

User's Guide

TRENDNET[®]



AC2600 MU-MIMO WiFi Router

TEW-827DRU

Table of Contents

Product Overview1

Package Contents	1
Features	2
Product Hardware Features.....	3
Application Diagram	4

Router Setup.....5

Creating a Home Network	5
Router Installation	6
Connect additional wired devices to your network.....	9

Basic Router Settings.....10

Access your router management page.....	10
Network Status	10
Committing your router configuration changes	11
Wireless Settings	12
Guest Network.....	13
Parental Control.....	15
Access Rule (MAC/IP Filter)	15
Website Filter.....	17
Web Management System (Router Limits™).....	18
Setup your router with Router Limits	18
Router Limits Content Management	20

Wireless Networking and Security23

How to choose the type of security for your wireless network	23
Secure your wireless network	24
Connect wireless devices to your router	26
Connect wireless devices using WPS	26

PBC (Software/Virtual Push Button).....	27
PIN (Personal Identification Number).....	27

Advanced wireless settings	28
Multiple SSID	28
Wireless bridging using WDS (Wireless Distribution System)	29
Wireless Client Bridge Mode	31
Advanced Settings	33
Steps to improve wireless connectivity	35

Advanced Router Settings36

Change your router login password	36
Manually configure your Internet connection	36
IPv6 Settings	37
Clone a MAC address.....	38
Change your router IP address	39
Set up the DHCP server on your router	39
Set up DHCP reservation	40
Enable/disable UPnP on your router	42
Enable/disable Application Layer Gateways (ALG).....	42
Denial of Service (DoS)	43
Allow/deny multicast streaming.....	43
IPv6 Firewall	44
Identify your network on the Internet	45
Set your router date and time	46
Create schedules	47
Access Control (IP Protocol Filter)	48
Inbound Filter	49
Open a device on your network to the Internet.....	50
DMZ	50

Virtual Server	50	Ping Watchdog	71
Special Applications	52	Auto Reboot	72
Allow remote access to your router management page	54	Wireless Client List	72
Add static routes.....	54	Check the router system information	73
Enable Dynamic Routing.....	55	View your router log.....	75
Using External USB Storage	56	Router Management Page Structure	76
File Sharing Server	56	Technical Specifications	77
iTunes Server	56	Troubleshooting	79
DLNA Server	56	Appendix	80
Samba Server	56		
FTP (File Transfer Protocol) Server	58		
BitTorrent Client Settings	59		
Virtual Private Networking (VPN)	60		
Creating a Virtual Private Network.....	60		
Router Maintenance & Monitoring.....	66		
Reset your router to factory defaults	66		
Router Default Settings	66		
Backup and restore your router configuration settings	67		
Reboot your router	67		
Upgrade your router firmware	68		
Allow/deny ping requests to your router from the Internet	70		
How to capture network packets	70		
Diagnostic Tools.....	71		

Product Overview



TEW-827DRU

Package Contents

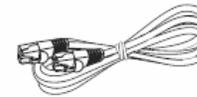
In addition to your router and 4 detachable high gain antennas, the package includes:



Power adapter (12V, 3A)



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 AC2600 MU-MIMO WiFi Router, model TEW-827DRU, is built to perform in a busy connected home. It generates two quad-stream WiFi networks—a 1,733Mbps WiFi AC and a concurrent 800Mbps WiFi N network. MU-MIMO technology processes multiple data streams simultaneously, increasing real-time WiFi performance when multiple devices access the network. Use the gigabit Ethernet ports and USB 3.0 share port to further extend network connectivity.

Easy Setup

Get up and running in minutes with the intuitive guided setup

AC2600 WiFi

Concurrent dual band, quad-stream 1,733Mbps WiFi AC + 800Mbps WiFi N bands

MU-MIMO Performance

MU-MIMO technology enables the router to process multiple data streams simultaneously—with so many connected devices in today's home, MU-MIMO increases real-time WiFi performance

Pre-Encrypted Wireless

For added convenience the WiFi is pre-encrypted with its own unique password

Wireless Coverage

External high gain antennas maximize wireless coverage

Gigabit Ports

Four gigabit ports support high performance wired connections

USB 3.0 Share Port

Share content across the network with the USB 3.0 share port

Guest Network

Create an isolated WiFi network for guest internet access only

Parental Controls

Limit access to specific websites and control connected device access to the network

Targeted Beamforming

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

File Sharing Support

Management controls to optimize BitTorrent sharing, iTunes server streams, and Samba (SMB) clients

*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions. For maximum performance of up to 1.733 Gbps use with a 1.733 Gbps 802.11ac wireless adapter. For maximum performance of up to 800 Mbps, use with an 800 Mbps 802.11n wireless adapter. Multi-User MIMO (MU-MIMO) requires the use of multiple MU-MIMO enabled wireless adapters.

** Due to regulatory requirements, the wireless channels specified cannot be statically assigned, but will be available within the available wireless channels when set to auto.

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, BitTorrent client, iTunes Server, and DLNA server.
2	Gigabit LAN Ports 1-4 (Black)	Connect Ethernet cables (also called network cables) from your router LAN ports to your wired network devices.
3	Gigabit WAN/Internet Port (Yellow)	Connect an Ethernet cable from your router Internet port to your modem.
4	WPS Button (Wi-Fi Protected Setup)	Push and hold this button for 3 seconds and release to activate WPS. The Power LED on front panel will blink when WPS is activated.
5	On/Off Power Switch	Push the router On/Off power switch to turn your router "On" (Inner position) or "Off" (Outer position).
6	Power Port	Connect the included power adapter from your router power port and to an available power outlet.
7	Reset Button	Using a pen or paperclip, push and hold the reset button for 15 seconds and release 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	Gigabit 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 Wireless LEDs	Solid Blue – 2.4GHz/5GHz radio is on. Blinking Blue – Data Transmit/Receive. Off – 2.4GHz/5GHz radio is off.
5	USB LED	Solid Blue – USB device is connected. Blinking Blue – Data Transmit/Receive. Off – No USB device connected.

Application Diagram

High Performance WiFi

Concurrent quad-stream WiFi networks and gigabit ports seamlessly network connected devices and high bandwidth streams such as 4K video.

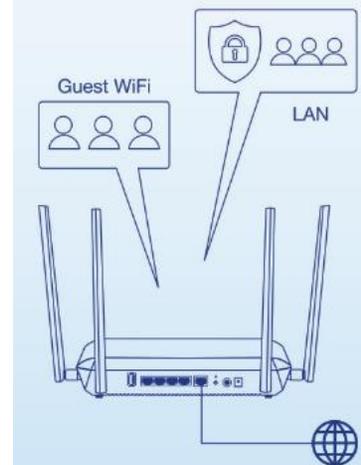
Built For Busy Homes

MU-MIMO technology processes multiple data streams simultaneously, increasing real-time WiFi performance when multiple devices access the network.



WiFi Guest Network

Create an isolated network for guest internet access only



Router Setup

Creating a Home Network

What is a network?

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

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

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

How to set up a home network

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

2. Make sure that your modem is working properly. Your modem is often provided by your Internet Service Provider (ISP) when you sign up for Internet service. If your modem is not working contact your ISP to verify functionality.
3. Set up your router. See "How to setup your router" below.
4. To connect additional wired computers or wired network devices to your network, see "[Connect additional wired devices to your network](#)" on page 9.
5. To set up wireless 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 6 for more detailed installation instructions.

Where to find more help

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

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

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)
 MTU: _____ (Default: 1500, change if required by ISP)
 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)
 MTU: _____ (Default: 1500, change if required by ISP)
 MAC Address: ____:____:____:____:____ Clone your PC MAC Address (Optional)

3. PPPoE Dynamic IP (DHCP) / PPPoE Static IP – Standard & Russian

Type (Dynamic IP/DHCP or Static IP)
 IP Address (Static IP): _____ (e.g. 215.24.24.129)
 Username: _____
 Password: _____
 Service Name: _____ (Optional)
 DNS Servers Address 1 (Static IP): _____
 DNS Servers Address 2 (Static IP): _____ (Optional)
 Reconnect Mode: Always / On Demand / Manual (Optional)

MTU: _____ (Default: 1500, change if required by ISP)
 MAC Address: ____:____:____:____:____ Clone your PC MAC Address (Optional)

4. PPTP - Standard & Russian

Type (Dynamic IP/DHCP or Static IP)
 PPTP IP Address: _____ (e.g. 215.24.24.129)
 PPTP Subnet Mask: _____ (e.g. 255.255.255.0)
 PPTP Gateway: _____ (e.g. 215.24.24.1)
 PPTP Server: _____ (e.g. 215.24.24.150)
 Username: _____
 Password: _____
 Reconnect Mode: Always / On Demand / Manual (Optional)
 DNS Servers Address 1 (Static IP): _____
 DNS Servers Address 2 (Static IP): _____ (Optional)
 MTU: _____ (Default: 1500, change if required by ISP)
 MAC Address: ____:____:____:____:____ Clone your PC MAC Address (Optional)
 MPPE (Microsoft® Point-to-Point Encryption) w/ MS-CHAPv2 Enabled: ____ (Yes or No)

5. L2TP - Standard & Russian

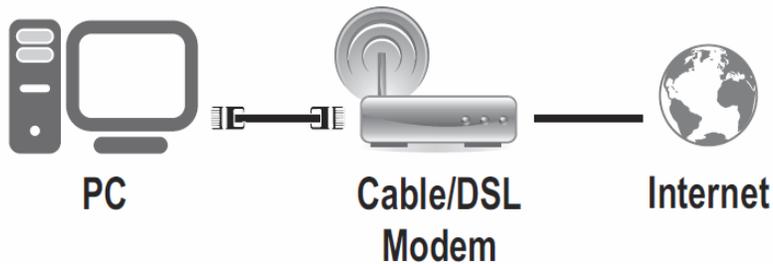
Type (Dynamic IP/DHCP or Static IP)
 L2TP IP Address: _____ (e.g. 215.24.24.129)
 L2TP Subnet Mask: _____ (e.g. 255.255.255.0)
 L2TP Gateway: _____ (e.g. 215.24.24.1)
 L2TP Server: _____ (e.g. 215.24.24.150)
 Username: _____
 Password: _____
 Reconnect Mode: Always / On Demand / Manual (Optional)
 DNS Servers Address 1 (Static IP): _____
 DNS Servers Address 2 (Static IP): _____ (Optional)
 MTU: _____ (Default: 1500, change if required by ISP)
 MAC Address: ____:____:____:____:____ Clone your PC MAC Address (Optional)
 MPPE (Microsoft® Point-to-Point Encryption) w/ MS-CHAPv2 Enabled: ____ (Yes or No)

Hardware Installation

1. Attach the antennas to the router and position them for the best WiFi coverage. It is recommended that you position all of the antennas vertically as shown below.



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

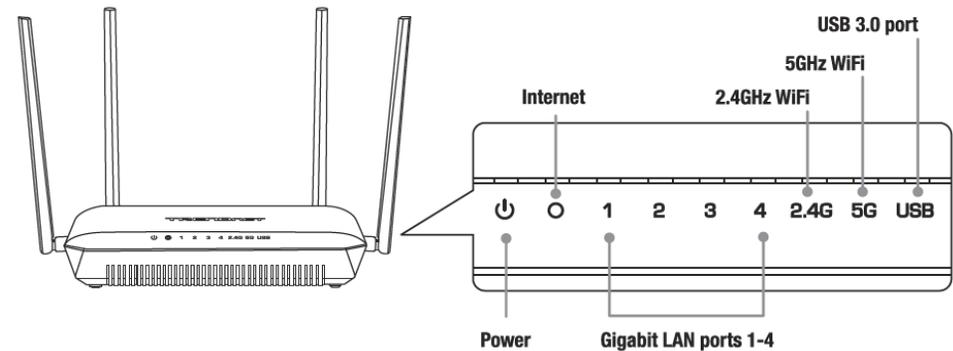


3. Turn off your modem.
 4. Disconnect the Network cable from your computer to your modem.
- Note:** If your modem includes a battery backup, remove the battery backup as well.

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



7. Connect the power adapter to the router and then to a power outlet. Push the power on the back of the router to the On (Inner) position.
8. Turn on your modem.
9. Verify that the blue LEDs on the front of the router (**Power, Internet, 2.4G, 5G**) and port number of your connected computer (**1, 2, 3, or 4**) are on.



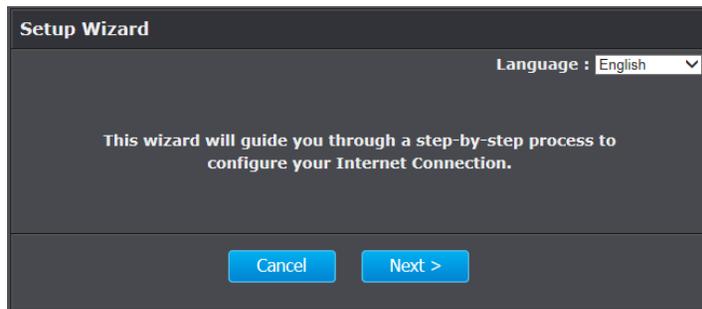
Setup Wizard

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-827dru> 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**.



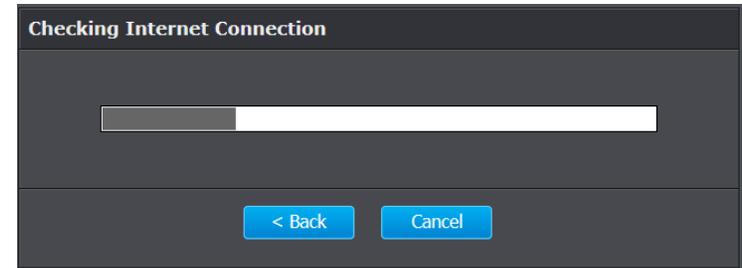
2. Select your Language and click **Next**.



3. The wizard will automatically detect your Internet connection.

Note: If the wizard is unable to detect your Internet connection type, you will be prompted to select it. 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 **Save** to complete the wizard.

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.

Confirm Settings	
Internet IP Address :	10.10.10.32
Internet Subnet Mask :	255.255.255.192
Internet Gateway Address :	10.10.10.62
DNS Server :	10.10.10.62/0.0.0.0
WAN MAC Address :	00:18:E7:95:6A:46
2.4GHzWireless Network Name (SSID) :	TRENDnet827_2.4GHz
2.4GHzWireless Security :	WPA2-PSK
5GHz Wireless Network Name (SSID) :	TRENDnet827_5GHz
5GHz Wireless Security :	WPA2-PSK

Preset Wireless Settings	
Wi-Fi Name/SSID (AC/N) TRENDnet827_5GHz_XXXX (N/B/G) TRENDnet827_2.4GHz_XXXX	
Wi-Fi Password XXXXXXXXXX	
Management Login http://tew-827dru username: admin password: XXXXXX	

Please wait while changes are being applied. On the following screen, click **Back** to go back to router login page.



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-827dru> 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-827dru> or IP address <http://192.168.10.1>. Your router will prompt you for a user name and password.



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

User Name: **admin**

Password: (xxxxxxxx)

Note: User Name and Password are case sensitive.

TEW-827DRU LOGIN	
User Name :	<input type="text"/>
Password :	<input type="password"/>
Language :	English <input type="button" value="v"/>
<input type="button" value="Login"/>	

Preset Wireless Settings	
Wi-Fi Name/SSID (AC/N)	TRENDnet827_5GHz_XXXX
(N/B/G)	TRENDnet827_2.4GHz_XXXX
Wi-Fi Password	XXXXXXXXXX
Management Login	http://tew-827dru
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 10).
2. Click on **Basic** and click on **Network Status**.

Network Status

Internet

Internet connection

Wireless

2.4GHz Name (SSID):
TRENDnet827_2.4GHz

5GHz Name (SSID):
TRENDnet827_5GHz

2.4GHz: WPA2-PSK (High Security)

5GHz: WPA2-PSK (High Security)

Guest Network

2.4GHz Guest Network (SSID):
Disabled

5GHz Guest Network (SSID):
Disabled

Connected Devices

JEREMY7

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.

