

IEEE 802.11n Wireless Series

**Long-Range USB Adapter**

# User Manual

Version: 2.0

Date: January 13, 2009

# FCC Certifications

## **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.

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.

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.

## **IMPORTANT NOTE:**

### **FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## CE Mark Warning



This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 Class B for ITE, the essential protection requirement of Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

### **Trademarks:**

All trade names and trademarks are the properties of their respective companies.

Copyright © 2009, All Rights Reserved.

# TABLE OF CONTENTS

OVERVIEW .....	1
UNPACKING INFORMATION .....	1
INTRODUCTION TO THE IEEE 802.11N WIRELESS USB ADAPTER .....	1
KEY FEATURES .....	2
INSTALLATION GUIDE .....	2
SOFTWARE INSTALLATION .....	2
MANAGEMENT GUIDE.....	5
<b>MAKING A BASIC NETWORK CONNECTION</b> .....	5
Select a configuration tool .....	5
To connect with Microsoft Zero Configuration tool.....	5
To connect with 802.11n Wireless LAN Utility .....	7
<b>INTRODUCTION TO THE 802.11N WIRELESS LAN UTILITY</b> .....	8
Interfaces.....	8
Link Status Information .....	9
Profile .....	10
Network .....	19
Advanced.....	20
Statistics .....	21
WMM .....	22
WPS .....	24
CCX.....	35
Radio On/Off.....	35
<b>AP MODE MANAGEMENT GUIDE FOR WINDOWS 2000/XP/VISTA</b> .....	36
Config .....	38
Security Setting .....	40
Access Control .....	41
MAC Table.....	42
Event Log .....	43
Statistics .....	44

# Overview

Thank you for purchasing this product. Read this chapter to know about your IEEE 802.11n Wireless USB Adapter.

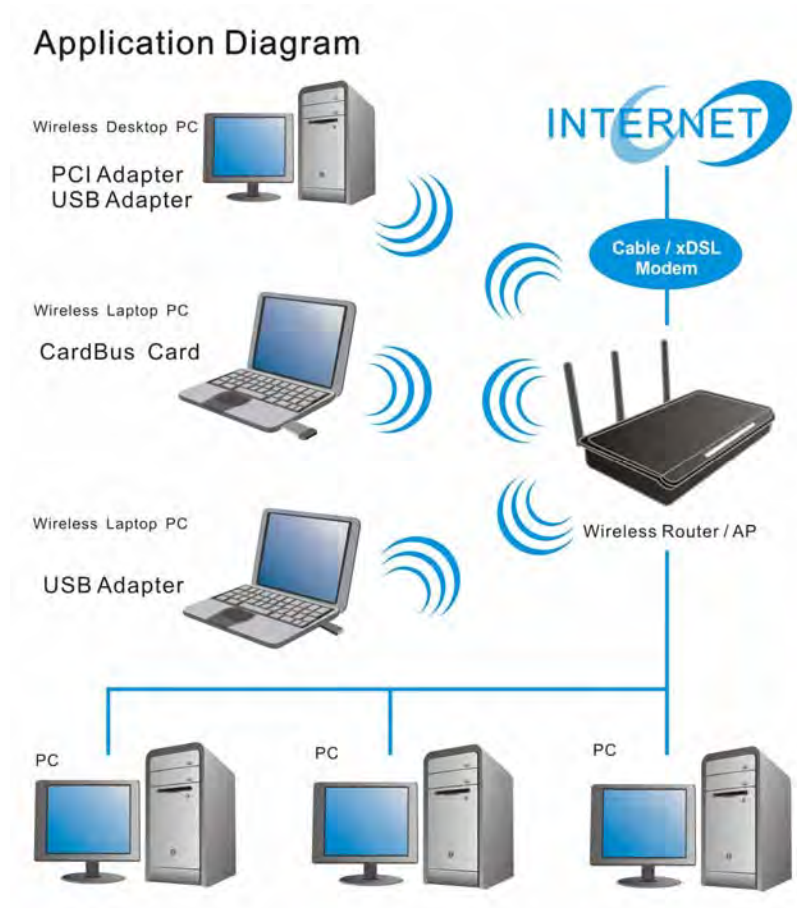
## Unpacking Information

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

1. IEEE 802.11n Wireless USB Adapter.
2. One Utility/ Manual CD.

## Introduction to the IEEE 802.11n Wireless USB Adapter

The IEEE 802.11n Wireless USB adapter provides users to launch IEEE 802.11n wireless network at 150 Mbps in the 2.4GHz (AWUS036NH/AWUS036NEH) or 2.4GHz&5.2GHz&5.8GHz (AWUS051NH) band, which is also compatible with IEEE 802.11b/g and IEEE 802.11a/b/g wireless devices at 11/54 Mbps. You can configure this adapter with ad-hoc mode to connect to other 2.4GHz (AWUS036NH/AWUS036NEH) or 2.4GHz&5.2GHz&5.8GHz (AWUS051NH) 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 wireless standards
- Supports wireless data encryption with 64/128-bit WEP, WPA, WPA2, TKIP, AES
- 2.4GHz (AWUS036NH / AWUS036NEH) frequency band, MIMO
- Supports QoS: WMM, WMM-PS
- 2.4GHz&5.2GHz&5.8GHz (AWUS051NH) frequency band, MIMO
- Complies with USB 2.0
- Supports multiple BSSID
- High speed transfer data rate up to 150 Mbps
- Supports driver for Windows 2000, XP 32/64, Vista 32/64, Windows 7, Linux (2.4.x/2.6.x), and Mac (10.3.x/10.4.x/10.5.x/10.6.x) Power PC & PC
- Supports auto-installation

## Installation Guide

### Software Installation

**Note:**

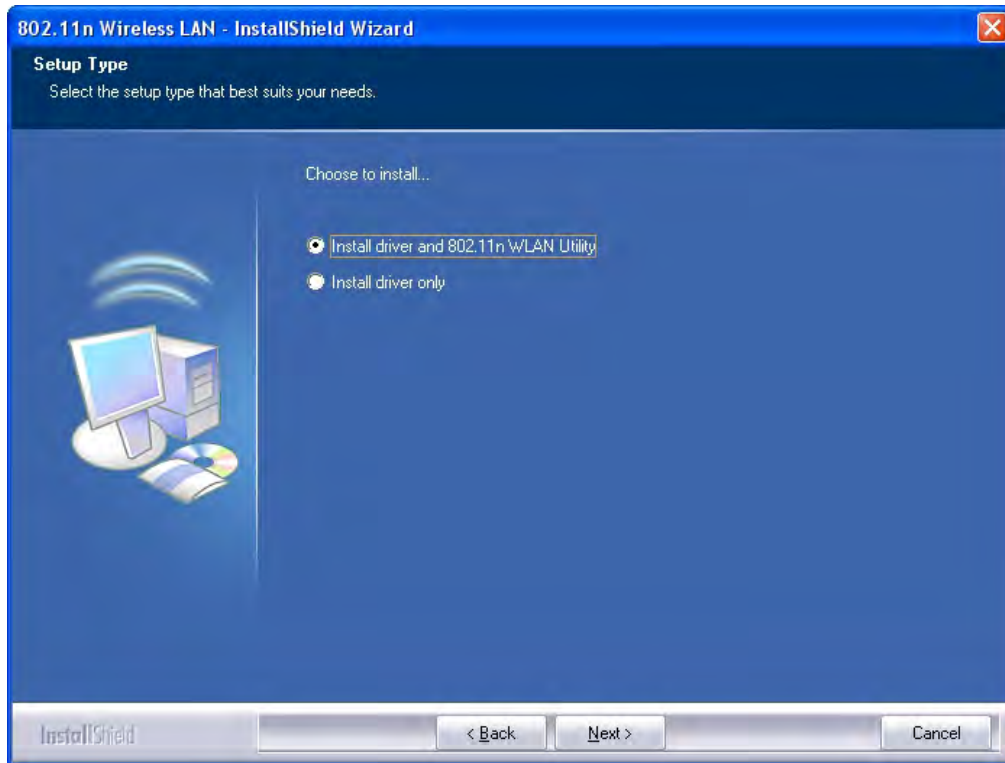
- For Linux or Mac driver installation guide, please refer to the instruction in [/Driver/Linux/README](#) or [/Driver/Mac/README](#) in the CD-Rom.
  - The following driver installation guide uses Windows XP as the presumed operation system. The procedures and screens in Windows 2000 and Vista are familiar with Windows XP.
1. 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** button of this product.

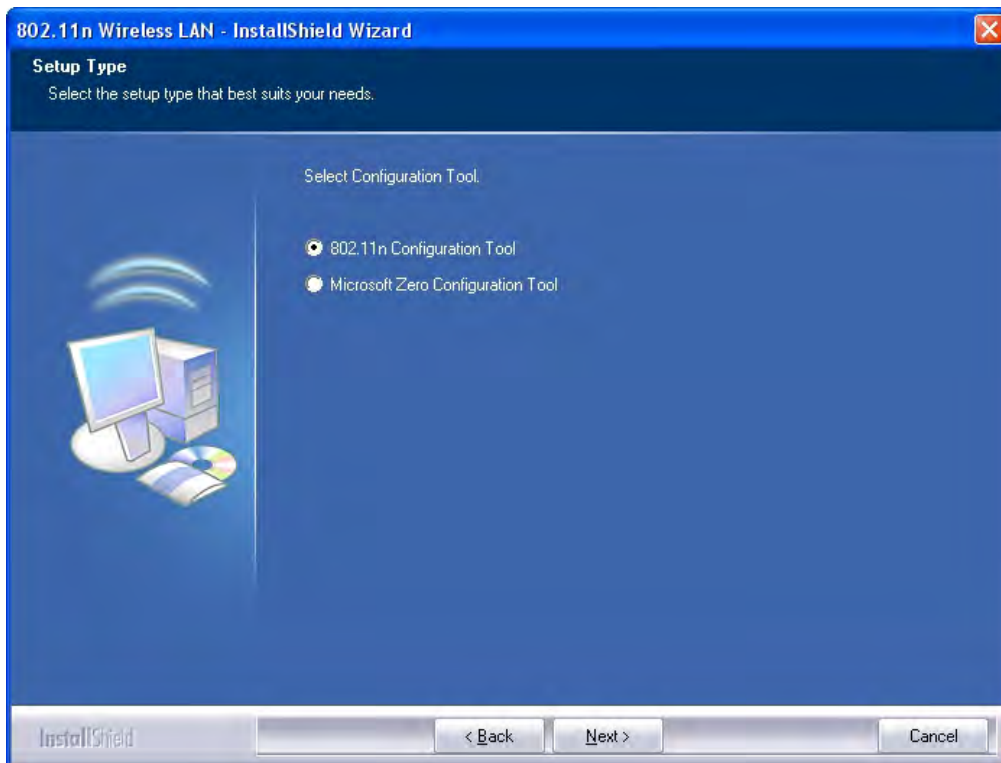
**Note:** If the CD-Rom fails to auto-run, please click on **My Computer > your CD-Rom drive > (folder of this product) > Driver** then double-click the **Setup** icon to start this menu.

3. Select if you are going to install the driver and wireless utility; or install the driver only.

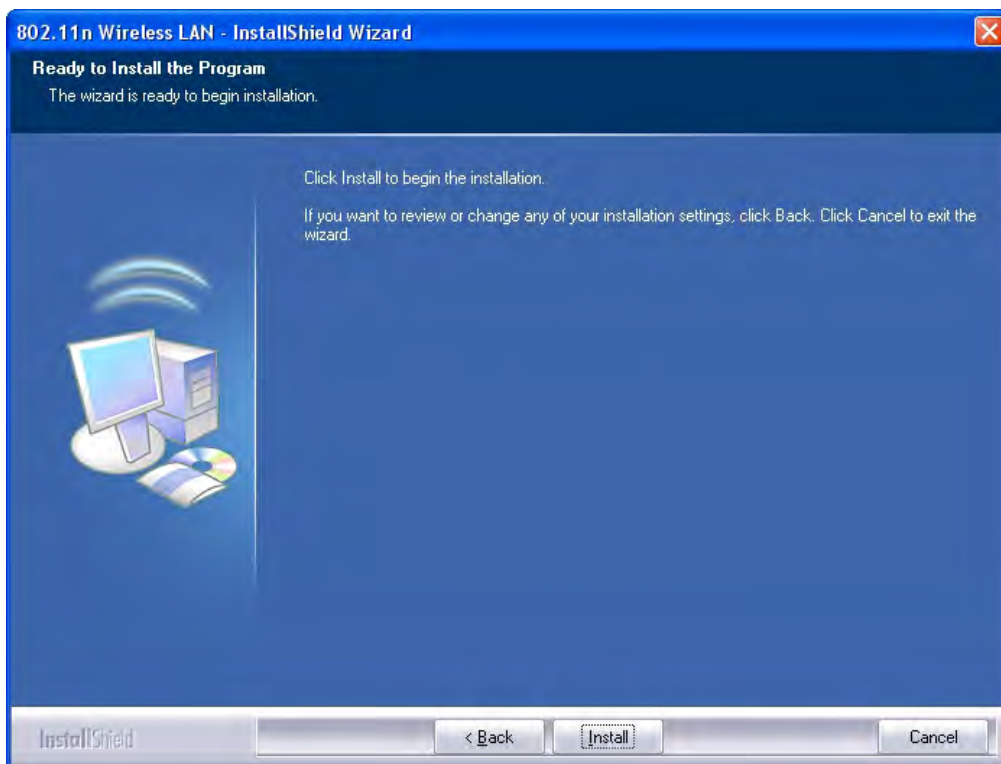


4. Select if you are going to configure your wireless network with this device or with Microsoft Zero Configuration tool.

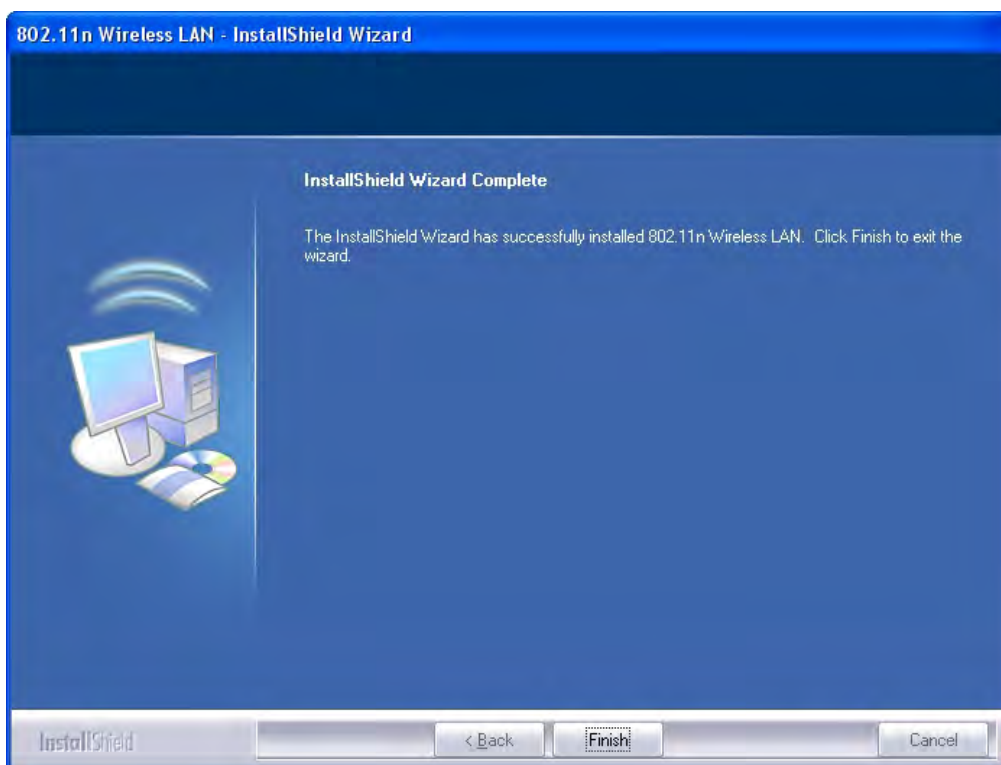
**Note:** This can be changed after installing this software.



