

User's Guide

TRENDNET[®]



AC3200 Tri Band Wireless Router

TEW-828DRU

Table of Contents

Product Overview	1
Package Contents	1
Features	1
Application Diagram	3
Router Setup.....	4
Creating a Home Network	4
Router Installation	5
Connect additional wired devices to your network.....	8
Basic Router Settings.....	9
Access your router management page.....	9
Network Status	9
Wireless Settings	10
Guest Network.....	13
Parental Control.....	15
Website Filter.....	15
IP Address Filter	16
MAC Address Filter	17
Wireless Networking and Security	18
How to choose the type of security for your wireless network	18
Secure your wireless network	19
Connect wireless devices to your router	21
Connect wireless devices using WPS	21
Advanced wireless settings.....	23
Multiple SSID.....	23
Wireless bridging using WDS (Wireless Distribution System)	24
Advanced Settings	26

Steps to improve wireless connectivity	27
Advanced Router Settings	28
Change your router login password	28
Manually configure your Internet connection	28
Change your device name	29
Change your device URL	29
IPv6 Settings	29
Clone a MAC address	30
Change your router IP address	30
Set up the DHCP server on your router	31
Set up DHCP reservation	32
Enable/disable UPnP on your router	33
Enable/disable Application Layer Gateways (ALG).....	33
Identify your network on the Internet	34
Set your router date and time	35
Create schedules	36
Access Control (IP Protocol Filter)	37
Protocol/IP Filter.....	37
Quality of Service.....	38
Open a device on your network to the Internet.....	39
DMZ	39
Virtual Server	39
Special Applications	41
Gaming.....	42
Allow remote access to your router management page	43
Add static routes	43
VLAN Configuration	44
Using External USB Storage	45

Samba Server 45

DLNA Server 46

FTP (File Transfer Protocol) Server 47

Virtual Private Networking (VPN)48

 Creating a Virtual Private Network..... 48

Router Maintenance & Monitoring.....53

 Reset your router to factory defaults 53

 Router Default Settings 53

 Backup and restore your router configuration settings 54

 Reboot your router 54

 Upgrade your router firmware 55

 Allow/deny ping requests to your router from the Internet 56

 Client List 56

 Check the router system information..... 57

 View your router log 59

Router Management Page Structure60

Technical Specifications 61

Appendix 64

Product Overview



TEW-828DRU

Package Contents

In addition to your router, the package includes:



Power adapter (12V, 3.5A)



CD-ROM with User's Guide



RJ-45 Ethernet cable (1.5m / 5ft.)



Multi- Language Quick Installation Guide

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

Features

TRENDnet's extreme performance AC3200 Tri Band Wireless Router, model TEW-828DRU, produces three concurrent wireless networks—two separate 1300 Mbps Wireless AC networks and a 600 Mbps Wireless N network. Smart Connect technology automatically groups slower and faster AC devices to separate WiFi AC bands. High performance Gigabit ports, a 1 GHz dual core processor, six high gain antennas, high power amplifiers, and a SuperSpeed USB 3.0 share port deliver extraordinary networking speed and range.

Easy Setup

Get up and running in minutes with the intuitive guided setup

Simultaneous Tri Band

Three concurrent WiFi bands maximize device networking speeds: two separate extreme performance 1300 Mbps Wireless AC networks and a 600 Mbps Wireless N network

Smart Connect Technology

Smart Connect technology virtually combines the two separate WiFi AC bands, so that only one WiFi AC network is visible, while managing each band individually. Slower and faster WiFi AC devices are grouped together and automatically assigned to the two separate WiFi AC bands, thereby optimizing networking speeds

Pre-Encrypted Wireless

For your convenience the router's WiFi bands are pre-encrypted with their own unique passwords

Wireless Coverage

High performance amplifiers and six high gain antennas maximize wireless coverage

Gigabit Ports

Gigabit ports support high performance wired connections

USB 3.0/2.0 Share Ports

Plug in a USB 3.0 flash or storage drive into the SuperSpeed USB 3.0 or the USB 2.0 share port

Guest Network

Create an isolated network for guest internet access only

Parental Controls

Control access to specific websites

One Touch Connection

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

Targeted Beamforming

Increased real-time performance by directing stronger wireless signals to your specific location

1 GHz Processor

Extreme performance 1 GHz dual core processor optimizes networking throughput

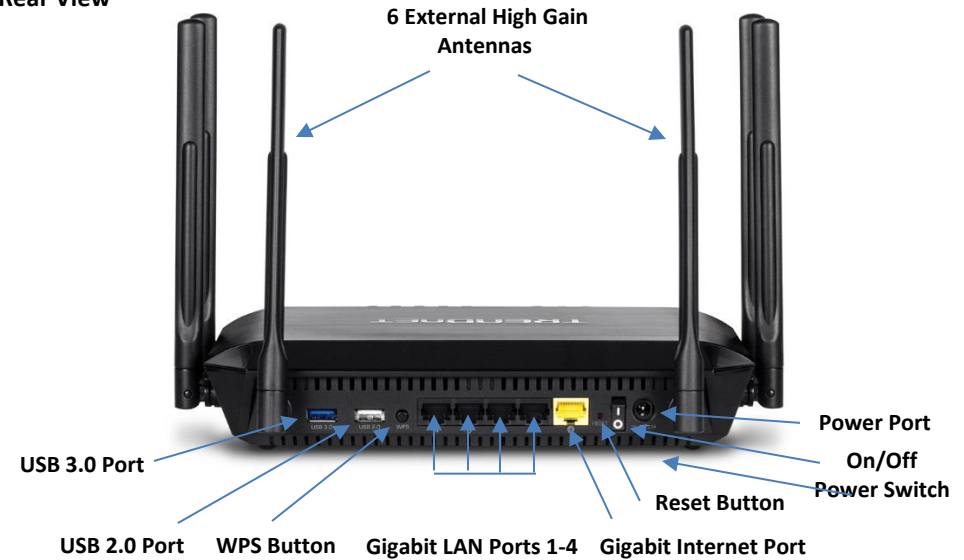
VPN Support

Secure remote access to the router with OpenVPN support

*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and cover-age will vary depending on interference, network traffic, building materials and other conditions. For maximum performance of up to 1.3 Gbps use with a 1.3 Gbps 802.11ac wireless adapter. 802.11n 2.4 GHz TurboQAM speeds requires clients with TurboQAM support.

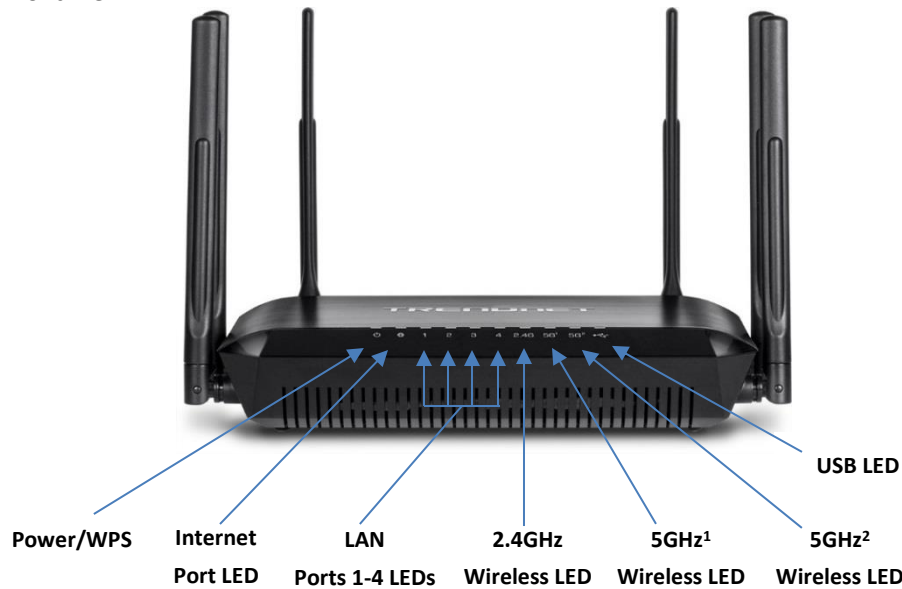
Product Hardware Features

Rear View



No	Item	Description
1	USB 3.0 Port	Connect USB storage devices to share over the network via FTP or Windows® SMB/CIFS, Samba.
2	USB 2.0 Port	Connect USB storage devices to share over the network via FTP or Windows® SMB/CIFS, Samba.
3	WPS Button (Wi-Fi Protected Setup)	Push and hold this button for 3 seconds to activate WPS. The Power LED will blink when WPS is activated.
4	LAN Ports 1-4	Connect Ethernet cables (also called network cables) from your router LAN ports to your wired network devices.
5	Internet Port	Connect an Ethernet cable from your router Internet port to your modem.
6	On/Off Power Switch	Push the router On/Off power switch to turn your router "On" (-) or "Off" (O).
7	Power Port	Connect the included power adapter from your router power port and to an available power outlet.
8	Reset Button	Press and hold this button for 10 seconds to reset the router.

Front View



No	Item	Description
1	Power/WPS LED	Solid Blue – Device is on Blinking Blue – WPS is activated. Off – No power
2	Internet Port LED	Solid Blue – Internet port is physically connected Blinking Blue – Data Transmit/Receive. Off – Internet port is physically disconnected.
3	LAN Ports 1-4 LEDs	Solid Blue – LAN port is physically connected Blinking Blue – Data Transmit/Receive. Off – LAN port is physically disconnected.
4	2.4GHz/5GHz ¹ /5GHz ² Wireless LED	Solid Blue – 2.4GHz/5GHz ¹ /5GHz ² radio is on. Blinking Blue – Data Transmit/Receive. Off – 2.4GHz/5GHz ¹ /5GHz ² radio is off.
5	USB LED	Solid Blue – USB device is connected. Blinking Blue – Data Transmit/Receive. Off – No USB device connected.

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. Using the Smart Connect feature, the two 5GHz radios improve bandwidth congestion by automatically assigning higher speed capable 5GHz wireless devices to one radio and slower legacy 5GHz wireless devices to the other.



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 8.
5. To set up wireless security on your router, see "[Wireless Networking and Security](#)" on page 18.

How to setup your router

Refer to the Quick Installation Guide or continue to the next section "[Router Installation](#)" on page 5 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 (Dynamic IP/DHCP)

Host Name: _____ (Optional, if required by ISP for Compatibility)
Primary DNS Server Address: _____. _____. _____. _____. _____. _____. (Optional)
Secondary DNS Servers Address : _____. _____. _____. _____. _____. _____. (Optional)
MAC Address: __:__:__:__:__:__ Clone your PC MAC Address (Optional)

2. Static IP/Fixed IP address

IP Address: _____. _____. _____. _____. _____. _____. (e.g. 215.24.24.129)
Subnet Mask: _____. _____. _____. _____. _____. _____.
Default Gateway IP Address: _____. _____. _____. _____. _____. _____.
Primary DNS Server Address: _____. _____. _____. _____. _____. _____.
Secondary DNS Servers Address : _____. _____. _____. _____. _____. _____. (Optional)
MAC Address: __:__:__:__:__:__ Clone your PC MAC Address (Optional)

3. PPPoE

Username: _____
Password: _____
On Demand Mode: Enabled/Disabled (Optional)
Max. Idle Time (On Demand Mode Enabled): _____ (seconds)
Keep Alive Mode: Enabled/Disabled (Optional)
MTU: _____ (Default: 1500, change if required by ISP)
MAC Address: __:__:__:__:__:__ Clone your PC MAC Address (Optional)

4. PPTP

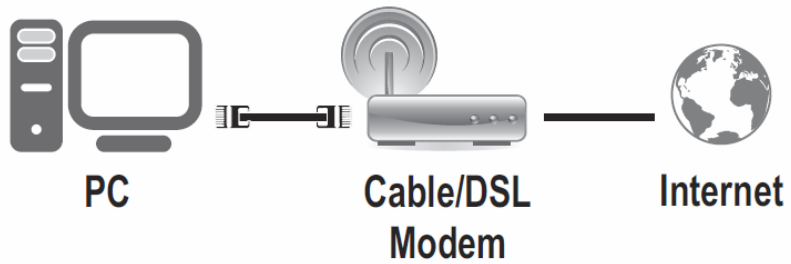
Protocol of Physical Connection (Dynamic IP/DHCP or Static IP)
PPTP Server: _____ (e.g. 215.24.24.150)
PPTP IP Address (Static IP): _____. _____. _____. _____. _____. _____. (e.g. 215.24.24.129)
PPTP Subnet Mask (Static IP): _____. _____. _____. _____. _____. _____. (e.g. 255.255.255.0)
PPTP Gateway (Static IP): _____. _____. _____. _____. _____. _____. (e.g. 215.24.24.1)
Username: _____
Password: _____
On Demand Mode: Enabled/Disabled (Optional)
Max. Idle Time (On Demand Mode Enabled): _____ (seconds)
Keep Alive Mode: Enabled/Disabled (Optional)
DNS Servers Address 1 (Static IP): _____. _____. _____. _____. _____. _____.
DNS Servers Address 2 (Static IP): _____. _____. _____. _____. _____. _____.
MTU: _____ (Default: 1500, change if required by ISP)
MAC Address: __:__:__:__:__:__ Clone your PC MAC Address (Optional)

5. PPTP

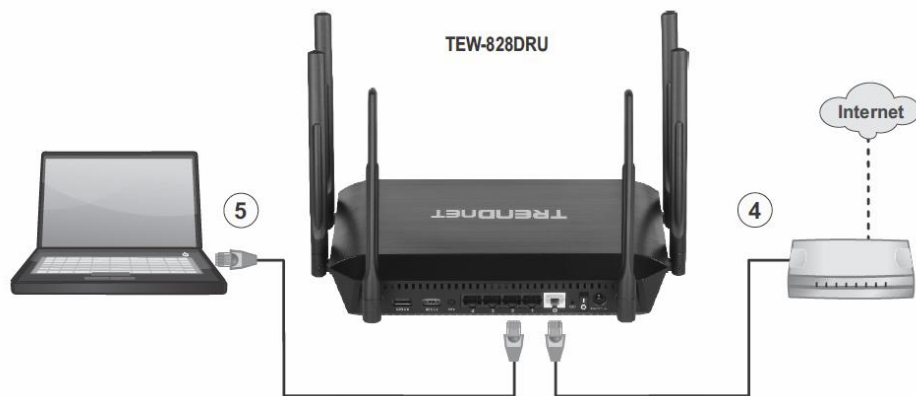
Protocol of Physical Connection (Dynamic IP/DHCP or Static IP)
PPTP Server: _____ (e.g. 215.24.24.150)
PPTP IP Address (Static IP): _____. _____. _____. _____. _____. _____. (e.g. 215.24.24.129)
PPTP Subnet Mask (Static IP): _____. _____. _____. _____. _____. _____. (e.g. 255.255.255.0)
PPTP Gateway (Static IP): _____. _____. _____. _____. _____. _____. (e.g. 215.24.24.1)
Username: _____
Password: _____
On Demand Mode: Enabled/Disabled (Optional)
Max. Idle Time (On Demand Mode Enabled): _____ (seconds)
Keep Alive Mode: Enabled/Disabled (Optional)
DNS Servers Address 1 (Static IP): _____. _____. _____. _____. _____. _____.
DNS Servers Address 2 (Static IP): _____. _____. _____. _____. _____. _____.
MTU: _____ (Default: 1500, change if required by ISP)
MAC Address: __:__:__:__:__:__ Clone your PC MAC Address (Optional)

Hardware Installation

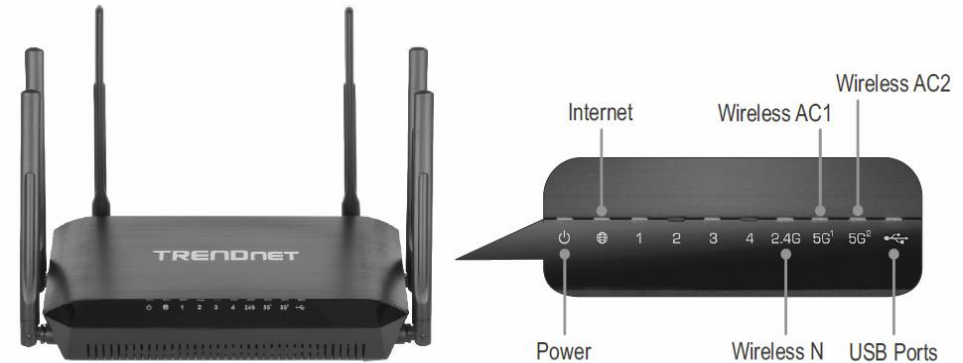
1. Verify that you have an Internet connection when connecting your computer directly to your modem.



