TRENDnet®

# User's Guide

## TEW-623PI

## Copyright



Version 1.0 (June, 2006)

## Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

## Trademark recognition

All product names used in this manual are the properties of their respective owners and are acknowledged.

## 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:**
**FCC Radiation Exposure Statement:**
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

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

# Chapter 1 - Getting Started with the TEW-623PI

Congratulations on purchasing the TEW-623PI! This manual provides information for setting up and configuring the TEW-623PI. This manual is intended for both home users and professionals. It is not required to read some of the more technical information in this manual (such as in “Wireless LAN Networking” and “Configuring Wireless Security”) to operate and enjoy the TEW-623PI. It is included for your reference only.

The following conventions are used in this manual:

NOTE

THE NOTE SYMBOL INDICATES ADDITIONAL INFORMATION ON THE TOPIC AT HAND.

THE TIP SYMBOL INDICATES HELPFULL INFORMATION AND TIPS TO IMPROVE YOUR NETWORK EXPERIENCE.

THE CAUTION SYMBOL ALERTS YOU TO SITUATIONS THAT MAY DEGRADE YOUR NETWORKING EXPERIENCE OR COMPROMISE YOUR SECURITY.

LIKE NOTES AND TIPS, THE IMPORTANT SYMBOL INDICATES INFORMATION THAT CAN IMPROVE NETWORKING. THIS INFORMATION SHOULD NOT BE OVER-LOOKED.

# Chapter 2 - 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 SETTTINGS SHOULD ONLY BE DONE BY AN AUTHORIZED ADMINISTRATOR.

## Transmission Rate (Transfer Rate)

The TEW-623PI provides various transmission (data) rate options for you to select. In most networking scenarios, the factory default Fully Auto setting proves the most efficient. This setting allows your TEW-623PI to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the TEW-623PI 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 TEW-623PI gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

## Types of Wireless Networks

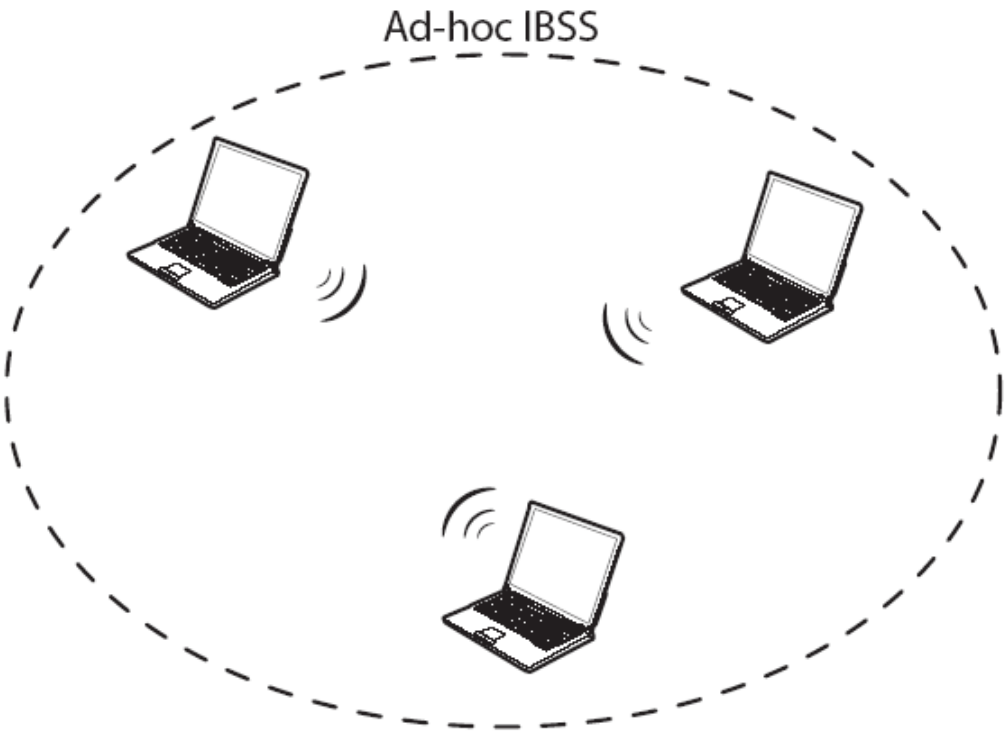
Wireless LAN networking works in either of the two modes: ad-hoc and infrastructure. In infrastructure mode, wireless devices communicate to a wired LAN via access points. Each access point and its wireless devices are known as a Basic Service Set (BSS). An Extended Service Set (ESS) is two or more BSSs 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 TEW-623PI 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

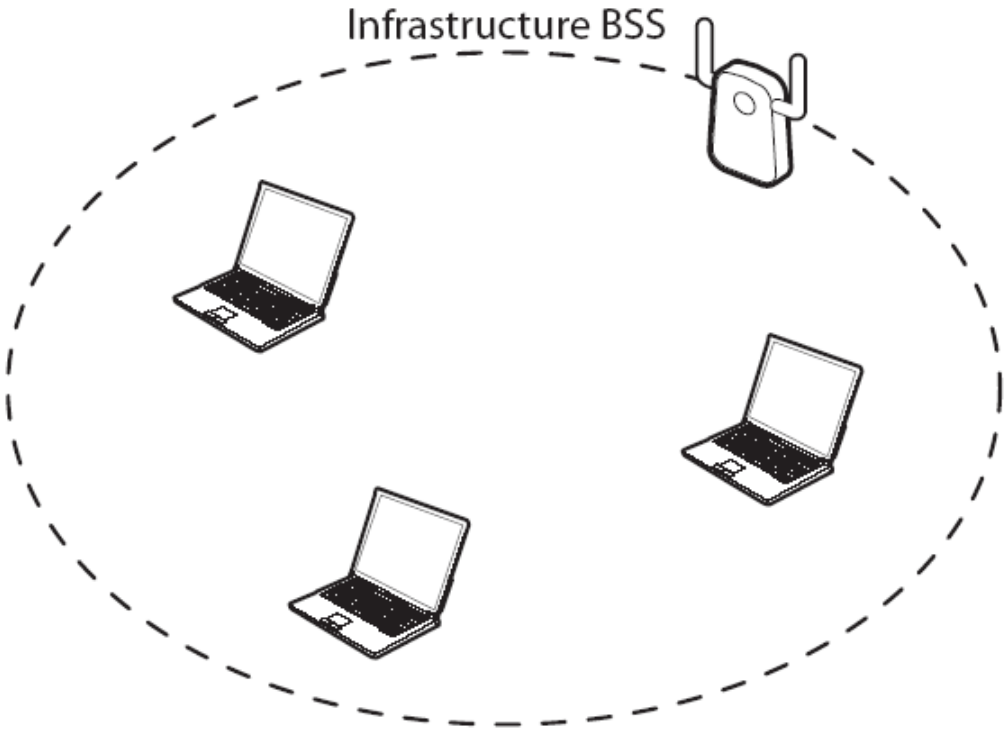
Ad-hoc mode does not require an access point or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