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



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






# Management Guide

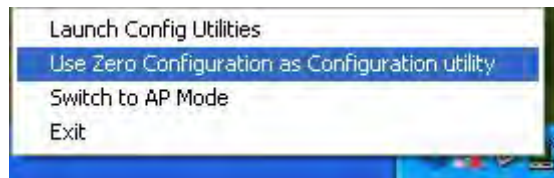
Read this chapter to understand the management interface of the device and how to manage the device.

## Making a Basic Network Connection


### 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.

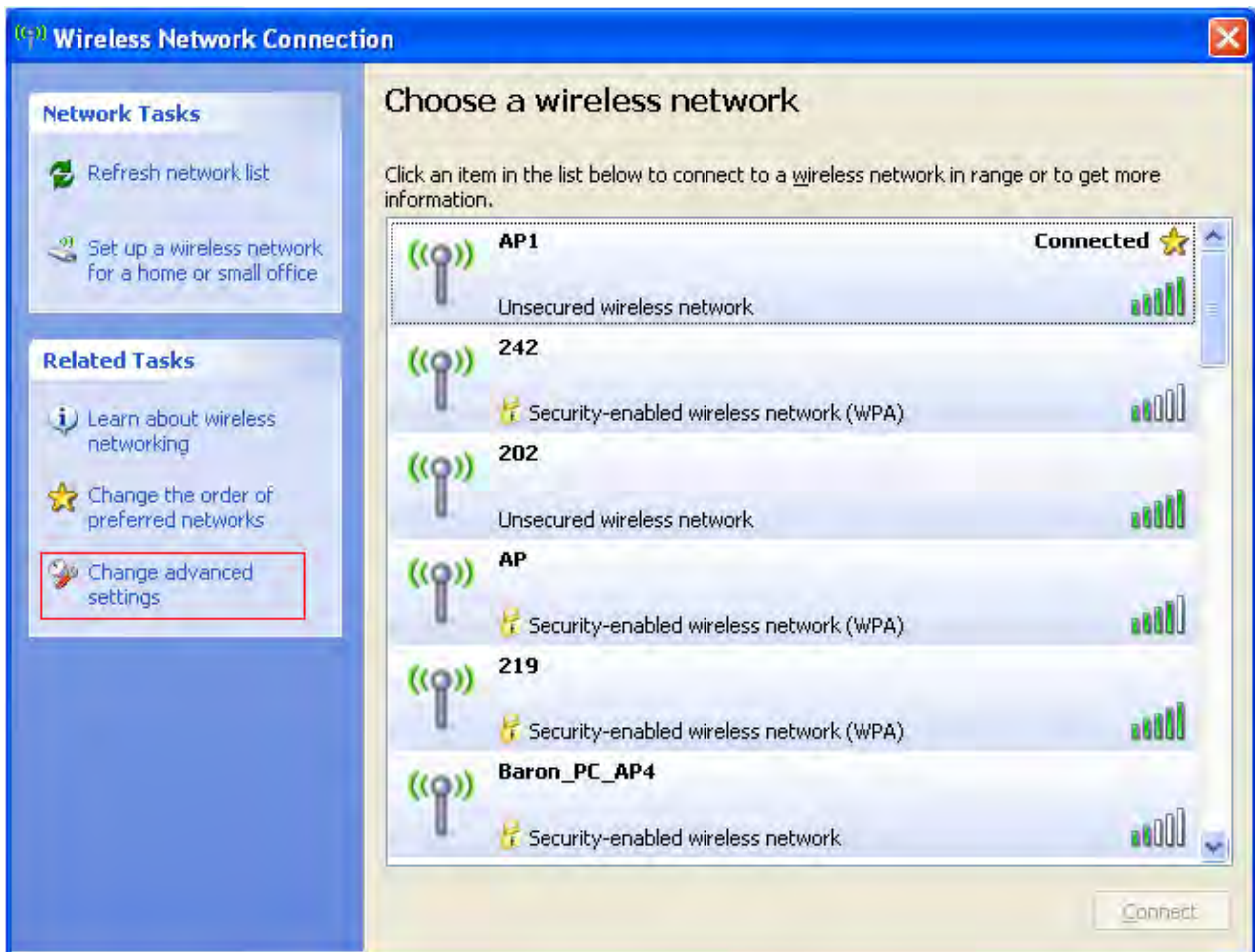


### To connect with Microsoft Zero Configuration tool


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.



## 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 and with no security setting. Right click on the  icon in the system tray and select **Launch Config utilities** if the Utility does not start. Please refer to the following chapters to get information regarding to the functions of this Utility.



The screenshot displays the 'Station Model' utility window. The top menu bar includes Profile, Network, Advanced, Statistics, WMM, WPS, Radio on/off, and About. Below the menu, there are sorting options for SSID, Channel, and Signal, along with a 'Show dBm' checkbox. The main area shows a list of available wireless networks:

SSID	Channel	Signal
MIS-6F-AP	1	31%
Wireless_11n_Router	6	52%

Buttons for 'Rescan', 'Add to Profile', and 'Connect' are located below the list. The bottom section provides detailed status and configuration for the selected 'Wireless\_11n\_Router' network:

- Status >> Wireless\_11n\_Router <=> 00-c0-ca-E2-DB-00
- Extra Info >> Link is Up [TxPower:100%]
- Channel >> 6 <=> 2437 MHz; central channel : 8
- Authentication >> Open
- Encryption >> NONE
- Network Type >> Infrastructure
- IP Address >> 0.0.0.0
- Sub Mask >> 0.0.0.0
- Default Gateway >>

Performance metrics are shown with progress bars:

- Link Quality >> 90%
- Signal Strength >> 57%
- Noise Strength >> 26%

Transmit and Receive statistics are also provided:

Category	Link Speed	Throughput
Transmit	1.0 Mbps	5,536 Kbps
Receive	90.0 Mbps	49,296 Kbps

Additional HT (High Throughput) parameters are listed at the bottom:

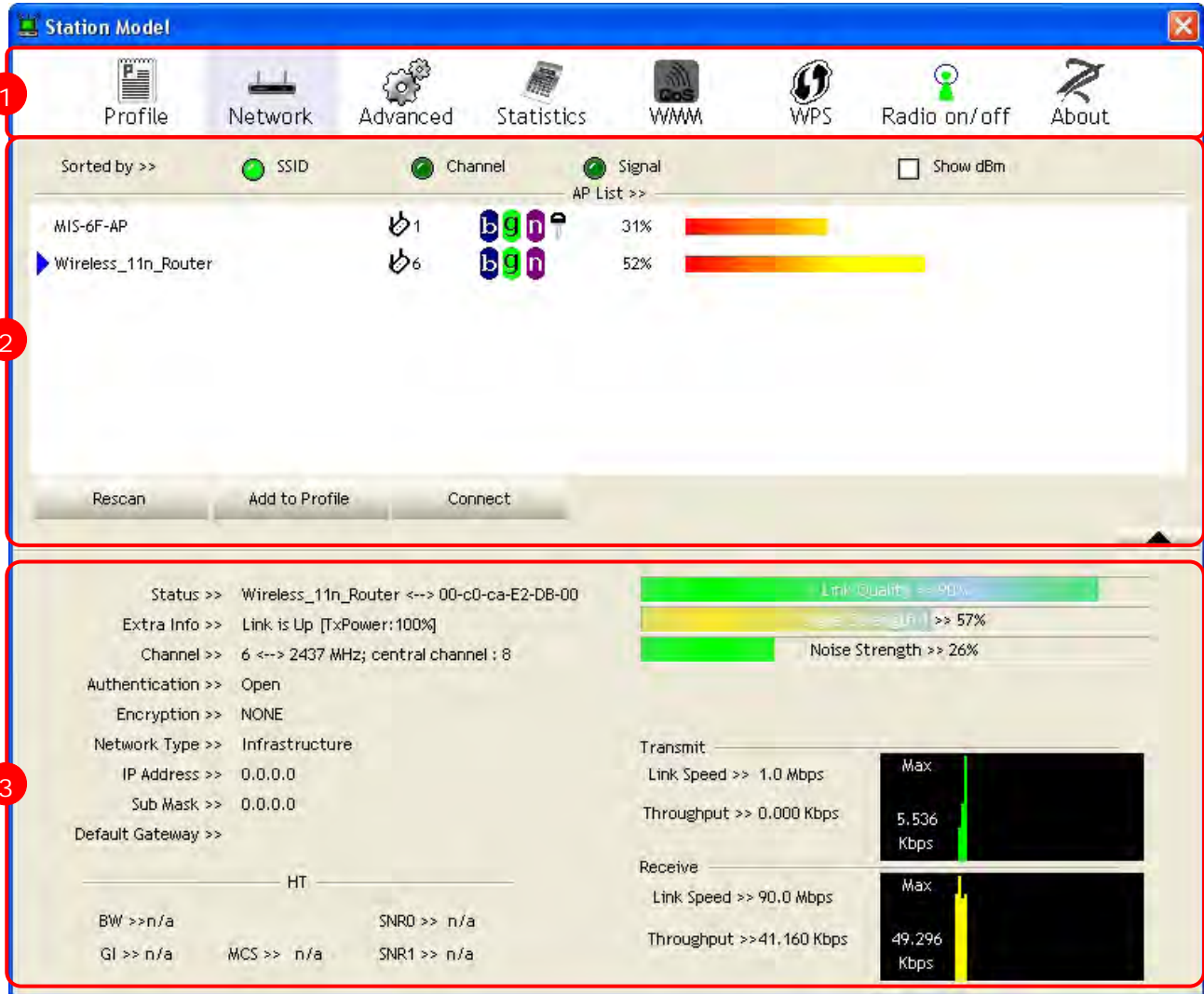
Parameter	Value
BW	n/a
GI	n/a
MCS	n/a
SNR0	n/a
SNR1	n/a

# Introduction to the 802.11n Wireless LAN Utility

**Note:** The Utility in Linux and Mac are different from the following.

## 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.

**Note:** Click  to enable/disable wireless connection status.

**2. Configuration Column:** Center of the Utility window. Make your changes for each function in this part.

**3. Link Status Information:** bottom of the utility window. Shows the connection status and system information.

## Link Status Information

The screenshot shows a network configuration page with four callouts:

- A:** Network information including Status (Wireless\_11n\_Router), Extra Info (Link is Up), Channel (6), Authentication (Open), Encryption (NONE), Network Type (Infrastructure), IP Address (192.168.1.150), Sub Mask (255.255.255.0), and Default Gateway (192.168.1.1).
- B:** HT status information including BW, GI, MCS, SNRO, and SNR1 values, all shown as n/a.
- C:** Link Quality (84%), Signal Strength 1 (34%), and Noise Strength (26%) displayed with a green bar.
- D:** Transmit and Receive throughput information. Transmit: Link Speed 1.0 Mbps, Throughput 0.768 Kbps. Receive: Link Speed 54.0 Mbps, Throughput 24.996 Kbps. Both are shown with bar graphs.

### A. Network Information:

Items	Information
<b>Status</b>	Show the connecting status. Also shows the SSID while connecting to a valid network.
<b>Extra Info</b>	Display link status in use.
<b>Channel</b>	Display current channel in use.
<b>Authentication</b>	Authentication mode in use.
<b>Encryption</b>	Encryption type in use.
<b>Network Type</b>	Network type in use.
<b>IP Address</b>	IP address of current connection.
<b>Sub Mask</b>	Subnet mask of current connection.
<b>Default Gateway</b>	Default gateway of current connection.
<b>Link Speed</b>	Show current transmit rate and receive rate.
<b>Throughput</b>	Display transmit and receive throughput in Mbps.

**B. HT:** Display current HT status in use, containing BW, GI, MCS, SNRO, and SNR1 value.

### C. Link Quality and Strength Bar:

Items	Information
<b>Link Quality</b>	Display connection quality based on signal strength and TX/RX packet error rate.
<b>Signal Strength 1</b>	Receive signal strength 1.
<b>Noise Strength</b>	Display noise signal strength.

User can choose to display Signal and Noise Strength as percentage or dBm format by mark the dBm checkbox.

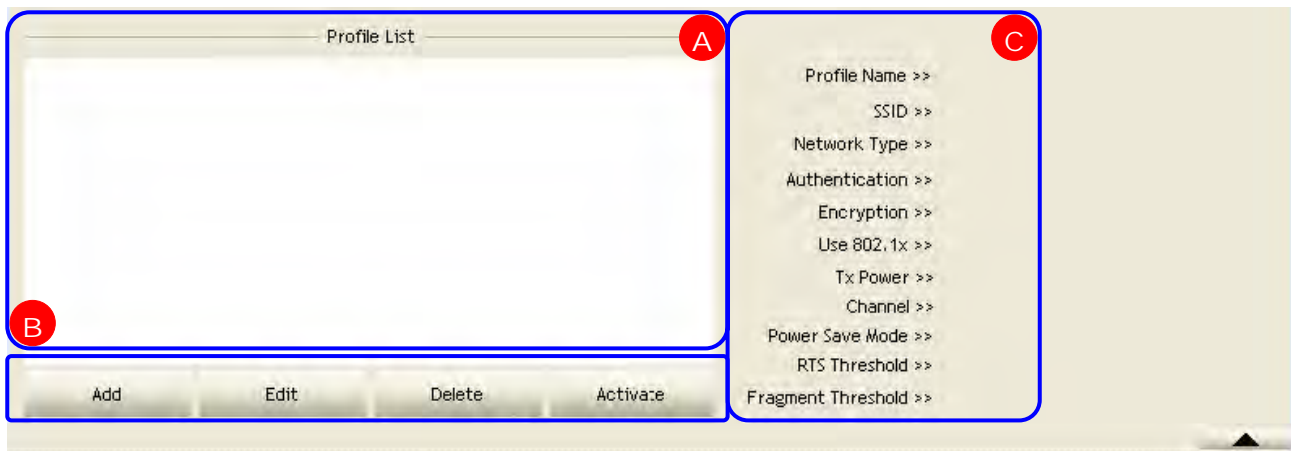
The screenshot shows a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS, Radio on/off, and About. Below the icons, there are checkboxes for SSID, Channel, Signal, and Show dBm. The 'Show dBm' checkbox is highlighted with a red box.

### D. Statistics:

Items	Information
<b>Link Speed</b>	Show current transmit rate and receive rate.
<b>Throughput</b>	Display transmit and receive throughput in Mbps.