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. Position the antennas as shown for optimal wireless coverage.



6. Connect your computer to one of the router LAN ports.
7. Connect the power adapter to the router and then to a power outlet. Switch the power on/off switch to the On position (-).
9. Turn on your modem.
10. Verify that the status LED indicators on the front of the router are illuminated: **Power, Internet, Wireless N, Wireless AC1, Wireless AC2.**



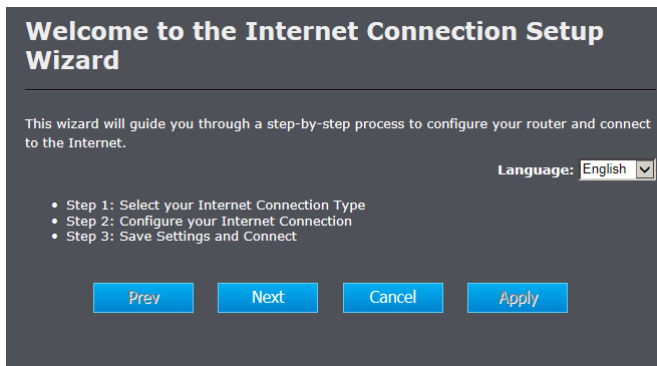
Setup Wizard

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and the wizard will automatically appear.

Note: If you have already configured your router before, the wizard will no longer appear automatically. In your web browser, go to <http://tew-828dru> or you can access the router management using the default IP address <http://192.168.10.1>. Your router will prompt you for a user name and password. Enter your user name and password and click **Advanced > Setup > Wizard**.

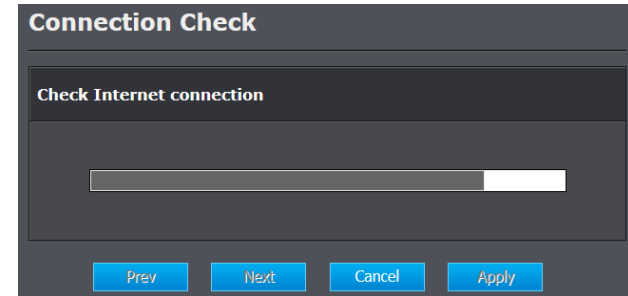


2. Click the Select your Language and click **Next**.



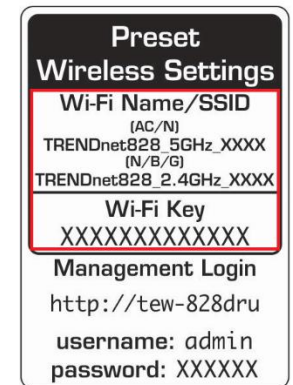
3. If the wizard is unable to detect your Internet connection type, you will be prompted to select your Internet connection type and configure your Internet settings. Select your Internet connection type and click **Next**.

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



4. Confirm your settings. This window displays your predefined router wireless settings and click **Apply** to complete the wizard. At the prompt, click **OK**.

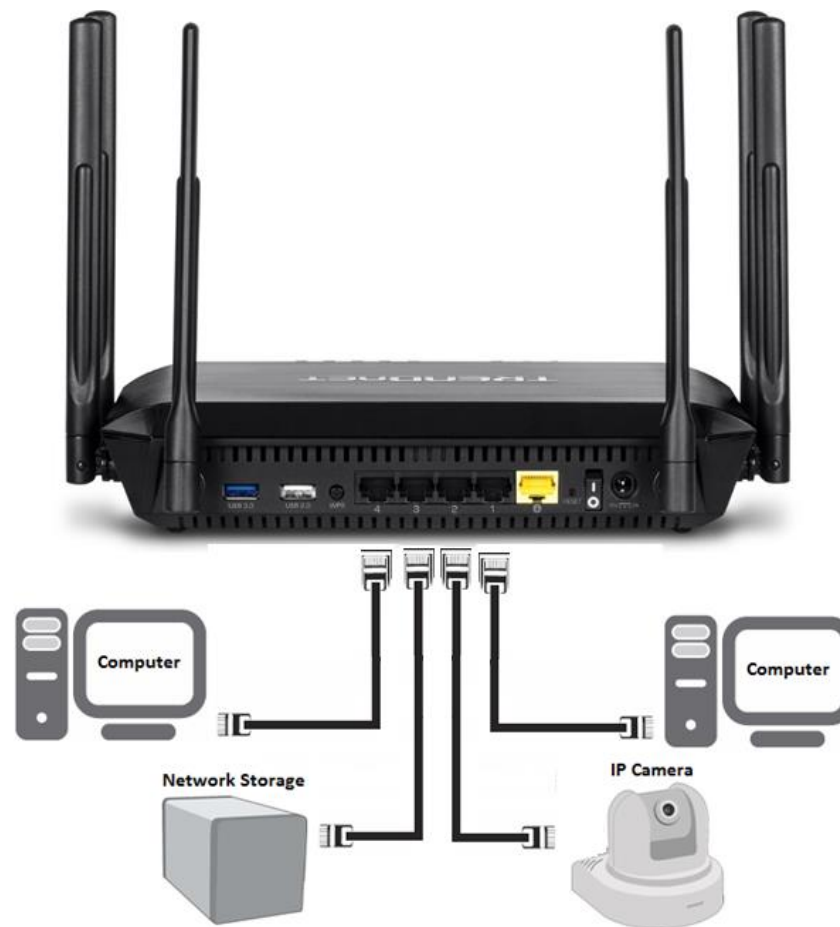
Note: For added security, the router wireless network is pre-encrypted with its own unique wireless network security key. You can find the unique network security key and the pre-assigned network name (SSID) on a sticker on the side of the router and on a label on the bottom of the router. You will need this information to connect to the router. To change the network security key, refer to page 19 "[Secure your wireless network](#)". If the router is reset to factory defaults, the wireless encryption will reset to the network security key printed on the product labels of the router.



Connect additional wired devices to your network

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

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



Basic Router Settings

Access your router management page

Note: Your router management page URL/domain name <http://tew-828dru> or IP address <http://192.168.10.1> is accessed through the use of your Internet web browser (e.g. Internet Explorer®, Firefox®, Chrome™, Safari®, Opera™) and will be referenced frequently in this User's Guide.

1. Open your web browser and go to URL/domain name <http://tew-828dru> 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 top of the router and on the label on the bottom of the router. Enter your **Username** and **Password**, select your preferred language, then click **Login**.

User Name: **admin**

Password: **(xxxxxxxx)**

Note: User Name and Password are case sensitive.

TEW-828DRU LOGIN

User Name:	<input style="width: 90%;" type="text"/>
Password:	<input style="width: 90%;" type="password"/>
Language:	English ▼

Login

Preset Wireless Settings

Wi-Fi Name/SSID

(AC/N)
TRENDnet828_5GHz_XXXX

(N/B/G)
TRENDnet828_2.4GHz_XXXX

Wi-Fi Key
XXXXXXXXXXXXXX

Management Login
<http://tew-828dru>

username: admin

password: XXXXXX

Network Status

Basic > Network Status

This section displays a brief summary of the router's basic settings and the connected devices.

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Basic** and click on **Network Status**.

Network Status

Internet

Internet connected

Wireless

2.4GHz SSID:
TRENDnet828_2.4GHz_1A2B

5GHz¹ SSID:
TRENDnet828_5GHz_1A2B

5GHz² SSID:
TRENDnet828_5GHz_1A2B

2.4GHz: WPA2-PSK
5GHz¹: WPA2-PSK
5GHz²: WPA2-PSK

Guest Network

2.4GHz Guest SSID:
Disabled

5GHz¹ Guest SSID:
Disabled

5GHz² Guest SSID:
Disabled

Connected Devices

PM-HP4525S

USB

No USB devices connected



Internet: The Internet icon displays green to indicate that your router has successfully established an Internet connection. The Internet icon displays orange to indicate that a physical connection has been established on the Internet port of the router but with no successful Internet connection has been established. The Internet icon displays red to indicate that the Internet is physically disconnected.



Guest Network: The Guest Network icon displays orange to indicate that there are no wireless guest networks currently enabled. The Guest Network icon will display green to indicate that you have at least one wireless guest network currently enabled.



USB: The USB icon displays orange to indicate that there are no USB devices connect to the USB port(s). The USB icon displays green to indicate that are USB devices connected to the USB port(s).



Wireless: The wireless icon displays green to indicate that wireless is enabled on both 2.4GHz and 5GHz bands. The wireless icon displays orange to indicate that only wireless band is enabled (2.4GHz or 5GHz). The wireless icon will display red to indicate that wireless is disabled on both 2.4GHz and 5GHz bands.



Wireless Security: The wireless security section will display the current security settings configured for your wireless networks. It is strongly recommended to enable security on your wireless networks.



Connected Devices: The connected devices section displays the list of network devices currently connected to your router.

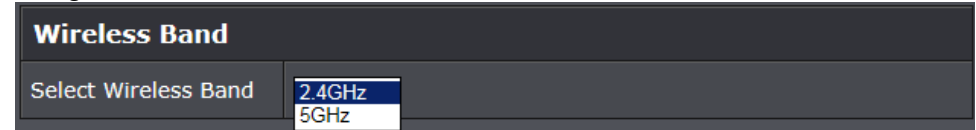
Wireless Settings

Basic > Wireless (2.4GHz or 5GHz (5GHz¹ and 5GHz²))

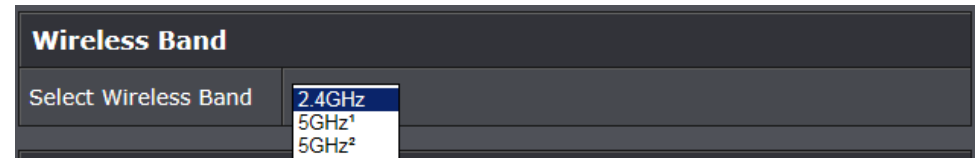
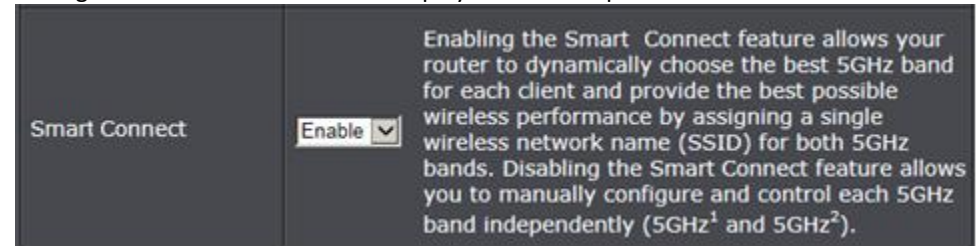
This section outlines available management options under basic wireless sub tab for both 2.4GHz and 5GHz wireless sections. You can refer to the page 15 [Wireless Networking & Security](#) to configure your wireless security settings.

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Basic** and click on **Wireless** (2.4GHz or 5GHz (or 5GHz¹and 5GHz²)).
3. Click the **Select Wireless Band** drop-down list to select the wireless band you would like to configure. 2.4GHz, 5GHz (5GHz¹ or 5GHz²)

The **Select Wireless Band** drop-down list will allow you to select which band to configure.



By default, the Smart Connect feature is enabled which will display only one 5GHz band to configure since both 5GHz¹and 5GHz² will operate together to automatically assign high speed and legacy clients in order to optimize bandwidth and speed. Disabling the Smart Connect feature under the 5GHz wireless settings will allow each 5GHz band to be configured individually and operate independently of one another in the router management interface and will be displayed in the drop-down list as 5GHz¹and 5GHz².



3. Please review the settings below. To save changes to this section, click **Apply** when finished.

- **Enabled** – Check the box to enable the wireless radio. Uncheck to disable the wireless radio. **Note:** *It is recommended to keep wireless radios enabled.*

Enabled



- **Wireless Network 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.

Wireless Name (SSID)

TRENDnet828_5GHz_1A2B

Wireless Mode: When applying the Wireless Mode setting, please keep in mind the following:

- Wireless devices that support 802.11n are backwards compatible and can connect wirelessly at 802.11g or 802.11b.
- Wireless devices that support 802.11ac are backwards compatible and can connect wirelessly at 802.11n or 802.11a.
- 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.
- Connecting at 802.11a or 802.11n will limit the capability of your 802.11ac 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.
- Allowing 802.11a or 802.11n devices to connect to an 802.11ac capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11ac.

802.11 Mode

802.11b/g/n mixed
802.11b/g only

802.11 Mode

802.11a/n/ac mixed
802.11a/ac only

- **Broadcast Network Name (SSID)**

- **Enabled (Recommended)** - 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.

Broadcast Network Name (SSID)

Enabled

- **Frequency (Channel)** – Selecting the **Auto** option will set your router to scan for the appropriate wireless channel to use automatically. The **Auto** option is only available for 2.4GHz and is not available for 5GHz channel settings. 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.

Frequency (Channel)

Auto

- **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, select **Auto 20/40MHz** (Options: 20MHz or Auto 20/40MHz). It is recommended to use the default channel bandwidth settings. For greater 802.11ac performance, select **Auto 20/40/80MHz** (Options: 20MHz, Auto 20/40MHz, Auto 20/40/80MHz). It is recommended to use the default channel width settings.

Note: *Please note that the default settings may provide more stability than the higher channel bandwidth settings such as Auto 20/40/80MHz 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 20/40MHz (Auto) for connectivity in busy wireless environments where there are several neighboring wireless networks in the area.
- **Auto 20/40MHz (11n) or Auto 20/40/80MHz (11ac)** –When this setting is active, this mode is capable of providing higher performance only if the wireless devices support the channel width settings.

