

User's Guide

TRENDNET[®]



**AC3000 Tri-Band Wireless Gigabit
Dual-WAN VPN SMB Router**

TEW-829DRU

Table of Contents

Product Overview	1
Package Contents	1
Features	1
Product Hardware Features.....	3
Applications	5
Router Installation	2
Desktop Hardware Installation	2
Rack Mount Hardware Installation.....	2
Basic Installation and Configuration	3
Basic Router Settings.....	8
Access your router management page.....	8
Saving and applying router configuration changes	8
Change your administrator password	8
Set your router date and time	9
Create time schedules	10
Change LAN IPv4 address settings.....	11
Configure LAN IPv4 DHCP server settings.....	12
Add static DHCP reservations	15
Add static host name entries.....	15
Add static ARP entries	16
Configure WAN1 / WAN2 interfaces for Internet connectivity	17
IPv6 settings.....	19
Virtual LANs (VLANs).....	20
Create a port-based VLAN.....	20
Create a port-based VLAN with 802.1Q tagging	21
Assigning VLAN IDs to Wireless SSIDs	24

Application layer gateway (ALG)	26
UPnP and NAT-PMP.....	27
Static routes.....	27
Dynamic routing protocols	28
Routing Information Protocol (RIP).....	28
OSPF (Open Shortest Path First)	29
Quality of Service (QoS).....	30
Dynamic DNS	32
File sharing server.....	33
Wake on LAN (WoL).....	34
Wireless Networking and Security.....	35
Wireless Settings	35
Primary SSID.....	35
Multiple SSID.....	37
How to choose the type of wireless security.....	38
Secure your wireless network	39
Guest Network.....	41
WiFi client bridge mode	42
Connect wireless devices using WPS	43
Steps to improve wireless connectivity.....	45
Firewall & security settings	46
General settings.....	46
Port forwarding rules.....	47
Port trigger rules.....	48
IP filtering	49
MAC filtering.....	50
Denial of service (DoS) prevention	51
DMZ Host.....	51

One-to-One NAT	52	IPsec	88
RADIUS Authentication	54	OpenVPN.....	89
Multiple WAN Configuration	55	Router Maintenance and Monitoring	90
Multiple WAN Management Settings	55	Managing access to the router management interface	90
MWAN Status.....	55	Local Access Management.....	90
Link Tracking	55	Remote Access Management	90
Default Traffic Rule	56	Diagnostic tools	91
Web Management System (Router Limits™)	57	Backup and restore your router configuration settings	92
Setup your router with Router Limits	57	Reboot your router.....	92
Router Limits Content Management	59	Scheduled automatic reboot	93
Virtual Private Networking (VPN)	62	Console access.....	93
Creating a Virtual Private Network (VPN).....	62	Command Line Interface	93
PPTP VPN Server	63	Router Default Settings	94
Setting up the PPTP VPN server	63	Reset your router to factory defaults	94
Setting up the PPTP VPN client (Windows).....	65	Upgrade your router firmware	95
L2TP VPN Server	66	Ping Watchdog	97
Setting up the L2TP VPN server without IPsec encryption	66	Local Access Management.....	97
Setting up the L2TP VPN server with IPsec encryption (PSK).....	68	Check the router status information	98
Setting up the L2TP VPN client (Windows) with IPsec encryption (PSK)	70	View routing table and ARP entries.....	100
IPsec (Internet Protocol Security)	72	View your router logging	101
Setting up IPsec site-to-site VPN (PSK).....	72	Configure router logging settings and setup external syslog server	101
Setting up IPsec server VPN (PSK with xAUTH)	75	Technical Specifications	102
Setting up IPsec site-to-site VPN Failover (PSK)	78	Troubleshooting	105
Secure Socket Layer VPN (SSL) / OpenVPN.....	83	Appendix	106
SSL VPN Server Setup	83		
SSL VPN Client Setup (Windows).....	84		
Certificate Management.....	88		

Product Overview



TEW-829DRU

Package Contents

In addition to your router, the package includes:

- Quick Installation Guide
- 6 x detachable high gain antennas
- Network cable (1.5 m/5 ft.)
- RJ-45 to RS-232 console cable (1.5m / 5 ft.)
- Power adapter (12V DC, 3 A)
- Rack mount kit

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 AC3000 Tri-Band Wireless Gigabit Dual-WAN VPN SMB Router, model TEW-829DRU, features three concurrent WiFi bands to maximize device networking speeds: two separate high performance 802.11ac networks (5GHz1: 1733Mbps / 5GHz2: 867Mbps), and a 400Mbps Wireless N network. It features dual-WAN ports for load balancing or fail-over modes, and encrypted Virtual Private Network (VPN) access for remote users. Dual-WAN ports smooth network loading, minimize network downtime, and allow employees to access your network from the Internet—all with a single router.

This wireless router features advanced management, QoS, VLAN, VPN, and other capabilities to ensure optimal performance, scalability, and protection of your network. Intelligently manage your offices' web access with our advanced content filtering tool, increase employee productivity and finally take control of your internet.

Dual-WAN

Supports up to two separate WAN internet connections for load-balancing or fail-over modes

Ports

2 x Gigabit WAN ports, 8 x Gigabit LAN ports, 1 x USB 3.0 port, 1 x Console port

Tri-Band WiFi

Three concurrent WiFi bands maximize device networking speeds: two separate high performance 802.11ac networks 1733Mbps (5GHz1) + 867Mbps (5GHz2) + 400Mbps (2.4GHz) bands

Pre-Encrypted Wireless

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

VPN

Supports IPsec, PPTP, L2TP w/ IPsec, and SSL VPN protocols for encrypted remote access to local area network (LAN) resources over the internet

Inter-VLAN Routing

Provides routing capabilities between VLANs

QoS

Intelligently prioritize voice, video, and other data traffic to improve network efficiency and overall performance