## 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.



**A. Profile List:** The list shows all the profiles you have added before.

**B. Buttons:** You can click on these buttons to add a new profile, edit, delete or activate an old profile.

**Note:** For Vista user, there are extra  and  buttons in this feature. Click on these buttons to import or export the selected profile.

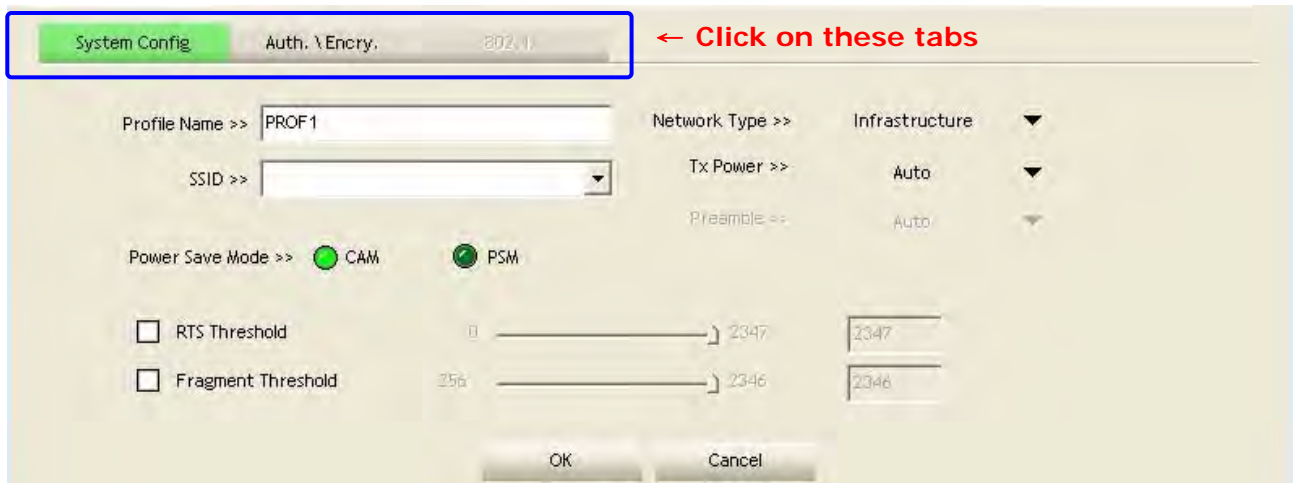
**C. Profile Information:** While you select a profile in the profile list, you can see the profile information shows on here.

Items	Information
<b>Profile Name</b>	The name of the selected profile.
<b>SSID</b>	The SSID of the wireless system.
<b>Network Type</b>	Shows Infrastructure / Ad-hoc to indicate the network type of the selected profile.
<b>Authentication</b>	Shows the authentication mode in use. There are total 8 modes: Open, Shared, LEAP, WPA, WPA-PSK, WPA2, WPA2-PSK and WPA-NONE.
<b>Encryption</b>	Shows the encryption mode in use. There are total 4 modes: None, WEP, TKIP and AES.
<b>Use 802.1x</b>	Shows Yes/No to indicate whether the selected profile use the 802.1x feature or not.
<b>Tx Power</b>	Shows the transmit power in use. There are total 7 types: Auto, 100%, 75%, 50%, 25%, 10% and Low.
<b>Channel</b>	Shows the channel in use (1~14) for Ad-Hoc mode.
<b>Power Save Mode</b>	Shows the power save mode in use. Two selections: CAM (Constantly Awake Mode) and PSM (Power Saving Mode).
<b>RTS Threshold</b>	Shows the RTS threshold value in use.
<b>Fragment Threshold</b>	Shows the fragment threshold in use.

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 click the **Add to Profile** button.



2. There are three tabs on the window:

System Config

Settings for: Profile Name, SSID, Network Type, Tx Power, Preamble, Power Save Mode, RTS Threshold, and Fragment Threshold.

Auth. \Encry.

Settings for: Authentication, Encryption, Preshared Key, and WEP Key.

802.1x

Settings for: EAP Method, Tunnel Authentication, and Session Resumption. For different EAP Method, you also have to configure different require of ID/Password, Client Certificate, or Server Certificate.

Please follow the steps below to fill in the information gradually.

3. In **System Config** section, fill in information for this profile:

The screenshot shows a 'System Config' dialog box with the following fields and values:

- Profile Name >> PROF1
- Network Type >> Infrastructure
- SSID >> [Dropdown menu]
- Tx Power >> Auto
- Preamble >> Auto
- Power Save Mode >>  CAM  PSM
- RTS Threshold:  [Slider from 0 to 2347] [Input: 2347]
- Fragment Threshold:  [Slider from 256 to 2346] [Input: 2346]
- Buttons: OK, Cancel

Items	Information
<b>Profile Name</b>	Choose a name for this profile, or use default name defined by system.
<b>SSID</b>	Fill in the intended SSID name or use the drop list to select from available APs.
<b>Network Type</b>	There are two types, infrastructure and 802.11 Ad-hoc modes. 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.
<b>Tx Power</b>	Transmit power, the amount of power used by a radio transceiver to send the signal out.
<b>Preamble</b>	Two selections: Auto, and Long Preamble. This can only be set up in Ad-hoc mode.
<b>Channel</b>	Channel in use for Ad-Hoc mode.
<b>Power Save Mode</b>	Choose from CAM (Constantly Awake Mode) or PSM (Power Saving Mode).
<b>RTS Threshold</b>	For adjusting the RTS threshold number by sliding the bar or key in the value directly. The default value is 2347.
<b>Fragment Threshold</b>	Adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346.



4. In **Auth. \ Encry.** section, select an encryption type and fill in the corresponding wireless network information:



Items	Information																						
<b>Authentication Type</b>	<p><b>For Windows 2000 User</b> There are 7 types supported: Open, Shared, LEAP, WPA, WPA-PSK, WPA2, WPA2-PSK, and WPA-NONE<sup>1</sup>. Please select a type from the drop down list.</p> <p><b>For Vista User</b> There are 7 types supported: Open, Shared, WPA, WPA-PSK, WPA2, WPA2-PSK, and CCKM. Please select a type from the drop down list.</p>																						
<b>Encryption Type</b>	<p><b>For Windows 2000 User</b> There are 4 types supported: None, WEP, TKIP and AES. The available encryption selection will differ from the authentication type you have chosen, the result is shown below:</p> <table border="1" data-bbox="456 1261 1369 1462"> <thead> <tr> <th>Authentication</th> <th>Available Encryption Selection</th> </tr> </thead> <tbody> <tr> <td>Open</td> <td>NONE, WEP</td> </tr> <tr> <td>Shared</td> <td>WEP</td> </tr> <tr> <td>LEAP</td> <td>(no selection)</td> </tr> <tr> <td>WPA/WPA2/WPA-PSK WPA2-PSK/WPA-NONE</td> <td>TKIP, AES</td> </tr> </tbody> </table> <p><b>For Vista User</b> There are 6 types supported: None, WEP, TKIP, AES, TKIP (MFP) and AES (MFP). The available encryption selection will differ from the authentication type you have chosen, the result is shown below:</p> <table border="1" data-bbox="461 1657 1362 1859"> <thead> <tr> <th>Authentication</th> <th>Available Encryption Selection</th> </tr> </thead> <tbody> <tr> <td>Open</td> <td>NONE, WEP</td> </tr> <tr> <td>Shared</td> <td>WEP</td> </tr> <tr> <td>WPA/ WPA-PSK/ WPA2-PSK</td> <td>TKIP, AES</td> </tr> <tr> <td>WPA2</td> <td>TKIP, AES, TKIP(MFP), AES(MFP)</td> </tr> <tr> <td>CCKM</td> <td>WEP, TKIP, AES</td> </tr> </tbody> </table>	Authentication	Available Encryption Selection	Open	NONE, WEP	Shared	WEP	LEAP	(no selection)	WPA/WPA2/WPA-PSK WPA2-PSK/WPA-NONE	TKIP, AES	Authentication	Available Encryption Selection	Open	NONE, WEP	Shared	WEP	WPA/ WPA-PSK/ WPA2-PSK	TKIP, AES	WPA2	TKIP, AES, TKIP(MFP), AES(MFP)	CCKM	WEP, TKIP, AES
Authentication	Available Encryption Selection																						
Open	NONE, WEP																						
Shared	WEP																						
LEAP	(no selection)																						
WPA/WPA2/WPA-PSK WPA2-PSK/WPA-NONE	TKIP, AES																						
Authentication	Available Encryption Selection																						
Open	NONE, WEP																						
Shared	WEP																						
WPA/ WPA-PSK/ WPA2-PSK	TKIP, AES																						
WPA2	TKIP, AES, TKIP(MFP), AES(MFP)																						
CCKM	WEP, TKIP, AES																						

<sup>1</sup> WPA-NONE is only available in Ad-hoc mode.

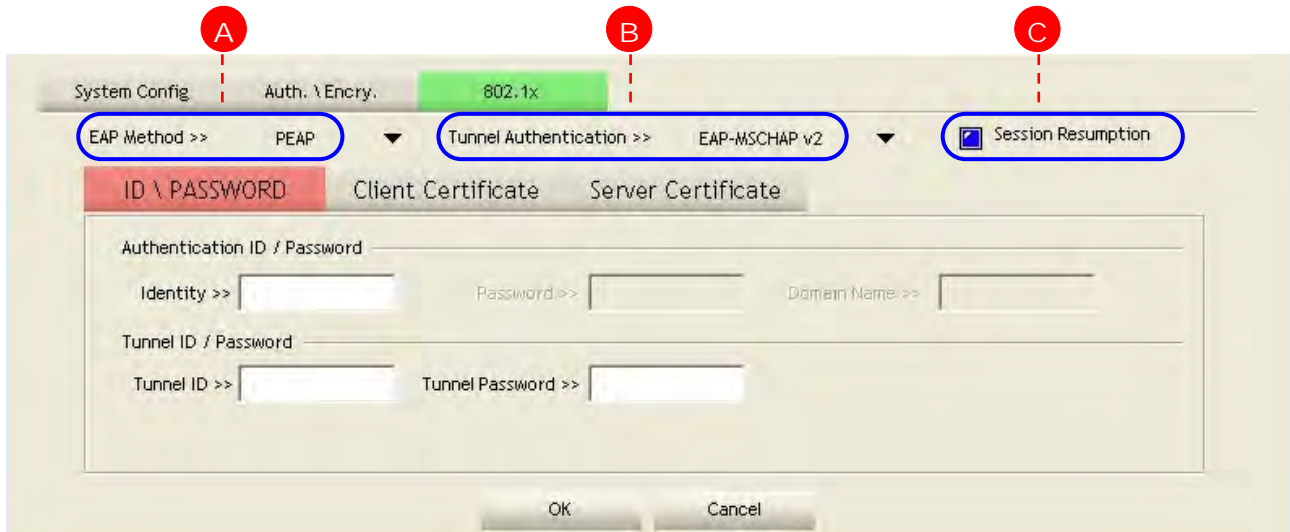
<b>Use 802.1x</b>	This checkbox appears while the environment is set to an Open authentication with WEP encryption. Mark the checkbox to make the 802.1x section available. The 802.1x section is also available in WPA and WPA2 authentication types.
<b>Preshared Key</b>	This is the shared secret between AP and STA. For WPA-PSK, WPA2-PSK and WPA-NONE authentication mode, this field must be filled with characters longer than 8 and less than 32 lengths. The following dialog appears if you have input invalid values. Invalid WPA Pre-Shared key. WPA-PSK used field should use 8-63 ASCII characters or 64 Hex characters.
<b>WEP Key</b>	Only available when using WEP encryption algorithm. The key must match AP's key. Select Hex <sup>1</sup> or ASCII <sup>2</sup> to setup the key value. The following dialog appears if you have input invalid values. Invalid WEP Key 1 length. WEP Key should be 10 or 26 hex digits Invalid WEP Key 1 length. WEP Key should be 5 or 13 ascii characters

<sup>1</sup> Hexadecimal digits consist of the numbers 0-9 and the letters A-F.

<sup>2</sup> ASCII (American Standard Code for Information Interchange) is a code for representing English letters as numbers from 0-127.

5. Specify the 802.1x information if you are using the 802.1X certification method.

Users that do not use this function or connecting to an open-wireless network please skip this part.



#### A. EAP Method:

**For Windows 2000 User:** There are total 5 modes: PEAP, TLS/Smart Card, TTLS, EAP-FAST, and MD5-Challenge.

**For Vista User:** There are total 4 modes: PEAP, TLS/Smart Card, EAP-FAST, and LEAP. Please select an EAP method from the drop down list.

Items	Information
<b>PEAP</b>	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.
<b>TLS/Smart Card</b>	Transport Layer Security. 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.
<b>TTLS</b>	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.
<b>EAP-FAST</b>	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.
<b>MD5-Challenge</b>	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.
<b>LEAP</b>	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.

**B. Tunnel Authentication:** The tunnel authentication will differ from the EAP method you have chosen, the result is shown below:

**For Windows 2000 User:**

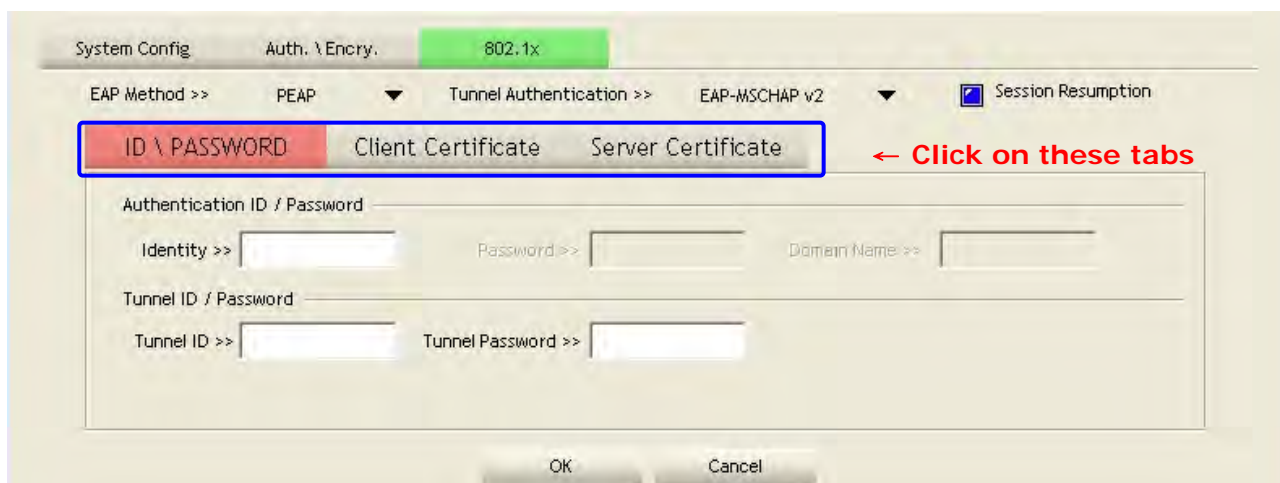
EAP Method	Tunnel Authentication
PEAP	EAP-MSCHAP v2 , EAP-TLS/Smart Card, Generic Token Card
TLS/Smart Card	(no selection)
TTLS	CHP, MS-CHAP, MS-CHAP-V2, PAP, EAP-MD5
EAP-FAST	Generic Token Card
MD5-Challenge	(no selection)

**For Vista User:**

EAP Method	Tunnel Authentication
PEAP	EAP-MSCHAP v2 , EAP-TLS/Smart Card, Generic Token Card
TLS/Smart Card	(no selection)
EAP-FAST	(no selection)
LEAP	(no selection)

**C. Session Resumption:** Mark to enable this function or unmark it to disable.

After doing the above settings, please click on the tabs below. There are several tabs on the window, please fill in the information gradually.



