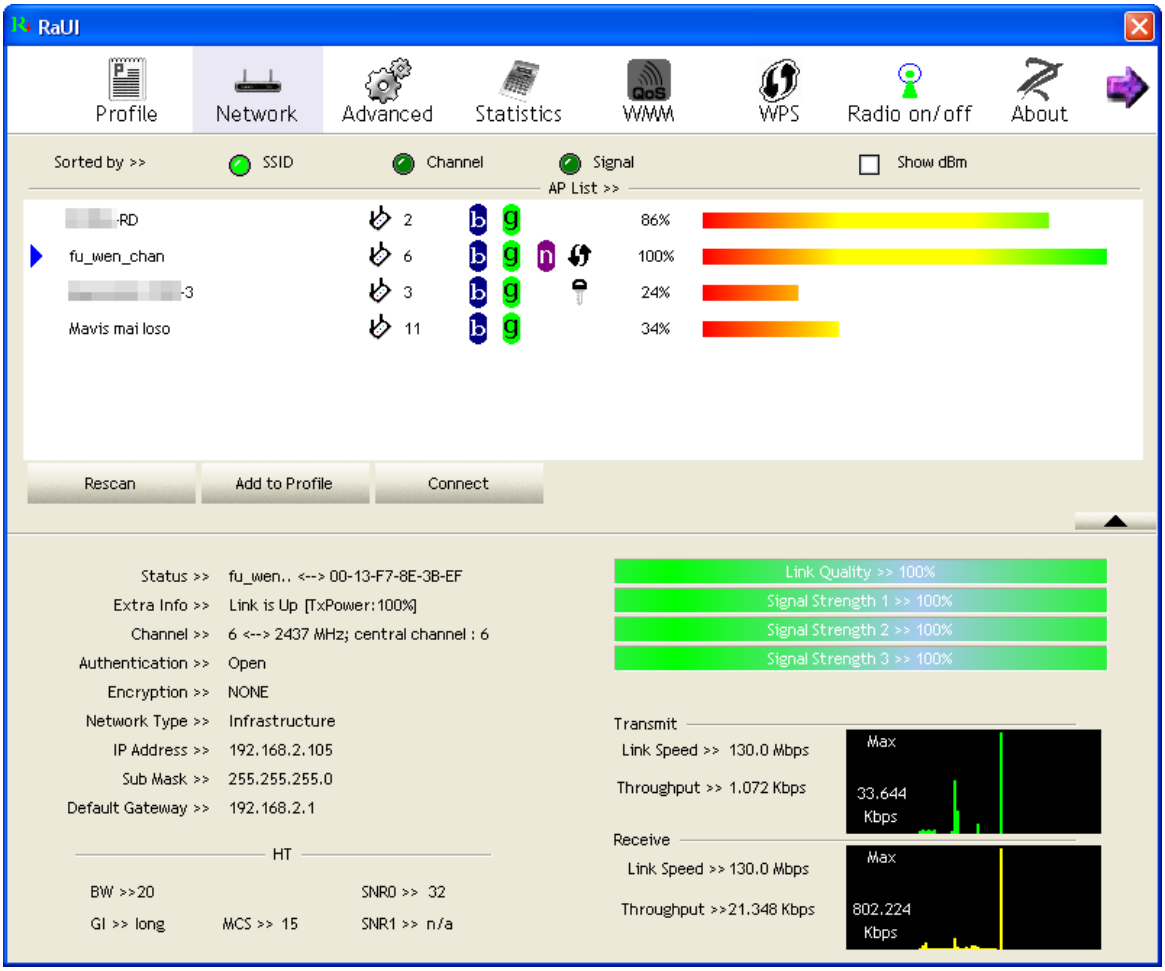
Use Certificate chain: Mark the checkbox to enable using certification chain.
Allow intimidate certificates: Mark to allow intimidate certification.
Server name: Enter an authentication sever name.

4.2.4 Network

This network lists the available wireless networks. The utility connects to a wireless network with best signal strength automatically. You can change the connecting network by clicking on the network name and click the "**Connect**" button. To see detail information of each network, please double click on each item to pop up the information window.

SSID, Channel and Signal buttons	Click each button to sort the listing networks by SSID, channel and Signal strength.
Signal buttons	channel and Signal strength.

Show dBm	Mark the checkbox to show the signal strength in dBm.
Rescan	To rescan available wireless networks.
Connect	Click this button to connect to a designated network.
Add to Profile	Click this button to add a network to profile after selecting a network.

