



**Dual Band Wireless-N
300Mbps Media USB Adapter**

EUB600



User's Manual

Version v1.2

Table of Contents

1	INTRODUCTION	3
	FEATURES & BENEFITS	3
	PACKAGE CONTENTS	4
	USB ADAPTER DESCRIPTION	4
	SYSTEM REQUIREMENTS	4
	APPLICATIONS	5
	NETWORK CONFIGURATION	5
2	USB ADAPTER FOR WINDOWS (XP, VISTA AND WIN7)	7
	BEFORE YOU BEGIN	7
	INSTALLING THE WINDOWS DRIVERS	8
	MAIN INTERFACE OF THE UTILITY	12
	SITE SURVEY	12
	LINK INFORMATION	13
	PROFILE	14
	ADVANCED	21
	ABOUT	21
3	AUTHENTICATION AND SECURITY	22
	<i>WEP Encryption</i>	22
	<i>WPA-PSK & WPA2-PSK Authentication & TKIP, AES Encryption</i>	23
	<i>Setting Up CCKM, 802.1X, WPA or WPA2</i>	24
4	UNINSTALL THE DRIVERS & CLIENT UTILITY	36
5	USB ADAPTER FOR MAC OS X	38
	INSTALLING THE DRIVERS	38
	PROFILES	41
	INFRASTRUCTURE MODE	41
	AD-HOC MODE	43
	AUTHENTICATION AND SECURITY	44
	<i>WEP Encryption</i>	44
	<i>WPA-PSK & WPA2-PSK Authentication & TKIP, AES Encryption</i>	45
	LINK STATUS	46
	SITE SURVEY	47
	STATISTICS	48
	ADVANCED CONFIGURATION	48
	WPS	49
	ABOUT	51
	APPENDIX A – GLOSSARY	52
	APPENDIX 2 – HOW TO SET WPS	65
	APPENDIX C – FCC INTERFERENCE STATEMENT	71
	APPENDIX C – EU DECLARATION OF CONFORMITY	72

1 Introduction

The high-speed wireless USB 2.0 client adapter is the most convenient way to let you put a desktop/notebook computer almost anywhere without the hassle of running network cables. Now you don't need to suffer from drilling holes and exposed cables. Once you are connected, you can do anything, just like the wired network. This USB client adapter operates seamlessly in 2.4GHz & 5GHz frequency spectrum supporting the 802.11a, 802.11b, 802.11g, and 802.11n wireless standards. It's the best way to add wireless capability to your existing wired network or simply surf the web.

To protect your wireless connectivity, the high-speed wireless USB 2.0 client adapter can encrypt all wireless transmissions through 64/128-bit WEP, WPA, WPA-PSK and WPA2-AES encryption and authentication allowing you to experience the most secure wireless connectivity available.

The EnGenius Dual Band USB Adapter (EUB600) implements Draft 2.0 technology which extremely improves wireless signal for your computer than existing wireless 802.11g technology. It supports the 2T2R MIMO architecture with fully forward compatibility with IEEE802.11n. The incredible speed of EUB600 USB adapter makes heavy traffic networking activities more flexible and takes the wireless into practical road. You could enjoy the racing speed of wireless connection, surfing on Internet without string wires.

Adding EnGenius EUB600 to your Notebook or Computer, it provides an excellent performance and cost-effective solution for doing media-centric activities such as streaming video, gaming, and enhances the QoS (WMM) without any reduction of performance. It extends 3 times network coverage and boosts 6 times transmission throughput than existing 11g product. Advanced power management and low power consumption among 11n products.

For more security-sensitive application, EUB600 supports Hardware-based IEEE 802.11i encryption/decryption engine, including 64-bit/128-bit WEP, TKIP, and AES. Also, it supports Wi-Fi alliance WPA and WPA2 encryption and is Cisco CCX V1.0, V2.0 and V3.0 compliant.

Features & Benefits

Features	Benefits
Dual Band Support 2.4Ghz & 5Ghz	Less Interference
Racing Speed up to 300Mbps data rate (2.4GHz & 5Ghz 11N technology)	Enjoy the Internet connection in crazy-fast speed, without the bottleneck of stringing wires.
Advanced power management	Low power consumption
WPA/WPA2 (IEEE 802.11i), WPA-PSK, WPA2-AES, WEP 64/128 Support	Powerful data security.

Support 2Tx * 2Rx Radio	With Intelligent Antenna enables
WMM (IEEE 802.11e) standard support	Wireless Multimedia Enhancements Quality of Service support (QoS) / enhanced power saving for Dynamic Networking
USB 2.0/1.1	USB 2.0 interface and compatible with USB 1.1

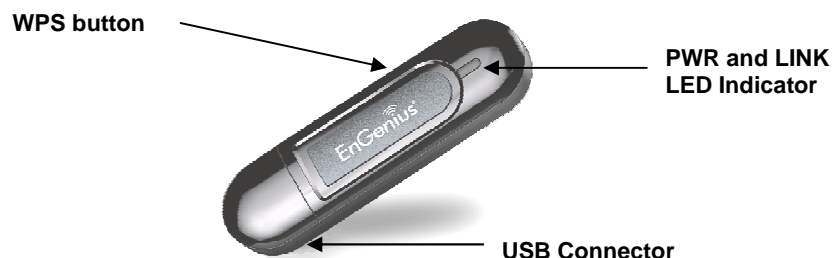
Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- One Wireless LAN USB Adapter
- One CD-ROM with Drivers and User's Manual Included
- One Quick Installation Guide
- One Technical Support Card

USB Adapter Description

The USB adapter is a standard USB adapter that fits into any USB interface.



System Requirements

The following are the minimum system requirements in order to use the USB adapter.

- PC/AT compatible computer with a USB interface.
- Windows 2000/XP/Vista/Win7 or MAC OS operating system.
- 30 MB of free disk space for installing the USB adapter driver and utility program.

Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

- a) **Difficult-to-wire environments**
There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.
- b) **Temporary workgroups**
Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.
- c) **The ability to access real-time information**
Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.
- d) **Frequently changed environments**
Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.
- e) **Small Office and Home Office (SOHO) networks**
SOHO users need a cost-effective, easy and quick installation of a small network.
- f) **Wireless extensions to Ethernet networks**
Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.
- g) **Wired LAN backup**
Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.
- h) **Training/Educational facilities**
Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

Network Configuration

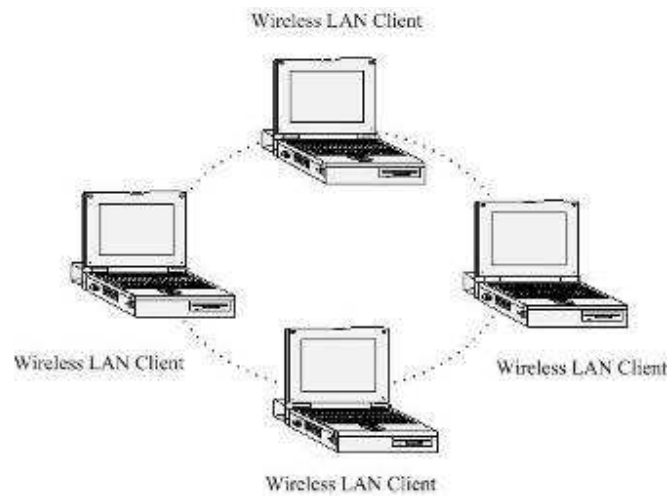
To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

- a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
- b) Infrastructure for enterprise LANs.

a) **Ad-hoc (peer-to-peer) Mode**

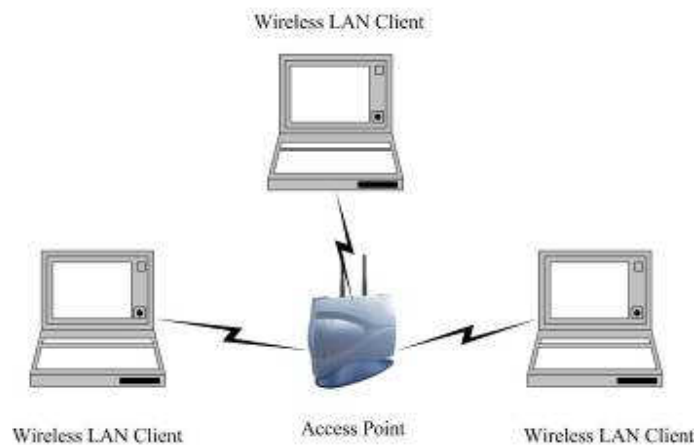
This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point.

This is the easiest and least expensive way for the SOHO to set up a wireless network. The image below depicts a network in ad-hoc mode.



b) Infrastructure Mode

The infrastructure mode requires the use of an Access Point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations. The image below depicts a network in infrastructure mode.



2 USB Adapter for Windows (XP, Vista and Win7)

Before You Begin

WiFi Alliance certification recommends WPA2 AES to be the security mechanism under 11N mode. System driver will automatically bring down wireless data rate to 54Mbps if other security method such as WEP or WPA is used under 11n mode.

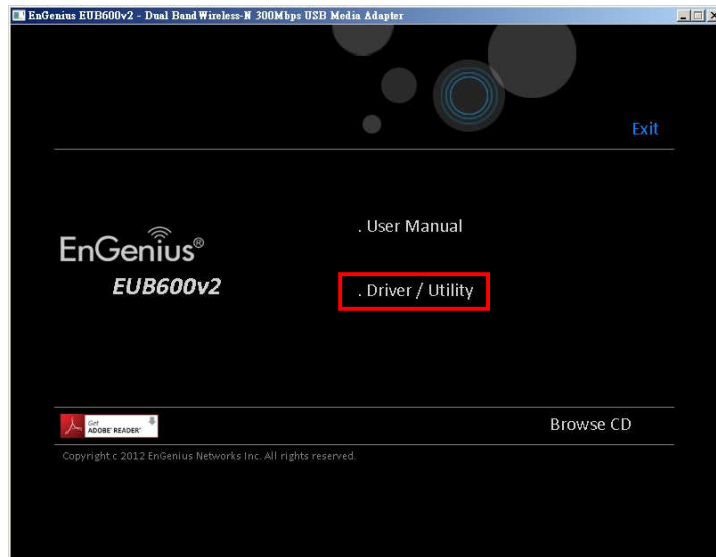
If your 11N router is using security mechanism other than WPA2 AES, you are recommended to disable security setting or change it to WPA2 AES to fully utilize 11N capability. This policy has no effect if connecting with b/g only wireless access point.

During the installation, XP may need to copy systems files from its installation CD. Therefore, you may need a copy of the Windows installation CD at hand before installing the drivers. On many systems, instead of a CD, the necessary installation files are archived on the hard disk in C:\WINDOWS\OPTIONS\CABS directory.

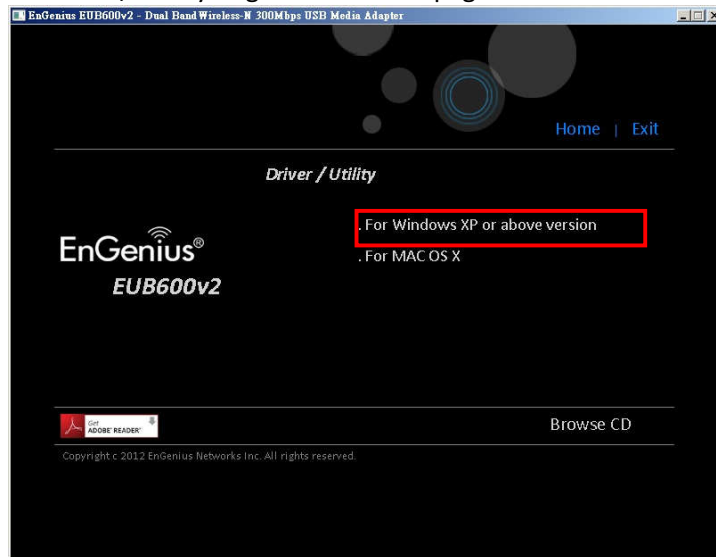
Installing the windows Drivers

Follow the steps below in order to install the USB adapter drivers:

1. Insert the CD-ROM that was provided to you in this package. The setup should run automatically. If the setup does not run automatically, then must manually select the **Autorun.exe** file from the CD-ROM drive.

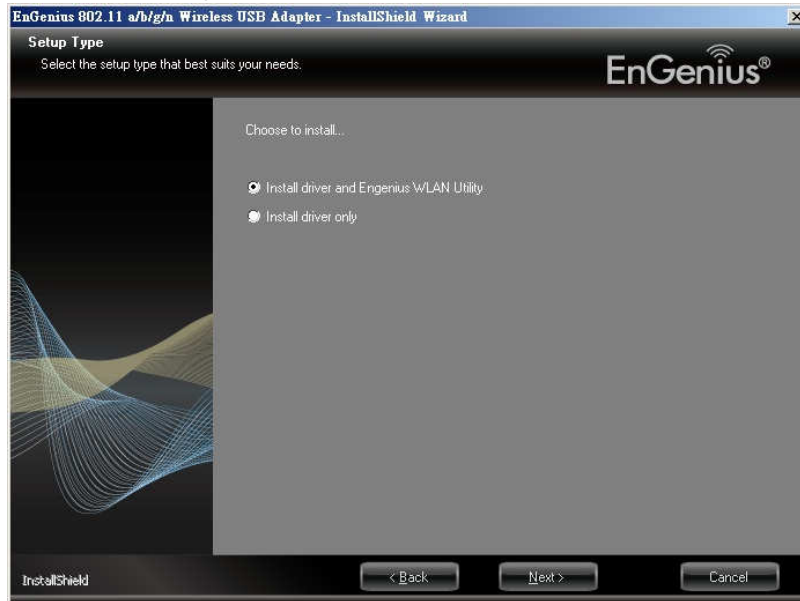


2. Click on Driver / Utility to go to the Driver page.

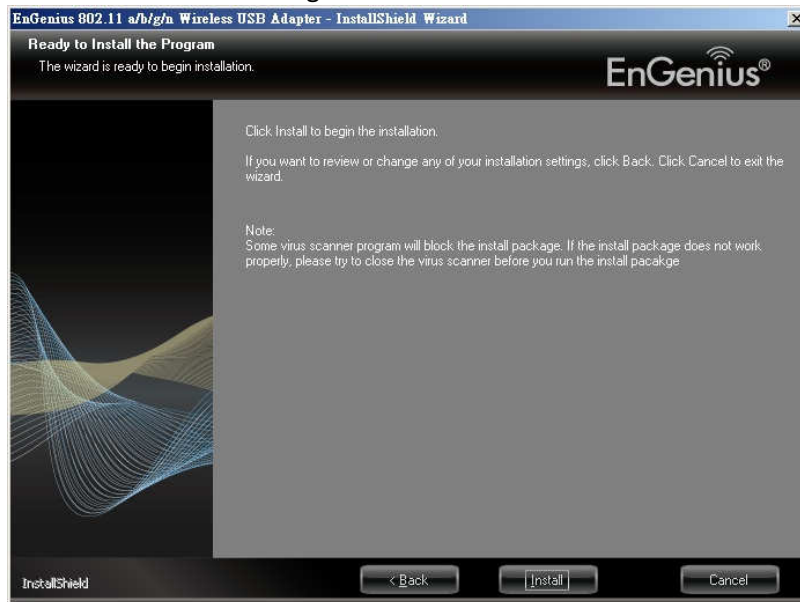


3. Click **For Windows XP or above version** to start the install process.

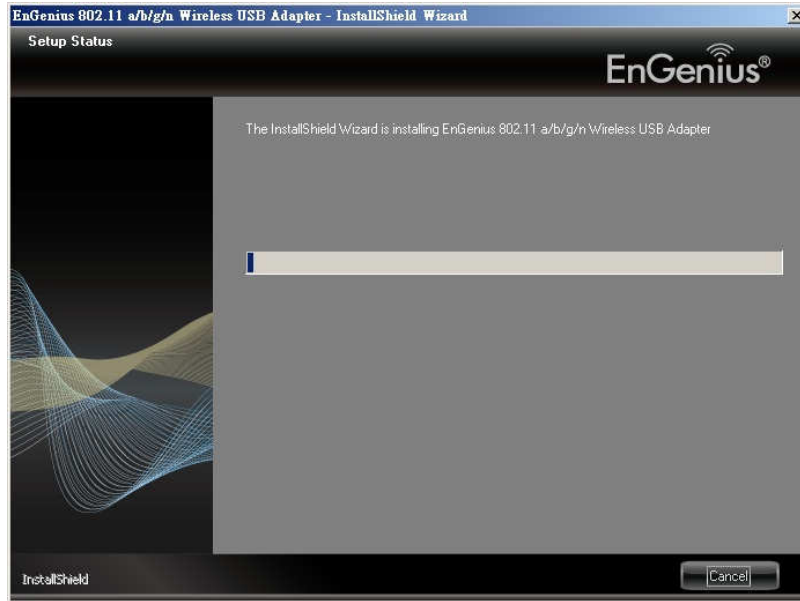
4. Once the setup begins you will see the **InstallShield Wizard**. Select **Install driver and EnGenius WLAN Utility** and then click on the **Next>** button.