**ID \ PASSWORD** Settings for: Authentication ID/Password, Tunnel ID/Password and Password Mode<sup>1</sup>.

**Client Certificate** Settings for using the Client Certificate function or not.

**Server Certificate** Settings for using the Server Certificate function or not.

**EAP-FAST** Setting for EAP-FAST method.

**SSO** Settings for Single Sign On. **Note:** This tab only appears in Vista system.

<sup>1</sup> Password mode is only available in EAP-FAST method.

## ID \ PASSWORD

System Config    Auth. \ Encry.    802.1x

EAP Method >> EAP-FAST    Tunnel Authentication >> Generic Token Card     Session Resumption

**ID \ PASSWORD**    EAP-FAST

Authentication ID / Password

Identity >>     Password >>     Domain Name >>

Tunnel ID / Password

Tunnel ID >>     Tunnel Password >>

Password Mode >>     Soft Token     Static Password

OK    Cancel

Items	Information
<b>Authentication ID / Password</b>	The identity, password and domain name for server. Only "EAP-FAST" and "LEAP" authentication can be keyed in domain name. Blank space can be keyed in domain name.
<b>Tunnel ID / Password</b>	Identity and Password for server.
<b>Password Mode</b>	Select the power save mode. <b>For Windows 2000 User</b> There are two selections: Soft Token and Static Password. <b>For Vista User</b> There are four selections: Soft Token, Static Password, Windows Logon and Prompt User.

## Client Certificate

System Config    Auth. \ Encry.    802.1x

EAP Method >> PEAP    Tunnel Authentication >> EAP-MSCHAP v2     Session Resumption

ID \ PASSWORD    **Client Certificate**    Server Certificate

Use Client certificate   

Issued To >>

Issued By >>

Expired On >>

Friendly Name >>

OK    Cancel

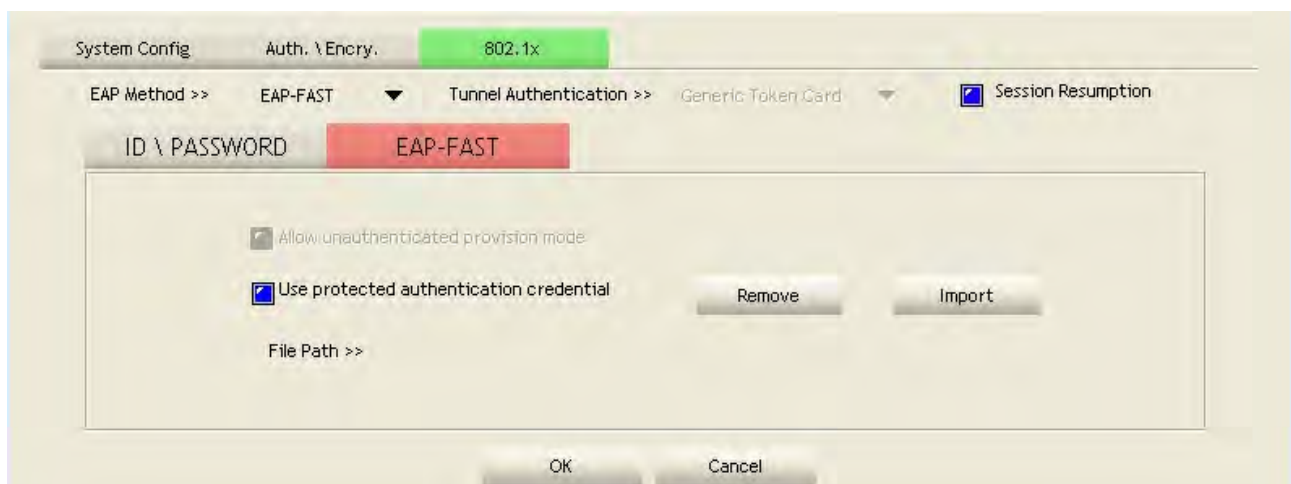
Items	Information
<b>Use Client certificate</b>	Client certificate for server authentication.
<b>Use my smart card</b>	Client certificate for server authentication.

## Server Certificate



Items	Information
<b>Use Certificate chain</b>	Mark the checkbox to enable using certification chain.
<b>Allow intimidate certificates</b>	Mark to allow intimidates certification.
<b>Server name</b>	Enter an authentication sever root.

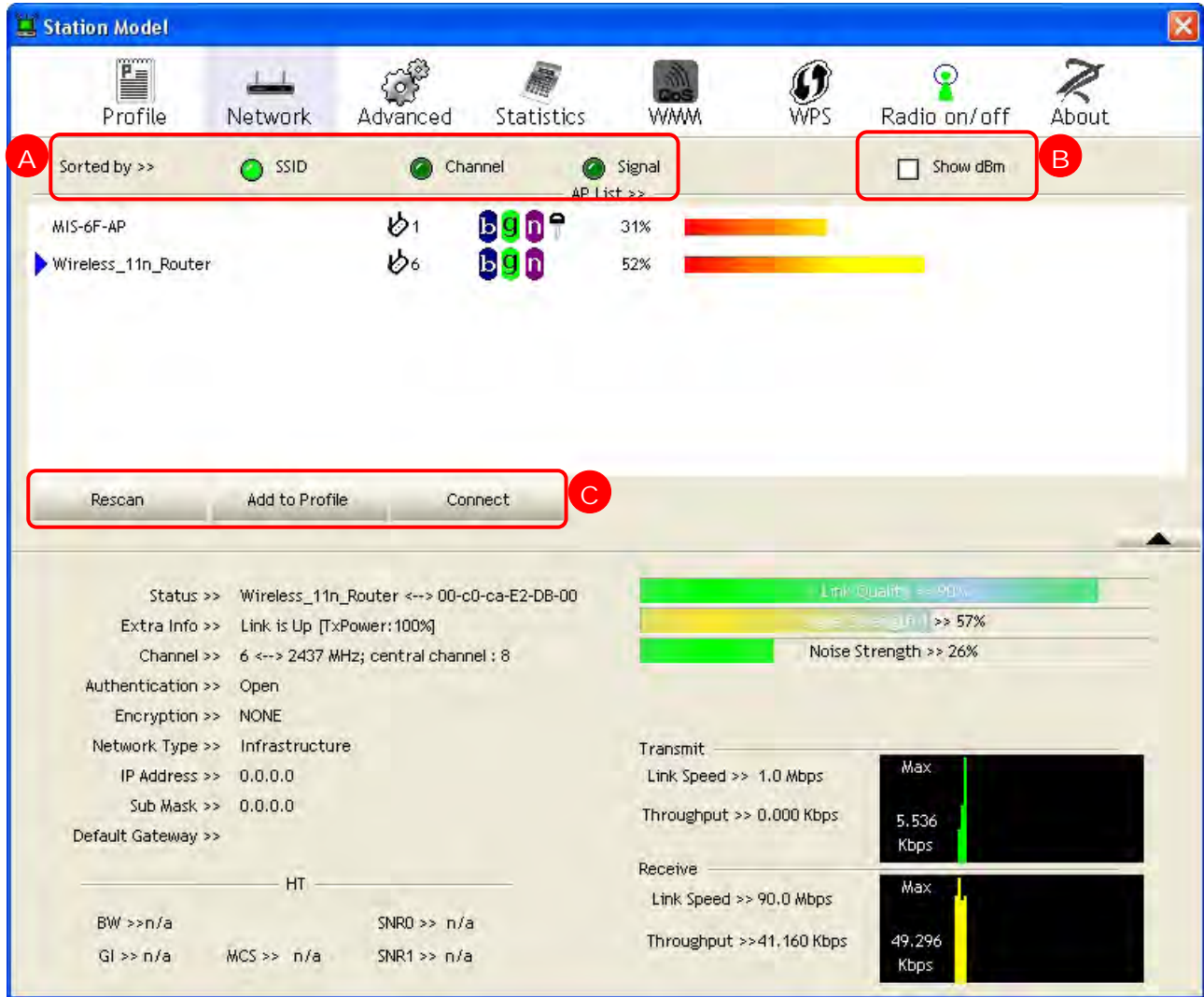
## EAP Fast



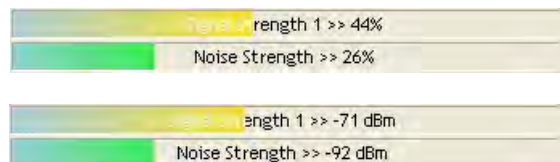
Items	Information
<b>Allow unauthenticated provision mode</b>	During the PAC can be provisioned (distributed one time) to the client automatically. It only supported "Allow unauthenticated provision mode" and use "EAP-MSCHAP v2" authentication to authenticate now. It causes to continue with the establishment of the inner tunnel even though it is made with an unknown server. Mark to enable unauthenticated provision mode.
<b>Use protected authentication credential</b>	Use protected authentication credential: Using PAC, the certificate can be provided to the client manually via disk or a secured network distribution method. Mark to use protected authentication credential.

## 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.



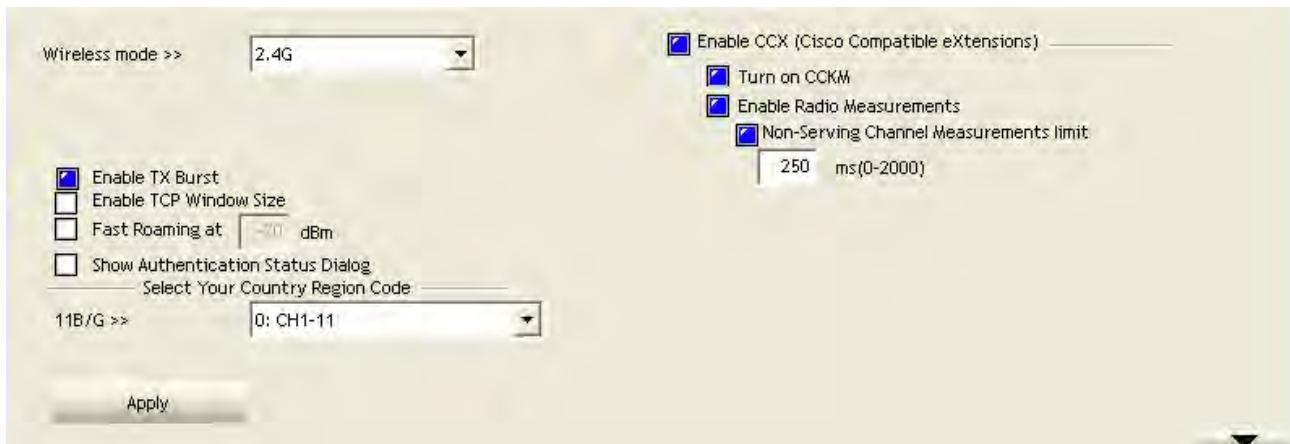
- A. Sorted by:** Click each button to sort the listing networks by SSID, channel and Signal strength.
- B. Show dBm:** Mark the checkbox to show the signal and noise strength in dBm, unmark to show in percentage.
- C. Buttons:** You can click on these buttons to add a new profile, edit, delete or activate an old profile.



Items	Information
<b>Rescan</b>	To rescan available wireless networks.
<b>Connect</b>	To connect to a designated network.
<b>Add to Profile</b>	To add a network to profile after selecting a network.

## Advanced

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



Items	Information
<b>Wireless mode</b>	Select wireless mode. 2.4G/5.2G&5.8G is supported.
<b>Enable TX Burst</b>	Select to enable connecting to a TX Burst supported device.
<b>Enable TCP Window Size</b>	Mark the checkbox to enable TCP window size, which help enhance throughput.
<b>Fast Roaming at __ dBm</b>	Mark the checkbox to enable fast roaming. Specify the transmit power for fast roaming.
<b>Show Authentication Status Dialog</b>	Mark the checkbox to show "Authentication Status Dialog" while connecting to an AP with authentication. Authentication Status Dialog displays the process about 802.1 x authentications.
<b>Select Your Country Region Code</b>	Eight countries to choose. Channel list:  1 ~ 11 channels (North America) 1 ~ 13 channels (General Europe) 1 ~ 14 channels (Japan)  IEEE802.11a 4 Channels (Japan) 19 Channels (Europe) 13 Channels (USA)
<b>Enable CCX (Cisco Compatible extensions)</b>	Select to enable CCX. This function can only be applied when connecting to a Cisco compatible device.
<b>Turn on CCKM</b>	Mark to enable CCKM.
<b>Enable Radio Measurements</b>	Mark to enable channel measurement every 0~2000 milliseconds.
<b>Non-Serving Channel Measurements limit</b>	Mark to revise the channel measurement.

**Note:** For Vista user, click on the CCX button to do more configuration. Please refer to [CCX](#) for more information.





## 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.

Item	Value
Frames Transmitted Successfully	120
Frames Retransmitted Successfully	14
Frames Fail To Receive ACK After All Retries	0
RTS Frames Successfully Receive CTS	0
RTS Frames Fail To Receive CTS	0

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

Item	Value
Frames Received Successfully	11
Frames Received With CRC Error	333
Frames Dropped Due To Out-of-Resource	0
Duplicate Frames Received	0


Items	Information
<b>Frames Received Successfully</b>	Frames received successfully.
<b>Frames Received With CRC Error</b>	Frames received with CRC error.
<b>Frames Dropped Due To Out-of-Resource</b>	Frames dropped due to resource issue.
<b>Duplicate Frames Received</b>	Duplicate received frames.
<b>Reset Counter</b>	Reset counters to zero.

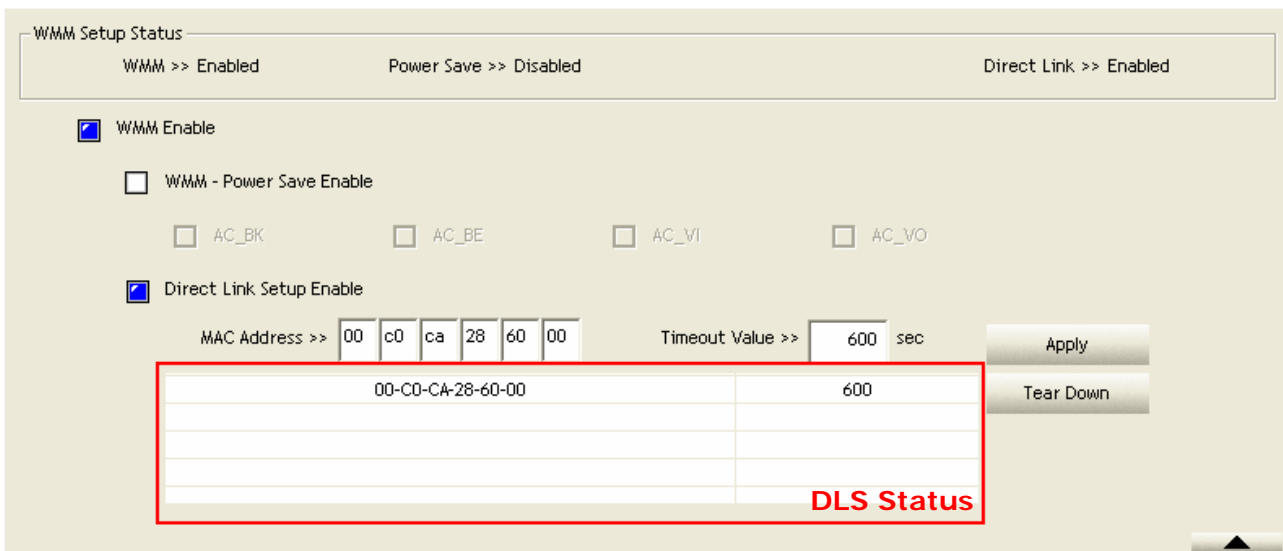
## WMM

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.