Enabling Auto 20/40MHz or Auto 20/40/80 MHz typically results in substantial performance increases when connecting an 802.11ac/n wireless client.

Channel BandWidth
 20 MHz
 Auto 20/40 MHz

Channel BandWidth
 20 MHz
 Auto 20/40 MHz
 Auto 20/40/80 MHz

Schedule: The schedule function allows you to define a schedule when the wireless should be turned on. To define a new schedule, click **Add New** and refer to page 36 "[Create Schedules](#)". After you have created a new schedule, you will be returned to the page to apply the new schedule. If you encounter issues, click the drop-down list and the new schedule will be available for selection. **Note:** *Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 35 to configure [Time Settings](#) and see page 36 "[Create Schedules](#)" to create a schedule.*

Schedule

Guest Network

Basic > Guest Network (2.4GHz or 5GHz¹ or 5GHz²)

Creating an isolated and separate wireless guest network (2.4GHz or 5GHz¹ or 5GHz²) 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 9).
2. Click on **Basic** and click on **Guest Network**.
3. Click **Select Wireless Band** drop-down list will allow you to select which band to configure for the guest network.

Wireless Band	
Select Wireless Band	2.4GHz 5GHz ¹ 5GHz ²

3. Review the Guest Zone settings, click **Apply** when finished.

- **Enabled** – Check this option to enable the wireless guest network.

Enabled	<input type="checkbox"/>
---------	--------------------------

- **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.

Wireless Name (SSID)	TRENDnet828_5GHz1_guest
----------------------	-------------------------

- **Wireless Client Isolation** – When this option is checked, wireless client devices connected to your guest network(s) will be restricted from accessing other guests.

Wireless Client Isolation	<input type="checkbox"/> (isolate guests from each other)
---------------------------	-----------------------------------------------------------

- **Internet Access Only** – When this option is checked, wireless client devices connected to your guest network(s) will be restricted from accessing your private LAN and wireless clients connected to your primary wireless network, Internet access only. If unchecked, allows wireless client devices connected your guest network(s) complete access to your private LAN, primary wireless network, and Internet.

Internet Access Only	<input checked="" type="checkbox"/> (prevents guests from accessing the private LAN network)
----------------------	----------------------------------------------------------------------------------------------

Schedule: The schedule function allows you to define a schedule when the wireless should be turned on. To define a new schedule, click **Add New** and refer to page 36 "[Create Schedules](#)". After you have created a new schedule, you will be returned to the page to apply the new schedule. If you encounter issues, click the drop-down list and the new schedule will be available for selection. **Note:** Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 35 to configure [Time Settings](#) and see page 36 "[Create Schedules](#)" to create a schedule.

Schedule	Always <input type="button" value="v"/>	<input type="button" value="Add New"/>
----------	-----------------------------------------	----------------------------------------

4. Under Security Policy, you can apply a different wireless security type and key to the guest network. Please refer to page 18 to find out about different security types and page 19 for wireless security configuration.

- **Security Mode** – Select the wireless security to use for the guest network.

Security Policy	
Security Mode	Disable <input type="button" value="v"/>

Advanced Guest Network Settings

Basic > Guest Network (2.4GHz or 5GHz¹ or 5GHz²) > Advanced Guest Network Settings

At the bottom of the guest network page, you can click the “Advanced Guest Network Settings” to configure the additional guest network options such as the guest network interface IP address, DHCP server IP address range, and DHCP reservation.

[Advanced Guest Network Settings](#)

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

In most cases, you do not need to change your guest network 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 guest network IP address settings as default. The guest network IP address settings should differ from your local LAN network IP address settings (Default: 192.168.10.1 / 255.255.255.0)*

Guest Network Interface Setting	
MAC Address	02:11:E0:04:49:5F
IP Address	192.168.20.1
Subnet Mask	255.255.255.0

- **IP Address** – Enter the new guest network IP address. (e.g. 192.168.100.1)
- **Subnet Mask** – Enter the new guest network subnet mask. (e.g. 255.255.255.0)

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 guest network. The DHCP server is enabled by default on your router. It is recommended to leave this setting enabled.

DHCP Server Setting	
DHCP Server	Enabled
DHCP Start IP	192.168.20.100
DHCP End IP	192.168.20.150
DHCP Lease Time	86400 (seconds)

- **DHCP Server** – Enable or Disable the DHCP server.
- **DHCP Start IP** – Changes the starting address for the DHCP server range. (e.g. 192.168.20.20)
- **DHCP End IP** – Changes the last address for the DHCP server range. (e.g. 192.168.20.30)
- **Lease Time** – Enter the lease time in seconds.

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 guest network.

DHCP Reservations List			
Hostname	MAC Address	IP Address	Enabled
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>

- **Hostname:** Enter a name of the device you will assign the DHCP reservation rule.
- **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)
- **IP Address:** Enter the IP address to assign to the reservation. (e.g. 192.168.10.101)
- **Enable:** Select enable to enable the setting

Parental Control

Basic > Parental Control

Parental control settings allow you to set up restrictions/filters specifically who is allowed or denied access to your network for a specified period of time and restricted access to web content.

Website Filter

Basic > Parental Control

You may want to block computers or devices on your network access to specific websites (e.g. www.xxxxxxxx.com, etc.), also called domains or URLs (Uniform Resource Locators). You may also apply a schedule when these websites are allowed or denied.

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Basic** and click on **Parental Control**.

3. Under **Website Filter**, click the **Website Filter Mode** drop-down list and select **Enabled** to enable website filtering.

4. **Enable** – Check this option to enable the filter rule.

5. Enter a **URL** (ex. www.xxxxxxxx.com) to apply for the filter or block.

6. **Schedule:** The schedule function allows you to define a schedule when the wireless should be turned on. To define a new schedule, click **Add New** and refer to page 36 "[Create Schedules](#)". After you have created a new schedule, you will be returned to the page to apply the new schedule. If you encounter issues, click the drop-down list and the new schedule will be available for selection. **Note:** *Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 35 to configure [Time Settings](#) and see page 36 "[Create Schedules](#)" to create a schedule.*

Note: Clicking **Cancel** will discard your settings and clear all fields.

7. Click **Add** to add the access rule to the **Web URL Filter List**.

Web URL Filter				
URL	Schedule	Enabled	Remove	Edit
www.xxxxxxxx.com	Always	Yes	Remove	Edit

Note: In the **Web URL Filter List**, you can edit a rule by clicking **Edit** in the Edit column next to the rule you would like to edit. You can also delete a rule by clicking **Remove** under the Remove column next to the rule you would like to delete.

8. Repeat steps 4 – 7 for any to block any additional domain names (URLs). When finished, click **Apply** at the bottom of the page to save your settings.

IP Address Filter

Basic > Parental Control

Every network device must be assigned or configured with a specific 32-bit IP address in order to communicate with your network which is typically assigned by your router DHCP server automatically. Using access rules, you can deny specific computers and other devices from using this router's wired or wireless network by specifying the IP address.

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Basic**, click on **Parental Control**.
3. Under **IP Filter Mode**, click the **IP Filter Mode** drop-down list and select **Enabled** to enable IP Address filtering.

IP Filter Rules

IP Filter Mode Enabled

4. **Enable** – Check this option to enable the filter rule.

Enable

- 5 Manually enter the **IP Address** (ex. 192.168.10.130) in the field to block.

IP Address << Host Name

Note: If the network device is connected to your router, you can also click the drop-down list to choose one of the network devices (IP Address) detected by your router.

Note: If your device is not listed, please refer to your computer or device documentation to find the IP address.

Note: Clicking **Cancel** will discard your settings and clear all fields.

Schedule: The schedule function allows you to define a schedule when the wireless should be turned on. To define a new schedule, click **Add New** and refer to page 36 "[Create Schedules](#)". After you have created a new schedule, you will be returned to the page to apply the new schedule. If you encounter issues, click the drop-down list and the new schedule will be available for selection. **Note:** Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 35 to configure [Time Settings](#) and see page 36 "[Create Schedules](#)" to create a schedule.

Schedule Always Add New

6. Click **Add** to add the access rule to the **IP Filter Rules List**.

IP Filter Rules				
IP Address	Schedule	Enabled	Remove	Edit
192.168.10.130	Always	Yes	Remove	Edit

Note: In the **IP Filter Rules List**, you can edit a rule by clicking **Edit** in the Edit column next to the rule you would like to edit. You can also delete a rule by clicking **Remove** under the Remove column next to the rule you would like to delete.

7. Repeat steps 4 – 6 for any to block any additional IPAddresses. When finished, click **Apply** at the bottom of the page to save your settings.

[Apply](#) [Cancel](#)

MAC Address Filter*Basic > Parental Control*

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

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Basic**, click on **Parental Control**.
3. Under **MAC Filters**, click the **MAC Filter Mode** drop-down list and select the action **Allow** (*whitelist*) to specify the addresses allows to access your network or the Internet or **Deny** (*blacklist*) to specify addresses denied access to your network or the Internet.

MAC Filters	
MAC Filter Mode	Disabled Allow Deny

4. Under **Add MAC Filter Rule**, manually enter the **MAC Address** (ex. (e.g. 00:11:22:AA:BB:CC) in the field to allow or block (depending on the action you chose in previous step).

Add MAC Filter Rule	
MAC Filters	<input type="text"/> << Host Name

Note: If the network device is connected to your router, you can also click the drop-down list to choose one of the network devices (MAC Address) detected by your router.

Note: If you device is not listed, please refer to your computer or device documentation to find the MAC address.

Note: Clicking **Cancel** will discard your settings and clear all fields.

5. Click **Add** to add the access rule to the **MAC Filters** rule list.

MAC Filters		
MAC Filters	Remove	Edit
00:11:22:AA:BB:CC	Remove	Edit

Note: In the **MAC Filters** list, you can edit a rule by clicking **Edit** in the **Edit** column next to the rule you would like to edit. You can also delete a rule by clicking **Remove** under the **Remove** column next to the rule you would like to delete.

6. Repeat steps 4 – 5 for any to block any additional MAC addresses. When finished, click **Apply** at the bottom of the page to save your settings.

Apply	Cancel
-------	--------

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 unsecured 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 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/ac
Highest Performance Under This Setting	Up to 54Mbps	Up to 54Mbps	Up to 600Mbps (11n) or 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

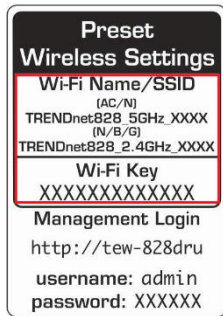
*Dependent on the maximum 802.11n data rate supported by the device (150Mbps, 300Mbps, 450Mbps) or maximum 802.11ac data rate supported by the device (433Mbps, 867Mbps, 1.3Gbps)

Secure your wireless network

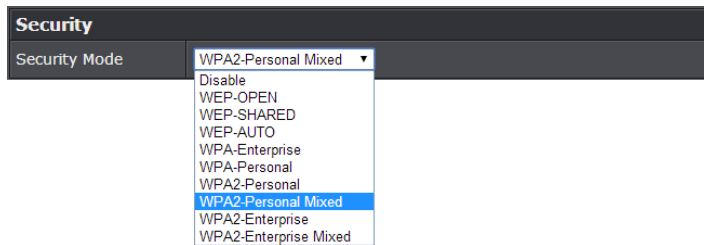
Basic > Wireless (2.4GHz or 5GHz¹ or 5GHz²)

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 18), you can set up wireless security.

Note: By default, your router is configured with a predefined wireless network name (SSID) and security key using WPA2-Personal. The predefined wireless network name and security can be found on the sticker on the side of the router or on the device label at the bottom of the router.



1. Log into your router management page (see [“Access your router management page”](#) on page 9).
2. Click on **Basic** and click on **Wireless**.
3. Click the **Select Wireless Band** drop-down list to select the wireless band you would like to configure. 2.4GHz, 5GHz (5GHz¹ or 5GHz²)
3. Under **Security**, click on the **Security Mode** drop-down list to select your wireless security type.



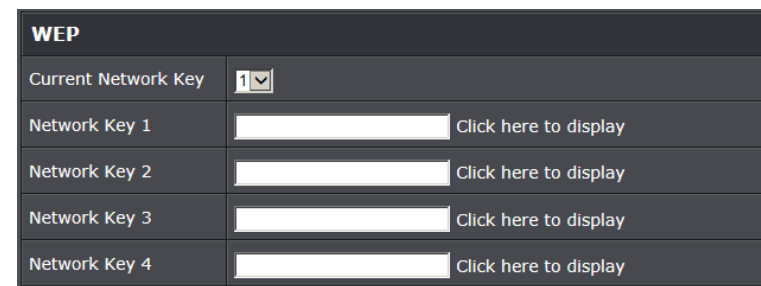
Selecting WEP

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

Note: Please note that WEP security is only available when 802.11 Mode is set to 802.11b/g only (2.4GHz) or 802.11a/ac only (5GHz). Also note, that using WEP will disable the use of WPS.

- **Security Mode:** Choose **WEP-OPEN** or **WEP-SHARED**.
Note: It is recommended to use *Open* since it is known to be more secure than *Shared Key*.
- **Current Network Key:** Choose the key index to use for security to the corresponding WEP Keys 1-4. You can only use one key at any given time.
Note: Please note that they wireless client key index 1-4 should also match the key index chosen here in order to establish connection.
- **Network Key 1-4:** Enter the WEP key. This is the password or key that is used to connect your computer to this router wirelessly. You can enter 64-bit or 128-bit key. You can enter up to four keys but only the one chosen as the Default Key will be used.
Note: It is recommended to use 128-bit because it is more secure to use a key that consists of more characters.
- **Hex/ASCII:** Enter the WEP key format. See the table below for the acceptable characters and lengths for each format.

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



Selecting WPA-PSK / WPA2-PSK / WPA2-PSK Mixed (WPA2-Personal recommended):

In the **Security Mode** drop-down list, select **WPA-PSK**, **WPA2-PSPK**, or **WPA2-PSK Mixed**. Please review the WPA-PSK settings to configure and click **Apply** to save the changes.

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

- **WPA Encryption (Cipher):** Select a Cipher Type to use.
 - 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 (preshared key)
 - This is the password or key that is used to connect your computer to this router wirelessly
Key Format: 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.

WPA	
WPA Encryption	AES <input type="button" value="v"/>
WPA passphrase	•••••••• <input type="button" value="Click here to display"/>
Network Key Rotation Interval	3600 (seconds)

Selecting WPA / WPA2 / WPA2 Mixed (WPA2 recommended):

The following section outlines options when selecting **WPA**, **WPA2**, or **WPA2 Mixed** (Enterprise, EAP, or RADIUS). This security type is also known as EAP (Extensible Authentication Protocol) or Remote Authentication Dial-In User Service or RADIUS.

Note: This security type requires an external RADIUS server, Pre-Shared Key only requires you to create a passphrase.

- **WPA Encryption (Cipher):** Select a Cipher Type to use.
 - When selecting **WPA2 Mixed** security, it is recommended to use **TKIP/AES**.
 - When selecting **WPA2** security, it is recommended to use **AES**.
- **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.
- **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.