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



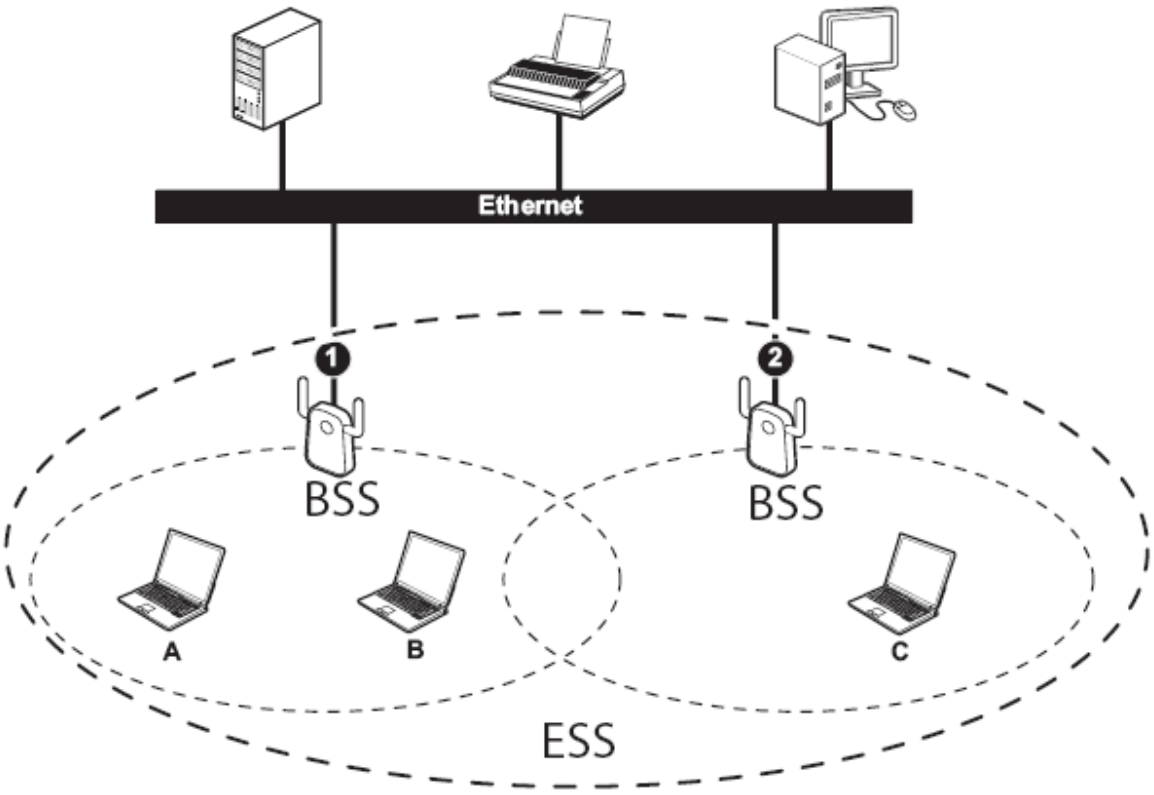

Ad-hoc (also known as peer-to-peer) network diagram

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




Infrastructure (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 TEW-623PI 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, its vital that security settings are clearly understood and applied.

DO NOT ATTEMPT TO CONFIGURE OR CHANGE SECURITY SETTTINGS 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.

The list below shows the possible wireless security levels on your TEW-623PI 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 TEW-623PI 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.

There are two ways to create WEP keys in your TEW-623PI.

- 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 TEW-623PI allows you to configure up to four WEP keys and only one key is used as the default transmit key at any one time.

# Chapter 3 - Hardware and Wireless Utility

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

## About Your Wireless N PCI Adapter

With the Adapter, you can enjoy wireless mobility within almost any wireless networking environment.

The following lists the main features of your Card.

- ✓ Automatic rate selection.
- ✓ Data rate up to 300Mbps.
- ✓ Offers 64-bit, 128-bit WEP (Wired Equivalent Privacy) data encryption for network security.
- ✓ Supports IEEE802.1x and WPA (Wi-Fi Protected Access).
- ✓ Three external antennas.
- ✓ Driver support for Windows Vista/XP/2000.

## Package Content

- ➢ Wireless N PCI Adapter
- ➢ Multi-Language Quick Installation Guide
- ➢ Easy Go CD-ROM

## System Requirement

- Pentium class desktop computers with at least one available PCI slot
- Microsoft Windows Vista, XP or 2K
- CD-ROM drive

## LED Definition

The following table describes the LEDs on the Wireless N PCI Adapter

| STATUS | POWER LED | LINK LED |
|---|---|---|
| *POWER OFF* | OFF | OFF |
| *POWER ON* | Slow Blinking | OFF |
| *Radio on without association* | Two LEDs slow blinking mutually | |
| *Associated without traffic* | Two LEDs slow blinking together | |
| *Associated with traffic* | Two LEDs blinking together per traffic amount | |

# Hardware and Wireless Utility Installation

Follow the instructions below to install the PCI Card and Wireless Utility.

**Windows Vista**

1. Insert the Utility and Driver CD-ROM into your computer's CD-ROM Drive.

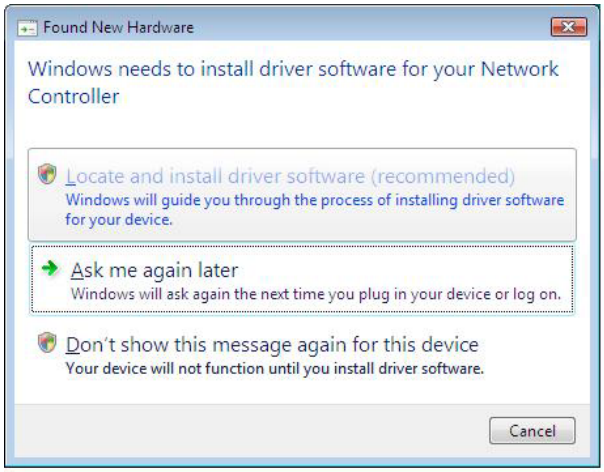
2. Turn off your computer, unplug the power cord and remove the computer's cover.

3. Pick a free PCI expansion slot and remover the protective bracket. Insert the Card into the slot until it is fully seated.

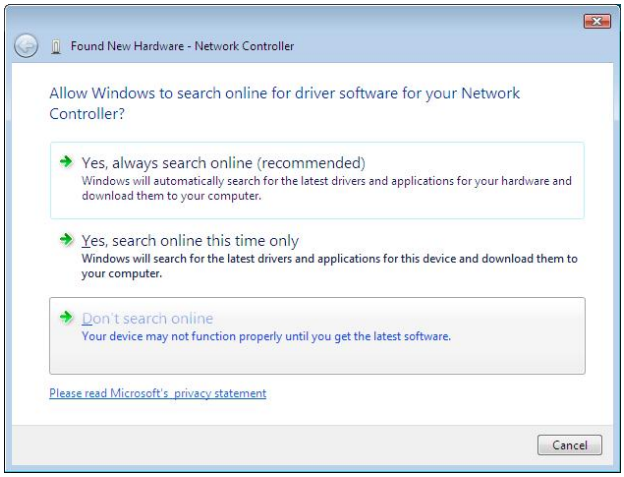
4. Secure the Card bracket with the screw from step 2. Replace the computer's cover.

5. Connect the external antenna to the Card from the SMA connector. And then, reconnect the power cord and power on the computer.

