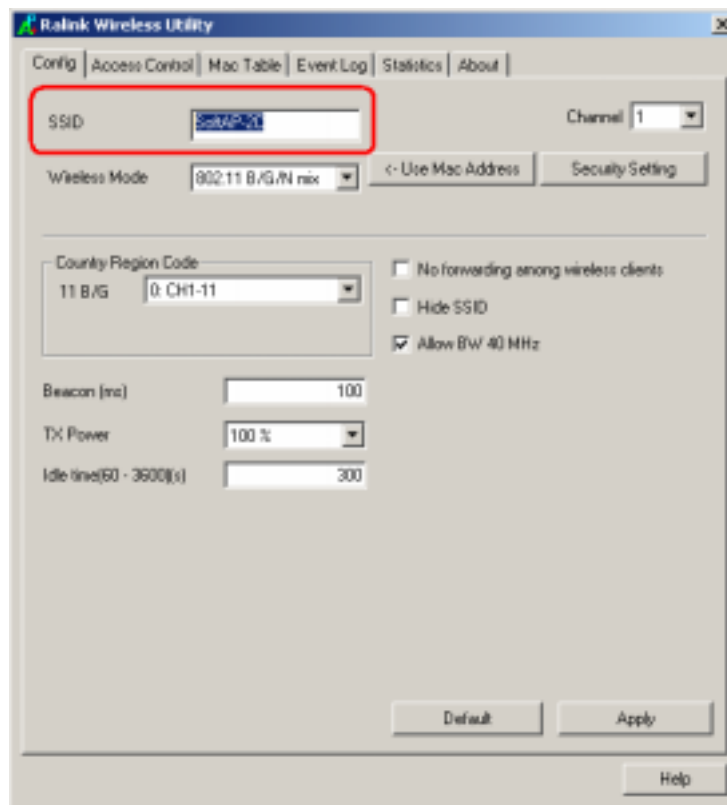
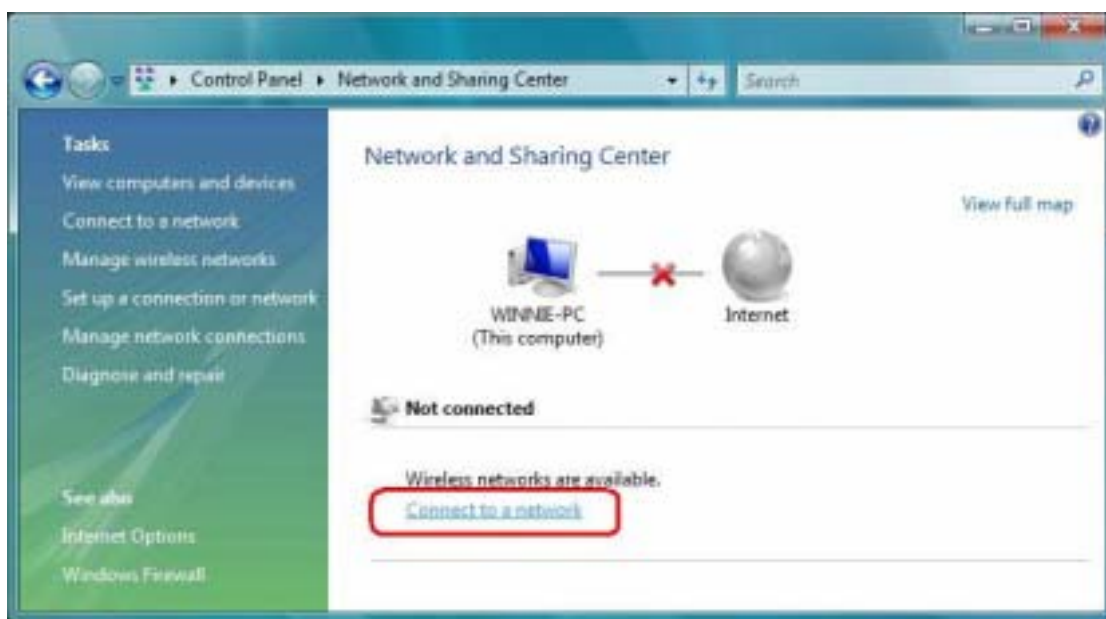


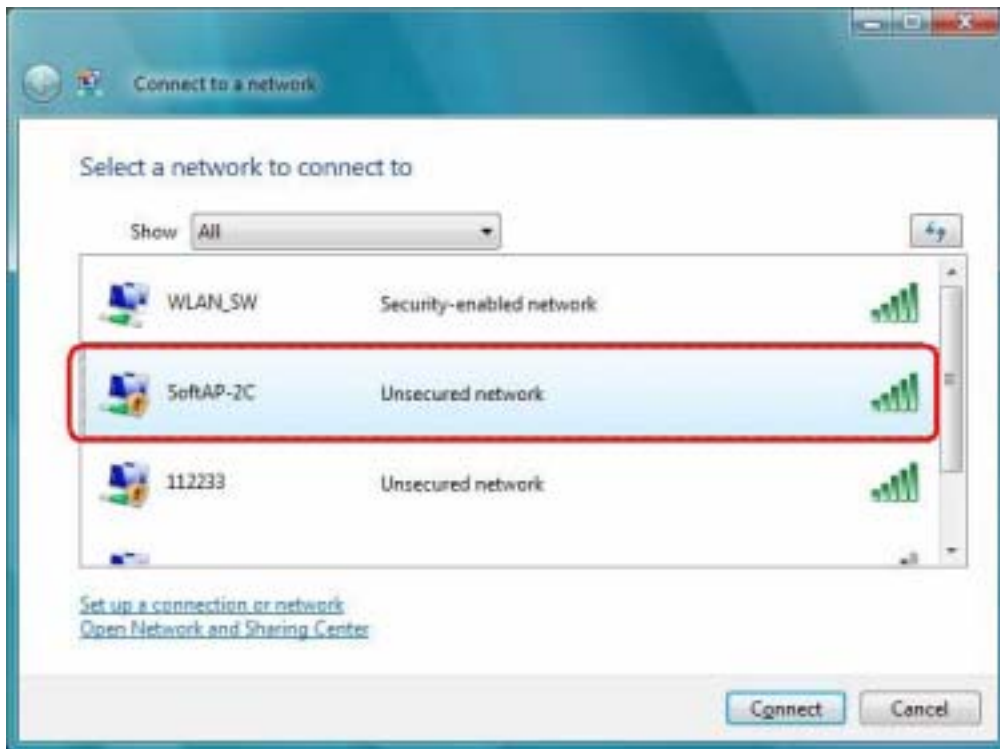
Step 6: After switch to AP mode, Ralink Wireless Utility will automatically pup-up. The Wireless Default SSID is assigned as “SoftAP-2C”.



Step 7: To make sure your Soft AP is working properly, you need to use another computer which with Wireless LAN feature to access SoftAP-2C AP. In the below example, use another PC with Wireless feature in Vista Operation System. Go to **Start → Control Panel → Choose “Network and Sharing Center”** option → Click **“Connect to a network”** to search the available networks.