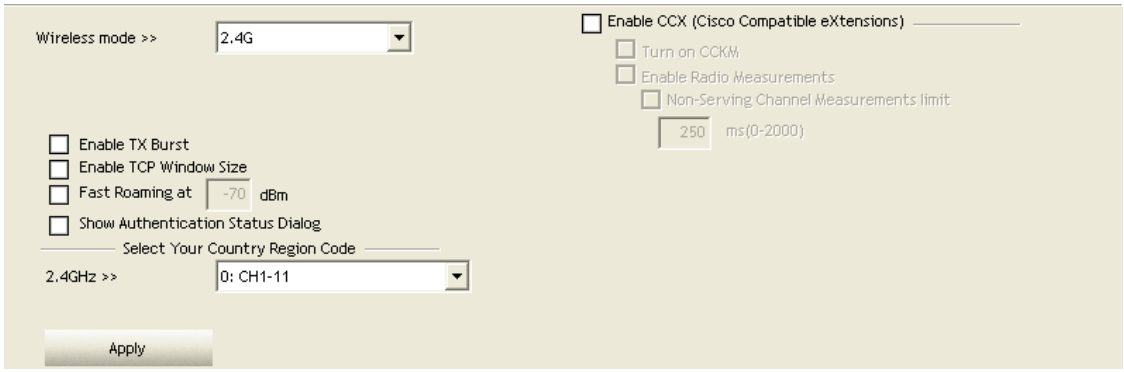


4.2.5 Advanced

This page provides advanced configurations to this adapter. Please refer to the following chart for definitions of each item.

Wireless mode	Click the drop list to select a wireless mode.
Enable TX Burst	Select to enable connecting to a TX Burst supported device.
Enable TCP Window Size	Mark the checkbox to enable TCP window size, which help enhance throughput.
Fast Roaming at __ dBm	Mark the checkbox to enable fast roaming. Specify the transmit power for fast roaming.
Show Authentication Status Dialog	Mark the checkbox to show **"Authentication Status Dialog"** while connecting to an AP with authentication. Authentication Status Dialog displays the process about 802.1x authentication

Enable CCX (Cisco Compatible extensions)	Select to enable CCX. This function can only be applied when connecting to a Cisco compatible device.



4.2.6 Statistics

4.2.6.1 Statistics Transmit

Statistics page displays the detail counter information based on 802.11 MIB counters. This page translates the MIB counters into a format easier for user to understand.

Frames Transmitted Successfully	Frames successfully sent.
Frames Retransmitted Successfully	Successfully retransmitted frames numbers
Frames Fail To Receive ACK After All Retries	Frames failed transmit after hitting retry limit
RTS Frames Successfully Receive CTS	Successfully receive CTS after sending RTS frame
RTS Frames Fail To Receive CTS	Failed to receive CTS after sending RTS
Restart Counter	Reset counters to zero

4.2.6.2 Statistics Receive

Frames Received Successfully	Frames received successfully
Frames Received With CRC Error	Frames received with CRC error
Frames Dropped Due To Out-of-Resource	Frames dropped due to resource issue
Duplicate Frames Received	Duplicate received frames.

4.2.7 WMM

This page allows users to activate the WMM function for this device. Please note that this function only works while connecting to a WMM compatible device.

WMM Enable	Enable Wi-Fi Multi-Media.
WMM - Power Save Enable	Enable WMM Power Save. Please enable WMM before configuring this function.
Direct Link Setup Enable	Enable DLS (Direct Link Setup). Please enable WMM before configuring this function.

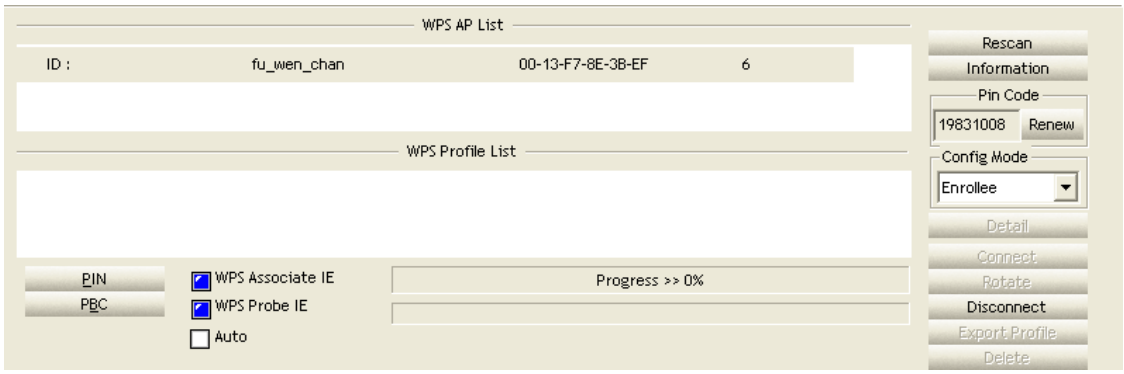
4.2.8 WPS

WPS Configuration: The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. This adapter supports the configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.

WPS AP List	Display the information of surrounding APs with WPS IE from last scan result. List information include SSID, SSID, Channel, ID (Device Password ID), Security-Enabled.
Rescan	Click to rescan the wireless networks.
Information	Display the information about WPS IE on the selected network. List information include Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar using PIN method. Each Network card has only one PIN Code of Enrollee.
Config Mode	Enrollee or an external Registrar.
Table of Credentials	Display all of credentials got from the Registrar. List information includes SSID, MAC Address, Authentication and Encryption Type. If STA Enrollee, credentials are created as soon as each WPS success. If STA Registrar, RaUI creates a new credential with WPA2-PSK/AES/64Hex-Key and doesn't change until next switching to STA Registrar.
Detail	Information about Security and Key in the credential.
Connect	Command to connect to the selected network inside credentials.
Rotate	Command connect to the next network inside credentials.
Disconnect	Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page of RaUI if exist. If there is an empty profile page, the driver will select any non-secue AP.
Delete	Delete an existing credential. And then select the next credential if exist. If there is an empty credential, the driver will select any non-security AP.