5. Click on the **Install** button to begin the installation.



6. Wait for a few seconds until the driver and client utility is installed.



7. The installation is complete. Click on the **Finish** button.



- Carefully insert the USB adapter into the USB port. Windows will then detect and install the new hardware.

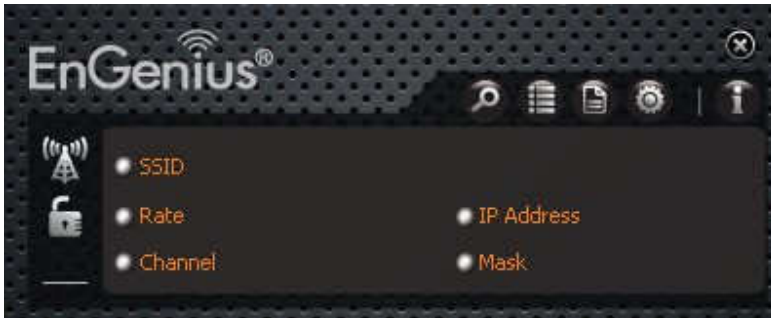


- An **EG** icon will then appear in the system tray. Right click on the **EG** icon and then click on **Launch Config Utility**.

Note: Click on **Use Zero Configuration as Configuration Utility** if you would like to use Windows Zero Configuration (XP only feature).



Main interface of the utility



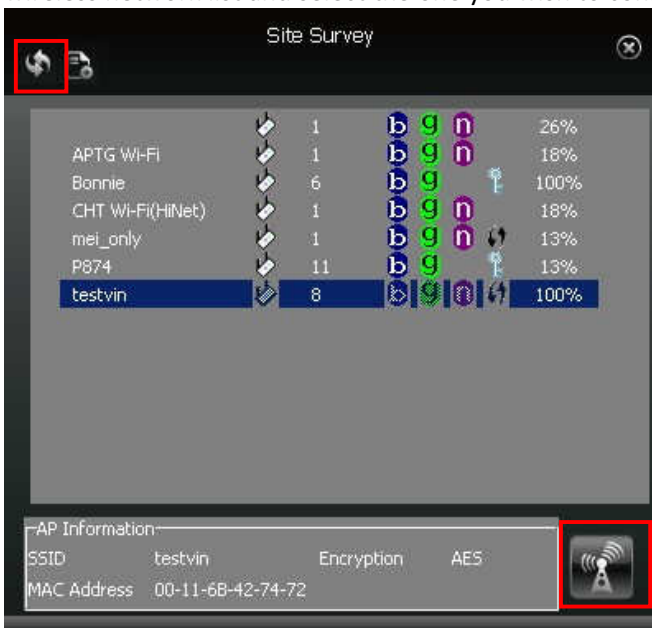
The function buttons on the top(From L to R)are respectively Site Survey, Link Information, Profile, Advanced, About, and MiniSize the Interface. While the left column displays Turn On/Off RF, Security /No security, and Signal status.

Site Survey



The “Site Survey” screen displays currently scanned wireless signals and you can click one to connect the signal. Select one and you may view the AP’s MAC address, wireless mode (A/B/G/N), authentication type, and encryption type, or WPS authentication and signal strength.

Before you connect to a wireless network, please click the “Rescan” button to update the wireless network list and select the one you wish to connect, then click the “Connect” icon.



Link Information

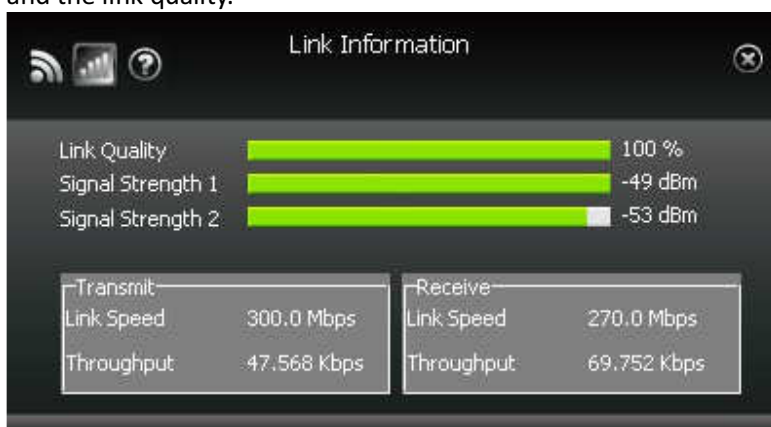


After successfully connected to one wireless network, you can view its detailed information by clicking the “Link Information” on the main interface.

1. “Link Status” screen displays the detailed information of the connected AP including its SSID,MAC address, authentication type, encryption type, network type and channel.



2. “Throughput” screen displays the signal strength of each of the wireless adapter’s antennas and the link quality.



3. “Statistics” screen is used to count the total Rx and Tx data packets, including transmitted, retransmitted and fail to receive ACK after all retries. You can click the “Reset Counter” button to clear the count.







Profile



Except the above common connection type, you can also connect to the wireless network by adding a profile on the “Profile” screen. The Profile screen is used to save the wireless network parameters. When the adapter is successfully connected to a network, the profile name of this network will automatically be added here, which helps the adapter to quickly connect to the wireless network next time. However, there’s one exception that when you have set the hidden SSID, namely the SSID can not be scanned, then you must manually connect by adding the profile name. The main interface is as shown below.



-  **Add:** create a new profile
-  **Delete:** delete the existing profile
-  **Edit:** modify the existing profile
-  **Import:** import the previously configured profile.

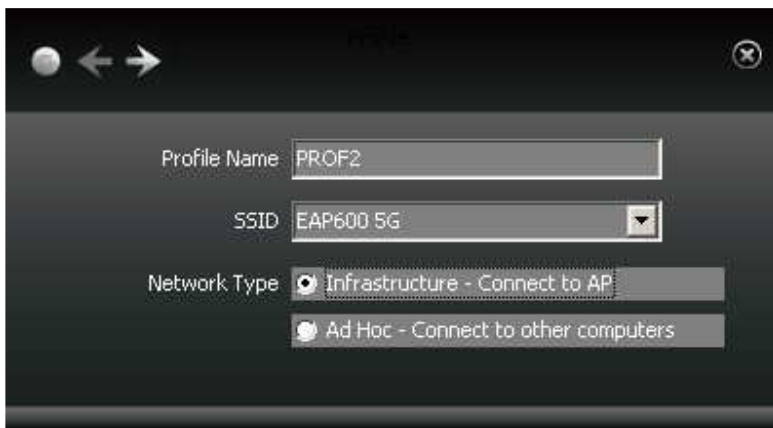


Export: export the configured profile.



Add WPS Profile: WPS setting requires that the connecting wireless device support WPS function. WPS helps you to fulfill wireless encryption fast as well as secure your wireless network. For detailed setting steps, refer to appendix2.

There are two network types for your option when clicking the “Add” button to add wireless adapter connection: Infrastructure and Ad-Hoc.



Infrastructure is an application mode that integrates the wired and wireless LAN architectures. It is different from Ad-Hoc in that in this mode the computer installed with the wireless network adapter has to fulfill the wireless communication via AP or wireless router. It can be divided into two modes: “wireless AP + wireless network adapter” and “wireless router + wireless network adapter”.

Ad-Hoc is a special wireless mobile network application mode. All nodes in the network are equal. Usually it is used to share resources by connecting the opposing computer’s wireless adapter.

1. Infrastructure Profile Management

When you are connecting the wireless adapter to an AP or a wireless router, please select the Infrastructure mode.

Click the “Add” button and select the network type as “

Infrastructure”, and enter the profile name and SSID or you can find the SSID you wish to connect from the drop-down list.



Click the next button to select the authentication type and encryption type such as WPA—PSK and AES, and then input the key and click next.



After a profile is successfully added, the profile name can be seen on the profile list, you can edit, import or export the profile, click "Active" to finish the connection, now you can also view the detailed connection status on the "Link Information" screen.

Note: Please refer to page.23 for detail security wireless encryption settings.



NOTE:

If the SSID broadcast function of the wireless router or AP you wish to connect is disabled, then the wireless adapter can not scan the SSID, thus you need to connect by creating the corresponding profile.

2.Ad-Hoc Profile management

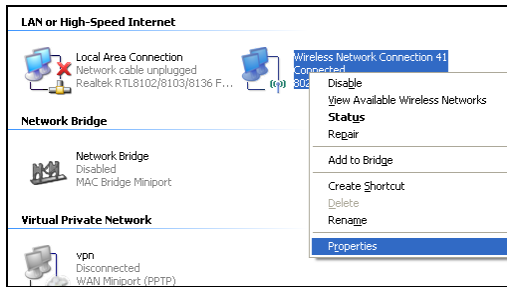
Using the Ad-hoc mode to establish a wireless network requires that each computer should be equipped with a wireless network adapter. By connecting these wireless adapters, computers are able to share the resources. The detailed setting steps are as follows:

1) Firstly you'll have to allocate a static IP to each wireless adapter to be connected in Ad-hoc mode.

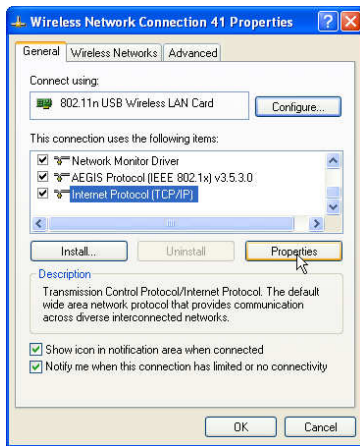
a.Right click "My Network Places" on your computer's desktop and select "Properties".



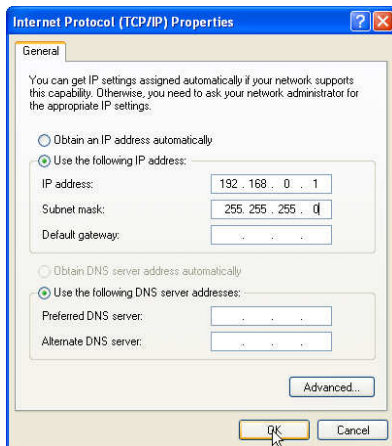
b.Right click "Wireless Network Connection", and select "Properties"



c. Select “Internet Protocol(TCP/IP)” and click “Properties”.

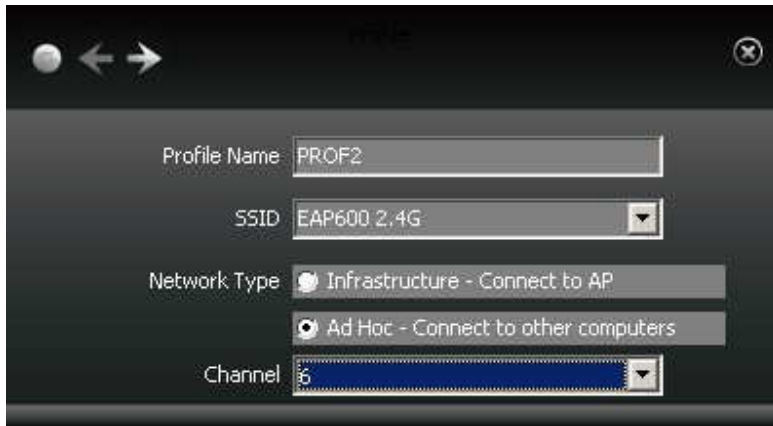


d. Please enter the IP address and subnet mask, and make sure this IP address is not used by other devices in the network. For example: if your wireless adapter’s IP address is 192.168.0.1 , then set other wireless adapters’ IP addresses within the range of 192.168.0.2—192.168.0.254. Click “Ok” to save the settings.



2) Create a new Ad-hoc profile

Click the “Add” button and enter the network name in the SSID field to identify the wireless network, and select Ad-hoc as the network type and then select the channel.



Click the “Next” button to select the authentication type and encryption type and then input the correct key and click “Next”.

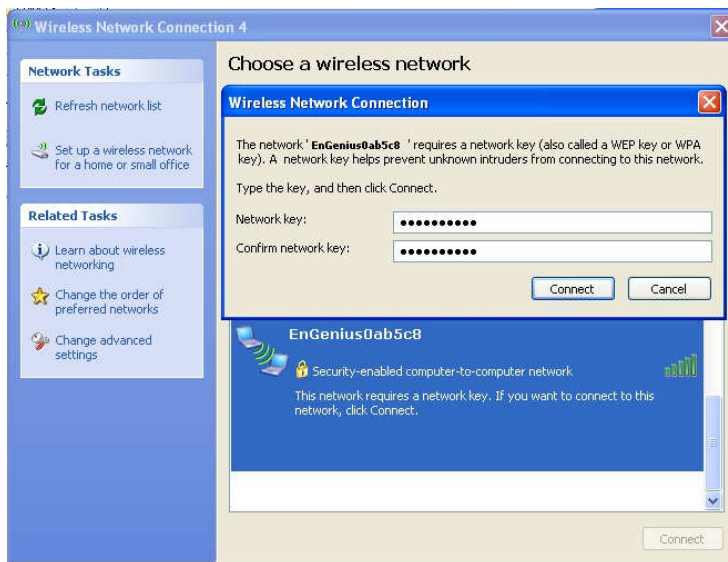


After a profile is successfully added, the profile can be seen on the profile list, select it and click the “Active” icon on the lower right corner.

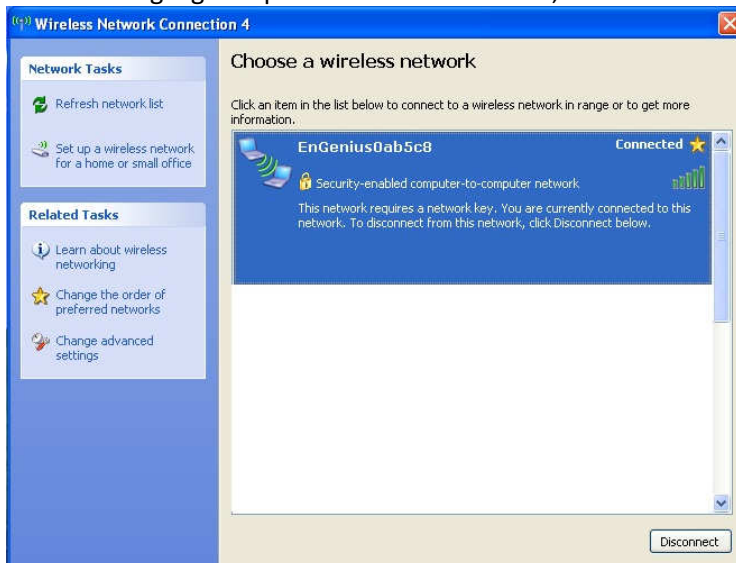
Note: Please refer to page.23 for detail security wireless encryption settings.



And then search for the wireless network on other clients. Double click the wireless network you have configured and you'll be prompted for the key .After entering the key, click "Connect".



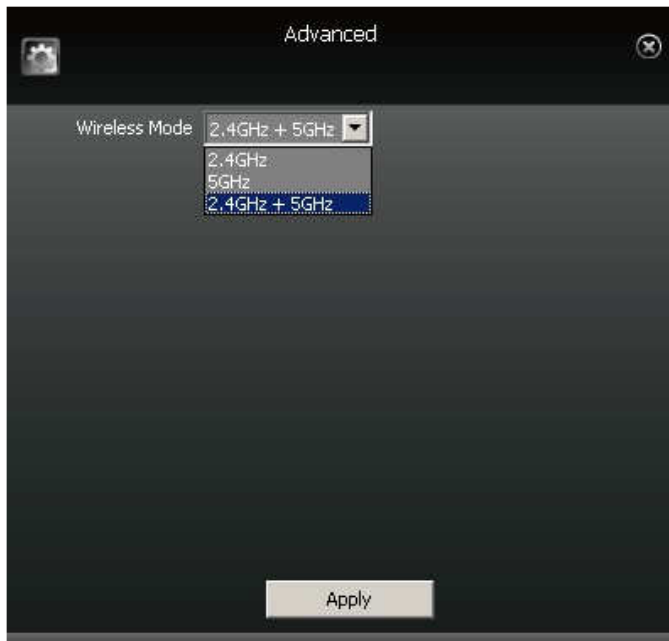
When the highlighted part shows "Connected", it indicates the connection is successful.



Advanced



This section is used to set the channels.



About



This screen mainly displays the version information of the UI's different programs as well as EnGenius's copyright statement.



