



Wireless N Adapter RNX-N150PCx

User Manual



FCC 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 or more 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.

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.
- 2) This device must accept any interference received, including interference that may cause undesired operation.

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

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

National Restrictions

2400.0-2483.5 MHz

Country	Restriction	Reason/remark
Bulgaria		General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy		If used outside of own premises, general authorization is required
Luxembourg		General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation		Only for indoor applications

Note: Please don't use the product outdoors in France.

Before We Begin

Thank you for purchasing this product, we would like to use this manual to help you know more about your RNX-N150PCx.

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice.



is a registered trademark of ROSEWILL INC. Other brands and product names are trademarks or registered trademarks of their respective holders. No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from ROSEWILL INC.

Copyright © 2009 ROSEWILL INC.

All rights reserved.

<http://www.rosewill.com>

Special Icons that needs your attention:



NOTE: This mark indicates that there is a note of interest or something you need to pay special attention to.



WARNING: This mark indicates warning or caution that there might be something can damage your device or property.

Table of Contents

Chapter 1 Product Overview	- 8 -
1.1 Package Content	- 8 -
1.2 Overview of the Product.....	- 8 -
1.3 Product Features.....	- 9 -
1.4 Product Specification.....	- 10 -
1.5 System Requirement.....	- 10 -
1.6 PCI Adapter LED Status.....	- 11 -
Chapter 2 Security Check List before Installation	- 12 -
Chapter 3 Installation Guide.....	- 13 -
3.1 Hardware Installation	- 13 -
3.2 Software Installation.....	- 14 -
Chapter 4 Connection Guide.....	- 17 -
4.1 Configures a Basic Network Connection	- 17 -
4.1.1 Selecting configuration tool.....	- 17 -
4.2 Connecting with Microsoft Zero Configuration	- 17 -
4.3 Connecting through Rosewill Utility.....	- 20 -
4.3.1 Steps to add wireless signal with Rosewill Utility for one time use	- 21 -
4.3.2 Steps to add wireless signal into Profile and keep for future record	- 22 -
Chapter 5 Utility Detailed Definition Guide	- 25 -
5.1 Tab Section Details:.....	- 25 -
5.1.1 Profile	- 25 -
5.1.2 Network.....	- 26 -

5.1.3	Advance	- 27 -
5.1.4	Statistics	- 27 -
5.1.5	WMM	- 29 -
5.1.6	WPS	- 29 -
5.1.7	About	- 31 -
5.2	Status Section Details	- 31 -
Chapter 6 Security Description Guide		- 33 -
6.1	Auth. \ Encry. Setting - WEP/TKIP/AES	- 33 -
6.2	802.1x Setup Details:	- 33 -
6.2.1	Method and Authentication:	- 34 -
6.2.2	ID\Password:	- 36 -
6.2.3	Client Certification:	- 36 -
6.2.4	EAP Method: EAP Fast	- 36 -
6.2.5	Server Certification	- 37 -
Chapter 7 Setup Examples Guide		- 38 -
7.1	WMM Setup Examples	- 38 -
7.1.1	Example to configure to Enable DLS (Direct Link Setup)	- 38 -
7.1.2	Example to Enable WMM – Power Save Enable	- 39 -
7.2	WPS Setup Examples	- 40 -
7.2.1	Example to Add to WPS Using PIN Method	- 40 -
7.2.2	Example to Add to WPS Using PBC Method	- 41 -
7.3	Security Settings: WEP/WPA/WPA2	- 43 -
7.3.1	Example to Configure Connection with WEP	- 43 -
7.3.2	Example to Configure Connection with WPA-PSK	- 44 -

Chapter 8 Troubleshooting	- 45 -
--	---------------

Chapter 1 Product Overview

Thank you for choosing Rosewill's 802.11n Wireless PIC adapter – RNX-N150PCx. This chapter is to introduce you more about this Wireless Adapter.

1.1 Package Content

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

1. Rosewill 802.11n Wireless PCI Adapter x 1
2. 2 dBi detachable Antenna x 1
3. Quick Installation Guide x 1
4. Resource CD x 1, including:
 - Rosewill Wireless N Client Utility and Driver
 - User Manual



Note: Make sure that the package contains the above items.

If any of the listed items are damaged or missing, please contact with your distributor.

1.2 Overview of the Product

PCI Adapter connects you with IEEE802.11n (Draft 2.0) networks at receiving rate up to an incredible 150Mbps! By using the reflection signal, 802.11n technology increases the range and reduces “dead spots” in the wireless coverage area. Unlike ordinary wireless networking of 802.11b/g standards that are confused by wireless reflections, 802.11n can actually use these reflections to increase four times transmission range of 802.11g products.

Besides, when both ends of the wireless link are 802.11n products, the PCI card can utilize twice radio band to increase three times transmission speed of ordinary 802.11g standard products, and can comply with backwards 802.11b/802.11g standards.

Soft AP supported by PCI Adapter can help you establish wireless LAN networking with lowest cost. Also WPS (PBC and PIN) encryption method can free you from remembering the long passwords. Complete WMM function makes your voice and video more smooth.

1.3 Product Features

- Complies with IEEE 802.11n (Draft 2.0), IEEE 802.11g, IEEE 802.11b standards
- Provides 32-bit PCI interface
- Provides 150Mbps receiving rate and 150Mbps sending rate
- Supports 20MHz/40MHz frequency width
- Auto-detects and changes the network transmission rate
- Provides two work modes: Infrastructure and Ad-Hoc
- Extended Antenna for ease of signal adjustment
- Supports Soft AP to establish your wireless LAN networking with lowest cost
- Supports 64/128-bit WEP, WPA, WPA2 encryption methods and 802.1x security authentication standard
- Supports WPS (PBC and PIN) encryption method to free you from remembering long passwords
- Supports WMM to make your voice and video more smooth
- Supports Windows® 2000, XP 32/64, Vista 32/64, Win 7 32/64

1.4 Product Specification

Standard IEEE 802.11n Draft 2.0 and IEEE802.11g/b	RF Output Power(Typical) 802.11b: up to 17 ± 1 dBm 802.11g: up to 15 ± 1 dBm 802.11n: up to 16 ± 1 dBm	Driver Support Windows® 2000, XP 32/64, Vista 32/64, Win7 32/64	
Frequency Band 2.400GHz ~ 2.484GHz	Interface PCI interface 2.2	Security 64/128-bit WEP (Hex & ASCII), WPA(TKIP with IEEE 802.1x), WPA2(AES with IEEE 802.1x)	
Data Rate 802.11n: up to 150Mbps Upstream and up to 150 Mbps downstream 802.11g: 54, 48, 36, 24, 18, 12, 9 & 6Mbps 802.11b: 11, 5.5, 2 and 1 Mbps with auto-rate fall back	Antenna 100 cm 2dBi External Detachable antenna	Dimension:	
		Without Bracket 120 x 80 x 15 mm 4.7 x 1.7 x 0.5 inches	With Bracket 4.7 x 4.7 x 1.7 inches
		Weight: (with Bracket and Antenna)	
		45 g	
Operation Temperature 0°C ~ 55°C ambient temperature	Storage Humidity 10% ~ 90% (Non-condensing)	Storage Temperature -20°C ~ 70°C ambient temperature	

1.5 System Requirement

You must have at least the following

- A desktop PC with an available 32-bit PCI slot
- Minimum 300MHz processor and 32MB memory
- Windows 98SE, ME, 2000, XP 32/64, Vista 32/64, Win7 32/64
- A CD-ROM Drive
- PCI controller properly installed and working in the desktop PC

- 802.11n or 802.11b/g Access Point (for infrastructure Mode) or another 802.11n or 802.11b/g wireless adapter (for Ad-Hoc; Peer-to-Peer networking mode.)

1.6 PCI Adapter LED Status

The status LED indicators of the PCI Adapter are described in the following.

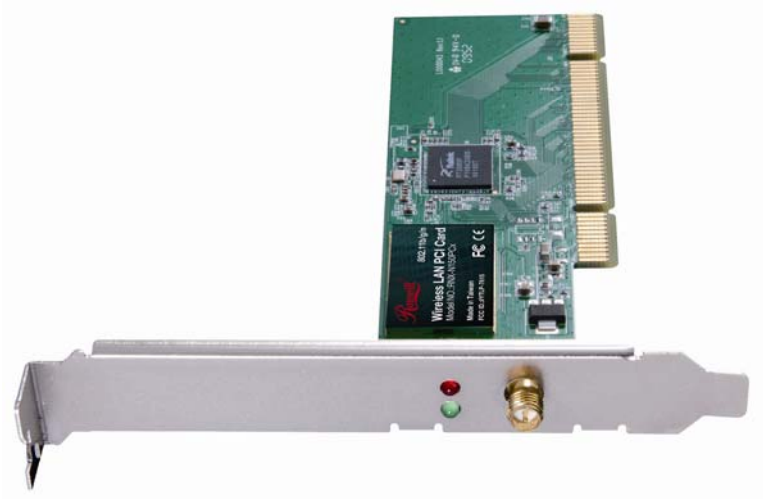


Figure 1-1 Wireless PCI Card LED

- Lnk/Act ON (Green): Indicates a valid connection.
- Lnk/Act Flashing: Indicates the Adapter is transmitting or receiving data

Chapter 2 Security Check List before Installation



Wireless Networks are very convenient, however, since it uses radio waves to send information. It can be vulnerable from those who intended to do harm. So we recommend you take additional steps to secure your wireless network.

- **Change the default wireless network name** or SSID on your wireless router
- **Change the default password** on your wireless router
- **Enable encryption.** We suggest enabling high level of the encryption such as WPA and above.
- **Install Anti-virus program and personal firewall software**
- When set your encryption password, please **select strong pass phrases** that are at least eight characters in length. Combines both letters and numbers to create stronger password and avoid using standard words that can be found in the dictionary.

- Please also remember to keep a record of your **wireless network name, default password** (The login name and password which you will need when linking into your wireless router through Internet explorer), **SSID** and **encryption password** (the password which you will need when connecting your wireless adapter with your wireless network) somewhere in case you need them in the future.