Rack Mount Design

Sturdy metal housing with rack mount brackets included

Wall Mountable

Wall mount ready

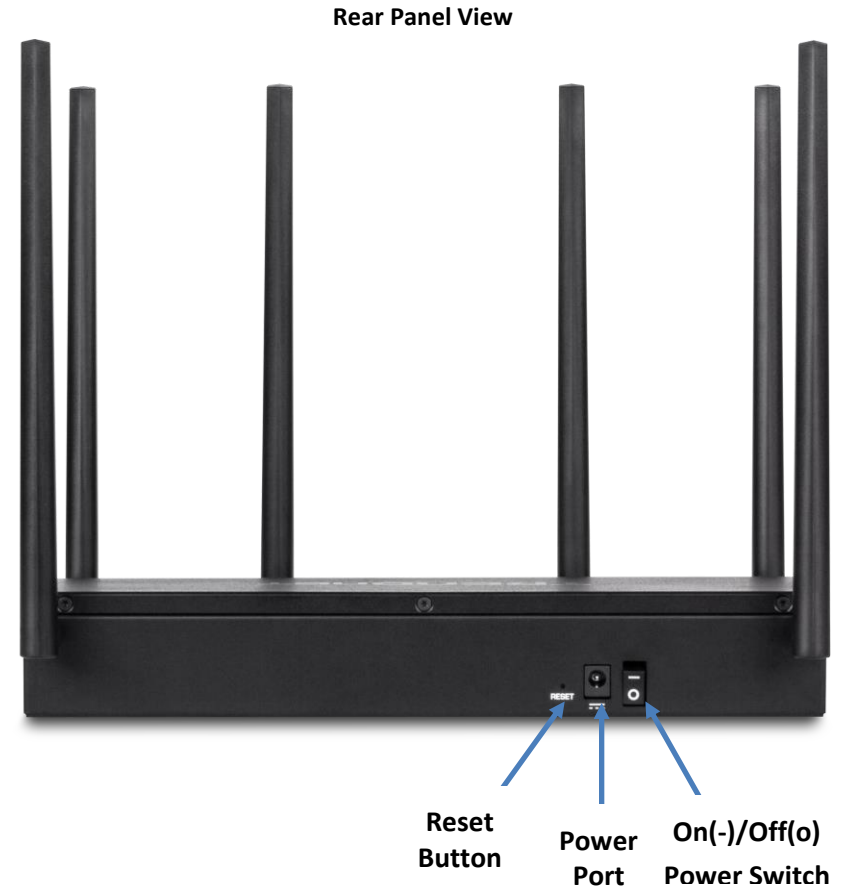
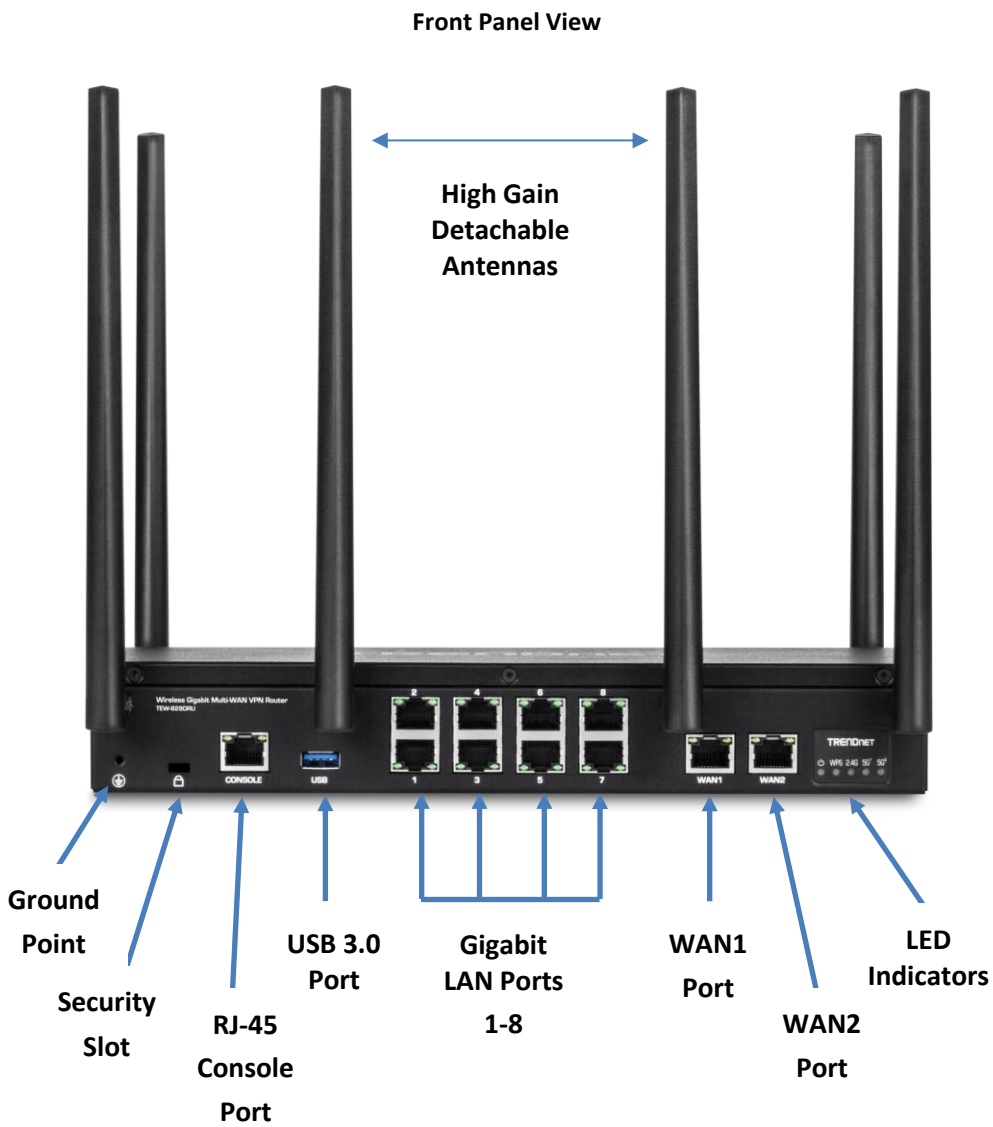
Online Firmware Updates