WPA	
WPA Encryption	AES <input type="button" value="v"/>
Network Key Rotation Interval	3600 (seconds)
Radius Server	
RADIUS Server	<input type="text"/>
RADIUS Port	1812
RADIUS Key	<input type="text"/>

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.

You can view the currently connected wireless client devices under *Advanced > Administrator > Client Status* in the router management page.

See the "[Appendix](#)" on page 64 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
 - (RECOMMENDED) Hardware Push Button method—with an external button located physically on your router and on your client device
 - WPS Software/Virtual Push Button - located in router management page
 - PIN (Personal Identification Number) Method - located in router management page
- Note:** Refer to your wireless device documentation for details on the operation of WPS.

Recommended Hardware Push Button (PBC) Method

- **Note:** It is recommended that a wireless key (passphrase or password) is created before connecting clients using the PBC method. By default your router is preconfigured with a wireless encryption key. 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. The Power/WPS LED will blink to indicate WPS has been activated on your router. (See "[Product Hardware Features](#)" on page 2)

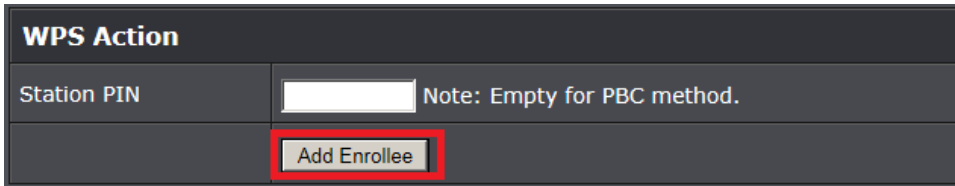
For connecting additional WPS supported devices, repeat this process for each additional device.

PBC (Software/Virtual Push Button)

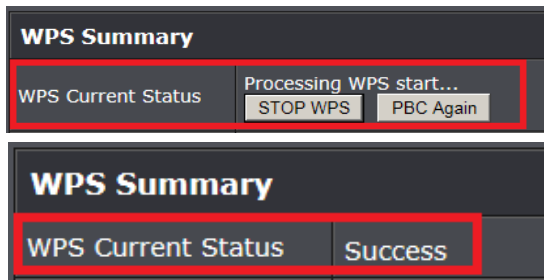
Advanced > Wireless (2.4GHz or 5GHz (5GHz¹ or 5GHz²)) > WPS

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 9).
2. Click on **Advanced**, then click on **Wireless (2.4GHz or 5GHz (5GHz¹ or 5GHz²))**, and click on **WPS**.
3. To add a wireless device to your network, under **WPS Action**, 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.



4. Wait for your router to finish the WPS process.
Note: You should a message on your WPS client device indicating WPS was successful. You can click **Stop WPS** to cancel the process or click **PBC Again** to restart the WPS process.

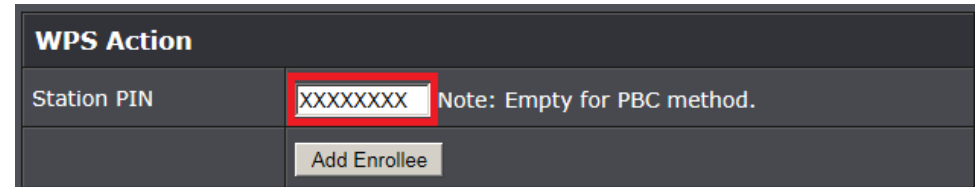


PIN (Personal Identification Number)

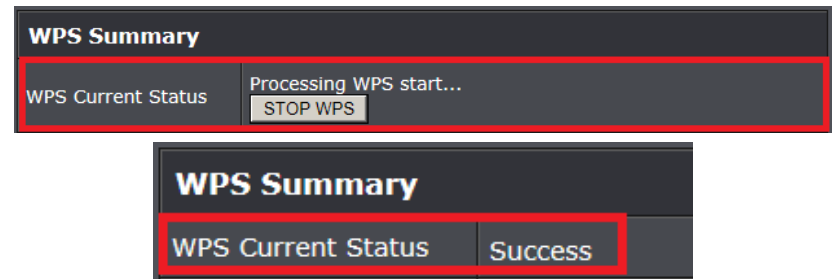
Advanced > Wireless (2.4GHz or 5GHz (5GHz¹ or 5GHz²)) > WPS

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 9).
2. Click on **Advanced**, then click on **Wireless (2.4GHz or 5GHz (5GHz¹ or 5GHz²))**, and click on **WPS**.
3. To add a wireless device to your network, next to **Client**, enter the 8-digit numeric PIN number of the wireless client device and click **Start PIN**. **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.



4. Wait for your router to finish the WPS process.
Note: You should a message on your WPS client device indicating WPS was successful. You can click **Stop WPS** to cancel the process.



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 (5GHz¹ or 5GHz²)) > Multiple SSID

The multiple SSID feature allows you to broadcast up to 3 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.

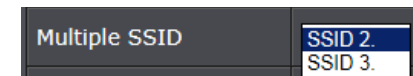
By default, your router functions in Access Point mode to allow wireless client devices to connect and access your network resources and access the Internet using a single SSID.

The diagram below shows your router in Access Point mode and clients connecting to your router using a single SSID.

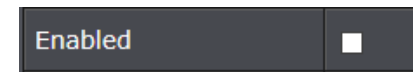


To configure multiple SSID on your router:

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Wireless (2.4GHz or 5GHz (5GHz¹ or 5GHz²))**, then click on **Multiple SSID**.
3. Click on the **Multiple SSID** drop-down list and select SSID to configure.



4. Next to Enabled, check the **Enabled** option to enable the additional SSID.



5. **Wireless Name (SSID):** Enter the wireless name (SSID) for additional SSID. This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. By default, the router's wireless name is unique to the device. It is recommended to change it to a name different from the primary SSID 1 and one that you can easily remember.



Schedule: The schedule function allows you to define a schedule when the wireless should be turned on. To define a new schedule, click **Add New** and refer to page 36 "[Create Schedules](#)". After you have created a new schedule, you will be returned to the page to apply the new schedule. If you encounter issues, click the drop-down list and the new schedule will be available for selection. **Note:** Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 35 to configure [Time Settings](#) and see page 36 "[Create Schedules](#)" to create a schedule.



6. **Security Mode** - You can configure your wireless security settings for the additional SSIDs. Please refer to page 18 to find out about different security types and page 19 for wireless security configuration.

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

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



Note: You can repeat the steps to enable and configure additional SSIDs.

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

Access Point with Multiple SSID



Wireless bridging using WDS (Wireless Distribution System)

Advanced > Wireless (2.4GHz or 5GHz (5GHz¹ or 5GHz²)) > 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 (5GHz¹ or 5GHz²)). 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.

The diagram below shows your router in Access Point mode and clients connecting to your router.



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 30](#) 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 31](#) for DHCP server options.
3. Configure the same wireless channel and use the same on all WDS supported wireless devices. See [page 10](#) 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-828DRU routers:

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced > Wireless (2.4GHz or 5GHz)**, and click on **WDS**.
3. Next to **Wireless Distribution System (WDS)**, in an empty field, enter the MAC address of the other WDS supported wireless device you are bridging. (e.g. 00:11:22:AA:BB:CC)

Wireless Distribution System (WDS)	
AP MAC Address	<input type="text"/>
	<input type="text"/>
	<input type="text"/>
	<input type="text"/>

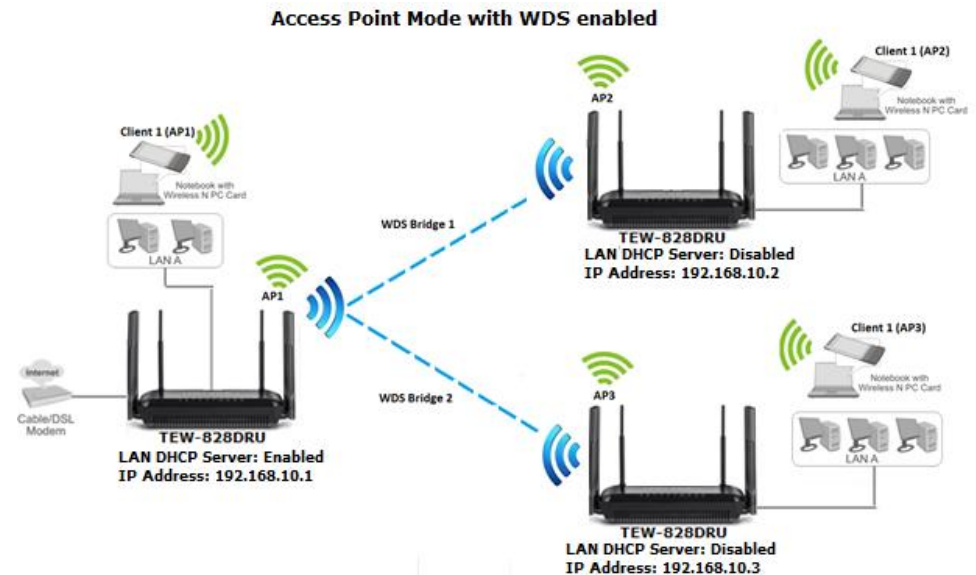
4. To save changes, click **Apply**.

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



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.

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.



Advanced Settings

Advanced > Wireless (2.4GHz or 5GHz (5GHz¹ or 5GHz²)) > 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.

- 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)
- 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.

- 20/40 MHz Coexistence (2.4GHz Only)** – This setting is enabled by default and allows 2.4GHz to fallback from 40MHz to 20MHz Channel Width operation depending on neighboring 2.4GHz wireless networks detected which may lower performance but improve stability. Turning this feature off will allow the 2.4GHz to operate in 40MHz regardless of neighboring networks which may improve performance but decrease connection stability in busy wireless environments.
- Xpress™ Technology:** A frame bursting technology used to improve wireless performance. The feature will only work with other Xpress™ supported devices. It is recommended to leave this feature On.
- Implicit Beamforming:** Technology capable of focusing RF energy directly toward a receiving client which may significantly improve connectivity, coverage and performance at slightly further ranges by leveraging information from the client device on initial connection and determining how to best focus RF beams toward the client device. This type of beamforming does not require the client device to support beamforming in order to function. Explicit beamforming is also supported and requires client devices to support beamforming in order to function. Explicit Beamforming is enabled by default and cannot be enabled or disabled in the router management page.

Advanced Wireless	
Beacon Interval	<input type="text" value="100"/> ms (range 20 - 1000, default 100)
DTIM	<input type="text" value="3"/> (range 1 - 255, default 3)
Fragment Threshold	<input type="text" value="2346"/> (range 256 - 2346, default 2346)
RTS Threshold	<input type="text" value="2347"/> (range 1 - 2347, default 2347)
Short Preamble	<input type="button" value="Disabled"/> ▾
20/40 MHz Coexistence	<input type="button" value="On"/> ▾
XPress™ Technology	<input type="button" value="On"/> ▾
MCS	<input type="text" value="Auto"/> ▾
Implicit Beamforming	<input type="button" value="Enabled"/> ▾

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.

Advanced Router Settings

Change your router login password

Advanced > Administrator > Management

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Administrator**, then click on **Management**.
3. Under the **Administrator Settings** section, in the **Password** field.

Note: The idle timeout setting is used to define the period of inactivity in the router management page before automatically logging out.

Administrator Settings	
Account	admin
Password (Max: 16 characters)
Idle Timeout	120 (120-3600 seconds)

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

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

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 predefined default password. If you reset the device to defaults, you will need to access the router management page use the predefined settings on the top or device labels.

Manually configure your Internet connection

Advanced > Setup > WAN

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Setup**, then click on **WAN**.
3. Under **WAN Connection Type** in drop-down list, select the type of Internet connection provided by your Internet Service Provider (ISP).

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

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

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

Change your device name

Advanced > Administrator > Management

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced**, then click on **Administrator**, and click on **Management**.
3. 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.

Device Name Settings	
Device Name	TEW-828DRU

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

Change your device URL

Advanced > Administrator > Management

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced**, then click on **Administrator**, 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.

Device URL Settings	
Device URL	tew-828dru

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

IPv6 Settings

Advanced > Setup > IPv6

IPv6 (Internet Protocol Version 6) is a new protocol that significantly increases the number of available Internet public IP addresses due to the 128-bit IP address structure versus IPv4 32-bit address structure. In addition, there are several integrated enhancements compared to the most commonly used and well known IPv4 (Internet Protocol Version 4) such as:

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

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

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Setup**, then click on **IPv6**.
3. Review the IPv6 Internet Connection settings and enter information settings specified by your ISP. Click **Apply** to save changes.

Note: Please contact your ISP for IPv6 service availability.

WAN IPv6 Setting	
IPv6 Connection Mode	<div style="border: 1px solid black; padding: 2px;"> Link Local Auto Configuration (SLAAC/DHCPv6) Static 6to4 Tunnel 6rd Tunnel </div>

You can click on **Advanced > Administrator > IPv6 Status** to check the IPv6 connection status.

Clone a MAC address

Advanced > Setup > WAN

On any home network, each network device has a unique MAC (Media Access Control) address. Some ISPs register the MAC address of the device (usually a router or a computer) connected directly to the modem. If your computer MAC address is already registered with your ISP and to prevent the re-provisioning and registration process of a new MAC address with your ISP, then you can clone the address (assign the registered MAC address of your previous device to your new router). If you want to use the MAC address from the previous device (computer or old router that directly connected to the modem), you should first determine the MAC address of the device or computer and manually enter it into your router using the clone MAC address feature.

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

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Setup**, then click on **WAN**.
3. Next to **MAC Address** field, enter the MAC address of your computer.

Note: You can also check the Advanced > Administrator > Client Status for the MAC addresses of the devices on your network, see [page 56](#) or refer to your computer or device documentation to find the MAC address.

MAC Address	<input type="text"/>
-------------	----------------------

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

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

Change your router IP address

Advanced > Setup > LAN

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 9).
2. Click on **Advanced** and click on **Setup**, then click on **LAN**.
3. In **LAN Interface Setting** section, Enter the 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)

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.

LAN Interface Setting	
MAC Address	D8:EB:97:AD:EB:44
IP Address	<input type="text" value="192.168.10.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>

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

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://\(new.ipaddress.here\)](http://(new.ipaddress.here)) to access your router management page. You can also use the default login URL <http://tew-828dru>

Set up the DHCP server on your router

Advanced > Setup > LAN

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 9).
2. Click on **Advanced** and click on **Setup**, then click on **LAN**.
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 ending 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 the DHCP lease time in minutes.
Note: The DHCP lease time is the amount of time a computer or device can keep an IP address assigned by the DHCP server. When the lease time expires, the computer or device will renew the IP address lease with the DHCP server, otherwise, if there is no attempt to renew the lease, the DHCP server will reallocate the IP address to be assigned to another computer or device.

DHCP Server Setting	
DHCP Server	Enabled <input type="button" value="v"/>
DHCP Start IP	192.168.10.101
DHCP End IP	192.168.10.199
DHCP Lease Time	86400 (seconds)

You can also view the current DHCP clients/connected devices in the Number of Dynamic DHCP Clients list under *Advanced > Administrator > Client Status*.

