User Manual

WL558USB

High Speed Wireless-N

USB 2.0 Adapter

2010 © All rights reserved. Version 1.0

No part of this document may be reproduced, republished, or retransmitted in any form or by any means whatsoever, whether electronically or mechanically, including, but not limited to, by way of photocopying, recording, information recording, or through retrieval systems without the express written permission. We reserve the right to revise this document at any time without the obligation to notify any person and/or entity. All other company or product names mentioned are used for identification purposes only and may be trademarks of their respective owners.

LIMITATION OF LIABILITY AND DAMAGES

THE PRODUCT AND THE SOFTWARES WITHIN ARE PROVIDED "AS IS," BASIS. THE MANUFACTURER AND MANUFACTURER'S RESELLERS (COLLECTIVELY REFERRED TO AS "THE SELLERS") DISCLAIM ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTIES ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE. IN NO EVENT WILL THE SELLERS BE LIABLE FOR DAMAGES OR LOSS, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL WILLFUL, PUNITIVE, INCIDENTAL, EXEMPLARY, OR CONSEQUENTIAL, DAMAGES, DAMAGES FOR LOSS OF BUSINESS PROFITS, OR DAMAGES FOR LOSS OF BUSINESS OF ANY CUSTOMER OR ANY THIRD PARTY ARISING OUT OF THE USE OR THE INABILITY TO USE THE PRODUCT OR THE SOFTWARES, INCLUDING BUT NOT LIMITED TO THOSE RESULTING FROM DEFECTS IN THE PRODUCT OR SOFTWARE OR DOCUMENTATION, OR LOSS OR INACCURACY OF DATA OF ANY KIND, WHETHER BASED ON CONTRACT, TORT OR ANY OTHER LEGAL THEORY, EVEN IF THE PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE PRODUCT OR ITS SOFTWARE IS ASSUMED BY CUSTOMER. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO THE PARTIES. IN NO EVENT WILL THE SELLERS' TOTAL CUMULATIVE LIABILITY OF EACH AND EVERY KIND IN RELATION TO THE PRODUCT OR ITS SOFTWARE EXCEED THE AMOUNT PAID BY CUSTOMER FOR THE PRODUCT.

Contents

About the Product

The Aztech WL558USB High Speed Wireless-N USB 2.0 Adapter is designed to provide a high-speed and unrivaled wireless performance for your computer. With a faster wireless connection, you can get a better Internet experience, such as downloading, gaming, video streaming and so on.

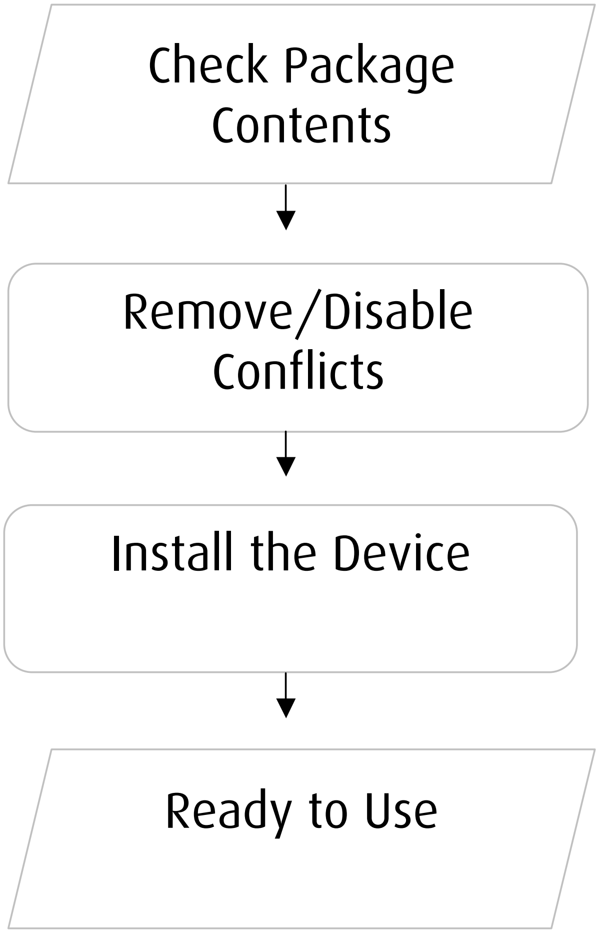
The WL558USB Adapter complies with IEEE 802.11g, and IEEE 802.11b standards. It can perfectly interoperate with all the 802.11n/g/b devices. The WL558USB’s auto-sensing capability allows high packet transfer rate of up to 300Mbps（2T2R） for maximum throughput. Additionally, the WL558USB adapter has good capability on anti-jamming and supports WEP, TKIP, AES， WPA and WPA2 encryption to prevent outside intrusion and protect your personal information from being exposed.

Featuring high performance transmission rates, simple installation and adaptability, as well as strong security, the WL558USB Adapter is the perfect solution for small office and home needs.

Note: Wireless connection speed is not correlated to Internet access speed. Internet access speed from popular broadband DSL or cable Internet services normally provides up to 3 Mbps connection, which can be easily handled even by the slower Wireless B protocol.

Getting Started

Setting up the device is easy. The flowchart below provides an outline of the steps needed to complete the installation. Brief descriptions appear beside each step. Detailed instructions are provided in the subsequent pages.



The package includes the Wireless N USB Adapter, Easy Start Guide, Resource CD and USB Extension.

Check proxy application, TCP/IP Settings, Internet Properties, and remove temporary Internet files.

Install the device and then connect to a wireless network.

Check Package Contents

Make sure that you have the following items. If any of the items is damaged or missing, please contact your dealer immediately.

- WL558USB
- Easy Start Guide
- Resource CD – contains WL558 Utility installer, and User Manual
- USB Cable

Using the USB Extension

The USB Extension helps you place the device to a more prominent location and to achieve a better reception of the wireless network. It is most useful for desktop computers with USB 2.0 ports placed behind the computer casing. USB ports placed in the front of the computer are usually the slower USB 1.0 variant.

To use the USB Extension, connect one end to a USB 2.0 port in your computer, and then attach the WL558USB at the other end.

Remove or Disable Conflicts

To make sure the device installation moves on smoothly, you need to remove or disable conflicts that may interfere the installation. Probable conflicts may include:

- Internet sharing applications
- Proxy software
- Security software
- Internet properties
- Temporary Internet files

Internet Sharing, Proxy, and Security Applications

Internet sharing, proxy software, and firewall applications may interfere with the installation. These should be removed or disabled before start the installation.

If you have any of the following or similar applications installed on your computer, remove or disable them according to the manufacturer's instructions.

Internet Sharing Applications	Proxy Software	Security Software
Microsoft Internet Sharing	WinGate	Symantec
	WinProxy	Zone Alarm

Configuring Internet Properties

To set the Internet Properties:

1. Click the Start button, and then click Run. This opens the Run dialog box.
2. Type control inetcpl.cpl, and then click OK. This opens Internet Properties.
3. Click Connections tab.
4. In Dial-up and Virtual Private Network settings, check Never dial a connection.
5. To close Internet Properties, click OK.

Removing Temporary Internet Files

Temporary Internet files are files from Web sites that are stored in your computer. Delete these files to clean the cache and remove footprints left by the Web pages you visited.

To remove temporary Internet files:

1. Click the Start button, and then click Run. This opens the Run dialog box.
2. Type control, and then click OK. This opens Control Panel.
3. Double-click Internet Options. This opens Internet Options.
4. In the Temporary Internet Files pane, click Delete Cookies.
5. Click Delete Files.
6. To close Internet Properties, click OK.

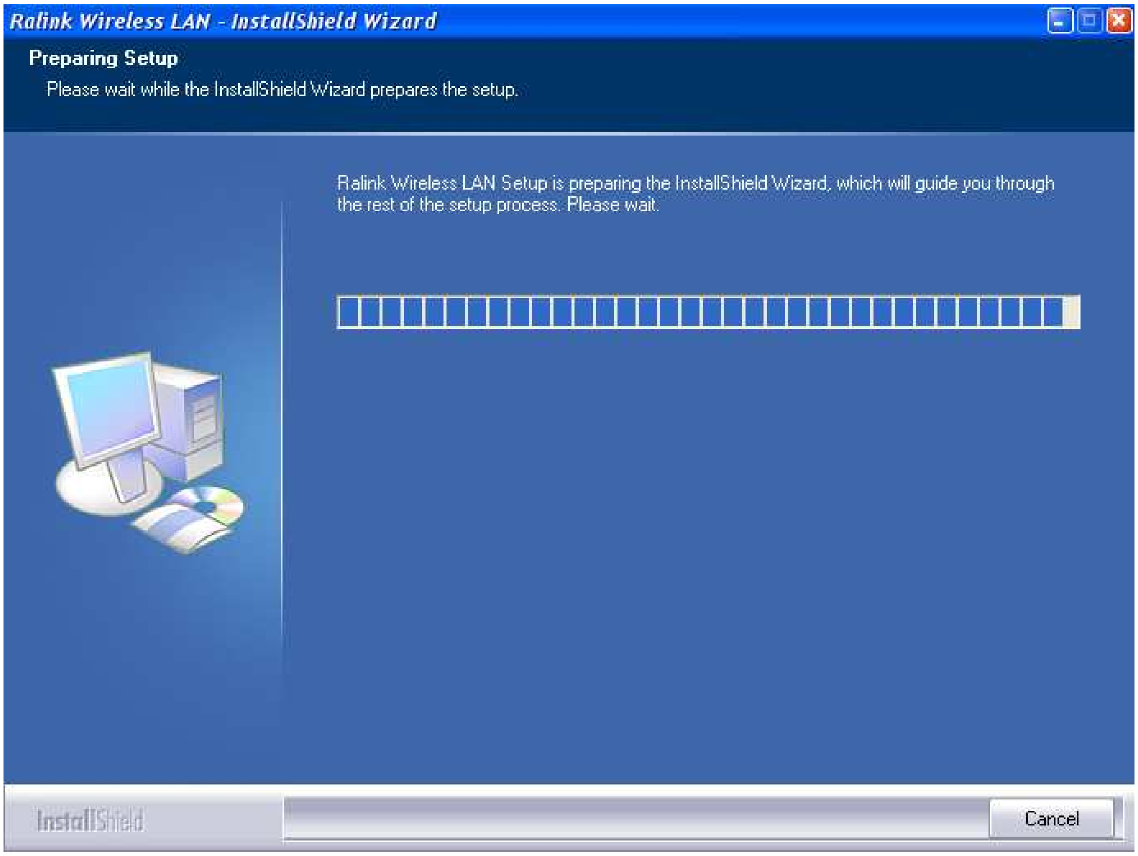
Installation

Here are the instructions on how to install the driver software for Windows 2000, XP, and Vista.

> **Note:** Do not connect the device until the Utility is completely installed.

To install the driver software:

1. Insert the Resource CD to the CD-ROM. This opens the WL558USB Utility Setup. If the Utility does not open automatically, click the Start button, and then click Run. Enter d:\setup.exe, where d is the CD-ROM drive.



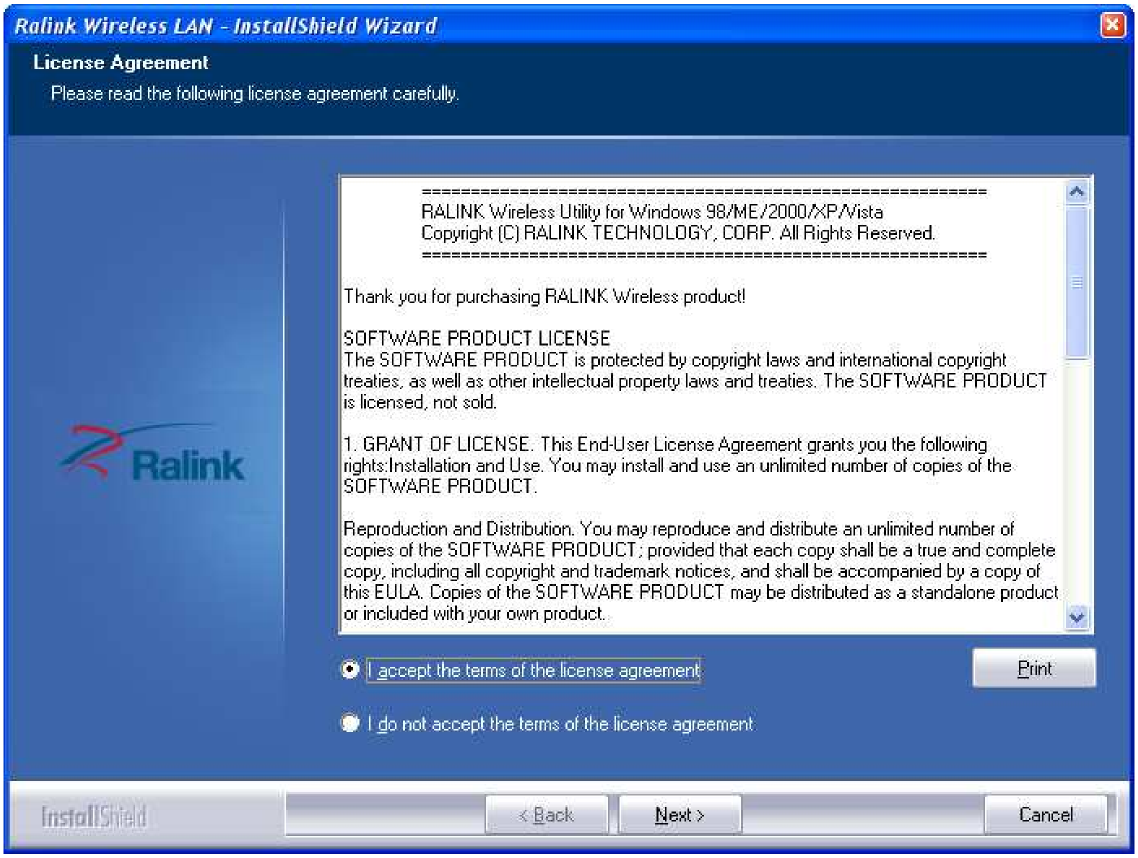
Ralink Wireless LAN - InstallShield Wizard

Preparing Setup

Please wait while the InstallShield Wizard prepares the setup.

