RT3072 USB Adapter User Manual

Contents:

1.0 Introduction

Thank you for purchasing the RT3072 USB Adapter. The RT3072 USB Adapter is a cost-effective product with high performance standards. This solidly profiled wireless adapter will allow you to seamlessly submerse yourself in the wireless world with ease and efficiency.

1.1 Compatibility

The adapter supports all IEEE 802.11 b/g protocols that pass the Wi-Fi tests. It's compatible with all Wi-Fi enabled products with a Wi-Fi logo. Use the adapter to connect to any broadcasting wireless network. The device also provides all data rates in IEE 802.11 b/g standards, with both short and long preambles to ensure its compatibility with both legacy and new wireless products. This saves end users the hassle of finding compatible products.

1.2 Security

We know the security of your network is important to you. This is why the RT3072 provides you with full security coverage from 64/128bit WEP encryptions and second generation WPA-PSK encryptions to the most advanced WPA2-AES encryptions. WPA2 is the latest security standard approved by Wi-Fi standards.

1.3 Features

The RT3072 USB Adapter offers many useful features. These features include, but are not limited to the following: Saving Mode, Adhoc Wireless Lan, and Wake on Lan (WOL). Please read this manual thoroughly to learn how to use all the features the R3072 has to offer.

1.4 Warnings and Disclaimer

To comply with the FCC RF exposure compliance requirements, no changes to the antenna or the device by the user are permitted. Any changes to the antenna or device by the user many result in the device exceeding the RF exposure requirements and void the user's authority to operate the device. This manual provides detailed user guidelines for the set-up and operation of the RT3072 USB Adapter. Though every effort has been made to ensure this document is up-to-date and accurate, more information may have become available subsequent to the production of this guide. If you have any questions or concerns regarding this product that are not resolved by this manual please contact the seller for tech support.

2.0 Specifications

2.1 Host System Connections

Interface	Fully complies with USB 2.0 or 1.1
USB Data Transfer Rate	USB high speed (480 Mbps) and full speed (12Mbps)

2.2 Wireless LAN (WLAN) Environment Connections

WLAN Interface	Multimode features
	Fully complies with IEEE 802.11 b/g specifications
WLAN Transfer Rate	802.11 b:DQPSK with data scrambling capability to provide data rates of 1,2,5.5, and 11Mbps
	802.11 g: A high speed Fast Fourier
	Transform(FFT)/ Inverse Fast Fourier Transform(IFFT) provides a data rate transfer of 6,9,12,18,24,36,48, and 54Mbps
WLAN Frequency Band	2.4 ~ 2.497 GHz (Industrial Scientific Medical Band)
Operation Channel	Channel 1~11
Coverage Area	Indoors: 100ft with straight path
Compatibility	Fully compatible to IEEE 802.11 b/g devices
Security	Hardware-based IEEE 802.11i encryption/decryption engine, including 64-bit/128-bit WEP, TKIP, and AES
Antenna	Detachable dipolar antenna

2.3 System Requirements

The RT3072 is compatible with the following Windows systems: Windows 98SE, Me, 2000, XP, Windows 7, and Windows 64 bit. It is also compatible with Mac OS and Linux. PCs must have a device driver installed that allows you to communicate with WLAN Mini USB adapter.

2.4 Package Contents

The following items should be included in your package 1 RT3072 USB Adapter, 1 Installation Software CD, and 1 USB Cable.
If an item is missing or damaged please contact the seller for a replacement.

3.0 RT3072 Installation and Removal

Warning: *Do not cover or block the airflow to the adapter; the adapter with reach a high temperature during use.*

3.1 Installation

The instructions listed below are for Windows XP but procedures are similar for Windows 98SE/Me/2000/and 7. If you previously installed a WLAN driver and utility please uninstall the old version before installing the RT3072. Once the aforementioned guidelines have been met follow the instructions listed below to install the device.

1. ***Do not*** plug the wireless LAN USB adapter into your computer's USB port before installing the software program.
2. Insert the provided installation disk into your computer. An auto installation window will appear. When the following screen appears click **Driver Installation**.
3. Choose a setup language from the menu then click **Next** to proceed.
4. The system with start the software installation for the WLAN USB adapter.
5. If the windows logo software installation screen appears click **Continue Anway** to proceed. This message will not appear for all drivers.
6. Click **Finish** to complete the installation.
7. After clicking **Finish** to complete the installation the dialog box will disappear. Go to your **Start** menu and click on **All Programs**, if "Ralink Wireless" is an option the program installed correctly.
8. Insert the wireless LAN USB adapter into your computer's USB port; the computer will detect and activate the adapter automatically.

3.2 Uninstalling the Device

There are two options for removing the device software from your computer. Take the following steps to remove the device software from your computer.

1. Go to Control Panel > Add or Remove Program > select Change or Remove Programs on left panel > select Ralink RT3072 wireless LAN Card > click on Remove button > follow prompts to remove program.
2. Go to Start > All Programs > Ralink Wireless > Uninstall > Click on when it prompts you to "Confirm Uninstall" > click Finish to complete the removal process

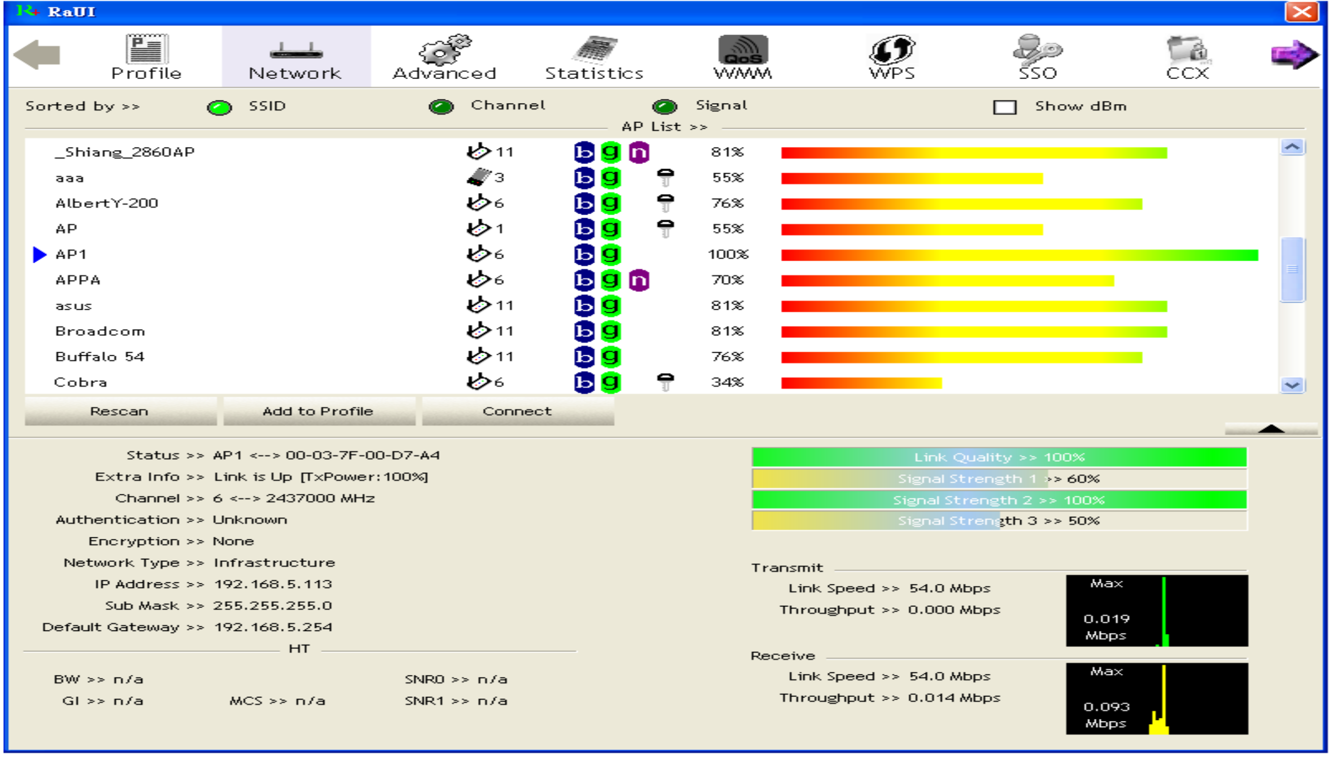
Appendix 1: How to use RaUL for Windows Vista, XP, and Windows 7

1.0 Ralink Wireless Utility (RaUI)

1.1 Starting RaUI

When starting RaUI, the system will connect to the AP with the best signal strength without setting a profile or matching a profile setting. When starting RaUI, it will issue a scan command to a wireless NIC. After two seconds, the AP list will be updated with the results of a BSS list scan. The AP list includes most used fields, such as SSID, network type, channel used, wireless mode, security status, and the signal percentage. The arrow icon indicates the connected BSS or IBSS network. The dialog box is shown in Figure 1.1A below.

Figure 1.1A The RaUI dialog box:



SSID	Channel			Signal
_Shiang_2860AP	11	b g n		81%
aaa	3	b g	🔑	55%
AlbertY-200	6	b g	🔑	76%
AP	1	b g	🔑	55%
▶ AP1	6	b g		100%
APPA	6	b g n		70%
asus	11	b g		81%
Broadcom	11	b g		81%
Buffalo 54	11	b g		76%
Cobra	6	b g	🔑	34%

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> None
Network Type >> Infrastructure
IP Address >> 192.168.5.113
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 60%
Signal Strength 2 >> 100%
Signal Strength 3 >> 50%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps

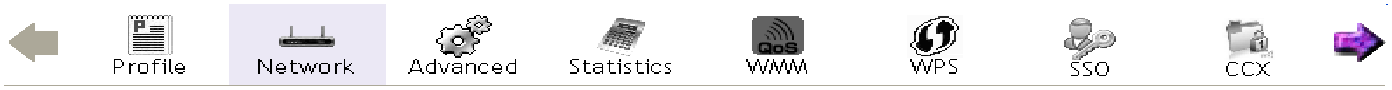
Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.014 Mbps

Figure 1.1A Description- how to read/ navigate the dialog box:

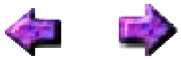
There are three sections to the RaUI dialog box. These sections are briefly described below.

① Button Section: Include buttons for selecting the Profile page, Network page, Advanced page, Statistics page, WMM page, WPS page, the About button, Radio On/Off button and Help.

Figure 1.1B Button Section:



1.1-3 Navigation Arrows:
Use to move menu left and right



② Function Section: This section includes information about the profile, network, advanced settings, statistics, WMM, WPS, and about options on the menu bar. After you select an option from the menu bar shown above a corresponding dialog box will appear with information and options related to your selection. Each option is explained in detail in sections 1.2 to 1.10.

③ Status Section: This section includes information about the link status, authentication status, AP's information and configuration, and retrying the connection when authentication fails. Each option is explained in detail in sections 1.11-1.13.

When starting RaUI a small Ralink icon appears in the notifications area of the taskbar, as shown in Figure 1.1B below. You can double click it to maximize the dialog box if you selected to close it earlier. You may also right click to close the RaUI utility.

Figure 1.1B Ralink Icon:

Additionally, the Ralink (R+) icon will change color to reflect current wireless network connection status. The status symbols are shown below:

R+ Indicates the connection and signal strength are good.

R+ Indicates the connection and signal strength are normal.

R+ Indicates that it is not yet connected.

R+ Indicates that a wireless NIC cannot be detected.

R+ Indicates that the connection and signal strength are weak.

1.2 Profile:

The Profile List keeps a record of your favorite wireless settings at home, in the office, and other public hot-spots. You can save multiple profiles and activate the correct one at your preference. Figure 1.2-1 shows the basic profile section.

Figure 1.2-A Profile Function:

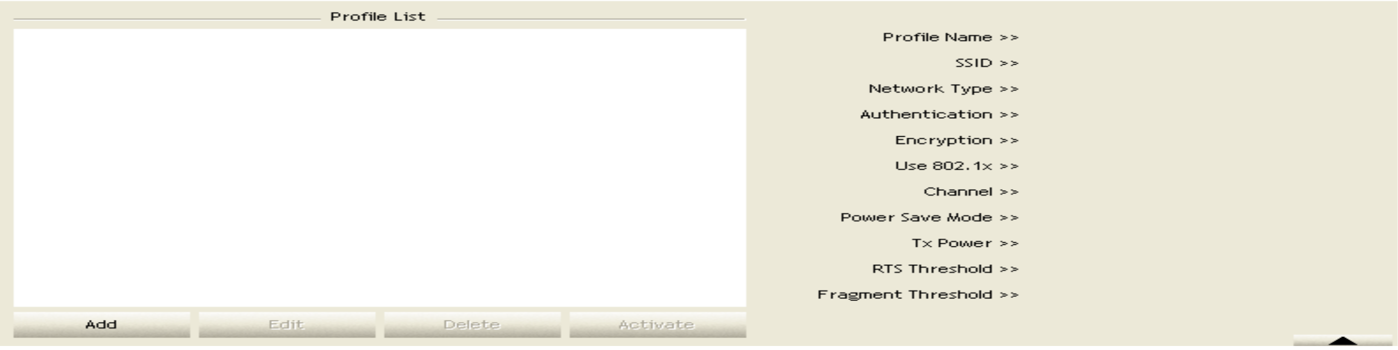


Figure 1.2-ADescription of Fields:

① Profile Name: Name of profile, preset to PROF* (* indicate 1, 2, 3...).
② SSID: The access point or Ad-hoc name.
③ Network Type: Indicates the networks type, including infrastructure and Ad-Hoc.
④ Authentication: Indicates the authentication mode used.
⑤ Encryption: Indicates the encryption Type used.
⑥ Use 802.1x: Shows if the 802.1x feature is used or not.
⑦ Cannel: Channel in use for Ad-Hoc mode.
⑧ Power Save Mode: Choose from CAM (Constantly Awake Mode) or Power Saving Mode.
⑨ Tx Power: Transmitting power, the amount of power used by a radio transceiver to send the signal out.
⑩ RTS Threshold: Users can adjust the RTS threshold number by sliding the bar or keying in the value directly.
⑪ Fragment Threshold: The user can adjust the Fragment threshold number by sliding the bar or key in the value directly.

Figure 1.2-A Description of icons and buttons:

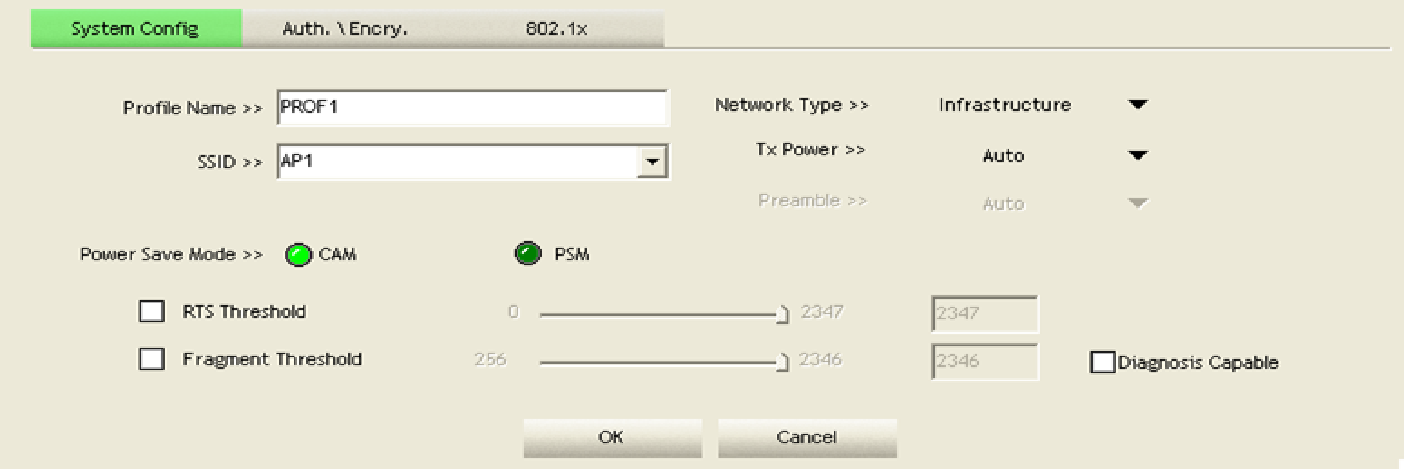
① ▶ Indicates if a connection is made from the currently activated profile.
② ▶ Indicates if the connection has failed on a currently activated profile.
③ Indicates the network type is infrastructure mode.
④ Indicates the network type is in Ad-hoc mode.
⑤ Indicates if the network is security-enabled.
⑥ Add Click to add a new profile.
⑦ Edit Click to edit an existing profile.
⑧ Delete Click to delete an existing profile.
⑨ Activate Activates selected profile.
⑩ ▼ Shows information of the related status section.
⑪ ▲ hides information of the related status section

1.2-1 Add/Edit Profile

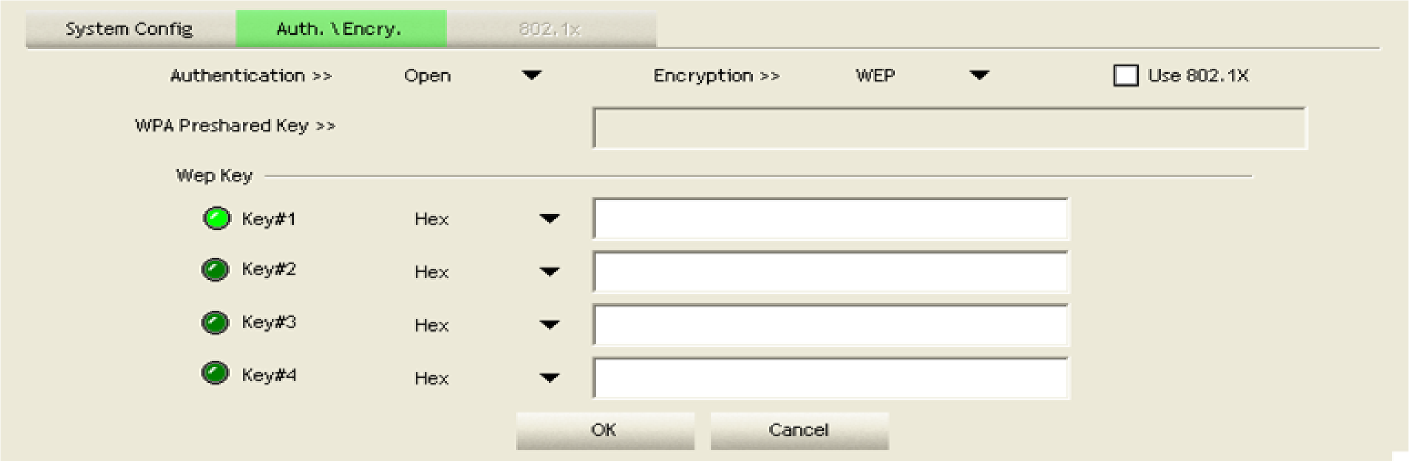
Listed below are the three methods for opening the Profile Editor Dialog box.

1. Open it by clicking the "Add to Profile" button in the Site Survey tab.
2. Open it by clicking the "Add" button in the Profile tab.
3. Open it by clicking the "Edit" button on the Profile tab.

Figure 1.2-1A Configuration:



Profile Name >> PROF1
SSID >> AP1
Network Type >> Infrastructure
Tx Power >> Auto
Preamble >> Auto
Power Save Mode >> ● CAM ● PSM
☐ RTS Threshold 0 2347 2347
☐ Fragment Threshold 256 2346 2346
☐ Diagnosis Capable



Authentication >> Open

Encryption >> WEP

☐ Use 802.1X

WPA Preshared Key >>

Wep Key

● Key#1 Hex

○ Key#2 Hex

○ Key#3 Hex

○ Key#4 Hex

Figure 1.2-1A Description of Fields:

① Profile Name: The user can chose any name for this profile, or use the default name defined by system.

② SSID: The user can key in the intended SSID name or select one of the available APs from the drop-down list.

③ Power Save Mode: Choose CAM (Constantly Awake Mode) or Power Saving Mode.

④ Network Type: There are two types, infrastructure and 802.11 Ad-hoc mode. Under Ad-hoc mode, user can also choose the preamble type.The available preamble types are auto and long. In addition, the channel field will be available for setup in Ad-hoc mode.

⑤ RTS Threshold: User can adjust the RTS threshold number by sliding the bar, or typing the value directly into the box to the right of the slider. The default value is 2347.

⑥ Fragment Threshold: User can adjust the Fragment threshold number by sliding the bar or typing the value directly into the box to the right of the slider. The default value is 2346.

⑦ Channel: Only available to set when in Ad-hoc mode. Users can choose the channel frequency to start their Ad-hoc network.

⑧ Authentication Type: There are 7 types of authentication modes supported by RaUI. They are: Open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK.

⑨ Encryption Type: For open and shared authentication mode, the selection of available encryption types are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode both TKIP and AES encryption are available.

⑩ 802.1x Setting: See "Section 2-2 802.1x Setting" for further information.

⑪ Pre-shared Key: This is the key shared between AP and STA. For WPA-PSK and WPA2-PSK authentication modes this field must be filled with a key between 8 and 32 characters in length.

⑫ WEP Key: Only valid when using WEP encryption algorithms. The key must be identical to the AP's key. There are several formats to enter the keys as shown below:

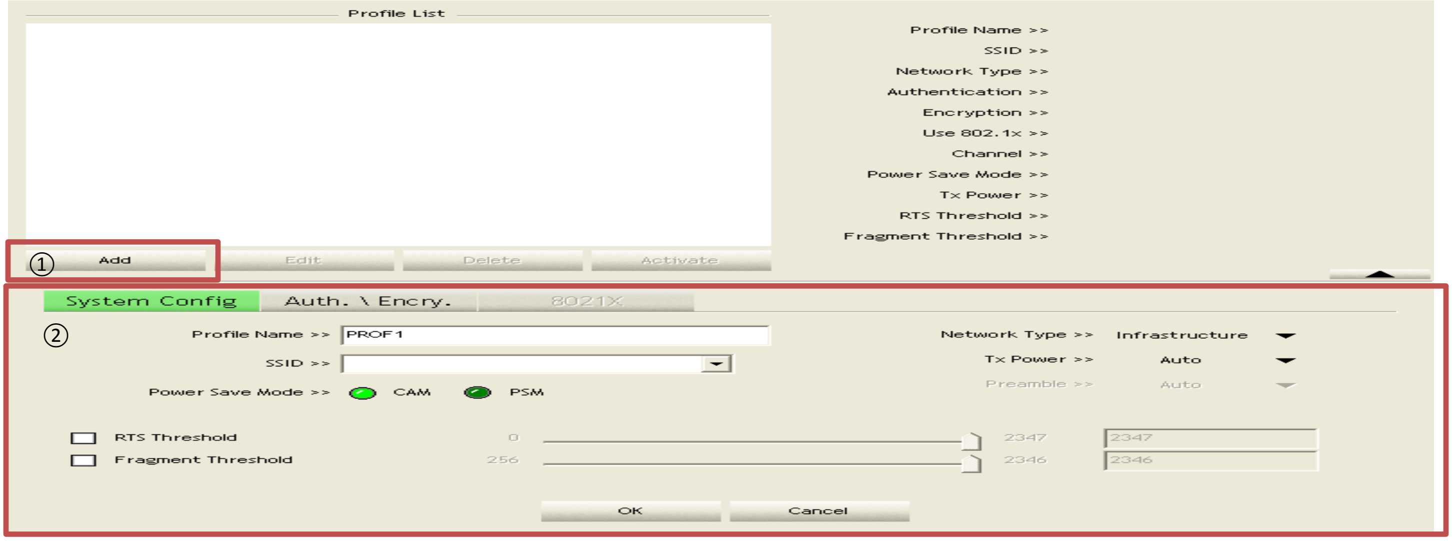
1. Hexadecimal - 40bits : 10 Hex characters
2. Hexadecimal - 128bits : 26 Hex characters.
3. ASCII - 40bits : 5 ASCII characters.
4. ASCII - 128bits : 13 ASCII characters

1.2-2 Example Add Profile

There are four simple steps to add a profile to the list. They are listed below.

① Click “Add” under the profile list box.

②The “ADwill appear below the profile list.



Profile Name >> PROF1

SSID >>

Power Save Mode >> ● CAM ○ PSM

Network Type >> Infrastructure

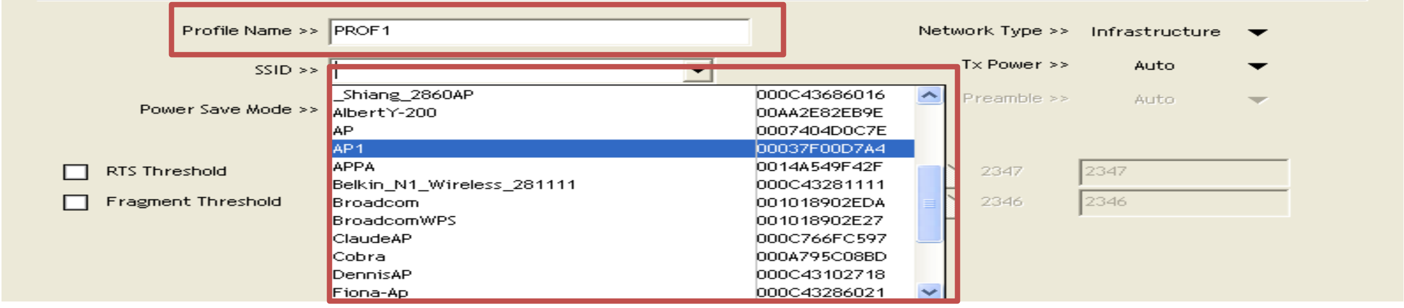
Tx Power >> Auto

Preamble >> Auto

☐ RTS Threshold 0 2347 2347

☐ Fragment Threshold 256 2346 2346

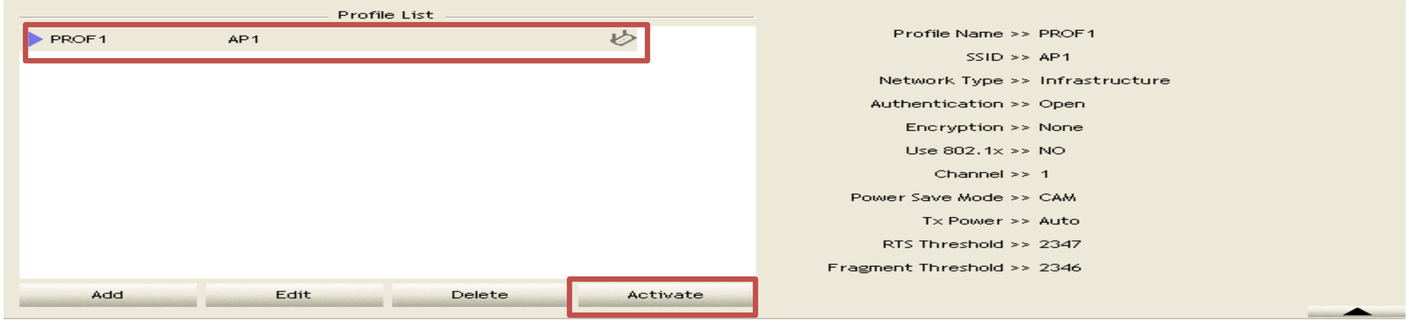
③ Specify a Profile Name. Select an AP from the SSID drop-down list. The AP list is from the last Network.