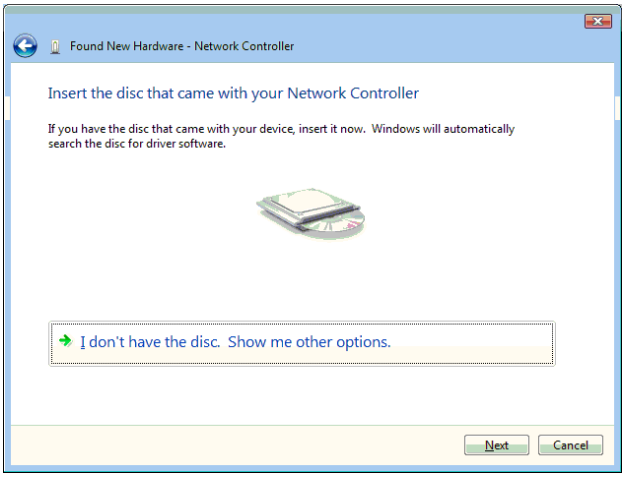
6. Click **Locate and install driver software (recommended).**




7. Click **Don't Search Online**.

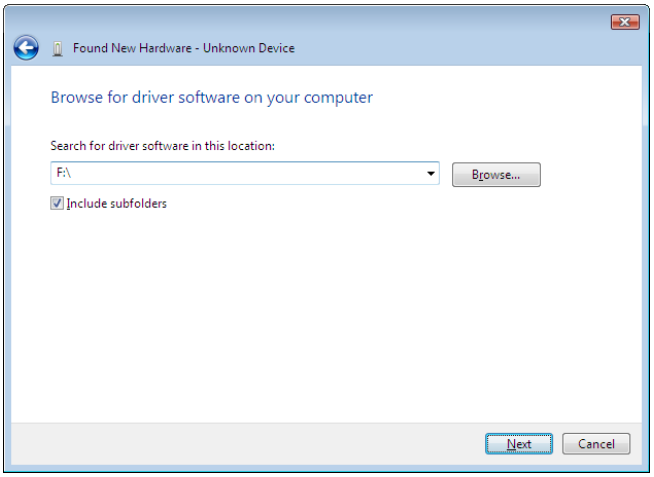


8. Click **I don't have disc. Show me other options.**



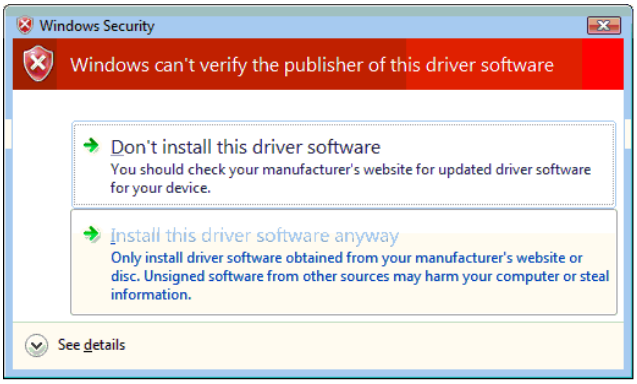

9. Click **Browse my computer for driver software (advanced)**.

10. Type in **F:**. Then click next or click browse to locate the drivers.

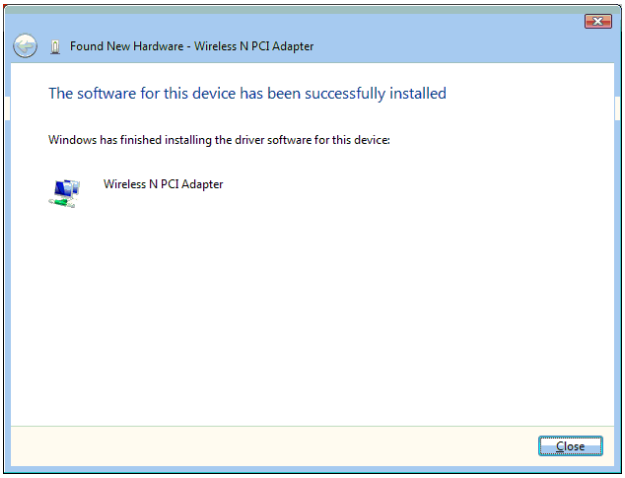



Note: F:\ represents the drive letter that is assigned to your CD-ROM drive.

11. Click **Install this driver software anyways**.



**12.** Click **Close**.

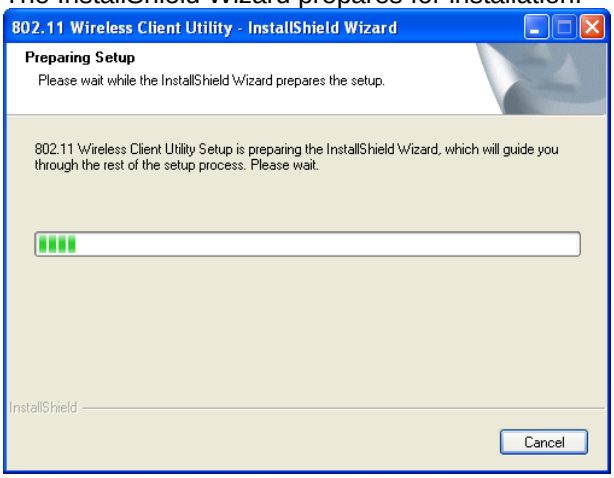



## Windows XP

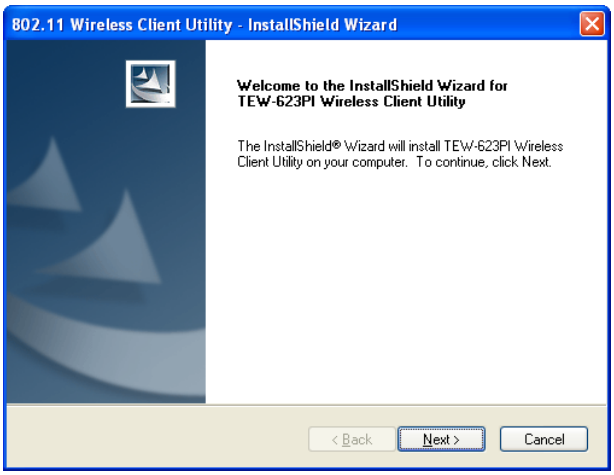
**1.** Insert the Driver and Utility CD into CD drive.

**2.** If your CD Autorun is enabled, the Main Installation Menu will show. Click **Install Driver & Utility**. (Otherwise open your CD folder and double-click on the "**setup.exe**" file)

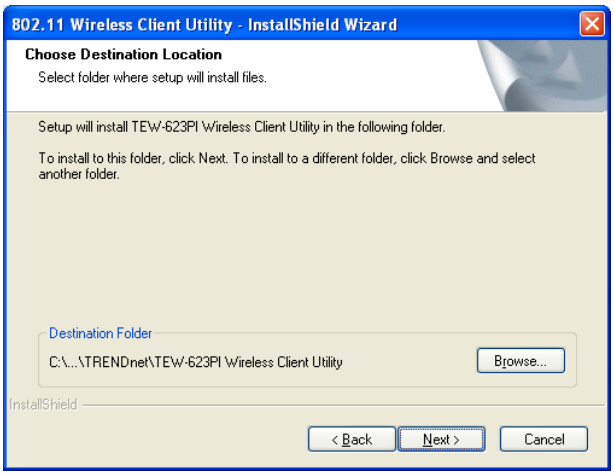
**3.** The InstallShield Wizard prepares for installation.



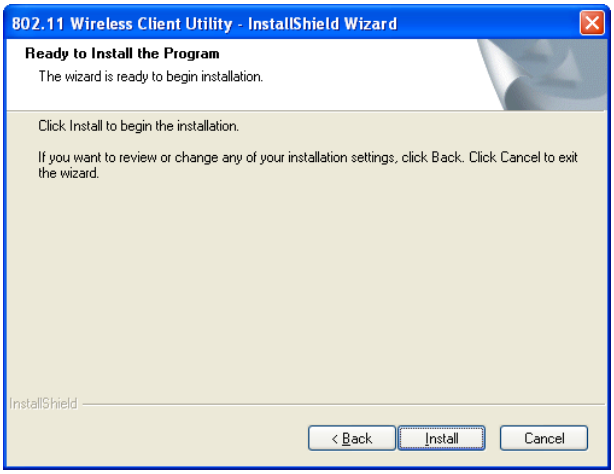

**4.** The InstallShield Wizard prompts you for confirmation. Click **Next** on the following menu.



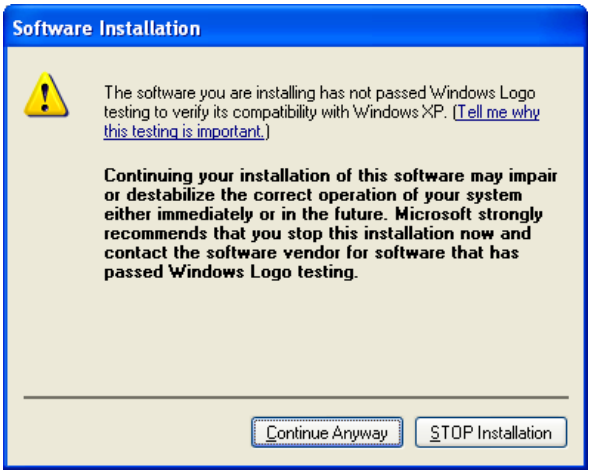

**5.** In the destination Folder screen you are asked to confirm the Destination Folder for the application software. If you would like, you may change the destination folder to another location. Click **Next.**



