Wireless LAN USB Adapter

User Manual 1.0

© 2010

Contents

1.	Win	dows W	Vireless Utility	4
	1.1	Windo	ws Zero Configuration for XP	4
		1.1.1	Ralink Wireless Utility and Windows Zero Configuration	4
		1.1.2	Windows Zero Configuration (WZC)	5
	1.2	Windo	ws AutoConfig Service for Vista	.10
		1.2.1	Ralink Wireless Utility and Windows AutoConfig Service	.10
		1.2.2	Windows AutoConfig Service	.11
2.	Rali	nk Wire	eless Utility (RaUI)	.18
	2.1	Start		.18
		2.1.1	Start RaUI	.18
	2.2	Profile		.21
		2.2.1	Profile	.21
		2.2.2	Add/Edit Profile	.22
		2.2.3	Example to Add Profile in Profile	.25
		2.2.4	Pre-logon Connect	.27
	2.3	Netwo	rk	.27
		2.3.1	Network	.27
		2.3.2	Example on Adding Profile in Network	.30
	2.4	Advan	ced	.31
		2.4.1	Advanced	.31
		2.4.2	Certificate Management	.32
	2.5	Link Iı	nformation	.33
		2.5.1	Link Status	.33
		2.5.2	Throughput	.34
		2.5.3	Statistics	.34
	2.6	About.		.35
		2.6.1	About	.35
	2.7	WPS		.36
		2.7.1	WPS	.36
		2.7.2	Example to Add to Registrar Using PIN Method	.38
		2.7.3	Example to Add to Registrar Using PBC Method	.41
		2.7.4	Example to Configure a Network/AP Using PIN or PBC Method.	.45
3.	Secu	urity		.47
	3.1	Auth.\	Encry. Setting – WEP/TKIP/AES	.47
	3.2	802.1x	Setting	.48
	3.3	Examp	ble to Configure Connection with WEP on	.51
	3.4	Examp	ble to Configure Connection with WPA-PSK	.53

	3.5 Example to Configure Connection with WPA	.55
4.	Appendix	.60
	4.1 Country Channel List	.60
	4.2 Acknowledgements	.62
5.	FAQ	.63
	5.1 FAQ	.63
6.	Installation	.63

1. Windows Wireless Utility

1.1 Windows Zero Configuration for XP

1.1.1 Ralink Wireless Utility and Windows Zero Configuration

Windows XP includes a wireless configuration utility named "Windows Zero configuration" (WZC) which provides basic configuration functions to the Ralink Wireless NIC. Ralink's utility (RaUI) additionally provides WPA functionality. To make it easier for the user to select the correct utility. RaUI will let users make a selection when it first runs after windows XP boots.

Right-clicking the icon will bring up the selection window and allow the user to make a selection.



Figure 1-1 RaUI.exe

RaUI can co-exist with <u>WZC</u>. When coexisting with <u>WZC</u>, RaUI only provides monitoring functions, such as surveying the link status, network status, statistic counters, advanced feature status, WMM status and WPS status. It won't interfere with WZC's configuration or profile functions. It is shown as Figure 1-2.



Figure 1-2 Select WZC or RaUI

If "Use RaConfig as Configuration utility" is selected, please jump to Section 2 on running RaUI.

If "Use Zero Configuration as Configuration utility" is selected, please continue. We will explain the difference between RaUI and <u>WZC</u>. Figure 1-3 shows the RaUI status when <u>WZC</u> is activated as the main control utility.

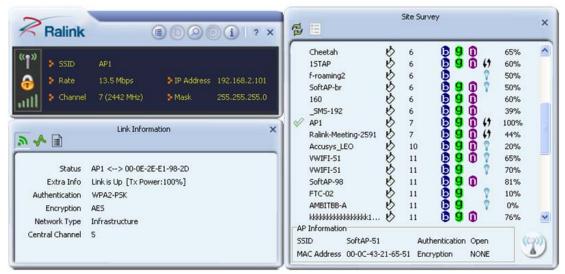


Figure 1-3 RaUI status with WZC active

When activating <u>WZC</u>, there are several difference with the RaUI status, compared to the RaUI status without <u>WZC</u> running.

- The profile button will be gray. Profile functionality is removed since the NIC is controlled by <u>WZC</u>.
- The Connect and Add Profile function will be gray. Profile functionality is removed since the NIC is controlled by <u>WZC</u>.

Please read through this document for full details on the other functions provided by RaUI.

1.1.2 Windows Zero Configuration (WZC)

• If there is no connection or it is lost, the status prompt will pop up, as shown in Figure 1-4.

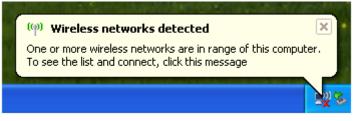


Figure 1-4 status prompt for no connection

• Right-click the network connection icon in taskbar.

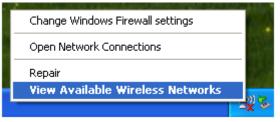


Figure 1-5 Select WZC main status

• Select "View Available Wireless Networks" and the "Wireless Network Connection" dialog box will pop up, as shown in Figure 1-6.

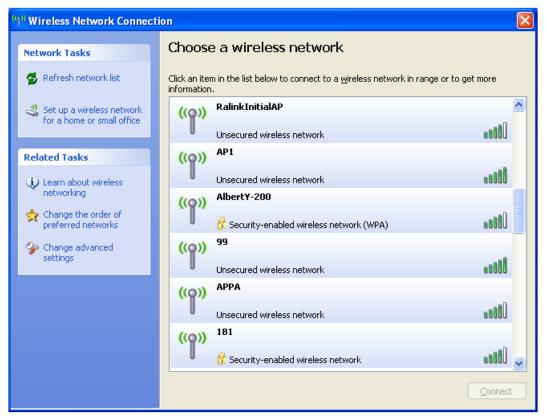


Figure 1-6 Wireless Network Connection

• Select the intended access point and click "Connect". Then click "Connect Anyway" as shown as Figure 1-7.

(⁽⁰⁾⁾ Wireless Network Connect	ion	×
Network Tasks	Choose a wireless network	
😴 Refresh network list	Click an item in the list below to connect to a wireless network in range or to get more information.	- 15
Set up a wireless network for a home or small office	((p)) RalinkInitialAP	
Related Tasks Wireless N	letwork Connection	
	y are connecting to the unsecured network "AP1". Information sent r this network is not encrypted and might be visible to other people. It over this this network,	
	Security-enabled wireless network (WPA)	
	((p)) 99 Unsecured wireless network	
	((^)) APPA	
		כ

Figure 1-7 Select intended AP: AP1, then click "Connect"

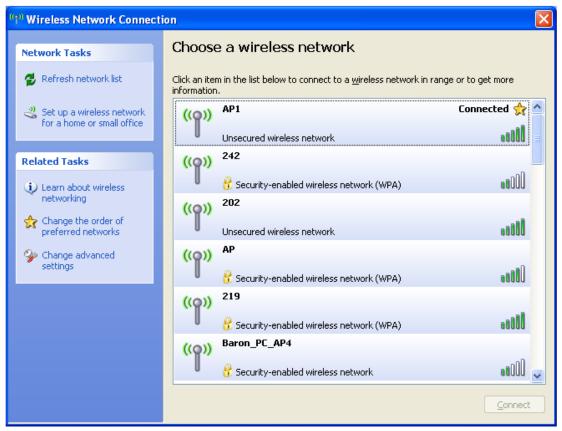


Figure 1-8 Connect AP: AP1 successfully

• If you want to modify information about the AP, click "Change advanced settings" as shown in Figure 1-9. Then select the "Wireless Networks" tab shown as Figure 1-10.

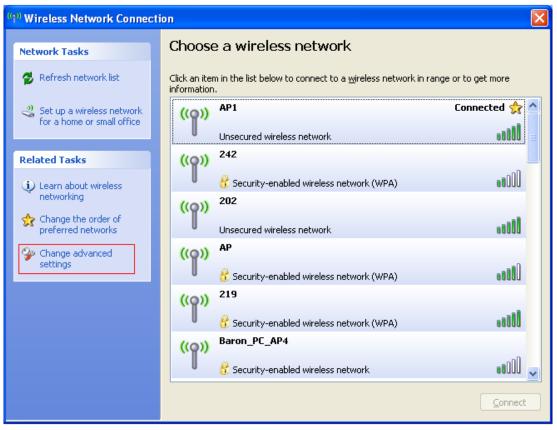


Figure 1-9 Click "Change advanced settings"

🕂 Wireless Network Connection Properties 🛛 🛛 🔀
General Wireless Networks Advanced
Use Windows to configure my wireless network settings
Available networks:
To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.
View Wireless Networks
Preferred networks: Automatically connect to available networks in the order listed below:
P AP1 (Automatic) Move up
Move <u>d</u> own
<u>A</u> dd <u>R</u> emove <u>Properties</u> Learn about <u>setting up wireless network</u> <u>Adyanced</u>
OK Cancel

Figure 1-10 Choose the "Wireless Networks" tab

• Click "Properties" as shown in Figure 1-11. Then click "OK" button.

AP1 properties ?	×
Association Authentication Connection	_
Network <u>n</u> ame (SSID): AP1	
Wireless network key	
This network requires a key for the following:	
Network Authentication:	
Data encryption: Disabled	
Network key:	
Confirm network key:	
Key inde <u>x</u> (advanced): 1	
This is a <u>computer-to-computer</u> (ad hoc) network; wireless access points are not used	
OK Cancel	

Figure 1-11 AP's properties

• After filling in the appropriate value, click "OK." The pop-up will indicate the status as shown in Figure 1-12.