3 Authentication and Security

WiFi Alliance certification recommends WPA2 AES to be the security mechanism under 11N mode. System driver will automatically bring down wireless data rate to 54Mbps if other security method such as WEP or WPA is used under 11n mode.

If your 11N router is using security mechanism other than WPA2 AES, you are recommended to disable security setting or change it to WPA2 AES to fully utilize 11N capability. This policy has no effect if connecting with b/g only wireless access point.

This step allows you to configure the authentication and encryption settings such as: WEP, WPA, WPA-PSK, WPA2, and 802.1x. Each security option is described in detail below.



WEP Encryption

The **WEP** tab displays the WEP settings. Encryption is designed to make the data transmission more secure. You may select 64 or 128-bit WEP (Wired Equivalent Privacy) key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase. The following information is included in this tab, as the image depicts below.



- **Authentication Type:** Select **Open** or **Shared** from the drop-down list.
- **Encryption:** Select **WEP** from the drop-down list.
- **Default TX Key:** Choose the Key 1~Key4 you want to use.
- **WEP Key Format (Hex or ASCII):** Type a character string into the field. For 64-bit enter 5 alphanumeric or 10 hexadecimal characters. For 128-bit enter 13 alphanumeric or 26 hexadecimal characters.
- Click on the right arrow button to save the changes.

WPA-PSK & WPA2-PSK Authentication & TKIP, AES Encryption

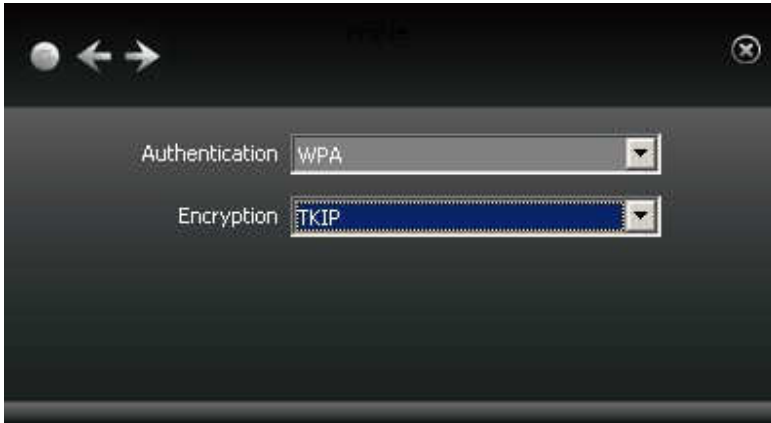
WPA-PSK (Pre-shared Key) is used in a Pre Shared Key mode that does not require an authentication server. Access to the Internet and the rest of the wireless network services is allowed only if the pre-shared key of the computer matches that of the Access Point. This approach offers the simplicity of the WEP key, but uses stronger TKIP encryption. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.



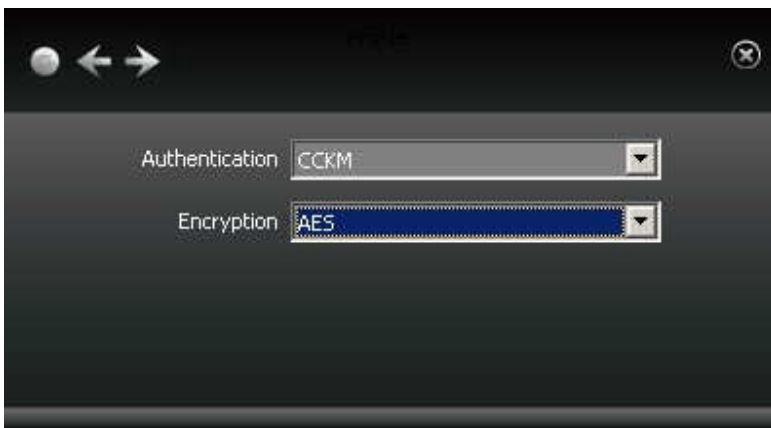
- **Authentication Type:** Select **WPA-PSK** or **WPA2-PSK** from the drop-down list.
- **Encryption:** Select **TKIP** or **AES** from the drop-down list.
- Click on the right arrow button to next step.
- **WPA Preshared key:** Enter a pass phrase which is between 8 and 63 characters long.
- Click on the right arrow button to save the changes.

Setting Up CCKM, 802.1X, WPA or WPA2

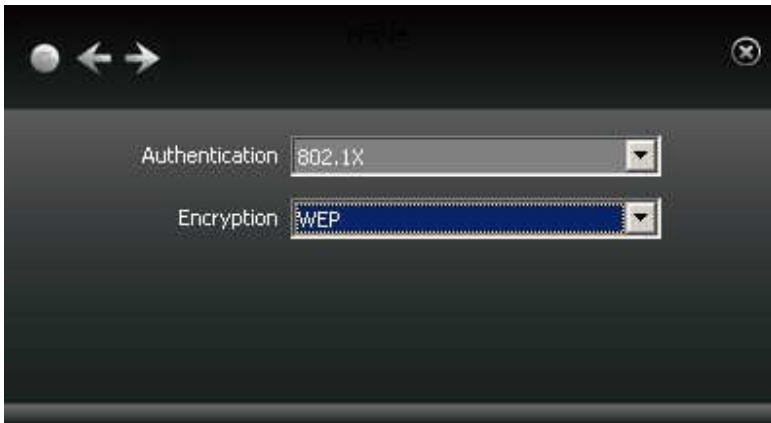
- a. In the Profile Settings security screen, select an authentication and encryption method.
- To set up WPA or WPA2 authentication, for Authentication select WPA or WPA2, and for Encryption select TKIP or AES. If WPA2 is selected, TKIP and AES are available with the added security of management frame protection (TKIP, AES). Click the right arrow to save your settings.



- To set up CCKM authentication, for Authentication select CCKM, and for Encryption select WEP, TKIP, or AES. Click the right arrow to save your settings.



- To set up 802.1X authentication, for Authentication select 802.1X, and for Encryption select WEP. Click the right arrow to save your settings.



- b. Select the EAP method (Extensible Authentication Protocol) supported by your network and follow the instructions given.

PEAP

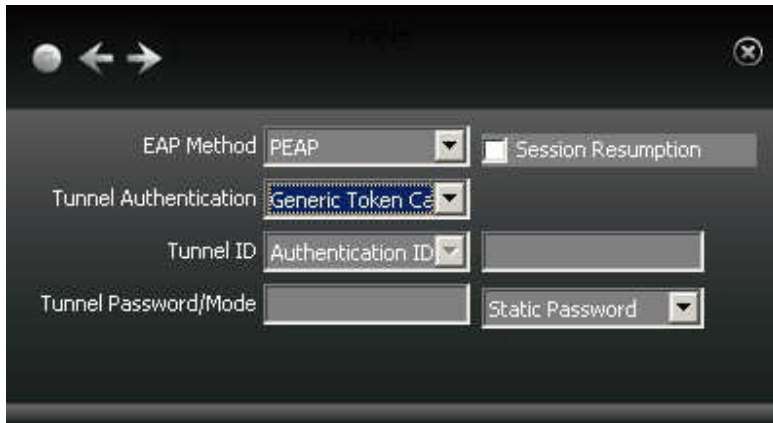
- i. If you select PEAP, for Tunnel Authentication select either EAP-MSCHAP v2, EAP-TLS/Smart Card, or Generic Token Card.
- If you select EAP-MSCHAP v2, in the Tunnel ID field type the name assigned to the user, and in the Tunnel Password field, type the password associated with the user name.



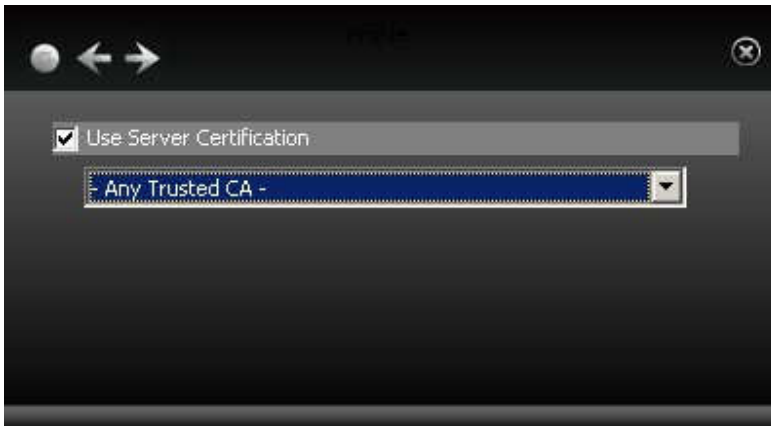
- If you select EAP-TLS/Smart Card, in the Tunnel ID field, select Authentication ID or Machine ID depending on whether user credentials are provided by a smart card or by the computer from which they are accessing the network. If Authentication ID is selected, in the adjacent field, type your user name.



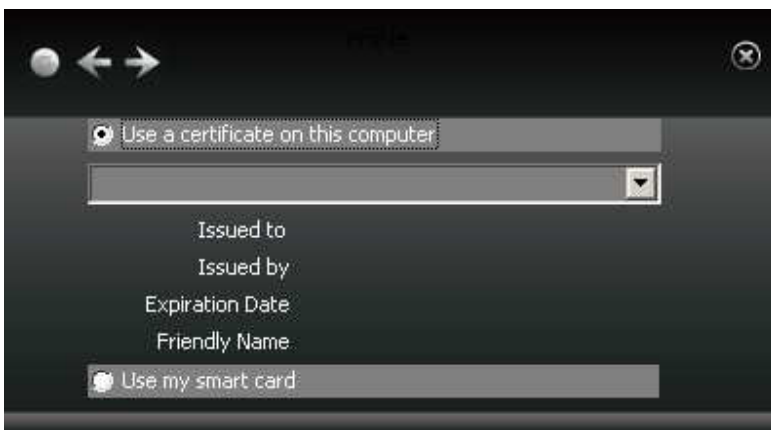
- If you select Generic Token Card, in Tunnel Password/Mode, you can select Static Password or Soft Token and for Vista/Windows 7 users, Windows Logon or Prompt User, depending on the method used to supply user credentials.
- If you select the Static Password option, then in the Tunnel ID field, type your user name, and in the Tunnel Password field, type the password associated with your user name.
- If you select Soft Token, your user credentials are supplied by software.
- If you select Windows Logon, your user credentials are based on those of your Windows user account.
- If you select Prompt User, when connecting to a network, a popup window appears, asking for your user name and password.



- ii. Click the right arrow to save your settings.
- iii. If you have selected PEAP > EAP-MSCHAP v2 or PEAP > Generic Token Card, then optionally select Use Server Certification, and from the drop-down box, select the certificate authority. Click the right arrow to save your settings.



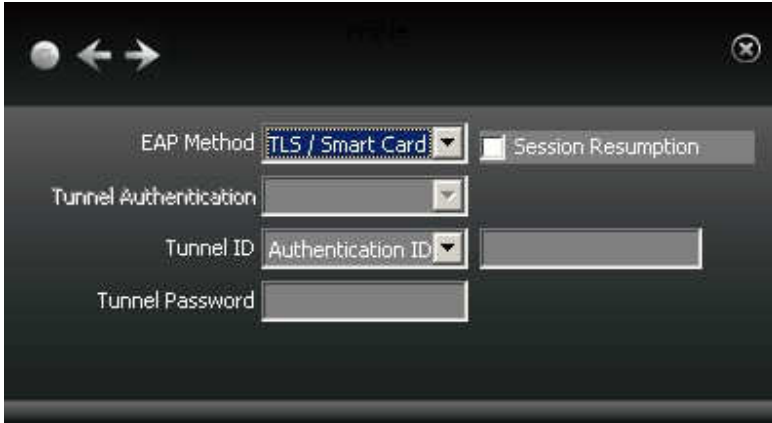
- iv. If you have selected PEAP > EAP-TLS/Smart Card, from the drop-down list, select the client certificate on your computer to be used by this security method, or for Vista and Windows 7 users, select "Use my smart card" to set up smart card-based user authentication. Click the right arrow to save your settings.



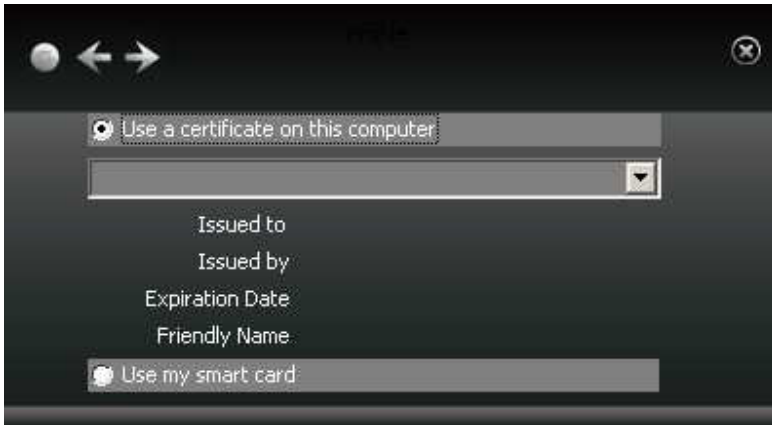
- v. You have completed setup of PEAP authentication.

TLS/Smart Card

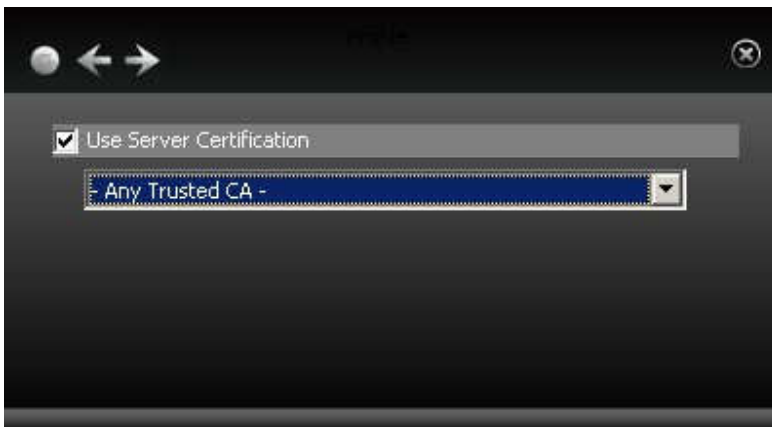
- vi. If you select TLS/Smart Card, select Authentication ID or Machine ID depending on whether user credentials are provided by a smart card or by the computer from which they are accessing the network. If Authentication ID is selected, in the adjacent field, type your user name. Click the right arrow to save your settings.



- vii. From the drop-down list, select the client certificate on your computer to be used by this security method, or for Vista and Windows 7 users, select "Use my smart card" to set up smart card-based user authentication. Click the right arrow to save your settings.



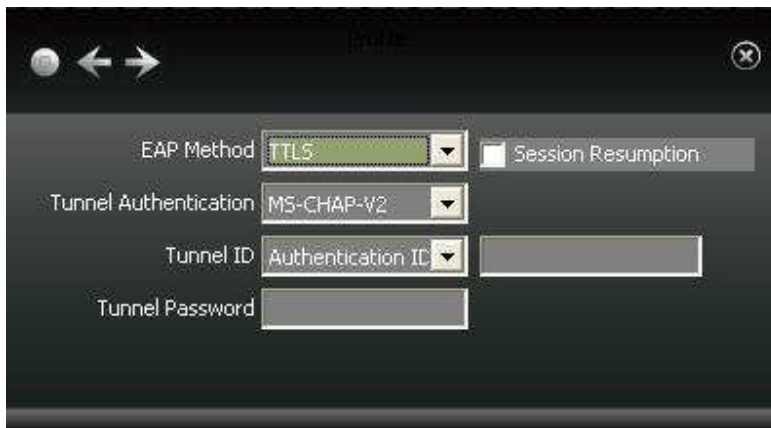
- viii. Optionally select Use Server Certification, and from the drop-down box, select the certificate authority. Click the right arrow to save your settings.



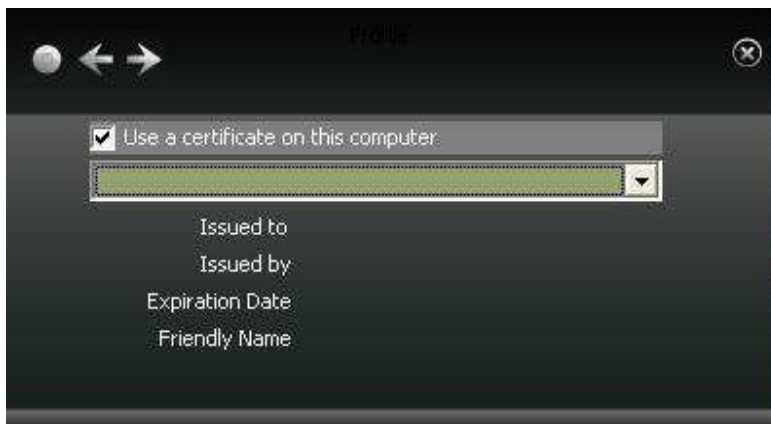
- ix. You have completed setup of TLS/Smart Card authentication.

