Rosewill®

Wireless LAN PCI Card RNX-N300X

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 pro-vide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not in-stalled 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.

Table of Content

Chapter 1 Overview

Thank you for choosing Rosewill's 802.11n 2T3R Wireless PCI adapter – RNX-N300X. This chapter is to introduce you more about this Wireless Adapter.

Package Content

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

1. Rosewill 802.11n Wireless PCI Adapter x 1
2. Quick Installation Guide x 1
3. 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.

1.1 Overview of the Product

The adapter is a draft 802.11n client device; it is designed to provide a high-speed and unrivaled wireless performance for your notebook. With a faster wireless connection, you can get a better Internet experience, such as downloading, gaming, video streaming and so on.

With the 802.11n technology, higher throughput improvements using MIMO (multiple input, multiple output antennas), the TL-WN951N's auto-sensing capability allows high packet transfer rate of up to 300Mbps for maximum throughput. It has good capability on anti-jamming, and it can also interoperate with other wireless (802.11b) products. The adapter supports WEP, WPA and WPA2 encryption to prevent outside intrusion and protect your personal information from being exposed.

The adapter is easy to install and manage. The Quick Setup Wizard guides you step-by-step through the installation process; the TP-LINK Wireless N Client Utility helps you create a wireless connection immediately.

With unmatched wireless performance, reception, and security protection, the TL-WN951N is the best choice for easily adding or upgrading wireless connectivity to your notebook computer.

1.2 Features

- Complies with IEEE802.11n (draft), IEEE802.11g, IEEE802.11b standards
- Supports WPA/WPA2 data security, IEEE802.1x authentication, TKIP/AES encryption, and 64/128/152-bit WEP encryption
- Supports high rate of up to 300Mbps for maximum throughput, supports automatically adjust to lower speeds due to distance or other operating limitations
- Supports QoS: WMM, WMM-PS
- Complies with PCI 2.3 or Mini PCI type III
- Supports Ad-Hoc and Infrastructure modes
- Good capability on anti-jamming
- Supports roaming between access points when configured in Infrastructure mode
- Ease to configure and provides monitoring information
- Supports Windows 2000, XP, Vista

1.3 LED Status

LED Indications	Status	Working Status
Status Green	Flashing Alternately	The adapter is trying to scan a networking connection.
Activity Green		
Status Green	Intermittently	The adapter is already connected but is not transmitting or receiving data.
Activity Green		
Status Green	Flashing	The adapter is transmitting or receiving data.
Activity Green		

Chapter 2 Installation Guide

2.1 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.

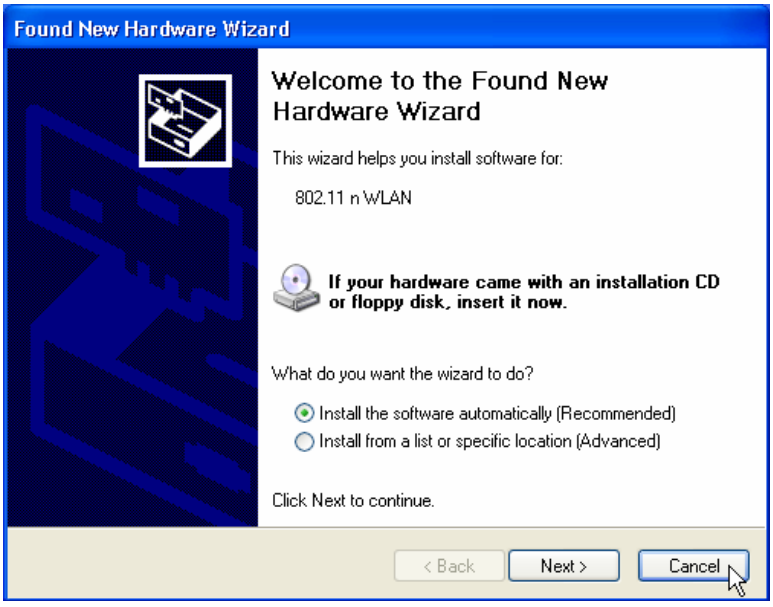
3. Slide the PCI Adapter into the PCI slot. Make sure that all of its pins are touching the slot's contacts. Once the adapter is firmly in place, secure its fastening tab to your PC's chassis with a mounting screw. Then, close your PC case.

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

2.2 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.

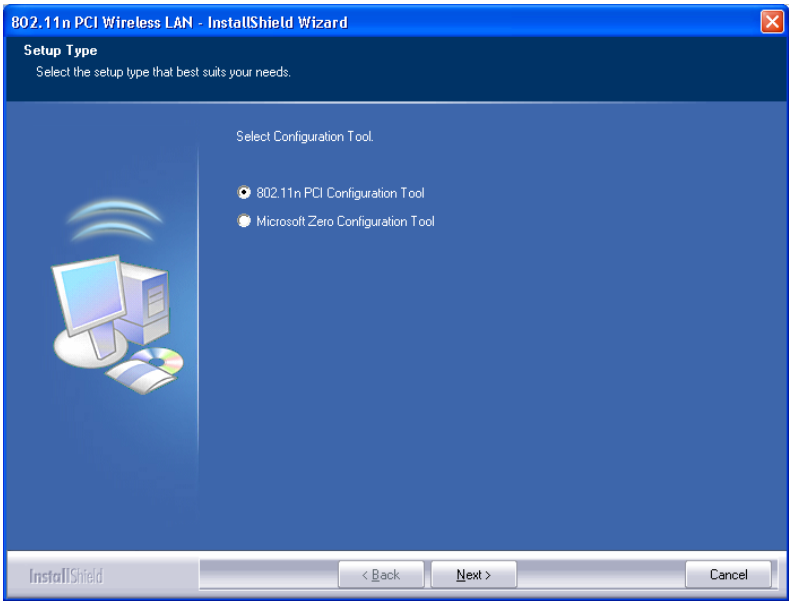
1. After Inserted PCI adapter into your computer. The system should find the newly installed device automatically. Click cancel to close this window.



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"** 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.

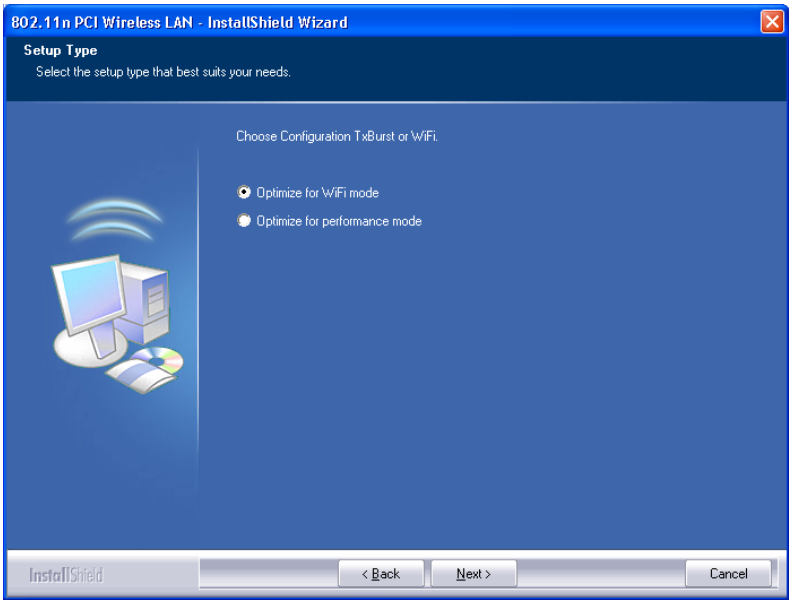
3. Select if you are going to configure your wireless network with this device or with Microsoft Zero Configuration tool.

   Note: This can be changed after installing this software.