Automatic notification of firmware updates






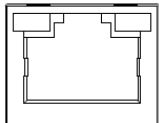
Management

Supports web browser (HTTP, HTTPS), CLI, SSH and Telnet management

Product Hardware Features



LED Indicators

LED	Description
	Solid Blue – Device is receiving power and turned on. Off – Device is not receiving power or turned off.
	Solid Blue – WPS connection process was successful. WPS LED will remain on after successful connection for 2 minutes. Blinking Blue – WPS is activated and setup process has started. Within 2 minutes, start the WPS process on your WPS client device to connect. Off – WPS setup process has stopped or has not been activated.
	Solid Blue – 2.4GHz (2-stream) wireless radio is turned on. Blinking Blue – Data transmission on 2.4GHz radio. Off – 2.4GHz (2-stream) wireless radio turned off.
	Solid Blue – 5GHz ¹ (4-stream) wireless radio is turned on. Blinking Blue – Data transmission on 5GHz ¹ radio. Off – 5GHz ¹ (4-stream) wireless radio turned off.
	Solid Blue – 5GHz ² (2-stream) wireless radio is turned on. Blinking Blue – Data transmission on 5GHz ² radio. Off – 5GHz ² (2-stream) wireless radio turned off.
Port LEDs 	LAN 1-8, WAN1 & WAN2 Ports LED (Right Side) Solid Green – Port is connected at 1Gbps link speed. Off – Port is connected at 10Mbps or 100Mbps link speed. LED (Left Side) Blinking Green - Data activity/transmission on port.

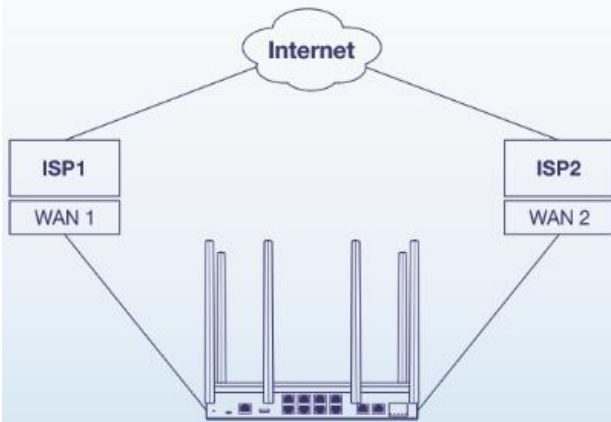
Port/Button Description

Ports/Buttons	Description
Grounding Point	Allows the device chassis to be connected to a known ground point for electrical safety and protection possible shock or surge during device operation and handling. (Grounding wire and screw not included.)
Security Slot	Allows for an optional cable lock attachment to secure the device to a physical location.
RJ-45 Console Port	Using the included RJ-45 to RS-232 console cable, this interface provides console/terminal (command line interface) access to the device for management and troubleshooting purposes. Terminal Settings: Baud: 115200 / Data: 8 / Stop: 1 / Parity: None / Flow: None
USB 3.0 Port	Allows for an optional USB storage device (flash drive, external HDD, etc.) to be connected and used as a network share through the Samba protocol. (FAT32/NTFS format only)
LAN Interface Ports 1-8	Connect network devices to the LAN interface ports 1-8 at Gigabit, 10Mbps/100Mbps Full/Half Duplex. By default, management access to the GUI and command line interface via default LAN IP address: 192.168.10.1 / 255.255.255.0
WAN1 Interface Port	Connects to your Internet Service Provider (ISP) equipment for Internet connectivity such as modem. By default, WAN mode is set for failover and WAN1 is configured as the primary WAN link for Internet connectivity.
WAN2 Interface Port	Connects to your Internet Service Provider (ISP) equipment for Internet connectivity such as modem. By default, WAN mode is set for failover and WAN2 is configured as the secondary WAN link for Internet connectivity.
Reset Button	Resets device to factory defaults. Using a paperclip, push and hold the reset button for 15 seconds and release to reset the device to factory defaults.
Power Port	Connects the included power adapter to supply device power.
On(-)/Off(o) Power Switch	Turns the device power On(-) or Off(o).

Applications

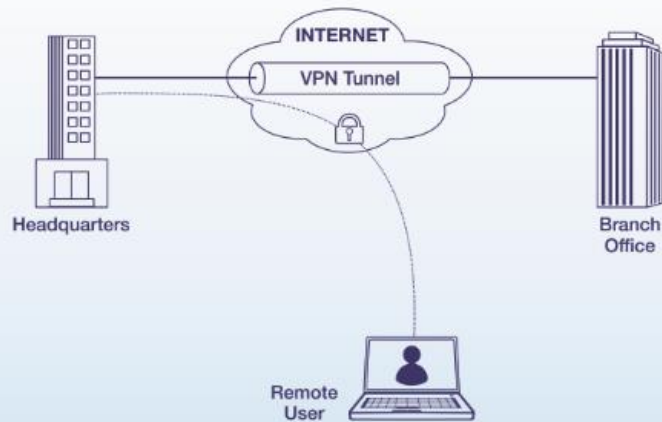
Dual-WAN

Connect up to two separate WAN internet connections to efficiently load-balance traffic by distributing network traffic to the best available link, or configure for redundancy using the WAN fail-over mode.