Ralink Wireless LAN Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.

2. Wizard will now move to next step for license agreement, check the option ‘I accept the terms of the license agreement’



License Agreement

Please read the following license agreement carefully.

==

RALINK Wireless Utility for Windows 98/ME/2000/XP/Vista
Copyright (C) RALINK TECHNOLOGY, CORP. All Rights Reserved.

==

Thank you for purchasing RALINK Wireless product!

SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. This End-User License Agreement grants you the following rights:Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.

Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.

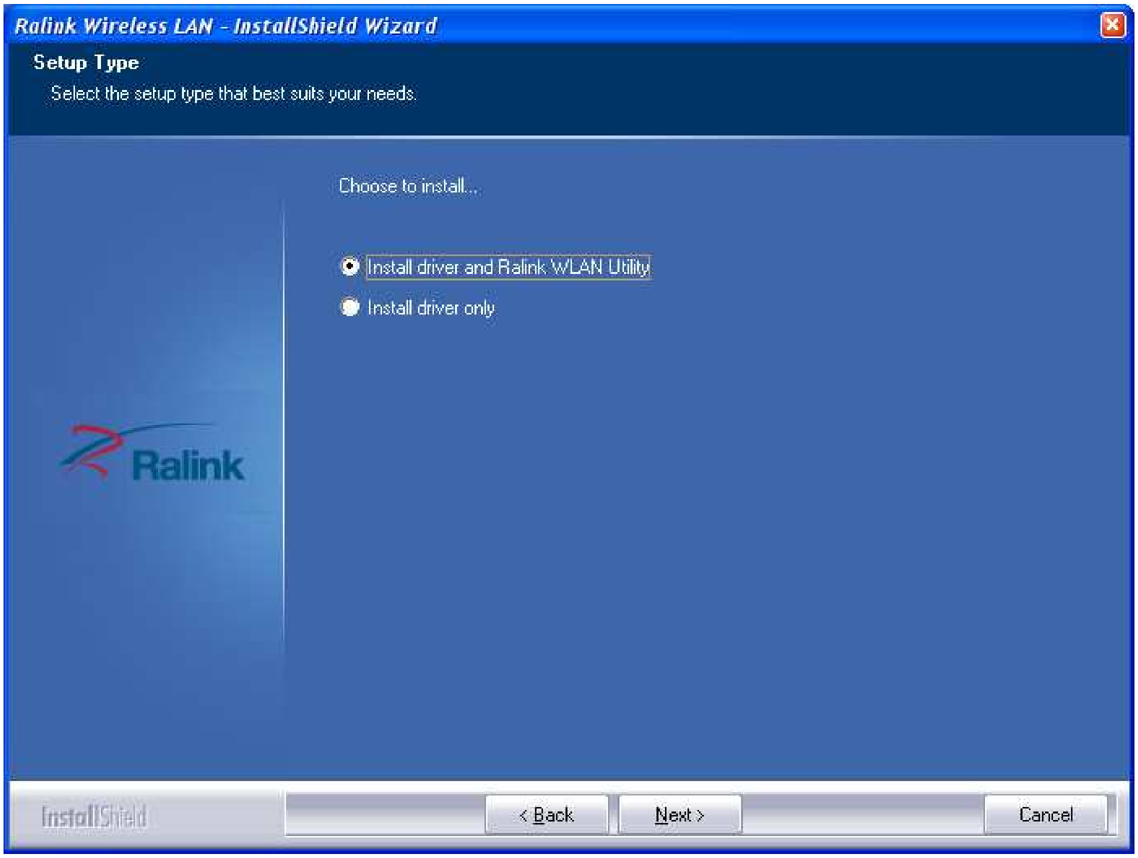
● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

3. Click Next.
4. Select either of the options available:

   a. Install driver and Ralink WLAN Utility, this will install driver for the adaptor, and the wireless utility

   b. Install driver only, this will install only the driver for the adaptor.



Setup Type

Select the setup type that best suits your needs.

Choose to install...

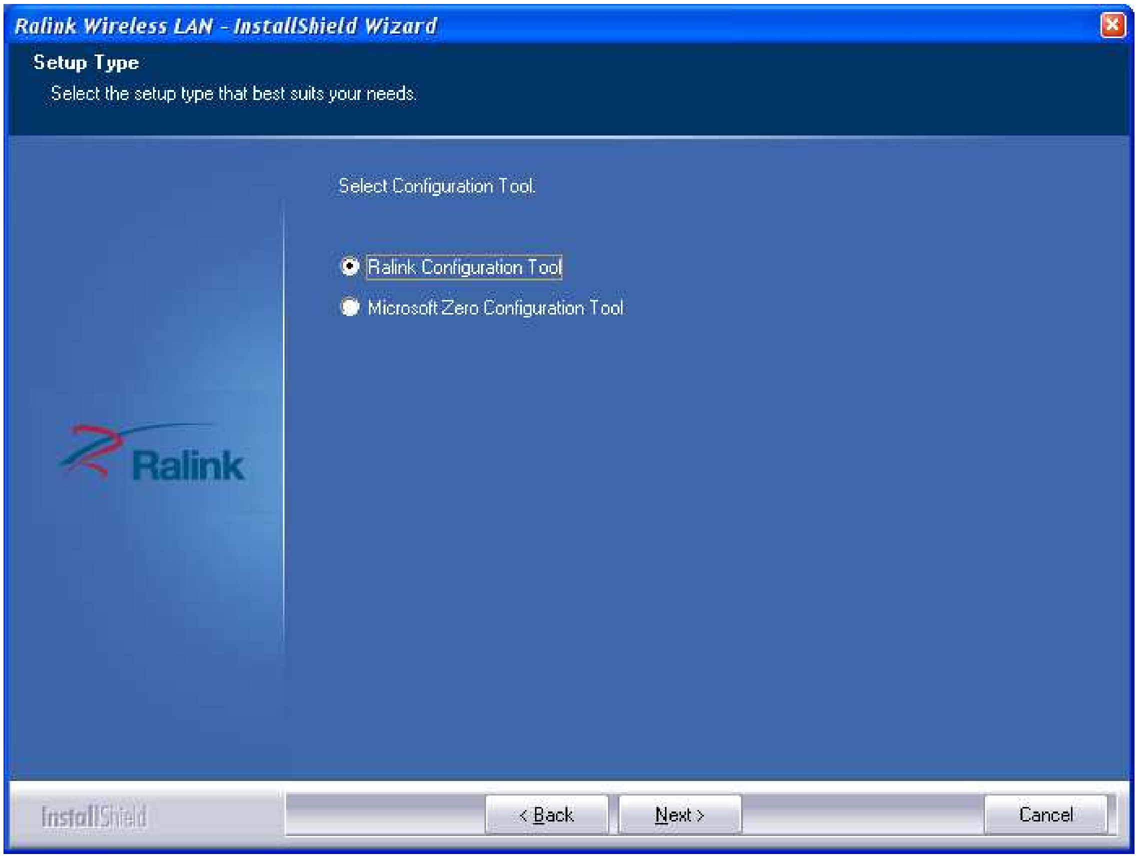
● Install driver and Ralink WLAN Utility

○ Install driver only

5. Click Next.
6. If you selected the first option, please select either one of the options available:

   a. Ralink Configuration Tool

   b. Microsoft Zero Configuration Tool



Setup Type

Select the setup type that best suits your needs.

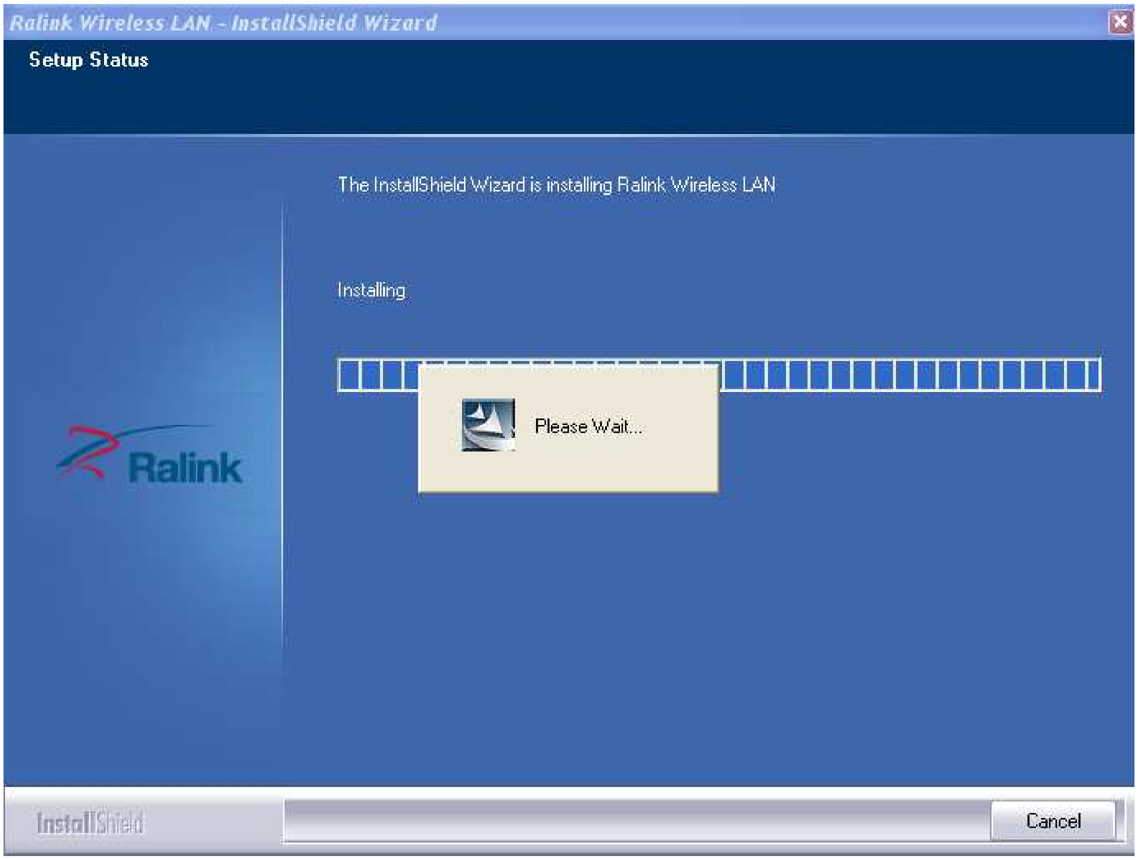
Select Configuration Tool.

● Ralink Configuration Tool

○ Microsoft Zero Configuration Tool

7. Click Next.

8. Click Install, required driver/utility is now being installed into the PC



Ralink Wireless LAN - InstallShield Wizard

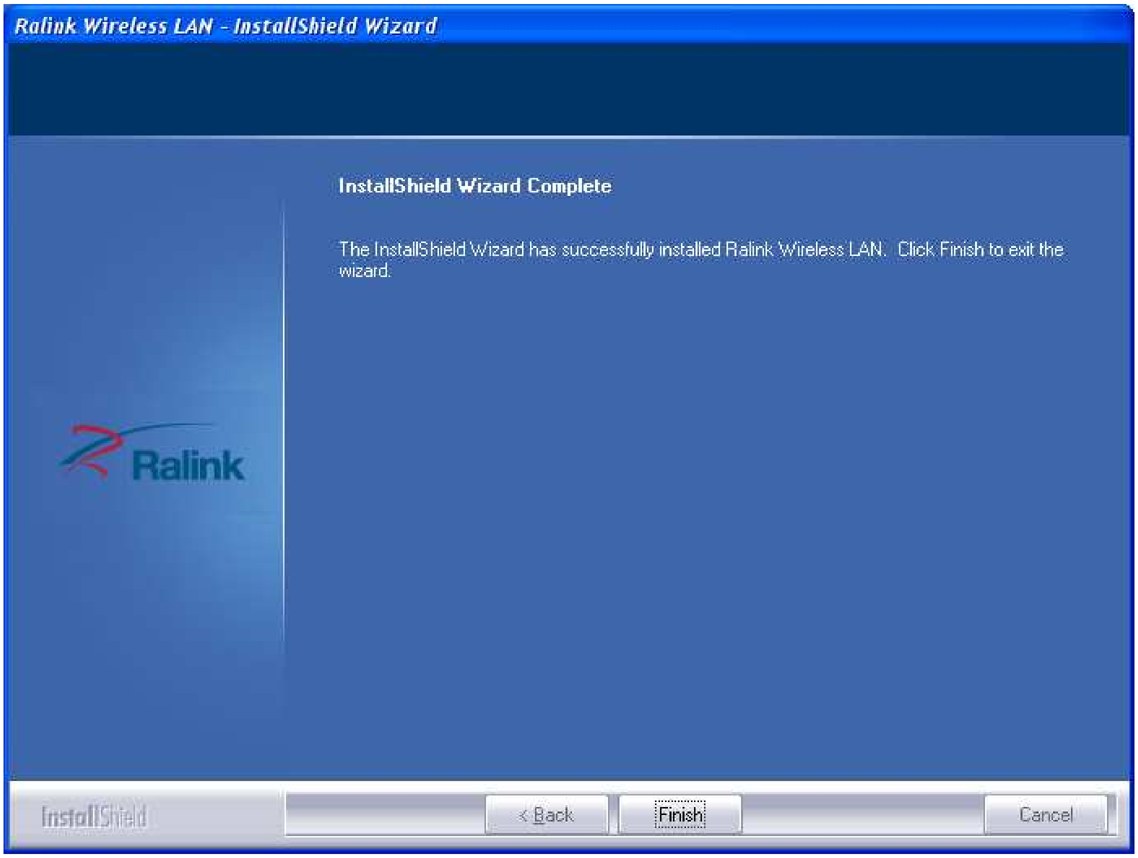
Setup Status

The InstallShield Wizard is installing Ralink Wireless LAN

Installing

Please Wait...