2.4GHz Wireless Connected Devices				
SSID	IP Address	MAC Address	Host Name	Link Rate
TRENDnet828_2.4GHz_1A2B	192.168.10.102	D8:EB:97:25:5A:C0	PM-HP4525S	39

Set up DHCP reservation

Advanced > Setup > LAN

DHCP (Dynamic Host Configuration Protocol) reservation (also called Static DHCP) allows your router to assign a fixed IP address from the DHCP server IP address range to a specific device on your network. Assigning a fixed IP address can allow you to easily keep track of the IP addresses used on your network by your computers or devices for future reference or configuration such as virtual server (also called port forwarding, see "[Virtual Server](#)" on page 39) or special applications (also called port triggering, see "[Special Applications](#)" on page 41).

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Setup**, then click on **LAN**.
3. Review the DHCP reservation settings.
 - **Hostname:** Enter a name of the device you will assign the DHCP reservation rule.
 - **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*)
 - **IP Address:** Enter the IP address to assign to the reservation. (e.g. 192.168.10.101)
 - **Enable:** Check the **Enabled** option to enable the reservation.

DHCP Reservations List			
Hostname	MAC Address	IP Address	Enabled
			<input type="checkbox"/>

After you have entered in the required information, click **Add** to add the DHCP Reservations entry to the list.



You will see the new reservation added to the DHCP Reservations List. This is a temporary list until you save changes by clicking **Apply**. You can continue to add more DHCP reservation entries which will appear in this list. Once you have saved the settings, the entries will appear under the DHCP Reservations list.

Under the DHCP Reservations List,

You can click the **Edit** to modify the reservation or click **Remove** option next to the entry to delete the reservation.

To save changes when modifying a reservation, click **Edit**.

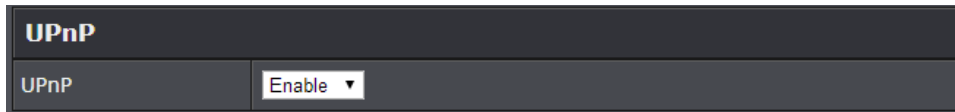
DHCP Reservations List					
Hostname	MAC Address	IP Address	Enabled	Remove	Edit
TRENDnet1	00:14:D1:26:E4:76	192.168.10.101	<input checked="" type="checkbox"/>	Remove	Edit

Enable/disable UPnP on your router

Advanced > Administrator > 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 9).
2. Click on **Advanced** and click on **Administrator**, then click **Advanced Network**.
3. Under the **UPnP** section, check the option to enable UPnP or uncheck to disable UPnP.



The screenshot shows a dark-themed interface with a section titled 'UPnP'. Below the title, there is a label 'UPnP' followed by a dropdown menu currently set to 'Enable'.

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

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

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



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 9).
2. Click on **Advanced** and click on **Firewall**, then click on **ALG**.
3. Review the applications to enable or disable. Click **Apply** to save the changes.
 - **Email Receiving (POP3):** Allows POP3 protocol through your router.
 - **Email Receiving (SMTP):** Allows SMTP protocol through your router.
 - **Streaming Video (RTP):** Allows RTP video protocol through your router.
 - **Streaming Media-VoIP (SIP):** Allows SIP protocol through your router.
 - **File Transfer (FTP):** Allows FTP protocol through your router.
 - **File Transfer (TFTP):** Allows TFTP protocol through your router.
 - **VPN Pass-Through:** Allows PPTP/L2TP VPN connections through your router.

Application Level Gateway (ALG) Configuration

Service Name	Description	Enabled
Email Receiving	Post Office Protocol - Version 3 (POP3)	<input checked="" type="checkbox"/>
Email Receiving	Simple Mail Transfer Protocol (SMTP)	<input checked="" type="checkbox"/>
Streaming Media	Real Time Transport Protocol (RTP)	<input checked="" type="checkbox"/>
Streaming Media - VoIP	Session Initiation Protocol (SIP)	<input checked="" type="checkbox"/>
File Transfer	File Transfer Protocol (FTP)	<input checked="" type="checkbox"/>
File Transfer	Trivial File Transfer Protocol (TFTP)	<input checked="" type="checkbox"/>
Remote Control	Telnet	<input checked="" type="checkbox"/>
VPN Pass-Through		<input checked="" type="checkbox"/>

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

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

Identify your network on the Internet

Advanced > Administrator > 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. Sign up for one of the DDNS available service providers list under **Server Address**. (e.g. *no-ip.com*, etc.)
2. Log into your router management page (see "[Access your router management page](#)" on page 9).
3. Click on **Advanced** and click on Administrator, then click on **Management**.

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

- **Dynamic DNS Provider Server:** 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*)
- **Account:** 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 for which you have signed up to. (NOT your router or wireless network password)

DDNS Settings	
Dynamic DNS Provider	None ▾
Host Name	<input type="text"/>
Account	<input type="text"/>
Password	<input type="password"/>

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



Set your router date and time

Advanced > Administrator > Time

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Administrator**, then click **Time**.
3. Review the Time settings. Click **Apply** to save settings.

- **Time Configuration:** Displays the current device time and date information.

Time Configuration	
System Time	Tue Jan 3 00:39:28 2012

- **Manually set time** – Set your router date and time manually in the Date and Time Settings section. **Note:** *Time is specified in 24-hour format.*

Date and Time Settings						
Date And Time	Year	2012	Month	Jan	Day	03
	Hour	00	Minute	39	Second	07

- **Automatically synchronize time using NTP** – Check the **Enable NTP Server** option to set your router date and time to synchronize with an NTP (Network Time Protocol) server address (e.g. pool.ntp.org). Enter the NTP server address next to Default NTP server, (e.g. pool.ntp.org). Click the **Time Zone** drop-down list to select the appropriate zone and you can optionally change your NTP Sync period.

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

NTP Settings	
Enable NTP Server	<input type="checkbox"/>

- **Enable Daylight Saving:** Check the option to configure the DST settings. Set the annual range when daylight saving is activated. To save changes, click **Apply**.

Daylight Saving Time	
Enable Daylight Saving	<input type="checkbox"/>

Create schedules

Advanced > Administrator > 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 under Advanced > Administrator > Time.

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

- Wireless (2.4GHz and 5GHz (5GHz¹ and 5GHz²))
- Guest Network
- Wireless Multiple SSID
- Parental Control (MAC Address/Web URL Filters)
- Security > Access Control (IP Protocol Filters)
- Virtual Server
- Special Applications (Port Trigger)
- Gaming (Port Range Forwarding)

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Administrator**, then click on **Schedule**.

3. Review the Schedule settings.

- **Rule Name:** Enter a name for the schedule you would like to apply.
- **Days:** Check the days you would like to the schedule to be active or select **Every Day** to set the schedule for all days.
- **Times Start - End:** Click the drop-down list to specify the time period the schedule should be active. Please note that the time must be specified in 24-hr format or check **All Day** to specify that the schedule should be active all 24 hours.

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

Add Schedule Rule	
Rule Name	<input type="text"/>
Days	<input type="checkbox"/> Every Day
	<input type="checkbox"/> Sun. <input type="checkbox"/> Mon. <input type="checkbox"/> Tue. <input type="checkbox"/> Wed. <input type="checkbox"/> Thu. <input type="checkbox"/> Fri. <input type="checkbox"/> Sat.
Times Start - End	<input type="checkbox"/> All Day
	<input type="text" value="00"/> : <input type="text" value="00"/> - <input type="text" value="00"/> : <input type="text" value="00"/>

Click **Add** to save the schedule to the **Schedule Rules** list. You can continue to add more schedules to the list. Click **Apply** to save the schedules created to the configuration.

Schedule Rules				
Rule Name	Days	Times Start - End	Remove	Edit

Access Control (IP Protocol Filter)

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.

Protocol/IP Filter

Basic > Parental Control

Every network device must be assigned or configured with a specific 32-bit IP address in order to communicate with your network which is typically assigned by your router DHCP server automatically. Using access rules, you can deny specific computers and other devices from using this router's wired or wireless network by specifying the IP address.

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Basic**, click on **Parental Control**.
3. Under **Access Control**, click the **LAN Client Filter Function** drop-down list and select **Enabled** to activate the feature.

LAN Client Filter Function

4. **Enable** – Check this option to enable the access control rule.

Enable

5. **LAN IP Address Range:** Enter the IP address or IP address range to apply the protocol/IP filter. (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.

LAN IP Address Range -

6. **Protocol** – Select the protocol type to filter. TCP, UDP.

Protocol

7. **Destination Port Range:** Enter the port number or range of port numbers to apply in the firewall rule. (e.g. 80-80 or 20-21). For all ports, use the port range 1 - 65534.

Destination Port Range -

Note: Clicking **Cancel** will discard your settings and clear all fields.

Schedule: The schedule function allows you to define a schedule when the wireless should be turned on. To define a new schedule, click **Add New** and refer to page 36 "[Create Schedules](#)". After you have created a new schedule, you will be returned to the page to apply the new schedule. If you encounter issues, click the drop-down list and the new schedule will be available for selection. **Note:** Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 35 to configure [Time Settings](#) and see page 36 "[Create Schedules](#)" to create a schedule.

Schedule

8. Click **Add** to add the access rule to the **LAN Client Filter Rules** List.

LAN Client Filter Rules

LAN IP Address Range	Protocol	Destination Port Range	Schedule	Enabled	Remove	Edit
----------------------	----------	------------------------	----------	---------	--------	------

Note: In the **IP Filter Rules List**, you can edit a rule by clicking **Edit** in the Edit column next to the rule you would like to edit. You can also delete a rule by clicking **Remove** under the Remove column next to the rule you would like to delete.

9. Repeat steps 4 – 8 for any to block any additional IP addresses and protocols/ports. When finished, click **Apply** at the bottom of the page to save your settings.

Quality of Service

Advanced > Setup > QoS

This section allows you to configure the router QoS settings and prioritize specific traffic to and from specific IP addresses. There are 5 priority queues (Highest, High, Medium, Low, Lowest) for inbound (LAN-WAN) and outbound traffic (WAN-LAN) that can be manually defined. **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 9).
2. Click on **Advanced**, click on **Setup**, and click on **QoS**.
3. To enable QoS, first, click the **Enable QoS** drop-down list and select **Enabled**.

Enable QoS	Enabled <input type="button" value="v"/>
------------	------------------------------------------

Note: Prioritize ACK will prioritize the confirmation message when using TCP. TPrioritize ICMP packets will prioritize ICMP requests such as ping for network connectivity testing. Both of these settings can be left at default Enabled.

4. Then, specify your BW Max or total bandwidth for each Class Setting (Inbound and Outbound).

Note: You can use an online Internet speed test tool (ex. www.speedtest.net) to determine your maximum inbound and outbound bandwidth.

Inbound Class Setting	
Inbound Classes (% Max Input BW)	
BW Max Inbound	1500 Kbit/s
%BW	
Highest	50 750 Kbit/s
High	30 450 Kbit/s
Medium	10 150 Kbit/s
Low	5 75 Kbit/s
Lowest	1 15 Kbit/s

Outbound Class Setting	
Outbound Classes (% Max Output BW)	
BW Max Outbound	384 Kbit/s
%BWMin %BWMax	
Highest	80 100 307 -- 384 Kbit/s
High	10 100 38 -- 384 Kbit/s
Medium	5 100 19 -- 384 Kbit/s
Low	3 100 11 -- 384 Kbit/s
Lowest	2 95 7 -- 364 Kbit/s

Note: The allocated bandwidth for each priority queue will automatically be calculated based on the BW Max that you have entered for each class. You can choose to use the default priority queue settings or make modifications to the % BW max % BW min settings (% of allocated bandwidth) for each queue. It is recommended to use the default settings.

5. Finally, create a QoS rule to specify the Source IP address, Source MAC address, or Destination IP address, the protocol and port number (service), and priority queue/class to assign for QoS. Any other traffic that does not otherwise have a QoS rule specified will automatically default to the priority queue specified in the Default Traffic Class setting. Click **Add** to apply the setting.

QoS Rule Add	
Add QoS Rule (Outbound)	
IP/MAC Address Filter	Any <input type="button" value="v"/> Address: <input type="text"/>
Protocol Filter	Any <input type="button" value="v"/>
Port Filter	Any <input type="button" value="v"/> Port List: <input type="text"/>
Class Assigned	Highest <input type="button" value="v"/>
Description	<input type="text"/>

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

1. Make the computer or network device (for which you are establishing a DMZ link) has a static IP address. Signing up for a Dynamic DNS service (outlined in [Identify Your Network](#) section page 34) will provide identification of the router's network from the Internet.
2. Log into your router management page (see "[Access your router management page](#)" on page 9).
3. Click on **Advanced** and click **Firewall**, then click on **DMZ**.
4. Select **Enable** in the **DMZ Settings** section.

DMZ Settings	Enabled ▾
--------------	-----------

5. Enter the IP address you assigned to the computer or network device to expose to the Internet.

DMZ IP Address	<input type="text"/>
----------------	----------------------

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

Virtual Server

Advanced > Firewall > Virtual Server

Virtual Server (also called port forwarding) allows you to define specific ports (used or required by a specific application) and forward them to a single IP address (a computer or device) on your network. Using this feature is more secure compared to using DMZ (see "[DMZ](#)" on page 39) 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 42.

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 34).

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Firewall**, then click on **Virtual Server**.
3. Select **Enabled** in the **Port Forward Function** drop-down list.

Port Forward	
Port Forward Function	Enabled ▾

4. Review the virtual server settings.

Check the option to the left most of the entry to enable and uncheck to disable.

- **Enable** – Check the option to enable the virtual server.
- **Protocol**: Select the protocol required for your device. **TCP** or **UDP**.
- **Public Port** – Enter the port number used to access the device from the Internet.
- **LAN IP Address**: Enter the IP address of the device to forward the port (e.g. *192.168.10.101*).

- **Private Port** – Enter the port number required by your device. Refer to the connecting device's documentation for reference to the network port(s) required.

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. It is recommended to assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.

- **Schedule:** The schedule function allows you to define a schedule when the wireless should be turned on. To define a new schedule, click **Add New** and refer to page 36 "[Create Schedules](#)". After you have created a new schedule, you will be returned to the page to apply the new schedule. If you encounter issues, click the drop-down list and the new schedule will be available for selection. **Note:** Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 35 to configure [Time Settings](#) and see page 36 "[Create Schedules](#)" to create a schedule.

Add Virtual Server Rule	
Enable	<input type="checkbox"/>
Protocol	TCP
Public Port	<input type="text"/>
LAN IP Address	<input type="text"/>
Private Port	<input type="text"/>
Schedule	Always <input type="button" value="Add New"/>

Click **Add** to add the access rule to the **Virtual Server Rules** List.

Note: Clicking **Cancel** will discard your settings and clear all fields.

