



**TRENDNET**®



User's Guide

**TEW-645UB**  
H/W: V1.0R

## **Federal Communication Commission Interference Statement**

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 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.

### **IMPORTANT NOTE:**

#### **Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. To maintain compliance with FCC RF exposure compliance requirements, please follow operation instruction as documented in this manual.

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

SAR compliance has been established in typical laptop computer(s) with USB slot, and product could be used in typical laptop computer with USB slot. Other application like handheld PC or similar device has not been verified and may not compliance with related RF exposure rule and such use shall be prohibited.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

### **CE Mark Warning**

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

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

# Table of Contents

Federal Communications Commission (FCC) Interference statement	2
CE Mark Warning	2
<b>Chapter 1 – Wireless LAN Networking</b>	
Transmission Rate	4
Type of Wireless Networks	4
Ad-Hoc (IBSS) Network	4
Infrastructure (BSS) Network	7
Wireless LAN Security	9
Data Encryption with WEP	10
<b>Chapter 2 - Getting Started</b>	
About Your 802.11n/b/g WLAN USB2.0 Adapter	11
Package Content	11
System Requirement	11
LED Definition	11
Wireless Utility and Adapter Hardware Installation	12
Using the Utility to Configure Your Network	16
Link Information	16
Site Survey	17
Profile	19
<b>Chapter 3 – Maintenance</b>	
Uninstalling the Driver	24
Uninstall the Client Utility	24
Upgrading the Wireless Utility	24
<b>Glossary</b>	<b>25</b>

# Chapter 1- Wireless LAN Networking

This section provides background information on wireless LAN networking technology.



---

THE INFORMATION IN THIS SECTION IS FOR YOUR REFERENCE. CHANGING NETWORK SETTINGS AND PARTICULARLY SECURITY SETTINGS SHOULD ONLY BE DONE BY AN AUTHORIZED ADMINISTRATOR.

---

## Transmission Rate (Transfer Rate)

---

The adapter provides various transmission (data) rate options for you to select. Options include Fully Auto, 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 22 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps and up to 300Mbps. In most networking scenarios, the factory default Fully Auto setting proves the most efficient. This setting allows your adapter to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the adapter automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the adapter gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

## Types of Wireless Networks

---

Wireless LAN networking works in either of the two modes: ad-hoc and infrastructure. In infrastructure mode, wireless devices communicate to a wired LAN via access points. Each access point and its wireless devices are known as a Basic Service Set (BSS). An Extended Service Set (ESS) is two or more BSS in the same subnet. In ad hoc mode (also known as peer-to-peer mode), wireless devices communicate with each other directly and do not use an access point. This is an Independent BSS (IBSS).

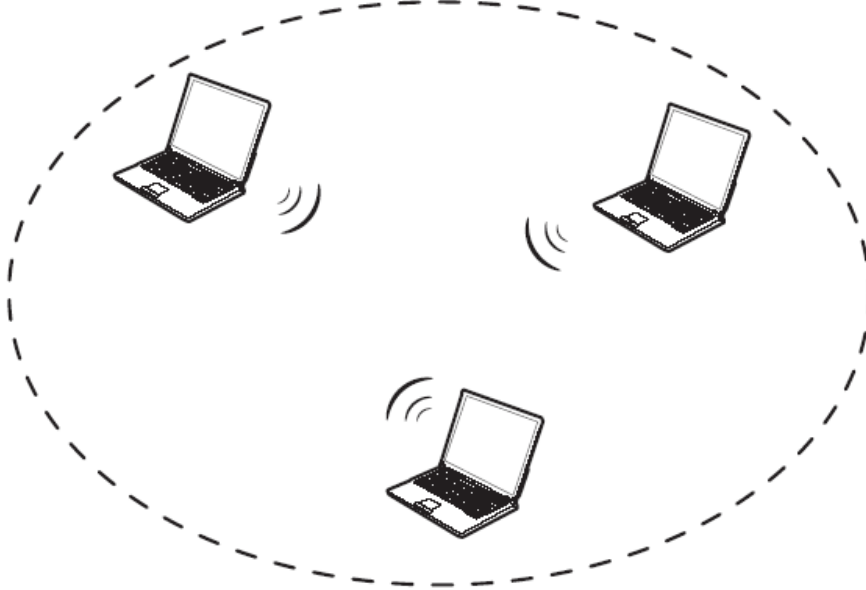
To connect to a wired network within a coverage area using access points, set the adapter operation mode to Infrastructure (BSS). To set up an independent wireless workgroup without an access point, use Ad-hoc (IBSS) mode.

### **AD-HOC (IBSS) NETWORK**

Ad-hoc mode does not require an access point or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

To set up an ad-hoc network, configure all the stations in ad-hoc mode. Use the same SSID and channel for each.

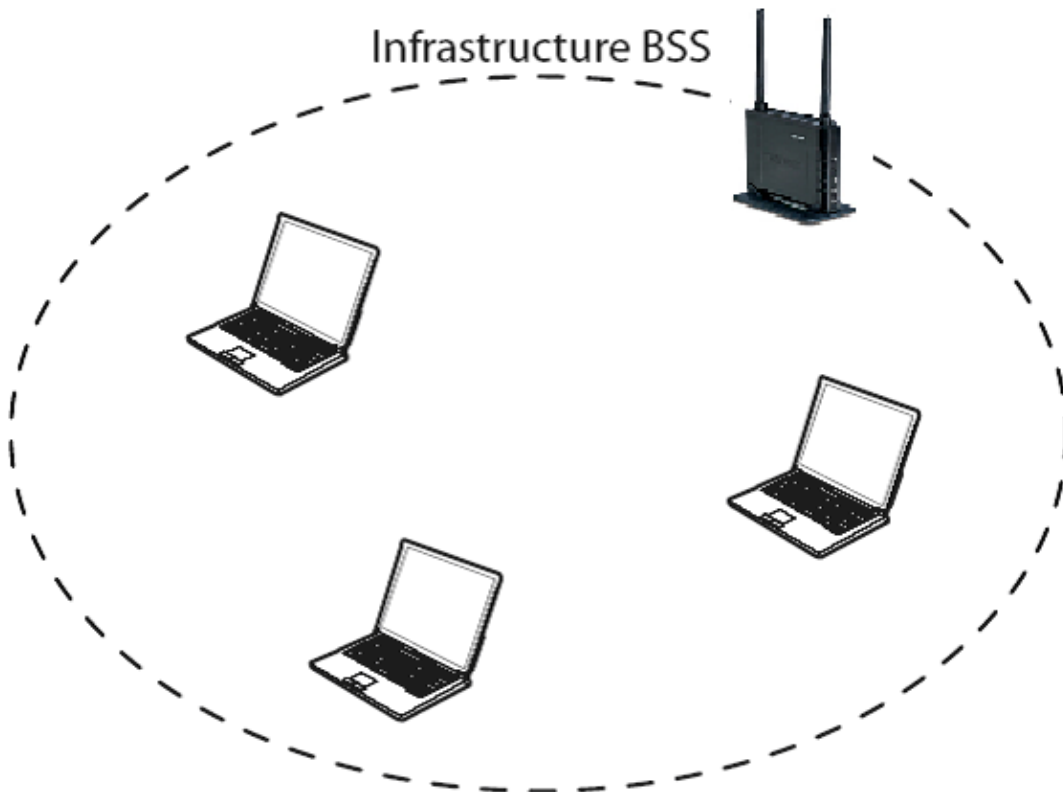
Ad-hoc IBSS



Ad-hoc (also known as peer-to-peer) network diagram

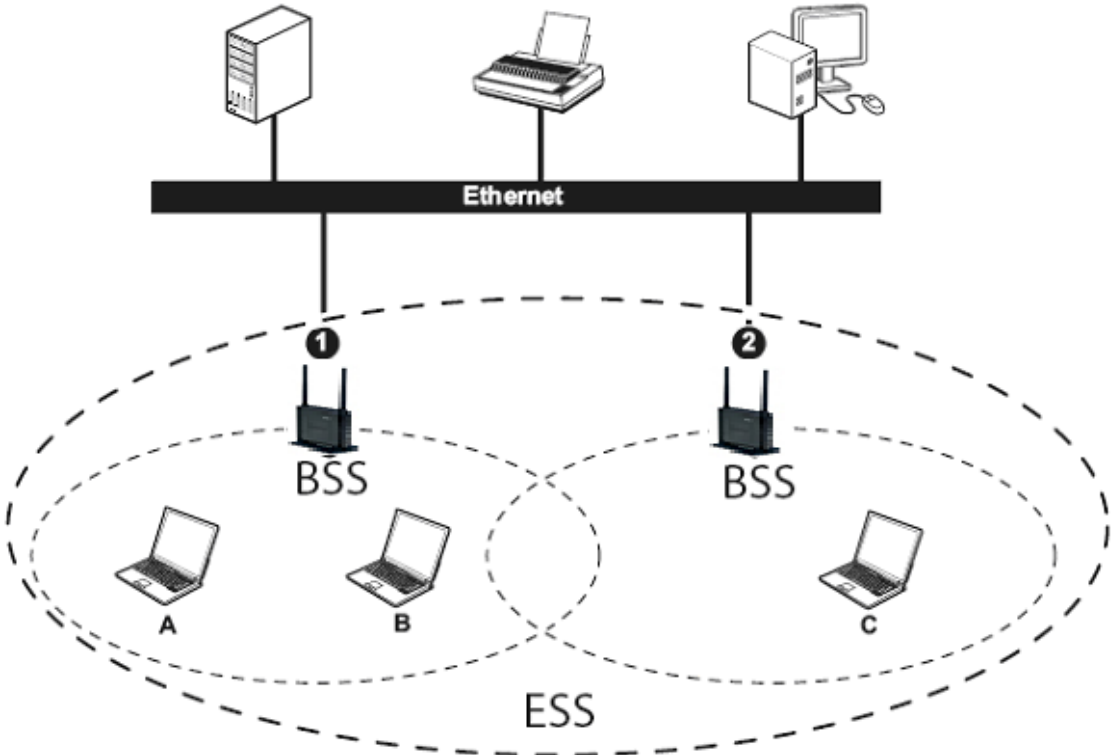
When a number of wireless stations are connected using a single access point, you have a Basic Service Set (BSS).