9. Click Finish to exit the wizard, installation is now complete.



Ralink Wireless LAN - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed Ralink Wireless LAN. Click Finish to exit the wizard.

Configuration

This chapter describes how to configure WL558USB to get connected to your WLAN router.

The adaptor's configuration in windows XP is similar with windows 2000 and windows Vista. This user guide describes the configuration for windows XP.

After installing the adaptor, the adaptor's tray icon will appear in your system tray. It appears at the right hand side bottom of the screen. The icon will change color to reflect current wireless network connection status. The status is shown as follows:

R+ : Indicates the connected and signal strength is good.

R+ : Indicates the connected and signal strength is normal.

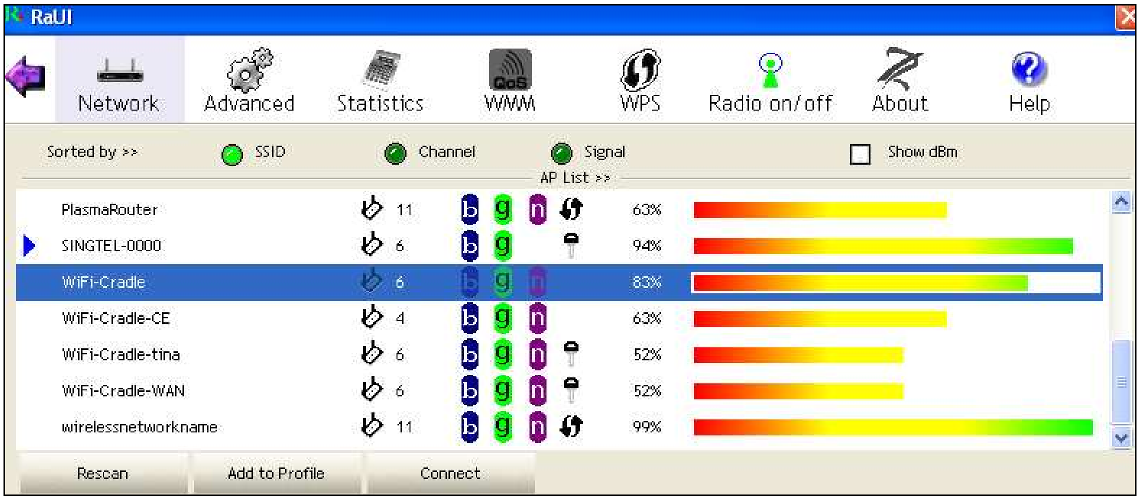
R+: Indicates that it is not yet connected.

R+: Indicates that a wireless NIC cannot be detected.

R+: Indicates that the connection and signal strength is weak.

Connecting to non-Secured Wireless AP

1. Select the AP desired

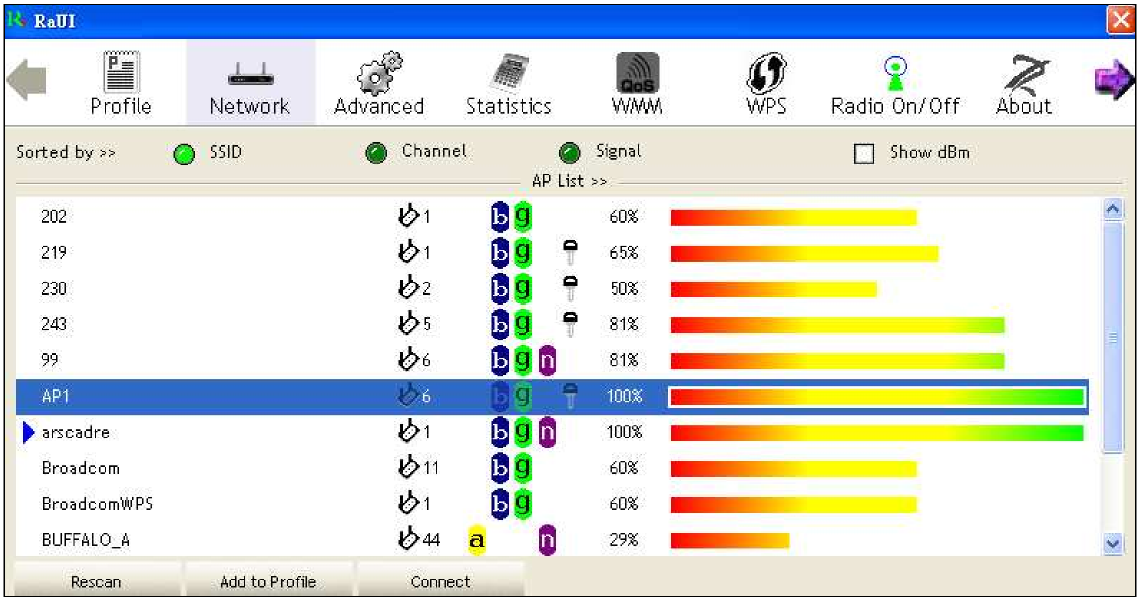


PlasmaRouter	11	b g n		63%
SINGTEL-0000	6	b g	🔑	94%
WiFi-Cradle	6	b g n		83%
WiFi-Cradle-CE	4	b g n		63%
WiFi-Cradle-tina	6	b g n	🔑	52%
WiFi-Cradle-WAN	6	b g n	🔑	52%
wirelessnetworkname	11	b g n		99%

2. Click Connect

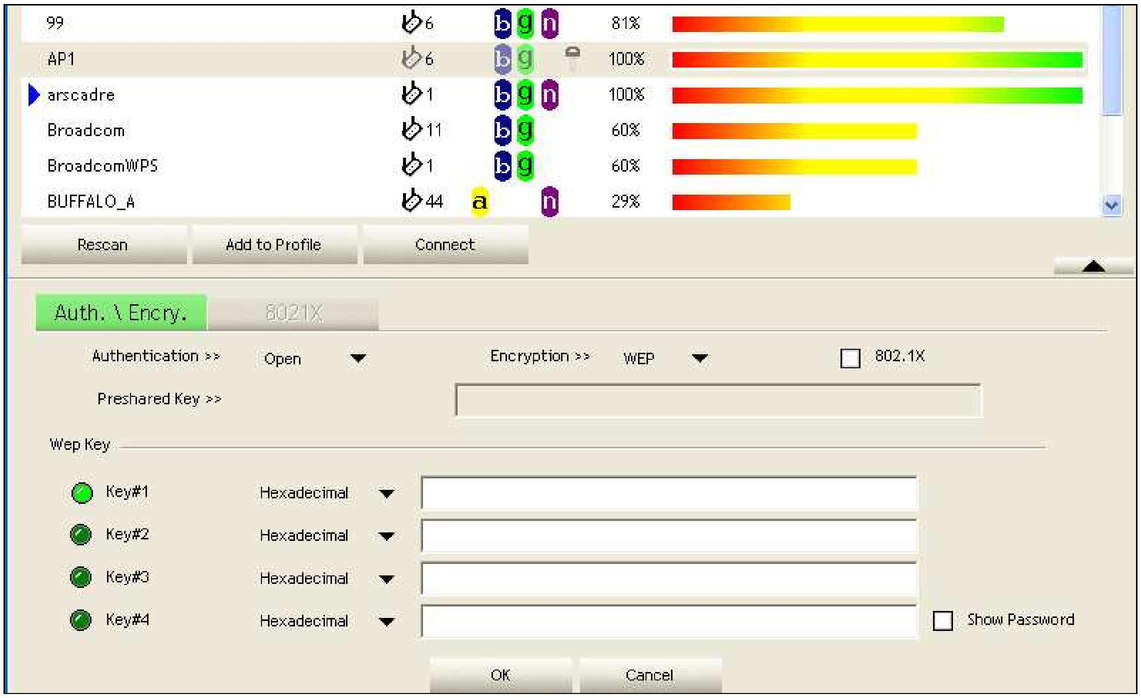
Connecting to WEP-Secured Wireless AP

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



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 below



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%

Authentication >> Open Encryption >> WEP □ 802.1X

Preshared Key >>

Wep Key

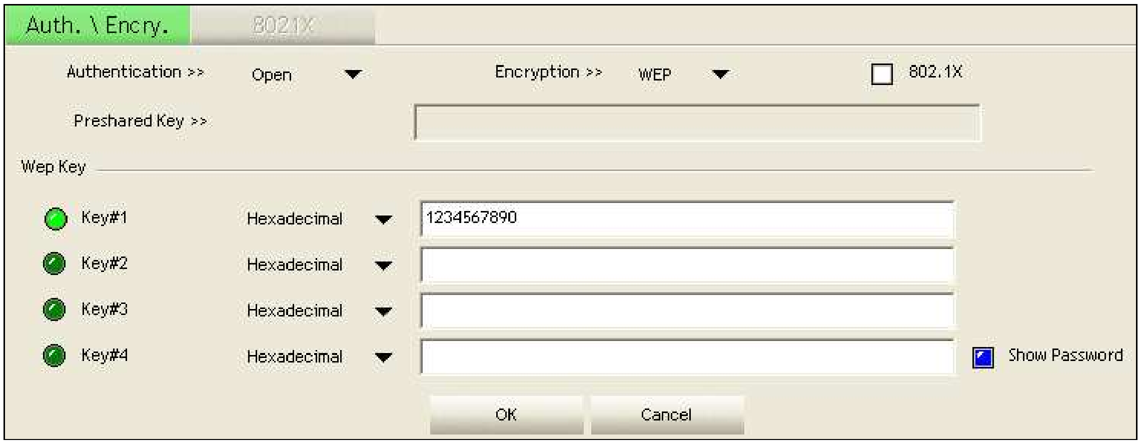
● Key#1 Hexadecimal

○ Key#2 Hexadecimal

○ Key#3 Hexadecimal

○ Key#4 Hexadecimal □ Show Password

3. Enter the key in the field as shown. The value must be the same as the key set in the Access Point.



Authentication >> Open Encryption >> WEP □ 802.1X

Preshared Key >>

Wep Key

● Key#1 Hexadecimal 1234567890

○ Key#2 Hexadecimal

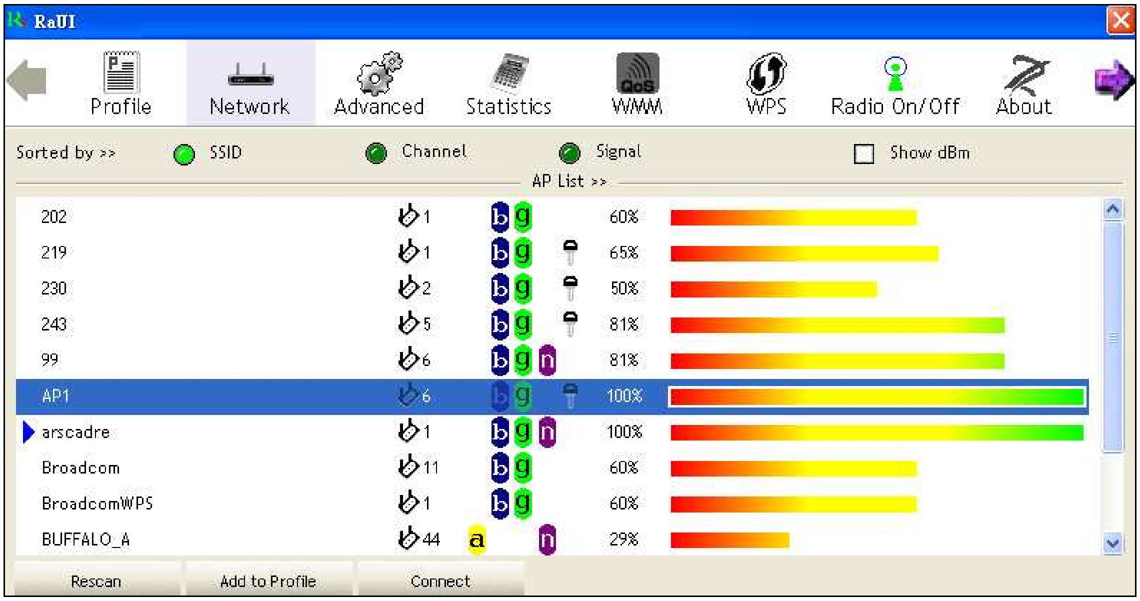
○ Key#3 Hexadecimal

○ Key#4 Hexadecimal ☑ Show Password

4. Click OK.

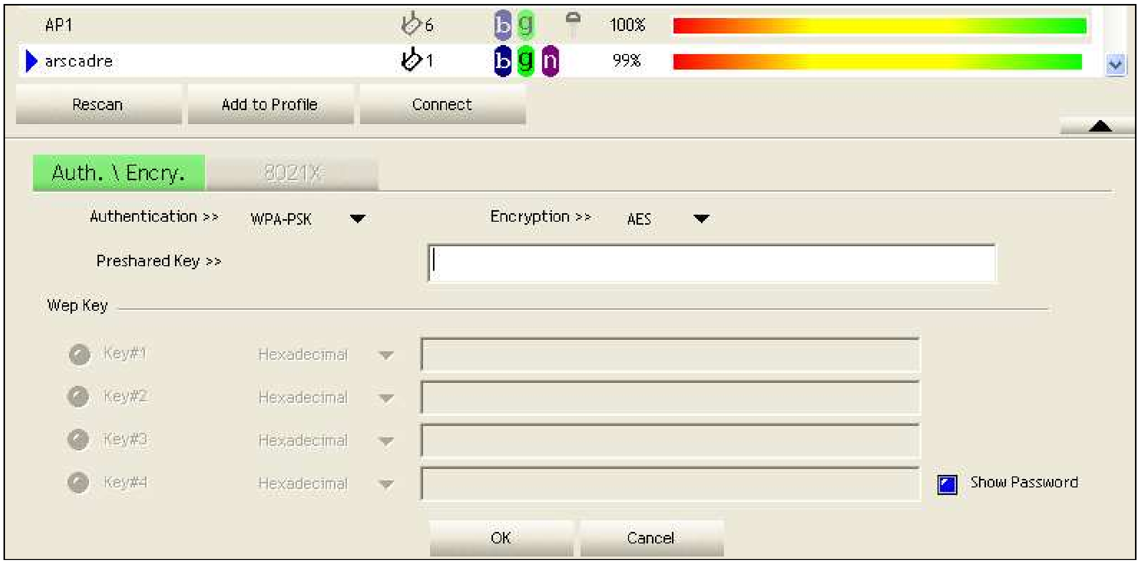
Connecting to WPA-PSK-Secured Wireless AP