Profile Name >> PROF1
SSID >>
Power Save Mode >>
☐ RTS Threshold 2347
☐ Fragment Threshold 2346
Network Type >> Infrastructure
Tx Power >> Auto
Preamble >> Auto

_Shiang_2860AP	000C43686016
AlbertY-200	00AA2E82EB9E
AP	0007404D0C7E
AP1	00037F00D7A4
APPA	0014A549F42F
Belkin_N1_Wireless_281111	000C43281111
Broadcom	001018902EDA
BroadcomWPS	001018902E27
ClaudeAP	000C766FC597
Cobra	000A795C08BD
DennisAP	000C43102718
Fiona-Ap	000C43286021

④ Now the profile the user set will appear in the profile list box. Click "Activate".



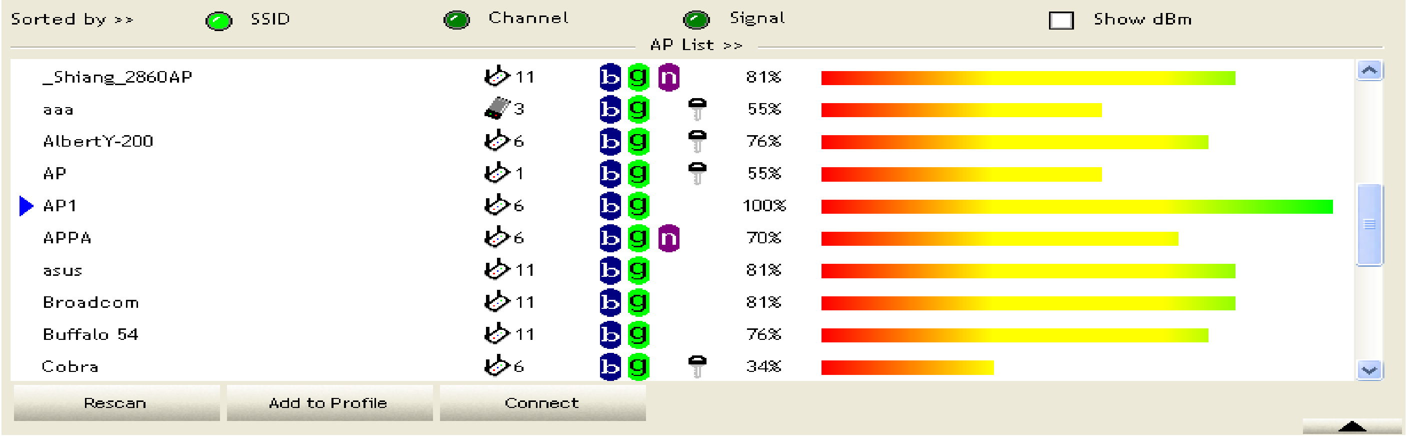
PROF1 AP1

Profile Name >> PROF1
SSID >> AP1
Network Type >> Infrastructure
Authentication >> Open
Encryption >> None
Use 802.1x >> NO
Channel >> 1
Power Save Mode >> CAM
Tx Power >> Auto
RTS Threshold >> 2347
Fragment Threshold >> 2346

1.3 Network

The system will display the information of local APs from the last scan result as part of the Network section. The Listed information includes the SSID, BSSID, Signal, Channel, Encryption Algorithm, Authentication, and Network type as shown in Figure 1.3A.

Figure 1.3A Network Function



	_Shiang_2860AP	11	b g n		81%
	aaa	3	b g	🔒	55%
	AlbertY-200	6	b g	🔒	76%
	AP	1	b g	🔒	55%
▶	AP1	6	b g		100%
	APPA	6	b g n		70%
	asus	11	b g		81%
	Broadcom	11	b g		81%
	Buffalo 54	11	b g		76%
	Cobra	6	b g	🔒	34%

Figure 1.3A Description of Fields:

① SSID: Name of BSS or IBSS network.
② Network Type: Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.
③ Channel: Channel in use.
④ Wireless Mode: AP support wireless mode. It may support 802.11a, 802.11b, 802.11g, or 802.11n wireless mode.
⑤ Security-Enable: Indicates if the AP provides a security-enabled wireless network.
⑥ Signal: Receive signal strength of the specified network.

Figure 1.3A Description of Icons and Buttons:

① ▶ Indicates that the connection is successful.
② Indicates the network type is in infrastructure mode.
③ Indicates the network type is in Ad-hoc mode.
④ 🔒 Indicates that the wireless network is security-enabled.
⑤ a Indicates 802.11a wireless mode.
⑥ b Indicates 802.11b wireless mode.
⑦ g Indicates 802.11g wireless mode.
⑧ n Indicates 802.11n wireless mode
⑨ Sorted by >> ● SSID ● Channel ● Signal Indicates whether the AP list is sorted by SSID, Channel, or Signal.

⑩ Connect Button to connect to the selected network.

⑪ Rescan Issues a rescan command to the wireless NIC to update information on the surrounding wireless network.

⑫ Add to Profile Adds the selected AP to the Profile setting. It will bring up a profile page and save the user's setting to a new profile.

⑬ ▼ Shows the Status Section.

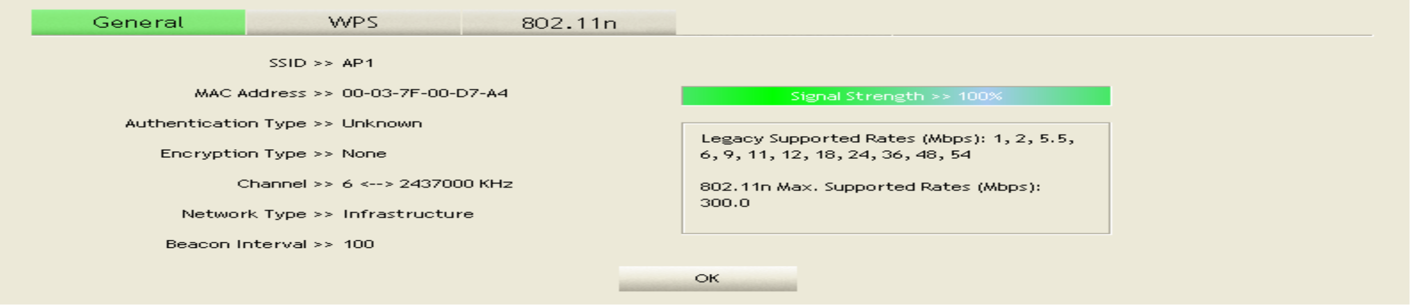
⑭ ▲ Hides the Status Section.

Connected Network:

1. When RaUI first runs, it will select the best AP to connect to automatically.
2. If the user wants to use another AP, they can click "Connect" for the intended AP to make a connection.
3. If the intended network uses an encryption other than "Not Use," RaUI will bring up the security page and let the user input the appropriate information to make the connection. Please refer to section 2.0 to learn how to fill in the security information.

When you double click an AP, you can see detailed information about that AP. The detailed AP information is divided into three parts. They are General, WPS, CCX information and 802.11n (The 802.11n button only exists for APs supporting N mode). A description of each type follows:

① General information contains the AP's SSID, MAC address, authentication type, encryption type, channel, network type, beacon interval, signal strength and supported rates as shown below.



SSID >> AP1

MAC Address >> 00-03-7F-00-D7-A4

Authentication Type >> Unknown

Encryption Type >> None

Channel >> 6 <--> 2437000 KHz

Network Type >> Infrastructure

Beacon Interval >> 100

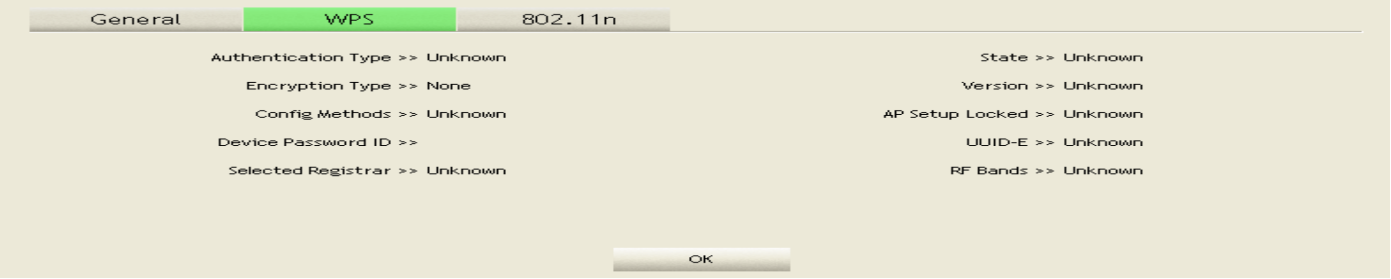
Signal Strength >> 100%

Legacy Supported Rates (Mbps): 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54

802.11n Max. Supported Rates (Mbps): 300.0

② WPS information contains the authentication type, encryption type, config. methods, device password ID, selected registrar, state, version, AP setup lock status, UUID-E and RF bands, as shown in Figure 1.3B. This information is explained in detail below.

Figure 1.3B WPS Information



Authentication Type >> Unknown

Encryption Type >> None

Config Methods >> Unknown

Device Password ID >>

Selected Registrar >> Unknown

State >> Unknown

Version >> Unknown

AP Setup Locked >> Unknown

UUID-E >> Unknown

RF Bands >> Unknown

Figure 1.3B Description of Fields:

1. Authentication Type: There are three types of authentication modes supported by RaConfig. They are: Open, Shared, WPA-PSK and WPA system.
2. Encryption Type: For open and shared authentication mode, the choices of the encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode the encryption type supports both TKIP and AES.
3. Config Methods: Corresponds to the methods the AP supports as an Enrollee for adding external Registrars as bitwise OR of values as shown below.

Value	Hardware Interface
0x0001	USBA (Flash Drive)
0x0002	Ethernet
0x0004	Label
0x0008	Display
0x0010	External NFC Token
0x0020	Integrated NFC Token
0x0040	NFC Interface
0x0080	Push Button
0x0100	Keypad

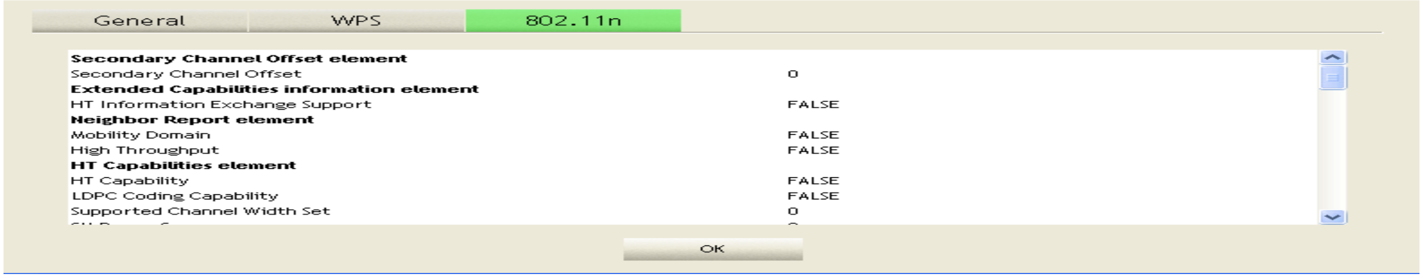
4. Device Password ID: Indicates the method or identifies the specific password that the selected Registrar intends to use. The AP in PBC mode must indicate 0x0004 within the two-minute Walk Time.

Value	Description
0x0000	Default (PIN)
0x0001	User-specified
0x0002	Rekey
0x0003	Display
0x0004	PushButton (PBC)
0x0005	Registrar-specified
0x0006-0x000F	Reserved

5. Selected Registrar: Indicates if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".
6. State: The current configuration state of the AP. The values are "Unconfigured" and "Configured".
7. Version: The specified WPS version.

8. AP Setup Locked: Indicates if the AP has entered a locked setup state.
9. UUID-E: The universally unique identifier (UUID) element generated by the Enrollee. The value is 16 bytes.
10. RF Bands: Indicates all of the RF bands available to the AP. A dual-band AP must provide it. The values are "2.4GHz" and "5GHz".

③ 802.11n information contains some related 802.11n information as shown below.

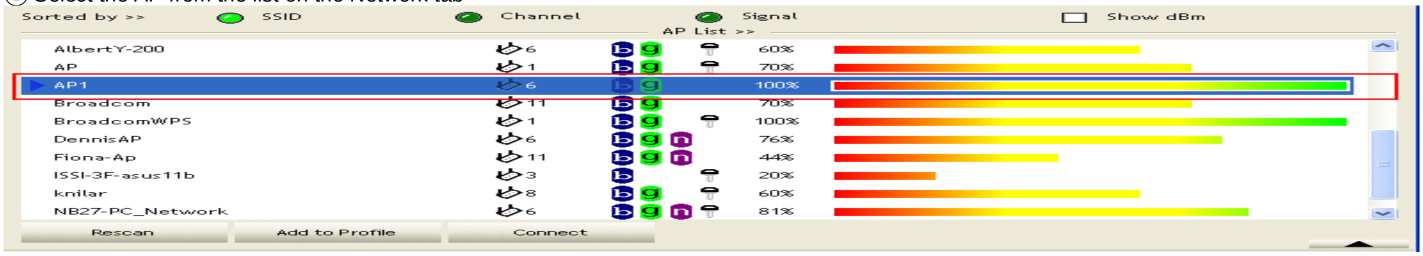


Secondary Channel Offset element
Secondary Channel Offset 0
Extended Capabilities information element
HT Information Exchange Support FALSE
Neighbor Report element
Mobility Domain FALSE
High Throughput FALSE
HT Capabilities element
HT Capability FALSE
LDPC Coding Capability FALSE
Supported Channel Width Set 0

1.3.1 Example of Adding a Profile to the Network

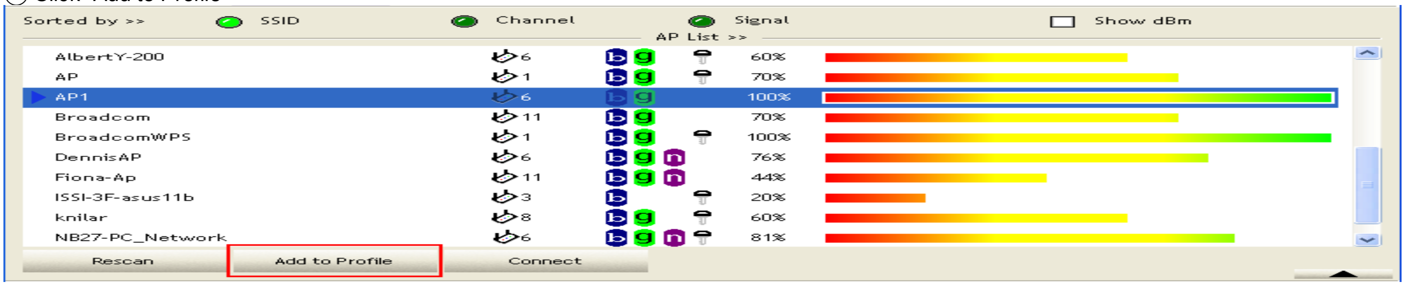
Follow the four simple steps listed below to add a profile to the network.

① Select the AP from the list on the Network tab



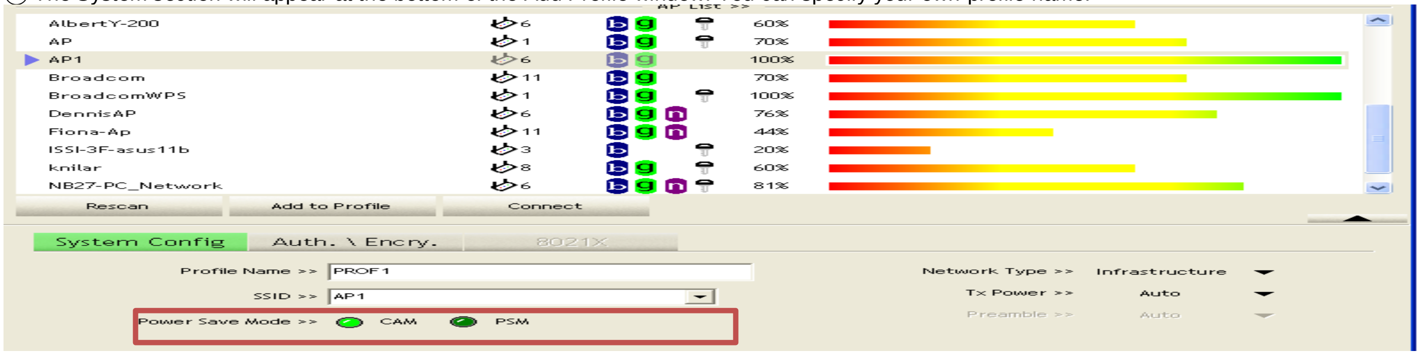
AlbertY-200	6	b g	60%
AP	1	b g	70%
AP1	6	b g	100%
Broadcom	11	b g	70%
BroadcomWPS	1	b g	100%
DennisAP	6	b g n	76%
Fiona-Ap	11	b g n	44%
ISSI-3F-asus11b	3	b	20%
knilar	8	b g	60%
NB27-PC_Network	6	b g n	81%

② Click "Add to Profile"



AlbertY-200	6	b g	60%
AP	1	b g	70%
AP1	6	b g	100%
Broadcom	11	b g	70%
BroadcomWPS	1	b g	100%
DennisAP	6	b g n	76%
Fiona-Ap	11	b g n	44%
ISSI-3F-asus11b	3	b	20%
knilar	8	b g	60%
NB27-PC_Network	6	b g n	81%

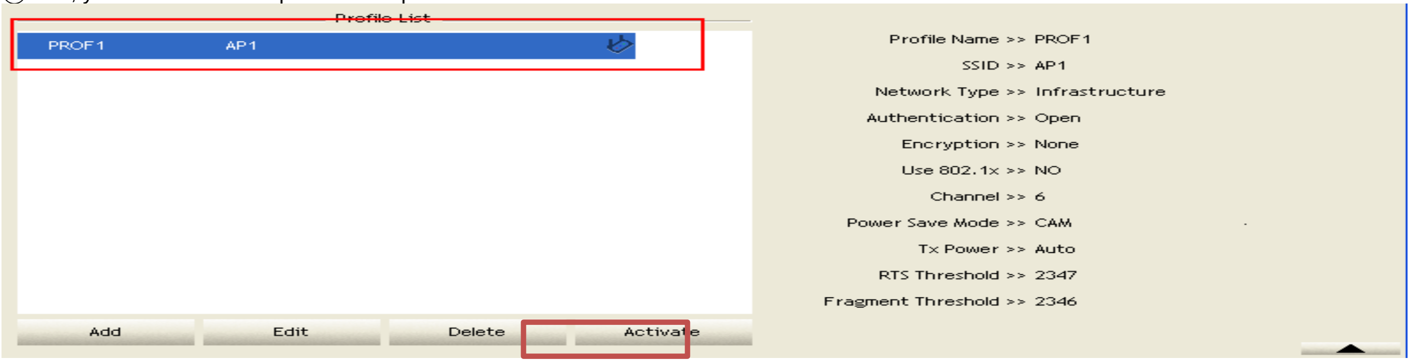
③ The System section will appear at the bottom of the Add Profile window. You can specify your own profile name.



AlbertY-200	6	b g	60%
AP	1	b g	70%
AP1	6	b g	100%
Broadcom	11	b g	70%
BroadcomWPS	1	b g	100%
DennisAP	6	b g n	76%
Fiona-Ap	11	b g n	44%
ISSI-3F-asus11b	3	b	20%
knilar	8	b g	60%
NB27-PC_Network	6	b g n	81%

Profile Name >> PROF1
SSID >> AP1
Power Save Mode >> CAM PSM
Network Type >> Infrastructure
Tx Power >> Auto
Preamble >> Auto

④Next, you will see the new profile in the profile list. Click "Activate".



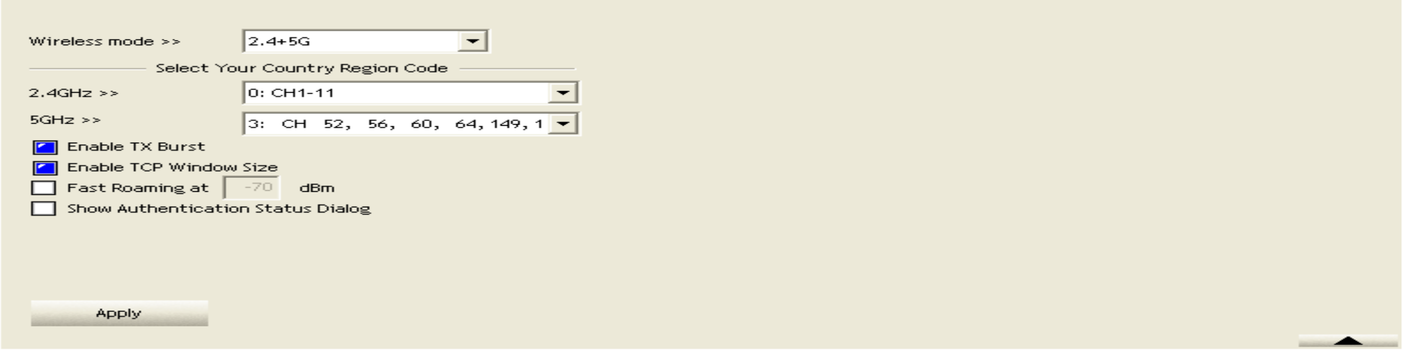
PROF1 AP1

Profile Name >> PROF1
SSID >> AP1
Network Type >> Infrastructure
Authentication >> Open
Encryption >> None
Use 802.1x >> NO
Channel >> 6
Power Save Mode >> CAM
Tx Power >> Auto
RTS Threshold >> 2347
Fragment Threshold >> 2346

1.4 Advanced Functions

Figure 1.4A shows the Advanced functions of RaUI.

Figure 1.4A Advanced Functions



Wireless mode >> 2.4+5G

Select Your Country Region Code

2.4GHz >> 0: CH1-11

5GHz >> 3: CH 52, 56, 60, 64, 149, 1

☑ Enable TX Burst

☑ Enable TCP Window Size

☐ Fast Roaming at -70 dBm

☐ Show Authentication Status Dialog

Figure 1.4A Description of Fields:

① Wireless mode: Select wireless mode. 2.4G, 5G, and 2.4+5G are supported.
② Wireless Protection: Users can choose from Auto, On, and Off. *(This is not supported by 802.11n adapters.)*
③ TX Rate: Manually select the transfer rate. The default setting is auto. *(802.11n wireless cards do not allow the user to select the TX Rate.)*
④ Enable TX Burst: Ralink's proprietary frame burst mode.
⑤ Enable TCP Window Size: Optimise the TCP window size to allow for greater throughput.
⑥ Fast Roaming at- dBm: enables fast roaming, which is set by the transmit power.
⑦ Select Your Country Region Code: There are eight countries to choose from in the country channel list. *(11A ListBox only shows for 5G adapter.)*
⑧ Show Authentication Status Dialog: When you connect to an AP with authentication, choose whether show the "Authentication Status Dialog" or not. The Authentication Status Dialog displays the processes during 802.1x authentication.
⑨ Apply: Applies the above changes.

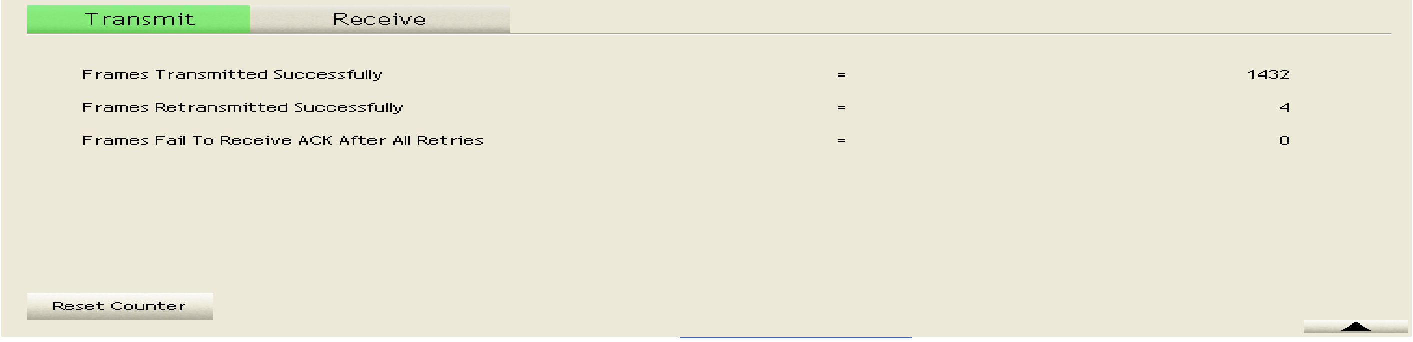
Figure 1.4A Description of Icons and Buttons:

①▼ Show status section information.
②▲ Hide status section information.

1.5 Statistics

The Statistics page displays detailed counter information based on 802.11 MIB counters. This page translates MIB counters into a user friendly format. Figure 1.5A and 1.5B show the detailed page layout.

Figure 1.5A Transmit Statistics Function



Frames Transmitted Successfully = 1432

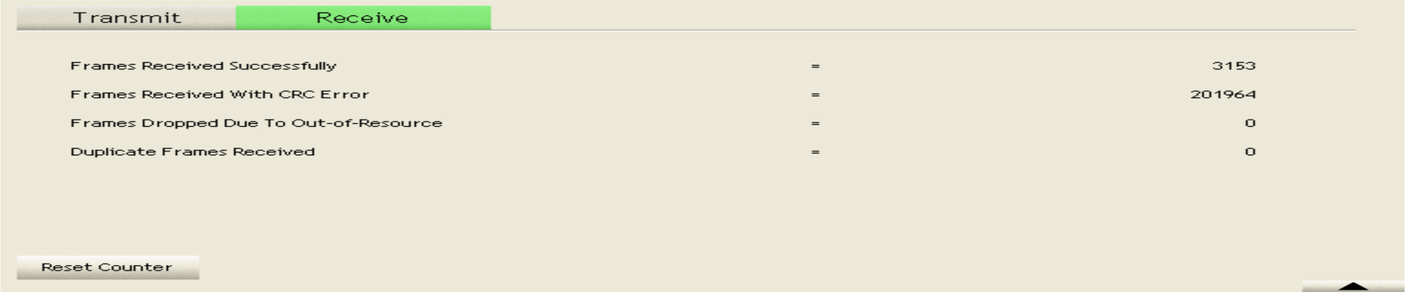
Frames Retransmitted Successfully = 4

Frames Fail To Receive ACK After All Retries = 0

Figure 1.5A Description of Fields

① Frames Transmitted Successfully: Shows how many frames were successfully sent.
② Frames Retransmitted Successfully: Shows how many frames were successfully retransmitted after retransmission.
③ Frames Fail To Receive ACK After All Retries: Shows how many frames failed transmit after hitting retry limit.
④ RTS Frames Successfully Receive CTS: Successfully receive CTS after sending RTS frame.
⑤ RTS Frames Fail To Receive CTS: Failed to receive CTS after sending RTS.
⑥ Reset: Resets counters to zero.