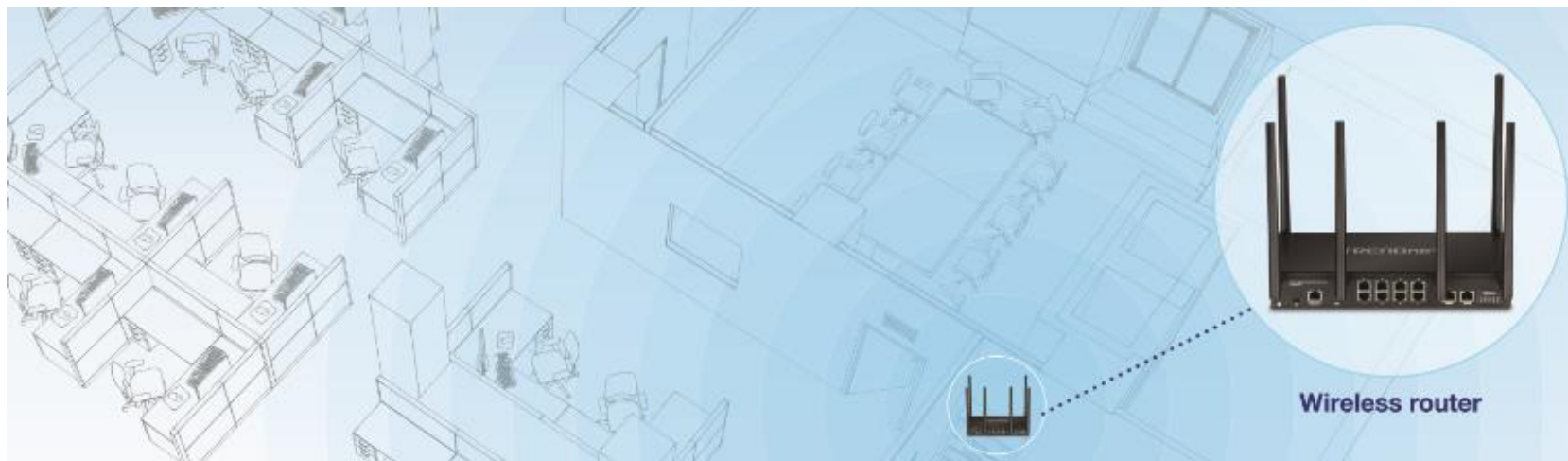
VPN

Create an encrypted VPN tunnel to access local area network resources remotely using IPSec, PPTP, L2TP w/ IPsec, and SSL VPN protocols.



AC3000 Tri-Band WiFi

Three concurrent WiFi bands maximize device networking speeds: two separate high performance 802.11ac networks 1733Mbps (5GHz1) + 867Mbps (5GHz2) + 400Mbps (2.4GHz) bands



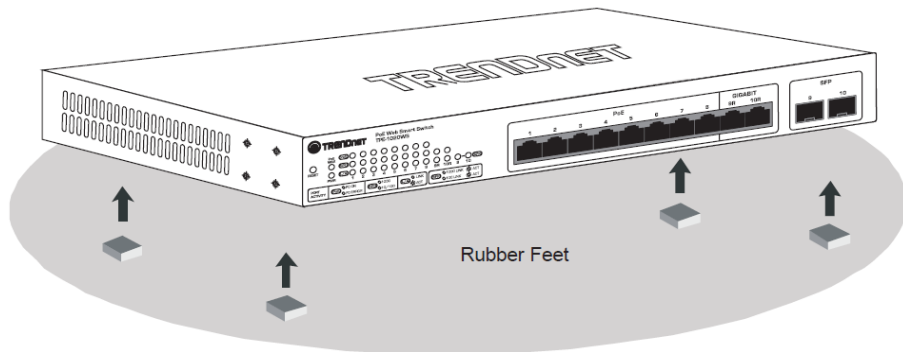
Router Installation

Desktop Hardware Installation

The site where you install the hub stack may greatly affect its performance. When installing, consider the following pointers:

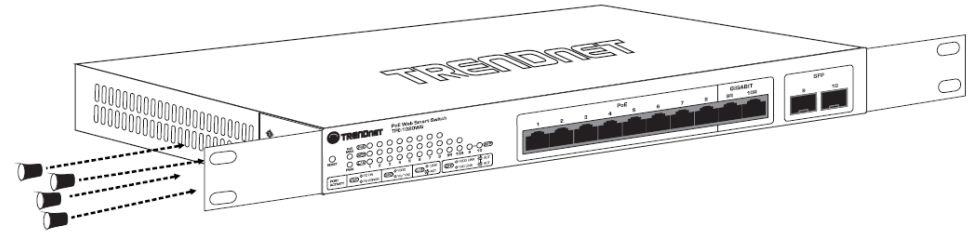
Note: The router model may be different than the one shown in the example illustrations.

- Install the Router in a fairly cool and dry place.
- Install the Router in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
- Leave at least 10cm of space at the front and rear of the hub for ventilation.
- Install the Router on a sturdy, level surface that can support its weight, or in an EIA standard-size equipment rack. For information on rack installation, see the next section, Rack Mounting.
- When installing the Router on a level surface, attach the rubber feet to the bottom of each device. The rubber feet cushion the hub and protect the hub case from scratching.

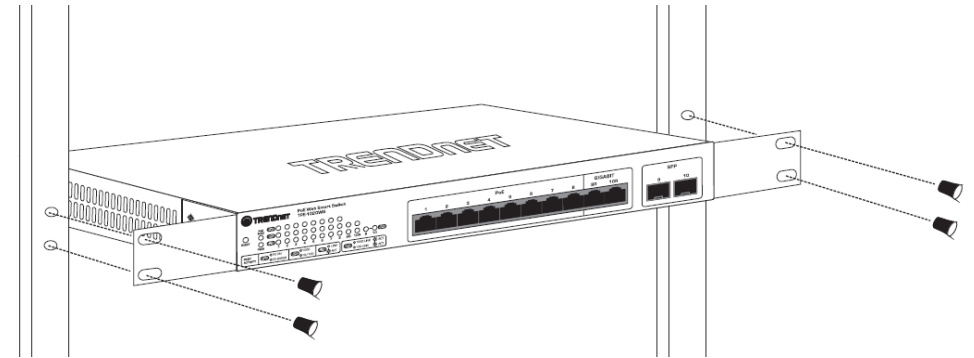


Rack Mount Hardware Installation

The router can be mounted in an EIA standard-size, 19-inch rack, which can be placed in a wiring closet with other equipment. Attach the mounting brackets at the router's front panel (one on each side), and secure them with the provided screws.



Then, use screws provided with the equipment rack to mount each router in the rack.