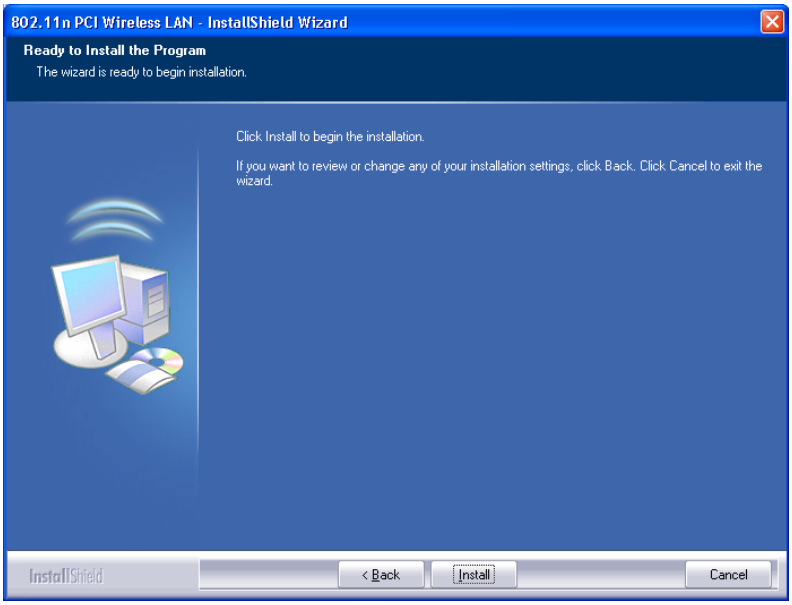


4. Select to optimize this adapter in WiFi mode or performance mode.

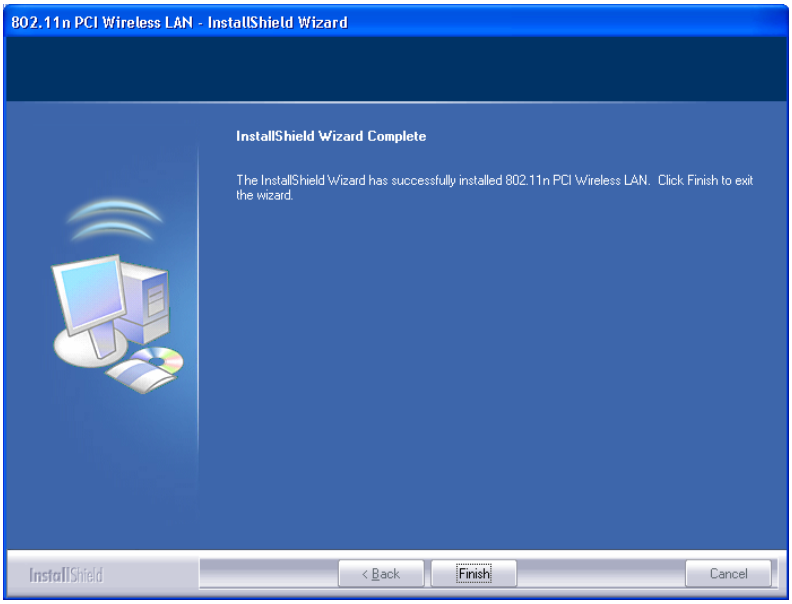
   Note: The performance mode is only valid while connecting to a TX burst supported AP. Users that uses the AP without TX Burst please select WiFi mode (standard mode).



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



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


802.11n PCI Wireless LAN - InstallShield Wizard
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed 802.11n PCI Wireless LAN. Click Finish to exit the wizard.
InstallShield
< Back
Finish
Cancel

Chapter 3 Management Guide

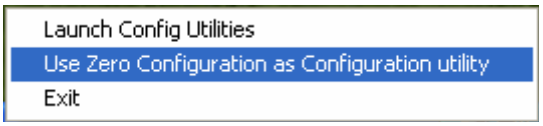
This chapter will help you understand the management interface of the device and how to manage the device.

3.1 Configures a Basic Network Connection

Selecting configuration tool

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

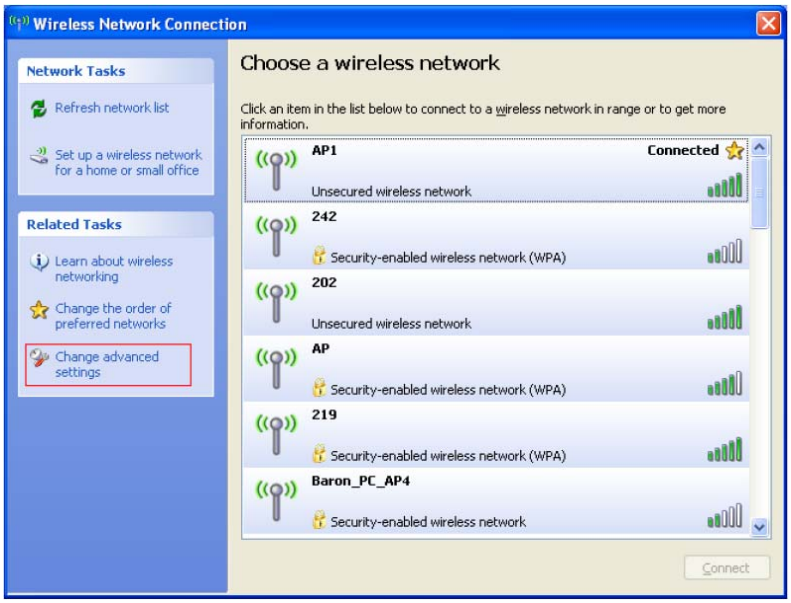
Note:
You could use either the software we provide or Microsoft Zero Configuration tool to configure this adapter. To switch between the two configuration tools, please right click on the  icon on system tray to select.



Connecting with Microsoft Zero Configuration

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.



Connect with Rosewill's 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.

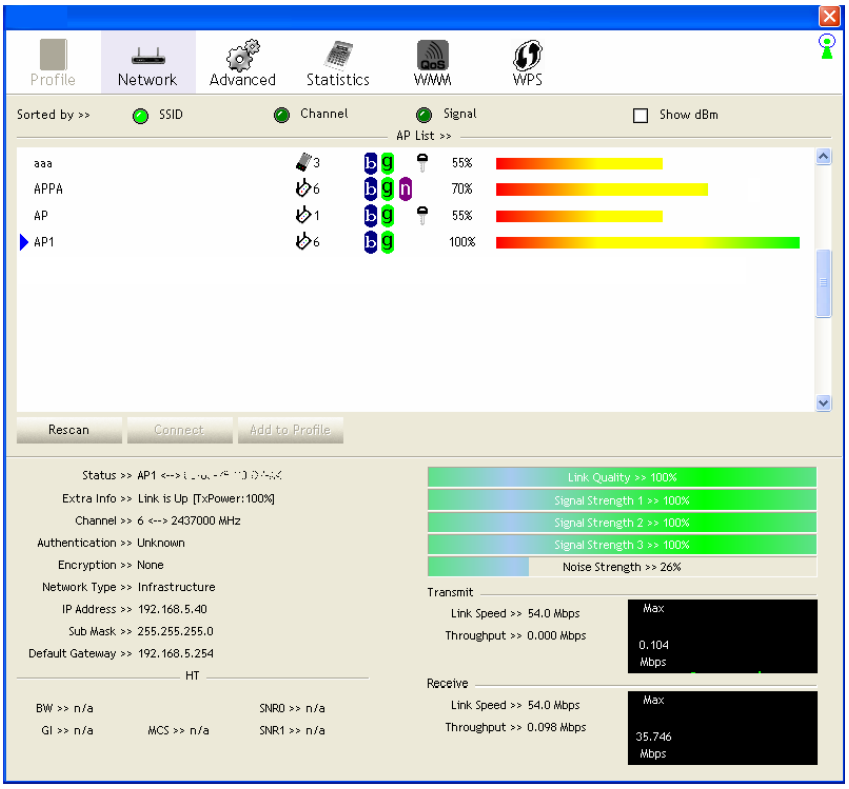
3.2 Introduction to the Wireless LAN Utility for Windows XP

3.2.1 Interfaces

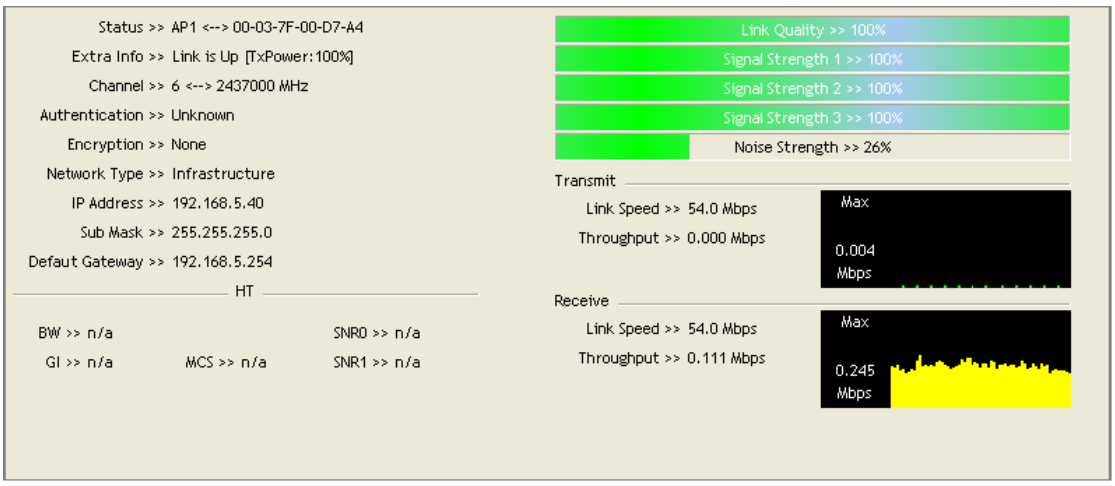
This Utility basically consisted of three parts:

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.