Infrastructure BSS



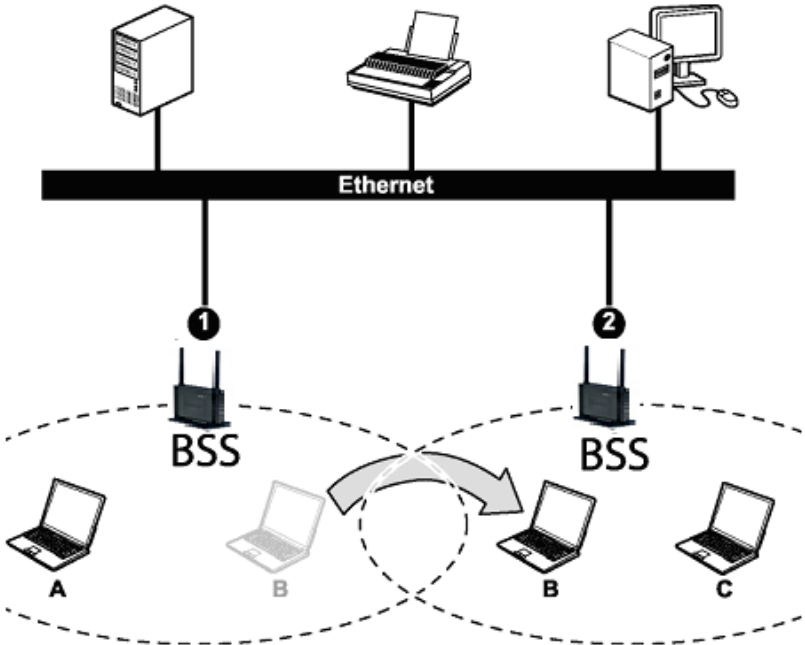
Infrastructure (IBSS) network diagram

In the ESS diagram below, communication is done through the access points, which relay data packets to other wireless stations or devices connected to the wired network. Wireless stations can then access resources, such as a printer, on the wired network.



Infrastructure (ESS) network diagram

In an ESS environment, users are able to move from one access point to another without losing the connection. In the diagram below, when the user moves from BSS (1) to BSS (2) the adapter automatically switches to the channel used in BSS (2).



Roaming in an ESS network diagram





## **WIRELESS LAN SECURITY**

Because wireless networks are not as secure as wired networks, it's vital that security settings are clearly understood and applied.

The list below shows the possible wireless security levels on your adapter starting with the most secure. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. EAP requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or the LAN to provide authentication service for wireless stations.

1. Wi-Fi Protected Access (WPA)
2. IEEE802.1X EAP with RADIUS Server authentication
3. WEP Encryption
4. Unique ESSID

## DATA ENCRYPTION WITH WEP

The WEP (Wired Equivalent Privacy) security protocol is an encryption method designed to try to make wireless networks as secure as wired networks. WEP encryption scrambles all data packets transmitted between the adapter and the access point or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.



DO NOT ATTEMPT TO CONFIGURE OR CHANGE SECURITY SETTINGS FOR A NETWORK WITHOUT AUTHORIZATION AND WITHOUT CLEARLY UNDERSTANDING THE SETTINGS YOU ARE APPLYING. WITH POOR SECURITY SETTINGS, SENSITIVE DATA YOU SEND CAN BE SEEN BY OTHERS.

---

There are two ways to create WEP keys in your adapter.

- Automatic WEP key generation based on a password phrase called a passphrase. The passphrase is case sensitive. You must use the same passphrase for all WLAN adapters with this feature in the same WLAN.
- For WLAN adapters without the passphrase feature, you can still take advantage of this feature by writing down the four automatically generated WEP keys from the Security Settings screen of the wireless utility and entering them manually as the WEP keys in the other WLAN adapter(s).

The adapter allows you to configure up to four WEP keys and only one key is used as the default transmit key at any one time.

The adapter supports up to four 64-BIT & 128-BIT WEP KEYS.

# Chapter 2 - Getting Started

This chapter introduces the Adapter and prepares you to use the Wireless Utility.

## 2.1 About Your 802.11 n/b/g WLAN USB2.0 Adapter

The Adapter is an 802.11n, 802.11b, and 802.11g compliant wireless LAN adapter. With the Adapter, you can enjoy wireless mobility within almost any wireless networking environment.

The following lists the main features of your Adapter.

- ✓ Your Adapter can communicate with other IEEE 802.11n/b/g compliant wireless devices.
- ✓ Wire-free access to networked resources from anywhere beyond the PC with any USB host interface.
- ✓ Support Infrastructure & Ad-Hoc mode
- ✓ Delivers receiving data rate up to 300 Mbps in 11n mode.
- ✓ For 802.11b/g, data rate dynamically shifts based on signal strength, for maximum availability and reliability of connection.
- ✓ Support both 20MHz & 40MHz bandwidth
- ✓ Support WEP 64/128, WPA, WPA2 encryption
- ✓ Support QoS – WMM
- ✓ Multi-path (1x2) design and two PCB antennas built-in design guarantee best transmitting / receiving quality.
- ✓ Support Windows-base wireless LAN GUI
- ✓ Support WPS enable on S/W utility

## 2.2 Package Content

- 802.11n/b/g WLAN USB2.0 Adapter
- USB Cradle
- Installation and Manual CD
- Quick Start Guide
- Warranty/Registration Card

## 2.3 System Requirement

- Pentium class notebook computers with at least one available USB slot
- Microsoft Windows Vista, XP and 2K
- CD-ROM drive

## 2.4 Wireless Utility & Adapter Hardware Installation

**NOTE: If you have connected the USB Adapter to your computer, please remove it first.**

Follow the instructions below to install the USB Adapter and Utility.

### **STEP 1**

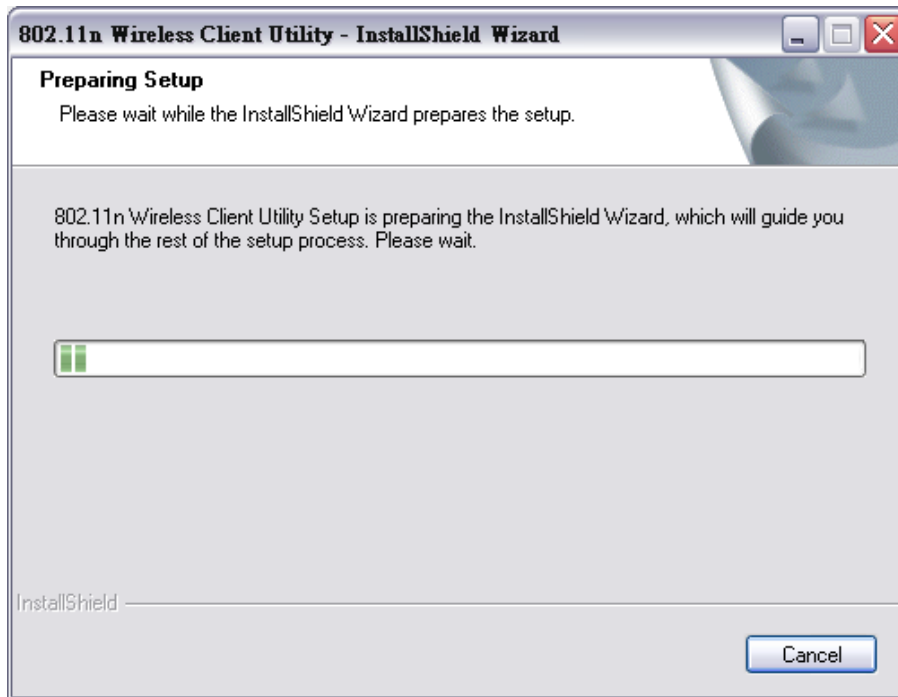
Insert the Driver and Utility CD into CD drive

**STEP 2**

If your CD Autorun is enabled, the installation procedures will be started. (Otherwise open your CD folder and double-click on the “setup.exe” file)

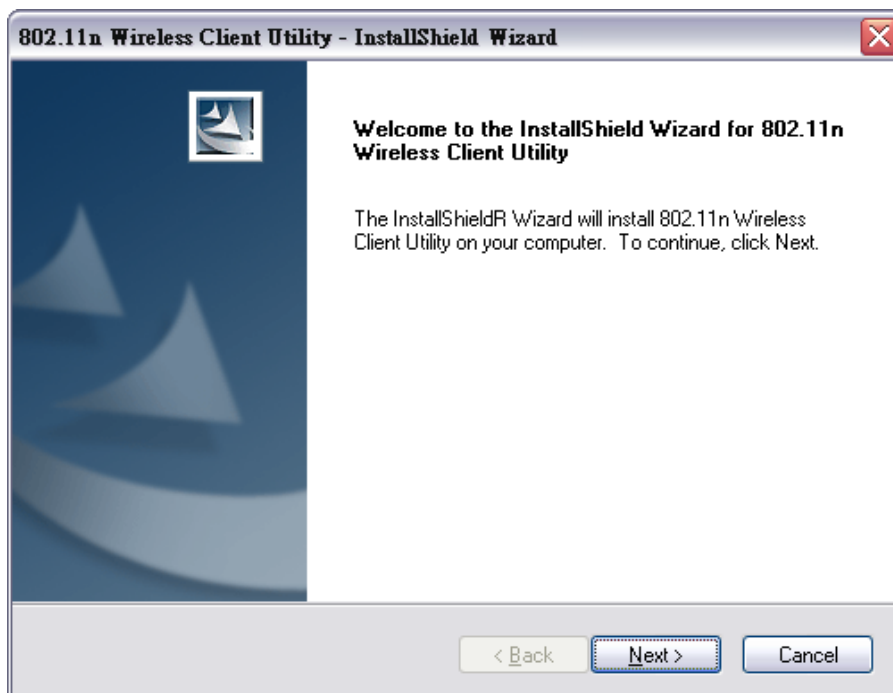
**STEP 3**

The InstallShield Wizard prepares for installation.



