



**DIGISOL<sup>TM</sup>**



# **DG-WN3300N**

802.11b/g/n 300Mbps Wireless LAN USB Adapter

## **User Manual**

**V3.1**

**2017-01-10**

As our products undergo continuous development the specifications are subject to change without prior notice

## **COPYRIGHT**

Copyright 2017 by DIGISOL SYSTEMS LTD. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company.

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents thereof without obligation to notify any person of such revision or changes.

## **Trademarks:**

DIGISOL™ is a trademark of Digisol Systems Limited. All other trademarks are the property of the respective manufacturers.

## **Safety**

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

# Index

<b>1. Product Information .....</b>	<b>5</b>
1-1 Introduction and Safety Information.....	5
1-2 Safety Information .....	5
1-3 System Requirements.....	6
1-4 Package Contents .....	6
1-5 Get familiar with your new wireless USB adapter.....	7
<b>2. Driver Installation and Configuration .....</b>	<b>8</b>
2-1 Network Adapter Installation.....	8
2-2 Configuration Utility.....	12
2-2-1 Utility Overview .....	13
2-3 Connect to Wireless Access Point.....	16
2-3-1 Using Realtek Utility.....	16
2-3-2 Using Windows Zero Configuration .....	23
2-4 Connection Profile Management.....	27
2-4-1 Add a new profile .....	28
2-4-2 Remove an existing profile .....	34
2-4-3 Edit an existing profile .....	34
2-4-4 Make a copy of existing profile.....	36
2-4-5 Set as default profile.....	37
2-5 Network Statistics, General Information and Status.....	38
2-5-1 General Information .....	38
2-5-2 Status .....	40
2-5-3 View Network Statistics .....	41
2-6 Establish secure connection with AP by WPS.....	42
2-6-1 PIN Code .....	44
2-6-2 Push Button .....	46
<b>3. Soft-AP Function .....</b>	<b>47</b>
3-1 Switch to AP Mode and Station Mode.....	47
3-1-1 Configure SSID and Channel .....	49
3-1-2 Setup Soft-AP Security .....	51
3-2 Advanced Settings.....	54
3-3 Wireless Statistics.....	55
3-4 Internet Connection Sharing (ICS) .....	56

---

<b>4 Virtual WI-FI Mode on Windows7/ Windows8 (32-bit) .....</b>	<b>57</b>
4-1 <i>Configure SSID and Soft-AP Security</i> .....	59
<b>5. Appendix .....</b>	<b>61</b>
5-1 <i>Hardware Specification</i> .....	61
5-2 <i>Troubleshooting</i> .....	62
5-3 <i>Glossary</i> .....	64

# 1. Product Information

## *1-1 Introduction and Safety Information*

Thank you for purchasing DG-WN3300N IEEE 802.11b/g/n 300Mbps wireless N USB adapter! This adapter has a tiny size design which enables users to plug it into the USB port of your computer. DG-WN3300N supports wireless standards IEEE802.11b/g, this wireless adapter also supports IEEE802.11n through which users can get data transfer speed up to 300Mbps.

*Other features of this Wireless USB adapter include:*

- IEEE 802.11b/g/n compatible.
- Wireless data transfer rate – upto 300Mbps.
- Supports 64/128-bit WEP, WPS, WPA, WPA2 with IEEE 802.1x functions for high level of security.
- Supports the most popular operating system: Windows XP/Vista/7/8 (32-bit).
- Supports soft AP function.
- Supports USB 2.0 interface.
- Portable and tiny size design.

## *1-2 Safety Information*

In order to keep the safety of users and your properties, please follow the safety instructions as mentioned below:

1. This wireless USB adapter is designed for indoor use only. **DO NOT** expose this wireless adapter to direct sun light, rain, or snow.
2. **DO NOT** put this USB adapter at or near a hot or humid place, like kitchen or bathroom. Also, do not leave this wireless adapter in the car in summer.
3. This USB adapter is small enough to put in a child's mouth, and it could cause serious injury or could be fatal. If they throw the USB adapter, it will be damaged. **PLEASE KEEP THIS USB ADAPTER OUT OF REACH OF CHILDREN.**

4. This USB adapter can get heated up when being used for a long time (This is normal and is not a malfunction). **DO NOT** put the USB adapter on a paper, cloth, or other flammable objects after the USB adapter has been used for a long time.
5. There's no user-serviceable part inside the USB adapter. If you find that the USB adapter is not working properly, please contact your dealer of purchase and ask for help. **DO NOT** disassemble the USB adapter yourself, warranty will be void.
6. If the USB adapter falls into water, **DO NOT USE IT AGAIN BEFORE YOU SEND IT TO THE DEALER OF PURCHASE FOR INSPECTION.**
7. If you smell something strange or even see some smoke coming out from the USB adapter, switch the computer off immediately, and call the dealer of purchase for help.

## *1-3 System Requirements*

- An empty USB 2.0 port
- Windows XP, Vista, Windows7 or Windows 8 (32-bit) operating system
- CD-ROM drive
- At least 100MB of available disk space

## *1-4 Package Contents*

Before you start using this wireless USB adapter, please check the following items in the package.

- DG-WN3300N 300Mbps Wireless USB Adapter (1 No.)
- Quick installation guide
- Installation software CD (includes User Manual & Driver/Utility)

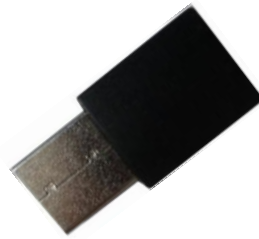
***If any of the above items are missing, contact your supplier as soon as possible.***

## 1-5 Get familiar with your new wireless USB adapter

1. USB interface
2. Status LED (Under the case)



**Top View**



**Bottom View**

LED Name	Light Status	Description
Status	Off	Wireless Radio is switched OFF.
	On	Steady light 5 seconds means WPS connection is established successfully.
	Blinking	i) Wireless network adapter is normally installed. ii) Linked to a wireless access point. iii) Transferring or receiving data. Fast Blinking three times per second means WPS is activated. The USB adapter will wait for 2 minutes to establish WPS connection.

## 2. Driver Installation and Configuration

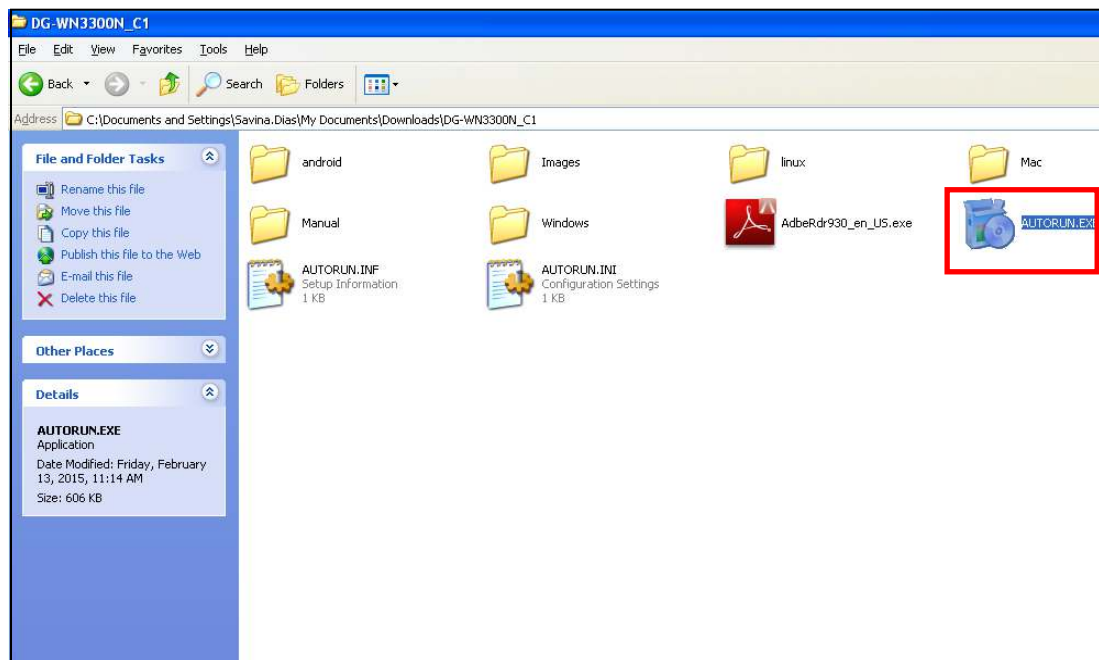
### 2-1 Network Adapter Installation

Please follow the instructions mentioned below to install your new wireless USB adapter:

**Note1:** The following installation was operated under Windows XP. (Procedures are similar for Windows Vista/XP/7/8.)

**Note2:** If you have installed the Wireless PC Adapter driver & utility before, please uninstall the previous version first.

1. Insert “**Installation Software CD**” into the CD/DVD ROM drive of your computer. ‘**AUTORUN.EXE**’ program will run automatically.



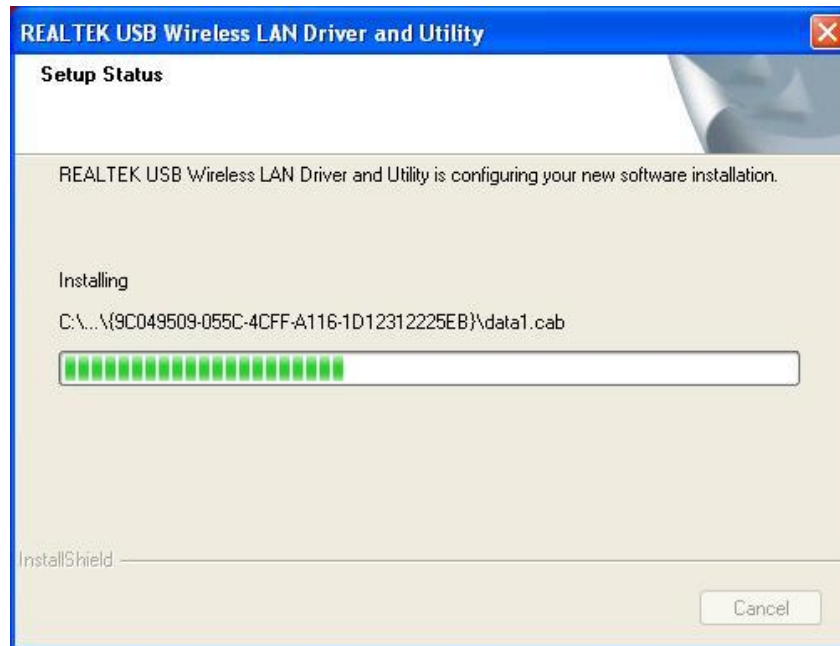




2. Click '**Drivers & Utility**' to begin with the driver and utility installation. The following screen appears. Click on "**Next**".



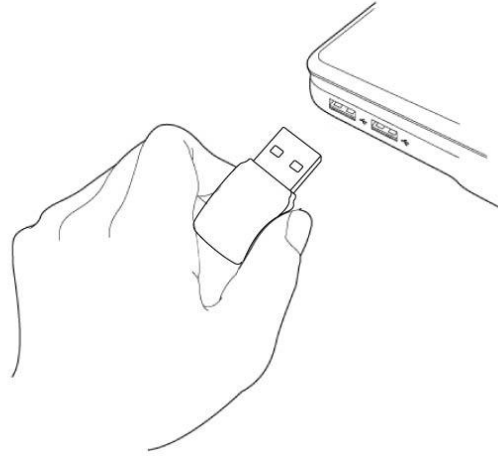
3. The Installation procedure will need few minutes to complete the setup, please be patient.



4. Click '**Finish**' to reboot your computer to complete the installation procedure. If you don't want to reboot the computer now, select '**No, I'll restart my computer later**' option and click '**Finish**'. Please note you have to reboot your computer before you can use your new wireless USB adapter.



5. Once computer has restarted, insert the wireless USB adapter into an empty USB 2.0 port.  
Never use force to insert the adapter, if you feel it's stuck, flip it over and try again.



6. A new icon will appear near the clock of system tray:



**HERE!**

Left-click the icon and it will launch the wireless network configuration utility, and you can right-click the icon to Hide or Quit the configuration utility.

The different color & logo indicates the different wireless connection status:



Wireless USB adapter not detected.



No connection with access point is established.



Connection with access point has been established.

For detailed instructions of wireless network configuration utility, please see next chapter.

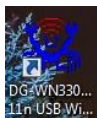
## 2-2 Configuration Utility

The Configuration Utility is a powerful application that helps you configure the Wireless USB Adapter and monitors the link status and the statistics during the communication process.

The Configuration Utility appears as an icon on the system tray and desktop of Windows. You can open it by double-clicking on the icon.

Right click the icon in the system tray, there are some items for you to operate the configuration utility.

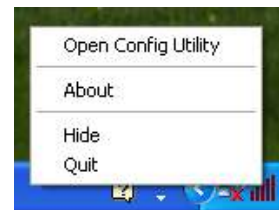
- Open Config Utility  
Select “Open Config Utility” to open the configuration utility.
- About  
Select “About” to show the utility information.
- Hide  
Select “Hide” to hide the utility in the system tray.
- Quit  
Select “Quit” to quit the utility in the system tray.



