



**TRENDNET**®



## User's Guide

**TEW-670AP**  
1.01

# Table of Content

<b>INTRODUCTION.....</b>	<b>3</b>
SUMMARY .....	3
KEY FEATURES.....	3
PACKAGE CONTENTS.....	4
SYSTEM REQUIREMENTS .....	4
WIRELESS PERFORMANCE CONSIDERATIONS .....	5
<b>PRODUCT OVERVIEW .....</b>	<b>6</b>
<b>INSTALLATION.....</b>	<b>7</b>
PC NETWORK ADAPTER SETUP (WINDOWS XP).....	7
WIZARD CONFIGURATION .....	8
<b>ADVANCE CONFIGURATION.....</b>	<b>10</b>
STATUS .....	10
LAN .....	11
SCHEDULE.....	12
EVENT LOG .....	13
MONITOR .....	13
<b>WIRELESS 2.4G &amp; 5G .....</b>	<b>14</b>
BASIC.....	14
MODE: WDS.....	15
ADVANCED.....	16
SECURITY.....	17
FILTER.....	19
WPS (WI-FI PROTECTED SETUP) .....	20
CLIENT LIST .....	21
<b>TOOLS.....</b>	<b>21</b>
PASSWORD .....	21
TIME .....	22
POWER SAVING .....	23
DIAGNOSTIC.....	23
FIRMWARE .....	23
BACKUP .....	24
RESTART .....	24
<b>APPENDIX A – FCC INTERFERENCE STATEMENT .....</b>	<b>25</b>
<b>LIMITED WARRANTY .....</b>	<b>26</b>

# Introduction

## Summary

The 300Mbps Concurrent Dual Band Wireless N Access Point provides high performance wireless n speed, coverage, and managed controls.

Concurrent Dual Band technology creates two separate wireless n networks at the same time—one on the 2.4GHz frequency and the other on the less congested 5GHz frequency. Assign high bandwidth clients to the uncongested 5GHz frequency and low bandwidth clients to the more common 2.4GHz frequency.

Multiple Input Multiple Output (MIMO) antenna technology reduces wireless dead spots. Wi-Fi Protected Setup (WPS) integrates other WPS supported devices at the touch of a button. Advanced features include 4 SSIDs per wireless band, access filters for each SSID, WMM Quality of Service data prioritization, WPA2-RADIUS encryption, and real-time bandwidth monitoring for each wireless band.

## Key Features

- IEEE 802.11n and IEEE 802.11a/b/g compliant
  - Transmits simultaneous 2.4GHz and 5GHz Wireless Local Area Network (WLAN) signals (with separate default SSIDs)
  - 1 x 10/100Mbps Auto-MDIX LAN port
  - Functional Access Point and WDS modes provide network flexibility
  - High-speed data rates up to 300Mbps using an IEEE 802.11n connection
  - 2 external antennas provide high-speed performance and expansive wireless coverage
  - Advanced wireless security with 64/128-bit WEP, WPA/WPA2-RADIUS and WPA-PSK/WPA2-PSK
  - Supports multiple SSIDs (up to 4 SSIDs per band)
  - Monitor bandwidth allocation through Web based graphical interface
  - User isolation support (AP mode) and MAC address filter controls
  - Wi-Fi Protected Setup (WPS) integrates wireless clients quickly
  - Wi-Fi Multimedia (WMM) QoS data prioritization
- 
- Easy setup via Web browser using the latest versions of Internet Explorer, FireFox, and Safari
  - Works with Windows, Linux, and Mac operating systems

*\*\* Theoretical wireless signal rate based on IEEE standard of 802.11a, b, g, n chipset used. Actual throughput may vary. Network conditions and environmental factors lower actual throughput rate. All specifications are subject to change without notice.*

## **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 back in its original package.

- TEW-670AP
- Multi-Language Quick Installation Guide
- CD-ROM (User's Guide)
- Cat. 5 Ethernet cable (1m / 3.2ft)
- Power adapter (12V, 1A)

## **System Requirements**

To begin using the TEW-670AP, make sure you meet the following as minimum requirements:

- PC/Notebook.
- Operating System – Microsoft Windows 7/Vista/XP/2000
- 1 Ethernet port.
- WiFi card/USB dongle (802.11 a/b/g/n) – optional.
- PC with a Web-Browser (Internet Explorer, Safari, Firefox, Opera etc.)
- Ethernet compatible CAT5 cables.

## **Wireless Performance Considerations**

There are a number of factors that can impact the range of wireless devices.

1. Adjust your wireless devices so that the signal is traveling in a straight path, rather than at an angle. The more material the signal has to pass through the more signal you will lose.
2. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
3. Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.
4. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.
5. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.
6. Any device operating on the 2.4GHz frequency will cause interference. Devices such as 2.4GHz cordless phones or other wireless remotes operating on the 2.4GHz frequency can potentially drop the wireless signal. Although the phone may not be in use, the base can still transmit wireless signal. Move the phone's base station as far away as possible from your wireless devices.

