

User's Guide

TRENDnet[®]



N300 WiFi Router

TEW-731BR

Contents

Product Overview	1
Package Contents	1
Features	1
Product Hardware Features.....	2
Application Diagram	4
Basic Router Setup	5
Creating a Home Network	5
Router Installation	6
Connect additional wired devices to your network.....	9
Wireless Networking and Security	10
How to choose the type of security for your wireless network	10
Secure your wireless network	11
Connect wireless devices to your router	12
Connect wireless devices using WPS	13
Basic wireless settings	14
Steps to improve wireless connectivity	16
Advanced wireless settings.....	18
Wireless Repeater.....	18
Access Control Filters	20
Access control basics	20
MAC address filters	20
Domain/URL Filters	21
Advanced Router Setup.....	22
Access your router management page.....	22

Set your router date and time	22
Manually configure your Internet connection	23
IPv6 Internet Connection Settings	23
Clone a MAC address	24
Change your router IP address	25
Set up the DHCP server on your router	25
Set up DHCP reservation	26
Enable/disable UPnP on your router	27
Identify your network on the Internet	27
Allow remote access to your router management page	28
Open a device on your network to the Internet.....	29
DMZ.....	29
Virtual Server	29
Special Applications	32
Router Maintenance & Monitoring	34
Reset your router to factory defaults	34
Router Default Settings	34
Backup and restore your router configuration settings	35
Restart your router	37
Check the router system information	38
View your router packet statistics	39
View wireless devices connected to your router	39
Router Management Page Structure	40
Technical Specifications	41
Troubleshooting	43
Appendix	44

Product Overview



TEW-731BR

Package Contents

In addition to your router, the package includes:

- Multi-Language Quick Installation Guide
- Network cable (1 m / 3.28 ft.)
- Power adapter (5V DC, 1A)

If any package contents are missing or damaged, please contact the retail store, online retailer, or reseller/distributor from which the product was purchased.

Features

TRENDnet's N300 WiFi Router, model TEW-731BR, offers up to 300 Mbps wireless N networking to share files, play games, and surf the internet. Control access to the internet and manage bandwidth for devices connected to router. For your convenience, the wireless network is setup and pre-encrypted out of the box.

Ease of Use

Easy Setup

Get up and running in minutes with the intuitive guided setup

One Touch Connection

Securely connect to the router at the touch of the Wi-Fi Protected Setup (WPS) button

Access Control

Pre-Encrypted

For your convenience the wireless network is pre-encrypted with its own unique password

Access Controls

Control access to specific websites and manage which devices can access the router

Performance

N300 Wireless

Proven 300 Mbps Wireless N

Fast Ethernet Ports

10/100 Mbps Ethernet ports connect up to four devices

Wireless Coverage

Dual 5 dBi antennas provide extended wireless coverage

IPv6

IPv6 network support

*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions.

Product Hardware Features

Rear View



- **Reset Button** – Push and hold this button for 10 seconds and release to reset your router to its factory defaults.
- **LAN Ports** – Connect Ethernet cables (also called network cables) from your router LAN ports to your wired network devices.
- **WAN Port** – Connect an Ethernet cable from your router WAN port to your modem.
- **Power Port** – Connect the included power adapter from your router power port and to an available power outlet.
- **Antennas** – The antennas broadcast wireless network signals.

Front View

- **Power LED** -This LED indicator is solid green when your router is powered on. Otherwise if this LED indicator is off, there is no power to your router.
- **WAN (Link/Activity) LED** – This LED indicator is solid green when your router WAN port is physically connected to the modem Network port (also called network port) successfully with a Network cable. The LED indicator will be blinking green while data is transmitted or received through the WAN port of your router.
- **WLAN (Link/Activity) LED** – This LED indicator is blinking green when the wireless is “On” and functioning properly on your router. This LED indicator will be blinking green rapidly while data is transmitted or received by your wireless clients or wireless network devices connected to your router.

Side View



- **WPS (Wi-Fi Protected Setup)** – Push and hold this button for 3 seconds to activate WPS. The button LED is blinking green when WPS is activated.

Application Diagram

The router is installed near the modem (typically supplied by your ISP “Internet Service Provider”) and physically connected to it from the router’s WAN port to the modem’s network port which connects to the Internet. Wireless signals from the router are broadcasted to wireless clients such as laptops (with wireless capability) thereby providing Internet access.

Basic Router Setup

Creating a Home Network

What is a network?

A network is a group of computers or devices that can communicate with each other. A home network of more than one computer or device also typically includes Internet access, which requires a router.

A typical home network may include multiple computers, a media player/server, a printer, a modem, and a router. A large home network may also have a switch, additional routers, access points, and many Internet-capable media devices such as TVs, game consoles, and Internet cameras.

- **Modem** – Connects a computer or router to the Internet or ISP (Internet Service Provider).
- **Router** – Connects multiple devices to the Internet.
- **Switch** – Connect several wired network devices to your home network. Your router has a built-in network switch (the LAN port 1-4). If you have more wired network devices than available Ethernet ports on your router, you will need an additional switch to add more wired connections.

How to set up a home network

1. For a network that includes Internet access, you'll need:
 - Computers/devices with an Ethernet port (also called network port) or wireless networking capabilities.
 - A modem and Internet service to your home, provided by your ISP (modem typically supplied by your ISP).
 - A router to connect multiple devices to the Internet.

2. Make sure that your modem is working properly. Your modem is often provided by your Internet Service Provider (ISP) when you sign up for Internet service. If your modem is not working contact your ISP to verify functionality.

3. Set up your router. See "How to setup your router" below.

4. To connect additional wired computers or wired network devices to your network, see "Connect additional wired devices to your network" on [page 9](#).

5. To set up wireless networking on your router, see "Wireless Networking and Security" on [page 10](#).

How to setup your router

Refer to the Quick Installation Guide or continue to the next section "Router Installation" on [page 6](#) for more detailed installation instructions.

Where to find more help

In addition to this User's Guide, you can find help below:

- <http://www.trendnet.com/support>
(documents, downloads, and FAQs are available from this Web page)

Before you Install

1. Obtain IP Address Automatically (DHCP)

Clone Mac Address (Optional)

WAN IP Address: . . .

(e.g. 215.24.24.129)

WAN Subnet Mask: . . .

WAN Gateway IP Address: . . .

DNS Server Address 1: _____ . _____ . _____ . _____

DNS Server Address 2: _____ . _____ . _____ . _____

User Name: _____

Password: _____

Verify Password: _____

User Name: _____

Password: _____

Verify Password: _____

IP Address: _____ (e.g. 215.24.24.129)

Type (Dynamic IP or Static IP)

My IP Address: . . .

(e.g. 215.24.24.129)

Subnet Mask: . . .

Gateway: . . .

Server IP: . . .

PPTP Account: _____

PPTP Password:

Retype Password: _____

Type (Dynamic IP or Static IP)

My IP Address: _____ . _____ . _____ . _____

(e.g. 215.24.24.129)

Subnet Mask: _____._____._____._____

Gateway: _____

Server IP: _____

L2TP Account: _____

L2TP Password: _____

Retype Password: _____

Type (Dynamic IP or Static IP)

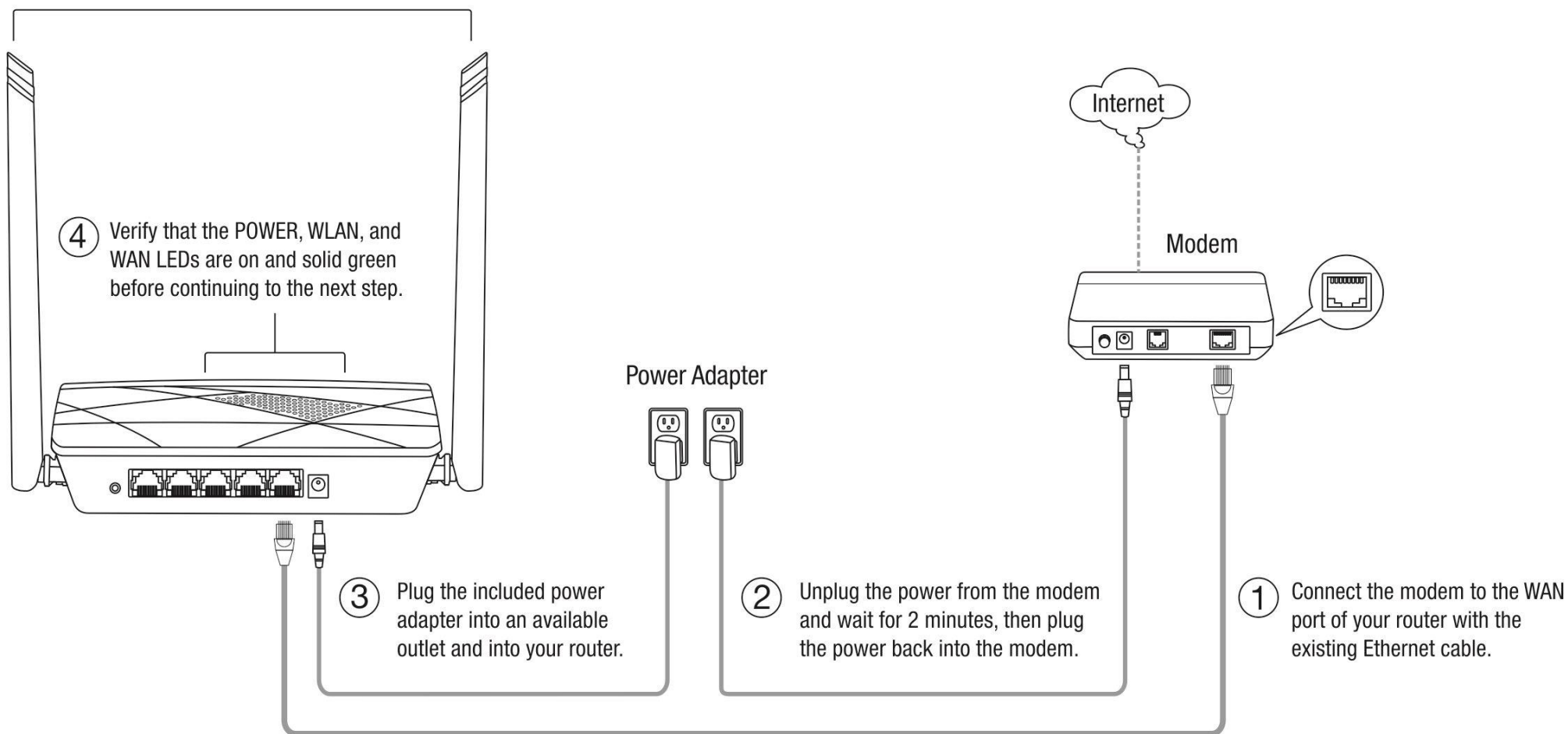
User Name:

Password: _____

Verify Password:

IP Address: _____ (e.g. 215.24.24.129)

It is recommended that you position the antennas vertically as shown for optimal wireless coverage.



Setup Wizard

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and enter <http://tew-731br> or <http://192.168.10.1> in the address bar of your web browser.

Note: If you have already configured your router before, the wizard will no longer appear automatically. In your web browser, go to <http://tew-731br> or you can access the router management using the default IP address <http://192.168.10.1>. Your router will prompt you for a user name and password. Enter your user name and password and click Login, then click on Wizard.



2. In the setup wizard, select your **Language** and select your **WAN Connection Type** and click **Next**. If you are unsure of the connection, keep the default setting "Dynamic IP" and click **Next** and continue to follow the instructions to complete the WAN connection setup.

Note: Dynamic IP (DHCP) is typical for most Internet services. You can verify your settings with your Internet Service Provider.

WAN Connection Type

The Setup supports three popular types of connection. To make sure the connection type your ISP provides, please refer to the ISP.

- ☒ Dynamic IP - Usually for Cable Modem and the router will automatically obtain an IP address from the DHCP server.
- ☐ Static IP - This type of connection uses a permanent, fixed (static) IP address that your ISP assigned.
- ☐ PPPoE - Usually for ADSL Modem and you will need a PPPoE username and password from your ISP.

English ▼

Cancel Next

3. Use the default or change the wireless settings and click **Next**. By default, a unique SSID (Wi-Fi Name) and wireless key (Wi-Fi Password) have already been preconfigured on your router. If you change the default settings, please write down the new wireless

settings to reference for your other wireless devices to connect to your router's wireless network.

Wireless

By default, a unique predefined WiFi Key/Password has already been assigned in order for clients to connect to your router WiFi network which can be located on the label located on the bottom of the device or on the wireless sticker included with your device for your convenience. If you would like to change the default WiFi Key/Password, please enter the WiFi Key/Password in the field below named "Key:", then click "Next". You can configure the wireless parameters and security settings of router on this step.

Disable the wireless radio. ☐

SSID: TRENDnet731_GZ9G

Channel: Auto

Mode: 2.4 GHz (B+G+N)

Channel Width: 20M

Wireless Security:

- ☐ Disable Security
- ☒ WPA-PSK/WPA2-PSK AES

Key: 7311R50050 (8-63 characters or 64 hex digits)

Cancel Back Next

4. Click **Finish** to complete the setup and wait for the configuration settings to apply, then, test your internet connection by accessing Internet sites in your web browser.

Setup Complete

Click the 'Finish' button to finish the Setup.

Tips: Please click "Setup" on the Menu, and then click "Internet Setup" for detail settings if the router still can not access the internet.

Cancel Back Finish

Preset Wireless Settings

Wi-Fi Name/SSID
TRENDnet731_2.4GHz_XXX

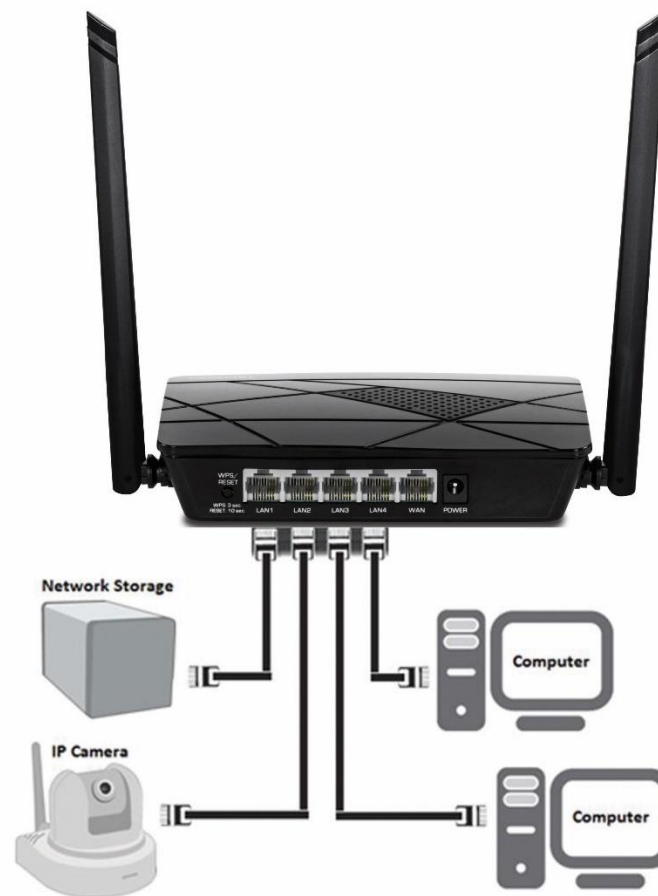
Wi-Fi Key
XXXXXXXXXXXX

Management Login
http://tew-731br
username: admin
password: XXXXX

Connect additional wired devices to your network

You can connect additional computers or other network enabled devices to your network by using Ethernet cables to connect them to one of the available LAN ports labeled 1,2,3,4 on your router.

Note: If you encounter issues connecting to your network, there may be a problem with your computer or device network settings. Please ensure that your computer or device network settings (also called TCP/IP settings) are configured to obtain IP address settings automatically (also called dynamic IP address or DHCP) and to Obtain DNS Server address settings automatically.



Wireless Networking and Security

How to choose the type of security for your wireless network

Setting up wireless security is very important. Leaving your wireless network open and unsecure could expose your entire network and personal files to outsiders. TRENDnet recommends reading through this entire section and setting up wireless security on your new router.

There are a few different wireless security types supported in wireless networking each having its own characteristics which may be more suitable for your wireless network taking into consideration compatibility, performance, as well as the security strength along with using older wireless networking hardware (also called legacy hardware).

It is strongly recommended to enable wireless security to prevent unwanted users from accessing your network and network resources (personal documents, media, etc.).

In general, it is recommended that you choose the security type with the highest strength and performance supported by the wireless computers and devices in your network. Please review the security types to determine which one you should use for your network.

Wireless Encryption Types

- **WEP:** Legacy encryption method supported by older 802.11b/g hardware. This is the oldest and least secure type of wireless encryption. It is generally not recommended to use this encryption standard, however if you have old 802.11b or 802.11g wireless adapters or computers with old embedded wireless

cards(wireless clients), you may have to set your router to WEP to allow the old adapters to connect to the router. **Note:** *This encryption standard will limit connection speeds to 54Mbps.*

- **WPA:** This encryption is significantly more robust than the WEP technology. Much of the older 802.11g hardware was been upgraded (with firmware/driver upgrades) to support this encryption standard. Total wireless speeds under this encryption type however are limited to 54Mbps.
- **WPA-Auto:** This setting provides the router with the ability to detect wireless devices using either WPA or WPA2 encryption. Your wireless network will automatically change the encryption setting based on the first wireless device connected. For example, if the first wireless client that connects to your wireless network uses WPA encryption your wireless network will use WPA encryption. Only when all wireless clients disconnect to the network and a wireless client with WPA2 encryption connects your wireless network will then change to WPA2 encryption. NOTE: WPA2 encryption supports 802.11n speeds and WPA encryption will limit your connection speeds to 54Mbps
- **WPA2:** This is the most secure wireless encryption available today, similar to WPA encryption but more robust. This encryption standard also supports the highest connection speeds. TRENDnet recommends setting your router to this encryption standard. If you find that one of your wireless network devices does not support WPA2 encryption, then set your router to either WPA or WPA-Auto encryption.

Note: *Check the specifications of your wireless network adapters and wireless appliances to verify the highest level of encryption supported.*

Below is brief comparison chart of the wireless security types and the recommended configuration depending on which type you choose for your wireless network.

Security Standard	WEP	WPA	WPA2
Compatible Wireless Standards	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g/n
Highest Performance Under This Setting	Up to 54Mbps	Up to 54Mbps	Up to 300Mbps*
Encryption Strength	Low	Medium	High
Additional Options	Open System or Shared Key, HEX or ASCII, Different key sizes	TKIP or AES, Preshared Key or RADIUS	TKIP or AES, Preshared Key or RADIUS
Recommended Configuration	Open System ASCII 13 characters	TKIP Preshared Key 8-63 characters	AES Preshared Key 8-63 characters

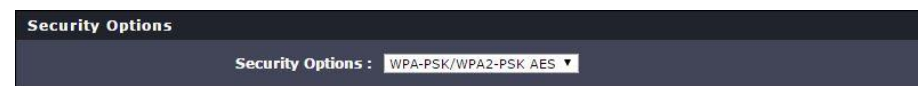
*Dependent on the maximum 802.11n data rate supported by the device (150Mbps, 300Mbps, or 450Mbps)

Secure your wireless network

Wireless > Security

After you have determined which security type to use for your wireless network (see “How to choose the security type for your wireless network” on [page 10](#)), you can set up wireless security.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Wireless**.
3. Click on the **Security Options** drop-down list to select your wireless security type.



Selecting WEP:

If selecting **WEP** (Wired Equivalent Privacy), please review the WEP settings to configure and click **Apply** to save the changes.

- **Authentication Type**– Choose **Automatic** or **Shared Keys**.

Note: It is recommended to use Automatic because it is known to be more secure than Shared Key.

- **WEP Key** – Choose the key length **64-bits** or **128-bits**.

Note: It is recommended to use 128-bit because it is more secure to use a key that consists of more characters.

- **Key 1-4**
 - This is where you enter the password or key needed for a computer to connect to the router wirelessly
 - You can define up to 4 passwords or 4 keys. Only one key can be active at a given time. Most users simply define one key.
 - Choose a key index 1, 2, 3, or 4 and enter the key.
 - When connecting to the router, the client must match both the password and the Key number. (e.g. if you have activated Key 2 with a password of 12345, then the client must select: Key 2 (entering Key 1, 3, or 4 will block the ability to connect) and enter password 12345)

Selecting **WPA-PSK, WPA2-PSK, or WPA-PSK/WPA2-PSK (WPA2 recommended)**:

First, from the Authentication Type row, select **WPA-PSK, WPA2-PSK, or WPA-PSK/WPA2-PSK**.

The following section outlines options when selecting **PSK** (Preshared Key Protocol), Create your Wireless security Passphrase (password or key):

- **Passphrase** – Enter the passphrase.
 - This is the password or key that is used to connect your computer to this router wirelessly
- **Confirmed Passphrase** – Re-enter the passphrase.

Note: 8-63 alphanumeric characters (a,b,c,?,*,/,1,2, etc.)

WEP Key Format	HEX	ASCII
Character set	0-9 & A-F, a-f only	Alphanumeric (a,b,c,?,*,/,1,2, etc.)
64-bit key length	10 characters	5 characters
128-bit key length	26 characters	13 characters

Connect wireless devices to your router

A variety of wireless network devices can connect to your wireless network such as:

- Gaming Consoles

- Internet enabled TVs
- Network media players
- Smart Phones
- Wireless Laptop computers
- Wireless IP cameras

Each device may have its own software utility for searching and connecting to available wireless networks, therefore, you must refer to the User's Manual/Guide of your wireless client device to determine how to search and connect to this router's wireless network.

See the "Appendix" on [page 44](#) for general information on connecting to a wireless network.

Connect wireless devices using WPS

WPS (Wi-Fi Protected Setup) is a feature that makes it easy to connect devices to your wireless network. If your wireless devices support WPS, you can use this feature to easily add wireless devices to your network.

Note: You will not be able to use WPS if you set the SSID Broadcast setting to Disabled.

There are two methods the WPS feature can easily connect your wireless devices to your network.

- Push Button Configuration (PBC) method
 - RECOMMENDED Hardware Push Button method—with an external button located physically on your router and on your client device
 - WPS Software/Virtual Push Button - located in router management page
- PIN (Personal Identification Number) Method - located in router management page

Note: Refer to your wireless device documentation for details on the operation of WPS.

Recommended Hardware Push Button (PBC) Method

- Note it is recommended that a wireless key (passphrase or password) is created before connecting clients using the PBC method. If no wireless key is defined when connecting via PBC, the router will automatically create an encryption key that is 64 characters long. This 64 character key will then have to be used if one has to connect computers to the router using the traditional connection method.

To add a wireless device to your network, simply push the WPS button on the wireless device you are connecting (consult client device User's Guide for length of time), then push and hold the WPS button located on your router for 3 seconds and release it. A blue LED on your router WPS button will flash indicating that the WPS setup process has been activated on your router. (See "Product Hardware Features" on [page 2](#))

For connecting additional WPS supported devices, repeat this process for each additional device.

PIN (Personal Identification Number)*Wireless > WiFi Protected Setup*

If your wireless device has WPS PIN (typically an 8-digit code printed on the wireless device product label or located in the wireless device wireless software utility), you can use this method.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Wireless**, and click on **Advanced Wireless**.
3. Make sure the **Disable PIN** selection is not checked.
4. Click on **WPS** on the left menu and click **Next**.
5. Next enter the WPS PIN of the wireless device you are connecting and click **Start PIN**.

Entry PIN of wireless NIC:

Note: You may need to initiate the WPS PIN on your wireless device first when using this method. Refer to your wireless device documentation for details on the operation of WPS.

Basic wireless settings*Wireless > Basic*

This section outlines available management options under the Basic Wireless sub tab.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Wireless**, and click on **Wireless Basic**.
3. To save changes to this section, click **Apply** when finished.

Name(SSID) : TRENDnet731_GZ9G

- **SSID** – This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. By default, the router's wireless name is unique to the device. If you choose to change the SSID, change it to a name that you can easily remember.

Mode : 802.11b/g/n ▼
Channel: Auto ▼ Current Channel: 3
Band Width : 20M ▼

- **Auto Channel** – In North America, this router can broadcast on 1 of 11 Channels (13 in Europe and other countries). Selecting Auto Channel enables the router to automatically select the best Channel for wireless communication.

- **Channel** – To manually set the channel on which the router will broadcast, click the drop-down list and select the desired Channel for wireless communication. The goal is to select the Channel that is least used by neighboring wireless networks.
- **802.11 Mode** - Select the appropriate mode for your network.
 - **2.4GHz 802.11b/g/n mixed mode** – Select this mode for the best compatibility. This mode allows older 802.11b and 802.11g wireless devices to connect to the router in addition to newer 802.11n devices.
 - **2.4GHz 802.11b/g mixed mode** – This mode only allows devices to connect to the router using older and slow 802.11b or 802.11g technology and it thereby reduces the router's maximum speed to 54Mbps (typically not recommended).
 - **2.4GHz 802.11n only mode** – This mode only allows newer 802.11n devices to connect to your router. This mode does ensure the highest speed and security for your network, however if you have older 802.11g wireless clients, they will no longer be able to connect to this router.
 - **2.4GHz 802.11n/g mixed mode** – This mode only allows devices to connect to the router using the older 802.11g technology and also the newer 802.11n technology. This mode allows older wireless clients to connect to the wireless router while also ensuring the highest speed and security for your network for newer wireless clients that are 802.11n.
 - **2.4GHz 802.11g only mode** – This mode only allows devices to connect to the router using older and slow 802.11g technology (typically not recommended).

- **2.4GHz 802.11b only mode** – This mode only allows devices to connect to the router using older and slow 802.11b technology (typically not recommended).

Note: Please check the specifications on your wireless devices for the highest wireless capability supported first before applying these settings. If you are unsure, it is recommended that you keep the default setting (2.4GHz 802.11b/g/n mixed mode) for the best compatibility.

When applying the 802.11 mode setting, please keep in mind the following:

- Wireless devices that support 802.11n are backwards compatible and can connect wirelessly at 802.11g or 802.11b.
 - Connecting at 802.11b or 802.11g will limit the capability of your 802.11n supported wireless devices from obtaining higher performance and data rates.
 - Allowing 802.11b or 802.11g devices to connect to an 802.11n capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11n.
 - Wireless devices that only support 802.11b or 802.11g will not be able to connect to a wireless network that is set to 802.11n only mode.
 - Wireless devices that only support 802.11b will not be able to connect to a wireless network that is set to 802.11g only mode.
-
- **Band Width** – This setting only applies to wireless devices connecting at 802.11n. Select the appropriate channel width for your wireless network.
 - **20 MHz** – This mode operates using a single 20MHz channel for wireless devices connecting at 802.11n. This setting may provide more stability than Auto 20/40 MHz for connectivity in busy wireless environments where there are several wireless networks in the area.
 - **Auto 20/40 MHz** – This mode can automatically switch between using a single 20MHz channel or 40MHz (two 20MHz channels). When 40MHz is active, this mode is capable of providing higher performance

only if the wireless devices support the 40MHz channel width.

Enabling 20/40MHz typically results in substantial performance increases when connecting to an 802.11n client.

- **SSID Broadcast**

- **Enabled** allows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your router.
- **Disabled** turns off the ability for wireless devices to find your network. It is still possible for wireless devices to be configured to connect to your wireless network.

Note: Setting this option to **Disabled**, will disable WPS functionality.

- **WMM** – Wi-Fi Multimedia is a Quality of Service (QoS) feature which prioritizes audio and video data packets. This feature requires the wireless device to also support WMM. Click **Enabled (recommended)** or **Disabled** to turn this feature on or off on your router.

Steps to improve wireless connectivity

There are a number of factors that can impact the range of wireless devices. Follow these tips to help improve your wireless connectivity:

1. 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.
 - a. For the widest coverage area, install your router near the center of your home, and near the ceiling, if possible.
 - b. Avoid placing the router on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), and masonry walls.
 - c. Any obstruction can weaken the wireless signal (even non-metallic objects), so the fewer obstructions between the router and the wireless device, the better.
 - d. Place the router in a location away from other electronics, motors, and fluorescent lighting.
 - e. Many environmental variables can affect the router's performance, so if your wireless signal is weak, place the router in several locations and test the signal strength to determine the ideal position.
2. 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.

3. 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.
4. 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.

If possible, upgrade wireless network interfaces (such as wireless cards in computers) from older wireless standards to 802.11n. If a wirelessly networked device uses an older standard, the performance of the entire wireless network may be slower. If you are still experiencing low or no signal, consider repositioning the wireless devices or installing additional access points.

Advanced wireless settings

Wireless > Advanced

These settings are advanced options that can be configured to change advanced wireless broadcast specifications. It is recommended that these settings remain set to their default values unless you are knowledgeable about the effects of changing these values. Changing these settings incorrectly can degrade performance.

Fragment Threshold(256-2346) : 2346

RTS Threshold(1-2347) : 2347

Preamble Type : Short Preamble ▼

Radio Power (Percent) : 100% ▼

- **RTS Threshold** – The Request To Send (RTS) function is part of the networking protocol. A wireless device that needs to send data will send a RTS before sending the data in question. The destination wireless device will send a response called Clear to Send (CTS). The RTS Threshold defines the smallest data packet size allowed to initiate the RTS/CTS function.
Default Value: 2347 (range: 1-2347)
- **Fragmentation Threshold** – Fragmentation in wireless networks is the process of breaking down data communications into smaller data packets in order to improve data efficiency when transferring or receiving data between wireless devices. The fragmentation threshold defines the maximum size of the data packets that are broken down.
Default Value: 2346 (range: 256~2346, even numbers only)
- **Preamble Type** – A setting that adds additional data header strings to help check the Wi-Fi data transmission errors.
 - **Short Preamble** - Using a short guard interval can increase throughput. However, it can also increase error rate in some

installations, due to increased sensitivity to radio-frequency reflections.

- **Long Preamble** – Using a long guard interval can decrease throughput. However, it can also decrease the error rate in some installations due to decreased sensitivity to radio-frequency reflections.
- **Radio Power (Percent)** – A setting that allows the power of the radio to be customized. By default, the setting is set to 100%. Decreasing the percentage of the radio power will reduce the Wi-Fi coverage area and throughput

Wireless Repeater

Wireless > Wireless Repeater

Wireless range extender or repeater mode allows the device to extend the range of an existing wireless network. The existing wireless signal can be broadcasted from your wireless router or other access point. In addition, other network enabled devices can connect to your network using the Ethernet LAN port.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Wireless**, and click on **Wireless Repeater**.
3. Enable the repeater mode by clicking on the **Repeater Enabled**, and click on the **Site Survey** button. This will allow the TEW-731BR to scan for the wireless network you would like to repeat or extend. If prompted to disable DHCP, click OK.

Note: Enabling repeater mode will set the DHCP mode to none.

☒ **Repeater Enabled(DHCP mode will be set to 'none' if the repeater is enabled.)**

[Site Survey](#)

5. Select the SSID you wish to connect to and click **Next** at the bottom of the page.

#	SSID	MAC Address	Channel	Signal	Security	Select
1	TEW-818DRU_2.4	d8:eb:97:ad:ec:9d	1	100%	WPA2-PSK(AES)	<input type="radio"/>
2	jdesk827-24G456	00:14:d1:11:22:11	6	100%	WPA2-PSK(AES)	<input checked="" type="radio"/>
3	RMA2016	d8:eb:97:ef:39:8a	4	100%	WPA2-PSK(AES)	<input type="radio"/>
4	Wally World	d8:eb:97:2a:cd:fe	11	100%	WPA2-PSK(AES)	<input type="radio"/>
5	TrendnetSkyN	d8:eb:97:2f:bd:cd	11	100%	WPA2-PSK(AES)	<input type="radio"/>
6	TRENDnetBCHQ	d8:eb:97:af:a8:38	1	100%	WPA-PSK(AES/TKIP)/WPA2-PSK(AES/TKIP)	<input type="radio"/>
7	Airtect	d8:eb:97:df:15:dc	7	100%	WPA2-PSK(AES)	<input type="radio"/>

Click 'Next' to Continue repeater settings

Next

6. If your wireless network requires an encryption key, enter it in the field provided and click **Apply**.

Security Options(WPA2-PSK)

Pre-Shared Key: (8-63 characters or 64 hex digits)

7. You can now disconnect your router and place in the location where you would like to extend or repeater your existing wireless network signal for increased coverage.

Access Control Filters

Access control basics

MAC address filters

Wireless > Advanced Wireless > ACL Setup

Every network device has a unique, 12-digit MAC (Media Access Control) address. Using MAC filters, you can allow or deny specific computers and other devices from using this router's wired or wireless network.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Wireless**, click on **Advanced Wireless**, and then click on **ACL Setup**.
3. Click on the box **Enable Wireless Access Control Mode**

4. Add the MAC addresses to the MAC Table first before applying the MAC filter function.

- **Add** – Saves a new MAC address entry.

Note: MAC filter can be configured to allow access to the listed MAC address and deny all others unlisted or vice versa. The recommended function is to choose to only allow access to the MAC addresses listed and deny all others unlisted because it is easier to determine the MAC addresses of devices in your network then to determine which MAC addresses you do not want to allow access.

- **MAC Address** – Enter the 12-digit MAC address. (e.g. 001122AABBCC)

Note: You can check the Dynamic DHCP List for the MAC addresses of the devices on your network, see "Setup the DHCP server on your router" on [page 25](#) or refer to your computer or device documentation to find the MAC address.

Click **Add** to save the new MAC address entry to the MAC Table. After clicking **Add**, the MAC address entry will appear in the list below. Repeat for each device.

To modify an existing MAC address entry, select the entry in the MAC Table.

- **Delete** – Removes an existing MAC address entry.
- **Delete all** – Removes all existing MAC address entries.

Domain/URL Filters

Advanced > URL Block

You may want to allow or block computers or devices on your network access to specific websites (e.g. www.trendnet.com, etc.), also called domains or URLs (Uniform Resource Locators). You may also enter a keyword (e.g. instead of complete URL to generally allow or block computers or devices access to websites that may contain the keyword in the URL or on the web page.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, and click on **URL Block**.

URL Blocking Capability

URL Blocking Capability: ☐ Disable ☐ Enable

[Apply Changes](#)

Keywords

Keyword:

[AddKeyword](#) [Delete Selected Keyword](#)

URL Blocking Table

Select	Filtered Keyword
--------	------------------

3. Enable **URL Blocking Capability** by selecting the **Enable** option.

Click **Apply** to save the changes.

4. Under **Keywords**, enter the URL address or keywords you wish to block and then click on **AddKeyword**. The URL address or keywords will display in the URL Blocking Table. Repeat for each additional website or keyword added.

URL Blocking Table	
Select	Filtered Keyword
<input type="radio"/>	www.trendnet.com

- **Delete Selected Keyword** -Delete an existing website/URL/domain or keyword entry that has been selected in the **URL Blocking Table**.

Advanced Router Setup

Access your router management page

Note: Your router management page URL/domain name <http://tew-731br> or IP address <http://192.168.10.1> is accessed through the use of your Internet web browser (e.g. Internet Explorer®, Firefox®, Chrome™, Safari®, Opera™) and will be referenced frequently in this User's Guide.

1. Open your web browser and go to URL/domain name <http://tew-731br> or IP address <http://192.168.10.1>. Your router will prompt you for a user name and password.

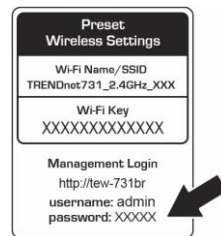


2. For added security, the router is preconfigured with a unique password. You can find the **Password** on a sticker on the side of the router and on the label on the bottom of the router. Enter your **Username** and **Password**, select your preferred language, then click **Login**.

User Name: **admin**

Password: **(xxxxxxxx)**

Note: User Name and Password are case sensitive.



Change your router login password

Maintenance > Admin

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance**, and click on **Admin**.
3. Under the **Admin** section, select the profile you wish to edit under the **User Account Table**.
4. Under the **Configuration**, input the old password, and then input the new password and confirm the password in the entry fields.
4. To save changes, click **Modify**.

Note: If you change the router login password, you will need to access the router management page using the User Name "admin" and the new password instead of the default password.

Set your router date and time

Maintenance > Time and Date

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance**, and click on **Time and Date**.

3. Next to **Time Zone**, click the drop-down list to select your **Time Zone** located under **NTB Configuration**.

4. Next to **Synchronize the clock with**, you can choose one of the following options:

- **System Time** – Set your router date and time manually in the **System Time** section. To save changes, click **Apply Changes**.
Note: Time is specified in 24-hour format.
OR
- **Automatic** – Set your router date and time to synchronize with an NTP (Network Time Protocol) server address (e.g. pool.ntp.org). Enter the NTP server address next to **Server** entry field, (e.g. pool.ntp.org). To save changes, click **Apply**.

Note: NTP servers are used for computers and other network devices to synchronize time across an entire network.

5. You can verify the time/date settings next to **System Time** at the top of the page. **System Time** displays the current date and time set on your router.

Manually configure your Internet connection

Setup > Internet Setup

1. Log into your router management page (see “Access your router management page” on [page 22](#)).

2. Click on **Setup**, and click on **Internet Setup**.

3. In the **WAN Access Type** drop-down list, click the type of Internet connection provided by your Internet Service Provider (ISP).

4. Complete the fields required by your ISP.

5. Complete the optional settings only if required by your ISP.

6. To save changes, click **Apply**.

*Note: If you are unsure which Internet connection type you are using, please contact your ISP. Note: If your ISP requires a host name to be specified, you can specify it under Main > LAN & DHCP Server, in the **Host Name** field. To save changes, click **Apply** at bottom of the page.*

IPv6 Internet Connection Settings

Setup > IPv6

IPv6 (Internet Protocol Version 6) is a new protocol that significantly increases the number of available Internet public IP addresses due to the 128-bit IP address structure versus IPv4 32-bit address structure. In addition, there are several integrated

enhancements compared to the most commonly used and well known IPv4 (Internet Protocol Version 4) such as:

- Integrated IPsec – Better Security
- Integrated Quality of Service (QoS) – Lower latency for real-time applications
- Higher Efficiency of Routing – Less transmission overhead and smaller routing tables
- Easier configuration of addressing

Note: In order to use IPv6 Internet connection settings, it is required that your ISP provide you with the IPv6 service. Please contact your ISP for availability and more information about the IPv6 service.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Setup** and click on **IPv6**.
3. Review the IPv6 Internet Connection settings and enter information settings specified by your ISP. Then click **Apply** to save the changes.

Select the IPv6 connection type provided by your ISP.

- Static IPv6
- Auto-configuration (SLAAC/DHCPv6)
- PPPoE
- Link-Local Only

Clone a MAC address

Setup > Internet Setup

On any home network, each network device has a unique MAC (Media Access Control) address. Some ISPs register the MAC address of the device (usually a router or a

computer) connected directly to the modem. If your computer MAC address is already registered with your ISP and to prevent the re-provisioning and registration process of a new MAC address with your ISP, then you can clone the address (assign the registered MAC address of your previous device to your new router). If you want to use the MAC address from the previous device (computer or old router that directly connected to the modem, you should first determine the MAC address of the device or computer and manually enter it into your router using the clone MAC address feature.

Note: For many ISPs that provide dynamic IP addresses automatically, typically, the stored MAC address in the modem is reset each time you restart the modem. If you are installing this router for the first time, turn your modem before connecting the router to your modem. To clear your modem stored MAC address, typically the procedure is to disconnect power from the modem for approximately one minute, then reconnect the power. For more details on this procedure, refer to your modem's User Guide/Manual or contact your ISP.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Setup**, and click on **Internet Setup**.
3. Under your Internet connection settings, find the **MAC Clone** section shown below.

4. Click either **Default MAC**, **MAC from PC**, or **MAC Manual**.

Default MAC – Uses the default MAC Address of the router

MAC from PC – Clones the MAC address from your connected PC

MAC manual – Allows you to manually input the MAC address

5. To save changes, click **Apply**.

Change your router IP address

Setup > LAN Network


In most cases, you do not need to change your router IP address settings. Typically, the router IP address settings only needs to be changed, if you plan to use another router in your network with the same IP address settings, if you are connecting your router to an existing network that is already using the IP address settings your router is using, or if you are experiencing problems establishing VPN connections to your office network through your router.

Note: If you are not encountering any issues or are not faced with one of the cases described above or similar, it is recommended to keep your router IP address settings as default.

Default Router IP Address: 192.168.10.1

Default Router Network: 192.168.10.0 / 255.255.255.0

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Setup**, and click on **LAN Network**.
3. Enter the router IP address settings.



The screenshot shows the 'LAN Interface Setup' page. It has two input fields: 'IP Address' with the value '192.168.10.1' and 'Subnet Mask' with the value '255.255.255.0'.

- **IP Address** – Enter the new router IP address.
(e.g. 192.168.200.1)
- **Subnet Mask** – Enter the new router subnet mask.
(e.g. 255.255.255.0)

Note: The DHCP address range will change automatically to your new router IP address settings so you do not have to change the DHCP address range manually to match your new router IP address settings.

4. To save changes, click **Apply**.

Note: You will need to access your router management page using your new router IP address to access the router management page. (e.g. Instead of using the default <http://192.168.10.1> using your new router IP address will use the following format using your new router IP address [http://\(new.router.ipaddress.here\)](http://(new.router.ipaddress.here)) to access your router management page.

Set up the DHCP server on your router

Setup > LAN Network

Your router can be used as a DHCP (Dynamic Host Configuration Protocol) server to automatically assign an IP address to each computer or device on your network. The DHCP server is enabled by default on your router. If you already have a DHCP server on your network, or if you do not want to use your router as a DHCP server, you can disable this setting. It is recommended to leave this setting enabled.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Setup**, and click on **LAN Network**.
3. Review the DHCP Server settings.

- **DHCP Server** – Enable or Disable the DHCP server.
- **IP Pool Range** – Changes the starting and ending address for the DHCP server range. (e.g. 192.168.10.20 – 192.168.10.30)

Note: The Start IP and End IP specify the range of IP addresses to automatically assign to computers or devices on your network.

- **Domain Name (Optional)** – Specifies a domain name to assign to computers or devices. (e.g. trendnet.com)

- **Lease Time** – Input the lease time.

Note: The DHCP lease time is the amount of time a computer or device can keep an IP address assigned by the DHCP server. When the lease time expires, the computer or device will renew the IP address lease with the DHCP server, otherwise, if there is no attempt to renew the lease, the DHCP server will reallocate the IP address to be assigned to another computer or device.

4. To save changes, click **Apply**.

Set up DHCP reservation

Setup > LAN Network

DHCP (Dynamic Host Configuration Protocol) reservation (also called Static DHCP) allows your router to assign a fixed IP address from the DHCP server IP address range to a specific device on your network. Assigning a fixed IP address can allow you to easily keep track of the IP addresses used on your network by your computers or devices for future reference or configuration such as virtual server (also called port forwarding, see “Virtual Server” on [page 29](#)) or special applications (also called port triggering, see “Special Applications” on [page 32](#)).

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Setup**, and click on **LAN Network**.
3. Review the DHCP reservation settings.

- **IP Address** – Enter the IP address to assign to the reservation. (e.g. 192.168.10.101)

Note: You cannot assign IP addresses outside of the DHCP range. The IP address is required to be within the DHCP IP address range (Start IP & End IP).

- **MAC Address** – Enter the MAC (Media Access Control) address of the computer or network device to assign to the reservation. (e.g. 00:11:22:AA:BB:CC)
- **Add** - Saves the reservation.

DHCP Static IP Table – You can view the list of reservations for computers or devices that have been created in this list.

DHCP Static IP Table

Select	IP Address	MAC Address
<input type="radio"/>	192.168.10.101	3C:8C:F8:80:00:5E

To modify an existing reservation, select the entry in the **DHCP Static IP Table**. When selected, the **IP Address** and **MAC Address** entry will automatically be filled.

DHCP Static IP Configuration

IP Address: 192.168.10.101

Mac Address: 3C8CF880005E (ex. 00E06710502)

[Add](#) [Update](#) [Delete Selected](#) [Reset](#)

DHCP Static IP Table

Select	IP Address	MAC Address
<input type="radio"/>	192.168.10.101	3C:8C:F8:80:00:5E

- **Update** – Saves changes to an existing reservation.
- **Delete Selected** – Removes an existing reservation.
- **Cancel** – Discards changes to existing reservation.
- **Reset** – Clears the **IP Address** and **MAC Address** entry fields.

Enable/disable UPnP on your router

Advanced > UPnP

UPnP (Universal Plug and Play) allows devices connected to a network to discover each other and automatically open the connections or services for specific applications (e.g. instant messenger, online gaming applications, etc.)

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Advanced**, and click on **UPnP**.
3. Next to **UPnP**, click **Enabled** or **Disabled** to turn the feature on or off on your router.

Note: It is recommended to leave this setting enabled, otherwise, you may encounter issues with applications that utilize UPnP in order allow the required communication between your computers or devices and the Internet.

4. To save changes, click **Apply Changes**.

UPnP ☒ Enabled ☐ Disabled

Identify your network on the Internet

Advanced > Dynamic DNS

Since most ISPs constantly change your home IP address, providing access to devices on your home or small office Local Area Network (such as IP Cameras) from the Internet requires setting up a Dynamic DNS service and entering the parameters into this management area. Dynamic DNS services allow your router to confirm its location to the given Dynamic DNS service, thereby providing the Dynamic DNS service with the ability to provide a virtual fixed IP address for your network. This means that even though your ISP is always changing your IP address, the Dynamic DNS service will be able to identify your network using a fixed address—one that can be used to view home IP Camera and other devices on your local area network.

Note: First, you will need to sign up for one of the DDNS service providers listed in the **Server Address** drop-down list.

1. Sign up for one of the DDNS available service providers list under **DDNS provider**. (e.g. [dyndns.com](#), [no-ip.com](#), etc.)
1. Log into your router management page (see “Access your router management page” on [page 22](#)).
3. Click on **Advanced** and click on **Dynamic DNS**.
4. Check the **Enable** box under **DDNS Configuration**.

5. In the **DDNS provider** drop-down list, select the provider you selected, and enter your information in the fields.

- **Host Name:** Personal URL provided to you by your Dynamic DNS service provider (e.g. www.trendnet.dyndns.biz)
- **User Name:** The user name needed to log in to your Dynamic DNS service account
- **Password:** This is the password to gain access to Dynamic DNS service (NOT your router or wireless network password) for which you have signed up to.

6. To save changes, click **Add**.

Allow remote access to your router management page

Advanced > Access Control List

You may want to make changes to your router from a remote location such as at your office or another location while away from your home.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Advanced**, and click on **Access Control List**.
3. Under the **ACL Settings** section, select **WAN** or **IP Address** and click **Web**

- **Port**— It is recommended to leave this setting as 8080.

Note: If you have configured port 8080 for another configuration section such as virtual server or special application, please change the port to use. (Recommended port range 1024-65534)

- **IP Address** — It is recommended to leave this setting as *, to allow remote access from anywhere on the Internet.

Note: You can enter a specific range of Internet IP addresses that are allowed to access your router management page, all others will be denied.

4. To save changes, click **Add**.

Open a device on your network to the Internet

This router can provide access to devices on your local area network to the Internet using the Virtual Server, Special Application, method (DMZ NOT recommended).

DMZ

Advanced > DMZ

You may want to expose a specific computer or device on your network to the Internet to allow anyone to access it. Your router includes the DMZ (Demilitarized Zone) feature that makes all the ports and services available on the WAN/Internet side of the router and forwards them to a single IP address (computer or network device) on your network. The DMZ feature is an easy way of allowing access from the Internet however, it is a very **insecure** technology and will open local area network to greater threats from Internet attacks. It is strongly recommended to use **Virtual Server** (also called port forwarding, see "Virtual Server" on [page 33](#)) to allow access to your computers or network devices from the Internet.

1. Make the computer or network device (for which you are establishing a DMZ link) has a static IP address (or you can use the DHCP reservation feature to ensure the device has a fixed IP address) (see "Set up DHCP reservation" on [page 25](#)).

A. Signing up for a Dynamic DNS service (outlined in the DDNS section) will provide identification of the router's network from the Internet.

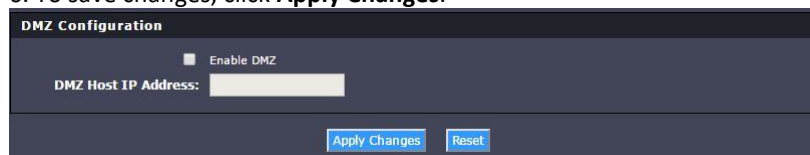
2. Log into your router management page (see "Access your router management page" on [page 22](#)).

3. Click on **Advanced**, and click on **DMZ**.

4. Next to **Enable DMZ**, click **Enable DMZ**.

5. Next, enter the IP address you assigned to the computer or network device to expose to the Internet in the **DMZ Host IP Address** field.

6. To save changes, click **Apply Changes**.



The screenshot shows the 'DMZ Configuration' page. At the top, there is a checkbox labeled 'Enable DMZ' which is currently unchecked. Below it is a text field labeled 'DMZ Host IP Address:'. At the bottom of the page, there are two buttons: 'Apply Changes' and 'Reset'.

Virtual Server

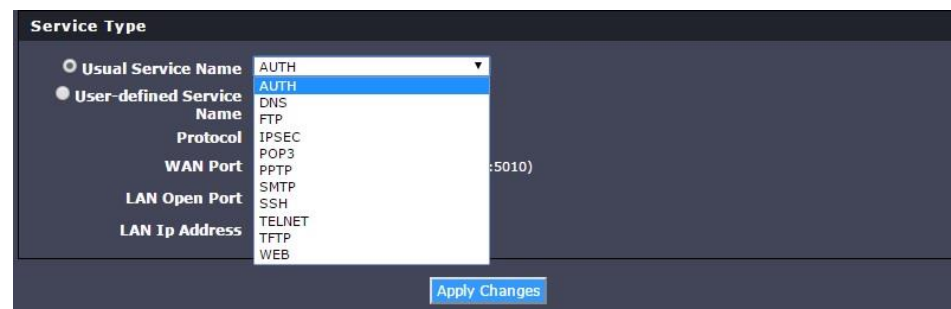
Advanced > Virtual Server

Virtual Server (also called port forwarding) allows you to define specific ports (used or required by a specific application) and forward them to a single IP address (a computer or device) on your network. Using this feature is more secure compared to using DMZ (see DMZ on [page 29](#)) in which DMZ forwards all ports instead of only specific ports used by an application. An example would be forwarding a port to an IP camera (TRENDnet IP cameras default to HTTP TCP port 80 for remote access web requests) on your network to be able to view it over the Internet.

Since most ISPs constantly change your home IP address, to be able to access the Virtual Server port(s) from the Internet it is recommended to setup Dynamic DNS service (See DynDNS section).

1. Log into your router management page (see "Access your router management page" on [page 22](#)).

2. Click on **Advanced**, and click on **Virtual Server**.



The screenshot shows the 'Virtual Server' configuration page. On the left, there are two radio buttons: 'Usual Service Name' and 'User-defined Service Name'. The 'User-defined Service Name' is selected. To the right of these buttons is a dropdown menu showing a list of services: AUTH, DNS, FTP, IPSEC, POP3, PPTP, SMTP, SSH, TELNET, TFTP, and WEB. The 'AUTH' service is currently selected. To the right of the dropdown menu, there are fields for 'WAN Port' (set to 5010) and 'LAN Open Port'. At the bottom right, there is a button labeled 'Apply Changes'.

To simplify configuration, there is a list of commonly used pre-defined virtual server entries to modify, otherwise, you can choose to manually add a new virtual server.

Service Type

☒ **Usual Service Name** AUTH

☐ **User-defined Service Name**

Protocol TCP

WAN Port 113 (ex. 5001:5010)

LAN Open Port 113

LAN IP Address

Apply Changes

3. Review the virtual server settings.

- **Usual Service Name** – Selecting an option from the drop down list will automatically enable virtual server with pre-defined settings. To disable, select **AUTH** from the drop down menu.
- **User-defined Service Name** – Enable and manually input your own virtual server
- **Protocol** – Select the protocol required for your device. **TCP, UDP.**
***Note:** Please refer to the device documentation to determine which ports and protocols are required.*

- **LAN Open Port** – Enter the port number required by your device. Refer to the connecting device's documentation for reference to the network port(s) required.
- **WAN Port** – Enter the port number used to access the device from the Internet.

***Note:** The **WAN Port** can be assigned a different port number than the **Private Port** (also known as port redirection), however it is recommended to use the same port number for both settings. Please refer to the device documentation to determine which ports and protocols are required.*

- **LAN IP Address** – Enter the IP address of the device to forward the port (e.g. 192.168.10.101).

Note: You should assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.

- **Apply Changes** – Saves a new virtual server entry.
- **Delete** – Delete the current virtual server entry.
- **Disable** – Disable the current virtual server entry.
- **Enable** – Enable the current virtual server entry

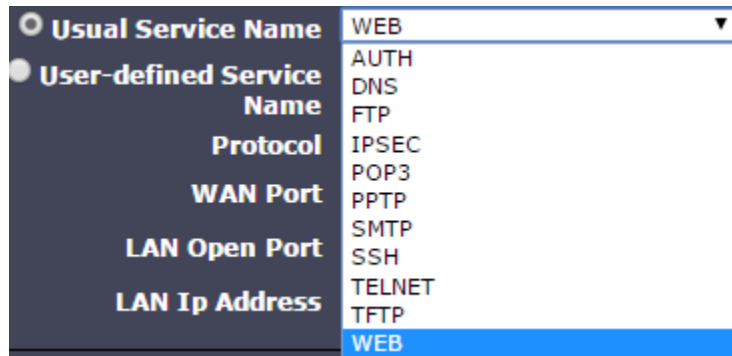
Current Virtual Server Forwarding Table

ServerName	Protocol	Local IP Address	Local Port	WAN Port	State	Action
DNS	udp	192.168.10.103	53-53	53-53	Enable	Delete Disable

Example: To forward TCP port 80 to your IP camera

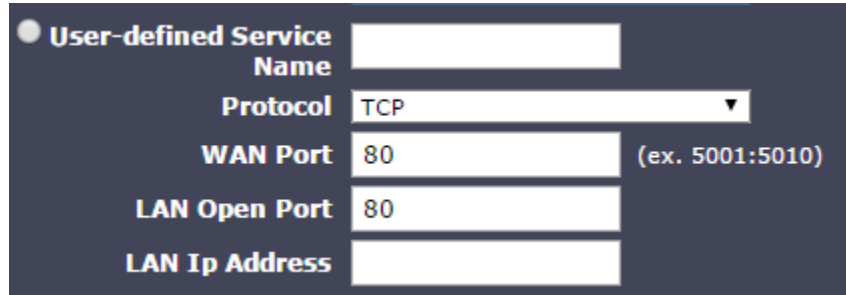
1. Setup DynDNS service (See DynDNS section).
 2. Access TRENDnet IP Camera management page and forward Port 80 (see product documentation)
 3. Make sure to configure your network/IP camera to use a static IP address or you can use the DHCP reservation feature (see "Set up DHCP reservation" on [page 25](#)).
- Note:** You may need to reference your camera documentation on configuring a static IP address.*
4. Log into your router management page (see "Access your router management page" on [page 22](#)).
 5. Click on **Advanced**, and click on **Virtual Server**.

6. Under the **Usual Service Name** drop-down menu, select **WEB**.




A screenshot of a configuration interface. On the left, there are labels for 'Usual Service Name', 'User-defined Service Name', 'Protocol', 'WAN Port', 'LAN Open Port', and 'LAN Ip Address'. To the right of these labels is a large drop-down menu. The menu is open, showing a list of service names: AUTH, DNS, FTP, IPSEC, POP3, PPTP, SMTP, SSH, TELNET, TFTP, and WEB. The 'WEB' option at the bottom of the list is highlighted in blue.

7. The fields will be populated with the selected pre-defined virtual server entry.



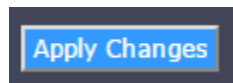
A screenshot of the same configuration interface. The 'User-defined Service Name' field is empty. The 'Protocol' field is set to 'TCP'. The 'WAN Port' field is set to '80' with a note '(ex. 5001:5010)' to its right. The 'LAN Open Port' field is set to '80'. The 'LAN Ip Address' field is empty.

8. Next to **LAN IP address**, enter the IP address assigned to the camera. (e.g. 192.168.10.101)



A screenshot of the 'LAN Ip Address' field. The field is a text box containing the IP address '192.168.10.101'.

9. To save the changes, click **Apply Changes**.



A screenshot of a button labeled 'Apply Changes'.

Special Applications

Advanced > Port Triggering

Special applications (also called port triggering) is typically used for online gaming applications or communication applications that require a range of ports or several ports to be dynamically opened on request to a device on your network. The router will wait for a request on a specific port or range of ports (or trigger port/port range) from a device on your network and once a request is detected by your router, the router will forward a single port or multiple ports (or incoming port/port range) to the device on your network. This feature is not typically used as most devices and routers currently use UPnP (Universal Plug and Play) to automatically configure your router to allow access for applications. See "Enable/disable UPnP on your router" on [page 27](#).

Note: Please refer to the device documentation to determine if your device supports UPnP first, before configuring this feature.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).

2. Click on **Advanced**, and click on **Port Triggering**. Enable Port Triggering by selecting the **Enable** option under **Port Triggering Status**.

To simplify configuration, there is a list of commonly used pre-defined special application entries to modify (in the drop down menu under **Usual Application Name**), otherwise, you can choose to manually add a new special application.

3. Review the special application settings.

- **Enabled** – Selecting **Enabled** turns on Port Triggering and selecting **Disabled** turns it off.
- **Usual Application Name** – Select from a list of commonly used pre-defined special application
- **User-defined Application Name** – Enter a name for the special application.
- **Trigger** – Port or port range requested by the device.
 - **Trigger Protocol** – Select the protocol requested by the device. **TCP**, **UDP**, or you can select **Both** to choose both TCP and **UDP**.
 - **Start Match Port** – Enter the beginning port range requested by the device. (e.g. 554 or 6112).
 - **End Match Port** – Enter the ending port range requested by the device (e.g. 554 or 6112)

Note: Please refer to the device documentation to determine which ports and protocols are required.

- **Incoming** – Port(s) forwarded to the device.

- **Open Protocol** – Select the protocol to be forwarded to the device. **TCP, UDP**, or you can select **Both** to choose both TCP and **UDP**.
- **Start Relate Port** – Enter the beginning port range to be forwarded to the device. (e.g. 2000,2069,2081,2200).
- **End Relate Port** – Enter the ending port range to be forwarded to the device. (e.g. 2038,2069,2081,2210).

Note: Please refer to the device documentation to determine which ports and protocols are required.

- **Apply Changes** – Saves a new special application.

To delete an existing application, click on the **Delete** button in the **Current Port Triggering Table** list.

Current Port Triggering Table

ServerName	Trigger Protocol	Direction	Match Port	Open Protocol	Relate Port	Action
Calista	tcp	outgoing	5190-5190	udp	3000-3000	Delete

- **Delete** – Removes an existing special application.

Router Maintenance & Monitoring

Reset your router to factory defaults

Maintenance > Reboot/Reset

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting. Before you reset your router to defaults, if possible, you should backup your router configuration first, see “Backup and restore your router configuration settings” on [page 35](#).

To reset your router to factory defaults.

- **Reset Button** – Located on the rear panel of your router, see “Product Hardware Features” on [page 2](#). Use this method if you are encountering difficulties with accessing your router management page.

OR
- **Reboot/Reset Management Page** – This is also known as a soft reboot or restart

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Maintenance** and click on **Reboot/Reset**.
3. Click on **Reset**. If prompted, click **Yes** or **Ok**.

Router Default Settings

Administrator User Name	admin
Administrator Password	Please refer to sticker or device label
Router Default URL	http://tew-731br
Router IP Address	192.168.10.1
Router Subnet Mask	255.255.255.0
DHCP Server IP Range	192.168.10.101-192.168.199
Wireless	Enabled
Wireless Network Name/Security Key	Please refer to sticker or device label

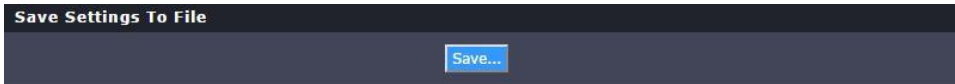
Backup and restore your router configuration settings

Tools > Settings

You may have added many customized settings to your router and in the case that you need to reset your router to default, all your customized settings would be lost and would require you to manually reconfigure all of your router settings instead of simply restoring from a backed up router configuration file.

To back up your router configuration:

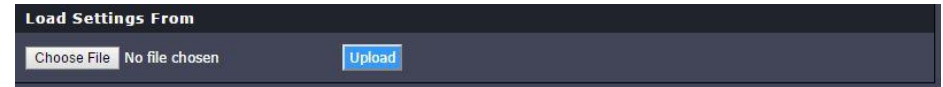
1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance** and click on **Backup/Restore**.
3. Under **Save Settings To File** click **Save**.



4. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: *cfg.bin*)

To restore your router configuration:

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance** and click on **Backup/Restore**.
3. Under **Load Settings From**, click on **Choose File**.



A separate file navigation window should open.

4. Select the router configuration file to restore and click **Open**. (Default Filename: *cfg.bin*).
5. Click the **Upload** button. If prompted, click **Yes** or **OK**.
6. Wait for the router to restore settings.

Upgrade your router firmware

Maintenance > Firmware Upgrade

TRENDnet may periodically release firmware upgrades that may add features or fix problems associated with your TRENDnet router model and version. To check if there is a firmware upgrade available for your device, please check your TRENDnet model and version using the link. <http://www.trendnet.com/downloads/>

In addition, it is also important to verify if the latest firmware version is newer than the one your router is currently running. To identify the firmware that is currently loaded on your router, log in to the router, click on the Status tab and then on the Device Information sub-tab. The firmware used by the router is listed at the top of this page. If there is a newer version available, also review the release notes to check if there were any new features you may want or if any problems were fixed that you may have been experiencing.

1. If a firmware upgrade is available, download the firmware to your computer.
2. Unzip the file to a folder on your computer.

Please note the following:

- Do not interrupt the firmware upgrade process. Do not turn off the device or press the Reset button during the upgrade.
- If you are upgrade the firmware using a laptop computer, ensure that the laptop is connected to a power source or ensure that the battery is fully charged.
- Disable sleep mode on your computer as this may interrupt the firmware upgrade process.
- Do not upgrade the firmware using a wireless connection, only using a wired network connection.
- Any interruptions during the firmware upgrade process may permanently damage your router.

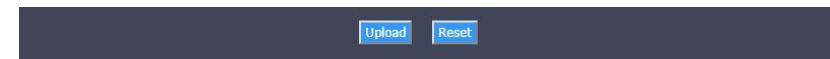
1. Log into your router management page (see "Access your router management page" on page 22).

2. Click on **Status** and click on **Device Info** to check your router's current firmware version under **System**.

System	
Firmware Version	1.00.01
Product Name	Wireless Router
Uptime	0 07:13:07
Date/Time	Thu Jan 1 07:13:07 1970

3. Click on **Maintenance** and click on **Firmware Upgrade**.

4. Depending on your web browser, under **Select File**, click **Browse** or **Choose File**.



5. Navigate to the folder on your computer where the unzipped firmware file (.bin) is located and select it.

6. Click **Upload**. If prompted, click **Yes** or **OK**.



Restart your router

Maintenance > Reboot/Restart

You may want to restart your router if you are encountering difficulties with your router and have attempted all other troubleshooting.

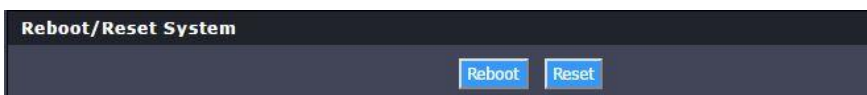
There are two methods that can be used to restart your router.

- **Turn the router off** for 10 seconds using the router On/Off switch located on the rear panel of your router, see “Product Hardware Features” on [page 2](#) .
Use this method if you are encountering difficulties with accessing your router management page. This is also known as a hard reboot or power cycle.
OR
- **Reboot/Restart Management Page** – This is also known as a soft reboot or restart.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).

2. Click on **Maintenance** and click on **Reboot/Reset**.

3. Click on the **Reboot** button. If prompted, click **Yes** or **OK**.



Check the router system information

Status > Device Info

You may want to check the system information of your router such as WAN (Internet) connectivity, wireless and wired network settings, router MAC address, and firmware version.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).

2. Click on **Status** and click on **Device Information**.

3. Review the device information.

- **Firmware Version** – The current firmware version your router is running.
- **Uptime** – The duration your router has been running continuously without a restart/power cycle (hard or soft reboot) or reset.

Firmware Version	1.00.01
Product Name	Wireless Router
Uptime	0 00:47:02
Date/Time	Thu Jan 1 00:47:02 1970

WAN (Internet) Information

- **IP Address** – The current IP address assigned to your router WAN port or interface configuration.
- **Subnet Mask** - The current subnet mask assigned to your router WAN port or interface configuration.
- **Gateway** – The current gateway assigned to your router WAN port or interface configuration.
- **DNS (Domain Name System)** – The current DNS address(es) assigned to your router port or interface configuration.

WAN Configuration

Interface	Protocol	IP Address	Gateway	DNS	Status
WAN	DHCP	0.0.0.0	0.0.0.0	0.0.0.0	Link Down (DHCP Client)

WLAN (Wireless Information)

- **SSID** – Displays the current wireless network name assigned to your router.
- **Channel** – Displays the current wireless channel your router is operating.
- **Encryption** – Displays the current wireless security configured on your router.
- **Repeater** – Displays if the repeater function is enabled or disabled

WLAN Configuration

Wireless	Enabled
Mode	AP
SSID	TRENDnet731_GZ9G
Encryption	WPA/WPA2 Mixed
Channel	2
Broadcast SSID	Enabled
WPS	Enabled
Repeater Status	Disconnected

Wired LAN Information

- **MAC Address** – The current MAC address of your router's wired LAN or interface configuration.
- **IP Address** - Displays your router's current IP address.
- **Subnet Mask** – Displays your router's current subnet mask.
- **DHCP Server** - Display your router's DHCP server status, enabled or disabled, and provides a link to the DHCP client listing. [DHCP Table](#)

LAN Configuration

IP Address	192.168.10.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	3C:8C:F8:80:00:5E

View your router packet statistics

Status > Statistics

You may want to check your router packet statistics for informational purposes only.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Status** and click on **Statistic**.
3. The table displays the amount of packets sent and received on your router's wired LAN, wireless, and WAN (Internet).

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
LAN1	0	0	0	0	0	0
LAN2						
LAN3						
LAN4						
WAN	0	0	0	0	0	0
WLAN	126596	0	71	10386	5	0

View wireless devices connected to your router

Status > Active Client Table

You may want to check the wireless devices connected to your router.

1. Log into your router management page (see “Access your router management page” on [page 25](#)).
2. Click on **Status** and click on **Active Client Table**.

3. The table displays the amount time each wireless device has been connected, the IP address, and the MAC address of each wireless device.

Active Wireless Client Table

Name	IP Address	MAC Address
DESKTOP-SC7ALS7	192.168.10.102	0c:8b:fd:91:06:4f

Router Management Page Structure

Setup

- Wizard
- Local Network
 - DHCP Server Settings
 - DHCP Static IP Configuration
- Internet Setup
 - MAC Clone
- IPv6

Wireless

- Wireless Basics
- WPS
- Advanced Wireless
- Wireless Repeater

Advanced

- Access Control List
- Port Triggering
- DMZ
- URL Block
- Dynamic DNS
- Traffic Control
- UPnP
- Telnet Configuration
- Virtual Server

Maintenance

- Reboot/Reset
- Firmware Upgrade
- Backup/Restore
- Admin
- Time and Date

Status

- Device Info
- Active Client Table
- Statistics

Help

- Menu
- Setup
- Wireless
- Advanced
- Maintenance
- Status

Technical Specifications

Standards

- IEEE 802.3
- IEEE 802.3x
- IEEE 802.3u
- IEEE 802.3az
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n (2.4 GHz up to 300 Mbps)

Hardware Interface

- 4 x 10/100 Mbps LAN ports
- 1 x 10/100 Mbps WAN port
- WPS / Reset button
- LED indicators

Special Features

- Internet Bandwidth Control
- IPv6 Support
- 5 dBi Antennas
- Multi-Language interface: English, Spanish, Portuguese
- Pre-encrypted wireless network

Access Control

- Wireless encryption: WEP, WPA / WPA2-PSK
- Firewall: NAT, SPI, Virtual Server, Port Triggering, DMZ Host, PPTP / L2TP / IPsec VPN Passthrough, allow / deny ping request from Internet
- Access Control: URL / Keyword Filter, IP Filter, Wireless MAC Filter

Quality of Service

- WMM
- Internet Bandwidth Control

Internet Connection Types

- Dynamic IP (DHCP)
- Static IP (Fixed)
- PPPoE (Dynamic IP / Static IP)
- IPv6 (Static, Auto-configuration (SLAAC / DHCPv6), Link-Local, PPPoE)

Management

- Local / remote web based management
- Upgrade firmware
- Backup / restore configuration
- Reboot
- Restore to factory defaults
- Wireless Repeater Mode

Frequency

- 2.412 - 2.484 GHz

Modulation

- 802.11b: CCK (11 Mbps & 5.5 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps)
- 802.11g: OFDM with BPSK, QPSK and 16/64-QAM
- 802.11n: BPSK, QPSK, 16-QAM, 64-QAM with OFDM

Media Access Protocol

- CSMA/CA with ACK

Antenna Gain

- 2 x 5 dBi external adjustable

Wireless Output Power

- 802.11b: FCC: 14 dBm (max.), ETSI: 17 dBm (max.) @ 11 Mbps
- 802.11g: FCC: 15 dBm (max.), ETSI: 17 dBm (max.) @ 54 Mbps
- 802.11n: FCC: 17 dBm (max.), ETSI: 14 dBm (max.) @ 300 Mbps

Receiving Sensitivity

- 802.11b: -80 dBm (typical) @ 11 Mbps
- 802.11g: -72 dBm (typical) @ 54 Mbps
- 802.11n: -72 dBm (typical) @ 300 Mbps

Wireless Channels

- FCC: 1-11
- ETSI: 1-13

Power

- Input: 100 – 240 V AC, 50 - 60 Hz
- Output: 5 V DC, 1 A external power adapter
- Consumption: 3.2 Watts (max.)

Operating Temperature

- 0 – 45 °C (32 – 113 °F)

Operating Humidity

- Max. 95% non-condensing

Certifications

- CE
- FCC

Dimensions

- 160 x 102 x 30 mm (6.2 x 4.3 x 1.3 in.)
- Antenna length: 195 mm (7.7 in.)

Weight

- 164 g (5.8 oz.)

*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions.

Troubleshooting

Q: I typed `http://192.168.10.1` in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the router management page?

Answer:

1. Check your hardware settings again. See "Router Installation" on [page 2](#).
2. Make sure the LAN and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to [Obtain an IP address automatically](#) or [DHCP](#) (see the steps below).
4. Make sure your computer is connected to one of the router's LAN ports
5. Press on the factory reset button for 15 seconds, the release.

Windows® 7/8/8.1/10

- a. Go into the **Control Panel**, click **Network and Sharing Center**.
- b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.
- c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

Windows® Vista

- a. Go into the **Control Panel**, click **Network and Internet**.
- b. Click **Manage Network Connections**, right-click the **Local Area Connection** icon and click **Properties**.
- c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

Windows® XP/2000

- a. Go into the **Control Panel**, double-click the **Network Connections** icon
- b. Right-click the **Local Area Connection** icon and the click **Properties**.
- c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

Note: If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.

Q: I am not sure what type of Internet Account Type I have for my Cable/DSL connection. How do I find out?

Answer:

Contact your Internet Service Provider (ISP) for the correct information.

Q: The Wizard does not appear when I access the router. What should I do?

Answer:

1. Click on Wizard on the left hand side.
2. Near the top of the browser, "Pop-up blocked" message may appear. Right click on the message and select Always Allow Pop-ups from This Site.
3. Disable your browser's pop up blocker.

Q: I went through the Wizard, but I cannot get onto the Internet. What should I do?

Answer:

1. Verify that you can get onto the Internet with a direct connection into your modem (meaning plug your computer directly to the modem and verify that your single computer (without the help of the router) can access the Internet).
2. Power cycle your modem and router. Unplug the power to the modem and router. Wait 30 seconds, and then reconnect the power to the modem. Wait for the modem to fully boot up, and then reconnect the power to the router.
3. Contact your ISP and verify all the information that you have in regards to your Internet connection settings is correct.

Q: I cannot connect wirelessly to the router. What should I do?

Answer:

1. Double check that the WLAN light on the router is lit.
2. Power cycle the router. Unplug the power to the router. Wait 15 seconds, then plug the power back in to the router.
3. Contact the manufacturer of your wireless network adapter and make sure the wireless network adapter is configured with the proper SSID. The preset SSID is TRENDnet(model_number).
4. To verify whether or not wireless is enabled, login to the router management page, click on *Wireless*.
5. Please see "Steps to improve wireless connectivity" on [page 16](#) if you continue to have wireless connectivity problems.

Appendix

How to find your IP address?

Note: Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.

Command Prompt Method

Windows® 2000/XP/Vista/7/8/8.1/10

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.
2. In the dialog box, type **cmd** to bring up the command prompt.
3. In the command prompt, type **ipconfig /all** to display your IP address settings.

MAC OS® X

1. Navigate to your **Applications** folder and open **Utilities**.
2. Double-click on **Terminal** to launch the command prompt.
3. In the command prompt, type **ipconfig getifaddr <en0 or en1>** to display the wired or wireless IP address settings.

Note: **en0** is typically the wired Ethernet and **en1** is typically the wireless Airport interface.

Graphical Method

MAC OS® 10.5-10.12

1. From the Apple menu, select **System Preferences**.
2. In System Preferences, from the **View** menu, select **Network**.
3. In the Network preference window, click a network port (e.g., Ethernet, AirPort, modem). If you are connected, you'll see your IP address settings under "Status:"

MAC OS® 10.4

1. From the Apple menu, select **Location**, and then **Network Preferences**.
2. In the Network Preference window, next to "Show:", select **Network Status**. You'll see your network status and your IP address settings displayed.

Note: If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.

How to configure your network settings to obtain an IP address automatically or use DHCP?

Note: Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.

Windows® 7/8/8.1/10

- a. Go into the **Control Panel**, click **Network and Sharing Center**.
- b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.
- c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

Windows® Vista

- a. Go into the **Control Panel**, click **Network and Internet**.
- b. Click **Manage Network Connections**, right-click the **Local Area Connection** icon and click **Properties**.
- c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

Windows® XP/2000

- a. Go into the **Control Panel**, double-click the **Network Connections** icon
- b. Right-click the **Local Area Connection** icon and the click **Properties**.
- c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

MAC OS® 10.4-10.12

- a. From the **Apple**, drop-down list, select **System Preferences**.
- b. Click the **Network** icon.
- c. From the **Location** drop-down list, select **Automatic**.
- d. Select and view your Ethernet connection.
 - In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Ethernet** and select the **TCP/IP** tab.
 - In MAC OS 10.5-10.9, in the left column, select **Ethernet**.
- e. Configure TCP/IP to use DHCP.
 - In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Using DHCP** and click the **Apply Now** button.

In MAC 10.5 & 10.6, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.

In MAC 10.7-10.9, from the **Configure IPv4** drop-down list, select **Using DHCP** and click the **Apply** button.

f. Restart your computer.

Note: If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.

How to find your MAC address?

In Windows® 2000/XP/Vista/7/8/8.1/10

Your computer MAC addresses are also displayed in this window, however, you can type **getmac -v** to display the MAC addresses only.

In MAC OS® 10.7-10.12

1. **Apple Menu > System Preferences > Network**
2. Select **Ethernet** from the list on the left.
3. Click the **Advanced** button.
3. On the **Hardware** tab, the **MAC Address** is your wired MAC Address.

In MAC OS® 10.5/10.6,

1. **Apple Menu > System Preferences > Network**
2. Select **Ethernet** from the list on the left.
3. Click the **Advanced** button.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.



In MAC OS® 10.4,

1. **Apple Menu > System Preferences > Network**
2. From the **Show** menu, select **Built-in Ethernet**.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.


How to connect to a wireless network using the built-in Windows utility?

Note: Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for connecting to a wireless network using the built-in utility.

Windows® 7/8/8.1/10

1. Open Connect to a Network by clicking the network icon ( or ) in the notification area.
2. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect**.
4. You may be prompted to enter a security key in order to connect to the network.
5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows® Vista

1. Open Connect to a Network by clicking the **Start Button**  and then click **Connect To**.
2. In the **Show** list, click **Wireless**.
3. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect**.
4. You may be prompted to enter a security key in order to connect to the network.
5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows® XP

1. Right-click the network icon in the notification area, then click **View Available Wireless Networks**.
2. In **Connect to a Network**, under **Available Networks**, click the wireless network you would like to connect to.
3. You may be prompted to enter a security key in order to connect to the network.
4. Enter in the security key corresponding to the wireless network, and click **Connect**.

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.



Operation of this device is restricted to indoor use only

IMPORTANT NOTE:

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 24cm between the radiator & your body.

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

Country Code selection feature to be disabled for products marketed to the US/CANADA

RoHS

This product is RoHS compliant.



Europe – EU Declaration of Conformity

TRENDnet hereby declare that the product is in compliance with the essential requirements and other relevant provisions under our sole responsibility.

Safety

EN 60950-1: 2006 + A11: 2009: + A1: 2010 + A12: 2011 + A2: 2013

EMC

EN 301 489-1 V1.9.2: 09-2011
EN 301 489-17 V2.2.1: 09-2012
EN 55022: 2010 + AC: 2011
EN 55024: 2010 + A1: 2015
EN 55032: 2015



Radio Spectrum & Health

EN 300 328 V1.9.1: 02-2015
EN 62311: 2008

Energy Efficiency

Regulation (EC) No. 1275/2008, Regulation, No. 278/2009, No. 801/2013

This product is herewith confirmed to comply with the Directives.

Directives

Low Voltage Directive 2014/35/EC
EMC Directive 2014/30/EC
R&TTE Directive 1999/5/EC
Ecodesign Directive 2009/125/EC
RoHS Directive 2011/65/EU
REACH Regulation (EC) No. 1907/2006

[cs] Česky [Czech]	TRENDnet tímto prohlašuje, že tento TEW-731BR je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES, 2014/35/ES, 2014/30/ES, 2011/65/EU, a 2009/125/ES.
[da] Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-731BR overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF, 2014/35/EF, 2014/30/EU, 2011/65/EU, og 2009/125/EF.
[de] Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TEW-731BR in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG, 2006/95/EG, und 2009/125/EG befindet.
[et] Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEW-731BR vastavust direktiivi 1999/5/EÜ, 2014/35/EÜ, 2014/30/EÜ, 2011/65/EU, ja 2009/125/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
[en] English	Hereby, TRENDnet, declares that this TEW-731BR is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC, 2014/35/EC, 2014/30/EC, 2011/65/EU, and 2009/125/EC.
[es] Español [Spanish]	Por medio de la presente TRENDnet declara que el TEW-731BR cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE, 2014/35/CE, 2014/30/CE, 2011/65/EU, 2009/125/CE y.
[el] Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑΤRENDnet ΔΗΛΩΝΕΙ ΟΤΙΤΕW-731BRΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK, 2014/35/EK, 2014/30/EK, 2011/65/EU, 2009/125/EK και.
[fr] Français [French]	Par la présente TRENDnet déclare que l'appareil TEW-731BR est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive Directiva 1999/5/CE, 2014/35/CE, 2014/30/CE, 2011/65/EU, 2009/125/CE y et.
[it] Italiano [Italian]	Con la presente TRENDnet dichiara che questo TEW-731BR è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva Directiva 1999/5/CE, 2014/35/CE, 2014/30/CE, 2011/65/EU, e 2009/125/CE.
Latviski [Latvian]	Ar šoTRENDnetdeklarē, ka TEW-731BR atbilstDirektīvas 1999/5/EK, 2014/35/EK, 2014/30/EK, 2011/65/EU, un 2009/125/EK būtiskajāmprasībām un citiemar to saistītajiemnoteikumiem.
Lietuvių	Šiuo TRENDnet deklaruoja, kad šis TEW-731BR atitinka esminius reikalavimus ir kitas 1999/5/EB, 2014/35/EB, 2014/30/EB, 2011/65/EU, ir

[lt] [Lithuanian]	2009/125/EB Direktyvos nuostatas.
[nl] Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEW-731BR in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG, 2014/35/EG, 2014/30/EG, 2011/65/EU, en 2009/125/EG.
[mt] Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TEW-731BR jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Direttiva 1999/5/KE, 2014/35/KE, 2014/30/KE, 2011/65/EU, u 2009/125/KE.
[hu] Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-731BRmegfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv, a 2014/35/EK, 2014/30/EK, 2011/65/EU, és a 2009/125/EK irányelv egyéb előírásainak.
[pl] Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEW-731BR jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/WE, 2014/35/WE, 2014/30/WE, 2011/65/EU, i 2009/125/WE.
[pt] Português [Portuguese]	TRENDnet declara que este TEW-731BR está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE, 2014/35/CE, 2014/30/CE, 2011/65/EU, e 2009/125/CE.
[sl] Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEW-731BR v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES, 2014/35/ES, 2014/30/ES, 2011/65/EU, in 2009/125/ES.
Slovensky [Slovak]	TRENDnettýmtovyhlasuje, že TEW-731BRspĺňazákladnépožiadavky a všetkypríslušnéustanoveniaSmernice 1999/5/ES, 2014/35/ES, 2014/30/ES, 2011/65/EU, a 2009/125/ES.
[fi] Suomi [Finnish]	TRENDnet vakuuttaa täten että TEW-731BR tyyppinen laite on direktiivin 1999/5/EY, 2014/35/EY, 2014/30/EY, 2011/65/EU, ja 2009/125/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[sv] Svenska [Swedish]	Härmed intygar TRENDnet att denna TEW-731BR står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG, 2014/35/EG, 2014/30/EG, 2011/65/EU, och 2009/125/EG.

Industry Canada Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Radiation Exposure Statement:

This equipment complies with IC 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.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Limited Warranty

TRENDnet warrants only to the original purchaser of this product from a TRENDnet authorized reseller or distributor that this product will be free from defects in material and workmanship under normal use and service. This limited warranty is non-transferable and does not apply to any purchaser who bought the product from a reseller or distributor not authorized by TRENDnet, including but not limited to purchases from Internet auction sites.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service. Specific warranty periods are listed on each of the respective product pages on the TRENDnet website.

- AC/DC Power Adapter, Cooling Fan, and Power Supply carry a one-year warranty.

Limited Lifetime Warranty

TRENDnet offers a limited lifetime warranty for all of its metal-enclosed network switches that have been purchased in the United States/Canada on or after 1/1/2015.

- Cooling fan and internal power supply carry a one-year warranty

To obtain an RMA, the ORIGINAL PURCHASER must show Proof of Purchase and return the unit to the address provided. The customer is responsible for any shipping-related costs that may occur. Replacement goods will be shipped back to the customer at TRENDnet's expense.

Upon receiving the RMA unit, TRENDnet may repair the unit using refurbished parts. In the event that the RMA unit needs to be replaced, TRENDnet may replace it with a refurbished product of the same or comparable model.

In the event that, after evaluation, TRENDnet cannot replace the defective product or there is no comparable model available, we will refund the depreciated value of the product.

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, or (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. International customers

shipping from outside of the USA and Canada are responsible for any return shipping and/or customs charges, including but not limited to, duty, tax, and other fees.

Refurbished product: Refurbished products carry a 90-day warranty after date of purchase. Please retain the dated sales receipt with purchase price clearly visible as evidence of the original purchaser's date of purchase. Replacement products may be refurbished or contain refurbished materials. If TRENDnet, by its sole determination, is unable to replace the defective product, we will offer a refund for the depreciated value of the product.

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").

Visit <http://www.trendnet.com/gpl> or the support section on <http://www.trendnet.com> and search 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 visit <http://www.gnu.org/licenses/gpl.txt> or <http://www.gnu.org/licenses/lgpl.txt> for specific terms of each license.

PWP07172015v3

2016/09/28



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