Virtual Server Rules

Protocol	Public Port	LAN IP Address	Private Port	Schedule	Enabled	Remove	Edit
----------	-------------	----------------	--------------	----------	---------	--------	------

Note: In the **Virtual Server List**, you can edit a rule by clicking **Edit** in the Edit column next to the rule you would like to edit. You can also delete a rule by clicking **Remove** under the Remove column next to the rule you would like to delete.

When finished, click **Apply** at the bottom of the page to save your settings.

Example: To forward TCP port 80 to your IP camera

1. Setup DynDNS service (see [Identify Your Network](#) section page 34).
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 9).
5. Click on **Advanced** and click on **Firewall**, then click on **Virtual Server**
6. Check the **Enable** option to enable the Virtual Server.
7. Next to **IP Address**, enter the IP address assigned to the camera. (e.g. 192.168.10.101)
8. Next to **Protocol**, make sure **TCP** is selected in the drop-down list.
10. The **Private Port** and **Public Port**, enter port number **80** is configured for both settings.
11. To save the changes, click **Add**.

Special Applications

Advanced > Firewall > Special Applications

Application rules (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 33.

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 9).
2. Click on **Advanced** and click on **Firewall**, then click on **Special Applications**.
3. Click the **Port Triggering** drop-down list, and select **Enabled**.

Port Trigger	
Port Trigger Function	Enabled ▾

4. Review the application rule settings.

- **Enable** – Check the option to enable the port trigger rule.
- **Match Protocol:** Select the protocol for the firewall ports required for your device. **TCP**, **UDP**, or **Any** (TCP and UDP).
- **Match Port Range:** Enter the ports or port range to be forwarded to the device. (e.g. 2000-2038,2200-2210).
- **Trigger Protocol:** Select the trigger port protocol requested by the device. **TCP**, **UDP**, or **Both** (TCP and UDP).

- **Trigger Port Range:** Enter the port requested by the device. (e.g. 554-554 or 6112-6112).
- **Schedule:** The schedule function allows you to define a schedule when the wireless should be turned on. To define a new schedule, click **Add New** and refer to page 36 "[Create Schedules](#)". After you have created a new schedule, you will be returned to the page to apply the new schedule. If you encounter issues, click the drop-down list and the new schedule will be available for selection. **Note:** Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 35 to configure [Time Settings](#) and see page 36 "[Create Schedules](#)" to create a schedule.

Add Port Trigger Rule	
Enable	<input type="checkbox"/>
Match Protocol	TCP ▾
Match Port Range	<input type="text"/> - <input type="text"/>
Trigger Protocol	TCP ▾
Trigger Port Range	<input type="text"/> - <input type="text"/>
Schedule	Always ▾ <input type="button" value="Add New"/>

Click **Add** to add the access rule to the **Port Trigger Rules** List.

Note: Clicking **Cancel** will discard your settings and clear all fields.

Port Trigger Rules						
Match Protocol	Match Port Range	Trigger Protocol	Trigger Port Range	Schedule	Enabled	Remove Edit

Note: In the **Port Trigger List**, you can edit a rule by clicking **Edit** in the Edit column next to the rule you would like to edit. You can also delete a rule by clicking **Remove** under the Remove column next to the rule you would like to delete.

When finished, click **Apply** at the bottom of the page to save your settings.

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 39) 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 34).

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Security**, then click on **Gaming**.
3. Click the **Gaming Function** drop-down list, and select **Enabled**.

Gaming	
Gaming Function	Enabled ▼

3. Review the virtual server settings.
 - **Enable** – Check the option to enable the gaming rule.
 - **IP Address:** Enter the IP address of the device to forward the ports (e.g. *192.168.10.101*).
 - **TCP Ports:** Enter the TCP port you would like to set.
 - **UDP Ports:** 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.
 - **Schedule:** The schedule function allows you to define a schedule when the wireless should be turned on. To define a new schedule, click **Add New** and refer to page 36 "[Create Schedules](#)". After you have created a new schedule, you will be returned to the page to apply the new schedule. If you encounter issues, click the drop-down list and the new schedule will be available for selection. **Note:**

Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 35 to configure [Time Settings](#) and see page 36 "[Create Schedules](#)" to create a schedule.

Add Gaming Rule	
Enable	<input type="checkbox"/>
LAN IP Address	<input type="text"/>
TCP Ports	<input type="text"/> - <input type="text"/>
UDP Ports	<input type="text"/> - <input type="text"/>
Schedule	Always ▼ <input type="button" value="Add New"/>

Click **Add** to add the access rule to the **Gaming Rules** List.

Note: Clicking **Cancel** will discard your settings and clear all fields.

Gaming Rules						
LAN IP Address	TCP Ports	UDP Ports	Schedule	Enabled	Remove	Edit

Note: In the **Gaming Rules** List, you can edit a rule by clicking **Edit** in the Edit column next to the rule you would like to edit. You can also delete a rule by clicking **Remove** under the Remove column next to the rule you would like to delete.

When finished, click **Apply** at the bottom of the page to save your settings.

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 as at your office or another location while away from your home.

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click **Administrator**, then click on **Management**.
3. Review the setting on the **Remote Management** section. Click **Apply** to save settings
 - **Remote Control (via WAN):** Click the drop-down list and select **Enable** to enable remote management or **Disable** to disable remote management.
 - **Remote 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)

Remote Management	
Remote Control (via WAN)	Enable ▾
Remote Port	8080

Add static routes

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 9).
2. Click on **Advanced** and click on **Setup**, then click on **Routing**.
3. Review the **LAN/WAN Static Routes** section. Click **Apply** to save settings.
 - **IP Address:** Enter the IP network address of the destination network for the route. (e.g. 192.168.20.0)
 - **Subnet Mask:** 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)

WAN Static Routes			
IP Address	Subnet Mask	Gateway	Metric
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

LAN Static Routes			
IP Address	Subnet Mask	Gateway	Metric
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

VLAN Configuration

Advanced > Setup > VLAN

This section allows you to configure the VLAN settings of router ports. Each port (LAN 1-4, WAN) can be set as either a tagged or untagged VLAN port to be used with other VLAN aware devices. VLAN ID 1 and 2 are reserved for the LAN and WAN default interfaces.

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 9).
2. Click on **Advanced** and click **Setup**, then click on **VLAN**.
3. Review the settings. Click **Apply** to save the settings.

Configuring Default Internet Setting

To configure the default Internet facing interface (WAN Port), check the Enabled option under the Default Internet Setting and enter the VID to assign. By default, the default Internet interface is set to an untagged VLAN port unless the Tagged option is checked changing it to a Tagged/Trunk VLAN port. If the default Internet interface is configured, the WAN port will automatically be excluded from the Virtual LAN Interface Setting.

Default Internet Setting

Enabled	Port Number	VID(3~4094)	Tagged
<input type="checkbox"/>	WAN Port	<input type="text"/>	<input type="checkbox"/>

Virtual LAN Interface Setting

To configure VLANs under the Virtual LAN Interface Setting, check the Enabled option and enter the VID to assign. For each port, click the drop-down list and select the VLAN assignment type (Untagged, Tagged, Excluded) to assign for the specified VID. If the default Internet interface setting (WAN port) is not configured, the WAN port is available to have a different switch port VLAN assignment.

Click **Add** to add the VLANs to the list, then click **Apply** to save the settings.

Virtual LAN Interface Setting

Enabled	VID (3~4094)	Port 1	Port 2	Port 3	Port 4	WAN Port
<input checked="" type="checkbox"/>	<input type="text"/>	Excluded ▾	Excluded ▾	Excluded ▾	Excluded ▾	Excluded ▾

VLAN List

Enabled	VID	Member	Remove	Edit
---------	-----	--------	--------	------

Using External USB Storage

Your router's USB port can be used to share files through the network when a USB storage device is connected on the back USB port. The router supports both FTP and SAMBA (SMB) filing sharing protocols.

Note: For security purposes, the USB SMB and FTP settings on your router are disabled by default. You will need to enable these settings in orders to allow access to your USB storage devices.

Note: For security purposes, the default USB SMB and FTP admin password is configured to the same predefined password used to log into your router management page.

Note: A USB device can be safely removed under Advanced > USB > Eject Device. Under the +|- column, check the option and click Safely Remove USB Device.



Samba Server

Advanced > USB > Samba Server

SMB (Samba) is a network protocol that allows you to access shared files through your network. In order to share files, you will need to plug in a USB storage device on the USB port on the back of the router.

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **USB**, then click on **Samba Server**.
3. Review the setting on **Samba Server Information** section. Click **Apply** to save settings.

- **Server Status:** Select enabled or disable for the feature.
- **Server Name:** You can change the name of your server which will be the name you will when accessing your USB storage device. (**Note:** You can also access the USB storage using the router IP address)
- **Workgroup:** Enter the workgroup name. It is recommended to keep the standard default "WORKGROUP". If you change this setting, you will need to change the workgroup name on all computers in your network that are allowed access to the USB storage in order to discover it automatically. Otherwise, you will need to access the server by IP address.
- **Description (optional):** Enter a description of the server.

Server Information	
Samba (SMB) Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Server Name	<input type="text" value="USBSHARE"/>
Workgroup	<input type="text" value="WORKGROUP"/>
Description (optional)	<input type="text"/>

4. Review the administrator settings required for your **File Sharing (SMB) Server**. Click **Apply** to save settings. Administrator will have read and write access to files. To define user accounts continue to the next step.

Note: For security purposes, the default administrator user name and password are set to your predefined user name and password setting to access the router management page.

Administrator	
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="••••"/> Note: The default administrator password is the same as the router's default management login password.

- **User Name:** Enter the user name to be used to access your files.
- **Password:** Enter the password for the user name. Re-type Password to confirm.

5. Review the **User Account List** section. Click **Apply** to save settings

User Account List			
User Name	Password	Permission	Enabled
		Read Only ▼	<input type="checkbox"/>
		Read Only ▼	<input type="checkbox"/>
		Read Only ▼	<input type="checkbox"/>
		Read Only ▼	<input type="checkbox"/>
		Read Only ▼	<input type="checkbox"/>

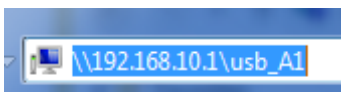
- **User Name:** Enter the user name to be used to access your files.
- **Password:** Enter the password for the user name.
- **Permission:** Select the permission you will grant to the user
- **Enabled:** Click to activate user account.

Under Windows®, you can access the USB storage device on your computer under **Computer > Network > USBSHARE > usb_A1**.

Note: Your computer will only be able to automatically discover the USB storage if you are set to a workgroup under the default name "WORKGROUP". Your computer will not be able to automatically discover the USB storage device if under a domain or different a workgroup name.



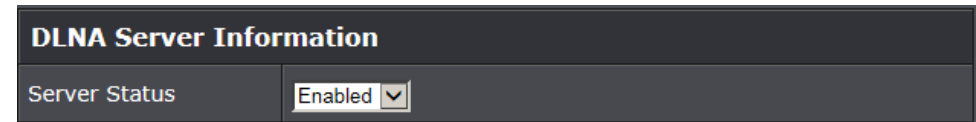
Under Windows®, if your computer cannot discover the USB storage automatically, you can access these files under your network map or by typing `\\<routerIPaddress>\usb_A1` (ex. `\\192.168.10.1\usb_A1`) on your browser's or file explorer address bar. Please follow the below steps to configure the router's SMB settings



DLNA Server

Advanced > USB > DLNA Server

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **USB**, then click on **DLNA Server**.
3. Click the **Server Status** drop-down list to enable the DLNA server and click **Apply**.



Note: The server name is the name you will see when scanning your network for DLNA compliant devices. You can edit the name if desired to something you can more easily recognize however, it is not required.

4. All DLNA compliant client devices such PS3, mobile phone, etc. be able to easily discover and access files on the USB storage through DLNA compliant protocols.

FTP (File Transfer Protocol) Server

Advanced > USB > FTP

FTP (File Transfer Protocol) is used to access shared files through the Internet. In order to share files, you will need to plug in a USB storage device on the USB port(s) on the back of the router.

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **USB**, then click on **FTP Server**.
3. Review the administrator settings required for your **FTP server**. Click **Apply** to save settings

FTP Server Information	
Server Status	Disabled ▾
Remote Access	Disabled ▾
Language(Codepage)	Traditional Chinese ▾

- **Server Status:** Select enable or disable for the feature.
- **Remote Access:** Selecting **Enabled** will allow access to the USB storage using FTP over the Internet (WAN) and local (LAN) networks. Selecting **Disabled** will disable FTP access over the Internet and allow LAN access only.
- **File Server Codepage:** Defines which character set to use when transferring data using FTP. It is recommended to leave these settings as default "Western European".

4. Review the administrator settings required for your **FTP server**. Click **Apply** to save settings

Administrator	
User Name	admin
Password	••••• Note: The default administrator password is the same as the router's default management login password.

- **User Name:** Enter the user name to be used to access your files.
- **Password:** Enter the password for the user name.

5. Review the **User Account List** section. Click **Apply** to save settings

User Account List			
User Name	Password	Permission	Enabled
		Read Only ▾	<input type="checkbox"/>
		Read Only ▾	<input type="checkbox"/>
		Read Only ▾	<input type="checkbox"/>
		Read Only ▾	<input type="checkbox"/>
		Read Only ▾	<input type="checkbox"/>

- **User Name:** Enter the user name to be used to access your files.
- **Password:** Enter the password for the user name.
- **Permission:** Select the permission you will grant to the user
- **Enabled:** Click to activate user account.

Signing up for a Dynamic DNS service (outlined in [Identify Your Network](#) section pg.39) will provide identification of the router's network from the Internet. You can access your shared files over the Internet by typing ex. [ftp://<router'sWANIPAddress>](#) or [ftp://myDDNSservice](#) in your web browser or file explorer address bar. You can access your share files locally by typing [ftp://<router'sLANIPAddress>](#) in your web browser or file explorer address bar.

You can find your router's WAN IP address settings under *Advanced > Administrator > Status*.

Virtual Private Networking (VPN)

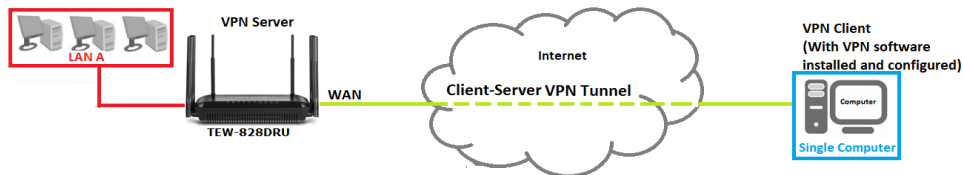
Creating a Virtual Private Network

What is a VPN?

A VPN provides secure communications typically over the Internet by creating a secure tunnel between two or more VPN routers (gateways) also known as a site-to-site VPN or between a single client computer and a VPN router (gateway) also known as a client-server VPN.

On your VPN router, only the following type of tunnel can be created:

- **Client-Server VPN** – A single client computer or device with VPN client software installed connects to a VPN router (gateway) allow the single client computer or device to securely communicate to the LAN network of the VPN router over the Internet.



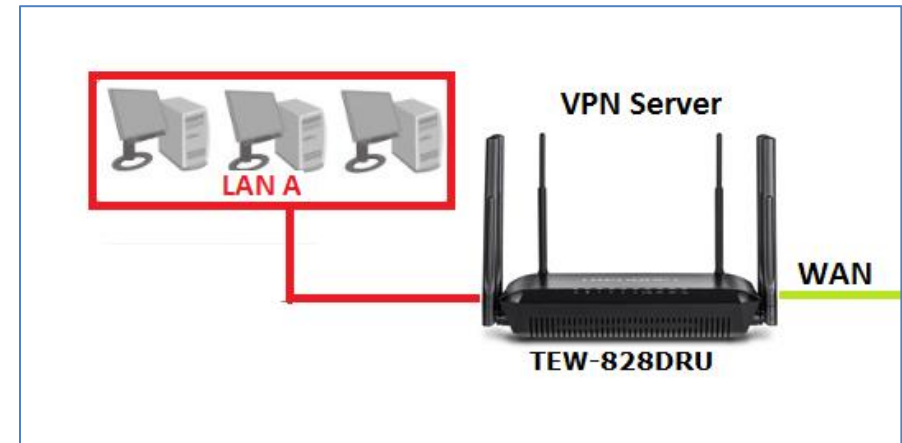
Tunneling methods supported by your router:

SSL VPN – This type of VPN is most commonly used in Client-Server VPN applications. Most modern operating systems may already include a built-in client software however, your router uses an SSL VPN implementation developed by OpenVPN which will require the installation of the OpenVPN client software supports operating systems such as Windows® XP and later (32-bit/64-bit) and Linux. One major benefit to using the SSL protocol for VPN is that most networks allow the SSL protocol to passthrough which eliminates the requirement for special rules or configuration such as PPTP/L2TP/IPsec.

Important Note: For any tunneling or VPN method used, to avoid IP address conflict and to ensure connectivity, it is required that each end (LAN IP network or single client) of the VPN tunnel is configured with a different IP network or subnet.

A. Router Configuration

Advanced > Setup > VPN



1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Setup**, then click on **VPN**.
3. Click the **OpenVPN Setting** drop-down list, and select **Enabled** to enable the VPN server on your router.

Note: You may receive a notification if Dynamic DNS is not configured on your router. If you are using VPN, it is not required however, strongly recommended to setup the Dynamic DNS feature on your router to prevent any issues with VPN connectivity if your public (WAN) Internet IP address dynamically changes. Please reference page 34 "[Identify your Network on the Internet](#)" for details on setting up the Dynamic DNS feature.

VPN Settings

OpenVPN Setting

Enabled

The additional server settings are optional (not required) and can be configured if any issues are encountered when attempting to establish VPN connectivity.

- **OpenVPN protocol:** TCP or UDP may be selected however, UDP is the default protocol used with the OpenVPN client software.
- **OpenVPN port:** A different port number may be entered however, 1194 is the default port used with the OpenVPN client software.
- **OpenVPN subnet/subnet mask:** The IP address subnet specifies the IP address range assigned to VPN client devices up establishing connectivity.

OpenVPN protocol	UDP ▾
OpenVPN port	1194
OpenVPN subnet	10.10.0.0
OpenVPN subnet mask	255.255.255.0

4. Click **Apply** to save the changes.

Apply	Cancel
-------	--------

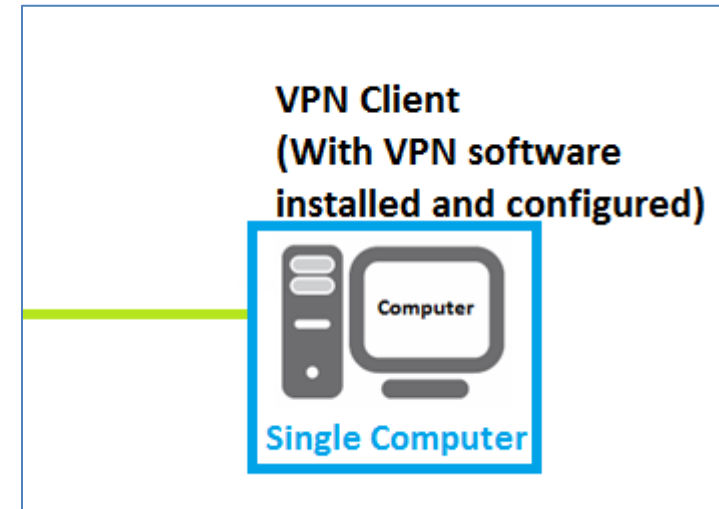
5. Under **VPN Client Configuration**, click on **Export** to download the configuration files for the VPN client computer. Please note that these files will need to be installed on the VPN client computer later on in order to establish VPN connectivity. (Default Filename: client.ovpn)

Note: Please do not change the filename for Windows installation. If installing in Linux, the *.ovpn* extension must be changed to *.conf*.


VPN Client Configuration	
Client Configuration Files	Export

B. Client Configuration

After the VPN server has been configured, the steps below will demonstrate how to setup a Windows® computer for VPN access to your router.



1. Make sure to copy or move the configuration files downloaded from your router to the VPN client computer and that your client computer has access to the Internet.
2. Download the appropriate OpenVPN software version for your operating system from the following URL: <https://openvpn.net/index.php/open-source/downloads.html>
Note: Please note there is also a link in the description in the router management page under *Advanced > Setup > VPN*.
3. Once you have downloaded the software, navigate to the location where you downloaded the file and double click to start the installation.

 openvpn-install-2.3.6-1601-x86_64 2

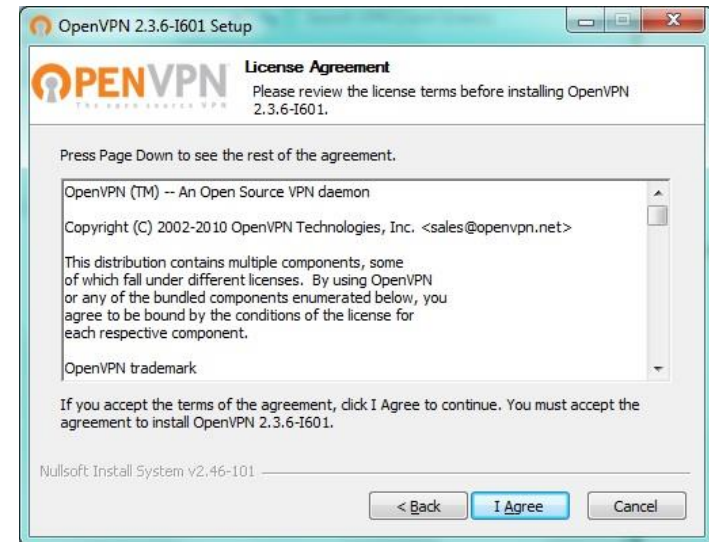
4. If prompted to run the file, click **Run**.



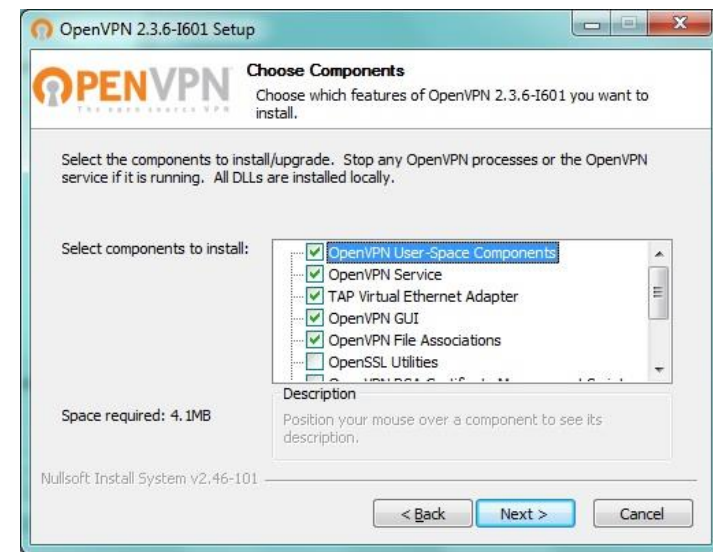
5. At the installation window, click **Next**.



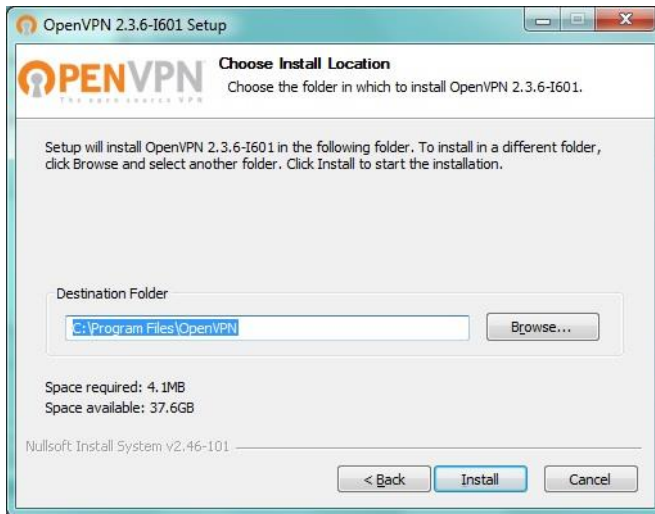
6. At the license agreement window, review the license agreement and click **I Agree**.



7. At the choose components window, click **Next**.



8. At the install location window, click **Install**.



9. At the prompt to install the TAP-Windows adapter, click **Install**.



10. At the installation completion window, click **Next**.



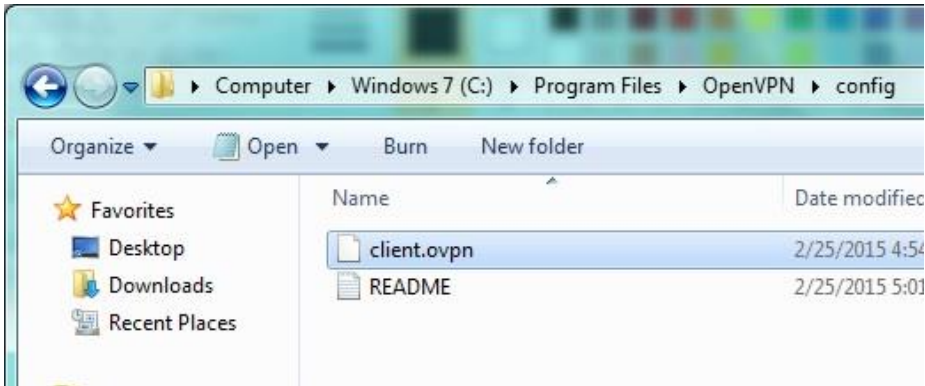
11. Make sure to uncheck the "Show Readme" and "Start OpenVPN GUI" options and click **Finish**.



12. Copy the client configuration file(s) (client.ovpn) downloaded from the router to the following path without any sub-folders.

client.ovpn

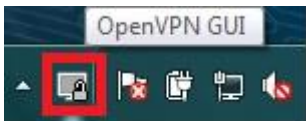
C:\Program Files\OpenVPN\config



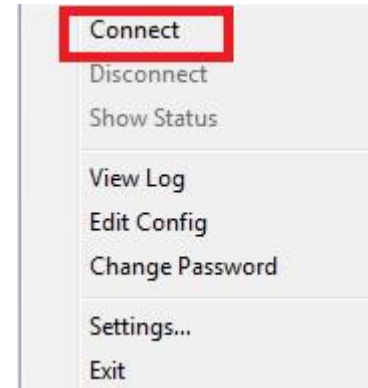
13. Double-click on the OpenVPN GUI shortcut on your desktop to start the OpenVPN Client software.



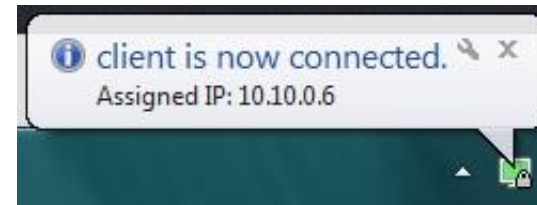
14. The OpenVPN system tray icon will appear in the bottom right corner. Right-click the icon to display the configuration menu.



15. After right-clicking the icon, the menu will appear. Click **Connect** to establish your VPN connection to your router.



16. If the VPN connection is successful, you will receive the notification below in the bottom right corner. You will be able to access resources securely from your router LAN network over the Internet such as shared folders, media, files, etc.



Note: To disconnect your VPN client connection, right click OpenVPN system tray icon and select **Disconnect**.

Router Maintenance & Monitoring

Reset your router to factory defaults

Advanced > 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 54.

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 2. 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 9).
2. Click on **Advanced** and click on **Administrator**, then click on **Settings Management**.
3. Next to **Load Factory Default Settings** and **Reset**, click **Load Default**. When prompted to confirm this action, click **OK**.

Load Factory Defaults

Load Default

Load Default

Router Default Settings

Administrator User Name	admin
Administrator Password	Please refer to sticker or device label
Router Default URL	http://tew-828dru
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 & 5GHz	Enabled
Wireless 2.4GHz & 5GHz Network Name/Encryption	Please refer to sticker or device label
Wireless 2.4GHz & 5GHz Guest Network	Disabled
Smart Connect (5GHz)	Enabled
USB SMB & FTP Settings	Disabled (Password same as Administrator)
USB SMB & FTP User Name	Disabled (Password same as Administrator)
USB SMB & FTP Password	Disabled

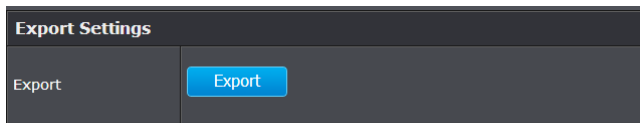
Backup and restore your router configuration settings

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:

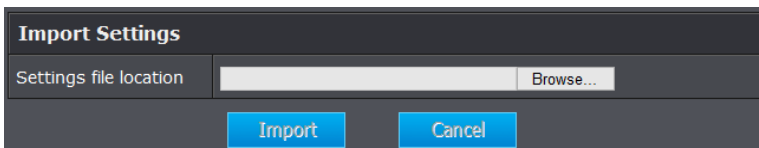
1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Administrator**, then click on **Settings Management**.
3. Next to **Export Settings** section and **Export**, click **Export**.



4. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: *TEW-828DRU_backup.cfg*)

To restore your router configuration:

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Administrator**, then click on **Settings Management**.
3. Next to **Import Settings** section and **Settings File Location**, click **Browse**.



4. A separate file navigation window should open.
5. Select the router configuration file to restore and click **Import**. (Default Filename: *TEW-828DRU_backup.cfg*). If prompted, click **Yes** or **OK**.
6. Wait for the router to restore settings.