TTLS (Windows XP only)

- x. For Windows XP users only. To apply TTLS, select a Tunnel Authentication method from the drop-down list. Options include CHAP, MS-CHAP, MS-CHAP v2, PAP, and EAP-MD5. For Tunnel ID, select Authentication ID or Machine ID depending on whether user credentials are provided by the user or by the computer from which they are accessing the network. If Authentication ID is selected, in the adjacent field, type your user name. For either Authentication ID or Machine ID, in the Tunnel Password field, type a password. Click the right arrow to save your settings.



- xi. From the drop-down list, optionally select the client certificate on your computer to be used by this security method, and click the right arrow to save your settings.



- xii. Next, optionally select 'Use Server Certification'. From the drop-down box, select the certificate authority. Click the right arrow to save your settings.



xiii. You have completed setup of TTLS authentication.

EAP-FAST

- xiv. If you are applying EAP-FAST authentication using Vista or Windows 7, click the right arrow to finish setting up EAP-FAST.
- xv. Otherwise, for Windows XP users only, select a Tunnel Authentication method from the drop-down list. Options include EAP-MS-CHAP v2, EAP-TLS/Smart Card, and Generic Token Card.
- If you select EAP-MSCHAP v2, for 'Tunnel ID', select Authentication ID or Machine ID depending on whether user credentials are provided by users or by the computer from which they are accessing the network. If Authentication ID is selected, in the adjacent field, type your user name. If either Authentication ID or Machine ID are selected, for Tunnel Password, type the associated password.



- If you select EAP-TLS/Smart Card, for 'Tunnel ID', select Authentication ID or Machine ID depending on whether user credentials are provided by a smart card or by the computer from which they are accessing the network. If Authentication ID is selected, in the adjacent field, type your user name.



- If you select Generic Token Card, for 'Tunnel ID', field requirements depend on the tunnel mode and identification method selected.
 - If 'Static Password' is selected for Tunnel Mode, and either Authentication ID or Machine ID are selected, type a password. For Authentication ID a user name is also required in the adjacent field.
 - If 'Soft Token' is selected for Tunnel Mode, no further settings are required.

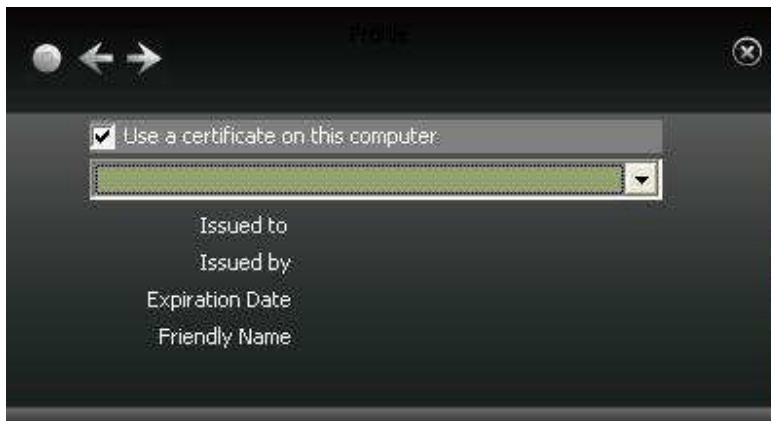


Click the right arrow to save your settings.

- xvi. For Windows XP users only, select 'Allow unauthenticated provision mode' to allow the allocation of PAC (protected authentication credentials) from the authentication server without authentication by users. Select 'Use protected authentication credential' to manually import a PAC. Click the right arrow to save your settings.



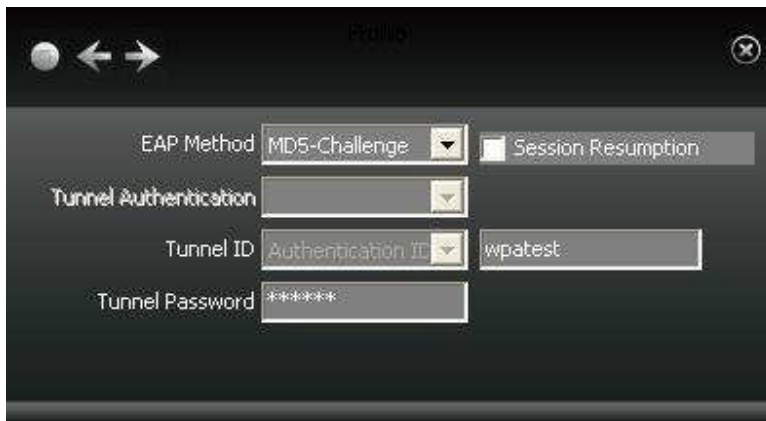
- xvii. For Windows XP users only, if you selected EAP-TLS/Smart Card as the tunnel authentication method, from the drop-down list select a security certificate on your computer. Click the right arrow to save your settings.



- xviii. For Windows XP, Vista and Windows 7, the Utility supports automatic login using your EAP-FAST settings on Windows startup. Select 'Use Pre-logon Connection' to enable this function. Click the right arrow to save your settings.
- xix. You have completed setup of EAP-FAST authentication.

MD5-Challenge (Windows XP, 802.1X only)

- xx. MD5-Challenge is available in Windows XP only. To apply MD5-Challenge, you need to have selected 802.1X as the security method. Type the Tunnel ID and Tunnel Password, and click the right arrow to save your settings.



- xxi. In the screen that appears select a Key and Key Format setting supported by the wireless router or AP to which you are connecting.
- If you select 'Hex(10 or 26 hex digits)', in the WEP Key field type a security key 10 or 26 characters long made up of digits '0'-'9' and letters 'A'-'F'.
 - If you select 'ASCII(5 or 13 ASCII characters)' in the WEP Key field, type a security key 5 or 13 characters long made up of digits '0'-'9' and letters 'a'-'z' and 'A'-'Z'.



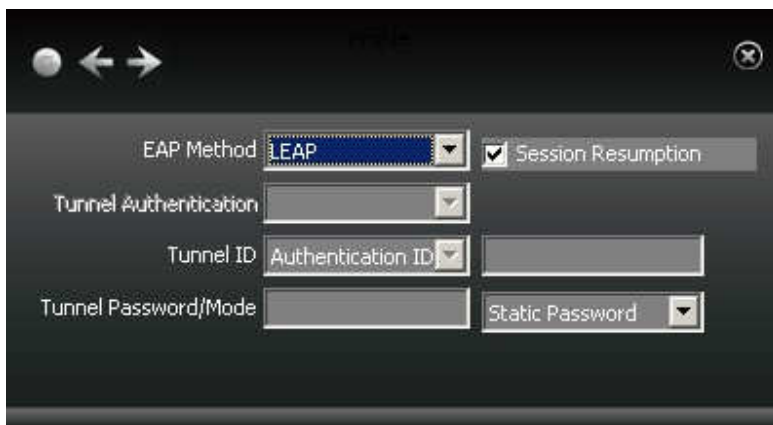
- xxii. Click the right arrow to save your settings and finish setting up MD5-Challenge authentication.



LEAP

- xxiii. For Windows XP users, to apply LEAP, in the Tunnel ID field, select Authentication ID or Machine ID depending on whether user credentials are provided by users or by the computer from which they are accessing the network. If Authentication ID is selected, in the adjacent field, type the user name. For both Authentication ID and Machine ID, type a password for the user.



- xxiv. For Windows Vista and 7 users, for Tunnel Mode, you can select Static Password, Windows Logon or Prompt User, depending on the method used to supply user credentials.
 - o If you select the Static Password option, then in the Tunnel ID field, type your user name, and in the Tunnel Password field, type the password associated with your user name.
 - o If you select Windows Logon, your user credentials are based on those of your Windows user account.
 - o If you select Prompt User, when connecting to a network, a popup window appears, asking for your user name and password.



- xxv. Click the right arrow to save your settings.
- xxvi. The Utility supports automatic login using your LEAP settings on Windows startup. Select 'Use Pre-logon Connection' to enable this function. Click the right arrow to save your settings.
- xxvii. You have completed setup of LEAP authentication.
 2. After you have set up security settings, a profile configured with your security settings appears in the Profile screen. To edit settings, click the Edit button , or to delete settings, click the delete button .

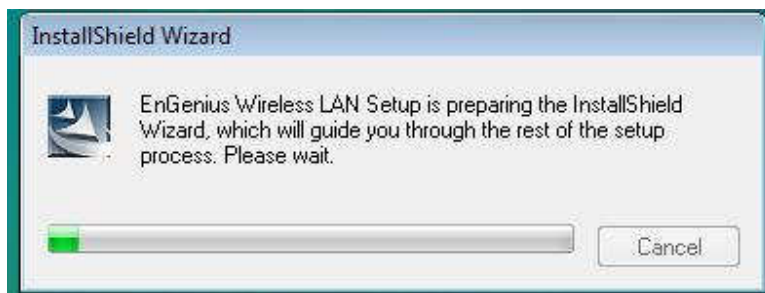
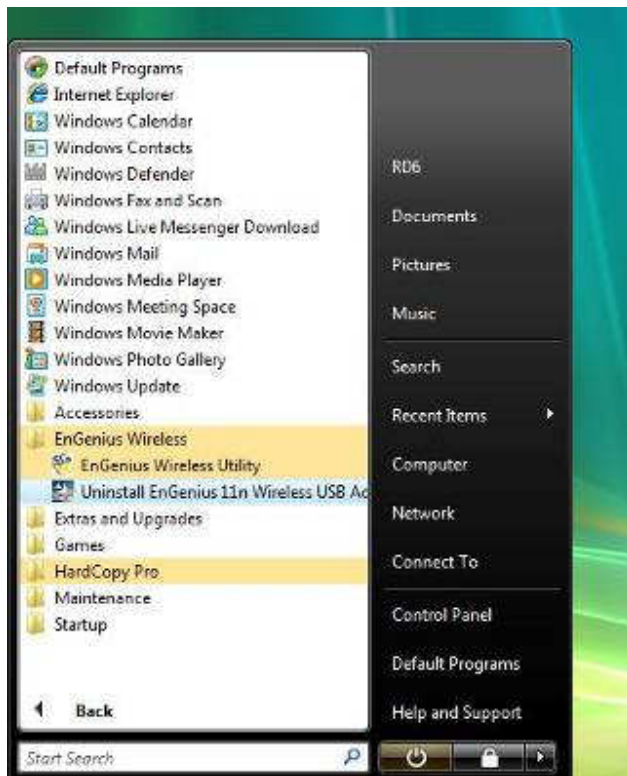


4 Uninstall the Drivers & Client Utility

If the USB client adapter installation is unsuccessful for any reason, the best way to solve the problem may be to completely uninstall the USB adapter and its utility and repeat the installation procedure again.

Follow the steps below in order to uninstall the client utility:

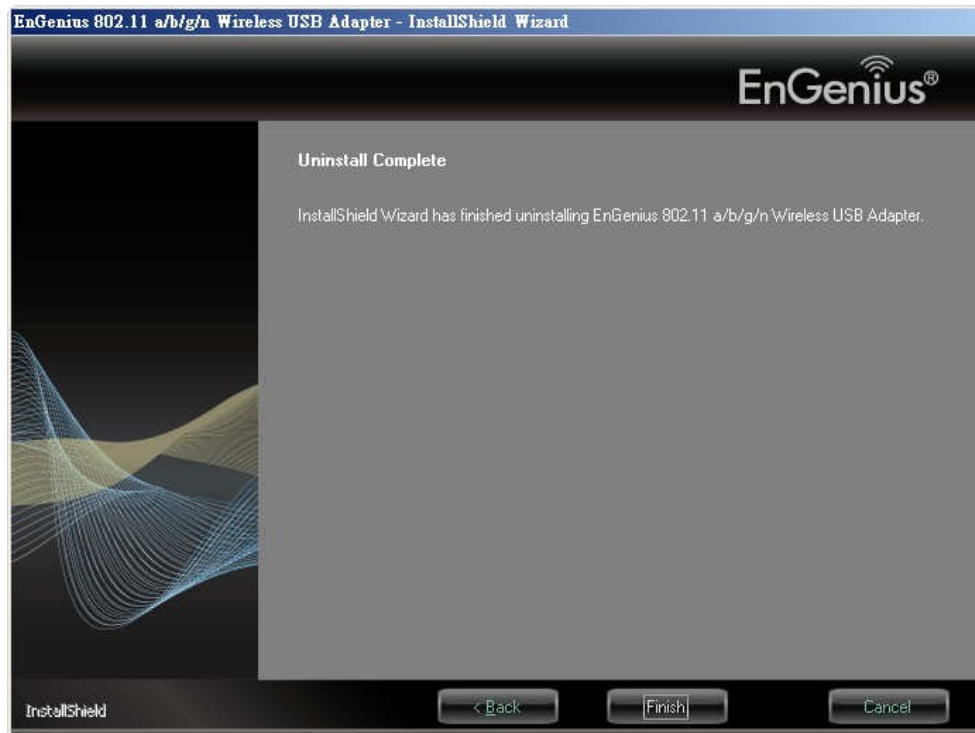
1. Click on **Start > EnGenius Wireless > Uninstall EnGenius Wireless USB Adapter**



2. The un-installation process will then begin.



3. Click on the **Yes** button to confirm the un-installation process and then click on the **Next** button.



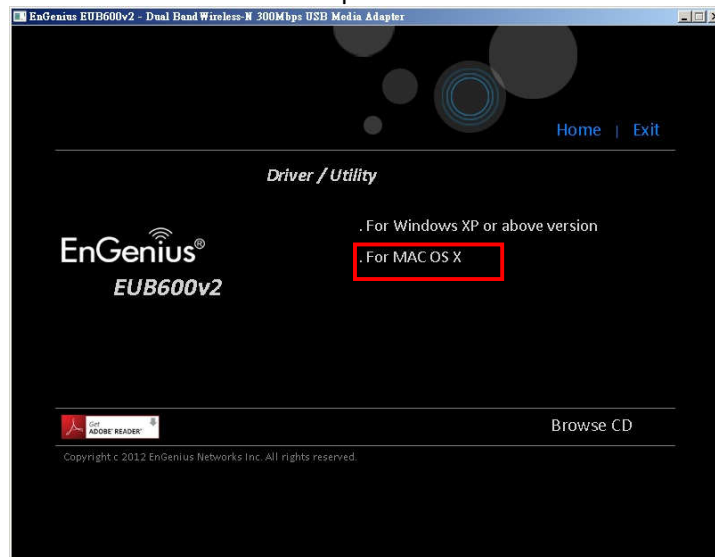
4. The un-installation process is complete. Select **Yes, I want to restart my computer now** radio button and then click on the Finish button. Then remove the USB adapter.

5 USB Adapter for MAC OS X

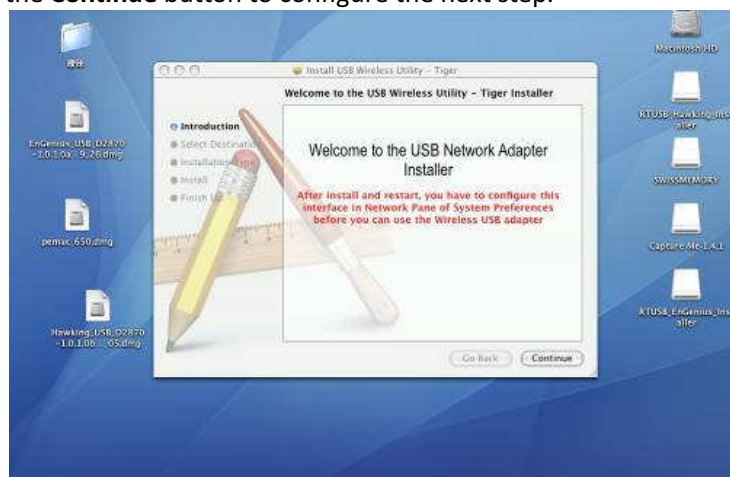
Installing the Drivers

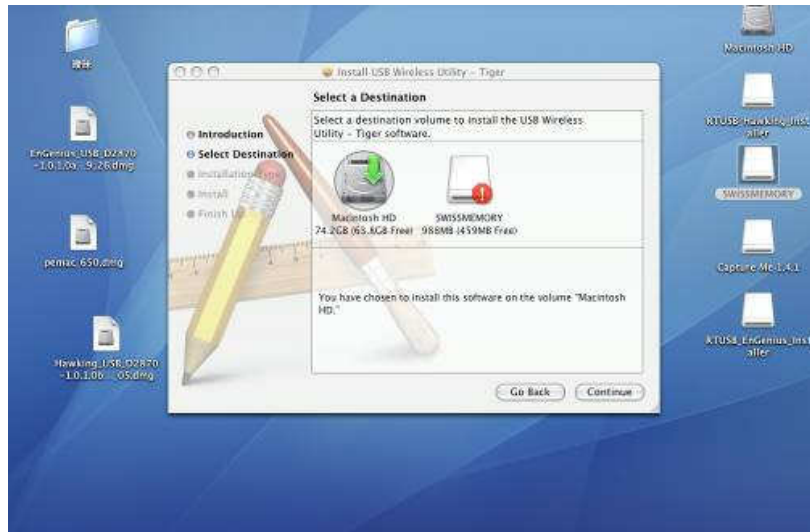
Follow the steps below in order to install the USB adapter drivers:

1. Insert the CD-ROM that was provided to you in this package. The setup should run automatically. If the setup does not run automatically, then you must manually select the **Autorun.exe** file from the CD-ROM drive.
2. Click on Driver / Utility to go to the Driver page.
3. Click **For MAC OS X** to start the install process.