Figure 1.5B Receive Statistics Function



Frames Received Successfully = 3153

Frames Received With CRC Error = 201964

Frames Dropped Due To Out-of-Resource = 0

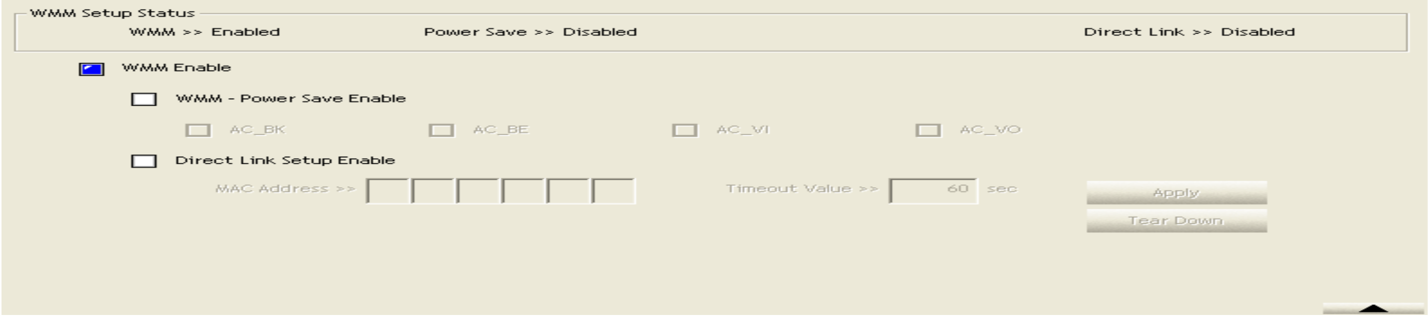
Duplicate Frames Received = 0

Figure 1.5B Description of Fields
① Frames Received Successfully: The number of frames successfully received.
② Frames Received With CRC Error: The number of frames received with a CRC error.
③ Frames Dropped Due To Out-of-Resource: The number of frames dropped due to a resource issue.
④ Duplicate Frames Received: The number of duplicate frames received.
⑤ Reset: Resets counters to zero.
Figure 1.5A and 1.5B Description of Icons and Buttons:
① ▼ Show status section information.
② ▲ Hide status section information.

1.6 WMM

Figure 1.6A shows the WMM function of RaUI. Included features are: WMM Enable, WMM - Power Save Enable, and DLS setup. A detailed description is given below.

Figure 1.6A WMM Function



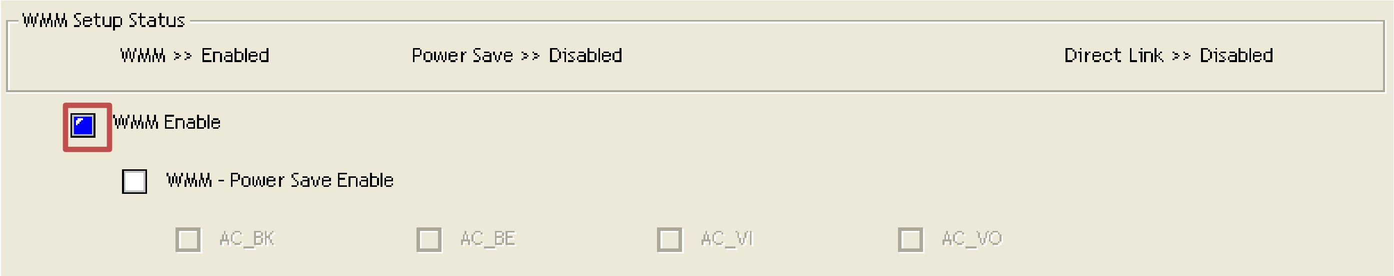
WMM Setup Status
WMM >> Enabled
Power Save >> Disabled
Direct Link >> Disabled
☑ WMM Enable
☐ WMM - Power Save Enable
☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO
☐ Direct Link Setup Enable
MAC Address >>
Timeout Value >> 60 sec

Figure 1.6 Description of Fields
①Direct Link Setup Enable : Enables DLS (Direct Link Setup). See 1.6-2 for setup instructions.
② WMM Enable : Enables Wi-Fi Multi-Media. See 1.6-1 for setup instructions.
③ WMM - Power Save Enable : Enables WMM Power Save. See 1.6-3 for setup instructions.
Figure 1.6 Description of Icons and Buttons:
① ▼ Show status section information.
② ▲ Hide status section information.

1.6-1 Example Configuration to Enable Wi-Fi Multi-Media (WMM)

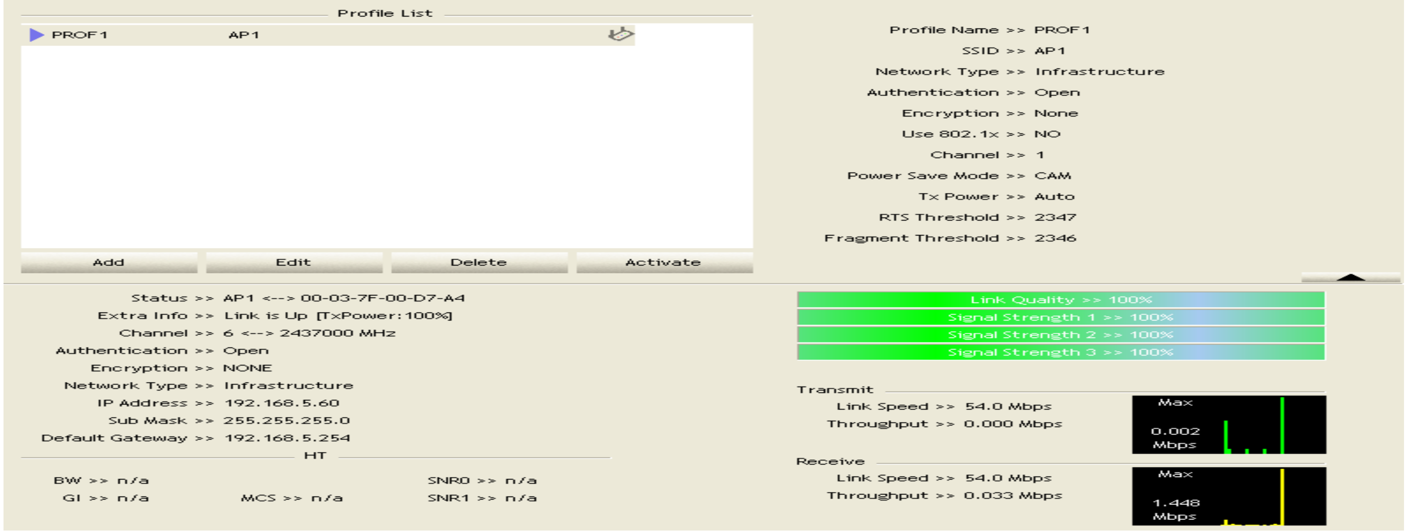
If you want to use "WMM-Power Save" or "Direct Link" you must enable WMM first. Enable WMM using the following steps:

① Click the box by "WMM Enable".



WMM Setup Status
WMM >> Enabled
Power Save >> Disabled
Direct Link >> Disabled
☑ WMM Enable
☐ WMM - Power Save Enable
☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO

② Go to the "Network" function. And add an AP that supports WMM features to the Profile list. The result will look like the image shown below.



Profile List
PROF1 AP1

Profile Name >> PROF1
SSID >> AP1
Network Type >> Infrastructure
Authentication >> Open
Encryption >> None
Use 802.1x >> NO
Channel >> 1
Power Save Mode >> CAM
Tx Power >> Auto
RTS Threshold >> 2347
Fragment Threshold >> 2346

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Open
Encryption >> NONE
Network Type >> Infrastructure
IP Address >> 192.168.5.60
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

HT
BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%

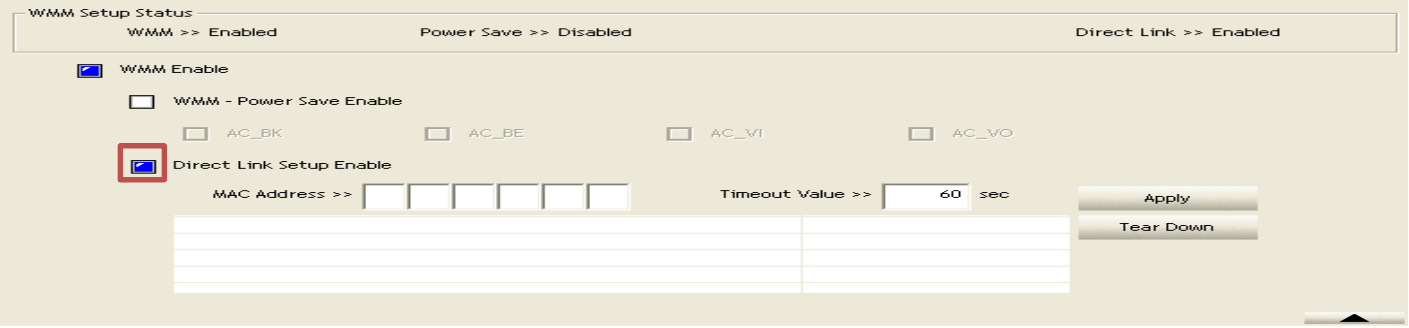
Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.033 Mbps

1.6-2 Example Configuration to Enable DLS (Direct Link Setup)

Follow the simple steps listed below to enable DLS.

① Check the box by "Direct Link Setup Enable."



WMM Setup Status

WMM >> Enabled

Power Save >> Disabled

Direct Link >> Enabled

☑ WMM Enable

☐ WMM - Power Save Enable

☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO

☑ Direct Link Setup Enable

MAC Address >>

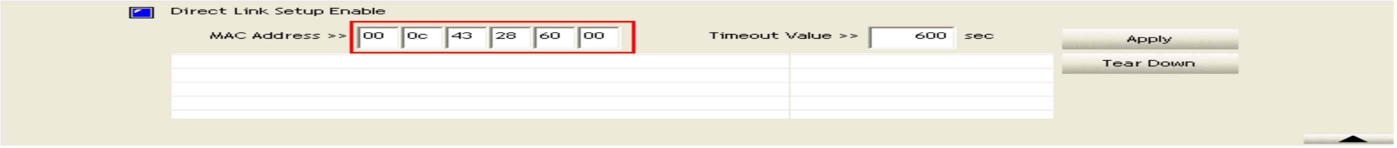
Timeout Value >> 60 sec

② Change to "Network" function. Add an AP that supports DLS features to the Profile. The result will look like the Profile Page in step 2 from section 1.6-1 above.

Explanation of the DLS settings:

① Fill in the blanks of Direct Link MAC address with MAC Address of STA as shown below. The STA must conform to these two conditions:

1. Connect with an AP that supports DLS features.
2. Ensure that DLS is enabled.

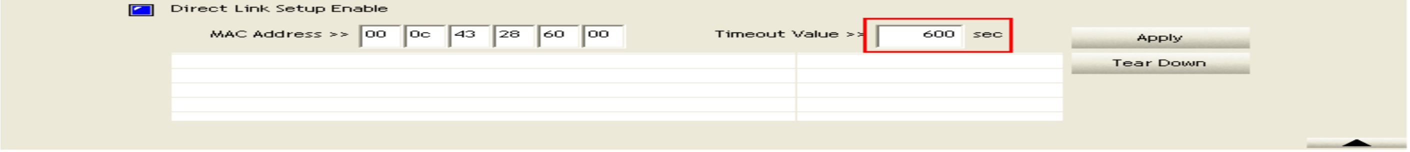


☑ Direct Link Setup Enable

MAC Address >> 00 0c 43 28 60 00

Timeout Value >> 600 sec

② Set the Timeout Value. The Timeout Value indicates the time in seconds before it disconnects automatically. The value is an integer. The integer must be between 0~65535. A zero value specifies that it stays connected. The default Timeout Value is 60 seconds.

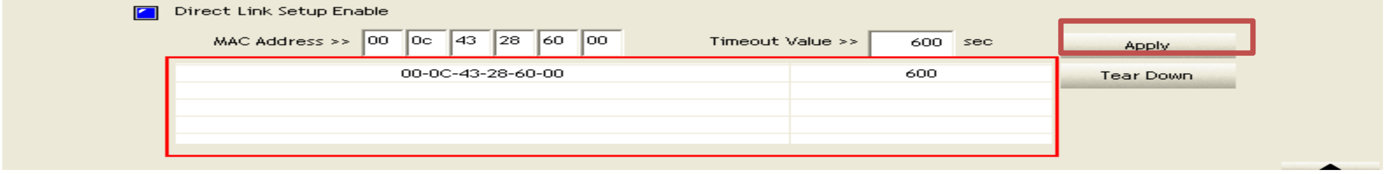


☑ Direct Link Setup Enable

MAC Address >> 00 0c 43 28 60 00

Timeout Value >> 600 sec

③ The MAC Address and the Timeout Value will appear in the grid. Click "Apply."



☑ Direct Link Setup Enable

MAC Address >> 00 0c 43 28 60 00

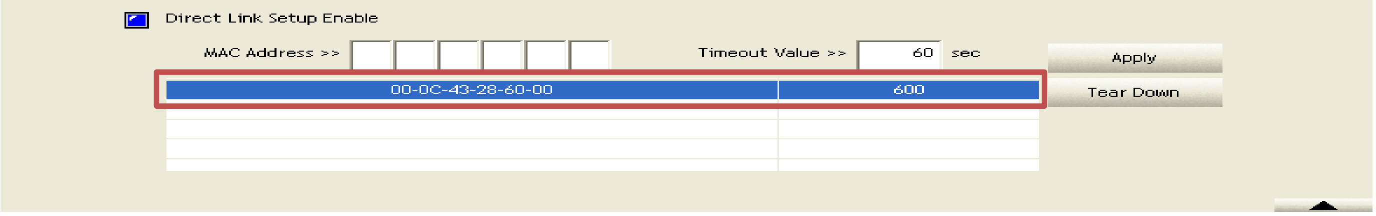
Timeout Value >> 600 sec

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

Description of DLS Status Grid:

① After configuring the DLS successfully, the MAC address and Timeout Value are displayed in the "DLS Status" gird as shown in step 3 under DLS settings above.

② To display the values of DLS Status in the MAC Address and Timeout Values fields under Direct Link Setup double click on the link from the DLS Status grid that you want to show up in the MAC Address and Timeout Value fields of Direct Link Setup and the information will appear in the Direct Link fields as shown in figure below.

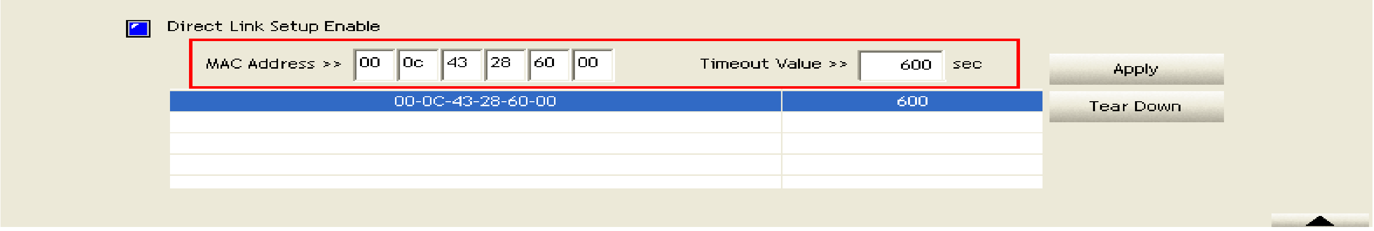


☑ Direct Link Setup Enable

MAC Address >>

Timeout Value >> 60 sec

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



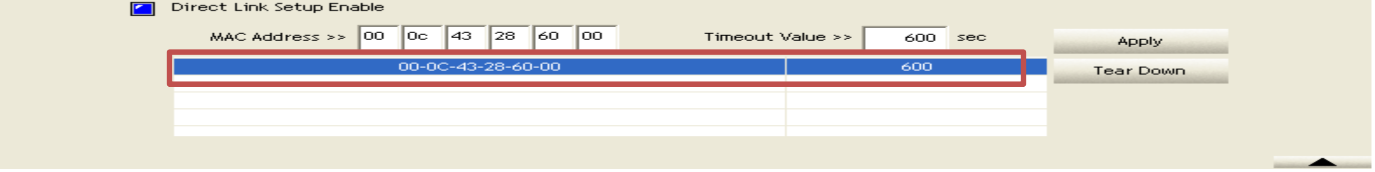
☑ Direct Link Setup Enable

MAC Address >> 00 0c 43 28 60 00

Timeout Value >> 600 sec

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

To Disconnect a Direct Link setup select a direct link STA from the grid then click the “Tear Down” button as shown below.

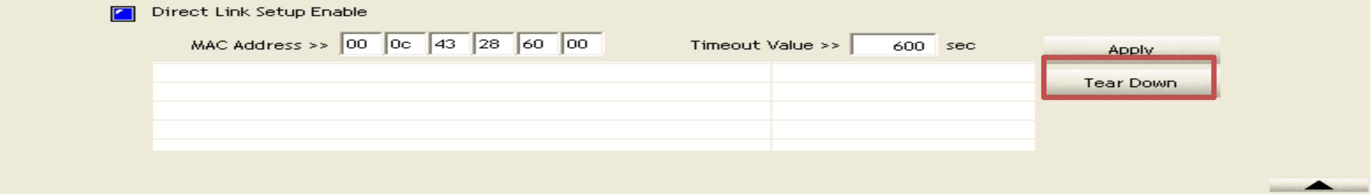


☑ Direct Link Setup Enable

MAC Address >> 00 0c 43 28 60 00

Timeout Value >> 600 sec

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



☑ Direct Link Setup Enable

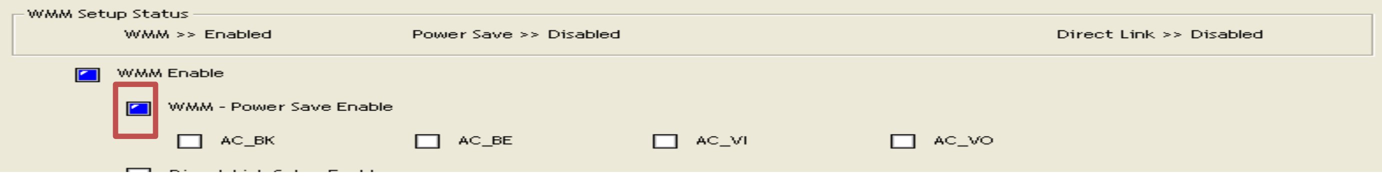
MAC Address >> 00 0c 43 28 60 00

Timeout Value >> 600 sec

1.6-3 Example Configuration to Enable WMM Power Save

To Enable WMM Power Save function take the steps listed below.

① Make sure that WMM is enabled then Click the "WMM-Power Save Enable" box.



WMM Setup Status

WMM >> Enabled

Power Save >> Disabled

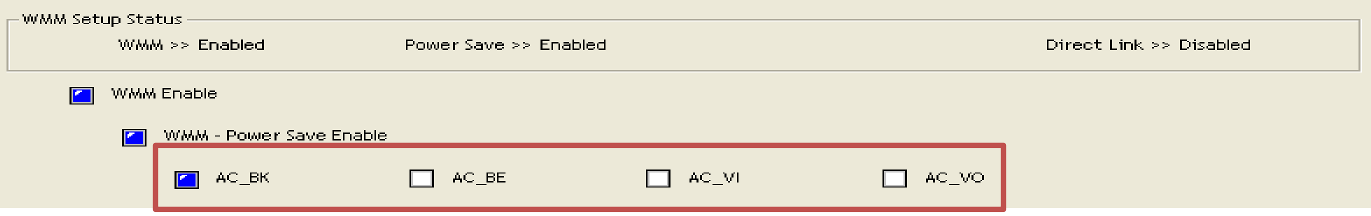
Direct Link >> Disabled

☑ WMM Enable

☑ WMM - Power Save Enable

☐ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO

② Please select which ACs you want to enable. WMM Power Save is now fully enabled.



WMM Setup Status

WMM >> Enabled

Power Save >> Enabled

Direct Link >> Disabled

☑ WMM Enable

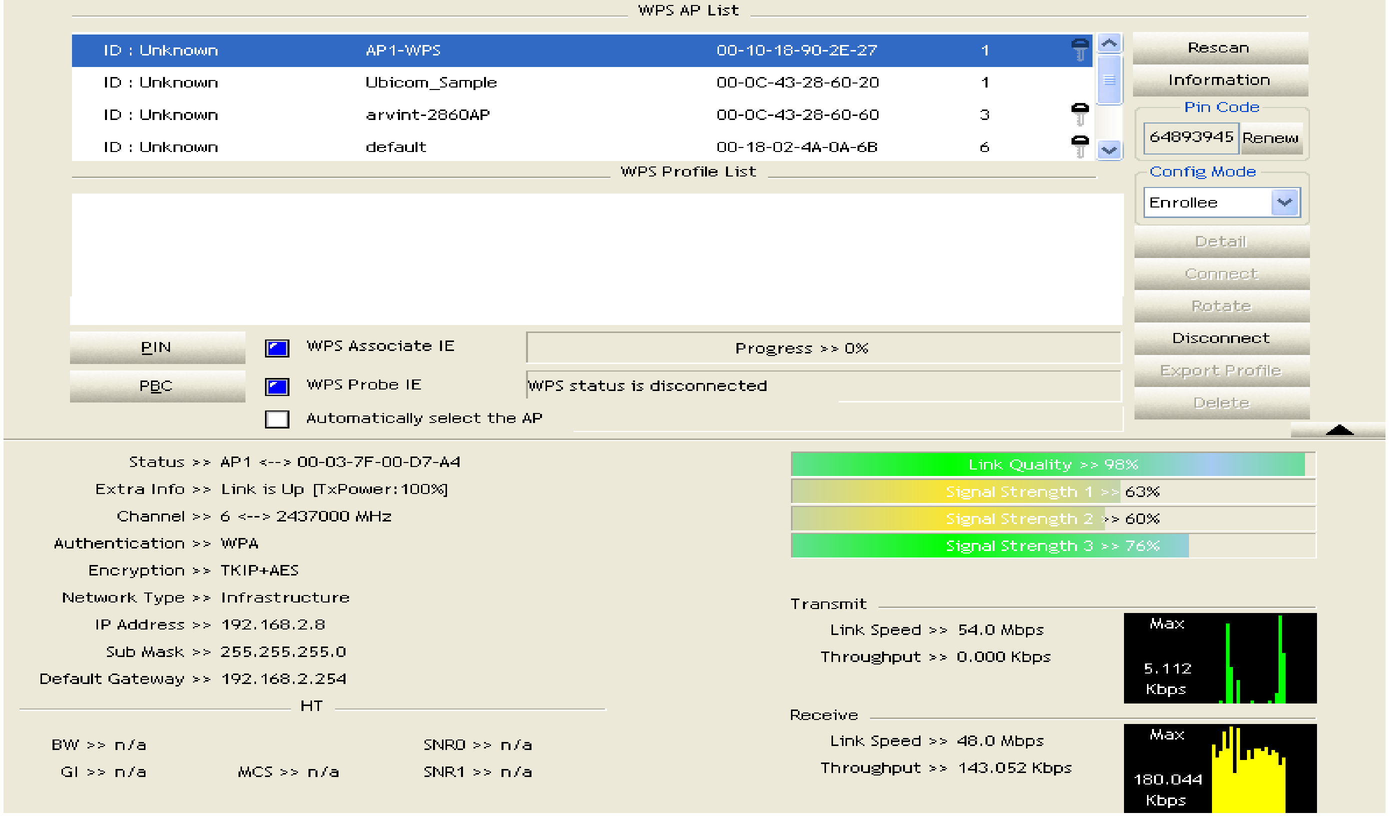
☑ WMM - Power Save Enable

☑ AC_BK ☐ AC_BE ☐ AC_VI ☐ AC_VO

1.7 WPS

Figure 1.7A below illustrates the RaUI WPS functions. A detailed description follows.

Figure 1.7A WPS Function



WPS AP List

ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

Status >> AP1 <--> 00-03-7F-00-D7-A4

Extra Info >> Link is Up [TxPower:100%]

Channel >> 6 <--> 2437000 MHz

Authentication >> WPA

Encryption >> TKIP+AES

Network Type >> Infrastructure

IP Address >> 192.168.2.8

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.2.254

HT

BW >> n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 98%

Signal Strength 1 >> 63%

Signal Strength 2 >> 60%

Signal Strength 3 >> 76%

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Kbps

Receive

Link Speed >> 48.0 Mbps

Throughput >> 143.052 Kbps

Figure 1.7A Description of Fields:

① 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. Ralink STA supports the configuration and setup using a PIN configuration method or a PBC configuration method through an internal or external Registrar.

② WPS AP List: Displays the information of the surrounding APs with WPS IE from the last scan result. The detailed information includes the SSID, BSSID, Channel, ID (Device Password ID), Security-Enabled.

③ Rescan: Issues a rescan command to the wireless NIC to update information on the surrounding wireless network.

④ Information: Displays the information about WPS IE on the selected network. The detailed list includes the Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands. Further details are available in section 1.3: Network (#2 figure 1.3C).

⑤ PIN Code: The user is required to enter an 8-digit PIN Code into Registrar. When an STA is the Enrollee, you can click "Renew" to regenerate a new PIN Code.

⑥ Config Mode: The station serving as an Enrollee or an external Registrar.

⑦ Table of Credentials: Displays all credentials obtained by the Registrar. The detailed list includes information about the SSID, MAC Address, Authentication and Encryption Type. If STA is the Enrollee, the credentials are created immediately with each WPS success. If STA is the Registrar, RaUI creates a new credential with WPA2-PSK/AES/64Hex-Key and doesn't change this until switching to STA Registrar.

⑧ Control items for credentials.

1. Detail: Command to obtain Information about Security and the Key in the credential.
2. Connect: Command to connect to the selected network inside credentials. The active selected credential is like the active selected Profile.
3. Rotate: Command to rotate networks or to connect to the next network inside credentials.
4. Disconnect: Stops the WPS action and disconnects the active link. It then selects the most recent profile on the Profile Page of RaUI. If there are no profiles, the driver will select any non-security AP.
5. Export Profile: Exports all credentials to a Profile.
6. Delete: Deletes an existing credential; then selects the next credential. If there are no other credentials the driver will select any non-security AP.

⑨ *PIN:Start to add to Registrar using PIN configuration method. If STA Registrar, remember to enter your PIN Code from your Enrollee before starting PIN. See section 1.7-2 for more information.

⑩ *PBC: Start to add to AP using PBC configuration method.
*After you click PIN or PBC, please do not rescan for at least 2 minutes after the connection has been made. If you want to abort this setup within the interval, restart PIN/PBC or click "Disconnect" to stop WPS action.

⑪ WPS associate IE: Sends the association request with WPS IE during the WPS setup. It is optional for STA.

⑫ WPS probe IE: Sends the probe request with WPS IE during WPS setup. It is optional for STA.

⑬ Progress Bar: Displays the rate of progress from Start to Connected.

⑭ Status Bar: Displays the current WPS Status.

⑮ Automatically select the AP: Starts to add to AP by using to select the AP automatically in PIN method.

There are examples in section 1.7-2 (PIN Enrollee Setup), section 1.7-3(PBC Enrollee Setup) and section 1.7-4Registrar Configures and AP)

Figure 1.7A Description of Icons and Buttons:

① ▼ Show status section information.

② ▲ Hide status section information.