Committing your router configuration changes

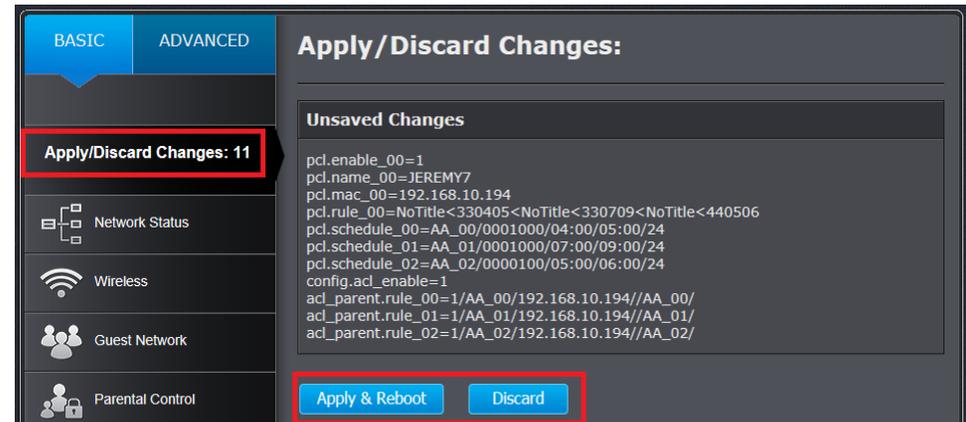
Apply/Discard Changes

The router allows you to make multiple changes to the configuration and apply or discard all the configuration changes you have made all at the same time using the Apply/Discard Changes section in the router management page.

After you have made multiple changes in the router configuration page, you will notice the Apply/Discard Changes counter with increase from 0 depending on the amount of changes you have applied. If the counter is not 0, you have pending configuration changes that will need to be applied.

Once you have completed your changes, to commit your changes to the router, you must click on the **Apply/Discard** section in the router management page, and click **Apply & Reboot** to commit the changes to the router. You can also click **Discard** to click discard all of the changes you have configured.

IMPORTANT NOTE: If you do not apply changes under the **Apply/Discard** section after you have made your router configuration changes, your router configuration changes will not be applied.



Wireless Settings

Basic > Wireless (2.4GHz or 5GHz)

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 18 [Wireless Networking & Security](#) to configure your wireless security settings.

1. Log into your router management page (see “[Access your router management page](#)” on page 10).
2. Click on **Wireless** and click on **Basic** scroll down to **Wireless Network Settings** (2.4GHz or 5GHz)
3. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

- **Radio On/Off** – Check the radio on/off button to enable/disable the wireless radio.

Note: It is recommended to keep wireless radios enabled.

New Schedule – The schedule function allows you to define a schedule when the wireless should be turned on. To define a new schedule, click **New Schedule** and refer to page 39 “[Create Schedules](#)”. After you have created a new schedule, 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 38 to configure [Time Settings](#) and see page 39 “[Create Schedules](#)” to create a schedule.

Radio On/Off	<input checked="" type="checkbox"/>	Always	New Schedule
--------------	-------------------------------------	--------	--------------

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.
- Wireless devices that only support 802.11n or 802.11a will not be able to connect to a wireless network that is set to 802.11ac only mode.
- Wireless devices that only support 802.11b or 802.11g will not be able to connect to a wireless network that is set to 802.11n only mode.
- Wireless devices that only support 802.11b will not be able to connect to a wireless network that is set to 802.11g only mode.
- Wireless devices that only support 802.11a will not be able to connect to a wireless network that is set to 802.11n only mode.

Wireless Mode	2.4GHz 802.11 b/g/n mixed mode
	2.4GHz 802.11 b/g mixed mode
	2.4GHz 802.11 n only
	2.4GHz 802.11 b/g/n mixed mode

Wireless Mode	5GHz 802.11 a/n/ac mixed mode
	5GHz 802.11 a only
	5GHz 802.11 n only
	5GHz 802.11 a/n mixed mode
	5GHz 802.11 a/n/ac mixed mode

- **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 Network Name (SSID)	TRENDnet827_2.4GHz
------------------------------	--------------------

- **Broadcast Network Name (SSID)**
 - **Enable** - allows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your router.
 - **Disable** - 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) Enable Disable

- **Frequency (Channel)** – Selecting the **AutoSelect** option will set your router to scan for the appropriate wireless channel to use automatically. 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) AutoSelect ▼

- **Channel Width:** 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 Width 20 MHz Auto 20/40 MHz

Channel Width 20 MHz Auto 20/40 MHz Auto 20/40/80 MHz

Guest Network

Basic > Guest Network (2.4GHz or 5GHz)

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

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Basic** and click on **Guest Network**.
3. Review the Guest Zone settings. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

Choose which band to enable the Guest Network (Wireless – 2.4GHz or 5GHz):

- **Radio On/Off** – Check this option to enable the wireless guest network.
 - New Schedule** – The schedule function allows you to define a schedule when the wireless guest network should be turned on. To define a new schedule, click **New Schedule** and refer to page 39 "[Create Schedules](#)". After you have created a new schedule, 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 38 to configure [Time Settings](#) and see page 39 "[Create Schedules](#)" to create a schedule.

Radio On/Off Always ▼ New Schedule

- **Wireless Network Name (SSID)** - This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. It is recommended to use a different name from your primary wireless network to a name that you can easily identify and differentiate from the

primary. You can reference your guests to access this network instead of the primary.

Wireless Network Name (SSID)	<input type="text"/>
------------------------------	----------------------

- **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 and allowed 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)
----------------------	--

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

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

4. Under Security Mode, 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	
Security Mode	<div style="border: 1px solid black; padding: 2px;"><p>WPA2-Personal ▼</p><p>Disable</p><p>WEP-OPEN</p><p>WEP-SHARED</p><p>WEP-AUTO</p><p>WPA-Enterprise</p><p>WPA-Personal</p><p style="background-color: #e0e0e0;">WPA2-Personal</p><p>WPA2-Personal Mixed</p><p>WPA2-Enterprise</p><p>WPA2-Enterprise Mixed</p></div>

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.

Access Rule (MAC/IP Filter)

Basic > Parental Control

Every network device has a unique, 12-digit MAC (Media Access Control) address. Every network device must be assigned or configured with a specific 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 MAC address or IP address.

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Basic**, click on **Parental Control**.
3. Check **Enable** to enable the access rule.

Enable	<input checked="" type="checkbox"/>
--------	-------------------------------------

4. Enter a **Computer Name**.

Computer Name	<input type="text"/>
---------------	----------------------

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/IP Address) detected by your router.

<< Host Name	<input type="text"/>	▼
--------------	----------------------	---

5. Select which **Address Type** to apply the filter. (MAC Address or IP Address)

Address Type	<input checked="" type="radio"/> IP	<input type="radio"/> MAC
--------------	-------------------------------------	---------------------------

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

6. If the MAC or IP address was not copied by selecting the Host Name from the drop-down list in Step 4, manually enter the **MAC Address** or **IP Address** in the field. Otherwise, move on to the next step.

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

7. **Schedule** – The schedule function allows you to define a schedule when the access should be allowed for the specified device MAC address or IP address. To define a new schedule, in the Schedule section, click **Define** and a table will appear to define the time slots when access is allowed for that specific device MAC or IP address. **Note:** Before defining a schedule, please ensure your Time settings are configured correctly. See page 38 to configure [Time Settings](#).

Schedule	Define
----------	--------

Active Schedule							
Host Name	192.168.20.17						
	Sun	Mon	Tue	Wed	Thu	Fri	Sat
12AM~1AM							
1AM~2AM							
2AM~3AM							
3AM~4AM							
4AM~5AM							
5AM~6AM							

8. To define the time slots to allow access for specific days, simply click on a box corresponding to the day and time slot allocated and the box will turn blue indicating that access has been allowed for that period on that day.

For example: To allow access on Tuesdays and Wednesdays from 5AM to 6AM, click on those corresponding boxes.

When finished setting the time slots allowed, click **OK**.

Active Schedule							
Host Name	192.168.20.17						
	Sun	Mon	Tue	Wed	Thu	Fri	Sat
12AM~1AM							
1AM~2AM							
2AM~3AM							
3AM~4AM							
4AM~5AM							
5AM~6AM							

9. Click **Save** to add the rule to the table.

Parental Control List				
Enable	Computer Name	Address	Edit	Delete
1 <input checked="" type="checkbox"/>	192.168.20.17	192.168.20.17		<input type="checkbox"/>

Note: In the **Parental Control List**, you can edit a rule by clicking  under the **Edit** column next to the rule you would like to edit. You can also delete a rule or specific rules by checking the box under the **Delete** column next to the rule(s) you would like to delete. Then click **Delete** those checked rules. If you would like to delete all rules, click **Delete All**.

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 10).

2. Click on **Basic** and click on **Parental Control**.

3. Check **Enable** to enable the web URL filter rule.

Enable	<input checked="" type="checkbox"/>
--------	-------------------------------------

4. Enter a **Rule Name**.

Rule Name	<input type="text"/>
-----------	----------------------

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

URL	<input type="text" value="www.xxxxxxxx.com"/>	(ex. www.xxxxxxxx.com)
-----	---	---

6. **Schedule**— The schedule function allows you to define a schedule when the access should be active and blocking the specified website. To define a new schedule, in the Schedule section, click **Define** and a table will appear to define the time slots when the specified URL/website should be blocked.

Note: Before defining a schedule, please ensure your Time settings are configured correctly. See page 38 to configure [Time Settings](#).

Schedule	Define
----------	--------

8. To define the time slots to block access to the specified URL/websites for specific days, simply click on a box corresponding to the day and time slot allocated and the box will turn blue indicating that access has been blocked for that period on that day.

For example: To block access to the website on Tuesdays and Wednesdays from 5AM to 6AM, click on those corresponding boxes.

When finished setting the time slots allowed, click **OK**.

Active Schedule							
Host Name	192.168.20.17						
	Sun	Mon	Tue	Wed	Thu	Fri	Sat
12AM~1AM							
1AM~2AM							
2AM~3AM							
3AM~4AM							
4AM~5AM							
5AM~6AM							

9. Click **Add** to add the access rule to the table.

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

URL Filter List					
Enable	Rule Name	URL	Address	Edit	Delete
<input checked="" type="checkbox"/>	trendnet.com	www.trendnet.com	192.168.10.101		

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

Web Management System (Router Limits™)

Router Limits web management system allows you to easily setup and monitor the content accessed by devices on your network to maximize Internet bandwidth usage, control, and productivity. Sign up today for your free account.

Note: Please make sure to set your router date and time settings correctly to ensure proper functionality of the Router Limits feature. Subscription based web management filtering content services are available with account sign up. Additional upgrades may be available with an additional cost. Services may be subject to change without notice.

Note: The Router Limits feature is only available on firmware 2.05 or above. Please make sure to upgrade the router to the appropriate firmware version.

Setup your router with Router Limits

Network > VPN

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Basic** and click on **Router Limits™**.
3. Check the **Enable** option. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

Note: You may be prompted to enable NTP server or configure the router time settings to the appropriate. To ensure there are no issues activating the service or using the scheduling features with your router, please ensure the time and date settings are configured correctly. Clicking OK will automatically enable the NTP server function on your router to obtain time setting from an Internet time server.

Router Limits Settings	
Enable	<input checked="" type="checkbox"/>
Current Status	
Pairing Code	

Save

4. Wait until the Current Status is Ready and your Pairing Code has been generated. Then click **Sign Up & Activate**.

Router Limits Settings	
Enable	<input checked="" type="checkbox"/>
Current Status	Ready
Pairing Code	
SIGN UP & ACTIVATE	

4. At the signup page, click **Yes, activate my hardware**.



[Features](#) [How It Works](#) [Pricing](#) [FAQs](#)

[Sign Up](#)

[Login](#)

GREAT DECISION! LET'S GET YOU SET UP..

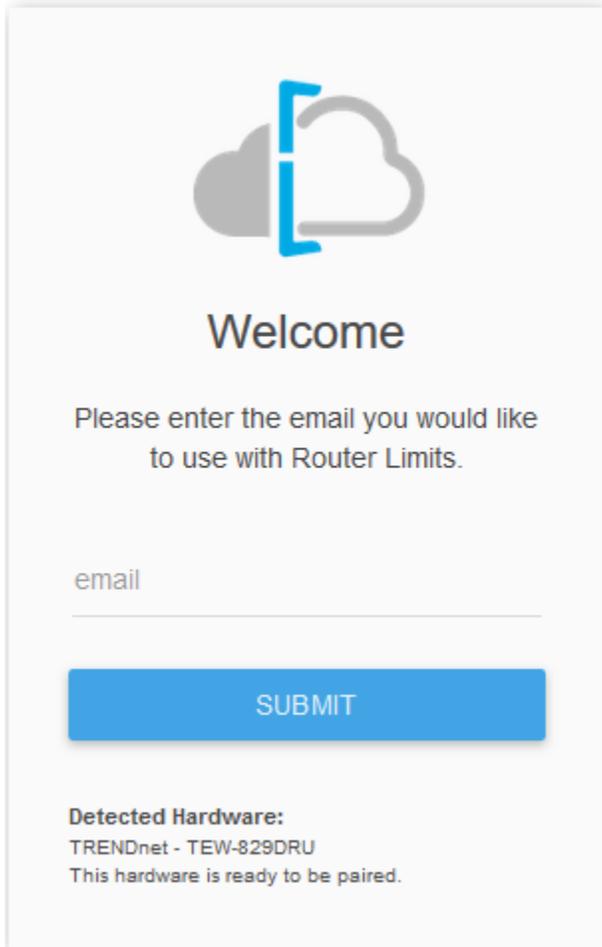
To use our service, you'll need hardware that is Router Limits Enabled.

Do you already have hardware?

Yes, activate my hardware

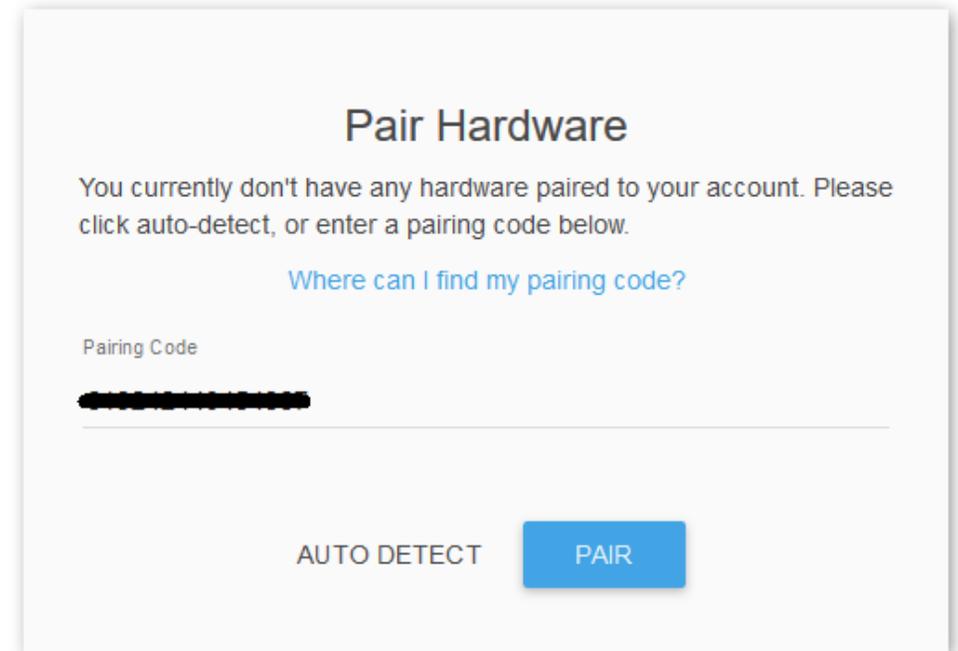
No, I need some

5. At the welcome page, enter your email address to use for account creation and sign up and click **Submit**. Follow the remaining steps to create your Router Limits account.