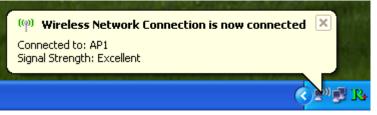


Figure 1-12 Network connection status

• Clicking the Ralink icon will bring up the RaUI main window. Users can find the surrounding APs in the list. The currently connected AP will be shown with a blue icon beside it, as shown in Figure 1-13. Users may use the advanced tab to configure more advanced features provided by Ralink's wireless NIC. For details on configuring the advanced features, please check the Advance setting section.

		dress 192.168.2.101	Cheetah 1STAP f-roamir	ě	6 D	904	65% 60%	
		255.255.255.0	SoftAP- 160		6 D 6 D	90	50% 50% 60%	
≁ ∎	Link Information	3	Accusys	Neeting-2591	6 D 7 D 7 D 10 D	904	44% 20%	
Extra Info Link Authentication WPA Encryption AES	<> 00-0E-2E-E1-98-2D is Up [Tx Power:100%] \2-PSK astructure		WWIFI-5 VWIFI-5 SoftAP- FTC-02 AMBITB	51 V 98 V		9099990	65% 70% 81% 10% 0% 76%	

Figure 1-13 Show connection status by using WZC to initiate the connection

1.2 Windows AutoConfig Service for Vista

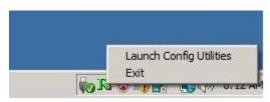
1.2.1 Ralink Wireless Utility and Windows AutoConfig Service

In Windows Vista, the Auto Config service provides basic wireless configuration functions for the Ralink Wireless Network Interface Controller. In order to perform these functions, the Auto Config service should first be enabled (Refer to Section 1-2-2).

Once the Ralink wireless utility is minimized, click the Ralink icon as shown in Figure 1-1. This will bring up the option menu shown as Figure 1-2 for the user to restore the utility window or terminate the utility.



Figure 1-1





The Ralink wireless utility as shown in Figure 1-3, provides profile management, the available networks listing, a statistical counter display, Wi-Fi multimedia (WMM), protected Wi-Fi setup, Cisco compatible extensions (CCX), call admission control (CAC), radio controls, Ralink driver/utility information, and help functions.



Figure 1-3 Ralink Utility

The Ralink wireless utility starts in compact mode as shown in Figure 1-3. Clicking the expanding icon at the bottom-right corner can change to the full mode as shown in Figure 1-4.

Ralink	()(i) ? ×	2		Site Sur	vey				>
SSID	AP1			118 SoftAP-33333	599	2 2 2	8 9 6 9	0	Ý 1	i5% .0% %0%	ŕ
👌 🕴 Rate	300.0 Mbps	P Address	192, 168, 2, 101	dlink-111	Ň	3	ğ	ň		1%	
1 👂 Channel	7 (2442 MHz)	Mask 🗧	255.255.255.0	001601D314B4 G	Ď	5	6 9	-		0%	
				wxx	Ď	6	69	0	0 :	9%	
	Link Informa		×	ExRegNW3135DB	0	6	69	0	() 7	6%	
A 🗈	LINK INFORMA	auon	×	Baron_Test baldwin	5	6	09	0	<u></u> 10	6% 5%	
				_wen	ě	6	0 9	0	•	9%	
Status	AP1 <> 00-0E-2E	-E1-98-2D		RT305x_AP	0	6	69	0	9	4%	
Extra Info	Link is Up [Tx Powe	er:100%]		Stitch	0	6 6	69	0	9 s	4%	
Authentication	WPA2-PSK			1STAP	Ø	6	6 9	0	() :	5%	
Encryption	AES			_SMS-192	0	6	0 9	Q		0%	
Network Type	Infrastructure			Cheetah	0	6	69	0	4	14%	
Central Channel	5			AP Information SSID 118 MAC Address 00-21-9	1.57-00		thentication	WPA AES			(9)

Figure 1-4 Ralink Utility in full mode

1.2.2 Windows AutoConfig Service

The following steps outline the procedure for starting/stopping the Windows AutoConfig service.

Select "Control Panel" from "Settings" in the start menu



Double-click the "Administrative Tools" icon

Control Panel +					👻 🌆 Searc	h		_
	Name + +	(I						_
Control Panel Home Classic View	Name - +	Category +		N.		P		
	Add Hardware	Administrative Tools	AutoPlay	Backup and Restore	Color Management	Date and Time	Default Programs	
	-			A	123g	D	F	
	Device Manager	Ease of Access Center	Folder Options	Fonts	Game Controllers	Indexing Options	Infrared	
		e,	Ø	Ĩ	L.)0	1	
	Internet Options	iSCSI Initiator	Keyboard	Mouse	Network and Sharing C	Offline Files	Pen and Input Devices	
	2.2	Nº12		1	2			
	People Near Me	Performance Informati	Personaliza	Phone and Modem	Power Options	Printers	Problem Reports a	
			6		()		Q	
	Program Updates	Programs and Features	Regional and Language	Scanners and Cameras	Security Center	Sound	Speech Recogniti	
					A	00		

Double-click "Services"

🕤 🔾 🗢 🔯 🔹 Control f	Panel + Administrative Tools		🔻 🐼 s	earch	
Organize 👻 📗 Views	+		 	- 28	0
Favorite Links More >> Folders Desktop Desktop Shufen Public Computer Network Control Panel Control Panel Control Panel Control Panel Control Panel Default Programs Ease of Access Cent Fonts Network and Sharing Performance Informa Performance Informa Perfonalization Performance Informa Perfonance Informa Perfonance Informa Performance Informa Per	Name Computer Management Data Sources (ODBC) SCSI Initiator Local Security Policy Memory Diagnostics Microsoft .NET Fram Microsoft .NET Fram Reliability and Perfor System Configuration Task Scheduler Windows Firewall wit	11/2/2006 8:54 PM 11/2/2006 8:53 PM 11/2/2006 8:54 PM 11/2/2006 8:56 PM 11/2/2006 8:55 PM 1/1/2100 9:39 AM 1/1/2100 9:39 AM 1/1/2100 10:20 AM 11/2/2006 8:55 PM 11/2/2006 8:53 PM 11/2/2006 8:53 PM 11/2/2006 8:54 PM	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	• KB KB	

Double-click "WLAN AutoConfig"

Services (Local)	😋 Services (Local)	-					
	Select an item to view its description.	Name 🔺	Description	Status	Startup Type	Log On As	
		🔍 Windows Backup	Provides W		Manual	Local System	
	1	Windows CardSpace	Securely e		Manual	Local System	
	1	Windows Color Sys	The WcsPl		Manual	Local Service	
	1	🔅 Windows Connect	Act as a R	Started	Manual	Local Service	
		🔍 Windows Defender	Scan your	Started	Automatic	Local System	
	1	Windows Driver Fo	Manages u	Started	Automatic	Local System	
	1	Windows Error Rep	Allows erro	Started	Automatic	Local System	
		🔍 Windows Event Coll	This servic		Manual	Network S	
	1	Windows Event Log	This servic	Started	Automatic	Local Service	
	1	Windows Firewall	Windows Fi	Started	Automatic	Local Service	
	1	🔅 Windows Image Ac	Provides im	Started	Automatic	Local Service	
	1	🔅 Windows Installer	Adds, modi		Manual	Local System	
	1	🔅 Windows Managem	Provides a	Started	Automatic	Local System	
	1	Windows Media Pla	Shares Win		Manual	Network S	
	1	Windows Modules I	Enables ins		Manual	Local System	
	1	🔆 Windows Presentat	Optimizes		Manual	Local Service	
	1	Windows Remote M	Windows R		Manual	Network S	
	1	Windows Search	Provides c	Started	Automatic	Local System	
	1	🔍 Windows Time	Maintains d	Started	Automatic	Local Service	
	1	🔅 Windows Update	Enables th	Started	Automatic (D	Local System	
		WinHTTP Web Prox	WinHTTP i		Manual	Local Service	
		Wired AutoConfig	This servic		Manual	Local System	
		WLAN AutoConfig	Dis servic	Started	Automatic	Local System	
		WMI Performance	Provides p		Manual	Local System	
		Workstation	Creates an	Started	Automatic	Local Service	

Manage the AutoConfig properties in the dialog box

Recovery 1 Wlansvc	Dependenci	es		
Wlansvc				
WLAN Auto	Config			
			oters, mana	ges 🔺
ZORAN COLL C	.exe + Loca	alSystemNet	workRestric	ted
Automatic				•
	i <u>p options.</u>			
Stopped				
Stop.		Pause	Res	ume
ne start param	eters that ap	ply when yo	u start the s	service
1	OK	1	- 1	Apply
	WLAN conn e: em32\svchost Automatic e service startu Stopped	WLAN connections and e: em32\svchost.exe +k Loca Automatic e service startup options, Stopped	WLAN connections and profiles. e: em32\svchost.exe +k LocalSystemNetv Automatic e service startup options. Stopped Stop Pause he start parameters that apply when yo	e: em32\svchost.exe +k LocalSystemNetworkRestric Automatic e service startup options. Stopped Stop Pause Res he start parameters that apply when you start the s

Windows profile manager can be accessed via control panel or network connection icon in the task bar.