Items	Information
<b>WMM Enable</b>	Enable Wi-Fi Multi-Media.
<b>WMM - Power Save Enable</b>	Enable WMM Power Save. Please enable WMM before configuring this function.
<b>Direct Link Setup Enable</b>	Enable DLS (Direct Link Setup). Please enable WMM before configuring this function.
<b>MAC Address</b>	Fill in the blanks of Direct Link with MAC Address of STA.
<b>Timeout Value</b>	Time of automatically disconnect after some seconds. The value is integer. The integer must be between 0~65535. It represents that it always connects if the value is zero. Default value of Timeout Value is 60 seconds.
<b>Apply / Tear Down</b>	After fill in the "MAC Address" and "Timeout Value", click "Apply" button to save your configuration. The result will appear in the following "DLS Status" blanks. To remove the configuration, please select the configuration in the blanks and then click "Tear Down" button.

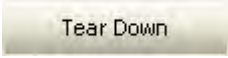
### Steps to enable Direct Link Setup function:

1. Click the "Direct Link Setup Enable" checkbox.
2. Change to "Network" function. Add an AP that supports DLS features to the Profile.
3. Fill in the blanks of Direct Link with MAC Address of STA. The STA must conform to these two conditions:
  - Connect with an AP that supports DLS features.
  - Ensure that DLS is enabled
4. Fill in the Timeout Value and then click .
5. After configuring the DLS successfully, the MAC address and Timeout Value are displayed in the "DLS Status".



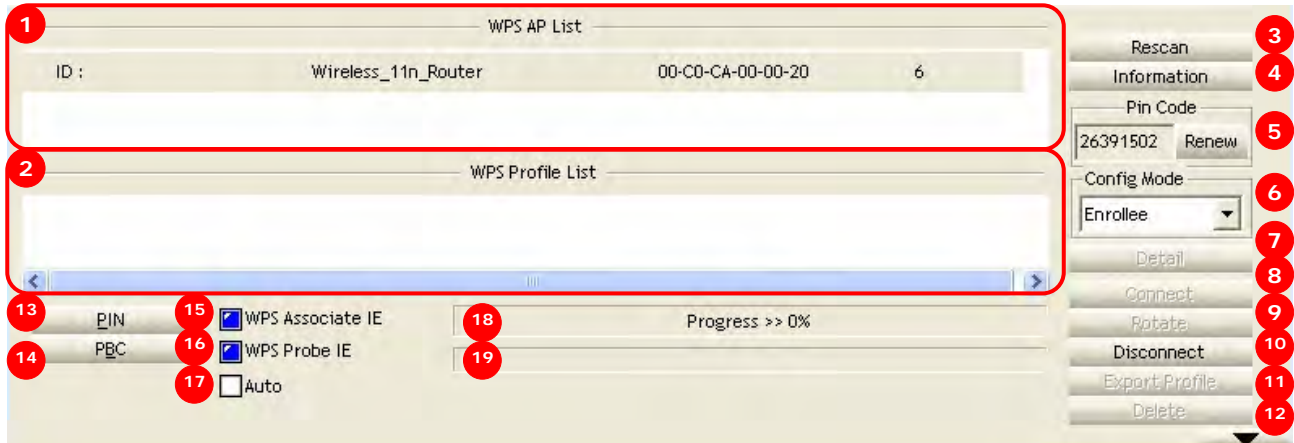
The screenshot shows the "WMM Setup Status" configuration page. At the top, it displays "WMM >> Enabled", "Power Save >> Disabled", and "Direct Link >> Enabled". Below this, there are several checkboxes: "WMM Enable" (checked), "WMM - Power Save Enable" (unchecked), and "Direct Link Setup Enable" (checked). Under "Direct Link Setup Enable", there are input fields for "MAC Address >>" (00 c0 ca 28 60 00) and "Timeout Value >>" (600 sec). Below these fields is a table with two columns: "MAC Address" and "Timeout Value". The first row contains the values "00-C0-CA-28-60-00" and "600". The table is highlighted with a red border and labeled "DLS Status" in red text. To the right of the table are "Apply" and "Tear Down" buttons.

MAC Address	Timeout Value
00-C0-CA-28-60-00	600

6. If you want to disconnect Direct Link Setup, select the list in "DLS Status" and then click on the  button.

## 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.



Items	Information
<b>1. WPS AP List</b>	Display the information of surrounding APs with WPS IE from last scan result. List information includes SSID, BSSID, Channel, ID (Device Password ID), and Security-Enabled.
<b>2. WPS Profile List</b>	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, Utility creates a new credential with WPA2-PSK/AES/64Hex-Key and doesn't change until next switching to STA Registrar.
<b>3. Rescan</b>	Click to rescan the wireless networks.
<b>4. Information</b>	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.
<b>5. Pin Code</b>	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. Click on the Renew button to renew the PIN code.
<b>6. Config Mode</b>	Enrollee or an external Registrar.
<b>7. Detail</b>	Information about Security and Key in the credential.
<b>8. Connect</b>	Command to connect to the selected network inside credentials.
<b>9. Rotate</b>	Command to connect to the next network inside credentials.
<b>10. Disconnect</b>	Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page of Utility if exists. If there is an empty profile page, the driver will select any non-security AP.
<b>11. Export Profile</b>	Click the "Export Profile" button will export the WPS profile.
<b>12. Delete</b>	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.
<b>13. PIN</b>	Start to add to Registrar using PIN configuration method.
<b>14. PBC</b>	Start to add to AP using PBC configuration method.
<b>15. WPS associate IE</b>	Send the association request with WPS IE during WPS setup. It is optional for STA.
<b>16. WPS probe IE</b>	Send the probe request with WPS IE during WPS setup. It is optional for STA.
<b>17. Auto</b>	Select the AP automatically.
<b>18. Progress Bar</b>	Display rate of progress from Start to Connected status.
<b>19. Status Bar</b>	Display currently WPS Status.

The following description divides into four parts:

- A. WPS Information on AP**
- B. Example of Adding to Registrar Using PIN Method**
- C. Example of Adding to Registrar Using PIN Method**
- D. Example of Configuring a Network/AP Using PIN or PBC Method**

**A. WPS Information on AP:** On Network AP list, double click on the AP then you can see the information appears below.

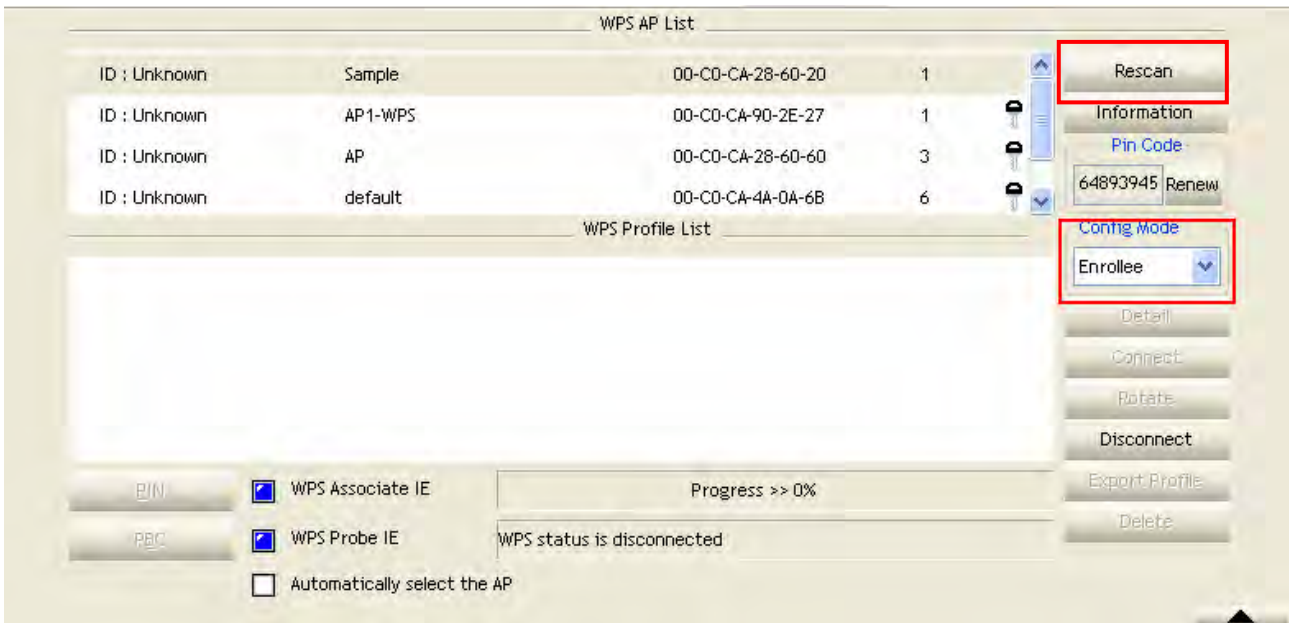


Items	Information
<b>Authentication Type</b>	There are three authentication modes supported by this utility. They are open, Shared, WPA-PSK and WPA system.
<b>Encryption Type</b>	For open and shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.
<b>Config Methods</b>	Correspond to the methods the AP supports as an Enrollee for adding external Registrars. (a bitwise OR of values)
<b>Device Password ID</b>	Indicates the method or identifies the specific password that the selected Registrar intends to use. APs in PBC mode must indicate 0x0004 within two-minute Walk Time.
<b>Selected Registrar</b>	Indicates if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".
<b>State</b>	The current configuration state on AP. The values are "Unconfigured" and "Configured".
<b>Version</b>	WPS specified version.
<b>AP Setup Locked</b>	Indicates if the AP has entered a setup locked state.
<b>UUID-E</b>	The universally unique identifier (UUID) element generated by the Enrollee. This is a 16 byte value.
<b>RF Bands</b>	Indicates all the RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz/5.8GHz" and "5GHz".

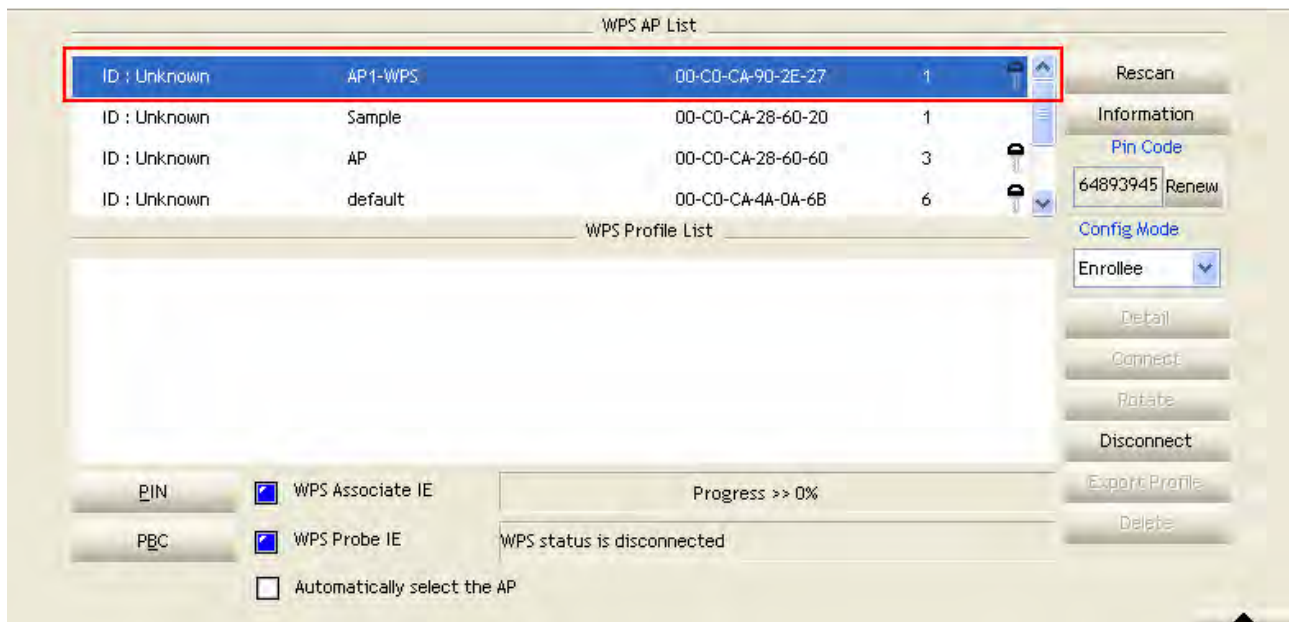
## B. Example of Adding to Registrar Using PIN Method

The user obtains a device password (PIN Code) from the STA and enters the password into the Registrar. Both the Enrollee and the Registrar use PIN Config method for the configuration setup. Please follow the step below.

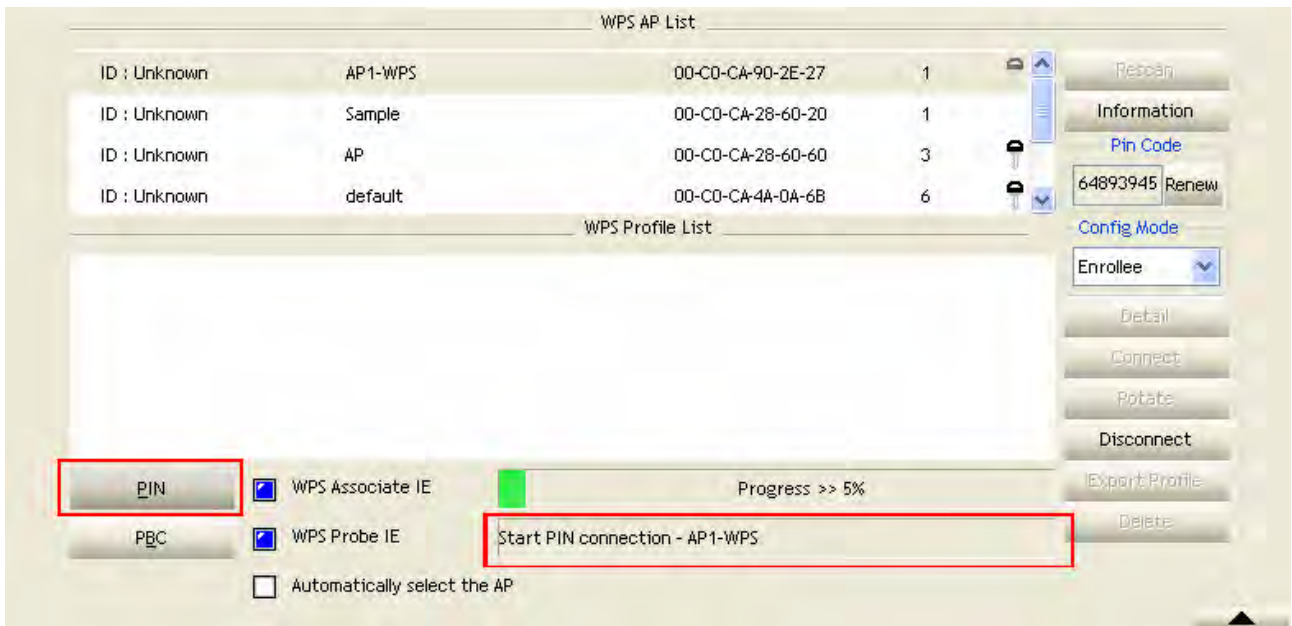
1. Select "Enrollee" from the Config Mode drop-down list.
2. Click "Rescan" to update available WPS APs.