Chapter 3 Installation Guide

3.1 Hardware Installation

To install the adapter, follow these steps listed below:

1. Turn off your desktop PC and disconnect the power.
2. Remove your PC case and locate an available PCI slot on the motherboard. Remove the metal slot cover on the back of the PC. Check with your computer manufacturer for instructions if needed.
3. Slide the PCI Adapter into the PCI slot. Make sure that all of its pins are touching the slot's contacts. Once the adapter is firmly in place, secure its fastening tab to your PC's chassis with a mounting screw as shown in **Figure 3-1**. Then, close your PC case.

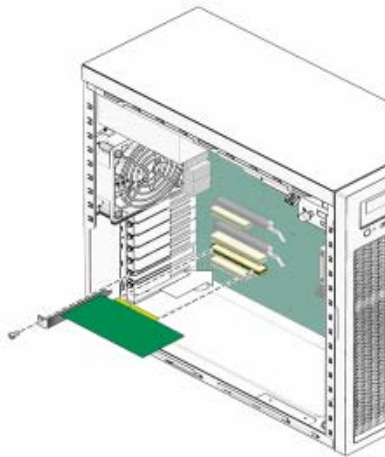


Figure 3-1

4. Reconnect your PC's power and turn on your desktop PC.



Note: Select **Cancel** when "Found New Hardware" window appears.

3.2 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. After Inserted PCI adapter into your computer. The system should find the newly installed device automatically like **Figure 3-2**. Click cancel to close this window.



Figure 3-2

2. Insert the CD-Rom that came with this product to your CD-Rom drive. The menu window pops up automatically as **Figure 3-3**. Please click the “**Driver**” button of this product. **Note:** If the CD-Rom fails to auto-run, please click on “**My Computer**”> your **CD-Rom Drive**> **(folder of this product)**> **Driver** then double-click the “**Setup**” icon to start this menu.



Figure 3-3

3. Select if you are going to configure your wireless network with this **Rosewill Utility** or with **Microsoft Zero Configuration tool**.

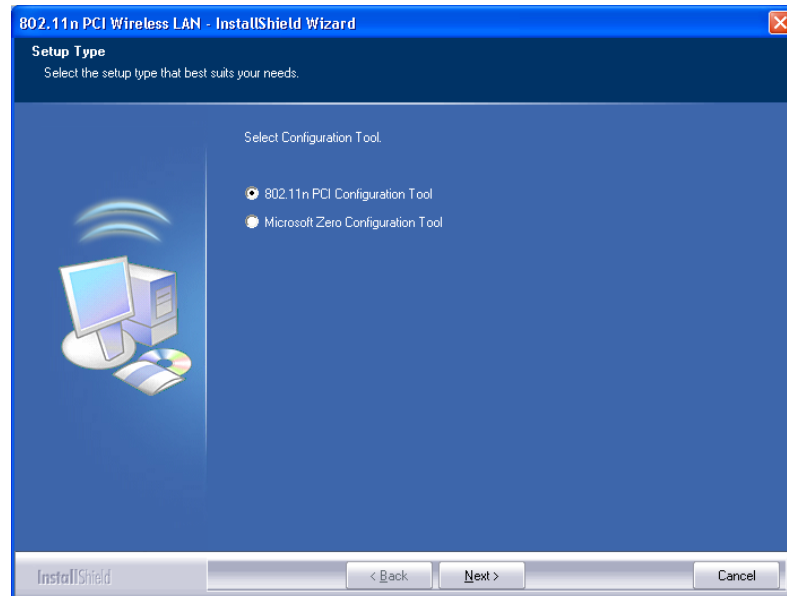


Figure 3-4

4. Click the **“Install”** button to start installing.

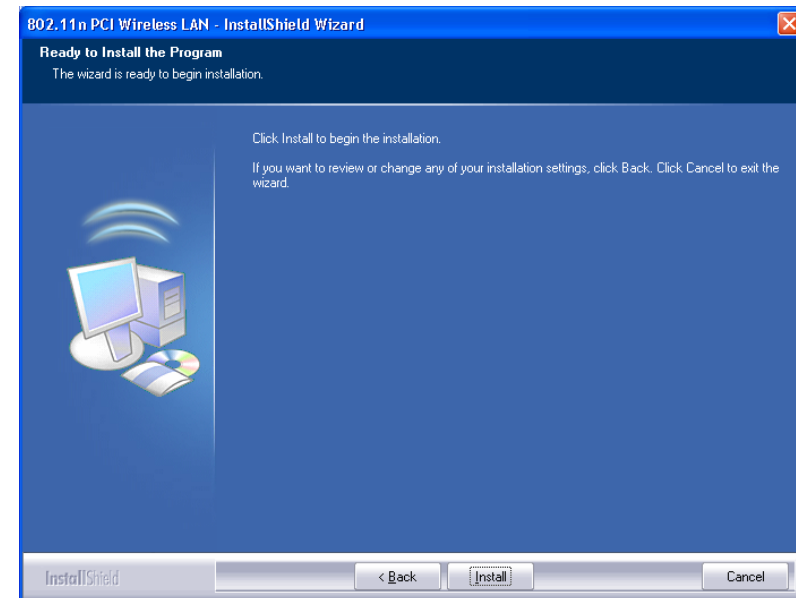


Figure 3-5

5. Click the **“Finish”** button to complete installation.

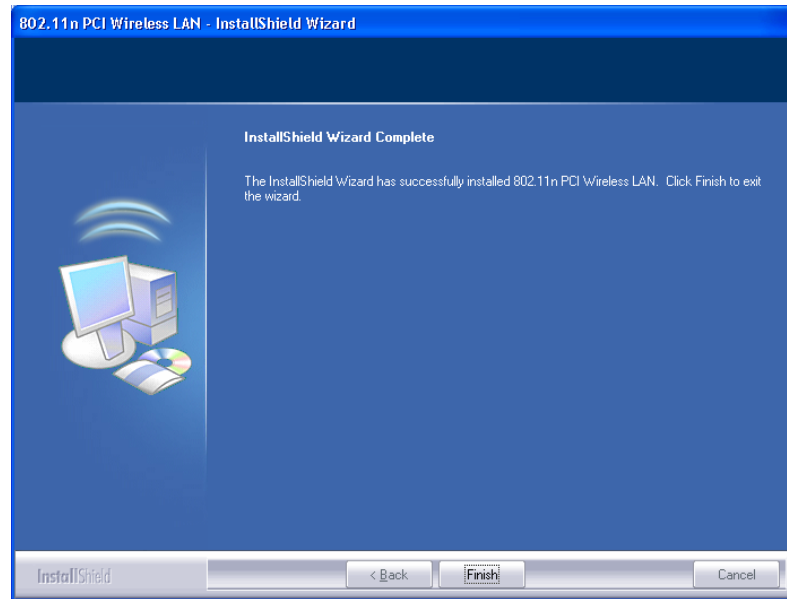


Figure 3-6

6. You may be prompt to restart your computer for the driver to take effect. Please select **“Restart”** or depending on your desire, you can select **“Restart Later”**

Chapter 4 Connection Guide

This chapter will help you understand the management interface of the device and how to manage the device.

4.1 Configures a Basic Network Connection

4.1.1 Selecting configuration tool

Windows XP includes a wireless configuration utility named "Windows Zero configuration" (WZC) which provides basic configuration functions to RNX-N150PCx. Rosewill's utility provides additional WPA functionality. This utility will let users make a selection when it first runs after windows XP boots.



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 mouse right click select  in the lower right hand corner of the Toolbars like **Figure 4-1**.



Figure 4-1

4.2 Connecting with Microsoft Zero Configuration

1. After specifying the Microsoft **Zero Configuration tool** to configure your wireless network, right click on the icon



on system tray as **Figure 4-2**. Select "**View available wireless Networks**" to specify your wireless network.



Figure 4-2

2. The tool shows the available wireless networks. Select your network SSID to connect with like **Figure 4-3**.

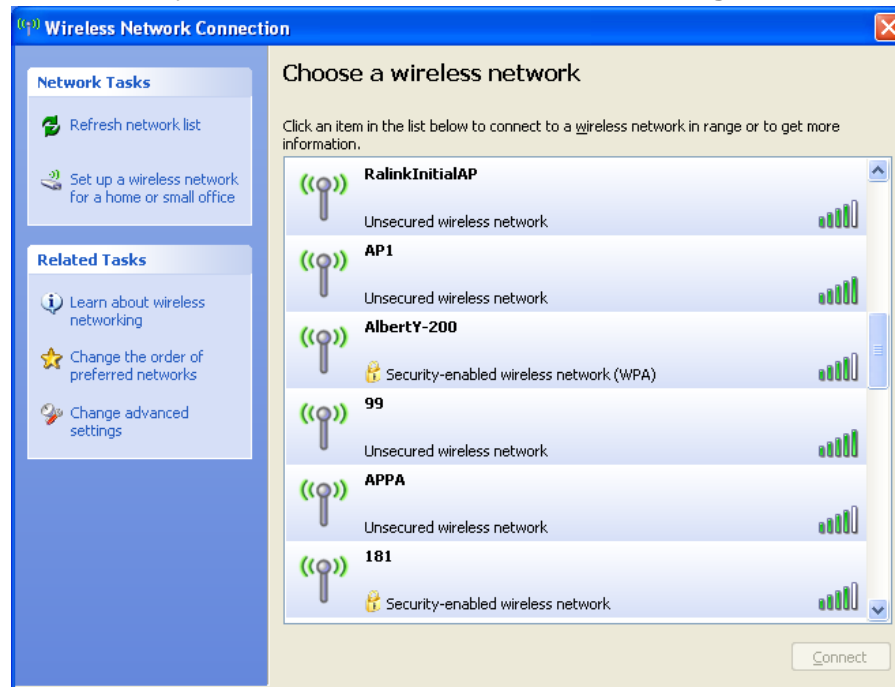


Figure 4-3

3. If your wireless Network has encryption enable, you will be ask to enter the password like **Figure 4-4**. Please enter your wireless password at “**Network key**” section twice and click “**Connect**” to confirm.