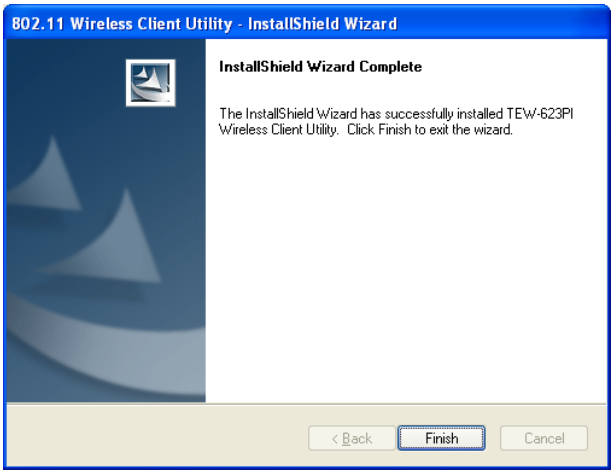
6. The wizard is ready to begin installation. Click **Install** on it.




7. At the Software Installation menu click **Continue Anyway.**




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



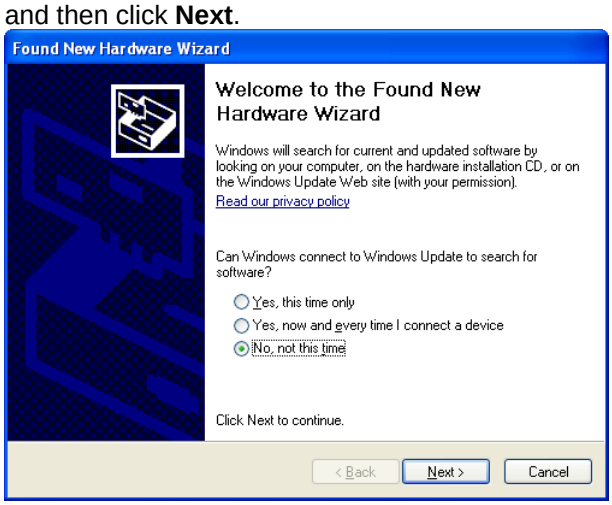

9. Turn off your computer, unplug the power cord and remove the computer's cover.

10. Pick a free PCI expansion slot and remover the protective bracket. Insert the Card into the slot until it is fully seated.

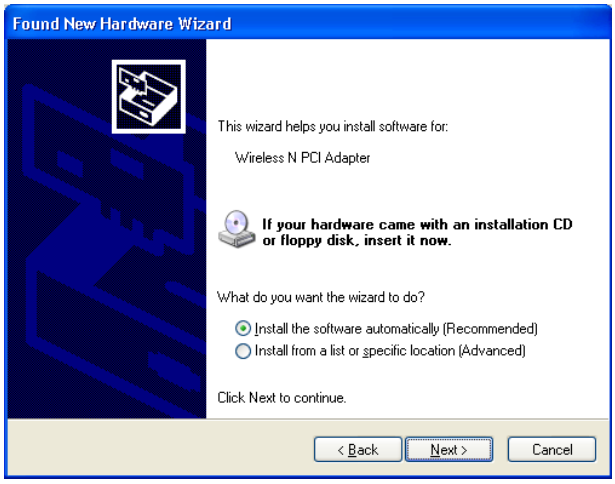
**11.** Secure the Card bracket with the screw from step 2. Replace the computer's cover.

**12.** Connect the external antenna to the Card from the SMA connector. And then, reconnect the power cord and power on the computer.

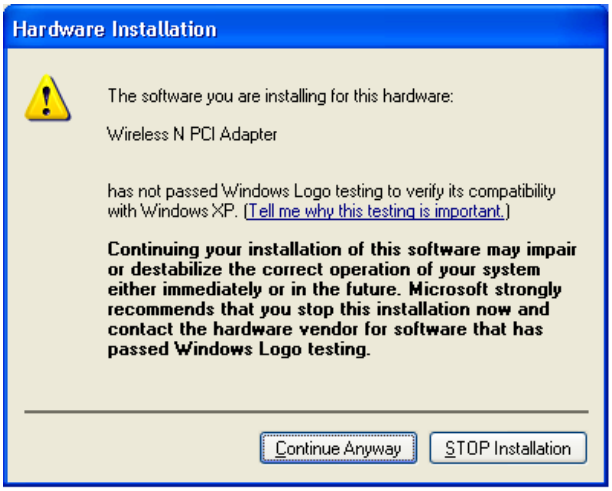
**13.** After power on, you will get the **"Found News Hardware Wizard**" menu. Select **No, not this time** and then click **Next**.



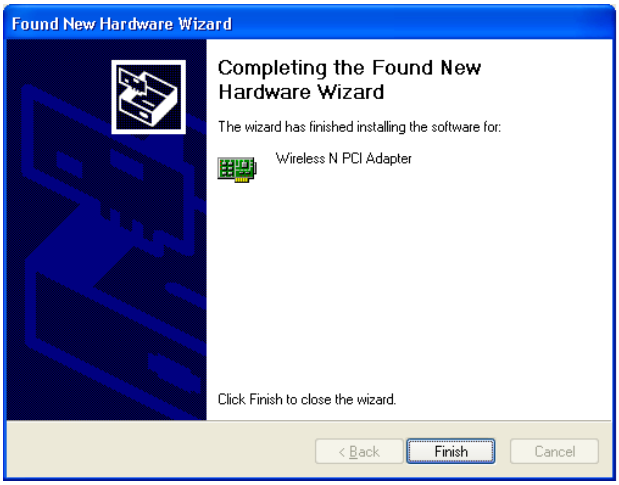

**14.** Choose "**Install the software automatically**" , and click **Next.**




**15.** At the hardware installation menu click **Continue Anyway.** (Our product has been tested under Windows XP and found to be fully compatible click **Continue Anyway.)**




**16.** The Windows has finished installing driver for the device. Click **Finish** to finish the installation.

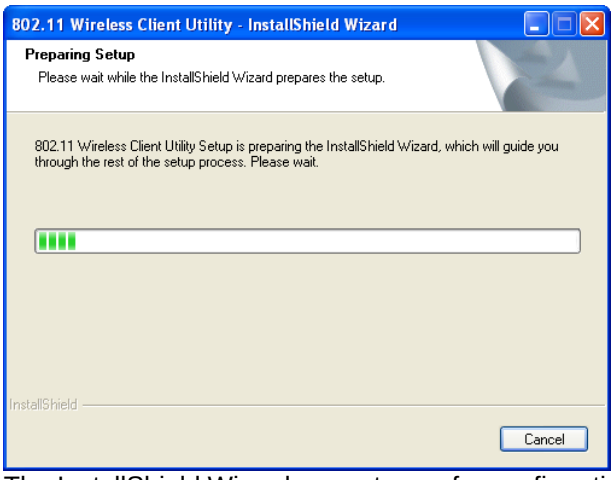



## Windows 2000

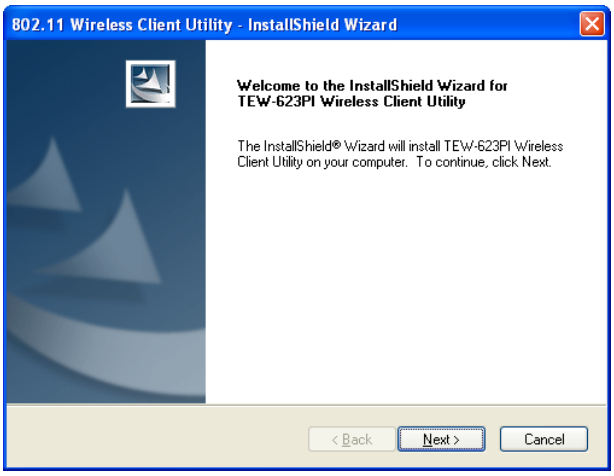
**1.** Insert the Driver and Utility CD into CD drive.