3. Select an AP (SSID/BSSID) that STA will join to.



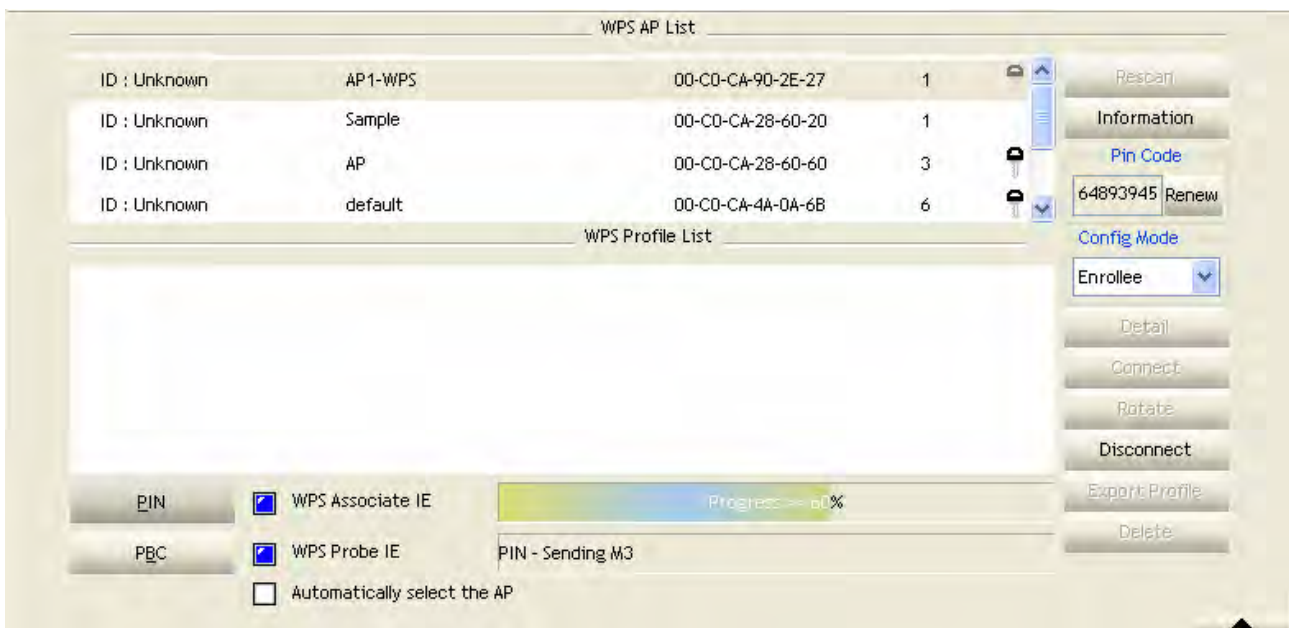
4. Click "PIN" to enter the PIN.
5. Enter the PIN Code of the STA into the Registrar when prompted by the Registrar.



**Note:**

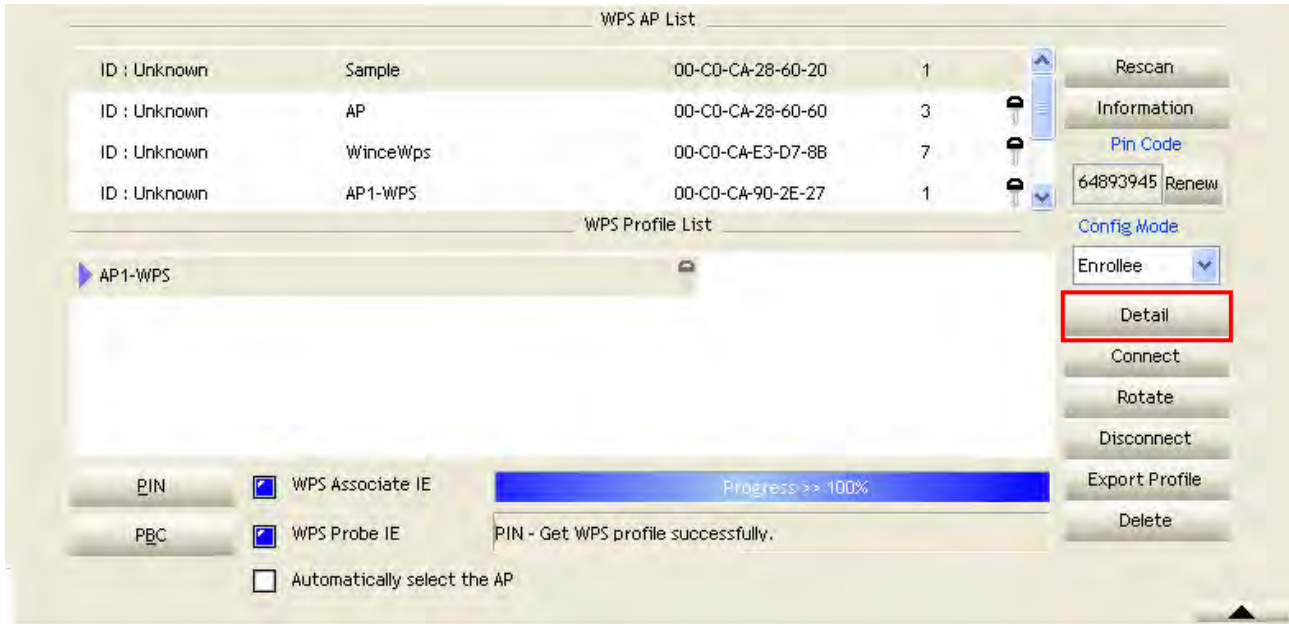
- Allow of an exchange between Step 4 and Step 5.
- If you use Microsoft Window Connection Now as an External Registrar, you must start PIN connection at STA first. After that, search out your WPS Device name and MAC address at Microsoft Registrar. Add a new device and enter PIN Code of STA at Microsoft Registrar when prompted.

6. The result should appear as the image below.

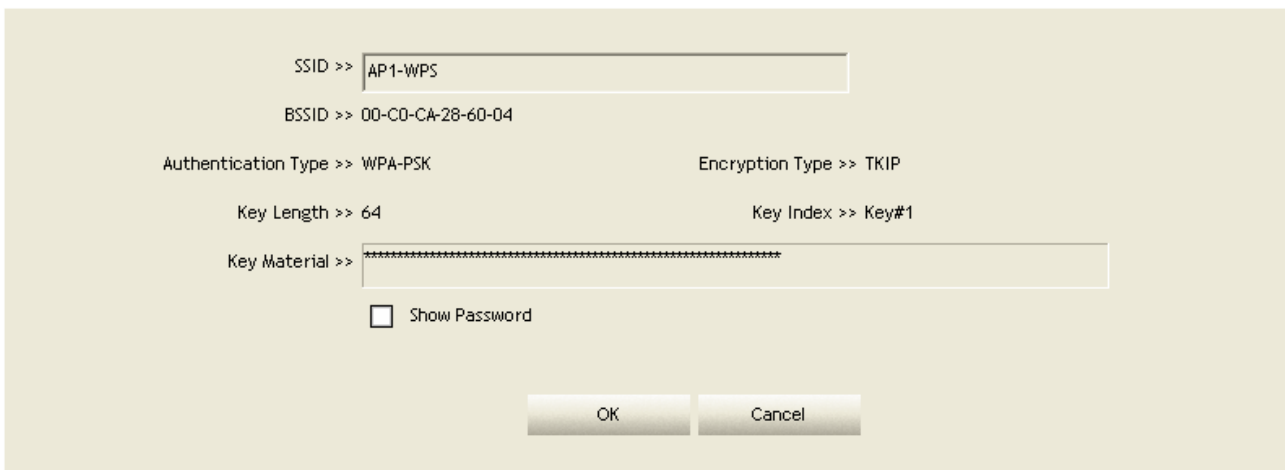




7. Configure one or more credentials. Then connect successfully.



8. Click "Detail." You can see the figure below.



### C. Example of Adding to the Registrar Using the PBC Method

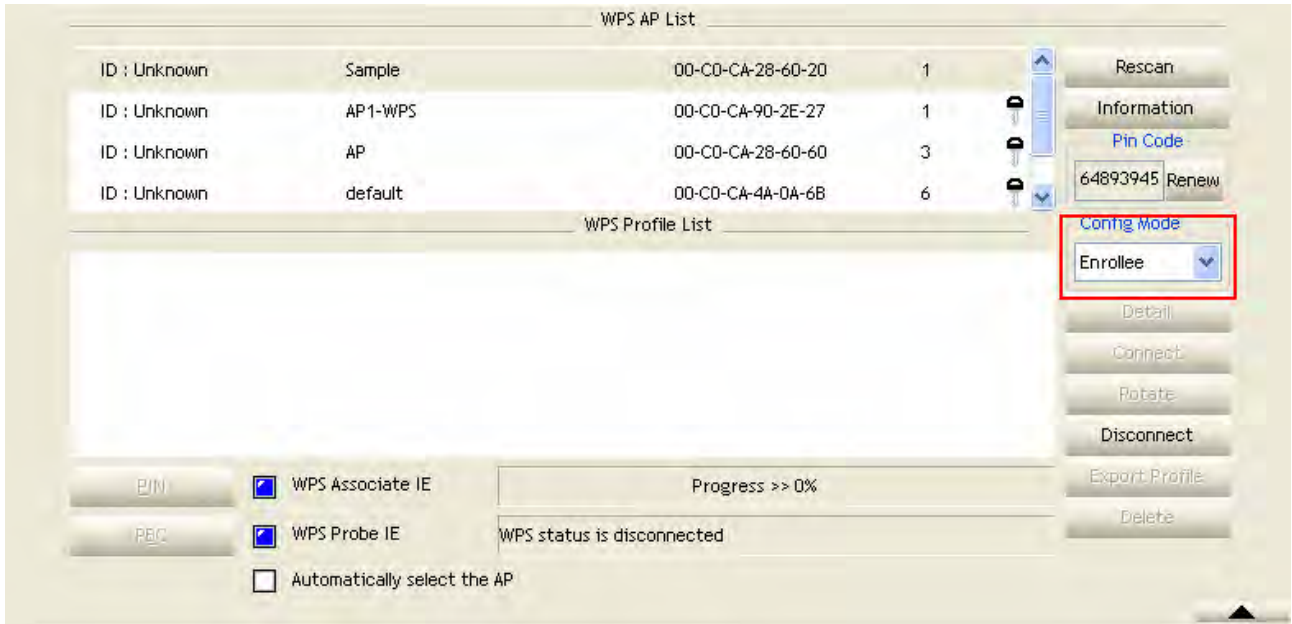
The PBC method requires the user to press a PBC button on both the Enrollee and the Registrar within a two-minute interval called the Walk Time. If there is only one Registrar in PBC mode, the PBC mode selected is obtained from ID 0x0004, and is found after a complete scan. The Enrollee can then immediately begin running the Registration Protocol.

If the Enrollee discovers more than one Registrar in PBC mode, it MUST abort its connection attempt at this scan and continue searching until the two-minute timeout.

**Note:** Before you press PBC on STA and candidate AP. Make sure all APs aren't PBC mode or APs using PBC mode have left their Walk Time. The user can configure WPS profiles with either PIN method or PBC method.

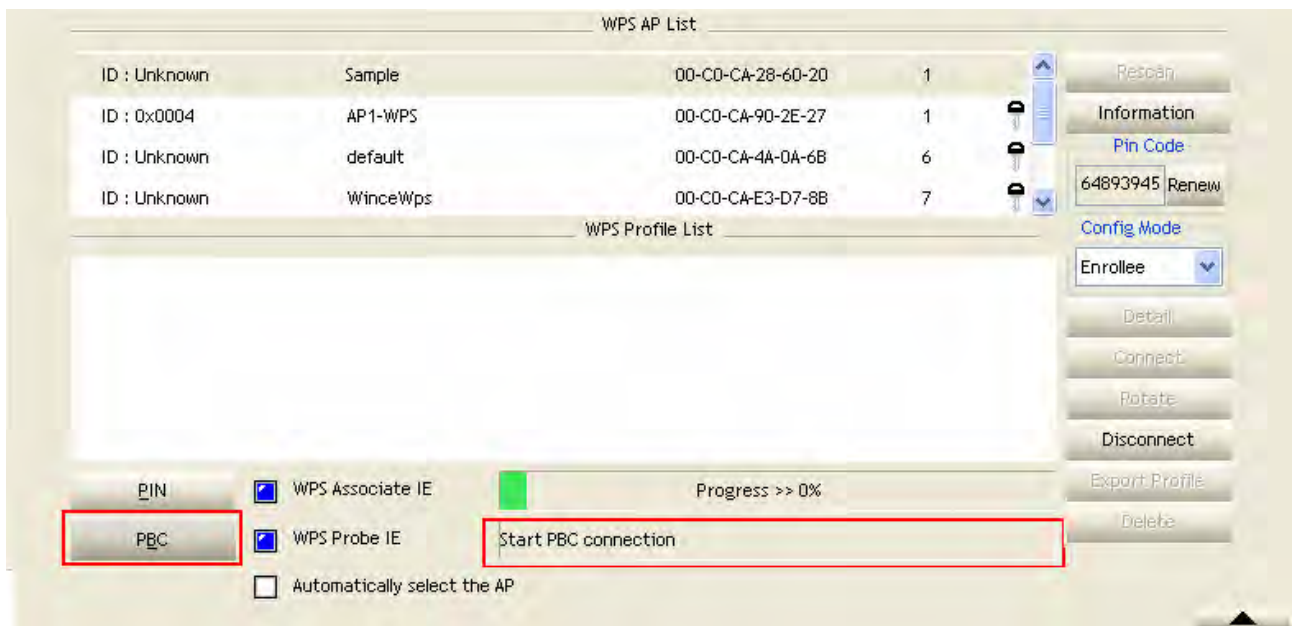
Please follow the steps below.