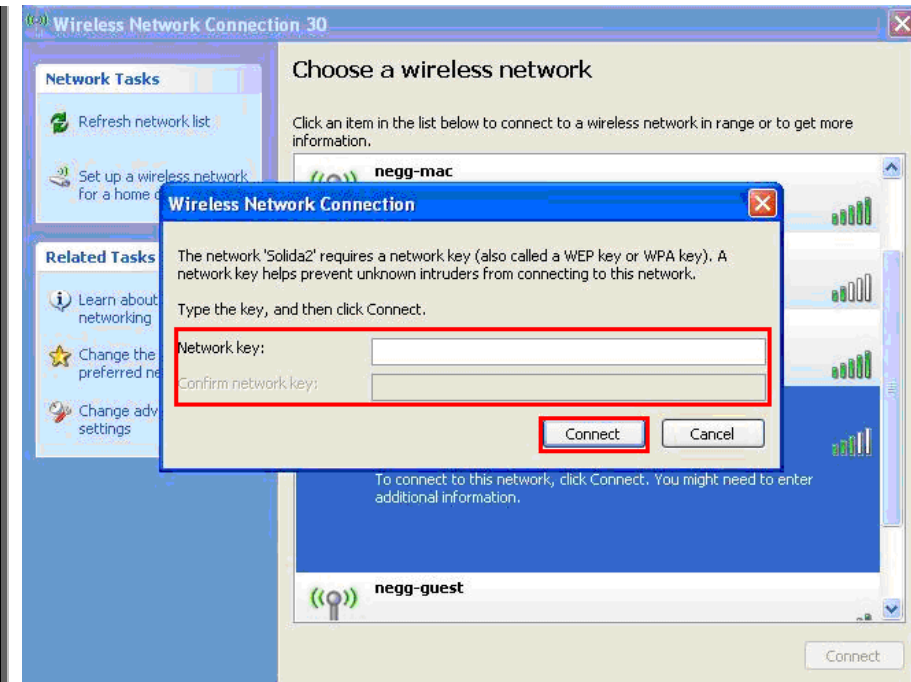


Figure 4-4

4. If your wireless Network does not contains encryption, select the intended access point and click “**Connect**”. Then click “**Connect Anyway**” like **Figure 4-5**.

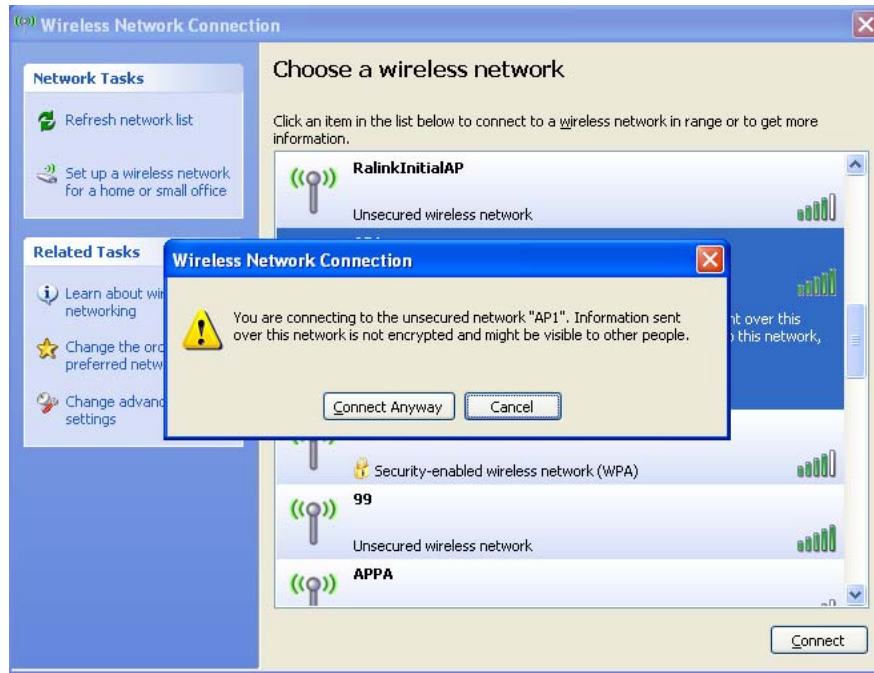


Figure 4-5

5. Once completed, you should see like **Figure 4-6** as your computer is now **"Connected"** with your wireless Network.

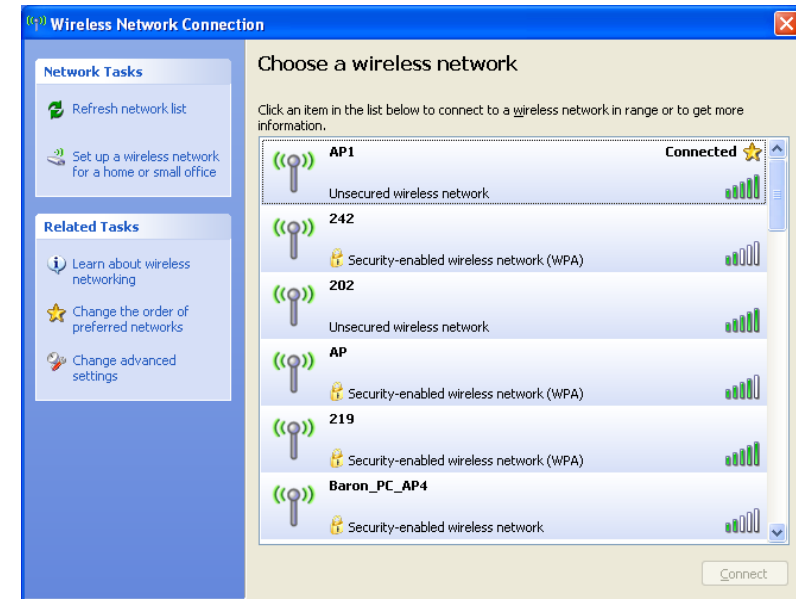


Figure 4-6

6. You should see the pop-up window on your low right hand corner indicate the connected status. As shown in **Figure 4-7**.

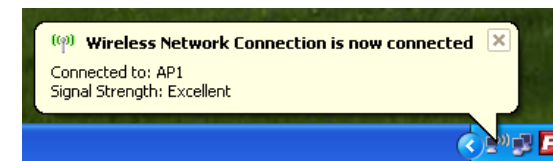



Figure 4-7

4.3 Connecting through Rosewill 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.

Clicking the Rosewill icon  on your desktop will bring up the utility main window. Users can find the surrounding AP signal in the list. The currently connected AP will be shown with a blue icon beside it, as shown in **Figure 4-8**. You can use the advanced tab to configure other advanced features provided by Rosewill's wireless NIC. For details on configuring the advanced features, please check with **Chapter 5**.

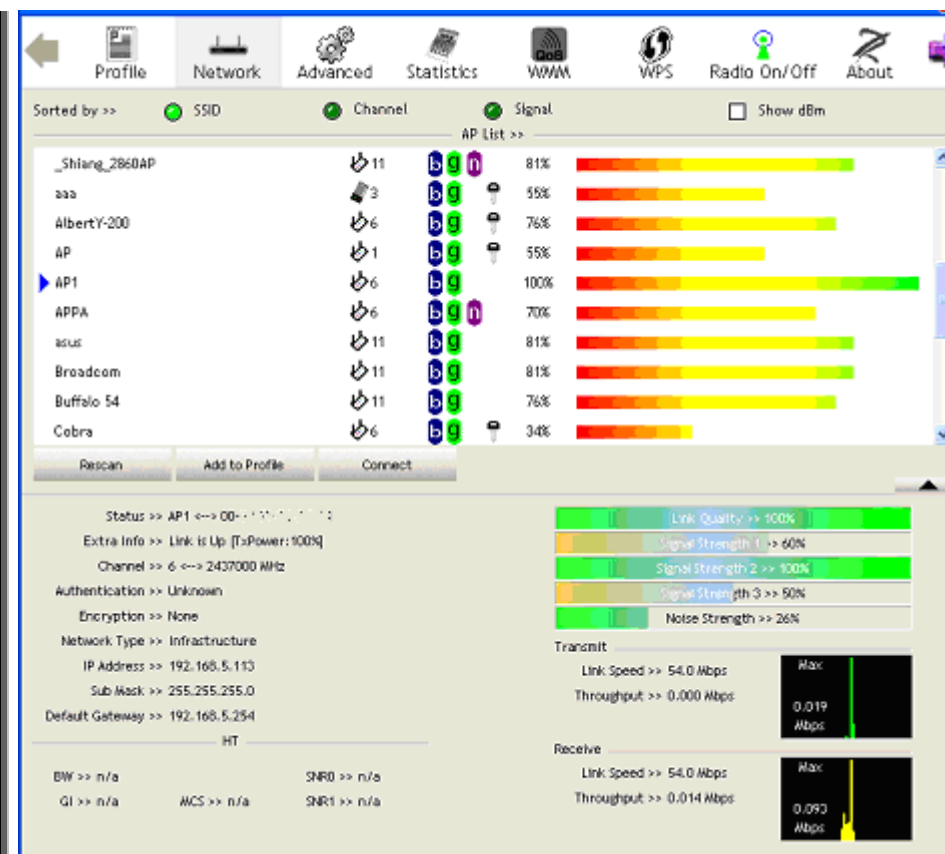



Figure 4-8

4.3.1 Steps to add wireless signal with Rosewill Utility for one time use

This section will lead you to link your wireless signal with your RNX-N150PCx. Please follow the **Figure 4-9** in adding the signal.

1. Click **“Rescan”** : Click on Rescan to search for all wireless signals near you.
2. Select your **desire SSID**: Click to select your wireless signal, in this example, you can see  next to AP1; meaning we have select AP1 as our desired SSID.
3. Click **“Add to Profile”** or **“Connect”** :
 - I. **Add to Profile**: This part will help your wireless adapter memorize the signal and password for your future use. Please see **Next Section** for more detail.
 - II. **Connect**: This is when you are in locations where you do not need your adapter to remember the signal.