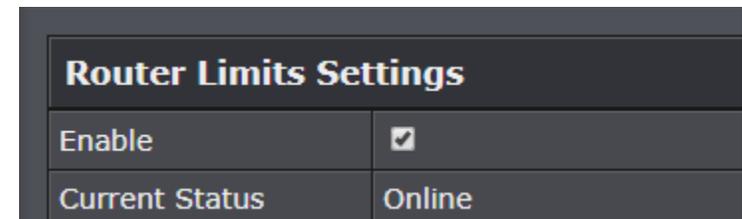
The screenshot shows a 'Welcome' page with a cloud icon. The text reads: 'Welcome', 'Please enter the email you would like to use with Router Limits.', and an 'email' input field. A blue 'SUBMIT' button is at the bottom. Below the button, it says 'Detected Hardware: TRENDnet - TEW-829DRU This hardware is ready to be paired.'

6. At the pair hardware page, the pairing code displayed should match the pairing code displayed in your router management page. If the pairing code does not match, you can click **Auto Detect** to automatically copy the router pairing code into the field or you can manually enter the correct pairing code. After you have verified the correct pairing code is entered, click **Pair**.



The screenshot shows a 'Pair Hardware' page. The text reads: 'Pair Hardware', 'You currently don't have any hardware paired to your account. Please click auto-detect, or enter a pairing code below.', and a link 'Where can I find my pairing code?'. Below this is a 'Pairing Code' input field with a blacked-out code. At the bottom are 'AUTO DETECT' and 'PAIR' buttons.

7. After your Router Limits account has been created and your router paired, you will automatically be brought to your web management dashboard. The Current Status on your router will display **Online** that the content management service is running and paired with your online account.

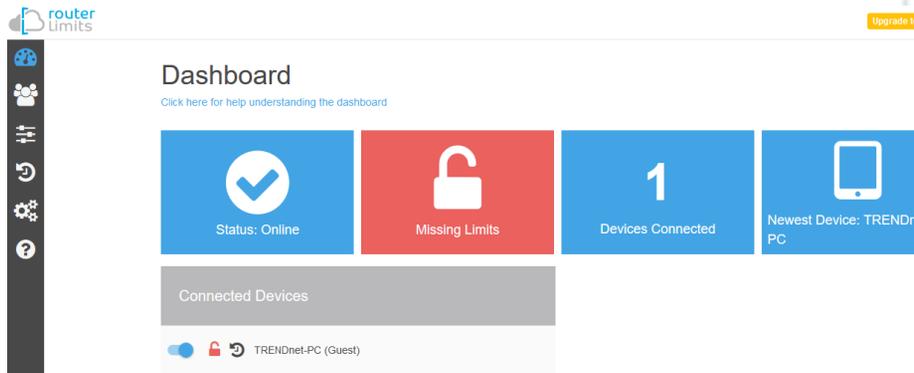


Router Limits Settings	
Enable	<input checked="" type="checkbox"/>
Current Status	Online

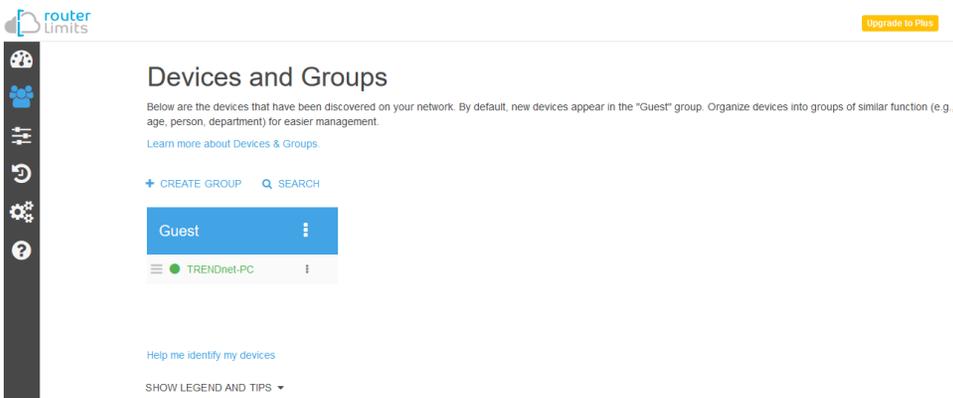
Router Limits Content Management

This section will provide a basic overview of the content management pages of your online Router Limits account.

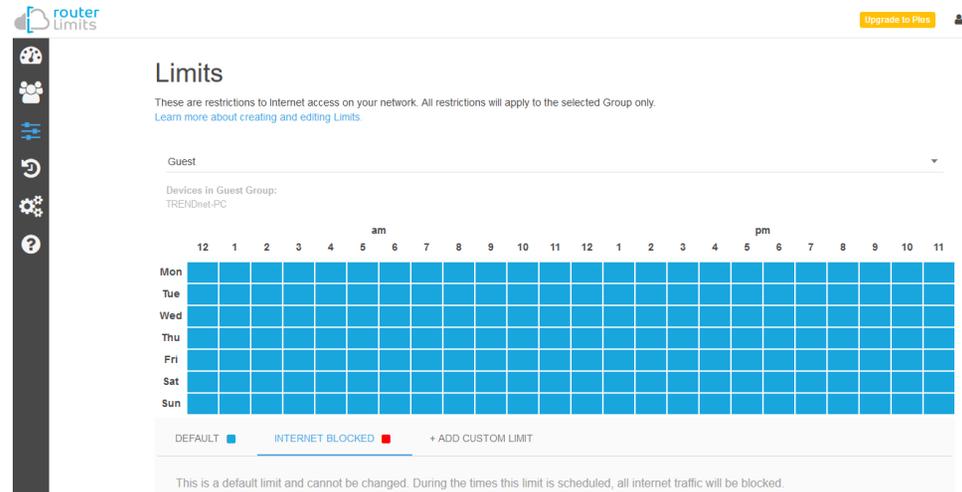
- 
Dashboard – This page displays an overview of the service status and the devices connected to your network.



- 
Devices and Groups – This page displays the groups and devices assigned to each group. Content filters and scheduling can be assigned for each group. By default, new devices are assigned to the Guest group. New groups can be created and devices reassigned to new groups for easy management.

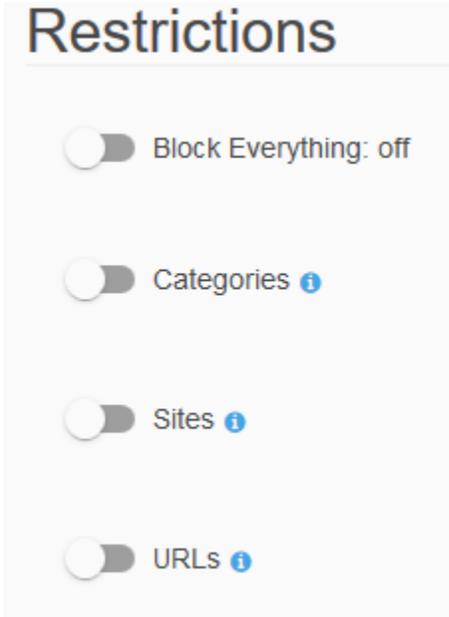


- 
Limits – Content filtering rules and scheduling are configured on this page. By default, all web content is allowed without restrictions. You can define new custom limits with a specific schedule along with a set of different restrictions or configuration options. Each template can be assigned to a specific group.



Restrictions

- **Block Everything** – Enabling this setting will completely block all Internet access. (Blacklist)
- **Categories** – Enabling this setting will block content based on categories such as social media, sports, shopping, and proxy websites, etc.
- **Sites** – Enabling this setting will block access to popular websites such as Facebook, Instagram, Youtube, Vimeo, Netflix, etc.
- **URLs** – Enabling this setting will allow you manually enter in specific domain names/URLs to block access.



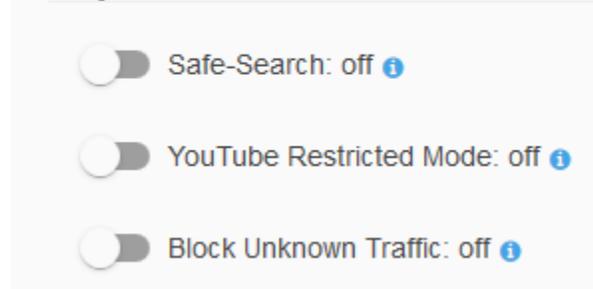
Exceptions – This setting allows you to configure exceptions and allow access.



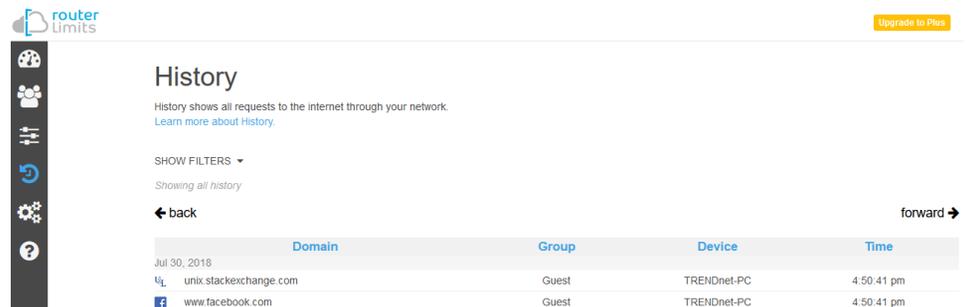
Options

- **Safe-Search** – Enables this setting enforces the use safe search to be enabled for Google and Bing search engines.
- **YouTube Restricted Mode** – Enabling this setting enforces YouTube safety mode. (Currently not supported on mobile devices)
- **Block Unknown Traffic** – Enabling this setting blocks all unknown IP addresses (specifically those used with VPN services or proxy services). It is recommended to leave this setting off unless explicitly required.

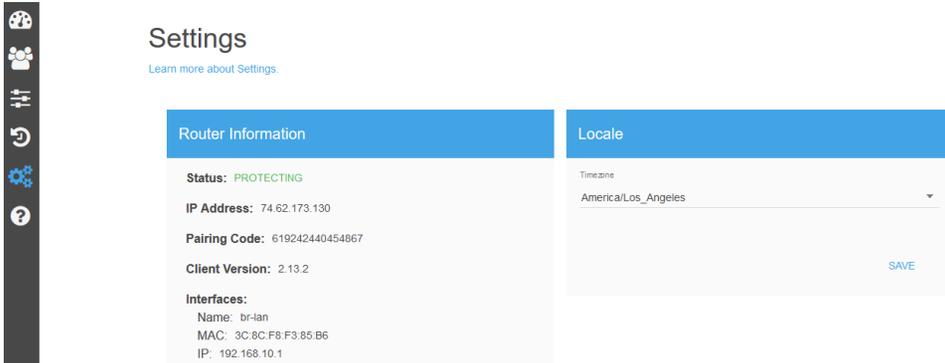
Options



-  **History** – This page will display the Internet access history through your router. This page will also displays timestamps of when websites were accessed and which devices access each site.



-  **Settings** – This page will display the current status of service account and router as well as allow you to set the time zone settings.



Settings

[Learn more about Settings.](#)

Router Information	Locale
<p>Status: PROTECTING</p> <p>IP Address: 74.62.173.130</p> <p>Pairing Code: 619242440454867</p> <p>Client Version: 2.13.2</p> <p>Interfaces:</p> <p>Name: br-lan</p> <p>MAC: 3C:8C:F8:F3:85:B6</p> <p>IP: 192.168.10.1</p>	<p>Timezone</p> <p>America/Los_Angeles</p> <p>SAVE</p>

-  **Support** – This page will display provide support on information on the Router Limits web management system and allow you to submit support tickets if needed.

You can access and manage your Router Limits account configuration settings through <https://routerlimits.com> and logging in.

If behind your router, you can also access your account by going to Services > Router Limits™ in your router management page and clicking **Manage Account**.

MANAGE ACCOUNT

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 800Mbps (11n) or 1.7 Gbps (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, 600Mbps, 800Mbps) or maximum 802.11ac data rate supported by the device (433Mbps, 867Mbps, 1.3Gbps, 1.7Gbps)

Secure your wireless network

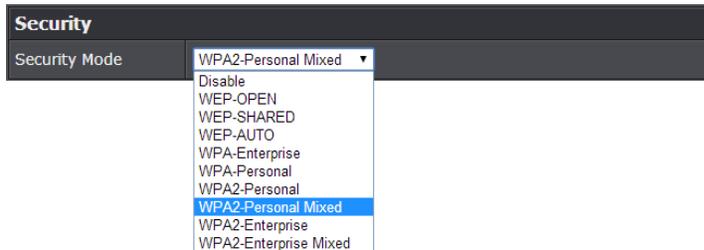
Basic > Wireless

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.

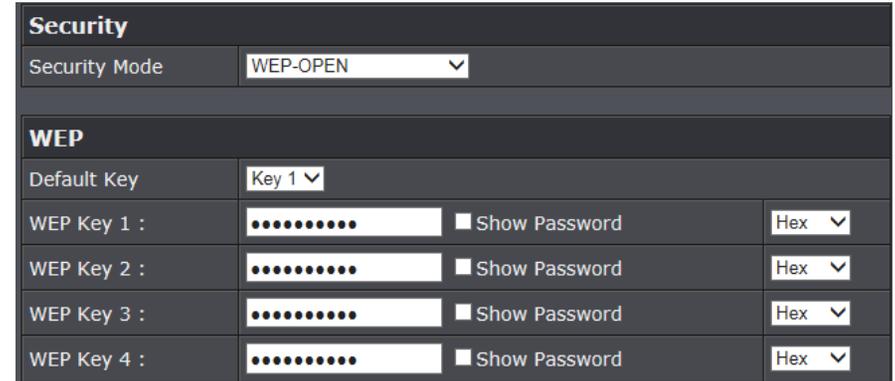


1. Log into your router management page (see “[Access your router management page](#)” on page 10).
2. Click on **Basic**, and click on **Wireless**.
3. Under **Security**, click on the **Security Mode** drop-down list to select your wireless security type.



Selecting WEP:

If selecting **WEP** (Wired Equivalent Privacy), please review the WEP settings. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.



- **Security Mode:** Choose **WEP-OPEN**, **WEP-SHARED**, or **WEP-AUTO**.
Note: It is recommended to use *Open* since it is known to be more secure than *Shared Key*.
- **Default 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.
- **WEP 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-PSK**, or **WPA2-PSK Mixed**. Please review the WPA-Personal settings. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

Security	
Security Mode	WPA2-PSK
WPA	
WPA Cipher	<input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES
Pre-Shared Key	•••••••• <input type="checkbox"/> Show Password
Key Update Interval	3600 seconds

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

- **WPA Cipher:** Select a Cipher Type to use.
 - When selecting **WPA2-Personal Mixed** security, it is recommended to use **TKIP/AES**.
 - When selecting **WPA2-Personal** security, it is recommended to use **AES**.
- **WPA Pre-Shared Key:** Enter the passphrase.
 - 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.)
- **Key Update Interval:** Enter the time interval (seconds) of when the network passphrase will rotate.
Note: It is recommended to use the default interval time. Your passphrase will not change, rotation of the key is part of the WPA protocol and designed to increase security.

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

Security	
Security Mode	WPA2
WPA	
WPA Cipher	<input type="radio"/> AES <input checked="" type="radio"/> TKIP/AES
Key Update Interval	3600 seconds
Radius Server	
IP Address	0.0.0.0
Port	1812
Shared Secret	<input type="checkbox"/> Show Password

The following section outlines options when selecting **WPA**, **WPA2-Enterprise**, or **WPA2-Enterprise Mixed** (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 Cipher:** Select a Cipher Type to use.
 - When selecting **WPA2-Personal Mixed** security, it is recommended to use **TKIP/AES**.
 - When selecting **WPA2-Personal** security, it is recommended to use **AES**.
- **Key Update 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.
- **IP Address:** Enter the IP address of the RADIUS server. (e.g. 192.168.10.250)
- **Port:** Enter the port your RADIUS server is configured to use for RADIUS authentication.
Note: It is recommended to use port 1812 which is typical default RADIUS port.
- **Shared Secret:** Enter the shared secret used to authorize your router with your RADIUS server.