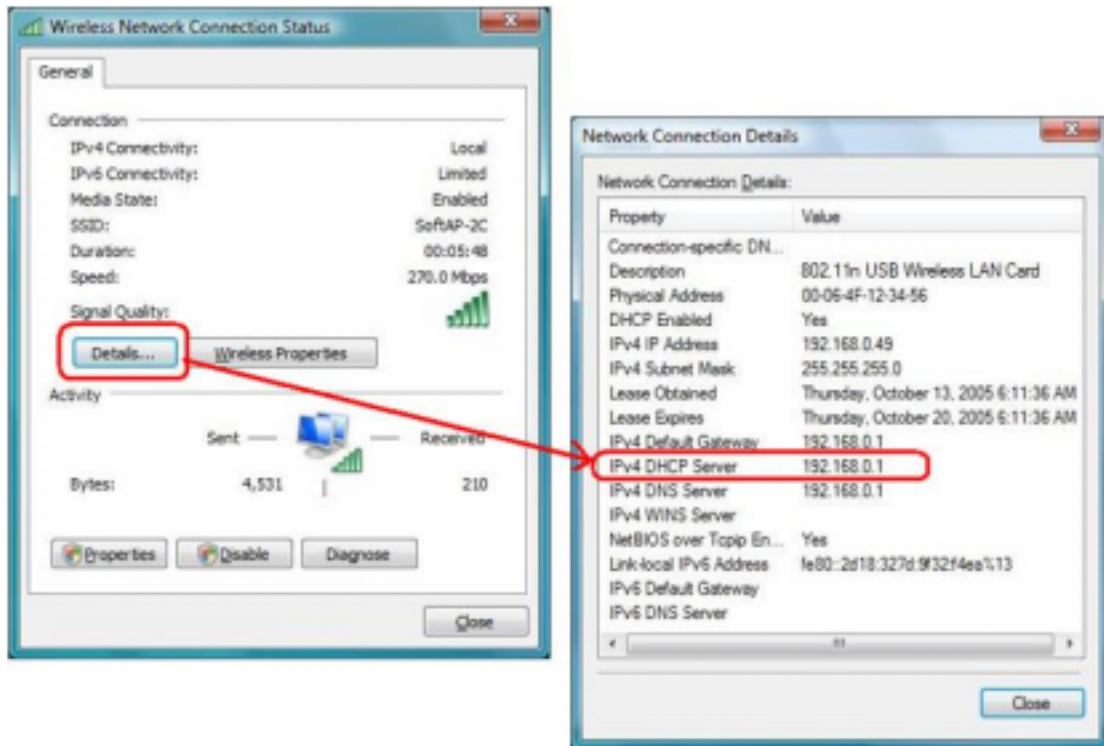
Step 8: Select the network “SoftAP-2C” and click “Connect” to establish the connection.



Step 9: After the computer is successful connected to SoftAP-2C, Network and Sharing Center screen will be shown as below. Click “View Status” to see the detail.

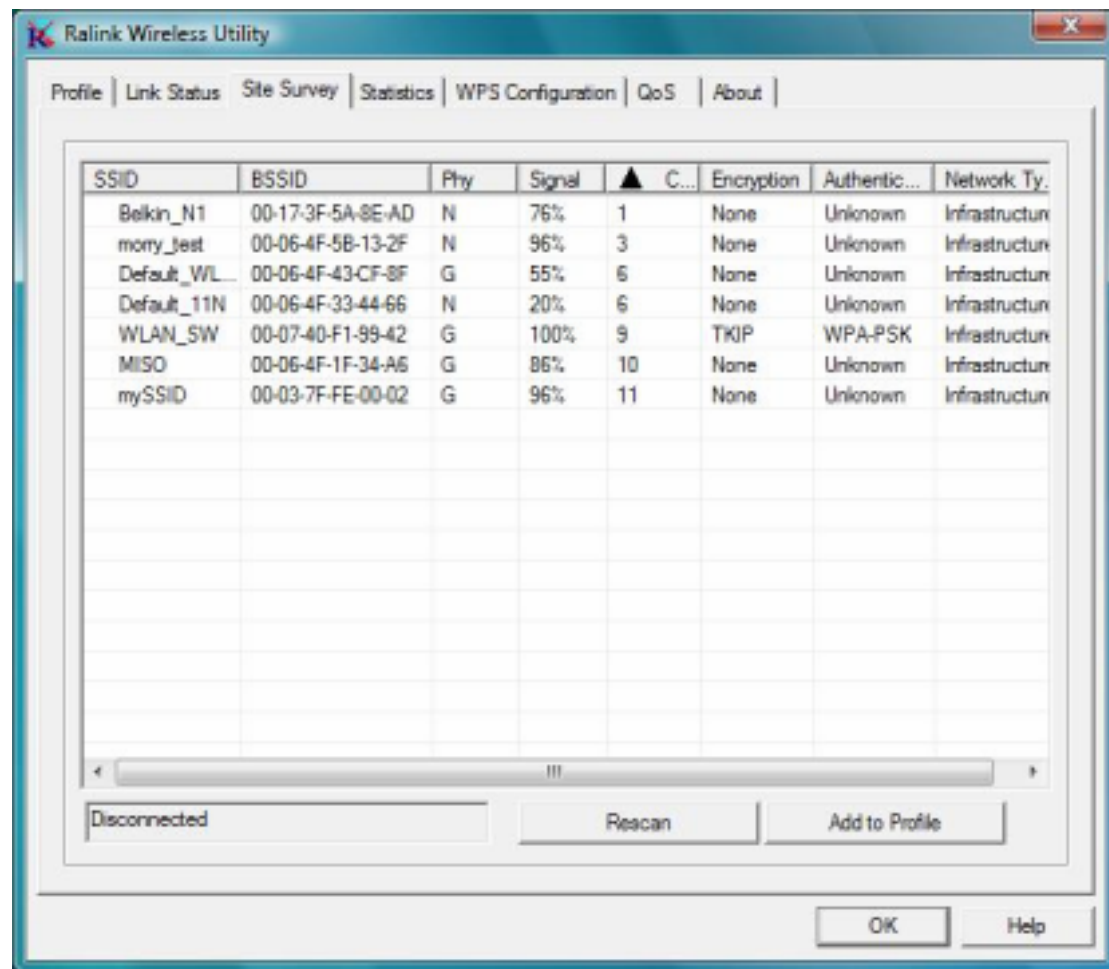


Step 10: In General tab, click “**Detail...**”, and then you can see the current Network connection details. If this computer is successful connect to **SoftAP-2C** Access Point, the **DHCP server** will be assigned to same IP address.



3.2 For Windows Vista

Ralink wireless utility is shown as below. There are 6 setting pages in Ralink wireless utility:

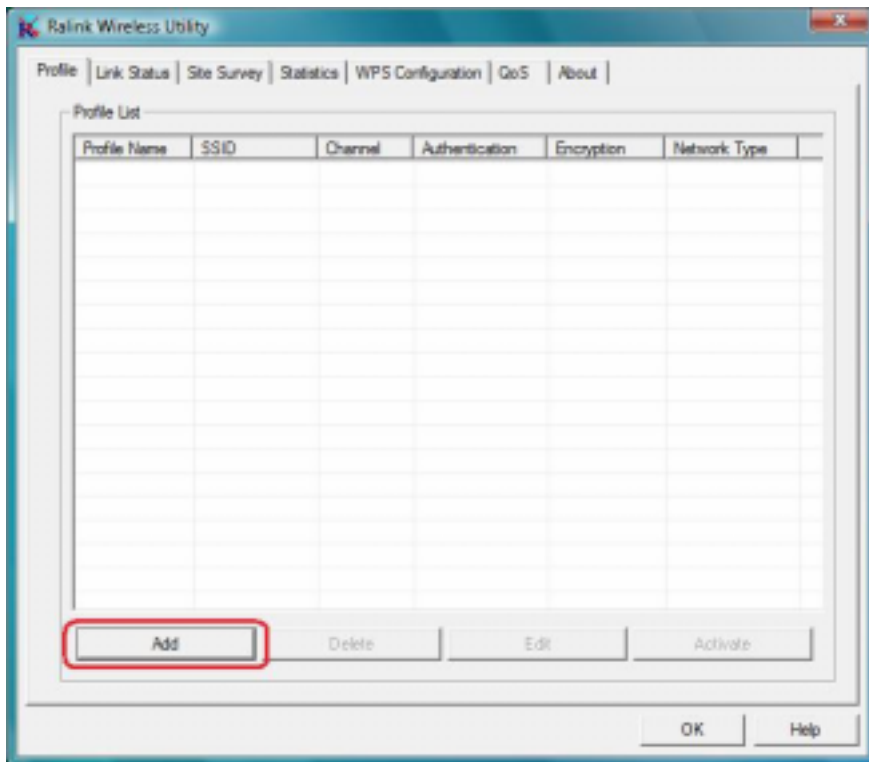


- **Profile** Page: Manage the profile.
- **Link Status** Page: Display current connection information.
- **Site Survey** Page: Display the available networks.
- **Statistics** Page: Display the packet counters
- **WPS Configuration** Page: Connect to WPS (Wi-Fi Protected Setup) capable APs.
- **QoS** Page: It involves “WMM Enable”, “WMM – Power Save Enable” and DLS setup
- **About** Page: Display Ralink driver and utility information.