**2.** If your CD Autorun is enabled, the Main Installation Menu will show. Then click **Install Driver & Utility**. (Otherwise open your CD folder and double-click on the "**setup.exe**" file)

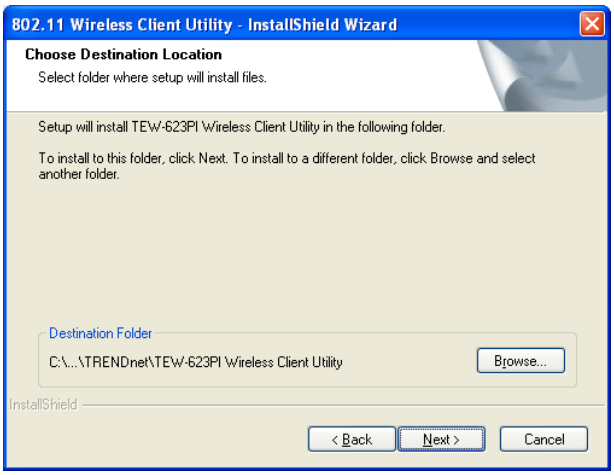
**3.** The InstallShield Wizard prepares for installation.



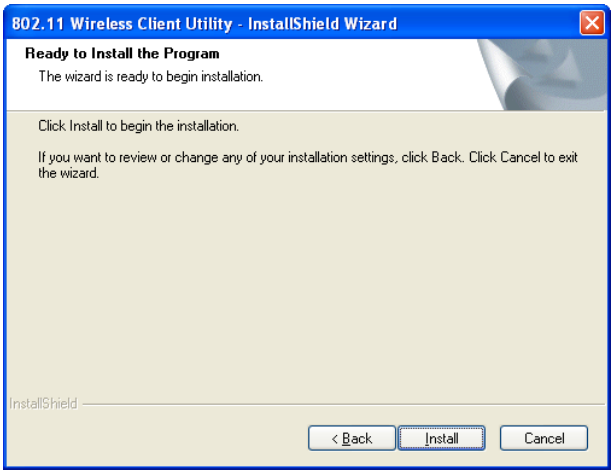

**4.** The InstallShield Wizard prompts you for confirmation. Click **Next** on the following menu.



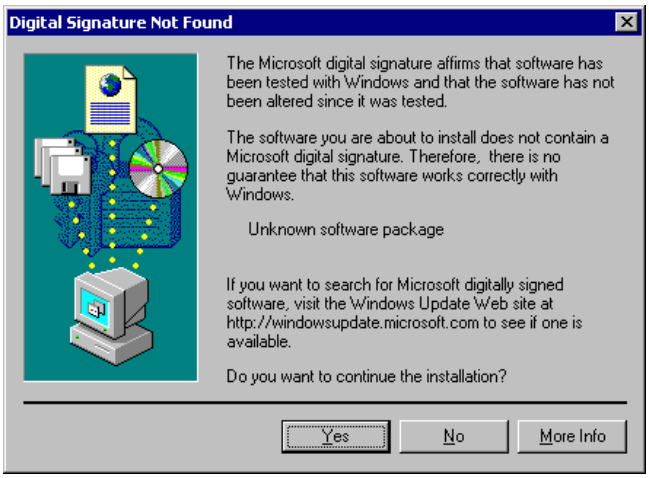

**5.** In the destination Folder screen you are asked to confirm the Destination Folder for the application software. If you would like, you may change the destination folder to another location. Click **Next.**



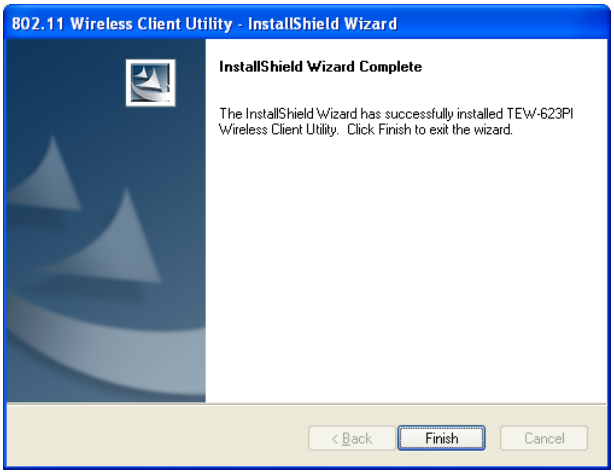
6. The wizard is ready to begin installation. Click **Install** on it.




7. Click **Yes.**




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




9. Turn off your computer, unplug the power cord and remove the computer's cover.

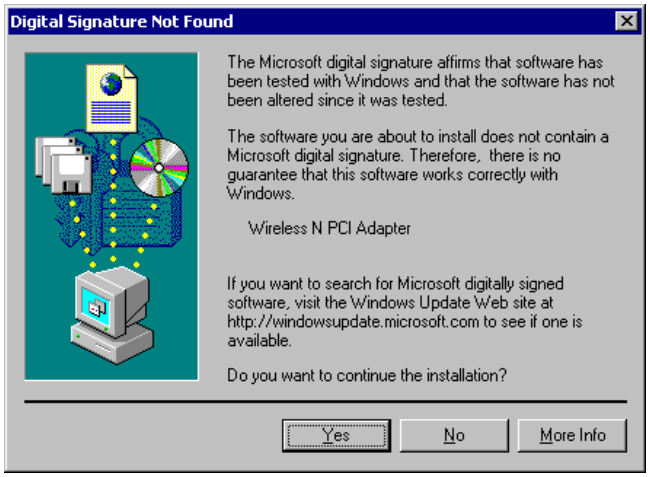
10. Pick a free PCI expansion slot and remover the protective bracket. Insert the Card into the slot until it is fully seated.

**11.** Secure the Card bracket with the screw from step 2. Replace the computer's cover.

**12.** Connect the external antenna to the Card from the SMA connector. And then, reconnect the power cord and power on the computer.

**13.** Drivers will install automatically.

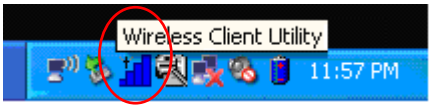
**14.** Click **Yes**.




.

# 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 double click the left 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.

## Link Information

Click the **Link Information** tab to see general information about the program and its operation.