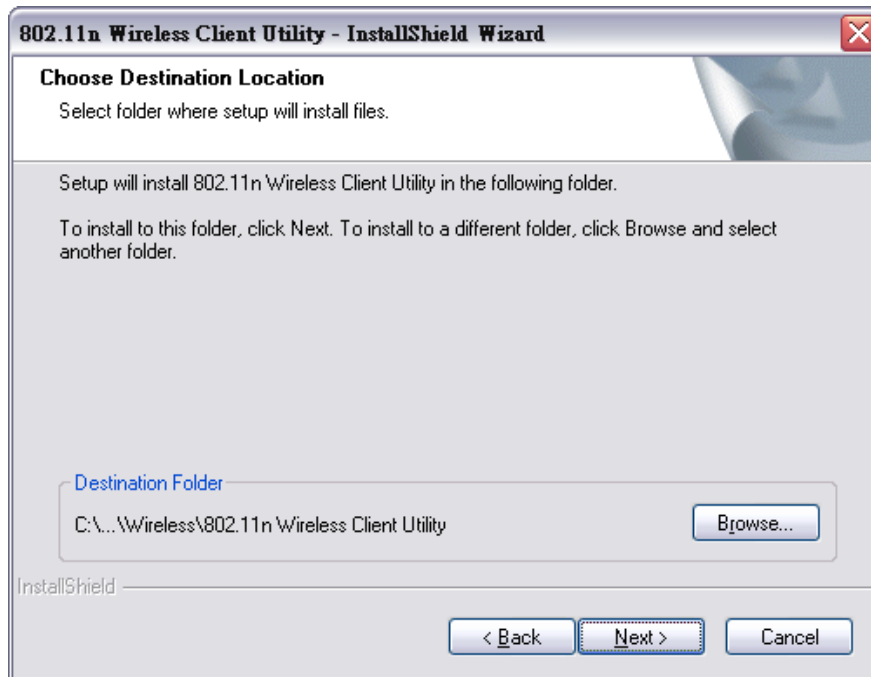
**STEP 4**

The InstallShield Wizard prompts you for confirmation. Click **Next** on the following menu.



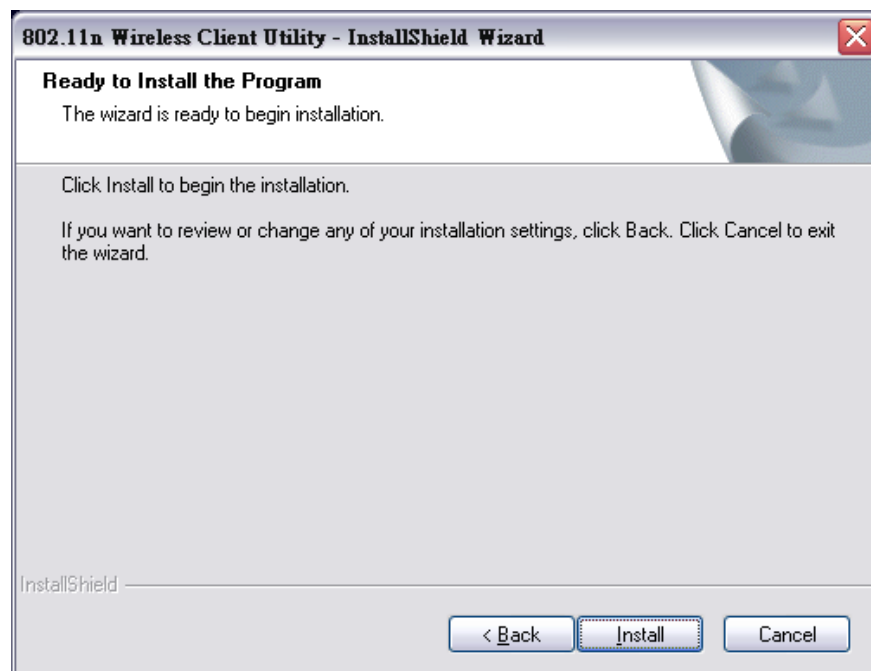
### STEP 5

In the destination Folder screen you are asked to confirm the Destination Folder for the application software. If you would like, you may change the destination folder to another location. Click **Next**



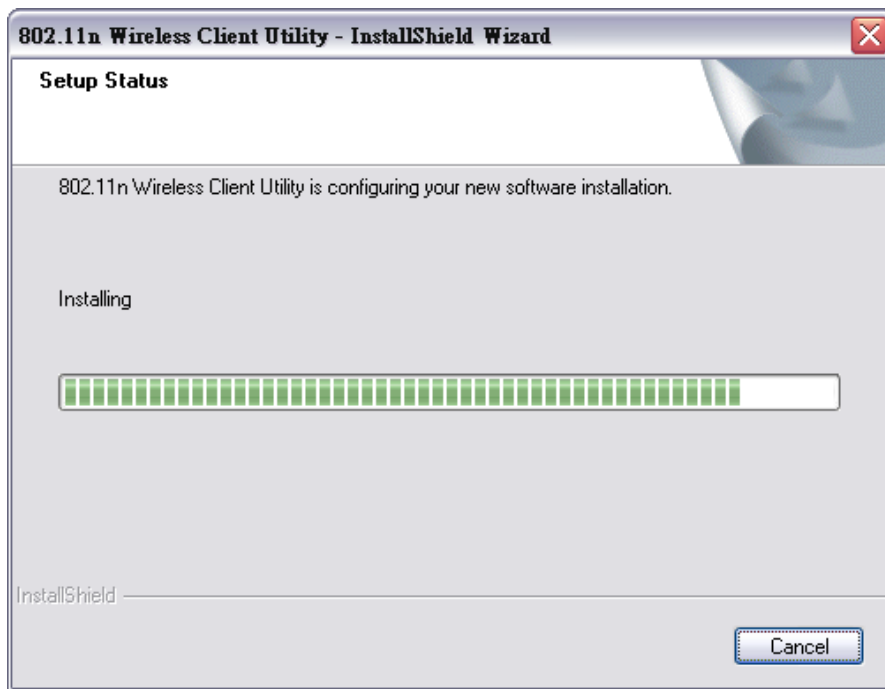
### STEP 6

The wizard is ready to begin installation. Click **Install** on it.



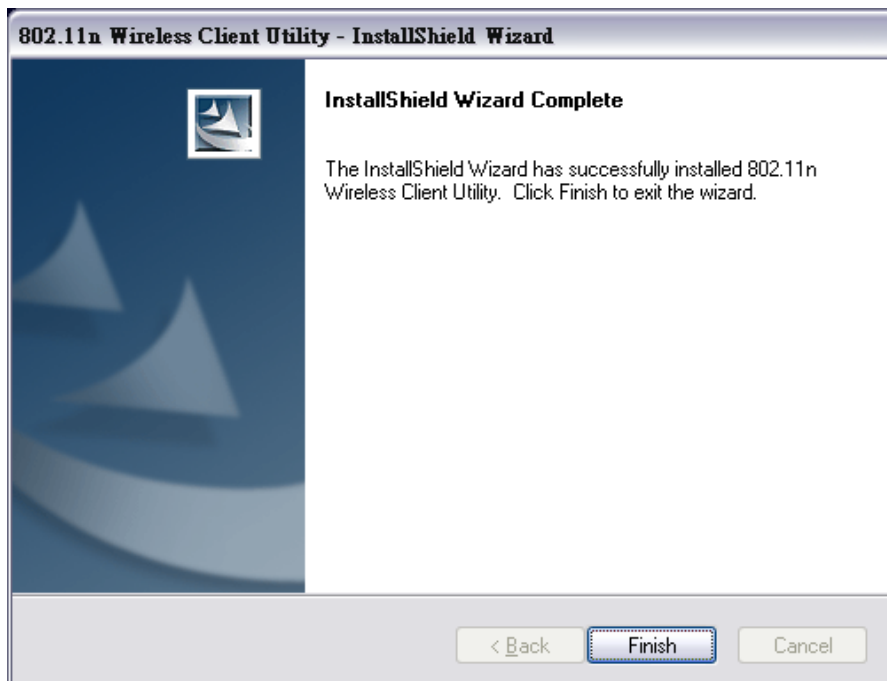
**STEP 7**

The Install shield Wizard setup for installation.



**STEP 8**

Click **Finish** to complete the client utility installation.



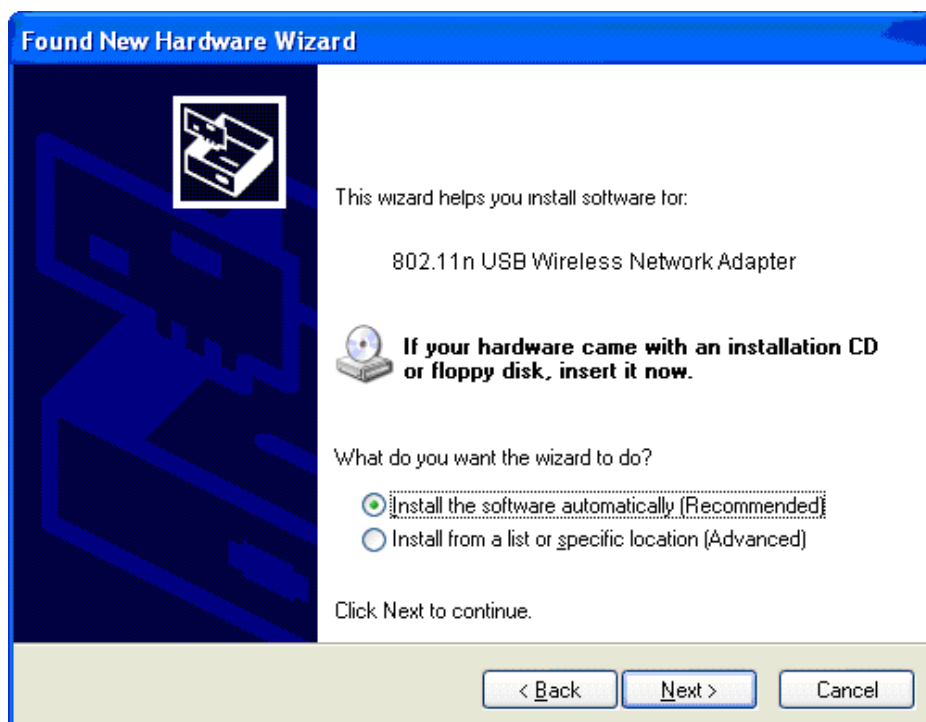
### STEP 9

At this moment please insert your USB Adapter to your Laptop through the cradle. After the following window pop up, click **Next** on the Found New Hardware Wizard



### STEP 10

Choose “Install the software automatically” , and click **Next**.