Reboot your router

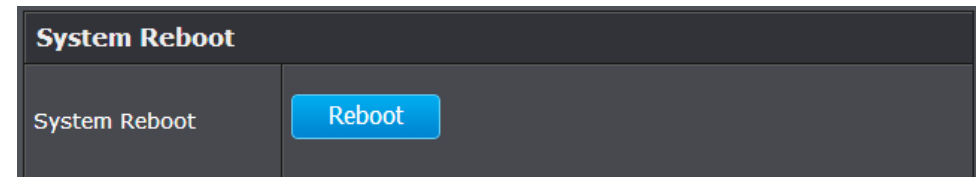
Advanced > Administrator > Settings Management

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 located on the rear panel of your router or disconnecting the power port, see "[Product Hardware Features](#)" on page 2.
Use this method if you are encountering difficulties with accessing your router management page. This is also known as a hard reboot or power cycle.
OR
- **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 9).
2. Click on **Advanced** and click on **Administrator**, then click on **Settings Management**.
3. Next to **System Reboot**, click **Reboot**.



4. Wait for the device to reboot.

Upgrade your router firmware

Advanced > Administrator > 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/>

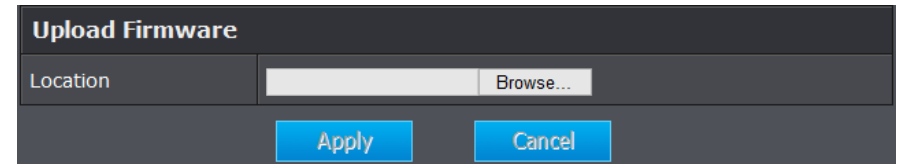
In addition, it is also important to verify if the latest firmware version is newer than the one your router is currently running. To identify the firmware that is currently loaded on your router, log in to the router, click on the Administrator section and then on the Status. The firmware used by the 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 9).
2. Click on **Advanced** and click **Administrator**, then click **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**.

Allow/deny ping requests to your router from the Internet

Advanced > Administrator > 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 9).
2. Click on **Advanced** and click on **Administrator**, then click on **Advanced Network**.
3. Next to **WAN Ping**, Click the **WAN Ping Respond** drop-down list and **Enabled** to allow your router to respond to ping requests from the Internet. You can also choose **Disabled** to block WAN ping requests from the Internet

WAN Ping	
WAN Ping Respond	Disabled ▾

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

Note: If you would like to discard the changes, click **Reset**.

Apply	Reset
--------------	--------------

Client List

Advanced > Administrator > Client Status

You can view the list of all active devices currently connected to your router.

1. Log into your router management page (see "[Access your router management page](#)" on page 9).
2. Click on **Advanced** and click on **Administrator**, then click on **Client Status**.

Wireless Devices Connected

- **IP Address:** The current IP address assigned to the device.
- **MAC Address:** The current MAC address of the device.
- **Host Name:** The host name of the device.
- **Rate:** Displays the estimated data rate established with the client.

Wired Connected Devices

#	IP Address	MAC Address	Host Name
1	192.168.10.101	00:14:D1:26:E4:76	Jeremy7

Wireless Devices Connected.

- **IP Address:** The current IP address assigned to the device.
- **MAC Address:** The current MAC address of the device.
- **Host Name:** The host name of the device.
- **Rate:** Displays the estimated data rate established with the client.

2.4GHz Wireless Connected Devices

SSID	IP Address	MAC Address	Host Name	Link Rate
TRENDnet828_2.4GHz_1A2B	192.168.10.102	D8:EB:97:25:5A:C0	PM-HP4525S	39

5GHz¹ Wireless Connected Devices

SSID	IP Address	MAC Address	Host Name	Link Rate
------	------------	-------------	-----------	-----------

5GHz² Wireless Connected Devices

SSID	IP Address	MAC Address	Host Name	Link Rate
------	------------	-------------	-----------	-----------

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 9).
2. Click on **Advanced** and click on **Administrator**, then click on **Router Status**.

System Information

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

System Info	
Firmware Version	1.0.0.2, Feb 10, 2015
System Time	Wed Jan 1 02:51:16 2014
System Up Time	02:51:25

Internet Configuration

- **Connected Type**: Displays the current WAN connection type applied.
- **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 DNS (Domain Name System) Server** – The current DNS address(es) assigned to your router port or interface configuration.

Internet Configuration	
Connected Type	DHCP Client
WAN IP Address	10.10.10.76
Subnet Mask	255.255.255.0
Default Gateway	10.10.10.254
Primary Domain Name Server	10.10.10.254
Secondary Domain Name Server	

- **DHCP WAN Type**: These buttons will be available in DHCP WAN type only.
 - **Renew**: Click this option to renew your WAN IP address.
 - **Release**: Click this option to release the WAN IP address of your router.
- **PPPoE WAN Type**: These buttons will be available in DHCP WAN type only.
 - **Connect**: Click this option to connect to your DSL ISP
 - **Disconnect**: Click this option to disconnect from your DSL ISP.

LAN Information

- **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.

LAN	
MAC Address	00:18:E7:95:85:03
IP Address	192.168.10.1
Subnet Mask	255.255.255.0

2.4GHz Wireless LAN

- **MAC Address:** The MAC address of your router's 2.4GHz wireless LAN interface configuration.
- **Network Name (SSID1) / Security Mode:** Displays the current 2.4GHz primary wireless network name and security mode assigned to your router.
- **Multiple SSID2 / Security Mode:** Displays the current 2.4GHz wireless network name and security mode of multiple SSID1 assigned to your router.
- **Multiple SSID3 / Security Mode:** Displays the current 2.4GHz wireless network name and security mode of multiple SSID2 assigned to your router.
- **Guest Network / Security Mode:** Displays the current 2.4GHz wireless network name and security mode of the guest network assigned to your router.

2.4GHz Wireless Network (802.11n/b/g)	
MAC Address	D8:EB:97:AD:EB:45
Channel	4
Network Name (SSID1) / Security Mode	TRENDnet828_2.4GHz_1A2B/WPA2-PSK
Multiple SSID2 / Security Mode	
Multiple SSID3 / Security Mode	
Guest SSID / Security Mode	TRENDnet828_2.4GHz_guest/Disable

5GHz (5GHz¹ or 5GHz²) Wireless LAN

- **MAC Address:** The MAC address of your router's 5GHz wireless LAN interface configuration.
- **Network Name (SSID1) / Security Mode:** Displays the current 5GHz primary wireless network name and security mode assigned to your router.
- **Multiple SSID2 / Security Mode:** Displays the current 5GHz wireless network name and security mode of multiple SSID1 assigned to your router.
- **Multiple SSID2 / Security Mode:** Displays the current 5GHz wireless network name and security mode of multiple SSID2 assigned to your router.
- **Guest Network / Security Mode:** Displays the current 5GHz wireless network name and security mode of the guest network assigned to your router.

5GHz ¹ Wireless Network (802.11ac/a/n)	
MAC Address	D8:EB:97:AD:EB:49
Channel	48
Network Name (SSID1) / Security Mode	TRENDnet828_5GHz_1A2B/WPA2-PSK
Multiple SSID2 / Security Mode	
Multiple SSID3 / Security Mode	
Guest SSID / Security Mode	TRENDnet828_5GHz1_guest/Disable

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 9).
2. Click on **Advanced** and click on **Administrator**, then click on **IPv6 Status**

IPv6 Internal Network Configuration	
Connected Type	Auto Configuration (SLAAC/DHCPv6)
Network Status	Disconnected
WAN IPv6 Address	
IPv6 Default Gateway	
Primary IPv6 DNS Server	
Secondary IPv6 DNS Server	
LAN IPv6 Address	
LAN IPv6 Link-Local Address	fe80::daeb:97ff:fead:eb44/64
LAN IPv6 Prefix	

View your router log*Advanced > 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 9).
2. Click on **Advanced** and click on **Administrator**, then click on **System Log**.
3. Check the **Enable System Log** option to enable logging. Then click **Apply**. The logging will display in the log window.

Note: Clicking **Refresh** will refresh the page to ensure display of the most recent logging information. Click **Clear** will clear and delete all of the current logging information.

System Log	
Enable System Log	<input checked="" type="checkbox"/>

Log Window

```
Jan 10 16:47:20 user.warn kernel: IN=br0 OUT=eth1 SRC=192.168.10.105 DST=131.253.34.240
LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=7198 DF PROTO=TCP SPT=49461 DPT=443 WINDOW=65535
RES=0x00 SYN URG=0
Jan 10 16:47:26 user.warn kernel: IN=br0 OUT=eth1 SRC=192.168.10.105 DST=131.253.34.240
LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=7199 DF PROTO=TCP SPT=49461 DPT=443 WINDOW=65535
RES=0x00 SYN URG=0
```

Clicking **Export** will allow you to download the log file to your local hard drive.

Export Log	
Export	<input type="button" value="Export"/>

Router Management Page Structure

BASIC

- Network Status
- Wireless
 - 2.4GHz Settings & Security
 - 5GHz Settings & Security
 - Smart Connect
- Guest Network
- Parental Control
 - Website Filter
 - IP Address Filter
 - MAC Address Filter

ADVANCED

- Administrator
 - Management
 - Administrator Password
 - Dynamic DNS
 - Remote Management
 - Upload Firmware
 - Settings Management
 - Export/Import configuration
 - Reset to factory default
 - Reboot

- Time
- Schedule
- Router Status
- IPv6 Status
- System Log
- Advanced Network
 - UPnP
- Client Status
- Setup
 - LAN Settings
 - IP Address Settings
 - DHCP Server Settings
 - DHCP Reservation
 - WAN Settings
 - Routing
 - IPv6
 - QoS
 - Wizard
 - VLAN
 - VPN
- Wireless 2.4GHz
 - Multiple SSID
 - WDS
 - Advanced

- WPS
- Wireless 5GHz
 - Multiple SSID
 - WDS
 - Advanced
 - WPS
- Security
 - Access Control (IP Protocol Filter)
- Firewall
 - DMZ
 - Virtual Server
 - Special Applications
 - Gaming
 - ALG
- USB
 - Samba Server
 - FTP Server
 - DLNA Server
 - Eject Device

Technical Specifications

Standards

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x
- IEEE 802.3ab
- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n (2.4 GHz 600 Mbps TurboQAM™*, 5 GHz up to 450 Mbps)
- IEEE 802.11ac (Band 1 and Band 2 up to 1300 Mbps)

Hardware Interface

- 4 x Gigabit LAN ports
- 1 x Gigabit WAN port
- 1 x USB 3.0 (Storage FTP, Samba)
- 1 x USB 2.0 (Storage FTP, Samba)
- Power switch
- WPS button
- Reset button
- LED indicators

Special Features

- Smart Connect automatically groups slower and faster AC devices to separate WiFi AC bands
- Multi-language interface: English, French, Spanish, German, Russian
- Pre-encrypted wireless network
- IPv6 support
- 1 guest network per band with option for internet access only
- Up to 2 additional SSIDs per band
- Dynamic DNS support for dyn.com and no-ip.com
- Samba/FTP server support

- Implicit and Explicit Beamforming

Access Control

- Wireless encryption up to WEP, WPA/WPA2-PSK, WPA/WPA2-RADIUS
- Firewall: NAT, SPI, Virtual Server, Special Applications, Gaming, DMZ Host, allow/deny ping request from internet
- ALG: PPTP/L2TP VPN Passthrough, Telnet, POP3/SMTP/TFTP/FTP/RTP/SIP Passthrough
- Parental (Access) Controls: MAC, URL, IP Filter
- OpenVPN support

Quality of Service

- WMM
- Inbound/outbound 5 priority queues

Internet Connection Types

- Dynamic IP (DHCP)
- Static IP (Fixed)
- PPPoE (Dynamic IP/Static IP)
- PPTP (Dynamic IP/Static IP)
- L2TP (Dynamic IP/Static IP)
- IPv6 (Static, Auto-configuration (SLAAC/DHCPv6), Link-Local, 6to4, 6rd)

Management/Monitoring

- Local/remote web based management
- Upgrade firmware
- Backup/restore configuration
- Internal logging
- Reboot
- Restore to factory defaults
- Ping test

Routing

- Static

Frequency

- 2.412 - 2.462 GHz
- 5.180 – 5.825 GHz

Modulation

- 802.11b: CCK, DQPSK, DBPSK
- 802.11a/g: OFDM with BPSK, QPSK and 16/64-QAM
- 802.11n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM with OFDM
- 802.11ac: OFDM with BPSK, QPSK and 16/64/256-QAM

Media Access Protocol

- CSMA/CA with ACK

Antenna Gain

- 2.4 GHz: 3 x 4.6 dBi (max.) external/5 GHz: 6 x 5 dBi (max.) external

Wireless Output Power

- 802.11a: 19 dBm (max.) @ 54 Mbps
- 802.11b: 26 dBm (max.) @ 11 Mbps
- 802.11g: 20 dBm (max.) @ 54 Mbps
- 802.11n (2.4 GHz): 20 dBm (max.) @ 600 Mbps
- 802.11n (5 GHz): 19 dBm (max.) @ 450 Mbps
- 802.11ac: 19 dBm (max.) @ 1300 Mbps

Receiving Sensitivity

- 802.11a: -72 dBm (typical) @ 54 Mbps
- 802.11b: -84 dBm (typical) @ 11 Mbps
- 802.11g: -75 dBm (typical) @ 54 Mbps
- 802.11n (2.4 GHz): -68 dBm (typical) @ 600 Mbps
- 802.11n (5 GHz): -68 dBm (typical) @ 450 Mbps
- 802.11ac: -55 dBm (typical) @ 1300 Mbps

Wireless Channels

- 2.4 GHz: 1-11
- 5 GHz: 36, 40, 44, 48, 149, 153, 157, 161, 165

Power

- Input: 100 – 240 V AC, 50 - 60 Hz
- Output: 12 V DC, 3.5 A external power adapter
- Consumption: 37.5 Watts max.

Operating Temperature

- 0 – 40 °C (32 – 104 °F)

Operating Humidity

- Max. 85% non-condensing

Certifications

- FCC

Dimensions

- 240 x 170 x 45 mm (9.5 x 6.7 x 1.8 in)

Weight

- 581 g (20.5 oz.)

*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and cover-age will vary depending on interference, network traffic, building materials and other conditions. For maximum performance of up to 1.3 Gbps use with a 1.3 Gbps 802.11ac wireless adapter. 802.11n 2.4 GHz TurboQAM speeds requires clients with TurboQAM support.

Troubleshooting

Q: I typed <http://tew-828dru> 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:

Access the router using the default IP address 192.168.10.1.

<http://192.168.10.1>

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 7/8/8.1

- 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 20 if you continue to have wireless connectivity problems.

Appendix

How to find your IP address?

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

Command Prompt Method

Windows 2000/XP/Vista/7/8/8.1

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

MAC OS X

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

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

Graphical Method

MAC OS 10.6/10.5

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

MAC OS 10.4

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

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

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

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

Windows 7/8/8.1

- 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 7/8/8.1

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.



IMPORTANT NOTE:

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

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

This device is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

Industry Canada Statement

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

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

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

This device and its antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with IC multi-transmitter product procedures.

Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.

les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une

utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

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

This radio transmitter (6337A-TEW828DRU) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (6337A-TEW828DRU) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Note: 以上Mark紅色的地方是要填IC ID或型號, 此句有放, 使用手冊要加列天線list (天線list請與測試報告一致)。

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-828DRU – 3 Years Warranty

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

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

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

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

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

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

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

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

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR 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

2015/2/25



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