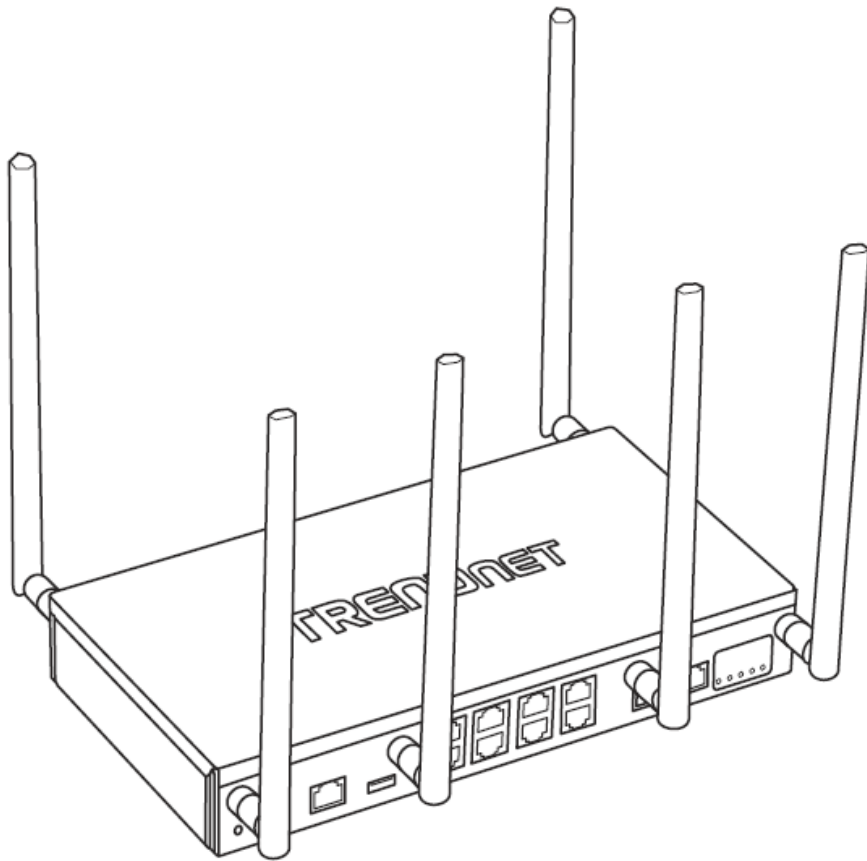


Note: The look of the router may be different than what is actually displayed.

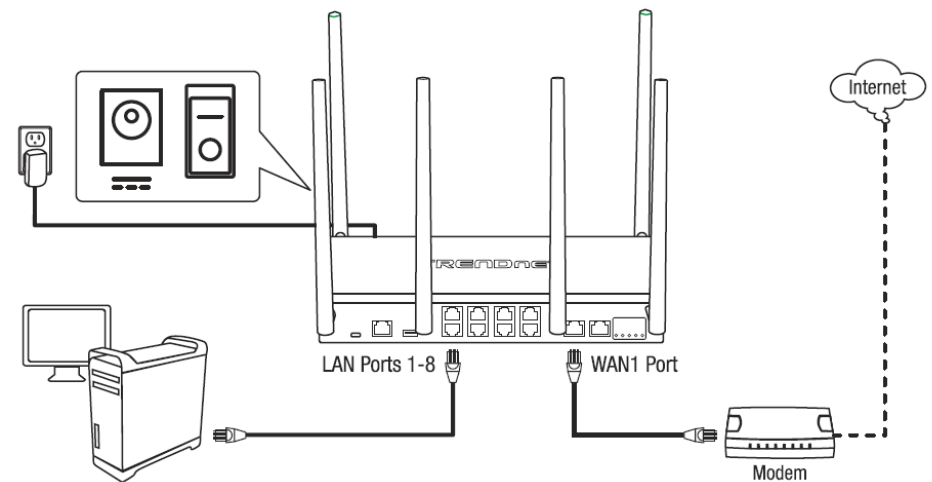
Basic Installation and Configuration

Note: It is recommended that you configured the wireless router from a wired computer.

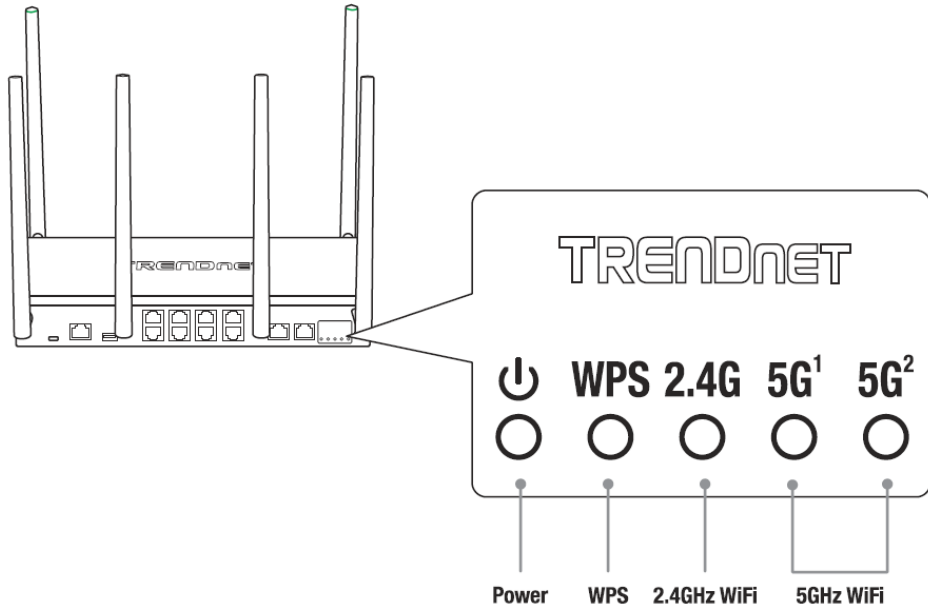
1. Attach the antennas to the front and back of the router and position them for the best WiFi coverage. It is recommended that you position all antennas vertically as shown for initial installation and adjust as needed later on.