3.2.2 Status Information

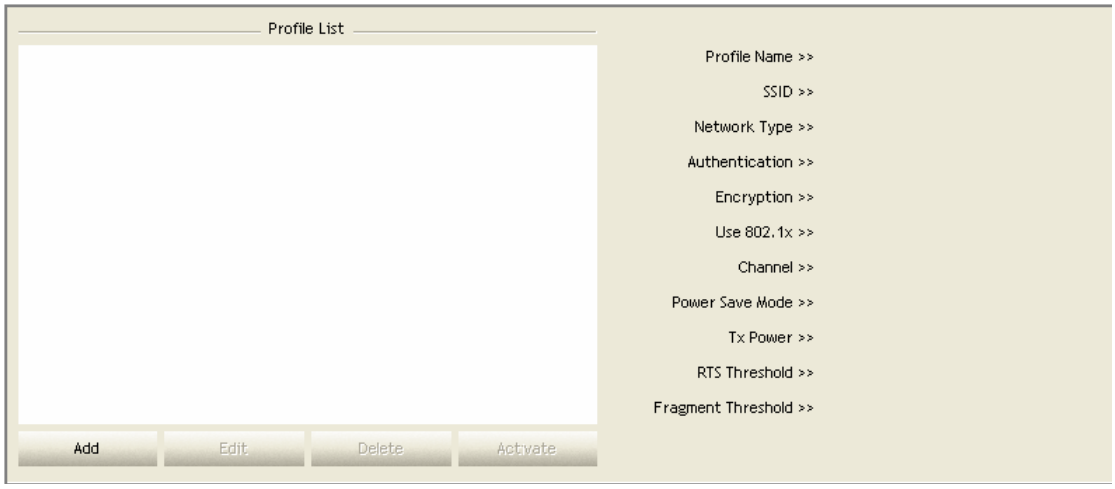


Status	Shows the connecting status. Also shows the SSID while connecting to a valid network.
Extra Info	Display link status in use
Channel	Display current channel in use
Authentication	Authentication mode in use.
Encryption	Encryption type in use.
Network Type	Network type in use

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.

3.2.3 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.

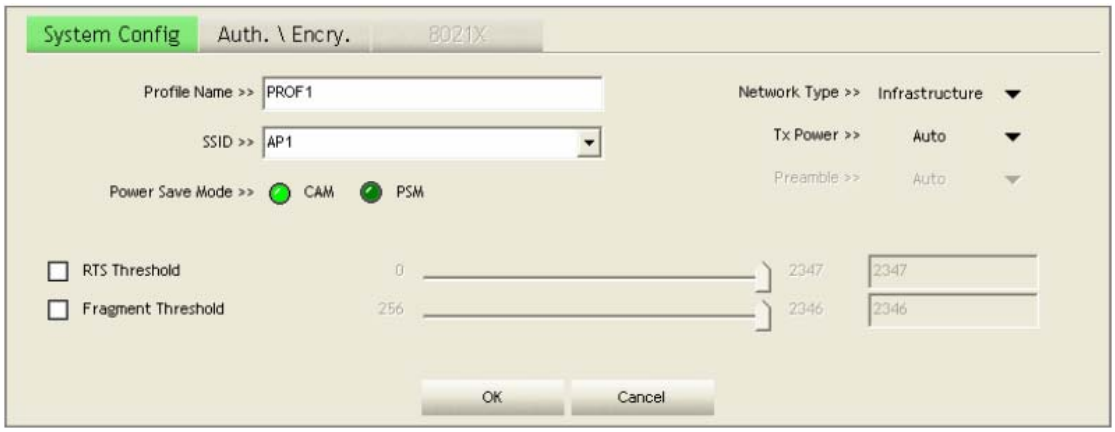


Adding a new profile

1. Click the **"Add"** button. The add profile window pops up.

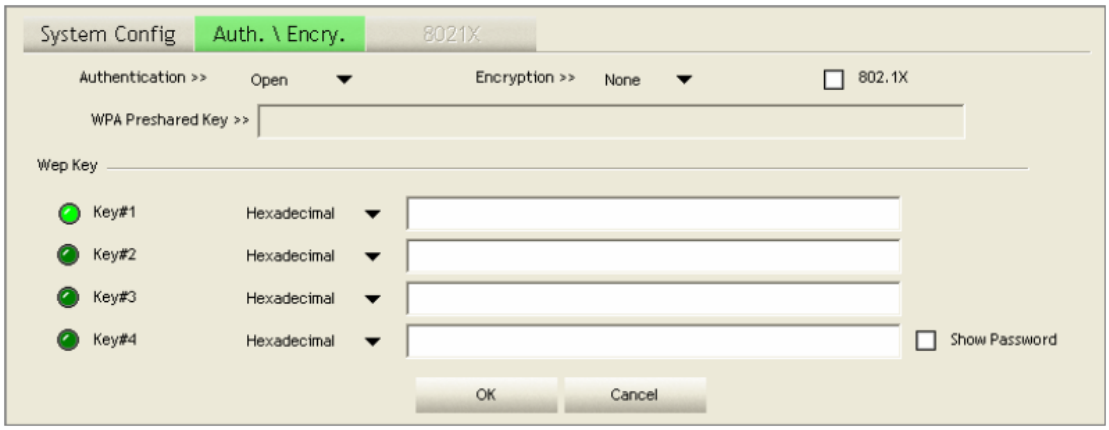
Note: you could also add a new profile quickly by selecting an available network in the "**Network**" function then press the **"Add to Profile"** button.

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.

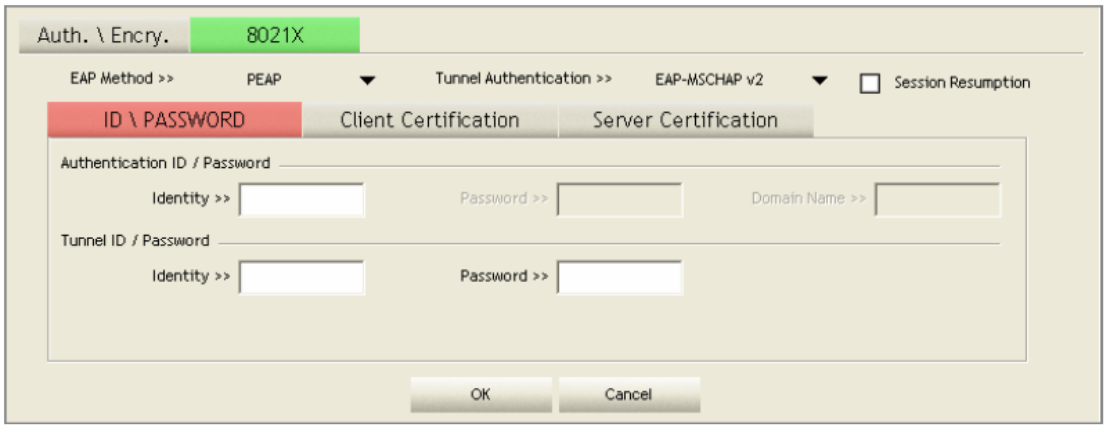
Users that don't use this function or connecting to an open-wireless network please skip this part.

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.

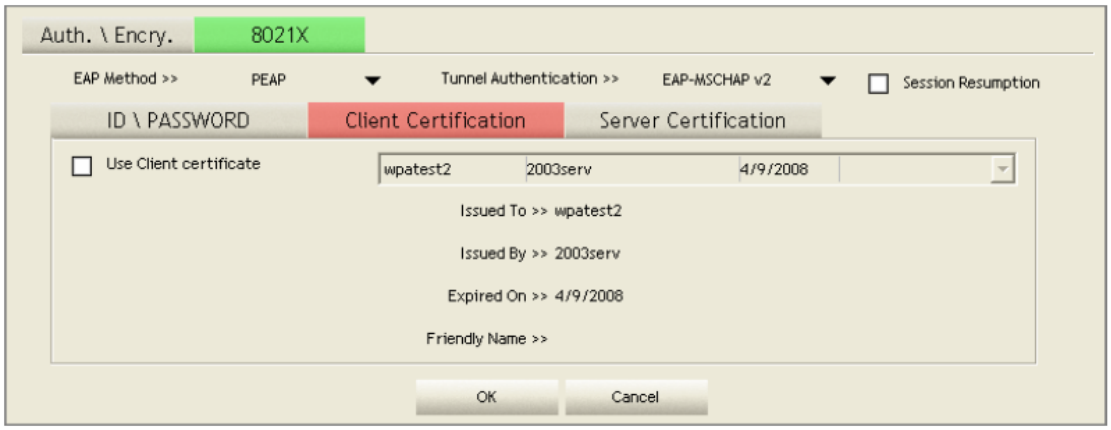
ID \ PASSWORD



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.