1. Select an AP with WPA-PSK encryption and click "Connect".



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 below



AP1	6	b g	100%
arscadre	1	b g n	99%

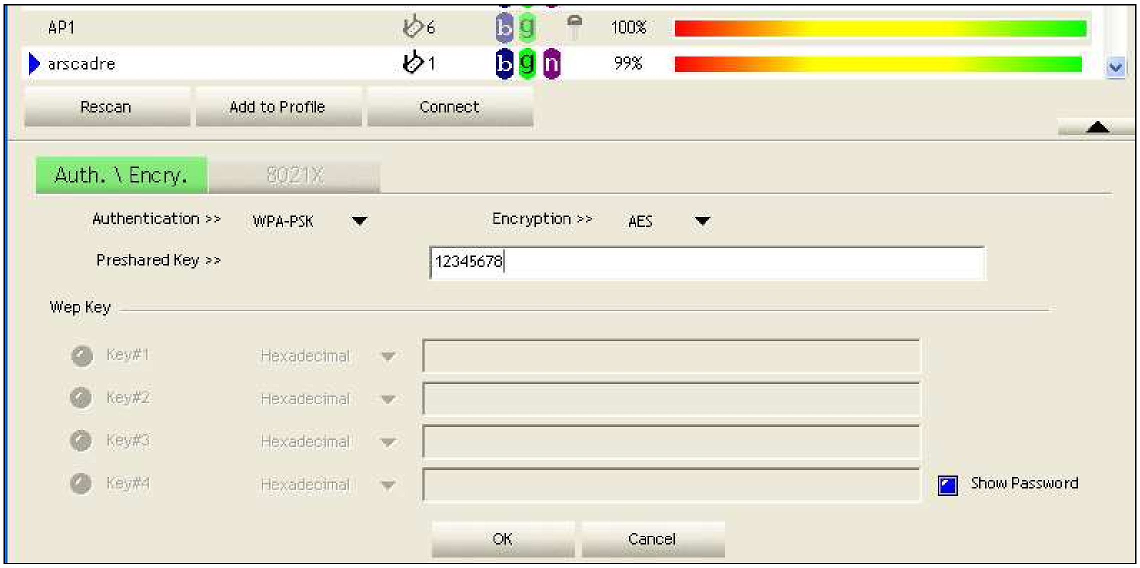
Authentication >> WPA-PSK

Encryption >> AES

Preshared Key >>

3. Select WPA-PSK as the Authentication Type. Select TKIP or AES encryption.

4. Enter the key in the field as shown. The value must be the same as the key set in the Access Point.



Authentication >> WPA-PSK

Encryption >> AES

Preshared Key >> 12345678

☑ Show Password

5. Click OK.

About WL558USB Utility

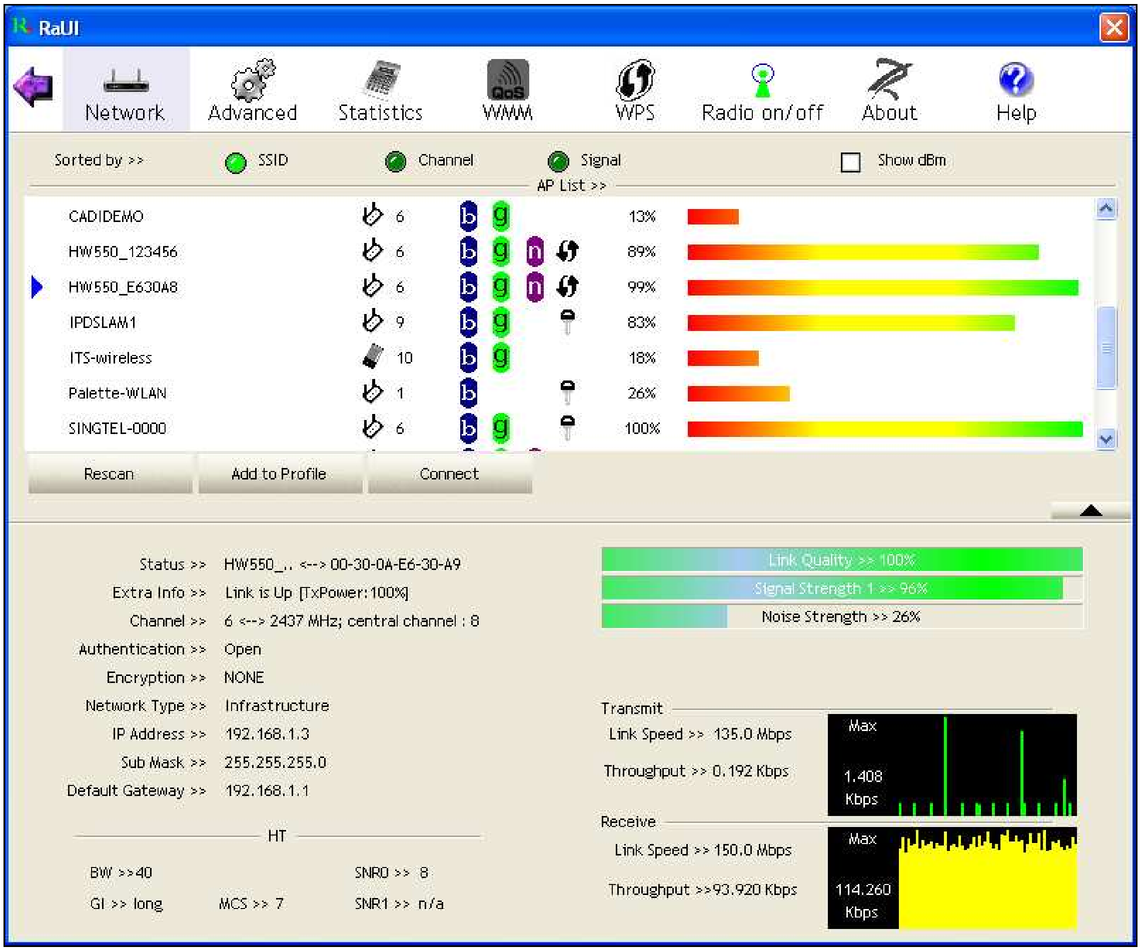
WL558USB Utility is a software application used in tandem with the device to connect to a wireless network and to configure the device settings. WL558USB Utility can be installed on computers running Windows 2000, XP, or Vista.

To connect to a wireless network:

1. Connect Wireless N USB adapter to a USB port.
2. When your device is detected, a new icon appears in the System tray . Double-click this icon to open WL558USB Utility.

Network Tab

When starting RaUI, the system will connect to the AP with 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 the below figure.



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

AP List >>

CADIDEMO	6	b g		13%
HW550_123456	6	b g n		89%
HW550_E630A8	6	b g n		99%
IPDSLAM1	9	b g		83%
ITS-wireless	10	b g		18%
Palette-WLAN	1	b		26%
SINGTEL-0000	6	b g		100%

Status >> HW550_.. <--> 00-30-0A-E6-30-A9
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437 MHz; central channel : 8
Authentication >> Open
Encryption >> NONE
Network Type >> Infrastructure
IP Address >> 192.168.1.3
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.1.1

HT
BW >>40 SNR0 >> 8
GI >> long MCS >> 7 SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 96%
Noise Strength >> 26%

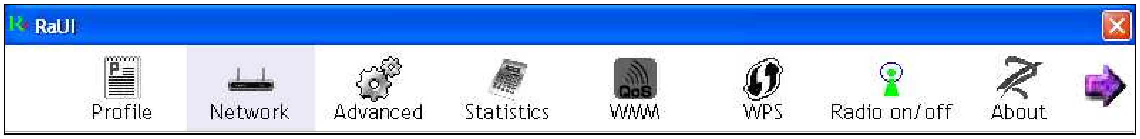
Transmit
Link Speed >> 135.0 Mbps
Throughput >> 0.192 Kbps

Receive
Link Speed >> 150.0 Mbps
Throughput >>93.920 Kbps

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

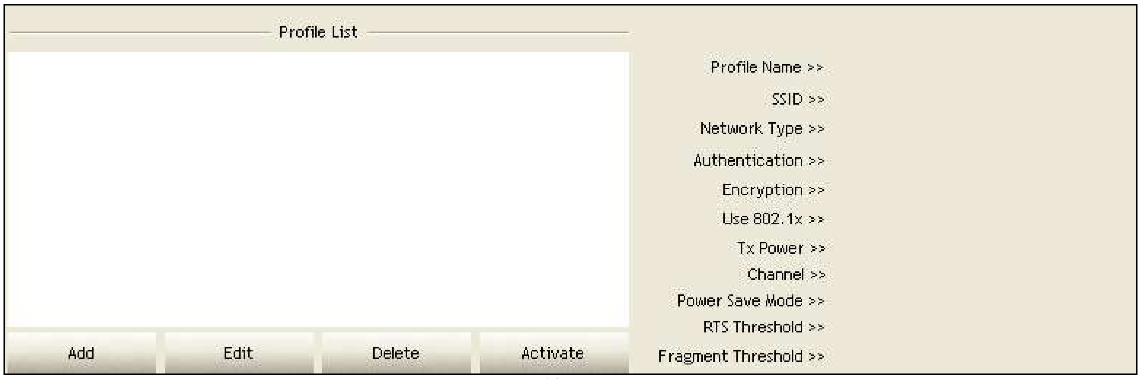
Button Section

Includes 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.

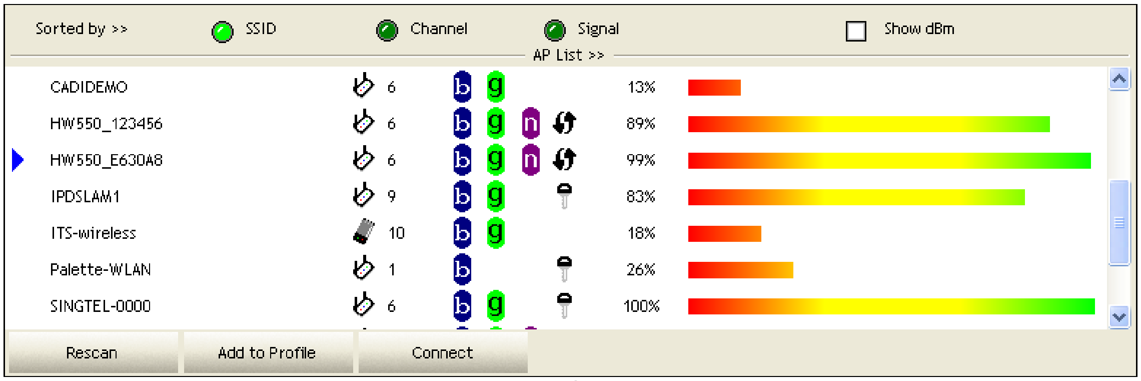


Function Section

Appears to present information and options related to the button.