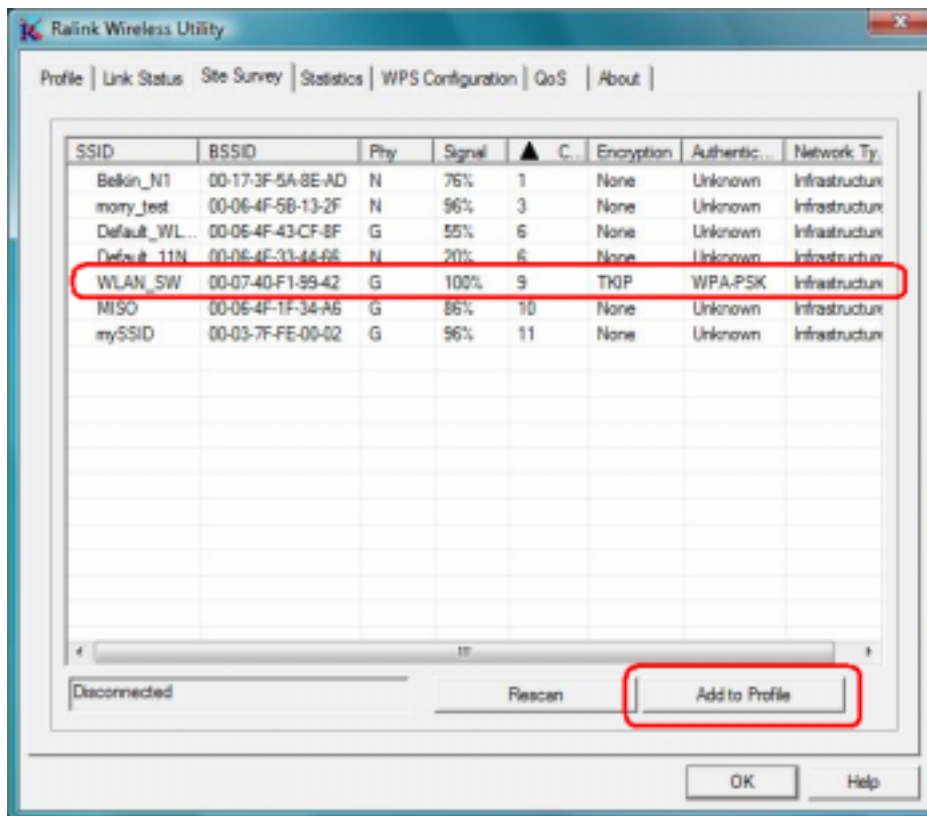
3.2.1 Profile

In the “**Profile**”, you can view and manage the current using Available Point(s). You can **Add**, **Delete**, **Edit**, or **Activate** the current Available Point(s). Also you can duplicate the AP or set current AP as Default.

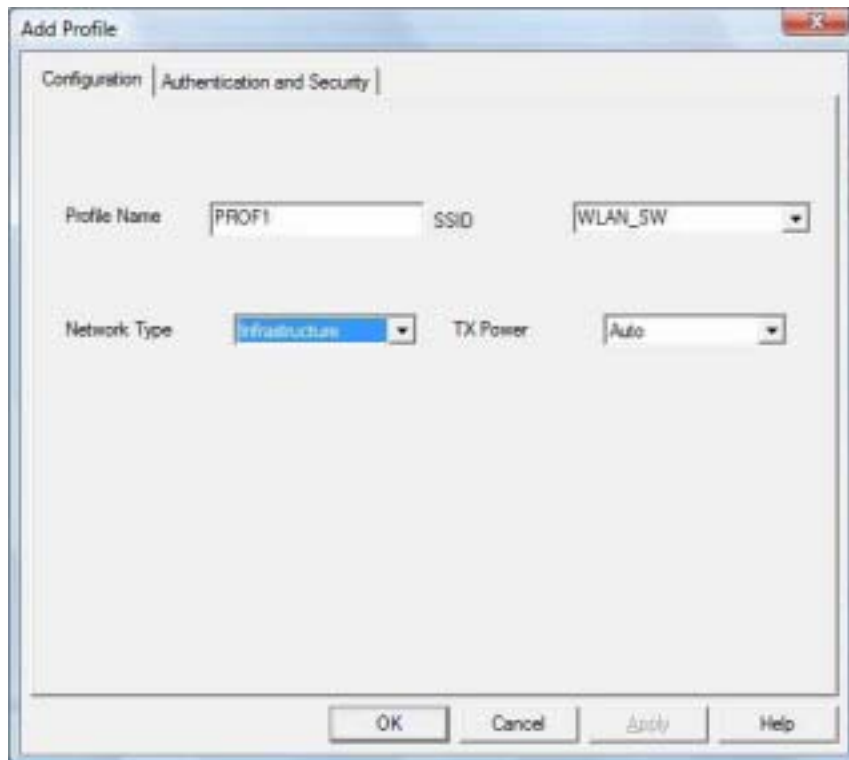
3.2.1.1 Add a profile



By either pushing the **“Add”** button on Profile Page or the **“Add to Profile”** button on Site Survey Page, it brings up the profile setting sheet which contains two setting pages -- **“Configuration”** page and **“Authentication and Security”** page.

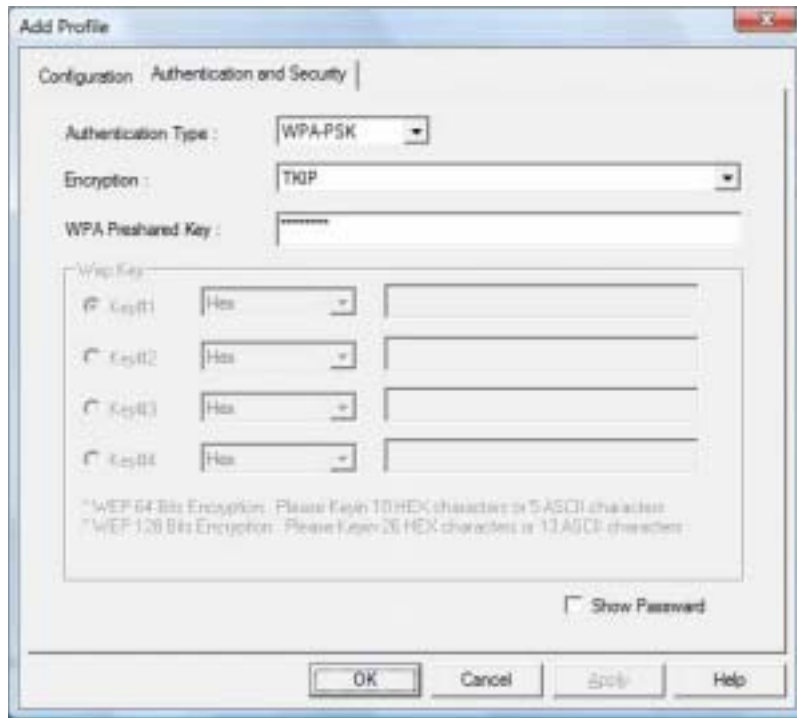


[Configuration page]



- Profile Name: Name of the profile
- SSID: Name of the desire network
- Network Type: Netowork of the desired network, either infrastructure or Ad-Hoc.
 - Infrastructure** – This operation mode requires the presence of a wireless Access Point. All communication is done via the Access Point or Router.
 - Ad-Hoc** – Select this mode if you want to connect to another wireless station in the Wireless LAN network without through an Access Point or Router.
- Tx-Power: The desired TX power level; the available options are 100%, 75%, 50% and Auto. If you want to lower the transmit power of the adapter for saving the power of the system, you can select the lower percentages from the list. The lower power will cause the lower signal strength and the coverage range.