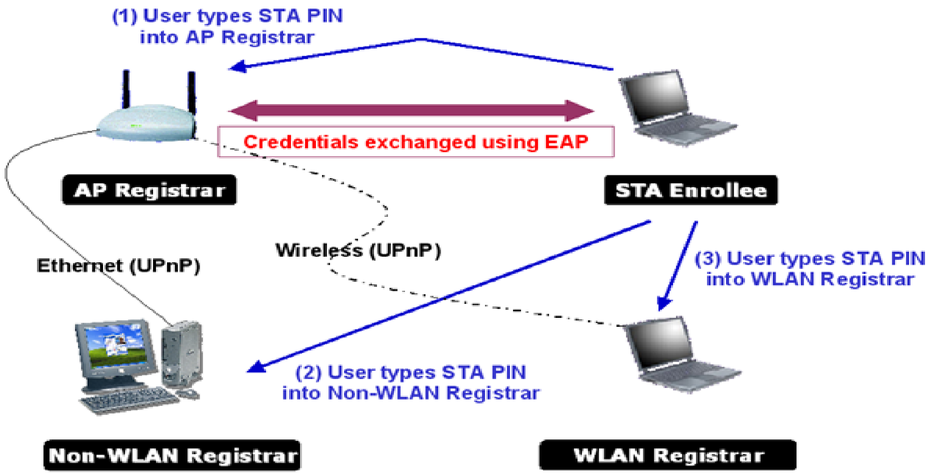
1.7-1 WPS Information on AP

The WPS information includes the authentication type, encryption type, config methods, device password ID, selected registrar, state, version, AP setup locked, UUID-E and RF bands. (see section 1.3: Network (#2 figure 1.3C))

1.7-2 Example of Adding to Registrar Using PIN Method

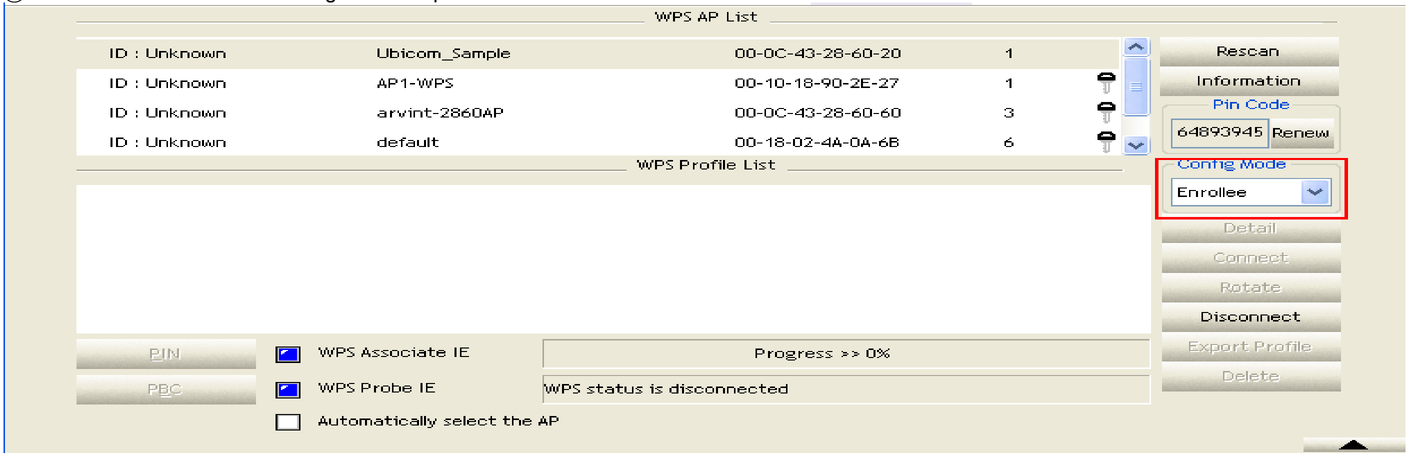
The user obtains a device password (PIN Code) from the STA and enters the password into the Registrar. Both the Enrollee and the Registrar use PIN Config method for the configuration setup. The following image outlines the process.

Figure 1.7-2A How to add to Registrar using PIN method



Instructions for Adding to Registrar using PIN method:

① Select “Enrolee” from the Config Mode drop-down list as shown below.



ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

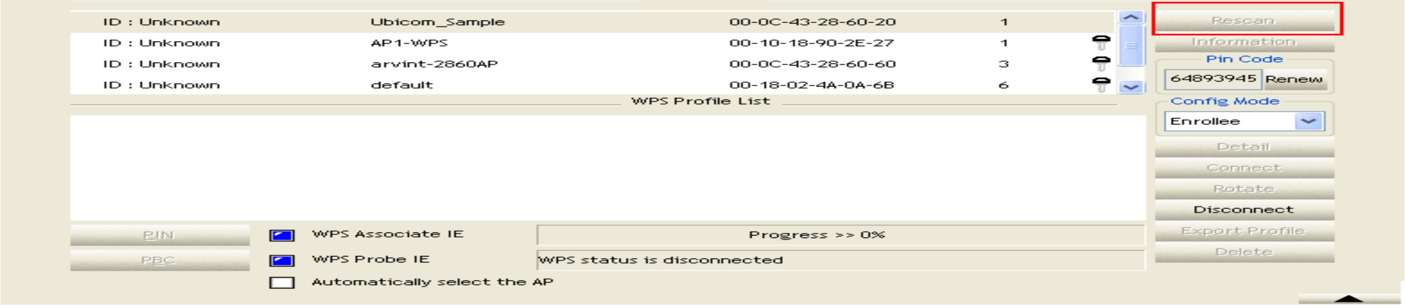
☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

② Click "Rescan" to update available WPS APs.



ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

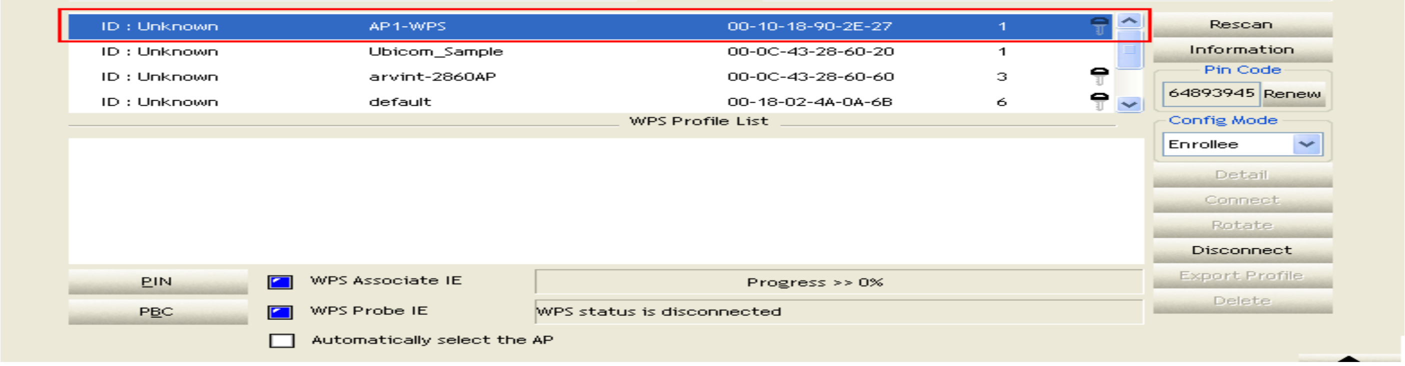
☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

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



ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

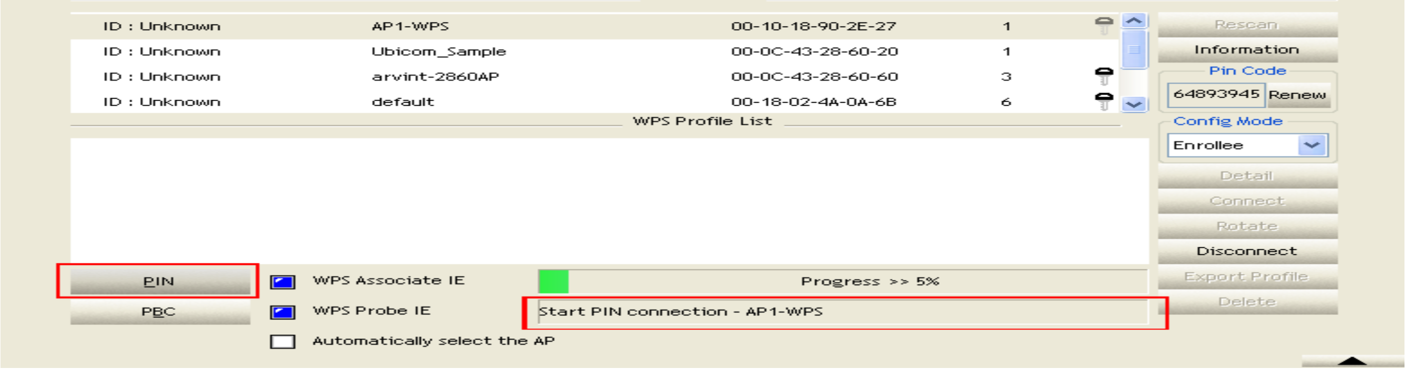
☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

④ Click "PIN" to enter the PIN.

⑤ Enter the PIN Code of the STA into the Registrar when prompted by the Registrar.**



ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

☐ Automatically select the AP

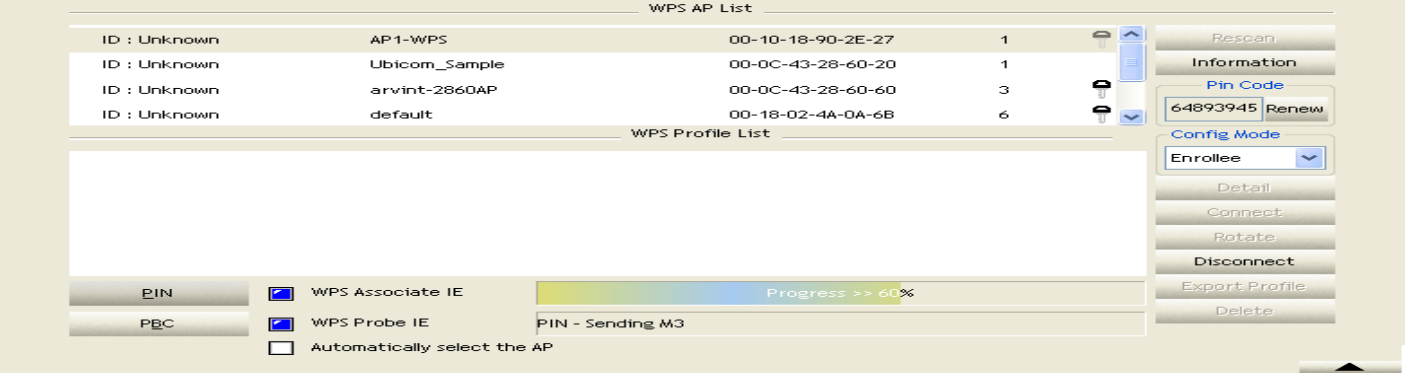
Progress >> 5%

Start PIN connection - AP1-WPS

**Allow for an exchange between Steps 4 and 5.

***If you are using a Microsoft Windows Connection as an External Registrar you must start the PIN connection at STA first; then search for your WPS Device name and MAC address on the Microsoft Registrar. Add a new device and enter the PIN Code of STA on the Microsoft Registrar when prompted.

⑥ If you have taken all the above steps the results will look like the below image.



ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

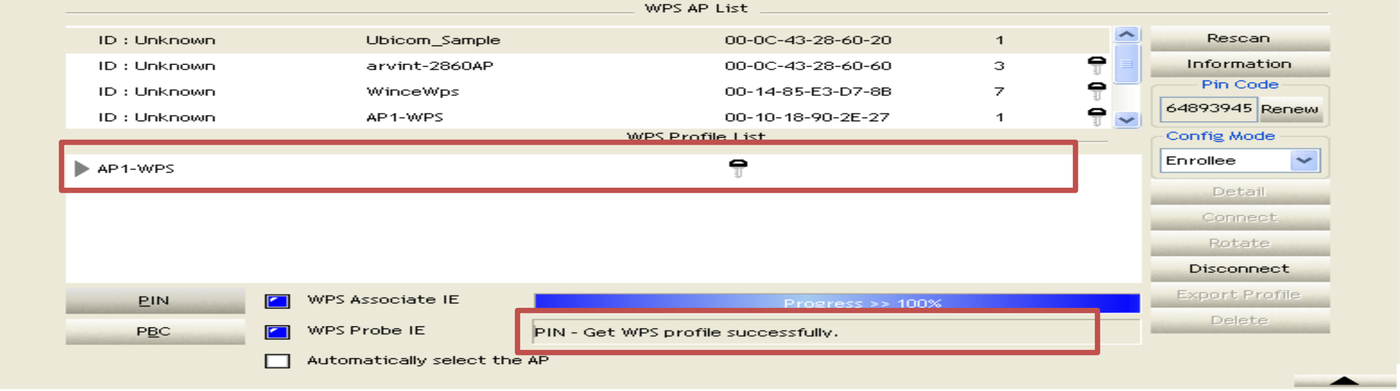
☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 60%

PIN - Sending M3

⑦ Configure one or more credentials. If the connection was successful the results will look like the below image.



ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1

AP1-WPS

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

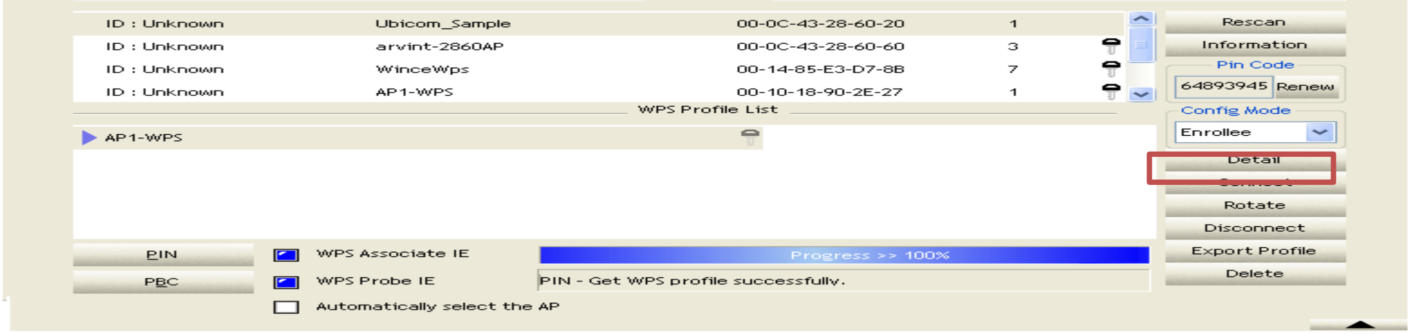
☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 100%

PIN - Get WPS profile successfully.

⑧ Click “Detail” to get a more information.



ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1

AP1-WPS

Pin Code: 64893945

Config Mode: Enrollee

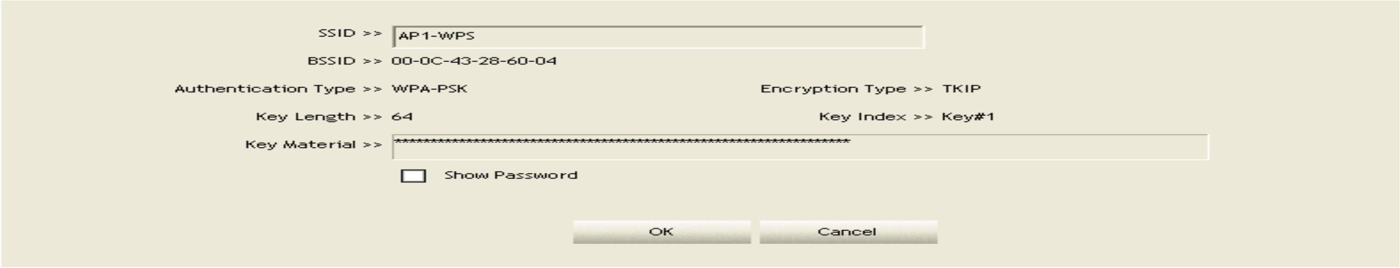
☑ WPS Associate IE

☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 100%

PIN - Get WPS profile successfully.



SSID >> AP1-WPS

BSSID >> 00-0C-43-28-60-04

Authentication Type >> WPA-PSK

Encryption Type >> TKIP

Key Length >> 64

Key Index >> Key#1

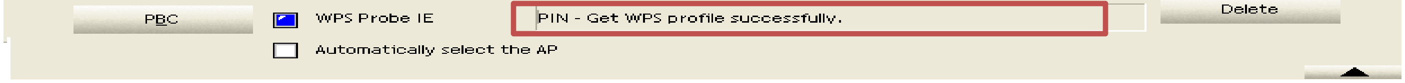
Key Material >> **

☐ Show Password

* If Credential#1 is reliable and present, the system will connect with Credential #1. If not, the system will automatically rotate to the next existing credential. The user can also click "Rotate" to rotate to the next usable credential.

Description of WPS Status Bar for PIN Config:

Figure 1.7B WPS Staus Barfor PIN Config



☑ WPS Associate IE

☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 100%

PIN - Get WPS profile successfully.

① Acceptable Pin Configurations: Start PIN connection - SSID > Begin associating to WPS AP > Associated to WPS AP > Sending EAPOL-Start > Sending EAP-Rsp (ID) > Receive EAP-Req (Start) > Sending M1 > Received M2 > (Received M2D > Sending EAP-Rsp (ACK)) > Sending

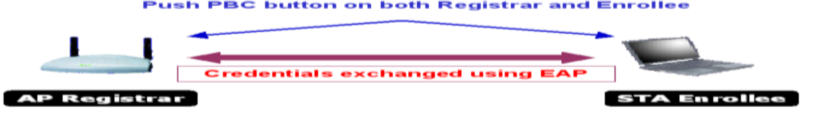
M3 > Received M4 > Sending M5 > Received M6 > Sending M7 > Received M8 > Sending EAP-Rsp(Done) > Configured > WPS status is disconnected > WPS status is connected successfully-SSID

② When errors occur within two minutes of connecting; the WPS status bar might report "WPS EAP process failed". If this occurs the following error messages might appear: 1. Receive EAP with wrong NONCE; or 2. Receive EAP without integrity.

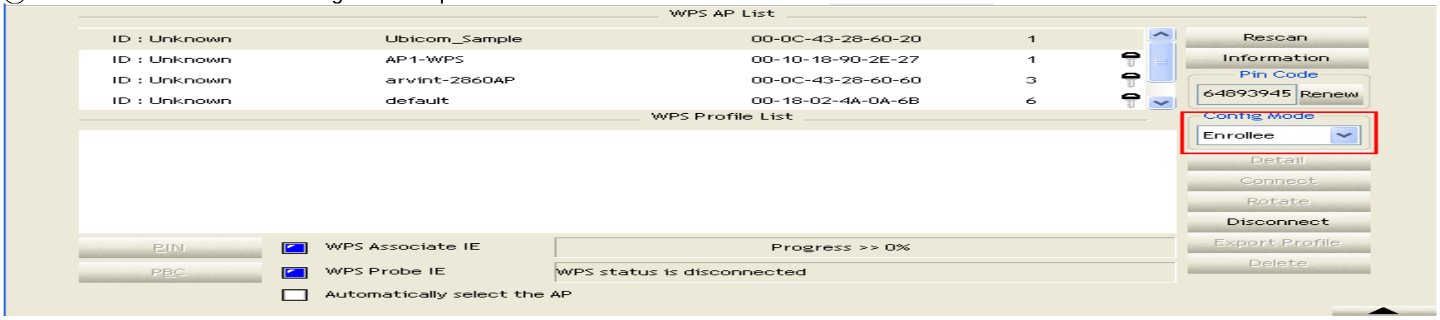
1.7-3 Example of Adding to the Registrar Using the PBC Method

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. *Before you press PBC on STA and candidate AP. Make sure all APs aren't in PBC mode or APs using PBC mode have left their Walk Time.*

Figure 1.7-3A PBC Button


Push PBC button on both Registrar and Enrollee
Credentials exchanged using EAP
AP Registrar
STA Enrollee

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



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

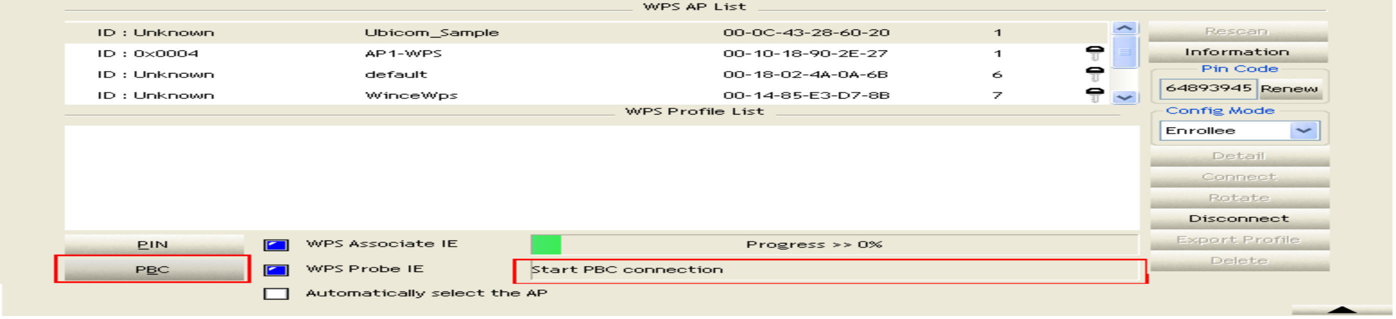
☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

② Click PBC to start the PBC connection.

③ Push the PBC on AP.



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : 0x0004	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	default	00-18-02-4A-0A-6B	6
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

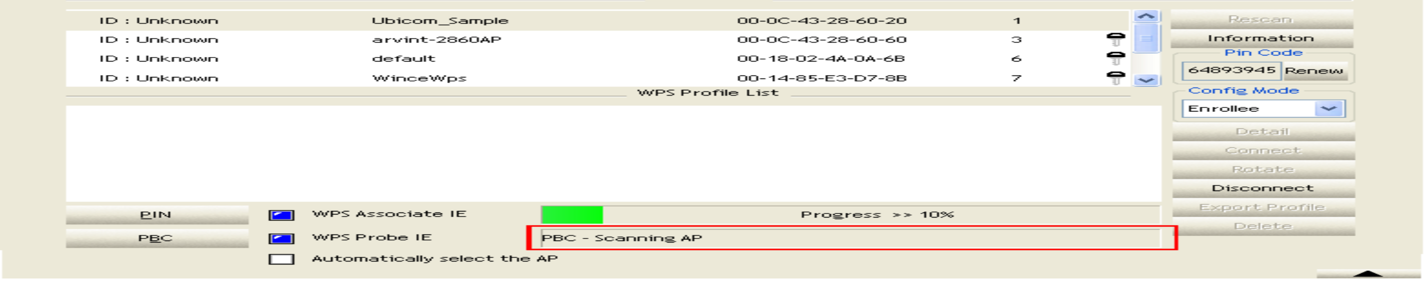
☐ Automatically select the AP

Progress >> 0%

Start PBC connection

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

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



WPS AP List

ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	default	00-18-02-4A-0A-6B	6
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

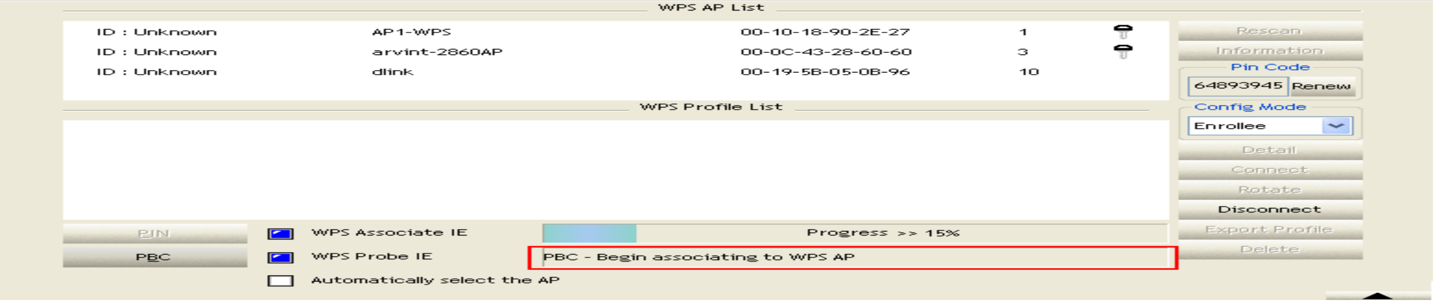
☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 10%

PBC - Scanning AP

⑤ When one AP is found, join it



WPS AP List

ID : Unknown	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	arvint-2860AP	00-0C-43-28-60-60	3
ID : Unknown	dlink	00-19-5B-05-0B-96	10

WPS Profile List

Pin Code: 64893945

Config Mode: Enrollee

☑ WPS Associate IE

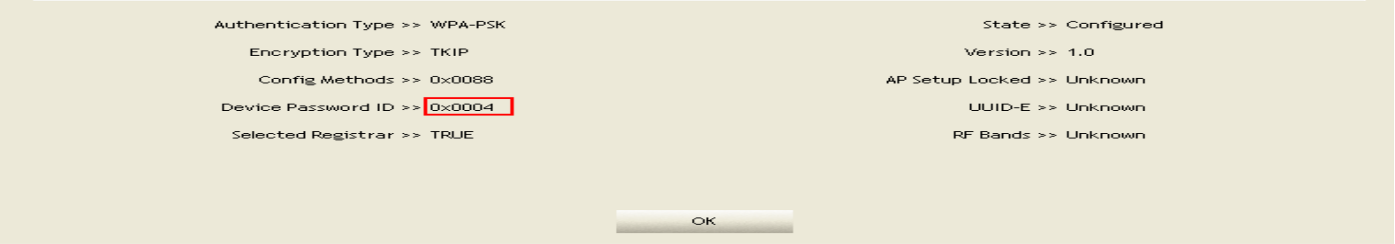
☑ WPS Probe IE

☐ Automatically select the AP

Progress >> 15%

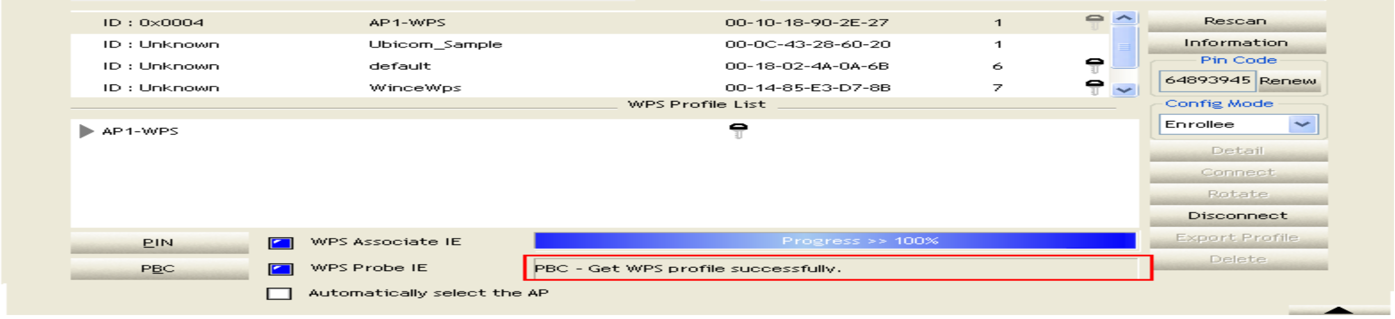
PBC - Begin associating to WPS AP

⑥ Check WPS Information on the available WPS APs.



Authentication Type >> WPA-PSK
Encryption Type >> TKIP
Config Methods >> 0x0088
Device Password ID >> 0x0004
Selected Registrar >> TRUE
State >> Configured
Version >> 1.0
AP Setup Locked >> Unknown
UUID-E >> Unknown
RF Bands >> Unknown

⑦ Configure and receive one or more credential(s).