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

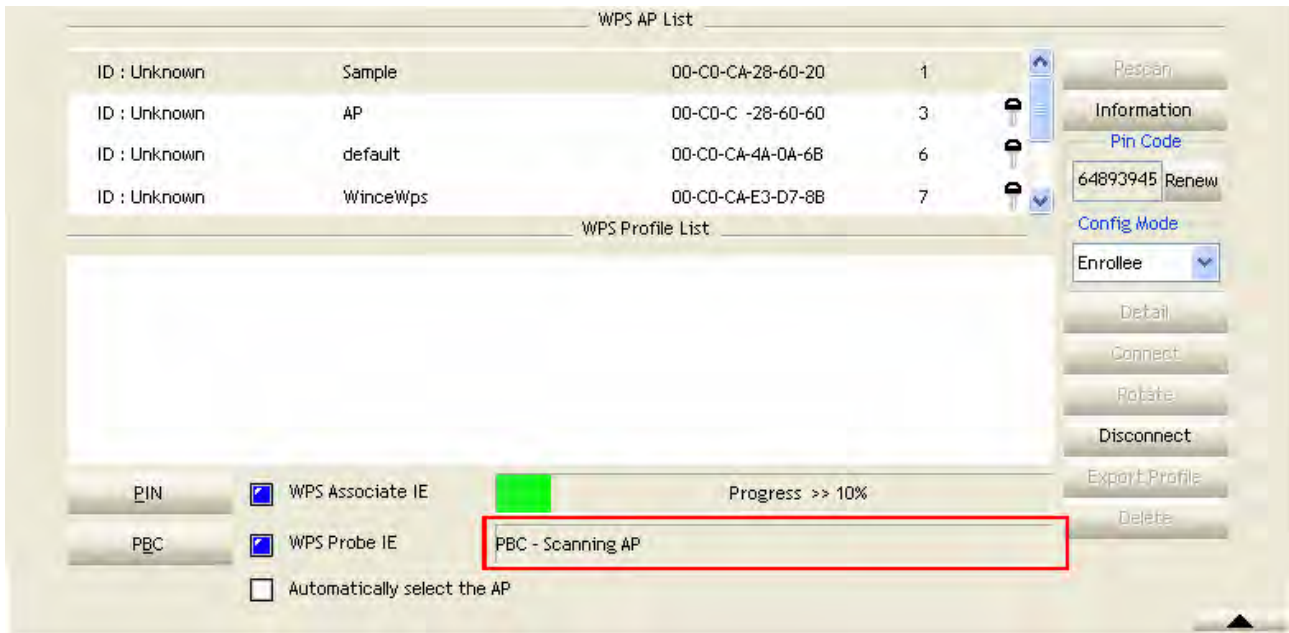


2. Click PBC to start the PBC connection.
3. Push the PBC on AP.

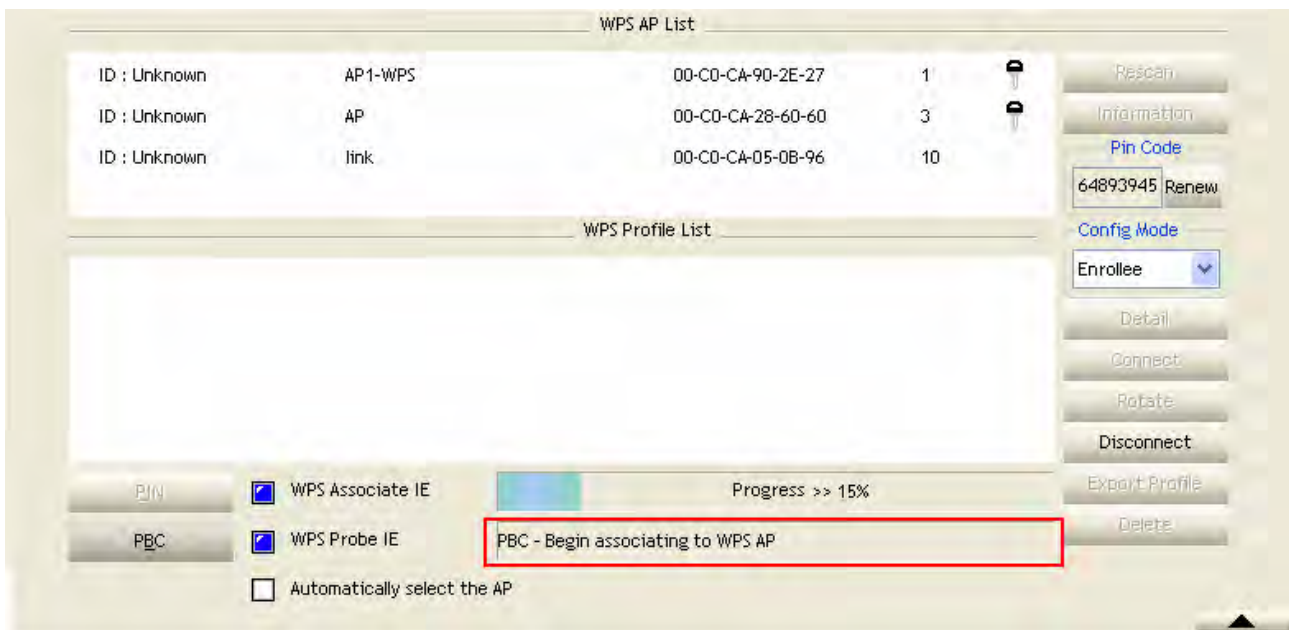
**Note:** Allow time for an exchange between Step 2 and Step 3.



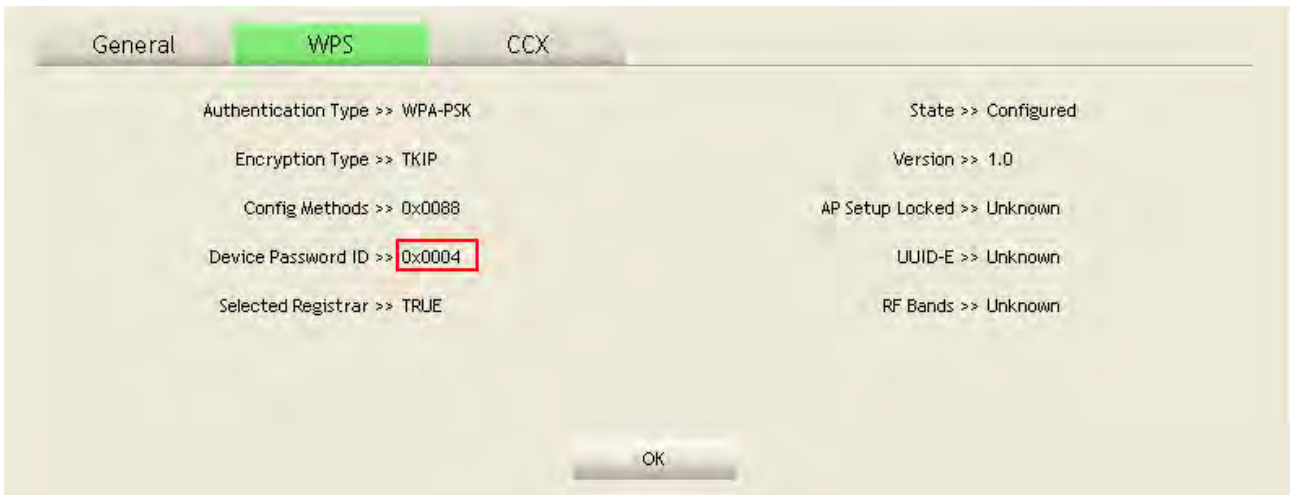
4. The progress bar as shown in the figure below indicates that scanning progress.



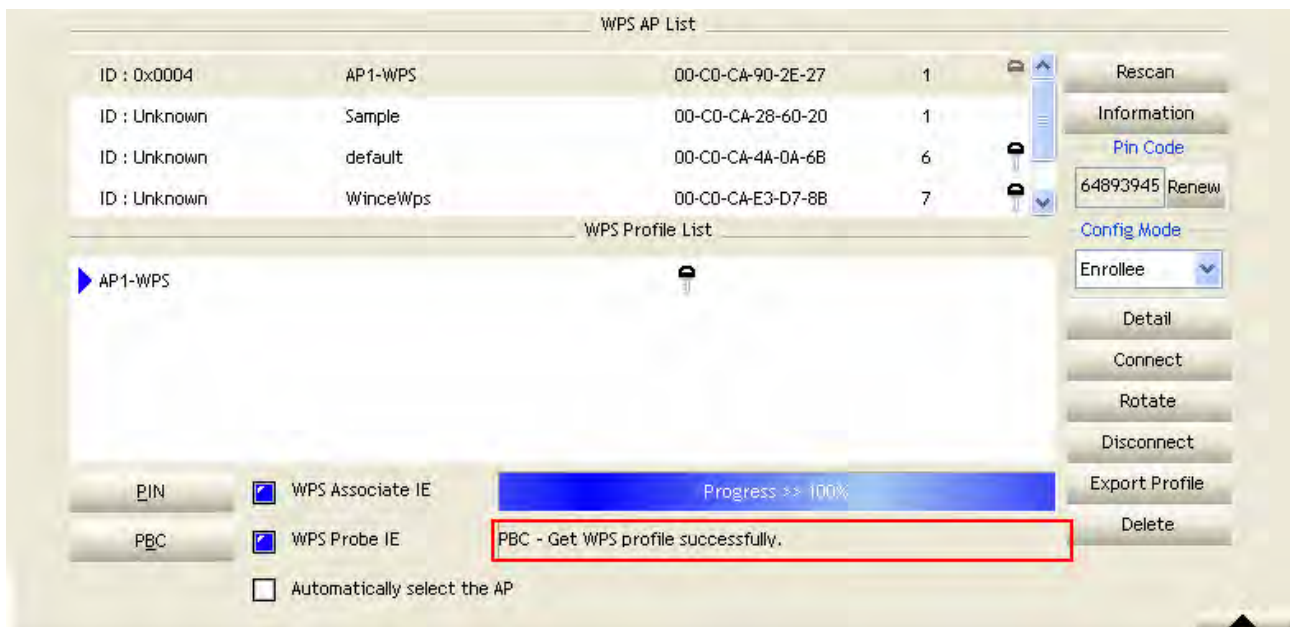
5. When one AP is found, join it.



6. Check WPS Information on the available WPS APs.

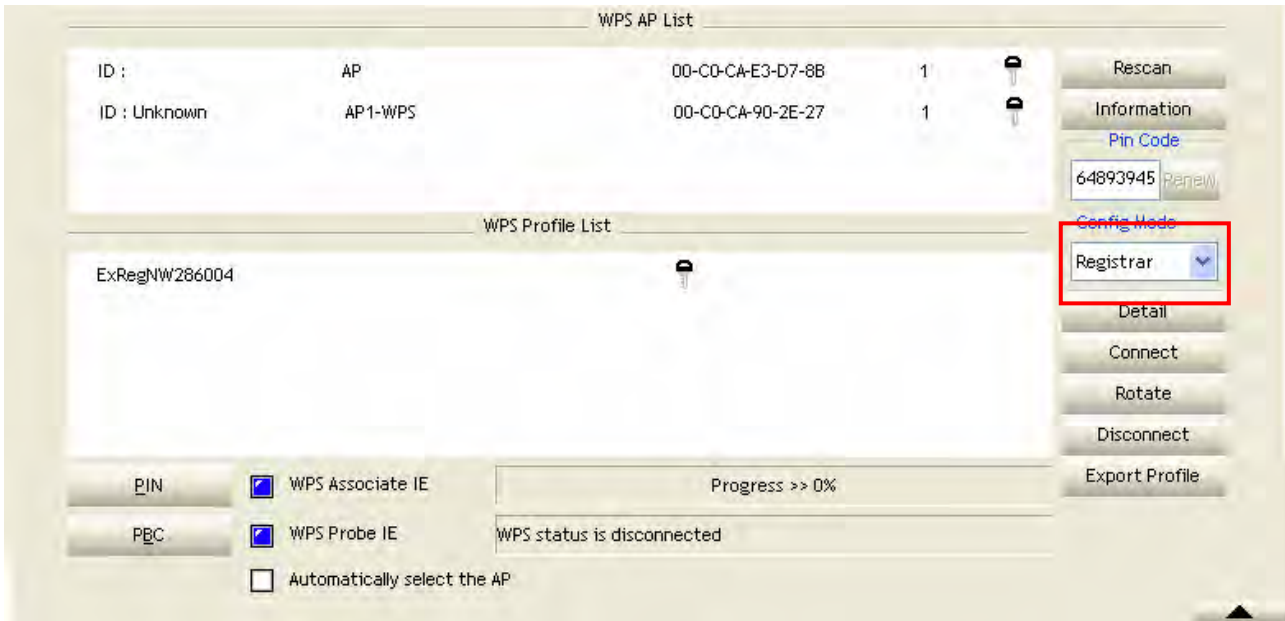


7. Configure and receive one or more credential(s). Then connect successfully. The result will be displayed as it is in the figure below.

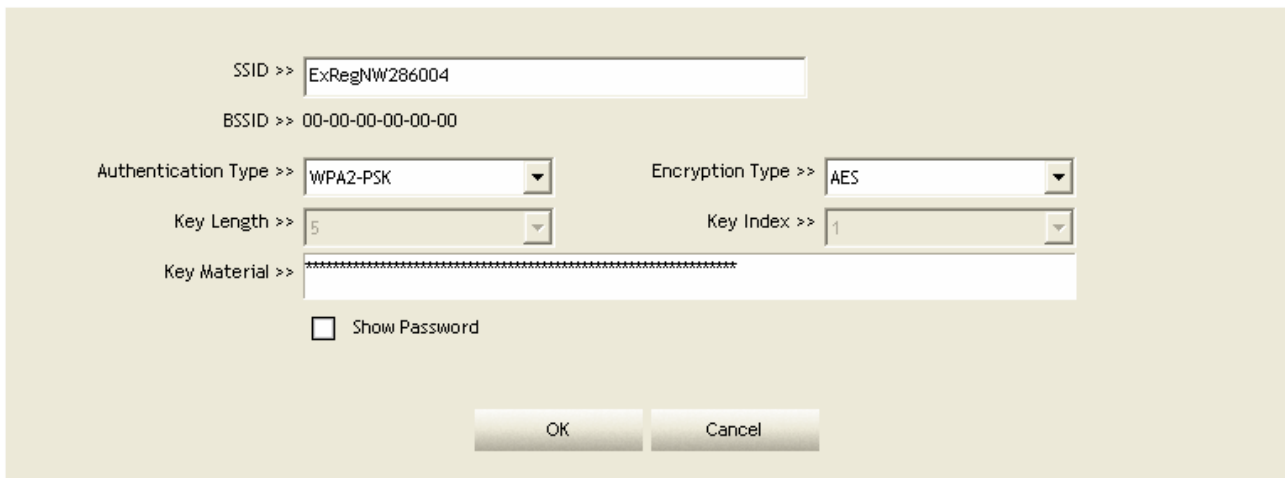


## D. Example of Configuring a Network/AP Using PIN or PBC Method

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

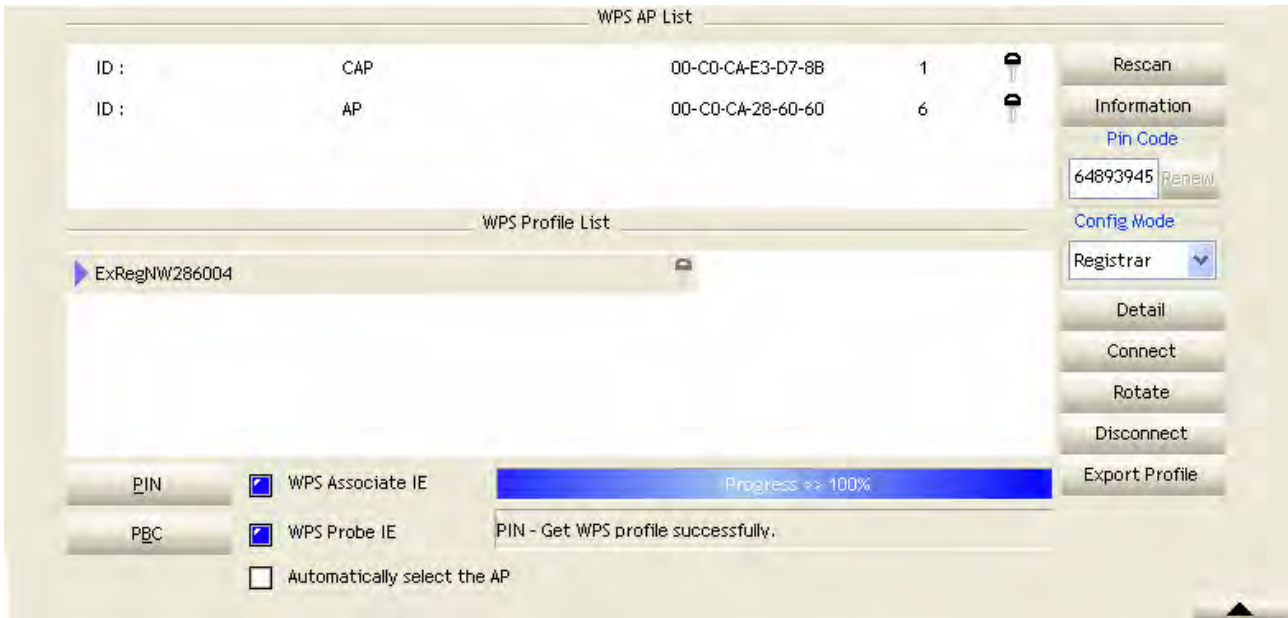


2. Enter the details of the credential and change configurations (SSID, Authentication, Encryption and Key) manually if needed.