Connect wireless devices to your router

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

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

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

You can view the currently connected wireless client devices under *Advanced > Wireless (2.4GHz or 5GHz) > Station List* in the router management page.

See the "[Appendix](#)" on page 72 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 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) > 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 10).
2. Click on **Advanced**, then click on **Wireless (2.4GHz or 5GHz)**, and click on **WPS**.
3. To add a wireless device to your network, next to **PBC**, click the **Start Push Button** 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.

WPS Action	
If you are using the Virtual Push Button method, click Start Push Button, then push and activate WPS on your wireless client device. If you are using the PIN method, enter the wireless client device PIN in the field and click Start PIN, then activate the WPS PIN method on your wireless client device.	
PIN	<input type="text"/> Start PIN
PBC	Start Push Button

4. Wait for your router to finish the WPS process.

Note: You should a message on your WPS client device indicating WPS was successful.

WPS Summary	
WPS Current Status	Processing...119
WPS Configured	Yes
WPS SSID	TRENDnet824_2.4GHz_7B7C
WPS Security Mode	WPA2 Only - PSK
WPS Encrypt Type	AES
WPS Key	oiuj04089
AP PIN	27984659

PIN (Personal Identification Number)

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

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

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Wireless**, and click on **Wi-Fi Protected Setup**.
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.

WPS Action	
If you are using the Virtual Push Button method, click Start Push Button, then push and activate WPS on your wireless client device. If you are using the PIN method, enter the wireless client device PIN in the field and click Start PIN, then activate the WPS PIN method on your wireless client device.	
PIN	<input type="text" value="XXXXXXXX"/> Start PIN
PBC	Start Push Button

4. Wait for your router to finish the WPS process.

Note: You should a message on your WPS client device indicating WPS was successful.

WPS Summary	
WPS Current Status	Processing...119
WPS Configured	Yes
WPS SSID	TRENDnet824_2.4GHz_7B7C
WPS Security Mode	WPA2 Only - PSK
WPS Encrypt Type	AES
WPS Key	oiuj04089
AP PIN	27984659

Advanced wireless settings

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

Multiple SSID

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

The multiple SSID feature allows you to broadcast up to 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 10).
2. Click on **Advanced** and click on **Wireless (2.4GHz or 5GHz)**, then click on **Multiple SSID**.
3. Next to Multiple SSID1 or SSID2, check **Radio On/Off** option to enable the additional SSID.
 - **New Schedule** – The schedule function allows you to define a schedule when the additional SSID should be turned on. To define a new schedule, click **New Schedule** and refer to page 39 "[Create Schedules](#)". After you have created a new schedule, 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 38 to configure [Time Settings](#) and see page 39 "[Create Schedules](#)" to create a schedule.*
4. **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.

Wireless Network Name (SSID)	trendnet2
------------------------------	-----------

Please refer to page 18 to find out about different security types and page 19 for wireless security configuration.

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



5. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

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

Wireless bridging using WDS (Wireless Distribution System)

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

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

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

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

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 33](#) 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 34](#) for DHCP server options.
3. Configure the same wireless channel and use the same on all WDS supported wireless devices. See [page 12](#) for configuring basic wireless settings.
4. Configure the same wireless security and key on all WDS supported devices. See page 24 for configuring wireless security settings.

To configure WDS bridging between TEW-827DRU routers:

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Wireless (2.4GHz or 5GHz)**, then click on **WDS**.
3. Click the WDS drop-down menu and select **Enable**.

Note: Please note to use the Local AP MAC address listed here to enter into the other WDS capable router's WDS configuration, not the MAC listed in the Router Status page.

WDS	Enable ▾
Local AP MAC Address	32:18:E7:95:6A:45

4. 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)

Remote AP MAC Address	<input type="text"/>
Remote AP MAC Address	<input type="text"/>
Remote AP MAC Address	<input type="text"/>
Remote AP MAC Address	<input type="text"/>

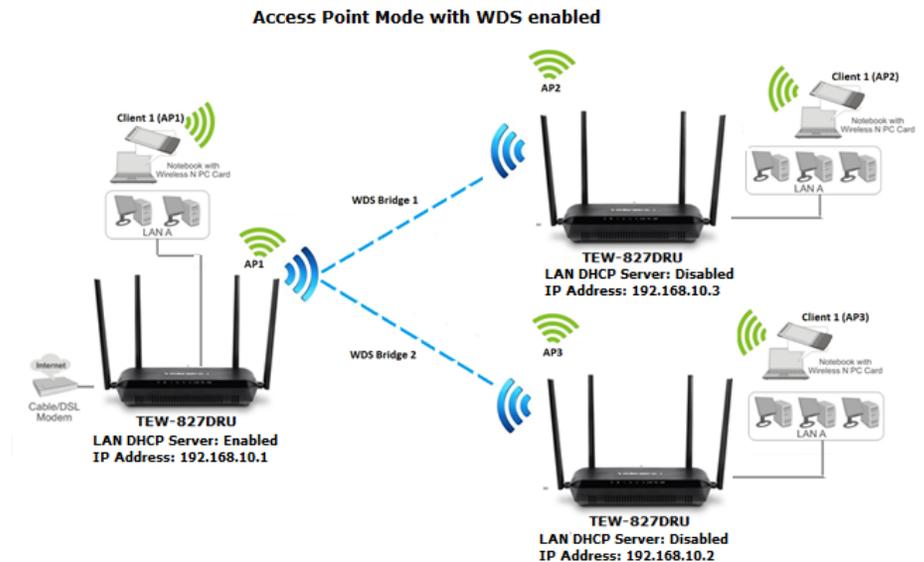
4. Under Security, configure the encryption type to use.

Note: Only WEP security is supported for WDS. You can find more information on wireless security on page 18.

5. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

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.



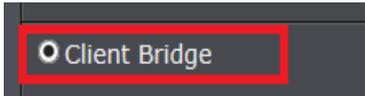
Wireless Client Bridge Mode

Advanced > Setup > Device Mode

Wireless client bridge mode The function of client bridge mode is to extend wireless connectivity to multiple wired Ethernet client devices. A typical application where this mode may be used is in your home entertainment/media center where multiple network enabled media devices require Internet or network connectivity such as an HD smart TV, game console, set top box, or DVR. The device will first establish connectivity (similar to a wireless enabled client device such as a laptop or mobile phone) to your wireless network (typically provided by a wireless router or access point) and bridge the connectivity to your network over to the wired client devices using the four LAN switch ports (1-4). After selecting and applying this mode, click on Wireless > Wireless Network and click Site Survey to scan for the wireless network to connect and enter the wireless security key (if required) to establish connectivity to your network. After you have successfully set up the device to connect to your wireless network, you can plug in the device in the area where you would like to bridge network connectivity to wired client devices using the four LAN switch ports (1-4). In this mode, the device can only connect to one band at a time (2.4GHz or 5GHz) and will not provide any of the access control features typically provided in router mode.

To configure your TEW-827DRU in client bridge mode:

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click **Setup**, then click on **Device Mode**.
3. Select **Client Bridge** and click **Apply & Reboot**.



4. Click on **Wireless** and click on **Wireless Network**, then click on **Site Survey** to scan for available wireless networks.

Site Survey

A screenshot of a web interface showing a button labeled 'Site Survey'. The button is highlighted with a red rectangular box.

5. Select the network you would like to connect to in the list by clicking on the wireless network name or SSID.

Site Survey							
SSID	BSSID	Channel	Signal Level	Mode	Security	Hz	
jdsk823-5G	D8:FE:E3:3E:B1:22	36	-25 dbm	802.11AC VHT80	WPA2-PSK AES	5G	
811wrt	D8:EB:97:A4:DD:2B	36	-47 dbm	802.11AC VHT20	WPA2-PSK AES	5G	
TRENDnet818_5GHz_0EVN	D8:EB:97:AD:EC:98	36	-46 dbm	802.11AC VHT80	WPA2-PSK AES	5G	
TrendnetOpWork5G	00:14:D1:B1:E1:B7	36	-85 dbm	802.11NA HT20	WPA2-PSK AES	5G	
Wally World 5G	00:14:D1:B1:8C:EE	44	-56 dbm	802.11NA HT20	WPA2-PSK AES	5G	
816_5GHz	00:1E:E3:30:F7:D5	44	-50 dbm	802.11AC VHT80	WPA/WPA2-PSK TKIP/AES	5G	

6. If the network selected requires a WiFi password/key, enter the key under **Wireless Security**.

Note: You can choose to enable MU-MIMO if the router/AP you are connecting to supports this feature.

Wireless Security	
Security Mode	WPA2-Personal ▼
WPA	
WPA Cipher	AES ▼
Pre-Shared Key :	<input type="password" value="••••••••"/> <input type="checkbox"/> Show Password

7. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**. After applying changes, you can check the connection status under Status > Connection Status.

Advanced Settings

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

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

- **Beacon Period:** A beacon is a management frame used in wireless networks that transmitted periodically to announce the presence and provide information about the router's wireless network. The interval is the amount time between each beacon transmission.
Default Value: 100 milliseconds (range: 100-1000)
- **DTIM:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.
- **Fragment Threshold:** Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value of 2346 bytes. Setting the Fragmentation value too low may result in poor performance.
- **RTS Threshold:** The Request To Send (RTS) function is part of the networking protocol. A wireless device that needs to send data will send a RTS before sending the data in question. The destination wireless device will send a response called Clear to Send (CTS). The RTS Threshold defines the smallest data packet size allowed to initiate the RTS/CTS function.
Default Value: 2347 (range: 1-2347)
- **TX Power:** This setting allows you to adjust the wireless transmit power to a lower setting. In busy wireless environments, lowering the transmit power may improve better performance and connectivity and decrease interference with neighboring wireless networks.
- **Short Preamble:** Using a short preamble can potentially increase throughput as the transfer time is 96 microseconds versus the more commonly used long

preamble 192 microseconds. However, using a short preamble is not supported using 802.11b legacy devices, in some cases cause wireless interoperability issues, and increase the error rate in some installations. The preamble is the info. sent from the wireless transmitter to the receiver indicating when data is incoming.

- **Short Slot:** Short Slot Override defines the amount of time a device waits after a data frame collision before retransmitting the data. Reducing the time from 20 microseconds (standard) to 9 microseconds can potentially increase throughput however, can also increase the error rate.
- **20/40 Coexistence (2.4GHz only):** 20/40 MHz Coexistence allows for the auto-fallback from 40MHz to 20MHz channel width operation when neighboring 802.11 wireless networks are detected.
- **Guard Interval:** 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.
- **MCS** – Allows you to lock down the wireless transmission rate.
- **Extension channel** – Allows you to assign either the upper or lower extension channels to use for channel bonding when establishing connectivity at the higher channel widths 40MHz and 80MHz.
- **A-MPDU:** Using Aggregate Multiple Protocol Data Unit will allow the all frames transmitted to be aggregated into larger size A-MPDU formatted frames before sending and receiving potentially increasing the overall throughput.
- **MU-MIMO (5GHz only):** Enables MU-MIMO functionality on your router to optimize downstream bandwidth for multiple concurrent wireless clients. Please note that wireless clients must also support MU-MIMO capability to utilize the functionality.

Advanced WirelessBeacon Period ms (range 100 - 1000, default 100)DTIM (range 1 - 255, default 1)Fragment Threshold (range 256 - 2346, default 2346)RTS Threshold (range 1 - 2347, default 2347)TX Power ▾Short Preamble Enable Disable**HT Physical Mode**Guard Interval long AutoMCS ▾A-MPDU Enable Disable**Multicast-to-Unicast Converter**Multicast-to-Unicast Enable Disable**MU-MIMO (TX-Beamforming)**MU-MIMO ▾

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 > Setup > Management

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Setup**, 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 to this section, click **Apply** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

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 side or bottom labels.

Manually configure your Internet connection

Advanced > Setup > WAN Settings

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Setup**, then click on **WAN Settings**.
3. Under **Internet Connection Type** in drop-down list, select the type of Internet connection provided by your Internet Service Provider (ISP).

WAN Connection Type	
Connection Type	DHCP
	STATIC
	DHCP
	PPPoE
	L2TP
	PPTP
	Russia PPPoE
	Russia PPTP
	Russia L2TP

4. Complete the fields required by your ISP.
5. Complete the optional settings only if required by your ISP.
6. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

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

IPv6 Settings

Advanced > Setup > IPv6 Settings

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:

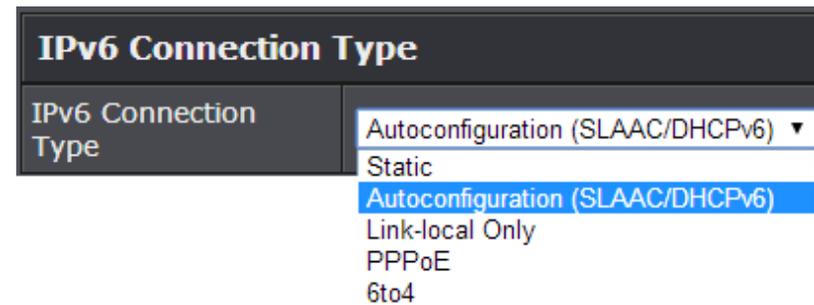
- Integrated IPsec – Better Security
- Integrated Quality of Service (QoS) – Lower latency for real-time applications
- Higher Efficiency of Routing – Less transmission overhead and smaller routing tables
- Easier configuration of addressing

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 10).
2. Click on **Advanced** and click on **Setup**, then click on **IPv6 Settings**.

3. Review the IPv6 Internet Connection settings and enter information settings specified by your ISP. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

Note: Please contact your ISP for IPv6 service availability.



Select the IPv6 connection type provided by your ISP.

- Static IPv6
- Auto-configuration (SLAAC/DHCPv6)
- PPPoE
- 6to4
- Link-Local Only

Clone a MAC address

Advanced > Setup > WAN Settings

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 10).
2. Click on **Advanced** and click on **Setup**, then click on **WAN Settings**.
3. In the MAC Address Clone section, click **Clone Your PC's MAC Address** to copy your computer's MAC address in the **MAC Address** field.

Note: You can also check the *Wireless Client List* for the MAC addresses of the devices on your network, see [page 64](#) or refer to your computer or device documentation to find the MAC address.

MAC Address	<input type="text" value=""/>	(Ex: 00:11:22:33:44:55)
	<input type="button" value="Copy Your PC's MAC Address"/>	

4. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

Change your router IP address

Advanced > Setup > LAN Settings

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 10).
2. Click on **Advanced** and click on **Setup**, then click on **LAN Settings**.
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	
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
MAC Address	00:18:E7:95:85:03

4. To save changes to this section, click **Apply** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**. **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-827dru>

Set up the DHCP server on your router

Advanced > Setup > LAN Settings

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 10).
2. Click on **Advanced** and click on **Setup**, then click on **LAN Settings**.
3. Review the DHCP Server settings. To save changes to this section, click **Apply** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

- **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:** Changes the lease time for IP addresses issued to DHCP clients before renewal. (e.g. 1440 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.
- **Local Domain Name:** Enter a domain name to issue to DHCP clients.
- **Primary DNS Server:** Enter a primary DNS server IP address to issue to DHCP clients.

- **Secondary DNS Server:** Enter a secondary DNS server IP address to issue to DHCP clients.

DHCP Server Setting	
DHCP Server	Enable ▾
DHCP Start IP	192.168.10.101
DHCP End IP	192.168.10.199
DHCP Lease Time	1440 (minutes)
Local Domain Name	trendnet.com
Primary DNS Server	192.168.1.249
Secondary DNS Server	0.0.0.0

You can also view the current DHCP clients in the **Number of Dynamic DHCP Clients** list under *Advanced > Setup > DHCP Client List*.

DHCP Clients		
MAC Address	IP Address	Expires in
00:14:D1:26:E4:76	192.168.10.101	0 Day 23:59:23

Set up DHCP reservation

Advanced > Setup > LAN Settings

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 42) or special applications (also called port triggering, see "[Special Applications](#)" on page 44).