PIN	Start to add to Registrar using PIN configuration method.
PBC	Start to add to AP using PBC configuration method.
WPS associate IE	Send the association request with WPS IE during WPS setup. It is optional for STA.
WPS probe IE	Send the probe request with WPS IE during WPS setup. It is optional for STA.
Progress Bar	Display rate of progress from Start to Connected status.
Status Bar	Display currently WPS Status.

Note: When you click PIN or PBC, please don't do any rescan within two-minute connection. If you want to abort this setup within the interval, restart PIN/PBC or press Disconnect to stop WPS action.



5 Appendix

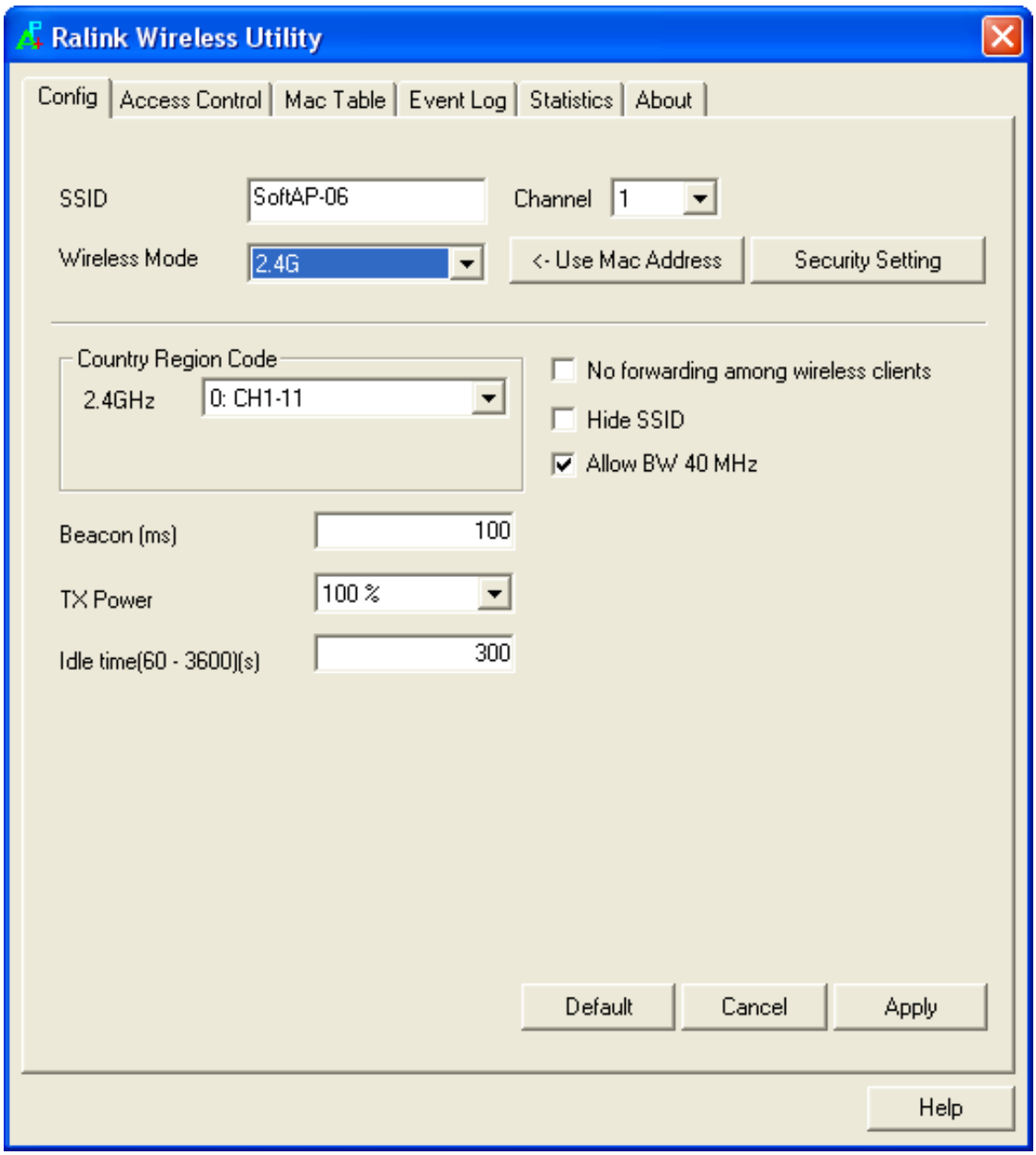
5.1 AP mode management guide

This adapter can be configured as AP mode. To function this adapter as an AP, please right click the icon on system tray and select "**Switch to AP mode"**. Please refer to the following introduction to information about this AP-mode utility.