1. Access via network connection icon

Right-click the network connection icon in the taskbar, then select "Network and Sharing Center" from the pop-up menu



Select "Manage wireless networks" from the tasks list

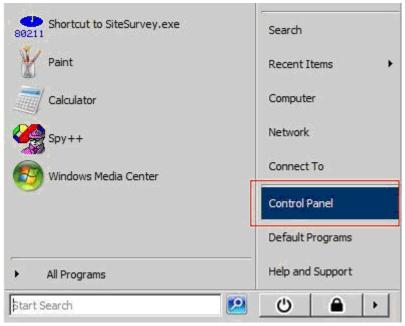
	Network and Sharing Center	👻 🚱 Search	
Tasks View computers and devices	Network and Sharing Center	þ.	View full map
Connect to a network Manage wireless networks Set up a connection or network Manage network connections	SHUFEN-PC (This computer)	Internet
Diagnose and repair	217 (Public network)		Customize
	Access	Local and Internet	
	Connection	Local Area Connection 2	View status
	22. Sharing and Discovery		
	Sharing and Discovery		
	Network discovery	© Off	•
	1 March 1 Marc	© Off ⊚ Off	
	Network discovery		
	Network discovery File sharing	• Off	
	Network discovery File sharing Public folder sharing	● Off ● Off	
See also	Network discovery File sharing Public folder sharing Printer sharing	 Off Off Off(no printers installed) 	• • • • • • • •

Right-click the network to bring up the profile managing menu

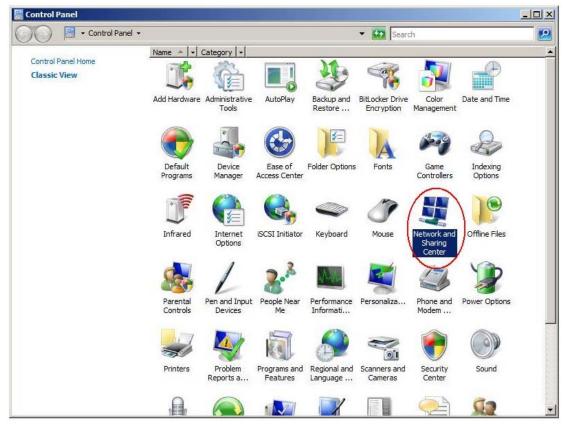
n Manage	Wireless Networks			_ [] ×
00	Tontrol Panel 🔻 Manage Wireless Ne	tworks	👻 🔀 Search	2
Window	ge wireless networks that use (Wireless ws tries to connect to these networks in the ord e network profiles.		r, drag a network up or down in tl	ne list. You can also add or
Add 🛛	📼 Remove 🛛 🛞 Adapter properties 🛛 🔒 Pro	ofile types 🛛 🙀 Network and Sharir	ng Center	0
Networks	you can view and modify (1)			Ξ
	223 Security: WPA2 Properties Remove network Rename	-enterprise Type: j	Any supported	Automatically connect
<u>.</u>	223 Profile name: 223 Security type: WPA2-Enterprise Radio type: Any supported	Mode: Automatically connect		

2. Access via control panel

Select "Control Panel" from the start menu



Double-click the "Network and Sharing Center" icon



Network and Sharing Center			_0×
Control Panel + N	letwork and Sharing Center	👻 🚱 Search	2
Tasks	Network and Sharing Center		0
View computers and devices Connect to a network Manage wireless networks Set up a connection or network Manage network connections	SHUFEN-PC (This computer	r)	View full map
Diagnose and repair	217 (Public network)		Customize
	Access	Local and Internet	
	Connection	Local Area Connection 2	View status
	Sharing and Discovery	© Off	•
	File sharing	© Off	-
	Public folder sharing	• Off	• • •
	Printer sharing	 Off(no printers installed) 	•
	Password protected sharing	© On	•
See also	Media sharing	© Off	-
Infrared Internet Options Windows Firewall	Show me all the files and folders Show me all the shared network		

Select "Manage wireless networks" from the tasks list

Right-click the network to bring up the profile managing menu

Manage	Wireless Networks			×
00	aff[] + Control Panel + Manage Wireless N	etworks	👻 🚱 Search	P
Window	ge wireless networks that use (Wireless ws tries to connect to these networks in the or enetwork profiles.	No. Solid and the real of the second	er, drag a network up or down in the list	t. You can also add or
🖧 Add 🛛	🗆 Remove 🛛 🖲 Adapter properties 🛛 🔒 Pr	ofile types 🛛 💺 Network and Sharir	ng Center	0
Networks	you can view and modify (1)			E
	Properties Remove network Rename			
	223 Profile name: 223 Security type: WPA2-Enterprise Radio type: Any supported	Mode: Automatically connect		

2. Ralink Wireless Utility (RaUI)

2.1 Start

2.1.1 Start RaUI

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 Figure 2-1.

Ralink	()() ? ×	2		Site Sur	vey				;
i SSID Rate III Channel	AP1 13.5 Mbps 7 (2442 MHz)	⇒ IP Address ∋ Mask	192.168.2.101 255.255.255.0	issue63 catch_me_if_you SoftAP-51 gg Claude0 iverson	0000000	1 1 1 1 1 1		0000 0	() () ?	70% 76% 76% 60% 55% 24%	
~ i	Link Informa	ation	×	pega2 dlink 001601D31484_G _SM5-192	しししい	2 3 5 6		0	69 17	39% 100% 44% 50%	-1
Extra Info	AP1 <> 00-0E-2E Link is Up [Tx Powe WPA2-PSK			Baron_Test 160 f-roaming2	0000	6 6	000	00	2	99% 55% 50%	
Encryption Network Type	AES Infrastructure			RT305x_AP_BFu Stitch AP Information	Ďb	6 6	© 9 © 9	00	8	96% 100%	-

Figure 2-1-1 RaUI section introduction

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

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 2-1-2 Button section

	Link Information	×
Status	AP1 <> 00-0E-2E-E1-98-2D	
Extra Info	Link is Up [Tx Power:100%]	
Authentication	WPA2-PSK	
Encryption	AES	
Network Type	Infrastructure	
Central Channel	5	

Figure 2-1-3 Link Information page

+ - 🕑 😰 🖹	Profile List	>
Profile Information		
FIUNE IN UNIDUUT		
Profile Name	Authentication	((2))

Figure 2-1-4 Profile page

issue63	3	1	6	9 0	69	70%	^
_catch_me_if_you	3	1	6	9 🛈	4	76%	
SoftAP-51	0	1		Ō		76%	
gg	-00000000000000000000000000000000000000	1	6	9 🛈	8	60%	
Claude0	3	1	000000000000000000000000000000000000000	9	8	55%	
iverson	3	1	6	9 🛈		24%	
pega2	3	2	6	g	47	39%	
dlink	3	3	6	9 🛈		100%	
001601D314B4_G	3	5	6	g	8	44%	
_SMS-192	3	6	6	9 🛈		50%	
Baron_Test	0	6	6	9 🛈		99%	
160	3	6	6	9 🛈		55%	
f-roaming2	3	6	6		8	50%	
RT305x_AP_BFu	3	6	6 (90		96%	
Stitch	3	6	6	9 🛈	8	100%	Y
AP Information	~			• •	1	100 /0	-

Figure 2-1-5 Network page

Wireless Mode —Select Your Co	2,4GHz + 5	100 TO 100			
2.4GHz	0: CH1-11				
5GHz	3: CH 52	, 56, 60,	64, 149, 15	3, 157, 161	

Figure 2-1-6 Advance page

Ralink	(c) Copyri	ght 2010, Ralink All rights reserv	
MAC Address	00-1C-1	10-01-FE-1B	
Firmware	0.22	EEPROM	1.1
SDK	1.0.4.0	Date	2010-03-04
Driver	1.4.9.0	Date	2009-11-26
Version Utility	4.0.0.0	Date	2010-03-07

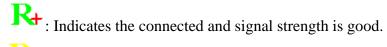
Figure 2-1-7 About page

When starting RaUI, a small Ralink icon appears in the notifications area of the taskbar, as shown in Figure 2-1-15. 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 RaUI utility.



Figure 2-1-8 Ralink icon in system tray

Additionally, the small icon will change color to reflect current wireless network connection status. The status is shown as follows:



+ : Indicates the connected and signal strength is normal.

R: Indicates that it is not yet connected.

: Indicates that a wireless NIC can not be detected.

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

2.2 Profile

2.2.1 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. Figure 2-2-1 shows the basic profile section.

+ - 🛛 😭 🖹	Profile List	~
Profile Information		
Profile Information Profile Name	Authentication	((2))

Figure 2-2-1 Profile function

Definition of each field:

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

• 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.

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

 $\boldsymbol{b}_{:}$ Indicates the network type is infrastructure mode.

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

 \square : Indicates if the network is security-enabled.

+ : Click to add a new profile.

Elick to edit an existing profile.

: Deletes an existing profile.

E: Import an existing profile.

Export an existing profile.

2: Activates the selected profile.

2.2.2 Add/Edit Profile

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

You can open it by clicking the "Add to Profile" button in the Site Survey tab. You can open it by clicking the "Add" button in the Profile tab.

You can open it by clicking the "Edit" button on the Profile tab.

+ +	Profile
Profile Name	PROF1
SSID	
Network Type	Infrastructure - Connect to AP
	🦳 Ad Hoc - Connect to other computer

Figure 2-2-1 Add a new Profile

Icons and buttons:

- To the next page.
- Sack to the previous page.
- Cancel button.