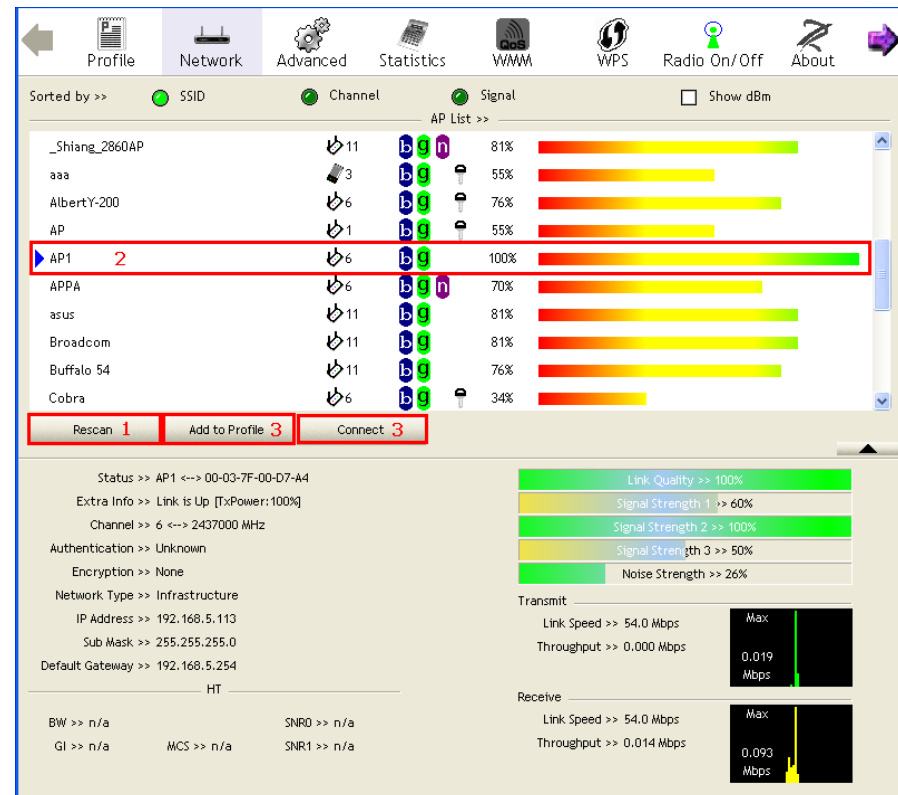




Figure 4-9

4.3.2 Steps to add wireless signal into Profile and keep for future record

Add to profile will help to store your wireless signal's information with your RNX-N150PCx. Please follow the **Figure 4-10** to add the signal into your profile so you don't have to enter them in the future.

There are two ways to "Add to Profile". You can add

through Network  tab or add through Profile  tab.

- **Adding to Profile through Network Tab. (Figure 4-10):**

1. First select "Add to Profile"
2. Choose the SSID you want to connect to. eg: **Rosewill-1**.
3. Key in your desired Profile Name, eg, HOME.
4. Or you can choose SSID with the pull-down window.
5. When complete, please select "Auth.\ Encry" to enter your password.

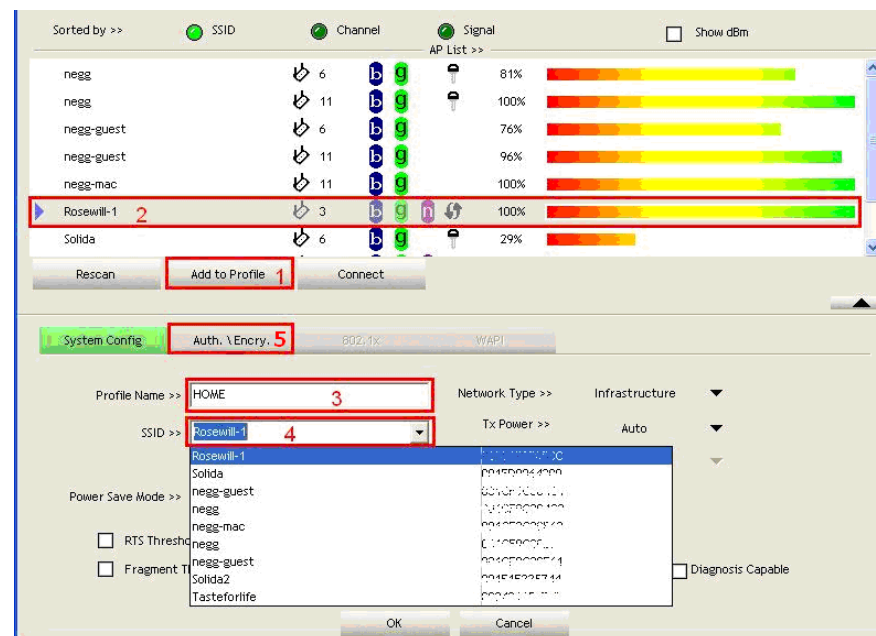


Figure 4-10

6. In Auth.\ Encry., First select Authentication of your wireless signal, Like **Figure 4-11**.
7. Enter your Wireless Network's password.
8. Click **OK** to complete the process.

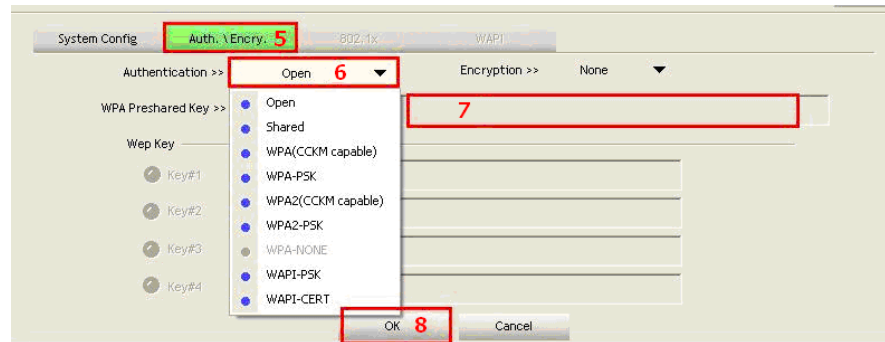


Figure 4-11



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.

● **Adding to Profile through Profile Tab. (Figure 4-12):**

1. First select “**Add**”
2. Key in your desired Profile Name, eg, HOME.
3. Choose the SSID by selecting the pull-down window.
4. When complete, please select “**Auth.\Encry**” to enter your password.

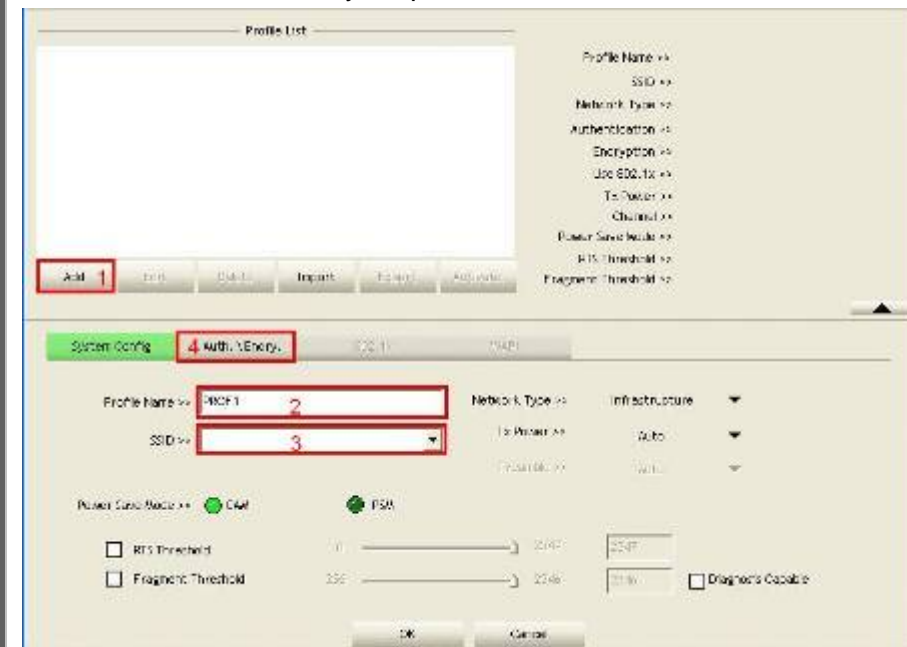


Figure 4-12

5. In Auth.\Encry. Like **Figure 4-13**.
6. First select Authentication of your wireless signal.
This should automatically provided to you when select your desired SSID.
7. Enter your password.
8. Click **OK** to complete the process.

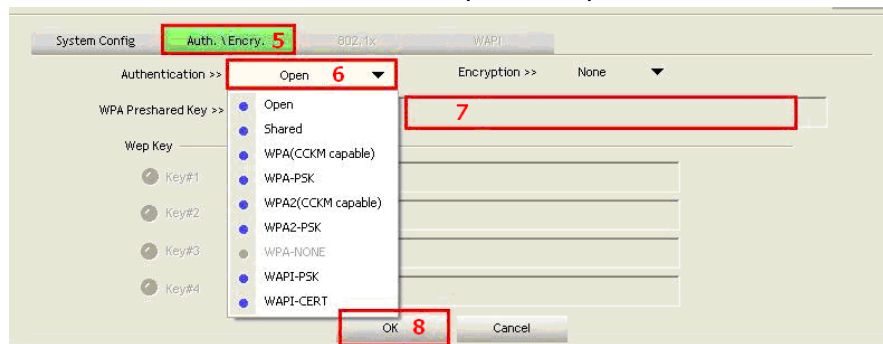


Figure 4-13

Chapter 5 Utility Detailed Definition Guide

The **Rosewill Utility** consisted of three parts:

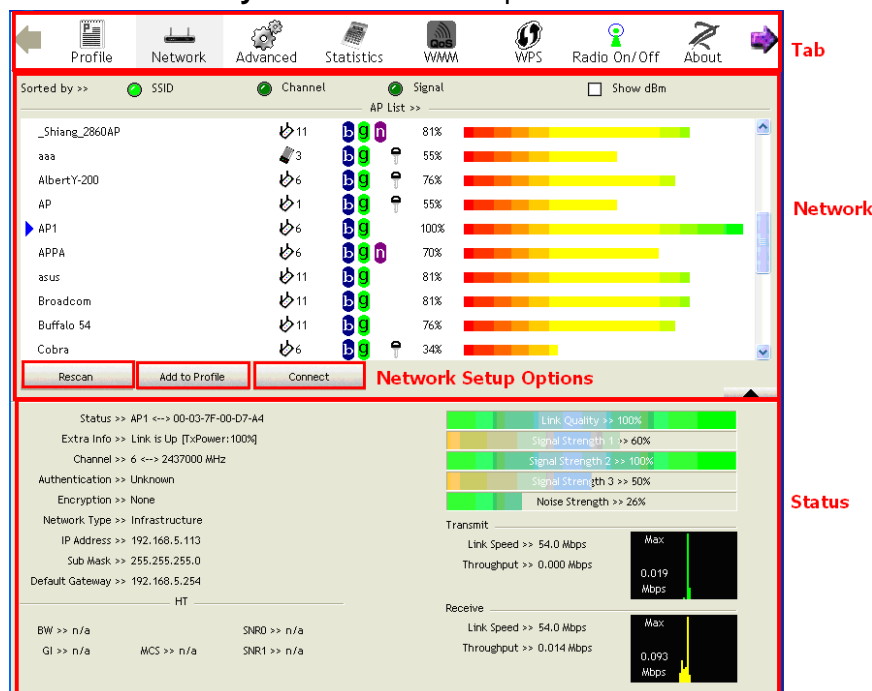


Figure 5-1

- 1 Tab Section:** on top of the window. You can click each button to access each configuration windows includes Profile page, Network Page, Advanced Page, Statistics Page, WMM Page, WPS Page, Radio On/Off function, and About

- 2 Network Section:** Provides you with information on the wireless signals around you. You have options to setup wireless network here with “Rescan”, “Add to Profile”, and “Connect”
- 3 Status Section:** bottom of the utility window. It shows the connection status and system information.

5.1 Tab Section Details



Figure 5-2

Tab Section provides you with the option to utilize RXN-N150PCx.

5.1.1 Profile

The Profile List keeps a record of your favorite wireless settings at home, office, and other public hot-spots. You can save multiple profiles, and activate the correct one at your preference. **Figure 5-4** shows the basic profile section.



Figure 5-3

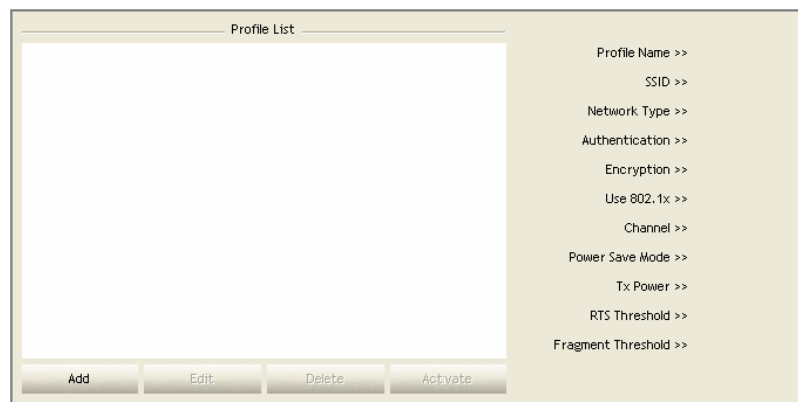


Figure 5-4

Definition of Each Fields in Profile:

Profile Name: Name of profile, preset to PROF* (* indicate 1, 2, 3...).

SSID: The access point or Ad-hoc name.

Network Type: Indicates the networks type, including infrastructure and Ad-Hoc.

Authentication: Indicates the authentication mode used.

Encryption: Indicates the encryption Type used.

Use 802.1x: Shows if the 802.1x feature is used or not.

Channel: Channel in use for Ad-Hoc mode.

Power Save Mode: Choose from CAM (Constantly Awake Mode) or Power Saving Mode.

Tx Power: Transmitting power, the amount of power used by a radio transceiver to send the signal out.

RTS Threshold: Users can adjust the RTS threshold number by sliding the bar or keying in the value directly.

Fragment Threshold: The user can adjust the Fragment threshold number by sliding the bar or key in the value directly.

5.1.2 Network

Network Tab 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 Status below.



Figure 5-5

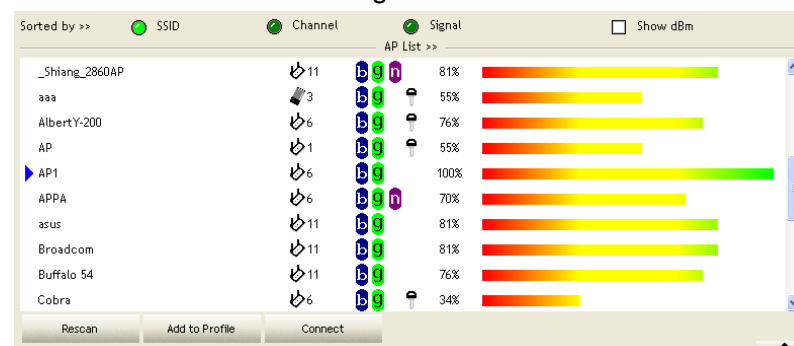


Figure 5-6

Definition of Each Fields in Network:

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

5.1.3 Advance

Advanced configurations for this adapter.



Figure 5-7

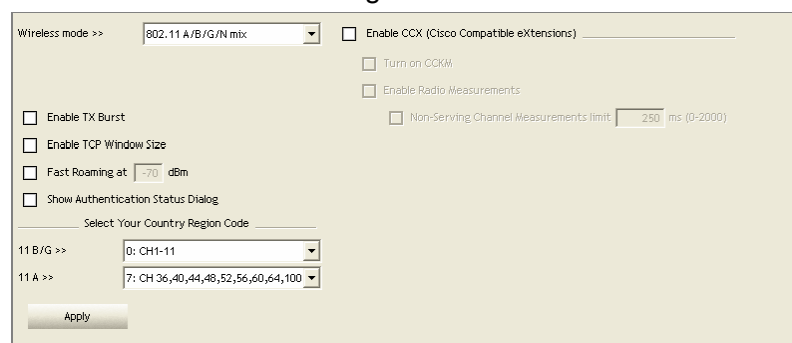


Figure 5-8

Definition of Each Fields in Advance:

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.

5.1.4 Statistics

Provides you with information on your wireless adapter.

Statistics 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.



Figure 5-9

Transmit			Receive
Frames Transmitted Successfully	=		1432
Frames Retransmitted Successfully	=		4
Frames Fail To Receive ACK After All Retries	=		0
RTS Frames Successfully Receive CTS	=		0
RTS Frames Fail To Receive CTS	=		0
Reset Counter			

Figure 5-10

Definition of Each Fields in Statistics - Transmit:

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

Transmit	Receive		
Frames Received Successfully	=		3153
Frames Received With CRC Error	=		201964
Frames Dropped Due To Out-of-Resource	=		0
Duplicate Frames Received	=		0
Reset Counter			

Figure 5-11

Definition of Each Fields in 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.

5.1.5 WMM

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



Figure 5-12

 WMM Setup Status
 WMM >> Enabled Power Save >> Disabled Direct Link >> Disabled
☒ WMM Enable
☐ WMM - Power Save Enable
☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO
☐ Direct Link Setup Enable
 MAC Address >> [][][][][][] Timeout Value >> [60] sec
 [Apply] [Tear Down]

Figure 5-13

Definition of Each Fields in WMM:

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.

5.1.6 WPS

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.



Figure 5-14

 WPS AP List

ID	AP1-WPS	SSID	Channel	Security-Enabled
ID : Unknown	Ubicom_Sample	00-10-18-9C-2E-27	1	
ID : Unknown	arvint-2060AP	00-0C-43-28-60-20	1	
ID : Unknown	arvint-2060AP	00-0C-43-20-60-60	3	
ID : Unknown	default	00-18-02-4A-0A-6B	6	

 WPS Profile List
 [Rescan]
 [Information]
 Pin Code
 26460208
 Config Mode
 Enrollee
 [Detail]
 [Connect]
 [Rotate]
 [Disconnect]
 [Delete]
 PIN ☒ WPS Associate IE Progress >> 0%
 PBC ☒ WPS Probe IE WPS status is disconnected

Figure 5-15

Definition of Each Fields in WPS:

WPS AP List: Display the information of surrounding APs with WPS IE from last scan result. List information includes SSID, BSSID, 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 includes 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-secure 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.

5.1.7 About

Click "About" displays the wireless card and driver version information as shown in Figure 5-16.



Figure 5-16



Figure 5-17

5.2 Status Section Details

The **Status** page displays detailed information about the current connection as shown in Figure 5-18.

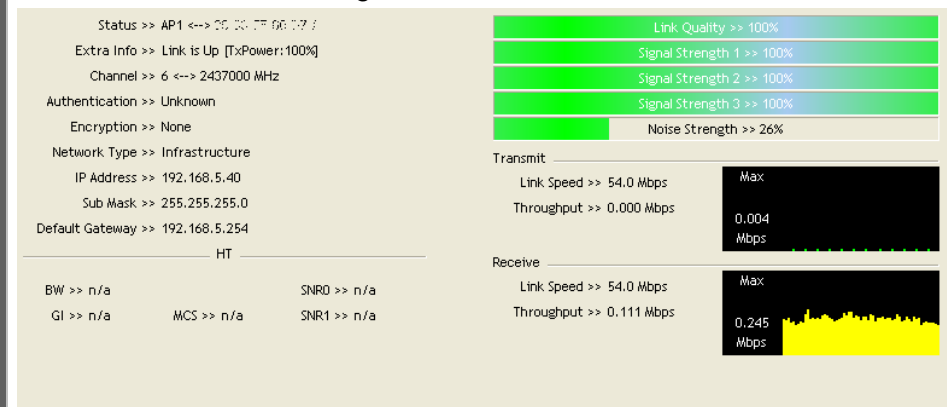


Figure 5-18

Definition of Each Fields in Status:

- Status:** Current connection status. If no connection, it will show Disconnected. Otherwise, the SSID and BSSID will show here.
- 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 about current connection.