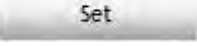
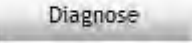
3. If the PIN configuration is setup, enter the PIN sent from the Enrollee.
4. Start PIN or PBC. The following procedures are as similar as section PIN Enrollee Setup or PBC Enrollee Setup.

5. If your AP Enrollee has been configured before the WPS process, the credential you set in advance will be updated to the AP itself. Otherwise, after a successful registration, the AP Enrollee will be re-configured with the new parameters, and the STA Registrar will connect to the AP Enrollee with these new parameters.



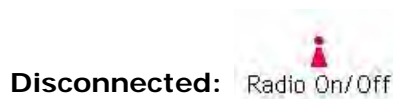
## CCX

This page is available for **Vista user only**. It provides CCX configurations to this adapter. Please refer to the following chart for definitions of each item.

Items	Information
<b>Enable CCX (Cisco Compatible extensions)</b>	Select to enable CCX. This function can only be applied when connecting to a Cisco compatible device.
<b>Turn on CCKM</b>	Mark to enable CCKM.
<b>Enable Radio Measurements</b>	Mark to enable channel measurement every 0~2000 milliseconds.
<b>Non-Serving Channel Measurements limit</b>	Mark to revise the channel measurement.
<b>Network EAP</b>	Enable the NetworkEAP authentication algorithm.
<b>Enable RF Roaming</b>	Enable RF roaming function
<b>Enable CAC (Tolerance)</b>	Enable the call admission control
<b>CAC</b>	There are four selections: ADDTS (Directly send TS), DELTS, and RESET. Select an item from the drop down list and then click on the  button.
<b>Diagnosis</b>	Select a profile which the user wants to diagnose, and then click on the Diagnose button to perform the test. 


## Radio On/Off

Click on the button to enable/disable wireless connection status.



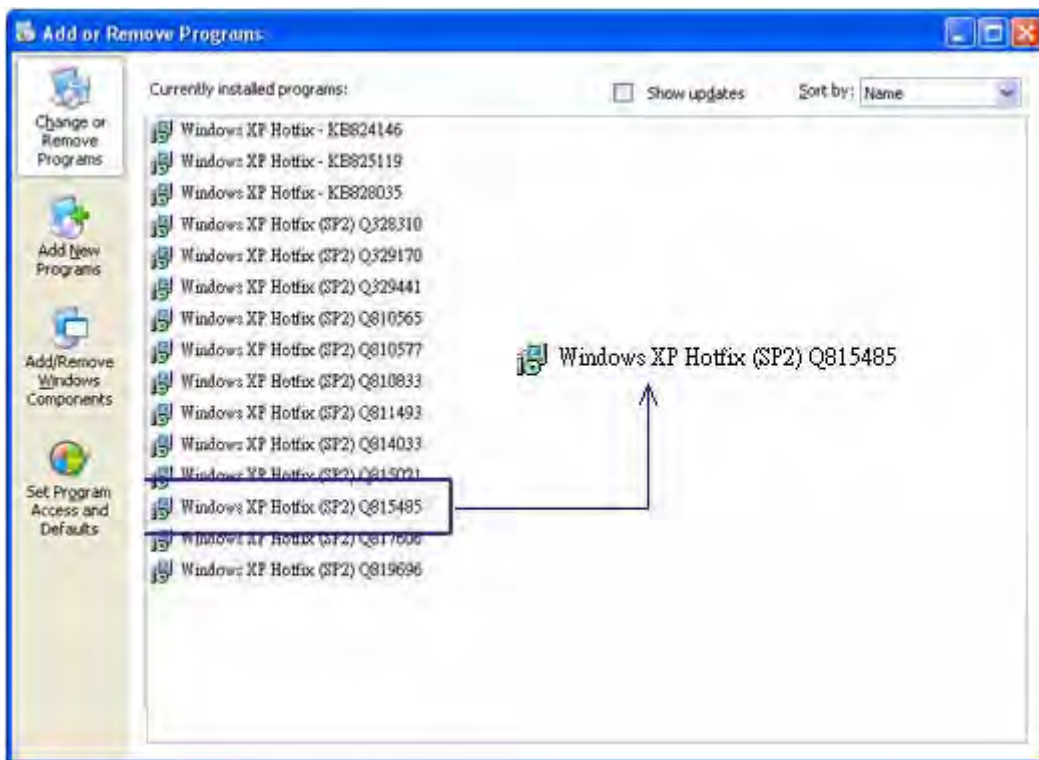
# AP mode management guide for Windows 2000/XP/Vista

If you wish to share the Internet access with the wireless stations in your environment, you can configure this wireless adapter as a software access point (Soft AP). In this mode, this wireless adapter becomes the wireless access point that provides local area network and Internet access for your wireless stations.

To use this adapter as an access point, please right click the  icon on system tray and select **Switch to AP mode**. Please refer to the following introduction and 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.





# Software Access Point (Soft AP) Application



## Config

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

The screenshot shows a configuration window with the following elements:

- 1. SSID: Text field containing "SoftAP-00".
- 2. Wireless Mode: Dropdown menu set to "2.4G".
- 3. Country Region Code: Dropdown menu set to "11 B/G" and "0: CH1-11".
- 4. Beacon (ms): Text field containing "100".
- 5. TX Power: Dropdown menu set to "100 %".
- 6. Idle time(60 - 3600)(s): Text field containing "300".
- 7. Channel: Dropdown menu set to "1".
- 8. <- Use Mac Address: Button.
- 9. Security Setting: Button.
- 10. No forwarding among wireless clients: Checkbox (unchecked).
- 11. Hide SSID: Checkbox (unchecked).
- 12. Allow BW 40 MHz: Checkbox (checked).
- 13. Default: Button.
- 14. Cancel: Button.
- 15. Apply: Button.

1. **SSID:** AP name of user type. User also can select [Use Mac Address] to display it.
2. **Wireless Mode:** Select wireless mode. Only 2.4G is supported.

**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

**Note:** Country Region code is not support for Vista.

- 4. Beacon (ms):** The time between two beacons. System default is 100 ms.
- 5. TX Power:** Manually force the AP transmits power. System default is 100%.
- 6. Idle Time:** Manually force the Idle Time using selected value. Default is 300.
- 7. Channel:** Manually force the AP using the channel. System default is channel 1.
- 8. 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).
- 9. Security Setting:** Authentication mode and encryption algorithm used within the AP. System default is no authentication and encryption.
- 10. No forwarding among wireless clients:** If there is no beacon among the wireless clients, they can't share information with each other.
- 11. Hide SSID:** Prevent this AP from recognized in wireless network. This is disabled as default.
- 12. Allow BW40 MHz:** Allow BW40 MHz capability.
- 13. Default:** Use system default value.
- 14. Cancel:** Cancel the above changes.
- 15. Apply:** Apply the above changes.

## Security Setting

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

The screenshot shows a 'Security Setting' dialog box with the following elements:

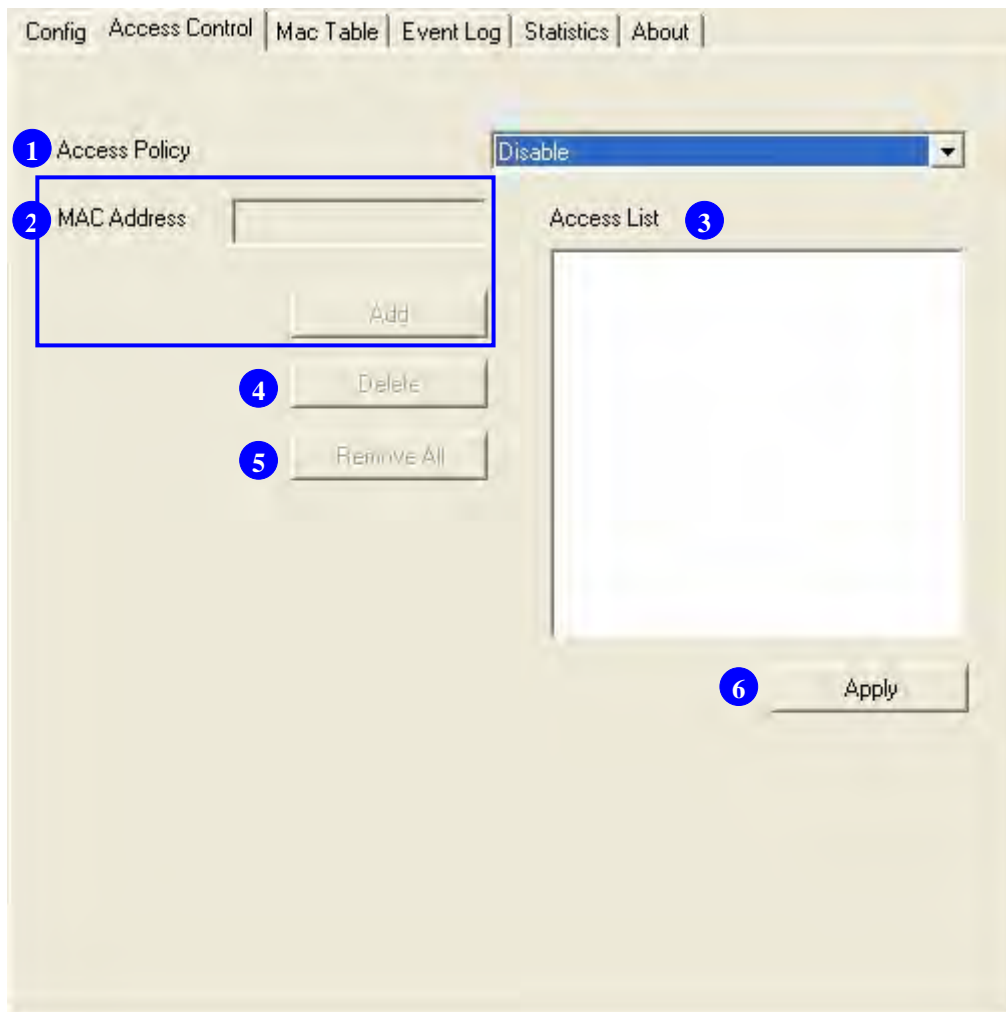
- 1** Authentication Type: Open
- 2** Encryption Type: WEP
- 3** WPA Pre-shared-Key: [Empty text box]
- 4** Group Rekey Interval: 10 seconds
- 5** Wep Key section with four radio buttons (Key#1 to Key#4) and dropdown menus (Hex).

\* WEP 64 Bits Encryption: Please Keyin 10 HEX characters or 5 ASCII characters \*  
\* WEP 128 Bits Encryption: Please Keyin 26 HEX characters or 13 ASCII characters

- 1. Authentication Type:** Select to be open, shared, WPA-PSK, WPA2-PSK, or WPA PSK/WPA2-PSK system.
- 2. Encryption Type:** Select an encryption type from the drop list.
- 3. 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 lengths.
- 4. Group Rekey Interval:** Only valid when using WPA-PSK encryption algorithm. The key will change compliance with seconds or beacon that user set.
- 5. 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.
  - Hexadecimal (40bits): 10 Hex characters.
  - Hexadecimal (128bits): 32Hex characters.
  - ASCII (40bits): 5 ASCII characters.
  - ASCII (128bits): 13 ASCII characters.

## Access Control

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



- 1. 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.
- 2. MAC Address:** Add allowed (or denied) MAC addresses to the MAC address list.
- 3. Access List:** Display all Mac Addresses that you designated.
- 4. Delete:** Delete Mac addresses that you selected.
- 5. Remove All:** Remove all Mac address in [Access List].
- 6. Apply:** Apply changes.





## Statistics

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

The screenshot shows a web interface with a navigation bar at the top containing tabs for 'Config', 'Access Control', 'Mac Table', 'Event Log', 'Statistics', and 'About'. The 'Statistics' tab is active. Below the navigation bar, there are two main sections: 'Transmit Statistics' (marked with a blue circle '1') and 'Receive Statistics' (marked with a blue circle '2').

**Transmit Statistics:**

Frames Transmitted Successfully	=	779
Frames Fail To Receive ACK After All Retries	=	13
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0
Frames Transmitted Successfully After Retry	=	779

**Receive Statistics:**

Frames Received Successfully	=	22
Frames Received With CRC Error	=	5091
Frames Dropped Due To Out-of-Resource	=	0
Duplicate Frames Received	=	0

At the bottom right of the statistics area, there is a button labeled 'RESET COUNTERS' (marked with a blue circle '3').

### 1. Transmit Statistics

Items	Information
<b>Frames Transmitted Successfully</b>	Frames that successfully sent.
<b>Frames Fail To Receive ACK After All Retries</b>	Frames that failed to transmit after hitting retry limit.
<b>RTS Frames Successfully Receive CTS</b>	Counts of CTS that successfully received after sending RTS frame.
<b>RTS Frames Fail To Receive CTS</b>	Counts of CTS that fail to be received after sending RTS frame.
<b>Frames Retransmitted Successfully</b>	Successfully retransmitted frames numbers.

### 2. Receive Statistics

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

**3. Reset Counters:** Reset counters to zero.