[Authentication and Security page]



- **Authentication Type:** The authentication of the desired network. For infrastructure network, the available modes are Open, Shared, WPA, WPA-PSK, WPA2, and WPA2-PSK.

Open: No authentication is needed among the wireless devices.

Shared: Only Wireless device using a shared key (WEP Key identified) is allowed to connecting each other. Setup the same key as the wireless device that the adapter intends to connect.

WPA: WPA provides a scheme of mutual authentication using either IEEE 802.1x/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. It provides a high level of assurance to enterprise, small business and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.

WPA-PSK – It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each wireless station in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.

WPA2 – Like WPA, WPA2 supports IEEE 802.1x/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Advanced Encryption Standard (AES). AES is required to the corporate user or government users. The difference between WPA and WPA2 is that WPA2 provides data encryption via the AES. In contrast, WPA uses Temporal Key Integrity Protocol (TKIP).

WPA2-PSK – WPA2-PSK is also for home and small business. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data encryption via the AES. In contrast, WPA-PSK uses Temporal Key Integrity Protocol (TKIP).

■ **Encryption:** The encryption of the desired network.

-- For Open and Shared authentications, the available encryption modes are **None** and **WEP**.

-- For WPA, WPA-PSK, WPA2 and WPA2-PSK authentications, the available modes are **TKIP** and **AES**.

None – Disable the Encryption mode.

WEP – Enabled the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Key Length & the key Index.

TKIP – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10000 packets (a packet is a kind of message transmitted over a network). This insures much greater security than the standard WEP security.

AES – AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network.

Note: All devices in the network should use the same encryption method to ensure the communication.

■ **WPA Pre-Shared Key:** The WPA-PSK key can be from 8 to 64 characters and can be letters or numbers. This same key must be used on all of the wireless stations in the network.

■ **WEP Key (Key1~Key4):** The WEP keys are used to encrypt data transmitted in the wireless network. There are two types of key length: 64-bit & 128-bit. Select the default encryption key from key1 to key4 by selected the radio button.

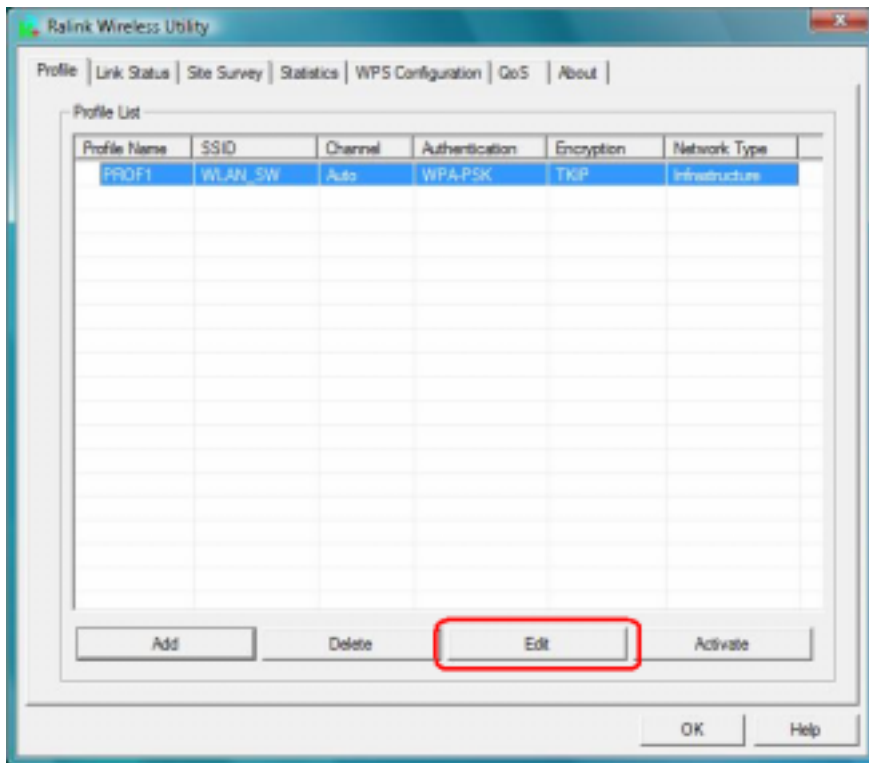
Fill the text box by following the rule below:

64-bit – Input 10-digit Hex values (in the “**A-F**”, “**a-f**”, and “**0-9**” range) or 5-digit ASCII characters (including “**a-z**” and “**0-9**”) as the encryption keys. For example: “**0123456aef**” or “**test1**”

128-bit – Input 26-digit Hex values (in the “**A-F**”, “**a-f**”, and “**0-9**” range) or 13-digit ASCII characters (including “**a-z**” and “**0-9**”) as the encryption keys. For example: “**01234567890123456789abcdef**” or “**administrator**”.

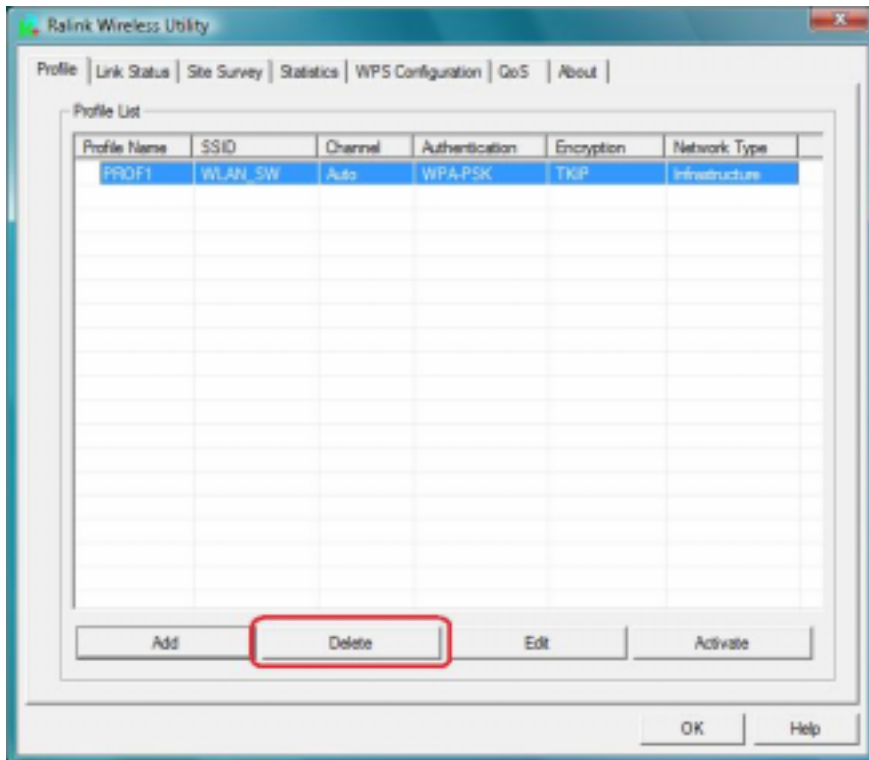
3.2.1.2 Edit a profile

Selecting an existing profile then clicking the “Edit” button on Profile Page brings up the profile setting sheet filled with the profile information for user modification.