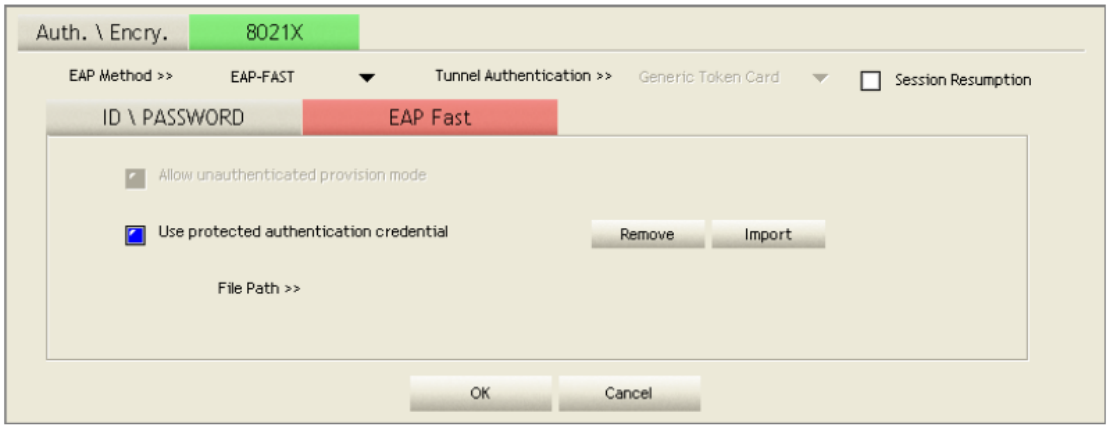
Tunnel ID / Password: Identity and Password for server.

Client Certification



Use Client certificate: Client certificate for server authentication.

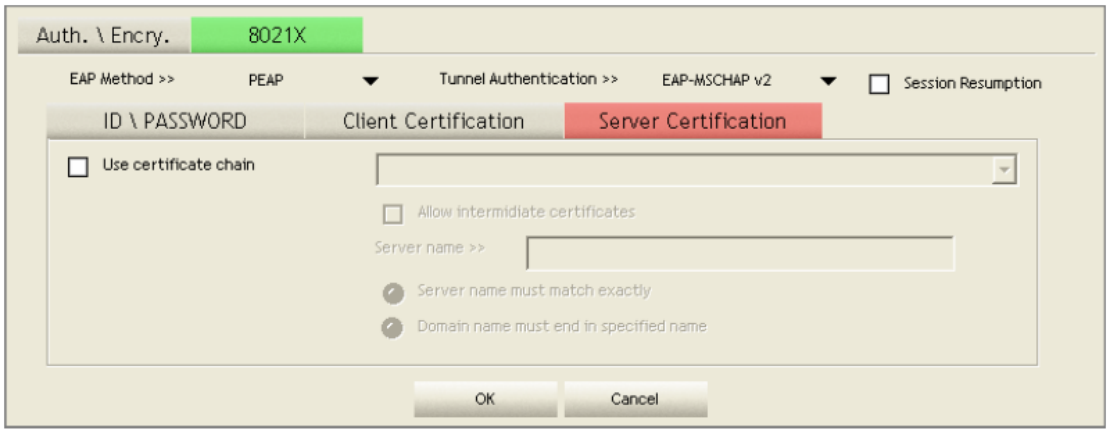
EAP Fast



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.

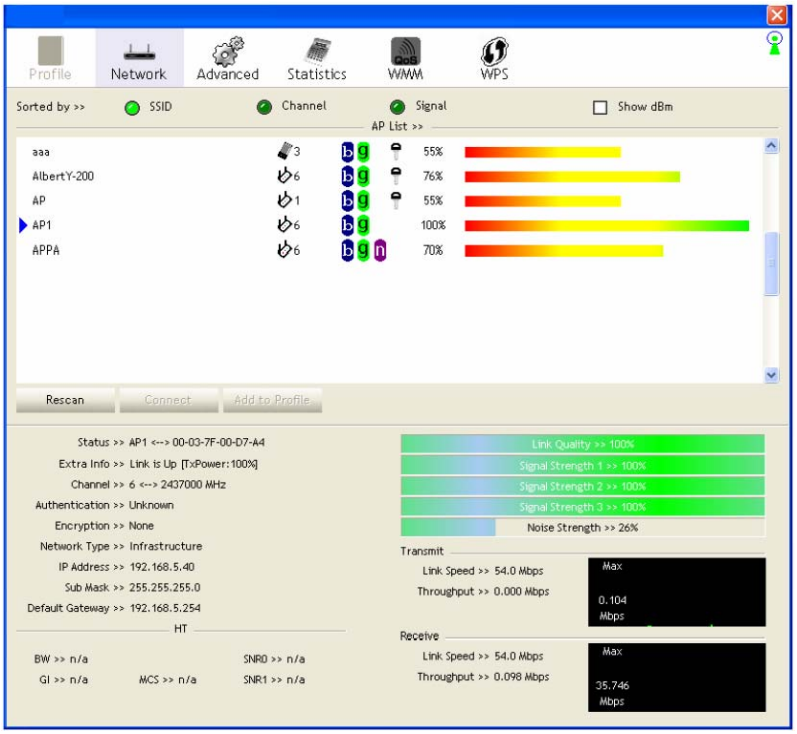
Allow intimidate certificates: Mark to allow intimidate certification.

Server name: Enter an authentication sever name.

3.2.4 Network

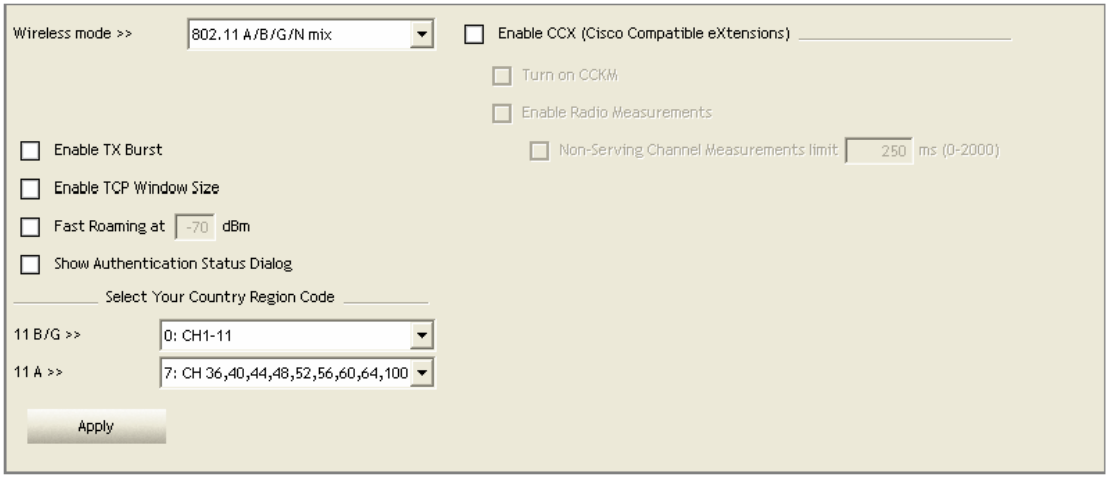
This network lists the available wireless networks. The utility connects to a wireless network with best signal strength automatically. You can change the connecting network by clicking on the network name and click the **"Connect"** button. To see detail information of each network, please double click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



3.2.5 Advanced

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

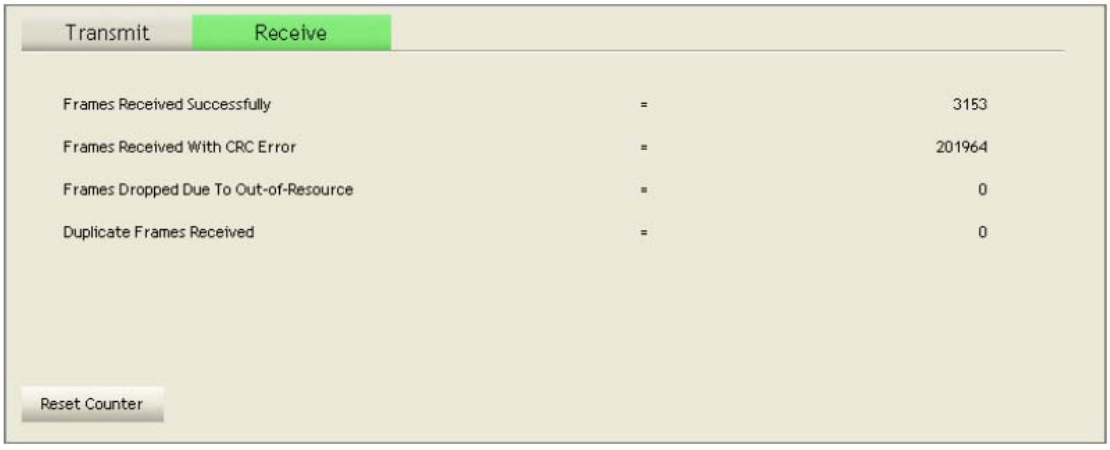


Wireless mode	Click the drop list to select a wireless mode.
Enable TX Burst	Select to enable connecting to a TX Burst supported device.
Enable TCP Window Size	Mark the checkbox to enable TCP window size, which help enhance throughput.
Fast Roaming at __ dBm	Mark the checkbox to enable fast roaming. 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.