Profile Name	PROF1
Tronic Name	p. Nor 4
SSID	
Network Type	Infrastructure - Connect to AP
	C Ad Hoc - Connect to other computer

Figure 2-2-2 Profile Name, SSID, Network Configuration

- Profile Name: The user can chose any name for this profile, or use the default name defined by system.
- SSID: The user can key in the intended SSID name or select one of the available APs from the drop-down list.
- Power Save Mode: Choose CAM (Constantly Awake Mode) or Power Saving Mode.
- Network Type: There are two types, infrastructure and 802.11 Ad-hoc modes. 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.

Authenticatio	on Open	•
Encryptic	on None	•
	June	

Figure 2-2-3 Authentication and Encryption Configuration

- 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, 802.1X, WAPI-PSK, and WAPI-CA.
- 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.

Default Tx Key	Key 1	
Key Format	Hex(10 or 26 hex digits)	-
WEP Key		

Figure 2-2-4 WEP Key Configuration

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

. + +	Profile	;
WPA Preshared Key		

Figure 2-2-5 Pre-shared Key Configuration

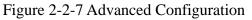
• Pre-shared Key: This is the key shared between the AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.

+ +	Profile	
EAP Method	PEAP	Session Resumption
unnel Authentication	EAP-MSCHAP v2 💌	
Tunnel ID	Authentication ID	
Tunnel Password		
Domain Name		

Figure 2-2-6 802.1x Configuration

• 802.1x Setting: This is introduced in the topic of "Section 3-2 : 802.1x Setting"

Tx Power	Automatic	-
Power Save Mode	CAM	
	C PSM	
Diagnostic Capabi	lity	
Use RTS Threshol	d /	o
Use Fragment Thr	eshold	256



- Power Save Mode: Choose CAM (Constantly Awake Mode) or Power Saving Mode.
- Channel: Only available for setting under Ad-hoc mode. Users can choose the channel frequency to start their Ad-Hoc network.
- RTS Threshold: User can adjust the RTS threshold number by sliding the bar, or key in the value directly. The default value is 2347.
- Fragment Threshold: User can adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346.

2.2.3 Example to Add Profile in Profile

• Click "Add" below the Profile List.

+ - 🛛 🕅 🕅	Profile List	Ŷ
Profile Information Profile Name	Authentication	((0))
SSID	Encryption	

• The "Add Profile" will appear.

Profile Name	PROF1
SSID	
Network Type	Infrastructure - Connect to AP
	C Ad Hoc - Connect to other computer

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

* *		
Profile Name	PROF1	
SSID		•
Network Type	_catch_me_if_you_can _wen 001601D314B4_G 1234567 Accusys_LEO Accusys_LEO Accusys_Lobby	
	AP1 Bayes Task	
	Baron_Test cert	~

• Now the profile which the user set appears in the profile list. Click "Activate".

+ - 🔀 🛛	1 🖻 🕖	Profile List		>
PROF1	AP1		8	\$
Profile Informati	00			
Profile Name		Authentication		((9))
SSID		Encryption		4

• Now the profile which the user active will connect to AP.

🔗 PROF1	AP1	8 B
Profile Inform	ation	Authentication WPA2-P5K

2.2.4 Pre-logon Connect

The Pre-logon Connect configuration page as shown in Figure 2-2-4.

Profile	×
Use Pre-logon Connection	
You need to restart the computer when using/non-using Pre-logon connection. (recommend)	

Figure 2-2-4 Pre-logon Connect Page

Field definitions:

• Pre-logon Connect: Use ID and Password in Profile.

** Recommend: You need to restart the computer when using/non-using Pre-logon connection.

2.3 Network

2.3.1 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 2-3-1-1.

cert	B	149 <mark>a</mark>		8	55%	~
wayne_5g	0	161 <mark>a</mark>	(D	39%	
🖉 AP1	3	7	69(0 ()	100%	
001601D314B4_G	<i>ტტტტტტტტტტტტტტტ</i>	5	69	8	50%	
1STAP	3	5 6	69(0 ()	65%	
160	3	6	69(D	34%	
Baron_Test	3	6		D	76%	
WXX	3	6	69(D 💡	34%	
Stitch	6	6	69(D 💡	99%	
ExRegNW3135DB	0	6	69(D ()	76%	
RT305x_AP_BFu	Ø	6	69(D	94%	
f-roaming2	0	6	10 10 9	8	55%	
cert	Ø	6	69		34%	
baldwin	Ø	6	9 (D 💡	50%	
Cheetah	6	6	6 9 (D	44%	~
AP Information						

Figure 2-3-1-1 Network function

Definition of each field:

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

Icons and buttons:

✓: Indicates that the connection is successful.

 $\boldsymbol{\mathcal{V}}$: Indicates the network type is in infrastructure mode.

- Indicates the network type is in Ad-hoc mode.
- \square : Indicates that the wireless network is security-enabled.
- a : Indicates 802.11a wireless mode.
- **b**: Indicates 802.11b wireless mode.
- **9**: Indicates 802.11g wireless mode.
- •: Indicates 802.11n wireless mode.

```
    Sorted by SSID
    Sorted by Channel
```

Sorted by Channel

Sorted by Signal Strength : Indicate that the AP list is sorted by SSID, Channel or

Signal.

: Button to connect to the selected network.

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

E: 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.

Connected network:

- When RaUI 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:

• General information contains the AP's SSID, MAC address, authentication type, encryption type, channel, network type, beacon interval, signal strength and supported rates. It is shown in Figure 2-3-1-2.

	cert	3	149 <mark>a</mark>		2	55%	1
	wayne_5g	0	161 <mark>a</mark>	l (i)	39%	
1	AP1	0	7		1 47	100%	
	001601D314B4_G	0	5	69	8	50%	
	1STAP	0	6	696	1 ()	65%	
	160	<i>ზხზხზხზხზხზხ</i> ტ	6)	34%	
	Baron_Test	0	6	696)	76%	
	WXX	0	6	696	1 8	34%	
	Stitch	0	6	696	1 8	99%	
	ExRegNW3135DB	v	6	696	1 ()	76%	
	RT305x_AP_BFu	3	6	690)	94%	
	f-roaming2	0	6	6	8	55%	
	cert	3	6	69	a	34%	
	baldwin	3	6	90	1 7	50%	
	Cheetah	B	6	696		44%	1

Figure 2-3-1-2 General information about the Access Point

2.3.2 Example on Adding Profile in Network

• Select the AP from the list on the Network tab

cert	v	149 <mark>a</mark>	<u> </u>	55%	^
wayne 5g	Ø	161 <mark>a</mark>	0	39%	
AP1	V	7 (5 9 0 47	100%	
001601D314B4	ςØ	5 (99 💡	50%	
1STAP	3	6 (5 9 🛈 💔	65%	
160	3	6 (990 990 990 990 990 990 47	34%	
Baron_Test	\$	6 (390	76%	
WXX	V	6 (390 🕈	34%	
Stitch	6	6 (390?	99%	
ExRegNW31350	ж 🖒	6 (5 9 🛈 💔	76%	
RT305x_AP_BF	u v	6 (390	94%	
f-roaming2	3	6 (9	55%	
cert	<u>,</u> вороророророро	6 (3 9 🧯	34%	
baldwin	0	6	9 🛈 💡	50%	
Cheetah	Ø	6 (390	44%	×
AP Information					

• Click "Add to Profile"

Sti Add to Profile	3	6	690	9 0	94%	1
f-roaming2	B	6		8	70%	
RT305x_AP_BFu	<i>სსსსსსსსსსსს</i>	6	090 090 090		34%	
WXX	3	6	690		44%	
SoftAP-br	3	6	690		39%	
Baron_Test	3	6	6 9 (55%	
160	3	6	690)	29%	
baldwin	3	6	9 (44%	
1STAP	3	6	b 9 (b 9 (1 ()	70%	
Cheetah	3	6	- 🕒 🤧 🕻)	44%	
ExRegNW3135DB	3	6	- 🕒 🧐 🕻	1 47	94%	
AP1	Ø	7) ()	100%	
kkkkkkkkkkkkkkkkk	0	11	- 🕒 🤨 🕻)	76%	
test_ssid	000	11	690		50%	
RedStone	B	11	69	8	0%	~

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

Profile Name	PROF1
SSID	AP1
Network Type	• Infrastructure - Connect to AP
	C Ad Hoc - Connect to other computer

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

	Site Survey	×
SSID AP1 Rate 13.5 Mbps IP Address 192.168.2.101 Channel 7 (2442 MHz) Mask 255.255.255.0	Stitch Ø 6 Ø 9 94% Froaming2 Ø Ø 70% 70% RT305x_AP_BFu Ø Ø Ø 34% wxx Ø Ø Ø ¶ 44% SoftAP-br Ø Ø ¶ 39% 39% Baron_Test Ø Ø ¶ 55% 55%	
Profile List ×	160 😢 6 15 9 10 29% baldwin ½ 6 9 10 7 44% 1STAP ½ 6 15 9 10 47 70% Cheetah ½ 6 15 9 10 44 %	
Profile Information Profile Name PROF1 Authentication WPA2-P5K	ExRegNW3135DB 6 6 9 9 0 47 94% AP1 7 8 9 0 47 100% kkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkkk	•

2.4 Advanced

2.4.1 Advanced

Figure 2-4 shows the Advance functions of RaUI.