**On the Desktop**



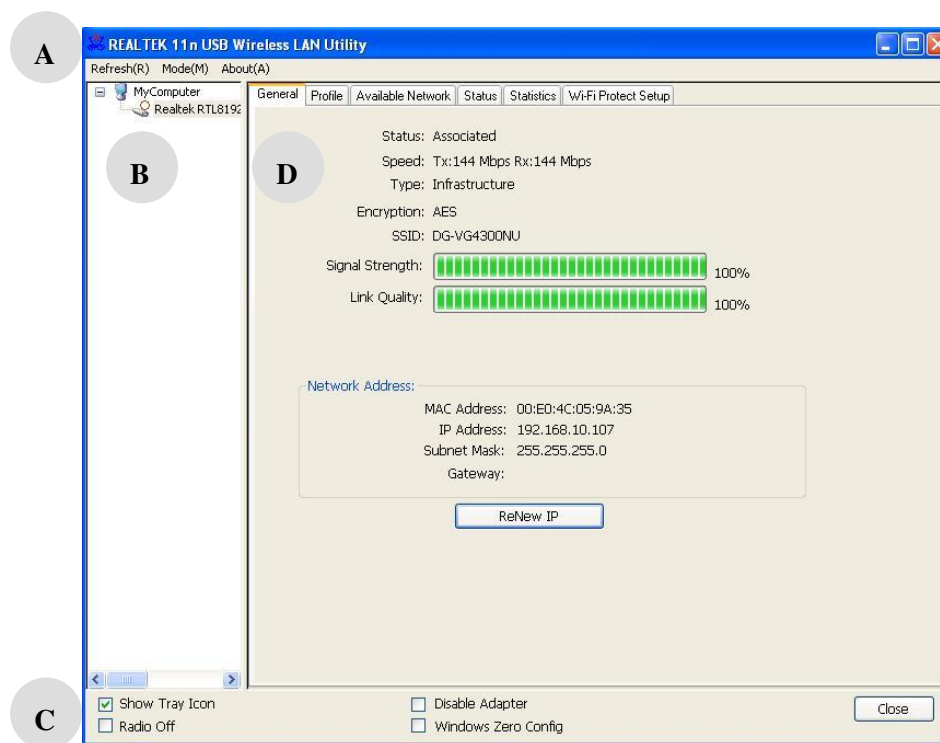
**In the System Tray**



**In the System Tray (Right Click)**

## 2-2-1 Utility Overview

There are several parts in the utility screen. Please refer to the following table for the description. (On Windows XP)

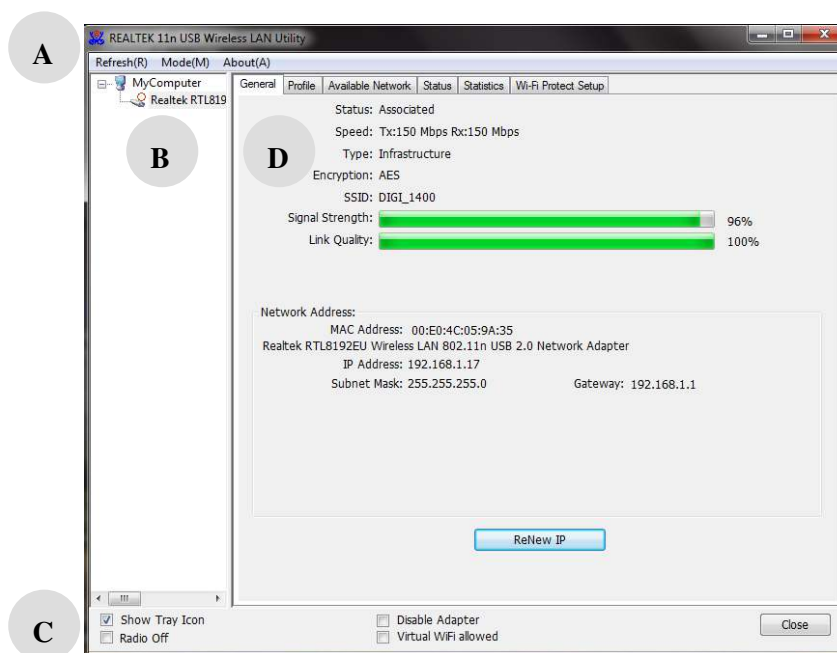


Parameter	Description
<p><b>A</b></p>	<p>Refresh – Refresh adapter list in the “B” block.</p> <p>Mode – There are two modes: Station and Access Point. If Station mode is selected, the adapter works as a wireless adapter. If Access Point mode is selected, the adapter will work as a wireless AP.</p> <p>About – To check the version of the utility, select this item.</p>
<p><b>B</b></p>	<p>This is a list for you to configure several adapters in your PC from the utility.</p>

<p><b>C</b></p>	<p>Show Tray Icon – To show the icon in the system tray, select the item.</p> <p>Disable Adapter – This function is for you to disable or enable the adapter.</p> <p>Radio Off – This function is for you to turn off or turn on the radio of the adapter. If the radio is turned off, the adapter will not work.</p> <p>Windows Zero Config – To configure the adapter from Windows XP Zero Configuration, check the item.</p>
<p><b>D</b></p>	<p>There are several tabs in the block for you to setup the function of the adapter. Please refer to the description in the following sections.</p>

For Windows 7/ Windows 8 (32-bit)

The Utility Interface is slightly different for Windows7/Windows8 (32-bit) as compared to Windows XP. Please refer to the following table for the description.



Parameter	Description
<p><b>A</b></p>	<p>Refresh – Refresh adapter list in the “B” block.</p> <p>Mode – There are two modes: Station &amp; Access Point</p>

	<p>Mode. If Station mode is selected, the adapter works as a wireless adapter. If Access Point mode is selected, the adapter will work as a wireless AP.</p> <p>About – To check the version of the utility, select this item.</p>
<b>B</b>	<p>This is a list for you to configure several adapters in your PC from the utility.</p>
<b>C</b>	<p>Show Tray Icon – To show the icon in the system tray, select the item.</p> <p>Disable Adapter – This function is for you to disable or enable the adapter.</p> <p>Radio Off – This function is for you to turn off or turn on the radio of the adapter. If the radio is turned off, the adapter will not work.</p> <p>Virtual WiFi allowed – Enable this option to configure this Adapter in Virtual Wi-fi Mode. Once you check this option, a new tab “Virtual Wi-fi” will be displayed in the utility as shown in the figure below.</p>
<b>D</b>	<p>There are several tabs in the block for you to setup the function of the adapter. Please refer to the description in the following sections.</p>

## 2-3 Connect to Wireless Access Point

To use wireless network, you have to connect to a wireless access point first. You can either use the Realtek utility (comes with wireless adapter driver), or Windows Zero Config utility (comes with Windows operating system) for configuration purpose.

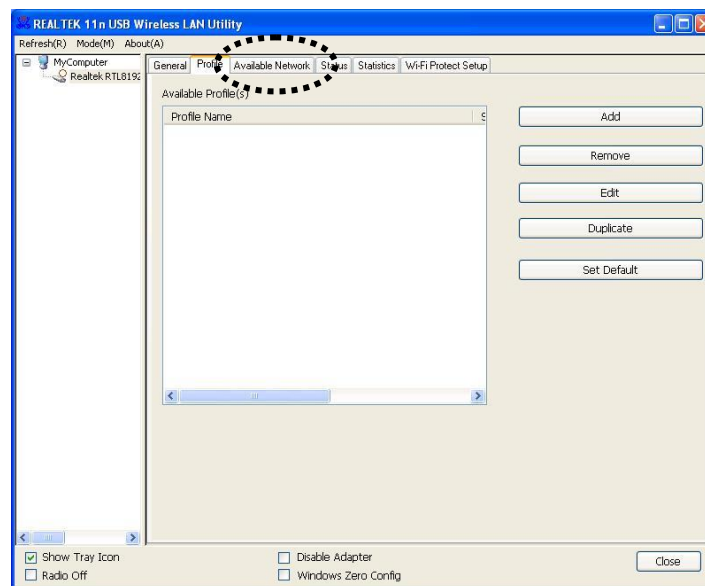
### 2-3-1 Using Realtek Utility

Please follow the instructions mentioned below to use Realtek configuration utility to connect to wireless access point.

1. Left-click the REALTEK configuration utility icon located at lower-right corner of computer desktop, and configuration menu will appear:

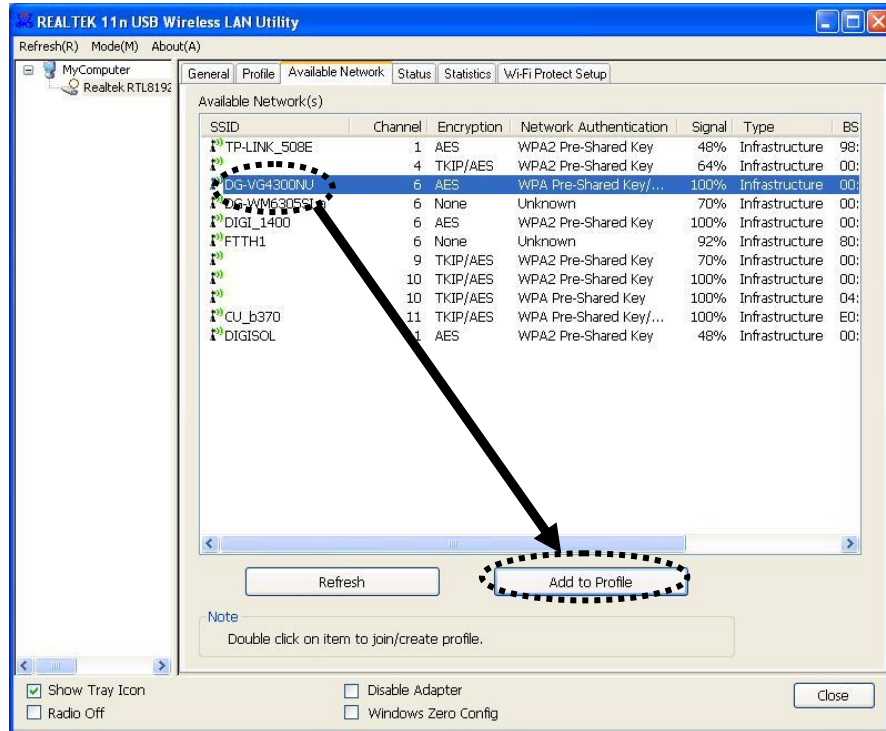


2. Wireless utility will appear. Click '**Available Network**' menu to search for wireless access points nearby.





3. Please wait for a while, and all wireless access points which can be reached by this wireless network adapter will be displayed here.

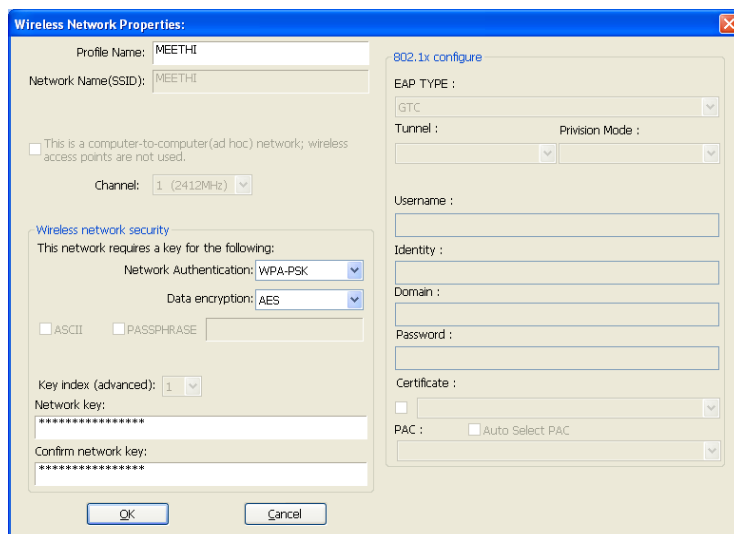


If the wireless access point you wish to connect does not appear here, you can click 'Refresh' button to scan for wireless access points again; if the wireless access point you're looking for still does not appear, try to move the computer closer.

When the access point you're looking for is on the list, left-click it and then double click it or click '**Add to Profile**'.

4. If a password is required to access the wireless access point, please input it in '**Network key**' (and input it again in 'Confirm network key' for confirmation). Click '**OK**' when the password is properly inputted.

**NOTE:** Network security type ('Network Authentication' and 'Data encryption') will be selected automatically based on wireless access point's security setting. It's not required to change these settings yourself.



The image shows a 'Wireless Network Properties' dialog box. It has two main sections: 'Wireless network security' and '802.1x configure'. In the 'Wireless network security' section, 'Profile Name' is 'MEETHI', 'Network Name (SSID)' is 'MEETHI', 'Channel' is '1 (2412MHz)', 'Network Authentication' is 'WPA-PSK', 'Data encryption' is 'AES', and 'Key Index (advanced)' is '1'. In the '802.1x configure' section, 'EAP TYPE' is 'GTC', 'Tunnel' is empty, 'Provision Mode' is empty, 'Username' is empty, 'Identity' is empty, 'Domain' is empty, 'Password' is empty, 'Certificate' is empty, and 'PAC' is 'Auto Select PAC'. There are 'OK' and 'Cancel' buttons at the bottom.

All options in this page will be filled automatically according to the access point you wish to add to profile. However, you can still modify any of them to meet your requirements.

Parameter	Description
Profile name	Define a recognizable profile name for you to identify the different networks. It can be any phrase to help you remember.
Network Name (SSID)	<p>The SSID is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. You may specify a SSID for the adapter and then only the device with the same SSID can interconnect to the adapter.</p> <p>This field will be filled as the access point you selected when SSID is not hidden and grayed out. If SSID is hidden, you have to input correct SSID yourself.</p>
This is a computer-to-computer (ad hoc) network	<p>There are two kinds of network types described as follows.</p> <p><b>Infrastructure</b> – This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point or Router.</p>

	<p><b>Ad Hoc</b> – Connect to another wireless adapter in the Wireless LAN network without an Access Point or Router.</p> <p>Check this box if you wish to connect to another computer / network device by ad hoc method. When not accessing the wireless access point, you have to check this box.</p>
Channel	<p>This setting is only available for Ad Hoc mode. Select the number of the radio channel used for networking. The channel setting should be the same with the network you are connecting to.</p>
Network Authentication	<p>This setting has to be consistent with the wireless networks that the adapter intends to connect.</p> <p><b>Open System</b> – No authentication is needed among the wireless network.</p> <p><b>Shared Key</b> – Only wireless stations using a shared key (WEP Key identified) are allowed to connect to each other.</p> <p><b>WPA-PSK</b> – It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each wireless station in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.</p> <p><b>WPA2-PSK</b> – WPA2-PSK is also for home and small business. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data</p>

	<p>encryption via the AES by default. In contrast, WPA-PSK uses Temporal Key Integrity Protocol (TKIP) by default.</p> <p><b>WPA 802.1X</b> – WPA provides a scheme of mutual authentication using either IEEE 802.1x/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. It provides a high level of assurance to enterprises, small businesses and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.</p> <p><b>WPA2 802.1X</b> – Like WPA, WPA2 supports IEEE 802.1x/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Advanced Encryption Standard (AES). AES is required to the corporate user or government users. The difference between WPA and WPA2 is that WPA2 provides data encryption via the AES by default. In contrast, WPA uses Temporal Key Integrity Protocol (TKIP) by default.</p> <p><b>WEP 802.1X</b> – It's a special mode for using IEEE 802.1x/EAP technology for authentication and WEP keys for data encryption.</p>
Data encryption	<p><b>Disabled</b> – Disable the WEP Data Encryption.</p> <p><b>WEP</b> – Enable the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Encryption keys.</p> <p><b>TKIP</b> – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This insures much greater security than the standard WEP security.</p> <p><b>AES</b> – AES has been developed to ensure the highest</p>