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

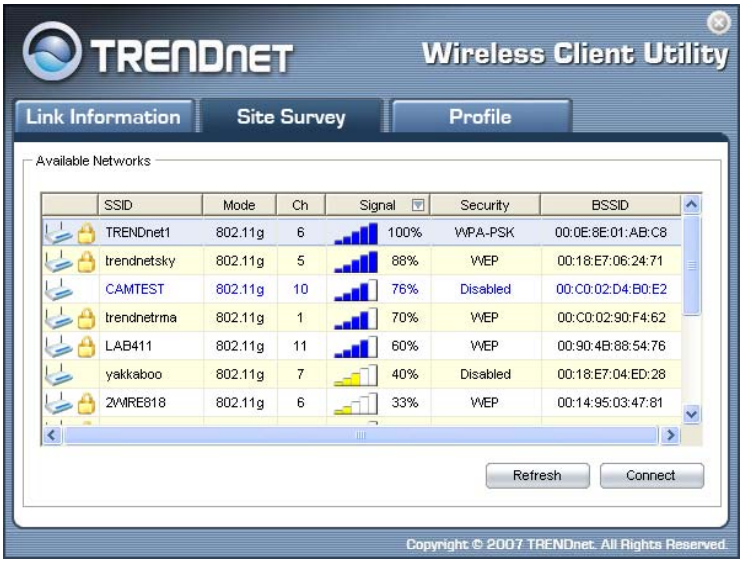
| Wireless Network Status | |
|---|---|
| **Profile Name** | The name of the current selected configuration profile. Set up the configuration name on the **Profile tab.** |
| **SSID** | Displays the wireless network name. |
| **Link Status** | Shows whether the station is associated to the wireless network. |
| **Network Type** | The type of network the station is connected to. The options include:<br>▪ **Infrastructure (access point)**<br>▪ **Ad Hoc** |
| **Wireless Mode** | Displays the wireless mode. 802.11g, 11b or 11n |
| **Transmit Rate** | Displays the current transmit rate in Mbps. |
| **AP MAC Address** | Displays the MAC address of the access point the wireless card is associated to. |
| **Signal Strength** | Shows the strength of wireless signal. |
| **Channel** | |
| **Control Channel** | Channel number of the control 20MHz channel |
| **Extension Channel** | To locate the 40MHz channel on combination with the control channel |

| | |
|---|---|
| **Channel Width** | 20MHz only or 40/20MHz channel support |
| **Security Status** | |
| **Security** | Shows the security type – Disable, WEP, WPA/WPA2, WAP-PSK/WAP2-PSK or 802.1X |
| **Authentication** | Displays the authentication mode. |
| **TCP/IP Status** | |
| **IP Address** | Displays the computer's IP address. |
| **Subnet Mask** | Displays subnet mask |
| **Gateway** | Displays gateway address |

## Site Survey

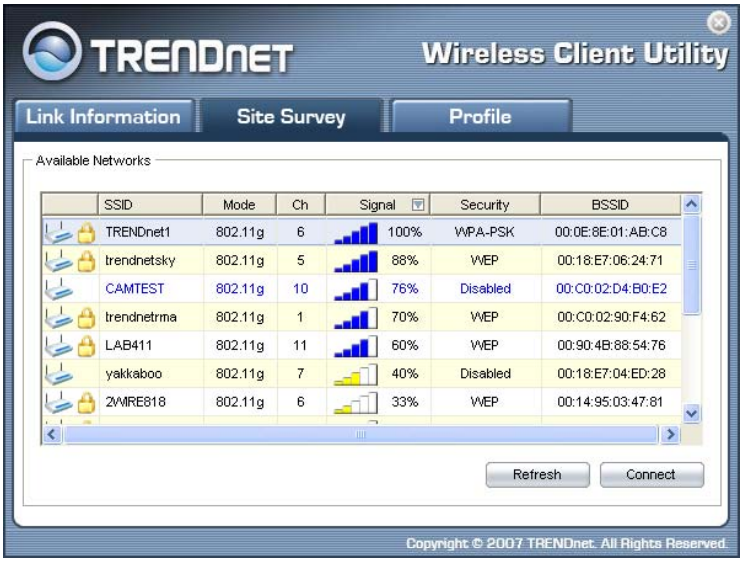
Click the **Site Survey** tab to see available infrastructure and ad hoc networks.

On this screen, click **Refresh** to refresh the list at any time.




### Connecting to a different network

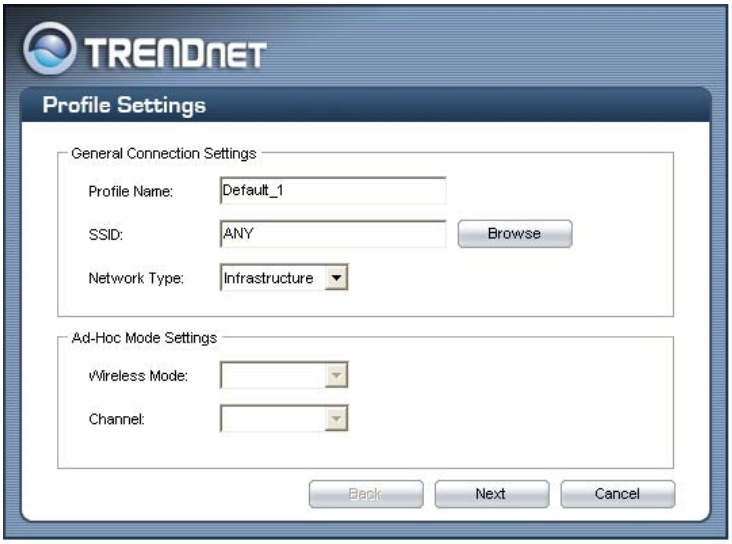
Hold your mouse pointer over the network icon, and click the right mouse button to select the network.




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.

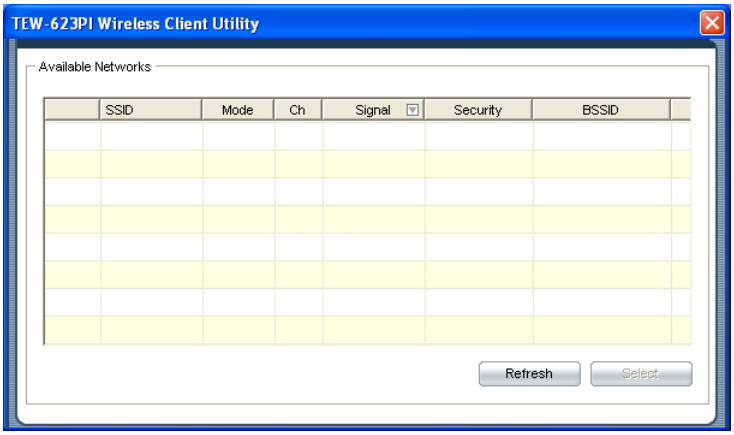
## Profile


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.

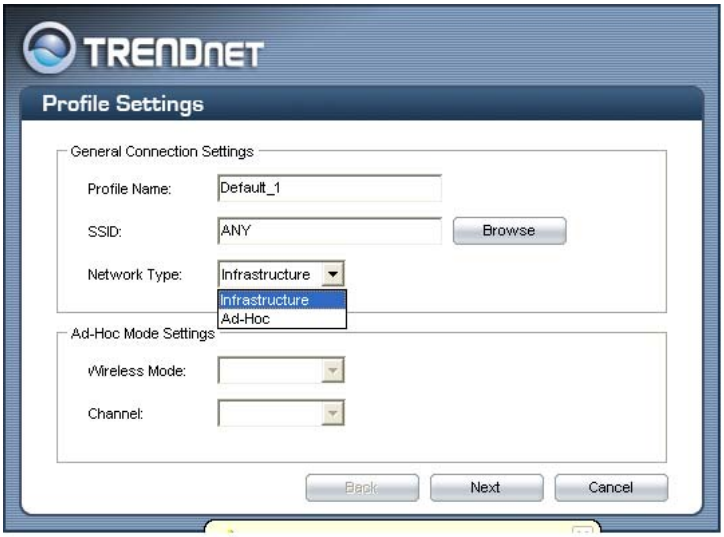



## Scan Available Networks

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.




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.

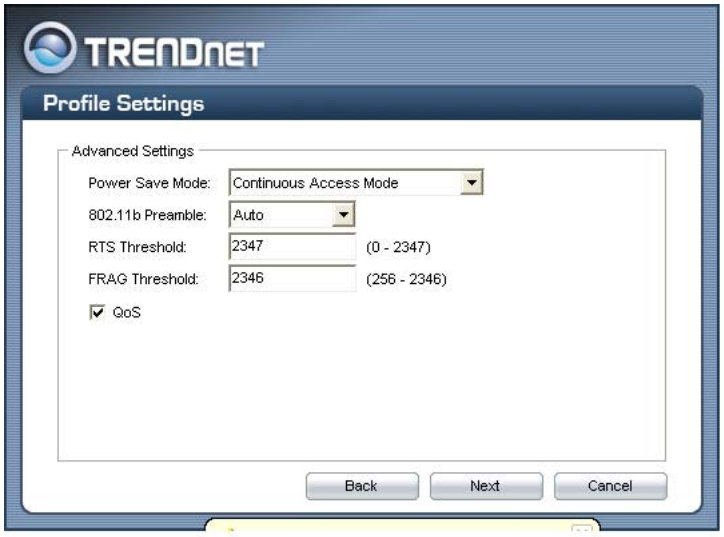

To define the security mode, select the security button of the desired security mode. And then click **Next** to continue. Please see following table for details of security modes.

| | |
|---|---|
| **WEP** | This card support three modes of WEP, include:<br>■ **64 Bits**<br>■ **128 Bits** |
| **WPA/WPA2** | Enables the use of Wi-Fi Protected Access (WPA).<br>Choosing WPA/WPA2 opens the WPA/WPA2 **Security Settings** screen. The options include:<br>■ **TLS (Transport Layer Security)** 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. |

| | |
|---|---|
| | ■ **PEAP (EAP-GTC)** (**Protected Extensible Authentication Protocol)** authenticates wireless LAN clients using only server-side digital certificates by creating an encrypted SSL/TLS tunnel between the client and the authentication server. The tunnel then protects the subsequent user authentication exchange.<br>■ **PEAP (EAP-MSCHAP V2)** (**Protected Extensible Authentication Protocol) To use PEAP (EAP-MSCHAP V2) security**, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager<br>■ **TTLS (Tunneled Transport Layer Security)** An EAP variant that provides mutual authentication using a certificate for server authentication, and via a secure TLS tunnel for the client |
| **WPA-PSK/WPA2-PSK** | Enables WPA/WPA2 Passphrase security.<br>Fill in the WPA/WPA2 Passphrase on **Security Settings** screen. |
| **802.1x** | Enables 802.1x security. This option requires IT administration.<br>Choosing 802.1x opens the 802.1x **Security Settings** screen. The options include:<br>■ **TLS**<br>■ **PEAP**<br>■ **TTLS** |

**Advanced Settings**

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



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

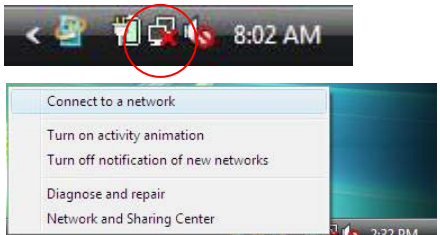
| | |
|---|---|
| **Power Save Mode** | Shows the power save mode. Power management is disabled in ad hoc mode. The options include:<br>• **Continuous Access Mode**<br>• **Maximum Power Saving**<br>• **Fast Power Saving** |
| **802.11b Preamble** | Displays the 802.11b preamble format.<br>The options include:<br>● **Long**<br>● **Short**<br>● **Auto** |
| **RTS Threshold** | Value from 0 ~ 2347 |
| **FRAG Threshold** | Value from 256 ~ 2346 |
| **Wireless Mode** | Enable or disable 802.11n mode. |

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

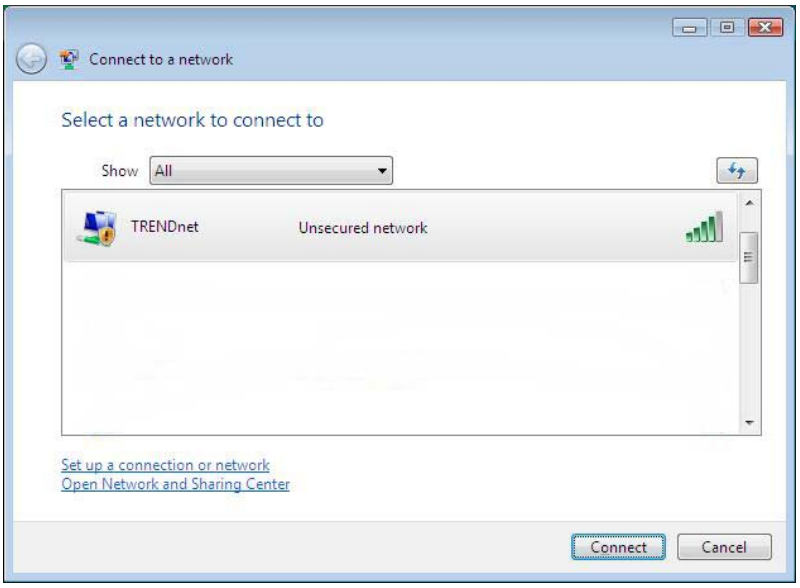

Windows Vista

Connecting to an Unsecured Wireless Connection

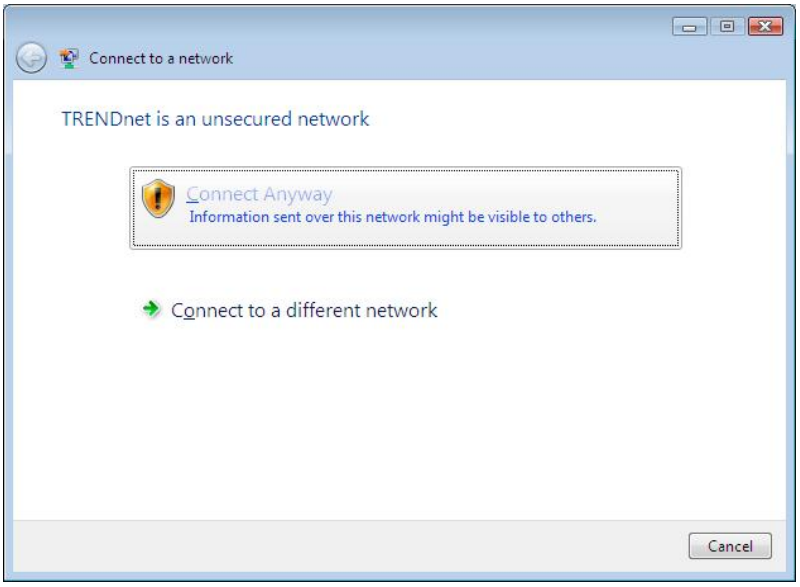
On the bottom right-hand corner of the screen, right click the wireless network connection icon and select Connect to a network.