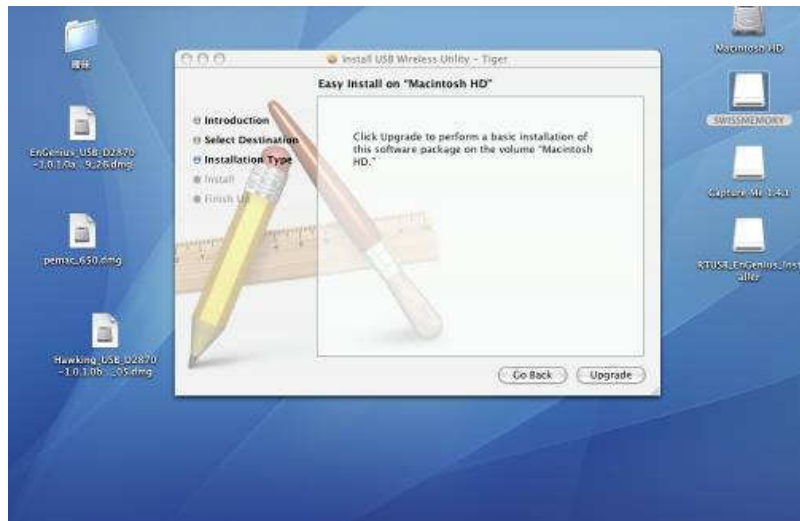


4. Click on the **Continue** button to configure the next step.

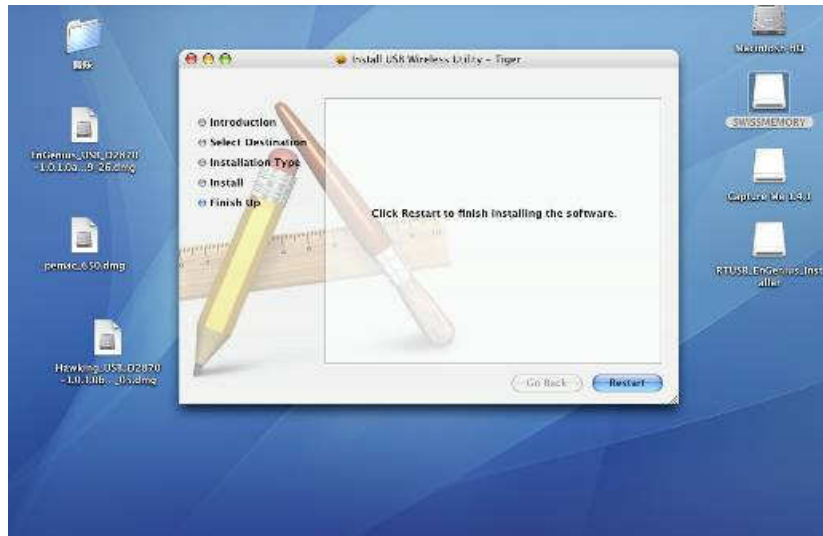




5. Select the **Macintosh HD** and then click on the **Continue** button.



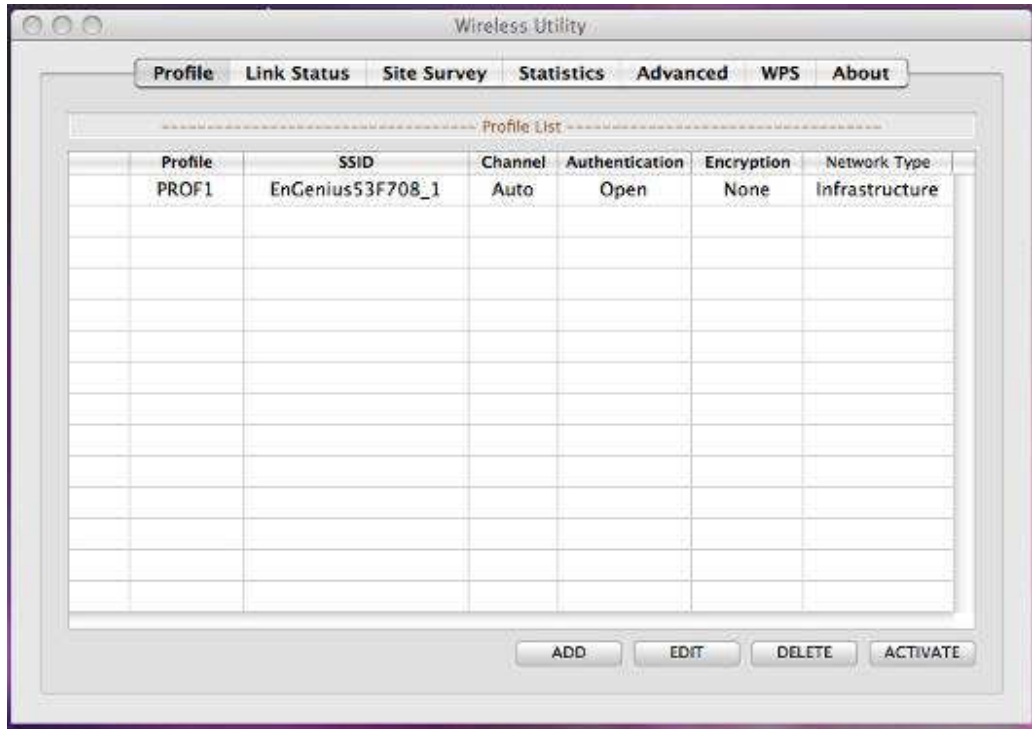
6. Click on the **Continue** button to configure the next step.



7. The installation is complete. Click on the **Restart** button.
8. Carefully insert the USB adapter into the USB port. MAC OS X will then detect and install the new hardware.
9. The Client Utility is installed in the **Applications** folder.

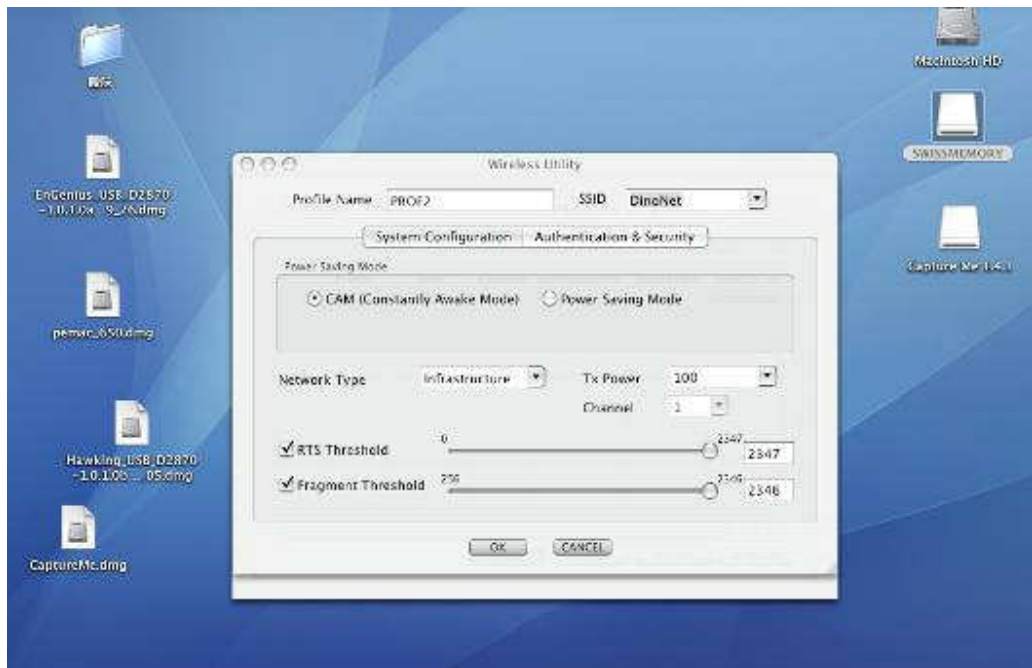
Profiles

The **Profile** tab is used to store the settings of multiple Access Points such as home, office, café, etc. When adding a profile you are required to enter a profile name and SSID as well as configure the power-saving mode, network type, RTS/fragmentation threshold and encryption/authentication settings. A profile can be configured as **Infrastructure** or **Ad-hoc** mode. The configuration settings for each mode are described below.



Infrastructure Mode

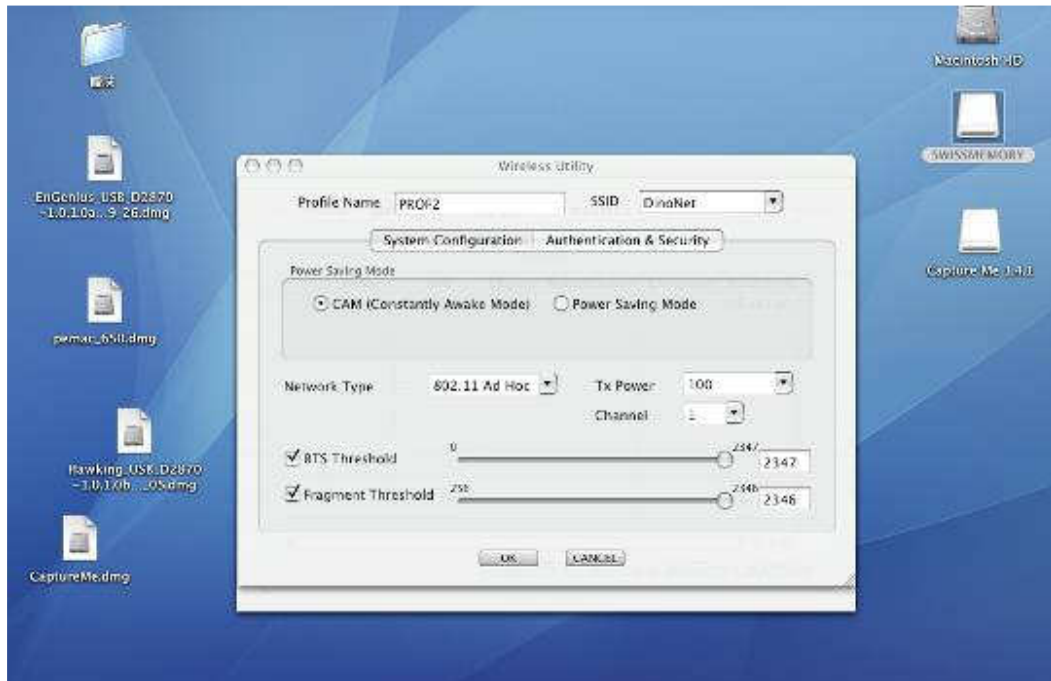
The infrastructure mode requires the use of an Access Point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations.



- **Profile:** Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID:** Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **PSM:** Select a power saving mode (PSM) option.
 - **CAM (Continuously Active Mode):** Select this option if your notebook is always connected to the power supply.
 - **PSM (Power Saving Mode):** Select this option if your notebook uses its battery power. This option minimizes the battery usage while the network is idle.
- **Network Type:** Select **Infrastructure** from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100%** or **auto**, if not, select one of the lower values for power saving.
- **RTS Threshold:** Place a check in this box if you would like to enable RTS Threshold. Any packet larger than the specified value (bytes) will send RTS/CTS handshake packet.
- **Fragment Threshold:** Place a check in this box if you would like to enable Fragment Threshold. Any packet larger than the specified value (bytes) will be fragmented.
- Click on the **OK** button to save the changes.

Ad-hoc Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network.



- **Profile:** Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID:** Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **Network Type:** Select **Ad-hoc** from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100%** or **auto**, if not, select one of the lower values for power saving.
- **Ad-hoc wireless mode:** Select a wireless mode from the drop-down list depending on the type of stations used in the ad-hoc network. Select MIX options if the network consists of 11a, 11b, 11g or 11n stations. Select ONLY options if the network consists of a specified type of wireless mode. For instance, if you are using 11N only AP, please select 11N.
- **RTS Threshold:** Place a check in this box if you would like to enable RTS Threshold. Any packet larger than the specified value (bytes) will send RTS/CTS handshake packet.
- **Fragment Threshold:** Place a check in this box if you would like to enable Fragment Threshold. Any packet larger than the specified value (bytes) will be

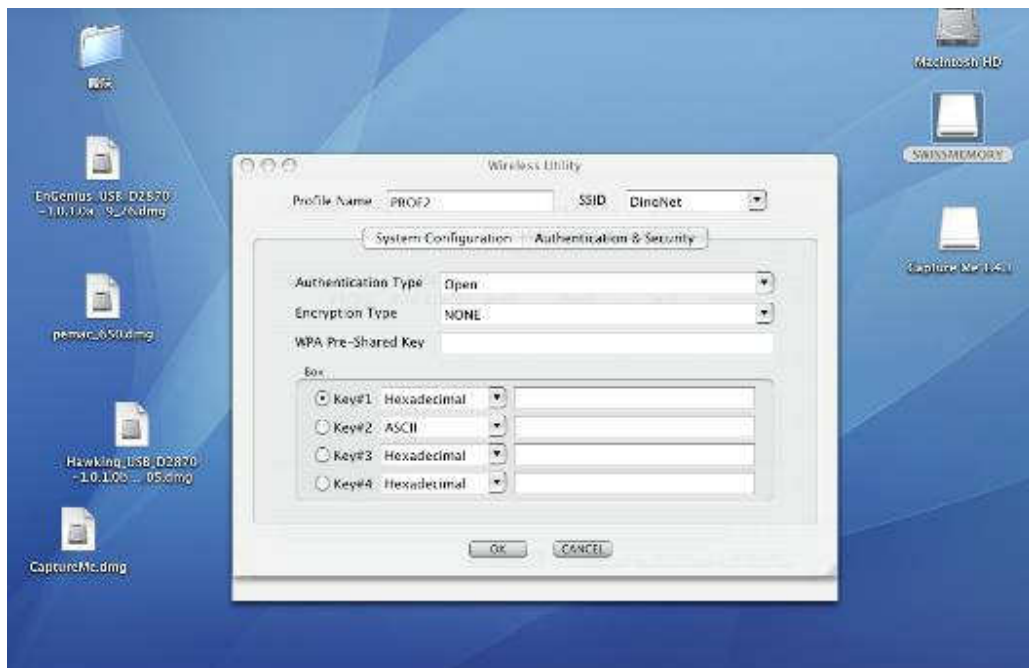
- fragmented.
- Click on the **OK** button to save the changes.

Authentication and Security

The **Security** tab allows you to configure the authentication and encryption settings such as: WEP, WPA-PSK, WPA2-PSK and 802.1x. Each security option is described in detail below.

WEP Encryption

The **WEP** tab displays the WEP settings. Encryption is designed to make the data transmission more secure. You may select 64 or 128-bit WEP (Wired Equivalent Privacy) key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase. The following information is included in this tab, as the image depicts below.