Sub Mask: Sub mask about current connection.

Default Gateway: Default gateway about current connection.

Link Speed: Show current transmit rate and receive rate.

Throughout: Display transmits and receive throughput in unit of 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 the surrounding environment noise signal strength.

HT: Display current HT status in use, containing BW, GI, MCS, SNR0, and SNR1 value. [\(Show the information only for 802.11n wireless card.\)](#)

Chapter 6 Security Description

6.1 Auth. \ Encry. Setting - WEP/TKIP/AES

Figure 6-1

Definition of Each Fields in Auth. \ Encry.:

Authentication Type: There are 7 authentication modes supported by Rosewill Utility. They are open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK.

Encryption Type: For open and shared authentication mode, the available encryption types are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.

802.1X: This is introduced in the topic of Section 3-2.

WPA Pre-shared Key: This is the shared key between the AP and STA. If operating in WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.

WEP Key: Only valid when using WEP encryption algorithm.

The key must match the AP's key. There are several formats to enter the keys.

Hexadecimal - 40bits: 10 Hex characters.

Hexadecimal - 128bits: 32Hex characters.

ASCII - 40bits: 5 ASCII characters.

ASCII - 128bits: 13 ASCII characters.

6.2 802.1x Setup Details

802.1x is an advance Security function which used for authentication of the "WPA" and "WPA2" certificate by the server. Sometimes you may need to use this function when your wireless network under enterprise level.

Figure 6-2

6.2.1 Method and Authentication

Definition of Each Fields in 802.1X Method and Authentication:

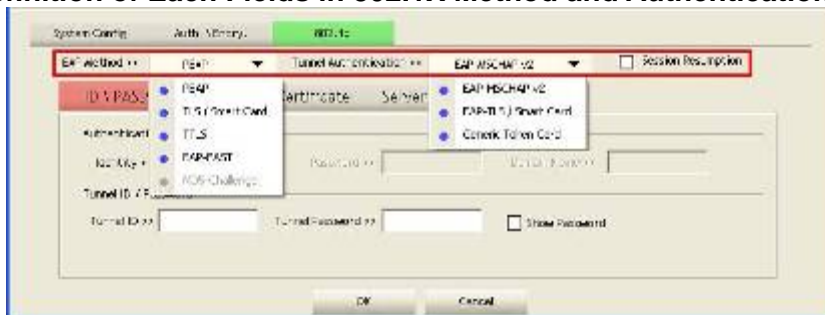


Figure 6-3

EAP Method:

PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authenticates data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.

TLS/Smart Card: Transport Layer Security. This provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.

TTLS: Tunneled Transport Layer Security. This security method

provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

EAP-FAST: Flexible Authentication via Secure Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be supplied (distributed one time) to the client either manually or automatically. Manually, it is delivered to the client via disk or a secured network distribution method. Automatically, it is supplied as an in-band, over the air, distribution. For tunnel authentication, only support "Generic Token Card" authentication.

LEAP: Light Extensible Authentication Protocol is an EAP authentication type used primarily by Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.

MD5-Challenge: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.

Tunnel Authentication:

Protocol: Tunnel protocol, List information include

"EAP-MSCHAP v2", "EAPTLS/Smart card", "Generic Token Card", "CHAP", "MS-CHAP", "MS-CHAP-V2", "PAP" and "EAP-MD5".

Tunnel Identity: Identity for tunnel.

Tunnel Password: Password for tunnel.

Session Resumption: The user can choose "Disable" and "Enable".

6.2.2 ID\Password

Definition of Each Fields in 802.1X ID\Password:

The screenshot shows the 'ID \ PASSWORD' configuration window. The 'Auth. \ Encry.' dropdown is set to '8021X'. The 'EAP Method >>' dropdown is set to 'PEAP'. The 'Tunnel Authentication >>' dropdown is set to 'EAP-MSCHAP v2'. The 'Session Resumption' checkbox is unchecked. The 'ID \ PASSWORD' tab is selected and highlighted with a red box. Below the tabs, there are two sections: 'Authentication ID / Password' and 'Tunnel ID / Password'. Each section has three input fields: 'Identity >>', 'Password >>', and 'Domain Name >>'.

Figure 6-4

ID \ PASSWORD

Authentication ID/Password: The identity, password and domain name for server.

Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain names can be keyed in the blank space.

Tunnel ID/Password: Identity and Password for the server.

6.2.3 Client Certification

Definition of Each Fields in 802.1X Client Certification:

The screenshot shows the 'Client Certification' configuration window. The 'Auth. \ Encry.' dropdown is set to '8021X'. The 'EAP Method >>' dropdown is set to 'PEAP'. The 'Tunnel Authentication >>' dropdown is set to 'EAP-MSCHAP v2'. The 'Session Resumption' checkbox is unchecked. The 'Client Certification' tab is selected and highlighted with a red box. Below the tabs, there is a section for 'Use Client certificate'. It includes a checkbox 'Use Client certificate', a dropdown menu for 'Issued To' (set to 'wptest2'), a text field for 'Issued By' (set to '2003serv'), a text field for 'Expired On' (set to '4/9/2008'), and a text field for 'Friendly Name'.

Figure 6-5

Use Client certificate: Client certificate for server authentication.

6.2.4 EAP Method: EAP Fast

The screenshot shows the 'EAP Method: EAP Fast' configuration window. The 'Auth. \ Encry.' dropdown is set to '8021X'. The 'EAP Method >>' dropdown is set to 'EAP-FAST'. The 'Tunnel Authentication >>' dropdown is set to 'Generic Token Card'. The 'Session Resumption' checkbox is unchecked. The 'EAP Fast' tab is selected and highlighted with a red box. Below the tabs, there is a section for 'EAP Fast'. It includes a checkbox 'Allow unauthenticated provision mode', a checkbox 'Use protected authentication credential' (checked), and a text field 'File Path >>'.

Figure 6-6

Definition of Each Fields in 802.1X EAP Method at EAP Fast:

Allow unauthenticated provision mode: During the PAC can be provisioned (distributed one time) to the client automatically. It only supported "Allow unauthenticated provision mode" and use "EAP-MSCHAP v2" authentication to authenticate now. It causes to continue with the establishment of the inner tunnel even though it is made with an unknown server.

Use protected authentication credential: Using PAC, the certificate can be provided to the client manually via disk or a secured network distribution method.

6.2.5 Server Certification

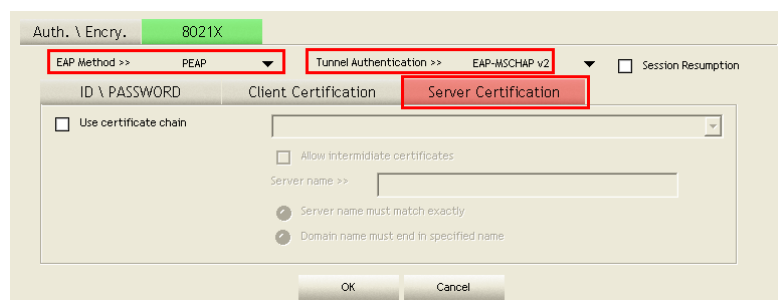


Figure 6-7

Definition of Each Fields in 802.1X Server Certification:

Certificate issuer: Select the server that issues the certificate.

Allow intermediate certificates: It must be in the server certificate chain between the server certificate and the server specified in the "certificate issuer must be" field.

Server name: Enter an authentication sever root.

Chapter 7 Setup Examples Guide

7.1 WMM Setup Examples

7.1.1 Example to configure to Enable DLS (Direct Link Setup)

1. Click "WMM Enable" to enable this function
2. Click the "Direct Link Setup Enable" checkbox

The screenshot shows the 'WMM Setup Status' window. At the top, it indicates 'WMM >> Enabled', 'Power Save >> Disabled', and 'Direct Link >> Enabled'. Below this, the 'WMM Enable' checkbox is checked and highlighted with a red box. Underneath, there are four unchecked checkboxes: 'WMM - Power Save Enable', 'AC_BK', 'AC_BE', 'AC_VI', and 'AC_VO'. The 'Direct Link Setup Enable' checkbox is also checked and highlighted with a red box. Below it, the 'MAC Address >>' field is empty, and the 'Timeout Value >>' is set to '60 sec'. There are 'Apply' and 'Tear Down' buttons at the bottom right.

Figure 7-1

3. Click the Network Tab to switch to the wireless router signal that support DLS function
4. Fill in the blanks of Direct Link with MAC Address of Station you want to connect to like **Figure 7-2**. The station must meet these two conditions:
 1. Connect with an AP that supports DLS features.
 2. Ensure that DLS is enabled.

This screenshot is similar to Figure 7-1, but the 'MAC Address >>' field is now filled with the hexadecimal values '00 0c 43 28 60 00', which are highlighted with a red box. The 'Timeout Value >>' remains '600 sec'. The 'Apply' and 'Tear Down' buttons are visible at the bottom right.

Figure 7-2

5. The Timeout Value indicates the time in seconds before it disconnects automatically. The value is an integer. The integer must be between 0~65535. **A zero value specifies that it stays connected.** The default Timeout Value is 60 seconds.

This screenshot is similar to Figure 7-2, but the 'Timeout Value >>' field is now filled with '600', which is highlighted with a red box. The 'MAC Address >>' field remains '00 0c 43 28 60 00'. The 'Apply' and 'Tear Down' buttons are visible at the bottom right.

Figure 7-3

6. Click "Apply". This Station will now be store in the list like **Figure7-4**. You can also remove the stored data by select and click "Tear Down" like Figure 7-5.

WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Link >> Enabled

☒ WMM Enable

☐ WMM - Power Save Enable

☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO

☒ Direct Link Setup Enable

MAC Address >> 00 0c 43 28 60 00 Timeout Value >> 600 sec Apply Tear Down

00-0C-43-28-60-00 600

Figure 7-4

WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Link >> Enabled

☒ WMM Enable

☐ WMM - Power Save Enable

☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO

☒ Direct Link Setup Enable

MAC Address >> Timeout Value >> 60 sec Apply Tear Down

00-0C-43-28-60-00 600 1. Select 2. Click

Figure 7-5

7.1.2 Example to Enable WMM – Power Save Enable

1. Click "WMM-Power Save Enable" to enable this option
2. Select the AC type you want to **enable**:
 - AC_BK: High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
 - AC_BE: Medium throughput and delay. Most traditional IP data is sent to this queue
 - AC_VI: Minimum delay. Time-sensitive video data is automatically sent to this queue
 - AC_VO: Time-sensitive data like VoIP and streaming media are automatically sent to this queue

WMM Setup Status

WMM >> Enabled Power Save >> Disabled Direct Link >> Disabled

☒ WMM Enable

☒ WMM - Power Save Enable

☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO

☐ Direct Link Setup Enable

MAC Address >> Timeout Value >> 60 sec Apply Tear Down

Figure 7-6

7.2 WPS Setup Examples

7.2.1 Example to Add to WPS Using PIN Method

WPS connection through PIN Method requires you enter the PIN Code into the Wireless Router that you want to connect to.

1. Select "Enrollee" from the Config Mode drop-down list.

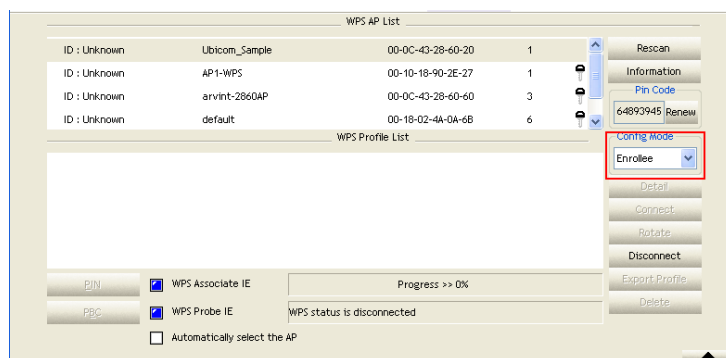


Figure 7-7

2. Click "Rescan" to update the available AP that supports WPS.

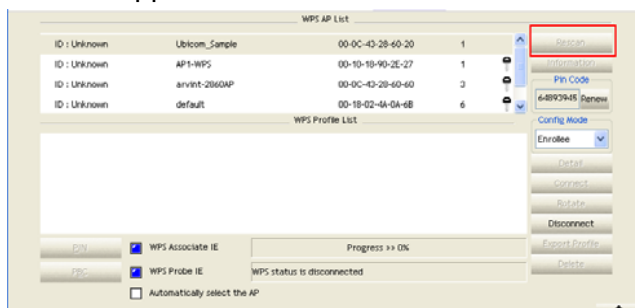


Figure 7-8

3. Select the AP that you want to join to.

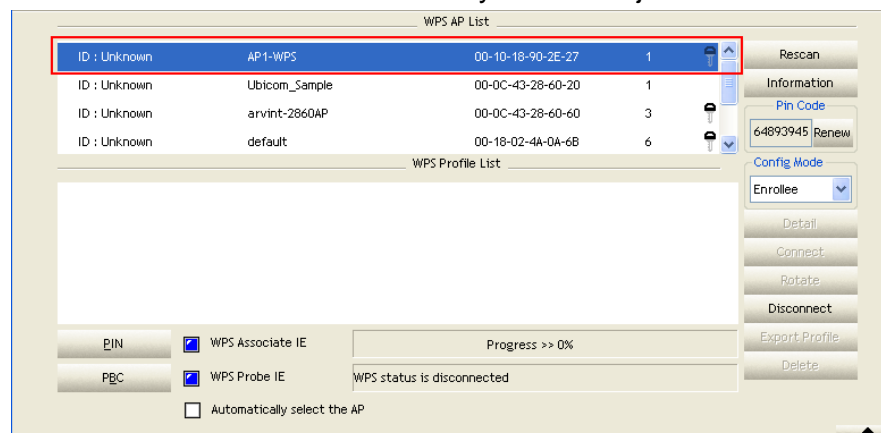


Figure 7-9

4. Click "PIN" to start the PIN entering process

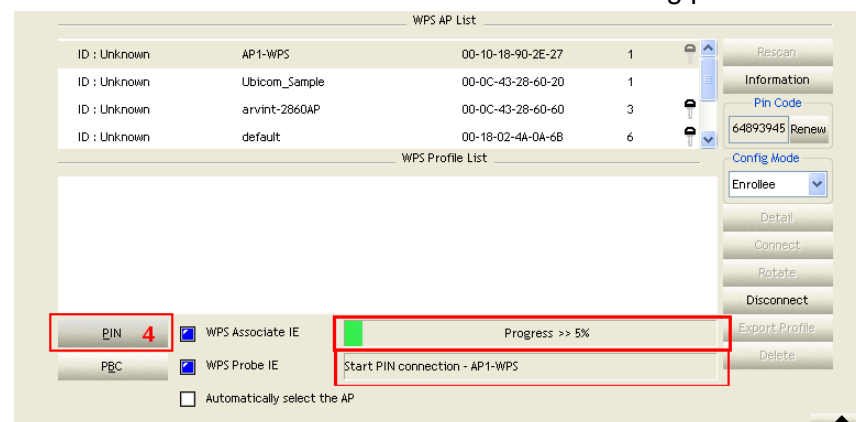


Figure 7-10

You should see "PIN – Begin associating to xxx (your AP)" in 5 like **Figure 7-10**; The process bar will start

5. You should enter the PIN number provided here to your AP.

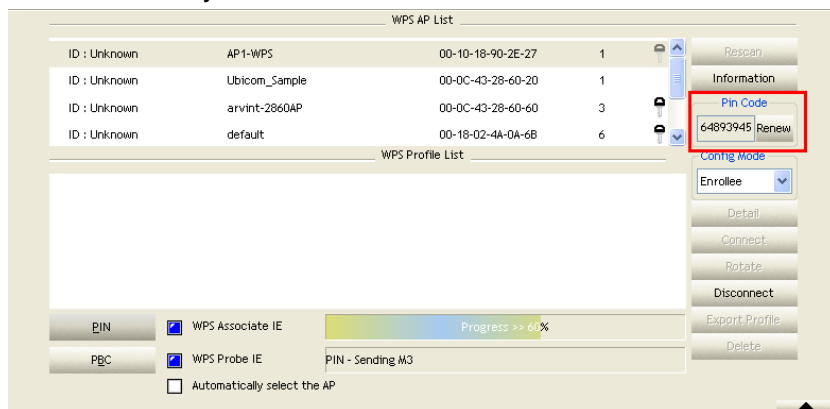


Figure 7-11

6. Once setup complete, you should see the utility shown as Figure 7-12

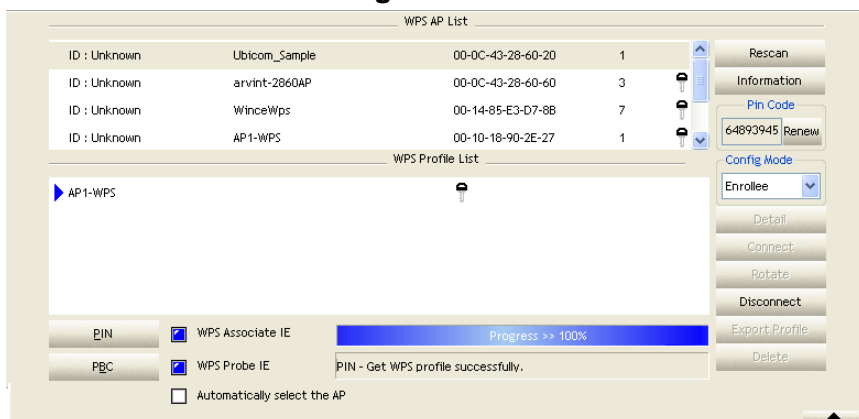


Figure 7-12



Note: If you use Microsoft Window Connection Now as an External Registrar, you must start PIN connection at STA first. After that, search out your WPS Device name and MAC address at Microsoft Registrar. Add a new device and enter PIN Code of STA at Microsoft Registrar when prompted.

7.2.2 Example to Add to WPS Using PBC Method

WPS connection through PBC Method requires you to press the button within 2 minutes with the Wireless Router that you want to connect to.