Wireless Mode -Soloct Your Co	2,4GHz + 5GHz 💌
2.4GHz	0: CH1-11
5GHz	3: CH 52, 56, 60, 64, 149, 153, 157, 161

Figure 2-4 Advance function

- Wireless mode: Select wireless mode. 2.4G, 5G and 2.4+5G are supported.(2.4G/5GHz options are depend on different products)
- Wireless Protection: Users can choose from Auto, on, and off. (This is not supported by 802.11n adapters.)

Auto: STA will dynamically change as AP announcement.

On: The frames are always sent with protection.

Off: The frames are always sent without protection.

- 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.)
- Enable TX Burst: Ralink's proprietary frame burst mode.
- Enable TCP Window Size: Optimize the TCP window size to allow for greater throughput.
- Fast Roaming at-: enables fast roaming, which is set by the transmit power.
- Select Your Country Region Code: There are eight countries to choose from in the country channel list. (11A ListBox only shows for 5G adapters.)
- 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.
- Apply the above changes.

2.4.2 Certificate Management

The Certificate Management configuration page as shown in Figure 2-4-2.

Install Certificate		
User certificate		Browse
Issuer certificate		Browse
	Install	
		UpMove
		DownMove
		Install AS
		Delete
Certificate Detail		

Figure 2-4-2 Certificate Management function

2.5 Link Information

2.5.1 Link Status

The link status page displays detailed information about the current connection as shown in Figure 2-5-1.

• ≁ 🗈	Link Information	
Status	AP1 <> 00-0E-2E-E1-98-2D	
Extra Info	Link is Up [Tx Power:100%]	
Authentication	WPA2-PSK	
Encryption	AES	
Network Type	Infrastructure	
Central Channel	5	

Figure 2-5-1 Link Status function

- Status: Current connection status. If no connection, if will show Disconnected. Otherwise, the SSID and BSSID will show here.
- Extra Info: Display link status in use.
- Channel: Display current channel in use.
- Authentication: Authentication mode in use.
- Encryption: Encryption type in use.
- Network Type: Network type in use.
- IP Address: IP address about current connection.

2.5.2 Throughput

The throughput page displays detailed information about the current connection as shown in Figure 2-5-2.

tint. A shirt	1 M 1		100.9/
Link Quality			100 %
Signal Strength :	1		-41 dBm
Signal Strength :	2		-76 dBm
Transmit		Deseive	
Transmit		Receive	
Transmit Link Speed	13.5 Mbps	Receive Link Speed	39.0 Mbps

Figure 2-5-2 Throughput function

- Link Speed: Show current transmit rate and receive rate.
- Throughout: Display transmits and receive throughput in unit of Mbps.
- Link Quality: Display connection quality based on signal strength and TX/RX packet error rate.
- Signal Strength 1: Receive signal strength 1, user can choose to display as percentage or dBm format.
- Signal Strength 2: Receive signal strength 2, user can choose to display as percentage or dBm format.
- Signal Strength 3: Receive signal strength 3, user can choose to display as percentage or dBm format.

2.5.3 Statistics

The Statistics page displays detailed counter information based on 802.11 MIB counters. This page translates that MIB counters into a format easier for the user to understand. Figure 2-5-1 shows the detailed page layout.

Transmit C Receive		Reset Counter
Transmitted Successfully	=	2613
Retransmitted Successfully	=	260
Fail To Receive ACK After All Retries	=	735

Figure 2-5-1 Statistics function

Transmit Statistics:



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

Receive Statistics:

Link Inform	nation	
🔿 Transmit 🛛 🙃 Receive		Reset Counter
Received Successfully	=	1152
Received With CRC Error	=	375989
Dropped Due To Out-of-Resource	=	0
Duplicate Frames Received	=	0

- Frames Received Successfully: The number of frames successfully received.
- Frames Received With CRC Error: The number of frames received with a CRC error.
- Frames Dropped Due to Out-of-Resource: The number of frames dropped due to a resource issue.
- Duplicate Frames Received: The number of duplicate frames received.
- Reset all the counters to zero.

2.6 About

2.6.1 About

Click "About" displays the wireless card and driver version information as shown in Figure 2-10.

	n.	out	
Version Utility	4.0.0.0	Date	2010-03-07
Driver	1.4.9.0	Date	2009-11-26
SDK	1.0.4.0	Date	2010-03-04
Firmware	0.22	EEPROM	1.1
MAC Address	00-1C-:	10-01-FE-1B	
Ralink	(c) Copyri	ght 2010, Ralink All rights reserv	

Figure 2-10 About function

Connect to Ralink's website: <u>Ralink Technology, Corp</u>.

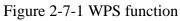
Display Configuration Utility, Driver, and EEPROM version information. Display Wireless NIC MAC address.

2.7 WPS

2.7.1 WPS

Figure 2-7-1 illustrates the RaUI WPS functions.

+ - 📝 😭 🛛	Profile List	×
	Add WPS Profile	
Profile Information		_
Profile Information Profile Name	Authentication	((2))



- 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.
- WPS AP List: Displays the SSID of the surrounding APs with WPS IE from the last scan result.
- PBC: Start to add to AP using PBC configuration method.
- 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.
- Auto: Starts to add to AP by using to select the AP automatically in PIN method.

WPS AP List		Auto
WPS Method	Push-Button Configuration(PBC)	
	🧭 PIN / numeric code	

Figure 2-7-1-1 WPS Profile

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

	Profile	
Pin Code	3813317	Renew
Config Mode	Registrar	WPS Profile

Figure 2-7-1-2 WPS PIN function

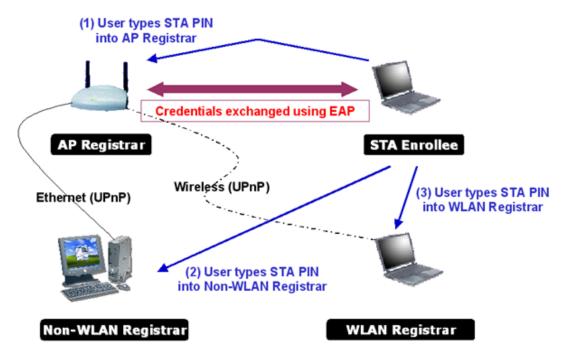
After the user clicks PIN or PBC, please do not rescan within two-minutes of the connection. If you want to abort this setup within the interval, restart PIN/PBC or click "Disconnect" to stop WPS action.

- Progress Bar: Displays the rate of progress from Start to Connected.
- Status Bar: Displays the current WPS Status.

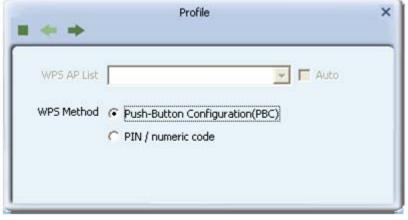
There are examples in <u>section 2-7-3</u>(PIN Enrollee Setup), <u>section 2-7-4</u>(PBC Enrollee Setup) and <u>section 2-7-5</u>(Registrar Configures and AP)

2.7.2 Example to Add 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.



• Select an AP (SSID/BSSID) that STA will join to and Select the "PIN/numeric code" method.



- Select "Enrollee" from the Config Mode drop-down list.
- Enter the PIN Code of the STA into the Registrar when prompted by the Registrar.

Pin Code 3813317 Renew
onfig Mode Enrollee 💽 WPS Profile

If you use <u>Microsoft Window Connection Now</u> as an External Registrar, you must start PIN connection at STA first. After that, search out your WPS Device name and MAC address at Microsoft Registrar. Add a new device and enter PIN Code of STA at Microsoft Registrar when prompted.

• Click "PIN" to enter the PIN

		0%	
WPS status is r	not used		
200			
	Start PIN		

• The result should appear as the image below.

0.00			
		15 %	
PIN - Begin as	ssociating to WPS AP		

• Configure one or more credentials

_		40 %	
PIN - Send	ling M1		

• Then connect successfully. The result appears as the following image.

Profile	×
100 %	
PIN - Get WPS profile successfully.	
Finish	

• Click "Finish"



Describe "WPS Status Bar" - "PIN - xxx" as follow:

• 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

- WPS configuration doesn't complete after a two-minute connection: WPS EAP process failed.
- When errors occur within **two minutes of connecting**, the WPS status bar might report "WPS EAP process failed".

Error messages might be:

- 1. Receive EAP with wrong NONCE.
- 2. Receive EAP without integrity.
- 3. Error PIN Code.
- 4. An inappropriate EAP-FAIL received.

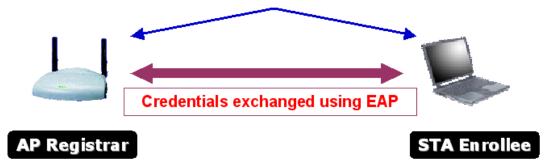
2.7.3 Example to Add to Registrar Using PBC Method

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 PBC mode or APs using PBC mode have left their Walk Time.

Push PBC button on both Registrar and Enrollee



• Select an AP (SSID/BSSID) that STA will join to and Select the "Push-button Configuration" method.

WPS AP List		luto
WPS Method	Push-Button Configuration(PBC)	
	🦵 PIN / numeric code	

- Click PBC to start the PBC connection.
- Push the PBC on AP.

-		0%	
WPS status is i	not used		
	Start PBC		

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

		10 %	
PBC - Scar	nning AP		
	Finish		

• When one AP is found, join it.