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Setup**, then click on **LAN Settings**.
3. Review the DHCP reservation settings. To save changes to this section, click **Apply** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.
 - **Enable** – Enable or Disable the DHCP reservation.
 - **Computer Name** – Enter a name of the device you will assign the DHCP reservation. **Note:** You can click the Computer Name drop-down list to select from an available computer in the DHCP server listing, click >> to copy the computer's host name/IP address information into the fields.
 - **IP Address** – Enter the IP address to assign to the reservation. (e.g. 192.168.10.101)
Note: You can click the Computer Name drop-down list to select from an available computer in the DHCP server listing, click >> to copy the computer's host name/IP address information into the fields.
 - **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)
Note: You can click Clone your PC's MAC Address to copy the current computer's MAC address into the MAC address field.
 - **Copy your PC's MAC** – To copy your current computer's MAC address to the field, you can click **Copy**.

Add DHCP Reservation	
Enable	<input type="checkbox"/>
Computer Name	<input type="text"/> << Host Name ▾
IP Address	<input type="text"/>
MAC Address	<input type="text"/> (Ex: 00:11:22:33:44:55)
Copy your PC's MAC	<input type="button" value="Copy"/>

Click **Add** - Saves the reservation.

Note: Click **Clear** discards and erases the current information.



You will see the new reservation added to the DHCP Reservations Ready Group. 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. You can click **Reset** to clear the entries in the list or check the Delete option, next to the entry to remove and click **Delete**.

DHCP Reservations Ready Group					
No.	Enable	Computer Name	IP Address	MAC Address	Delete
1	<input checked="" type="checkbox"/>		192.168.10.101	00:14:D1:26:E4:76	<input type="checkbox"/>

Under the DHCP Reservations List,

You can click the  icon to edit the reservation or check the Delete option next to the entry to remove and click **Delete Selected** to delete the reservation. You can also click **Delete All** to delete all DHCP reservation entries from the list.

DHCP Reservations List					
Enable	Computer Name	IP Address	MAC Address	Edit	Delete
1 <input checked="" type="checkbox"/>		192.168.10.101	00:14:D1:26:E4:76		<input type="checkbox"/>

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

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

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 10).
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.

UPnP	
UPnP	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 to this section, click **Apply** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

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 10).
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.
 - **Streaming Media (RTSP):** Allows RTSP protocol through your router typically used in streaming media applications.
 - **Streaming Media-VoIP (SIP):** Allows SIP protocol through your router typically used in VoIP applications
 - **Streaming Media-VoIP (H.323):** Allows H.323 protocol through your router typically used in video/audio conferencing applications.
 - **File Transfer (FTP):** Allows FTP protocol through your router used for file transfer over a network or the Internet.
 - **File Transfer (TFTP):** Allows TFTP protocol through your router used for file transfer over a network or the Internet.
 - **VPN Passthrough:** Allows VPN client connections through your router.

Application Level Gateway (ALG) Configuration

Service Name	Description	Enable
Streaming Media	Real Time Streaming Protocol (RTSP)	<input checked="" type="checkbox"/>
Streaming Media-VoIP	Session Initiation Protocol(SIP)	<input checked="" type="checkbox"/>
Streaming Media-VoIP	NetMeeting (H.323)	<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"/>
VPN Pass-Through	PPTP/L2TP/IPsec	<input checked="" type="checkbox"/>

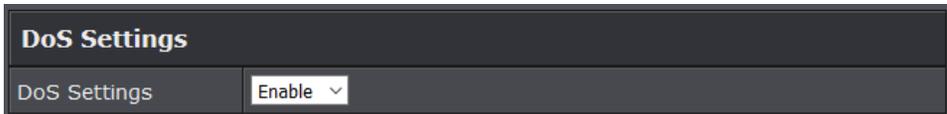
5. To save changes to this section, click **Apply** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

Denial of Service (DoS)

Advanced > Firewall > DoS

The router supports prevention against common denial of service attacks. Malicious users use denial of service attacks to temporarily or permanently disrupt the availability of services from a network resource such as your router. Typically, DoS attacks are achieved by flooding a specific network resource excess and unnecessary requests which results in the network resource to stop responding or process requests much slower compared to normal operation due to the excessive and unnecessary requests received by the DoS attack.

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced**, click on **Firewall**, and click then click **DoS**.
3. Click the **DoS Settings** drop-down list to select **Enable** to enable DoS prevention.



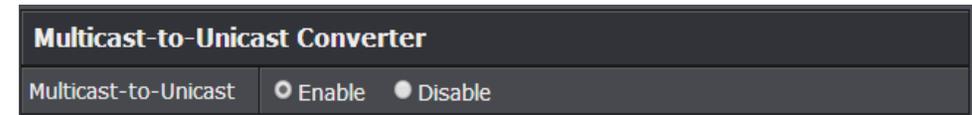
4. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

Allow/deny multicast streaming

Advanced > Wireless (2.4GHz or 5GHz)

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

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Wireless (2.4GHz or 5GHz)**, then and click on **Advanced**.
3. Next to **Multicast-to-Unicast Converter**, select the option to enable or disable.



4. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

IPv6 Firewall

Advanced > Firewall > IPv6 Firewall

If you are using IPv6 Internet connectivity with your Internet Service Provider (ISP), you may want to enable IPv6 security on your router to prevent internal access using IPv6 protocol to your internal LAN network.

When IPv6 Internet connectivity is established, the IPv6 simple security enables a basic IPv6 firewall which allows all outgoing requests from the originating internal LAN to go out to the Internet, denies all incoming requests from the originating outside WAN/Internet and allow only ongoing communications/sessions established that originated from the internal LAN, similar to the IPv4 NAT function (RFC6092). Enabling IPv6 simple security also denies all ICMPv6 ping requests incoming from Internet into your internal IPv6 LAN network (RFC4890). To enable basic IPv6 security, you can enable the IPv6 Simple Security setting, then Save & Reboot. If you would like to create more specific IPv6 firewall rules, you can create and specify these rules in the Add IPv6 Firewall Rule section.

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced**, click on **Firewall**, and click then click **IPv6 Firewall**.

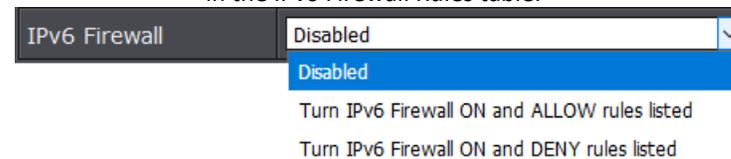
firewall settings. To save changes to this section, click **Apply** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

- **IPv6 Simple Security:** Click the drop-down list and select **Enable** to enable IPv6 basic firewall and select **Disable** to disabled the IPv6 basic firewall. Enabling this setting also denies incoming ICMPv6 requests.
- **IPv6 Ingress Filter:** If IPv6 Simple Security is not enabled, select **Enable** to only deny incoming ICMPv6 requests. All other IPv6 incoming communication will be allowed unless otherwise specified by a specific IPv6 firewall rule.

IPv6 Simple Security	Enabled ▾
IPv6 Ingress Filtering	Enabled ▾

To add a specific IPv6 firewall rule, under **Add IPv6 Firewall Rule**, select the action for the firewall rules table review the settings below. Click **Add** to add the rule to the table. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

- **IPv6 Firewall** – Selecting the action will allow specific IPv6 firewall rules to be created.
 - a. **Turn IPv6 Firewall ON and DENY rules listed** – This will set the action to deny IPv6 traffic for all of the specific IPv6 firewall rules listed in the IPv6 Firewall Rules table.
 - b. **Turn IPv6 Firewall ON and ALLOW rules listed** – This will set the action to allow IPv6 traffic for all the specific IPv6 firewall rules listed in the IPv6 Firewall Rules table.



- **Rule Enable:** Check this option to enable the IPv6 firewall rule.
- **Rule Name:** Enter a name for the IPv6 firewall rule.
- **Source IP Range:** Enter the IPv6 address or IPv6 address range and select the Interface (**WAN** or **LAN**) where the traffic will be originating. (ex. If this is an outbound traffic rule, the IPv6 address should be the local IPv6 address or range of devices on your LAN and interface should be set to LAN)
- **Destination IP Range:** Enter the IPv6 address or IPv6 address range and select the Interface (**WAN** or **LAN**) where the traffic will be going. (ex. If this is an outbound traffic rule, IPv6 address should be the destination outside Internet IPv6 address where the traffic will be going and interface should be set to WAN)
- **Protocol** – Select the protocol you would like to allow or deny for the IPv6 firewall rule. **TCP, UDP, or Both.** (**Note: Both means TCP and UDP protocols**)
- **Port Range** – Enter the port range you would like to allow or deny for the IPv6 firewall rule.
- **Schedule (Optional)** – The schedule function allows you to define a schedule when the port trigger should be turned on. To define a new schedule, click **New Schedule** and refer to page 39 "[Create Schedules](#)". After you have created a new schedule, 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 38 to configure [Time Settings](#) and see page 39 "[Create Schedules](#)" to create a schedule.**

Add IPv6 Firewall Rule	
Rule Enable	<input type="checkbox"/>
Rule Name	<input type="text"/>
Source IP Range	<input type="text"/> WAN <input type="button" value="v"/> (Ex: 2001:db8:1234::1111:2222:3333 - 2001:db8:1234::1111:2222:6666)
Destination IP Range	<input type="text"/> LAN <input type="button" value="v"/>
Protocol	TCP <input type="button" value="v"/>
Port Range	<input type="text"/> - <input type="text"/>
Schedule	Always <input type="button" value="v"/> <input type="button" value="New Schedule"/>

Identify your network on the Internet

Advanced > Setup > Management

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

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

1. 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 10).
3. Click on **Advanced** and click on **Setup**, 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 <input type="button" value="v"/>
Host Name	<input type="text"/>
Account	<input type="text"/>
Password	<input type="password"/>

5. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

Set your router date and time

Advanced > Administrator > Time

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Administrator**, then click **Time**.
3. Review the Time settings. To save changes to this section, click **Apply** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

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

Time Configuration	
System Time	Fri Jan, 9, 1970 12:41:19

- **Enable Daylight Saving:** Check the option to enable daylight savings time and set the annual range when daylight saving is activated.

Daylight Saving Time					
Enable Daylight Saving	<input checked="" type="checkbox"/>				
Daylight Saving Offset	+1:00 ▾				
Daylight Saving Dates	Month	Week	Day of Week	Hour	
	DST Start	Jan ▾	1st ▾	Sun ▾	0 ▾
DST End	Jan ▾	1st ▾	Sun ▾	0 ▾	

You can choose one of the following options to set the device time and date:

- **Automatically synchronize with Internet Time Server** – 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 checked="" type="checkbox"/>
NTP Server	Select NTP Server ▾
Time Zone	(GMT-08:00) Pacific Time (US/Canada), Tijuana ▾
NTP synchronization	300 (1~300) Minute

- **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. In addition, you can click *Synchronize with Your Computer's Time Settings* to copy the time and date settings from your computer.

Date and Time Settings						
Date And Time	Year	2014 ▾	Month	May ▾	Day	22 ▾
	Hour	11 ▾	Minute	31 ▾	Second	54 ▾

Create schedules

Advanced > Setup > Schedule

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

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

- Wireless (2.4GHz and 5GHz)
- Guest Network
- Access Control (IP Protocol Filters)
- Virtual Server
- Special Applications
- Gaming

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Setup**, then click on **Schedule**.

3. Review the Schedule settings. To save changes to this section, click **Add** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

- **Rule Name:** Enter a name for the schedule you would like to apply.
- **Day(s)/Select Day(s):** Check **Select Day(s)** to select the days in the **Select Day(s)** section or select **All Week** to set the schedule for all days.
- **All Day – 24 Hours** – Check the option to set the schedule to 24 hours or define the schedule under **Start Time** and **End Time**.
- **Start/End Time:** Select the start and end time you would like the schedule to follow.

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

Add Schedule Rule	
Rule Name	<input type="text"/>
Day(s)	<input type="radio"/> Select Day(s) <input type="radio"/> All Week <input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat
All Day - 24hrs	<input type="checkbox"/>
Start Time	00 ▾ : 00 ▾
End Time	00 ▾ : 00 ▾

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.

Block a specific service or multiple services

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Security**, then click on **Access Control**.
3. Next to **Enable Access Control**, click the **Enable** option.

Access Control	
Enable Access Control	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

4. Review the **Add Services Block Rule**. Click **Add** to save the rule. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

- **Rule Enable** – Checking this option turns on the Protocol/IP Filter and unchecking turns it off.
- **Rule Name** – Enter a name for the Protocol/IP Filter.
- **Schedule (Optional)** – The schedule function allows you to define a schedule when the access control filter should be turned on. To define a new schedule, click **New Schedule** and refer to page 42 "[Create Schedules](#)". After you have created a new schedule, 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 41 to configure [Time Settings](#) and see page 42 "[Create Schedules](#)" to create a schedule.

- **Client 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.

Add Services Block Rule	
Rule Enable	<input type="checkbox"/>
Rule Name	<input type="text"/>
Schedule	<input type="checkbox"/> Always <input type="button" value="New Schedule"/>
Client IP Address Range	<input type="text"/> ~ <input type="text"/>

To simplify configuration, there is a list of commonly used pre-defined Protocol/IP Filters to modify otherwise, you can choose to manually add a new Protocol/IP Filter.

- **Service** – Select **Predefined** to select from the predefined services listed or select **Manually** to specifically enter the TCP or UDP port number or port range numbers to block. (e.g. 80-80 or 20-21).

Service	<input type="radio"/> Predefined <input checked="" type="radio"/> Manually	Enabled
Web Browsing	HTTP, TCP Port 80	<input type="checkbox"/>
Email Sending	SMTP, TCP Port 25	<input type="checkbox"/>
Email Receiving	POP3, TCP Port 110	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
DNS Query	UDP Port 53	<input type="checkbox"/>
TCP Protocol	All TCP Port	<input type="checkbox"/>
UDP Protocol	All UDP Port	<input type="checkbox"/>

TCP Ports	<input type="text"/>	Ex: 21 or 300-500
UDP Ports	<input type="text"/>	Ex: 21 or 300-500

Block all services

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Security**, then click on **Access Control**.
3. Next to **Enable Access Control**, click the **Enable** option.

Access Control	
Enable Access Control	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

4. Review the **Add All Services Block Rule**. Click **Add** to save the rule. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

- **Rule Enable** – Checking this option turns on the Protocol/IP Filter and unchecking turns it off.
- **Rule Name** – Enter a name for the Protocol/IP Filter.
- **Schedule (Optional)** – The schedule function allows you to define a schedule when the access control filter should be turned on. To define a new schedule, click **New Schedule** and refer to page 42 "[Create Schedules](#)". After you have created a new schedule, 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 41 to configure [Time Settings](#) and see page 42 "[Create Schedules](#)" to create a schedule.
- **Client 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.

Note: In the **Block Rule List**, you can edit a rule by clicking  under the **Edit** column next to the rule you would like to edit. You can also delete a rule by clicking  under the **Delete** column next to the rule you would like to delete.

Inbound Filter

Advanced > Security > Inbound Filter

Inbound Filters allows you to allow or deny a specific range of IP addresses. You can create a predefined range of IP addresses to apply to a specific feature.

Note: You can apply a predefined inbound filter to the following features:

- Virtual Server
- Gaming
- Remote Management

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Access**, and click on **Inbound Filter**.
3. Review the inbound filter settings. Click **Add** to save the Inbound Filter. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

- **Rule Name** – Enter a name for the IP address range.
- **Rule Action** – Select **Allow** to allow the specified IP address range or **Deny** to deny the specified IP address range.
- **IP Address** - Enter the IP address range (e.g. 192.168.1.20-192.168.1.30).

Add Inbound Filter Rule	
Rule Name	<input type="text"/>
Rule Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny
IP Address	<input type="text"/> ~ <input type="text"/>

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

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 45) 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 40) 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 10).
3. Click on **Advanced** and click **Firewall**, then click on **DMZ**.
4. Click the **DMZ Enable** drop-down list, and select **Enable**.