	<p>degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network.</p> <p>Note: All devices in the network should use the same encryption method to ensure the communication. Select the data encryption type from drop-down menu. This setting must be identical with the setting of wireless access point you wish to connect.</p>
ASCII / PASSPHRASE	<p>When the encryption type is 'WEP', it's required to input a set of 'passphrase' to connect to the wireless access point. Check 'ASCII' or 'PASSPHRASE' depends on the security setting of access point, and input it in the box; if you select 'PASSPHRASE' you also need to select the length of the key.</p> <p>The passphrase must be identical with the setting of wireless access point you wish to connect.</p>
Key index	<p>Select WEP key index. For most of the access points you can select '1', but please refer to the setting of the access point.</p>
Network key / Confirm network key	<p>When the encryption type is 'WPA' or 'WPA2-PSK', it's required to input a network key to connect to the wireless access point. Please input the same network key in the 'confirm network key' box.</p>
EAP TYPE Provision Mode	<p>When authentication type is any of 802.1X, you have to select EAP type, tunnel, and provision mode from dropdown menu. This setting must be identical with your 802.1x authentication server.</p> <p><b>GTC</b> – GTC is an authentication protocol which allows the exchange of clear text authentication credentials across the network.</p> <p><b>TLS</b> – TLS is the most secure of the EAP protocols but not easy to use. It requires that digital certificates be exchanged in the authentication phase. The server</p>

	<p>presents a certificate to the client. After validating the server's certificate, the client presents a client certificate to the server for validation.</p> <p><b>LEAP</b> – LEAP is a pre-EAP, Cisco-proprietary protocol, with many of the features of EAP protocols. Cisco controls the ability of other vendors to implement this protocol, so it should be selected for use only when limited vendor choice for client, access-point, and server products is not a concern. When you have set up LEAP authentication, you have to enter the user name and password of your computer.</p> <p><b>PEAP &amp; TTLS</b> – PEAP and TTLS are similar and easier than TLS in that they specify a stand-alone authentication protocol be used within an encrypted tunnel. TTLS supports any protocol within its tunnel, including CHAP, MSCHAP, MSCHAPv2 and PAP. PEAP specifies that an EAP-compliant authentication protocol must be used; this adaptor supports MD5, TLS, GTC (Generic Token Card) and MSCHAPv2. The client certificate is optional required for the authentication.</p>
Tunnel	<p>Includes MD5, GTC, TLS and MSCHAP-v2 when EAP type is selected as 'PEAP'.</p> <p>Includes CHAP, MSCHAP, MSCHAP-V2 and PAP when EAP type is selected as 'TTLS'.</p>
Username	The certificate username in the RADIUS server.
Identity	User's identity in the RADIUS server.
Domain	IP address or domain name of the RADIUS server.
Password	User's password in the RADIUS server.
Certificate	Select the certificate for RADIUS server authentication. If certification is required to authenticate with 802.1x authentication server, please select a local certificate from dropdown list.
PAC	Check this box and PAC (Privilege Access

	Certificate) will be automatically selected.
--	--

Please click 'OK' when ready.

5. Network adapter will attempt to connect to access point now, this may require few seconds to minutes, please be patient. When the '**Status**' becomes '**Associated**', your computer is connected to access point you selected. Click 'Close' to close configuration menu.

*NOTE: If you are connected to an access point but the connection has dropped soon, please check security settings and re-check password spelling.*

### 2-3-2 Using Windows Zero Configuration

Windows XP and Vista has a built-in wireless network configuration utility, called as 'Windows Zero Configuration' (WZC). You can also use WZC to configure your wireless network parameter:

1. Right-click Realtek configuration utility icon, and click '**Open Config Utility**'.



2. Check '**Windows Zero Config**' box.

*Note: This check box will be visible only if the "Wireless Zero Configuration" service is enabled on the machine.*

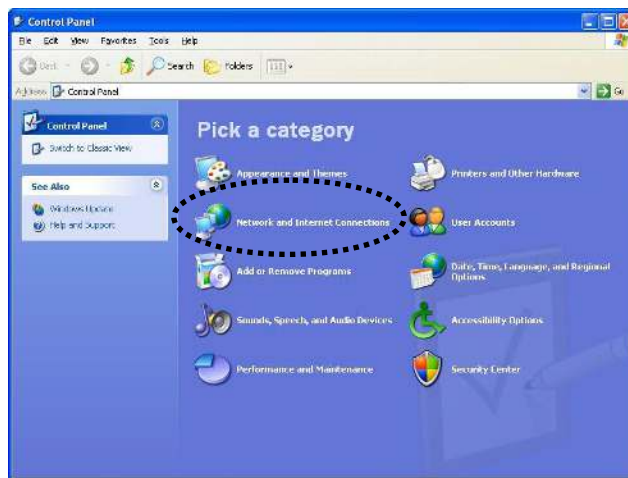
3. A message indicating that you have been switched to Windows Zero Configuration mode will appear. Click '**OK**' to continue.



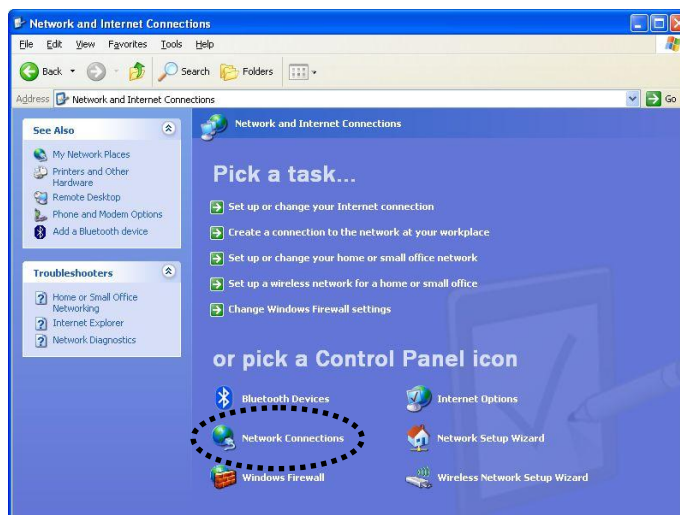


*NOTE: To return to use REALTEK utility, uncheck 'Windows Zero Config' box.*

4. Click '**Start**' button (should be located at the bottom-left corner of windows desktop), click '**Control Panel**', then click '**Network and Internet Connections**' in Control Panel.



5. Double click '**Network Connections**'.

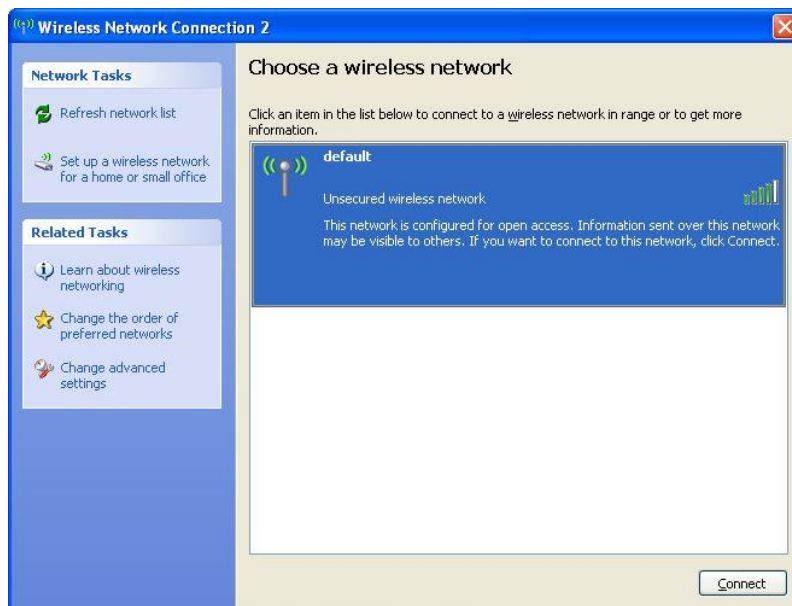




6. Right-click '**Wireless Network Connection**' (it may have a number as suffix if you have more than one wireless network card, please make sure you right-click the 'Realtek RTL8192EU Wireless LAN 802.11n USB 2.0 Network Adapter'), then select '**View Available Wireless Networks**'.



7. All wireless access points in proximity will be displayed here. If the access point you want to use is not displayed here, please try to move your computer closer to the access point, or you can click 'Refresh network list' to rescan access points. Click the access point you want to use if it's shown, then click '**Connect**'.

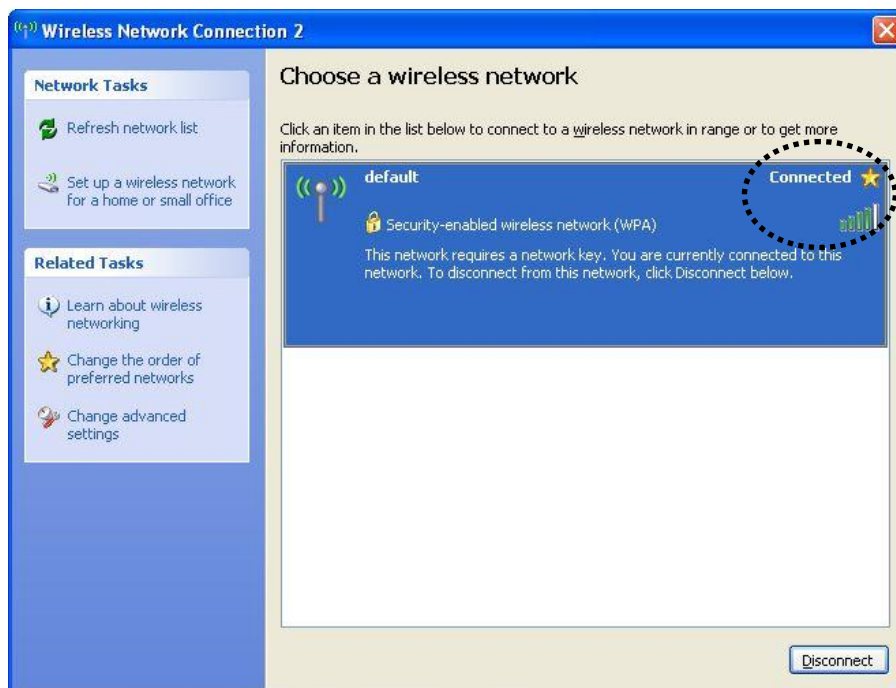


8. If the access point is protected by encryption, you have to input its security key or passphrase here. It must match the encryption setting on the access point.

If the access point you selected does not use encryption, you'll not be prompted for security key or passphrase.



9. If you can see '**Connected**' message, the connection between your computer and wireless access point is successfully established.



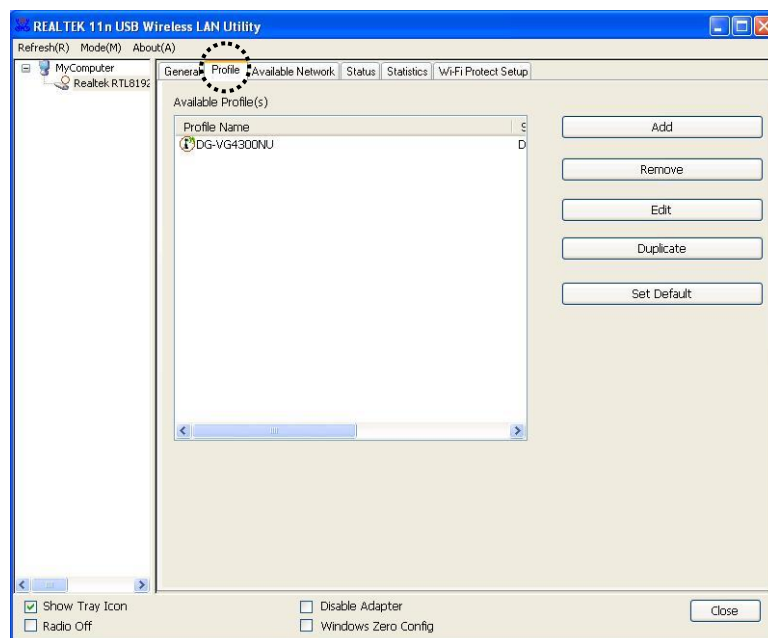
## 2-4 Connection Profile Management

If you need to connect to different wireless access points at different time, for example, access point of your home, office, cybercafe, or public wireless service, you can store the connection parameters (SSID, encryption, passphrase, security etc.) as a profile for every access point, so you don't have to input these parameters every time when you want to connect to a specific wireless access point.

To manage profiles, right-click the DIGISOL configuration utility icon located at lower-right corner of computer desktop, then click '**Open Config Utility**'.



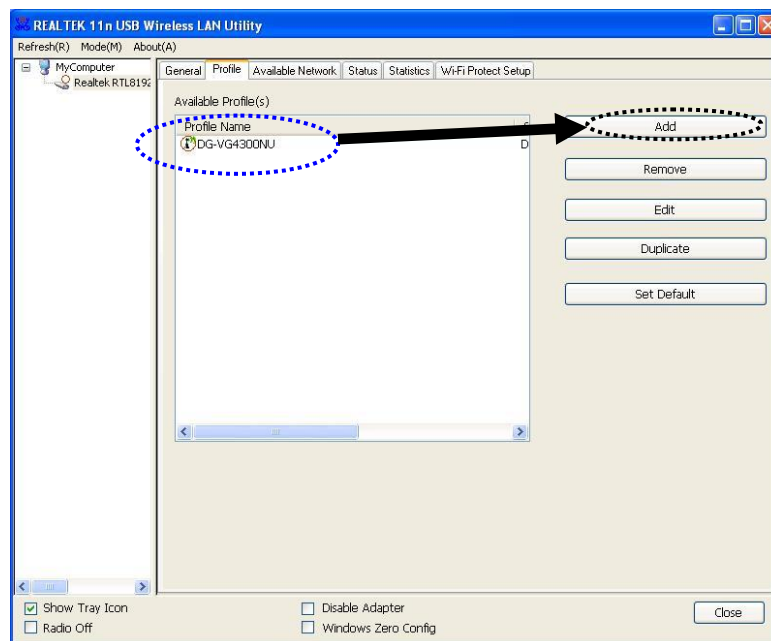
Click the '**Profile**' menu.



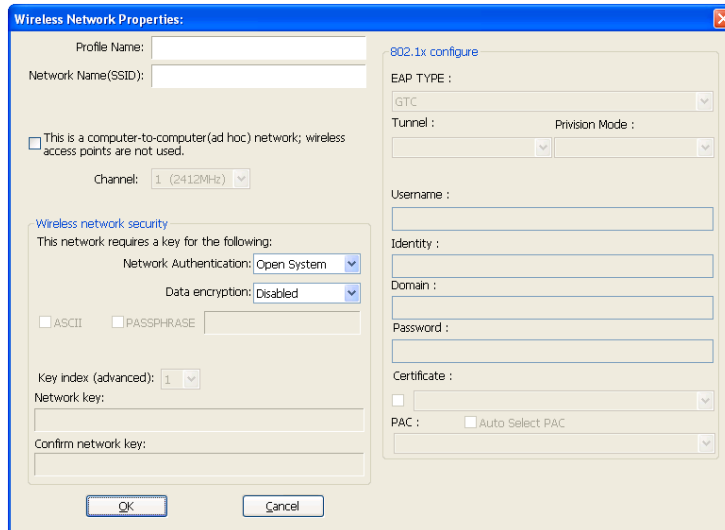
## 2-4-1 Add a new profile

By this function you can setup the connection parameters for a specific wireless access point in advance, when connecting it for the first time.