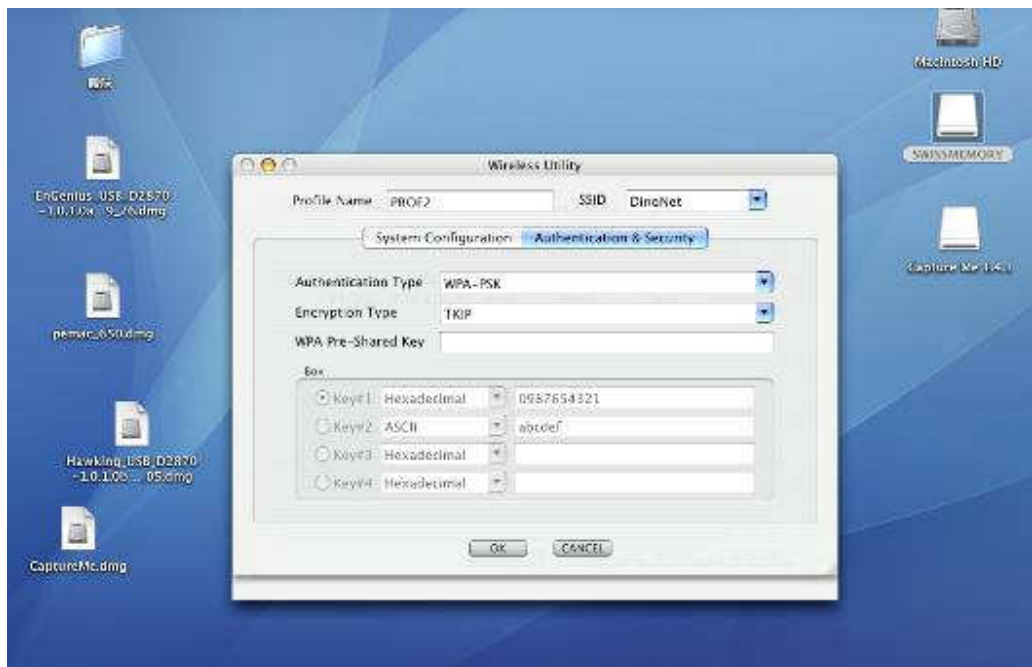


- **Authentication Type:** Select **Open** or **Shared** from the drop-down list.
- **Encryption:** Select WEP from the drop-down list.
- **WEP Key:** Type a character string into the field. For 64-bit enter 5 alphanumeric or 10 hexadecimal characters. For 128-bit enter 13 alphanumeric or 26 hexadecimal characters.
- Click on the **OK** button to save the changes.

- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

WPA-PSK & WPA2-PSK Authentication & TKIP, AES Encryption

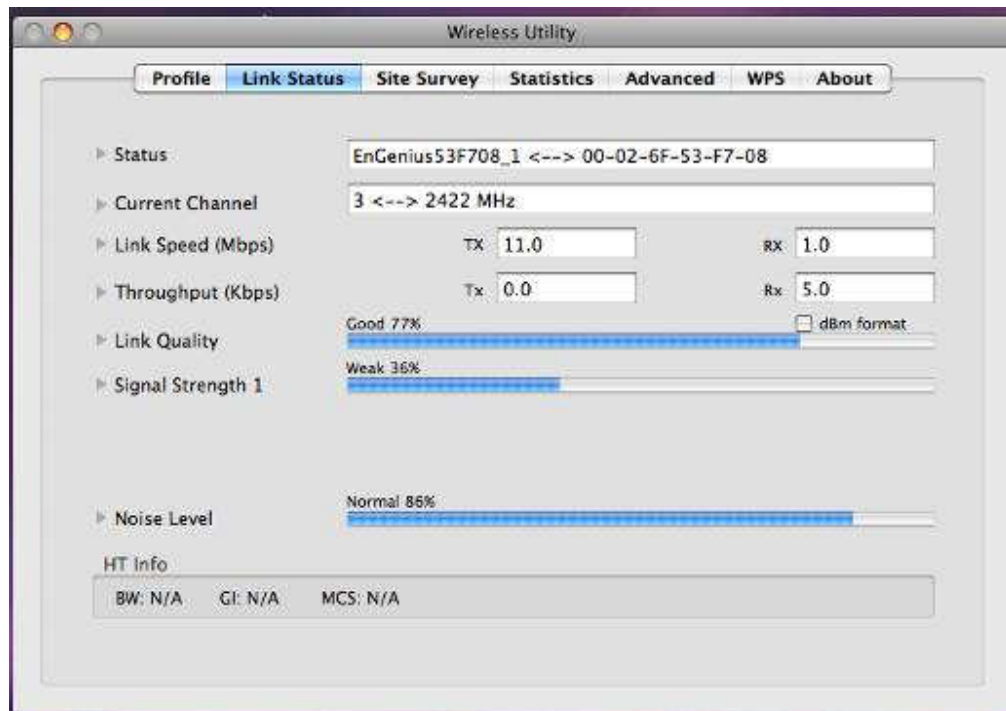
WPA – PSK (Pre-shared Key) is used in a Pre Shared Key mode that does not require an authentication server. Access to the Internet and the rest of the wireless network services is allowed only if the pre-shared key of the computer matches that of the Access Point. This approach offers the simplicity of the WEP key, but uses stronger TKIP encryption. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.



- **Authentication Type:** Select **WPA** or **WPA2** from the drop-down list.
- **Encryption:** Select **TKIP** or **AES** from the drop-down list.
- **WPA Preshared key:** Enter a pass phrase which is between 8 and 32 characters long.
- Click on the **OK** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

Link Status

The **Link Status** tab displays the current status of the wireless radio. The following information is included in this tab, as the image depicts below.

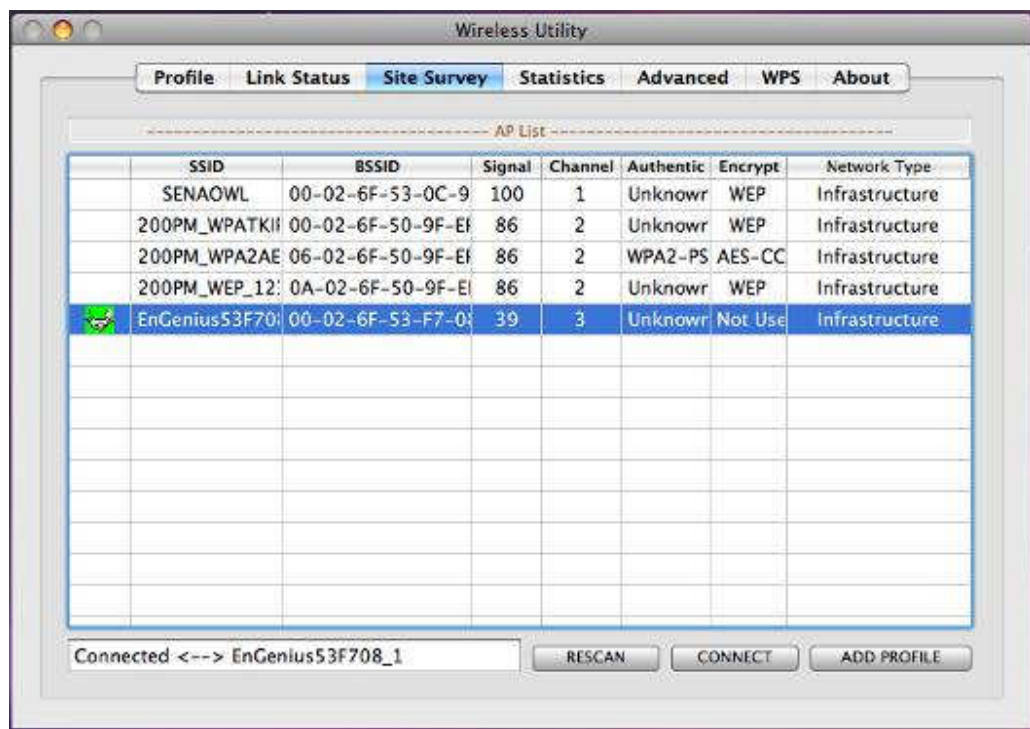


- **Status:** This indicates the state of the client. There are three options:
 - **Associated:** Indicates that the wireless client is connected to an Access Point (AP). The BSSID is shown in the form of 12 HEX digits, which is the MAC address of the AP.
 - **Scanning:** Indicates that the wireless client is searching for an AP in the area.
 - **Disconnected:** Indicates that there are no APs or clients in the area.
- **Current Channel:** The operating frequency channel that the client is using (infrastructure mode).
- **Link Speed:** The current rate at which the client is transmitting and receiving.
- **Throughput (bytes/sec):** Displays the Tx (transmit) and Rx (receive) kilo-bytes per second.
- **Link Quality:** In infrastructure mode, this bar displays the transmission quality between an AP and a client. In Ad-hoc mode, this bar displays the transmission quality between one client, and another.
- **Signal Strength:** This bar displays the strength of the signal received from an AP or client.
- **Noise Level:** Displays the background noise level; a lower level indicates less interference.
- **HT: High Through-Put / 802.11 n Section**
- **BW: Channel Bandwidth**

- **GI:** Guard Interval
- **MCS:** Modulation Coding Scheme
- **dBm Check Box.** When you click on the check box as the drawing below. The signal strength and noise level will be shown as the dBm measurements.

Site Survey

The **Site Survey** tab displays a list of Access Points and Stations in the area, and allows you to connect to a specific one. The following information is included in this tab, as the image depicts below.

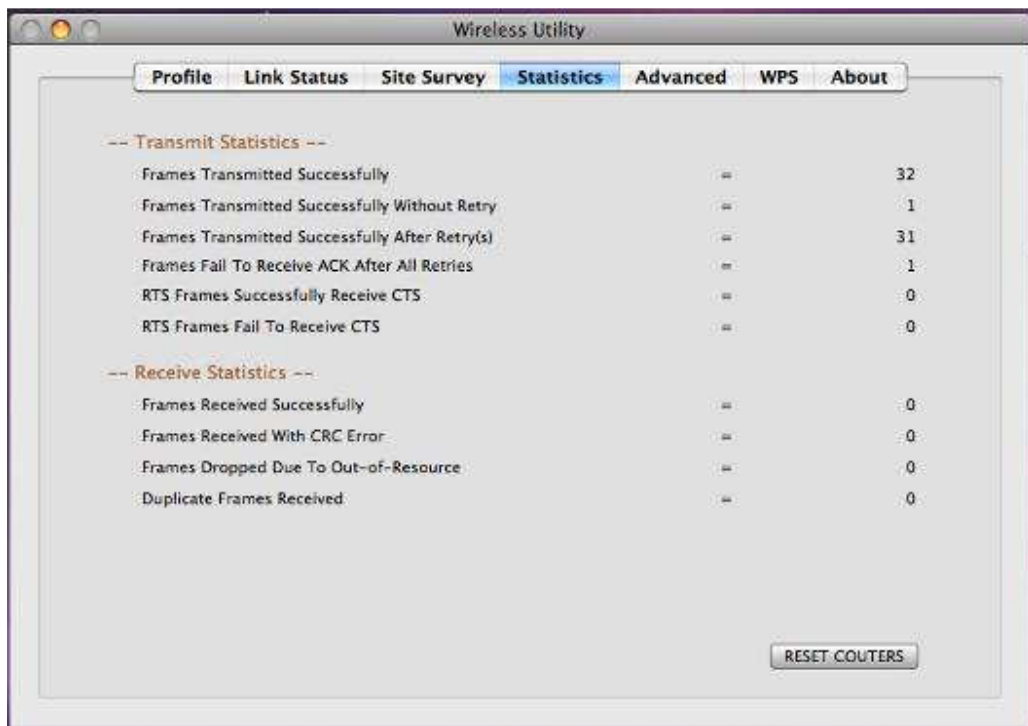


- **SSID:** Displays the SSID of the Access Point. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **BSSID:** Displays the MAC address of the Access Point.
- **Signal:** Displays the receiving signal strength from the Access Point.
- **Channel:** Displays the channel number of the Access Point.
- **Authentication:** displays the authentication on the Access Point, this includes WPA, WPA-PSK, WPA2, or Unknown.
- **Encryption:** Displays the encryption on the Access Point, this includes WEP, TKIP, AES or None.
- **Network Type:** Indicates whether the SSID is a Station (Ad-hoc) or Access Point (Infrastructure).
- **Rescan:** Click on this button to view a list of Access Points in the area.
- **Connect:** to connect with a specific Access Point, select the SSID from the list, and then click on the **Connect** button.

- **Add Profile:** Click on this button to add the SSID and its associated settings into a profile.
- Click on the **OK** button if you have made any changes.

Statistics

The **Statistics** tab displays transmit and receive packet statistics in real-time. Information included is frames transmitted/received successfully, transmitted successfully without and after retry, received with CRC error, duplicate frames received, etc.

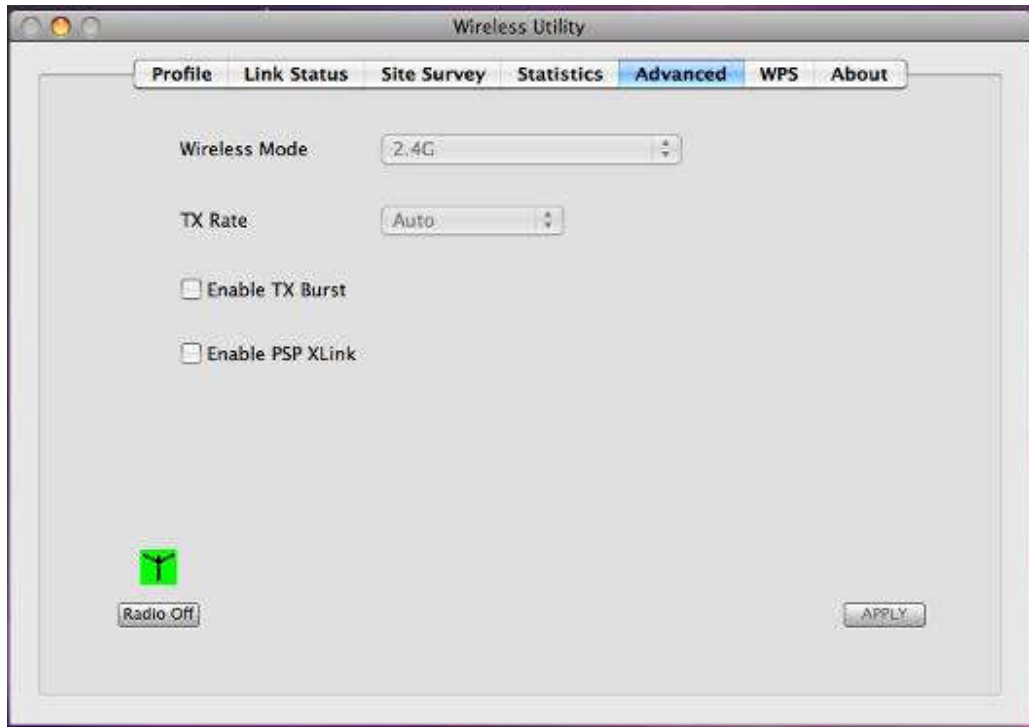


-- Transmit Statistics --		
Frames Transmitted Successfully	=	32
Frames Transmitted Successfully Without Retry	=	1
Frames Transmitted Successfully After Retry(s)	=	31
Frames Fail To Receive ACK After All Retries	=	1
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0
-- Receive Statistics --		
Frames Received Successfully	=	0
Frames Received With CRC Error	=	0
Frames Dropped Due To Out-of-Resource	=	0
Duplicate Frames Received	=	0

RESET COUNTERS

Advanced Configuration

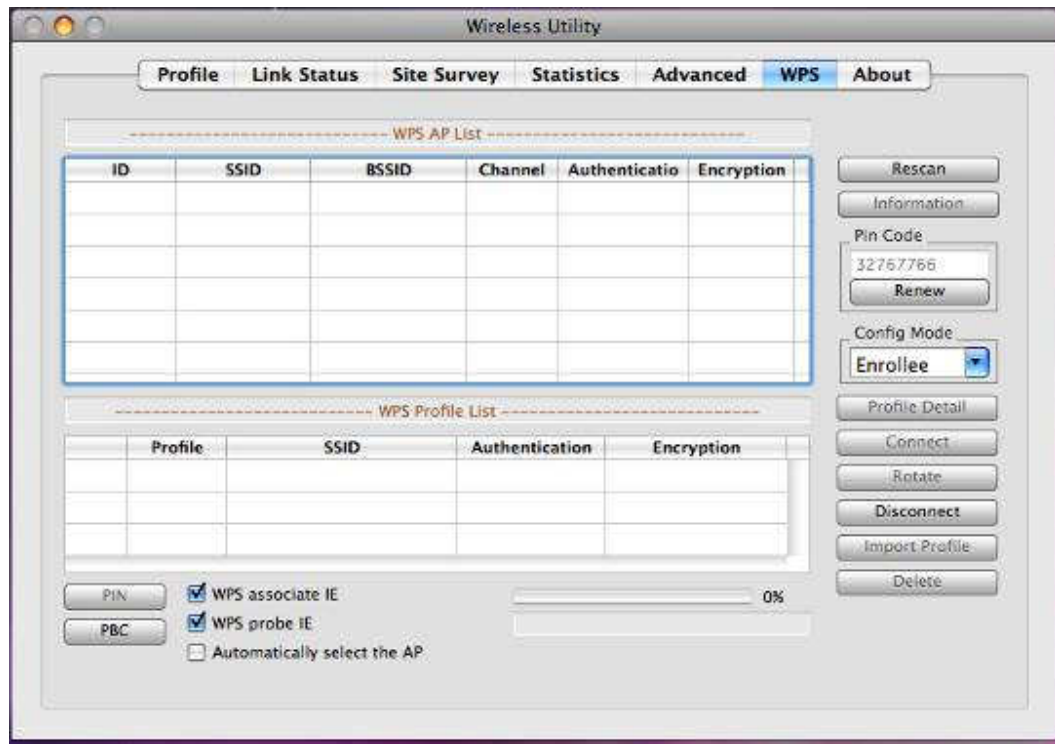
The **Advanced** tab is used to configure advanced wireless settings.



- **Wireless mode:** Select 802.11 2.4GHz, 5GHz and 2.4+5GHz.
- **Tx Rate:** The transmit rate should be set to auto by default.
- **Tx BURST:** Click the check box will enhance the throughput
- Click on the **Apply** button to save the changes.

WPS

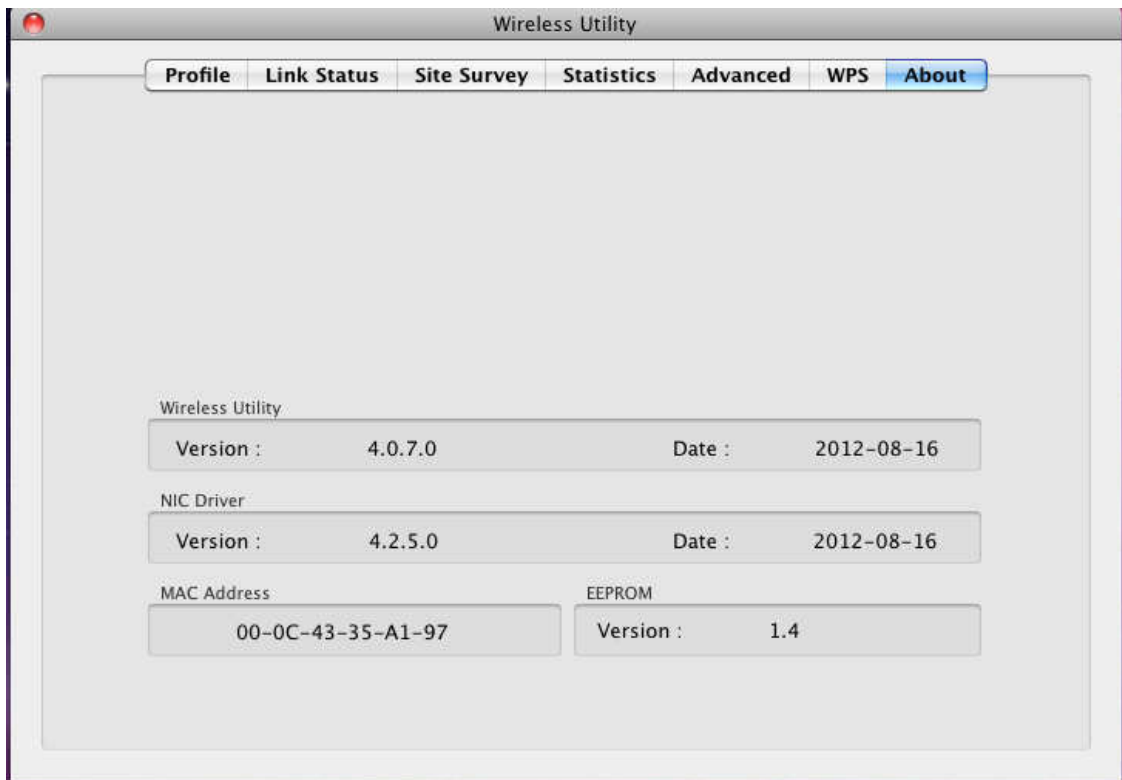
WPS (Wireless Push Button) is used for WiFi Protected Setup. By pressing this button, the security settings of the device will automatically synchronize with other wireless devices on your network that support Wi-Fi Protected Setup.



- **Rescan:** Click on this button to view a list of Access Points in the area.
- **Renew:** Regenerate a new PIN code
- **Config Mode:** switch between Enrollee or Registrar
- **Profile Detail:** show profile of the selected party
- **Connect:** Click on the AP to start WPS connection with the AP
- **Disconnect:** Click to terminate WPS connection
- **Import Profile:** Load pre-stored profile database
- **Delete:** Remove the selected item

About

The **About** tab displays information about the device, such as: the network driver version and date, configuration utility version and date, and the NIC (Network Interface Card) firmware version and date.



Appendix A – Glossary

8

802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

A

Access Control List

ACL. This is a database of network devices that are allowed to access resources on the network.

Access Point

AP. Device that allows wireless clients to connect to it and access the network

ActiveX

A Microsoft specification for the interaction of software components.

Address Resolution Protocol

ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

Ad-hoc network

Peer-to-Peer network between wireless clients

ADSL

Asymmetric Digital Subscriber Line

Advanced Encryption Standard

AES. Government encryption standard

Alphanumeric

Characters A-Z and 0-9

Antenna

Used to transmit and receive RF signals.

AppleTalk

A set of Local Area Network protocols developed by Apple for their computer systems

AppleTalk Address Resolution Protocol

AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

Application layer

7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

ASCII

American Standard Code for Information Interchange. This system of characters is most commonly used for text files

Attenuation

The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication

To provide credentials, like a Password, in order to verify that the person or device is really who

they are claiming to be

Automatic Private IP Addressing

APIPA. An IP address that that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

B

Backward Compatible

The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

Bandwidth

The maximum amount of bytes or bits per second that can be transmitted to and from a network device

Basic Input/Output System

BIOS. A program that the processor of a computer uses to startup the system once it is turned on

Baud

Data transmission speed

Beacon

A data frame by which one of the stations in a Wi-Fi network periodically broadcasts network control data to other wireless stations.

Bit rate

The amount of bits that pass in given amount of time

Bit/sec

Bits per second

BOOTP

Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

Bottleneck

A time during processes when something causes the process to slowdown or stop all together

Broadband

A wide band of frequencies available for transmitting data

Broadcast

Transmitting data in all directions at once

Browser

A program that allows you to access resources on the web and provides them to you graphically

C

Cable modem

A device that allows you to connect a computer up to a coaxial cable and receive Internet access from your Cable provider

CardBus

A newer version of the PC Card or PCMCIA interface. It supports a 32-bit data path, DMA, and consumes less voltage

CAT 5

Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

Client

A program or user that requests data from a server

Collision

When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie

Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

D

Data

Information that has been translated into binary so that it can be processed or moved to another device

Data Encryption Standard

Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged

Database

Organizes information so that it can be managed updated, as well as easily accessed by users or applications.

Data-Link layer

The second layer of the OSI model. Controls the movement of data on the physical link of a network

DB-25

A 25 pin male connector for attaching External modems or RS-232 serial devices

DB-9

A 9 pin connector for RS-232 connections

dBd

Decibels related to dipole antenna

dB_i

Decibels relative to isotropic radiator

dBm

Decibels relative to one milliwatt

Decrypt

To unscramble an encrypted message back into plain text

Default

A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

Demilitarized zone

DMZ: A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

DHCP

Dynamic Host Configuration Protocol: Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that request them

Digital certificate:

An electronic method of providing credentials to a server in order to have access to it or a network

Direct Sequence Spread Spectrum

DSSS: Modulation technique used by 802.11b wireless devices

DMZ

"Demilitarized Zone". A computer that logically sits in a "no-mans land" between the LAN and the WAN. The DMZ computer trades some of the protection of the router's security mechanisms for the convenience of being directly addressable from the Internet.

DNS

Domain Name System: Translates Domain Names to IP addresses

Domain name

A name that is associated with an IP address

Download

To send a request from one computer to another and have the file transmitted back to the requesting computer

DSL

Digital Subscriber Line. High bandwidth Internet connection over telephone lines

Duplex

Sending and Receiving data transmissions at the same time

Dynamic DNS service

Dynamic DNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always be linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports Dynamic DNS, whenever the IP address changes

Dynamic IP address

IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

E

EAP

Extensible Authentication Protocol

Email

Electronic Mail is a computer-stored message that is transmitted over the Internet

Encryption

Converting data into cyphertext so that it cannot be easily read

Ethernet

The most widely used technology for Local Area Networks.

F

Fiber optic

A way of sending data through light impulses over glass or plastic wire or fiber

File server

A computer on a network that stores data so that the other computers on the network can all access it

File sharing

Allowing data from computers on a network to be accessed by other computers on the network with different levels of access rights

Firewall

A device that protects resources of the Local Area Network from unauthorized users outside of the local network

Firmware

Programming that is inserted into a hardware device that tells it how to function

Fragmentation

Breaking up data into smaller pieces to make it easier to store

FTP

File Transfer Protocol. Easiest way to transfer files between computers on the Internet

Full-duplex

Sending and Receiving data at the same time

G

Gain

The amount an amplifier boosts the wireless signal

Gateway

A device that connects your network to another, like the internet

Gbps

Gigabits per second

Gigabit Ethernet

Transmission technology that provides a data rate of 1 billion bits per second

GUI

Graphical user interface

H

H.323

A standard that provides consistency of voice and video transmissions and compatibility for videoconferencing devices

Half-duplex

Data cannot be transmitted and received at the same time

Hashing

Transforming a string of characters into a shorter string with a predefined length

Hexadecimal

Characters 0-9 and A-F

Hop

The action of data packets being transmitted from one router to another

Host

Computer on a network

HTTP

Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

HTTPS

HTTP over SSL is used to encrypt and decrypt HTTP transmissions

Hub

A networking device that connects multiple devices together

I

ICMP

Internet Control Message Protocol

IEEE

Institute of Electrical and Electronics Engineers

IGMP

Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers

IIS

Internet Information Server is a WEB server and FTP server provided by Microsoft

IKE

Internet Key Exchange is used to ensure security for VPN connections

Infrastructure

In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

Internet

A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

Internet Explorer

A World Wide Web browser created and provided by Microsoft

Internet Protocol

The method of transferring data from one computer to another on the Internet

Internet Protocol Security

IPsec provides security at the packet processing layer of network communication

Internet Service Provider

An ISP provides access to the Internet to individuals or companies

Intranet

A private network

Intrusion Detection

A type of security that scans a network to detect attacks coming from inside and outside of the network

IP

Internet Protocol

IP address

A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

IPsec

Internet Protocol Security

IPX

Internetwork Packet Exchange is a networking protocol developed by Novell to enable their Netware clients and servers to communicate

ISP

Internet Service Provider

J

Java

A programming language used to create programs and applets for web pages

K

Kbps

Kilobits per second

Kbyte

Kilobyte

L

L2TP

Layer 2 Tunneling Protocol

LAN

Local Area Network

Latency

The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

LED

Light Emitting Diode

Legacy

Older devices or technology

Local Area Network

A group of computers in a building that usually access files from a server

LPR/LPD

"Line Printer Requestor"/"Line Printer Daemon". A TCP/IP protocol for transmitting streams of printer data.

M

MAC Address

A unique hardware ID assigned to every Ethernet adapter by the manufacturer.

Mbps

Megabits per second

MDI

Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

MDIX

Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

MIB

Management Information Base is a set of objects that can be managed by using SNMP

Modem

A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

MPPE

Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

MTU

Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet

Multicast

Sending data from one device to many devices on a network

N

NAT

Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

NetBEUI

NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

NetBIOS

Network Basic Input/Output System

Netmask

Determines what portion of an IP address designates the Network and which part designates the Host

Network Interface Card

A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

Network Layer

The third layer of the OSI model which handles the routing of traffic on a network

Network Time Protocol

Used to synchronize the time of all the computers in a network

NIC

Network Interface Card

NTP

Network Time Protocol

O

OFDM

Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

OSI

Open Systems Interconnection is the reference model for how data should travel between two devices on a network

OSPF

Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

P

Password

A sequence of characters that is used to authenticate requests to resources on a network

Personal Area Network

The interconnection of networking devices within a range of 10 meters

Physical layer

The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

Ping

A utility program that verifies that a given Internet address exists and can receive messages. The utility sends a control packet to the given address and waits for a response.

PoE

Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

POP3

Post Office Protocol 3 is used for receiving email

Port

A logical channel endpoint in a network. A computer might have only one physical channel (its Ethernet channel) but can have multiple ports (logical channels) each identified by a number.

PPP

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

PPPoE

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

PPTP

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

Preamble

Used to synchronize communication timing between devices on a network

Q

QoS

Quality of Service

R

RADIUS

Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

Reboot

To restart a computer and reload its operating software or firmware from nonvolatile storage.

Rendezvous

Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

Repeater

Retransmits the signal of an Access Point in order to extend its coverage

RIP

Routing Information Protocol is used to synchronize the routing table of all the routers on a network

RJ-11

The most commonly used connection method for telephones

RJ-45

The most commonly used connection method for Ethernet

RS-232C

The interface for serial communication between computers and other related devices

RSA

Algorithm used for encryption and authentication

S

Server

A computer on a network that provides services and resources to other computers on the network

Session key

An encryption and decryption key that is generated for every communication session between two computers

Session layer

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

Simple Mail Transfer Protocol

Used for sending and receiving email

Simple Network Management Protocol

Governs the management and monitoring of network devices

SIP

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SOHO

Small Office/Home Office

SPI

Stateful Packet Inspection

SSH

Secure Shell is a command line interface that allows for secure connections to remote computers

SSID

Service Set Identifier is a name for a wireless network

Stateful inspection

A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass through the firewall

Subnet mask

Determines what portion of an IP address designates the Network and which part designates the Host

Syslog

System Logger -- a distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

T

TCP

Transmission Control Protocol

TCP Raw

A TCP/IP protocol for transmitting streams of printer data.

TCP/IP

Transmission Control Protocol/Internet Protocol

TFTP

Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

Throughput

The amount of data that can be transferred in a given time period

Traceroute

A utility displays the routes between you computer and specific destination

U

UDP

User Datagram Protocol

Unicast

Communication between a single sender and receiver

Universal Plug and Play

A standard that allows network devices to discover each other and configure themselves to be a part of the network

Upgrade

To install a more recent version of a software or firmware product

Upload

To send a request from one computer to another and have a file transmitted from the requesting computer to the other

UPnP

Universal Plug and Play

URL

Uniform Resource Locator is a unique address for files accessible on the Internet

USB

Universal Serial Bus

UTP

Unshielded Twisted Pair

V

Virtual Private Network

VPN: A secure tunnel over the Internet to connect remote offices or users to their company's network

VLAN

Virtual LAN

Voice over IP

Sending voice information over the Internet as opposed to the PSTN

VoIP

Voice over IP

W

Wake on LAN

Allows you to power up a computer through its Network Interface Card

WAN

Wide Area Network

WCN

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

WDS

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

Web browser

A utility that allows you to view content and interact with all of the information on the World Wide Web

WEP

Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

Wide Area Network

The larger network that your LAN is connected to, which may be the Internet itself, or a regional or corporate network

Wi-Fi

Wireless Fidelity

Wi-Fi Protected Access

An updated version of security for wireless networks that provides authentication as well as encryption

Wireless ISP

A company that provides a broadband Internet connection over a wireless connection

Wireless LAN

Connecting to a Local Area Network over one of the 802.11 wireless standards

WISP

Wireless Internet Service Provider

WLAN

Wireless Local Area Network

WPA

Wi-Fi Protected Access. A Wi-Fi security enhancement that provides improved data encryption, relative to WEP.

X

xDSL

A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

Y

Yagi antenna

A directional antenna used to concentrate wireless signals on a specific location

Appendix 2 – How to Set WPS

WPS setting supports two modes :PBC and PIN. The detailed setting steps are as follows:

1. Wireless Connection in PBC Mode

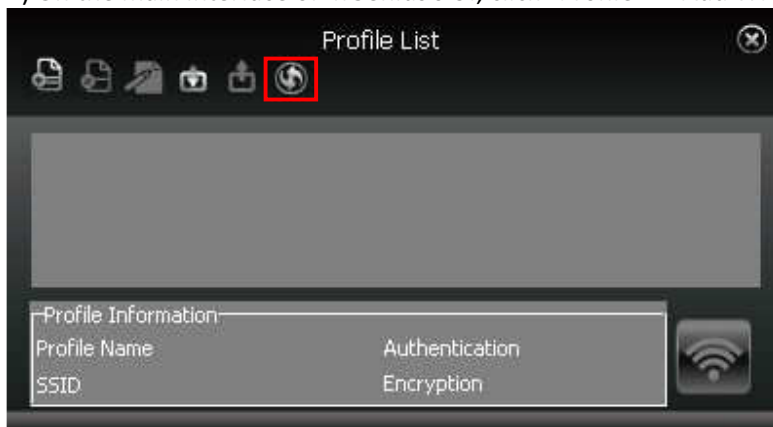
1.1 Enable the router's WPS-PBC feature.

If your router provides WPS button, just press and hold it for about 1 second, then the WPS LED will be flashing for about 2 minutes, which indicates the router's WPS feature has been enabled. Otherwise, you can also log on to the router's web-based utility to enable the PBC mode in WPS settings screen(For detailed settings, please refer to your router's user guide).