2. Connect a network cable from the WAN1 port of your router to your modem.
3. Connect a network cable from one of the LAN ports (1-8) of your router to your computer.
4. Connect the includes power adapter from a power outlet to your router power port and push the Power On(-)/Off(o) switch into the On(-) position.



5. The Power (⏻), 2.4G, 5G¹, 5G² LEDs will turn on solid indicating that the router is ready.



6. Open your web browser on the connected computer and in the address bar, enter <http://tew-829dru> or <http://192.168.10.1> and press **Enter** to access the router web configuration page.



7. Enter the default **User Name** and **Password**, then click **LOGIN**. By default, the pre-configured user name and password are located on the included preset wireless settings sticker or device label located on the bottom of the router.

Authorization Required

Please enter your username and password.

Username

Password

Preset Wireless Settings

Wi-Fi Name/SSID
 (AC/N)
 TRENDnet829_5GHz1_XXXX
 TRENDnet829_5GHz2_XXXX
 (N/B/G)
 TRENDnet829_2.4GHz_XXXX

Wi-Fi Password
 XXXXXXXXXXXX

Management Login
<http://tew-829dru>
 username: admin
 password: XXXXXX

8. To change the administrator password for the router configuration, click **Administrator** and click **Administration**.

Note: By default, the administrator password has been pre-configured for your convenience and can be located on the included wireless settings sticker or on the device label located on the bottom of the router. If you are modifying the administrator password, you will need to log into the router configuration using the new password.

Administrator


System


Administration


9. Enter the new administrator password in the **Password** field and re-type the new password in the **Confirmation** field. Click **Apply** to save and commit the changes.


Router Password

Changes the administrator password for accessing the device


Password 

 Max length: 20 characters

Confirmation 

 Confirm password

Idle Timeout

 120~3600 seconds

APPLY

10. To change your router's LAN IPv4 address settings, click on **Network** and click **LAN**.

Network

LAN

11. Under Common Configuration and General Setup, enter the new LAN IPv4 address and subnet mas in the **IPv4 address** and **IPv4 netmask** fields. Click **Apply** to save and commit the changes. Please wait for the new address settings to be applied and log back into the router web configuration page using the new LAN IPv4 address.

Note: If your computer IP address settings are not automatically updated to the new settings, you may need to manually renew your computer IP address settings in order for you to log back into the router web configuration with the new LAN IPv4 address settings.

Common Configuration

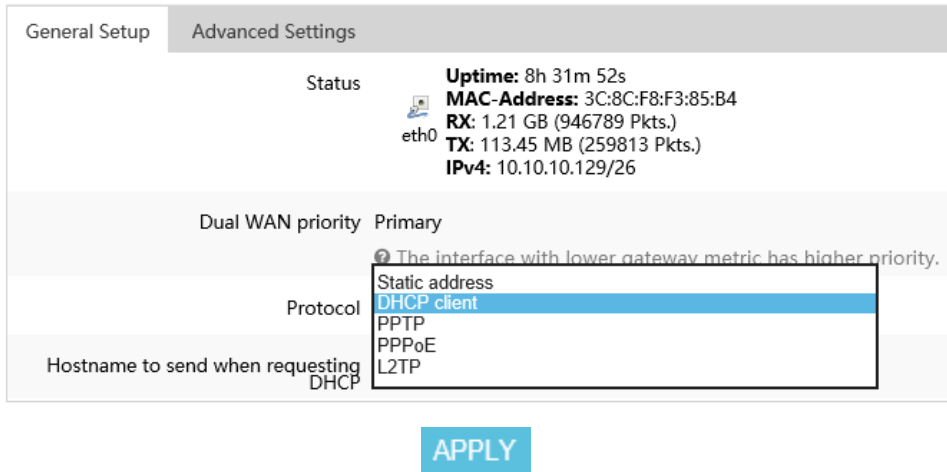
General Setup	Advanced Settings
Status	Uptime: 8h 25m 38s MAC-Address: 3C:8C:F8:F3:85:B6 br-lan RX: 112.68 MB (281165 Pkts.) TX: 1.22 GB (947340 Pkts.) IPv4: 192.168.50.1/24
Mode	NAT <input type="button" value="v"/>
IPv4 address	192.168.10.1
IPv4 netmask	255.255.255.0 <input type="button" value="v"/>

12. To configure your WAN1 Internet connection settings, click **Network** and click **WAN1**.



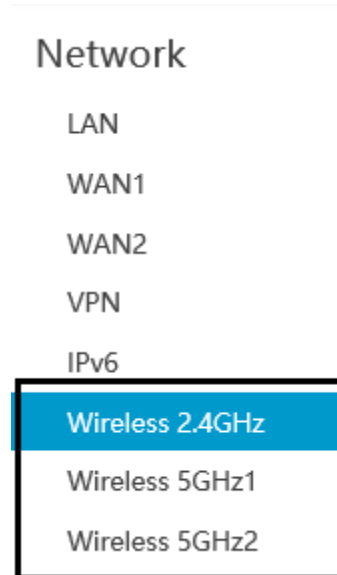
13. Under Common Configuration and General Setup, click the **Protocol** drop-down list and select the appropriate protocol (**Static address, DHCP client, PPTP, PPPoE, L2TP**) for your Internet connection. DHCP client is the typical protocol in which the connection settings are automatically obtained by your ISP (Internet Service Provider). If you are unsure about the Internet connection settings, please contact your ISP for details. After you have completed the Internet connection settings, click **Apply** to save and commit the changes.

Common Configuration



14. To configure your wireless network name/SSID and wireless encryption settings, click **Network** and click the wireless band you would like to configure. **Wireless 2.4GHz**, **Wireless 5GHz1**, or **Wireless 5GHz2**.

Note: By default, the wireless network name/SSID has been pre-configured for your convenience and can be located on the included wireless settings sticker or on the device label located on the bottom of the router. If you are modifying the wireless settings, you will need to connect to the router with your WiFi clients using the new settings.