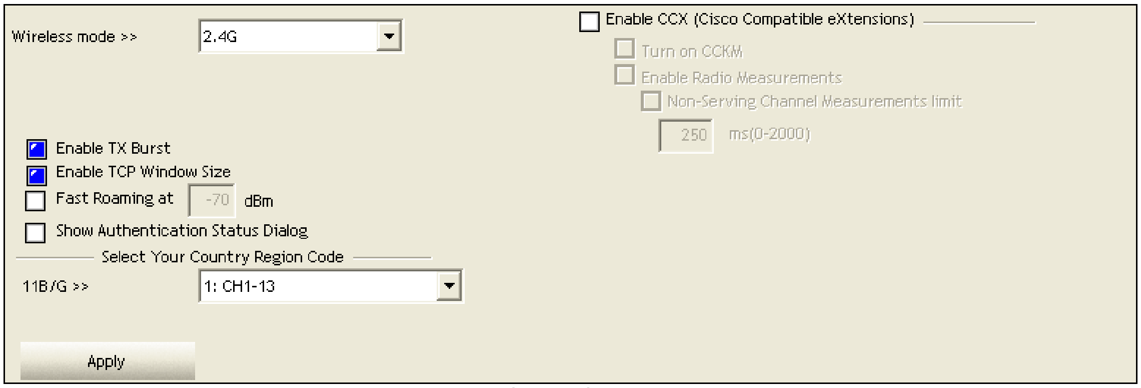


Profile page



SSID	Channel		Signal
CADIDEMO	6	b g	13%
HW550_123456	6	b g n	89%
HW550_E630A8	6	b g n	99%
IPDSLAM1	9	b g	83%
ITS-wireless	10	b g	18%
Palette-WLAN	1	b	26%
SINGTEL-0000	6	b g	100%

Network page



Wireless mode >> 2.4G

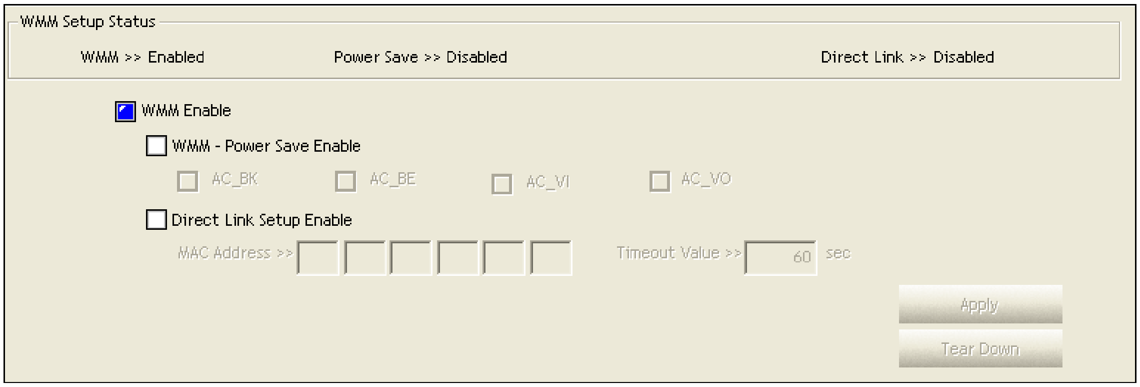
☑ Enable TX Burst
☑ Enable TCP Window Size
□ Fast Roaming at -70 dBm
□ Show Authentication Status Dialog

Select Your Country Region Code

11B/G >> 1: CH1-13

□ Enable CCX (Cisco Compatible eXtensions)
□ Turn on CCKM
□ Enable Radio Measurements
□ Non-Serving Channel Measurements limit
250 ms(0-2000)

Advanced page



WMM Setup Status

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

☑ WMM Enable

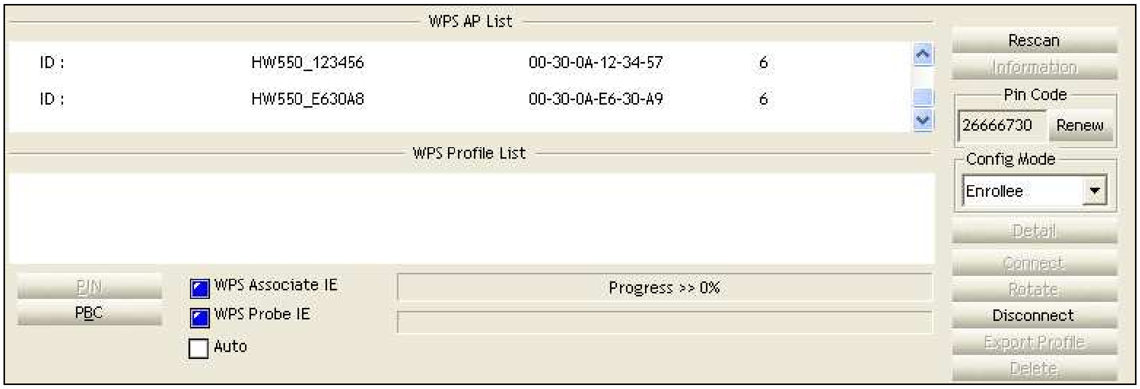
□ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

□ Direct Link Setup Enable

MAC Address >>   Timeout Value >> 60 sec

WMM page



WPS AP List

ID :	HW550_123456	00-30-0A-12-34-57	6
ID :	HW550_E630A8	00-30-0A-E6-30-A9	6

WPS Profile List

Pin Code: 26666730

Config Mode: Enrollee

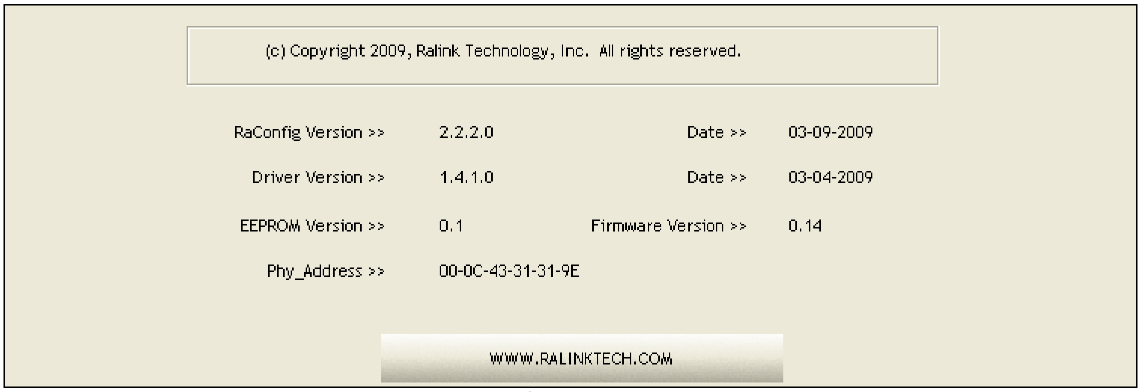
☑ WPS Associate IE

☑ WPS Probe IE

□ Auto

Progress >> 0%

WPS page



(c) Copyright 2009, Ralink Technology, Inc. All rights reserved.

RaConfig Version >> 2.2.2.0   Date >> 03-09-2009

Driver Version >> 1.4.1.0   Date >> 03-04-2009

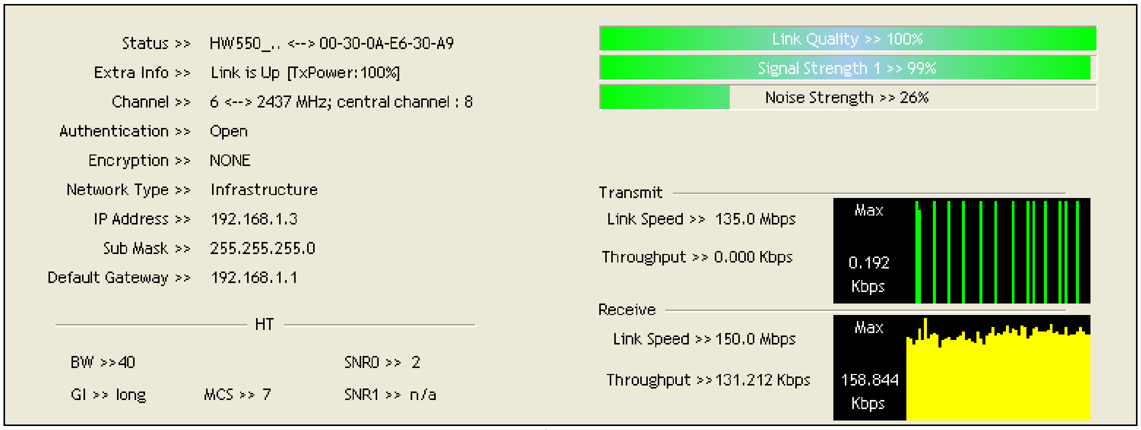
EEPROM Version >> 0.1   Firmware Version >> 0.14

Phy_Address >> 00-0C-43-31-31-9E

About page

Status Section

This section includes information about the link status, authentication status, AP's information and configuration, and retrying the connection when authentication is failed.



Status >> HW550_.. <--> 00-30-0A-E6-30-A9
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437 MHz; central channel : 8
Authentication >> Open
Encryption >> NONE
Network Type >> Infrastructure
IP Address >> 192.168.1.3
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.1.1

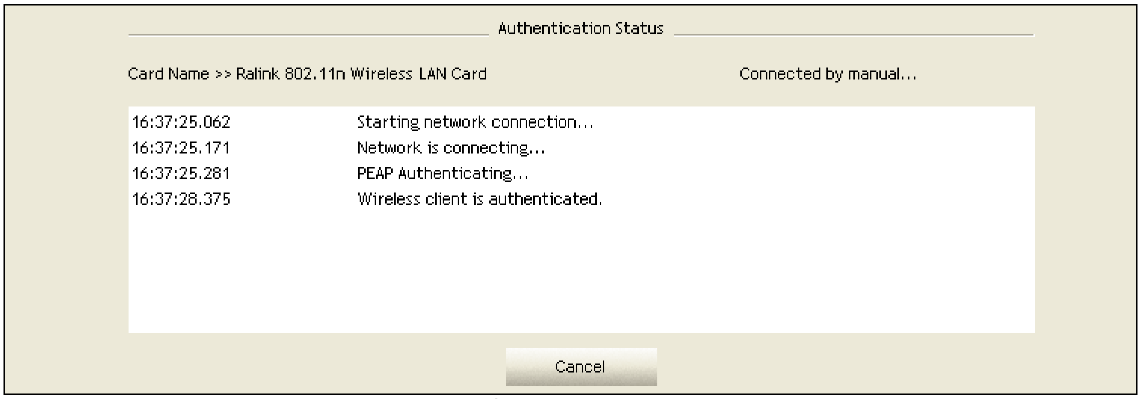
HT
BW >>40
SNR0 >> 2
GI >> long
MCS >> 7
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 99%
Noise Strength >> 26%

Transmit
Link Speed >> 135.0 Mbps
Throughput >> 0.000 Kbps
Max
0.192 Kbps

Receive
Link Speed >> 150.0 Mbps
Throughput >> 131.212 Kbps
Max
158.844 Kbps

Link Status

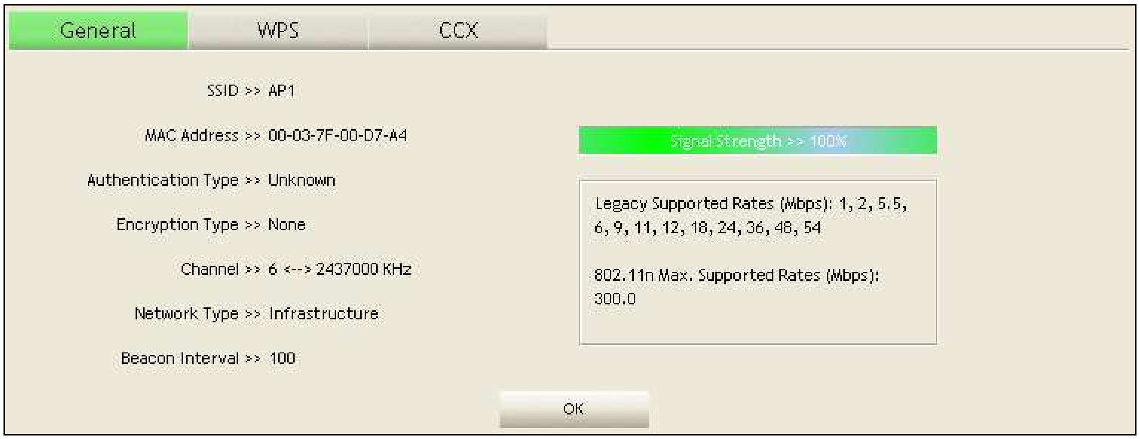


Authentication Status

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

```
16:37:25.062        Starting network connection...
16:37:25.171        Network is connecting...
16:37:25.281        PEAP Authenticating...
16:37:28.375        Wireless client is authenticated.
```

Authentication Status



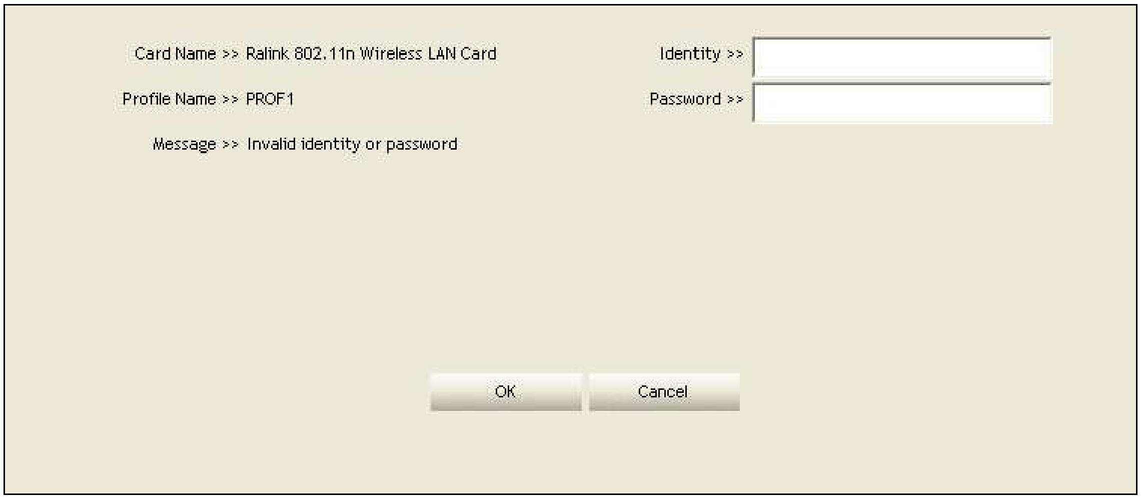
SSID >> AP1
MAC Address >> 00-03-7F-00-D7-A4
Authentication Type >> Unknown
Encryption Type >> None
Channel >> 6 <--> 2437000 KHz
Network Type >> Infrastructure
Beacon Interval >> 100