ID : 0x0004	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	default	00-18-02-4A-0A-6B	6
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7

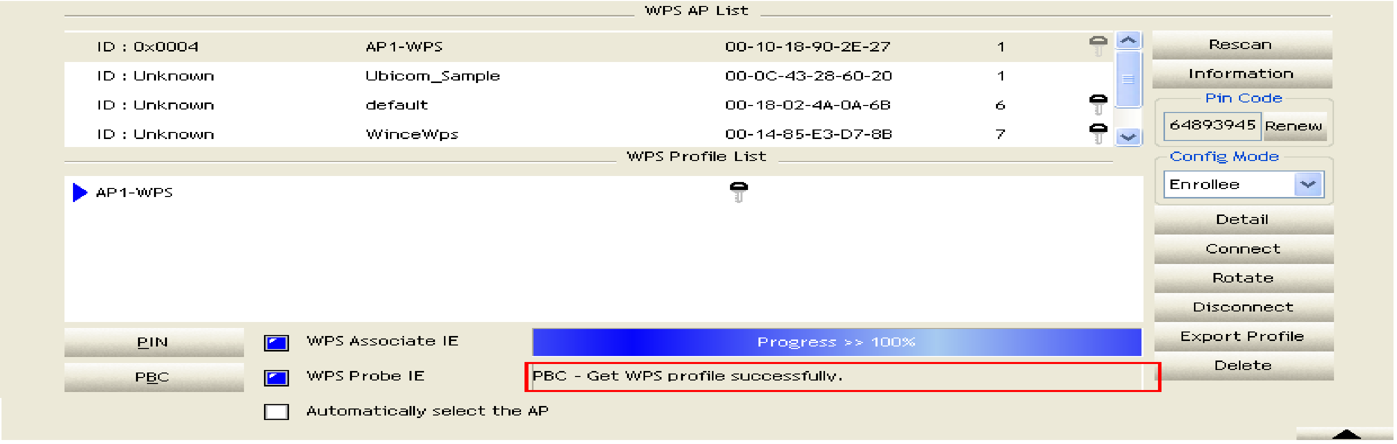
AP1-WPS

Pin Code: 64893945

Config Mode: Enrollee

PBC - Get WPS profile successfully.

⑧ Then connect successfully. The result will look like the figure below.



ID : 0x0004	AP1-WPS	00-10-18-90-2E-27	1
ID : Unknown	Ubicom_Sample	00-0C-43-28-60-20	1
ID : Unknown	default	00-18-02-4A-0A-6B	6
ID : Unknown	WinceWps	00-14-85-E3-D7-8B	7

AP1-WPS

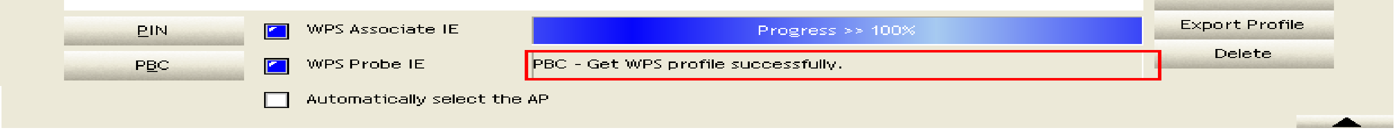
Pin Code: 64893945

Config Mode: Enrollee

PBC - Get WPS profile successfully.

Description of WPS Status Bar for PBC Config:

Figure 1.7-2B WPS Status Bar for PBC Config



PBC - Get WPS profile successfully.

① A successful PBC Configuration : Start PBC connection > Scanning AP > Begin associating to WPS AP > Associated to WPS AP > Sending EAPOL-Start > Sending EAP-Rsp (ID) > Receive EAP-Rsp (Start) > Sending M1 > Received M2 > Sending M3 > Received M4 > Sending M5 > Received M6 > Sending M7 > Received M8 > Sending EAP-Rsp (Done) > Configured > WPS status is disconnected > WPS status is connected successfully-SSID

② No PBC AP available: Scanning AP > No PBC AP available > Scanning AP > No PBC AP available >...

③ Too Many PBC AP available: Scanning AP > Too Many PBC AP available > Scanning AP > Too Many PBC AP available >...

④ When Errors occur within two-minutes of establishing a connection, the WPS status bar might report "WPS Eap process failed". If this happens one of the following error messages might appear: 1. Receive EAP with wrong NONCE; 2.Receive EAP without integrity; or 3.An inappropriate EAP-FAIL received.

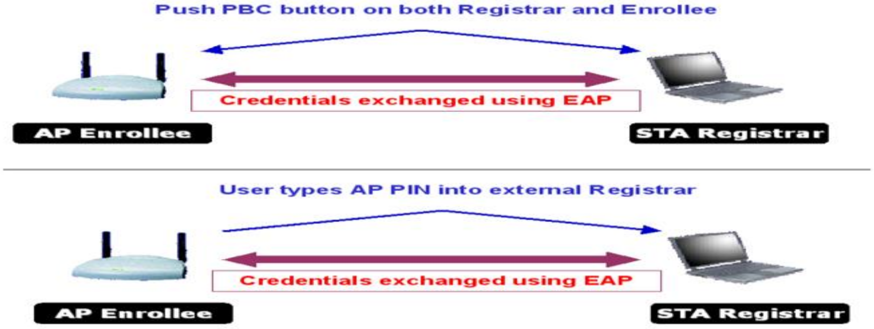
Description "Multiple PBC session overlaps":

①vDual bands: AP1 is a G-Band AP using PBC mode. (ID = 0x0004); AP2 is a A-Band AP using PBC mode. (ID = 0x0004); They have the same UUID-E; STA would regard these two APs as a dual-radio AP and select one band to connect.

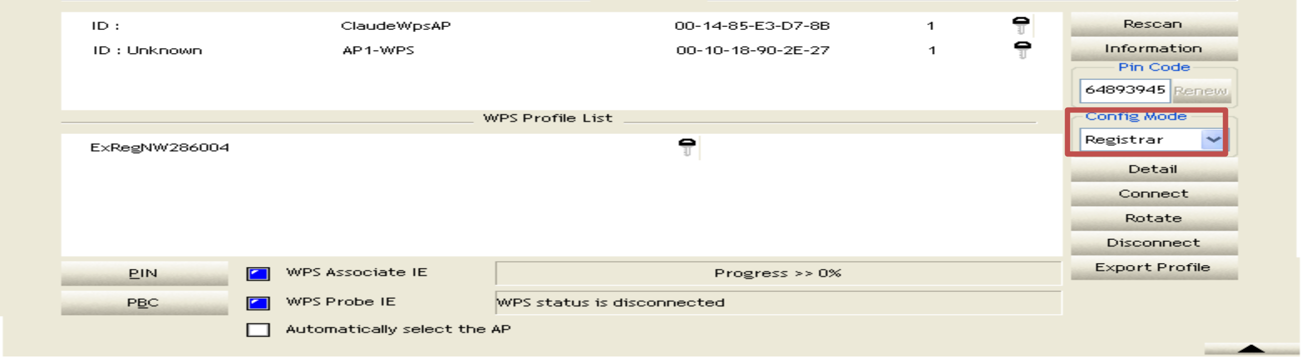
②vDifferent UUID-E :AP1 is a G-Band AP using PBC mode. (ID = 0x0004); AP2 is a G-Band AP using PBC mode. (ID = 0x0004); They have the different UUID-E; STA would regard these two APs as two different APs and wait until only one PBC AP is available.

1.7-4 Example of Configuring a Network/AP Using PIN or PBC Method

Figure 1.7-4A Configuring a Network/AP Using PIN or PBC Method


Push PBC button on both Registrar and Enrollee
Credentials exchanged using EAP
AP Enrollee
STA Registrar
User types AP PIN into external Registrar
Credentials exchanged using EAP
AP Enrollee
STA Registrar

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



ID : ClaudeWpsAP 00-14-85-E3-D7-8B 1
ID : Unknown AP1-WPS 00-10-18-90-2E-27 1

Pin Code: 64893945

Config Mode: Registrar

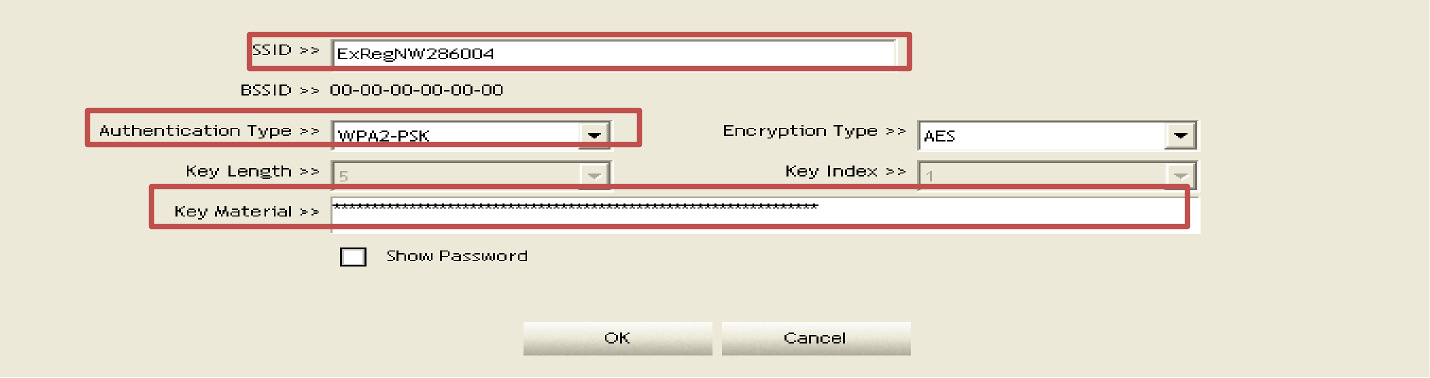
ExRegNW286004

☑ WPS Associate IE
☑ WPS Probe IE
☐ Automatically select the AP

Progress >> 0%

WPS status is disconnected

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



SSID >> ExRegNW286004

BSSID >> 00-00-00-00-00-00

Authentication Type >> WPA2-PSK

Encryption Type >> AES

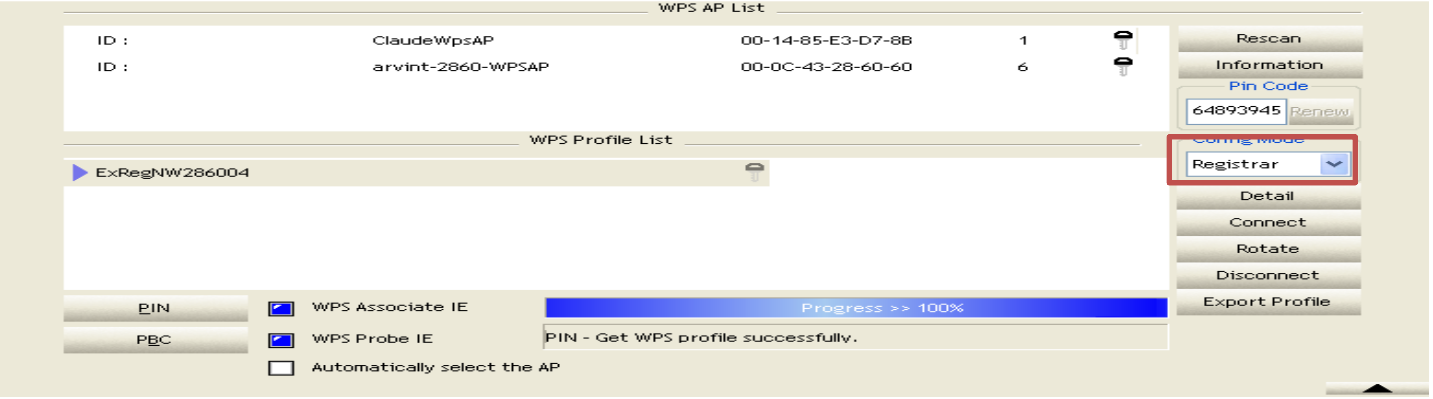
Key Length >> 5

Key Index >> 1

Key Material >> **

☐ Show Password

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 to those in section 1.7-2 (PIN Enrollee Setup or section) 1.7-3 (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.



ID : ClaudeWpsAP 00-14-85-E3-D7-8B 1
ID : arvint-2860-WPSAP 00-0C-43-28-60-60 6

Pin Code: 64893945

Config Mode: Registrar

ExRegNW286004

☑ WPS Associate IE
☑ WPS Probe IE
☐ Automatically select the AP

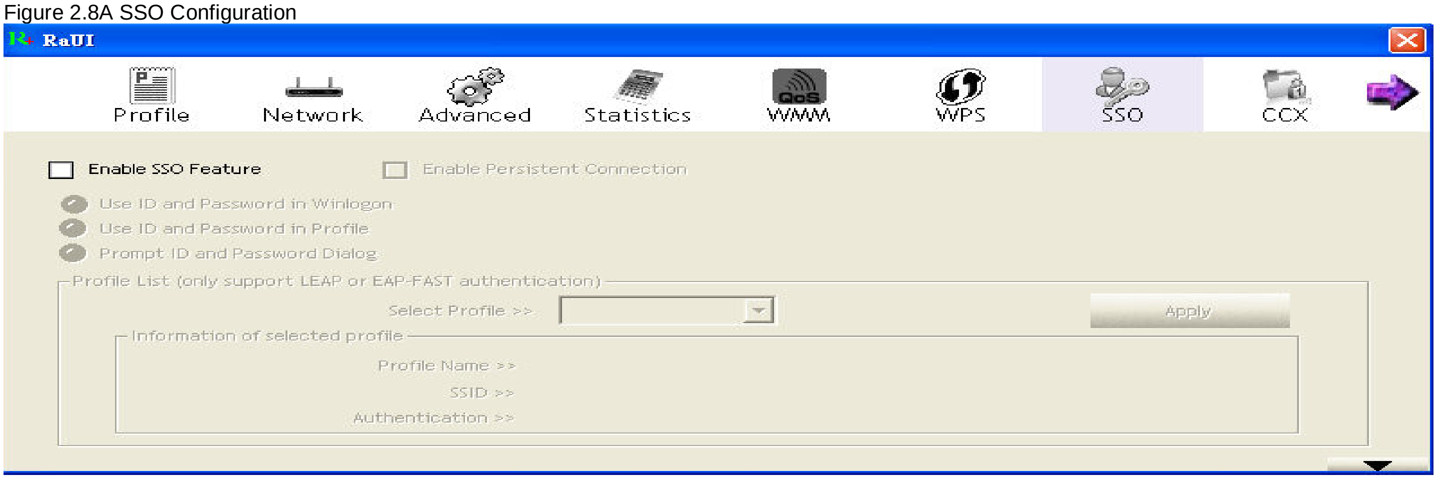
Progress >> 100%

PIN - Get WPS profile successfully.

1.8 SSO (Single Sign-On)

The SSO configuration page is shown below in Figure 2.8A.

Figure 2.8A SSO Configuration



☐ Enable SSO Feature
☐ Enable Persistent Connection
○ Use ID and Password in Winlogon
○ Use ID and Password in Profile
○ Prompt ID and Password Dialog
Profile List (only support LEAP or EAP-FAST authentication)
Select Profile >>
Information of selected profile
Profile Name >>
SSID >>
Authentication >>

Figure 2.8A Description of Fields:

① Enable SSO feature: Choose which SSO methods to log on.

1. Use ID and Password in Winlogon: Use the ID and password in Windows logon
2. Use ID and Password in Profile: Use the ID and password in RaUI profile settings
3. Prompt ID and Password in Dialog: Use the ID and password in pop-up authentication dialog

② Enable Persistent Connection: Use ID and Password for a previously activated Profile and don't show any authentication dialog.

③ Profile List (only support LEAP or EAP-FAST authentication).

1. Select Profile: Select a profile containing LEAP or EAP-Fast authentication
2. Information of selected profile: Profile information, such as profile name, SSID.

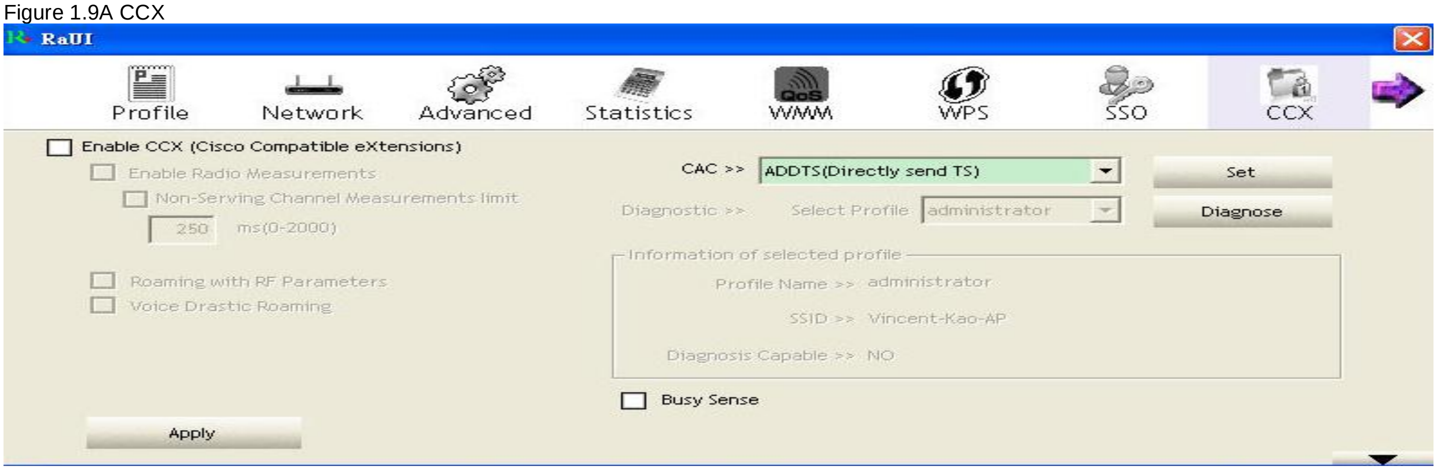
Figure 2.8A Description of Icons and Buttons:

① Apply Hit the Apply button to make the settings effective.

1.9 CCX (Cisco Compatible EXtensions)

The CCX configuration page is shown below in Figure 1.9A.

Figure 1.9A CCX



☐ Enable CCX (Cisco Compatible eXtensions)
☐ Enable Radio Measurements
☐ Non-Serving Channel Measurements limit
250 ms(0-2000)
☐ Roaming with RF Parameters
☐ Voice Drastic Roaming
CAC >> ADDTS(Directly send TS)
Diagnostic >> Select Profile administrator
Information of selected profile
Profile Name >> administrator
SSID >> Vincent-Kao-AP
Diagnosis Capable >> NO
☐ Busy Sense

Figure 1.9A Description of Fields:

①Enable CCX (Cisco Compatible eXtensions): Choose whether Cisco Compatible eXtensions are supported or not.

1. Enable Radio Measurement: Enable the radio measurement, the non-serving channel measurement limit is between 0 and 1023 milliseconds.
2. Roaming with RF Parameters: Roaming by a set of RF parameters from AP
3. Voice Drastic Roaming: Diagnose roaming function by voice traffic test
4. CAC (Tolerance) : Enable the call admission control
5. Diagnostic: Select a profile which the user want to diagnose, then hit the Diagnose button to perform the diagnostic test
6. Busy Sense: Force Wireless NIC to detect noise more sensitively

Figure 1.9A Description of Icons and Buttons:

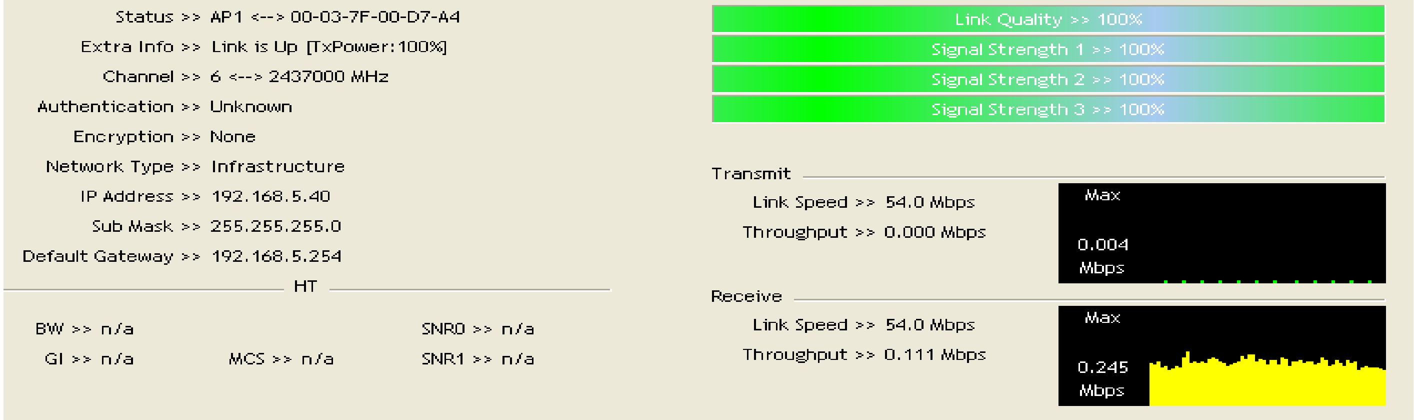
① Apply Hit the Apply button to make the settings effective.

1.10 About Ralink

Click "About" displays the wireless card and driver version information as shown in Figure 1.10A. Use it to connect to Ralink's website; view Configuration Utility, Driver, and EEPROM version information; and view the Wireless NIC MAC address.

1.11 Link Status

Figure 1.11A Link Status



Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> None
Network Type >> Infrastructure
IP Address >> 192.168.5.40
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

HT
BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps

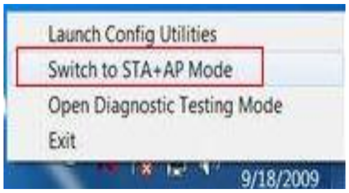
Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.111 Mbps

Figure 1.11A Description of Fields:
① Status : Current connection status. If no connection, if will show Disconnected. Otherwise, the SSID and BSSID will show here.
② Extra Info : Displays link status in use.
③ Channel : Displays current channel in use.
④ Authentication : Authentication mode in use.
⑤ Encryption : Encryption type in use.
⑥ Network Type : Network type in use.
⑦ IP Address : IP address of current connection.
⑧ Sub Mask : Sub mask of current connection.
⑨ Default Gateway : Default gateway about current connection.
⑩ Link Speed : Show current transmit rate and receive rate.
⑪ Throughput : Display transmits and receive throughput in unit of Mbps.
⑫ Link Quality : Display connection quality based on signal strength and TX/RX packet error rate.
⑬ Signal Strength 1 : Receive signal strength 1, user can choose to display as percentage or dBm format.
⑭ Signal Strength 2 : Receive signal strength 2, user can choose to display as percentage or dBm format.
⑮ Signal Strength 3 : Receive signal strength 3, user can choose to display as percentage or dBm format.
⑯ HT : Display current HT status in use, containing BW, GI, MCS, SNR0, and SNR1 value. (Show the information only for 802.11n wireless card.)

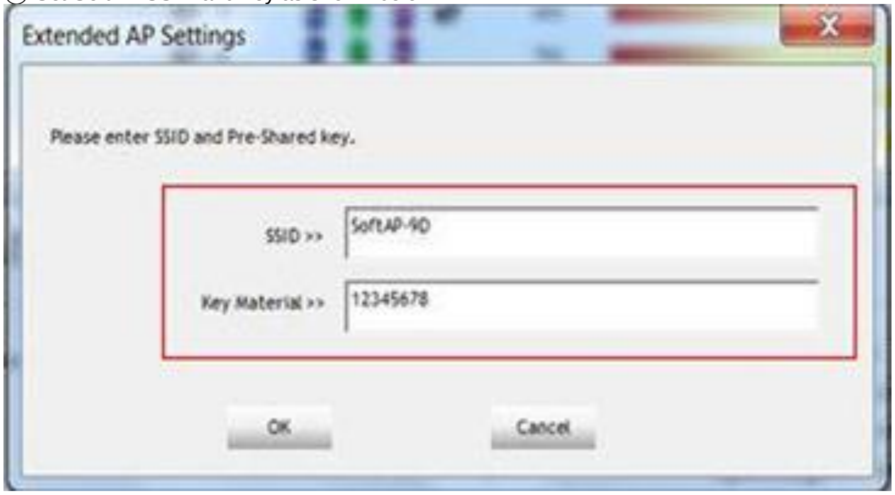
1.12 SoftAP (Only supported by Windows7)

Windows 7 allows the wireless device to be in both station (STA) and AP mode. Follow the steps listed below to open or close AP function.

① Right click the Ralink icon in the systems tray in the bottom right corner. Then Click "Switch to STA+AP mode" item in RaUI system tray menu as shown below.



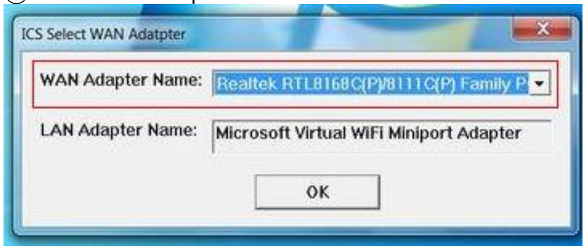
② Set SoftAP SSID and key as shown below.



Please enter SSID and Pre-Shared key.

SSID >> SoftAP-9D
Key Material >> 12345678

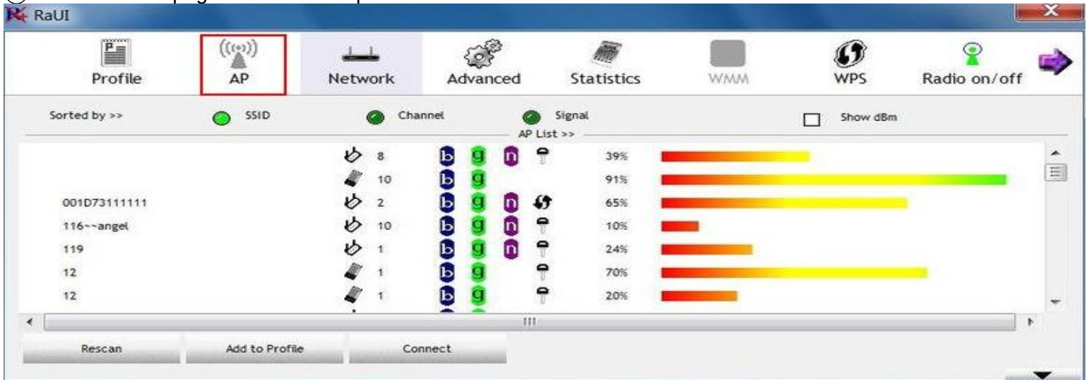
③ Select WAN adapter as shown below.



WAN Adapter Name: Realtek RTL8168C(P)/8111C(P) Family P

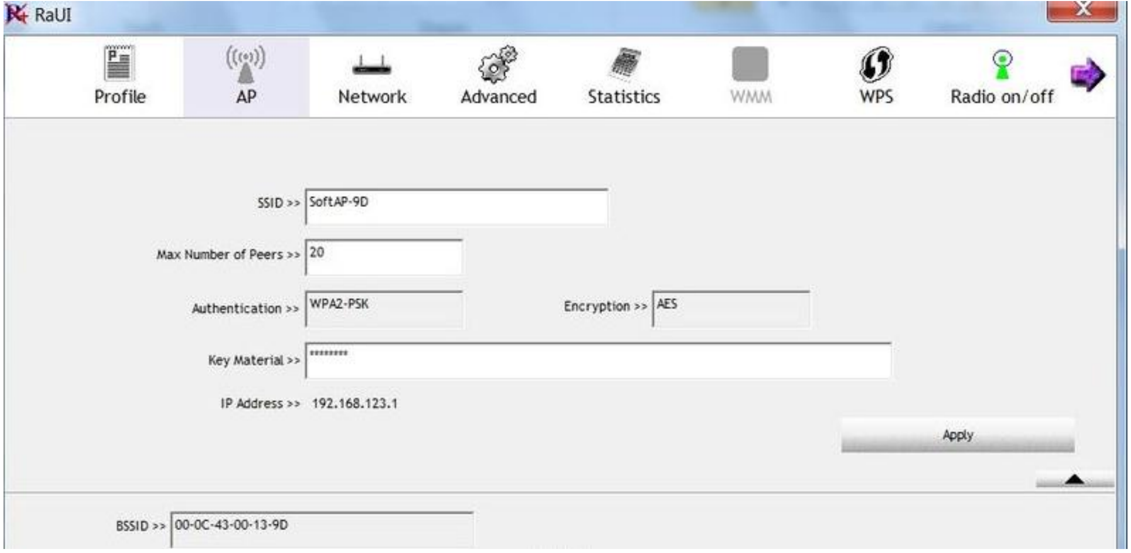
LAN Adapter Name: Microsoft Virtual WiFi Miniport Adapter

④ Select SoftAP page to set SoftAP parameter as shown below.



SSID	Channel	Signal
	8	39%
	10	91%
001D73111111	2	65%
116~~angel	10	10%
119	1	24%
12	1	70%
12	1	20%

⑤ Set SoftAP parameter in SoftAP page as shown below.



SSID >> SoftAP-9D

Max Number of Peers >> 20

Authentication >> WPA2-PSK

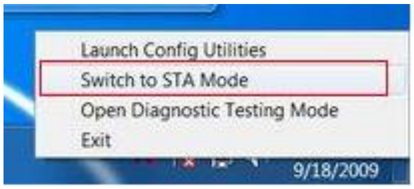
Encryption >> AES

Key Material >> ********

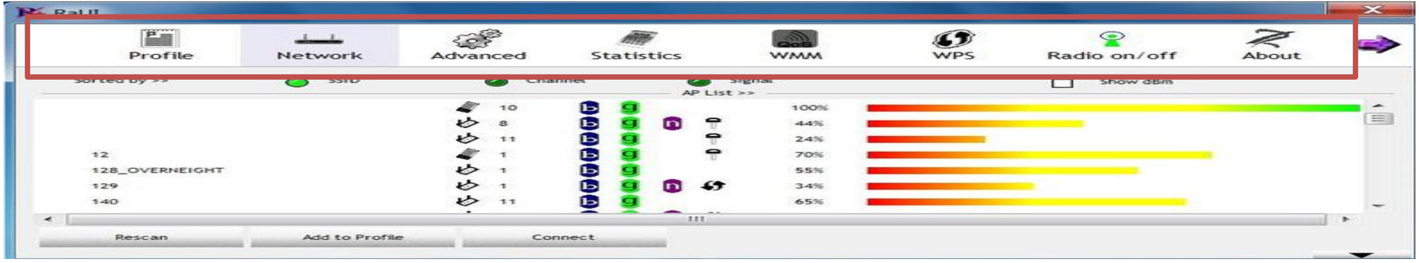
IP Address >> 192.168.123.1

BSSID >> 00-0C-43-00-13-9D

⑥ Right Click the Ralink Icon in the bottom right corner of your system tray. Click "Switch to STA mode" to close SoftAP function as shown in below.



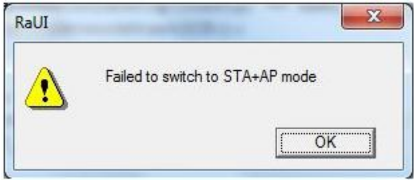
⑦ SoftAP function is closed as shown in the below image by the absence of the AP Icon on the menu bar.



SSID	Channel	Signal
	10	100%
	8	44%
	11	24%
12	1	70%
128_OVERNEIGHT	1	55%
129	1	34%
140	11	65%

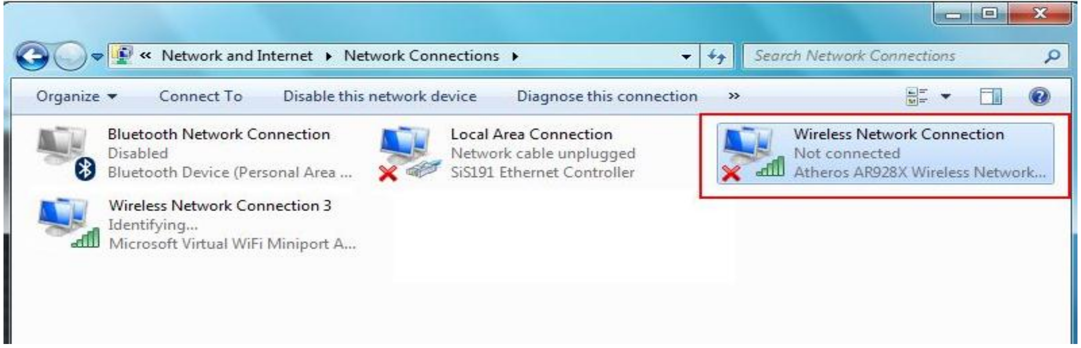
1.12-1 Trouble starting SoftAP in Windows 7

If you are attempting to switch to STA+AP mode and the pop-up message show below appears take the following actions to fix this issue:



Failed to switch to STA+AP mode

① Because virtual wi-fi miniport adapter is enabled for one wireless adapter, please disable other non-Ralink wireless adapters as show below, then try switching to STA+AP mode again.


« Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Connect To
Disable this network device
Diagnose this connection
»

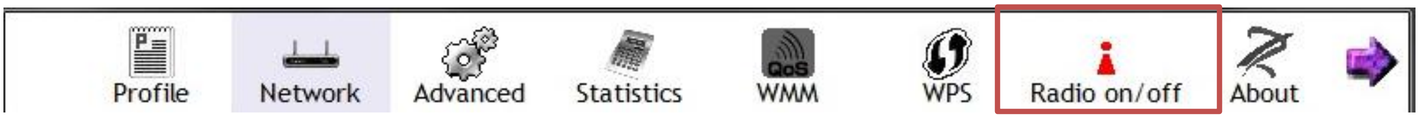
Bluetooth Network Connection
Disabled
Bluetooth Device (Personal Area ...

Local Area Connection
Network cable unplugged
SiS191 Ethernet Controller

Wireless Network Connection
Not connected
Atheros AR928X Wireless Network...

Wireless Network Connection 3
Identifying...
Microsoft Virtual WiFi Miniport A...

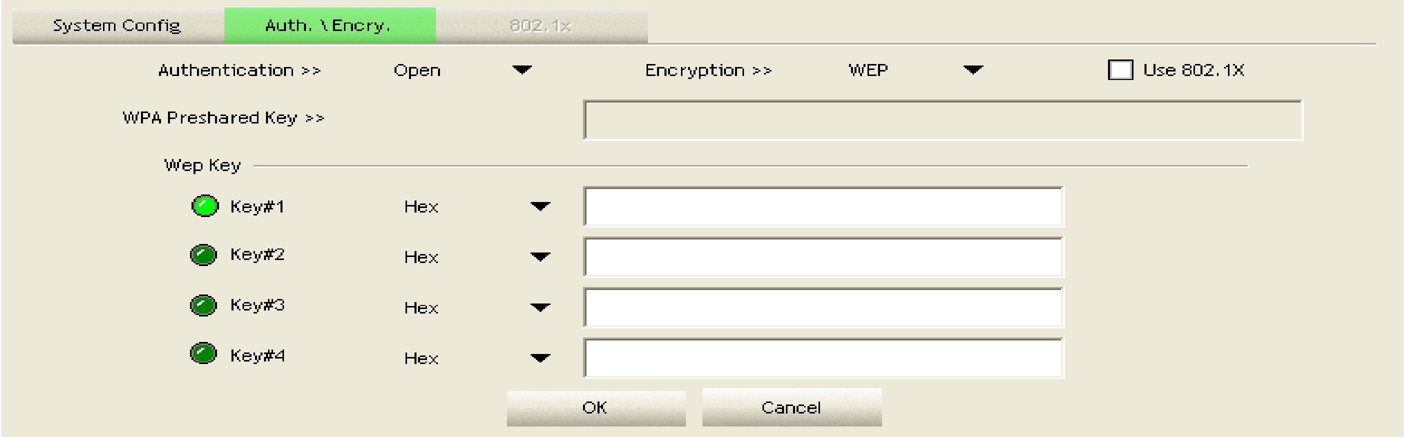
② The Radio must be turned on first if you want to use STA+AP mode. If radio is turned off and you try to switch to STA+AP mode as shown below the pop-up message shown above will appear.



2.0 Security

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

Figure 2.1A Auth.\Encry. Settings



Authentication >> Open
Encryption >> WEP
☐ Use 802.1X
WPA Preshared Key >>
Wep Key
● Key#1 Hex
● Key#2 Hex
● Key#3 Hex
● Key#4 Hex

Figure 2.1A Description of Fields:

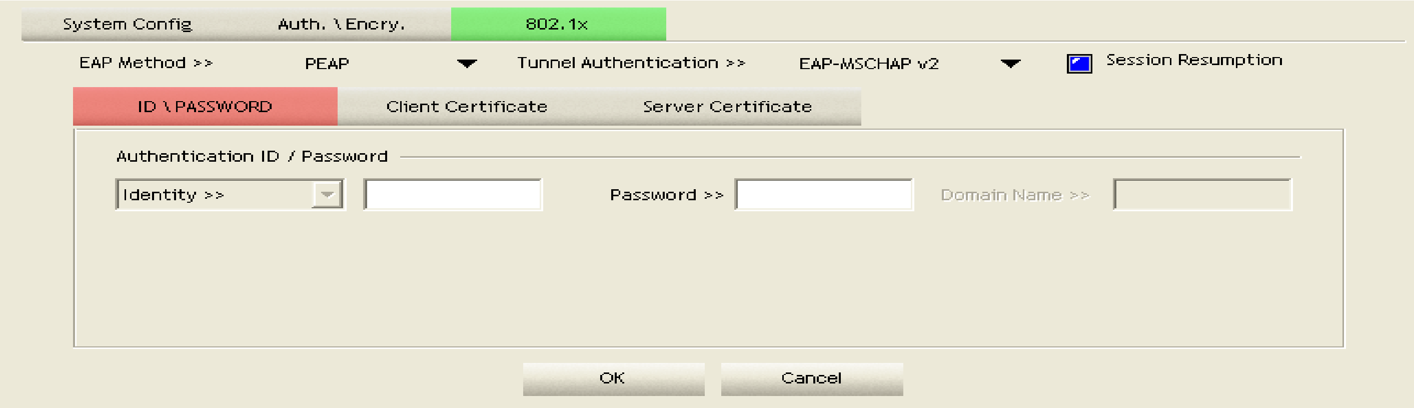
① Authentication Type: There are 7 authentication modes supported by RaUI. They are Open, Shared, WPA and WPA-PSK, WPA2 and WPA2-PSK.
② Encryption Type: For open and shared authentication mode, the available encryption types are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.
③ 8021X: This is introduced in Section 2.2.
④ Pre-shared Key: This is the shared key between the AP and STA. If operating in WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.
⑤ WEP Key: Only valid when using WEP encryption algorithm. The key must match the AP's key. There are several formats to enter the keys.

1. Hexadecimal - 40bits: 10 Hex characters.
2. Hexadecimal - 128bits: 32Hex characters.
3. ASCII - 40bits: 5 ASCII characters.
4. ASCII - 128bits: 13 ASCII characters.

2.2 802.1X Settings

802.1x is used for authentication of the "WPA" and "WPA2" certificate by the server.

Figure 2.2A 801.2X Settings



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

☑ Session Resumption

Figure 2.2A Description of Fields:

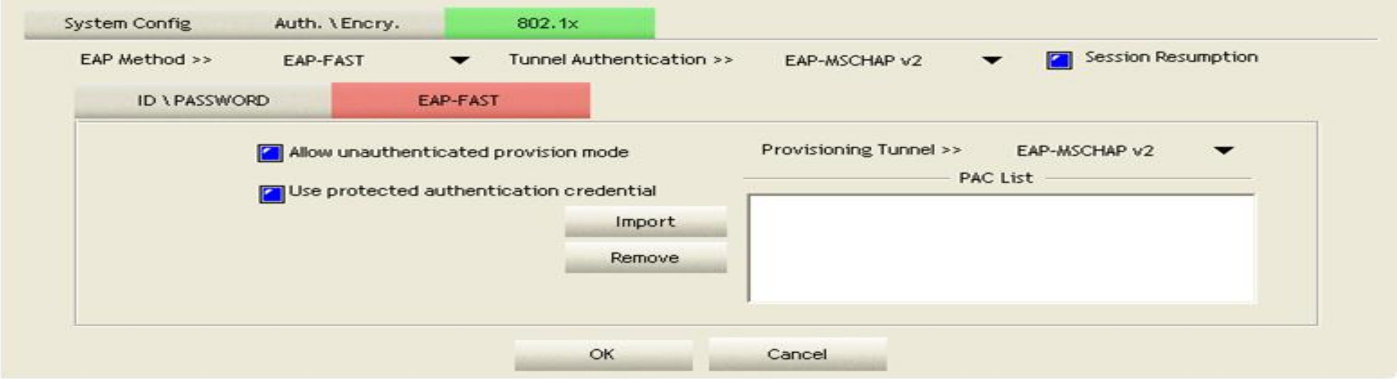
Authentication Types:

① PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authenticates data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.

② TLS/Smart Card: 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.

③ TTLS: Tunneled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

④ EAP-FAST: Flexible Authentication via Secure Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be supplied (distributed one time) to the client either manually or automatically. Manually, it is delivered to the client via disk or a secured network distribution method. Automatically, it is supplied as an in-band, over the air, distribution. Tunnel authentication, only supports "Generic Token Card" authentication. (See figure and description below for more information.)



EAP Method >> EAP-FAST

Tunnel Authentication >> EAP-MSCHAP v2

☑ Session Resumption

☑ Allow unauthenticated provision mode

☑ Use protected authentication credential

Provisioning Tunnel >> EAP-MSCHAP v2

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

⑤LEAP: 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.

⑥ MD5-Challenge: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.

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

⑦ Tunnel Authentication:

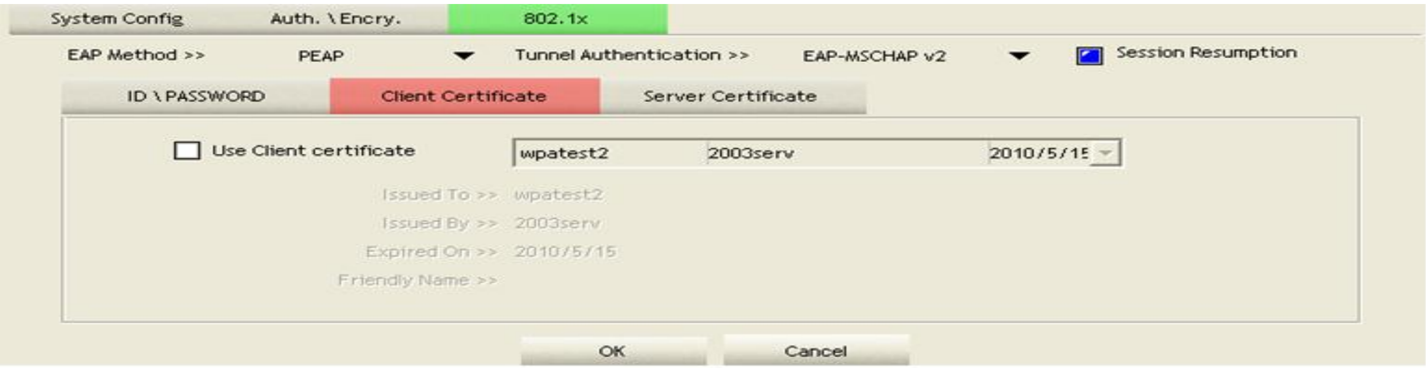
1. Protocol: Tunnel protocol, List information include "EAP-MSCHAP v2", "EAP-TLS/Smart card", "Generic Token Card", "CHAP", "MS-CHAP", "MS CHAP-V2", "PAP" and "EAP-MD5".
2. Tunnel Identity: Identity for tunnel.
3. Tunnel Password: Password for tunnel.

ID/Password

① Authentication ID/Password: The identity, password and domain name for server. Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain names can be keyed in the blank space.

② Tunnel ID/Password: Identity and Password for the server.

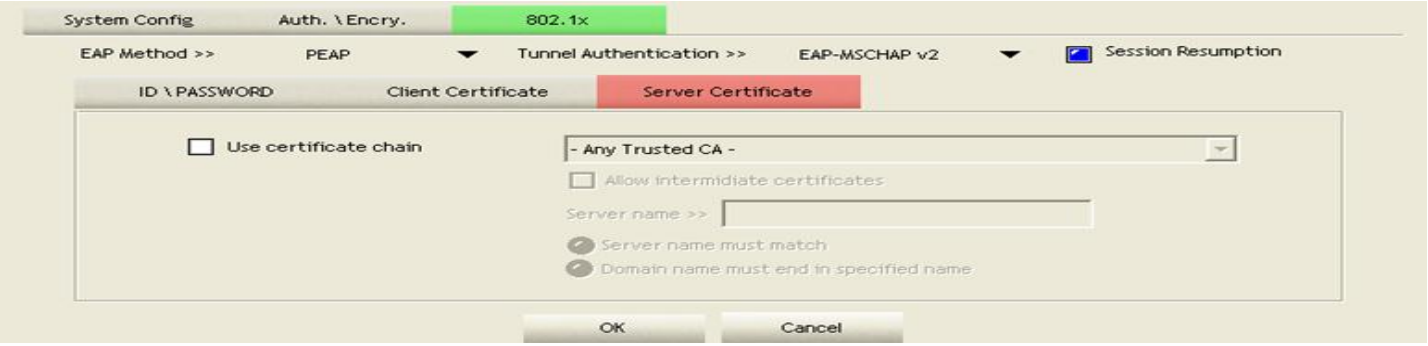
Client Certification



EAP Method >> PEAP
Tunnel Authentication >> EAP-MSCHAP v2
☑ Session Resumption
☐ Use Client certificate wpatest2 2003serv 2010/5/15
Issued To >> wpatest2
Issued By >> 2003serv
Expired On >> 2010/5/15
Friendly Name >>

① Use Client certificate: Client certificate for server authentication.

Server Certification



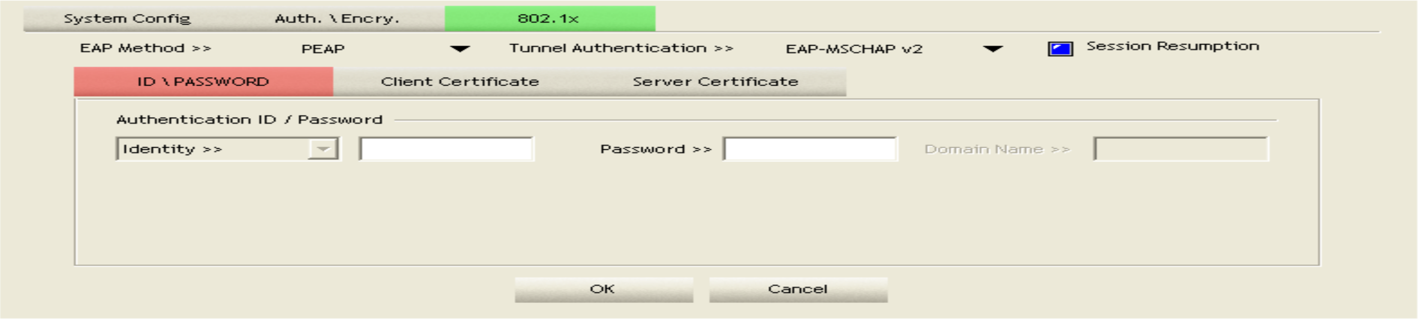
EAP Method >> PEAP
Tunnel Authentication >> EAP-MSCHAP v2
☑ Session Resumption
☐ Use certificate chain - Any Trusted CA -
☐ Allow intermidiate certificates
Server name >>
○ Server name must match
○ Domain name must end in specified name

① Certificate issuer: Select the server that issues the certificate.
② Allow intermediate certificates: It must be in the server certificate chain between the server certificate and the server specified in the "certificate issuer must be" field.
③ Server name: Enter an authentication sever root.

2.3 Example of Reconnecting an 802.1x Authenticated Connection after the 802.1x Authenticated connection has Failed in Profile

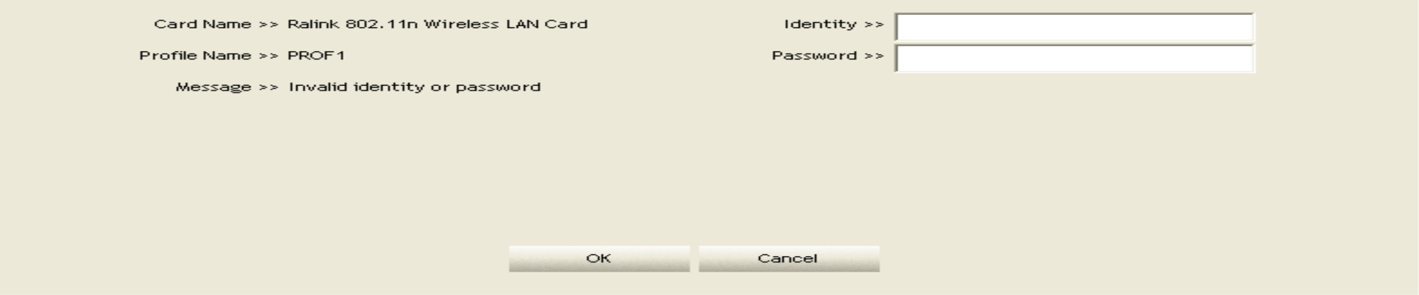
There are two situations where a user is able to reconnect an 802.1x authenticated connection and authenticate successfully after an 802.1x authenticated connection has failed on the profile page. They are as follows: When keying in an identity, or there is password or domain name error.

① Authentication type chooses "PEAP", key identity into test. Tunnel Protocol is "EAP-MSCHAP-v2, the tunnel identity and tunnel password are tested. Those settings are the same as our intended AP's setting.



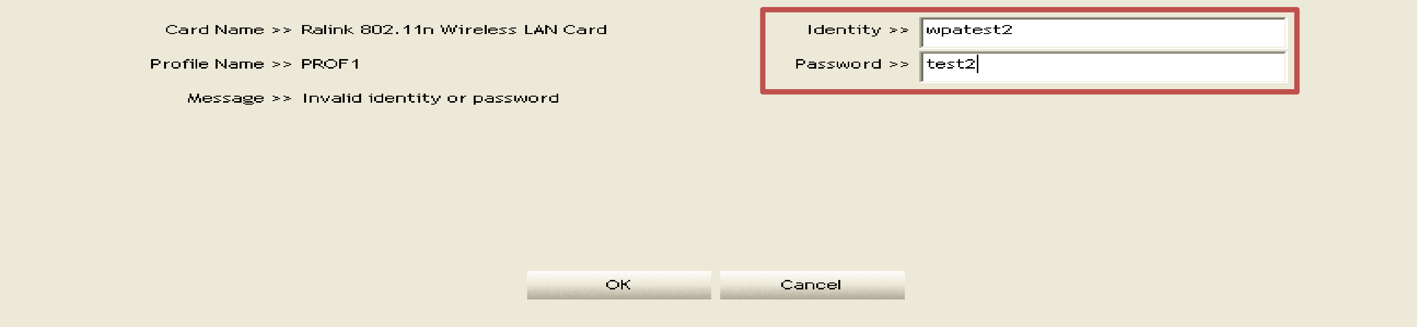
EAP Method >> PEAP
Tunnel Authentication >> EAP-MSCHAP v2
☑ Session Resumption
Authentication ID / Password
Identity >>
Password >>
Domain Name >>

② After keying in the identity and password errors, the result will appear as in the image below.



Card Name >> Ralink 802.11n Wireless LAN Card
Profile Name >> PROF1
Message >> Invalid identity or password
Identity >>
Password >>

③ If you want to disconnect, click "Cancel" on the Authentication Failure dialog box. If you want to reconnect, key in the identity into the identity field. The tunnel identity is wpatest2 and the tunnel password is test2. Those setting are the same as our intended AP's setting.



Card Name >> Ralink 802.11n Wireless LAN Card

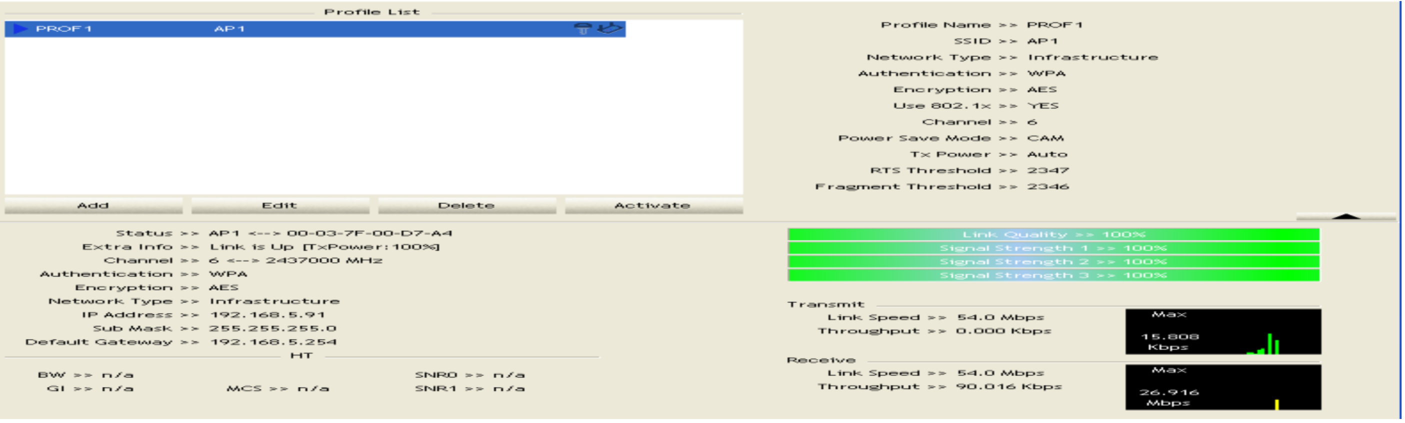
Profile Name >> PROF1

Message >> Invalid identity or password

Identity >> wpatest2

Password >> test2

④ Click "OK". If it has connected successfully. The result will appear as the below image.



Profile List

PROF1 AP1

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> WPA
Encryption >> AES
Network Type >> Infrastructure
IP Address >> 192.168.5.91
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

HT
BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Profile Name >> PROF1
SSID >> AP1
Network Type >> Infrastructure
Authentication >> WPA
Encryption >> AES
Use 802.1x >> YES
Channel >> 6
Power Save Mode >> CAM
Tx Power >> Auto
RTS Threshold >> 2347
Fragment Threshold >> 2346

Link Quality >> 100%
Signal Strength 1 >> 100%
Signal Strength 2 >> 100%
Signal Strength 3 >> 100%

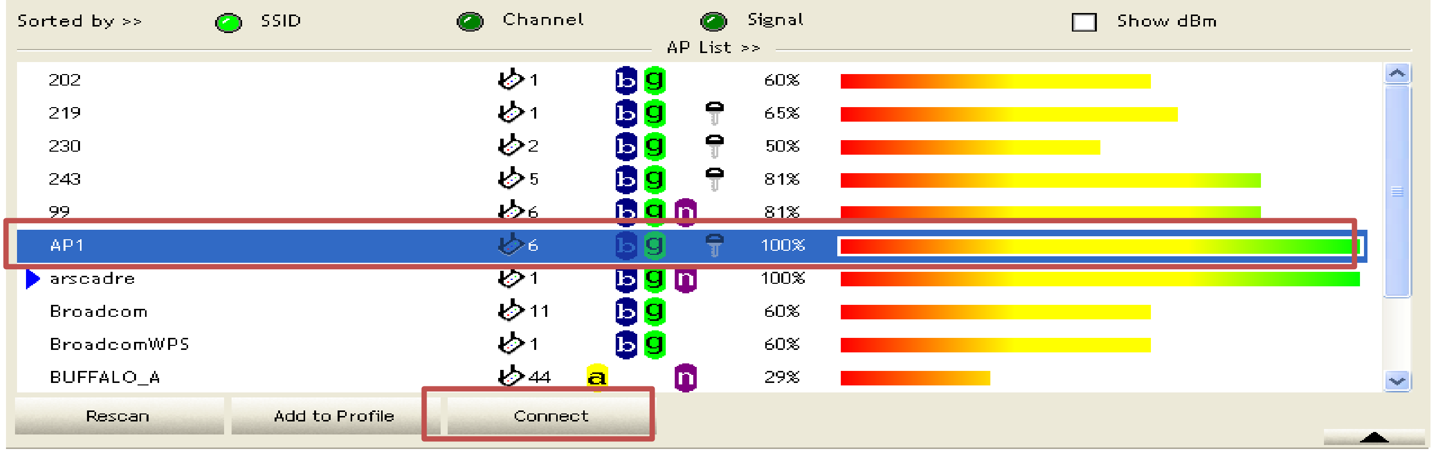
Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Kbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 90.016 Kbps

2.4 Example of Configuring a Connection with WEP On

Follow the 4 simple steps listed below to configure a connection with WEP On

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

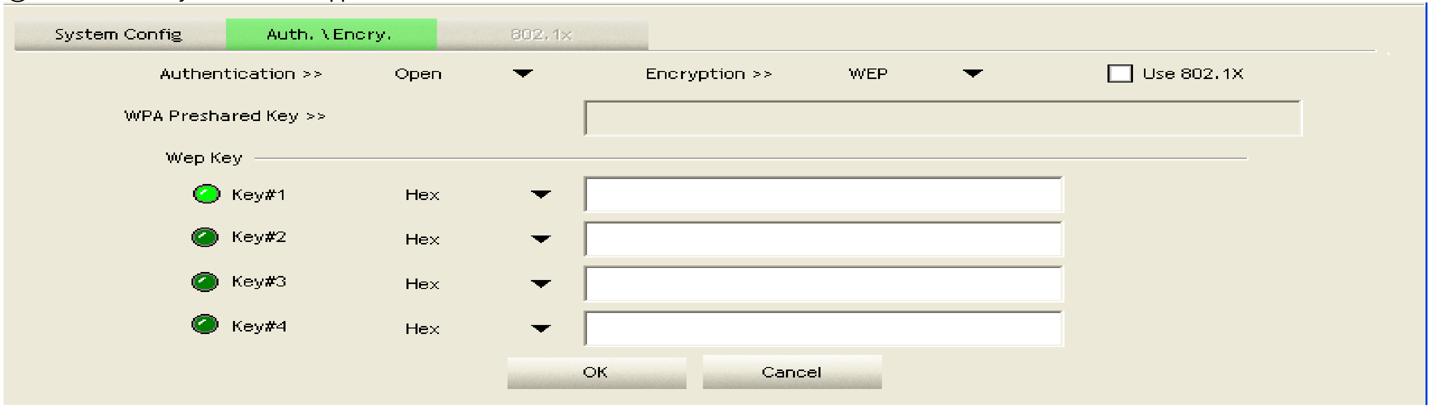


Sorted by >> ● SSID ● Channel ● Signal ☐ Show dBm

AP List >>

SSID	Channel		Signal
202	1	b g	60%
219	1	b g	65%
230	2	b g	50%
243	5	b g	81%
99	6	b g n	81%
AP1	6	b g	100%
arscadre	1	b g n	100%
Broadcom	11	b g	60%
BroadcomWPS	1	b g	60%
BUFFALO_A	44	a n	29%

② The Auth.\Encry. function will appear as shown below.



Authentication >> Open

Encryption >> WEP

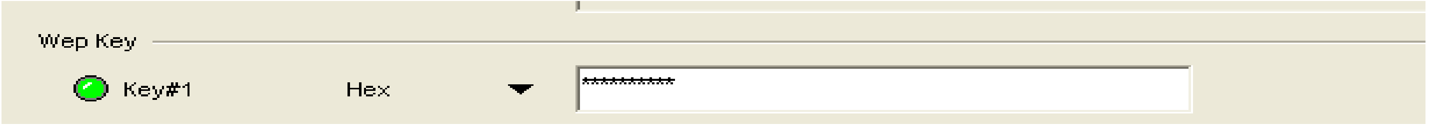
☐ Use 802.1X

WPA Preshared Key >>

Wep Key

● Key#1 Hex
○ Key#2 Hex
○ Key#3 Hex
○ Key#4 Hex

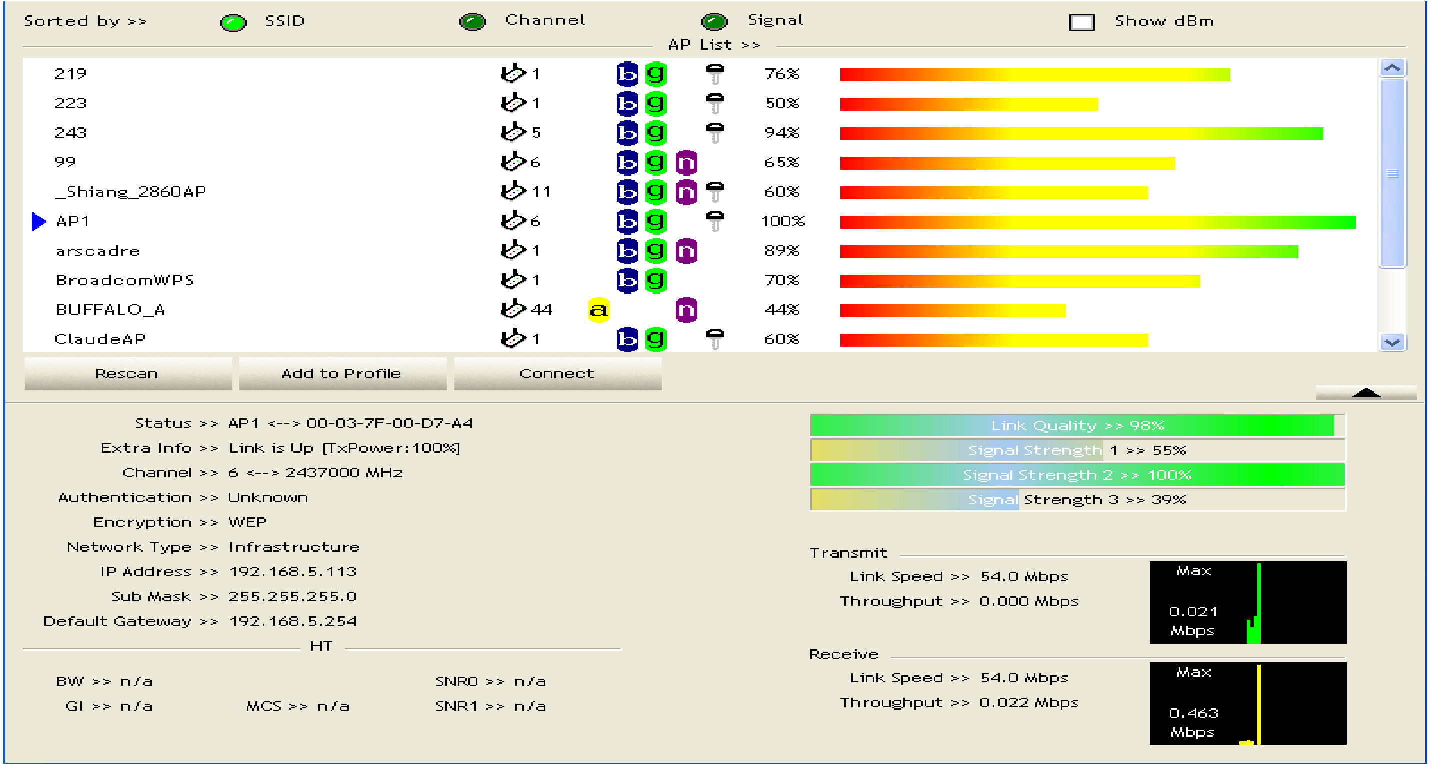
③ Enter 1234567890 in the Key#1 Hexadecimal field. This value is same as our intended AP's setting.



Wep Key

● Key#1 Hex ***********

④ Click "OK". The dialog box shown below will appear



Sorted by >> ● SSID ● Channel ● Signal ☐ Show dBm

AP List >>

SSID	Channel	Mode	Signal
219	1	b g	76%
223	1	b g	50%
243	5	b g	94%
99	6	b g n	65%
_Shiang_2860AP	11	b g n	60%
AP1	6	b g	100%
arscadre	1	b g n	89%
BroadcomWPS	1	b g	70%
BUFFALO_A	44	a n	44%
ClaudeAP	1	b g	60%

Status >> AP1 <--> 00-03-7F-00-D7-A4
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437000 MHz
Authentication >> Unknown
Encryption >> WEP
Network Type >> Infrastructure
IP Address >> 192.168.5.113
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.5.254

HT

BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Link Quality >> 98%
Signal Strength 1 >> 55%
Signal Strength 2 >> 100%
Signal Strength 3 >> 39%

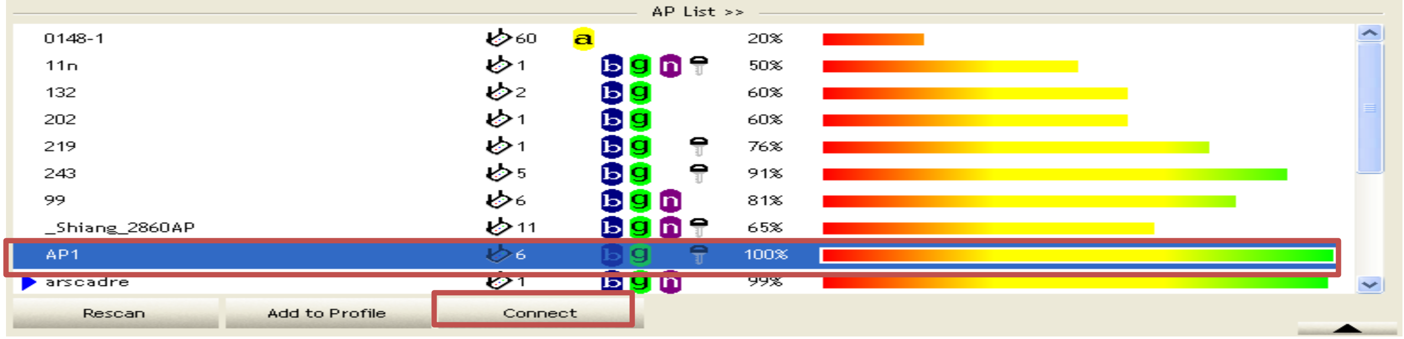
Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Mbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 0.022 Mbps

2.5 Example to Configure Connection with WPA-PSK

Follow the four simple steps listed below to configure a connection with WPA-PSK.

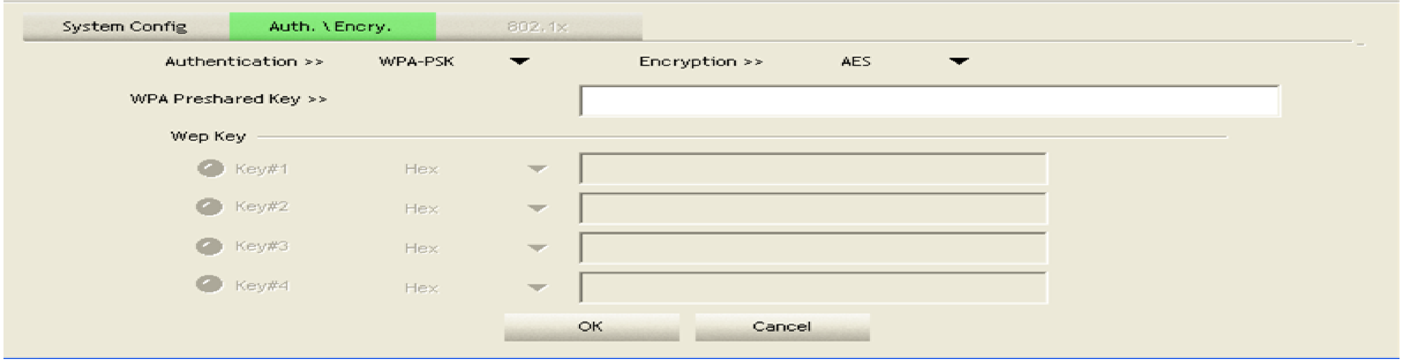
① Select the AP with a WPA-PSK authentication mode and click "Connect".



AP List >>

SSID	Channel	Mode	Signal
0148-1	60	a	20%
11n	1	b g n	50%
132	2	b g	60%
202	1	b g	60%
219	1	b g	76%
243	5	b g	91%
99	6	b g n	81%
_Shiang_2860AP	11	b g n	65%
AP1	6	b g	100%
arscadre	1	b g n	99%

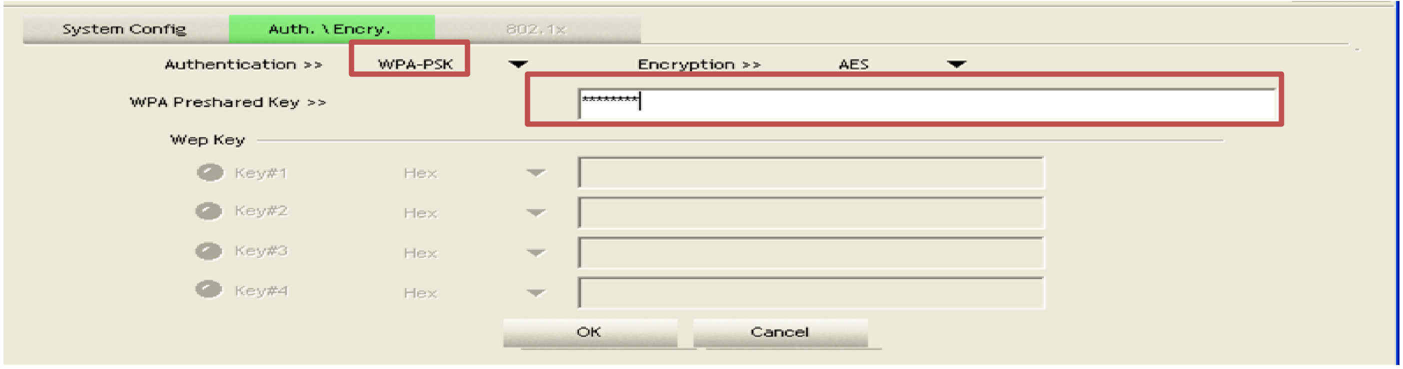
② Auth.\Encry. function appears.



Authentication >> WPA-PSK
Encryption >> AES
WPA Preshared Key >>

Wep Key

③ Select WPA-PSK as the Authentication Type. Select TKIP or AES encryption. Enter the WPA Pre-Shared Key as "12345678".



Authentication >> WPA-PSK

Encryption >> AES

WPA Preshared Key >> ********

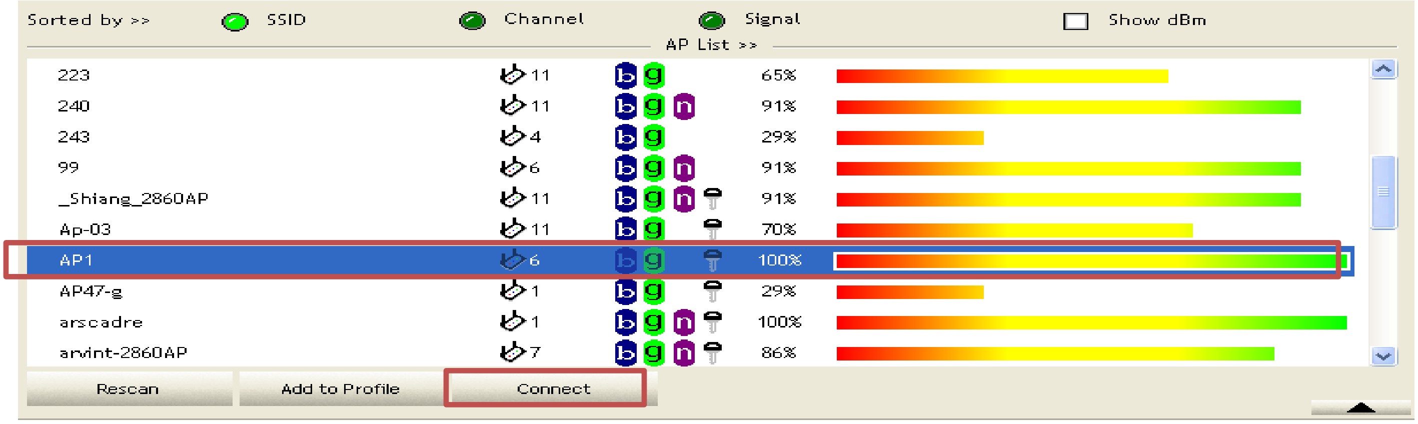
Key#1 Hex
Key#2 Hex
Key#3 Hex
Key#4 Hex

④ Click "OK" the resulting screen should look like the image from step 4 in the last section. ***Be careful****, if the you entered the incorrect WPA Pre-Shared Key you won't be able to exchange any data frames even though the AP can be connected.*

2.6 Example to Configure Connection with WPA

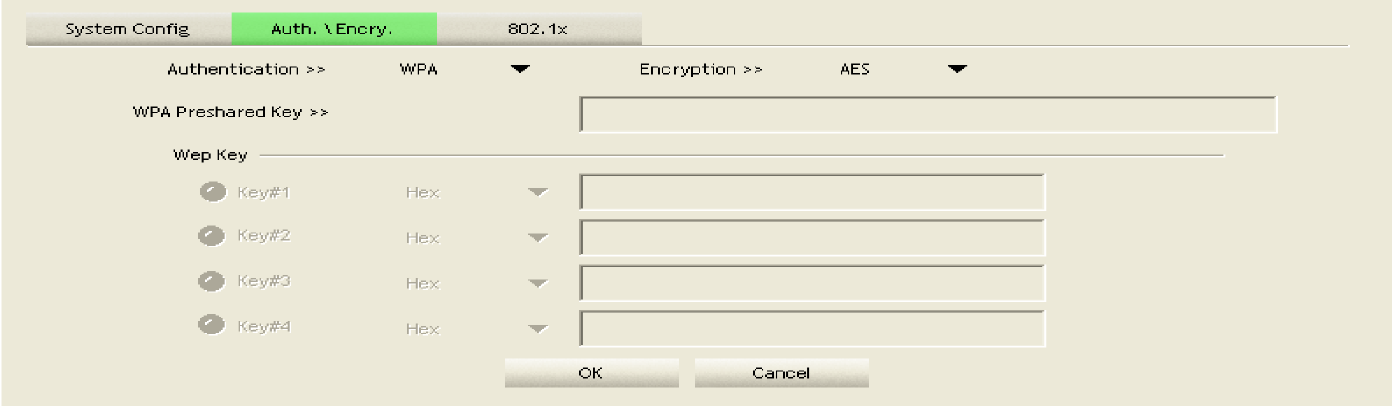
Follow the three easy steps listed below to configure a connection with WPA.

① Select an AP with WPA authentication mode and click "Connect".



223	11	b g	65%
240	11	b g n	91%
243	4	b g	29%
99	6	b g n	91%
_Shiang_2860AP	11	b g n	91%
Ap-03	11	b g	70%
AP1	6	b g	100%
AP47-g	1	b g	29%
arscadre	1	b g n	100%
arvint-2860AP	7	b g n	86%

② The Auth.\Encry. function will open at the bottom of the screen. (If AP setup security to Both (TKIP + AES), the system will define that AES security is severe.)



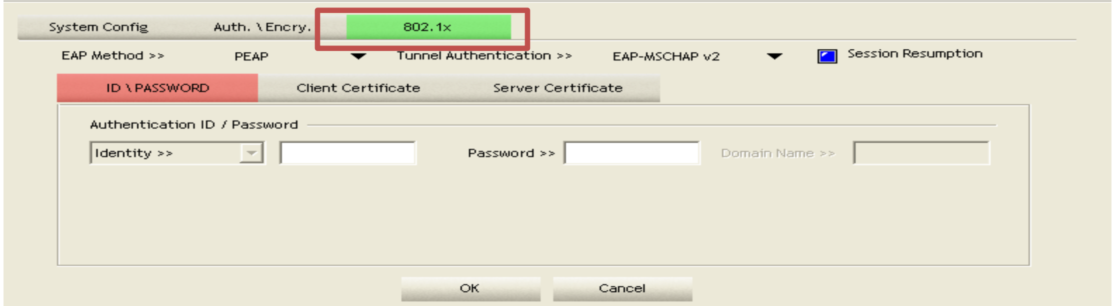
Authentication >> WPA

Encryption >> AES

WPA Preshared Key >>

Key#1 Hex
Key#2 Hex
Key#3 Hex
Key#4 Hex

③ Click the "8021X" tab and the settings page will appear.



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

☑ Session Resumption

Identity >>

Password >>

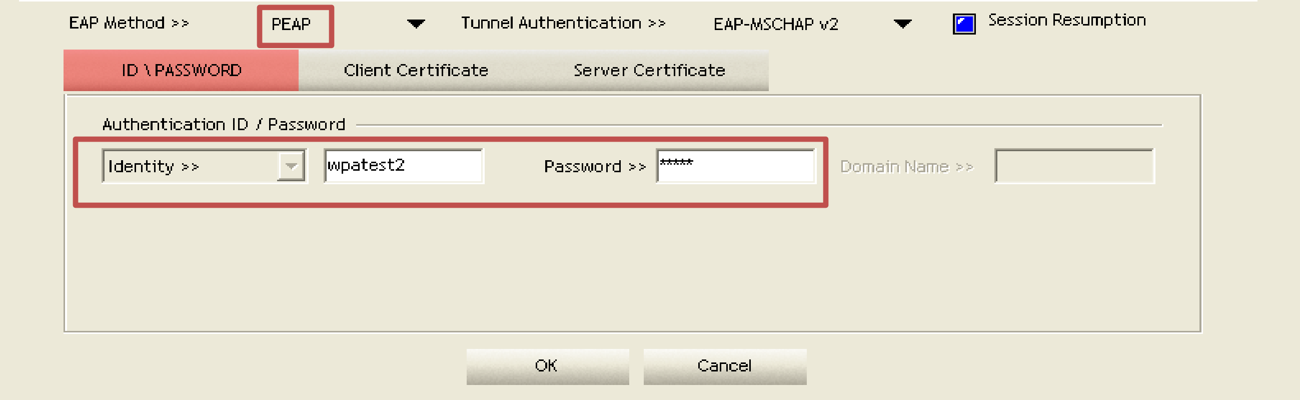
Domain Name >>

④Instructions for setting up each Authentication type:

*If you want to disconnect, please click cancel button in Authentication Status function. *In Profile function, show "Profile Name" option only when adding AP to Profile function.

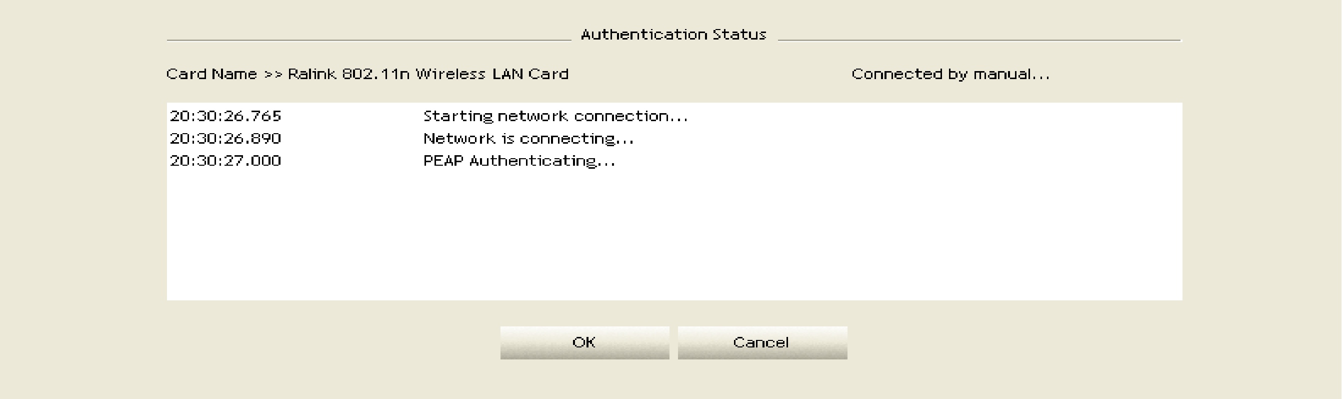
① **PEAP**:

1. Select "PEAP" as the Authentication type from the drop-down list. Key-in "wpatest2" for the identity. "Select "EAP-MSCHAP v2" from the drop-down list for tunnel authentication and key-in the tunnel identity "wpatest2" and the tunnel password "test2". These settings are the same as our intended AP's setting.



EAP Method >> PEAP
Tunnel Authentication >> EAP-MSCHAP v2
☑ Session Resumption
Identity >> wpatest2
Password >> *****
Domain Name >>

2. Click OK. The result should look like the dialog box below.

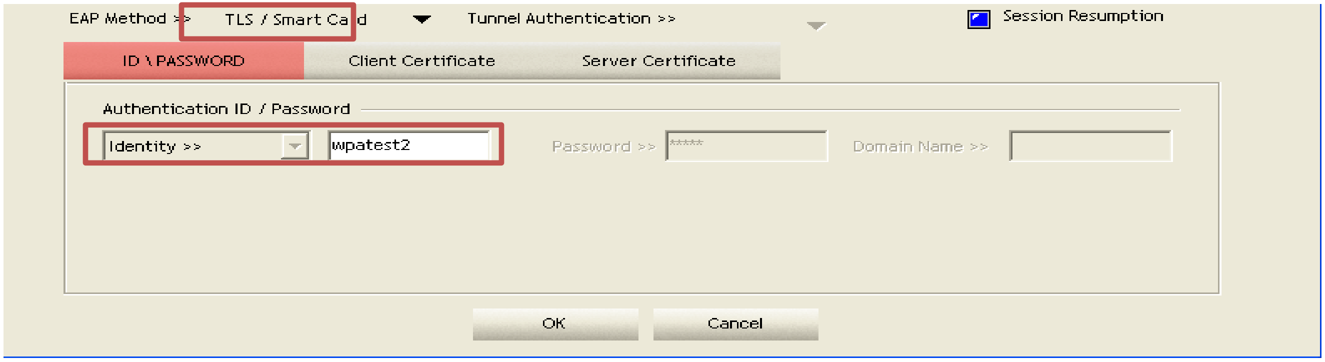


Card Name >> Ralink 802.11n Wireless LAN Card
Connected by manual...

```
20:30:26.765          Starting network connection...
20:30:26.890          Network is connecting...
20:30:27.000          PEAP Authenticating...
```

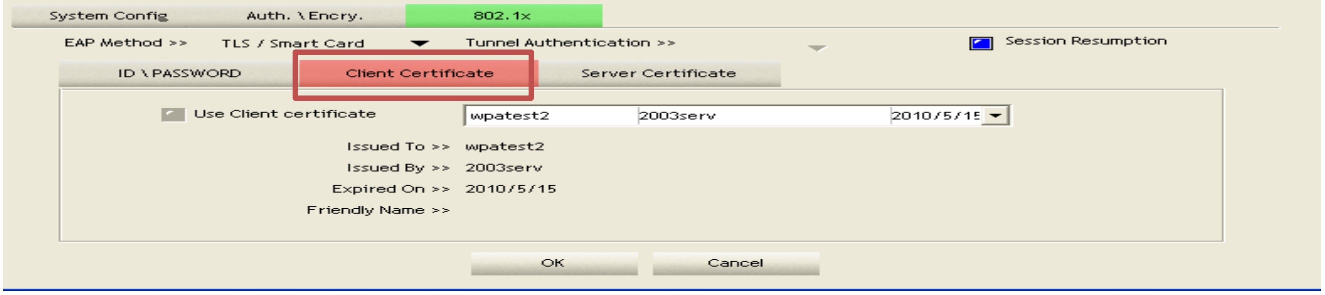
② **TLS / Smart Card:**

1. "Select TLS / Smart Card" from the Authentication type drop-down list. TLS only requires the identification to be set as "wpatest2" for server authentication.