15. To change the wireless network name/SSID for the selected wireless band, under Interface Configuration and General Setup, enter the new name in the **ESSID** field and click **Apply** to save and commit the changes.

Note: The wireless network name/SSID is the name your WiFi clients will need to search and discover when connecting to your router wireless network.


Interface Configuration

General Setup	Wireless Security	MAC-Filter	Advanced Settings
ESSID TRENDnet829_2.4GHz_YCE1			
Hide ESSID <input type="checkbox"/>			
APPLY			

16. To change the wireless encryption key for the selected wireless band, under Interface Configuration Wireless Security, enter the new encryption in the **Key** field and click **Apply** to save and commit the changes.

Note: WPA2-PSK AES wireless encryption is strongly recommended. The wireless encryption key is the key your WiFi clients will need to enter when connecting to your router wireless network.

Interface Configuration

General Setup	Wireless Security	MAC-Filter	Advanced Settings
Encryption		WPA2-PSK	▼
Cipher		Force CCMP (AES)	▼
Key		●●●●●●●●	
APPLY			

Basic Router Settings

Access your router management page

Note: Your router management page URL/domain name <http://tew-829dru> 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-829dru> 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 pre-configured with a unique administrator password. You can find the **Password** on the sticker included in the router package contents or on the device label located on the bottom of the router. Enter your **Username** and **Password**, then click **LOGIN**.

- User Name: **admin**
- Password: **(xxxxxxxx)**

Note: User Name and Password are case sensitive.

Authorization Required

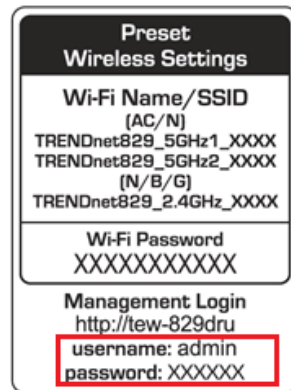
Please enter your username and password.

Username

Password

LOGIN

RESET



Saving and applying router configuration changes

In the router management page, pages may include all, some, or one of the options below. Some configuration changes may require a device reboot.



- **Reset** – Clicking this option will reset all settings to their previous configuration on a specific page.
- **Apply** – Clicking this option will save and apply the configuration changes on a specific page which will take effect immediately.
- **Save** – Clicking this option will temporarily save the changes and allow you to temporarily save multiple configuration changes and apply all configuration changes at the same time. When a configuration setting has been temporarily saved, a notification will appear in the top right corner of the router management page indicated that there are unsaved changes and the number of pending configuration changes. When you are ready to save and apply the configuration changes permanently, click on the notification in the top right corner.

UNSAVED CHANGES: 6

A list of all pending configuration changes will be displayed. If you are ready to permanently save all configuration changes, click **Apply**. Otherwise, to discard changes, click **Revert** to discard all pending configuration changes.

Legend:

■ Section added ■ Section removed ■ Option changed ■ Option removed

```
system.ntp
system.ntp.enabled=1
system.ntp.server+=us.pool.ntp.org
```

```
system.cfg02e48a
system.cfg02e48a.conloglevel=8
system.cfg02e48a.cronloglevel=8
system.cfg02e48a.timezone=PST8PDT,M3.2.0,M11.1.0
system.cfg02e48a.zonename=America/Los Angeles
```

APPLY

REVERT

Change your administrator password

Administrator > Administration






By default, the administrator password has been pre-configured a unique password for your convenience. You can find the pre-configured administrator password on the wireless sticker included in your router package contents or also located on the router device label located on the bottom of the device. This section will allow you to change the default administrator password used to log into your router management page.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Administrator** and click on **Administration**.
3. Enter the new administrator password in the **Password** and re-enter the new password in the **Confirmation** field. Click **Apply** to save and commit the changes

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

Router Password

Changes the administrator password for accessing the device

Password	<input type="password"/>	
	 Max length: 20 characters	
Confirmation	<input type="password"/>	
	 Confirm password	
Idle Timeout	<input type="text" value="3600"/>	
	 120~3600 seconds	

Note: If you change the administrator password, you will need to access the router management page using the User Name "admin" and the new password instead of the pre-configured default password. If you reset the device to factory defaults, you will need to access the router management page using the pre-configured settings on the included wireless sticker in the router package contents or on device label located on the bottom of the router.

Set your router date and time

Administrator > System

It is recommended to set the router date and time for scheduling functions and logging functions for monitoring and troubleshooting.


1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Administrator** and click on **System**.
3. Review the settings below. Click **Apply** to save and commit the changes.

System Properties

- **Local Time** – Displays the current day, date, and time. Clicking the **SYNC WITH BROWSER** button will automatically copy the current day, date, and time settings from the web browser and allows the time to be set manually.
- **Hostname** – Modifies the router host name. The host name identifies is the name used to identify the router to other computer or devices on the network. Modifying this setting will modify the hostname used when accessing the router management page using the hostname or when using the Samba USB share feature.
- **Timezone** – Click the drop-down list to select the appropriate time zone.

Time Synchronization

- **Enable NTP client** – Enables the NTP client to configure router to obtain time and date settings from an external network time server.
 - **NTP server candidates** – Enter the domain name of the network time server to obtain time and settings. (e.g. pool.ntp.org)

Note: You can add multiple time servers by clicking  . If one server is not available, your router will try the next available server in the list.