Note: In Windows® XP, it provides WPA support at hotfix Q815485 However, you have to make sure that hotfix Q815485 (require XP SP1 installed) has been installed in your system before you can start using WPA features. You can check the installation of hotfix in add/remove software page under control panel.

5.1.1 Config

This page provides overall configuration to this adapter. Please find the following items for identification to each field.



1. SSID: AP name of user type. User also can select [Use Mac Address] to display it.

2. Wireless Mode: Select wireless mode. 802.11 b/g mix, 802.11b only, 802.11g only, 802.11 b/g/n mix mode are supported. When wireless card is 802.11n, system default is 802.11 b/g/n mix; Otherwise system default is 802.11 b/g mix (802.11 b/g/n mix selection item only exists for b/g/n adapter).

3. Country Region Code: eight countries to choose. Country channel list:

Classification	Range

0: FCC (Canada)	CH1 ~ CH11
1: ETSI	CH1 ~ CH13
2: SPAIN	CH10 ~ CH11
3: FRANCE	CH10 ~ CH13
4: MKK	CH14 ~ CH14
5: MKKI (TELEC)	CH1 ~ CH14
6: ISRAEL	CH3 ~ CH9
7: ISRAEL	CH5 ~ CH13

4. Wireless Protection: Auto, on, and off. System default is auto.
   a. Auto: STA will dynamically change as AP announcement.
   b. On: Always send frame with protection.
   c. Off: Always send frame without protection.

5. Beacon (ms): The time between two beacons. System default is 100 ms.

6. TX Power: Manually force the AP transmits power. System default is 100%.

7. TX Rate: Manually force the Transmit using selected rate. Default is auto.

8. Idle Time: Manually force the Idle Time using selected value. Default is 300.

9. Channel: Manually force the AP using the channel. System default is channel 1.

10. Use Mac Address: Use MAC address of used wireless card to be AP name. System default is APX (X is last number of Mac Address).

11. Security Setting: Authentication mode and encryption algorithm used within the AP. System default is no authentication and encryption.

12. No forwarding among wireless clients: No beacon among wireless client, clients can share information each other. System default is no forwarding.

13. Hide SSID: Prevent this AP from recognized in wireless network. This is disabled as default.

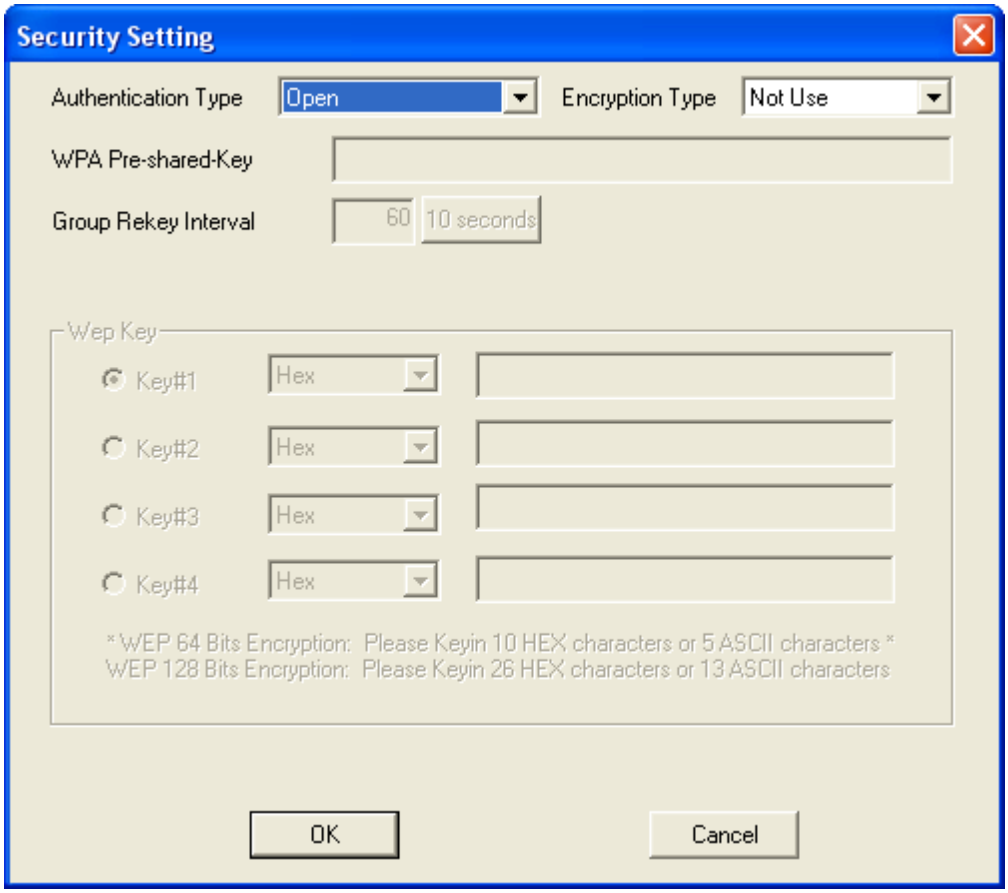
14. Allow BW40 MHz: Allow BW40 MHz capability.