3.2.6 Statistics

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.

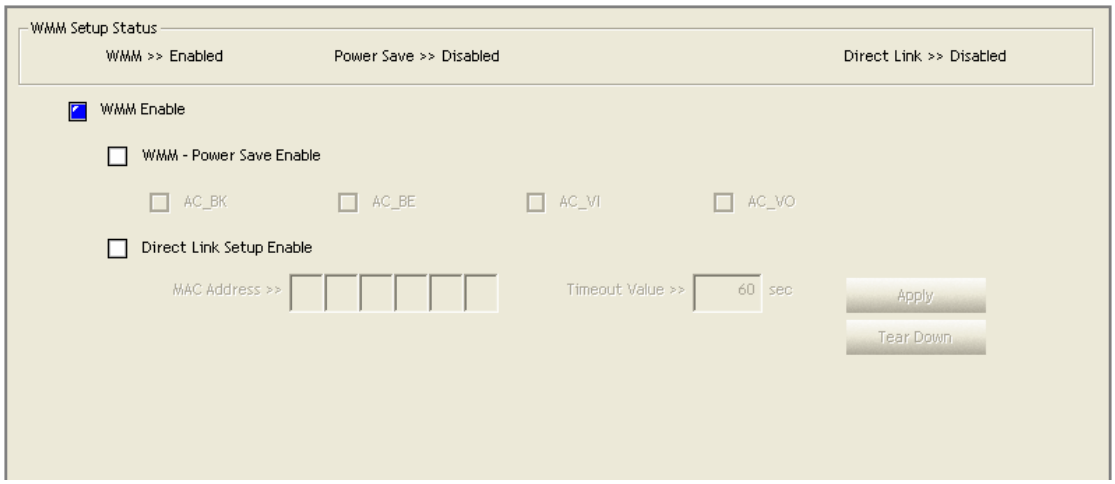
Frames Transmitted Successfully	Frames successfully sent.
Frames Retransmitted Successfully	Successfully retransmitted frames numbers
Frames Fail To Receive ACK After All Retries	Frames failed transmit after hitting retry limit
RTS Frames Successfully Receive CTS	Successfully receive CTS after sending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



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.

3.2.7 WMM

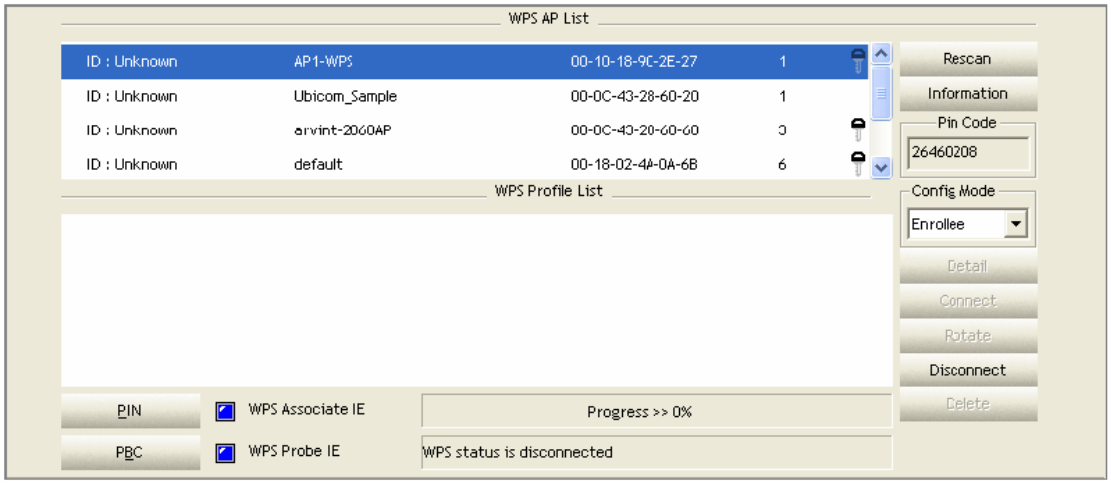
This page allows users to activate the WMM function for this device. Please note that this function only works while connecting to a WMM compatible device.



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.

3.2.8 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 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

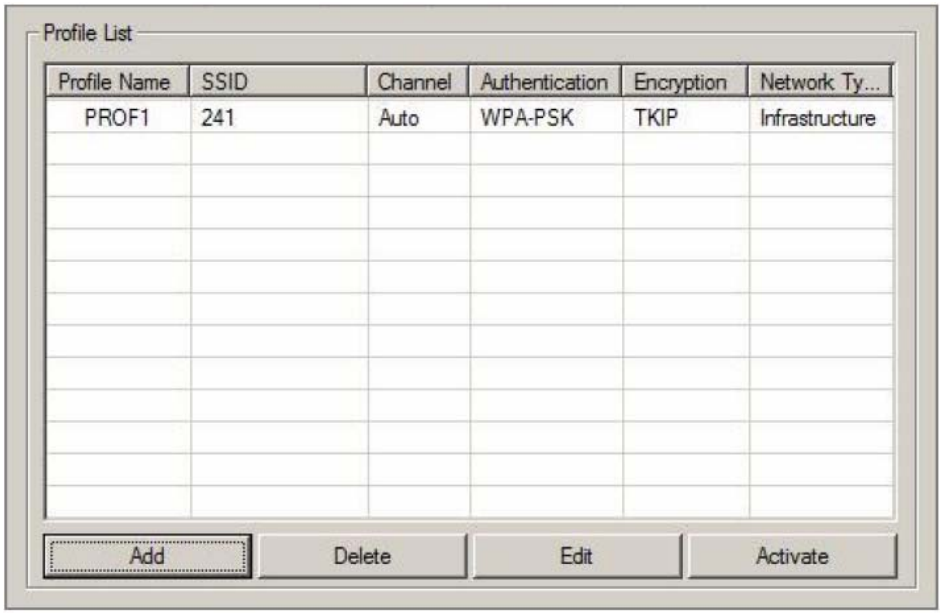
Note: When you click PIN or PBC, please don't do any rescan within two-minute connection. If you want to abort this setup within the interval, restart PIN/PBC or press Disconnect to stop WPS action.

3.3 Introduction to the configuration utility for Windows Vista™

This utility also helps Windows Vista™ users to configure the wireless network. Please refer to the following sections for introduction.

3.3.1 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 environment quickly.

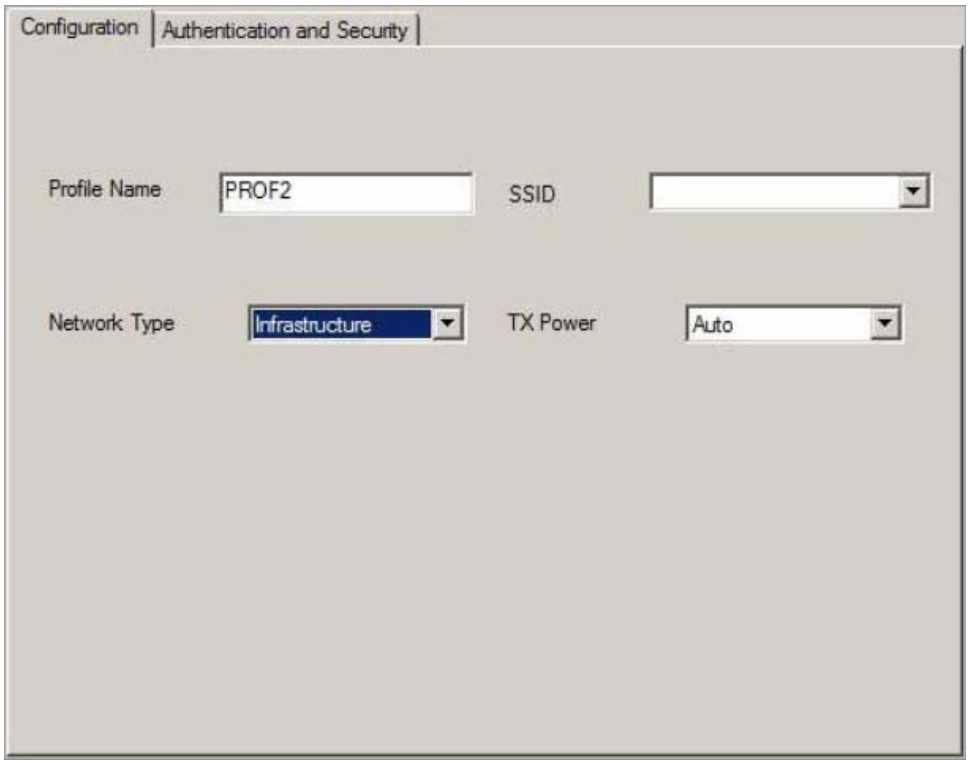


To add a new profile for Vista:

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 “**Site Survey**” function then press the **“Add to Profile”** button.