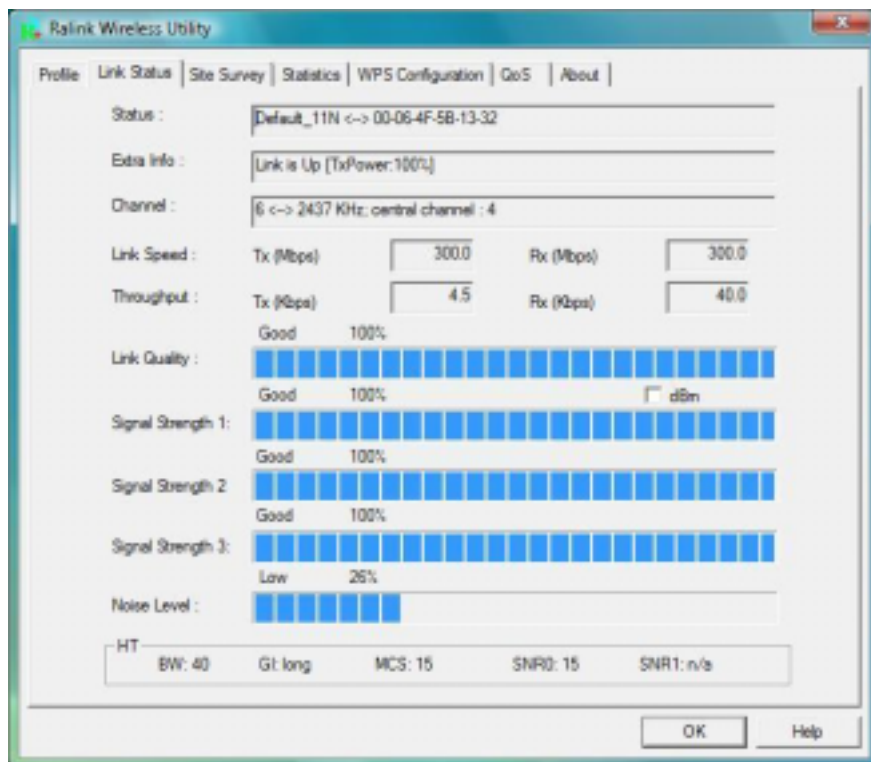
3.2.1.3 Delete a profile

Selecting an existing profile then clicking the “Delete” button on Profile Page to deletes the profile.

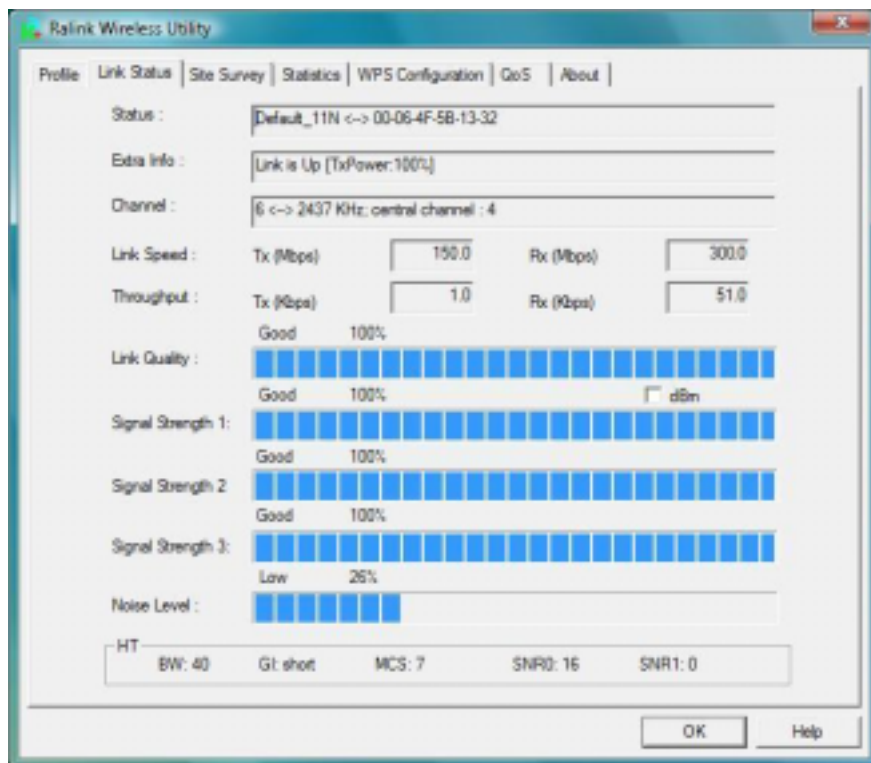


3.2.2 Link Status

In this section, you can immediately monitor the current connected link status, such as Link Speed, Throughput, Link Quality, Signal Strength, Noise Level ...etc.



(for Tx Link Speed up to 300 Mbps model)



(for Tx Link Speed up to 150 Mbps model)

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

Extra Info: Display the link status and current channel in use.

Channel: Display the number of the radio channel and the frequency used for the networking.

Link Speed (Mbps): Display the transmission and reception rate of the network. The maximum transmission rate is 300/150Mbps (depend on model).

Throughput (Kbits/sec): Display transmits and receives throughput in unit of K bits/sec.

Link Quality: Display connection quality based on signal strength and TX/RX packet error rate.

dBm: If you want to know the signal strength in the unit of dBm, select the check box.

Signal Strength: Receive signal strength, user can choose to display as percentage or dBm format.

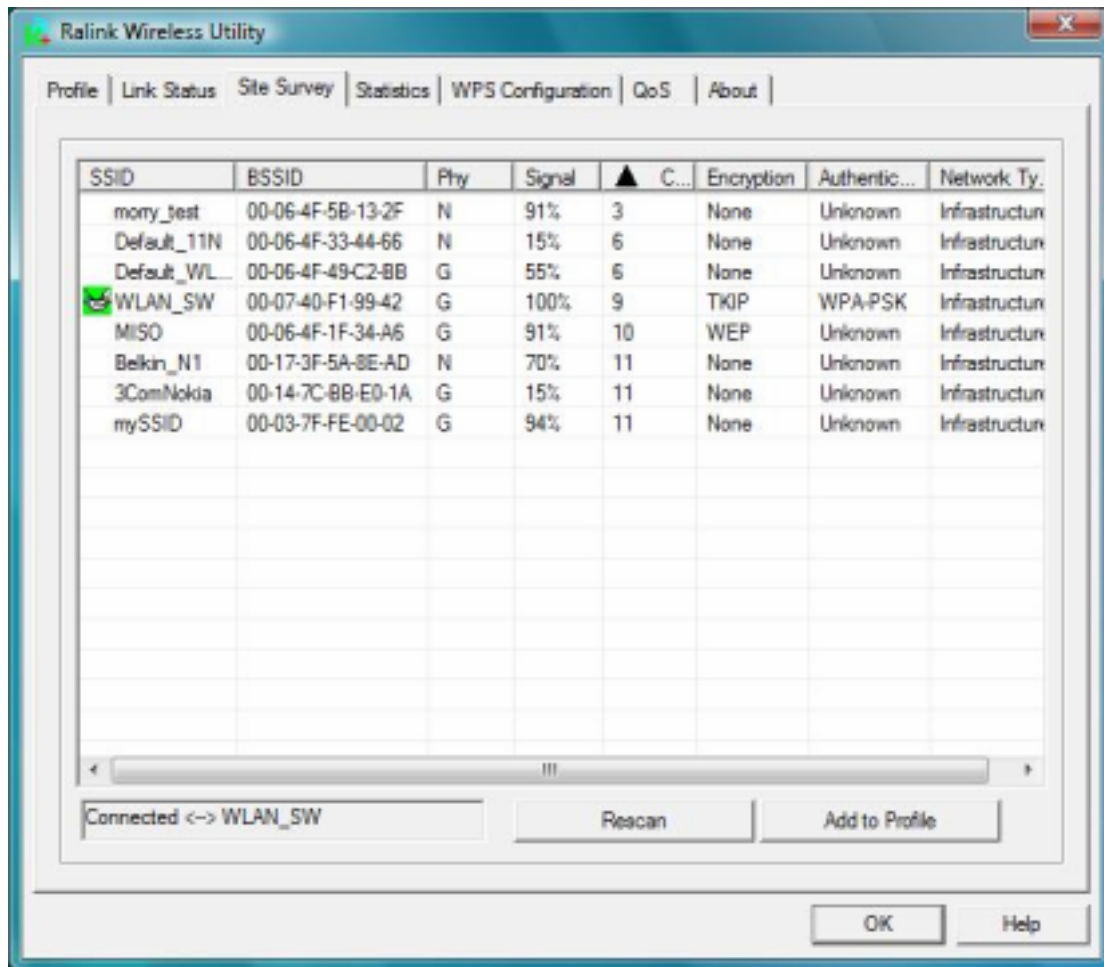
Signal Strength2: Receive signal strength 2, user can choose to display as percentage or dBm format.