DMZ Enable	Enable ▼
------------	----------

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

DMZ IP Address	192. 168. 10. 1
----------------	-----------------

6. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

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 45) 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 48.

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 40).

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Firewall**, then click on **Virtual Server**.
3. Review the virtual server settings. Click **Add** to save settings. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

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

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

- **Inbound Filter:** Select the defined IP address range to allow access. (see “[Inbound Filter](#)” section on page 44).
- **Schedule (Optional)** – The schedule function allows you to define a schedule when the virtual server should be turned on. To define a new schedule, click **New Schedule** and refer to page 42 “[Create Schedules](#)”. After you have created a new schedule, 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 41 to configure [Time Settings](#) and see page 42 “[Create Schedules](#)” to create a schedule.

Add Virtual Server	
Rule Enable	<input type="checkbox"/>
Rule Name	<input type="text"/>
IP Address	<input type="text"/>
Protocol	TCP ▾
Public Port	<input type="text"/>
Private Port	<input type="text"/>
Inbound Filter	<input type="checkbox"/> Allow All ▾ <input type="button" value="New Inbound Filter"/>
Schedule	<input type="checkbox"/> Always ▾ <input type="button" value="New Schedule"/>

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

Example: To forward TCP port 80 to your IP camera

1. Setup DynDNS service (see [Identify Your Network](#) section page 40).
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 10).
5. Click on **Advanced** and click on **Firewall**, then click on **Virtual Server**
6. Check the **Rule 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**. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

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 37.

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 10).
2. Click on **Advanced** and click on **Firewall**, then click on **Special Applications**.
3. Click the **Port Triggering** drop-down list, and select **Enable**. To save changes to this section, click **Add** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

Port Trigger Function	
Port Triggering	Enable ▾

4. Review the application rule settings. Click **Add** to save settings. Check the option to the left most of the entry to enable and uncheck to disable.

- **Rule Enable** – Check the option to enable the port trigger rule.
- **Rule Name** – Enter a name for the port trigger rule.

- **IP Address:** Enter the IP address of the device to forward the port (e.g. 192.168.10.101).
- **Match Protocol:** Select the protocol for the firewall ports required for your device. **TCP, UDP, or Any** (TCP and UDP).
- **Match Port:** Enter the ports or port range to be forwarded to the device. (e.g. 2000-2038,2200-2210).
- **Trigger Protocol (Trigger):** Select the trigger port protocol requested by the device. **TCP, UDP, or Any**.
- **Trigger Port:** Enter the port requested by the device. (e.g. 554-554 or 6112-6112).
- **Schedule (Optional)** – The schedule function allows you to define a schedule when the port trigger should be turned on. To define a new schedule, click **New Schedule** and refer to page 42 "[Create Schedules](#)". After you have created a new schedule, 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 41 to configure [Time Settings](#) and see page 42 "[Create Schedules](#)" to create a schedule.

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

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

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 45) 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 40).

1. Log into your router management page (see “[Access your router management page](#)” on page 10).
2. Click on **Advanced** and click on **Security**, then click on **Gaming**.
3. Review the virtual server settings. To save changes to this section, click **Add** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

- **Rule Enable** – Check the option to enable the gaming rule.
- **Rule Name** – Enter a name for the gaming rule.
- **IP Address:** Enter the IP address of the device to forward the ports (e.g. 192.168.10.101).
- **TCP Ports to Open:** Enter the TCP port you would like to set.
- **UDP Ports to Open:** Enter the UDP port you would like to set.
Note: Please refer to the device documentation to determine which ports and protocols are required. You should assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.
- **Inbound Filter:** Select the defined IP address range to allow access. (see “[Inbound Filter](#)” section on page 44).
- **Schedule (Optional)** – The schedule function allows you to define a schedule when the gaming rule should be turned on. To define a new schedule, click **New Schedule** and refer to page 42 “[Create Schedules](#)”. After you have created a new schedule, 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 41 to configure [Time Settings](#) and see page 42 “[Create Schedules](#)” to create a schedule.

Add Gaming Rule	
Rule Enable	<input type="checkbox"/>
Rule Name	<input type="text"/> << Application Name ▼
IP Address	<input type="text"/>
TCP Ports To Open	<input type="text"/> (ex. 80, 689, 50-60, 1020-5000)
UDP Ports To Open	<input type="text"/> (ex. 80, 689, 50-60, 1020-5000)
Inbound Filter	<input type="checkbox"/> Allow All ▼ New Inbound Filter
Schedule	<input type="checkbox"/> Always ▼ New Schedule

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

Allow remote access to your router management page

Advanced > Setup > Management

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

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click **Setup**, then click on **Management**.
3. Review the setting on the **Remote Management** section. To save changes to this section, click **Apply** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

- **Remote Control (via Internet):** 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 Internet)	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 10).
2. Click on **Advanced** and click on **Setup**, then click on **Routing**.
3. Review the Routing section. Click **Add** to save settings. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

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

Add Static Route	
Destination IP Address	<input type="text" value="0.0.0.0"/>
Destination IP Netmask	<input type="text" value="0.0.0.0"/>
Gateway	<input type="text" value="0.0.0.0"/>
Metric	<input type="text" value="1"/> Ex. 1(highest) - 15(lowest)
Interface	<input type="text" value="WAN"/>

When adding static routes, they will appear in the Static Route List. To delete a route, check the box in the No. column to select which routes to delete, then click **Delete**.

Static Route List					
No.	IP	Netmask	Gateway	Metric	Interface
1 <input type="checkbox"/>	192.168.20.0	255.255.255.0	10.10.10.2	1	WAN

Enable Dynamic Routing

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. If you have other routing devices that support dynamic routing protocol, you can enable these routing protocols on your router to learn and automatically generate the routes needed between these networks.

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 10).
2. Click on **Advanced** and click on **Setup**, then click on **Routing**.
3. Review the Routing section. To save changes to this section, click **Save** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

- **Enable RIP:** Click the drop-down list to enable or disable RIP dynamic routing protocol.
- **RIP mode:** Depending on which RIP version dynamic routing protocols your other routing devices support, click the appropriate version v1 or v2.

Note: If selecting RIP v2, this requires basic password authentication between routing devices using this protocol. The password must match on all routing devices connected in order successfully exchange routing information.

RIP	
Enable RIP	<input type="text" value="Enable"/>
RIP mode	<input checked="" type="radio"/> v1 <input type="radio"/> v2

You can also view the current routing table under Routing Table.

Routing Table				
IP	Netmask	Gateway	Metric	Interface
192.168.20.0	255.255.255.0	10.10.10.2	1	WAN
10.10.10.0	255.255.255.0	0.0.0.0	0	WAN
192.168.10.0	255.255.255.0	0.0.0.0	0	LAN
0.0.0.0	0.0.0.0	10.10.10.254	0	WAN

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.

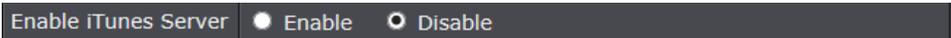


File Sharing Server

iTunes Server

Advanced > USB > File Sharing Server

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **USB**, then click on **File Sharing Server**.
3. Check the **Enable** option to enable the iTunes server and click **Apply**. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

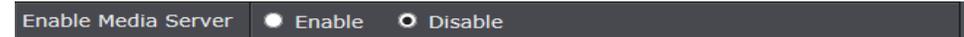


4. Computers with the iTunes application installed will be able to discover and browse the media found on the USB storage over the network.

DLNA Server

Advanced > USB > File Sharing Server

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **USB**, then click on **File Sharing Server**.
3. Check the **Enable** option to enable the DLNA server and click **Apply**. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.



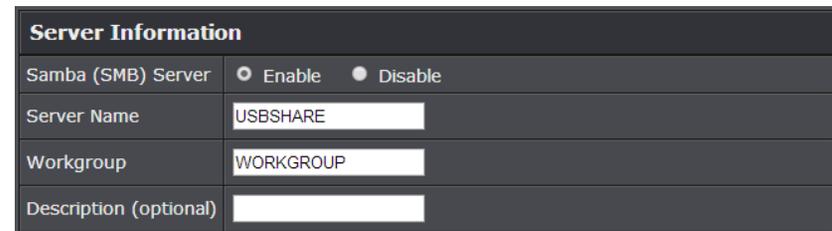
4. All DLNA compliant client devices such PS3, mobile phone, etc. be able to easily discover and access files on the USB storage through DLNA compliant protocols.

Samba Server

Advanced > USB > File Sharing 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 10).
2. Click on **Advanced** and click on **USB**, then click on **File Sharing Server**.
3. Review the setting on **Server Information** section. Click **Apply** to save settings. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.



- **Samba (SMB) Server:** Select enable 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.

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.

Set Administrator	
Administrator	<input type="text" value="admin"/>
New Password	<input type="password"/>
Re-type Password	<input type="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 **Add** to add the account.

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

- **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. You can allow the user **Read Only** or **Read-Write** access to the USB storage.

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 **錯誤! 超連結參照不正確** (ex. [\\192.168.10.1\usb_A1](http://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



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 on the back of the router.

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
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. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

Server Information	
FTP Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Access From Internet	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
File Server Codepage	
Language	Western European ▼

- **FTP Server:** Select enable or disable for the feature.
- **Authentication:** Selecting **Enable** will require user name and password authentication in order to access the USB storage using FTP. Selecting **Disable** will disable the user name and password authentication requirement for access the USB storage which can be access anonymously.
- **Access From Internet:** Selecting **Enable** will allow access to the USB storage using FTP over the Internet (WAN) and local (LAN) networks. Selecting **Disable** 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 **User Account List** section. Click **Add** to add the account.

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

- **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. You can allow the user **Read Only** or **Read-Write** access to the USB storage.

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. 錯誤! 超連結參照不正確。 > or <ftp://myDDNSservice> in your web browser or file explorer address bar. You can access your share files locally by typing 錯誤! 超連結參照不正確。 > in your web browser or file explorer address bar.

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

BitTorrent Client Settings

Advanced > USB > BitTorrent

The router has an integrated BitTorrent client that can be used for downloading torrents directly to the external USB storage device connected to one of the router's USB ports. You can set parameters such as the maximum upload/download speeds, peer number, and connection port.

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **USB**, then click on **BitTorrent**.
3. Click the **Status** drop-down list and select **Enable**. Then click **Apply**.

Status	Enable ▾
--------	----------

4. This page allows you to configure the maximum bandwidth limits, seeding ratio, max peer number and peer number for peers, connection port, and enable/disable encryption. After you have completed your configuration changes click **Apply**. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

Download / Upload	
Download Maximum Speed	<input type="radio"/> Auto <input checked="" type="radio"/> Manual 100 Kbit/s
Upload Maximum Speed	<input type="radio"/> Auto <input checked="" type="radio"/> Manual 20 Kbit/s
Seeding	
Seeding Ratio	<input type="radio"/> No Limit <input checked="" type="radio"/> 2.0000
Storage	
Device	usb_A1 (14.91 GB/6.65 GB) ▾
Peer Number	
Total Maximum Peer Number	240
Peer Number Per Torrent	60
Connection Port	
	<input checked="" type="radio"/> Auto <input type="radio"/> Manual 51413
Other Settings	
<input checked="" type="checkbox"/>	Disable auto download after uploading torrents
<input type="checkbox"/>	Enable encryption

5. After you have configured your client settings. Click **Download Manager** at the top of the page to manage your torrent downloads.



6. You can add new torrent files to the list under **Upload Torrent** by clicking **Browse**, and navigating to the location of the torrent file and selecting it. Once you have selected the torrent file, click **Add** to add the torrent to your download list.

Note: You can continue to add more torrent downloads by clicking **Browse** and selecting each file one at a time.

Upload Torrent
<input type="text" value="Browse..."/>

7. The torrent download list will allow you to **Start All** or **Stop All** downloads. The **Action** section will allow you to delete or remove the specified torrent download.

File Name	Progress & Size	DL Rate / UP Rate	Time Left	Action
Start All		Stop All		

Note: You can click the **Settings** button at the top to return to the router management page.

Virtual Private Networking (VPN)

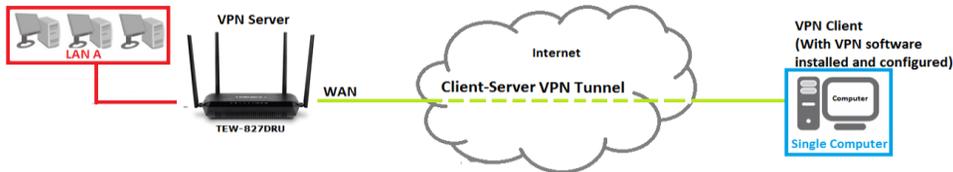
Creating a Virtual Private Network

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.

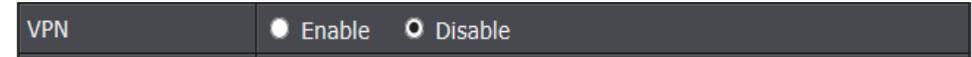
A. Router Configuration

Advanced > Setup > VPN



1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Setup**, then click on **VPN**.
3. Next to **VPN**, click **Enable**.

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 37 "[Identify your Network on the Internet](#)" for details on setting up the Dynamic DNS feature.



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

- **Port:** A different port number may be entered however, 1194 is the default port used with the OpenVPN client software.
- **Protocol:** TCP or UDP may be selected however, UDP is the default protocol used with the OpenVPN client software.
- **IP / Subnet Mask:** The IP address subnet specifies the IP address range assigned to VPN client devices up establishing connectivity.
- **User Authentication:** This is an additional layer of authentication that be added as a requirement to connect. To add users, you scroll down to the bottom of the page and add users. You will be prompted on the client side for user name and password if enabling this feature.

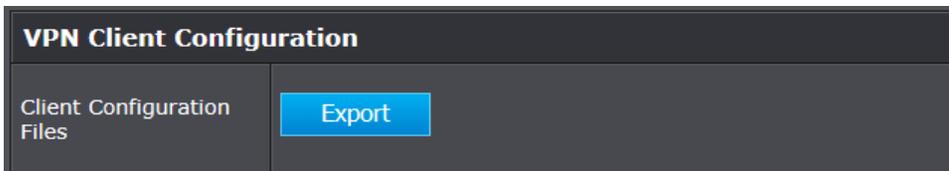
Port	1194
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
IP	10.8.0.0
Subnet Mask	255.255.255.0
User Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

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



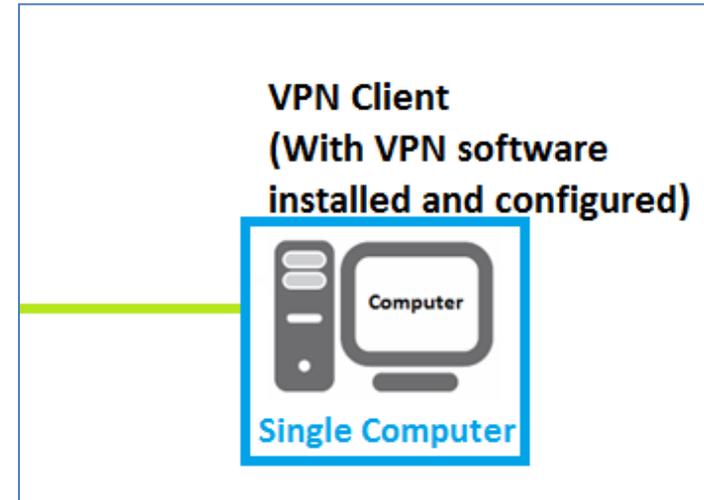
5. Under **VPN Client Configuration**, click on **Export** to download the configuration files for the VPN client computer. Please note that these files will need to be installed on the VPN client computer later on in order to establish VPN connectivity. (Default Filename: client.ovpn)

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

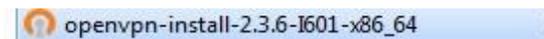


B. Client Configuration

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.