2. Fill in the information of this wireless network and its relative security settings. Please note that the information should be corresponding to the wireless network you are connecting to.



Deleting profile:

Click the "Delete" button to delete the selected profile.

Editing profile:

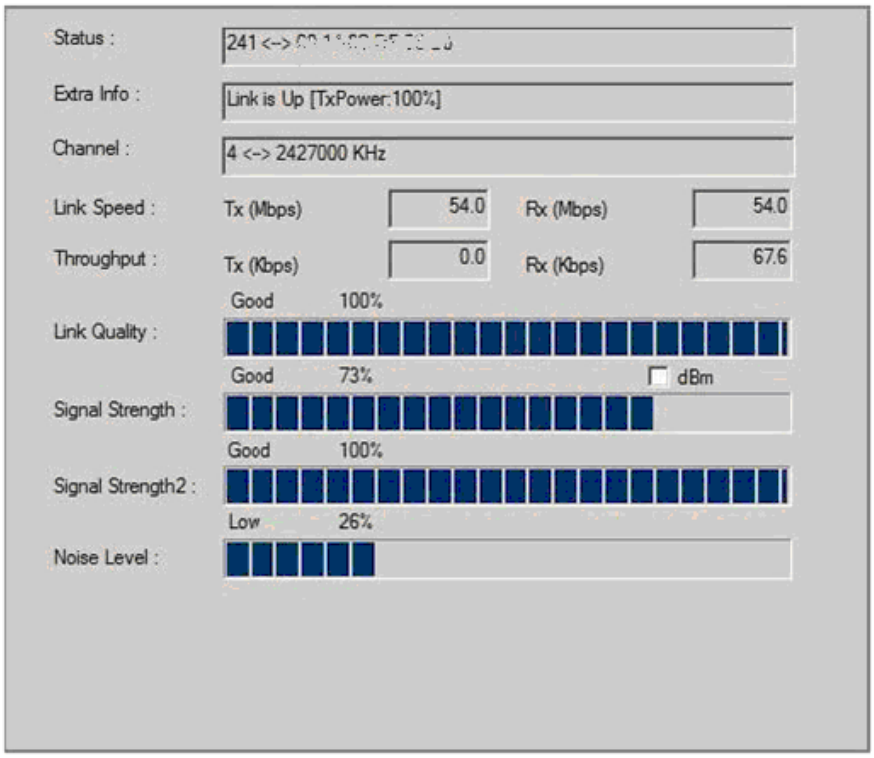
Click the "**Edit**" button to pop up the profile-setting page for users to edit the existing profile.

Activating profile:

Click the "**Activate**" button to activate the selected profile.

3.3.2 Link Status

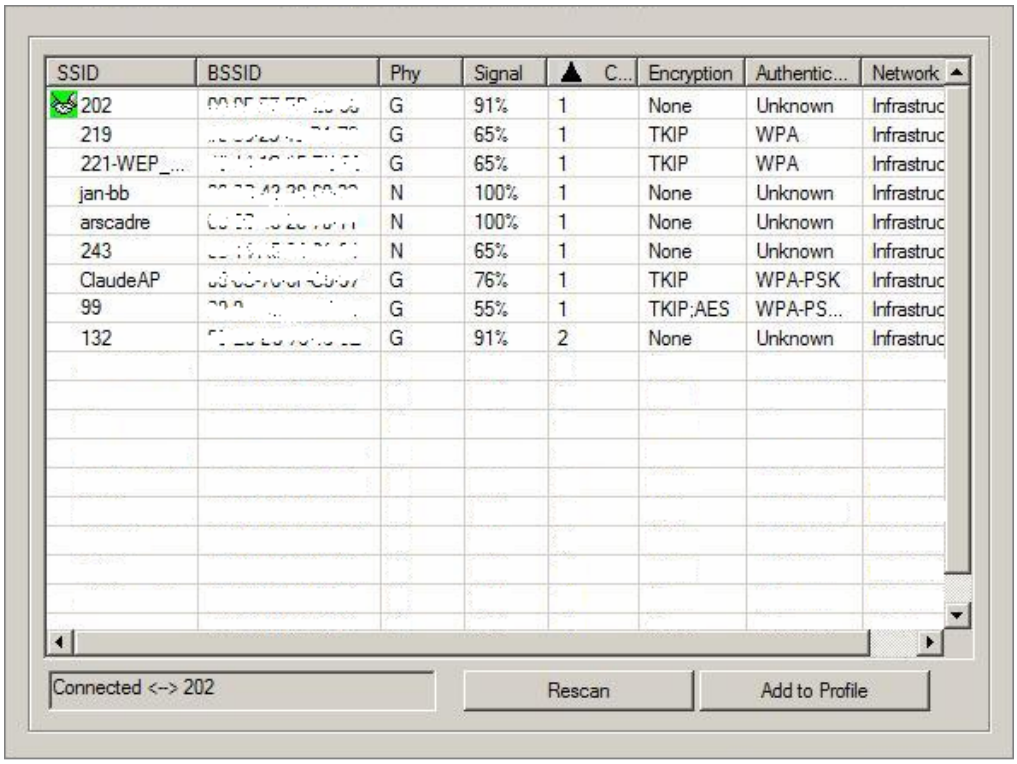
This Link status shows the information about the connecting. Please refer to the following chart for definition.



Status	Display current connection status.
Extra Info	Display link status and current channel in use.
Link Speed	Display current transmitting and receiving rates
Throughput	Display transmitting and receiving throughputs.
Link Quality	Display connecting quality based on signal strength and TX/RX packet error rate.
Signal Strength	Display receiving signal strength either in percentage or dBm format
Noise Level	Display noise signal strength.

3.3.3 Site Survey

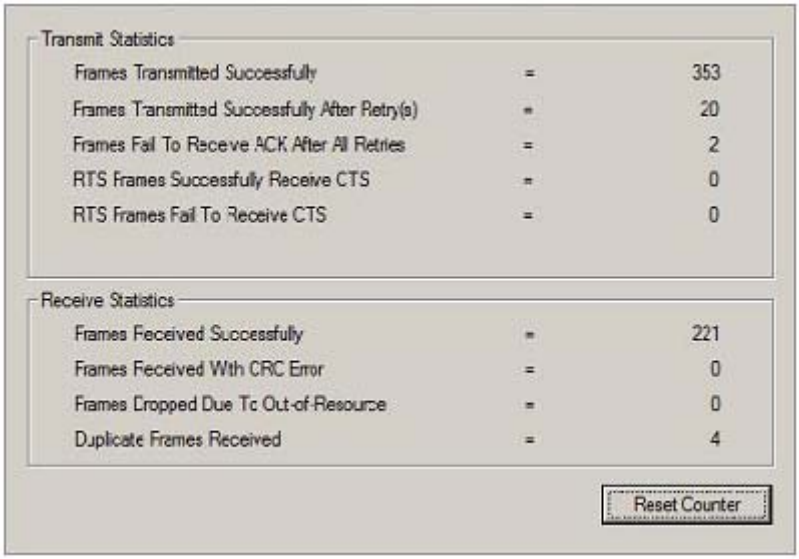
This page shows the available wireless networks within the coverage of this network adapter. You could check the status of wireless network around your computer or add a network into your profile.



SSID	Name of the network.
BSSID	AP MAC address or random numbers generated for IBSS
Phy Type	Phy Type of the network
Signal	Signal strength of the network
Channel	The channel in use
Encryption	Encryption algorithm. The supported algorithms are WEP, TKIP, AES, and Not Use.
Authentication	Authentication mode. The supported modes are Unknown, WPA-PSK, WPA2-PSK, WPA and WPA2.
Network Type	Infrastructure or Ad-Hoc
Rescan	Click the rescan button to perform re-scanning.
Add to profile	Select a network then push the add-to-profile button to bring up the profile-setting to add a wireless network profile.