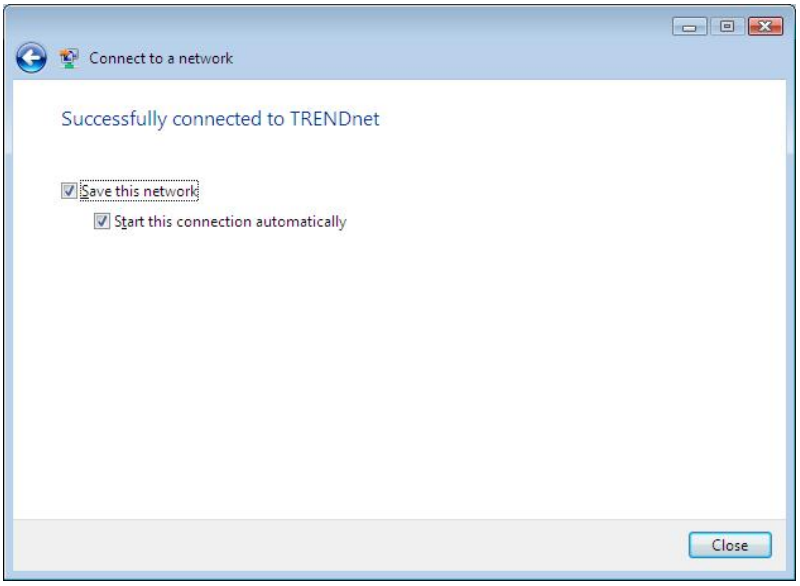
Select the desired network and then click Connect.




Click Connect Anyway.



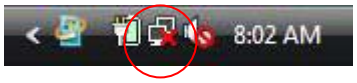

Click Close.

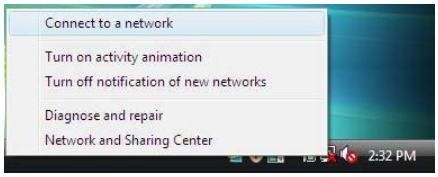



Connecting to a Secured Wireless Connection (WEP-PSK and WPA-PSK)

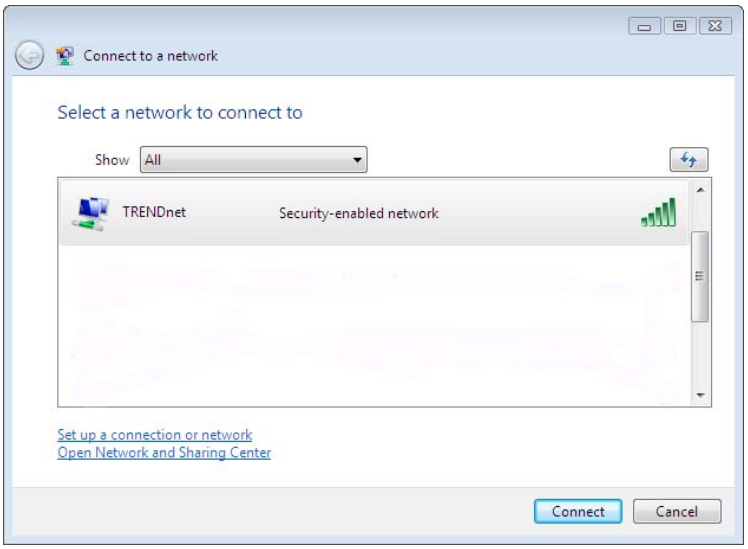
Note: Make sure you know the wireless encryption key before proceeding. If you are not sure, contact the network administrator or log on to your wireless router.

On the bottom right-hand corner of the screen, right click the wireless network connection icon and select Connect to a network.

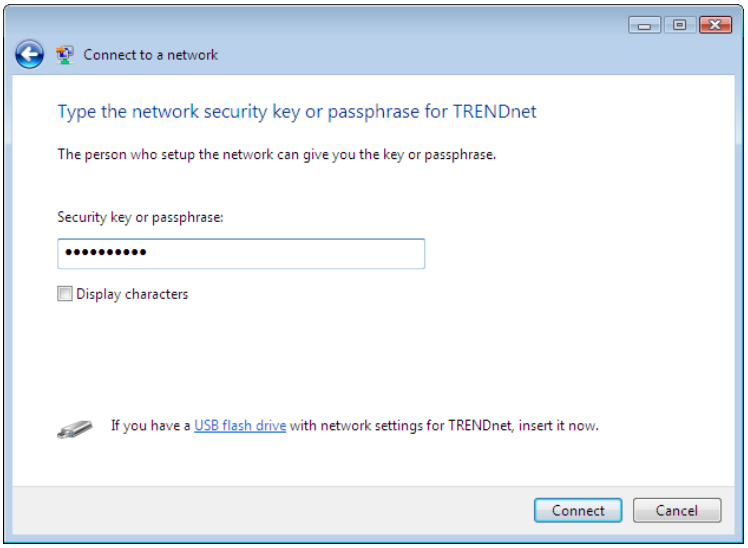


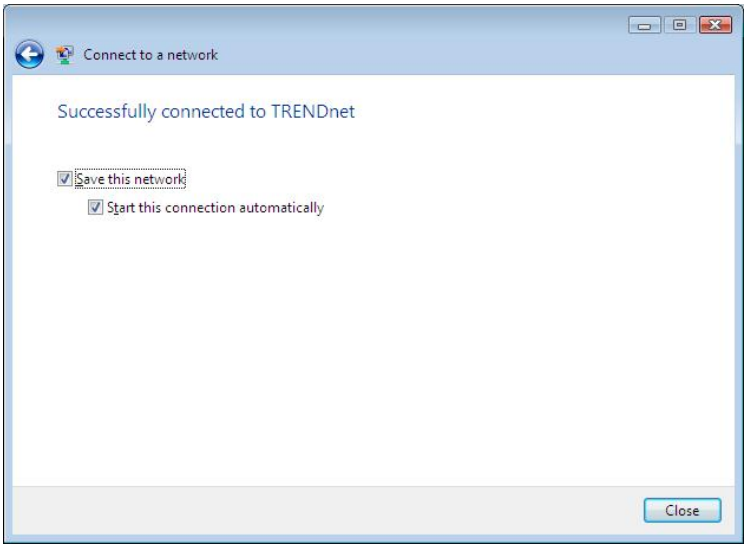

Select the desired network and then click Connect.




Enter the security key and then click Connect.


Connect to a network
Type the network security key or passphrase for TRENDnet
The person who setup the network can give you the key or passphrase.
Security key or passphrase:
Display characters
If you have a USB flash drive with network settings for TRENDnet, insert it now.
Connect
Cancel

Click Close.


Connect to a network
Successfully connected to TRENDnet
Save this network
Start this connection automatically
Close

# Chapter 4 - Maintenance

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

## Uninstall the Driver

Follow the steps below to remove (or uninstall) the Card 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 Card**

**Step 5.** Right-click mouse button on "**TRENDnet TEW-623PI Wireless N PCI Adapter**", and choose **Uninstall**

**Step 6.** Click **OK** to confirm that you are going to uninstall the driver

## 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 **802.11 Wireless Client Utility,** and click the **Uninstall** button

## 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 3.2* 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 WPC-370A 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/PA2

Wi-Fi Protected Access (WPA) and WPA2 is a subset of the IEEE 802.11i 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

# Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

**TEW-623PI 3 Years**

If a product does not operate as warranted above during the applicable warranty period, TRENDnet shall, at its option and expense, repair the defective product or deliver to customer an equivalent product to replace the defective item. All products that are replaced will become the property of TRENDnet. Replacement products may be new or reconditioned.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product through any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet office within the applicable warranty period for a Return Material Authorization (RMA) number, accompanied by a copy of the dated proof of the purchase. Products returned to TRENDnet must be pre-authorized by TRENDnet with RMA number marked on the outside of the package, and sent prepaid, insured and packaged appropriately for safe shipment.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF

THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.
Note: AC/DC Power Adapter, Cooling Fan, Cable and Power Supply carry 1-Year Warranty

# TRENDnet Technical Support


## US • Canada

**Toll Free Telephone:** 1(866) 845-3673

24/7 Tech Support

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

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

English/Espanol - 24/7
Francais/Deutsch - 11am-8pm, Monday - Friday MET

## Worldwide

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

English/Espanol - 24/7
Francais/Deutsch - 11am-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