**STEP 11**

Click **Finish** to complete the installation.





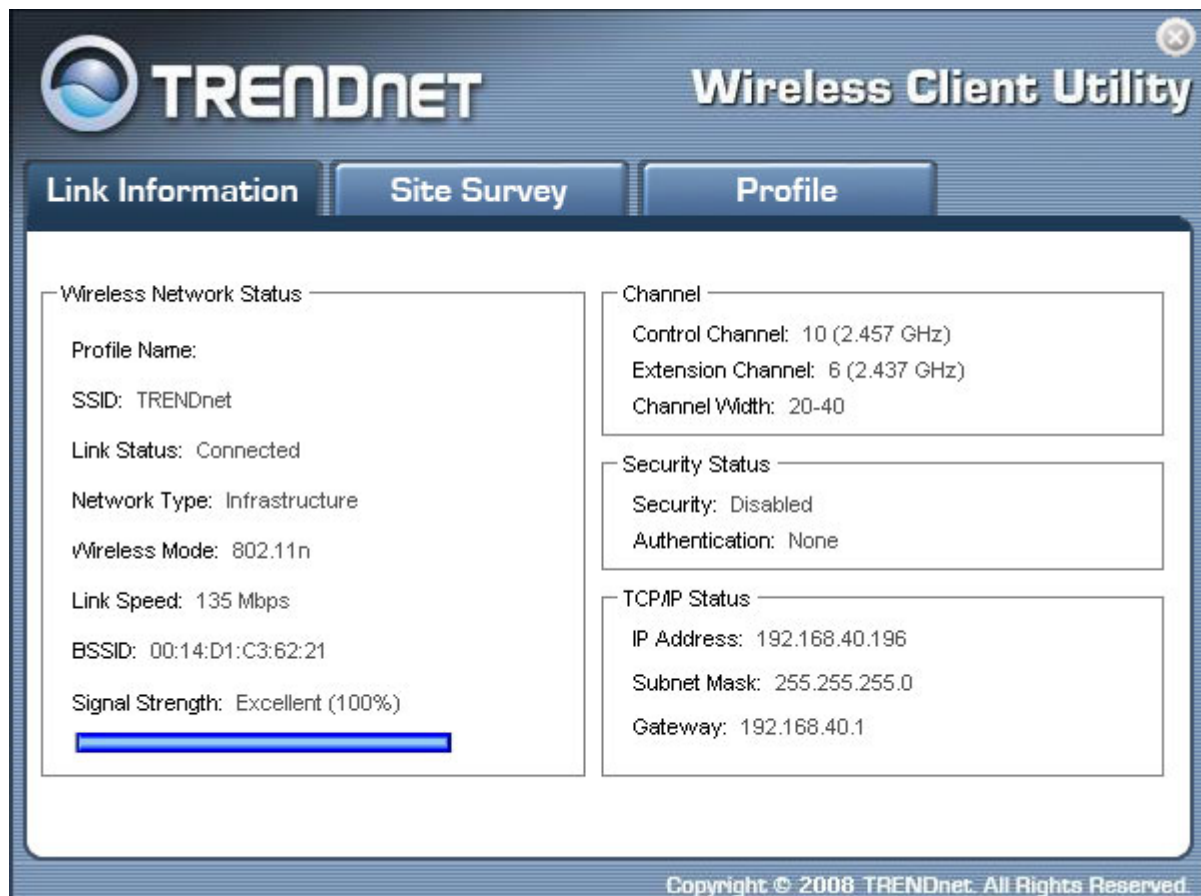
## 2.6 Using the Utility to Configure Your Network

The following are explanations on how to configure and use the Utility program. After completing the installation procedure, a new icon as shown below will automatically appear in the lower right tray bar.



Hold your mouse pointer over the icon, and press the right mouse button to open the Wireless Client Utility.

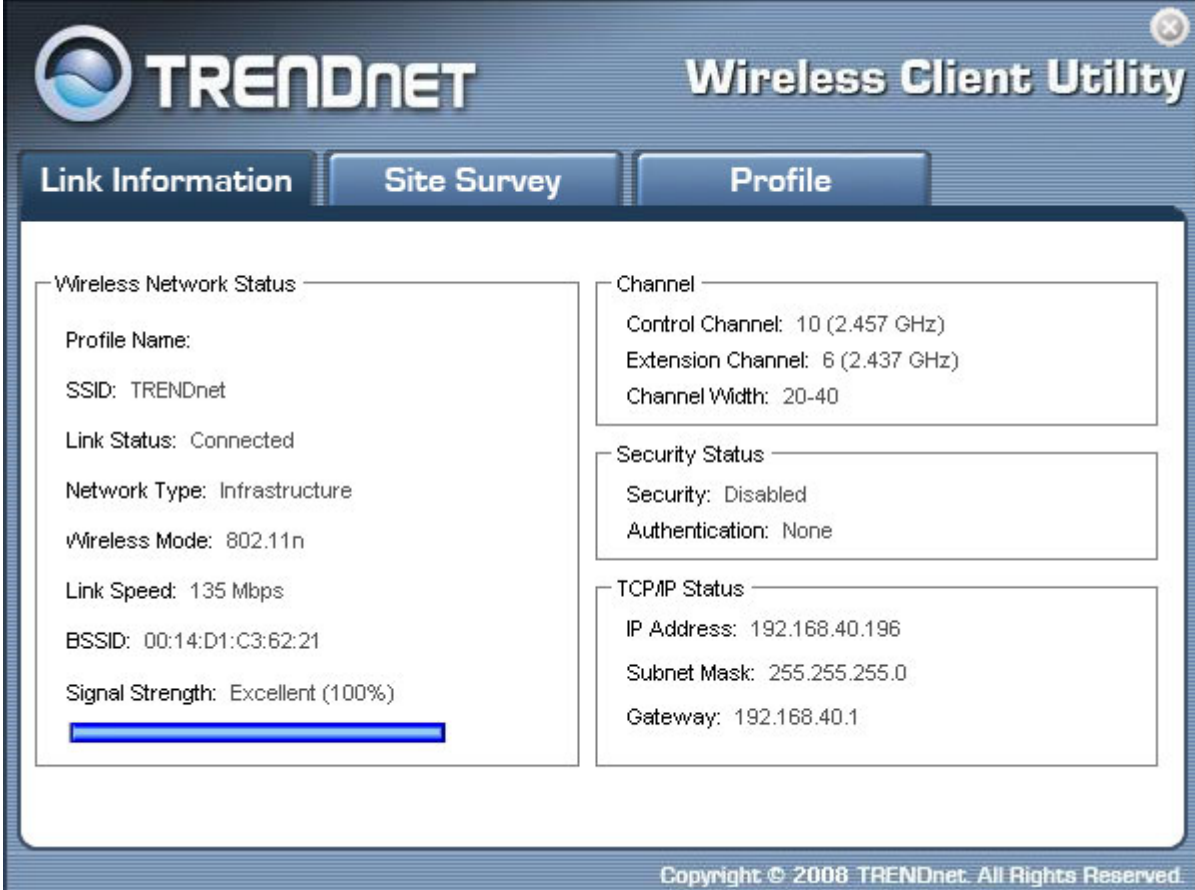
The Wireless Client Utility window as shown below will appear.



The user can now use any of the management functions available in the IEEE 802.11 Wireless Client Utility.

## 2.6.1 Link Information

Click the **Link Information** tab to see general information about the program and its operations. The Link Information tab does not require any configuration.



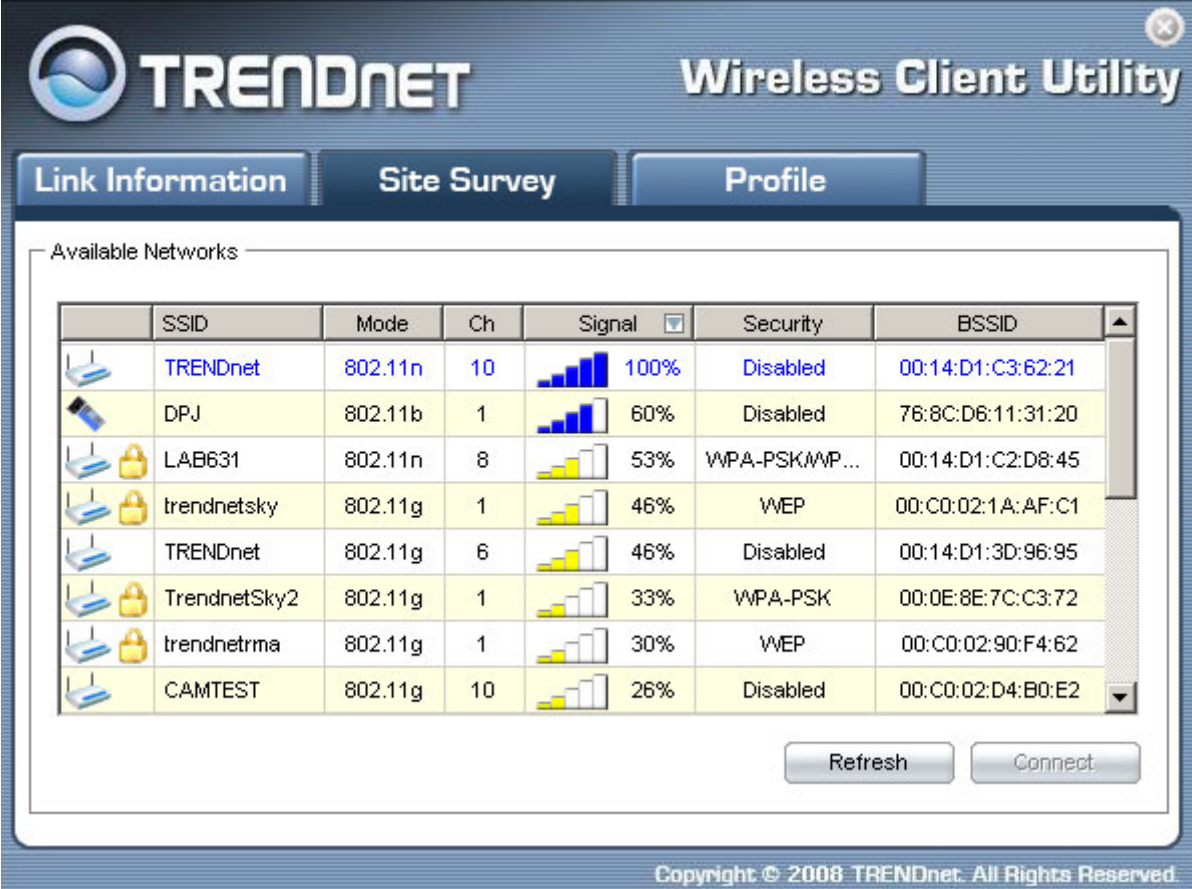
The screenshot displays the TRENDnet Wireless Client Utility interface. At the top left is the TRENDnet logo, and at the top right is the title "Wireless Client Utility" with a close button. Below the title are three tabs: "Link Information" (selected), "Site Survey", and "Profile". The main content area is divided into two columns. The left column, titled "Wireless Network Status", contains the following information: Profile Name (empty), SSID: TRENDnet, Link Status: Connected, Network Type: Infrastructure, Wireless Mode: 802.11n, Link Speed: 135 Mbps, BSSID: 00:14:D1:C3:62:21, and Signal Strength: Excellent (100%) with a full blue progress bar. The right column contains three sections: "Channel" with Control Channel: 10 (2.457 GHz), Extension Channel: 6 (2.437 GHz), and Channel Width: 20-40; "Security Status" with Security: Disabled and Authentication: None; and "TCP/IP Status" with IP Address: 192.168.40.196, Subnet Mask: 255.255.255.0, and Gateway: 192.168.40.1. At the bottom right, there is a copyright notice: "Copyright © 2008 TRENDnet. All Rights Reserved."

