

User's Guide

TRENDnet[®]



N300 Wireless Gigabit Router

TEW-733GR

Table of Contents

Product Overview	1
Package Contents	1
Features	1
Product Hardware Features.....	2
Application Diagram	4
Basic Router Setup	4
Creating a Home Network	4
Router Installation	5
Connect additional wired devices to your network.....	7
Wireless Networking and Security	8
How to choose the type of security for your wireless network	8
Secure your wireless network	9
Connect wireless devices to your router	11
Connect wireless devices using WPS	12
Basic wireless settings	13
Guest Zone.....	15
Steps to improve wireless connectivity	16
Advanced wireless settings.....	16
Access Control Filters	17
Access control basics	17
MAC address filters	17
Parental Controls/URL Filters.....	17
Protocol/IP filters	18
Advanced Router Setup.....	19
Access your router management page.....	19

Change your router login password	19
Change your device name	19
Manually configure your Internet connection	20
Clone a MAC address.....	20
IPv6 Internet Connection Settings.....	20
Auto Detection	21
Static IPv6.....	21
Auto-configuration.....	22
PPPoE	22
IPv6 in IPv4 Tunnel	23
6to4	24
6rd	24
Link-local Only	24
LAN IPv6 Address Settings.....	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
Allow/deny VPN connections through your router	27
Allow/deny multicast streaming.....	27
Enable SPI	28
Identify your network on the Internet	28
Set your router date and time	29
Create schedules	29
Open a device on your network to the Internet.....	30
DMZ.....	30
Virtual Server	31

Port Forwarding	32
Application Rules.....	33
Allow remote access to your router management page	33
Internet Bandwidth Control.....	34
Add static routes to your router	34
Router Maintenance & Monitoring.....	35
Reset your router to factory defaults	35
Router Default Settings	35
Backup and restore your router configuration settings	36
Upgrade your router firmware	36
Restart your router	37
Check connectivity using the router management page	37
Check the router system information.....	38
View your router log	40
Send router logs to your email	41
Setup a syslog server from router	42
View your router packet statistics	42
View your router active sessions	43
View your routing table	43
View devices connected to your router.....	44
View wireless devices connected to your router.....	44
View your router's IPv6 network information	44
Router Management Page Structure	45
Technical Specifications.....	46
Troubleshooting.....	47
Appendix	48

Product Overview

TEW-733GR



Package Contents

In addition to your router, the package includes:

- Multi-Language Quick Installation Guide
- CD-ROM (User's Guide)
- Network cable (1.5 m / 5 ft.)
- Power adapter (12V 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 Wireless Gigabit Router, model TEW-733GR, offers proven high performance 300 Mbps wireless n networking and gigabit wired Ethernet ports. Embedded GREENnet technology reduces power consumption by up to 50%. For your security this router comes pre-encrypted and features a guest network. Seamlessly stream HD video with this powerful router.

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

Security

Pre-Encrypted

For your security the router is pre-encrypted with a unique password

Guest Network

Create a secure isolated network for guest internet access only

Parental Controls

Control access to specific websites

Performance

N300 Wireless

Proven 300 Mbps Wireless N

Gigabit Ports

Gigabit ports extend high performance wired connections

Wireless Coverage

Extensive wireless coverage with MIMO antenna technology

Quality of Service (QoS)

Advanced QoS prioritizes video and audio transmissions

Compatibility

Compatible with older Wireless G devices

Energy Savings

Embedded GREENnet technology reduces power consumption by up to 50%

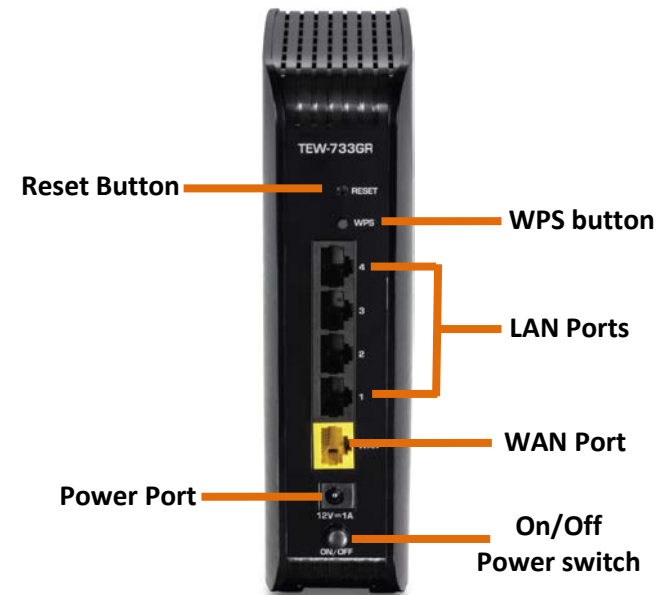
IPv6

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.

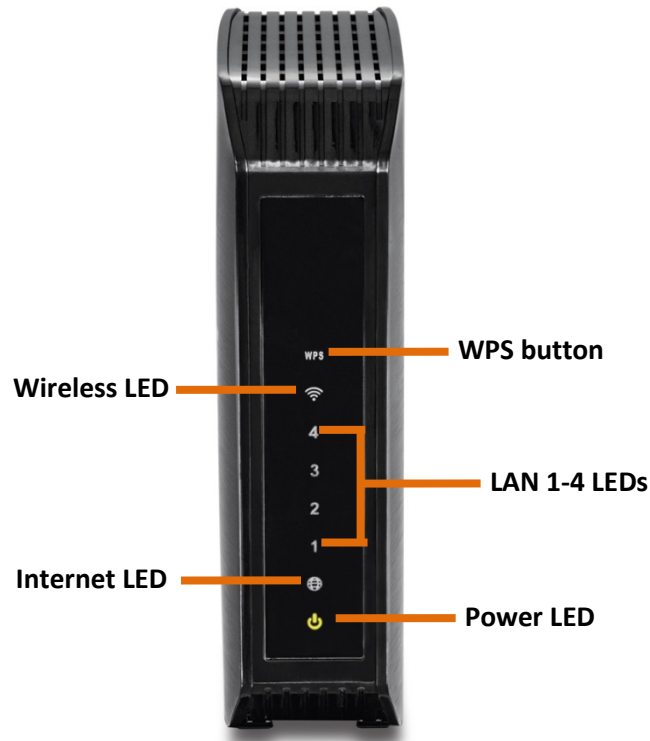
Product Hardware Features

Rear View



- **Reset Button:** Use an item such as a paperclip to push and hold this button for 10 seconds and release to reset your router to its factory defaults.
- **WPS Button:** Wi-Fi Protected Setup Button (WPS), press for 3 seconds to activate feature.
- **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.
- **On/Off Power Switch:** Push the router On/Off power switch to turn your router "On" (Inner position) or "Off" (Outer position).

Front View



- **Internet (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.
- **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.

- **WPS LED:** This LED indicator blinks when WPS is active and searching for WPS clients.
- **Wireless (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.
- **LAN 1-4 (Link/Activity) LEDs:** These LED indicators are solid green when the LAN ports are successfully connected to your wired network devices (which are turned on). These LED indicators will blink green while data is transmitted or received through your router's LAN ports.

Application Diagram



The router is installed near the modem typically supplied by your ISP "Internet Service Provider. The router's WAN port is physically connected 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 throughout your network.

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 10.
5. To set up wireless networking on your router, see "[Secure your wireless network](#)" on page 12.

How to setup your router

Refer to the Quick Installation Guide or continue to the next section "[Router Installation](#)" on page 8 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)

Router Installation

Before you Install

Many Internet Service Providers (ISPs) allow your router to connect to the Internet without verifying the information fields listed below. Skip this section for now and if your router cannot connect to the Internet using the standard installation process, come back to this page and contact your ISP to verify required ISP specification fields listed below.

1. Obtain IP Address Automatically (DHCP)

Host Name (Optional)

Clone Mac Address (Optional)

2. Fixed IP address

WAN IP Address: _____. _____. _____. _____.
(e.g. 215.24.24.129)

WAN Subnet Mask: _____. _____. _____. _____.
(e.g. 255.255.255.0)

WAN Gateway IP Address: _____. _____. _____. _____.
(e.g. 215.24.24.1)

DNS Server Address 1: _____. _____. _____. _____.
(e.g. 215.24.24.1)

DNS Server Address 2: _____. _____. _____. _____.
(e.g. 215.24.24.1)

3. PPPoE to obtain IP automatically

User Name: _____

Password: _____

Verify Password: _____

4. PPPoE with a fixed IP address

User Name: _____

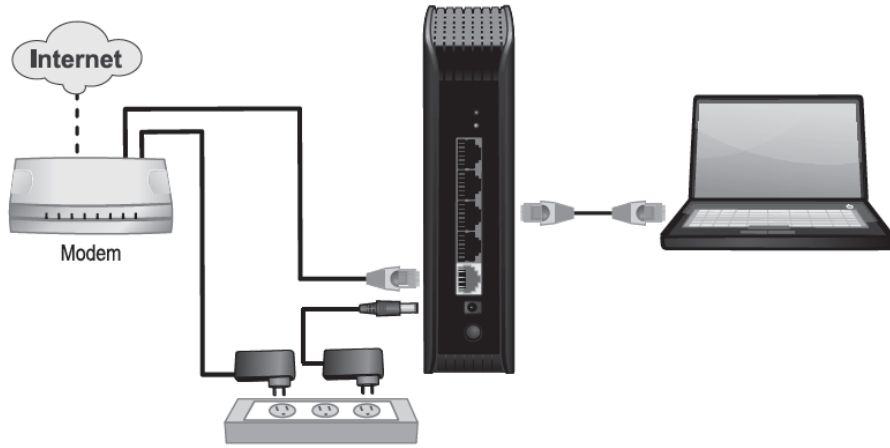
Password: _____

Verify Password: _____

IP Address: _____. _____. _____. _____. (e.g. 215.24.24.129)

Hardware Installation

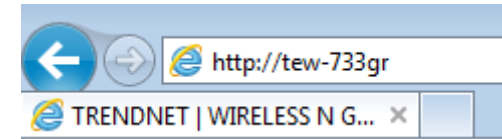
1. Verify that you have an Internet connection when connecting your computer directly to your modem.



2. Turn off your modem.
3. Disconnect the Network cable from your computer to your modem.
4. Use a Network cable and connect the WAN port (yellow port) on the router to your modem.
5. Use another Network cable and connect your computer to one of the four LAN ports on the router.
6. Plug in the power adapter, connect it to the router's power port, and then push the On/Off Power Switch to the "On" position (pushed in).
7. Turn on your modem.
8. Verify that the following front panel LED indicators on your router: Power (Solid Green), Status (Blinking Green), LAN 1, 2, 3, or 4 (Solid/Blinking Green for ports for which devices are connected), WAN (Solid/Blinking Green), and WLAN (Blinking Green).

Setup Wizard

1. Open your web browser and the router's configuration screen will automatically appear. If not type, <http://tew-733gr> on the address bar of your web browser.

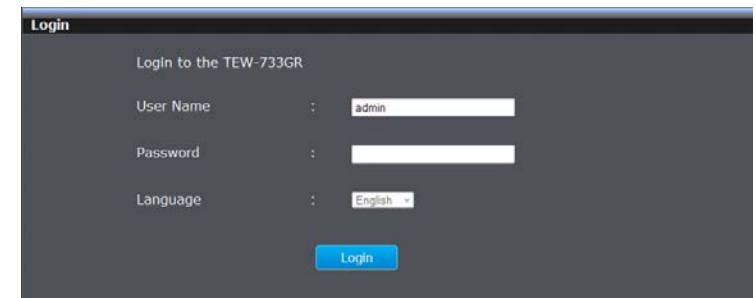


2. Select the language to use on the bottom drop-down list to select your preferred language. Enter the default user name and password and then click **Login** to continue.

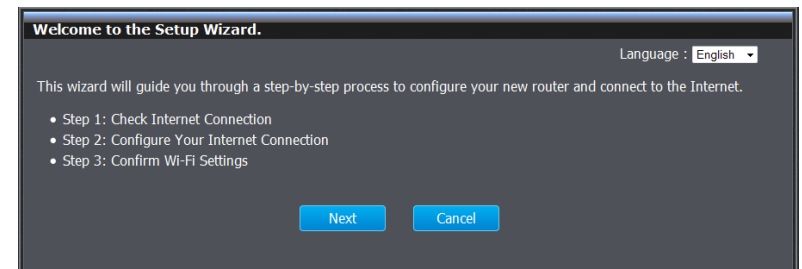
Default User Name: **admin**

Default Password: Please refer to the device label or wireless sticker on the unit for more information.

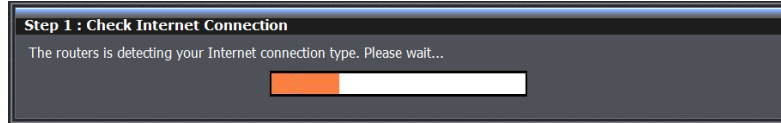
Note: For added security your router has a unique login password and wireless settings.



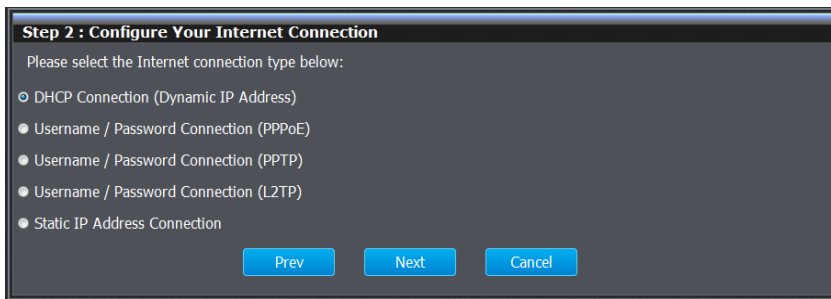
3. Once you are logged in to the router. You will begin the router's setup wizard. Click Next.



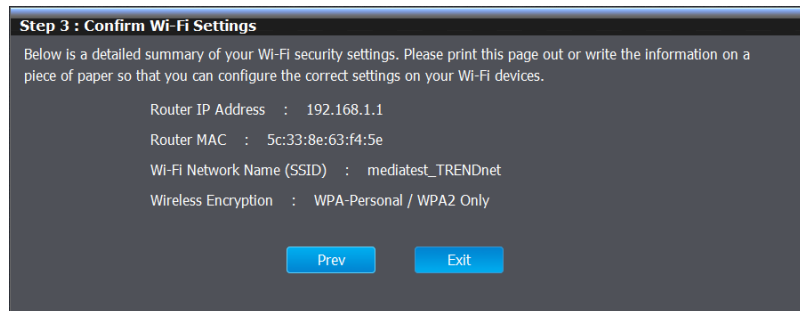
4. The setup wizard will detect your internet connection. Continue to step 6 if your internet connection type was detected.



5. If the wizard was unable to detect your internet connection type you will be asked to select your internet connection type. Click Next to continue. Please contact your ISP (Internet Service Provider) for additional information of your internet connection type.



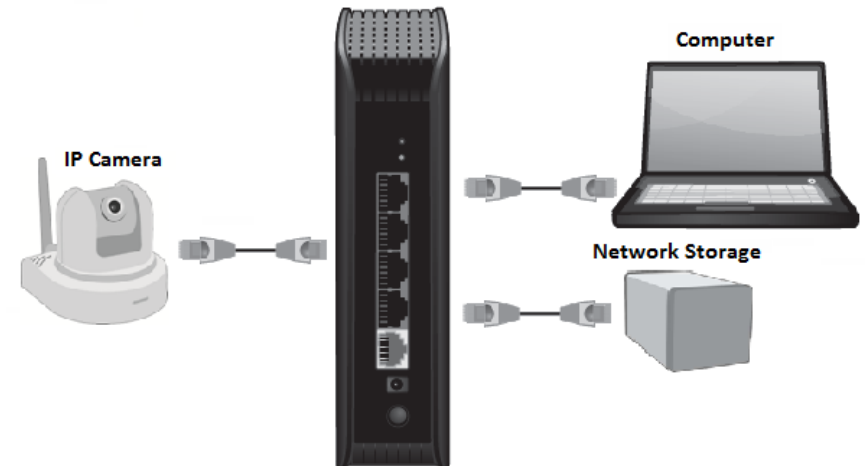
6. Verify your wireless settings and click Exit to complete the wizard.



Note: For added security your router comes with preconfigured wireless settings, please refer to the device label or wireless sticker on the unit for more information.

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. Check the status of the LED indicators (1, 2, 3, or 4) on the front panel of your router to ensure the physical cable connection from your computer or device.



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 802.11 b 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 450Mbps*
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 11), 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**, and click on **Security**.
3. Click on the **Authentication Type** drop-down list to select your wireless security type.

Wireless Security Mode

Security Mode: None (dropdown menu open showing: None, WEP, WPA-Personal, WPA-Enterprise)

Selecting WEP:

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

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64-bit keys you must enter 10 hex digits into each key box. For 128-bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64-bit keys, and a maximum of 13 characters for 128-bit keys.

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**. This means you will **NOT** get 11N performance due to the fact that WEP is not supported by the Draft 11N specification.

WEP Key Length: 64 bit (10 hex digits) (length applies to all keys)

Authentication: Both

WEP Key 1:

- **WEP:** Choose **Open System** or **Shared Key**.
Note: It is recommended to use Open System because it is known to be more secure than Shared Key.
- **Mode:** Choose **HEX** or **ASCII**.
Note: It is recommended to use ASCII because of the much larger character set that can be used to create the key.
- **WEP Key:** Choose the key length **64-bit** or **128-bit**.
Note: It is recommended to use 128-bit because it is more secure to use a key that consists of more characters.

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

- **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, WPA-Auto, or WPA2 (WPA2 recommended):

WPA	
<p>Use WPA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.</p> <p>To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher).</p>	
WPA Mode	WPA2 Only
Cipher Type	AES
Group Key Update Interval	3600 (seconds)
Pre-Shared Key	
<p>Enter an 8 to 63 ASCII or 8 to 64 HEX alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.</p>	
Pre-Shared Key	1234567890

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

Then from the PSK/EAP row, select either **PSK** or **EAP**

- **PSK** stands for Preshared Key
- **EAP** stands for Extensive Authentication Protocol, also called Remote Authentication Dial-In User Service or RADIUS).

Note: EAP requires an external RADIUS server, PSK only requires you to create a passphrase.

The following section outlines options when selecting **PSK** (Preshared Key Protocol),

- Select a Cipher Type. When selecting **WPA** security, it is recommended to use **TKIP**.
- When selecting **WPA-Auto** security, it is recommended to use **AES**.
- When selecting **WPA2** security, it is recommended to use **AES**.

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.)

The following section outlines options when selecting **EAP** (Extensive Authentication Protocol),

EAP (Extensible Authentication Protocol) is also called Remote Authentication Dial-In User Service or RADIUS.

Select a Cipher Type

- When selecting **WPA** security, it is recommended to use **TKIP**.
- When selecting **WPA-Auto** security, it is recommended to use **AES**.
- When selecting **WPA2** security, it is recommended to use **AES**.

WPA	
<p>Use WPA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.</p> <p>To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher).</p>	
WPA Mode	WPA2 Only ▼
Cipher Type	AES ▼
Group Key Update Interval	3600 (seconds)
EAP (802.1x)	
<p>When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.</p>	
RADIUS server IP Address	
RADIUS server Port	1812
RADIUS server Shared Secret	
Advance Setting	Advanced >>

- **RADIUS Server 1/2** - Configure the RADIUS server settings.

Note: RADIUS Server 2 is optional and can be configured as a backup if there are any issues with RADIUS Server 1.

- **IP** – Enter the IP address of the RADIUS server. (e.g. 192.168.10.250)
- **Port** – Enter the port your RADIUS server is configured to use for RADIUS authentication.

Note: It is recommended to use port 1812.

- **Shared Secret** – Enter the shared secret used to authorize your router with your RADIUS server.

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 51 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

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 Green 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 5)

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

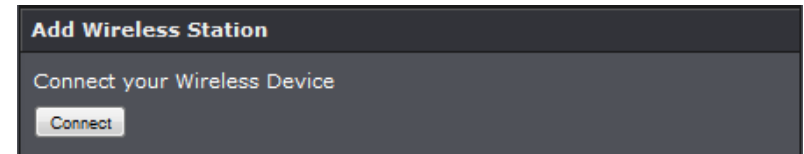
Note it is recommended that a wireless key (passphrase or password) is created before connecting clients using the PBC method. If no wireless key is defined when connecting via PBC, the router will automatically create an encryption key that is 64 characters long. This 64 character key will then have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

PBC (Software/Virtual Push Button)

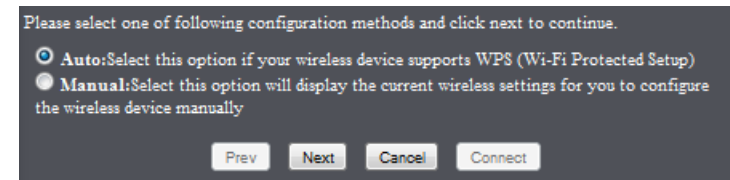
Wireless > WiFi Protected Setup

In addition to the hardware push button located physically on your router, the router management page also has push button which is a software or virtual push button you can click to activate WPS on your router.

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Wireless**, and click on **WPS**.
3. To add a wireless device to your network, simply click **Connect** under **Add Wireless Station** to begin WPS.



4. You will receive an option of Auto and Manual. Select Auto and click Next to continue with WPS.



5. Select **PBC** option to continue using WPS PBC method and click Next .

There are two ways to add wireless device to your wireless network:

- PIN (Personal Identification Number)
- PBC (Push Button Configuration)

☒ PIN :

please enter the PIN from your wireless device and click the below "Connect" Button within 120 seconds

☐ PBC

please press the push button on your wireless device and click the below "Connect" Button within 120 seconds

Prev Next Cancel Connect

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.

5. You will receive a success message indicate that the wireless device successfully connected using WPS.

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 **WPS**.
3. To add a wireless device to your network, simply click **Connect** under **Add Wireless Station** to begin WPS.

Add Wireless Station

Connect your Wireless Device

Connect

4. You will receive an option of Auto and Manual. Select Auto and click Next to continue with WPS.

Please select one of following configuration methods and click next to continue.

☒ **Auto:** Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)

☐ **Manual:** Select this option will display the current wireless settings for you to configure the wireless device manually

Prev Next Cancel Connect

5. Select **PIN** option and enter your wireless device's PIN information. Click **Next** to continue.

There are two ways to add wireless device to your wireless network:

- PIN (Personal Identification Number)
- PBC (Push Button Configuration)

☒ PIN :

please enter the PIN from your wireless device and click the below "Connect" Button within 120 seconds

☐ PBC

please press the push button on your wireless device and click the below "Connect" Button within 120 seconds

Prev Next Cancel Connect

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 **Basic**.
3. To save changes to this section, click **Save Settings** when finished.

• Wireless

Enable Wireless	<input checked="" type="checkbox"/> Always	New Schedule
-----------------	--	--------------

- **Enable:** Check the box to enable wireless networking on your router.
- **Disable:** Uncheck the box to disable wireless networking
- **Schedule:** Select an applied schedule rule on the drop down list of when the wireless network will be enabled. Select **Always** to have wireless network always enabled.
- **New Schedule:** Click this button to set a new schedule rule.

- **Wireless Network Name (SSID):** The acronym SSID 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 has a predefined SSID (refer to the wireless sticker or device label). If you choose to change the SSID, change it to a name that you can easily remember.

Wireless Network Name	TRENDnet733	(This is also called the SSID.)
-----------------------	-------------	---------------------------------

- **802.11 Mode:** Select the appropriate mode for your network.

802.11 Mode	Mixed 802.11n, 802.11g and 802.11b
-------------	------------------------------------

- **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 802.11g 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.

- **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.

Enable Auto Channel Scan	<input type="checkbox"/>
--------------------------	--------------------------

- **Channel:** To manually set the channel on which the router will broadcast, uncheck **Auto Channel**, then 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.

Wireless Channel	2.452 GHz - CH 9
------------------	------------------

- **Transmission Rate:** Set the transmission rate of your wireless network. Please note that it is best that this setting remains on the default setting of **Best**.

Transmission Rate	Best (Automatic)	(Mbit/s)
-------------------	------------------	----------

- **802.11 Mode:** Select the appropriate mode for your network.

802.11 Mode Mixed 802.11n, 802.11g and 802.11b ▼

- **Channel Width:** This setting only applies to wireless devices connecting at 802.11n. Select the appropriate channel width for your wireless network.

Channel Width 20/40 MHz(Auto) ▼

- **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.

- **Visibility Status**

Visibility Status ☒ Visible ☐ Invisible

- **Visible:** Allows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your router.
- **Invisible:** 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 **Invisible**, may cause issues with your wireless adapters.

- **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.

WMM Enable ☒ (Wireless QoS)

Guest Zone

Access > Guest Zone

Creating an isolated and separate wireless guest network allows wireless clients to connect to your network for Internet access only and keep your local LAN network safe by restricting guest access to your LAN network resources such as shared documents and media files on your computers, network storage, and printers.

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Access** and click on **Guest Zone**.

Guest Zone	
Wireless Band	2.4GHz Band
Enable Guest Zone	<input type="checkbox"/> Always ▼ <input type="button" value="New Schedule"/>
Wireless Network Name	TRENDnet733_2.4GHz (This is also called the SSID.)
Enable Routing Between Zones	<input type="checkbox"/>
Security Mode	None ▼

3. Review the Guest Zone settings, click **Save Settings** to continue.

- **Enabled:** Check the option to enable the Guest Network. Select **Always** to have guest zone enabled always or select a schedule rule in the pull down menu.
- **Wireless Network Name (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. It is recommended to use a different name from your primary wireless network to a name that you can easily identify and differentiate from the primary. You can reference your guests to access this network instead of the primary.
- **Enable Routing Between Zone:** Select this option to allow guests to restrict your guest to only have access to the Internet.
- **Security Mode:** Select the wireless security you would like to apply to the guest zone.

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.

Advanced Wireless Settings	
Wireless Band	2.4GHz Band
Transmit Power	100% ▾
Beacon Period	100 (milliseconds, Range: 20~1000, default: 100)
Preamble Type	<input type="radio"/> Short Preamble <input checked="" type="radio"/> Long Preamble

- **Transmit Power:** The transmit power of your wireless radio can be adjusted in percentages.
Default Value:100%
- **Beacon Period:** A beacon is a management frame used in wireless networks that transmitted periodically to announce the presence and provide information about the router's wireless network. The interval is the amount time between each beacon transmission.
Default Value:100 milliseconds (range: 20-1000)
- **Preamble Type:** Select Short or Long Preamble

Access Control Filters

Access control basics

MAC address filters

Access > Filter > MAC Filters

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 **Access**, click on **Filter**, and click on **MAC Filters**. Click **Save Settings** to apply rule.

3. Review the MAC Filter options.

- **Turn Off:** Disables MAC address filter.
- **Mac Filter ON and Allow** computers/devices with MAC addresses listed below to access the local network (LAN/WLAN), web management, and the Internet.
- **Mac Filter ON and Deny** computers/devices with MAC addresses listed below to access the local network (LAN/WLAN), web management, and the Internet

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.

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

	MAC Address		DHCP Client List	Schedule
<input type="checkbox"/>		<<	Computer Name ▾	Always ▾ New Schedule
<input type="checkbox"/>		<<	Computer Name ▾	Always ▾ New Schedule
<input type="checkbox"/>		<<	Computer Name ▾	Always ▾ New Schedule
<input type="checkbox"/>		<<	Computer Name ▾	Always ▾ New Schedule
<input type="checkbox"/>		<<	Computer Name ▾	Always ▾ New Schedule

Note: Do not configure this setting until you have added the MAC addresses to the MAC Table first. The recommended option is to only **Allow** access to the MAC addresses listed and deny all others unlisted.

- **Check box:** Check the box to enable rule.
- **MAC Address** – Enter the 12-digit MAC address.(e.g. 00-11-22-AA-BB-CC)
- **Schedule:** Select **Always** to have rule always on or select a schedule rule.

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 28 or refer to your computer or device documentation to find the MAC address.

Parental Controls/URL Filters

Access > Filter > Domain/URL Blocking

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 **Access**, click on **Parental Control**. Click **Save Settings** to apply rule.

40 -- Website Filtering Rules

Configure Website Filter below:

Turn OFF WEBSITE FILTERING

Remaining number of rules that can be created.: 40

	Website URL	Schedule
<input type="checkbox"/>		Always <input type="button" value="New Schedule"/>
<input type="checkbox"/>		Always <input type="button" value="New Schedule"/>
<input type="checkbox"/>		Always <input type="button" value="New Schedule"/>
<input type="checkbox"/>		Always <input type="button" value="New Schedule"/>

3. Review the Domain/URL blocking options.

- **Turn Off:** Disables Website Filter address filter.
- **Allow** computers to access only the websites listed below to access the local network (LAN/WLAN), web management, and the Internet.
- **Deny** computers access only the websites listed below.

4. Enter the website you would like to apply.

	Website URL	Schedule
<input type="checkbox"/>		Always <input type="button" value="New Schedule"/>
<input type="checkbox"/>		Always <input type="button" value="New Schedule"/>
<input type="checkbox"/>		Always <input type="button" value="New Schedule"/>

- **Check box:** Check the box to enable rule.
- **Website URL:** Enter the website URL you would like to filter.
- **Schedule:** Select **Always** to have rule always on or select a schedule rule.

Protocol/IP filters

Access > Protocol/IP Filters

You may want to block computers or devices on your network access to specific ports (used or required by a specific application) to the Internet.

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Access**, click on **Protocol/IP Filters**. Click **Add** to apply rule.

Add Inbound Filter Rule

Name			
Action	Allow		
Remote IP Range	Enable	Remote Start IP Address	Remote End IP
	<input type="checkbox"/>	0.0.0.0	255.255.255.255
	<input type="checkbox"/>	0.0.0.0	255.255.255.255
	<input type="checkbox"/>	0.0.0.0	255.255.255.255

3. Review the Domain/URL blocking options.

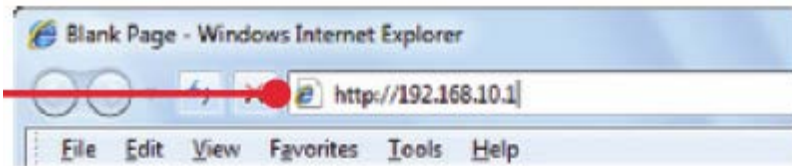
- **Name:** Enter the name of the rule to apply.
- **Action:** Select the action to apply to the rule.
 - **Allow:** Allows the listed IP address
 - **Deny:** Denies the listed IP address.
- **Check box:** Check the box to enable rule.
- **IP Address:** Enter the IP address of the rule that will reflect on the selected action.
- **Subnet Mask:** Enter the subnet mask of the IP address.

Advanced Router Setup

Access your router management page

Note: Your router management page <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 (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to <http://192.168.10.1>. Your router will prompt you for a user name and password.



2. Next to Language, click the drop-down list to select your preferred language. Enter the default user name and password and then click **Login**.

Default User Name: **admin**

Default Password: Please refer to the wireless sticker placed on the side of the unit or the device label

Change your router login password

Main > Password

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Main**, and click on **Password**.
3. Under the **Administrator** section, in the **New Password** field, enter the new password, and in the **Confirm Password** field, retype the new password again to confirm.
4. To save changes, click **Save Settings**.

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

Change your device name

Main > Password

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Main**, and click on **Password**.
3. In the **Gateway Name** field, enter the new device name to display on your network to identify the router. Click **Save Settings** to apply changes.

Manually configure your Internet connection

Main > WAN

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Main**, and click on **WAN**.
3. In the **Connection 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**.

Internet Connection Type	
Choose the mode to be used by the router to connect to the Internet.	
My Internet Connection is	<div> <div>PPPoE (Username / Password)</div> <div>Static IP</div> <div>Dynamic IP (DHCP)</div> <div>PPPoE (Username / Password)</div> <div>PPTP (Username / Password)</div> <div>L2TP (Username / Password)</div> <div>DS-Lite</div> </div>

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.

Clone a MAC address

Main > WAN

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 **Main**, and click on **WAN**.
3. Under your Internet connection settings, find the **MAC Address** section shown below.

MAC Address	<input type="text"/>
Clone Your PC's MAC Address	<input type="button" value="Clone Your PC's MAC Address"/>

4. Click either **Clone MAC Address** to clone the MAC address of the computer you are currently using or manually enter the 12-digit MAC address of your old router.
5. To save changes, click **Save Settings**.

IPv6 Internet Connection Settings

Network > IPv6 Setting

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 **Main**, and click on **IPv6**.
3. Review the IPv6 Internet Connection settings and select your IPv6 type under My IPv6 Connection section. Click **Save Settings** to continue.

IPv6 Connection Type	
Choose the mode, used by the router, to connect to the IPv6 Internet.	
My IPv6 Connection is	Link-local Only
LAN IPv6 Address Settings	
Use this section to configure the internal network settings of your router.	
LAN IPv6 Link-local Address	fe80::5e33:8eff:fe63:f45e /64

Auto Detection

IPv6 DNS Settings

- **Obtain IPv6 DNS Servers automatically:** Allows the router to automatically obtain IPv6 DNS server IP addresses.
- **Use the following IPv6 DNS Servers:** Manually enters the IPv6 DNS server IP addresses.
- **Primary DNS Server:** Enter the primary IPv6 DNS server address. This field is only available when Use the following IPv6 DNS Servers is selected.
- **Secondary DNS Server:** Enter the secondary IPv6 DNS server address. This field is only available when Use the following IPv6 DNS Servers is selected.

LAN IPv6 Address Settings

- **Enable DHCP-PD:** Tick the check box to enable the DHCP Prefix Delegation feature.
- **LAN IPv6 Address:** Enter the LAN IPv6 address.
- **LAN IPv6 Link-local Address:** This field displays the LAN IPv6 link-local address.
- **Address Auto-configuration Settings**
- **Enable automatic IPv6 address assignment:** Tick the check box to enable automatic IPv6 address assignment.
- **Enable automatic DHCP-PD in LAN:** Tick the check box to enable automatic DHCP-PD in LAN.
- **Auto-configuration Type:** The available IPv6 auto configuration types are SLAAC+RDNSS, SLAAC+Stateless DHCP, and Stateful DHCPv6.
- **Router Advertisement Lifetime:** Displays the router advertisement lifetime in minutes. This field appears when SLAAC+RDNSS or SLAAC+Stateless DHCP is selected.
- **IPv6 Address Range (Start):** Enter the start IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Range (End):** Enter the end IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Lifetime:** Displays the IPv6 address lifetime in minute. This field appears when Stateful DHCPv6 is selected.

Static IPv6

WAN IPv6 Address Settings

- **Use Link-local Address:** Tick the check box to use the link-local address. Deselect this to enter WAN IP information below in this section.
- **IPv6 Address:** Enter the IPv6 address.
- **Subnet Prefix Length:** Enter the subnet prefix length.
- **Default Gateway:** Enter the default gateway IPv6 address.
- **Primary DNS Server:** Enter the primary IPv6 DNS server address.
- **Secondary DNS Server:** Enter the secondary IPv6 DNS server address.
- **LAN IPv6 Address Settings**
- **LAN IPv6 Address:** Enter the LAN IPv6 address.

- **LAN IPv6 Link-local Address:** This field displays the LAN IPv6 link-local address.
- Address Auto-configuration Settings
- **Enable automatic IPv6 address assignment:** Tick the check box to enable automatic IPv6 address assignment.
- **Auto-configuration Type:** The available IPv6 auto configuration types are SLAAC+RDNSS, SLAAC+Stateless DHCP, and Stateful DHCPv6.
- **Router Advertisement Lifetime:** Enter the router advertisement lifetime in minutes. This field is only available when SLAAC+RDNSS or SLAAC+Stateless DHCP is selected.
- **IPv6 Address Range (Start):** Enter the start IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Range (End):** Enter the end IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Lifetime:** Displays the IPv6 address lifetime in minute. This field is only available when Stateful DHCPv6 is selected.

Auto-configuration

IPv6 DNS Settings

- **Obtain IPv6 DNS Servers automatically:** Allows the router to automatically obtain IPv6 DNS server IP addresses.
- **Use the following IPv6 DNS Servers:** Manually enters the IPv6 DNS server IP addresses.
- **Primary DNS Server:** Enter the primary IPv6 DNS server address. This field is only available when Use the following IPv6 DNS Servers is selected.
- **Secondary DNS Server:** Enter the secondary IPv6 DNS server address. This field is only available when Use the following IPv6 DNS Servers is selected.

LAN IPv6 Address Settings

- **Enable DHCP-PD:** Tick the check box to enable the DHCP Prefix Delegation feature.
- **LAN IPv6 Address:** Enter the LAN IPv6 address.
- **LAN IPv6 Link-local Address:** This field displays the LAN IPv6 link-local address.
- Address Auto-configuration Settings

- **Enable automatic IPv6 address assignment:** Tick the check box to enable automatic IPv6 address assignment.
- **Enable automatic DHCP-PD in LAN:** Tick the check box to enable automatic DHCP-PD in LAN.
- **Auto-configuration Type:** The available IPv6 auto configuration types are SLAAC+RDNSS, SLAAC+Stateless DHCP, and Stateful DHCPv6.
- **Router Advertisement Lifetime:** Displays the router advertisement lifetime in minutes. This field appears when SLAAC+RDNSS or SLAAC+Stateless DHCP is selected.
- **IPv6 Address Range (Start):** Enter the start IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Range (End):** Enter the end IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Lifetime:** Displays the IPv6 address lifetime in minute. This field appears when Stateful DHCPv6 is selected.

PPPoE

PPPOE Internet Connection Type

- **PPPoE Session:** Select the PPPoE session. To share this connection with IPv4, click the Share with IPv4 radio button. To create a new connection, click the Create a new session radio button.
- **Address Mode:** Select the PPPoE IP address is dynamic or static.
- **IP Address:** Enter the static IPv6 address. This field is available when Static IP is selected.
- **Username:** Enter the IPv6 PPPOE username. This field is available when Create a new session is selected.
- **Password:** Enter the IPv6 PPPOE password. This field is available when Create a new session is selected.
- **Verify Password:** Re-type the IPv6 PPPOE password. This field is available when Create a new session is selected.
- **Service Name:** Enter the service name. This is optional. This field is available when Create a new session is selected.
- **Reconnect Mode:** Select the reconnect mode as Always on, or Manual.
- **MTU:** Enter the Maximum Transmission Unit (MTU) value.

IPv6 DNS Settings

- **Obtain IPv6 DNS Servers automatically:** Allows the router to automatically obtain IPv6 DNS server IP addresses.
- **Use the following IPv6 DNS Servers:** Manually enters the IPv6 DNS server IP addresses.
- **Primary DNS Server:** Enter the primary IPv6 DNS server address. This field is only available when Use the following IPv6 DNS Servers is selected.
- **Secondary DNS Server:** Enter the secondary IPv6 DNS server address. This field is only available when Use the following IPv6 DNS Servers is selected.

LAN IPv6 Address Settings

- **Enable DHCP-PD:** Tick the check box to enable the DHCP Prefix Delegation feature.
- **LAN IPv6 Address:** Enter the LAN IPv6 address.
- **LAN IPv6 Link-local Address:** This field displays the LAN IPv6 link-local address.

Address Auto-configuration Settings

- **Enable automatic IPv6 address assignment:** Tick the check box to enable automatic IPv6 address assignment.
- **Enable automatic DHCP-PD in LAN:** Tick the check box to enable automatic DHCP-PD in LAN.
- **Auto-configuration Type:** The available IPv6 auto configuration types are SLAAC+RDNSS, SLAAC+Stateless DHCP, and Stateful DHCPv6.
- **Router Advertisement Lifetime:** Displays the router advertisement lifetime in minutes. This field appears when SLAAC+RDNSS or SLAAC+Stateless DHCP is selected.
- **IPv6 Address Range (Start):** Enter the start IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Range (End):** Enter the end IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Lifetime:** Displays the IPv6 address lifetime in minute. This field appears when Stateful DHCPv6 is selected.

IPv6 in IPv4 Tunnel

IPv6 in IPv4 Tunnel Settings

- **Remote IPv4 Address:** Enter the remote IPv4 address.
- **Remote IPv6 Address:** Enter the remote IPv6 address.
- **Local IPv4 Address:** Enter the local IPv4 address.
- **Local IPv6 Address:** Enter the local IPv6 address.
- **Subnet Prefix Length:** Enter the subnet prefix length value.

IPv6 DNS Settings

- **Obtain IPv6 DNS Servers automatically:** Allows the router to automatically obtain IPv6 DNS server IP addresses.
- **Use the following IPv6 DNS Servers:** Manually enters the IPv6 DNS server IP addresses.
- **Primary DNS Server:** Enter the primary IPv6 DNS server address. This field is only available when Use the following IPv6 DNS Servers is selected.
- **Secondary DNS Server:** Enter the secondary IPv6 DNS server address. This field is only available when Use the following IPv6 DNS Servers is selected.

LAN IPv6 Address Settings

- **Enable DHCP-PD:** Tick the check box to enable the DHCP Prefix Delegation feature.
- **LAN IPv6 Address:** Enter the LAN IPv6 address.
- **LAN IPv6 Link-local Address:** This field displays the LAN IPv6 link-local address.
- **Address Auto-configuration Settings**
- **Enable automatic IPv6 address assignment:** Tick the check box to enable automatic IPv6 address assignment.
- **Enable automatic DHCP-PD in LAN:** Tick the check box to enable automatic DHCP-PD in LAN.
- **Auto-configuration Type:** The available IPv6 auto configuration types are SLAAC+RDNSS, SLAAC+Stateless DHCP, and Stateful DHCPv6.
- **Router Advertisement Lifetime:** Displays the router advertisement lifetime in minutes. This field appears when SLAAC+RDNSS or SLAAC+Stateless DHCP is selected.
- **IPv6 Address Range (Start):** Enter the start IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.

- **IPv6 Address Range (End):** Enter the end IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Lifetime:** Displays the IPv6 address lifetime in minute. This field appears when Stateful DHCPv6 is selected.

6to4

WAN IPv6 Address Settings

- **6to4 Address:** Displays the 6 to 4 IP address.
- **6to4 Relay:** Enter the 6to4 relay address.
- **Primary DNS Server:** Enter the primary IPv6 DNS server address.
- **Secondary DNS Server:** Enter the secondary IPv6 DNS server address.

LAN IPv6 Address Settings

- **LAN IPv6 Address:** Enter the LAN IPv6 address.
- **LAN IPv6 Link-local Address:** This field displays the LAN IPv6 link-local address.

Address Auto-configuration Settings

- **Enable automatic IPv6 address assignment:** Tick the check box to enable automatic IPv6 address assignment.
- **Auto-configuration Type:** The available IPv6 auto configuration types are SLAAC+RDNSS, SLAAC+Stateless DHCP, and Stateful DHCPv6.
- **Router Advertisement Lifetime:** Displays the router advertisement lifetime in minutes. This field appears when SLAAC+RDNSS or SLAAC+Stateless DHCP is selected.
- **IPv6 Address Range (Start):** Enter the start IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Range (End):** Enter the end IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Lifetime:** Displays the IPv6 address lifetime in minute. This field appears when Stateful DHCPv6 is selected.

6rd

WAN IPv6 Address Settings

- **Enable Hub and Spoke Mode:** Tick the check box to enable the hub and spoke mode.

- **6rd Configuration:** Select the 6rd configuration option. Options to choose from are 6rd DHCPv4 option and Manual Configuration.
- **6rd IPv6 Prefix:** Enter the 6rd IPv6 address and prefix value.
- **IPv4 Address Mask Length:** Enter the IPv4 mask length.
- **Assigned IPv6 Prefix:** Displays the IPv6 prefix.
- **6rd Border Relay IPv4 Address:** Enter the 6rd border relay IPv4 address.
- **Primary DNS Server:** Enter the primary IPv6 DNS server address.
- **Secondary DNS Server:** Enter the secondary IPv6 DNS server address.

LAN IPv6 Address Settings

- **LAN IPv6 Address:** This field displays the LAN IPv6 address.
- **LAN IPv6 Link-local Address:** This field displays the LAN IPv6 link-local address.
- **Address Auto-configuration Settings**
- **Enable automatic IPv6 address assignment:** Tick the check box to enable automatic IPv6 address assignment.
- **Auto-configuration Type:** The available IPv6 auto configuration types are SLAAC+RDNSS, SLAAC+Stateless DHCP, and Stateful DHCPv6.
- **Router Advertisement Lifetime:** Displays the router advertisement lifetime in minutes. This field appears when SLAAC+RDNSS or SLAAC+Stateless DHCP is selected.
- **IPv6 Address Range (Start):** Enter the start IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Range (End):** Enter the end IPv6 address in the range. This field is only available when Stateful DHCPv6 is selected.
- **IPv6 Address Lifetime:** Displays the IPv6 address lifetime in minute. This field appears when Stateful DHCPv6 is selected.

Link-local Only

LAN IPv6 Address Settings

- **LAN IPv6 Link-local Address:** This field displays the LAN IPv6 link-local address.

Change your router IP address

Main > LAN & DHCP Server

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 **Main**, and click on **LAN** to enter the LAN setting section.
3. Under Router Settings, enter the router IP address you would like to assign. .

Router Settings	
Use this section to configure the internal network settings of your router. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address here, you may need to adjust your PC's network settings to access the network again.	
Router IP Address	<input type="text" value="192.168.10.1"/>
Default Subnet Mask	<input type="text" value="255.255.255.0"/>
Host Name	<input type="text" value="tew-733gr"/>
Local Domain Name	<input type="text"/> (optional)
Enable DNS Relay	<input checked="" type="checkbox"/>

- **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)

- **Host Name:** Enter the host name you of your router
- **Local Domain Name:** Enter the domain name to assign to the router
- **DNS Relay:** Select this option to transfer the DNS server information from your ISP to your computer. If selected, your computer uses the router for a DNS server.

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 **Save Settings**.

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

Main > LAN & DHCP Server

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 **Main**, and click on **LAN**.
3. Review the DHCP Server settings.

DHCP Server Settings	
Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.	
Enable DHCP Server	<input checked="" type="checkbox"/>
DHCP IP Address Range	100 to 199 (addresses within the LAN subnet.)
DHCP Lease Time	10080 (minutes)
Always broadcast	<input checked="" type="checkbox"/> (Compatibility for some DHCP clients.)

- **DHCP Server:** Enable or Disable the DHCP server.
 - **DHCP IP Address Range:** Enter the start and end for the DHCP server range.
Note: The Start IP and End IP specify the range of IP addresses to automatically assign to computers or devices on your network.
 - **Lease Time:** Enter the DHCP lease time in minutes.
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 **Save Settings**.

Dynamic DHCP List – You can view the list of active lease entries for computers or devices that have been assigned IP addresses automatically from the DHCP server on your router.

Number of Dynamic DHCP Clients			
Host Name	IP Address	MAC Address	Expired Time
PM	192.168.10.100	00:26:2d:5b:46:53	6 Days 23 Hours 37 Minutes

Set up DHCP reservation

Main > LAN

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 34) or special applications (also called port triggering, see [“Special Applications”](#) on page 36).

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



Add DHCP Reservation	
Enable	<input type="checkbox"/>
Computer Name	<input type="text"/> << Computer Nam ▾
IP Address	<input type="text"/>
MAC Address	<input type="text"/>
Clone Your PC's MAC Address	<input type="text"/> Clone Your PC's MAC Address
<input type="button" value="Add / Update"/> <input type="button" value="Clear"/>	

- **Check box:** Check the box to enable rule.
- **Name:** Enter a name for the reservation.
- **Static DHCP:** Enable or Disable the DHCP reservation feature.
- **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) or click

Clone Your PC's MAC Address to automatically copy your computer's MAC address.

- **Add/Update:** Saves the reservation.

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

DHCP Reservations List					
Enable	Host Name	IP Address	MAC Address		
<input checked="" type="checkbox"/>	TRENDnet	192.168.10.100	00:26:2d:5b:46:53		

Enable/disable UPnP on your router

Management > Remote Management

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.) UPnP is enabled on your router by default to allow specific applications required by your computers or devices to allow connections through your router as they are needed.

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

UPNP	
Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.	
Enable UPnP	<input checked="" type="checkbox"/>

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 **Save Settings**.

Allow/deny VPN connections through your router

Management > Remote Management

A Virtual Private Network (VPN) is a network that uses a public network, such as the Internet, to provide secure communications between a remote computer or network and another network. Some offices often provide VPN access to their networks to enable employees to work from their remote office/home office, or while traveling.

If your office or place of work has allowed and authorized access for you to access their network through VPN, the default VPN settings in your router have been configured to pass through the most common types of VPN protocols, which typically do not require any additional configuration changes.

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

Application Level Gateway (ALG) Configuration	
PPTP	<input checked="" type="checkbox"/>
IPSec (VPN)	<input checked="" type="checkbox"/>
RTSP	<input checked="" type="checkbox"/>
SIP	<input checked="" type="checkbox"/>

3. Next to **PPTP**, **L2TP**, or **IPsec** (depending the VPN protocol your corporation requires) click **Enabled** or **Disabled** to turn the VPN pass through feature on or off on your router.

Note: It is recommended to leave these settings enabled.

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

Allow/deny multicast streaming

Management > Remote Management

In some cases, applications require multicast communication (also called IP multicast which is the delivery of information to a specific group of computers or devices in a single transmission) typically used in media streaming applications. Multicast streaming

is enabled by default on your router to allow applications that require multicast communication through your router which typically does not require additional configuration changes.

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Access**, and click on **Advanced Network**. View the options and click **Save Setting** to apply changes.

IPv4 Multicast Streams	
Enable IPv4 Multicast Streams	<input type="checkbox"/>
Wireless Enhanced Mode	<input type="checkbox"/>

- **Enable IPv4 Multicast Streams:** Click box to enable the IPv4 multicast streams feature. This feature will allow multicast traffic to pass through the router from the Internet (IPv4).
- **Wireless Enhanced Mode:** Click box to enable wireless enhanced mode.

Enable SPI

Access> Firewall & DMZ

Stateful Packet Inspection (SPI, is known as dynamic packet filtering, helps to prevent cyber-attacks. It validates that the traffic passing through the session conforms to the protocol.

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Access**, and click on **Firewall & DMZ**. Click box next to **Enable SPI**.

Firewall Settings	
Enable SPI	<input type="checkbox"/>

Identify your network on the Internet

Main > 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 **Server Address**. (e.g. *dyndns.com*, *no-ip.com*, etc.)
2. Log into your router management page (see "[Access your router management page](#)" on page 22).
3. Click on **Main** and click on **Dynamic DNS**. View the options and click **Save Setting** to apply changes.

Dynamic DNS Settings	
Enable Dynamic DNS	<input type="checkbox"/>
Server Address	DynDns.org(Custom) ▾
Host Name	<input type="text"/>
Username or Key	<input type="text"/>
Password or Key	<input type="password"/>
Verify Password or Key	<input type="password"/>
Timeout	567 (hours)
Status	Disconnected

4. Next to DDNS, click **Enabled**.
5. In the **Server Address** 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.
- **Timeout:** Enter the time duration of the Dynamic DNS feature.
- **Status:** Display the current status of the router's Dynamic DNS

Set your router date and time

Main > Time

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

Time and Date Configuration					
Time	2000/01/02 00:16:57				
Time Zone	(GMT-08:00) Pacific Time (US & Canada, Tijuana)				
Enable Daylight Saving	<input type="checkbox"/>				
Daylight Saving Offset	+01:00				
Daylight Saving Dates		Month	Week	Day of Week	Time
DST Start		Jan	1st	Sun	12:00 AM
DST End		Jan	1st	Sun	12:00 AM
Automatic Time and Date Configuration					
<input checked="" type="checkbox"/> Automatically synchronize with Internet time server.					
NTP Server Used	3.us.pool.ntp.org		Update Now		
Set the Time and Date manually.					
Year	2013	Month	Jan	Day	2
Hour	0	Minute	16	Second	57
Synchronize with your computer's time settings.					

3. Next to **Time Zone**, click the drop-down list to select your **Time Zone**. Click **Save Settings** to apply changes.

4. Check the **Enable Daylight Saving** box to enable daylight savings options. You will then need to configure the daylight savings start and end date/time.

5. Select which option you would like to apply for time settings.

- **Automatic:** Click the box to enter the NTP server to use.

OR

- **Manual:** Manually enter the date and time settings you would like to apply to the router.

Automatic Time and Date Configuration					
<input checked="" type="checkbox"/> Automatically synchronize with Internet time server.					
NTP Server Used	3.us.pool.ntp.org		Update Now		
Set the Time and Date manually.					
Year	2013	Month	Jan	Day	2
Hour	0	Minute	16	Second	57
Synchronize with your computer's time settings.					

Create schedules

Advanced > Schedule

For additional security control, your router allows you to create schedules to specify a time period when a feature on your router should be activated and deactivated. Before you use the scheduling feature on your router, ensure that your router system time is configured correctly.

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Tools** and click on **Schedule**.
3. Review the Schedule settings. Click **Add** to save settings.

10 -- Add Schedule Rule	
Name	<input type="text"/>
Day(s)	<input type="radio"/> All Week <input type="radio"/> Select Day(s)
Select Day(s)	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat
All Day - 24 Hours	<input type="checkbox"/>
Time Format	12-hour ▼
Start Time	12 : 0 AM ▼ (hour:minute)
End Time	11 : 59 PM ▼ (hour:minute)

- **Name:** Enter the name for the time and date schedule.
- **Days(s):** Click the All Week radio button to use all the weekdays for this schedule. Click the Select Day(s) radio button to use only the selected days in the week.
- **Select Day(s):** When the Select Day(s) radio button is selected, tick the check box to select which day of the week to be used.
- **All Day – 24 hrs:** Select this option use all the hours in a day.
- **Time Format:** Select the time format. Options to choose from are 12-hour and 24-hour.
- **Start Time:** Enter the starting time of a day when the schedule to begin.
- **End Time:** Enter the ending time of a day when the schedule will end.

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

Access > 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 34) 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 29).
 - 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 **Access**, and click on **Firewall & DMZ**.

DMZ Host	
<p>The DMZ (Demilitarized Zone) option allows a single computer on your local network to be accessible from the WAN side of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer's IP address into the DMZ for unrestricted Internet access.</p> <p>Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.</p>	
Enable DMZ	<input type="checkbox"/>
DMZ IP Address	<input type="text"/> << Computer Name ▼

4. Next to **DMZ Enable**, click **Enabled**.
5. Next to **DMZ Host IP**, enter the IP address you assigned to the computer or network device to expose to the Internet.
6. To save changes, click **Save Settings**.

Virtual Server

Access > 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 33) 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 **Access**, and click on **Virtual Server**.

3. Review the virtual server settings.

- **Enabled:** Check the box to enable rule.
- **Name:** Enter a name for the virtual server.
- **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.

- **Public Port:** Enter the port number used to access the device from the Internet.
Note: The **Public 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.
- **Private Port:** Enter the port number required by your device. Refer to the connecting device's documentation for reference to the network port(s) required.
- **Protocol:** Select the protocol required for your device. **TCP**, **UDP**, or you can select **Both** to choose both TCP & UDP (recommended).
Note: Please refer to the device documentation to determine which ports and protocols are required.
- **Schedule:** Select Always to have rules always on or select schedule on the pull down list.
- **Inbound Filter:** Select Allow All to have rule allows or select an inbound filter on the pull down list.

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 29).
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 **Access**, and click on **Virtual Server**.

Name TRENDnet Cam <<	Public Port 80	Protocol Both ▾	Schedule Always ▾
Application Name ▾			
<input checked="" type="checkbox"/> IP Address 192.168.10.30 <<	Private Port 80	Inbound Filter Allow All ▾	
Computer Name ▾			

- Click box to enable rule.
- Next to **Name**, you can enter another name for the virtual server.
- Next to **IP Address**, enter the IP address assigned to the camera. (e.g. 192.168.10.30)
- The **Private Port** and **Public Port**, make sure port number **80** is configured for both settings.
- Next to **Schedule**, select Always to have rule always on.
- Next to **Inbound Filter**, select Allow All.
- To save the changes, click **Save Settings**.

Port Forwarding

Access > Virtual Server

Port forwarding allows you to define a specific port or a range of 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 33) 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).

- Log into your router management page (see "[Access your router management page](#)" on page 22).
- Click on **Access**, and click on **Virtual Server**.

24 -- Port Forwarding Rules				
Remaining number of rules that can be created.: 24				
			Ports to Open	
<input type="checkbox"/>	Name Application Name ▾	Public Port ~	Traffic Type All ▾	
<input type="checkbox"/>	IP Address Computer Name ▾	Private Port ~	Schedule Always ▾	
<input type="checkbox"/>	Name Application Name ▾	Public Port ~	Traffic Type All ▾	
<input type="checkbox"/>	IP Address Computer Name ▾	Private Port ~	Schedule Always ▾	

- Review the Port Forwarding Rules settings.

- **Enabled:** Check the box to enable rule.
- **Name:** Enter a name for the port forwarding rule.
- **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.

- **Public Port:** Enter the port or range of ports used to access the device from the Internet.
Note: The **Public 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.
- **Private Port:** Enter the port or range of ports required by your device. Refer to the connecting device's documentation for reference to the network port(s) required.
- **Protocol:** Select the protocol required for your device. **TCP**, **UDP**, or you can select **Both** to choose both TCP & UDP (recommended).

Application Rules

Access > Application Rules

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 30.

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 **Access**, and click on **Special AP**.

24 -- Application Rules					
Remaining number of rules that can be created.: 24					
			Port	Traffic Type	Schedule
<input type="checkbox"/>	Name <input type="text"/>	Application Application Name	Trigger <input type="text"/>	Protocol All	Schedule Always
<input type="checkbox"/>	Name <input type="text"/>	Application Application Name	Firewall <input type="text"/>	Protocol All	Schedule Always
<input type="checkbox"/>	Name <input type="text"/>	Application Application Name	Trigger <input type="text"/>	Protocol All	Schedule Always
<input type="checkbox"/>	Name <input type="text"/>	Application Application Name	Firewall <input type="text"/>	Protocol All	Schedule Always

3. Review the special application settings.
 - **Enabled:** Check the box to enable rule.
 - **Name:** Enter a name for the application rule.

- **Trigger Port:** Enter the port number used to trigger the application rule.
- **Protocol:** Select the protocol required for your device. **TCP**, **UDP**, or you can select **Both** to choose both TCP & UDP (recommended).

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

- **Schedule:** Select Always to have rules always on or select schedule on the pull down list.

Allow remote access to your router management page

Main > Password

You may want to make changes to your router from a remote location such as 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 **Main**, and click on **Password**.

Administration	
Enable Remote Management	<input type="checkbox"/>
Remote Admin Port	8080
Remote Admin	Inbound Filter
	Allow All
Details	Allow All

3. Under the **Enable Remote Management** section, click the box to enable setting.
 - **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)
 - **Remote Admin:** Verify if that there are no Inbound Filter rules that would prevent your remote access.
4. To save changes, click **Save Settings**.

Internet Bandwidth Control

Access > Internet Bandwidth Control

You may want to prioritize traffic for specific computers or devices on your network to have higher priority. QoS involves prioritization of network traffic. QoS can be targeted at a network interface, toward a given server or router's performance, or in terms of specific applications.

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Access**, and click on **Internet Bandwidth Control**.
3. Review the Internet Bandwidth Control settings. Click **Save Settings** to apply changes.

Internet Bandwidth Control	
Enable Internet Bandwidth Control :	<input type="checkbox"/>
Uplink Speed :	2048 kbps << Select Transmission Rate
Downlink Speed :	8192 kbps << Select Transmission Rate

- **Enable:** Enable or Disable the Internet Bandwidth Control through the router.
- **Uplink Speed:** Enter the uplink speed value or select a predefined uplink speed option from the drop-down menu.
- **Download Speed:** Enter the download speed value or select a predefined download speed option from the drop-down menu.

Add static routes to your router

Routing > Static

You may want set up your router to route computers or devices on your network to other local networks through other routers. Generally, different networks can be determined by the IP addressing assigned to those networks. Generally speaking and for the case of an example, your network may have 192.168.10.x IP addressing and another network may have 192.168.20.x IP addressing and because the IP addressing of these two networks are different, they are separate networks. In order to communicate

between the two separate networks, static routing needs to be configured. Below is an example diagram where routing is needed for devices and computers on your network to access the other network.

Note: Configuring this feature assumes that you have some general networking knowledge.

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

32 -- Route List			
Remaining number of rules that can be created.: 32			
		Metric	Interface
<input type="checkbox"/>	Name <input type="text"/>	Destination IP Address <input type="text"/>	1 WAN (192.168.10.12 ▾)
	Netmask <input type="text"/>	Gateway <input type="text"/>	
<input type="checkbox"/>	Name <input type="text"/>	Destination IP Address <input type="text"/>	1 WAN (192.168.10.12 ▾)
	Netmask <input type="text"/>	Gateway <input type="text"/>	

3. Review the static route settings. Click **Save Settings** to apply rule.

- **Enabled:** Check the box to enable rule.
- **Name:** Enter a name for the routing rule.
- **Destination IP Address:** Enter the IP network address of the destination network for the route.
(e.g. 192.168.20.0)
- **Network Mask:** Enter the subnet mask of the destination network for the route.
(e.g. 255.255.255.0)
- **Gateway Address:** Enter the gateway to the destination network for the route.
(e.g. 192.168.10.2)
- **Metric** – Enter the metric or priority of the route. The metric range is 1-16, the lowest number 1 being the highest priority. (e.g. 1)
- **Interface** – Click the drop-down list and select the Interface on your router where the route is active.
(e.g. LAN)

Router Maintenance & Monitoring

Reset your router to factory defaults

Tools > Restart

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 39.

There are two methods that can be used to reset your router to factory defaults.

- **Reset Button** – Located on the rear panel of your router, see "[Product Hardware Features](#)" on page 5. Use this method if you are encountering difficulties with accessing your router management page.

OR

- **Router Management Page**

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Tools** and click on **Restart**.
3. Under **Restore factory default settings**, click **Restore Factory Defaults**. When prompted to confirm this action, click **OK**.

Restore To Factory Default Settings

Restore Factory Defaults

Router Default Settings

Administrator User Name	admin
Administrator Password	Note: Please refer to the wireless sticker placed on the side of the unit or the device label
Router IP Address	192.168.10.1
Router Subnet Mask	255.255.255.0
DHCP Server IP Range	192.168.10.101-192.168.10.199
Wireless	Enabled
SSID (wireless network name)	For added security the default SSID is preconfigured with randomized characters. Note: Please refer to the wireless sticker placed on the side of the unit or the device label under the unit for the default wireless information.
Wireless Security	For added security the wireless security is enabled with randomizes characters. Note: Please refer to the wireless sticker placed on the side of the unit or the device label under the unit device label for the default wireless security key
802.11 Mode	2.4GHz 802.11b/g/n mixed mode
Channel	Auto Channel

Note: Basic login information can be found on the wireless sticker and also the device label, located on the bottom of your router.

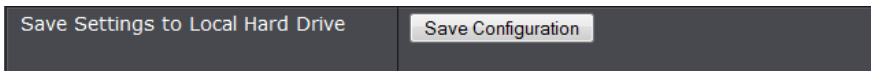
Backup and restore your router configuration settings

Tools > Restart

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 backup your router configuration:

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Tools** and click on **Restart**.
3. Under **Save Settings to Local Hard Drive** click to **Save Configuration**, 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 **Tools** and click on **Restart**.
3. Under **Load Settings From Local Hard Drive**, click on **Browse** or **Choose File**.



4. A separate file navigation window should open. Select the router configuration file to restore and click **Load**. (Default Filename: *cfg.bin*). If prompted, click **Yes** or **OK**.
5. Wait for the router to restore settings.

Upgrade your router firmware

Tools > Firmware

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).

- Click on **Tools** and click on **Firmware** to check your router's current firmware version at the top of the page.

Firmware Information	
Current Firmware Version	1.00
Current Firmware Time	04/24/2013 15:38:00

- Depending on your web browser, next to **Upload**, click **Browse** or **Choose File**.

Firmware Upgrade	
Note: Some firmware upgrades will reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration.	
To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file and click on the Upload button.	
Upload	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>

- Navigate to the folder on your computer where the unzipped firmware file (.bin) is located and select it.
- Click **Upload**. If prompted, click **Yes** or **OK**.

Restart your router

Tools > 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 5.

Note: 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

- Router Management Page** – This is also known as a soft reboot or restart.

- Log into your router management page (see "[Access your router management page](#)" on page 22).
- Click on **Tools** and click on **Reboot the Device**. Next to Reboot The Device section, click **Yes** or **OK**.

Reboot The Device	<input type="button" value="Reboot the Device"/>
-------------------	--

Check connectivity using the router management page

Tools > Ping Test

For troubleshooting purposes, you may want to check your router connectivity using the ping (also known as a network connectivity test) test tool on your router management page.

- Log into your router management page (see "[Access your router management page](#)" on page 22).
- Click on **Tools** and click on **Ping Test**.
- Enter in the IP address (e.g. 192.168.10.101) or host name (e.g. www.trendnet.com) to test.
- Click **Ping**.

Ping Test	
Host Name or IP Address	<input type="text"/> <input type="button" value="Ping"/>
IPv6 Ping Test	
Host Name or IPv6 Address	<input type="text"/> <input type="button" value="Ping"/>

- You will receive a *success* or *fail* result message of the address you entered providing a basic indicating of the router's connectivity to the Internet or devices that are connected to your network. Click **Back** to bring you back to the **Ping Test** page.

Ping Result

trendnet.com is alive!

Check the router system information*Status > Device Information*

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.

General

General	
Time	2000/01/02 02:15:28
System Up Time	1 Day 2 Hour 15 Min 29 Sec
Firmware Version	1.00 Wed 24 Apr 2013

- **Time:** The current time of your router.
- **System Up Time:** The duration your router has been running continuously without a restart/power cycle (hard or soft reboot) or reset.
- **Firmware Version:** The current firmware version of your router.

WAN (Internet) Information

WAN	
Connection Type	DHCP Client
Cable Status	Connected
Network Status	Connected
	<input type="button" value="Renew"/> <input type="button" value="Release"/>
Connection Up Time	1 Day 2 Hour 12 Min 46 Sec
MAC Address	5c:33:8e:63:f4:5f
IP Address	192.168.10.126
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
Primary DNS Server	192.168.10.1
Secondary DNS Server	0.0.0.0

- **Connection Type:** The WAN/Internet connection type your router is using.
- **Cable Status:** The status of your network cable on your Internet/WAN port.
- **Network Status:** Displays the current WAN (Internet) connection status. When using DHCP Client (or Dynamic IP address) Internet connection type, you will provide the option to Release and Renew your IP address settings.

Note: Other Internet connection types such as PPPoE will provide the option to Connect and Disconnect.

- **Connection Up Time:** Display the duration of your router's Internet connection.
- **MAC Address:** The current MAC address used by your router's WAN port or interface configuration.
- **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.
- **Default 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.

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.

LAN	
MAC Address	5c:33:8e:63:f4:5e
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled

Wireless Information

Wireless LAN	
Wireless Radio	Enabled
MAC Address	5c:33:8e:63:f4:5e
802.11 Mode	Mixed 802.11n, 802.11g and 802.11b
Channel Width	20MHz
Channel	9
Network Name (SSID)	mediatest_TRENDnet
Wi-Fi Protected Setup	Enabled/Configured
Security	WPA2-PSK
Guest Zone Wireless Radio	Disabled
Guest Zone Network Name (SSID)	TRENDnet733_2.4GHz_guest
Guest Zone Security	WPA2-PSK

- **Wireless Radio:** The status of your wireless radio.
- **MAC Address:** The current MAC address of your router's wireless or interface configuration.
- **802.11 Mode:** Displays the 802.11 mode of your router.
- **Channel Bandwidth:** Displays the channel bandwidth of your router.
- **Channel:** Displays the channel of your router is operating in.
- **Network Name (SSID):** Your router's wireless network name or SSID.
- **Wi-Fi Protected Setup:** The status of your router's Wi-Fi Protected Setup (WPS).
- **Security:** The wireless security type applied to your router.
- **Guest Zone Wireless Radio:** Displays the status of the router's guest network.
- **Guest Zone Wireless Radio:** Displays the status of the router's guest network.
- **Guest Zone Network Name:** Displays your router's guest network's name.
- **Guest Zone Security:** Displays the security type of your wireless guest network.

View your router log

Status > Log

Your router log can be used to obtain activity information on the functionality of your router or for troubleshooting purposes.

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Status** and click on **Log**.
3. Select the type of logs to display

Log Type & Level	
Log Type	<input checked="" type="radio"/> System <input type="radio"/> Firewall & Security <input type="radio"/> Router Status
Log Level	<input type="radio"/> Critical <input type="radio"/> Warning <input checked="" type="radio"/> Information

4. Review the device log information.

Time	Message
Sun Jan 2 02:13:55 2000	Got new client [54:26:96:52:E1:A6] associated from BAND24G-1.1 (2.4 Ghz)
Sun Jan 2 02:13:55 2000	DHCP: Server sending ACK to 192.168.1.102. (Lease time = 604800)
Sun Jan 2 02:13:55 2000	DHCP: Server receive REQUEST from 54:26:96:52:e1:a6.
Sun Jan 2 02:09:24 2000	Web login success from 192.168.1.101

- **Time:** Displays the time of the log entry. If the time is inaccurate, make sure to set the router date and time correctly.
- **Message** – Displays the log message.

Router Log Navigation

- **First Page:** Displays the first page of the log.
- **Last Page:** Displays the last page of the log.
- **Previous Page:** Display the log page previous to the current.
- **Next Page:** Displays the log page next to the current.
- **Clear Log:-** Clears all logging

5. To save current logs to a local hard drive, click **Save**.

Send router logs to your email

Tools > Email Setting

You may want send your router log to your e-mail address or to an external log server (also known as Syslog server) so you can check it periodically while away from home. You may also want to only see specific categories of logging.

Send router logs to your e-mail address

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Status** and click on **Log Setting**.
3. Click box next to **Enable Email Notification**.

4. Review the e-mail log settings.

- **From Email Address:** Enter a sender e-mail address. (e.g. router@trendnet.com)
Note: This does not need to be real e-mail address, only used for identification purposes when checking your e-mail.
- **To Email Address:** Enter your e-mail address.
- **Email Subject:** Enter the subject of the email logs.
- **SMTP Server:** Enter the IP address (e.g. 10.10.10.10) or domain name (e.g. mail.trendnet.com) of your e-mail server.
- **SMTP Server Port:** Enter the port used by your e-mail service. (e.g. Default SMTP Server Port: 25)
- **SMTP Authentication** – Set this option to **Enabled** if your e-mail service requires authentication. If not, leave this setting to **Disabled**.
Note: If you are unsure of this setting check with your e-mail service provider if authentication is required.
- **Account:** Enter your account user name for your e-mail service.
- **Password:** Enter your password for your e-mail service.
- **Send Mail Now:** Click this option to send an e-mail with the current router log using your email settings.

- **When log is full:** The router log will be e-mailed to your e-mail address when router internal log is full.

Email Log When Full	
Enable Log When Full :	<input type="checkbox"/>

Setup a syslog server from router

Tools > Syslog

You may want send your router log to a syslog server.

Note: To use this feature you must have a syslog server software properly installed on your computer that will assigned as the syslog server.

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Tools** and click on **Syslog**.

Syslog Settings	
Enable Logging to SysLog Server	<input checked="" type="checkbox"/>
Syslog Server IP Address	<input type="text"/> << Computer Name ▼

3. Click box next to **Enable Logging to Syslog Server**.
4. Enter the IP address of the computer you want to assign as your syslog server. You can also select your computer from the drop down list.

Email Settings	
From Email Address	<input type="text"/>
To Email Address	<input type="text"/>
Email Subject	<input type="text"/>
SMTP Server Address	<input type="text"/>
SMTP Server Port	25 <input type="text"/>
Enable Authentication	<input type="checkbox"/>
Account Name	<input type="text"/>
Password	<input type="text"/>
Verify Password	<input type="text"/> <input type="button" value="Send Mail Now"/>

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 LAN (wired), WAN (Internet), Wireless.

LAN Statistics			
Sent	519527	Received	511228
TX Packets Dropped	0	RX Packets Dropped	0
Collisions	0	Errors	0
WAN Statistics			
Sent	259962	Received	342793
TX Packets Dropped	0	RX Packets Dropped	0
Collisions	0	Errors	0
Wireless Statistics - 2.4GHz Band			
Sent	163531	Received	230940
TX Packets Dropped	0	RX Packets Dropped	0
Collisions	0	Errors	82

- **Refresh Statistics:** Click to refresh the list.
- **Reset Statistics:** Click to clear the current list.

View your router active sessions

Status > Active Session

You may want to check for any active session on your router for trouble shooting purposes.

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Status** and click on **Active Session**.
3. The table displays the amount of current active session on your router.

NAPT Sessions		
TCP Sessions : 11		
UDP Sessions : 2		
Total : 13		
NAPT Active Sessions		
IP Address	TCP Sessions	UDP Sessions
192.168.1.1	0	1
192.168.1.105	1	0
192.168.1.104	3	0
192.168.1.101	7	1

- **Refresh:** Click to refresh the list.

View your routing table

Status > Active Session

You may want to check for any active routes through your router for trouble shooting purposes.

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Routing** and click on **Routing Table**.
3. The table displays the amount of current active session on your router.

Routing Table					
Destination	Gateway	Netmask	Metric	Iface	Creator
192.168.1.0	0.0.0.0	255.255.255.0	0	LAN	SYSTEM
192.168.10.0	0.0.0.0	255.255.255.0	0	INTERNET	SYSTEM
239.0.0.0	0.0.0.0	255.0.0.0	0	LAN	SYSTEM
0.0.0.0	192.168.10.1	255.255.255.255	100	INTERNET	SYSTEM

View devices connected to your router

Status > Device Information

You may want to check all the devices connected to 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 Information**.
3. The table displays all devices connected to your router.

Lan Computers		
MAC Address	IP Address	Name (if any)
00:26:2d:5b:46:53	192.168.1.101	PM
28:0d:fc:3d:25:ea	192.168.1.102	(unknown)
7c:ed:8d:af:1a:06	192.168.1.103	(unknown)
b8:17:c2:b3:b8:91	192.168.1.105	Apple-TV
00:90:a9:c4:17:2f	192.168.1.107	WDTVLIVE

View wireless devices connected to your router

Status > Wireless

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 22).
2. Click on **Status** and click on **Wireless**.
3. The table displays the all wireless clients connected to your router.

Number Of Wireless Clients - 2.4GHz Band : 5					
MAC Address	IP Address	Mode	Rate (Mbps)	Signal (%)	
28:0D:FC:3D:25:EA	192.168.1.102	11g	54	100	
7C:ED:8D:AF:1A:06	192.168.1.103	11n	65	100	
B8:17:C2:B3:B8:91	192.168.1.105	11n	65	100	
00:90:A9:C4:17:2F		11n	130.0	100	
54:26:96:52:E1:A6	192.168.1.104	11n	65	100	

View your router's IPv6 network information

Status > IPv6

You may want to check your router's IPv6 status.

1. Log into your router management page (see "[Access your router management page](#)" on page 22).
2. Click on **Status** and click on **IPv6**.
3. The table displays your router's IPv6 settings and IPv6 clients connected to your router.

IPv6 Connection Information	
IPv6 Connection Type	Link-Local
IPv6 Default Gateway	None
LAN IPv6 Link-Local Address	fe80::5e33:8eff:fe63:f45e /64
LAN IPv6 Computers	
IPv6 Address	Name (if any)
fe80::ba17:c2ff:feb3:b891	Apple-TV
fe80::5626:96ff:fe52:e1a6	DeL-Iphone

Router Management Page Structure

Main

- Setup Wizard
- LAN
 - DHCP Server
 - DHCP Reservation
- WAN
 - Clone MAC Address
- Password
 - Remote Admin
- Time
- Dynamic DNS
- IPv6

Wireless

- Basic
 - Wireless Security
- Advanced
- Wi-Fi Protected Setup

Status

- Device Information
- Log
- Log Setting
- Statistic
- Wireless
- IPv6

Routing

- Static
- Routing Table

Access

- MAC Filter
- Protocol/ IP Filters
- Virtual Server
- Firewall & DMZ
 - SPI
- Port Forwarding
- Application Rules
- Internet Bandwidth Control
- Guest Zone
- Advanced Network
 - UPnP
 - WAN Port Speed
- Guest Zone
- Parental Control
 - URL Filter

Tools

- Restart
 - Save Configuration Settings
 - Restore Configuration Settings
 - Reset to Factory Default
 - Reboot
- Firmware
 - Upgrade Firmware

- Ping Test
- Email Settings
 - Email Log
- Syslog
- Schedules

Technical Specifications

Hardware	
Standards	Wired: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), Wireless: IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
Internet Protocol	IPv4 and IPv6
LAN	4 x 10/100/1000 Mbps Auto-MDIX
WAN	1 x 10/100/1000 Mbps Auto-MDIX
WPS Button	Wi-Fi Protected Setup (WPS) connects with other WPS compliant devices
Reset Button	Reset unit back to factory default (press and hold for 10 seconds)
Network Protocols / Features	Static and dynamic routing, UPnP, DHCP, server, Dynamic DNS (DynDNS.com), NTP, IPsec / PPTP / L2TP VPN pass through, IPv6
Quality of Service	Internet bandwidth control
Internet Connection Type	IPv6, Dynamic IP, Static (fixed) IP, PPPoE, PPTP, L2TP
Firewall	NAT, SPI, DMZ host, virtual servers, MAC / IP filters and URL filter
Management / Monitoring	Local / remote configuration, upgrade firmware, backup / restore configuration via web browser, internal system log, ping test tool
Supported Web Browser	Internet Explorer 6.0 or above, Firefox 2.0 or above, Chrome, Opera, Safari
LED Indicator	WPS, Wireless, LAN 1-4, WAN (Internet), Power
Power Adapter	Input: 100 ~ 240 V, 50~60 Hz, 0.4 A Output: 12 V DC, 1 A external power adapter
Power Consumption	10 watts (max.)

Dimension (L x W x H)	45 x 118 x 164 mm (1.8 x 4.6 x 6.5 in)
Weight	244 g (8.6 oz)
Temperature	Operation: 0°~ 40°C (32°F~ 104°F) Storage: -20°~ 60°C (-4°F~140 °F)
Humidity	Max. 95% (non-condensing)
Certifications	CE, FCC
Wireless	
Frequency	2.4 GHz: 2.4 ~2.48
Modulation	CCK, DQPSK, DBPSK, OFDM, BPSK, QPSK, 16/64/256-QAM
Data Rate	802.11b: up to 11 Mbps 802.11g: up to 54 Mbps 802.11n: up to 300 Mbps
Security	64/128-bit WEP, WPA/WPA2-PSK, WPA/WPA2-RADIUS
Guest network	1 per wireless band
Access Control	MAC Address Filter (Up to 24 entries)
Output Power	802.11b: 19 dBm (typical) 802.11g: 15 dBm (typical) 802.11n: 18 dBm (typical)
Receiving Sensitivity	802.11b: -76 dBm (typical) @ 11 Mbps 802.11g: -65 dBm (typical) @ 54 Mbps 802.11n: -79 dBm (typical) @ 300 Mbps
Channels	2.4 GHz: 1~11 (FCC), 1~13 (ETSI)

*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 8.
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 5 seconds, the release.

Windows 7

- 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 19 if you continue to have wireless connectivity problem

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

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 10.6/10.5

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

- 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 10.4/10.5/10.6

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

In MAC 10.6, from the **Configure** 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

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 10.4

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.



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.


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

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 device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

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

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

Radiation Exposure Statement:

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

RoHS

This product is RoHS compliant.

**Europe – EU Declaration of Conformity**

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



Limited Warranty

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

TEW-733GR – 3 Years Warranty

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

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

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

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

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

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

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

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

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

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

PWP05202009v2

2013/09/12



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