Noise Level: Display the noise signal strength.

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

3.2.3 Site Survey

When you open the Configuration Utility, the system will scan all the channels to find all the access points/stations within the accessible range of your adapter and automatically connect to the wireless device with the highest signal strength. From the “**Site Survey**”, all the network nearby will be listed. You can change the connection to another network or add one of the networks to your own profile list.



SSID: Name of BBS of IBSS network.

BSSID: MAC address of AP or randomly generated of IBSS.

Signal: Receive signal strength of specified network.

Channel: Channel in use.

Encryption: Encryption algorithm used within than BBS or IBSS. Valid value includes WEP, TKIP, AES, and Not Use.

Authentication: Authentication mode used within then network, including Unknown, WPA-PSK, WPA2-PSK, WPA and WPA2.

Network Type: Network type in use, Infrastructure or Ad-Hoc.

Rescan: Issue an rescan command to wireless NIC to update information on surrounding wireless network.

Re-Scanning: Clicking the re-scan button to perform the re-scanning action.


Add to Profile: Add the selected AP to Profile setting. It will bring up profile page and save user's setting to a new profile.

[Connect A Network]

(1) When Raconfig first ran, it will select the best AP to connect automatically.

(2) If user wants to connect to other AP, he can double-click mouse on the intended AP to make connection.

(3) If the intended network has encryption other than “Not Use”, Raconfig will bring up the security page and let use input the appropriate information to make the connection.

 This icon indicates the changes is successful.

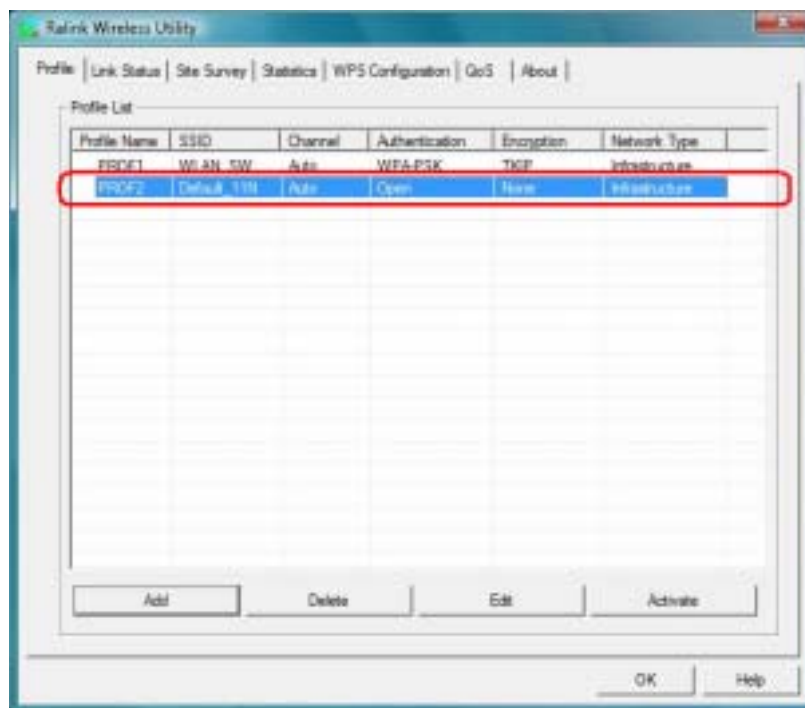
⦿ Example 1: Open and Non-Encrypted

Step 1 – Choose “Open” authentication type

Step 2 – Choose “None” encryption type



Step 3 – After the profile is saved, click “Activate” button on Profile Page to activate the profile.

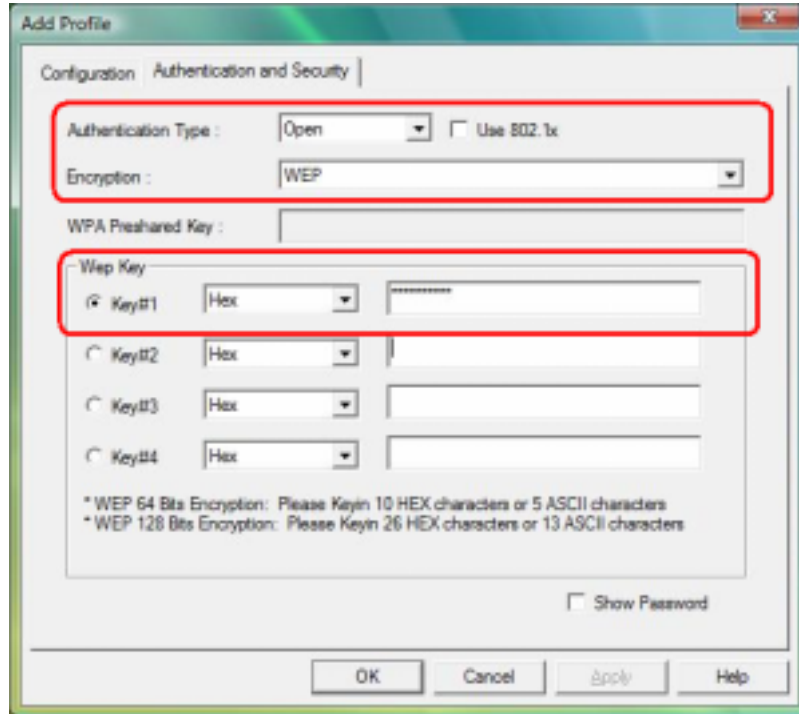


① **Example 2: WEP-Encrypted**

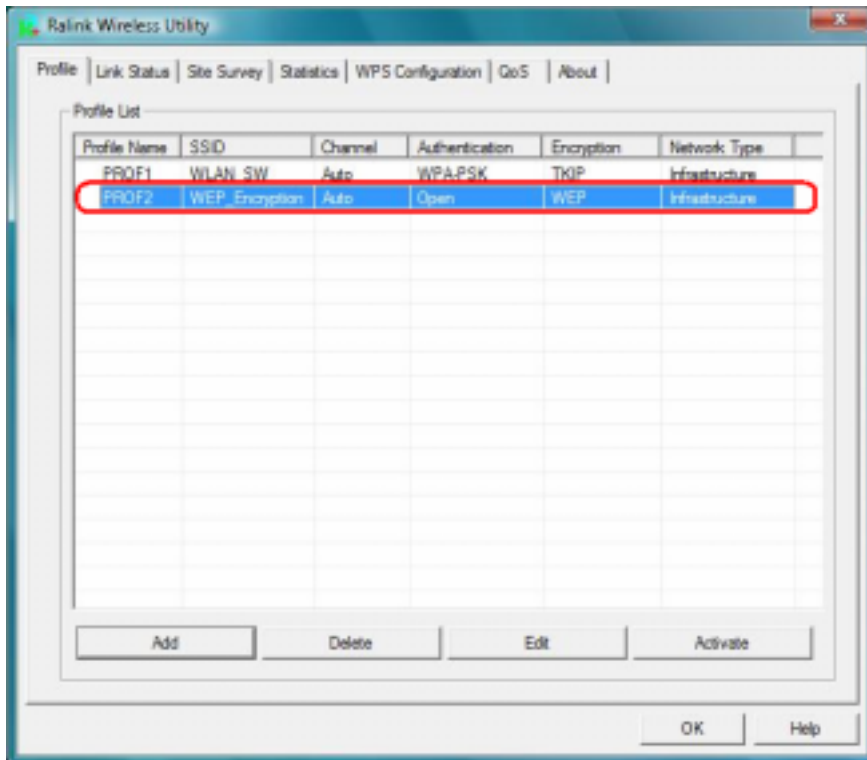
Step 1 – Choose “**Open**” or “**Shared**” authentication type

Step 2 – Choose “**WEP**” encryption type

Step 3 –Enter the WEP KEY



Step 4 –After the profile is saved, click the “**Activate**” button on Profile Page to activate the profile.