The following table describes the items found on the Link Information screen.

















<b>Wireless Network Status</b>	
<b>Profile Name</b>	The name of the current selected configuration profile. Set up the configuration name on the <b>Profile tab</b> .
<b>SSID</b>	Displays the wireless network name.
<b>Link Status</b>	Shows whether the station is associated to the wireless network.
<b>Network Type</b>	The type of network the station is connected to. The options include:
<b>Wireless Mode</b>	Displays the wireless mode. 802.11g, 11b or 11n
<b>Channel</b>	Shows the currently connected channel.
<b>Transmit Rate</b>	Displays the current transmit rate in Mbps.
<b>BSSID</b>	Displays the BSSID of the wireless network that the wireless adapter is associated to.
<b>Signal Strength</b>	Shows the strength of the signal.
<b>Security Status</b>	
<b>Security</b>	Shows the security type – Disable, WEP, WPA/WPA2, WAP-PSK/WAP2-PSK or 802.1X
<b>Authentication</b>	Displays the authentication mode.
<b>TCP/IP Status</b>	
<b>IP Address</b>	Displays the computer's IP address.
<b>Subnet Mask</b>	Displays subnet mask
<b>Gateway</b>	Displays gateway address

## 2.6.2 Site Survey

Click the **Site Survey** tab to see available infrastructure and ad hoc networks. On this screen, click **Refresh** to refresh the list at any time.



The screenshot shows the 'Wireless Client Utility' interface with the 'Site Survey' tab selected. The 'Available Networks' section contains a table with the following data:

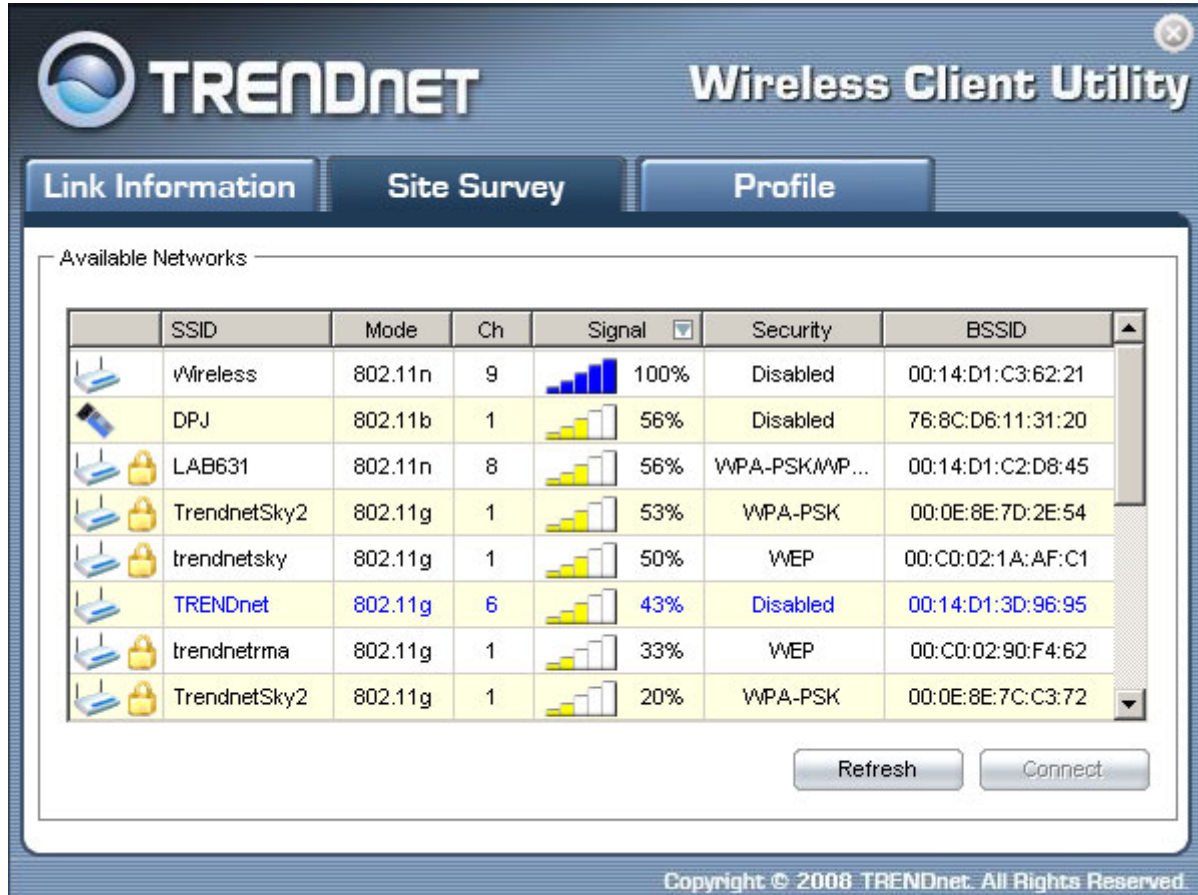
	SSID	Mode	Ch	Signal	Security	BSSID
	TRENDnet	802.11n	10	 100%	Disabled	00:14:D1:C3:62:21
	DPJ	802.11b	1	 60%	Disabled	76:8C:D6:11:31:20
	LAB631	802.11n	8	 53%	WPA-PSK/WP...	00:14:D1:C2:D8:45
	trendnetsky	802.11g	1	 46%	WEP	00:C0:02:1A:AF:C1
	TRENDnet	802.11g	6	 46%	Disabled	00:14:D1:3D:96:95
	TrendnetSky2	802.11g	1	 33%	WPA-PSK	00:0E:8E:7C:C3:72
	trendnetrma	802.11g	1	 30%	WEP	00:C0:02:90:F4:62
	CAMTEST	802.11g	10	 26%	Disabled	00:C0:02:D4:B0:E2

Below the table are two buttons: 'Refresh' and 'Connect'.

Copyright © 2008 TRENDnet. All Rights Reserved.

### Connecting to a different network

Hold your mouse pointer over the network icon, and click the right mouse button to select the network.



The screenshot shows the TRENDnet Wireless Client Utility interface. At the top, there are three tabs: "Link Information", "Site Survey", and "Profile". The "Site Survey" tab is selected. Below the tabs, there is a section titled "Available Networks" containing a table of detected wireless networks. The table has columns for SSID, Mode, Ch, Signal, Security, and BSSID. The "Signal" column includes a bar chart and a percentage value. The "Security" column shows the security type, with "Disabled" in blue text. The "BSSID" column shows the MAC address. At the bottom right of the table area, there are "Refresh" and "Connect" buttons. The copyright notice "Copyright © 2008 TRENDnet. All Rights Reserved." is visible at the bottom of the window.

	SSID	Mode	Ch	Signal	Security	BSSID
	wireless	802.11n	9	100%	Disabled	00:14:D1:C3:62:21
	DPJ	802.11b	1	56%	Disabled	76:8C:D6:11:31:20
	LAB631	802.11n	8	56%	WPA-PSK/WP...	00:14:D1:C2:D8:45
	TrendnetSky2	802.11g	1	53%	WPA-PSK	00:0E:8E:7D:2E:54
	trendnetsky	802.11g	1	50%	WEP	00:C0:02:1A:AF:C1
	TRENDnet	802.11g	6	43%	Disabled	00:14:D1:3D:96:95
	trendnetrma	802.11g	1	33%	WEP	00:C0:02:90:F4:62
	TrendnetSky2	802.11g	1	20%	WPA-PSK	00:0E:8E:7C:C3:72

Click the **Connect** button to connect the available network. If no configuration profile exists for that network, the Profile Settings window opens to ask to create a profile for the network. Follow the procedures to create profile for that network.

### 2.6.3 Profile

The screenshot displays the 'Profile' tab in the Trendnet Wireless Client Utility. The interface is divided into two main sections: 'Profile List' and 'Profile Information'.

**Profile List:** A table with columns for Name and SSID. The first row is highlighted in blue and contains the text 'Default' and 'ANY'. Below it are several empty rows with a yellow background.

Name	SSID
Default	ANY

**Profile Information:** A list of configuration parameters for the selected profile:

- Profile Name: Default
- SSID: ANY
- Network Type: Infrastructure
- Channel: Auto
- Security: Disabled
- Authentication: None

At the bottom of the interface, there are several buttons: Add, Edit, Delete, Import, Export, Connect, and WPS.

Copyright © 2008 TRENDnet. All Rights Reserved.

To add a new configuration profile, click **Add** on the Profile tab.

To modify a configuration profile, select the configuration from the Profile list and click the **Edit** button.

**TRENDNET**

### Profile Settings

General Connection Settings

Profile Name:

SSID:

Network Type:

Ad-Hoc Mode Settings

Channel:

### Scan Available Networks

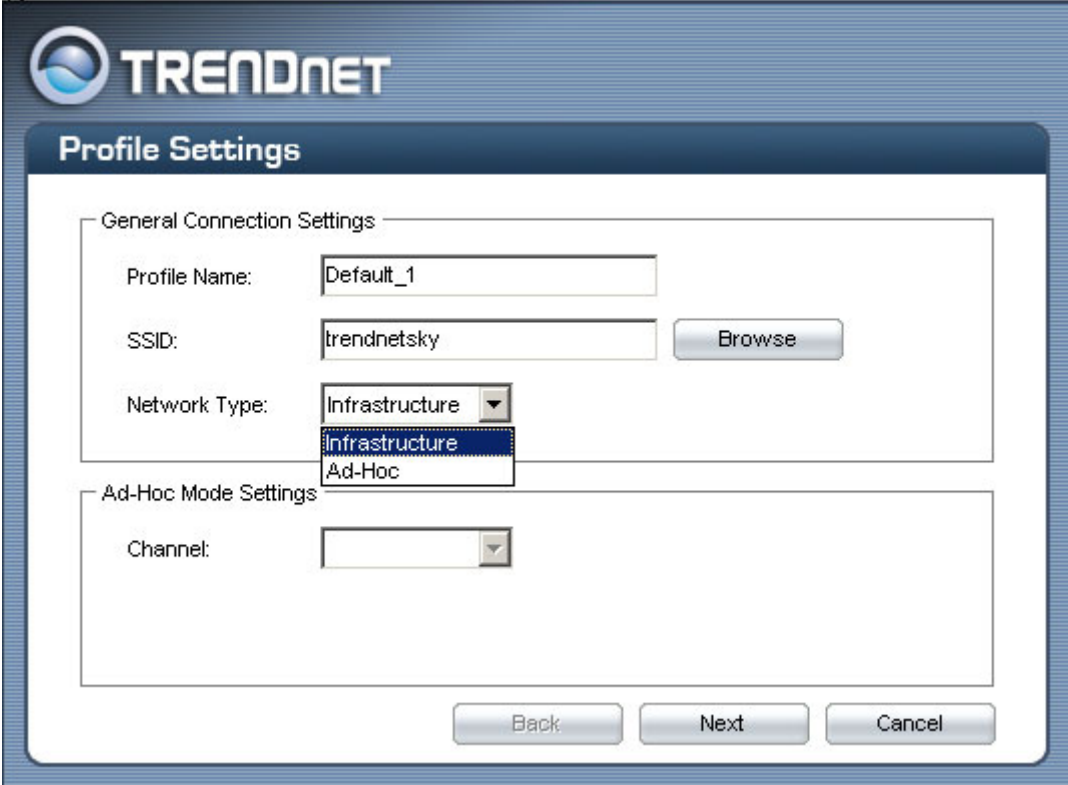
Click the **Browse** button on the Profile Settings screen to scan for available infrastructure and ad hoc networks. On this list, click **Refresh** to refresh the list at any time.

Wireless Client Utility

Available Networks

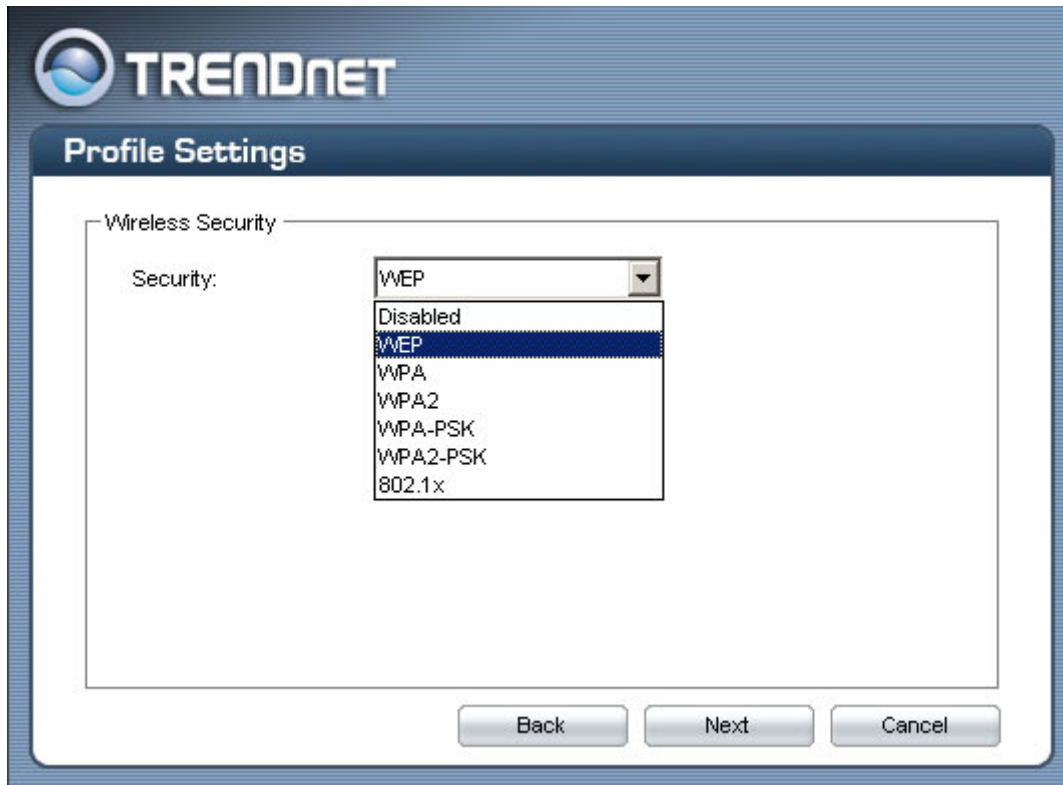
SSID	Mode	Ch	Signal	Security	BSSID
Searching...					

To configure a profile for Ad-Hoc or Infrastructure mode, select the Network Type field on the Profile Settings.



Click **Next** to continue the profile setting.





To define the security mode, select the security button of the desired security mode. And then click **Next** to continue. Please see following table for details of security modes.

Security Modes table

<p><b>WPA/WPA2</b></p>	<p>Enables the use of Wi-Fi Protected Access (WPA).          Choosing WPA/WPA2 opens the WPA/WPA2 <b>Security Settings</b> screen. The options include:</p> <ul style="list-style-type: none"> <li>• <b>TLS (Transport Layer Security)</b> is a Point-to-Point Protocol (PPP) extension supporting additional authentication methods within PPP. Transport Layer Security (TLS) provides for mutual authentication, integrity-protected cipher suite negotiation, and key exchange between two endpoints.</li> <li>• <b>PEAP (EAP-GTC) (Protected Extensible Authentication Protocol)</b> authenticates <u>wireless LAN clients</u> using only <u>server-side digital certificates</u> by creating an <u>encrypted SSL/TLS</u> tunnel between the client and the <u>authentication server</u>. The tunnel then protects the subsequent user authentication exchange.</li> <li>• <b>PEAP (EAP-MSCHAP V2) (Protected Extensible Authentication Protocol) To use PEAP (EAP-MSCHAP V2) security</b>, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager</li> <li>• <b>TTLS (Tunneled Transport Layer Security)</b> An <u>EAP</u> variant that provides mutual authentication using a certificate for server authentication, and via a secure <u>TLS</u> tunnel for the client</li> </ul>
<p><b>WPA-PSK/WPA2-PSK</b></p>	<p>Enables WPA/WPA2 Passphrase security.          Fill in the WPA/WPA2 Passphrase on <b>Security Settings</b> screen.</p>
<p><b>802.1x</b></p>	<p>Enables 802.1x security. This option requires IT administration.          Choosing 802.1x opens the 802.1x <b>Security Settings</b> screen. The options include:</p> <ul style="list-style-type: none"> <li>• <b>TLS</b></li> <li>• <b>PEAP</b></li> <li>• <b>TTLS</b></li> </ul>

## Advanced Settings

After Security Settings finished, the **Advanced Settings** screen will be shown as following.

The screenshot shows the TrendNet Profile Settings interface. The 'Advanced Settings' section includes the following fields and options:

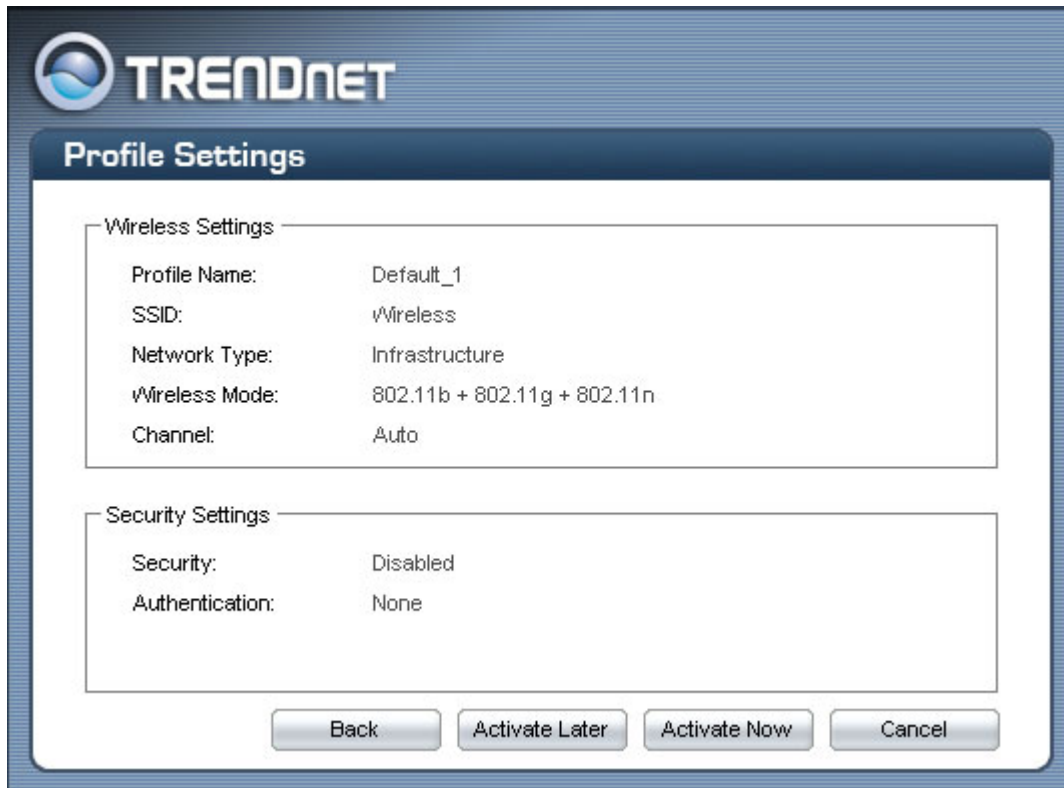
- Power Save Mode: Continuous Access Mode
- 802.11b Preamble: Auto
- RTS Threshold: 2347 (0 - 2347)
- FRAG Threshold: 2346 (256 - 2346)
- QoS

Navigation buttons at the bottom: Back, Next, Cancel.