If you want to create a new profile, click '**Profile**' menu, then click '**Add**' button.



You'll be prompted to input connection parameters for the wireless access point you wish to connect:



The image shows a 'Wireless Network Properties' dialog box. It has two main sections. The left section contains fields for 'Profile Name', 'Network Name (SSID)', a checkbox for 'This is a computer-to-computer (ad hoc) network; wireless access points are not used.', a 'Channel' dropdown set to '1 (2412MHz)', 'Wireless network security' options (Network Authentication: Open System, Data encryption: Disabled), and 'Key' fields. The right section is titled '802.1x configure' and includes 'EAP TYPE' (GTC), 'Tunnel' and 'Provision Mode' dropdowns, 'Username', 'Identity', 'Domain', 'Password', 'Certificate', and 'PAC' fields with an 'Auto Select PAC' checkbox. 'OK' and 'Cancel' buttons are at the bottom.

Required parameters are explained below:

Parameter	Description
Profile name	Define a recognizable profile name for you to identify the different networks. It can be any phrase to help you remember.
Network Name (SSID)	<p>The SSID is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. You may specify a SSID for the adapter and then only the device with the same SSID can interconnect to the adapter.</p> <p>This field will be filled as the access point you selected when SSID is not hidden and grayed out. If SSID is hidden, you have to input correct SSID yourself.</p>
This is a computer-to-computer (ad hoc) network	<p>There are two kinds of network types described as follows.</p> <p><b>Infrastructure</b> – This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point or Router.</p>

	<p><b>Ad Hoc</b> – Connect to another wireless adapter in the Wireless LAN network without an Access Point or Router.</p> <p>Check this box if you wish to connect to another computer / network device by ad hoc method. When not accessing the wireless access point, you have to check this box.</p>
Channel	<p>This setting is only available for Ad Hoc mode. Select the number of the radio channel used for the networking. The channel setting should be the same with the network you are connecting to.</p>
Network Authentication	<p>This setting has to be consistent with the wireless networks that the adapter intends to connect.</p> <p><b>Open System</b> – No authentication is needed among the wireless network.</p> <p><b>Shared Key</b> – Only wireless stations using a shared key (WEP Key identified) are allowed to connect to each other.</p> <p><b>WPA-PSK</b> – It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each wireless station in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.</p> <p><b>WPA2-PSK</b> – WPA2-PSK is also for home and small business. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data encryption via the AES by default. In contrast,</p>

	<p>WPA-PSK uses Temporal Key Integrity Protocol (TKIP) by default.</p> <p><b>WPA 802.1X</b> – WPA provides a scheme of mutual authentication using either IEEE 802.1x/Extensible Authentication Protocol (EAP) or pre-shared key (PSK) technology. It provides a high level of assurance to enterprises, small businesses and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1x authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.</p> <p><b>WPA2 802.1X</b> – Like WPA, WPA2 supports IEEE 802.1x/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Advanced Encryption Standard (AES). AES is required to the corporate user or government users. The difference between WPA and WPA2 is that WPA2 provides data encryption via the AES by default. In contrast, WPA uses Temporal Key Integrity Protocol (TKIP) by default.</p> <p><b>WEP 802.1X</b> – It's a special mode for using IEEE 802.1x/EAP technology for authentication and WEP keys for data encryption.</p>
Data encryption	<p><b>Disabled</b> – Disable the WEP Data Encryption.</p> <p><b>WEP</b> – Enable the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Encryption keys.</p> <p><b>TKIP</b> – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This insures much greater security than the standard WEP security.</p> <p><b>AES</b> – AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution</p>

	<p>defined by IEEE 802.11i for the security in the wireless network.</p> <p>Note: All devices in the network should use the same encryption method to ensure the communication. Select the data encryption type from the drop-down menu. This setting must be identical with the setting of wireless access point you wish to connect.</p>
ASCII / PASSPHRASE	<p>When the encryption type is 'WEP', it's required to input a set of 'passphrase' to connect to wireless access point. Check 'ASCII' or 'PASSPHRASE' depends on the security setting of access point, and input it in the box; if you select 'PASSPHRASE' you also need to select the length of the key.</p> <p>The passphrase must be identical with the setting of wireless access point you wish to connect.</p>
Key index	<p>Select WEP key index. For most of access points you can select '1', but please refer to the setting of the access point.</p>
Network key / Confirm network key	<p>When the encryption type is 'WPA' or 'WPA2-PSK', it's required to input a network key to connect to the wireless access point. Please input the same network key in the 'confirm network key' box.</p>
EAP TYPE Provision Mode	<p>When authentication type is any of 802.1X, you have to select EAP type, tunnel, and provision mode from dropdown menu. This setting must be identical with your 802.1x authentication server.</p> <p><b>GTC</b> – GTC is an authentication protocol which allows the exchange of clear text authentication credentials across the network.</p> <p><b>TLS</b> – TLS is the most secure of the EAP protocols but not easy to use. It requires that digital certificates be exchanged in the authentication phase. The server presents a certificate to the client. After validating the server's certificate, the client presents a client certificate to the server for validation.</p>



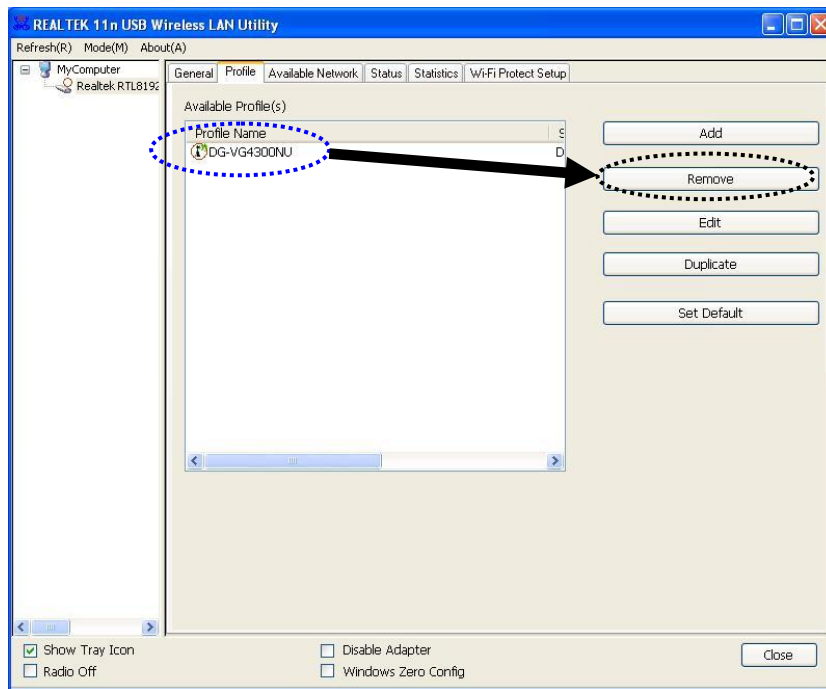
	<p><b>LEAP</b> – LEAP is a pre-EAP, Cisco-proprietary protocol, with many of the features of EAP protocols. Cisco controls the ability of other vendors to implement this protocol, so it should be selected for use only when limited vendor choice for client, access-point, and server products is not a concern. When you have set up LEAP authentication, you have to enter the user name and password of your computer.</p> <p><b>PEAP &amp; TTLS</b> – PEAP and TTLS are similar and easier than TLS in that they specify a stand-alone authentication protocol be used within an encrypted tunnel. TTLS supports any protocol within its tunnel, including CHAP, MSCHAP, MSCHAPv2 and PAP. PEAP specifies that an EAP-compliant authentication protocol must be used; this adaptor supports MD5, TLS, GTC (Generic Token Card) and MSCHAPv2. The client certificate is optional required for the authentication.</p>
Tunnel	<p>Includes MD5, GTC, TLS and MSCHAP-v2 when EAP type is selected as ‘PEAP’.</p> <p>Includes CHAP, MSCHAP, MSCHAP-V2 and PAP when EAP type is selected as ‘TTLS’.</p>
Username	The certificate username in the RADIUS server.
Identity	User’s identity in the RADIUS server.
Domain	IP address or domain name of the RADIUS server.
Password	User’s password in the RADIUS server.
Certificate	Select the certificate for RADIUS server authentication. If certification is required to authenticate with 802.1x authentication server, please select a local certificate from dropdown list.
PAC	Check this box and PAC (Privilege Access Certificate) will be automatically selected.

When all required parameters are set, click ‘OK’ to create and save a new profile.

## 2-4-2 Remove an existing profile

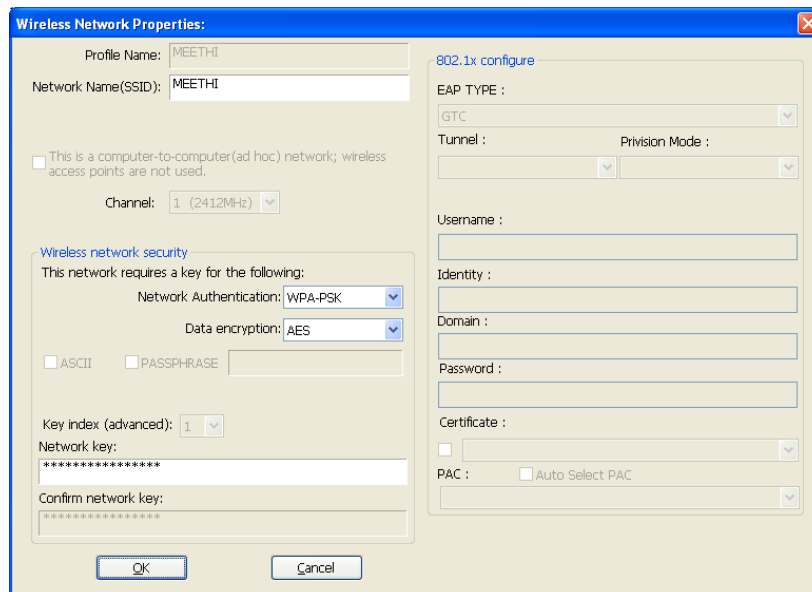
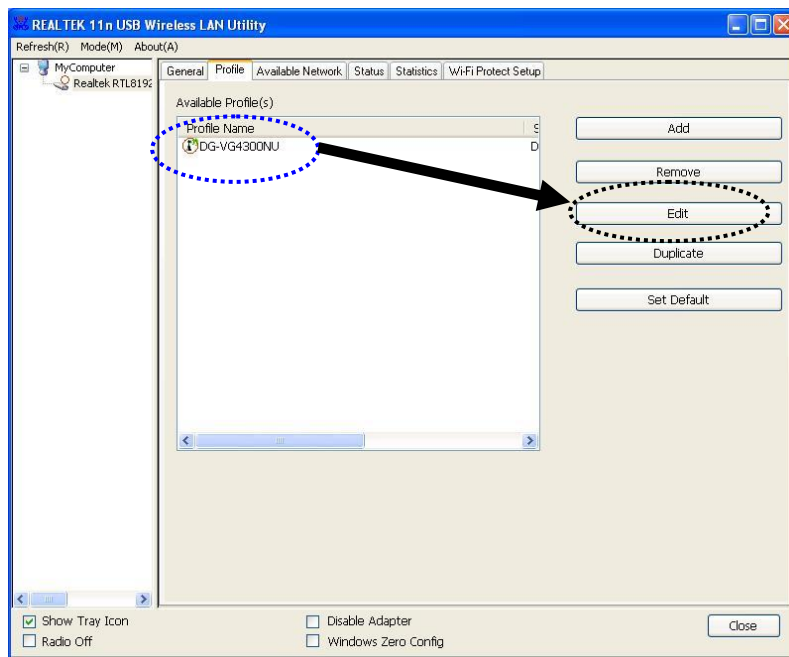
When you no longer need an existing profile, you can remove it.

If you want to remove a profile, click '**Profile**' menu, then select an existing profile which you wish to remove, and then click '**Remove**' button.



## 2-4-3 Edit an existing profile

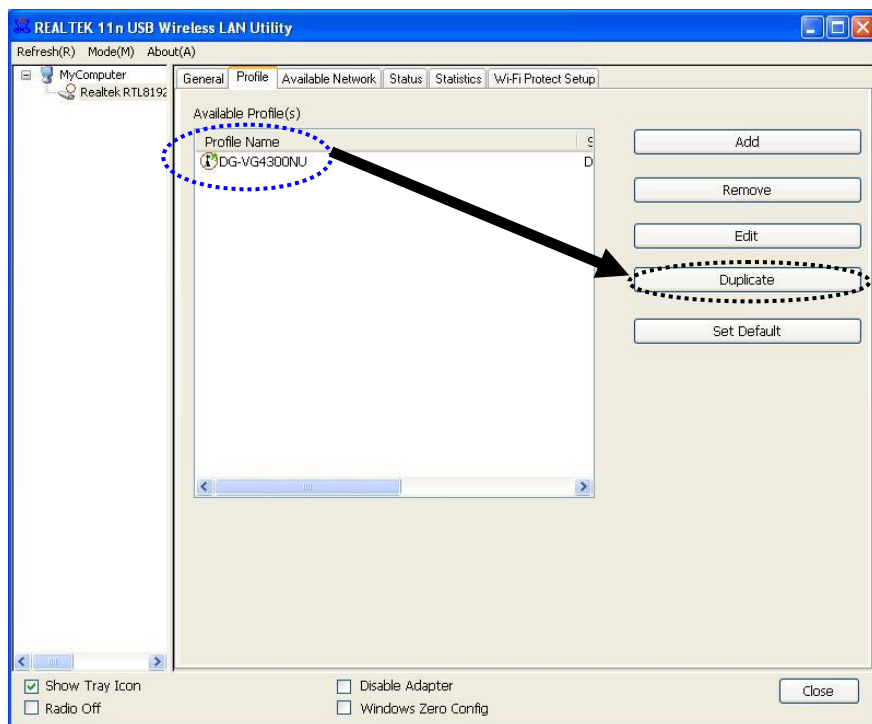
If you have added a profile before, and you wish to change the content of the profile, you can use this function. Please select a profile from the list first, then click '**Edit**' button. You'll be provided with the contents of selected profile, and you can edit them. Click '**OK**' to save changes, or click '**Cancel**' to discard changes.



## 2-4-4 Make a copy of existing profile

If you need to make a copy of a specific profile, you can use this function. This function is very convenient when you need to build a new profile with parameters that are similar to any existing profile.