15. Default: Use system default value.

16. Apply: Apply the above changes.

5.1.2 Security Setting

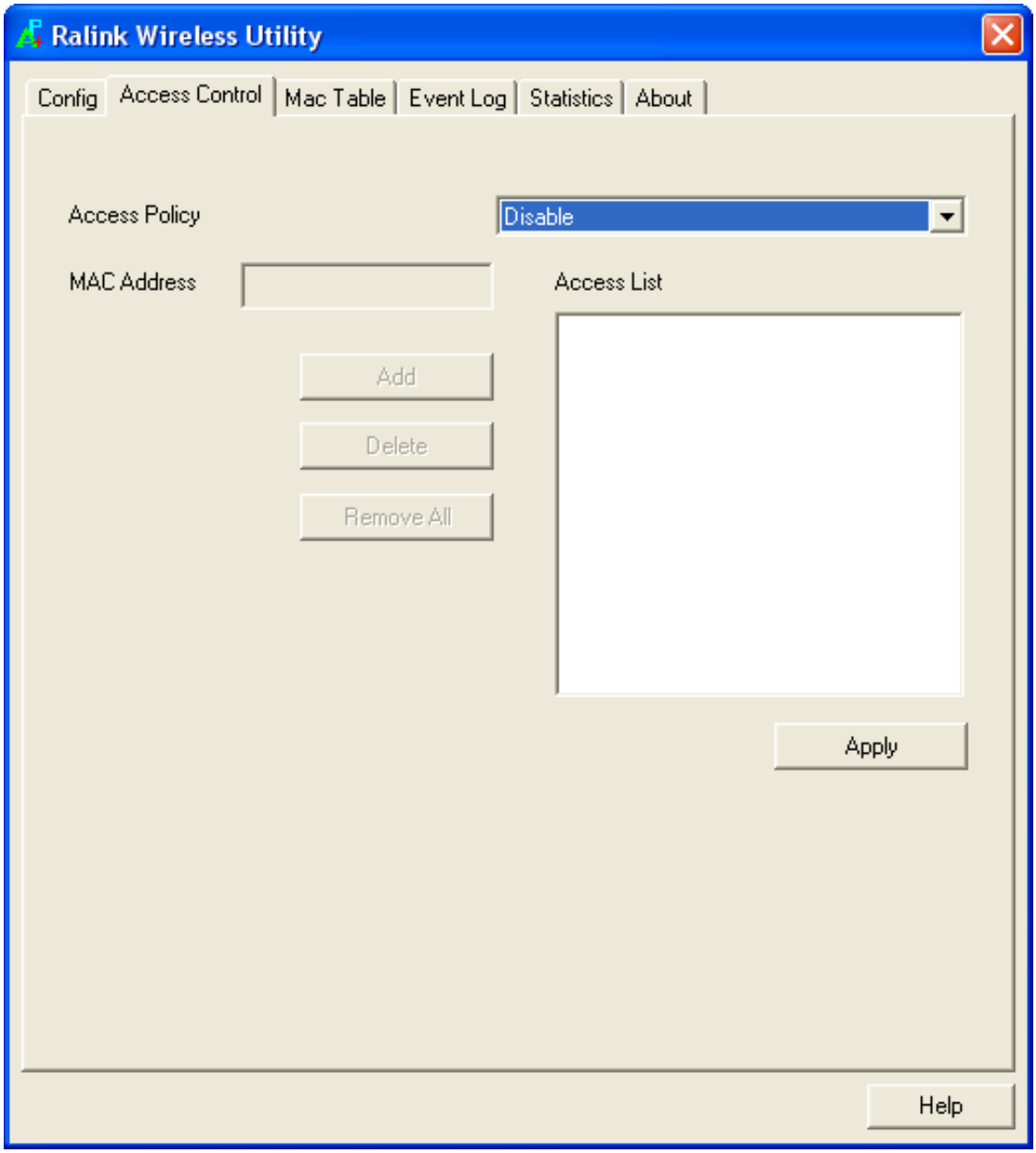
This page pops up after clicking the Security Settings button. Please follow the instructions below:



Authentication Type	Select to be open or WPA-PSK system.
Encryption Type	Select an encryption type from the drop list.
WPA Pre-shared Key	A shared string between AP and STA. For WPA-PSK authentication mode, this field must be filled with character longer than 8 and less than 32 length. (PCI only)
Group Rekey Interval	Only valid when using WPA-PSK encryption algorithm. The key will change compliance with seconds or beacon that user set. (PCI device only)
WEP Key	Only valid when using WEP encryption algorithm. The key must match the key on AP. There are several formats to enter the keys. a. Hexadecimal (40bits): 10 Hex characters. b. Hexadecimal (128bits): 32Hex characters. c. ASCII (40bits): 5 ASCII characters. d. ASCII (128bits): 13 ASCII characters.