1.2 Perform PBC connection on the UI of the wireless adapter

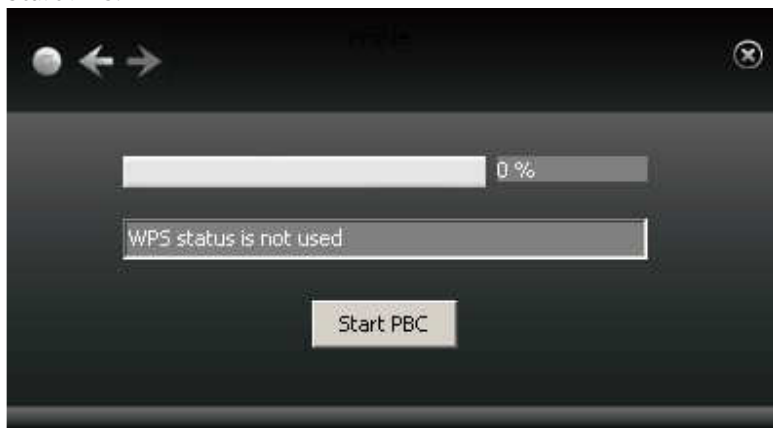
1) On the main interface of EnGenius's UI, click "Profile"—"Add WPS Profile".



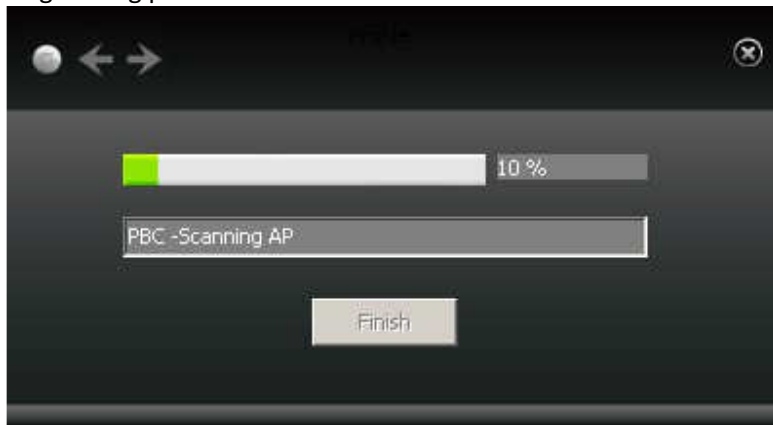
2) On the Profile screen, select "Push-Button Configuration"(PBC) and then click the "Next" button, select "Start PBC" two minutes after the router enables the WPS function. The connection is established when the negotiating process finishes.



Start PBC:



Negotiating process:



A profile forms automatically after the connection is successfully established.



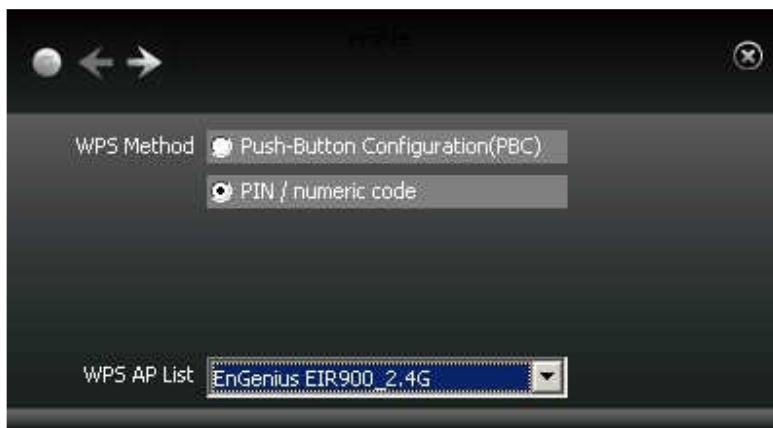
1.3 Using the wireless adapter's WPS button to perform PBC connection.

If your wireless adapter provides a WPS button, you may use the button to perform PBC connection.

- a). Run the adapter's UI and switch to STATION mode
- b). Two minutes after the router's WPS-PBC is enabled, press the adapter's WPS button to connect in PBC mode.
- c). You may view the PBC connection process on the UI's PBC screen.

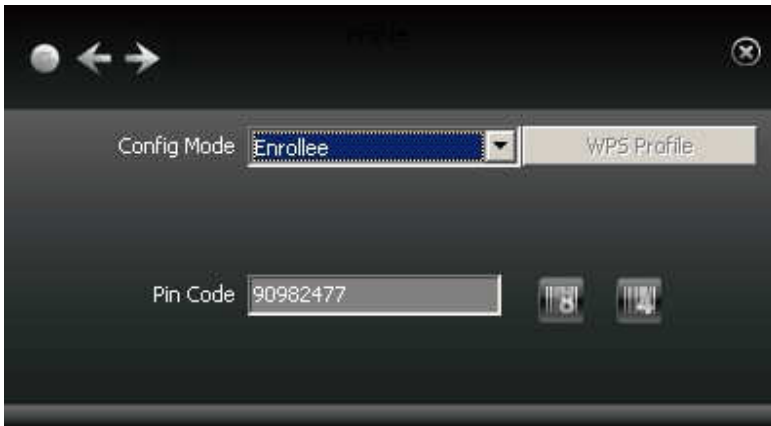
2. Wireless Connections in PIN Mode

On the "Add WPS Profile" screen, select "PIN" as the WPS Method. You may select the wireless AP to be connected in WPS mode on the WPS AP drop-down List, or select "Auto" and then click the next button.

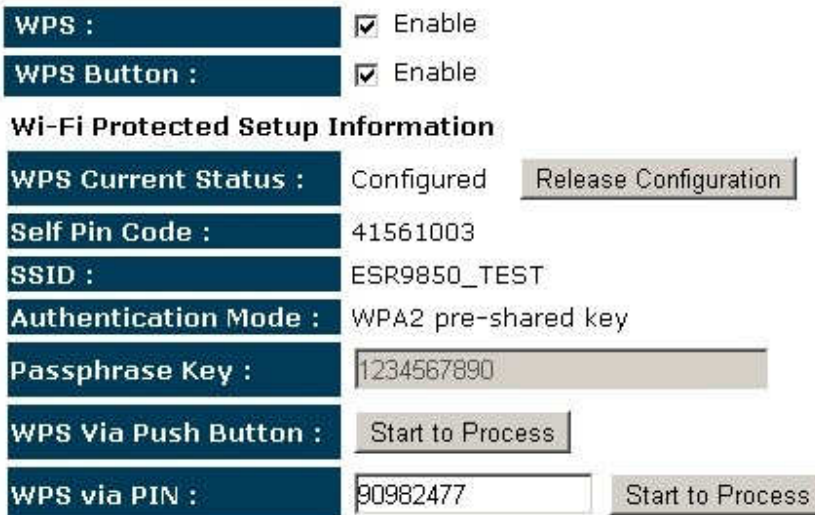


2.1 Enrollee Mode

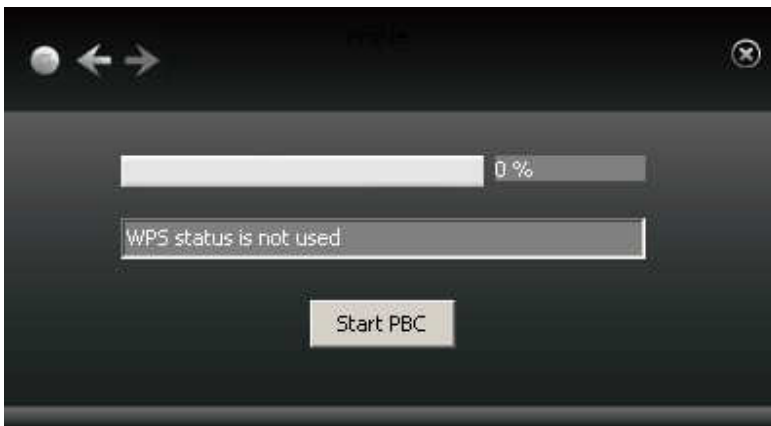
The PIN code field lists the adapter's current PIN code, when you select "Enrollee" as the Config Mode, you need to copy this PIN code and input it in the PIN code field of the router's WPS setting screen.



First enter its WPS configuration screen,enable WPS settings and select PIN for WPS mode and then input 90982477 in the PIN code field,and then click the “Save” button. When the WPS indicator of the Router starts flashing,it indicates that WPS feature is enabled.

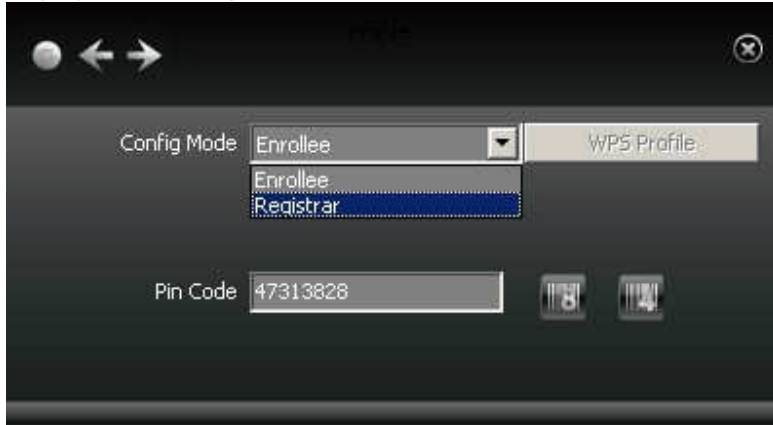


Click the next button on the Profile screen and click “Start PIN” to start the PIN code negotiation.

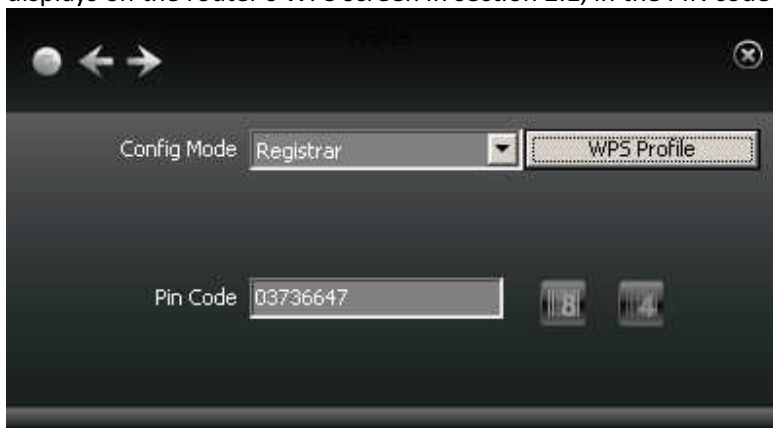


2.2 Registrar Mode

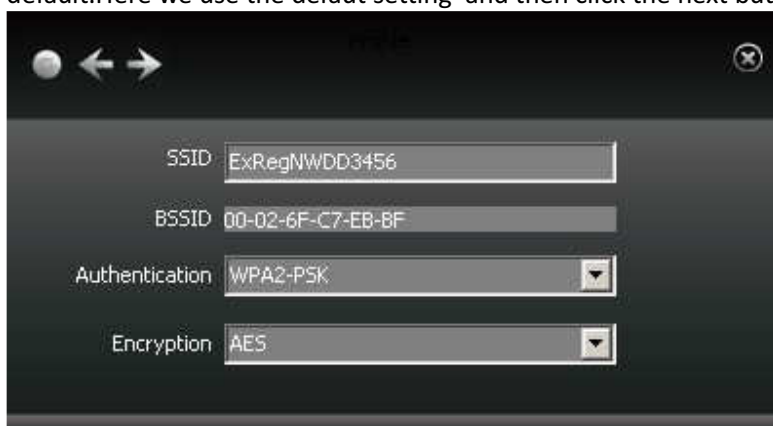
On the “Add WPS Profile” screen, select the SSID of the AP that need to negotiate in WPS mode instead of selecting “Auto”.Then select “PIN” as the WPS method and click the next button to display the folowing screen:



Select “Registrar” as the config mode and enter the router’s PIN code,such as 03736647 that displays on the router’s WPS screen in section 2.1, in the PIN code field here.



Now you can view the SSID ,authenticaiton type,and encrytion type that need to be negotiated by the WPS in registrar mode.These values can be modified but we recommend using the default.Here we use the default setting and then click the next buton.

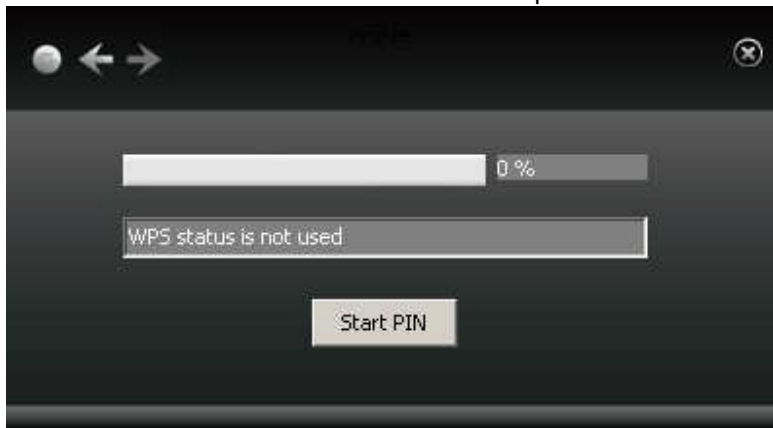


You can view the negotiation key on the screen below ,but you are not recommended to modify

it,just click the next buton.



Then click “Start PIN” on the screen below to perform WPS connection.



NOTE:

- 1.Under the WPS connection mode, when multiple routers simultaneously enable the WPS function, it may cause connection failure.
- 2.If the router connect to the adapter using the WPS, only one client can be connected at one time, and so if the router need to connect to multiple clients through WPS, you should repeat the WPS operation.

Appendix C – FCC Interference Statement

Federal Communication Commission Interference Statement

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.

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 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.

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

The product comply with the FCC portable RF exposure limit set forth for an uncontrolled environment and are safe for intended operation as described in this manual. The further RF exposure reduction can be achieved if the product can be kept as far as possible from the user body or set the device to lower output power if such function is available.

The USB dongle transmitter is approved for use in typical laptop computers. To comply with FCC RF exposure requirements, it should not be used in other devices or certain laptop and tablet computer configurations where the USB connectors on the host computer are unable to provide or ensure the necessary operating configurations intended for the device and its users or bystanders to satisfy RF exposure compliance requirements.

Appendix C – EU Declaration of Conformity

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN60950-1

Safety of Information Technology Equipment

EN62479 : 2010

Assessment of the compliance of low power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz)

EN 300 328 V1.7.1

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.8.1

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V2.1.1

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

EN 301 893 V1.5.1

Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive

This device is a 5 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

CE 0560

 Česky [Czech]	<i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets typebetegnelse]</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erkläre <i>[Name des Herstellers]</i> , dass sich das Gerät <i>[Gerätetyp]</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab <i>[tootja nimi = name of manufacturer]</i> seadme <i>[seadme tüüp = type of equipment]</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, <i>[name of manufacturer]</i> , declares that this <i>[type of equipment]</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente <i>[nombre del fabricante]</i> declara que el <i>[clase de equipo]</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>[name of manufacturer]</i> ΔΗΛΩΝΕΙ ΟΤΙ <i>[type of equipment]</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
 Français [French]	Par la présente <i>[nom du fabricant]</i> déclare que l'appareil <i>[type d'appareil]</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente <i>[nome del costruttore]</i> dichiara che questo <i>[tipo di apparecchio]</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>[name of manufacturer / izgatavotāja nosaukums]</i> deklarē, ka <i>[type of equipment / iekārtas tips]</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>[manufacturer name]</i> deklaruoja, kad šis <i>[equipment type]</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart <i>[naam van de fabrikant]</i> dat het toestel <i>[type van toestel]</i> in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, <i>[isem tal-manifattur]</i> , jiddikjara li dan <i>[il-mudel tal-prodott]</i> jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, <i>[gyártó neve]</i> nyilatkozom, hogy a <i>[... típus]</i> megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym <i>[nazwa producenta]</i> oświadczam, że <i>[nazwa wyrobu]</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	<i>[Nome do fabricante]</i> declara que este <i>[tipo de equipamento]</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	<i>[Ime proizvajalca]</i> izjavlja, da je ta <i>[tip opreme]</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	<i>[Meno výrobcu]</i> týmto vyhlasuje, že <i>[typ zariadenia]</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	<i>[Valmistaja = manufacturer]</i> vakuuttaa täten että <i>[type of equipment = laitteen tyyppimerkintä]</i> tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar <i>[företag]</i> att denna <i>[utrustningstyp]</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Appendix C – Industry Canada statement:

This device complies with RSS-210 of the Industry Canada 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.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Caution :

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.