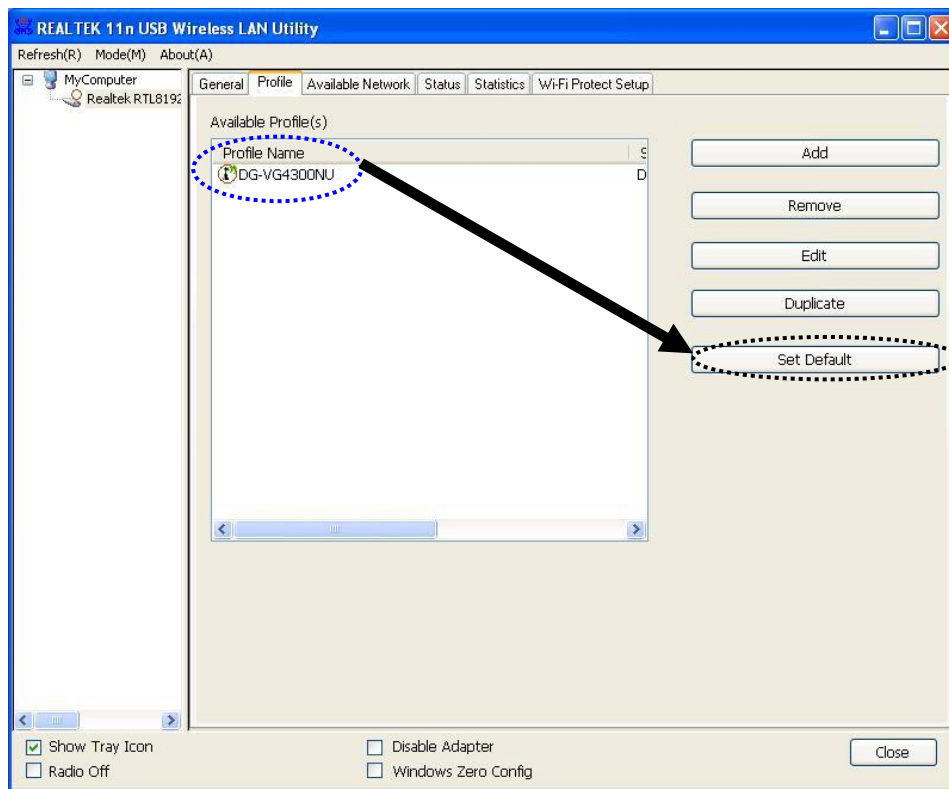
To do this, select an existing profile, then click '**Duplicate**' button.



You'll be prompted to input a profile name, please use an identical name that does not exist in profile list.

## 2-4-5 Set as default profile

If you wish to use a specific profile as default connection, you can select a profile in the list, and click '**Set Default**'. Selected profile will become default selection and DIGISOL configuration utility will attempt to connect to selected access point.

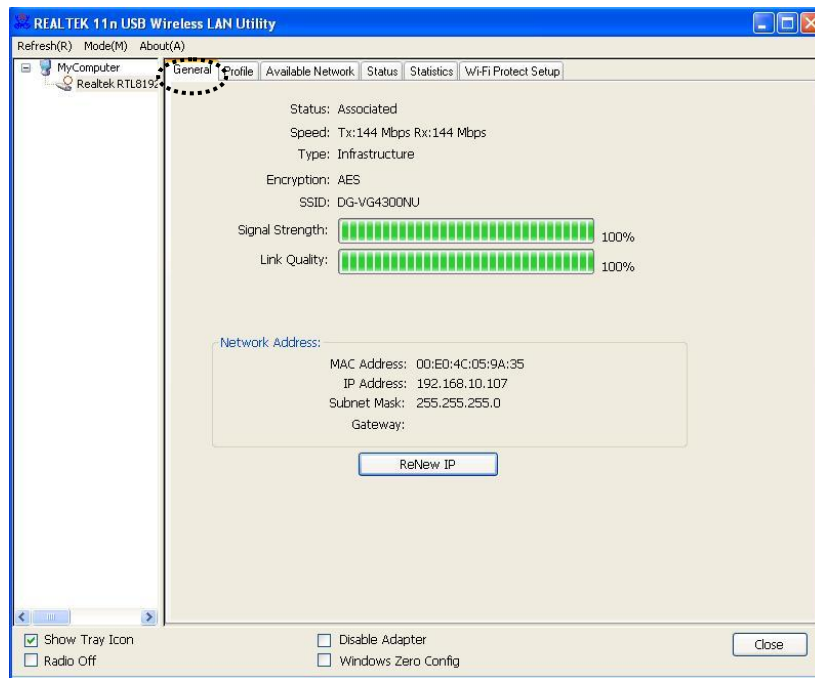


## 2-5 Network Statistics, General Information and Status

The configuration utility provides information about network statistics and link status. If you want to know how your wireless network adapter works, you can use these functions to get detailed information about the wireless connection you're using.

### 2-5-1 General Information

If you want to know the general information of the access point you're connecting to, click '**General**' menu:



All general information like Link Speed, Network Type, Encryption Method, SSID, Signal Strength, Link Quality and Network Address of the adapter will be displayed here. This information is very useful when you encounter some problem in connecting to the access point.

If you wish to get a new IP address from DHCP server, you can click 'ReNew IP' button

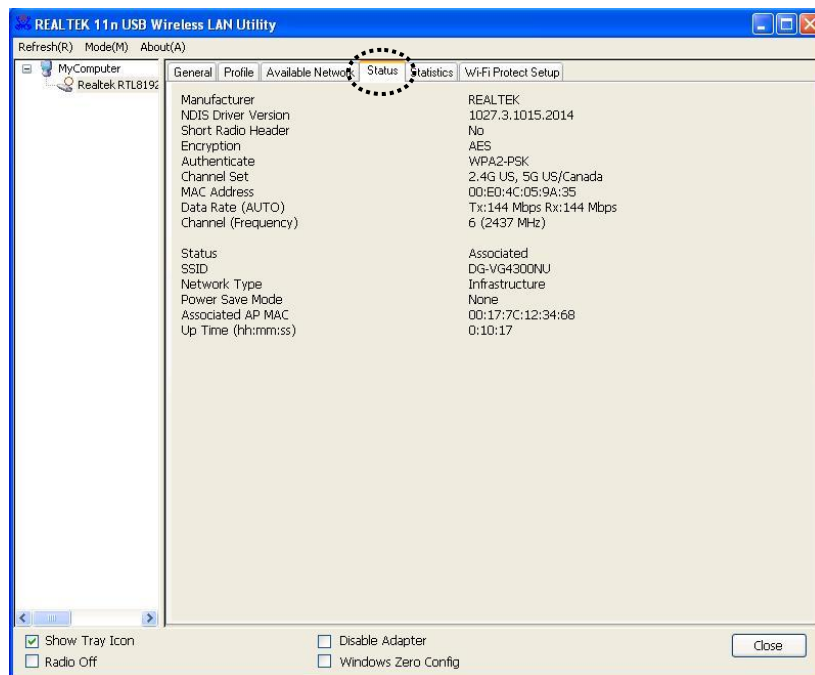
The table below explains the general information displayed.

Parameter	Description
Status	It will show the connection status of the adapter.
Speed	It shows the current speed.
Type	<b>Infrastructure</b> – This operation mode requires the presence of an 802.11 Access Point. All communication is done via the Access Point or Router. <b>IBSS</b> – Select this mode if you want to connect to another wireless station in the Wireless LAN network without an Access Point or Router.
Encryption	It displays the encryption setting of the current connection including None, WEP, TKIP or AES.
SSID	The SSID is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs.
Signal Strength	It indicates the wireless signal strength.
Link Quality	It indicates the wireless link quality.
Network Address	It shows the MAC, IP address and other information of the adapter.

## 2-5-2 Status

This screen shows the information of manufacturer, driver version, settings of the wireless network the adapter is connecting to, linking time and link status. If you don't ensure the status of the adapter and the network you are connecting, please go to the screen for more details.

If you want to know the status of your wireless network adapter, click '**Status**' menu.

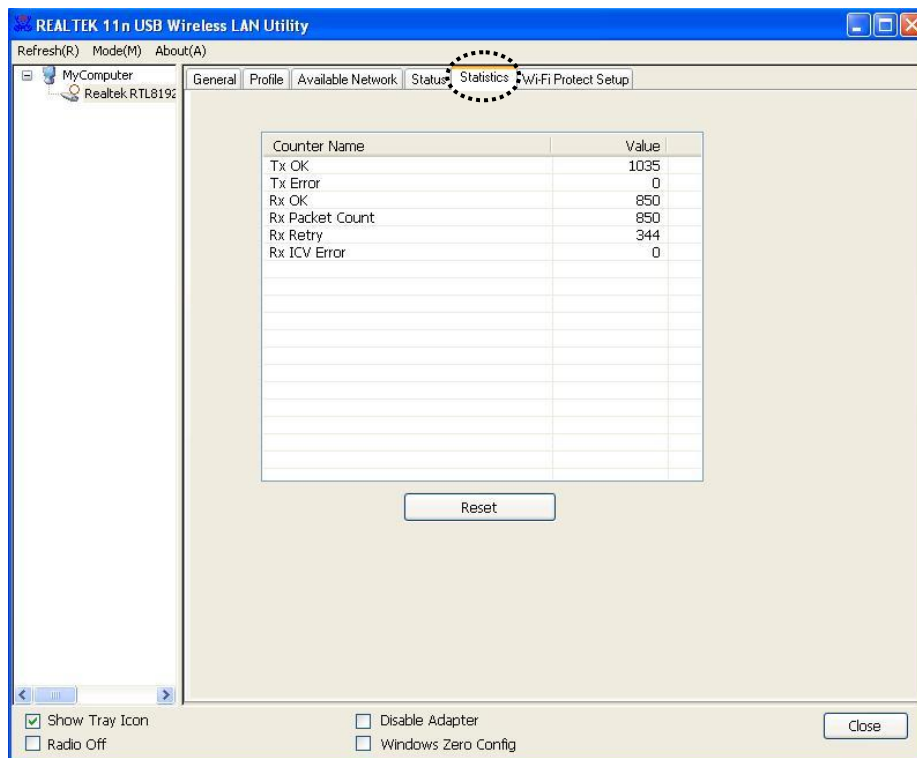




### 2-5-3 View Network Statistics

You can get the real time information about the packet transmission and receiving status during wireless communication from this screen.

To view the statistical data of wireless network adapter, click '**Statistics**' menu, and the statistics of wireless connection will be displayed:



All connection-related statistics is displayed here. You can click '**Reset**' button, to reset the statistics of all items back to 0.

## *2-6 Establish secure connection with AP by WPS*

Wi-Fi Protected Setup (WPS) is the latest wireless network technology which makes wireless network setup become very simple. If you have WPS-enabled wireless access point, and you want to establish a secure connection to it, you don't have to configure the wireless access point and setup data encryption by yourself. All you have to do is to go to the WPS setup page of this wireless adapter, click a button, and then press a specific button or enter a set of 8-digit code on the wireless access point you wish to establish a secure connection - just three simple steps.

For older wireless access points, it's possible to perform a firmware upgrade to become a WPS-enabled access point. Since they may not have a hardware button to press for WPS setup, you can use an alternative WPS setup method - input the pin code. Every WPS-compatible wireless USB adapter supports pin code configuration method; you can just input the code to wireless access point, and the wireless access point and wireless network adapter will do the rest for you.

This wireless network adapter is compatible with WPS. To use this function, the wireless access point you wish to connect to must support WPS function too. Now, please follow the instructions mentioned below to establish secure connection between WPS-enabled wireless access point and your wireless USB adapter.

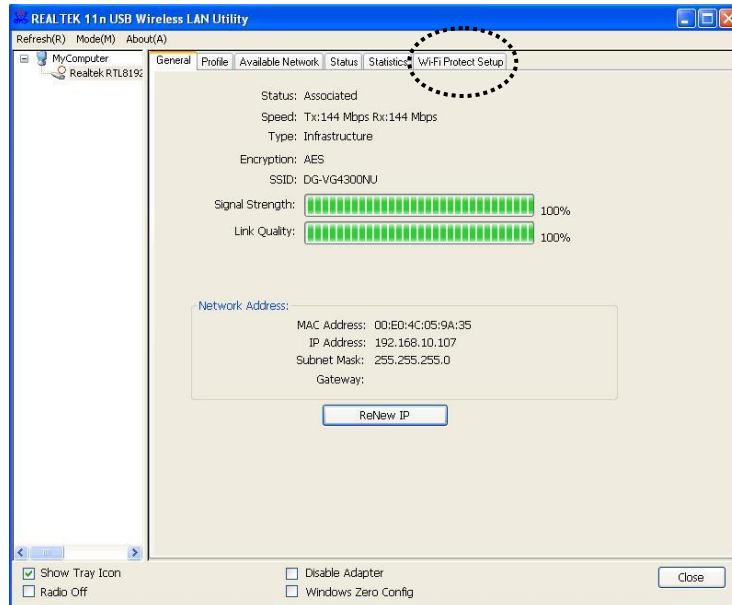
This wireless network adapter supports 2 kinds of WPS: PIN code and Push-Button.

Please follow the instructions below to setup WPS:

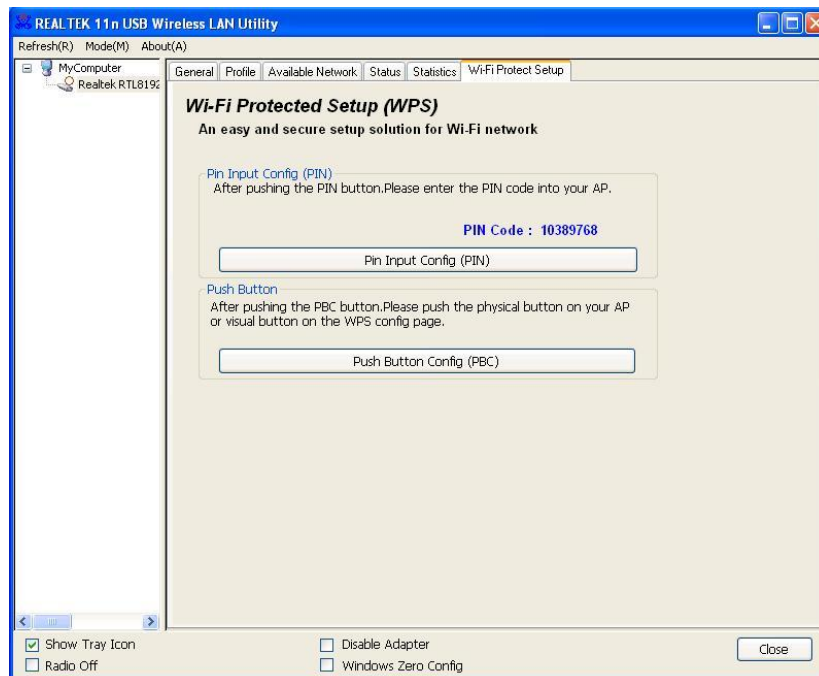
1. Right-click Realtek configuration utility icon, and click '**Open Config Utility**'.



2. Click 'Wi-Fi Protect Setup' menu.



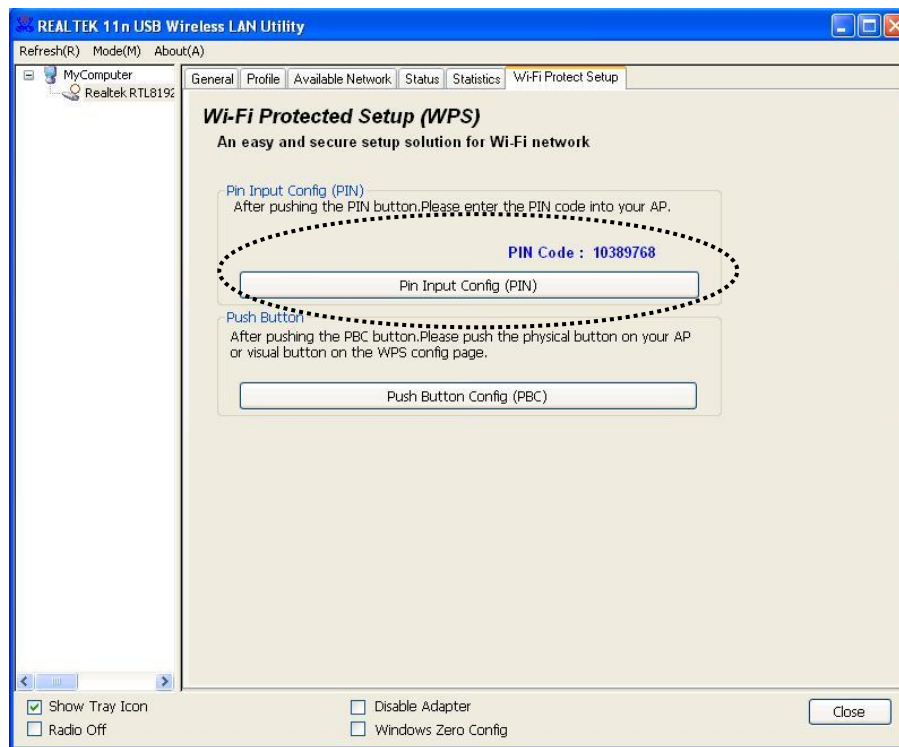
3. You can use PIN code or Push-Button configuration, and WPS-compatible wireless access point must use the same type of WPS. For instructions on setup each type of WPS, see next 2 chapters for detailed instructions.



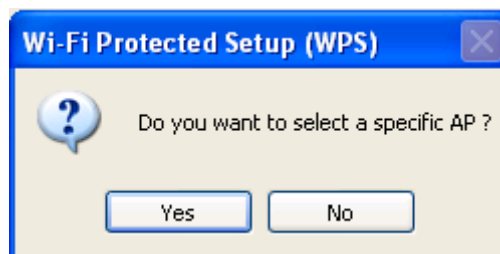
## 2-6-1 PIN Code

The PIN code of your wireless USB adapter is an eight-digit number located at the upper-right position of configuration utility. Remember it, and input the number to your wireless access point as the WPS PIN code (Please refer to the user manual of your wireless access point for instructions about how to do this)

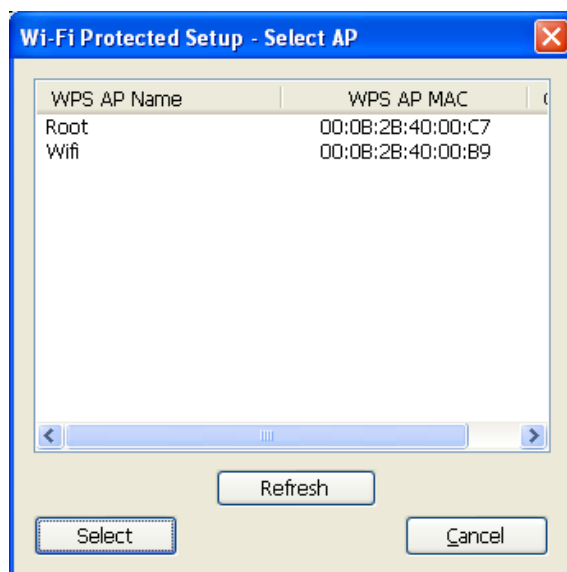
To use PIN Code, please click '**Pin Input Config (PIN)**' button:



You'll be prompted to select an access point you wish to connect. If you know its SSID, click '**Yes**', otherwise click '**No**'.



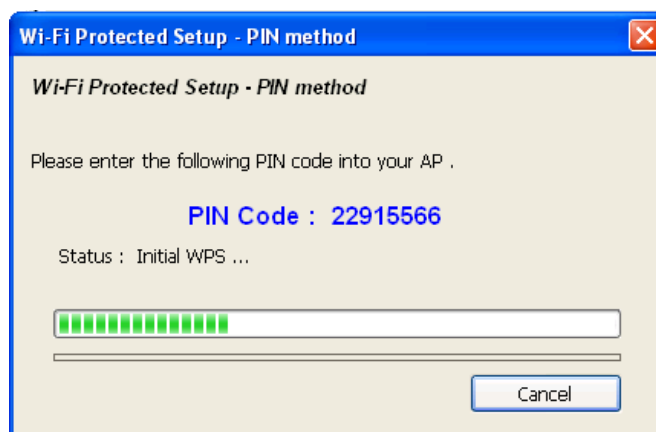
If you select '**Yes**', a list of all WPS-compatible AP nearby will be displayed; you can click '**Refresh**' to rescan, then select an AP and click '**Select**' button.



If you select 'No', wireless network adapter will prompt you to enter 8-digit PIN code into your AP, without selecting an AP in advance.

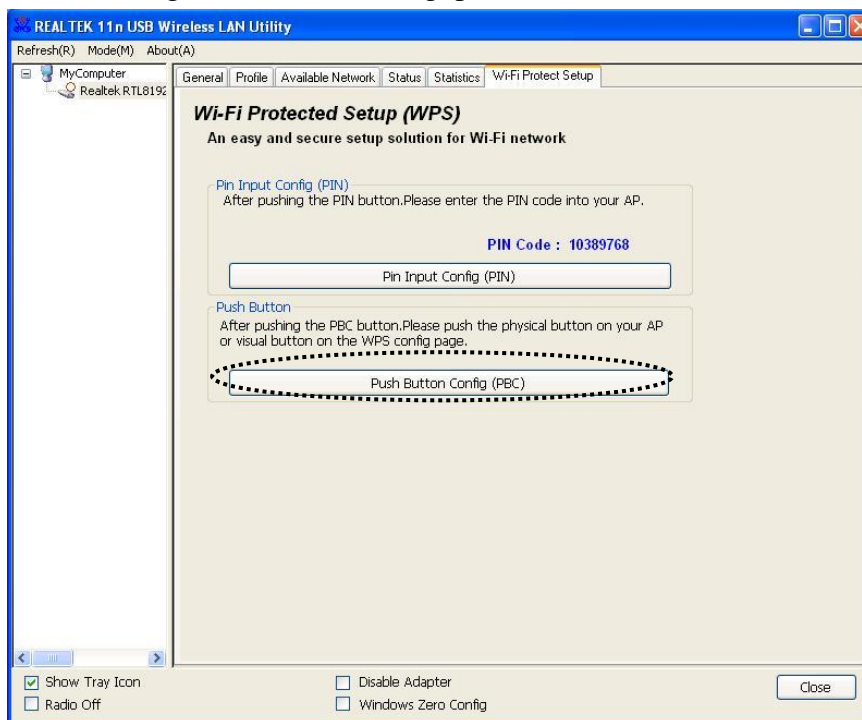
After you select 'Yes' or 'No' in previous step, network adapter will attempt to connect to WPS-compatible AP and an 8-digit number will appear. Please input this number to AP's configuration menu within 2 minutes, and network adapter will establish secure connection with AP automatically.

To stop this procedure before connection is established, click '**Cancel**'.

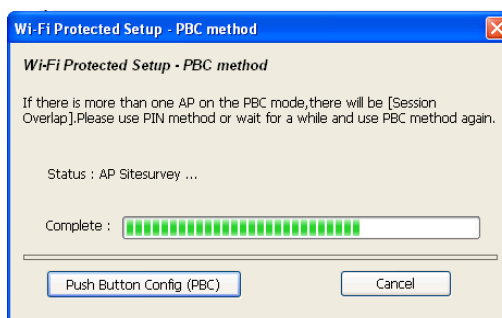


## 2-6-2 Push Button

To use Push-Button WPS configuration, please click 'Push Button Config (PBC)' button. This is the easiest way to establish secure connection by WPS, but if there're more than one WPS-compatible AP using Push-Button config, please use PIN Code instead.



After you click Push Button Config, a message box will appear:



Please activate Push-Button function on wireless access point now, and wireless network adapter will establish secure connection with access point within one minute.

## 3. Soft-AP Function

DIGISOL DG-WN3300N can act as a wireless service provider also. You can switch this wireless adapters operating mode to ‘AP’ mode to simulate the function of a real wireless access point by software, and all other computers and wireless devices can connect to your computer wirelessly, even share the internet connection you have.

Please follow the instructions in following chapters to use the AP function of your wireless adapter.

### *3-1 Switch to AP Mode and Station Mode*

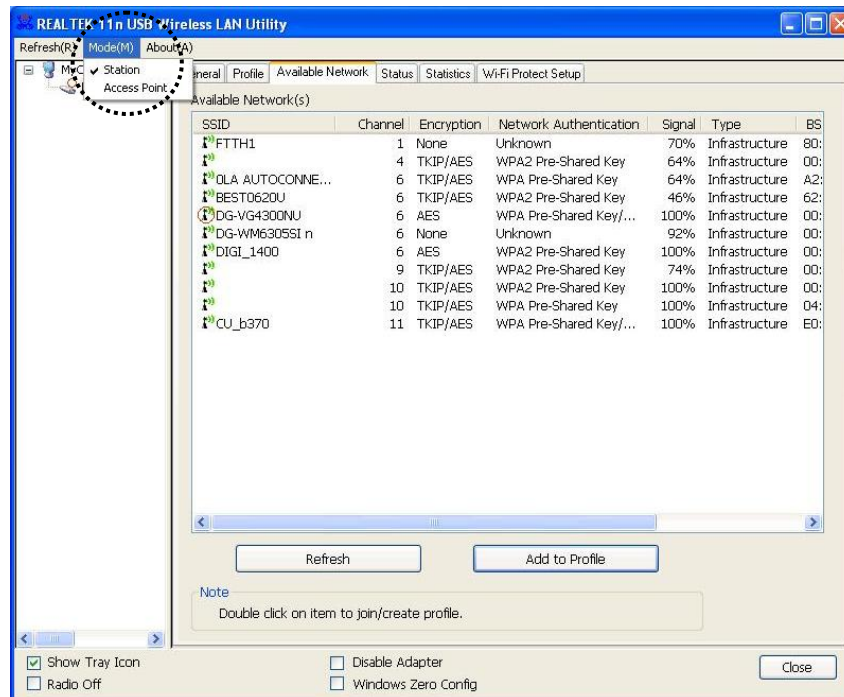
The operating mode of the wireless adapter is ‘Station Mode’ (becoming a client of other wireless access points) by default.

Please follow the instructions mentioned below to switch to AP mode:

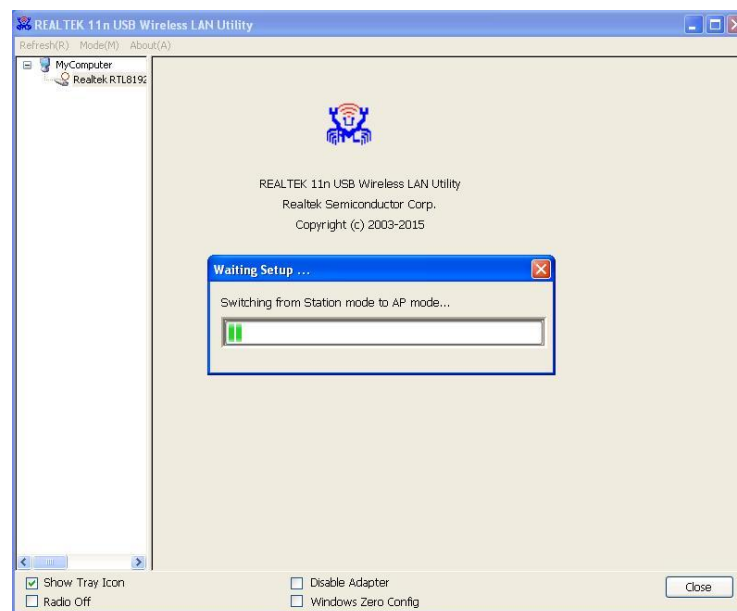
1. Right-click REALTEK configuration utility icon, and click ‘Open Config Utility’.



## 2. Select 'Mode', and then select 'Access Point'.



It requires few seconds to switch to AP mode, please be patient.

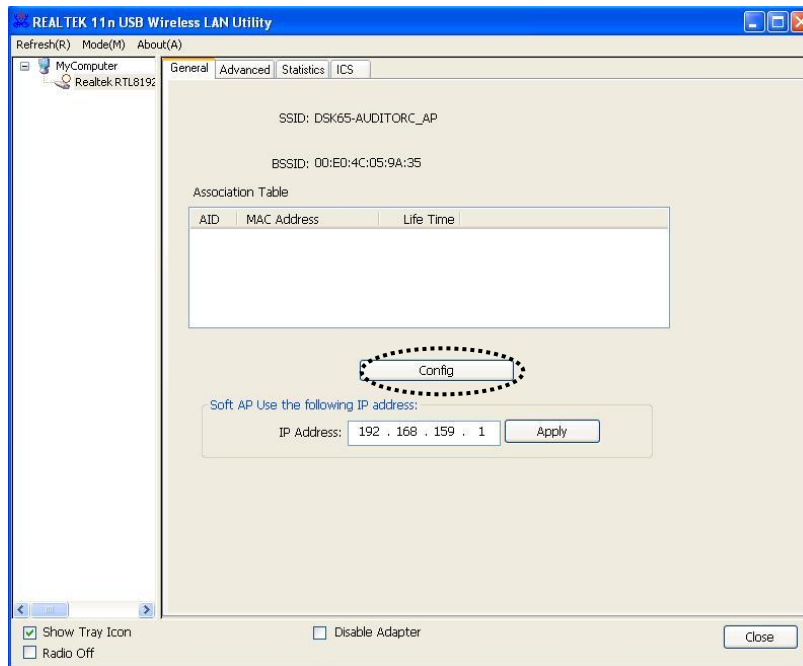


After mode switch is complete, you'll see information of software AP, which shows AP's SSID and connected wireless clients.