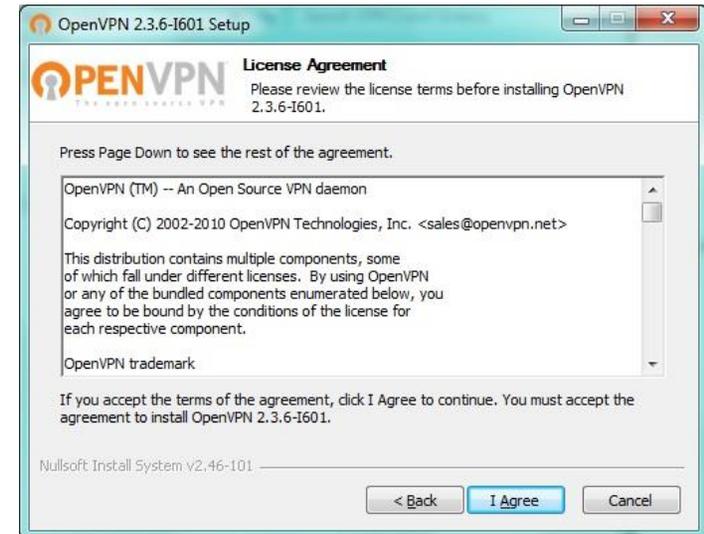
4. If prompted to run the file, click **Run**.



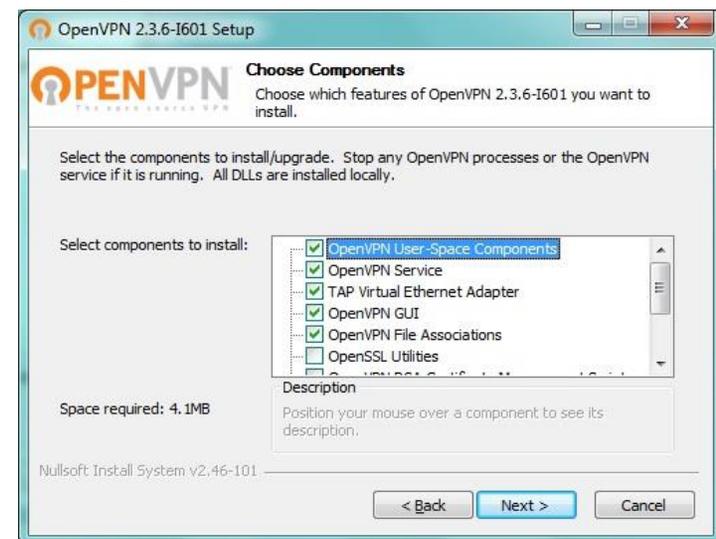
5. At the installation window, click **Next**.



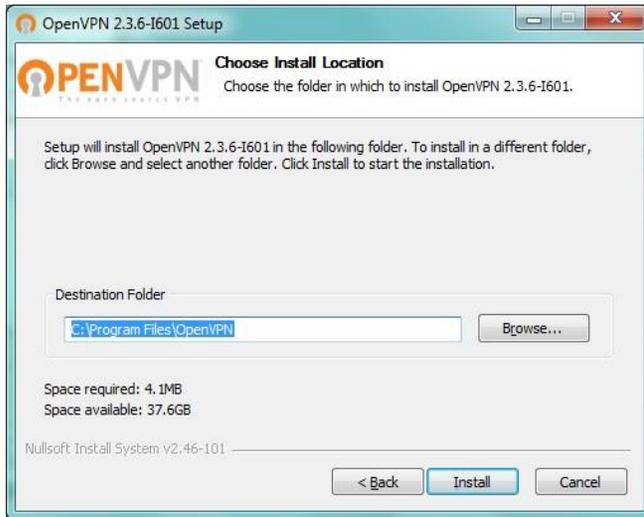
6. At the license agreement window, review the license agreement and click **I Agree**.



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**.



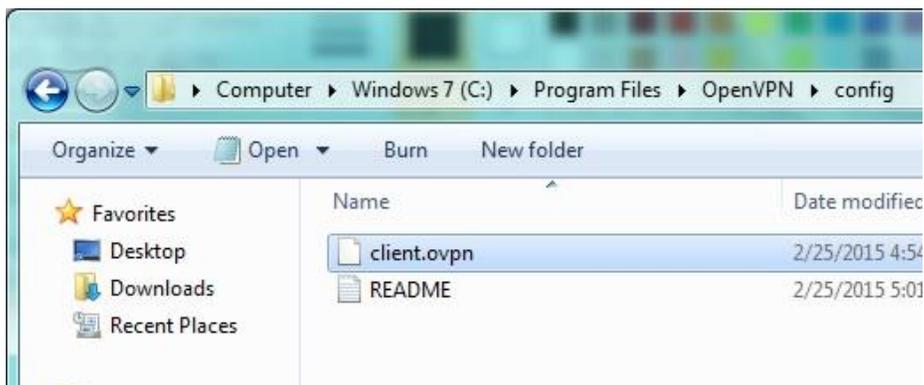
11. Make sure to uncheck the "Show Readme" and "Start OpenVPN GUI" options and click **Finish**.



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



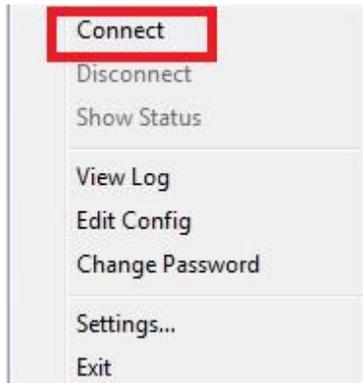
13. Double-click on the OpenVPN GUI shortcut on your desktop to start the OpenVPN Client software.



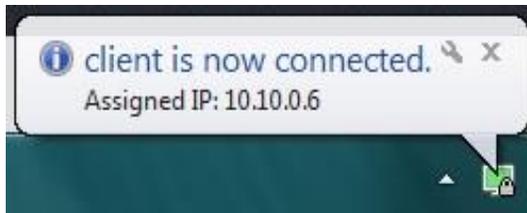
14. The OpenVPN system tray icon will appear in the bottom right corner. Right-click the icon to display the configuration menu.



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 59.

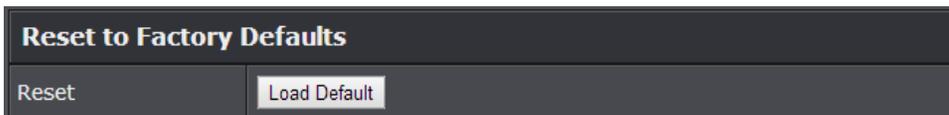
There are two methods that can be used to reset your router to factory defaults.

- **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 10).
2. Click on **Advanced** and click on **Administrator**, then click on **Settings Management**.
3. Next to **Reset to Factory Default Settings** and **Reset**, click **Load Default**. When prompted to confirm this action, click **OK**.



Router Default Settings

Administrator User Name	admin
Administrator Password	Please refer to sticker or device label
Router Default URL	http://tew-827dru
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 Network Name/Encryption	Please refer to sticker or device label
Wireless 2.4GHz & 5GHz Guest Network	Disabled
USB SMB & FTP Settings	Disabled
USB SMB & FTP User Name	Same as Administrator
USB SMB & FTP Password	Same as Administrator

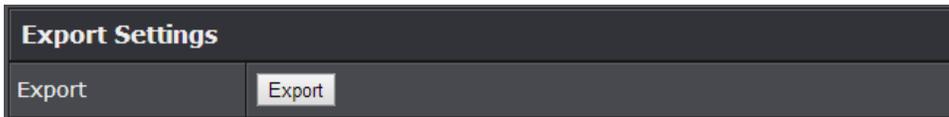
Backup and restore your router configuration settings

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 10).
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-827DRU_config.bin*)

To restore your router configuration:

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
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-827DRU_config.bin*). If prompted, click **Yes** or **OK**.
6. Wait for the router to restore settings.

Reboot your router

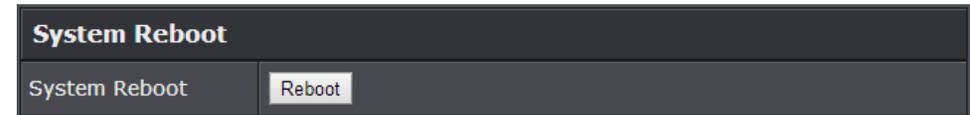
Advanced > Administrator > Settings Management

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 10).
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 > Setup > 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/support>

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.

Online Firmware Upgrade (requires router to be connected to Internet)

When your router has detected a new firmware available online, a notification will appear in the top right corner of the router management page.

You can click the link or go to Advanced > Setup > Upload Firmware.

New firmware is available

Under the Online Firmware Upgrade section, it will list the current firmware version loaded on your router. Click **Check** to manually check if there is a new firmware available online.

Online Firmware Upgrade	
Current Version	2.00, 14, Jun, 2017
Online Check	<input type="button" value="Check"/>

If a new firmware version is available, the details of the new version will appear such as the firmware version, firmware file size, and release notes about the new firmware.

To start the online firmware upgrade process, click **Apply**. Please wait for the online firmware upgrade procedure to complete successfully.

Firmware Upgrade Information	
New Version	
Size	
Release Note:	
<ul style="list-style-type: none"> - Support Auto Firmware Upgrade - Support LAN Domain and DNS 	
DO NOT upgrade using a wireless connection.	
Upgrading firmware using a wireless connection may damage the device. Please upgrade the firmware using a wired connection only.	
<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>

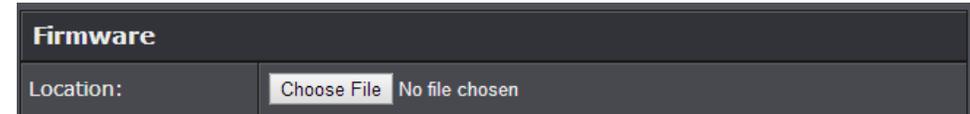
Manual Firmware Upgrade

1. If a firmware upgrade is available, check the router model on our website <http://www.trendnet.com/support> and 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 10).
2. Click on **Advanced** and click **Setup**, then click **Firmware**.
3. Depending on your web browser, in the **Upload Firmware** section, click **Browse** or **Choose File**.



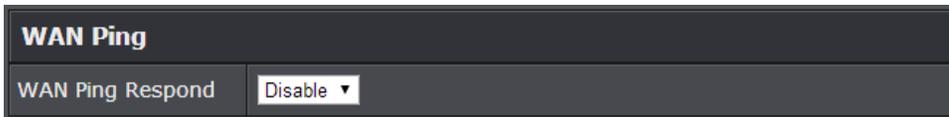
4. Navigate to the folder on your computer where the unzipped firmware file (.bin) is located and select it.
5. Click **Apply**. If prompted, click **Yes** or **OK**.

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 10).
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 **Enable** to allow your router to respond to ping requests from the Internet. You can also choose **Disable** to block WAN ping requests from the Internet



WAN Ping	
WAN Ping Respond	Disable ▾

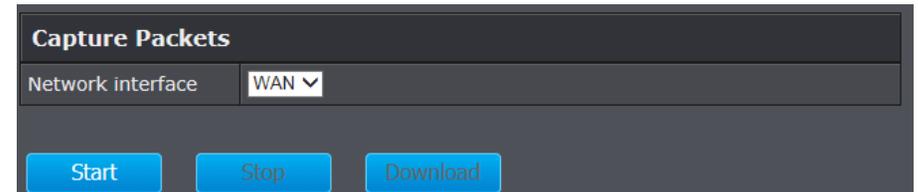
4. To save changes to this section, click **Apply** when finished. Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

How to capture network packets

Advanced > Administrator > Advanced Network

The router has the built-in capability to capture network packets for troubleshooting purposes.

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Administrator**, then click on **Advanced Network**.
3. Under **Capture Packets**, click the **Network Interface** drop-down list and select interface you would like to capture packets on (LAN or WAN). Click **Start** to start the capture and click **Stop** to stop the capture. You can click **Download** to download the packet capture file to view in the packet capture program such as Wireshark.



Capture Packets		
Network interface	WAN ▾	
Start	Stop	Download

Diagnostic Tools

Advanced > Administrator > Diagnostics

The router also provides additional tools for network troubleshooting such as ping test, traceroute, nslookup, and netstat.

Ping Test	
IP	<input type="text"/>
Packet Length	64 <input type="text"/> (bytes)
Number of Pings	4 <input type="text"/>
<input type="button" value="Ping"/>	
Traceroute Parameter	
Target	<input type="text"/>
<input type="button" value="Traceroute"/>	
Nslookup	
Option	Google <input type="text"/>
<input type="button" value="Nslookup"/>	
Netstat	
Option	Display all sockets <input type="text"/>
Resolve name	No <input type="text"/>
<input type="button" value="Netstat"/>	

Ping Watchdog

Advanced > Setup > Ping Watchdog

The ping watchdog feature allows the router automatically reboot when communication (ping) connectivity is lost to a specific device IP address. For example, if your router lost connectivity to an address located on the Internet (assuming complete connectivity had been dropped or lost), the router will automatically initiate a device reboot in an attempt to help resolve the connectivity issue and resume Internet connectivity.

- **Enable:** Enables or disables the ping watchdog feature.
- **IP Address to Ping:** The IP address or URL to check connectivity.
- **Startup Delay:** The delay time that router will wait after reboot to start the connectivity (ping) test to the specified IP address or URL.
- **Ping Interval:** The time interval between each connectivity (ping) test to the specified IP address or URL.
- **Threshold:** The number of consecutive times the connectivity (ping) test is allowed to fail before the router initiates an automatic reboot.

Ping Watchdog	
Enable	<input type="checkbox"/>
IP Address To Ping	www.google.com <input type="text"/>
Startup Delay	300 <input type="text"/> (seconds)
Ping Interval	1800 <input type="text"/> (seconds)
Threshold	10 <input type="text"/>

Auto Reboot

Advanced > Setup > Auto Reboot

The scheduled automatic reboot feature allows you to set a daily or weekly schedule for the router to initiate an automatic reboot in an attempt to resolve any connectivity issues or intermittent problems that may occur with your device. Before using the scheduled automatic reboot feature, *please ensure your Time settings are configured correctly. See page 41 to configure [Time Settings](#).*

- **Rule Name:** Enter a name for the schedule you would like to apply.
- **Day(s)/Select Day(s):** Check **Select Day(s)** to select the days in the **Select Day(s)** section or select **All Week** to set the schedule for all days.
- **All Day – 24 Hours** – Check the option to set the schedule to 24 hours or define the schedule under **Start Time** and **End Time**.
- **Start Time:** Select the start time you would like the schedule to follow.
Note: The schedule defined will define the time/day the feature will be activated.

Commit your changes to the router by clicking on **Apply/Discard Changes** in the left-hand menu, and click **Apply & Reboot**.

Add Rule	
Rule Name	<input type="text"/>
Day(s)	<input checked="" type="radio"/> Select Day(s) <input type="radio"/> All Week
	<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
Start Time	<input type="text" value="00"/> : <input type="text" value="00"/>
<input type="button" value="Add"/> <input type="button" value="Clear"/>	

Wireless Client List

Advanced > Administrator > Client Status

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

1. Log into your router management page (see "[Access your router management page](#)" on page 10).
2. Click on **Advanced** and click on **Administrator**, then click on **Client Status**.

Connected Devices: Lists all of the currently connected devices via wired physical connection through the four Gigabit LAN ports.

2.4GHz/5GHz Wireless Connected Devices: Lists all of the currently connected wireless devices on either 2.4GHz or 5GHz band/radio.

- **IP Address:** The current IP address of the client device.
- **MAC Address:** The MAC address of the client device.
- **Hostname:** The device host name of the client device
- **SSID:** The SSID the client device is currently connected.
- **Mode:** Displays the 802.11 mode associated with the client.
- **Signal Level:** Displays the estimated signal strength (RSSI) of the client device to the router.
- **Link Rate:** Displays the estimated link rate of the client device connection to the router.