The following table describes the items found on the Advanced Settings screen.

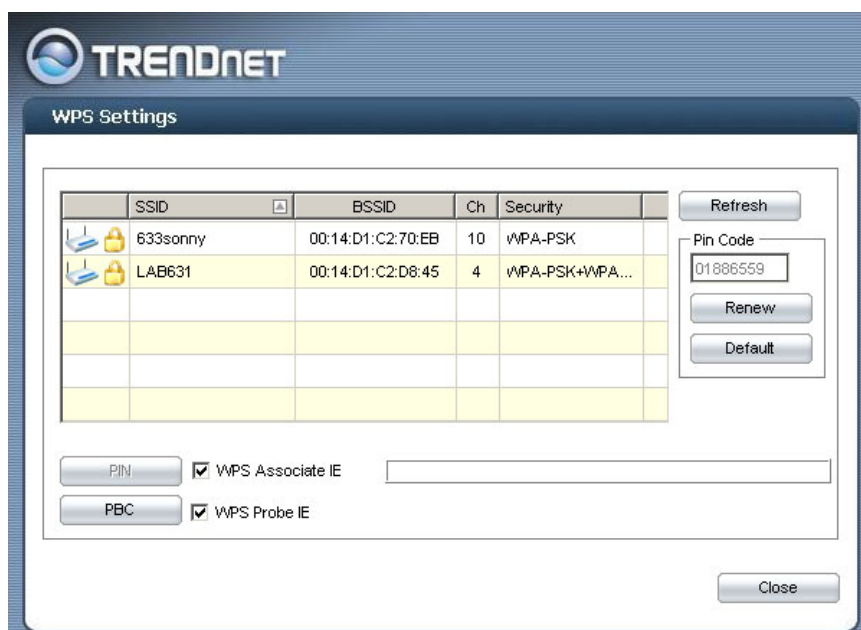
<b>Power Save Mode</b>	Shows the power save mode. Power management is disabled in ad hoc mode. The options include: <ul style="list-style-type: none"><li>• <b>Continuous Access Mode</b></li><li>• <b>Maximum Power Saving</b></li><li>• <b>Fast Power Saving</b></li></ul>
<b>802.11b Preamble</b>	Displays the 802.11b preamble format. The options include: <ul style="list-style-type: none"><li>• <b>Long</b></li><li>• <b>Short</b></li><li>• <b>Auto</b></li></ul>
<b>RTS Threshold</b>	Value from 0 ~ 2347
<b>FRAG Threshold</b>	Value from 256 ~ 2346

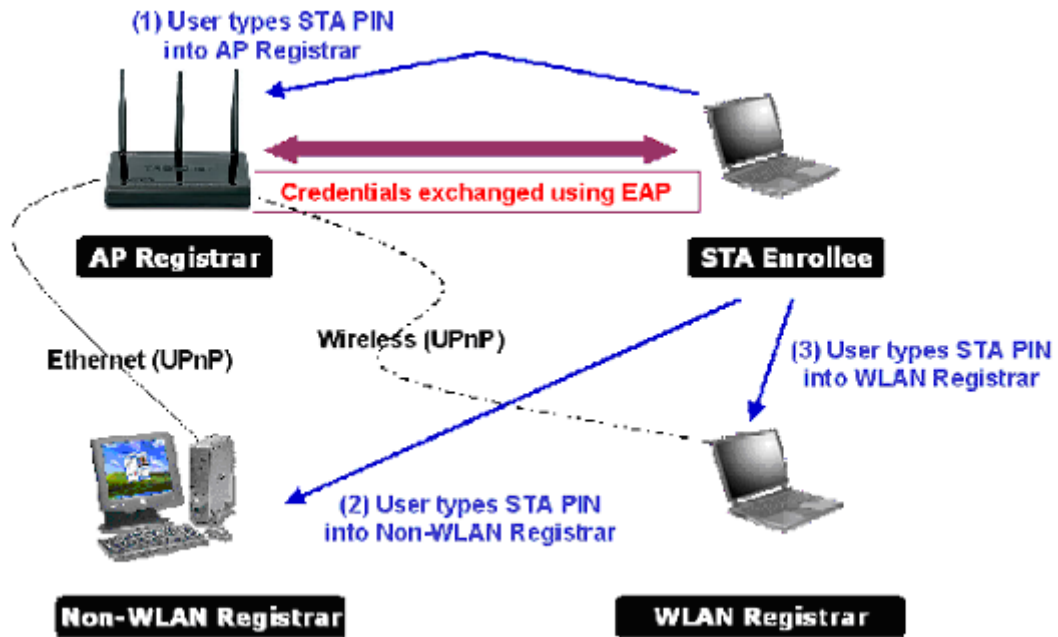
After advance settings are finished, the following screen showed as below. You can activate the profile now or later.



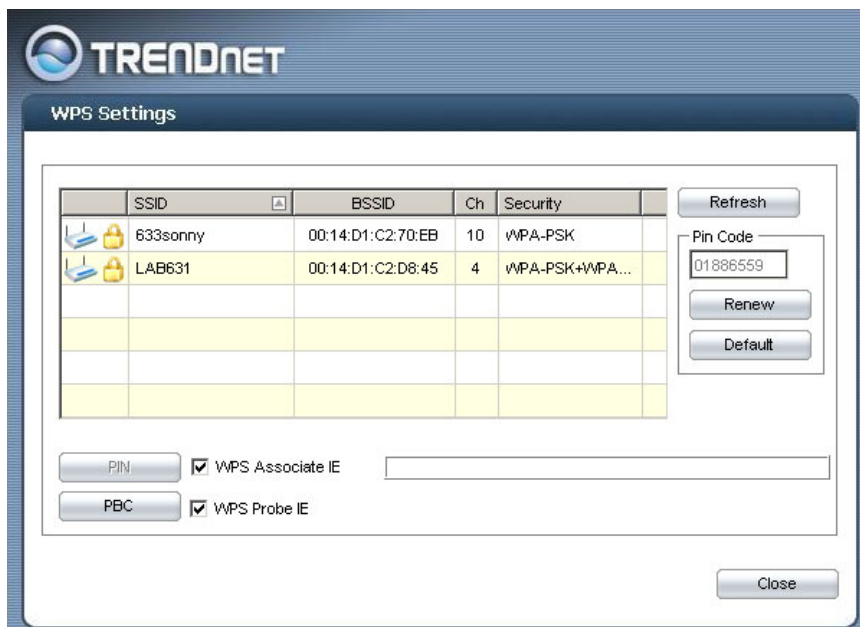
### WPS Setting

The user obtains a device password (PIN Code) from the STA and enters the password into the Registrar. Both the Enrollee and the Registrar use PIN Config method for the configuration setup. The detail indicates as follows.

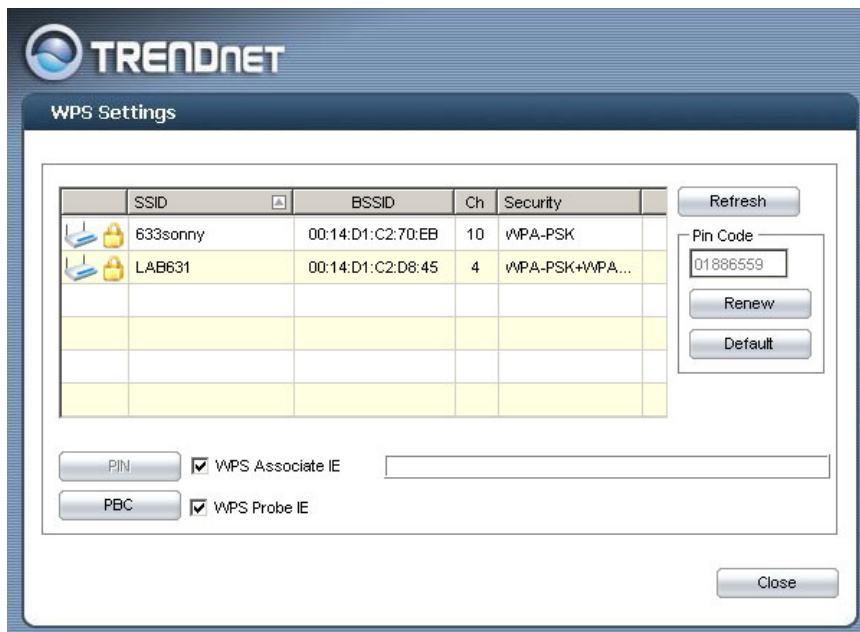




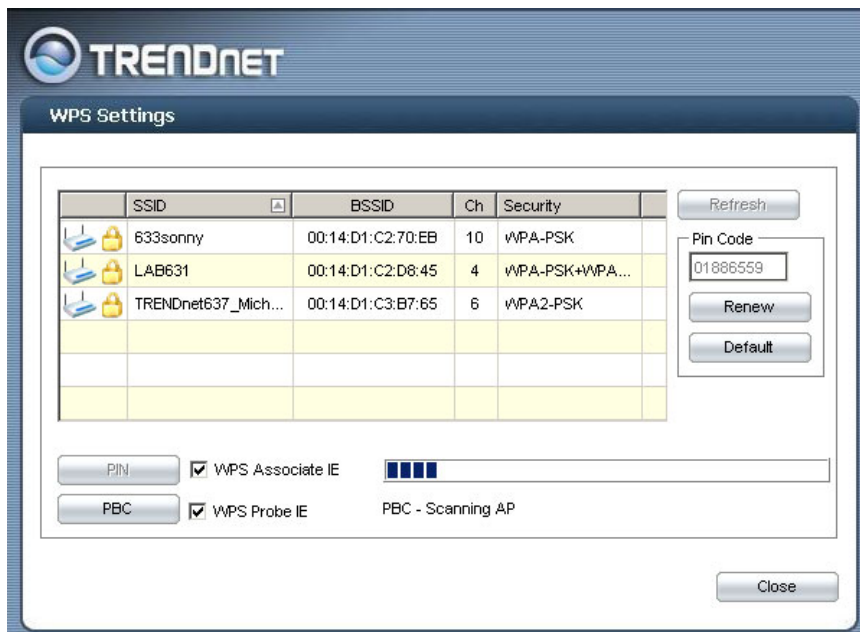
1. Click "Refresh" button to update available WPS APs.