5.1.3 Access Control

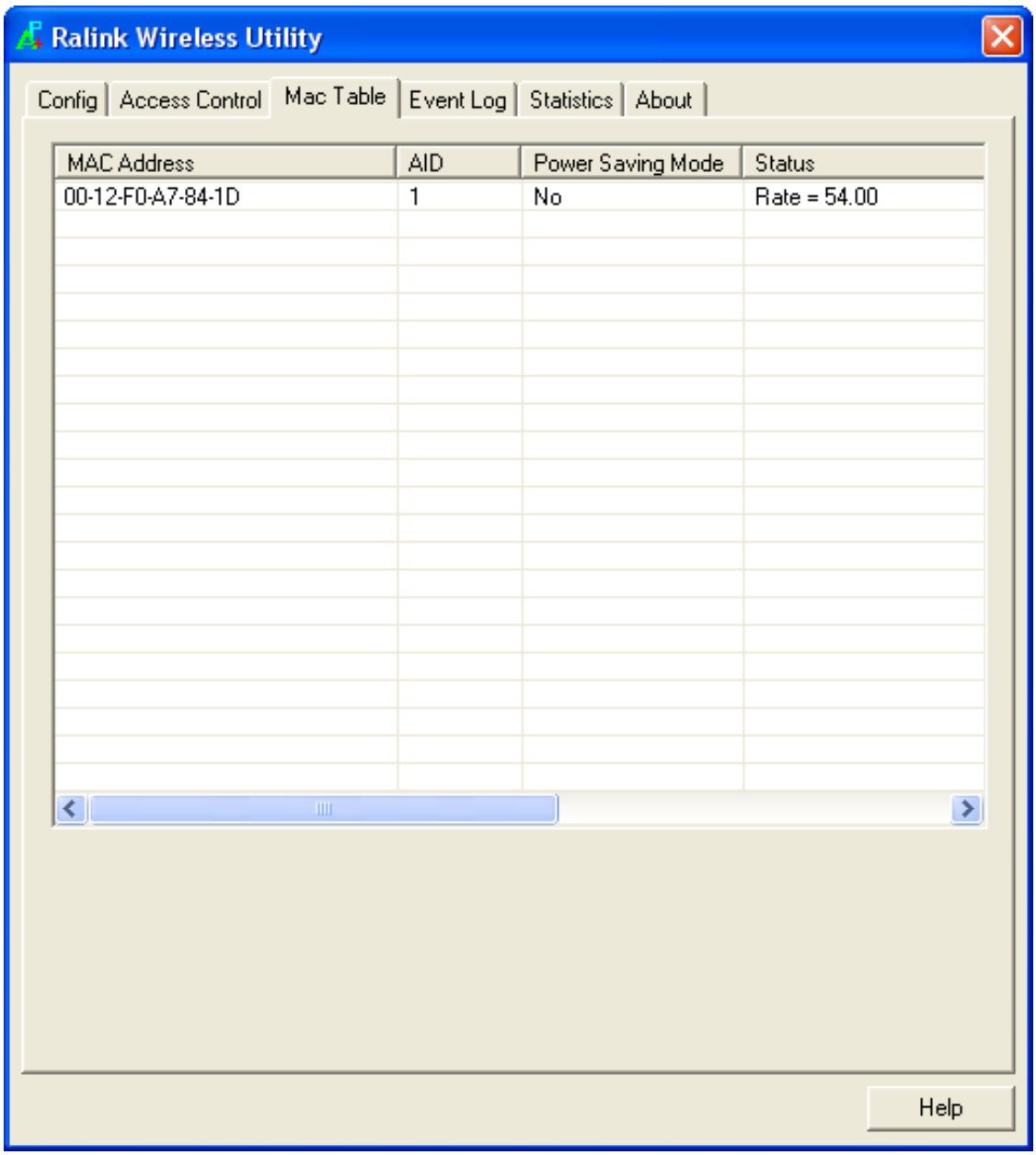
This function filters users to use this device by designating MAC address. Please refer to the following chart for introduction.



Access Policy	Choose a method to process access control from the drop list to determine the MAC addresses that you designated are allowed to access the AP or not.
MAC Address	Add allowed (or denied) MAC addresses to the MAC address list.
Access List	Display all Mac Addresses that you designated.
Delete	Delete Mac addresses that you selected.
Remove All	Remove all Mac address in Access List.
Apply	Apply changes.

5.1.4 MAC Table

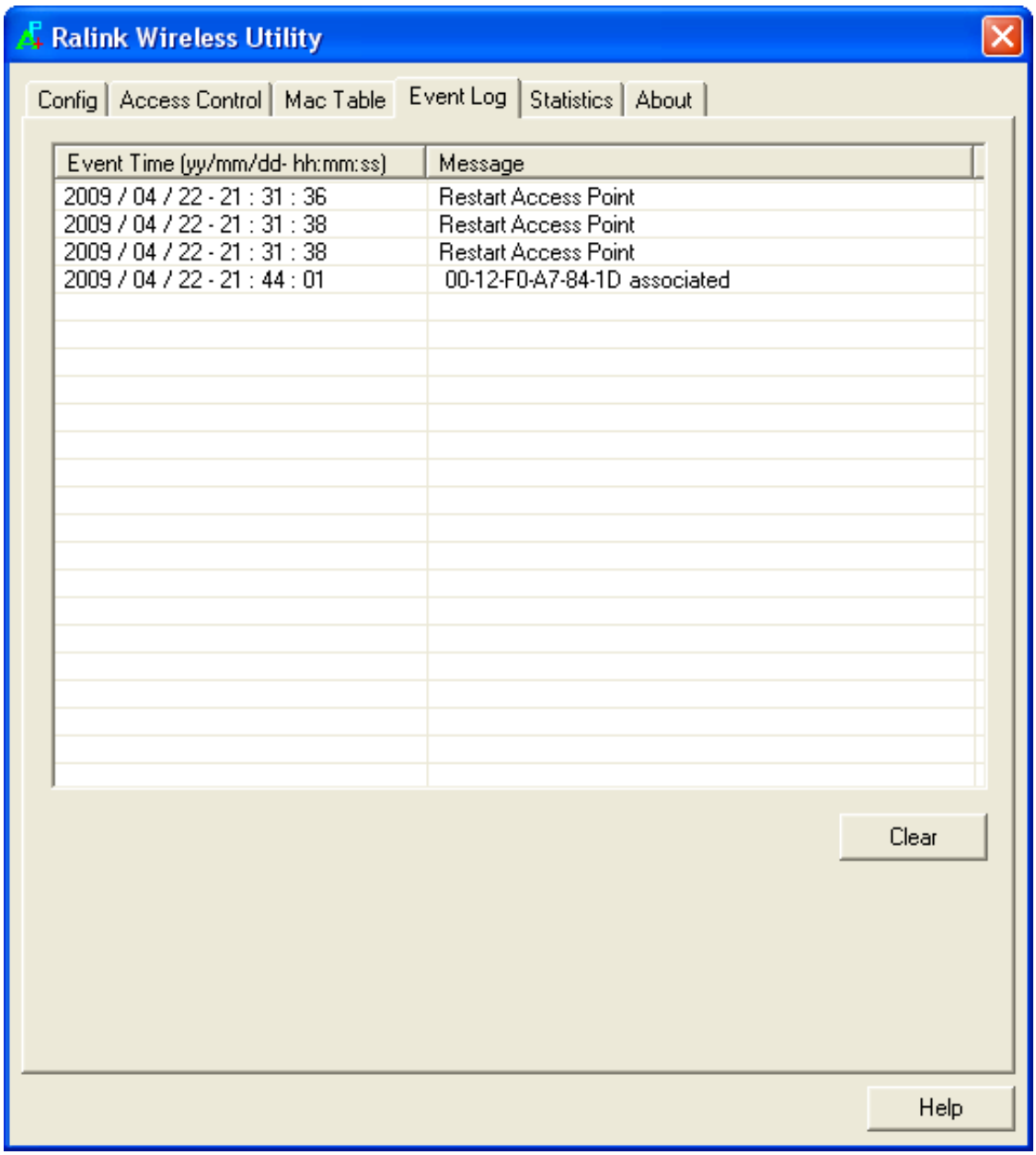
This page displays the station detail information of current connection.



MAC Address	The station MAC address of current connection.
AID	Raise value by current connection.
Power Saving Mode	Check if the connected station supports power saving.

5.1.5 Event Log

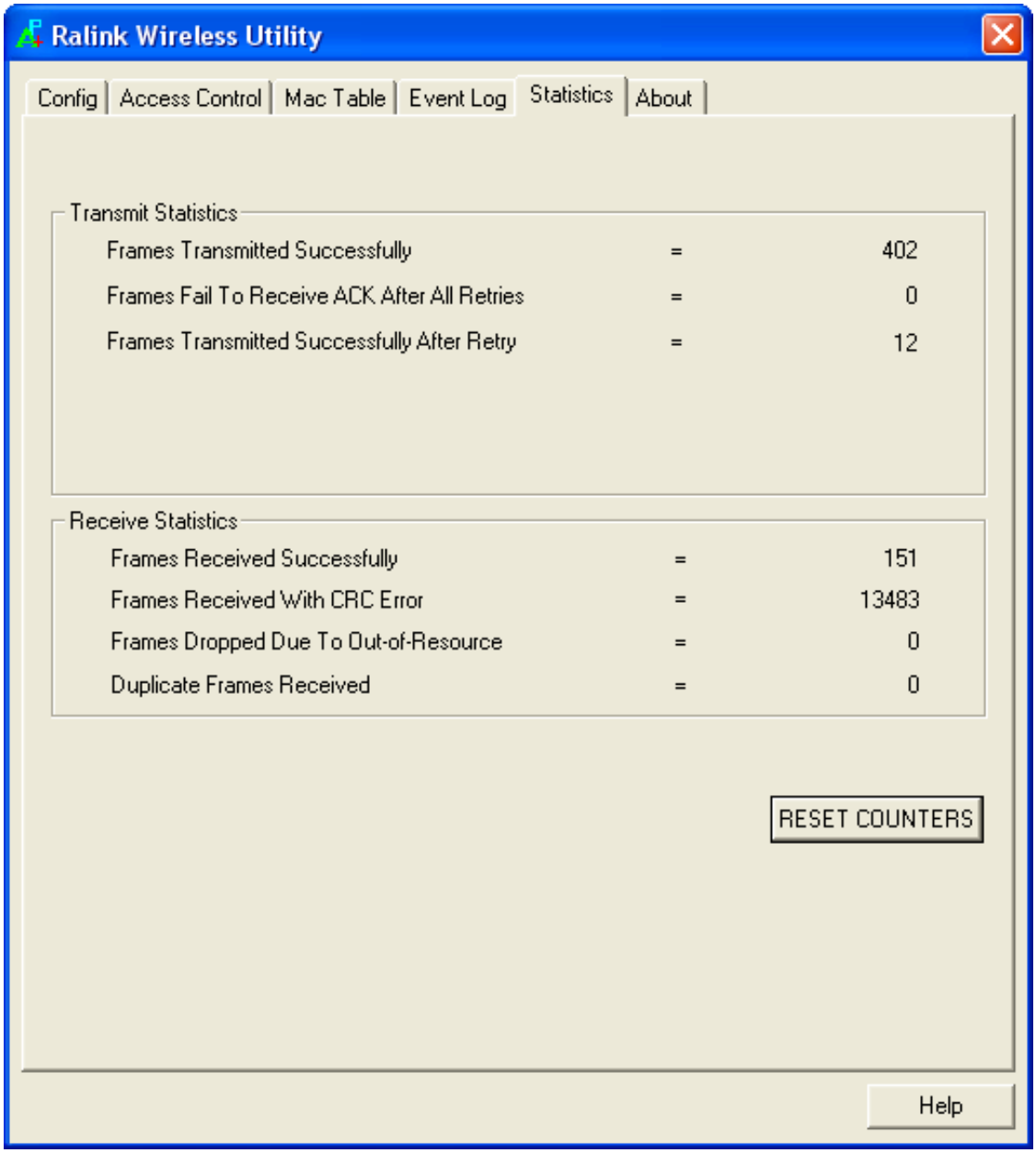
Record Soft AP all event time and message.



Event Time (yy/mm/dd-hh:mm:ss)	Record event time.
Message	All event messages.

5.1.6 Statistics

Statistics page displays the detail counter information based on 802.11 MIB counters.



Frames Transmitted Successfully	Frames that successfully sent.
Frames Fail To Receive ACK After All Retries	Frames that failed to transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Counts of CTS that successfully received after sending RTS frame.
RTS Frames Fail To	Counts of CTS that fail to be received after sending RTS

Receive CTS	frame.
Frames Retransmitted Successfully	Successfully retransmitted frames numbers.
Frames Received Successfully	Frames received successfully.
Frames Received With CRC Error	Frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Frames dropped due to resource issue.
Duplicate Frames Received	Duplicate received frames.
Reset Counters	Reset counters to zero.

5.2 Troubleshooting

If you encounter any problem when you're using this wireless network card, don't panic! Before you call your ealer of purchase for help, please check this troubleshooting table, the solution of your problem could be very simple, and you can solve the problem by yourself!

Scenario	Solution
I can't find any wireless access point	1. Click 'Rescan' for few more times and see if you can find any wireless access point or wireless device. 2. Please move closer to any known wireless access point. 3. 'Ad hoc' function must be enabled for the wireless device you wish to establish a direct wireless link. 4. Please adjust the position of network card (you may have to move your computer if you're using a notebook computer) and click 'Rescan' button for few more times. If you can find the wireless access point or wireless device you want to connect by doing this, try to move closer to the place where the wireless access point or wireless device is located.
Nothing happens when I click 'Launch config utilities'	1. Please make sure the wireless network card is firmly inserted into your computer's PCI slot. If the Wireless configuration utility's icon is black, the network card is not detected by your computer. Switch the computer off and insert the card again. If this doesn't work, contact the dealer of purchase for help. 2. Reboot the computer and try again. 3. Remove the driver and re-install. 4. Contact the dealer of purchase for help.
I can not establish connection	1. Click 'Connect' for few more times.

with a certain wireless access point.	2. If the SSID of access point you wish to connect is hidden, you have to input correct SSID of the access point you wish to connect. Please contact the owner of access point to ask for correct SSID. 3. You have to input correct passphrase / security key to connect an access point with encryption. Please contact 4. the owner of access point to ask for correct passphrase / security key. The access point you wish to connect only allows network cards with specific MAC address to establish connection. Please go to 'About' tab and write the value of 'Phy_Addess' down, then present this value to the owner of access point so he / she can add the MAC address of your network card to his / her access point's list.
The network is slow / having problem when transferring large files	1. Move closer to the place where access point is located. 2. Enable 'Wireless Protection' in 'Advanced' tab. 3. Try a lower TX Rate in 'Advanced' tab. 4. Disable 'Tx Burst' in 'Advanced' tab. 5. Enable 'WMM' in 'QoS' tab if you need to use multimedia / telephony related applications. 6. Disable 'WMM – Power Save Enable' in 'QoS' tab. 7. There could be too much people using the same radio channel. Ask the owner of the access point to change the channel number. Please try one or more solutions listed above.

Federal Communication Commission Interference Statement

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.