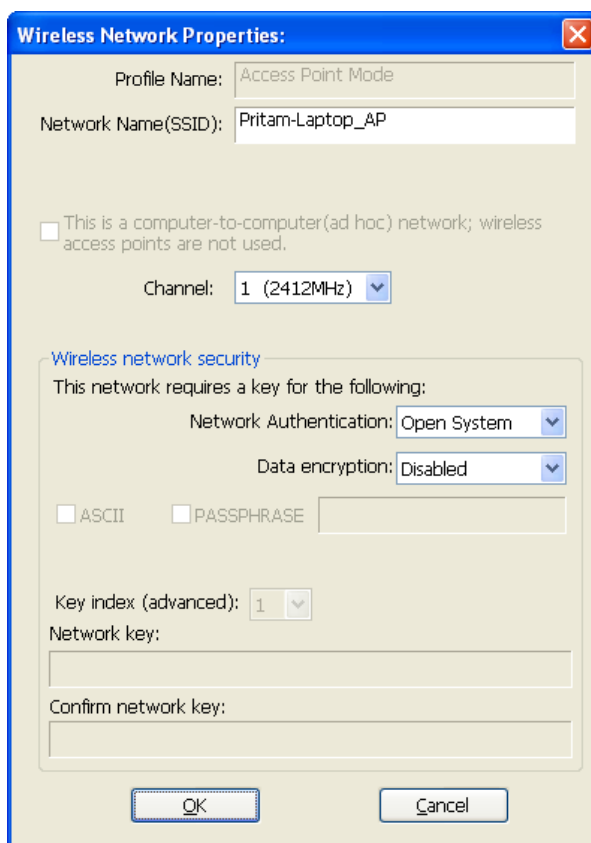
### 3-1-1 Configure SSID and Channel

To configure software AP, click ‘**Config**’ button:



Parameter	Description
SSID	<p>The SSID is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs.</p> <p>The default SSID of the AP is “Computer Name_AP”. Wireless adapters that connect to the AP should set up the same SSID as the AP.</p>
BSSID	Displays the MAC address of the wireless adapter.
Association Table	All the wireless adapters connected to the software AP will be displayed in the list.
Config	Click “Config“ for setting more configuration of the AP.

The ‘Wireless Network Properties’ are displayed.



**Wireless Network Properties:**

Profile Name: Access Point Mode

Network Name(SSID): Pritam-Laptop\_AP

☐ This is a computer-to-computer(ad hoc) network; wireless access points are not used.

Channel: 1 (2412MHz)

**Wireless network security**

This network requires a key for the following:

Network Authentication: Open System

Data encryption: Disabled

☐ ASCII ☐ PASSPHRASE

Key index (advanced): 1

Network key:

Confirm network key:

OK Cancel

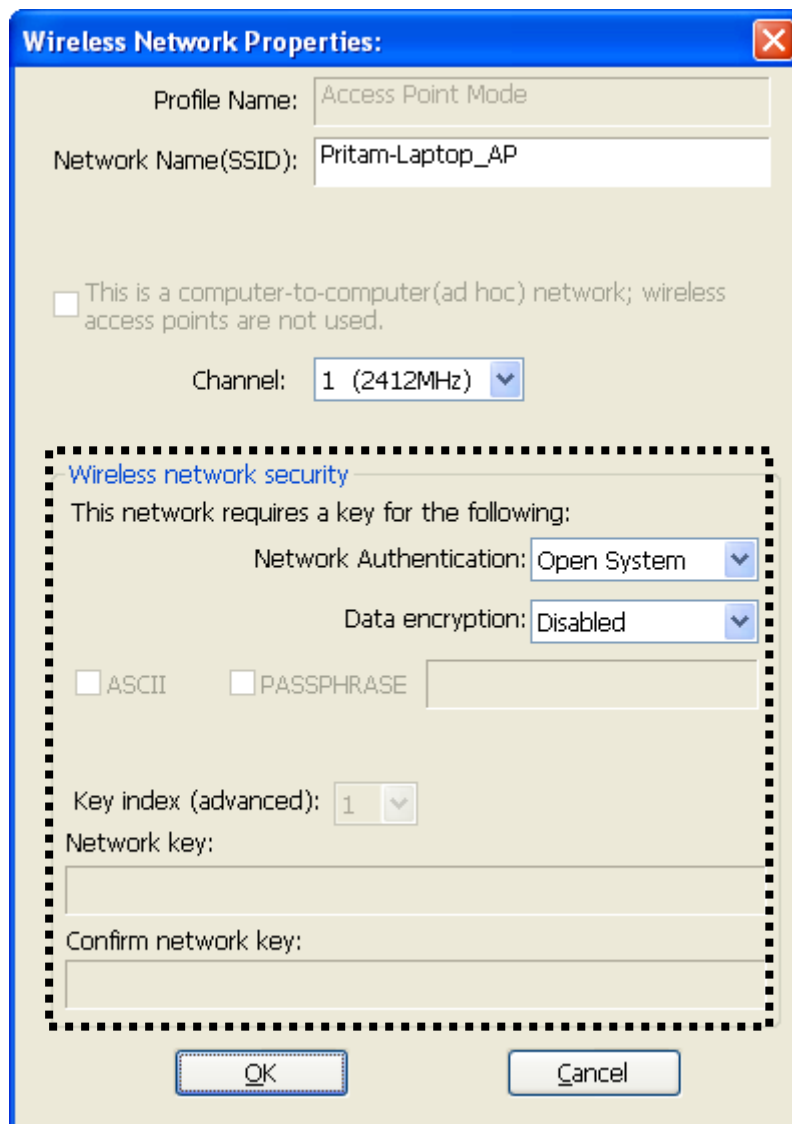
Please note that Ad-Hoc mode is not available when network adapter is in AP mode. The description of major setup items are listed below:

Parameter	Description
Network Name (SSID)	Please input the SSID (the name used to identify this wireless access point) here. Up to 32 characters can be accepted here.
Channel	Please select the wireless channel you wish to use, from 1 to 13.

To save changes, click '**OK**'; otherwise click '**Cancel**' to leave this menu and keep settings untouched.

### 3-1-2 Setup Soft-AP Security

To setup security options for Soft-AP, configure '**Wireless Network Security**' section as follows:



The image shows a Windows-style dialog box titled "Wireless Network Properties:". It contains the following fields and options:

- Profile Name:** Access Point Mode
- Network Name (SSID):** Pritam-Laptop\_AP
- ☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used.
- Channel:** 1 (2412MHz) [dropdown arrow]
- Wireless network security** (indicated by a dashed border):
  - This network requires a key for the following:
    - Network Authentication:** Open System [dropdown arrow]
    - Data encryption:** Disabled [dropdown arrow]
  - ☐ ASCII ☐ PASSPHRASE [text field]
  - Key index (advanced):** 1 [dropdown arrow]
  - Network key:** [text field]
  - Confirm network key:** [text field]
- Buttons:** OK, Cancel

The description of setup items about wireless security are listed below:

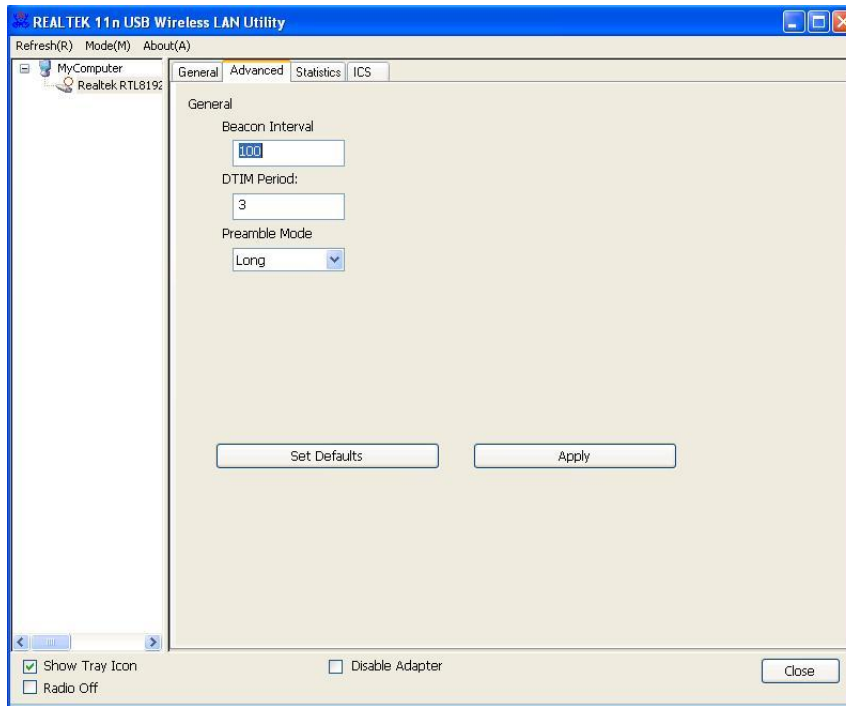
Parameter	Description
Network Authentication	<p>This setting has to be consistent with the wireless networks that the USB adapter intends to connect.</p> <p><b>Open System</b> – No authentication is needed among the wireless network.</p> <p><b>Shared Key</b> – Only wireless stations using a shared key (WEP Key identified) are allowed to connect to each other.</p> <p><b>WPA-PSK</b> – It is a special mode designed for home and small business users who do not have access to network authentication servers. In this mode, known as Pre-Shared Key, the user manually enters the starting password in their access point or gateway, as well as in each wireless station in the network. WPA-PSK takes over automatically from that point, keeping unauthorized users that don't have the matching password from joining the network, while encrypting the data traveling between authorized devices.</p> <p><b>WPA2-PSK</b> – WPA2-PSK is also for home and small business. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data encryption via the AES by default. In contrast, WPA-PSK uses Temporal Key Integrity Protocol (TKIP) by default.</p>
Data encryption	<p><b>Disabled</b> – Disable the WEP Data Encryption.</p> <p><b>WEP</b> – Enable the WEP Data Encryption. When the item is selected, you have to continue setting the WEP Encryption keys.</p> <p><b>TKIP</b> – TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This insures much greater security than the standard WEP security.</p>

	<p><b>AES</b> – AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network.</p> <p>Note: All devices in the network should use the same encryption method to ensure the communication. Select the data encryption type from drop-down menu. This setting must be identical with the setting of wireless access point you wish to connect.</p>
ASCII / PASSPHRASE	<p>When the encryption type is ‘WEP’, it’s required to input a set of ‘passphrase’ to connect to the wireless access point. Check ‘ASCII’ or ‘PASSPHRASE’ depends on the security setting of access point, and input it in the box; if you select ‘PASSPHRASE’ you also need to select the length of the key.</p> <p>The passphrase must be identical with the setting of wireless access point you wish to connect.</p>
Key index	<p>Select WEP key index. For most of the access points you can select ‘1’, but please refer to the setting of the access point.</p>
Network key / Confirm network key	<p>When the encryption type is ‘WPA’ or ‘WPA2-PSK’, it’s required to input a network key to connect to the wireless access point. Please input the same network key in the ‘confirm network key’ box.</p>

To save changes, click ‘**OK**’; otherwise click ‘**Cancel**’ to leave this menu and keep settings untouched.

## 3-2 Advanced Settings

If you want to setup advanced settings of software access point, select '**Advanced**' menu. Only if required change these parameters.



The description of all setup items are listed in the table below:

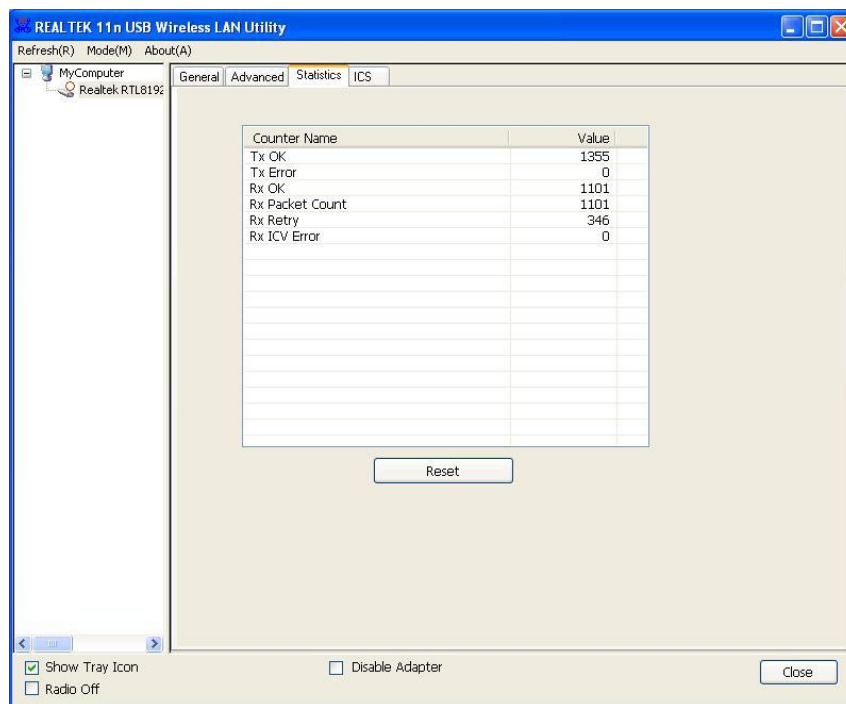
Parameter	Description
Beacon Interval	Beacon Interval specifies the duration between beacon packets (milliseconds). The range for the beacon period is between 20-1000 milliseconds with a typical value of 100.
DTIM Period	Please input DTIM (Delivery Traffic Indication Message) here. Determines the interval the Access Point will send its broadcast traffic. Default value is 3 beacons.
Preamble Mode	The preamble defines the length of the CRC block for communication among the wireless stations. There are two modes including Long and Short. High network traffic areas should use the shorter preamble type.

Set Defaults	Reset all settings back to factory default value.
Apply	Save changes.

If you changed any setting here which causes problems in communicating with wireless clients, click '**Set Defaults**' to reset all settings back to default setting.

### 3-3 Wireless Statistics

Select '**Statistics**' menu and the data statistics about software access point will be displayed. You can get the real time information about the packet transmission and receiving status during wireless communication from this screen.