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

Access Point's Information



Card Name >> Ralink 802.11n Wireless LAN Card

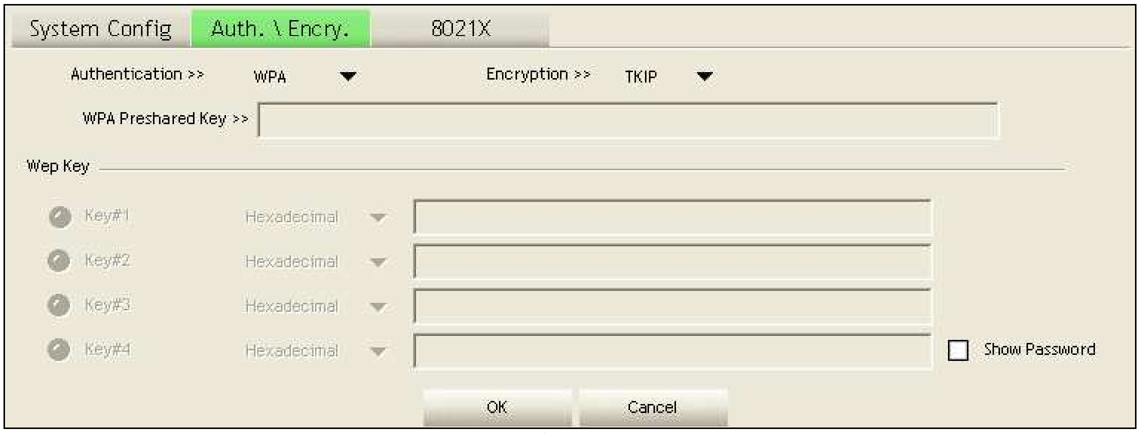
Profile Name >> PROF1

Message >> Invalid identity or password

Identity >>

Password >>

Retry the connection



Authentication >> WPA

Encryption >> TKIP

WPA Preshared Key >>

Wep Key

○ Key#1	Hexadecimal	
○ Key#2	Hexadecimal	
○ Key#3	Hexadecimal	
○ Key#4	Hexadecimal	

□ Show Password

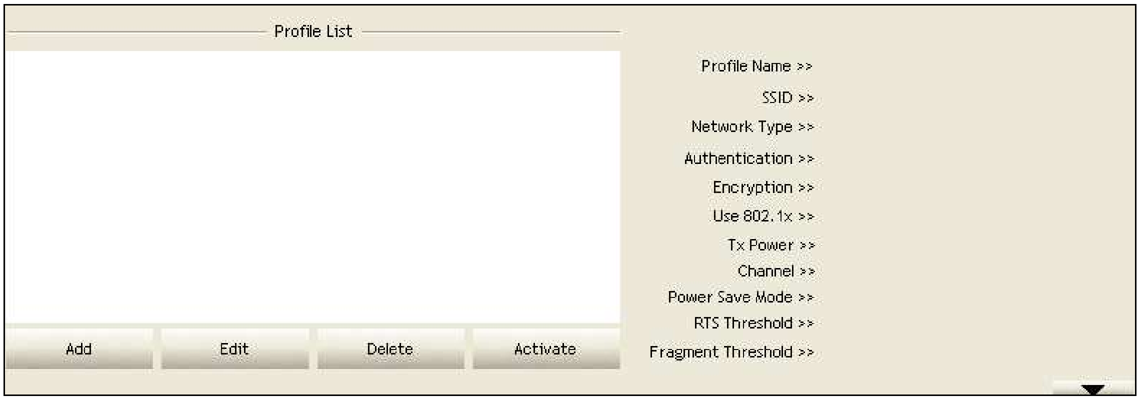
Configuration

When starting the utility, a small Ralink icon appears in the notifications area of the taskbar, as shown in the picture below.

You can double click it to maximize the dialog box if you selected to close it earlier. You may also use the mouse's right button to close the utility.

Profile

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



Definition of each field:

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.

Icons and buttons:

▶ : Indicates if a connection made from the currently activated profile.

▶ : Indicates if the connection has failed on a currently activated profile.

: Indicates the network type is infrastructure mode.

: Indicates the network type is in Ad-hoc mode.

🔑 : Indicates if the network is security-enabled.

Add : Click to add a new profile.

Edit : Click to edit an existing profile.

Delete : Deletes an existing profile.

Activate : Activates the selected profile.

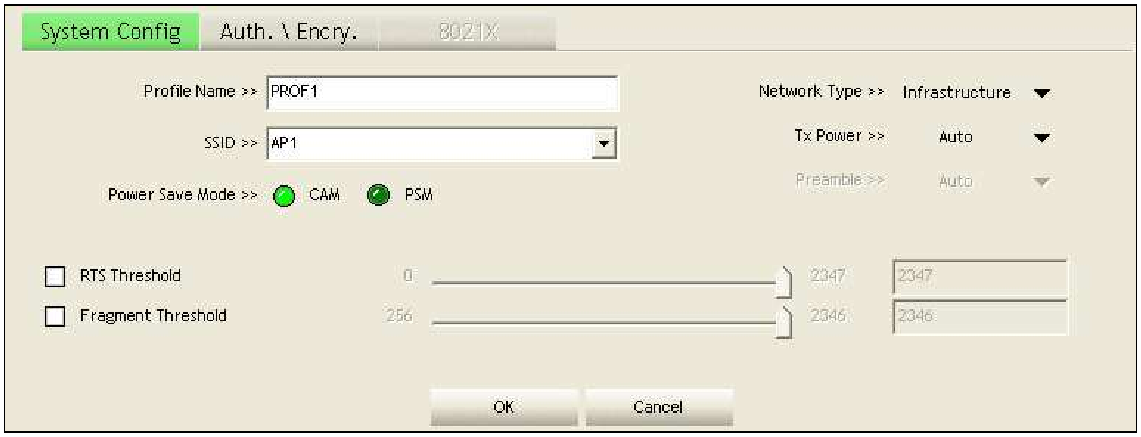
▼ : Shows information of the related status section.

▲ : Hides information of the related status section.

Add/Edit Profile

There are three methods to open the Profile Editor dialog box.

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



Profile Name >> PROF1

SSID >> AP1

Power Save Mode >> ● CAM ○ PSM

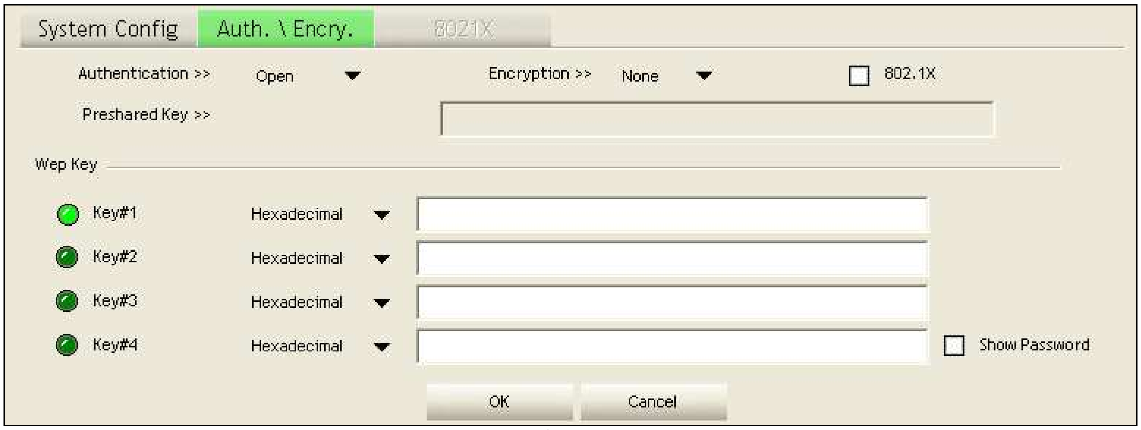
Network Type >> Infrastructure

Tx Power >> Auto

Preamble >> Auto

□ RTS Threshold 0 2347 2347

□ Fragment Threshold 256 2346 2346



Authentication >> Open

Encryption >> None

□ 802.1X

Preshared Key >>

Wep Key

● Key#1 Hexadecimal

○ Key#2 Hexadecimal

○ Key#3 Hexadecimal

○ Key#4 Hexadecimal

□ Show Password

Configuration

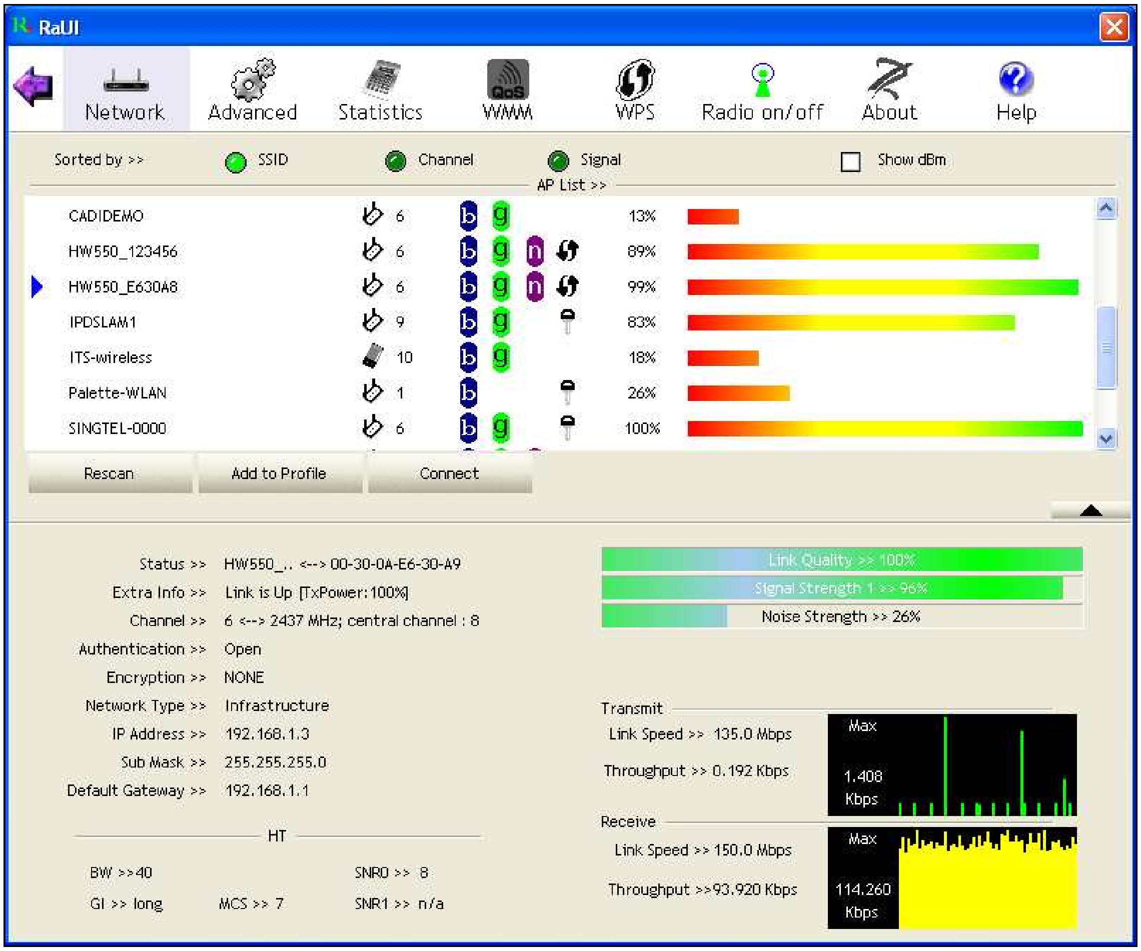
Parameter definitions

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 type includes 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 key in the value directly. The default value is 2347.

6. Fragment Threshold: User can adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346.
7. Channel: Only available for setting under Ad-hoc mode. Users can choose the channel frequency to start their Ad-hoc network.
8. Authentication Type: There are 7 type 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 type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, both TKIP and AES encryption is available.
10. 802.1x Setting: This is introduced in the 802.1x topic.
11. Pre-shared Key: This is the key shared between the AP and STA. For WPA-PSK and WPA2-PSK authentication mode, 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 listed below:
    a. Hexadecimal - 40bits : 10 Hex characters.
    b. Hexadecimal - 128bits : 26Hex characters.
    c. ASCII - 40bits : 5 ASCII characters.
    d. ASCII - 128bits : 13 ASCII characters.

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 below.



CADIDEMO	6	b g	13%
HW550_123456	6	b g n	89%
HW550_E630A8	6	b g n	99%
IPDSLAM1	9	b g	83%
ITS-wireless	10	b g	18%
Palette-WLAN	1	b	26%
SINGTEL-0000	6	b g	100%

Status >> HW550_.. <--> 00-30-0A-E6-30-A9
Extra Info >> Link is Up [TxPower:100%]
Channel >> 6 <--> 2437 MHz; central channel : 8
Authentication >> Open
Encryption >> NONE
Network Type >> Infrastructure
IP Address >> 192.168.1.3
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.1.1

HT
BW >>40
GI >> long
MCS >> 7
SNR0 >> 8
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> 96%
Noise Strength >> 26%

Transmit
Link Speed >> 135.0 Mbps
Throughput >> 0.192 Kbps
Max
1.408 Kbps

Receive
Link Speed >> 150.0 Mbps
Throughput >>93.920 Kbps
Max
114.260 Kbps

Network function

Definition of each field

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.

Icons and buttons

▶ : Indicates that the connection is successful.

: Indicates the network type is in infrastructure mode.

: Indicates the network type is in Ad-hoc mode.

🔑 : Indicates that the wireless network is security-enabled.

a : Indicates 802.11a wireless mode.

b : Indicates 802.11b wireless mode.

g : Indicates 802.11g wireless mode.

n : Indicates 802.11n wireless mode.

Sorted by >> ● SSID ● Channel ● Signal : Indicates that the AP list is sorted by SSID, Channel or Signal.

Connect : Button to connect to the selected network.

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

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.

▼ : Shows the Status Section.

▲ : Hides the Status Section.

Connected network

When utility first runs, it will select the best AP to connect to automatically.

If the user wants to use another AP, they can click "Connect" for the intended AP to make a connection.