1. Select "Enrollee" from the Config Mode drop-down list.

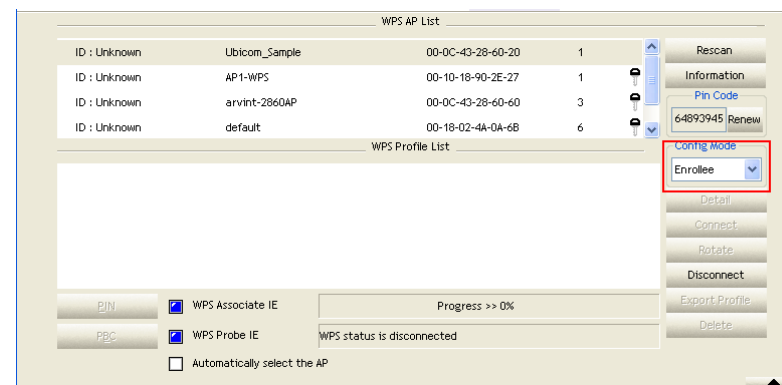


Figure 7-13

2. Click PBC to start the PBC connection

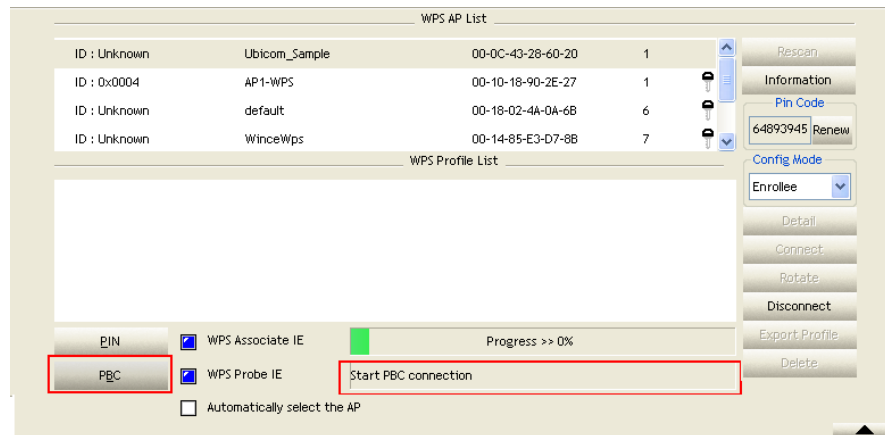


Figure 7-14

3. Push the PBC button on AP which should look like this



4. You should see the Status bar indicating searching for AP. Please allow some process time.

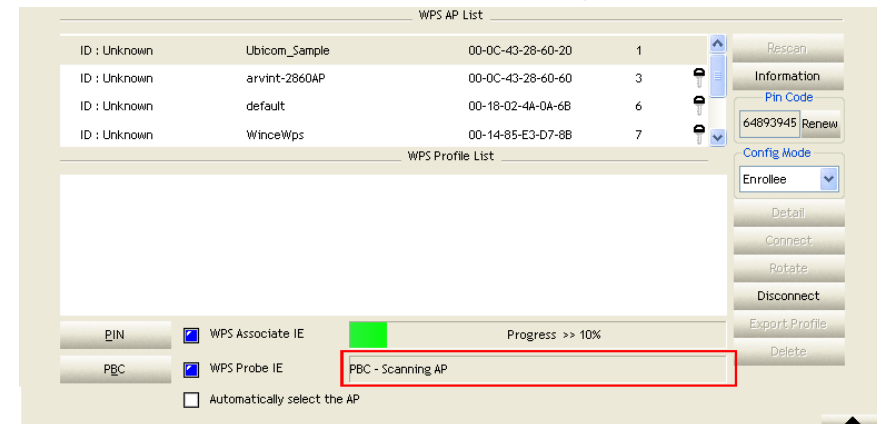


Figure 7-15

5. Once the right AP found, the utility will start process.

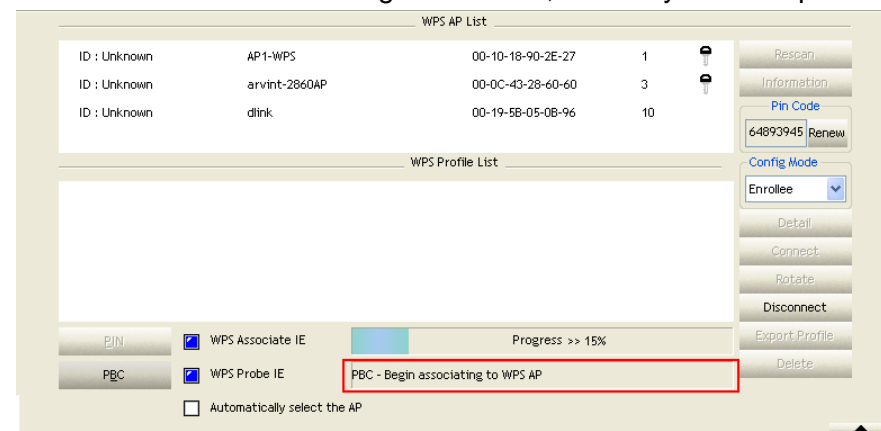


Figure 7-16

6. When connect successfully. The result will be displayed as it is in the figure below.

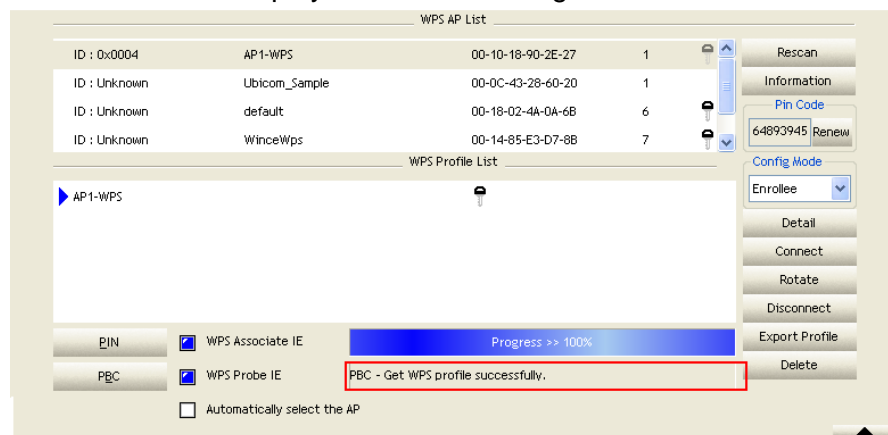


Figure 7-17



Note: WPS Status Bar Message:

- WPS EAP process failed:
- WPS configuration doesn't complete after two-minute connection
- Receive EAP with wrong NONCE
- Receive EAP without integrity
- An inappropriate EAP-FAIL received

7.3 Security Settings: WEP/WPA/WPA2

7.3.1 Example to Configure Connection with WEP

1. Select an AP with WEP encryption and click "Connect".

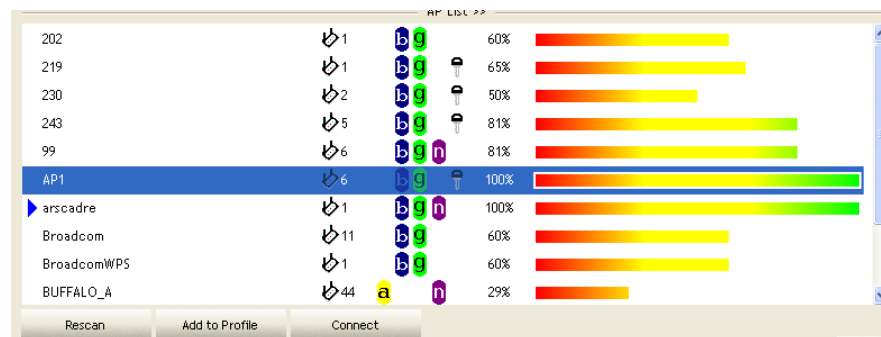


Figure 7-18

2. The Auth.\Encry. function will appear as below, select with WEP encryption.



Figure 7-19

3. Enter your password in the Key#1 Hexadecimal field. This value is same as your intended AP's setting. Click "OK", then this process will be complete.



Note: if the WPA Pre-Shared Key entered is not correct, you won't be able to exchange any data frames, even though the AP can be connected.

7.3.2 Example to Configure Connection with WPA-PSK

1. Select an AP with WPA-PSK authentication mode and click "Connect".
2. The Auth.\Encry. function will appear as below **select WPA-PSK** as the Authentication Type, then **select TKIP or AES** for encryption. **Enter the WPA Pre-Shared Key**. The WPA Pre-Shared Key here is use your intended AP's setting. (12345678 here is just a reference, please use a more complex password for better protect of your wireless network).

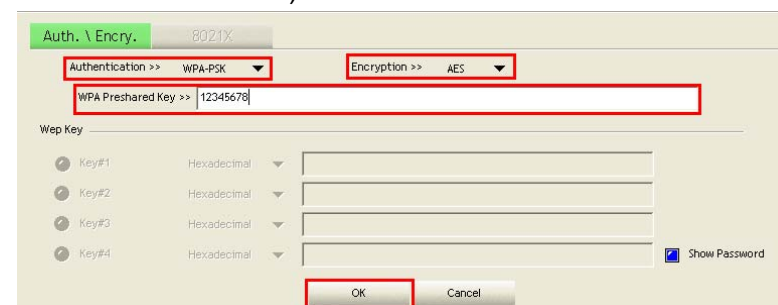


Figure 7-20

3. Click "OK", then the process is complete.

Chapter 8 Troubleshooting

This chapter provides solutions to problems that may occur during the installation and operation of PCI Adapter. Read the descriptions below to solve your problems.

1. The PCI Adapter does not work properly.

Reinsert PCI Adapter into your PC's PCI slot. Right click on My Computer and select Properties. Select the device manager and click on the Network Adapter. You will find PCI Adapter if it is installed successfully. If you see the yellow exclamation mark, the resources are conflicting. You will see the status of PCI Adapter. If there is a yellow question mark, please check the following: Make sure that your PC has a free IRQ (Interrupt ReQuest, a hardware interrupt on a PC.) Make sure that you have inserted the right adapter and installed the proper driver. If PCI Adapter does not function after attempting the above steps, remove it and do the following: Uninstall the driver software from your PC. Restart your PC and repeat the hardware and software installation as specified in this User Guide.

2. I cannot communicate with the other computers linked via Ethernet in the Infrastructure configuration.

Make sure that the PC to which PCI Adapter is associated is powered on. Make sure that PCI Adapter is configured on the same channel and with the same security options as with the other computers in the Infrastructure configuration.

3. What should I do when the computer with PCI Adapter installed is unable to connect to the wireless network and/or the Internet?

Check that the LED indicators for the broadband modem are indicating normal activity. If not, there may be a problem with the broadband connection. Check that the LED indicators on the wireless router are functioning properly. If not, check that the AC power and Ethernet cables are firmly connected. Check that the IP address, subnet mask, gateway, and DNS settings are correctly entered for the network. In Infrastructure mode, make sure the same Service Set Identifier (SSID) is specified on the settings for the wireless

clients and access points. In Ad-Hoc mode, both wireless clients will need to have the same SSID. Please note that it might be necessary to set up one client to establish a BSS (Basic Service Set) and wait briefly before setting up other clients. This prevents several clients from trying to establish a BSS at the same time, which can result in multiple singular BSSs being established, rather than a single BSS with multiple clients associated to it. Check that the Network Connection for the wireless client is configured properly. If Security is enabled, make sure that the correct encryption keys are entered on both PCI Adapter and the access point.

Thank you for purchasing a quality Rosewill Product.

Please register your product at: www.rosewill.com for complete warranty information and future support for your product.

Support: techsupport@rosewill.com