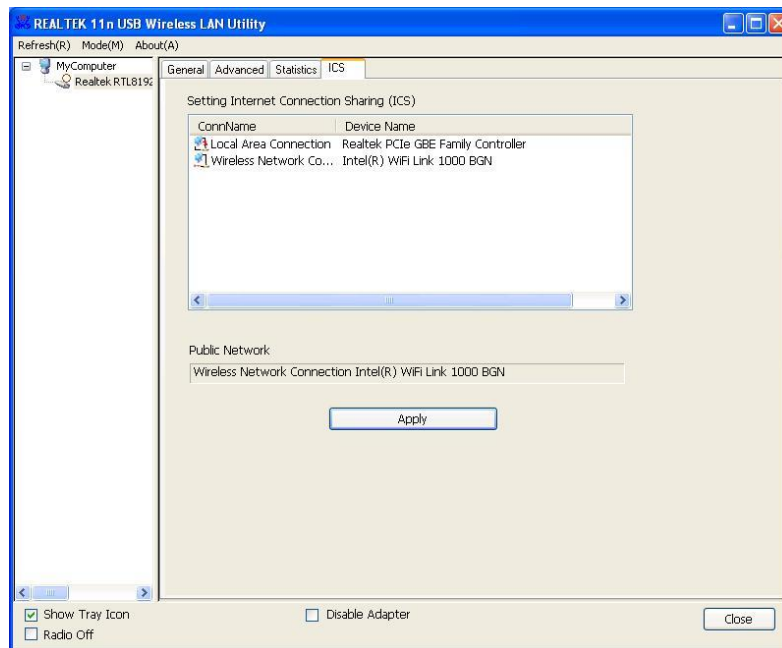


Click '**Reset**' to reset the value of every item back to '0'.

### 3-4 Internet Connection Sharing (ICS)

In this page, you can assign a network card on your computer as the path for all wireless clients to get connected to Internet.

If you have more than one network card, select the one you wish to use as Internet gateway.

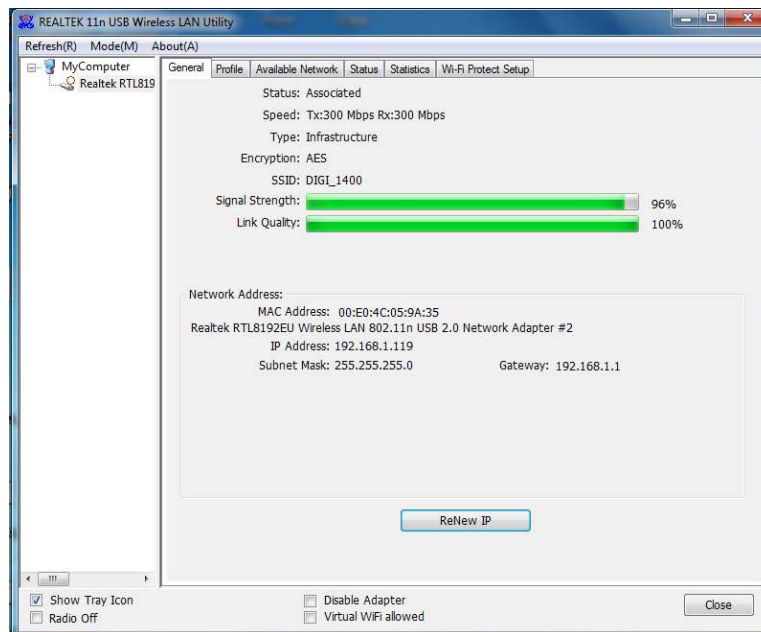


Click '**Apply**' to save changes.



## 4 Virtual WI-FI Mode on Windows7/ Windows8 (32-bit)

The operating mode of wireless adapter is ‘**Station Mode**’ (becoming a client of other wireless access point) by default.

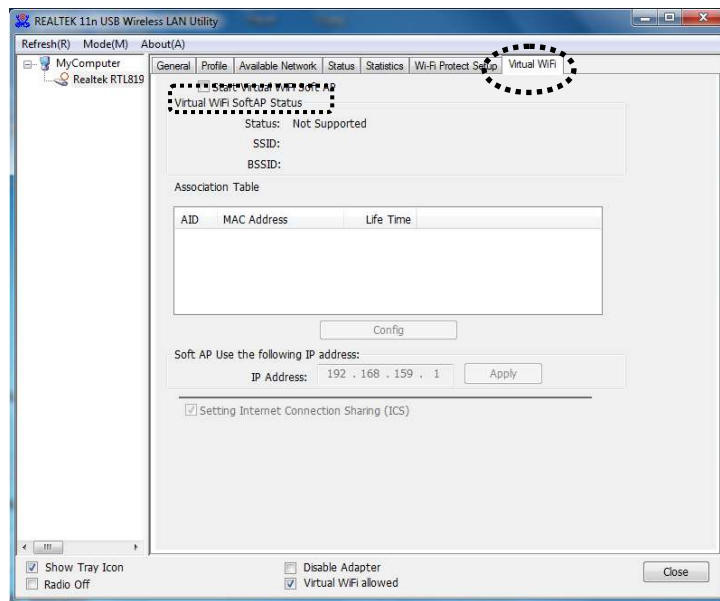


Next, follow the below instructions to switch to Virtual WiFi mode:

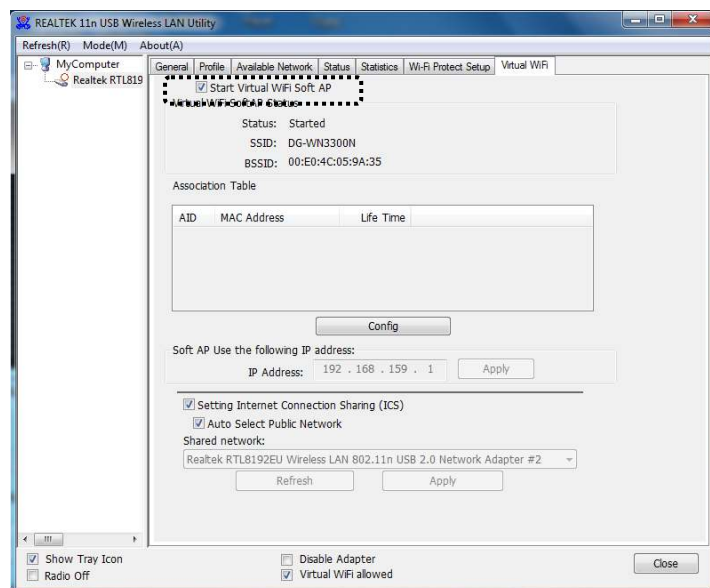
**Note: The virtual wi-fi mode is operational only in Windows7/Windows8 and not Windows XP.**

1. Check mark the Option “**Virtual Wi-Fi allowed**” in the utility, it will display a new tab as “**Virtual Wi-Fi**” in the utility. Click on that tab to configure “**Virtual Wi-Fi**” settings.

You can define the IP address for Virtual Wi-fi AP so that the other wireless clients connecting to this network will get the IP address in same range eg: here it is 192.168.159.x range.

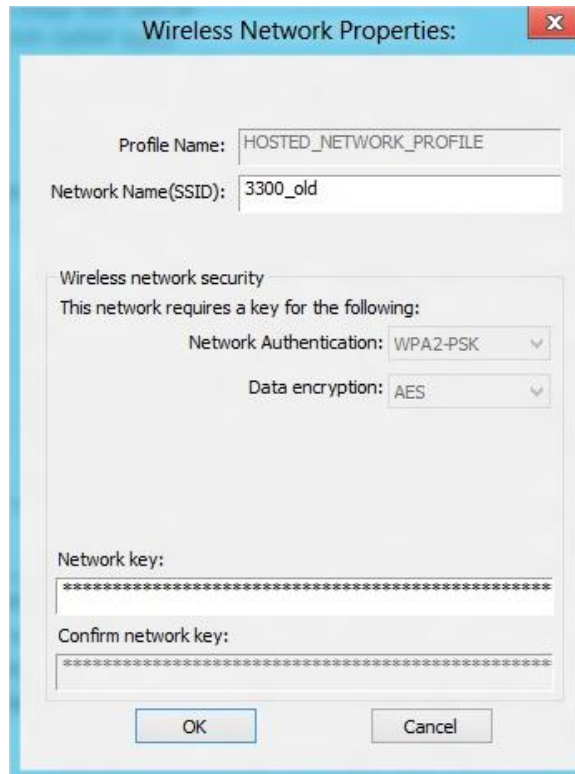


2. Select “Start Virtual Wi-Fi Soft AP” option, the following screen will be displayed:



## 4-1 Configure SSID and Soft-AP Security

To configure Access Point, click '**Config**' button as shown above:



The image shows a 'Wireless Network Properties' dialog box. It has a title bar with a close button. Inside, there are two text input fields: 'Profile Name' with the value 'HOSTED\_NETWORK\_PROFILE' and 'Network Name(SSID)' with the value '3300\_old'. Below these is a section titled 'Wireless network security' with a sub-label 'This network requires a key for the following:'. There are two dropdown menus: 'Network Authentication' set to 'WPA2-PSK' and 'Data encryption' set to 'AES'. At the bottom, there are two password fields: 'Network key:' and 'Confirm network key:', both with masked characters. At the very bottom are 'OK' and 'Cancel' buttons.

Please note that Ad-Hoc mode is not available when network adapter is in AP mode.  
The description of major setup items are listed below:

Parameter	Description
Network Name (SSID)	Please input the SSID (the name used to identify this wireless access point) here. Up to 32 numerical characters can be accepted here.
Network Authentication	<p>This setting has to be consistent with the wireless networks that the adapter intends to connect.</p> <p>In this Mode, WPA2-PSK is a default authentication setting &amp; this field is grayed out.</p> <p><b>WPA2-PSK</b> – WPA2-PSK is also for home and small</p>

	business. The difference between WPA-PSK and WPA2-PSK is that WPA2-PSK provides data encryption via the AES by default.
Data encryption	<p>In this Mode, AES is a default Encryption setting &amp; this field is grayed out.</p> <p><b>AES</b> – AES has been developed to ensure the highest degree of security and authenticity for digital information and it is the most advanced solution defined by IEEE 802.11i for the security in the wireless network.</p> <p>Note: All devices in the network should use the same encryption method to ensure the communication. Select the data encryption type from drop-down menu. This setting must be identical with the setting of wireless access point you wish to connect.</p>
Network key / Confirm network key	When the encryption type is WPA2-PSK, it's required to input a network key to connect to the wireless access point. Please input the same network key in the 'confirm network key' box.

To save changes, click 'OK'; otherwise click 'Cancel' to leave this menu and keep settings untouched.

## 5. Appendix

### *5-1 Hardware Specification*

- Standards: IEEE 802.11b/g/n
- Interface: USB 2.0
- Frequency Band: 2.4000 ~ 2.4835GHz (Industrial Scientific Medical Band)
- Data Rate: 11b: 1/2/5.5/11Mbps
  - 11g: 6/9/12/24/36/48/54Mbps
  - 11n (20MHz): MCS0-15 (Up to 144Mbps)
  - 11n (40MHz): MCS0-15 (Up to 300Mbps)
- Securities: WEP 64/128, WPA, WPA2 , WPS and IEEE 802.1x
- Antenna: Internal Antenna (2T2R)
- Drivers: Windows XP/Vista/Windows 7/ Windows 8 (32-bit)
- LED: Status
- Dimension: 33(L) x 16(W) x 6(H) mm
- Temperature: Operating: (0°C~40°C)
  - Storage: (-40°C ~70°C)
- Humidity: Operating: 10%~90% (Non-Condensing)
  - Storage: 5%~90% (Non-Condensing)

## 5-2 Troubleshooting

If you encounter any problem when you're using this wireless network adapter, don't panic. Before you call your dealer of purchase for help, please check this troubleshooting table, the solution of your problem could be very simple, and you can solve the problem yourself.

Scenario	Solution
I can't find any wireless access point / wireless device in 'Site Survey' function.	<ol style="list-style-type: none"><li>1. Click 'Rescan' for few more times and see if you can find any wireless access point or wireless device.</li><li>2. Please move closer to any known wireless access point.</li><li>3. 'Ad hoc' function must be enabled for the wireless device you wish to establish a direct wireless link.</li><li>4. Please adjust the position of the network adapter (you may have to move your computer if you're using a notebook computer) and click 'Rescan' button for few more times. If you can find the wireless access point or wireless device you want to connect by doing this, try to move closer to the place where the wireless access point or wireless device is located.</li></ol>
Nothing happens when I click 'Open Config Utility'	<ol style="list-style-type: none"><li>1. Please make sure the wireless network adapter is inserted into your computer's USB port.</li><li>2. Reboot the computer and try again.</li><li>3. Remove the adapter and insert it into another USB port.</li><li>4. Remove the driver and re-install.</li><li>5. Contact the dealer of purchase for help.</li></ol>
I cannot establish connection with a certain wireless access point	<ol style="list-style-type: none"><li>1. Click 'Add to Profile' for few more times.</li><li>2. If the SSID of access point you wish to connect is hidden (nothing displayed in 'SSID' field in 'Site Survey' function), you have to input correct SSID of the access point you wish to connect. Please contact the owner of access point to ask for correct SSID.</li><li>3. You have to input correct passphrase / security key to connect an access point with encryption. Please contact the owner of access point to ask for correct passphrase /</li></ol>

	<p>security key.</p> <p>4. The access point you wish to connect only allows network cards with specific MAC addresses to establish connection. Please go to 'Status' menu and write down the value of 'MAC Address', then present this value to the owner of access point so he / she can add the MAC address of your network adapter to his / her access point's list.</p>
The network is slow / having problem when transferring large files	<p>1. Move closer to the place where access point is located.</p> <p>2. There could be too many people using the same radio channel. Ask the owner of the access point to change the channel number.</p>

Please try one or more solutions listed above.

## 5-3 Glossary

**IEEE 802.11n standard:** 802.11n will work by utilizing multiple wireless antennas in tandem to transmit and receive data. The associated term MIMO (Multiple Input, Multiple Output) refers to the ability of 802.11n and similar technologies to coordinate multiple simultaneous radio signals. MIMO increases both the range and throughput of a wireless network. An additional technique employed by 802.11n involves increasing the channel bandwidth.

**IEEE 802.11g standard:** 802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks.

802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

The standard specifically calls for:

- A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.
- B. A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

**IEEE 802.11b standard:** The IEEE 802.11b Wireless LAN standard subcommittee, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

**Ad-hoc:** An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN card, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

**Infrastructure:** An integrated wireless and wired LAN is called an infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.



**BSS ID:** A specific Ad-hoc LAN is called an Independent Basic Service Set (IBSS) wherein the wireless devices directly communicate with each other without a central AP/ router.

**WEP:** WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802.11 standard.

**TKIP:** TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

**AES:** AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

**DSSS and FHSS:** Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.

Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

**Spread Spectrum:** Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

**WPS:** WPS stands for Wi-Fi Protected Setup. It provides a simple way to establish unencrypted or encrypted connections between wireless clients and access point

automatically. User can press a software or hardware button to activate WPS function, and WPS-compatible wireless clients and access point will establish connection by themselves. There are two types of WPS: PBC (Push-Button Configuration) and PIN code.

This product comes with limited lifetime warranty. For further details about warranty policy and Product Registration, please visit support section of **[www.digisol.com](http://www.digisol.com)**