If you are still experiencing low or no signal consider repositioning the wireless devices or installing additional access points. The use of higher gain antennas may also provide the necessary coverage depending on the environment.

# Product Overview



Front View

- Power/ Status
- Ethernet
- WLAN 2.4GHz
- WLAN 5GHz
- WPS



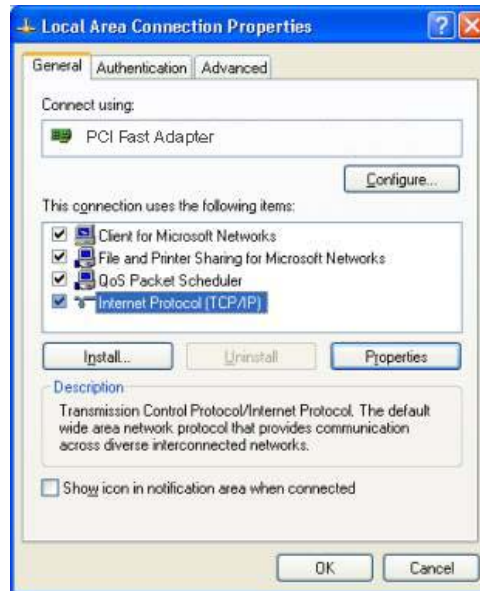
Rear View

- RJ-45: 1 \* 10/100 Fast Ethernet
- Reset Button (5 second for reboot, 5~10 seconds for reset to factory default )
- Power Jack
- WPS push button (Wi-Fi Protected Setup)

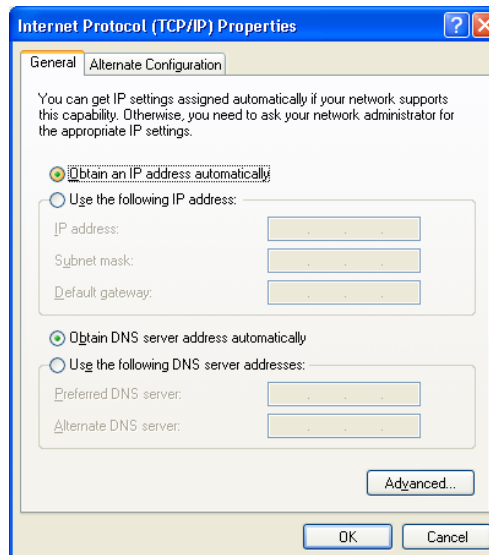
# Installation

## PC Network Adapter setup (Windows XP)

1. Select *Control Panel - Network Connection*.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:



3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.



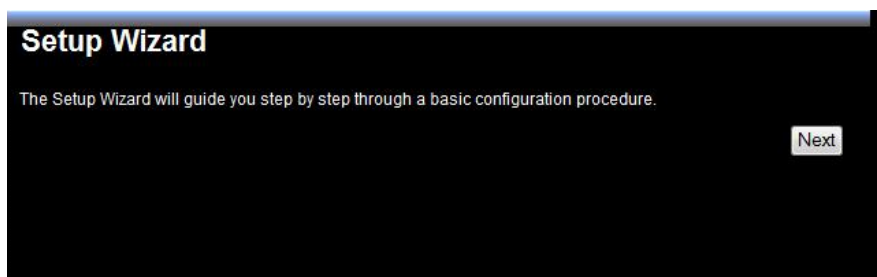
5. Ensure your TCP/IP settings are correct. The default IP address of the TEW-670AP is 192.168.10.100. To manage the TEW-670AP your IP address must be within the same IP scheme 192.168.10.xx

## Wizard Configuration

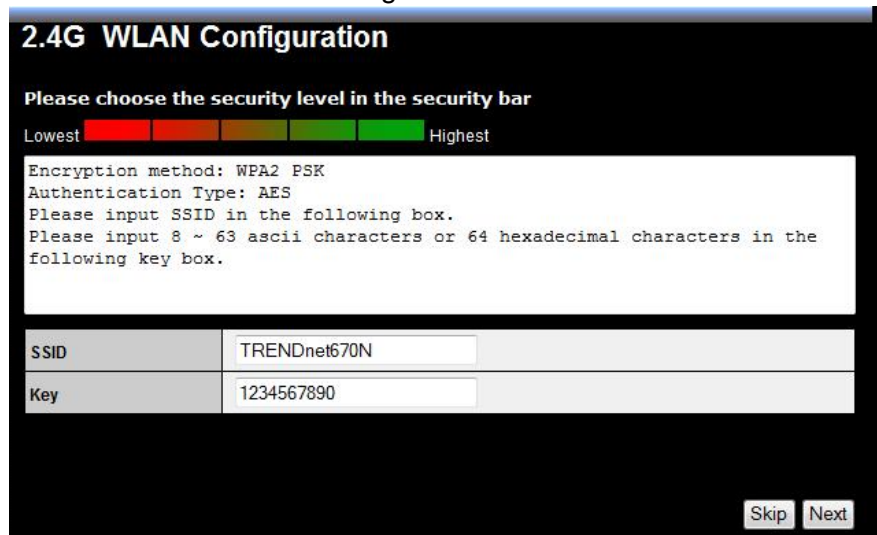
1. Open your browser (e.g. Internet Explorer).
2. Type in `http://192.168.10.100` in the address bar and press Enter.