If the intended network uses 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 the example on 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.) The introduction is as 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.
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 bandsThe information is further explained as follows :
    a. Authentication Type: There are three types of authentication modes supported by RaConfig. They are open, Shared, WPA-PSK and WPA system.
    b. 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.
    c. Config Methods: Correspond to the methods the AP supports as an Enrollee for adding external Registrars, (a bitwise OR of values.)

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

d. 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

e. Selected Registrar: Indicates if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".

f. State: The current configuration state of the AP. The values are "Unconfigured" and "Configured".

g. Version: The specified WPS version.

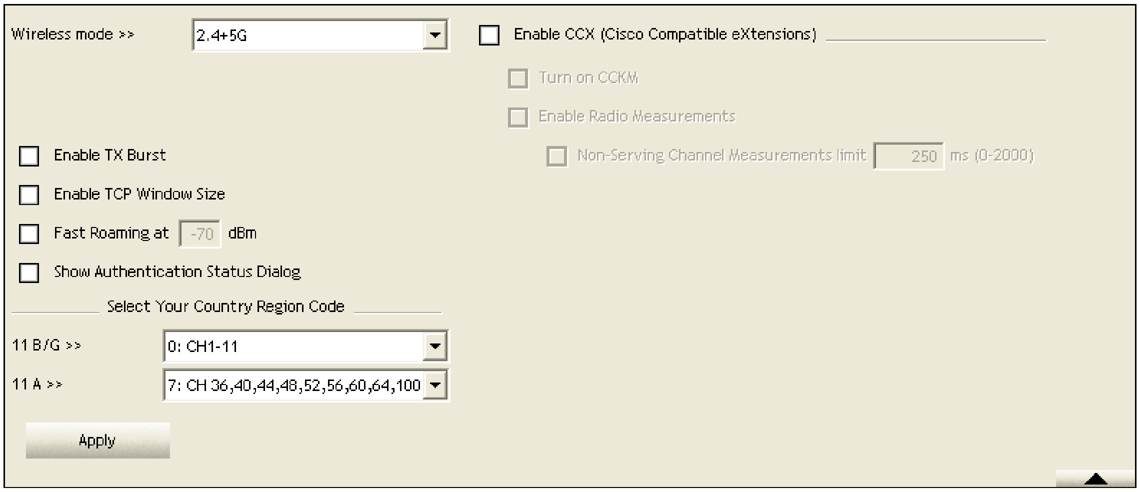
h. AP Setup Locked: Indicates if the AP has entered a locked setup state.

i. UUID-E: The universally unique identifier (UUID) element generated by the Enrollee. The value is 16 bytes.

j. 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".

Advanced

The following shows the Advance functions of the utility.



Wireless mode >> 2.4+5G

□ Enable CCX (Cisco Compatible eXtensions)

□ Turn on CCKM

□ Enable Radio Measurements

□ Non-Serving Channel Measurements limit 250 ms (0-2000)

□ Enable TX Burst

□ Enable TCP Window Size

□ Fast Roaming at -70 dBm

□ Show Authentication Status Dialog

Select Your Country Region Code

11 B/G >> 0: CH1-11

11 A >> 7: CH 36,40,44,48,52,56,60,64,100

Definition of each field

1. Wireless mode: supported wireless mode.
2. Enable TX Burst: Ralink's proprietary frame burst mode.
3. Enable TCP Window Size: Optimise the TCP window size to allow for greater throughput.
4. Fast Roaming at-: enables fast roaming, which is set by the transmit power.
5. 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.

6. Enable CCX (Cisco Compatible Extensions): Choose whether Cisco Compatible Extensions are supported or not.

   a. LEAP turn on CCKM.

   b. Enable Radio Measurement: can measure the channel every 0~2000 milliseconds.

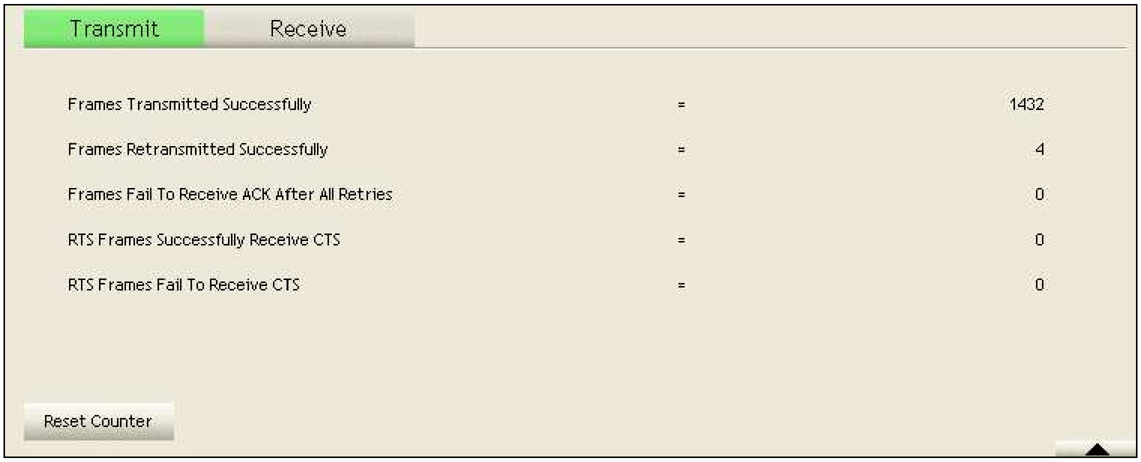
Icons and buttons

▼: Shows the Status Section.

▲ : Hides the Status Section.

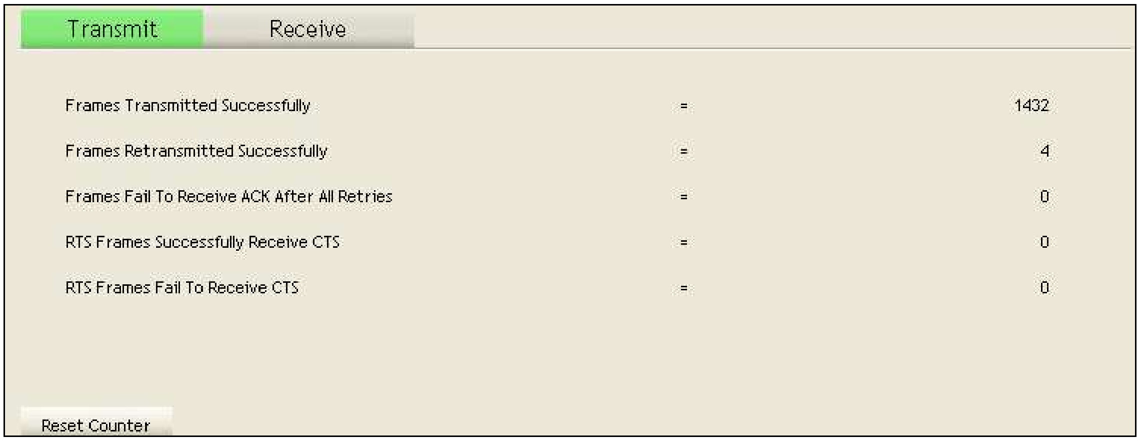
Statistics

The Statistics page displays detailed counter information based on 802.11 MIB counters. The following shows the detailed page layout.



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

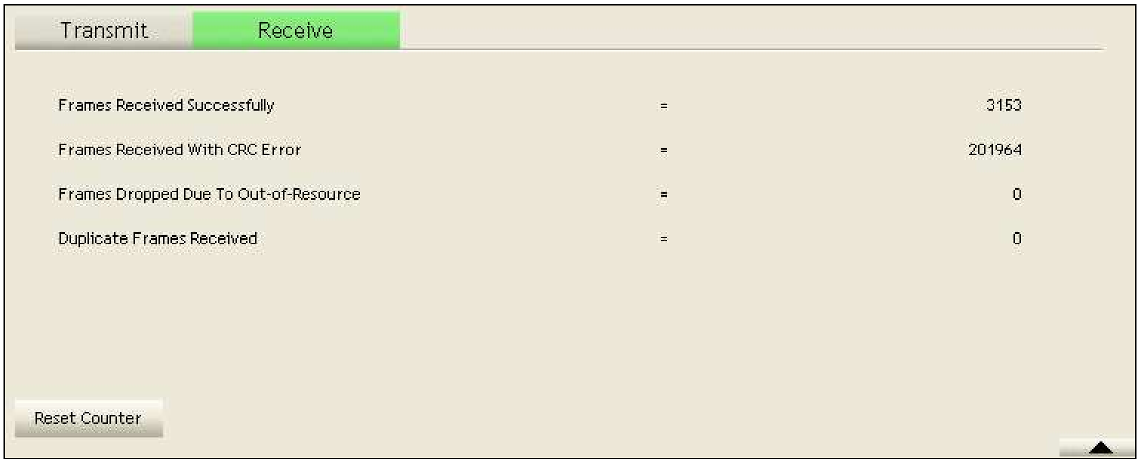
Transmit Statistics:



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

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

Receive Statistics:



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

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 all the counters to zero.

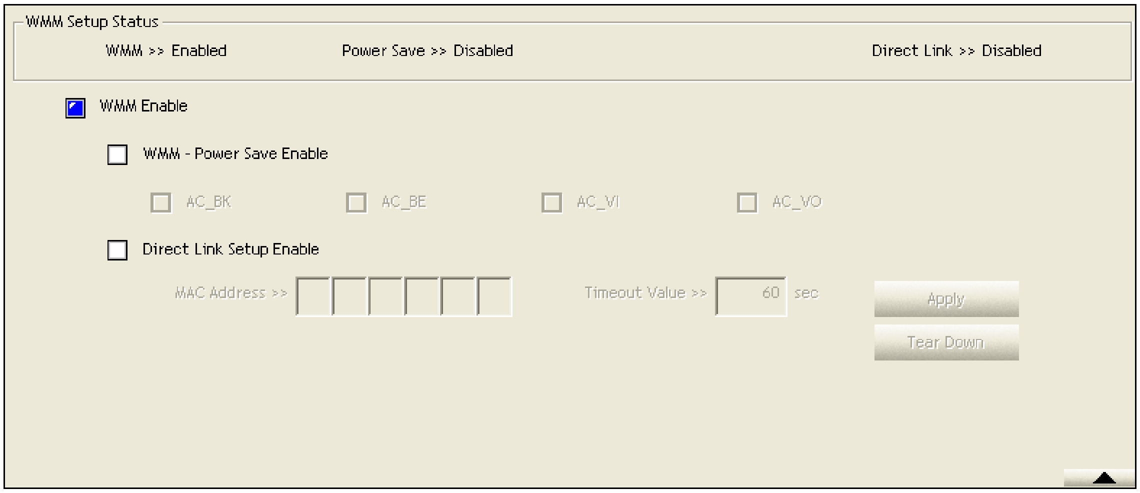
Icons and buttons

▼: Shows the Status Section.

▲: Hides the Status Section.

WMM

The following picture shows 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

1. WMM Enable : Enable Wi-Fi Multi-Media.
2. WMM - Power Save Enable: Enable WMM Power Save.
3. Direct Link Setup Enable: Enable DLS (Direct Link Setup).

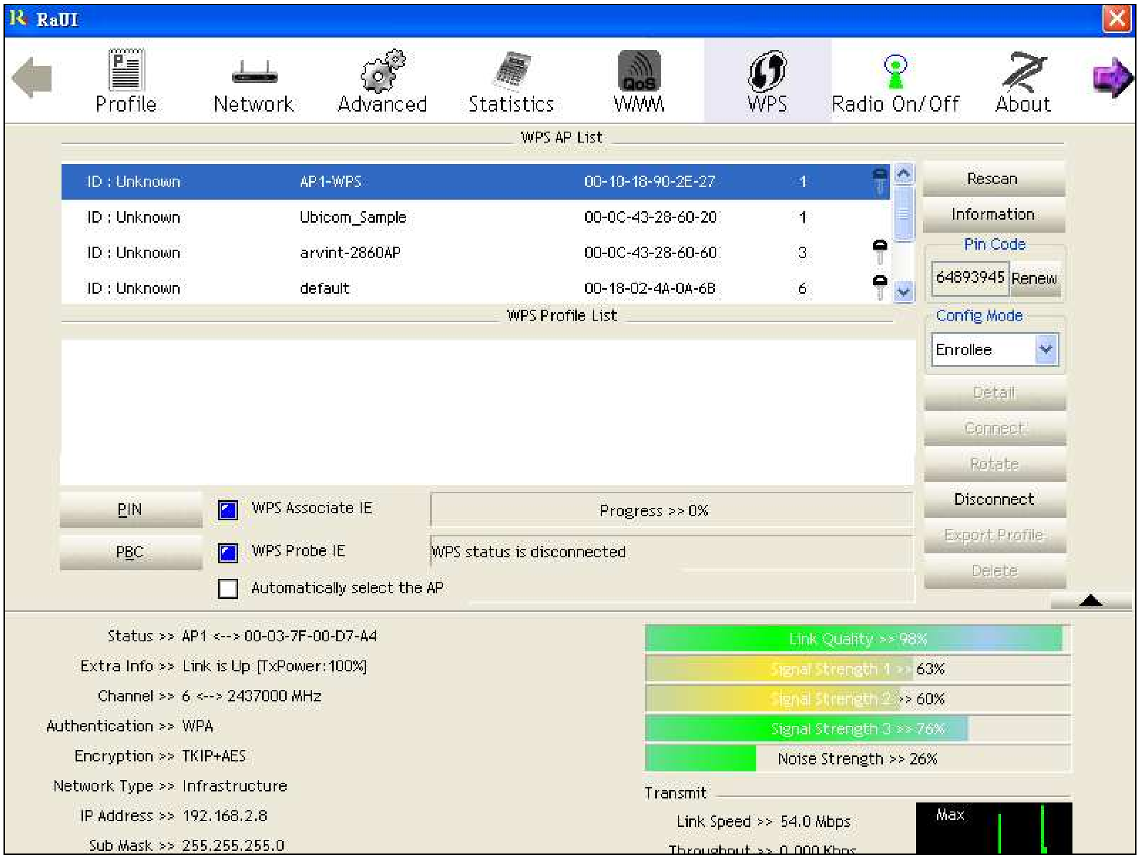
Icons and buttons

▼: Shows the Status Section.