_	_	70.0/	
	ME	70 %	
PBC - Sending	M5		

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

Profile	>
	100 %
PS profile successfully.	
ĺ	
Finish	
	PS profile successfully.

• Then connect successfully. The result will be displayed as it is in the figure below.

2	Ralink)(i) ? ×
"†" ∂ ,111	 SSID Rate Channel 	AP1 54.0 Mbps 7 (2442 MHz)		192,168,2,101 255,255,255,0
	OF1 4	Profile L Profile L AP1	ist	۲ ف ۲
	Information Name PROF AP1		hentication WPA ryption TKIP	2-P5K

Describe "WPS Status Bar" - "PBC - xxx" as follow:

• 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

• No PBC AP available:

Scanning AP ~> No PBC AP available ~> Scanning AP ~> No PBC AP available ~>...

• Too Many PBC AP available:

Scanning AP ~> Too Many PBC AP available ~> Scanning AP ~> Too Many PBC AP available ~>...

- WPS configuration doesn't complete after **two-minute connection**: WPS EAP process failed.
- When Errors occur within two-minutes of establishing a connection, the WPS status bar might report "WPS EAP process failed".

Error messages might be:

- 1. Receive EAP with wrong NONCE.
- 2. Receive EAP without integrity.
- 3. An inappropriate EAP-FAIL received.

Describe "Multiple PBC session overlaps" as follow:

- Dual 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.

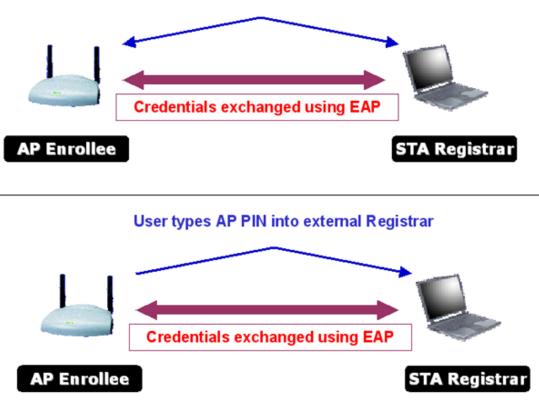
• Different UUID-E :

AP1 is a G-Band AP using PBC mode. (ID = 0x0004)

AP2 is a G-Band AP using PBC mode. (ID = 0x0004)

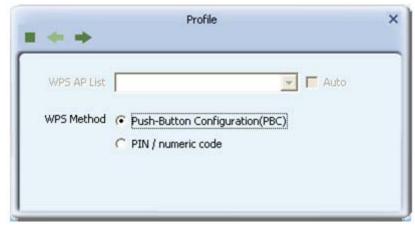
They have the different UUID-E.

STA would regard these two APs as two different APs and wait until only one PBC AP is available.



Push PBC button on both Registrar and Enrollee

Select an AP (SSID/BSSID) that STA will config and Select the "PIN/numeric code" method.



- Select "Registrar" from the Config Mode drop-down list.
- Enter the PIN Code of the STA into the Registrar when prompted by the Registrar.

Pin Code	31289207	Renew
Config Mode	Registrar	WPS Profile
ntig Mode	Registrar	WPS Profile

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

	10	
SSID	ExRegNW01FE1B	
BSSID	00-0E-2E-E1-98-2D	
Authentication	WPA2-PSK	•
Encryption	AES	-

- Start PIN or PBC. The following procedures are as similar as <u>section 2-7-3</u> (PIN Enrollee Setup) or <u>section 2-7-4</u>(PBC Enrollee Setup),
- 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.

Describe "WPS Status Bar" - "PIN - xxx" as follow:

A successful PIN Configuration:

Start PIN connection - SSID ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive M1 ~> Sending M2 ~> Receive M3 ~> Sending M4 ~> Receive M5 ~> Sending M6 ~> Receive M7 ~> Sending M8 ~> Receive EAP Rsp (Done) ~> Sending EAP Rsp (ACK) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

Describe "WPS Status Bar" - "PBC - xxx" as follow:

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 M1 ~> Sending M2 ~> Receive M3 ~> Sending M4 ~> Receive M5 ~>
Sending M6 ~> Receive M7 ~> Sending M8 ~> Receive EAP Rsp (Done) ~>
Sending EAP Rsp (ACK) ~> Configured ~> WPS status is disconnected ~> WPS
status is connected successfully-SSID
```

3. Security

Authentication	Open	•
Encryption	None	-

3.1 Auth.\ Encry. Setting – WEP/TKIP/AES

Figure 3-1 Auth.\Encry. Settings in the Profile Page

- Authentication Type: There are 7 authentication modes supported by RaUI. They are Open, Shared, WPA and WPA-PSK, WPA2 and WPA2-PSK, 802.1x, WAPI-PSK and WAPI-CA.
- Encryption Type: For open and shared authentication mode, the available encryption types are none and WEP. For Shared and 802.1x authentication mode, the selection of available encryption is WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, both TKIP and AES encryption is available. For WAPI-PSK and WAPI-CA authentication mode, only SMS4 encryption is available.

Authentication	802.1X	•
Encryption	WEP	

Figure 3-1-2 Authentication \ Encryption Settings in the Profile Page
8021X: This is introduced in the topic of <u>Section 3-2</u>.

Ĩ

Figure 3-1-3 Pre-shared Key Configuration

• 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.

Default Tx Key	Key 1	-
Key Format	Hex(10 or 26 hex digits)	<u>-</u>
WEP Key	-	

Figure 3-1-4 WEP Key Configuration

- 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.

3.2 802.1x Setting

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

EAP Method	PEAP	• •	Session Resumption
unnel Authentication	EAP-MSCHAP v2		
Tunnel ID	Authentication II		
Tunnel Password		_	
Domain Name			

Authentication type:

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.(Only support XP)

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

Tunnel Authentication:

- 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".
- Tunnel Identity: Identity for tunnel.

• Tunnel Password: Password for tunnel.

ID \ PASSWORD

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

Client Certification



Use Client certificate: Client certificate for server authentication. **EAP Fast**

Allow unauthenticated provision mode	
Provisioning Tunnel EAP-M5CHAP v2	•
Use protected authentication credential	
	Import
	Remove

- 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

Use Server	Contification	
Use berver		
Allow int	ermidiate certificates	
Server Name		

- Certificate issuer: Select the server that issues the certificate.
- 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.
- Server name: Enter an authentication sever root.

3.3 Example to Configure Connection with WEP on

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

6	100% 39%		091	7	1	
80.	39%	3 (4				AP1
6		U 💔 🗆	69(7	0	Ralink-Meeting-2591
	55%	8	69	11	0	ClaudeAP
6	29%	D	9 (11	3	WAPI_Cert
6	60%	D	69(11	3	kkkkkkkkkkkkkkkkk
6	70%	8	69	11	0	VWIFI-S1
6	44%	D	69(11	3	test_ssid
6	60%	D ()	69(11	0	0000
6	42%	D 🕈 🗌	0	64 <mark>a</mark>	0	Sam_AP
6	29%	<u> </u>		149 <mark>a</mark>	0	cert
6	44%	D 💡 🗌	0	161 <mark>a</mark>	0	wayne_5g
6	24%	D	0	161 <mark>a</mark>	0	lalala
6	15%		b 9 b 9(1	4	PPP
	70%	<u>ה</u>	(B) (C) (C)	1	4	SoftAP-FE
	60° 42° 29° 44° 24°	D () D 7 D 7	9 9 0 0 0	11 64 <mark>a</mark> 149 <mark>a</mark> 161 <mark>a</mark> 161 <mark>a</mark>	♦	uuuuu Sam_AP cert wayne_5g lalala

• The Auth.\Encry. function will appear as below;

Ralink	■ □ ⊘ ③ 1 ? ×	Site Survey	×
SSID Rate Channel	1234567 36.0 Mbps IP Address 192.168.1.108 1 (2412 MHz) Mask 255.255.255.0	dlink 10 3 10 9 10 81% _SMS-192 10 6 10 9 10 39% Cheetah 10 6 10 9 10 44% ExRegNW3135DB 10 6 10 9 10 44% Baron_Test 10 6 10 9 10 46% RT305x_AP_BFu 10 6 10 9 10 76%	
= + +	Profile X	Stitch Ø Ø Ø Ø Ø 91% wxx Ø 6 D 9 N 39% 1STAP Ø 6 D G D N 44% 000 4 6 D G 81%	-
Authentication Encryption	Open	baldwin Ø Ø Ø Ø 39% AP1 Ø 7 Ø Ø 100% Ralink-Meeting-2591 Ø 7 Ø Ø 10% ClaudeAP Ø 11 Ø Ø 55% WAPI_Cert Ø 11 Ø 0 29%	>
		AP Information SSID AP1 Authentication Open MAC Address 00-0E-2E-E1-98-2D Encryption WEP	2

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

Ralink	()() ? ×	2	9	5ite Surv	ey				>
				dlink	ø	3	69	0		81%	1
🎽 🕻 SSID 1	234567			_SMS-192	0	6	69	Ô		39%	
Rate 3	6.0 Mbps	TD Address	192.168.1.108	Cheetah	0	6	6 9	Ō		44%	
	oro muhz	P IP Address	192,166,1,100	ExRegNW3135DB	3	6	6 9	0	47	81%	
Channel 1	(2412 MHz)	🐉 Mask	255.255.0.0	Baron_Test	3	6	6 9	0		86%	
				RT305x_AP_BFu	0	6	6 9	0		76%	
	D file		×	Stitch	3	6	🛛 🔁 🧕	0	8	91%	
	Profile		~	WXX	0	6	6 9	0	8	39%	
				1STAP	3	6	6 9	0	49	44%	
				000	4	6	6 9			81%	
Default Tx Key	Key 1		-	baldwin	3	6	9	0	8	39%	
	1			AP1	\$	7	- 🕒 🨉	0	67	100%	
Key Format	Hex(10 or 2)	6 bex diaits)	•	Ralink-Meeting-2591	3	7	6 9	0	47	39%	
	1			ClaudeAP	\$	11	6 9		8	55%	
WEP Key	***	4		WAPI_Cert	\$	11	9	0		29%	
WLF KCY	1	1	_	AP Information						_	
		<mark>⊢</mark> Sho	w Password	SSID AP1 MAC Address 00-0E-2E-8	1.08.1		nentication	n Op WE		((2))

• Click "OK". The dialog box will appear as below;

Ralink		i) ? x	, 🔳	Site Surve	/	×
(1) (1) (1) (1) (1) (1) (1) (1)	AP1 11.0 Mbps ▶ IP Address 192 7 (2442 MHz) ▶ Mask 255	2.168.2.101 5.255.255.0	dlink _SMS-192 Cheetah ExRegNW3135DB Baron_Test RT305x_AP_BFu	3 6 6 6 6 6		81% ^ 39% 44% 81% 86% 76%
<u>∧</u> ∧	Link Information	×	Stitch wxx 1STAP	6 6 6 6		91% 39% 44%
Status Extra Info Authentication Encryption	AP1 <> 00-0E-2E-E1-98-2D Link is Up [Tx Power:100%] Open WEP	×	000 baldwin AP1 Ralink-Meeting-2591 ClaudeAP	4 6 10 10 11 4 5 11 5 11		81% 39% 100% 39% 55%
Network Type	Infrastructure	S	WAPI_Cert P Information SID AP1 IAC Address 00-0E-2E-		9 D Intication Open ption WEP	29%

3.4 Example to Configure Connection with WPA-PSK

- Site Survey × 2 000 ^ Cheetah 0 55% 6 Ď g 0 RT305x_AP_BFu 6 86% 9 0 ExRegNW3135DB 6 99% 49 90 Ō 6 WXX 44% 6 g RT61AP_Z 29% baldwin 6 29% n AP1 b 1 100% もも 9 🛈 💔 1STAP 6 39% DD 90 NAP2-WEP-197 8 8 20% g 0 55% test_ssid 11 6 g VWIFI-S1 11 76% **VWIFI-S1** 11 D g 0 39% 6 g 11 ClaudeAP 65% Ь FTC-02 11 C 34% RT2860AP1 11 g Ь 0 24% * **AP Information** SSID AP1 Authentication WPA-PSK... TKIP+AES MAC Address 00-0E-2E-E1-98-2D Encryption
- Select the AP with a WPA-PSK authentication mode and click "Connect".

• Auth.\Encry. function appears.

Ralink		Site Survey	×
**** > SSID	RT2860AP1	001601D31484_G 🔥 5 D 9 7 50% Stitch 6 D 9 D 7 86%	
👩 🖡 Rate	1.0 Mbps PIP Address 192.168.0.195	Baron_Test 🤌 6 D 9 10 86% Cheetah 🔣 6 D 9 10 55%	
Channel	11 (2462 MHz) 🌗 Mask 255.255.255.0	RT305x_AP_BFu 🔌 6 5 9 🝈 86%	
		📙 ExRegNW3135DB 🤌 6 🕒 99%	
	Profile X) wxx 🤌 6 📴 💆 🛈 🍸 44%	
= + +		RT61AP_Z & 6 5 9 7 29% baldwin & 6 9 1 7 29%	=
ſ	11 A	AP1 🤌 7 ট 9 🛈 († 100%)	
Authentication	WPA2-PSK	1STAP 🤌 6 📴 ਉ 🕦 📢 39%	
		NAP2-WEP-197 🤌 8 🧕 👰 🌹 20%	
Encryption	AES	test_ssid 🔌 11 📴 9 🕦 55%	
		VWIFI-51 🕑 11 📴 9 76%	1000
		VWIFI-51 🎸 11 📴 🥊 🗊 🌹 39%	×
1			in
1		MAC Address 00-0E-2E-E1-98-2D Encryption TKIP+AES	99)
1		MAC AUGRESS 00-0E-2E-E1-90-2D EIICRYPUOIT TRIP+AES	-

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

	Site Survey 🗙
Image: SSID RT2860AP1 Image: Rate 1.0 Mbps IP Address 192.168.0.195 Image: Channel 11 (2462 MHz) Mask 255.255.0.0	001601D31484_G 5
Profile X	wxx 2 6 15 9 10 7 44% RT61AP_Z 2 6 15 9 7 29% baldwin 2 6 9 10 7 29%
WPA Preshared Key ******	AP1
	WWIFI-51 11 9 1 39% AP Information SSID AP1 Authentication WPA-PSK MAC Address 00-0E-2E-E1-98-2D Encryption TKIP+AES

• Click "OK". Be careful, if the WPA Pre-Shared Key entered is not correct, you won't be able to exchange any data frames, even though the AP can be connected.

Ralink	00	(i) ? ×	2 🗉	Site Surv	эу	>
SSID Solution Solutio		s 192.168.2.101 255.255.255.0	001601D314B4_G Stitch Baron_Test Cheetah RT305x_AP_BFu ExRegNW3135DB	56666 6666		50% 86% 86% 55% 86% 99%
a 🔸 🗈	Link Information	×	wxx RT61AP_Z baldwin ✔ AP1	じゅ じゅ じゅ ち		44% 29% 29% 100%
Status Extra Info Authentication Encryption Network Type	AP1 <> 00-0E-2E-E1-98-2D Link is Up [T× Power:100%] WPA2-P5K AE5 Infrastructure		AP1 1STAP NAP2-WEP-197 test_ssid VWIFI-S1 VWIFI-S1	ビック ビック ビック ビック ビック 11 ビック 11		100% 39% 20% 55% 76% 39%
Central Channel	5		AP Information SSID AP1 MAC Address 00-0E-2E		entication WPA-P9 yption TKIP+A	

3.5 Example to Configure Connection with WPA

- Site Survey × 2 RT61AP_Z 69 8 29% ~ 6 Ď 90 8 baldwin 6 29% Ċ 0 AP1 7 q 100% 9 0 1STAP 6 49 39% 0 NAP2-WEP-197 8 2 20% g 0 🤣 test_ssid 11 55% りりりりりり g **VWIFI-S1** 11 76% ğ 0 **VWIFI-S1** 11 39% g ClaudeAP 11 65% g FTC-02 34% 11 g 0 RT2860AP1 11 24% g นนนนน 11 29% Ô 64 a 42% Sam_AP 149 <mark>a</mark> cert 10% lalala 161 **a** ۵ 15% AP Information Authentication WPA SSID AP1 MAC Address 00-0E-2E-E1-98-2D Encryption TKIP+AES
- Select an AP with WPA authentication mode and click "Connect".

• The Auth.\Encry. function pop up. (If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.)

Ralink		Site Survey	×