3. Click **<OK>** to navigate into TEW-670AP configuration home page.



Click **<Next>** to enter WLAN configuration.



Drag the security bar to your settings or enter the name for your wireless network (SSID) and security key. Click **<Next>** to proceed. Repeat steps for setting 5GHz band.



**Setup Successfully**

System Configuration	
Operation Mode	AP

2.4G WLAN Configuration	
SSID	TRENDnet670N
Security	WPA2 pre-shared key
WLAN Key	1234567890

5G WLAN Configuration	
SSID	TRENDnet670A
Security	WPA2 pre-shared key
WLAN Key	1234567890

Verify if settings are accurate and click **Reboot** to apply settings.

**NOTE:**

After Wireless settings are applied, you need to connect from your WLAN client with the security settings you just finished configuring. Remember the type of security & security key.

# Advance Configuration

TEW-670AP provides web-interface for configuration through web browser, such as Internet Explorer, Firefox or Safari.

## Status

This page allows you to monitor the current status of your AP. You can use the status page to quickly see if you have any updated firmware available (bug fixes, updates). You can navigate from this page with a few interesting options for reminding or skipping this page forever & so forth.

Once you click on **<OK>** button to go to the requested page, you can see the status page of the TEW-670AP.

Status	
You can use the Status page to monitor the connection status for WLAN/LAN interfaces, firmware and hardware version numbers.	
System	
Model	Dual Band Wireless N Access Point
Mode	AP
Uptime	3 days 23 hours 3 min 24 sec
Current Date/Time	2009/01/04 23:03:25
Serial Number	266B00003
Kernel version	1.0.2
Firmware version	1.0.2
LAN Settings	
IP address	192.168.10.100
Subnet Mask	255.255.255.0
MAC address	00:14:D1:AA:21:80
WLAN Settings	
Wireless_2.4G Setting	
Channel	11
SSID_1	
ESSID	TRENDnet670N
Security	WPA2 pre-shared key
BSSID	00:14:D1:AA:21:80
Associated Clients	0
WLAN Settings	
Wireless_5G Setting	
SSID_1	
ESSID	TRENDnet670A
Security	WPA2 pre-shared key
BSSID	00:14:D1:AA:21:84
Associated Clients	0

**System:** You can see the UP time, hardware information, serial number as well as firmware version information.

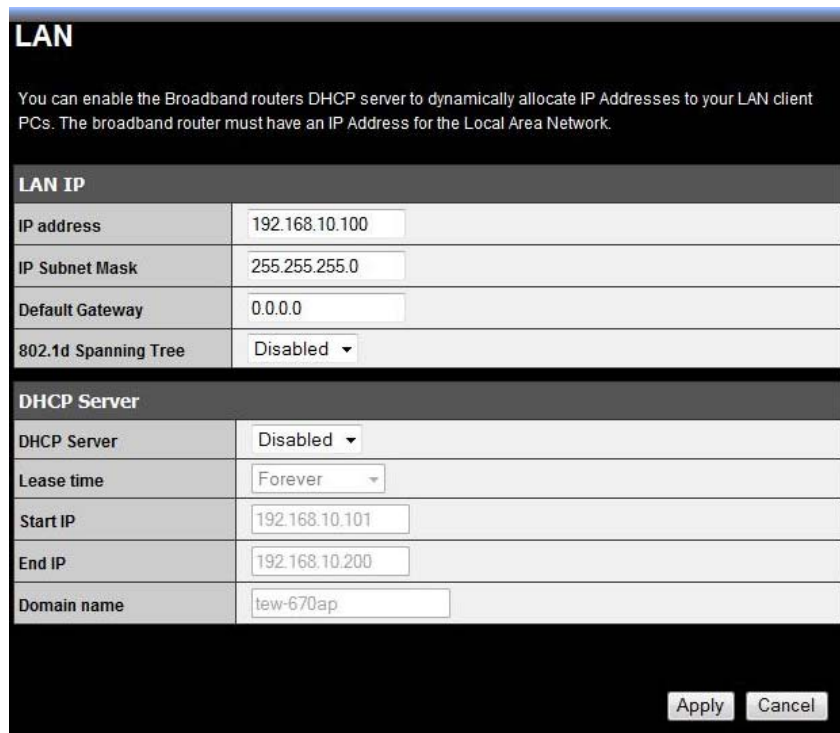
**LAN Settings:** This section displays the Broadband router LAN port's current LAN information. It also shows whether the DHCP Server function is enabled / disabled.

**WLAN Settings:** This section displays the current WLAN configuration settings you've configured in the Wizard / Basic Settings / Wireless Settings section. Wireless configuration details such as SSID, Security settings, BSSID, Channel number, mode of operation are briefly shown.

## LAN

The LAN Tabs reveals LAN settings which can be altered at will. If you are an entry level user, try accessing a website from your browser. If you can access website without a glitch, just do not change any of these settings.

Click **<Apply>** at the bottom of this screen to save the changed configurations.



The screenshot shows a configuration window titled "LAN". At the top, there is a note: "You can enable the Broadband routers DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network." Below this, the settings are organized into two sections: "LAN IP" and "DHCP Server".

LAN IP	
IP address	192.168.10.100
IP Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
802.1d Spanning Tree	Disabled ▾

DHCP Server	
DHCP Server	Disabled ▾
Lease time	Forever ▾
Start IP	192.168.10.101
End IP	192.168.10.200
Domain name	tew-670ap

At the bottom right of the window, there are two buttons: "Apply" and "Cancel".

### **LAN IP**

**IP address:** 192.168.0.1. It is the AP's LAN IP address (Your LAN clients default gateway IP address). It can be changed based on your own choice.

**IP Subnet Mask:** 255.255.255.0 Specify a Subnet Mask for your LAN segment.

**Default Gateway:** Specify a gateway for your LAN segment.

**802.1d Spanning Tree:** This is disabled by default. If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops.

### **DHCP Server**

**DHCP Server:** This will enable or disable the Dynamic Pool setting..

**Lease time:** This is the lease time of each assigned IP address.

**Start IP:** This will be the beginning of the pool of IP addresses available for client devices.

**End IP:** This will be the end of the pool of IP addresses available for client devices.

**Domain name:** The Domain Name for the existing or customized network.

## Schedule

This page allows user to set up schedule function for Firewall and Power Saving.

**Schedule**

You can use the Schedule page to Start/Stop the Services regularly. The Schedule will start to run, when it get GMT Time from Time Server. Please set up the Time Server correctly in Toolbox. The services will start at the time in the following Schedule Table or it will stop.

Enabled Schedule Table (up to 8)

NO.	Description	Service	Schedule	Select
-----	-------------	---------	----------	--------

Add Edit Delete Selected Delete All

Apply Cancel

Add schedule, edit schedule options to allow configuration of firewall and power savings services. Fill in the schedule and select type of service. Click **<Apply>** to implement those settings.

**Schedule**

You can use the Schedule page to Start/Stop the Services regularly. The services will start at the time in the following Schedule Table or it will stop.

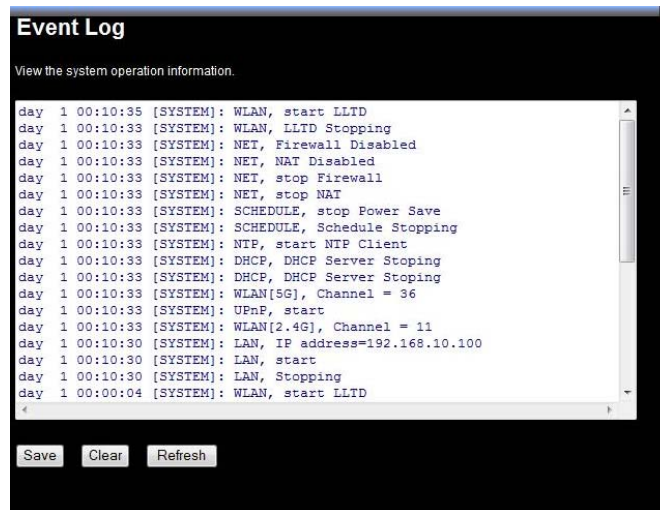
Schedule Description	schedule 01
Service	<input type="checkbox"/> Power Saving
Days	<input type="checkbox"/> Every Day <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun
Time of day	<input type="checkbox"/> All Day (use 24-hour clock) From 0 : 0 To 0 : 0

Apply Cancel

The schedule table lists the pre-schedule service-runs. You can select any of them using the check box.

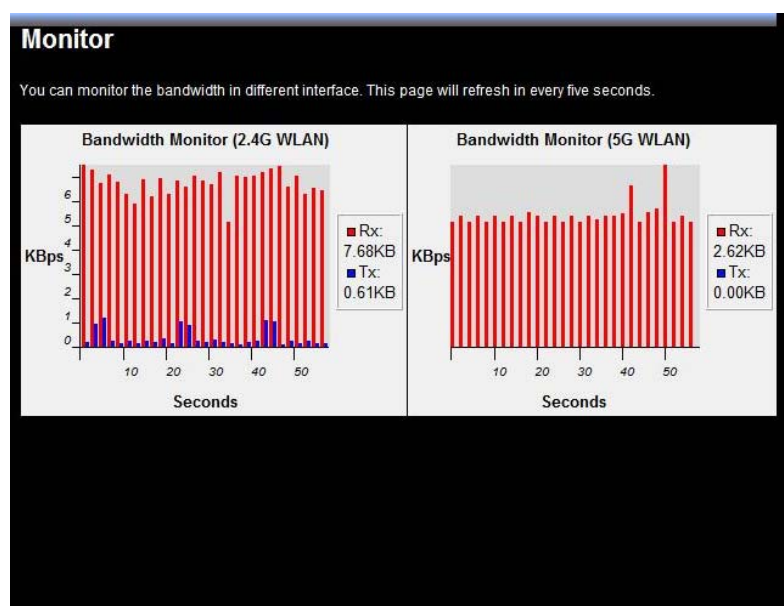
## Event Log

View **operation event log**. This page shows the current system log of the Broadband router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved **<Save>** to a local file for further processing or the system log can be cleared **<Clear>** or it can be refreshed **<Refresh>** to get the most updated information. When the system is powered down, the system log will disappear if not saved to a local file.



## Monitor

Show histogram for network connection on LAN & WLAN. Auto refresh keeps information updated frequently.



# WIRELESS 2.4G & 5G

TEW-670AP is a dual band concurrent product, therefore two wireless radio configurations are provided. Both radios share the same features except for open band and available channels under “Basic” section.

## Basic

Basic	
This page allows you to define SSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point	
Radio	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode	AP
Band	2.4 GHz (802.11n)
Enabled SSID#	1
SSID1	TRENDnet670N
Auto Channel	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	11

Apply Cancel

**Radio:** You can turn on/off wireless radio. If wireless Radio is off, you cannot associate with AP through wireless.

**Mode:** In this device, we support two operation modes which are **Access Point** and **WDS** (Wireless Distribution System).

**Band:** You can select the wireless standards running on your network environment.

### **Band 2.4G:**

**2.4 GHz(B):** If all of your clients are 802.11b, select this one.

**2.4 GHz(G):** If all of your clients are 802.11g, select this one.

**2.4 GHz(B/G):** Either an 802.11b or an 802.11g wireless devices are in your environment.

**2.4 GHz(N):** If all of your clients are 802.11n, select this one.

**2.4 GHz(B/G/N):** Either 802.11b, 802.11g, or 802.11n wireless devices are in your environment.

### **Band 5G**

**5 GHz (A):** If all of your clients are 802.11a, select this one.

**5 GHz (N):** If all of your clients are 802.11n, select this one.

**5 GHz (A/N):** Either 802.11a or 802.11n wireless devices are in your environment.

**Enable SSID#:** We support 4 multiple SSIDs in this device. Please select how many SSIDs you would like to use in your network environment.

**ESSID1~4:** ESSID is the name of your wireless network. It might be a unique name to identify this wireless device in the Wireless LAN. It is case sensitive and up to 32 printable characters. You might change the default ESSID for added security.

**Auto Channel:** Device will search all valid channels, then decide a most clean channel and change to this channel if you enable this function. Depend on this function enable or not, you will see different item below **Auto Channel**.

**Channel:** If Auto Channel is disabled, you should choose a static channel and AP will use this channel to communicate with other clients.

Basic	
This page allows you to define SSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point	
Radio	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode	AP
Band	5 GHz (802.11a/n)
Enabled SSID#	1
SSID1	TRENDnet670A
Auto Channel	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	36 5.180 GHz
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

## Mode: WDS

Wireless Distribution System, a system that enables the wireless interconnection of access point, allows a wireless network to be expended using multiple access points without a wired backbone to like them. Each WDS APs need setting as same channel and encryption type.

Radio	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode	WDS
Band	2.4 GHz (802.11n)
Enabled SSID#	1
SSID1	TRENDnet670N
Channel	11
MAC address 1	000000000000
MAC address 2	000000000000
MAC address 3	000000000000
MAC address 4	000000000000
WDS Data Rate	300M
Set Security	<input type="button" value="Set Security"/>

**MAC address 1~4:** Please enter the MAC address of the neighboring APs that participates in WDS, we support 4 devices now.

**Set Security:** WDS Security depends on your AP security settings. Note: it does not support **mixed mode** such as WPA-PSK/WPA2-PSK Mixed mode.

## **Advanced**

This tab allows you to set the advanced wireless options. The options included are Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, and Preamble Type. You should not change these parameters unless you know what effect the changes will have on the router.

Advanced		
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router		
Fragment Threshold	2346	(256-2346)
RTS Threshold	2347	(1-2347)
Beacon Interval	100	(20-1024 ms)
DTIM Period	1	(1-255)
N Data rate	Auto	
Channel Bandwidth	<input checked="" type="radio"/> Auto 20/40 MHz	<input type="radio"/> 20 MHz
Preamble Type	<input type="radio"/> Long Preamble	<input checked="" type="radio"/> Short Preamble
CTS Protection	<input checked="" type="radio"/> Auto	<input type="radio"/> Always <input type="radio"/> None
Tx Power	100 %	

Apply Cancel

**Fragment Threshold:** This specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.

**RTS Threshold:** When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.

**Beacon Interval:** is the interval of time that this wireless router broadcasts a beacon. A Beacon is used to synchronize the wireless network.

**DTIM Period:** Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages

**Data Rate:** The “Data Rate” is the rate that this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.

**N Data Rate:** The “Data Rate” is the rate that this access point uses to transmit data packets for N compliant wireless nodes. Highest to lowest data rate can be fixed.



**Channel Bandwidth:** This is the range of frequencies that will be used.

**Preamble Type:** The “Long Preamble” can provide better wireless LAN compatibility while the “Short Preamble” can provide better wireless LAN performance.

**CTS Protection:** It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to a lot of frame-network that is transmitted.

**TX Power:** This can be set to a bare minimum or maximum power.

## **Security**

This Access Point provides complete wireless LAN security functions, included are WEP, IEEE 802.1x, IEEE 802.1x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function, and are setup with the same security key.

Security	
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.	
SSID Selection	TRENDnet670A ▾
Broadcast SSID	Enable ▾
WMM	Enable ▾
Encryption	WPA pre-shared key ▾
WPA type	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key type	Passphrase ▾
Pre-shared Key	1234567890
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**ESSID Selection:** This broadband router support multiple ESSID, you could select and set up the wanted ESSID.

**Broadcast ESSID:** If you enabled “Broadcast ESSID”, every wireless station located within the coverage of this access point can discover this access point easily. If you are building a public wireless network, enabling this feature is recommended. Disabling “Broadcast ESSID” can provide better security.

**WMM:** Wi-Fi MultiMedia if enabled supports QoS for experiencing better audio, video and voice in applications.

**Encryption:** When you choose to disable encryption, it is very insecure to operate TEW-670AP.

## WEP Encryption

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as a default key. Then the router can receive any packets encrypted by one of the four keys.

SSID Selection	TRENDnet670N ▾
Broadcast SSID	Enable ▾
WMM	Enable ▾
Encryption	WEP ▾
Authentication type	<input checked="" type="radio"/> Open System <input type="radio"/> Shared Key <input type="radio"/> Auto
Key Length	64-bit ▾
Key type	Hex (10 characters) ▾
Default key	Key 1 ▾
Encryption Key 1	*****
Encryption Key 2	*****
Encryption Key 3	*****
Encryption Key 4	*****
802.1x Authentication	<input type="checkbox"/> Enable 802.1x Authentication

**Authentication Type:** There are two authentication types: "**Open System**" and "**Shared Key**". When you select "**Open System**", wireless stations can associate with this wireless router without WEP encryption. When you select "**Shared Key**", you should also setup a WEP key in the "**Encryption**" page. After this has been done, make sure the wireless clients that you want to connect to the device are also setup with the same encryption key.

**Key Length:** You can select the WEP key length for encryption, 64-bit or 128-bit. The larger the key will be the higher level of security is used, but the throughput will be lower.

**Key Type:** You may select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.

**Key1 - Key4:** The WEP keys are used to encrypt data transmitted in the wireless network. Use the following rules to setup a WEP key on the device. 64-bit WEP: input 10-digits Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

Click **<Apply>** at the bottom of the screen to save the above configurations. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

## Enable 802.1x Authentication

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.

## WPA Pre-Shared Key Encryption

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be cracked by hackers. This is the best security available.

SSID Selection	TRENDnet670N ▾
Broadcast SSID	Enable ▾
WMM	Enable ▾
Encryption	WPA RADIUS ▾
WPA type	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
RADIUS Server IP address	<input type="text"/>
RADIUS Server port	1812
RADIUS Server password	<input type="text"/>

## WPA-Radius Encryption

Wi-Fi Protected Access (**WPA**) is an advanced security standard of IEEE 802.1x authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.

It uses **TKIP** or **CCMP (AES)** to change the encryption key frequently. Press **<Apply>** button when you are done.

## Filter

This wireless router supports MAC Address Control, which prevents unauthorized clients from accessing your wireless network.

### Filter

For security reason, the Access Point features MAC Address Filtering which only allows authorized MAC Addresses to associate with the Access Point

Enable Wireless Access Control

Description	MAC address
<input type="text"/>	<input type="text"/>

#### MAC Address Filtering Table

NO.	Description	MAC address	Select
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**Enable wireless access control:** Enable the wireless access control function  
**Adding an address into the list**

Enter the "MAC Address" and "Comment" of the wireless station to be added and then click **<Add>**. The wireless station will now be added into the "Current Access Control List" below. If you are having any difficulties filling in the fields, just click "Clear" and both "MAC Address" and "Comment" fields will be cleared.

**Remove an address from the list**

If you want to remove a MAC address from the "Current Access Control List", select the MAC address that you want to remove in the list and then click "Delete Selected". If you want to remove all the MAC addresses from the list, just click the **<Delete All>** button. Click **<Reset>** will clear your current selections.

Click **<Apply>** at the bottom of the screen to save the above configurations.

**WPS (Wi-Fi Protected Setup)**

WPS is the simplest way to establish a connection between the wireless clients and the wireless router. You don't have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both wireless client and wireless router, and the WPS will do the rest for you.

The wireless router supports two types of WPS: WPS via Push Button and WPS via PIN code. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the 'Start to Process' button in the web configuration interface. If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the wireless router.

WPS	
WPS	<input checked="" type="checkbox"/> Enable
Wi-Fi Protected Setup Information	
WPS Current Status	Configured <input type="button" value="Release Configuration"/>
Self Pin Code	11497004
SSID	TRENDnet670A
Authentication Mode	WPA2 pre-shared key
Passphrase Key	<input type="text" value="1234567890"/>
WPS Via Push Button	<input type="button" value="Start to Process"/>
WPS via PIN	<input type="text"/> <input type="button" value="Start to Process"/>

**WPS:** Check the box to enable WPS function and uncheck it to disable the WPS function.

**WPS Current Status:** If the wireless security (encryption) function of this wireless router is properly set, you'll see a 'Configured' message here. Otherwise, you'll see '**UnConfigured**'.

**Self Pin Code:** This is the WPS PIN code of the wireless router. You may need this information when connecting to other WPS-enabled wireless devices.

**SSID:** This is the network broadcast name (SSID) of the router.

**Authentication Mode:** It shows the active authentication mode for the wireless connection.

**Passphrase Key:** It shows the passphrase key that is randomly generated by the wireless router during the WPS process. You may need this information when using a device which doesn't support WPS.

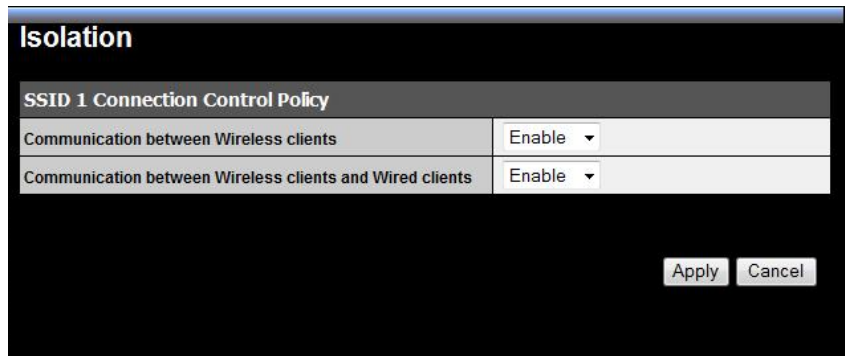
**Interface:** If device is set to repeater mode, you can choose “**Client**” interface to connect with other AP by using WPS, otherwise you may choose “**AP**” interface to do WPS with other clients.

**WPS via Push Button:** Press the button to start the WPS process. The router will wait for the WPS request from the wireless devices within 2 minutes.

**WPS via PIN:** You can fill-in the PIN code of the wireless device and press the button to start the WPS process. The router will wait for the WPS request from the wireless device within 2 minutes.

## Client List

This WLAN Client Table shows the Wireless client associate to this Wireless Router.



SSID 1 Connection Control Policy	
Communication between Wireless clients	Enable ▾
Communication between Wireless clients and Wired clients	Enable ▾

Apply Cancel

## TOOLS

### Password

You can change the password required to log into the broadband AP's system web-based management. By default, the password is: admin. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

**Password**

You can change the password that you use to access the router, this is not your ISP account password.

Old Password	<input type="text"/>
New Password	<input type="text"/>
Repeat New Password	<input type="text"/>

Apply Reset

**Old Password:** Fill in the current password to allow changing to a new password.

**New Password:** Enter your new password and type it again in **Repeat New Password** for verification purposes

## Time

The Time Zone allows your AP to reference or base its time on the settings configured here, which will affect functions such as Log entries and Schedule settings.

**Time**

The Router reads the correct time from NTP servers on the Internet and sets its system clock accordingly. The Daylight Savings option merely advances the system clock by one hour. The time zone setting is used by the system clock when displaying the correct time in schedule and the log files.

Time Setup	Synchronize with the NTP Server ▾
Time Zone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾
NTP Time Server	<input type="text"/>
Daylight Saving	<input type="checkbox"/> Enable From <input type="text" value="January"/> <input type="text" value="1"/> To <input type="text" value="January"/> <input type="text" value="1"/>

Apply Reset

**Time Setup:** Select “Synchronize with the NTP Server” or “Synchronize with PC”.

**Time Zone:** Select the time zone of the country you are currently in. The router will set its time based on your selection.

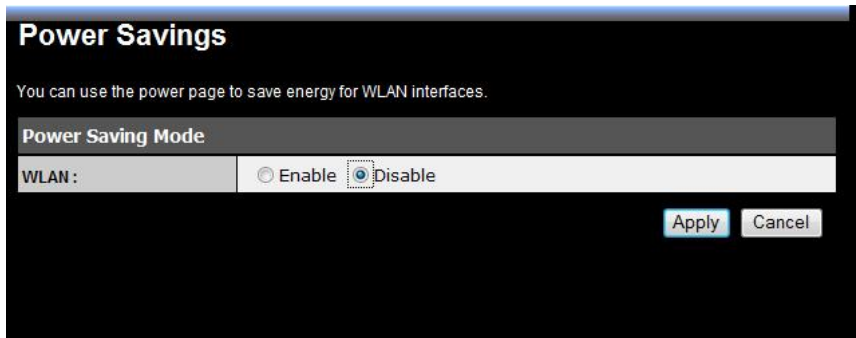
**NTP Time Server:** The router can set up external NTP Time Server.

**Daylight Savings:** The router can also take Daylight Savings into account. If you wish to use this function, you must select the Daylight Savings Time period and check/tick the enable box to enable your daylight saving configuration.

Click **<Apply>** at the bottom of the screen to save the above configurations.

## Power Saving

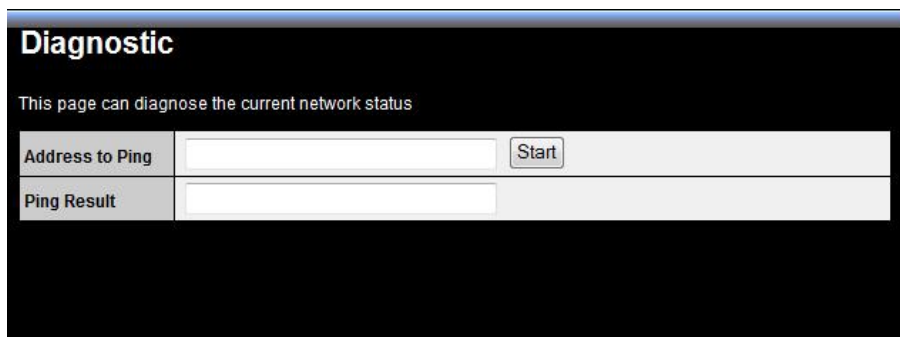
Saving power in WLAN/Ethernet mode can be enabled/disabled in this page.



The screenshot shows a web interface titled "Power Savings". Below the title is a descriptive sentence: "You can use the power page to save energy for WLAN interfaces." Underneath, there is a section labeled "Power Saving Mode". Within this section, there is a label "WLAN:" followed by two radio button options: "Enable" and "Disable". The "Disable" option is selected. At the bottom right of the form, there are two buttons: "Apply" and "Cancel".

## Diagnostic

This page could let you diagnosis your current network status.



The screenshot shows a web interface titled "Diagnostic". Below the title is a descriptive sentence: "This page can diagnose the current network status". The interface contains two rows of input fields. The first row is labeled "Address to Ping" and has a text input field followed by a "Start" button. The second row is labeled "Ping Result" and has a text input field.

## Firmware

This page allows you to upgrade the router's firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.



The screenshot shows a web interface titled "Firmware". Below the title is a descriptive sentence: "You can upgrade the firmware of the router in this page. Ensure, the firmware you want to use is on the local hard drive of your computer. Click on Browse to browse and locate the firmware to be used for your update." Underneath, there is a section labeled "Firmware File:" followed by a text input field and a "Browse..." button. At the bottom right of the form, there are two buttons: "Apply" and "Cancel".

Once you've selected the new firmware file, click <Apply> at the bottom of the screen to start the upgrade process

## Backup

This page allows you to save the current router configurations. When you save the configurations, you also can re-load the saved configurations into the router through the **Restore Settings**. If extreme problems occur you can use the **Restore to Factory Defaults** to set all configurations to its original default settings.



The screenshot shows a web interface titled "Backup". It contains a text block explaining the function: "Use BACKUP to save the routers current configuration to a file named config.dif. You can use RESTORE to restore the saved configuration. Alternatively, you can use RESTORE TO FACTORY DEFAULT to force the router to restore the factory default settings." Below this are three rows of controls:

Restore to factory default	<input type="button" value="Reset"/>
Backup Settings	<input type="button" value="Save"/>
Restore Settings	<input type="button" value="Browse..."/> <input type="button" value="Upload"/>

**Backup Settings:** This can save the Broadband router current configuration to a file named "config.bin" on your PC. You can also use the **<Upload>** button to restore the saved configuration to the Broadband router. Alternatively, you can use the "**Restore to Factory Defaults**" tool to force the Broadband router to perform a power reset and restore the original factory settings.

## Restart

You can reset the broadband AP when system stops responding correctly or stop functions.



The screenshot shows a web interface titled "Restart". It contains a text block: "In the event the system stops responding correctly or stops functioning, you can perform a restart. Your settings will not be changed. To perform the restart, click on the APPLY button." Below this are "Apply" and "Cancel" buttons. A "Message from webpage" dialog box is overlaid on the screen, asking "Do you really want to restart the device?" with "OK" and "Cancel" buttons.



# FCC Interference Statement

## 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.

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.

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.

### **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.

We declare that the product is limited in CH1~CH11 by specified firmware controlled in the USA.  
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

# 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.

## TBW-670AP – 2 Years Warranty

AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1 year warranty.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

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 by 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 within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

**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 REPLACE. 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, NEGLIGENCE, 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 DATA, 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.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Go to <http://www.trendnet.com/gpl> or <http://www.trendnet.com> Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please go to <http://www.gnu.org/licenses/gpl.txt> or <http://www.gnu.org/licenses/lgpl.txt> for specific terms of each license.



**TRENDnet<sup>®</sup>**

## Product Warranty Registration

Please take a moment to register your product online.  
Go to TRENDnet's website at <http://www.trendnet.com/register>