Connected Devices		
IP Address	MAC Address	Host Name
192.168.10.101	00:1c:c0:24:49:12	JEREMY10
192.168.10.103	d4:be:d9:03:7f:9f	EXJALIEN

2.4GHz Wireless Connected Devices					
SSID	IP Address	MAC Address	Host Name	Signal Level	Link Rate

5GHz Wireless Connected Devices					
SSID	IP Address	MAC Address	Host Name	Signal Level	Link Rate

Check the router system information

Advanced > Administrator > 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 10).
2. Click on **Advanced** and click on **Administrator**, then click on **Status**

System Information

- **Firmware Version** – The current firmware version your router is running.
- **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	1.00, 12, May, 2014
System Time	Sat Jan 10 17:40:59 1970
System Up Time	10 Days, 1:40:54

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.
- **WAN MAC Address:** Displays the current WAN MAC address.
- **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	Dynamic IP (DHCP)
WAN IP Address	10.10.10.114
WAN MAC Address	00:18:E7:95:85:04
Subnet Mask	255.255.255.0
Default Gateway	10.10.10.254
Primary Domain Name Server	10.10.10.254
Secondary Domain Name Server	0.0.0.0

- **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 (SSID) / Security Mode:** Displays the current 2.4GHz primary wireless network name and security mode assigned to your router.
- **Multiple SSID1 / Security Mode:** Displays the current 2.4GHz wireless network name and security mode of multiple SSID1 assigned to your router.
- **Multiple SSID2 / 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	
MAC Address	C0:A0:BB:6E:08:C3
Channel	1
Network Name (SSID) / Security Mode	TRENDnet823_2.4GHz_XXXX / WPA2 Only - PSK
Multiple SSID1 / Security Mode	
Multiple SSID2 / Security Mode	
Guest Network / Security Mode	

5GHz Wireless LAN

- **MAC Address:** The MAC address of your router's 5GHz wireless LAN interface configuration.
- **Network Name (SSID) / Security Mode:** Displays the current 5GHz primary wireless network name and security mode assigned to your router.
- **Multiple SSID1 / 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 Wireless	
MAC Address	C0:A0:BB:6E:08:C5
Channel	40
Network Name (SSID) / Security Mode	TRENDnet823_5GHz_XXXX / WPA2 Only - PSK
Multiple SSID1 / Security Mode	
Multiple SSID2 / Security Mode	
Guest Network / Security Mode	

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 10).
2. Click on **Advanced** and click on **Administrator**, then click on **IPv6 Status**

IPv6 Connection Information	
IPv6 Connection Type	Auto Configuration (SLAAC/DHCPv6)
Network Status Address	Disconnected
<div style="display: flex; justify-content: space-around;"> Renew Release </div>	
WAN IPv6 Address	
IPv6 Default Gateway	
LAN IPv6 Address	
LAN IPv6 Link-Local Address	fe80::218:e7ff:fe95:8503/64
Primary DNS Server	
Secondary DNS Server	
LAN IPv6 Computers	
IPv6 Address	Name (if any)
fe80::3551:6b9e:729b:50a2	Jeremy7

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 10).
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 SPI=49461 DPT=443 WINDOW=65535
RES=0x00 SYN URGF=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 SPI=49461 DPT=443 WINDOW=65535
RES=0x00 SYN URGF=0

```

Router Management Page Structure

BASIC

- Network Status
- Wireless
 - 2.4GHz Settings & Security
 - 5GHz Settings & Security
- Guest Network
- Parental Control
 - MAC/IP Address Filter
 - Website Filter
- Router Limits

ADVANCED

- Administrator
 - Status
 - IPv6 Status
 - System Log
 - Advanced Network
 - UPnP
 - Settings Management
 - Export/Import configuration
 - Reset to factory default
 - Reboot
 - Time
- Setup
 - LAN Settings

- IP Address Setting
 - DHCP Server Setting
 - DHCP Reservation
- WAN Settings
- Routing
- IPv6 Settings
- Schedule
- Upload Firmware
- Management
 - Administrator Password
 - Dynamic DNS
 - Remote Management
- DHCP Client List
- Wizard
- VPN
- Ping Watchdog
- Auto Reboot
- Wireless 2.4GHz
 - Advanced
 - Multiple SSID
 - MAC Filter (Wireless)
 - WPS
 - Station List
- Wireless 5GHz

- Advanced
- Multiple SSID
- MAC Filter (Wireless)
- WPS
- Station List
- Security
 - Access Control (IP Protocol Filter)
 - Inbound Filter
- Firewall
 - DMZ
 - Virtual Server
 - Special Applications
 - Gaming
 - ALG
 - DoS
 - IPv6 Firewall
- USB
 - File Sharing Server
 - FTP Server
 - BitTorrent
 - Eject Device

Technical Specifications

Standards

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x
- IEEE 802.3ab
- IEEE 802.3az
- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n (up to 800 Mbps @ 256QAM)*
- IEEE 802.11ac (up to 1733 Mbps)*

Hardware Interface

- 4 x Gigabit LAN ports
- 1 x Gigabit WAN port
- 1 x USB 3.0 (Storage FTP, Samba, iTunes® Media Server, BitTorrent Client)
- Power switch
- WPS button
- Reset button
- LED indicators

Special Features

- Multi-User MIMO for increased bandwidth efficiency and better user experience*
- Multi-Language interface: English, French, Spanish, German, Russian, Portuguese
- 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, no-ip.com, and easydns.com
- Samba/FTP server support
- 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/IPsec VPN Passthrough, TFTP/FTP/RTSP/SIP/H.323 Passthrough
- Parental (Access) Controls: MAC, URL, IP Filter

Quality of Service

- WMM

Internet Connection Types

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

Management/Monitoring

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

Routing

- Static
- Dynamic (RIP v1/2)

Frequency

- 2.412 - 2.472 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 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: 4 x 3 dBi (max.) detachable/external; 5 GHz: 4 x 5 dBi

Wireless Output Power (max output power without antenna gain)

- 802.11a: FCC: 26 dBm (max.) / ETSI: 22 dBm (max.) / IC: 26 dBm (max.)
- 802.11b: FCC: 27 dBm (max.) / ETSI: 15 dBm (max.) / IC: 27 dBm (max.)
- 802.11g: FCC: 25 dBm (max.) / ETSI: 16 dBm (max.) / IC: 25 dBm (max.)
- 802.11n (2.4 GHz): FCC: 25 dBm (max.) / ETSI: 16 dBm (max.) / IC: 25 dBm (max.)
- 802.11n (5 GHz): FCC: 25 dBm (max.) / ETSI: 23 dBm (max.) / IC: 25 dBm (max.)
- 802.11ac: FCC: 25 dBm (max.) / ETSI: 24 dBm (max.) / IC: 25 dBm (max.)

Receiving Sensitivity (per chain)

- 802.11a: -70 dBm (typical) @ 54 Mbps
- 802.11b: -83 dBm (typical) @ 11 Mbps
- 802.11g: -70 dBm (typical) @ 54 Mbps
- 802.11n (2.4 GHz): -59 dBm (typical) @ 800 Mbps
- 802.11n (5 GHz): -59 dBm (typical) @ 800 Mbps
- 802.11ac: -55 dBm (typical) @ 1733 Mbps

Wireless Channels

- 2.4 GHz: FCC: 1-11; ETSI: 1-13
- 5 GHz: FCC: 36, 40, 44, 48, 149, 153, 157, 161, 165; ETSI: 36, 40, 44, 48, (52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140)**

Power

- Input: 100 – 240 V AC, 50 - 60 Hz
- Output: 12V DC, 1.5A external power adapter
- Consumption: 17.4W (max.)

Operating Temperature

- 0 – 40 °C (32 – 104 °F)

Operating Humidity

- Max. 95% non-condensing

Certifications

- CE
- FCC
- IC

Dimensions

- 250 x 180 x 45 mm (9.8 x 7.1 x 1.8 in.)

Weight

- 612 g (21.6 oz.)

Disclaimers

*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions. For maximum performance of up to 1.733 Gbps use with a 1.733 Gbps 802.11ac wireless adapter. For maximum performance of up to 800 Mbps, use with an 800 Mbps 802.11n wireless adapter. Multi-User MIMO (MU-MIMO) requires the use of multiple MU-MIMO enabled wireless adapters.

** Due to regulatory requirements, the wireless channels specified cannot be statically assigned, but will be available within the available wireless channels when set to auto.

Troubleshooting

Q: I typed <http://tew-827dru> 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 28 if you continue to have wireless connectivity problems.

Appendix

How to find your IP address?

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

Command Prompt Method

Windows 2000/XP/Vista/7/8/8.1/10

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

MAC OS X

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

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

Graphical Method

MAC OS 10.6/10.5

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 7/8/8.1/10

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

Windows Vista

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

Windows XP/2000

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

MAC OS 10.4/10.5/10.6

- a. From the **Apple**, drop-down list, select **System Preferences**.
- b. Click the **Network** icon.
- c. From the **Location** drop-down list, select **Automatic**.
- d. Select and view your Ethernet connection.
 - In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Ethernet** and select the **TCP/IP** tab.
 - In MAC OS 10.5/10.6, in the left column, select **Ethernet**.
- e. Configure TCP/IP to use DHCP.

In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Using DHCP** and click the **Apply Now** button.

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

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

f. Restart your computer.

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

How to find your MAC address?

In Windows 2000/XP/Vista/7/8.1/10,

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

In MAC OS 10.4,

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 7/8/8.1/10

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

Windows Vista

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

Windows XP

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

Federal Communication Commission Interference Statement

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

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

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

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

Operation of this device is restricted to indoor use only

IMPORTANT NOTE:

Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24cm between the radiator & your body.

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

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

RoHS

This product is RoHS compliant.



Europe – EU Declaration of Conformity

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

Safety

EN 62368-1:2014

EMC

EN 301 489-1 V2.1.1 (2017-02)

EN 301 489-17 V3.1.1 (2017-02)

EN 55032: 2012+ AC: 2013

EN 55024: 2010



Radio Spectrum & Health

EN 300 328 V2.1.1 (2016-11)

EN 301 893 V2.1.1 (2017-05)

EN 62311: 2008

Energy Efficiency

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

This product is herewith confirmed to comply with the Directives.

Directives

Low Voltage Directive 2014/35/EU

EMC Directive 2014/30/EC

RE Directive 2014/53/EU

EMF Directive 1999/519/EC 2013/35/EU

Ecodesign Directive 2009/125/EC

RoHS Directive 2011/65/EU

WEEE Directive 2012/19/EU

REACH Regulation (EC) No. 1907/2006

Lot 26 Statement: This product is inappropriate for the intended use according to HiNA requirements.

 Český [Czech]	TRENDnet tímto prohlašuje, že tento TEW-827DRU je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/35/ES, 2014/30/ES, 2014/53/EU, 2013/35/EU, 2009/125/ES, 2011/65/EU, a 2012/19/EU.
 Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-827DRU overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/35/EF, 2014/30/EF, 2014/53/EU, 2013/35/EU, 2009/125/EF, 2011/65/EU, og 2012/19/EU.
 Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TEW-827DRU in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/35/EG, 2014/30/EG, 2014/53/EU, 2013/35/EU, 2009/125/EG, 2011/65/EU, und 2012/19/EU befindet.
 Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEW-827DRU vastavust direktiivi 2014/35/EÜ, 2014/30/EÜ, 2014/53/EU, 2013/35/EU, 2009/125/EÜ, 2011/65/EU, ja 2012/19/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, TRENDnet, declares that this TEW-827DRU is in compliance with the essential requirements and other relevant provisions of Directive 2014/35/EC, 2014/30/EC, 2014/53/EU, 2013/35/EU, 2009/125/EC, 2011/65/EU, and 2012/19/EU.
 Español [Spanish]	Por medio de la presente TRENDnet declara que el TEW-827DRU cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/35/CE, 2014/30/CE, 2014/53/EU, 2013/35/EU, 2009/125/CE, 2011/65/EU, 2012/19/EU y.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑΤRENDnet ΔΗΛΩΝΕΙ ΟΤΙΤΕW-827DRUΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/35/EK, 2014/30/EK, 2014/53/EU, 2013/35/EU, 2009/125/EK, 2011/65/EU, 2012/19/EU και.
 Français [French]	Par la présente TRENDnet déclare que l'appareil TEW-827DRU est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/35/CE, 2014/30/CE, 2014/53/EU, 2013/35/EU, 2009/125/CE, 2011/65/EU, 2012/19/EU et.
 Italiano [Italian]	Con la presente TRENDnet dichiara che questo TEW-827DRU è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti

	stabilitate dalla direttiva 2014/35/CE, 2014/30/CE, 2014/53/EU, 2013/35/EU, 2009/125/CE, 2011/65/EU, e 2012/19/EU.
 Latviski [Latvian]	AršoTRENDnetdeklarē, ka TEW-827DRU atbilstDirektīvas 2014/35/EK, 2014/30/EK, 2014/53/EU, 2013/35/EU, 2009/125/EK, 2011/65/EU, un 2012/19/EU būtiskajāmprasībām un citiemar to saistītajiemnoteikumiem.
 Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TEW-827DRU atitinka esminius reikalavimus ir kitas 2014/35/EB, 2014/30/EB, 2014/53/EU, 2013/35/EU, 2009/125/EB, 2011/65/EU, ir 2012/19/EU Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEW-827DRU in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/35/EG, 2014/30/EG, 2014/53/EU, 2013/35/EU, 2009/125/EG, 2011/65/EU, en 2012/19/EU.
 Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TEW-827DRU jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/35/KE, 2014/30/KE, 2014/53/EU, 2013/35/EU, 2009/125/KE, 2011/65/EU, u 2012/19/EU.
 Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-827DRU megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv, a 2014/35/EK, 2014/30/EK, 2013/35/EU, 2009/125/EK, 2011/65/EU, és a 2012/19/EU irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEW-827DRU jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/35/WE, 2014/30/WE, 2014/53/EU, 2013/35/EU, 2009/125/WE, 2011/65/EU, i 2012/19/EU.
 Português [Portuguese]	TRENDnet declara que este TEW-827DRU está conforme com os requisitos essenciais e outras disposições da Directiva 2014/35/CE, 2014/30/CE, 2014/53/EU, 2013/35/EU, 2009/125/CE, 2011/65/EU, e 2012/19/EU.
 Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEW-827DRU v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/35/ES, 2014/30/ES, 2014/53/EU, 2013/35/EU, 2009/125/ES, 2011/65/EU, in 2012/19/EU.

Slovensky [Slovak]	TRENDnet týto vyhlasuje, že TEW-827DRU spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/35/ES, 2014/30/ES, 2014/53/EU, 2013/35/EU, 2009/125/ES, 2011/65/EU, a 2012/19/EU.
 Suomi [Finnish]	TRENDnet vakuuttaa täten että TEW-827DRU tyyppinen laite on direktiivin 2014/35/EY, 2014/30/EY, 2014/53/EU, 2013/35/EU, 2009/125/EY, 2011/65/EU, ja 2012/19/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar TRENDnet att denna TEW-827DRU står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/35/EG, 2014/30/EG, 2014/53/EU, 2013/35/EU, 2009/125/EG, 2011/65/EU, och 2012/19/EU.

Industry Canada Statement

This device complies with Industry Canada's licence-exempt RSSs. 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;
- 2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This radio transmitter (IC: 6337A-TEW827DRUV2) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain 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 (IC: 6337A-TEW827DRUV2) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Type	Manufacture	Gain	Connector
Dipole	WHAYU	3 dBi (2.4G) /5dBi (5.0G)	R-SMA

Caution:

the device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

Avertissement:

les dispositifs fonctionnant dans la bande de 5150 à 5250MHz 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;

Radiation Exposure Statement:

This equipment complies with Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 29cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme Canada limites d'exposition aux radiations dans un environnement non contrôlé. Cet équipement doit être installé et utilisé à distance minimum de 29cm entre le radiateur et votre corps.

Limited Warranty

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

Limited Warranty

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

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

Limited Lifetime Warranty

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

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

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

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

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

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

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

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

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation, a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. International customers

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

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

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, OR USE OF TRENDNET'S PRODUCTS.

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

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

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

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

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

PWP07172015v3

2019/01/10



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