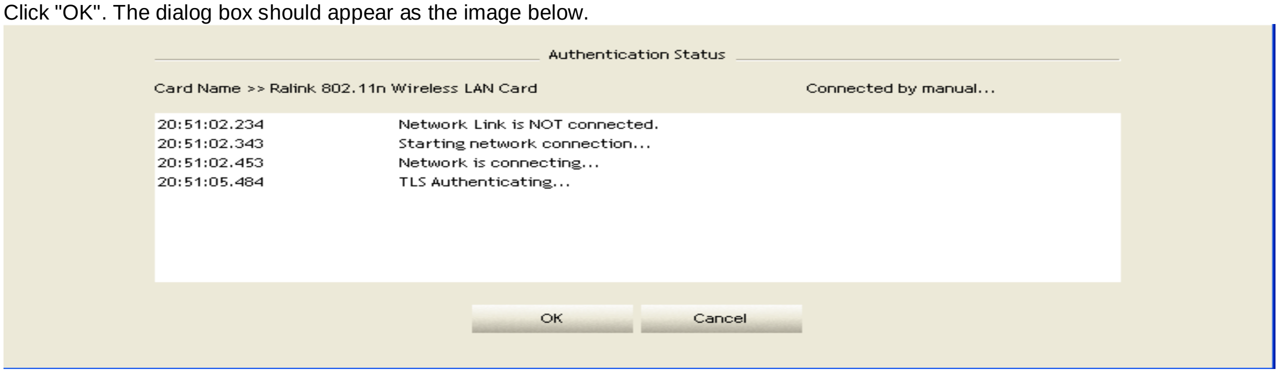
EAP Method >> TLS / Smart Card
Tunnel Authentication >>
☑ Session Resumption
Identity >> wpatest2
Password >> *****
Domain Name >>

2. TLS must use client certification. Click "Client Certification" and select a certification for server authentication.



EAP Method >> TLS / Smart Card
Tunnel Authentication >>
☑ Session Resumption
☑ Use Client certificate   wpatest2   2003serv   2010/5/15
Issued To >> wpatest2
Issued By >> 2003serv
Expired On >> 2010/5/15
Friendly Name >>

3. Click "OK". The dialog box should appear as the image below.



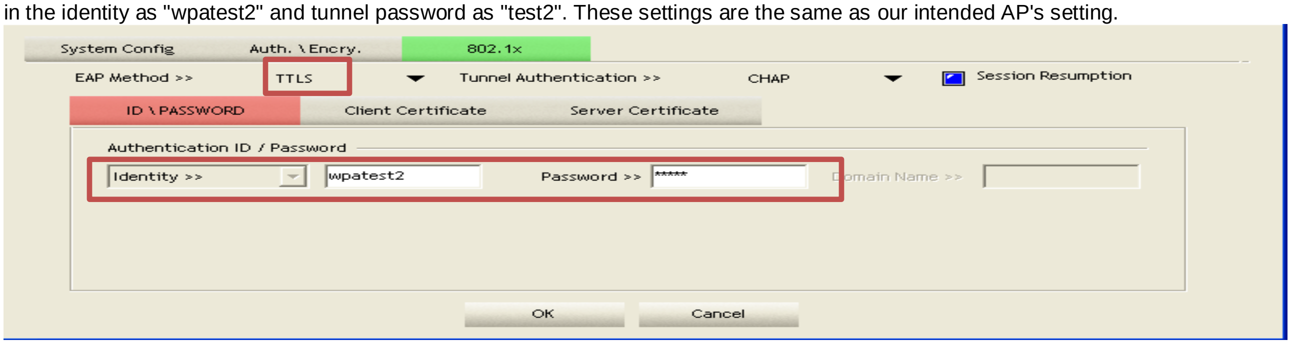
Authentication Status

Card Name >> Ralink 802.11n Wireless LAN Card   Connected by manual...

```
20:51:02.234              Network Link is NOT connected.
20:51:02.343              Starting network connection...
20:51:02.453              Network is connecting...
20:51:05.484              TLS Authenticating...
```

③TTLS:

1. Select TTLS from the Authentication type drop-down list. Key-in the identity as "wpatest2". Select CHAP for tunnel authentication, and key-in the identity as "wpatest2" and tunnel password as "test2". These settings are the same as our intended AP's setting.

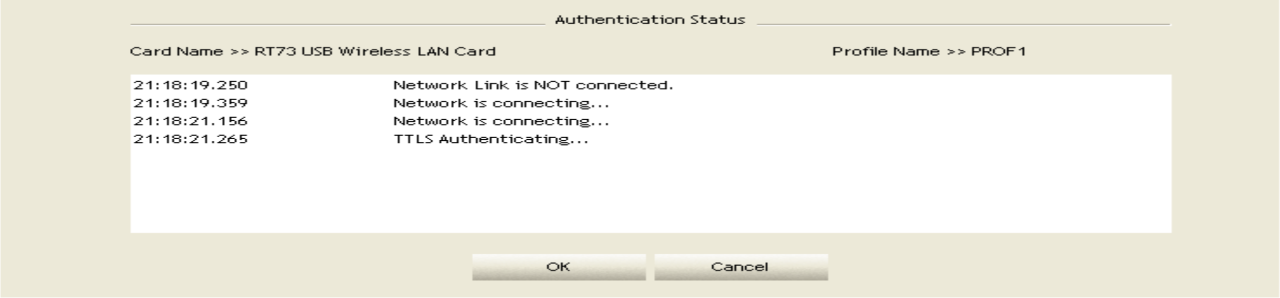


EAP Method >> TTLS   Tunnel Authentication >> CHAP   Session Resumption

Authentication ID / Password

Identity >> wpatest2   Password >> *****   Domain Name >>

2. Click "OK". The dialog box should appear as the image below.



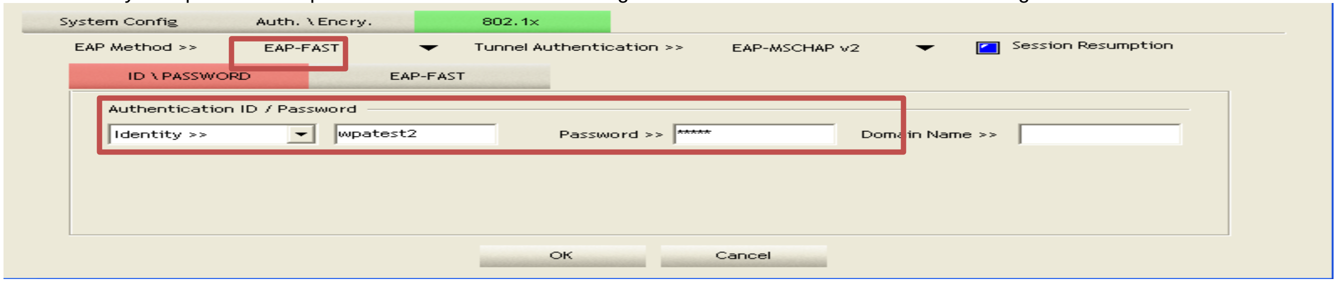
Authentication Status

Card Name >> RT73 USB Wireless LAN Card   Profile Name >> PROF1

```
21:18:19.250              Network Link is NOT connected.
21:18:19.359              Network is connecting...
21:18:21.156              Network is connecting...
21:18:21.265              TTLS Authenticating...
```

④EAP-FAST:

1. Select EAP-FAST from the Authentication type drop-down list. Key-in the identity as "wpatest2" and a domain name into the blank field. The tunnel identity is "wpatest2" and password is "test2". These setting are the same as our intended AP's setting.

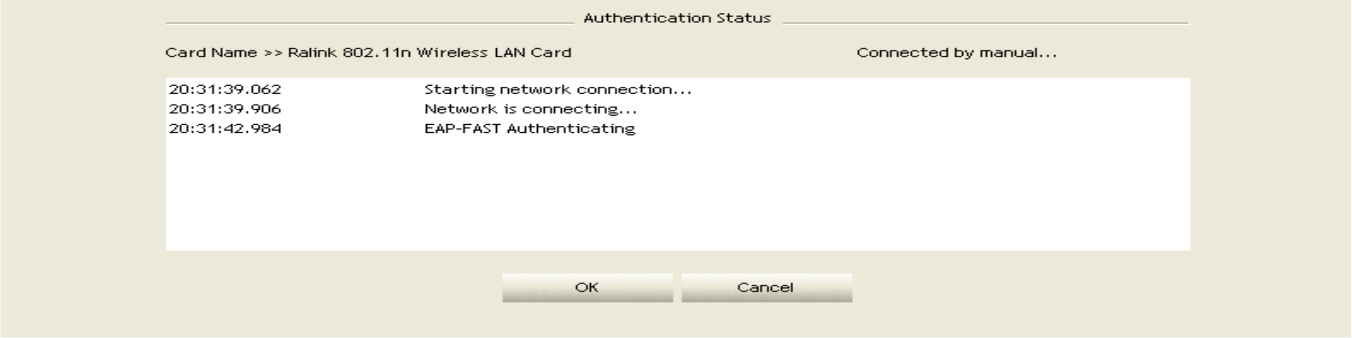


EAP Method >> EAP-FAST   Tunnel Authentication >> EAP-MSCHAP v2   Session Resumption

Authentication ID / Password

Identity >> wpatest2   Password >> *****   Domain Name >>

2. Click "OK". The dialog box should appear as the image below.



Authentication Status

Card Name >> Ralink 802.11n Wireless LAN Card   Connected by manual...

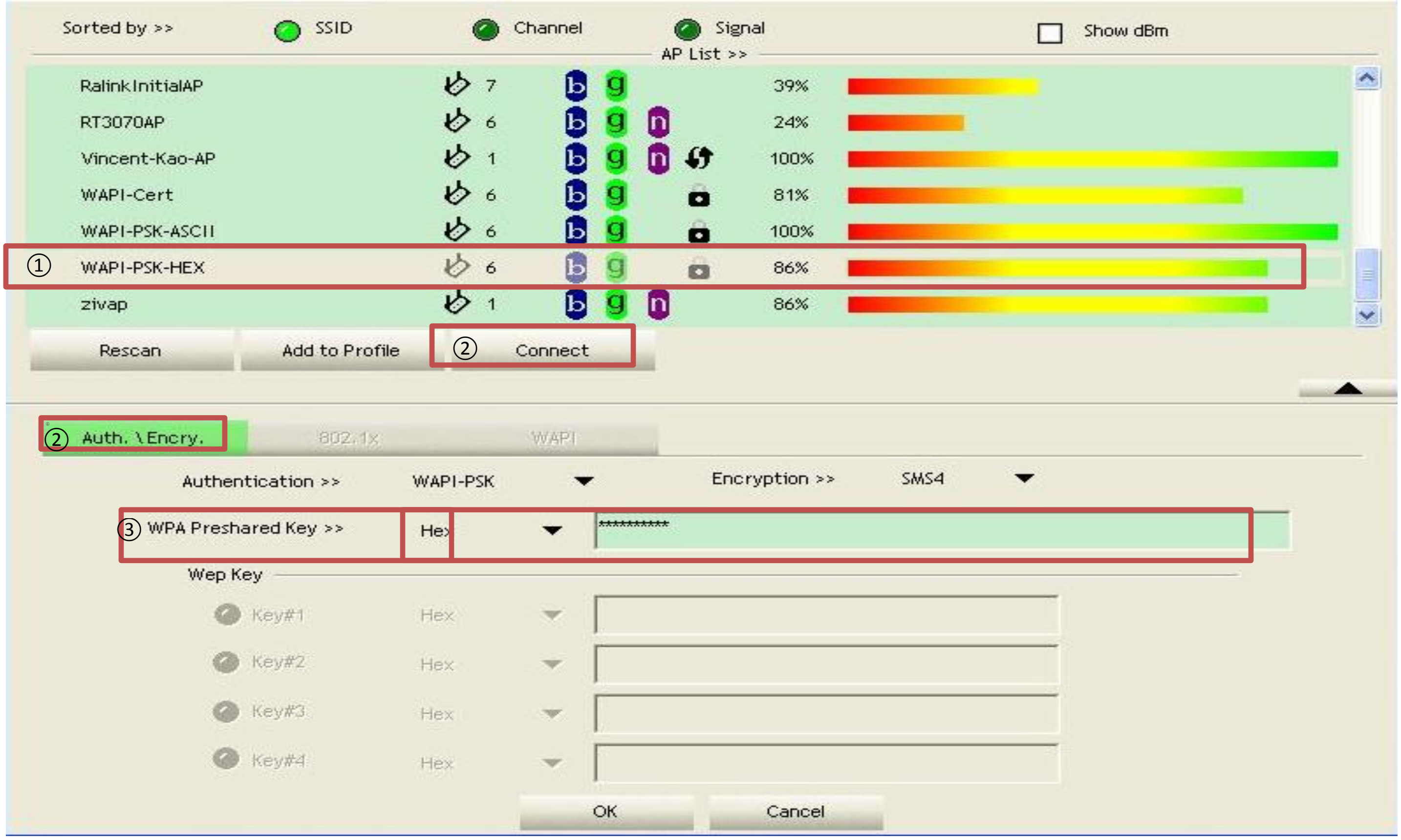
```
20:31:39.062              Starting network connection...
20:31:39.906              Network is connecting...
20:31:42.984              EAP-FAST Authenticating
```

2.7 Using WAPI or WAPI-CERT Authentication Mode to Configure a Connection with WPA

You can configure a connection with WPA using either WAPI authentication mode or WAPI-CERT authentication mode. Follow the steps listed below to configure a connection using one of these methods.

WAPI authentication mode

① Select an AP with WAPI authentication mode.
② Press "Connect" button, "Auth. \ Encry" window will appear, authentication mode is WAPI-PSK
③ Enter "1234567890" in the "WPA Preshared Key" "HEX" field.

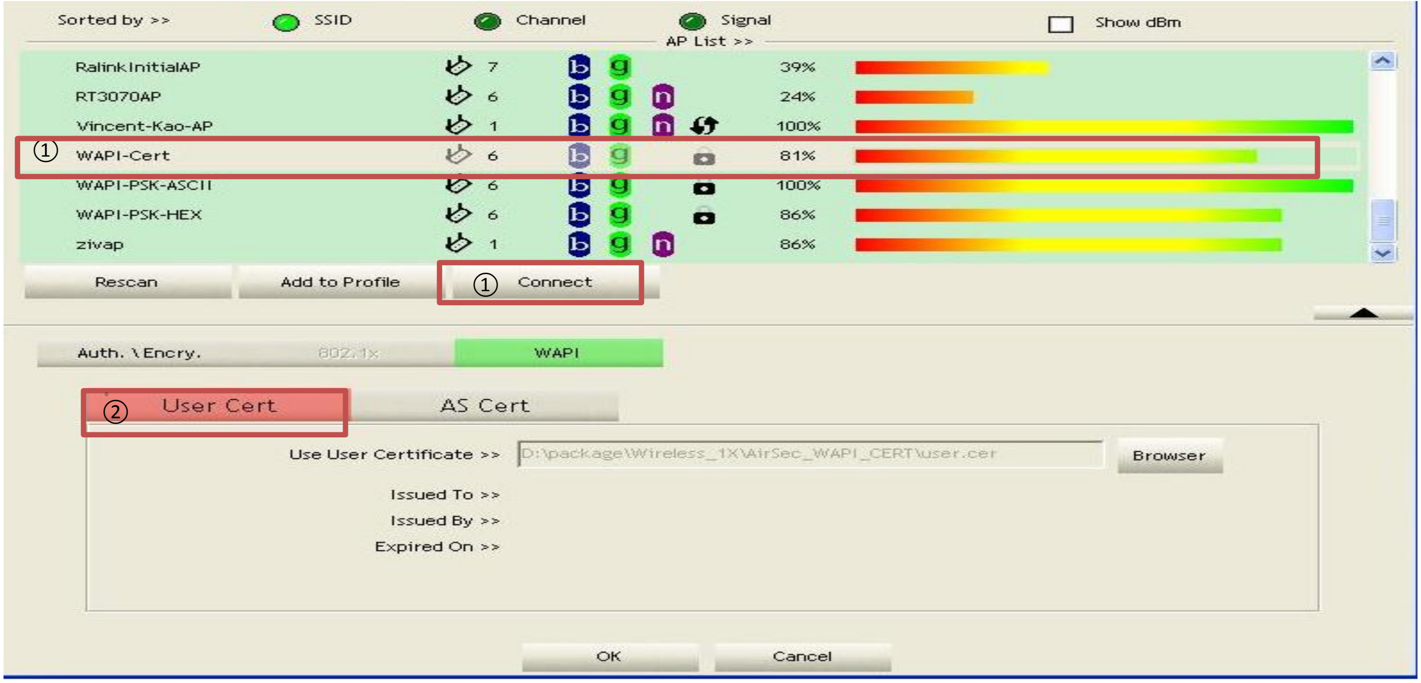


SSID	Channel	Signal
RalinkInitialAP	7	39%
RT3070AP	6	24%
Vincent-Kao-AP	1	100%
WAPI-Cert	6	81%
WAPI-PSK-ASCII	6	100%
① WAPI-PSK-HEX	6	86%
zivap	1	86%

Authentication >> WAPI-PSK
Encryption >> SMS4
③ WPA Preshared Key >> Hex ***********

WAPI-CERT authentication mode

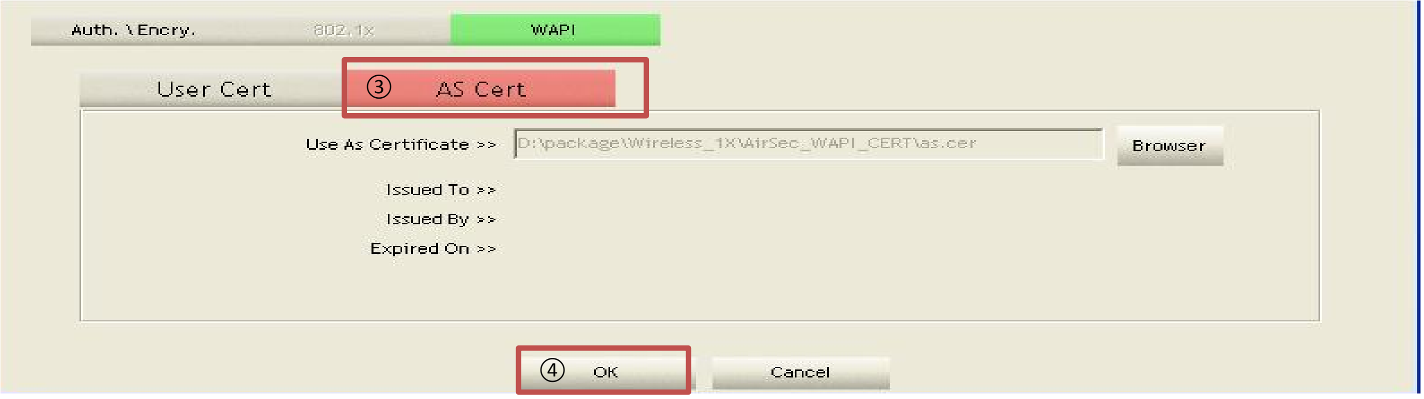
① Select an AP with WAPI-CERT authentication mode and press connect.
② Select user certificate.



SSID	Channel	Signal
RalinkInitialAP	7	39%
RT3070AP	6	24%
Vincent-Kao-AP	1	100%
① WAPI-Cert	6	81%
WAPI-PSK-ASCII	6	100%
WAPI-PSK-HEX	6	86%
zivap	1	86%

Use User Certificate >> D:\package\Wireless_1X\AirSec_WAPI_CERT\user.cer

③Select authentication server certificate.
④Click "OK" to start connection. *Be careful, if the WAPI Pre-Shared Key or certificate is not correct, you won't be able to exchange any data frames, even though the AP can be connected.*



Use As Certificate >> D:\package\Wireless_1X\AirSec_WAPI_CERT\as.cer

3.0 Guest Account, Country Channel List, and Acknowledgements

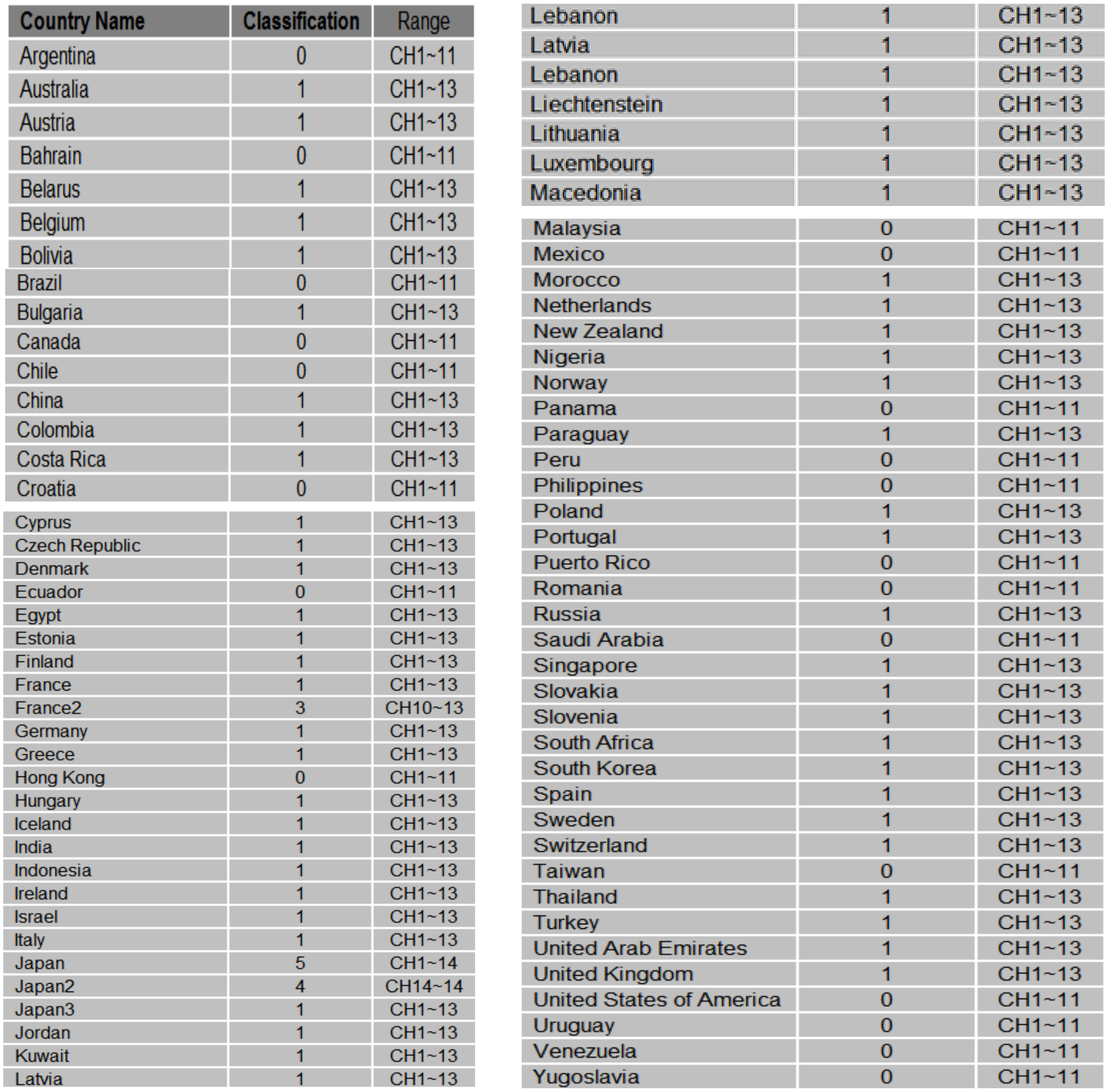
3.1 Guest Account

The guest account has the following restraints:

1. The Guest Account can only "Activate" the profile. It can't "Add to Profile" on the network page.
2. The Guest account can't switch to AP(XP/Vista) or STA+AP(Windows7) mode

3.2 Country Channel List

Below is the Country channel list, listing channels, classifications, and ranges for each country.



Country Name	Classification	Range
Argentina	0	CH1~11
Australia	1	CH1~13
Austria	1	CH1~13
Bahrain	0	CH1~11
Belarus	1	CH1~13
Belgium	1	CH1~13
Bolivia	1	CH1~13
Brazil	0	CH1~11
Bulgaria	1	CH1~13
Canada	0	CH1~11
Chile	0	CH1~11
China	1	CH1~13
Colombia	1	CH1~13
Costa Rica	1	CH1~13
Croatia	0	CH1~11
Cyprus	1	CH1~13
Czech Republic	1	CH1~13
Denmark	1	CH1~13
Ecuador	0	CH1~11
Egypt	1	CH1~13
Estonia	1	CH1~13
Finland	1	CH1~13
France	1	CH1~13
France2	3	CH10~13
Germany	1	CH1~13
Greece	1	CH1~13
Hong Kong	0	CH1~11
Hungary	1	CH1~13
Iceland	1	CH1~13
India	1	CH1~13
Indonesia	1	CH1~13
Ireland	1	CH1~13
Israel	1	CH1~13
Italy	1	CH1~13
Japan	5	CH1~14
Japan2	4	CH14~14
Japan3	1	CH1~13
Jordan	1	CH1~13
Kuwait	1	CH1~13
Latvia	1	CH1~13
Lebanon	1	CH1~13
Latvia	1	CH1~13
Lebanon	1	CH1~13
Liechtenstein	1	CH1~13
Lithuania	1	CH1~13
Luxembourg	1	CH1~13
Macedonia	1	CH1~13
Malaysia	0	CH1~11
Mexico	0	CH1~11
Morocco	1	CH1~13
Netherlands	1	CH1~13
New Zealand	1	CH1~13
Nigeria	1	CH1~13
Norway	1	CH1~13
Panama	0	CH1~11
Paraguay	1	CH1~13
Peru	0	CH1~11
Philippines	0	CH1~11
Poland	1	CH1~13
Portugal	1	CH1~13
Puerto Rico	0	CH1~11
Romania	0	CH1~11
Russia	1	CH1~13
Saudi Arabia	0	CH1~11
Singapore	1	CH1~13
Slovakia	1	CH1~13
Slovenia	1	CH1~13
South Africa	1	CH1~13
South Korea	1	CH1~13
Spain	1	CH1~13
Sweden	1	CH1~13
Switzerland	1	CH1~13
Taiwan	0	CH1~11
Thailand	1	CH1~13
Turkey	1	CH1~13
United Arab Emirates	1	CH1~13
United Kingdom	1	CH1~13
United States of America	0	CH1~11
Uruguay	0	CH1~11
Venezuela	0	CH1~11
Yugoslavia	0	CH1~11

3.3 Acknowledgments

The settings outlined in this appendix are used in the test platform by RaLink technology corp. Users can set the function in accordance with their AP. This product includes software written and developed by the following developers: MDC and its licensors, OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/), cryptographic software written by Eric Young (eay@cryptsoft .com), and Tim Hudson (tjh@cryptsoft.com).

Appendix 2: How to Operate the RT3072 on Linux and MAC

1.0 Operating the RT3072on Linux

The driver should automatically install when using a Lenox system.

2.0 Operating the RT3072 on MAC

To install the RT3072 on a MAC follow he steps listed below:

1. To install the 3072 on a MAC you first need set your security settings for "Allow applications downloaded from:" to "Anywhere."
2. Then insert the driver CD in to your computer and open the 3072 folder.
3. Inside the Mac folder you will see a file that ends in .dmg. Double click on this file and open "USBWireless-Install.pkg".
4. Follow the instructions on the screen.
5. When you are done all you need to do is restart the computer and you drivers will be installed.