SSID Rate Channel	test_ssid 6.5 Mbps IP Address 192.168.1.18 11 (2462 MHz) Mask 255.255.255.0	RT61AP_Z baldwin baldwin constraints constraints constraints constraints AP1 <	
= + +	Profile X	WWIFI-S1 Image: Work of the state of the st	
Authentication Encryption	WPA	FTC-02 Image: Constraint of the second sec	
		AP Information SSID AP1 Authentication WPA MAC Address 00-0E-2E-E1-98-2D Encryption TKIP+AES	•)

• Click "8021X" and the setting page will appear.

Ralink	1)(i) ? ×	B	Ξ							
2))					T61AP_Z	Ø	6	0		8	29%	1
SSID	test_ssid				aldwin	6	6		n n	Y	29%	_
🕥 🚯 Rate	6.5 Mbps	IP Address	192.168.1.18		P1	Ø	7	6	D	7	100%	
Channel	11 (2462 MHz)	Mask	255.255.255.0		STAP	V.	6	b R	φ,	47	39%	
	11 (2462 MHZ)	# MidSK	200,200,200,0	1	AP2-WEP-197	v.	8	0	Q	2	20%	
				/ 🎸 t	est_ssid	0	11	- D 9	D		55%	
	Profile		×) V	WIFI-S1	V.	11	- D 🤤		7	76%	
					WIFI-S1	LA LA	11	- D 🤅		0	39%	
-				V	W1F1-51	Ý	11	- W G	Ψ	¥	J970	
* *					laudeAP	ě	11	6	ĵΨ.	\$	65%	
* 		-		0		999			j	8		
EAP Method		💌 🔽 Session	Resumption	C F	laudeAP	9999	11		0	8	65%	
	PEAP		Resumption	C F F	laudeAP TC-02	ବବବବ	11 11		Ū.	÷ •	65% 34%	
	PEAP		Resumption	C F F L	laudeAP TC-02 T2860AP1	000000	11 11 11 11		Ū.	47 17	65% 34% 24%	
unnel Authentication	PEAP		Resumption	T T T T T T T T T T T T T T T T T T T	laudeAP TC-02 T2860AP1 uuuu	000000000	11 11 11 11 64		0	* * * *	65% 34% 24% 29%	1
unnel Authentication Tunnel ID	PEAP EAP-MSCHAP v2 Authentication II		Resumption	F F U U S	laudeAP TC-02 T2860AP1 uuuu am_AP	ବନ୍ଦ୍ୱର୍ବ୍ଦ୍ୱର	11 11 11 64 149		0	\$° ₽ ₽	65% 34% 24% 29% 42%	
unnel Authentication	PEAP EAP-MSCHAP v2 Authentication II		Resumption	C F F U S C k	laudeAP TC-02 T2860AP1 uuuu am_AP ert	000000000	11 11 11 64 149		000	₹ ₹ \$ \$	65% 34% 24% 29% 42% 10%	

• Authentication type and setting method:

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 as "wpatest2" and the tunnel password as "test2". These settings are the same as our intended AP's setting.

EAP Method	PEAP	Session Resumption
unnel Authentication	EAP-MSCHAP v2]
Tunnel ID	Authentication IC	wpatest2
Tunnel Password	****	
Domain Name		-

2. Click to next page.

*If you want to disconnect, please click cancel button in Authentication Status function. *In Profile function, show "Profile Name" option only in adding AP to Profile function. 3. If the connection is successful, the dialog will appear as below.

Ralink		? × 🔁			Site Su	rvey				3
Ì [™] → SSID → Rate ↓ Channel	AP1 1.0 Mbps IP Address 192.168.: 7 (2442 MHz) Mask 255.255.:		RT61AP_Z baldwin AP1 1STAP NAP2-WEP-197 test ssid	0000000	6 6 7 6 8 11	0000	00000	9 9 67 9	29% 29% 100% 39% 20% 55%	
*	Link Information	×	VWIFI-S1 VWIFI-S1 ClaudeAP	666	11 11 11		0	Ŷ	76% 39% 65%	
Status Extra Info Authentication	AP1 <> 00-0E-2E-E1-98-2D Link is Up [Tx Power:100%] WPA		FTC-02 RT2860AP1 uuuuu Sam_AP	0000	11 11 11 64	b b b a	000	6	34% 24% 29% 42%	
Encryption Network Type Central Channel	TKIP+AES Infrastructure 5		cert lalala P Information 5ID AP1	66	161	a a Ithenticatio	On WP		10% 15%	(q))

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.

++	Profile	
EAP Method	TLS / Smart Card 💌	Session Resumption
unnel Authentication	¥	
Tunnel ID	Authentication IC 💌	wpatest2
Tunnel Password		
Domain Name		

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



3. Click to the next page.

*If you want to disconnect, please click "Cancel" on the Authentication Status function page.*In Profile function, show "Profile Name" option only in adding AP to Profile function.4. If it connected successfully, the result will appear as in the image below.

Ralink	()(i) ? ×	R3	=	1	Site Surv	<i>.</i> ,			
Image: SSID Image: SSID <t< th=""><th>AP1 1.0 Mbps 7 (2442 MHz)</th><th>▶ IP Address > Mask</th><th>192.168.1.18 255.255.255.0</th><th>~</th><th>RT61AP_Z baldwin AP1 1STAP NAP2-WEP-197 test_ssid</th><th>000000</th><th>6 6 7 6 8 11</th><th>0000</th><th></th><th>29% 29% 100% 39% 20% 55%</th><th></th></t<>	AP1 1.0 Mbps 7 (2442 MHz)	▶ IP Address > Mask	192.168.1.18 255.255.255.0	~	RT61AP_Z baldwin AP1 1STAP NAP2-WEP-197 test_ssid	000000	6 6 7 6 8 11	0000		29% 29% 100% 39% 20% 55%	
	Link Inform	ation	×		VWIFI-S1 VWIFI-S1 ClaudeAP	NO CO	11 11 11	6 9 6 9 6 9	0	76% 39% 65%	
Status Extra Info Authentication Encryption	AP1 <> 00-0E-2E Link is Up [Tx Pow WPA TKIP+AES				FTC-02 RT2860AP1 uuuuuu Sam_AP cert	000000	149			34% 24% 29% 42% 10%	
Network Type Central Channel	Infrastructure 5			SS	lalala Information ID AP1 AC Address 00-0E-2	2E-E1-98-		henticatio	n WPA TKIP+4	15% ES	

TTLS:

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.

* *	Profile	
EAP Method	TTLS 💌	Session Resumption
Tunnel Authentication	СНАР	1
Tunnel ID	Authentication ID 💌	wpatest2
Tunnel Password	****	
Domain Name		- -

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

*If you want to disconnect, please click "Cancel" on the Authentication Status function page.*In Profile function, show "Profile Name" option only in adding AP to Profile function.3. If the connection is successful, the dialog box will appear as the image below.

Ralink	• • • • • • • • • • • • • • • • • • •	Site Survey	×
(1) SSID Rate Channel	AP1 1.0 Mbps IP Address 192.168.1.18 7 (2442 MHz) Mask 255.255.0	RT61AP_Z ₺ 6 10 9 29% baldwin 6 9 10 29% ✓ AP1 4 7 10 9 10 7 15TAP 4 6 10 9 10 4 NAP2-WEP-197 4 10 9 10 7 test_ssid 4 11 10 9 10 55%	~
a � ∎	Link Information X		
Status Extra Info Authentication Encryption	AP1 <> 00-0E-2E-E1-98-2D Link is Up [Tx Power:100%] WPA TKIP+AES	FTC-02 11 9 7 34% RT2860AP1 11 5 9 0 24% uuuuu 11 5 9 0 24% sam_AP 11 5 9 0 47	1
Network Type	Infrastructure 5	cert V 149 a 10% lalala V 161 a 10% AP Information SSID AP1 Authentication WPA MAC Address 00-0E-2E-E1-98-2D Encryption TKIP+AES	• •

EAP-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.

Profile		
EAP-FAST	Session Resumption	
EAP-MSCHAP v2 💌		
Authentication ID	wpatest2	

	EAP-FAST	EAP-FAST Session Resumption EAP-MSCHAP v2 Authentication IC wpatest2

- 2. Click to the next page.
- 3. If the connection is successful, the dialog box will appear as the image below.

Ralink	000)() ? ×	2		Site Survey			×
SSID SRate Channel		192.168.1.18 255.255.255.0	RT61AP_Z baldwin AP1 1STAP NAP2-WEP-197 test ssid	0000000	6 D 7 D 6 D 8 D 11 D	9 0 0 9 0 0 9 0 0 9 0 0 9 0 0 9 0 0	29% 29% 100% 39% 20% 55%	~
	Link Information	×	VWIFI-S1 VWIFI-S1 ClaudeAP	ももも	11 D 11 D 11 D		76% 39% 65%	
Status Extra Info	AP1 <> 00-0E-2E-E1-98-2D Link is Up [Tx Power:100%]		FTC-02 RT2860AP1 uuuuu	ももも	11 D	9 0 0 9 0 0	34% 24% 29%	UII J
Authentication Encryption Network Type	WPA TKIP+AES Infrastructure		Sam_AP cert lalala	666	64 <mark>a</mark> 149 <mark>a</mark> 161 <mark>a</mark>	0 7	42% 10% 15%	~
Central Channel	5		AP Information SSID AP1 MAC Address 00-0E-2	E-E1-98-	Authentica 2D Encryption		ES (P

*If you want to disconnect, please click "Cancel" on the Authentication Status function page. *In Profile function, show "Profile Name" option only in adding AP to Profile function.

4. Appendix

4.1 Country Channel List

Country channel list, channel classification and range.

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

IcelandIndiaIndonesiaIreland	1 1 1 1 1 1	CH1~13 CH1~13 CH1~13 CH1~13
Indonesia	1	CH1~13
	1	
Ireland	-	CH1-13
	1	CIII~15
Israel		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

4.2 Acknowledgements

The above settings are used in the test platform by RaLink technology corp. Users can set the function in accordance with their AP.

Acknowledgements:

"This product includes software developed by MDC and its licensors. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)". This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

5. FAQ

5.1 FAQ

If you create an adhoc profile for 2.4G channel, and then switch wireless mode to 5G(as Figure 5-1), device will re-send beacon at the first channel of 5G. Note the original adhoc profile will keep previous settings.

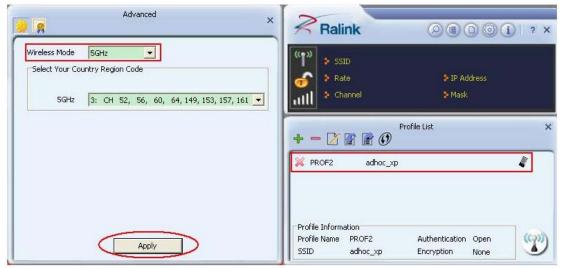


Figure 5-1 Switch wireless mode when activate an adhoc profile

6. Installation

This device shall be fixed in wall or other vertical plane via the metal bracket, and then the device shall be connect to computer or other USB terminal via the length of 4.5 meter USB cable.

Only the following antennas authorized for use with this product to comply with the FCC requirement:

Model:	Length (cm)	Gain (dBi)	Frequency Band	Туре
AO-24015	129	15	2.4-2.5GHz	Omni
AO-24008.1	52	8	2.4-2.5GHz	Omni

This device must be installed to provide a separation distance of at least 20 cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter, to ensure compliance with the FCC RF exposure requirements.

FCC Caution

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE 1: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

NOTE 2: Any changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE 3: This device must be installed to provide a separation distance of at least 20 cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter.