User's Guide

TRENDnet®

AC750 Dual Band Wireless Router

TEW-810DR

Table of Contents

Table of Contents 2

Product Overview 4

Package Contents 4
Features 4
Product Hardware Features 5
Application Diagram 6

Router Setup 7

Creating a Home Network 7
Router Installation 8
Connect additional wired devices to your network 10

Wireless Networking and Security 11

How to choose the type of security for your wireless network 11
Secure your wireless network 12
Connect wireless devices to your router 13
Connect wireless devices using WPS 14

Basic 15

Access your router management page 15
Network Status 16
Wireless settings 17
Guest Network 18
Steps to improve wireless connectivity 19
Parental Control 19

Access Control Filters 20

Access control basics 20
Service and Port blocking 20
IP blocking 21
Website Filter 22
Inbound Filter 22

ADVANCED 23

Change your router IP address 23
Set up the DHCP server on your router 23
Set up DHCP reservation 24
Manually configure your Internet connection 25
Manually configure your DNS server setting 25
Manually configure your MTU setting 26
Clone a MAC address 26
Add static routes to your router 27
Enable RIP on your router 27
IPv6 Internet Connection Settings 28
Prioritize traffic using QoS (Quality of Service) 29
Advanced wireless settings 29
Multiple SSID 29
Wireless bridging using WDS (Wireless Distribution System) 30
Additional wireless settings 31
Wireless security (Wireless MAC filter) 33
Set your router date and time 33
Create schedules 34
Open a device on your network to the Internet 35
DMZ 35
Virtual Server 35
Special Applications 36
Gaming 37
Enable/disable Application Layer Gateways (ALG) 38
Enable/disable UPnP on your router 39

Router Maintenance & Monitoring 39

Change your router login password 39
Change your device name 40
Change your device URL 40
Identify your network on the Internet 41
Allow remote access to your router management page 42
Reset your router to factory defaults 42
Router Default Settings 43
Backup and restore your router configuration settings 43
Upgrade your router firmware 44
Reboot your router 45
Allow/deny ping requests to your router from the Internet 46
Check the router system information 46

Router Management Page Structure 50

Technical Specifications 51

Troubleshooting 53

Appendix 54

Product Overview

TEW-810DRU

Package Contents

In addition to your router, the package includes:

- CD-ROM (Utility and User's Guide)
- Multi-Language Quick Installation Guide
- Network cable Ethernet Cable (1.5m / 5ft.)
- Power Adapter (12V, 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

Designed to handle multiple HD streams in a busy connected home, TRENDnet's AC750 Dual Band Wireless Router, model TEW-810DR, creates two concurrent wireless networks—a high speed 433 Mbps Wireless AC network and a 300 Mbps Wireless N network to connect common wireless devices.

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

Encrypted Wireless

For your security the router arrives pre-encrypted with its own unique password

Guest Network

Create a secure, isolated network for guest internet access only

Parental Controls

Control access to specific websites or types of content

Performance

Next Generation Wireless AC

802.11ac provides uninterrupted HD video streaming in a busy connected home

Simultaneous Dual Band

High speed 433 Mbps Wireless AC band + 300 Mbps Wireless N

Ethernet Ports

Ethernet ports maintain high performance network connections

Backward Compatible

Compatible with Wireless N and older Wireless G devices

Energy Savings

Embedded GREENnet technology reduces power consumption by up to 50%

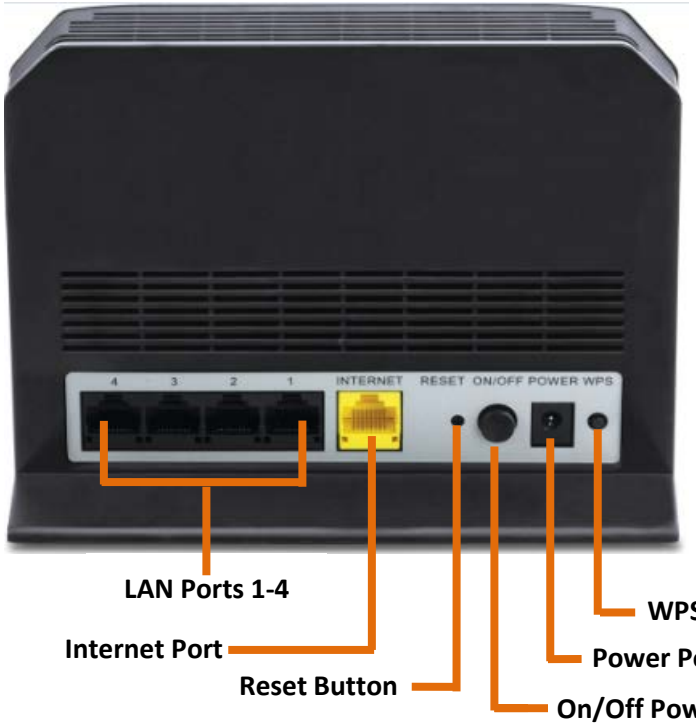
IPv6

IPv6 network support

*For maximum performance of up to 433 Mbps use with at least a 433 Mbps 802.11ac wireless adapter. 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



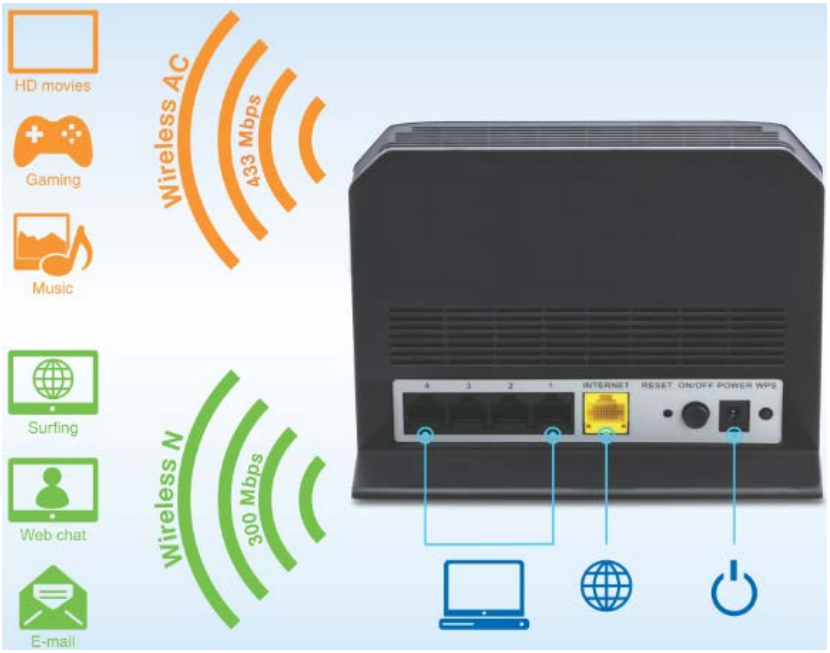
- **LAN Ports 1-4:** Connect Ethernet cables (also called network cables) from your router LAN ports to your wired network devices.
- **Internet Port:** Connect an Ethernet cable from your router Internet port to your modem.
- **Reset Button:** Press and hold this button for 10 seconds to reset the router.
- **On/Off Power Switch:** Push the router On/Off power switch to turn your router "On" (Inner position) or "Off" (Outer position).
- **Power Port:** Connect the included power adapter from your router power port and to an available power outlet.
- **WPS Button (Wi-Fi Protected Setup):** Push and hold this button for 5 seconds to activate WPS. The Power LED will blink when WPS is activated.

Front View

Power/WPS LED: The indicator is solid green when your router is powered on. Otherwise if this LED indicator is off, there is no power to your router. The indicator will also blink when WPS is activated. The LED will stop blinking and remain solid green automatically once WPS process is completed.

Internet Port (Link/Activity) LED – This LED indicator is solid green when your router Gigabit Internet port is physically connected to the modem network or Ethernet port with a network or Ethernet cable (modem turned on). The LED indicator will be blinking green while data is transmitted or received through the Gigabit Internet port of your router.

Application Diagram



The router is installed near the modem (typically supplied by your ISP "Internet Service Provider") and physically connected to it from the router's Internet port to the modem's network port which connects to the Internet. 2.4GHz wireless signals from the router are broadcasted to wireless clients such as laptops (with wireless capability) and the less congested 5GHz wireless signals from the router are broadcasted to other wireless client devices such as TVs, game consoles, or media bridges thereby providing Internet access for all wireless client devices.

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 security on your router, see "Wireless Networking and Security" on page 11.

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)
MAC Address: ___:___:___:___:___:___ Enter your PC's MAC address (Optional)
DNS Servers Address 1: _____. _____._____._____ (Optional)
DNS Servers Address 2: _____. _____._____._____ (Optional)

2. Static/Fixed IP address
MAC Address: ___:___:___:___:___:___ Enter your PC's MAC address (Optional)
IP Address: _____. _____._____._____ (e.g. 215.24.24.129)
Subnet Mask: _____. _____._____._____
Default Gateway IP Address: _____. _____._____._____
DNS Servers Address 1: _____. _____._____._____
DNS Servers Address 2: _____. _____._____._____

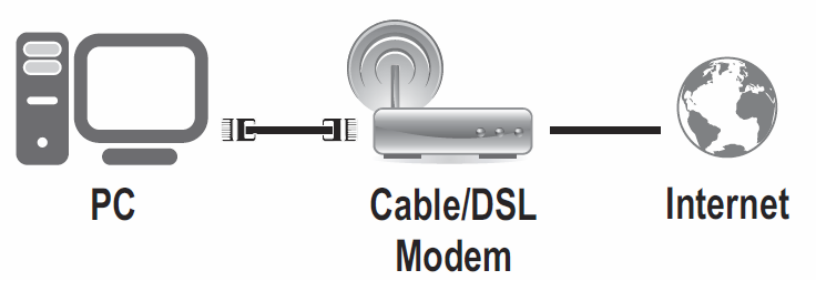
3. PPPoE to obtain IP automatically
User Name: _____
Password: _____

4. PPTP
Type (Dynamic IP/DHCP or Static IP)
PPTP Server: _____ (IP address)
IP Address: _____. _____._____._____ (e.g. 215.24.24.129)
Subnet Mask:_____. _____._____._____
Default Gateway:_____. _____._____._____
Server IP: _____. _____._____._____
DNS Servers Address 1: _____. _____._____._____
DNS Servers Address 2: _____. _____._____._____
User Name: _____
Password: _____

5. L2TP
Type (Dynamic IP/DHCP or Static IP)
L2TP Server: _____ (IP address)
IP Address: _____. _____._____._____ (e.g. 215.24.24.129)
Subnet Mask:_____. _____._____._____
Default Gateway:_____. _____._____._____
Server IP: _____. _____._____._____
DNS Servers Address 1: _____. _____._____._____
DNS Servers Address 2: _____. _____._____._____
User Name: _____
Password: _____

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. Connect your modem to the router Internet port (yellow).
5. Connect your computer to one of the router LAN ports.

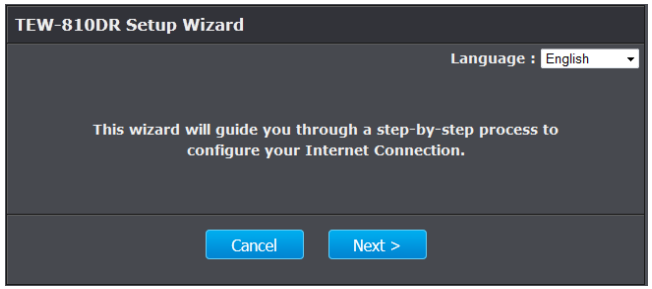
6. Connect the power adapter to the router and then to a power outlet.
7. Press the power on / off switch of the router and turn on your modem.
8. Verify that the status LED indicators on the front of the router are illuminated: **Power, Internet**.

Internet Setup Wizard

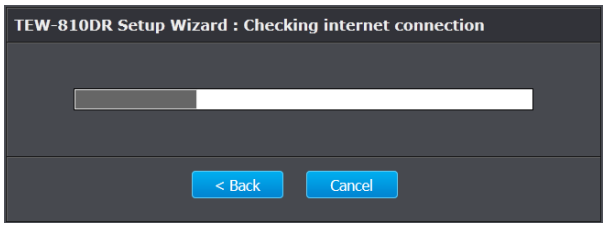
1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and the installation wizard will automatically open. If the wizard does not appear, type http://tew-810dr into the address bar of your web browser and press enter. Enter your User Name and Password, click Login and then click Advanced > Setup > Wizard.

   Note: *You can also access the device using the default IP address (http://192.168.10.1).*

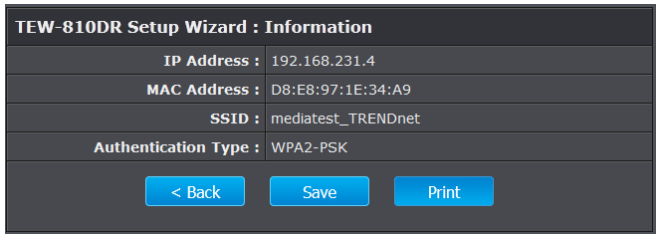
2. Select your language and click next to start the installation wizard.



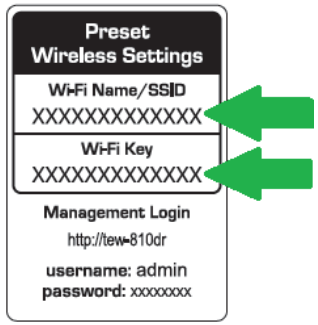
3. The router will detect your internet connection type.



4. Once complete the installation wizard is completed, the wizard will display your router's settings. Click **Save** to apply settings and continue. Click Print if you would like to print your settings for future reference.



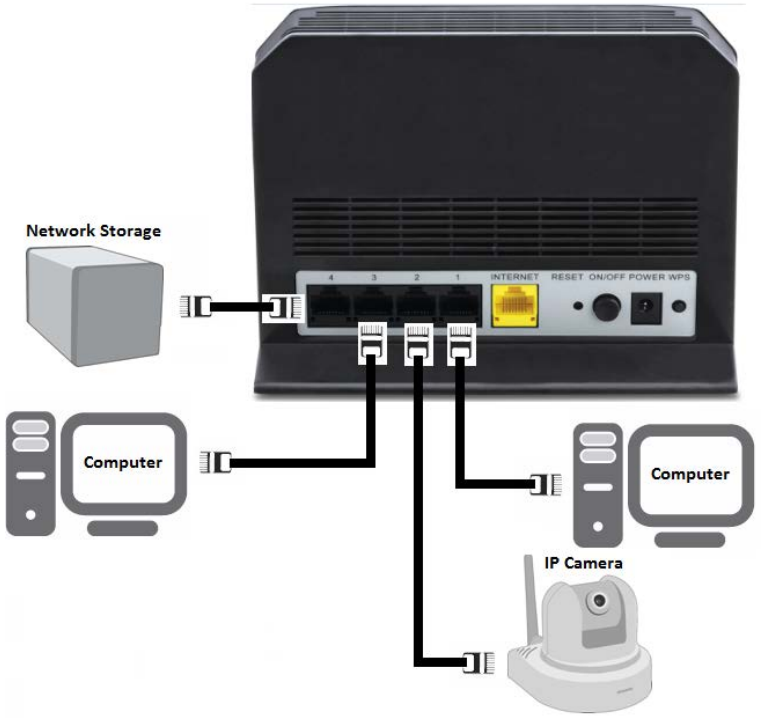
2. Select your language and click next to start the installation wizard.
5. Open a different web browser window to verify you have Internet connection.
6. For added security, the router is pre-encrypted with its own unique wireless network security key. You can find the unique network security key and pre-assigned network name (SSID) on a sticker on the front of the router and on a label on the bottom of the router. If you would like to change the wireless settings, continue to the next page to launch the wireless setup wizard.



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 (11n) and up to 1.3Gbps (11ac)***
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

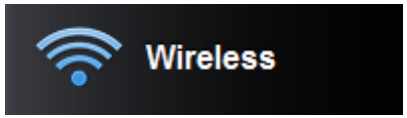
*Dependent on the maximum 802.11n/ac data rate supported by the device (150Mbps, 300Mbps, 450Mbps, 867Mbps, or 1.3Gbps)

Secure your wireless network

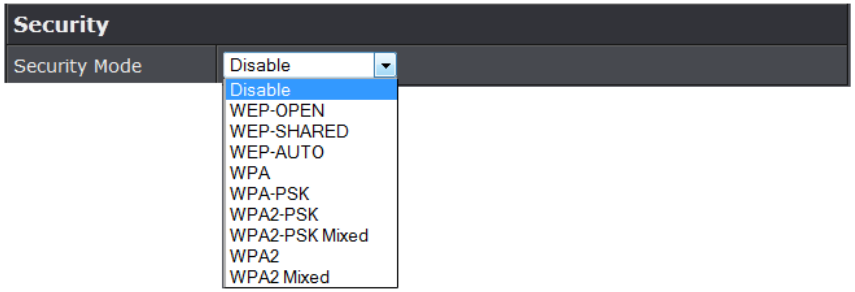
Wireless (2.4GHz or 5GHz)> Security

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 16).
2. Click on the **Wireless** button.



3. Underneath the basic wireless band section, you will see **Security Mode**. Click on the drop-down list to select your wireless security type.



Selecting WEP-OPEN, WEP-SHARED:

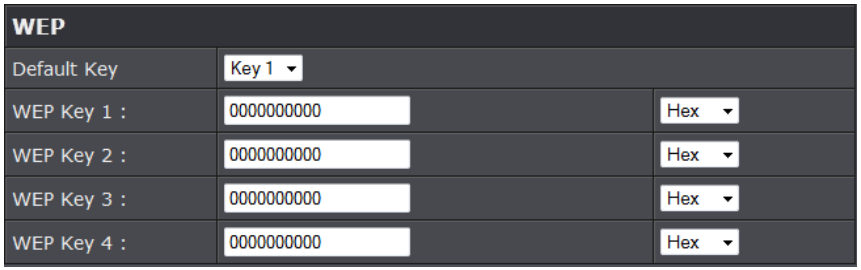
If selecting **WEP** (Wired Equivalent Privacy), please review the WEP settings to configure and click **Apply** to save the changes.

Note: WEP security is only available in the Security Mode list when **802.11 n-mode** is set to **Off** under **Wireless (2.4GHz or 5GHz)** > **Basic**.

Note: *WPS functionality is not available when using WEP.*

In the **Security Mode** drop-down list, select **WEP-OPEN** or **WEP-SHARED**.

Note: *It is recommended to use WEP-OPEN because it is known to be more secure than Shared Key.*



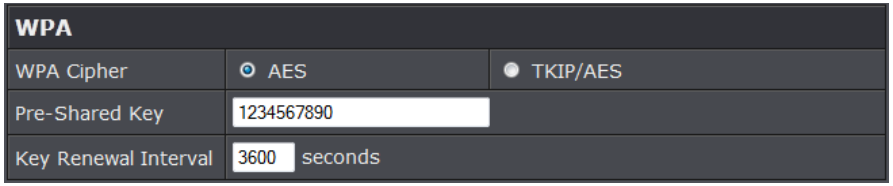
- **Current Network Key** - You can define up to 4 keys however, only one key can be active at any given time. Most users simply define one key. Click the drop-down list to select which of the 4 keys is the active key.
- **Network Key 1-4**
  - o This is where you enter the WEP key needed for a computer to connect to the router wirelessly
  - o 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.
  - o Choose a key index 1, 2, 3, or 4 and enter the key.
  - o 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)

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

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

- **Click here to display** - Typically, the password characters are masked for security purposes. This link displays actual characters of the currently assigned password for your reference.

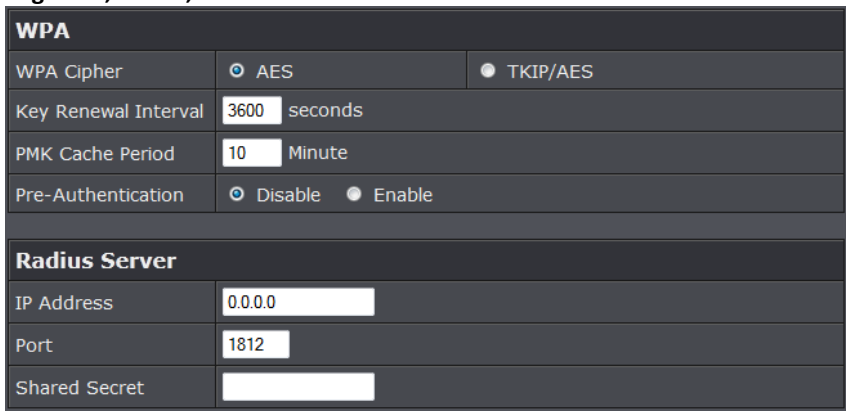
Selecting WPA-PSK, WPA2-PSK, WPA2-PSK, or Mixed (WPA2-PSK recommended):
In the **Security Mode** drop-down list, select **WPA-**.



The following section outlines options when selecting **WPA-PSK, WPA2-PSK,** or **WPA2-PSK Mixed** (Preshared Key Protocol),

- **WPA Encryption:** Select a Cipher Type to use. When selecting **WPA-PSK** security, it is recommended to use **TKIP + AES**.
  - When selecting **WPA2-PSK Mixed** security, it is recommended to use **TKIP+AES.**
  - When selecting **WPA2-PSK** security, it is recommended to use **AES**.
- **WPA passphrase:** Enter the passphrase.
  - This is the password or key that is used to connect your computer to this router wirelessly
    Note: *8-63 alphanumeric characters (a,b,C,?,*, /,1,2, etc.)*
  - **Network Key Rotation Interval:** Enter the time interval (seconds) of when the network passphrase will rotate. ***Note:*** *It is recommended to use the default interval time. Your passphrase will not change, rotation of the key is part of the WPA protocol and designed to increase security.*

Selecting WPA, WPA2, or WPA2 Mixed:



The following section outlines options when selecting **WPA. WPA2** or **WPA2 Mixed** known as EAP (Extensible Authentication Protocol). Also known as called Remote Authentication Dial-In User Service or **RADIUS**.

Note: *This security type requires an external RADIUS server, PSK only requires you to create a passphrase.*

- **RADIUS Server:** Enter the IP address of the RADIUS server. (e.g. *192.168.10.250)*
- **RADIUS Port:** Enter the port your RADIUS server is configured to use for RADIUS authentication.
  Note: *It is recommended to use port 1812 which is typical default RADIUS port.*
- **RADIUS Key:** 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 54 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 or if you are using WEP security.*

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

- Push Button Configuration (PBC) method
  - o (RECOMMENDED) Hardware Push Button method–with an external button located physically on your router and on your client device
  - o WPS Software/Virtual Push Button - located in router management page
- PIN (Personal Identification Number) Method - located in router management page
  Note: *Refer to your wireless device documentation for details on the operation of WPS.*

Recommended Hardware Push Button (PBC) Method

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

To add a wireless device to your network, simply push the WPS button on the wireless device you are connecting (consult client device User's Guide for length of time), then push and hold the WPS button located on your router for 3 seconds and release it. A blue LED on your router WPS button will flash indicating that the WPS setup process has been activated on your router. (See "Product Hardware Features" on page 5)

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

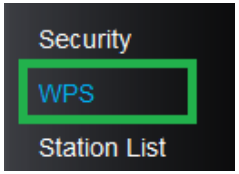
PBC (Software/Virtual Push Button)

Wireless (2.4GHz or 5GHz)> WPS

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 16).
2. Click on the **Advanced** tab.

3. Select wireless band you would like to configure, **Wireless 2.4GHz** or **Wireless 5GHz** and click on **WPS**.



4. To add a wireless device to your network, simply click the **Add Enrollee** button in the router management page, then push the WPS button on the wireless device (consult wireless device's User's Guide for length of time) you are connecting.

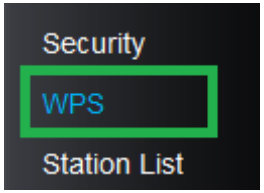
PIN (Personal Identification Number)

Wireless (2.4GHz or 5GHz)> WPS

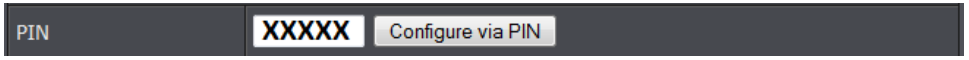
If your wireless device has WPS PIN (typically an 8-digit code printed on the wireless device product label or located in the wireless device wireless software utility), you can use this method.

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Select wireless band you would like to configure, **Wireless 2.4GHz** or **Wireless 5GHz** and click on **WPS**.



4. Next to **Station PIN**, enter the WPS PIN of the wireless device you are connecting and click the **Add Enrollee** button.



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

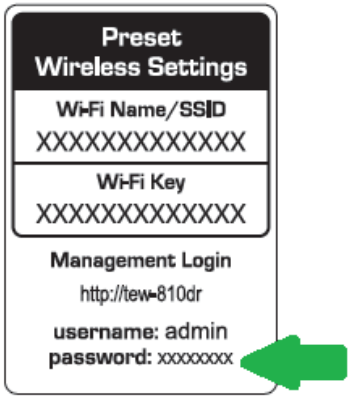
Basic

Access your router management page

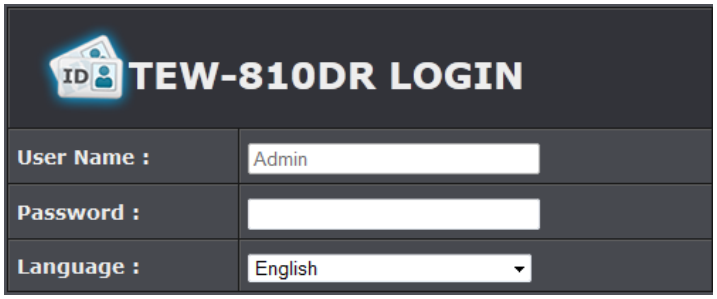
Note: *Your router management page URL/domain name http://tew-810dr or IP address http://192.168.10.1 is accessed through the use of your Internet web browser (e.g. Internet Explorer, Firefox, Chrome, Safari, Opera) and will be referenced frequently in this User's Guide.*

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to URL/domain name http://tew-810dr or IP address http://192.168.10.1. Your router will prompt you for a user name and password.

2. For added security, the router is preconfigured with a unique password. You can find the **Password** on a sticker on the side of the router and on the label on the bottom of the router.



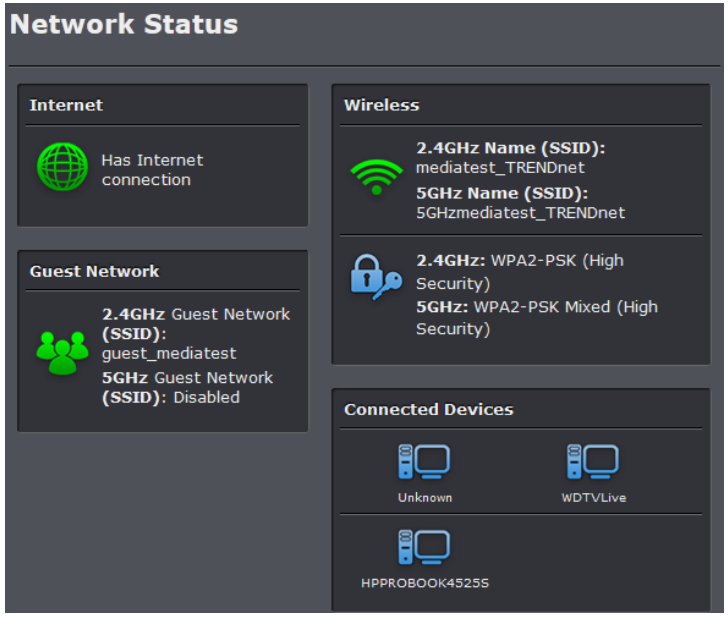
3. Enter your **Username** and **Password**, select your preferred language, then click **Login**.



- **User Name:** admin
- **Password: (xxxxxxxx)**
  Note: *User Name and Password are case sensitive.*

Network Status

This screen appears when you login into your router. This section provides an over view of your router.



Internet: This icon turns green to indicate that your network has a valid Internet connection. Amber color indicates a physical connection on the Internet port of the router but with no valid Internet connection. Red color indicates disconnected Internet port.

Guest Network: The section provides your router's guest network SSID. This icon turns green to indicate when your router's wireless network is enabled. Red color indicates your router's wireless network is disabled.

Wireless: This icon turns green to indicate when your router's wireless network is enabled. Red color indicates your router's wireless network is disabled.

Security: This section provides your router's wireless network security information.

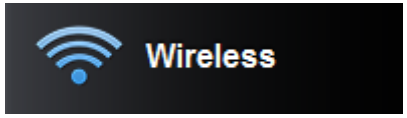
Connected Devices: This section provides information of all connected devices on your router.

Wireless settings

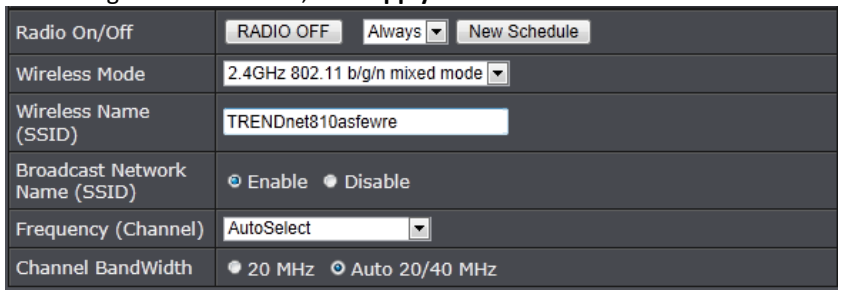
Wireless (2.4GHz or 5GHz)> Basic

This section outlines available management options under basic wireless sub tab for both 2.4GHz and 5GHz wireless sections.

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on **Wireless** and under the **Basic** tab.



3. To save changes to this section, click **Apply** when finished.



- **Radio On/Off:**
  - **On:** Turns on wireless radio.
  - **Off:** Turns off wireless radio.
  - **Schedule:** Select the schedule rule you would like to apply to your wireless network. (See "Create Schedule" section on page 34).
- **Wireless Mode**
  - **Auto:** Select this option if you have non-802.11n wireless clients (802.11a/b/g) connecting to your wireless network.
  - **Off:** The router will operate in 802.11n mode only, non-802.11n wireless clients will not be able to connect when this option is selected.

When applying the 802.11 n-mode setting on 2.4GHz, 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.
- **Wireless Name (SSID):** Enter the wireless name (SSID) for your wireless network. This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. By default, the router's wireless name is unique to the device. If you choose to change the SSID, change it to a name that you can easily remember.
- **Broadcast Network Name (SSID):**
  - **Enabled** allows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your router.
  - **Disabled** turns off the ability for wireless devices to find your network. It is still possible for wireless devices to be configured to connect to your wireless network. Disabling this setting will disable WPS functionality.
- **Frequency (Channel):** To manually set the channel on which the router will broadcast, click the drop-down list and select the desired Channel for wireless communication. The goal is to select the Channel that is least used by neighboring wireless networks.
- **Channel Bandwidth:** Select the appropriate channel width for your wireless network. This setting only applies to 802.11n and 802.11ac. For greater 802.11n performance in 2.4GHz, select **40MHz** (Options: 20MHz or 40MHz). For greater 802.11ac performance in 5GHz, select **80MHz** (Options: 20MHz, 40MHz, or 80MHz) It is recommended to use the default channel bandwidth settings.

  Note: *Please note that this setting may provide more stability than the higher channel bandwidth settings such as 40 MHz or 80MHz for connectivity in busy wireless environments where there are several wireless networks in the area.*
  - **20 MHz:** This mode operates using a single 20MHz channel for wireless devices connecting at 802.11n on both 2.4GHz and 5GHz. This setting may provide more stability than 40MHz or 80MHz for connectivity in busy wireless environments where there are several neighboring wireless networks in the area.
  - **Auto 20/40 MHz (2.4GHz wireless) or Auto 20/40/80 MHz (5GHz wireless):** When 40MHz or 80MHz is active, this mode is capable of providing higher

performance only if the wireless devices support the channel bandwidth settings. Enabling 40MHz or 80MHz typically results in substantial performance increases when connecting an 802.11n or 802.11ac client. ***Note:*** *Please note that 80MHz channel bandwidth is only available for 802.11ac 5GHz.*

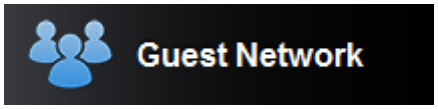
Guest Network

Wireless (2.4GHz or 5GHz) > Guest Network

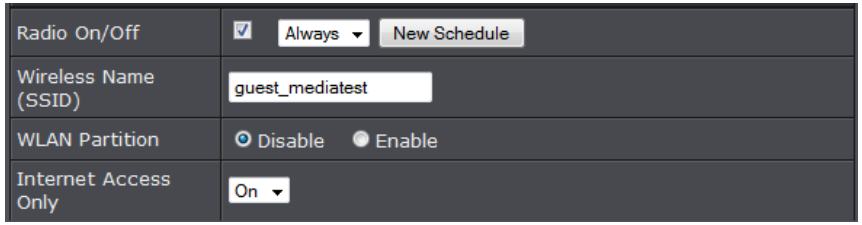
Creating an isolated and separate wireless guest network (2.4GHz or 5GHz) allows wireless clients to connect to your network for Internet access only and keep your local LAN network safe by restricting guest access to your LAN network resources such as shared documents and media files on your computers, network storage, and printers.

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Basic** tab.

3. Click on **Guest Network** section.



4. Review the Guest Network settings, click **Apply** when finished.



- **Radio On/Off:**
  - **On:** Turns on wireless radio.
  - **Off:** Turns off wireless radio.
  - **Schedule:** Select the schedule rule you would like to apply to your wireless network. (See "Create Schedule" section on page 34).
- **Wireless 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.
- **WLAN Partition**: Enabling this option will restrict guests from communicating with each other over the guest network such as share files**.**
- **Internet Access Only:** By default, the option is checked to allow guests to only access the Internet and restrict access to your local LAN network. Please note that unchecking this option will open access to local LAN network to guests.

5. Apply wireless security to your guest network (see "How to choose the type of security for your wireless network" on page 11).

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.

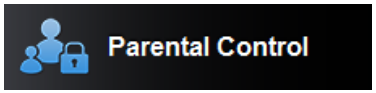
If possible, upgrade wireless network interfaces (such as wireless cards in computers) from older wireless standards to 802.11n or 802.11ac. If a wirelessly networked device uses an older standard, the performance of the entire wireless network may be slower. If you are still experiencing low or no signal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

Parental Control

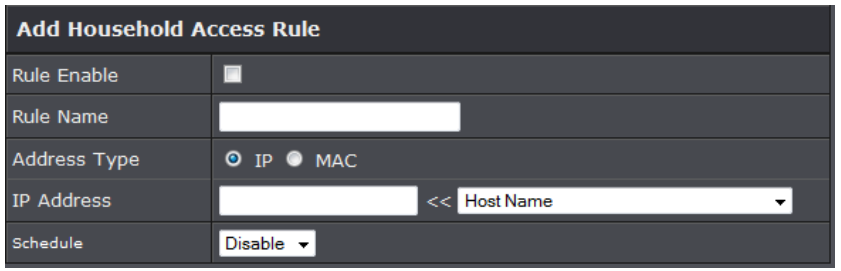
This section allows you to setup and block specific network clients from access certain webpage, similar to URL filter.

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Basic** tab.

3. Click on the **Parental Control** section.

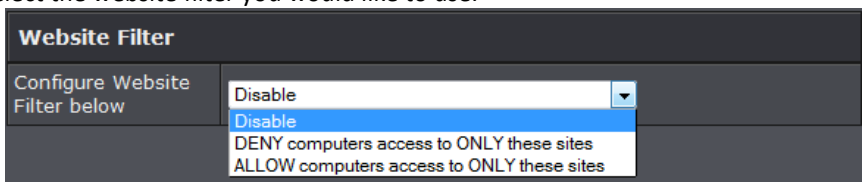


4. Review the household access rule section and click **Add** to continue.



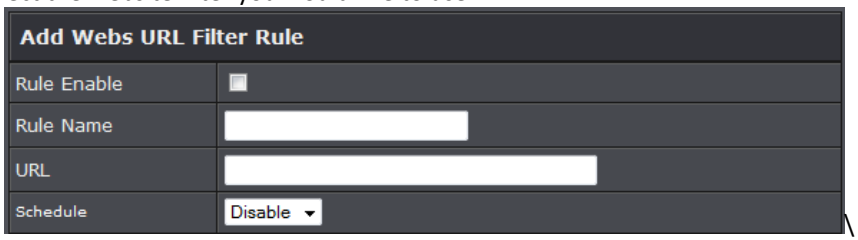
- **Rule Enable:** Check this option to enable the rule.
- **Rule Name:** Enter the name of that you would like to apply to the rule.
- **Address Type:** Select the type of address you would like to use, IP address or MAC address.
- **IP Address:** Enter your client's address.
- **Schedule:** Select the schedule rule you would like to apply to your wireless network. (See "Create Schedule" section on page 34).

5. Select the website filter you would like to use.



- **Disable:** Select this option if you would like to disable website filter.
- **DENY:** Select this option to deny only website listed.
- **ALLOW:** Select this option to allow only website listed.

6. Select the website filter you would like to use.



- **Rule Enable:** Check this potion to enable URL rule
- **Rule Name:** Enter the name of the URL rule
- **URL:** Enter the URL to apply to the rule
- **Schedule:** Click the drop-down list to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule. (See "Create Schedule" section on page 34).

Access Control Filters

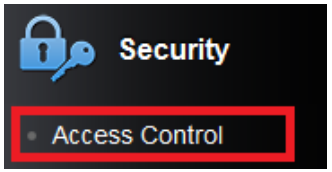
Access control basics

Advanced > Security > Access Control

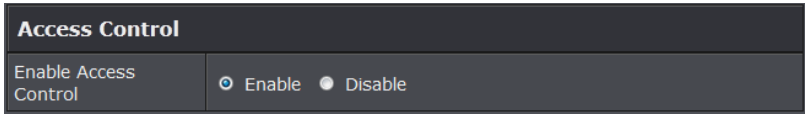
You may want to block computers or devices on your network access to specific ports (used or required by a specific application) to the Internet.

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Security** section and click on **Access Control**.



4. Select enable next Enable Access Control to open the access control features. Click **Apply** to save changes.



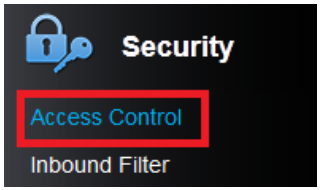
Service and Port blocking

Advanced > Security > Access Control

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 15).
2. Click on the **Advanced** tab.

3. Click on the **Security** section and click on **Access Control**.



4. Review the settings under **LAN Client Filter Rules** section. Click **Apply** to save settings.

Add Port Range and Service Block Rule	
Policy Enable	☐
Policy Name	
Schedule	Always
Client IP Address	~
Rule Define	Special Service User Define

- **Enable:** Click to enable rule.
- **Policy Name:** Enter the name of the rule you would like to assign.
- **Schedule:** Select the defined schedule you would like to have the rule to be applied (see "Create Schedule" section on page 34).
- **Client IP Address:** Enter the IP addresses or IP range to apply the rule.
- **Rule Define: Select the rule type.**
  - o **Special Services:** Select this option to select predefined services.

Service	Description	Enabled
WWW	HTTP, TCP Port80, 8080	☐
Email Sending	SMTP, TCP Port 25	☐
Email Receiving	POP3, TCP Port 110	☐
File Transfer	FTP, TCP Port 21	☐
Telnet Service	TCP Port 23	☐
DNS Query	UDP Port 53	☐
TCP Protocol	All TCP Port	☐
UDP Protocol	All UDP Port	☐

  - o **User Define:** Select this option to manually assign the TCP and UDP ports

Rule Define	Special Service User Define
TCP Ports	Ex: 21 or 300-500
UDP Ports	Ex: 21 or 300-500

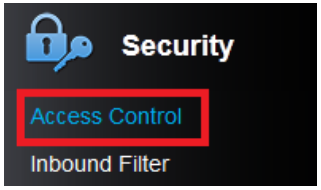
IP blocking

Advanced > Security > Access Control

You may want to block certain IP addresses or a range of IP address access to your network.

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Security** section and click on **Access Control**.



4. Review the settings under **LAN Client Filter Rules** section. Click **Apply** to save settings.

Add IP Range Block Rule	
Rule Enable	☐
Rule Name	
IP Address	(ex: 192.168.10.1, 192.168.10.0/24, 192.168.10.1-192.168.10.20)
Schedule	Always

- **Enable:** Click to enable rule.

- **Rule Name:** Enter the name of the rule you would like to assign.
- **LAN IP Address Range:** Enter the IP address or IP address range to apply the protocol (e.g. *192.168.10.20-192.168.10.20* or *192.168.10.20-192.168.10.30)*. ***Note:*** *The filter will not be applied to IP addresses outside of the range specified.*
- **Schedule:** Select the defined schedule you would like to have the rule to be applied (see "Create Schedule" section on page 34).

Website Filter

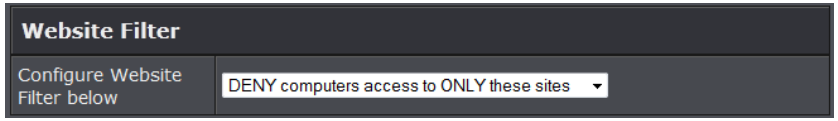
Advanced > Security > Access Control

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 15).
2. Click on the **Advanced** tab.

3. Click on the **Security** section and click on **Access Control**.

4. Select to **ALLOW** or **DENY** websites listed.



5. Review the website rule settings and click **Apply** to save changes.

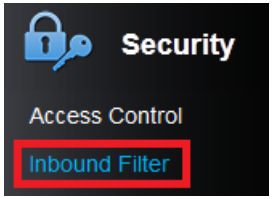
- **Rule Enable:** Check this potion to enable URL rule
- **Rule Name:** Enter the name of the URL rule
- **URL:** Enter the URL to apply to the rule
- **Schedule:** Click the drop-down list to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule. (See "Create Schedule" section on page 34).

Inbound Filter

Advanced > Security > Inbound Filter

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Security** section and click on **Access Control**.



4. Review the inbound filter settings and click **Apply** to save changes.

- **Rule Name:** Enter the name of the URL rule
- **Rule Action:** Select the action you would like to apply to the rule.
- **IP Address:** Enter the IP address you would like to apply the rule.

ADVANCED

Change your router IP address

Advanced > Setup > LAN Setting

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.

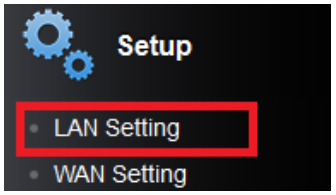
> ***Note:*** *If you are not encountering any issues or are not faced with one of the cases described above or similar, it is recommended to keep your router IP address settings as default.*

Default Router IP Address: 192.168.10.1

Default Router Network: 192.168.10.0 / 255.255.255.0

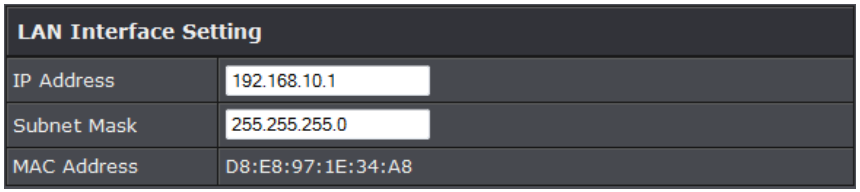
1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **LAN Setting**.



4. In **LAN Interface Setting** section, Enter the router IP address settings. Click **Apply** to save settings.

> ***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.*



- **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*)
- **MAC Address:** Displays your router's MAC address
  Note: *You will need to access your router management page using your new router IP address. (e.g. Instead of using the default http://192.168.10.1 your new router IP address will use the following format using your new IP address http://(new.ipaddress.here) to access your router management page. You can also use the default login URL http://tew-810dr*

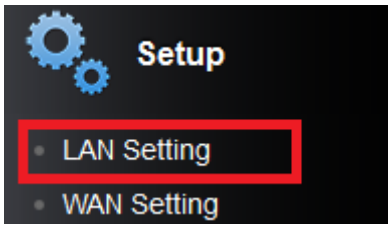
Set up the DHCP server on your router

N Advanced > Setup > LAN Setting

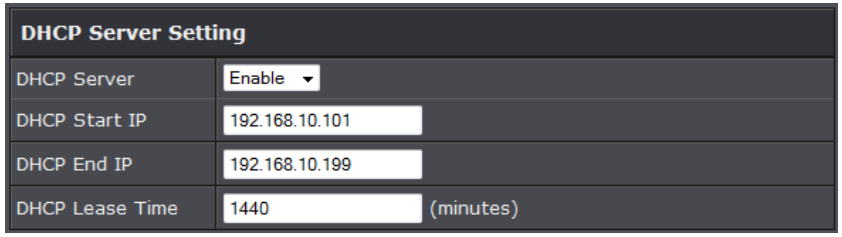
Your router can be used as a DHCP (Dynamic Host Configuration Protocol) server to automatically assign an IP address to each computer or device on your network. The DHCP server is enabled by default on your router. If you already have a DHCP server on your network, or if you do not want to use your router 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 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **LAN Setting**.



3. Review the DHCP Server settings. Click **Apply** to save settings.



- **DHCP Server:** Enable or Disable the DHCP server.
- **DHCP Start IP:** Changes the starting address for the DHCP server range. (e.g.*192.168.10.20)*
- **DHCP End IP:** Changes the last address for the DHCP server range. (e.g. *192.168.10.30)*
  Note: *The Start IP and End IP specify the range of IP addresses to automatically assign to computers or devices on your network.*
- **DHCP Lease Time:** Enter in minutes the DHCP lease time you would like to apply.
  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.*

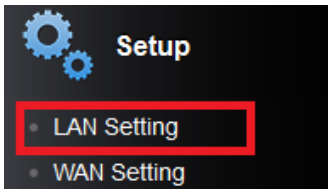
Set up DHCP reservation

Network > LAN Setting

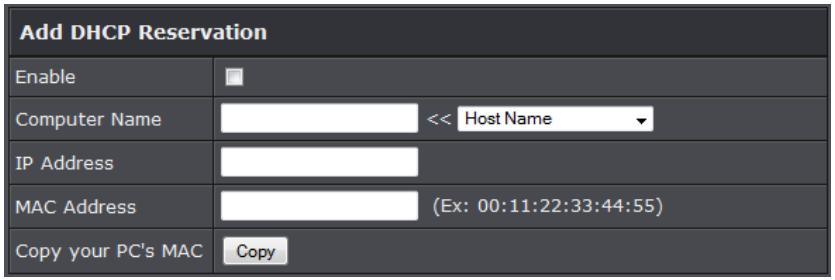
DHCP (Dynamic Host Configuration Protocol) reservation (also called Static DHCP) allows your router to assign a fixed IP address from the DHCP server IP address range to a specific device on your network. Assigning a fixed IP address can allow you to easily keep track of the IP addresses used on your network by your computers or devices for future reference or configuration such as virtual server (also called port forwarding, see "Virtual Server" on page 35) 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 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **LAN Setting**.



3. Review the DHCP reservation settings. Click **Apply** to save settings.



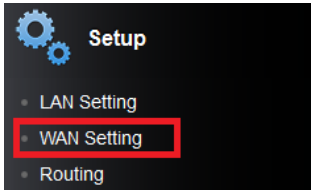
- **Enable:** Check the box to enable DHCP reservation rule.
- **Computer Name:** Enter a name of the device you will assign the DHCP reservation rule or select your device from the pull down menu.
- **IP Address:** Enter the IP address to assign to the reservation. (e.g. 192.168.10.101)
- **MAC Address:** 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)*
- **Copy your PC's MAC:** Click this option to copy's your computer's MAC address to the MAC address field.

Manually configure your Internet connection

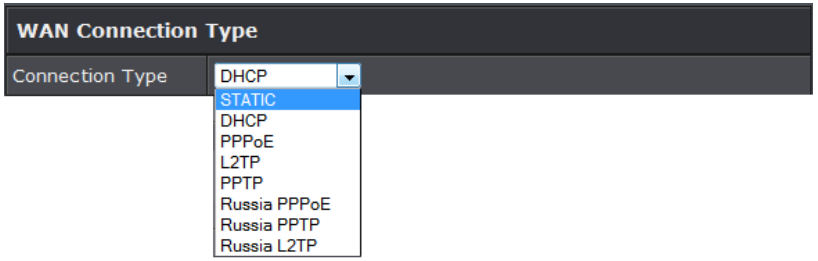
Advanced > Setup > WAN Setting

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **WAN Setting**.



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



5. Complete the fields required by your ISP.
6. Complete the optional settings only if required by your ISP.
7. To save changes, click **Apply**.

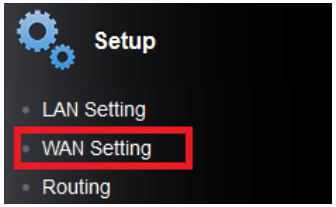
Note: *If you are unsure which Internet connection type you are using, please contact your ISP.*

Manually configure your DNS server setting

Advanced > Setup > WAN Setting

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **WAN Setting**.



4. Enter both Primary and Secondary DNS servers to use. Click **Apply** to save settings.

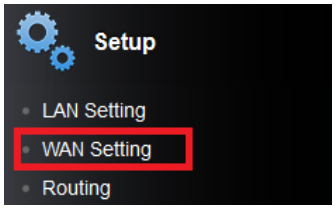
Note: *If you are unsure which DNS to use, please contact your ISP.*

Manually configure your MTU setting

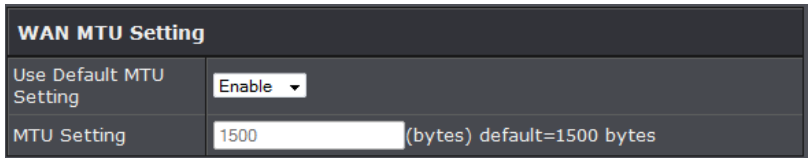
Advanced > Setup > WAN Setting

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **WAN Setting**.



4. Under "**Use Default MTU Setting** select Disable to manually enter your MTU setting.



Note: *If you are unsure which DNS to use, please contact your ISP.*

Clone a MAC address

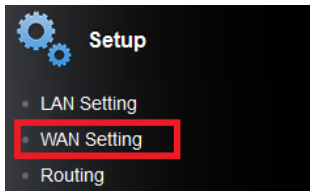
Advanced > Setup > WAN Setting

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.

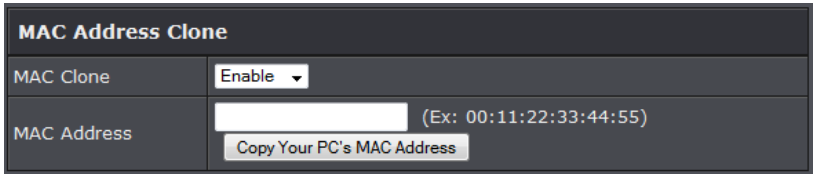
Note: *For many ISPs that provide dynamic IP addresses automatically, typically, the stored MAC address in the modem is reset each time you restart the modem. If you are installing this router for the first time, turn your modem before connecting the router to your modem. To clear your modem stored MAC 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 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **WAN Setting**.



4. Next to MAC Clone select Enable on the pull down menu. Manually enter you MAC address or click **Copy Your PC's MAC address** to copy your computer's MAC address.



Note: *You can check the DHCP Client List for the MAC addresses of the devices on your network, see page 36 or refer to your computer or device documentation to find the MAC address.*

Add static routes to your router

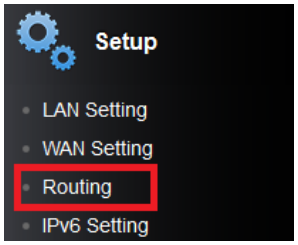
Advanced > Setup > Routing

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.

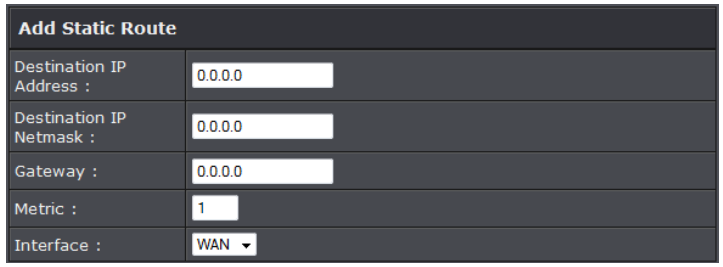
Note: *Configuring this feature assumes that you have some general networking knowledge.*

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **Routing**.



4. Review the **LAN/WAN Static Routes** section. Click **Apply** to save settings.



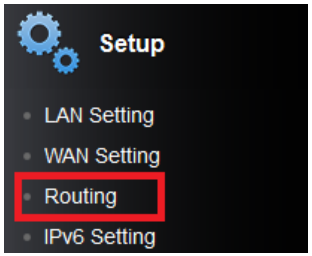
- **Destination IP Address:** Enter the IP network address of the destination network for the route. (e.g. *192.168.20.0*)
- **Destination IP Netmask:** Enter the subnet mask of the destination network for the route. (e.g. *255.255.255.0*)
- **Gateway:** Enter the gateway to the destination network for the route. (e.g. *192.168.10.2*)
- **Metric:** Enter the metric or priority of the route. The metric range is *1-15*, the lowest number *1* being the highest priority. (e.g. *1*)
- **Interface:** Select **WAN** on the pull down menu.

Enable RIP on your router

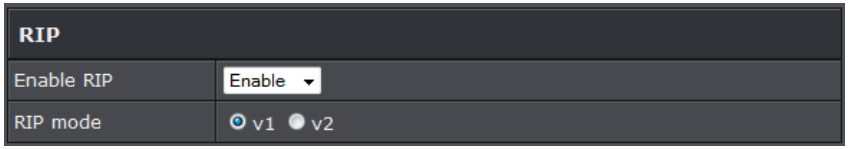
Advanced > Setup > Routing

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **Routing**.



4. Review the **LAN/WAN Static Routes** section. Click **Apply** to save settings.



- **Enable RIP:** Select Enable on the pull down to enable RIP
- **RIP mode:** Select the RIP version to use.

IPv6 Internet Connection Settings

Advanced > Setup > IPv6 Setting

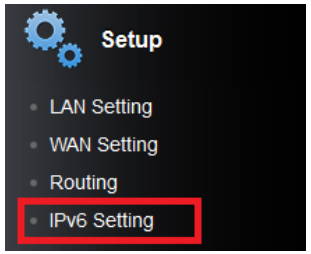
IPv6 (Internet Protocol Version 6) is a new protocol that significantly increases the number of available Internet public IP addresses due to the 128-bit IP address structure versus IPv4 32-bit address structure. In addition, there are several integrated enhancements compared to the most commonly used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

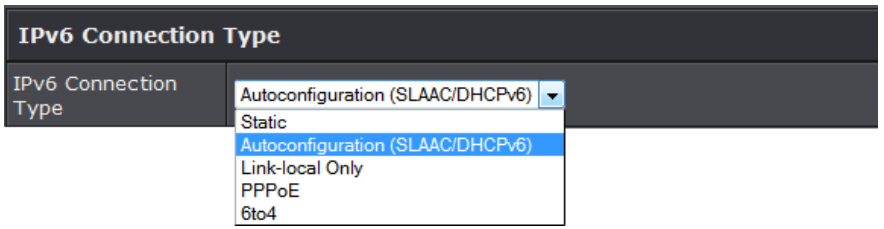
Note: *In order to use IPv6 Internet connection settings, it is required that your ISP provide you with the IPv6 service. Please contact your ISP for availability and more information about the IPv6 service.*

1. Log into your router management page (see "Access your router management page on page 15").
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **IPv6 Setting**.



4. Review the IPv6 Internet Connection settings and enter information settings specified by your ISP.



- **IPv6 Connection Type:** Select your IPv6 connection.
  - o **6to4:** 6to4 is provided as a transitional mechanism for migrating from IPv4 to IPv6. It allows IPv6 packets to be transmitted over an IPv4 network through the automatic tunneling technology and routes traffic between 6to4 and IPv6 networks.

- **Native IPv6 only:** Native IPv6 refers to a network where IPv6 is the only transport protocol.
- **6to4 + Native IPv6:** Supports 6to4 and Native IPv6 simultaneously.

- **LAN Network Prefix:** Enter the LAN Network Prefix here. This can be based on ULA (Unique Local Address).
- **DNS server**: IPv6 DNS address will be provided by your local ISP.
- **6to4 subnet ID:** Specifies, in hexadecimal notation, a subnet ID other than 0

Prioritize traffic using QoS (Quality of Service)

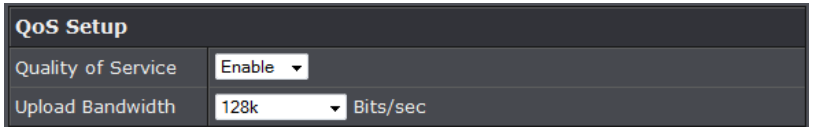
Advanced > Setup > QoS

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 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **IPv6 Setting**.

4. Review the QoS settings. Click **Apply** to save your setting.



- **Enable QoS:** Enable or Disable the Quality of service through the router.
- **Upload Bandwidth:** Select your upload bandwidth on the pull down menu.

Advanced wireless settings

The advanced wireless features provide can provide you with additional options for setting up your wireless network such as multiple SSID and WDS (Wireless Distribution System) or wireless bridging.

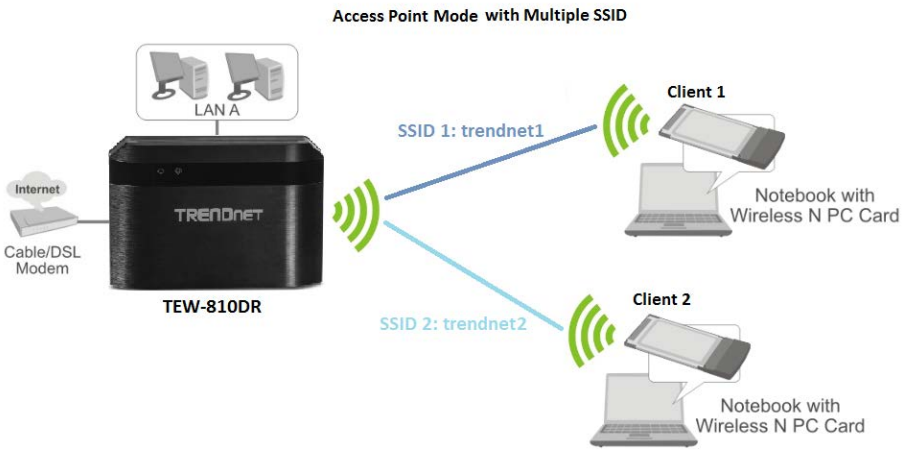
Multiple SSID

Advanced > Wireless (2.4GHz or 5GHz) > Multiple SSID

The multiple SSID feature allows you to broadcast up to 2 additional SSIDs (or wireless network names). When wireless devices are searching for available wireless networks to connect to, the SSIDs (or wireless network names) will appear as separate and different wireless networks. Since they appear as separate wireless networks, they are also referred to as virtual APs (Access Points) since they appear as separate wireless access points but are actually all being broadcasting and managed by a single wireless access point. Each virtual AP can be configured each with a different SSID (or wireless network name), security type and additional settings for wireless devices to connect. You can use the multiple SSID feature to setup guest wireless accounts with a different security type to keep your primary wireless network security information private. The diagram shows an example of a client connecting to SSID 1 and another client connecting to SSID 2.

By default, your router functions in Access Point mode to allow wireless client devices to connect and access your network resources and access the Internet using a single SSID.

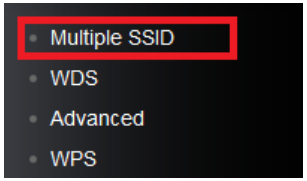
The diagram shows an example of a client connecting to SSID 1 and another client connecting to SSID 2.



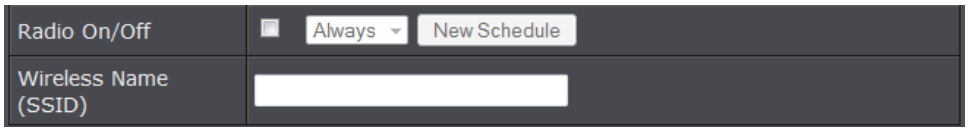
To configure multiple SSID on your router:

1. Log into your router management page (see "Access your router management page" on page 16).
2. Click on the **Advanced** tab.

3. Select the wireless band you would like to configure **Wireless 2.4GHz** or **Wireless 5GHz** and click on **Multiple SSID**.



4. Review the Multiple SSID settings, click **Apply** when finished.



- **Enabled:** Check the option to enable the Guest Network. Select a schedule rule you would like to apply to your wireless network. (See "Create Schedule" section on page 34) or select Always to have radio always on.
- **Wireless 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.

5. Under Security Policy, you can apply a different wireless security type and key to the guest network. Please refer to How to choose the type of security for your wireless network page 11 to find out about different security types and Secure your wireless network page 12 for wireless security configuration.

Note: *You can repeat the steps to enable and configure additional SSIDs. You can configure your wireless security settings for the additional SSIDs under Wireless (2.4GHz or 5GHz)>Security. Under the Security Policy section, click the Wireless Name (SSID) drop-down list to select the additional SSIDs to configure. Please refer to page 15 to find out about different security types and page 16 for wireless security configuration.*

Wireless bridging using WDS (Wireless Distribution System)

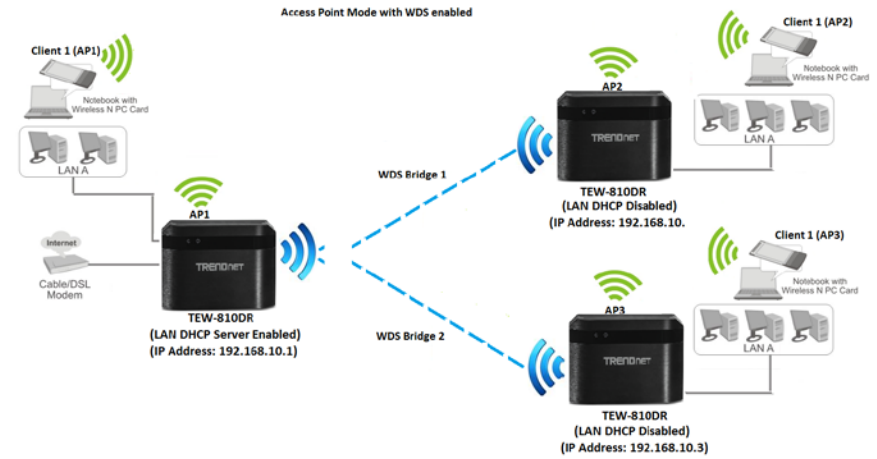
Advanced > Wireless (2.4GHz or 5GHz) > WDS

Wireless bridging using WDS allows the device to create a wireless bridge with other WDS supported wireless routers and access points configured in WDS mode to bridge groups of network devices together wirelessly. Simultaneously, the router will also function in access point mode allowing wireless client devices such as computers, game consoles, mobile phones, etc. to connect in order to access network resources from multiple groups of network devices as well as the Internet.

Note: *You can create up to four WDS bridge connections on each wireless band (2.4GHz and 5GHz). WDS (Wireless Distribution System) is not currently standardized and may not connect to different model wireless routers or access points, therefore, when using WDS, it is recommended to use the same model and version for wireless bridging.*

By default, your router functions in Access Point mode to allow wireless client devices to connect and access your network resources and access the Internet.

In the diagram below, the blue color represents the WDS wireless bridged connections between the routers. The green color represents access point mode connections between wireless client devices and the routers.



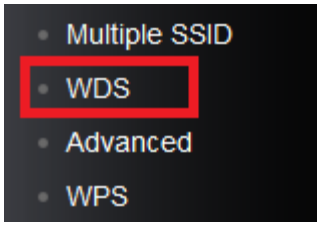
Note: *Before configuring WDS, please ensure the following first:*

1. *Make sure different IP addresses are assigned to each WDS supported wireless device used for bridging. (ex. 192.168.10.1,192.168.10.2, 192.168.10.3) to avoid IP address conflict. See page 34 for changing the LAN IP address.*
2. *If you are using more than one WDS supported router, please make sure the LAN DHCP server is enabled on only one and disabled on all others to avoid IP address conflict. See page 35 for DHCP server options.*
3. *Configure the same wireless channel and use the same on all WDS supported wireless devices. See page 20 for configuring basic wireless settings.*
4. *Configure the same wireless security and key on all WDS supported devices. See page 15 for configuring wireless security settings.*

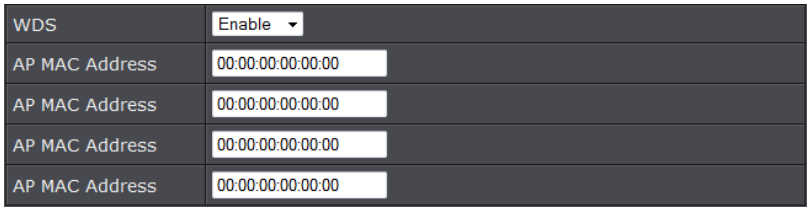
To configure WDS bridging between TEW-810DRU routers:

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Select wireless band you would like to configure, **Wireless 2.4GHz** or **Wireless 5GHz** and click on **WDS**.



4. Select Enable for WDS and enter the MAC address of the other WDS supported wireless device you are bridging next to AP MAC Address field. (e.g. *00:11:22:AA:BB:CC).* To save settings, click **Apply**.



For additional routers, make sure to disable the DHCP server first on all additional routers and configure the LAN IP address to be different on each router. You will connect devices to the LAN ports 1-4 only on all additional routers and the WAN port is not used. Then, repeat the steps for additional routers you are bridging.

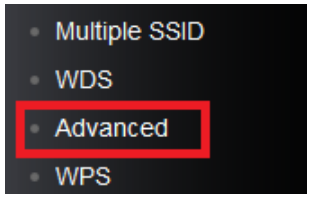
Additional wireless settings

Advanced > Wireless (2.4GHz or 5GHz) > Advanced

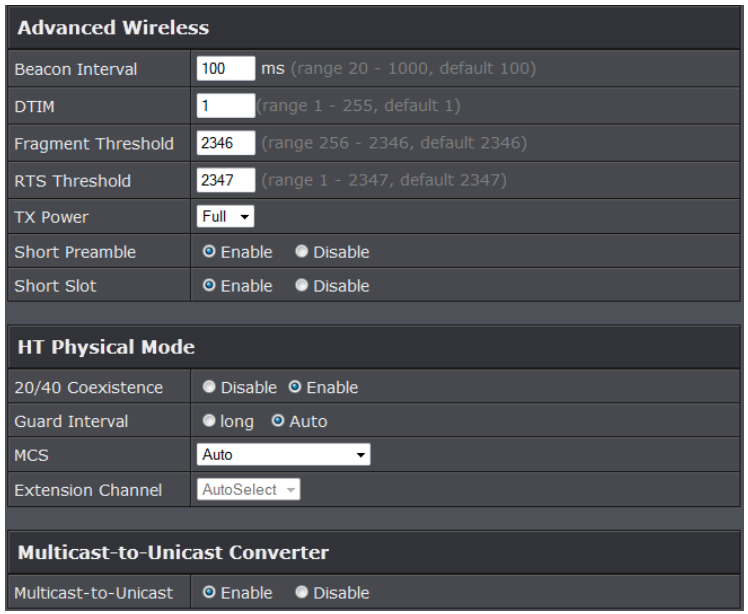
These settings are advanced options that can be configured to change advanced wireless broadcast specifications. It is recommended that these settings remain set to their default values unless you are knowledgeable about the effects of changing these values. Changing these settings incorrectly can degrade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

1. Log into your router management page (see "Access your router management page on page 15").
2. Click on the **Advanced** tab.

3. Select wireless band you would like to configure, **Wireless 2.4GHz** or **Wireless 5GHz** and click on **Multiple SSID**.



4. Review the Multiple SSID settings, click **Apply** when finished.



- **Beacon Interval:** 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: 25-1000)
- **DTIM:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.
- **Fragment Threshold:** Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value of 2346 bytes. Setting the Fragmentation value too low may result in poor performance.
- **RTS Threshold:** The Request To Send (RTS) function is part of the networking protocol. A wireless device that needs to send data will send a RTS before sending the data in question. The destination wireless device will send a response called Clear to Send (CTS). The RTS Threshold defines the smallest data packet size allowed to initiate the RTS/CTS function.
  Default Value: 2347 (range: 1-2347)
- **TX Power:** Select the wireless transmit power of your wireless router.
- **Short Preamble:** Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Short Slot:** Is the time the device waits before retransmitting a packet after a collision.
- **20/40 Coexistence:** Allows legacy wireless clients to connect to your wireless network.
- **Guard Interval:** Allows distinct wireless packets to no interfere with each other.
- **MCS:** Modulation and coding scheme, defines the transmission rate of your wireless router.
- **Extension Channel:** Allows you to select your wireless router's extended channel when higher wireless bandwidth is used.

- **Multicast-to-Unicast:** Allows the wireless router to convert multicast traffic to unicast.
  Note: *It is recommended to keep the default setting – Auto.*

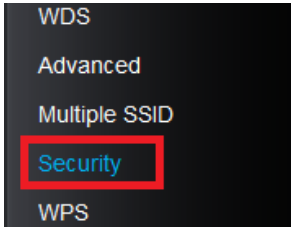
Wireless security (Wireless MAC filter)

Advanced > Wireless (2.4GHz or 5GHz) > Security

You may want to block wireless computers or devices on your network. This feature allows you to protect your wireless network using MAC address.

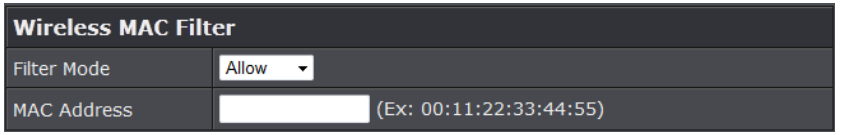
1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Select the wireless band you would like to configure **Wireless 2.4GHz** or **Wireless 5GHz** and click on **Security**.



4. Select the wireless SSID from the pull down menu you would like to apply the MAC filter to.

5. Review the Wireless MAC filter settings and click **Apply** to save changes.



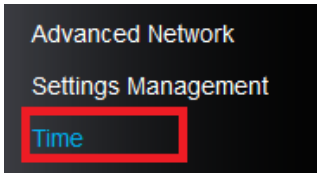
- Filter Mode: Select the wireless filter mode you would like to apply.
  - o **Disable:** Select this option if you would like to disable filter.
  - o **Allow:** Select this option to allow only listed MAC addresses.
  - o **Reject:** Select this option to deny only listed MAC addresses.
- **MAC address:** Enter the MAC address of the wireless client you would like to apply to the MAC filter.

Set your router date and time

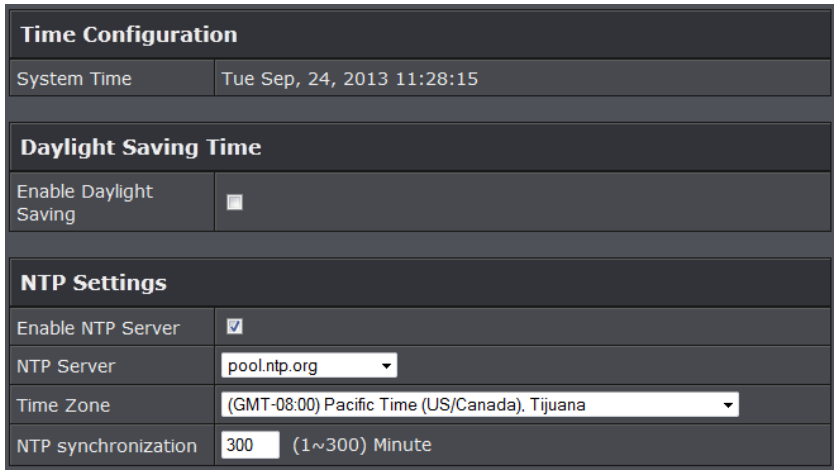
Advance > Administrator > Time

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on **Administrator** section and click **Time**.



4. Review the Time settings. Click **Apply** to save settings.



- **Sytem Time:** Displays the current device time and date information.
- **Enable Daylight Saving:** Check the option to configure the DST settings. Set the annual range when daylight saving is activated.
- **Enable NTP Server:** Check to enable NTP server. If option is not selected you will need to manually set your time.
- **NTP Server: Select the NTP server to use on the pull down menu.**
- **Time Zone:** Select from the pull down menu your time zone.

  ***Note**: NTP servers are used for computers and other network devices to synchronize time across an entire network.*
- **NTP synchronization:** Enter the time duration in minutes of when the router will synchronize with the NTP server.
- **Manually set time:** This option is available when Enable NTP Server option is not enabled.
  ***Note:** Time is specified in 24-hour format.*

Create schedules

Advance > Setup> Schedule

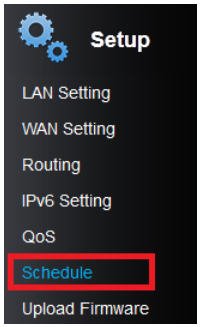
For additional security control, your router allows you to create schedules to specify a time period when a feature on your router should be activated and deactivated. Before you use the scheduling feature on your router, ensure that your router system time is configured correctly.

***Note:** You can apply a predefined schedule to the following features:*

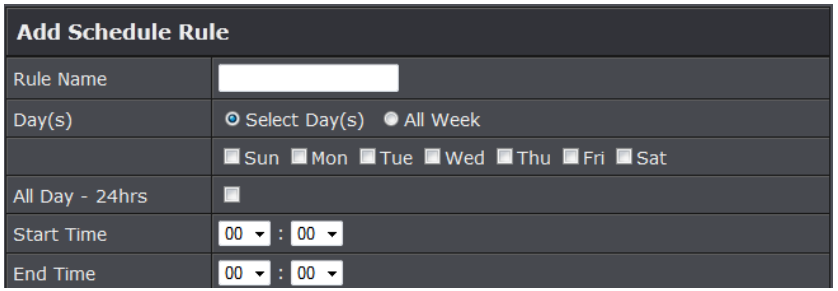
- *Virtual Server*
- *Access Control (Domain/URL Filters & IP/Protocol LAN Client Filters)*
- *Special Applications*
- *Gaming*

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on **Setup** section and click **Schedule**.



3. Review the Schedule settings. Click **Apply** to save settings.



- **Rule Name:** Enter a name for the schedule you would like to apply.
- **Days:** Check the days you would like the rule to be applied or select **All Week** to enable the rule all week.
- **Start/End Time:** Select the start and end time you would like the schedule to follow.

Note: *The schedule defined will define the time/day the feature will be activated.*

Open a device on your network to the Internet

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

DMZ

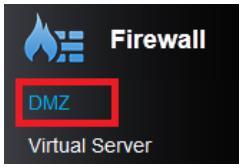
Advanced > Firewall > DMZ

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 35) to allow access to your computers or network devices from the Internet.

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Firewall** section and click on **DMZ**.



4. Select Enable in the DMZ Settings section. Enter the IP address you assigned to the computer or network device to expose to the Internet. Click **Apply** to save settings.

Virtual Server

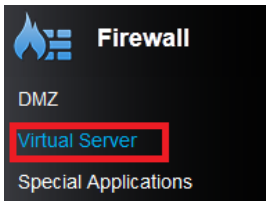
Advanced > Firewall > Virtual Server Rules

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 35) 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. To open several ports please refer to "Gaming" section on page 37.

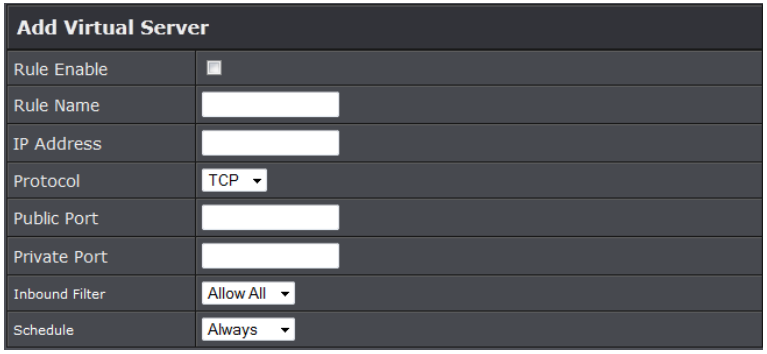
Since most ISPs constantly change your home IP address, to be able to access the Virtual Server port(s) from the Internet it is recommended to setup Dynamic DNS service (outlined in Identify Your Network section page 41).

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Firewall** section and click on **Virtual Server Rule**.



4. Select Enable in the Virtual Server Function section. Review the virtual server settings. Click **Add** to save settings.



- **Rule Enable:** Check to enable virtual server rule
- **Rule Name:** Enter the name you would like to assign to the virtual server rule.
- **IP Address:** Enter the IP address of the device to forward the port (e.g. *192.168.10.101)*.
- **Protocol**: Select the protocol required for your device. **TCP** or **UDP**.

  Note: *Please refer to the device documentation to determine which ports and protocols are required.* 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/Private Public Port:** Enter the port number used to access the device from the Internet.
- **Inbound Filter:** Select the defined inbound filter you would like to apply or select **Allow All**.
- **Schedule:** Select the defined schedule you would like to have the rule to be applied (see "Create Schedule" section on page 34).

  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.*

Example: To forward TCP port 80 to your IP camera

1. Setup DynDNS service (see Identify Your Network section page 41).
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.

   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 15).
5. Click on **Advanced** then **Firewall**, click on **Virtual Server**.
6. Click **Enabled** to turn on this virtual server.
7. Next to **Rule Name**, you can enter another name for the virtual server, otherwise, leave the default name.
8. Next to **IP Address**, enter the IP address assigned to the camera. (e.g. *192.168.10.101*)
9. Next to **Protocol**, make sure **TCP** is selected in the drop-down list.
10. The **Private Port** and **Public Port**, make sure port number **80** is configured for both settings.
11. Select **Allow All** on **Inbound Filter** section.
12. Select **Always** for **Schedule** section.
13. To save the changes, click **Add.**

Special Applications

Advanced > Firewall > Special Applications

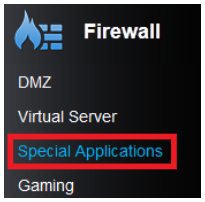
Special applications (also called port triggering) is typically used for online gaming applications or communication applications that require a range of ports or several ports to be dynamically opened on request to a device on your network. The router will wait for a request on a specific port or range 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 39.

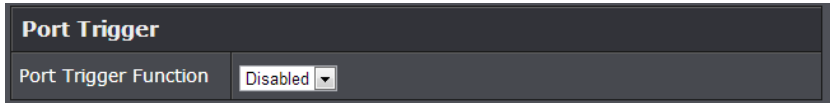
Note: *Please refer to the device documentation to determine if your device supports UPnP first, before configuring this feature.*

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

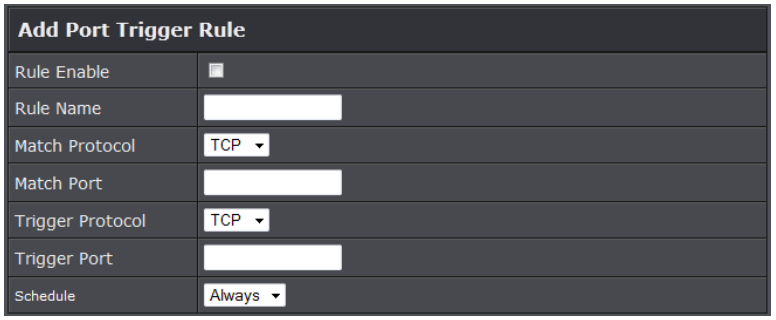
3. Click on the **Firewall** section and click on **Special Applications**.



4. Select **Enable** under **Port Triggering Function**.



5. Review the special application settings. Click **Apply** to save settings.



- **Rule Enable:** Check to enable port triggering rule
- **Rule Name:** Enter the name you would like to assign to the port triggering rule.
- **Match Protocol:** Select the protocol to be forwarded to the device. **TCP** or **UDP.**
- **Match Port:** Enter the ports or port range to be forwarded to the device. (e.g. *2000-2038 ,2200-2210).*
- **Trigger Protocol:** Select the protocol requested by the device. **TCP** or **UDP.**
- **Trigger Port:** Enter the ports or port range requested by the device. (e.g. *554-554 or 6112-6112).*

  Note: *Please refer to the device documentation to determine which ports and protocols are required.*
- **Schedule:** Select the defined schedule you would like to have the rule to be applied (see "Create Schedule" section on page 34).

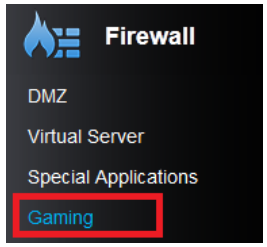
Gaming

Advanced > Firewall > Gaming

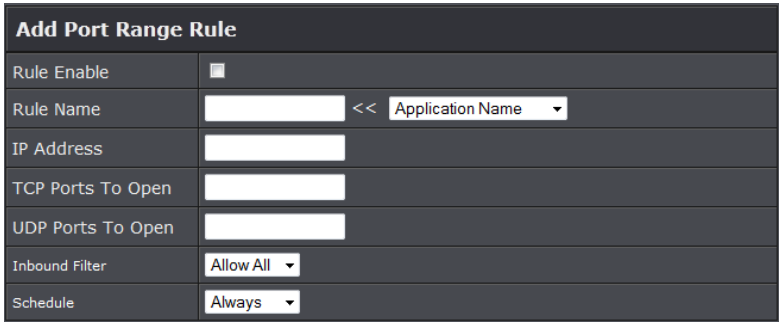
Gaming allows you to define multiple ports (used or required by a specific application or game) and forward them to a single IP address (a computer or device) on your network. Using this feature is more secure compared to using DMZ (see "DMZ" on page 35) in which DMZ forwards all ports instead of only specific ports used by an application. 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 "Identify your network over the Internet" section on page 41).

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Firewall** section and click on **Special Applications**.



4. Review the port range settings. Click **Add** to save settings.



- **Rule Enable:** Check to enable port triggering rule
- **Rule Name:** Enter the name you would like to assign to the port triggering rule or select from a predefine list on the pull down menu.
- **IP Address:** Enter the IP address of the device to forward the port (e.g. *192.168.10.101)*.
- **TCP Ports to Open**: Enter the TCP port you would like to set.
- **UDP Ports to Open**: Enter the UDP port you would like to set.

  Note: *Please refer to the device documentation to determine which ports and protocols are required.* 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.
- **Inbound Filter:** Select the defined inbound filter you would like to apply or select **Allow All**.
- **Schedule:** Select the defined schedule you would like to have the rule to be applied (see "Create Schedule" section on page 34).

Enable/disable Application Layer Gateways (ALG)

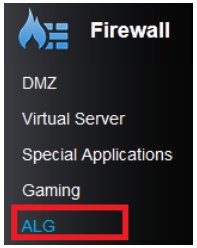
Advanced > Firewall > ALG

You may want to configure your router to allow computers the use of specific high layer applications or service sessions to pass through. Application Layer Gateways (ALG) allows you to easily enable or disable these applications to pass through your router.

Note: *It is recommended to leave these settings enabled.*

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Firewall** section and click on **Special Applications**.



4. Review the applications to enable or disable. Click **Apply** to save the changes.

Application Level Gateway (ALG) Configuration		
Service Name	Description	Enable
Streaming Media	Real Time Streaming Protocol (RTSP)	☑
Streaming Media-VoIP	Session Initiation Protocol(SIP)	☑
Streaming Media-VoIP	NetMeeting (H.323)	☑
File transfer	File Transfer Protocol (FTP)	☑
File transfer	Trivial File Transfer Protocol (TFTP)	☑
IPSec		☑

- **Streaming Media (RTSP):** Allows STMP video protocol through your router.
- **Streaming Media-VoIP (SIP):** Allows SIP protocol through your router.
- **Streaming Media-VoIP (H.323):** Allows H.323 protocol through your router.
- **File Transfer (FTP):** Allows FTP protocol through your router.
- **File Transfer (TFTP):** Allows TFTP protocol through your router.
- **IPSec:** Allows IPSec VPN connections through your router.

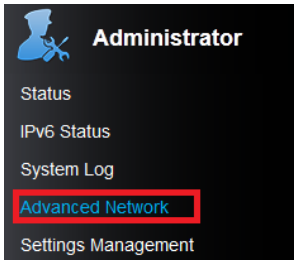
Enable/disable UPnP on your router

Advanced > Advanced Network

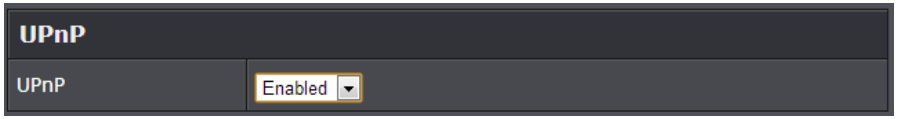
UPnP (Universal Plug and Play) allows devices connected to a network to discover each other and automatically open the connections or services for specific applications (e.g. instant messenger, online gaming applications, etc.) UPnP is enabled on your router by default to allow specific applications 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 15).
2. Click on the **Advanced** tab.

3. Click on the **Administrator** section and click on **Advanced Network**.



4. Click the **UPnP** drop-down list and select **Enabled** to enable UPnP or **Disabled** to disable UPnP. Click **Apply** to save settings.



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.*

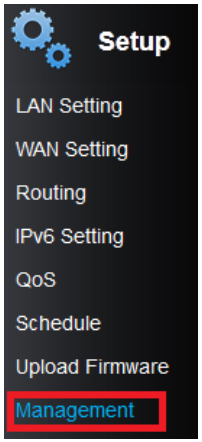
Router Maintenance & Monitoring

Change your router login password

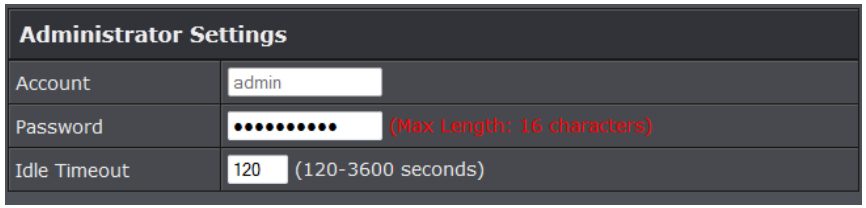
Advanced > Setup > Management

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **Management**.



4. Under the **Administrator Settings** section, in the **Password** field, enter the new password. Click **Apply** to save settings.



- **Idle Timeout:** Enter the idle timeout in seconds before automatically logging you out of the router management page.

  Note: *If you change the router login password, you will need to access the router management page using the User Name "admin" and the new password instead of the default password "admin". If you reset the device to defaults, you will need to access the router management page use the predefined settings on the side or bottom labels.*

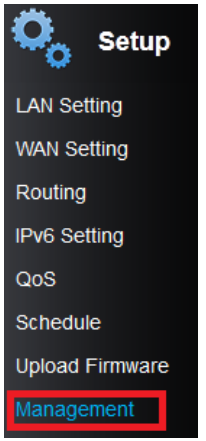
Change your device name

Advanced > Setup > Management

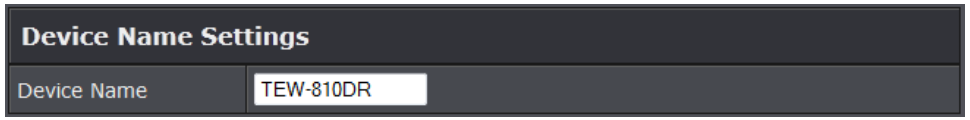
1. Log into your router management page (see "Access your router management page" on page 15).

2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **Management**.



4. Under the **Device Name Settings** section, in the **Device Name** field, enter the new device name to display on your network to identify the router. Click **Apply** to save settings.



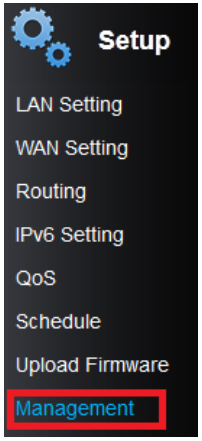
Change your device URL

Advanced > Serup > Management

1. Log into your router management page (see "Access your router management page" on page 15).

2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **Management**.



3. Under the **Device URL Settings** section, in the **Device URL** field, enter the new device URL used to log into the router management page.

Note: *Even if the LAN IP address of the router is changed, the device URL will still allow to use the name as reference to log into the router management page.*

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

Identify your network on the Internet

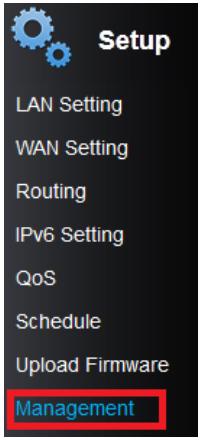
Advanced > Setup > Management

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.

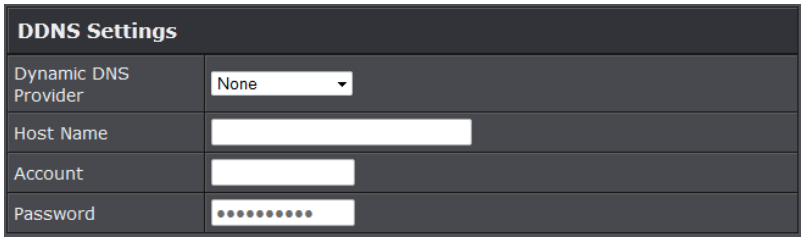
Note: *First, you will need to sign up for one of the DDNS service providers listed in the* ***Server Address*** *drop-down list.*

1. Log into your router management page (see "Access your router management page on page 15").
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **Management**.



4. Review the **DDNS Settings** section. Click **Apply** to save settings.



- **Dynamic DNS Provider:** Click the drop-down list Select your DDNS service.
- **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.

Note: *If you would like to discard the changes, click* ***Cancel*** *before you click* ***Save****.*

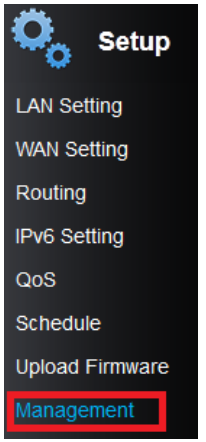
Allow remote access to your router management page

Advanced > Administrator > Management

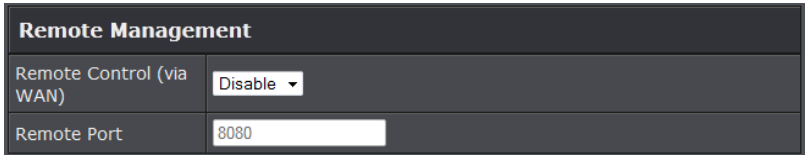
You may want to make changes to your router from a remote location such at your office or another location while away from your home.

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **Management**.



4. Review the setting on **the Remote Management** section. Click **Apply** to save settings



- **Remote Control:** Select enable or disable for the feature.
- **Port:** Enter the port to assign remote access to the router. 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)*

Reset your router to factory defaults

Advance > Administrator > Settings Management

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 51.

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

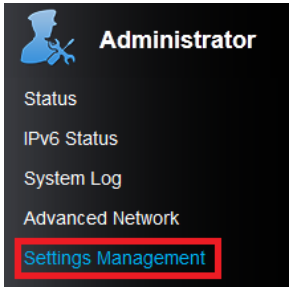
- **Reset Button** – Located on the side panel of your router, see "Product Hardware Features" on page 5. Use this method if you are encountering difficulties with accessing your router management page.

  OR

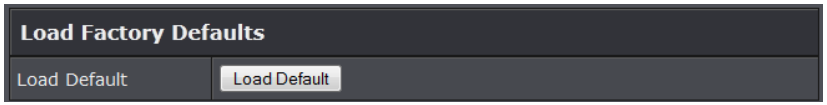
- **Router Management Page**

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Administrator** section and click on **Settings Management**.



4. Under **Load Factory Default**, click **Load Default**. When prompted to confirm this action, click **OK**.



Router Default Settings

Administrator User Name	admin
Administrator Password	Please refer sticker or device label
Router IP Address	192.168.10.1
Router Subnet Mask	255.255.255.0
DHCP Server IP Range	192.168.10.101-192.168.199
Wireless 2.4GHz	Enabled
Wireless 2.4GHz Encryption	Please refer sticker or device label
Wireless 5Ghz	Enabled
Wireless 5GHz Encryption	Please refer sticker or device label

Backup and restore your router configuration settings

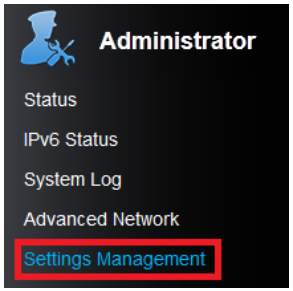
Advanced > Administrator > Settings Management

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.

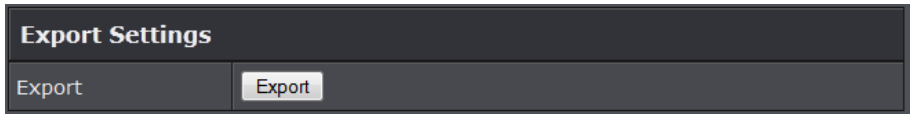
To backup your router configuration:

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Administrator** section and click on **Settings Management**.



4. Under **Export Settings** section, click **Export**.

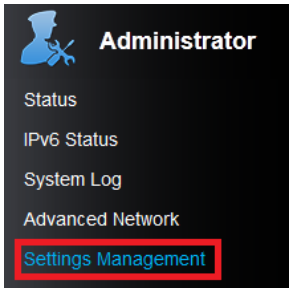


5. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: *.cfg)*

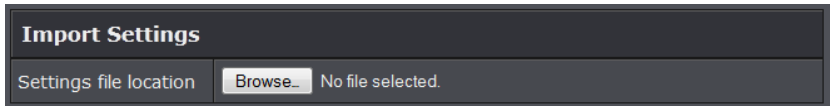
To restore your router configuration:

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Administrator** section and click on **Settings Management**.



4. Under **Import Settings**, next to **Settings file location**, depending on your web browser, click on **Browse** or **Choose File**.



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

Upgrade your router firmware

Advanced > Setup > Upload 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 Administrator section and then on the Status. 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.

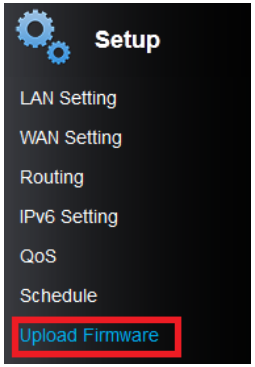
2. Unzip the file to a folder on your computer.

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.

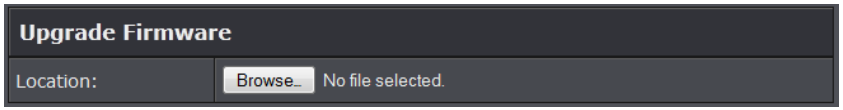
1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Setup** section and click on **Upload Firmware**.



3. Depending on your web browser, in the **Upload Firmware** section, click **Browse** or **Choose File**.

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



5. Click **Apply**. If prompted, click **Yes** or **OK**.

Reboot your router

Administrator > Settings Management

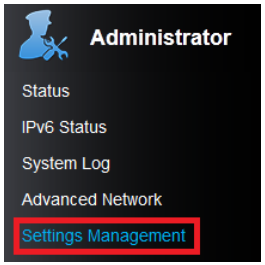
You may want to restart your router if you are encountering difficulties with your router and have attempted all other troubleshooting.

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

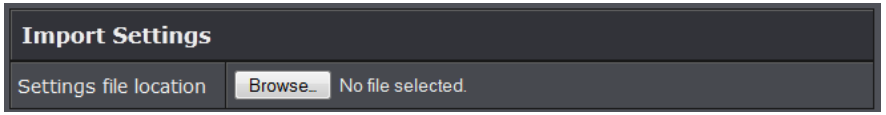
- **Turn the router** off for 10 seconds using the router On/Off switch (EU version only) located on the rear panel of your router or disconnecting the power port, **sees** "Product Hardware Features" on page 5.
  Use this method if you are encountering difficulties with accessing your router management 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.

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Administrator** section and click on **Settings Management**.



3. Under **System Reboot** section, click **Reboot**.



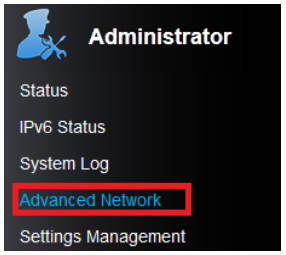
Allow/deny ping requests to your router from the Internet

Advanced > Advanced Network

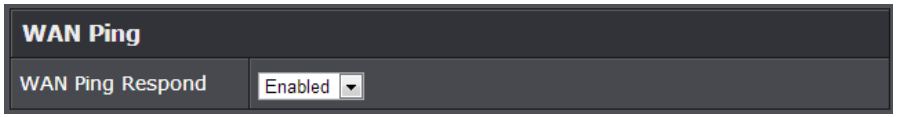
To provide additional security, you may want to disable your router from responding to ping or ICMP (Internet Control Message Protocol) requests from the Internet. A ping is network communication test to check if a device with IP address is alive or exists on the network. By disabling this feature, you can conceal your router's IP address and existence on the Internet by denying responses to ping requests from the Internet. You can additionally use this feature as a tool for troubleshooting purposes.

1. Log into your router management page (see "Access your router management page" on page 15).
2. Click on the **Advanced** tab.

3. Click on the **Administrator** section and click on **Settings Management**.



4. Click the **WAN Ping Respond** drop-down list and select **Enabled** to allow ping requests from your router to the Internet. Click **Apply** to save settings.



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

Note: *If you would like to discard the changes, click* ***Cancel*** *before you click* ***Save****.*

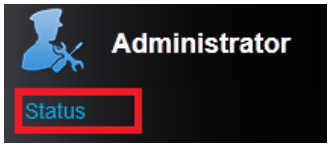
Check the router system information

Advanced > Administrator > Router Status

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 15).
2. Click on the **Advanced** tab.

3. Click on the **Administrator** section and click on **Router Status**.



System Info

System Info	
Firmware Version	1.00, 18, Sep, 2013
System Time	Wed Sep 25 09:44:02 2013
System Up Time	0 Day, 1:23:47

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

Internet Configurations

Internet Configurations	
Connected Type	Dynamic IP (DHCP)
WAN IP Address	192.168.231.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.231.254
Primary Domain Name Server	192.168.231.254
Secondary Domain Name Server	0.0.0.0

- **Connected Type:** The WAN connection type applied on your router.
- **WAN 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.
- **Primary/Secondary Domain Name System:** The current DNS address(es) assigned to your router port or interface configuration.
- **Renew (DHCP WAN Type):** Click this option to renew your WAN IP address.
- **Release (DHCP WAN Type):** Click this option to release the WAN IP address of your router.
- **Connect (PPPoE WAN Type):** Click this option to connect to your DSL ISP
- **Disconnect (PPPoE WAN Type):** Click this option to disconnect from your DSL ISP.

LAN Information

LAN	
MAC Address	D8:E8:97:1E:34:A8
IP Address	192.168.10.1
Subnet Mask	255.255.255.0

- **MAC Address:** The current MAC address of your router's wireless or interface configuration.
- **IP Address:** Displays your router's current IP address.
- **Subnet Mask:** Displays your router's current subnet mask.

2.4GHz Wireless

2.4GHz Wireless	
MAC Address	D8:E8:97:1E:34:A8
Channel	10
Network Name (SSID) / Security Mode	mediatest_TRENDnet / WPA2 Only - PSK
Multiple SSID1 / Security Mode	
Multiple SSID2 / Security Mode	
Guest Network / Security Mode	guest_mediatest / Auto (WPA or WPA2) - PSK

- **MAC Address:** The MAC address of your router's wireless LAN or interface configuration.
- **Channel:** Displays the current wireless channel your router is operating.

- **Network Name (SSID)/ Security Mode:** Displays the current wireless network name assigned to your router and the wireless security applied to the SSID
- **Multiple SSSID/ Security:** Displays the current wireless network name assigned to your router and the wireless security applied to the SSID
- **Guest Network/ Security Mode:** Displays the current wireless network name assigned to your router and the wireless security applied to the SSID

5GHz Wireless LAN

5GHz Wireless	
MAC Address	D8:E8:97:1E:34:AA
Channel	149
Network Name (SSID) / Security Mode	5GHzmediatest_TRENDnet / disable
Multiple SSID1 / Security Mode	
Multiple SSID2 / Security Mode	
Guest Network / Security Mode	

- **MAC Address:** The MAC address of your router's wireless LAN or interface configuration.
- **Channel:** Displays the current wireless channel your router is operating.
- **Network Name (SSID)/ Security Mode:** Displays the current wireless network name assigned to your router and the wireless security applied to the SSID
- **Multiple SSSID/ Security:** Displays the current wireless network name assigned to your router and the wireless security applied to the SSID
- **Guest Network/ Security Mode:** Displays the current wireless network name assigned to your router and the wireless security applied to the SSID

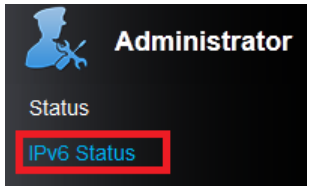
IPv6 Status

Advanced > Administrator > IPv6 Status

You can view the current IPv6 status on your router.

1. Log into your router management page (see "Access your router management page on page 15").
2. Click on the **Advanced** tab.

3. Click on the **Administrator** section and click on **IPv6 Status**.



IPv6 Connection Information

IPv6 Connection Information	
IPv6 Connection Type	Auto Configuration (SLAAC/DHCPv6)
Network Status Address	Disconnected

- **IPv6 Connection Type:** The type of IPv6 being used on your router.
- **Network Type Status:** Your IPv6 network status.
- **Renew (DHCP WAN Type):** Click this option to renew your WAN IP address.
- **Release (DHCP WAN Type):** Click this option to release the WAN IP address of your router.

WAN IPv6 Address	
IPv6 Default Gateway	
LAN IPv6 Address	
LAN IPv6 Link-Local Address	fe80::dae8:97ff:fe1e:34a8/64
Primary DNS Server	
Secondary DNS Server	

- **WAN IPv6 Address:** Your IPv6 WAN IP address
- **IPv6 Default Gateway:** IPv6 default gateway
- **Network Prefix:** IPv6 prefix used
- **Primary/Secondary IPv6 DNS Server:** IPv6 DNS server

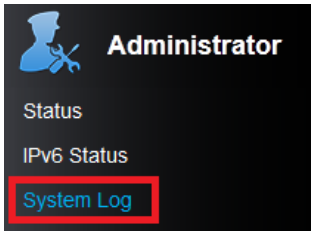
View your router log

Administrator > System Log

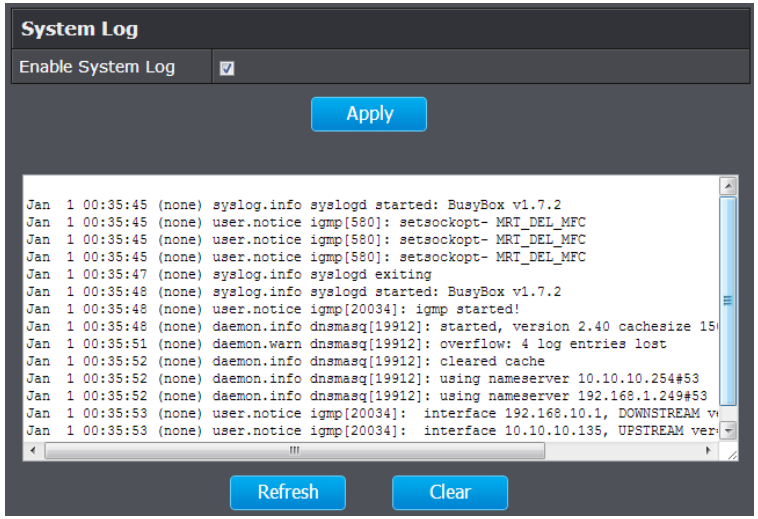
Your router log can be used to obtain activity information on the functionality of your router or for troubleshooting purposes.

1. Log into your router management page (see "Access your router management page on page 15").
2. Click on the **Advanced** tab.

3. Click on the **Administrator** section and click on **System Log**.



4. Select **Enable System Log** and click Apply to save settings.



- **Refresh:** Click to refresh screen.
- **Clear:** Click to clear the screen.

Router Management Page Structure

BASIC

Network Status

- Internet Status
- Guest Network Status
- Wireless
- Connected Devices

Wireless

- 2.4 GHz Wireless Network
- Security
- 5GHz Wireless Network
- Security

Guest Network

- 2.4 GHz Guest Network
- Security
- 5GHz Guest Network
- Security

Parental Control

- Web URL Filter

ADVANCE

Administrator

- Status
- IPv6 Status
- System Log
- Advanced Network
- Settings Management
    - Export Settings
    - Import Settings
    - Load Factory Default
    - Reboot
- Time

Setup

- LAN Setting
    - DHCP Server
    - DHCP Reservations
- WAN Setting
    - Clone MAC
- Routing
    - RIP
- IPv6 Setting
- QoS
- Schedule
- Upload Firmware
- Management
    - Password
    - Device URL
    - Device Name
    - DDNS Settings
    - Remote Management
- Wizard

Wireless 2.4GHz

- WDS
- Advanced
- Multiple SSID
- Security
    - Wireless MAC filter
- WPS
- Station List

Wireless 5GHz

- WDS
- Advanced
- Multiple SSID
- Security
    - Wireless MAC filter
- WPS
- Station List

Security

- Access Control
    - Port Filter
    - IP Filter
    - MAC Filter
    - Website Filter
- Inbound Filter

Firewall

- DMZ
- Virtual Server Rules
- Special Applications
- Gaming
- ALG

Technical Specifications

Hardware	
Standards	Wired: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), IEEE 802.3ab (1000Base-T) Wireless: IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, 802.11a
Internet Protocol	IPv4 and IPv6
LAN	4 x 10/100Mbps Auto-MDIX
WAN	1 x 10/100 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 routing, UPnP, DHCP, server, Dynamic DNS (DynDNS.com), NTP, VPN/RTSP/SIP pass through, IPv6
Quality of Service	WMM and Internet Bandwidth Control (Configurable Upload / Download)
Firewall	NAT, SPI, DMZ host, virtual server, port forwarding MAC, IP and URL filter, Schedules (wireless, MAC filter, virtual server, port forwarding, firewall rule, application rule, guest network, and URL filter), Inbound IP filter (virtual server)
Management / Monitoring	Local / remote configuration, upgrade firmware, backup / restore configuration via web browser, internal system log (Categories: System, Firewall & Security, Router Status / Filter: Critical, Warning, Information), syslog, email log, active sessions,
Supported Web Browser	Internet Explorer 8.0 or above, Firefox, Chrome, Opera, Safari
LED Indicator	Power, WAN (Internet), Wireless, WPS, USB
Power Adapter	Input: 100 ~ 240 V, 50~60 Hz, 0.3 A
	Output: 12 V DC, 1A external power adapter
Power Consumption	8 watts (max.)
Dimension (L x W x H)	151 x 113 x 60 mm (5.9 x 4.4 x 2.3 in.)
Weight	255 g (9 oz)
Temperature	Operation: 0°~ 40°C (32°F~ 104°F)
Humidity	Max. 95% (non-condensing)
Certifications	CE, FCC
Wireless	
Frequency	2.4 GHz: 2.412~2.472 5 GHz: 5.1805 ~ 5.805
Modulation	CCK, DQPSK, DBPSK, OFDM, BPSK, QPSK, 16/64-QAM
Data Rate	802.11a: up to 54 Mbps 802.11b: up to 11 Mbps 802.11g: up to 54 Mbps 802.11n: up to 300 Mbps (for 2.4GHz) 802.11n: up to 150 Mbps (for 5 GHz) 802.11ac: up to 433 Mbps
Security	64/128-bit WEP, WPA/WPA2-PSK, WPA/WPA2-RADIUS
Guest network	1 per wireless band, access control between 2.4GHz and 5GHz guest zones
Output Power	802.11a: 15 dBm (typical) @ 54 Mbps 802.11b: 26 dBm (typical) @ 11 Mbps 802.11g: 22 dBm (typical) @ 54 Mbps 802.11n: 22 dBm (typical) @ 300 Mbps (for 2.4 GHz) 802.11n: 15 dBm (typical) @ 150 Mbps (for 5 GHz) 802.11ac: 12 dBm (typical) @ 433 Mbps

Receiving Sensitivity	802.11a: -72 dBm (typical) @ 54 Mbps 802.11b: -90 dBm (typical) @ 11 Mpbs 802.11g: -75 dBm (typical) @ 54 Mbps 802.11n: -70 dBm (typical) @ 300 Mbps (for 2.4 GHz) 802.11n: -70 dBm (typical) @ 150 Mbps (for 5 GHz) 802.11ac: -56 dBm (typical) @ 433 Mbps
Channels	2.4 GHz: 1~11 (FCC), 1~13 (ETSI) 5 GHz: 36, 40, 44, 48, 149, 153, 157, 161, 165 (FCC) 36, 40, 44, 48 (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 15 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 problems.

Appendix

How to find your IP address?

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

Command Prompt Method

Windows 2000/XP/Vista/7

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

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,

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

1. Open Connect to a Network by clicking the network icon ( or ) in the notification area.

2. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect.**

4. You may be prompted to enter a security key in order to connect to the network.

5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows Vista

1. Open Connect to a Network by clicking the **Start Button**.  and then click **Connect To.**

2. In the **Show** list, click **Wireless**.

3. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect.**

4. You may be prompted to enter a security key in order to connect to the network.

5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows XP

1. Right-click the network icon in the notification area, then click **View Available Wireless Networks**.

2. In **Connect to a Network**, under **Available Networks**, click the wireless network you would like to connect to.

3. You may be prompted to enter a security key in order to connect to the network.

4. Enter in the security key corresponding to the wireless network, and click **Connect**.

Federal Communication Commission Interference Statement

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

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

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

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

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, 2006/95/EC and 2009/125/EC.

Regulation (EC) No. 1275/2008
Regulation (EC No. 278/2009
EN60950-1 : 2006+A11 : 2009

Safety of Information Technology Equipment

EN 300 328 V1.7.1 : (2006-10)

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.9.2 : (2011-09)

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V2.2.1 : (2012-09)

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for 2,4 GHz wideband transmission systems, 5 GHz high performance RLAN equipment and 5,8 GHz Broadband Data Transmitting Systems

EN 301 893 V1.6.1 : (2011-11)

Broadband Radio Access Networks (BRAN);5 GHz high performance RLAN;Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive

This device is a 2.4/5G GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

cs Česky [Czech]	TRENDnet tímto prohlašuje, že tento TEW-810DRU je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-810DRU overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TEW-810DRU in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEW-810DRU vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, TRENDnet, declares that this TEW-810DRU is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Español [Spanish]	Por medio de la presente TRENDnet declara que el TEW-810DRU cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑTRENDnet ΔΗΛΩΝΕΙ ΟΤΙTEW-810DRU ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente TRENDnet déclare que l'appareil TEW-810DRU est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano[Italian]	Con la presente TRENDnet dichiara che questo TEW-810DRU è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
lv Latviski [Latvian]	AršoTRENDnetdeklarē, ka TEW-810DRU deklarē, ka [type of equipment / iekārtas tips] atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
lt Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TEW-810DRU atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEW-810DRU in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TEW-810DRU jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-810DRU megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEW-810DRU] jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	TRENDnet declara que este TEW-810DRU está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEW-810DRU v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
sk Slovensky [Slovak]	TRENDnettýmtovyhlasuje, že TEW-810DRU spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	TRENDnet vakuuttaa täten että TEW-810DRU tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar TRENDnet att denna TEW-810DRU står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

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-810DRU – 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, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

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

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

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 2013/9/26

TRENDnet®

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