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



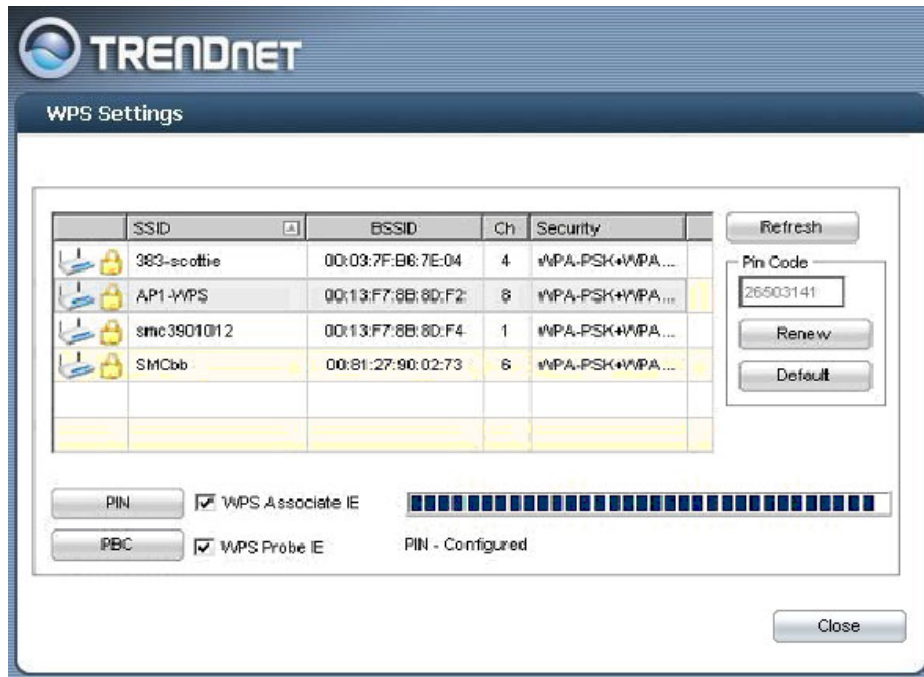
3. Click "PIN" button to start PIN connection.



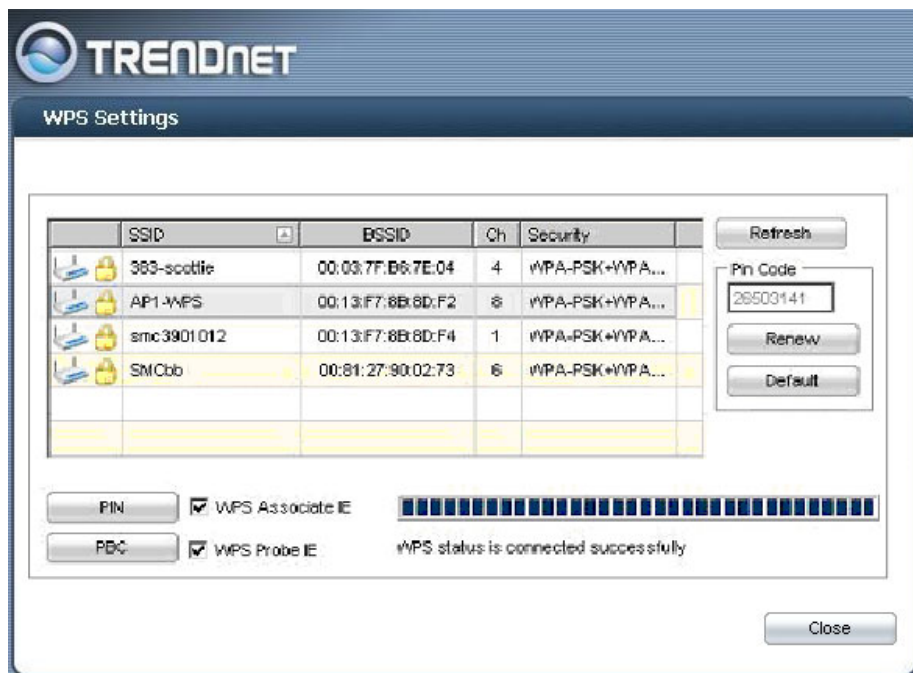
4. Enter PIN Code of STA into the Registrar when prompted by the Registrar.

\*Allow of an exchange between Step 3 and Step 4.

5. The result will look like the below figure.



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



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

1. A successful PIN Configuration :

Start PIN connection - SSID ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive EAP-Req (Start) ~> Sending M1 ~> Received M2 ~> (Received M2D ~> Sending EAP-Rsp (ACK)) ~> Sending M3 ~> Received M4 ~> Sending M5 ~> Received M6 ~> Sending M7 ~> Received M8 ~> Sending EAP-Rsp(Done) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

2. WPS configuration doesn't complete after **two-minute connection** :

WPS Eap process failed.

3. When Errors occur within **two-minute connection**, the WPS status bar might report on "WPS Eap process failed".

Error messages might be :

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



# Chapter 3 – Maintenance

This chapter describes how to uninstall or upgrade the Wireless Utility.

## 3.1 Uninstall the Driver

Follow the steps below to remove (or uninstall) the USB Adapter driver from your computer.

- Step 1.** To remove the driver from the OS, go to **Start -> Control Panel**
- Step 2.** Double-click **System**
- Step 3.** Under **Hardware** tab, click **Device Manager**.
- Step 4.** Double-click **Network Adapter**
- Step 5.** Right-click mouse button on “**802.11n USB Wireless Network Adapter**”, and choose **Uninstall**
- Step 6.** Click **OK** to confirm that you are going to uninstall the driver

## 3.2 Uninstall the Client Utility

Follow the steps below to remove the Client Utility from your computer.

- Step 1.** To remove the utility from the OS, go to **Start -> Control Panel**
- Step 2.** Double-click **Add-Remove Programs**
- Step 3.** Select **802.11n Wireless Client Utility**, and click the **Remove** button

## 3.3 Upgrading the Wireless Utility

To perform the upgrade, follow the steps below.

- Step 1.** Download the latest version of the utility from the web site and save the file on your computer.
- Step 2.** Follow the steps in *Section 2.2* to remove the current Wireless Utility from your computer.
- Step 3.** Restart your computer if prompted.
- Step 4.** After restarting, refer to the procedure in the Chapter 2 to install the new utility.

# Glossary

For unfamiliar terms used below, look for entries elsewhere in the glossary.

## **AD-HOC (IBSS)**

Ad-hoc mode does not require an AP or a wired network. A network that transmits wireless from computer to computer without the use of a base station (access point).

Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

## **CHANNEL**

A radio frequency used by a wireless device is called a channel.

## **EAP AUTHENTICATION**

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1X transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

## **ENCRYPTION**

The reversible transformation of data from the original to a difficult-to-interpret format. Encryption is a mechanism for protecting confidentiality, integrity, and authenticity of data. It uses an encryption algorithm and one or more encryption keys.

## **FRAGMENTATION THRESHOLD**

This is the maximum data fragment size that can be sent before the packet is fragmented into smaller packets.

## **IEEE 802.1X**

The IEEE 802.1X standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using an external RADIUS server.

## **INFRASTRUCTURE (BSS)**

When a number of wireless stations are connected using a single AP, you have a Basic Service Set (BSS).

## **ROAMING**

In an infrastructure network, wireless stations are able to switch from one BSS to another as they move between the coverage areas. During this period, the wireless stations maintain uninterrupted connection to the network. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate AP depending on the signal strength, network utilization among other factors.

## **SSID**

The SSID (Service Set Identity) is a unique name shared among all wireless devices in a wireless network. Wireless devices must have the same SSID to communicate with each other.

## **TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)**

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server.

## **USER AUTHENTICATION**

WPA applies IEEE 802.1X and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. If you do not have an external RADIUS server, use WPA-PSK/WPA2-PSK (WPA -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, clients will be granted access to a WLAN.

## **WEP**

WEP (Wired Equivalent Privacy) encryption scrambles all data packets transmitted between the WCB-321A and the AP or other wireless stations to keep network communications private. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

## **WPA/WPA2**

Wi-Fi Protected Access (WPA) and WPA2 (future upgrade) is a subset of the IEEE 802.11 security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption. WPA2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.



# TRENDNET®

## Customer Support

Visit [www.trendnet.com/support](http://www.trendnet.com/support)

### Email:

[support@trendnet.com](mailto:support@trendnet.com)



## Europe (Germany • France • Italy • Spain • Switzerland • UK)

**Toll Free Telephone:** +00800 60 76 76 67

English/Espanol - 24/7

Francais/Deutsch - 11 am-8pm, Monday - Friday MET

## Worldwide

**Telephone:** +(31) (0) 20 504 05 35

English/Espanol - 24/7

Francais/Deutsch - 11 am-8pm, Monday - Friday MET

## Product Warranty Registration

Please take a moment to register your product online.

Go to TRENDnet's website at <http://www.trendnet.com/register>

# TRENDNET®

20675 Manhattan Place  
Torrance, CA 90501  
USA