▲ : Hides the Status Section.

WPS

The following shows the WPS functions.



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

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

Link Quality >> 98%
Signal Strength 1 >> 63%
Signal Strength 2 >> 60%
Signal Strength 3 >> 76%
Noise Strength >> 26%

Link Speed >> 54.0 Mbps
Throughput >> 0.000 Kbps

Definition of each field

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.
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 re-generate 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.
    a. Detail: Command to obtain Information about Security and the Key in the credential.
    b. Connect: Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
    c. Rotate: Command to rotate to connect to the next network inside credentials.
    d. 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.
    e. Export Profile: Exports all credentials to a Profile.

f. Delete: Deletes an existing credential. And then selects the next credential. If there is not another credential, the driver will select any non-security AP.

9. PIN: Start to add to Registrar using PIN configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.
10. PBC: Start to add to AP using PBC configuration method.

After the user clicks PIN or PBC, please do not rescan within two-minutes of the connection. 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.

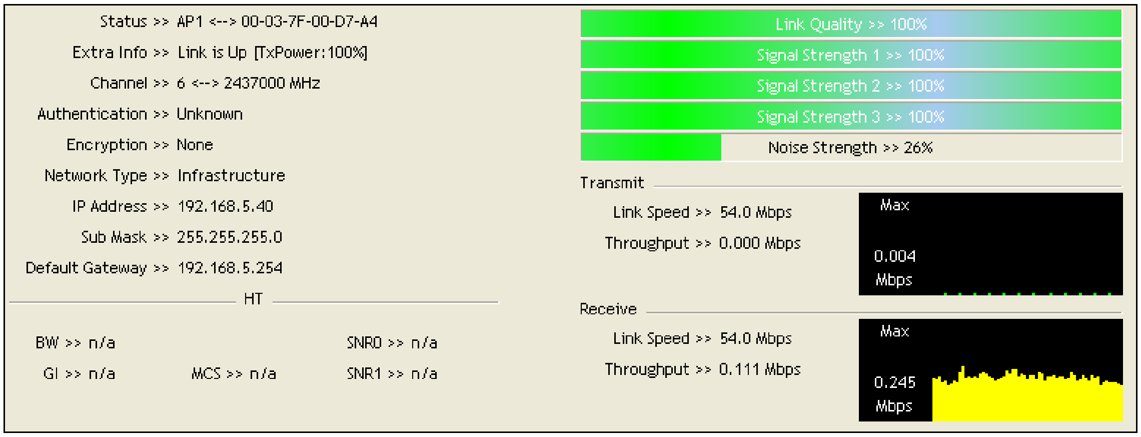
Icons and buttons

▼ : Shows the Status Section.

▲ : Hides the Status Section.

Link Status

The link status page displays detailed information about the current connection as shown below.



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%

Noise Strength >> 26%

Transmit

Link Speed >> 54.0 Mbps

Throughput >> 0.000 Mbps

Receive

Link Speed >> 54.0 Mbps

Throughput >> 0.111 Mbps

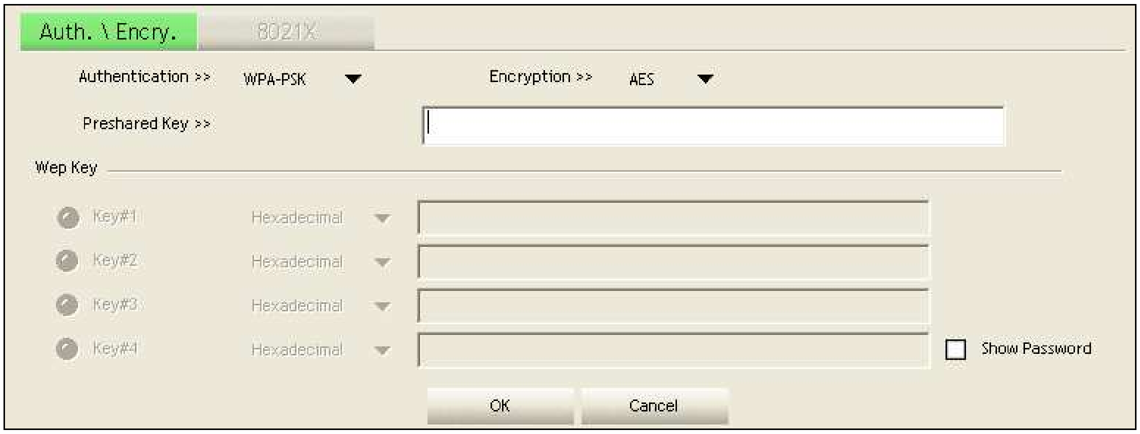
Definition of each field

1. Status : Current connection status. If no connection, if will show Disconnected. Otherwise, the SSID and BSSID will show here.
2. Extra Info : Display link status in use.
3. Channel : Display 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 about current connection.
8. Sub Mask : Sub mask about 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. Noise Strength : Display noise signal strength.
17. HT : Display current HT status in use, containing BW, GI, MCS, SNR0, and SNR1 value.

Security

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



Authentication >> WPA-PSK

Encryption >> AES

Preshared Key >>

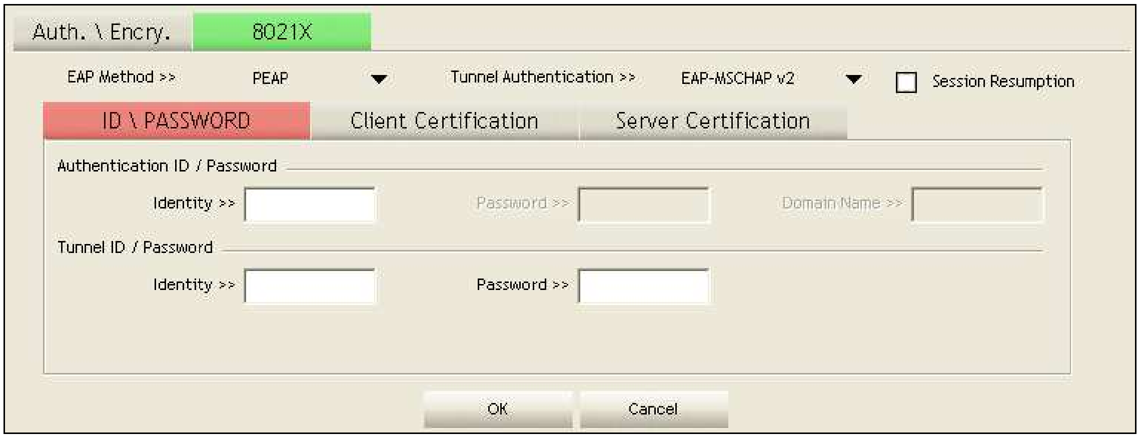
Definition of each field

1. Authentication Type: There are 7 authentication modes supported by the utility. They are open, Shared, LEAP, 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

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.
6. Hexadecimal - 40bits: 10 Hex characters.
7. Hexadecimal - 128bits: 32Hex characters.
8. ASCII - 40bits: 5 ASCII characters.
9. ASCII - 128bits: 13 ASCII characters.

802.1x Setting

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



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Session Resumption

Authentication type:

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. For tunnel authentication, only support "Generic Token Card" authentication.
5. LEAP: Light Extensible Authentication Protocol is an EAP authentication type used primarily by Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.
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.

Session Resumption

User can choose to "Disable" and "Enable".

Tunnel Authentication

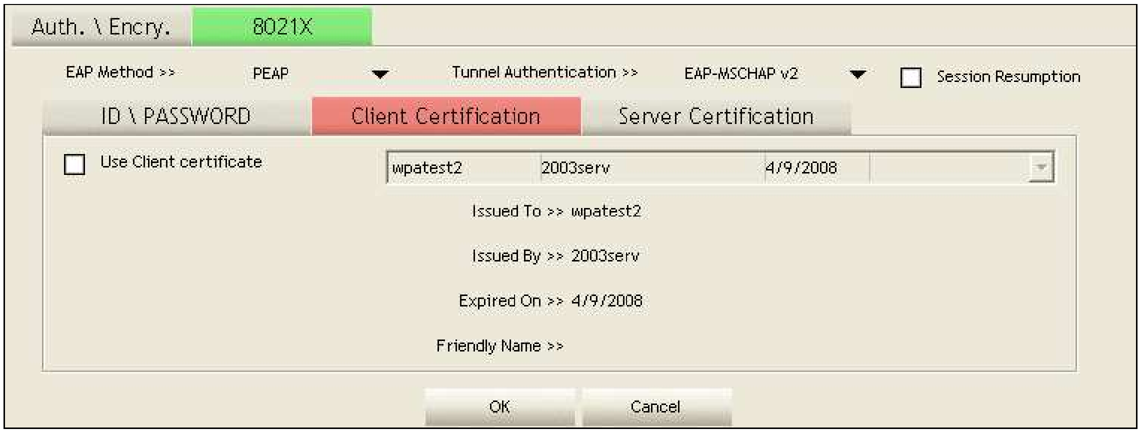
1. Protocol: Tunnel protocol, List information include "EAP-MSCHAP v2", "EAP-TLS/Smart card", "Generic Token Card", "CHAP", "MS-CHAP", "MS-CHAP-V2", "PAP" and "EAP-MD5".
2. Tunnel Identity: Identity for tunnel.

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 4/9/2008

Issued To >> wpatest2

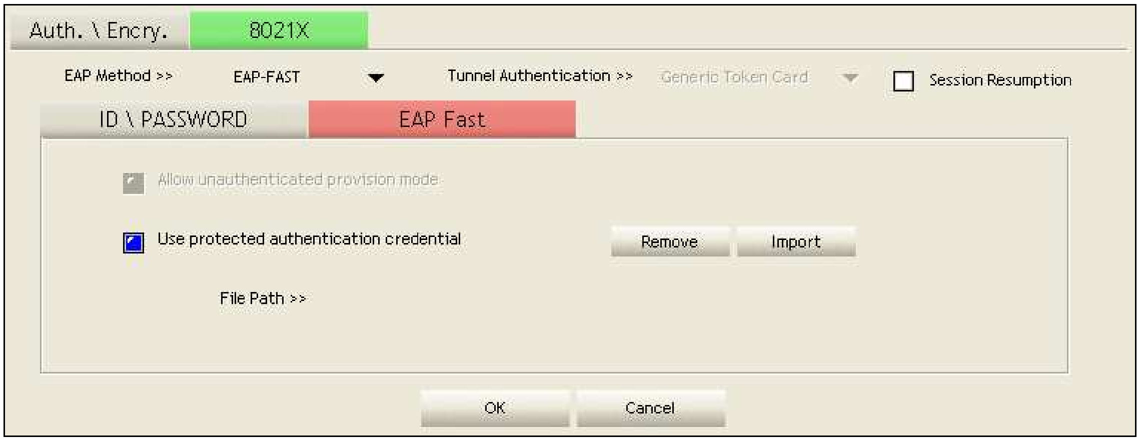
Issued By >> 2003serv

Expired On >> 4/9/2008

Friendly Name >>

Use Client certificate: Client certificate for server authentication.

EAP Fast



EAP Method >> EAP-FAST

Tunnel Authentication >> Generic Token Card

□ Session Resumption

☑ Allow unauthenticated provision mode

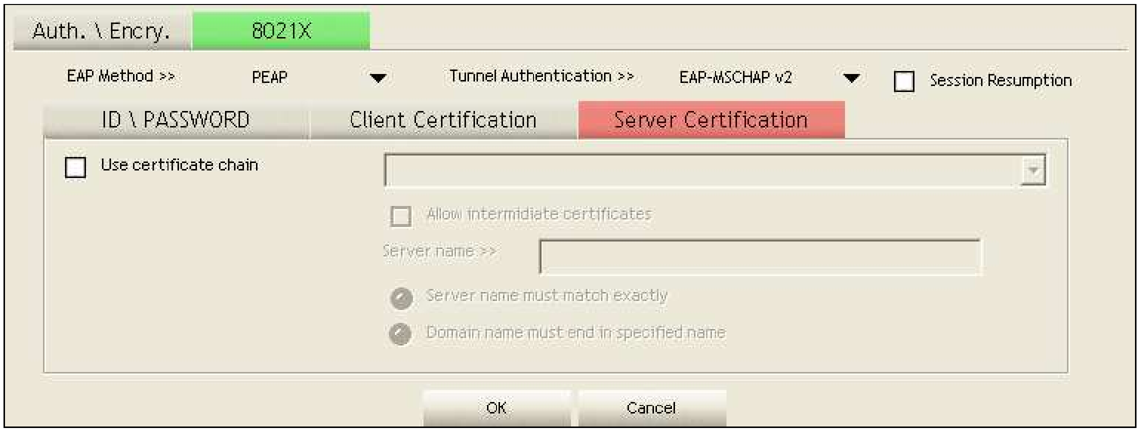
☑ Use protected authentication credential

File Path >>

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

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

Server Certification



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

□ Session Resumption

□ Use certificate chain

□ Allow intermidiate certificates

Server name >>

○ Server name must match exactly

○ 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.

⚠ Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do not open the device. Opening or removing the device can expose you to dangerous voltage points or other risks. Only qualified service personnel can service the device. Please contact your vendor for further information.
- Do not use your device during a thunderstorm. There may be a risk of electric shock brought about by lightning.
- Do not expose your device to dust or corrosive liquids.
- Do not use this product near water sources.
- Do not obstruct the ventilation slots.