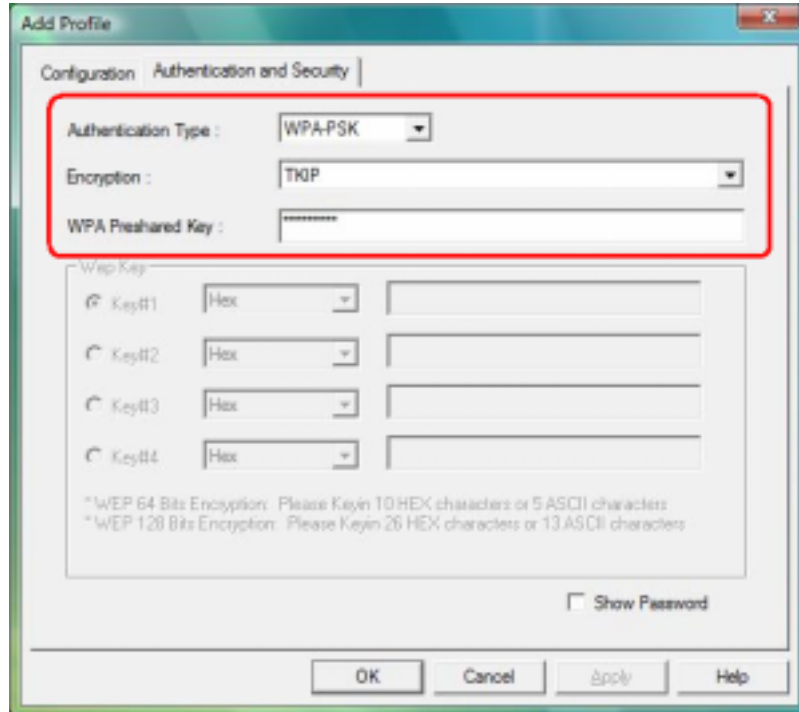


③ **Example 3: WPA-PSK/WPA2-PSK**

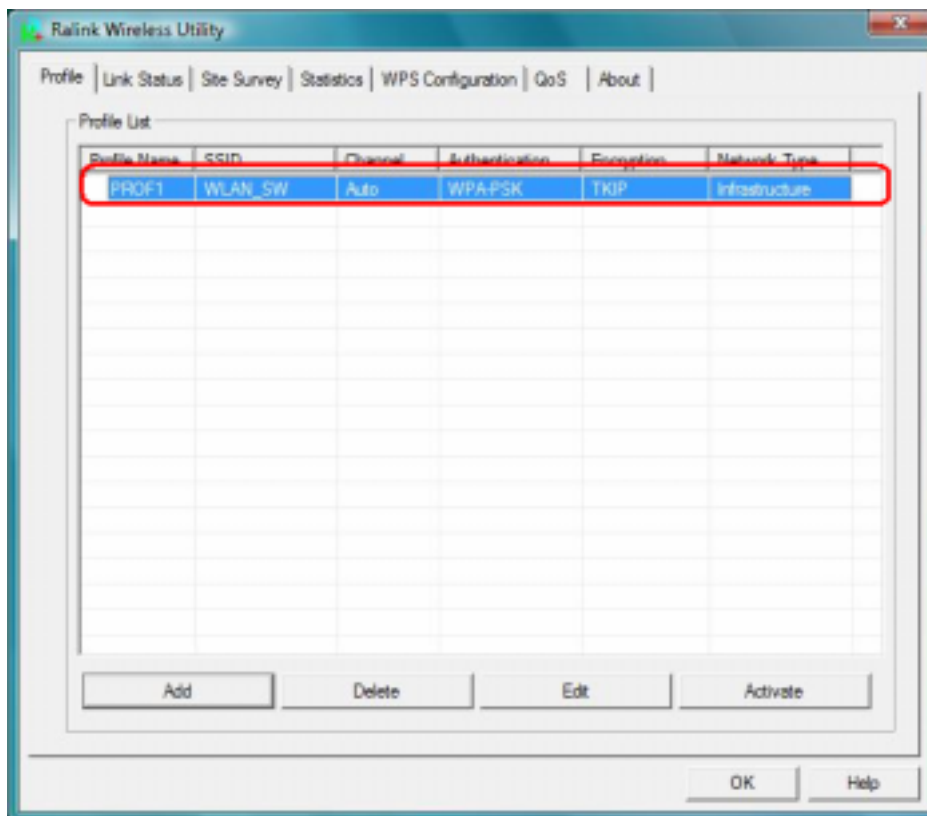
Step 1 – Choose “WPA-PSK” or “WPA2-PSK” authentication type

Step 2 – Choose “TKIP” or “AES” encryption type

Step 3 –Enter the pre-shared KEY



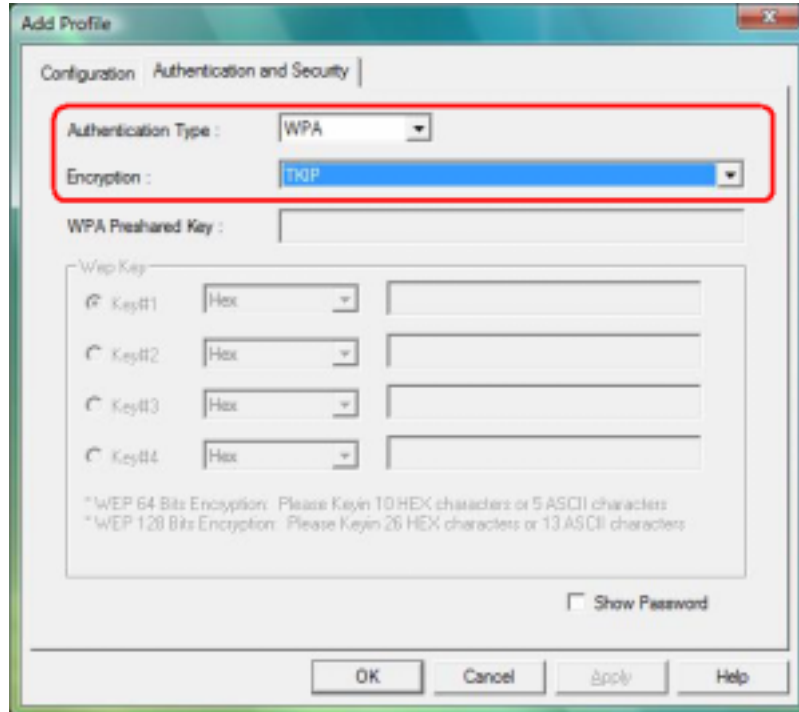
Step 4 –After the profile is saved, click the “**Activate**” button on Profile Page to active the profile.



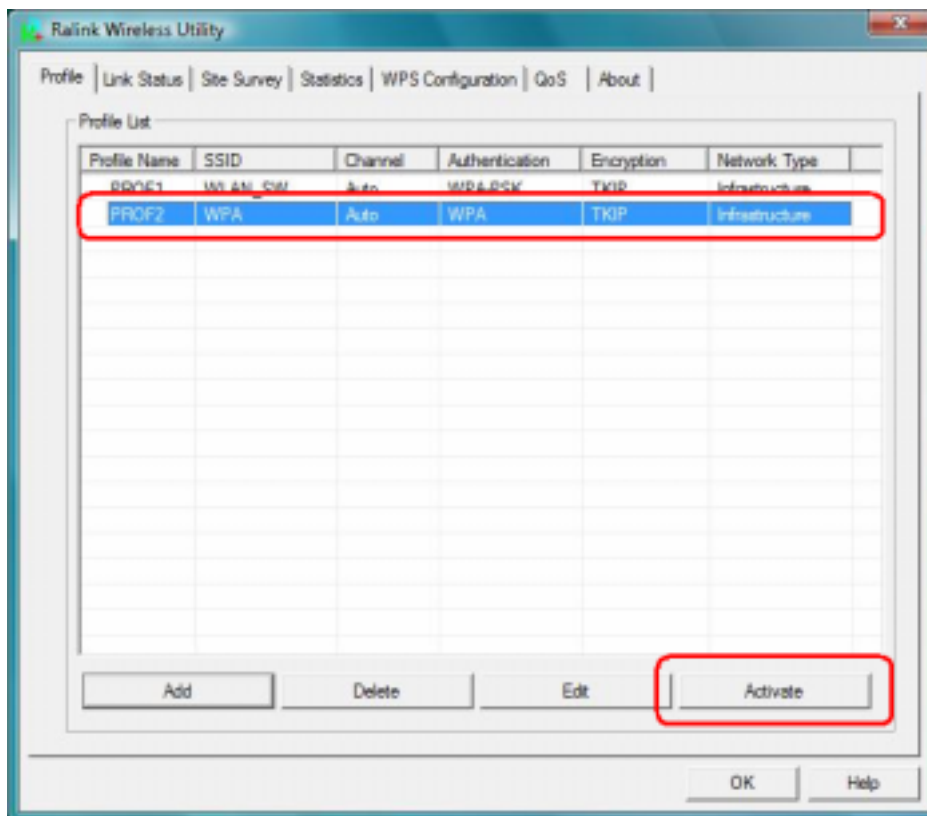
④ **Example 4:WPA/WPA2**

Step 1 – Choose “WPA” or “WPA2” authentication type

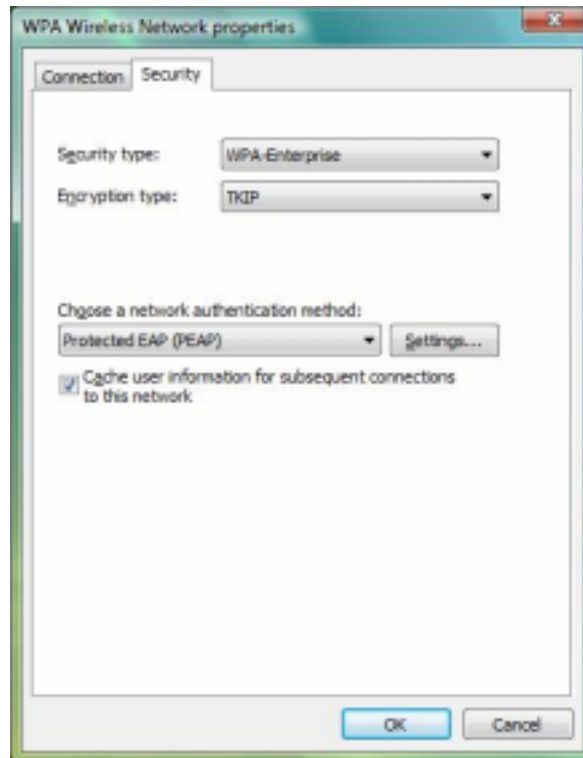
Step 2 – Choose “TKIP” or “AES” encryption type



Step 3 –After the profile is saved, click the “**Activate**” button on Profile Page to active the profile.

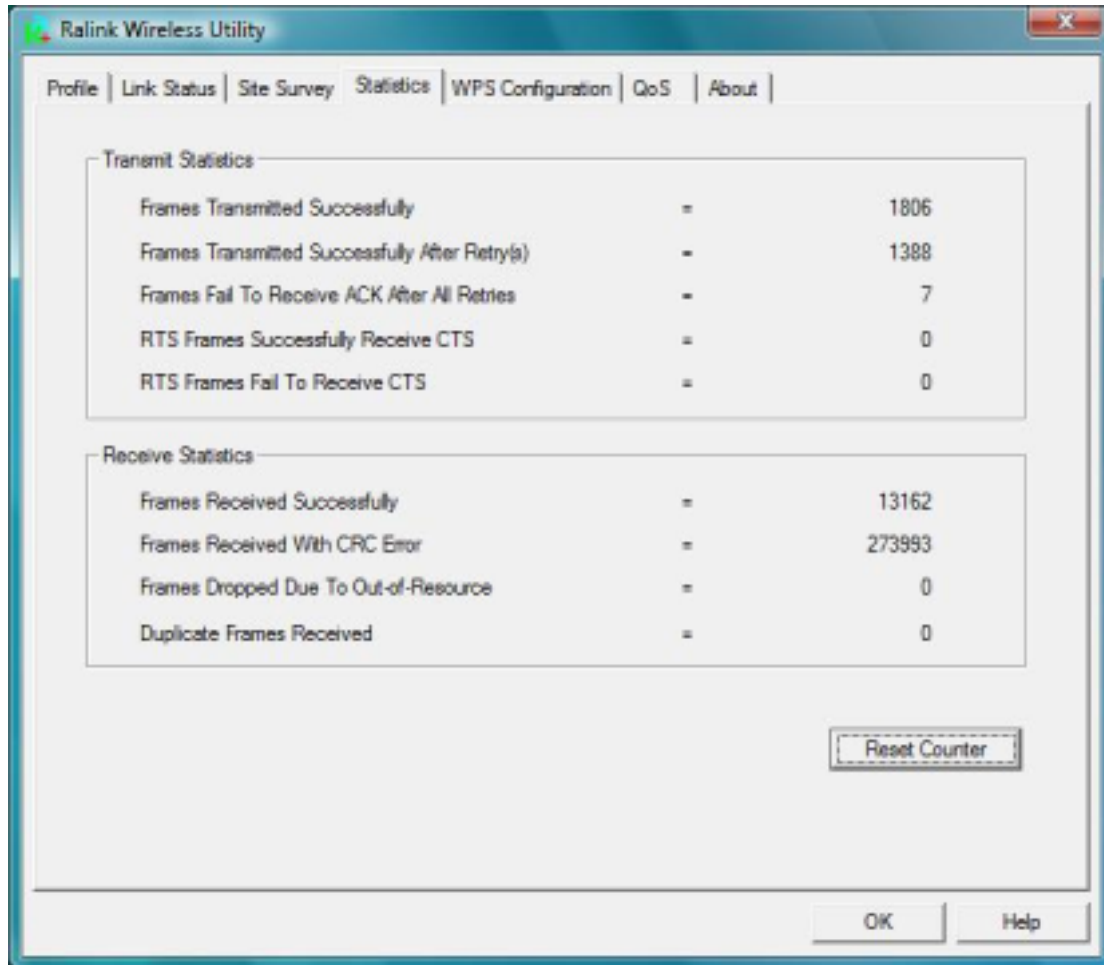


Step 4 –The Windows profile setting dialog is popped-up for user to modify.



3.2.4 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. You may reset the counters to Zero by clicking "**Reset Counter**".



[Transmit Statistics]

Frames Transmitted Successfully: Frames successfully sent

Frames Transmitted Successfully After Retry: Frames sent successfully with retry.

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 frames.

RTS Frames Fail To Receive CTS: Failed to receive CTS after sending RTS frames.

[Receive Statistics]

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.