3.3.4 Statistic

This page provides the statistics about the connection of this adapter.



Frames Transmitted Successfully	Frames sent successfully
Frames Transmitted Successfully After Retry	Frames sent successfully with retry
Frames Fail To Receive ACK After All Retries	Frames transmitted failed after hitting the retrying limit
RTS Frames Successfully Receive CTS	CTS frames received successfully after sending RTS frames
RTS Frames Fail To Receive CTS	The missing CTS frames after sending RTS frames
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 insufficient resource
Duplicate Frames Received	Duplicate frames received

WPS Configuration

This page provides users to connect this adapter to a WPS (Wi-Fi Protected Setup) AP. Those available WPS supported AP are listed on the upper column. Select the AP that you want to connect to and click the **"Connect"** button to activate.

WPS Associate IE:

If the "WPS Associate IE" option is checked, station sends a association request with WPS IE during WPS setup.

WPS Configuration

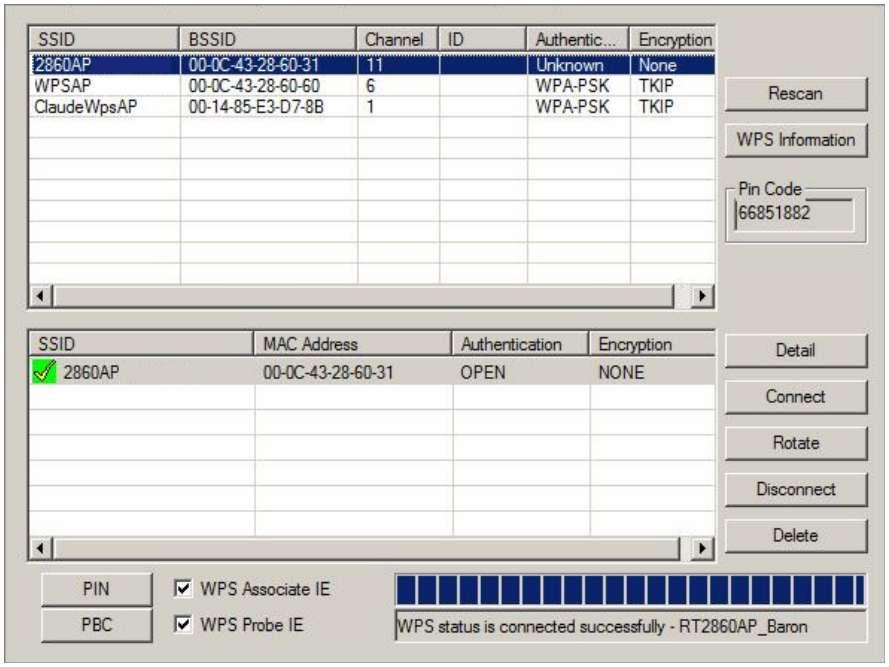
This page provides users to connect this adapter to a WPS (Wi-Fi Protected Setup) AP. Those available WPS supported AP are listed on the upper column. Select the AP that you want to connect to and click the "**Connect**" button to activate.

WPS Associate IE:

If the "WPS Associate IE" option is checked, station sends a association request with WPS IE during WPS setup.

WPS Probe IE:

If the "WPS Probe IE" option is checked, station probes a request with WPS IE during WPS setup.



Re-scanning:

Click the **"rescan"** button to perform the re-scanning.

WPS AP Information:

Click the "**WPS information**" button to bring up the WPS capable AP information dialog window. The window shows the information including:

Authentication Type:

There are three types of supported authentication modes including Open, Shared, WPA-PSK and WPA modes.

Encryption Type:

For Open and Shared authentication modes, the available encryption types are None

and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication modes, the available encryption types are TKIP and AES.

Config Methods:

This attribute contains the config methods supported and enabled by the selected Registrar.

Device Password ID:

Device Password ID indicates the method or identifies the specific password that the selected Registrar intends to use.

Selected Registrar:

Selected Registrar indicates if the user has recently activated a Registrar to add an Enrollee.

State:

This attribute is used to indicate the current configuration state. This attribute is either "Un-configured" or "Configured".

Version:

This attribute is the specified WPS version.

AP Setup Locked:

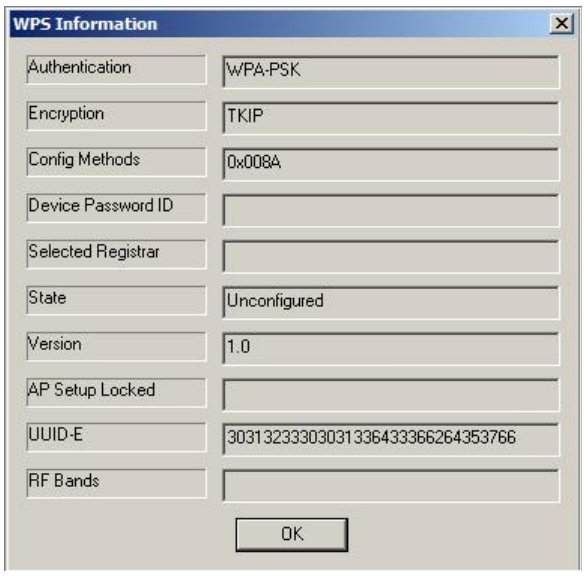
AP Setup Locked indicates if AP has entered a setup locked state.

UUID-E:

UUID-E is universally unique identifier (UUID) generated by the Enrollee.

RF Bands:

RF Bands indicate the available RF bands.



Configure WPS profiles:

The user can configure WPS profiles with either PIN method or PBC method.

PIN Method:

Step 1: The Registrar enters the pin code generated by station.

Step 2: Push the "PIN" button.

PBC Method:

Push the "PBC" button within 2 second while the Registrar pushes the button.

Manage WPS profiles:

The received WPS profiles are listed in the lower frame, and the listed WPS profile attributes are SSID, MAC address, authentication type, and encryption type.

WPS profile detail information:

Selecting a profile then pushing the "Detail" button brings up the WPS profile.

This profile shows information including:

Connect with WPS profile:

Clicking the "Connect" button will connect to the AP with the selected WPS profile.

Rotate WPS profiles:

If there are more than two WPS profiles, clicking the "Rotate" button will rotate to next profile and connect to AP with this profile. If the connection can't be established successfully, station will perform the WPS profile rotation repeatedly.

Disconnect from WPS AP:

Click the "Disconnect" button to stop the WPS connection.

Delete WPS profile:

Click the "Delete" button to delete the selected WPS profile.

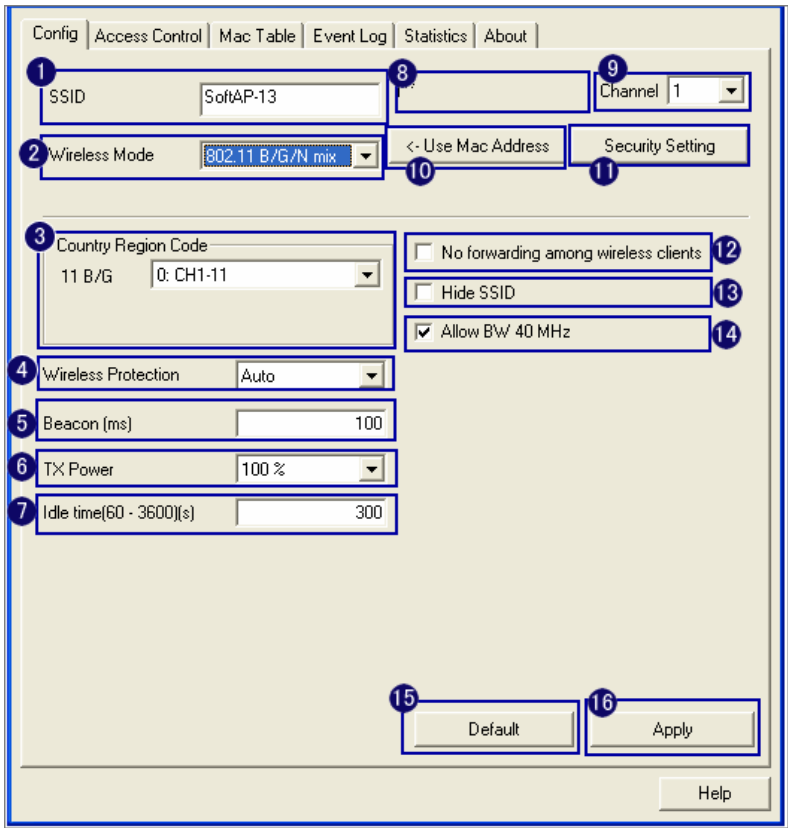
Chapter 4 AP mode management guide

This adapter can be configured as AP mode. In order to set 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.

4.1 Configuration

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.

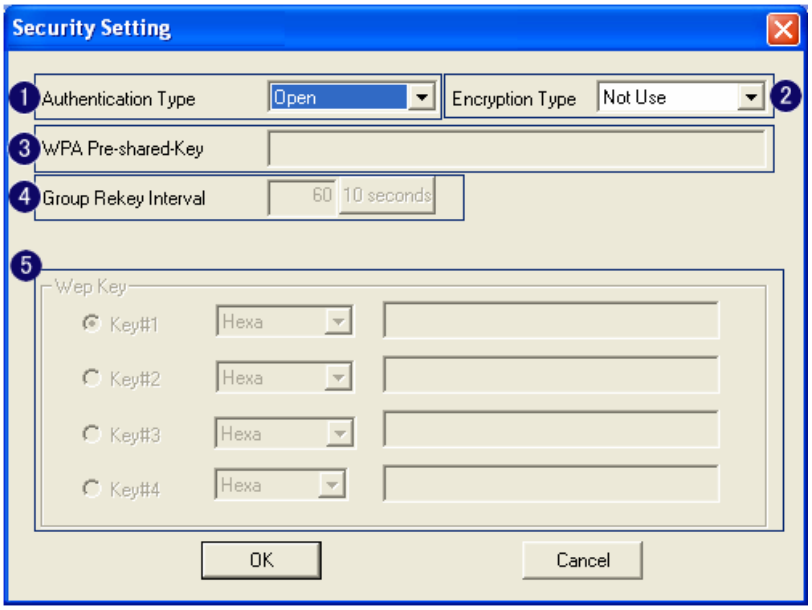
14. Allow BW40 MHz: Allow BW40 MHz capability.

15. Default: Use system default value.

16. Apply: Apply the above changes.

4.2 Security Setting

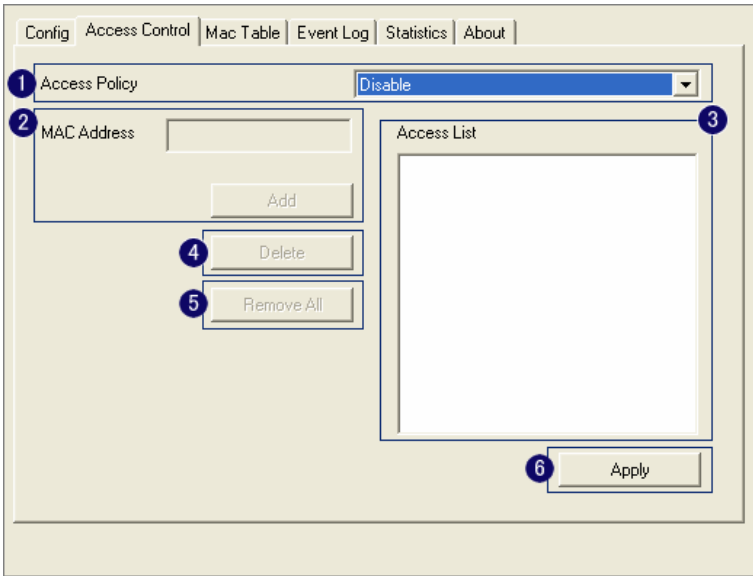
This page pops up after clicking the Security Settings button. Please follow the instructions below:



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.

4.3 Access Control

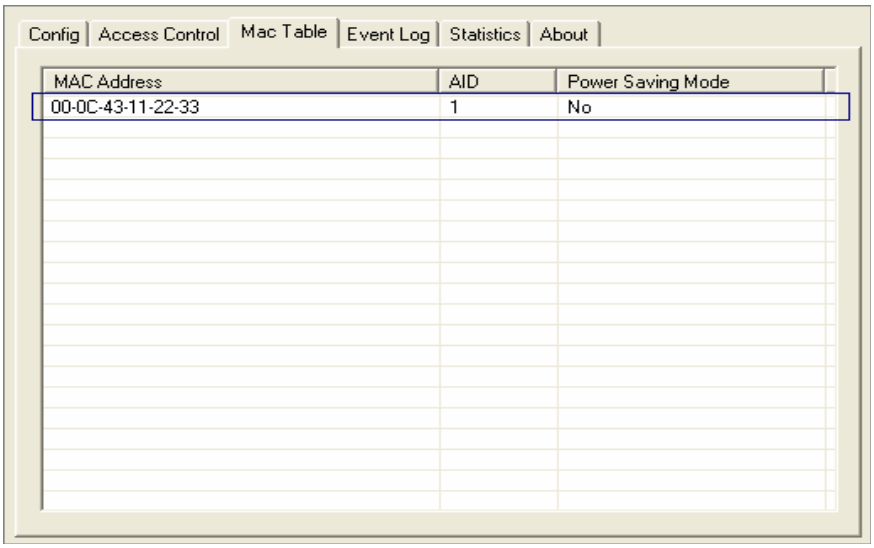
This function filters users to use this device by designating MAC address. Please refer to the following chart for introduction.



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.

4.4 MAC Table

This page displays the station detail information of current connection.

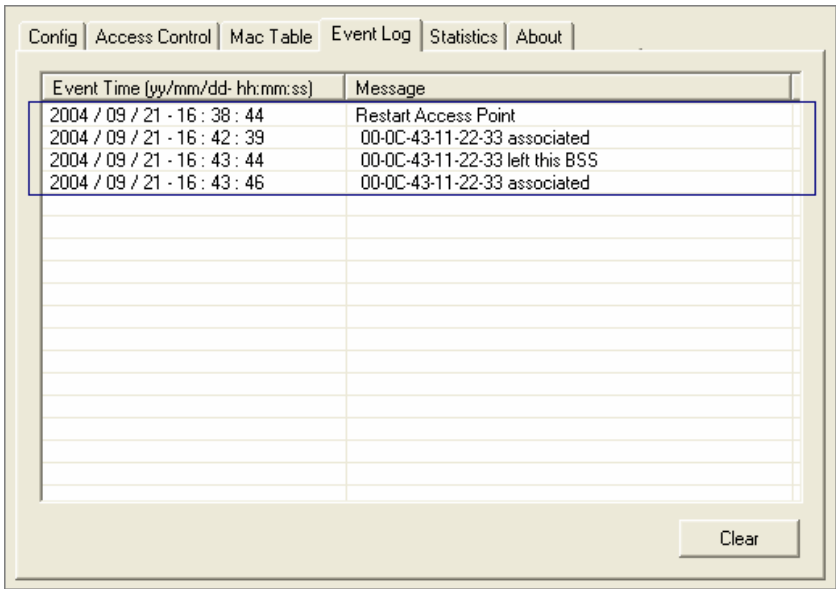


MAC Address	The station MAC address of current connection.
AID	Raise value by current connection.

Power Saving Mode Check if the connected station supports power saving.

4.5 Event Log

Record Soft AP all event time and message.

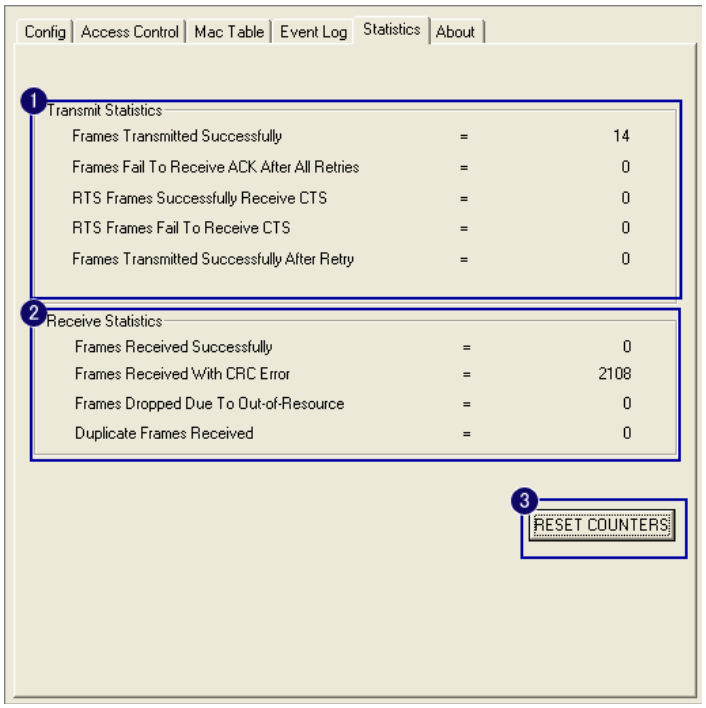


Event Time (yy/mm/dd-hh:mm:ss) Record event time.

Message All event messages.

4.6 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 Receive CTS	Counts of CTS that fail to be received after sending RTS 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.

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.