System Properties

General Settings	Logging
Local Time	Tue Jul 24 21:57:01 2018 SYNC WITH BROWSER
Hostname	ROUTER
Timezone	UTC ▼

Time Synchronization

Enable NTP client

NTP server candidates 

Create time schedules

Administrator > Schedule

Your router allows you to create schedules to specify a time period when a feature should be activated and deactivated. Before you use the scheduling feature on your router, ensure that your router system time and date settings are configured correctly.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Administrator** and click **Schedule**.
3. Review the settings below. Click **Add** to add the new schedule to the list and **Apply** to save and commit the changes.
 - **Name** – Enter a name for the new schedule rule.
 - **Days** – Choosing **Daily** will set the set the schedule rule to occur at the specified time every day. Choosing **Select Day(s)** will allow to manually select which specific days for the schedule.
 - **All Day – 24 Hrs** – Checking this option will set the schedule to run all 24 hours instead of manually configured a specified time period.
 - **Start Time / End Time** – Manually define a time period for the schedule.
Note: *The time period is specified in 24 hour format.*

Schedule Rules

Name	Days	Start Time	End Time	
Always	Every day	00:00	23:59	EDIT DELETE

Name

Days Daily Select Day(s)

Sunday Monday Tuesday Wednesday Thursday Friday Saturday

All Day - 24 Hrs

Start Time :

End Time : [ADD](#)

Change LAN IPv4 address settings

Network > LAN

Note: The default LAN interface IPv4 address settings is 192.168.10.1 / 255.255.255.0 and also assigned to LAN ports 1-8 by default. If the LAN IPv4 address settings are modified, you will need to log into the router management page with the new IPv4 address settings.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click **LAN**.
3. Under the Common Configuration section, you can enter the new LAN interface IP address settings.
 - **IPv4 address** – Enter the new LAN IPv4 address. (e.g. 192.168.50.1)
 - **IPv4 netmask** – Select or Enter the new LAN IPv4 subnet mask. The drop-down menu will list class A, B, C, or custom which will allow you to manually enter a custom subnet mask. (e.g. 255.255.255.0)

Common Configuration

General Setup	Advanced Settings
Status	Uptime: 0h 0m 32s MAC-Address: 3C:8C:F8:F3:85:B6 RX: 105.19 KB (985 Pkts.) TX: 460.19 KB (641 Pkts.) IPv4: 192.168.10.1/24
Mode	NAT <input type="button" value="v"/>
IPv4 address	192.168.10.1
IPv4 netmask	255.255.255.0 <input type="button" value="v"/>

4. Click **Apply** to

APPLY

Below is a reference of the additional LAN settings if you choose to make other configuration changes to these sections.

General Setup

- **Status – LAN Interface (br-lan)**
 - **Uptime** – Displays the amount time the LAN interface has been up and continuously running. This time will reset if the router is powered off or router is rebooted.
 - **MAC-Address** – Displays the current MAC address assigned to the LAN interface.
 - **Rx** – Displays the total amount of data received by the LAN interface in MB (# of packets) since the start of the currently displayed uptime.
 - **Tx** – Displays the total amount of data transmitted by the LAN interface in MB (# of packets) since the start of the currently displayed uptime.
 - **IPv4:** Displays the current IPv4 address settings assigned to the LAN interface.
- **Mode – Allows you to change the function between NAT mode or Route Only (NAT-less).**
 - **NAT** – The default router mode which uses network address translation between the local internal (LAN/VLAN) interfaces and external (WAN1/WAN2) interfaces translating public and private IP addressing.
 - **Route Only (NAT-less)** – This mode disables the NAT function between internal and external interfaces and may also be known as classical routing mode. This mode should only be used when the router is using for local internal IP routing only

Advanced Settings

- **Override MAC Address** – This parameter allows you to assign a new LAN interface (br-lan) MAC address. Typically, this parameter does not need to be modified. (e.g. AA:BB:CC:DD:EE:FF)
- **Override MTU** – The default MTU (maximum transfer unit) or frame size is set to 1500 bytes. This parameter allows you to assign a new MTU size. Typically, this parameter does not need to be modified.
- **Use gateway metric** – This is automated metric or priority value assigned to the LAN network interface route in the routing table. Typically, this parameter does

not need to be modified. (Lower value = Higher priority in route table, 0 being the highest priority.)

Configure LAN IPv4 DHCP server settings

Network > LAN

Note: The internal DHCP server function is enabled by default on the LAN interface to automatically distribute IP address settings to network devices connected to the LAN and wireless LAN interfaces. The internal DHCP server only supports only class C IP address range. The default IP range is 101 – 199 (192.168.10.101 – 192.168.10.199)

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click **LAN**.
3. Under the DHCP Server/Relay section, you can modify or enter the new DHCP settings and click **Apply** to save and commit the changes.
 - **DHCP mode** – Allows you to set the mode to Enable, Disable, or Relay.
 - **Enable** – Using this setting enables the DHCP server function the LAN interface.
 - **Disable** - Using this setting disabled the DHCP server function on the LAN interface.
 - **Relay** – Using this setting allows you to use an external DHCP server instead of your router's internal DHCP server to distribute IP address settings on the LAN interface. If choosing this setting, enter the IP address of your external DHCP relay server.
 - **Start** – Enter the starting value of DHCP IPv4 address range. (e.g. If your LAN IPv4 address is 192.168.50.1, entering 120 will define the first IP address of the DHCP pool is 192.168.50.120)
 - **End** – Enter the ending value of DHCP IPv4 address range. (e.g. If your LAN IPv4 address is 192.168.50.1, entering 200 will define the last IP address of the DHCP pool is 192.168.50.200)

- **Lease Time** – Enter the lease time in hours (h) or minutes (m) DHCP clients will hold their IP address settings before automatically requesting a new lease (IP address settings) from the internal DHCP server. (e.g. To specify 24 hours, enter 24h. To specify 480 minutes, enter 480m.)
- **WINS server** – Enter the IPv4 address of your WINS (Windows Internet Name Server) for internal host name resolution on your local network to be distributed to DHCP clients. The WINS server provides host name to IP address resolution for the NetBIOS naming service. This parameter is optional. (e.g. 192.168.50.250)
- **Primary DNS** – Enter the IPv4 address of your primary DNS (Domain Name System) server for Internet domain name resolution to be distributed to DHCP clients. By default, the internal DHCP server uses DNS relay and provides the router LAN IPv4 address as the primary DNS server to DHCP clients. The DNS server provides Internet domain name to IP address resolution when computers are accessing or browsing Internet websites. This parameter is optional. (e.g. If entering 8.8.8.8, this DNS server will be provided DHCP clients instead of the router's LAN IPv4 address to resolve Internet domain names such as trendnet.com)
- **Secondary DNS** – Enter the IPv4 address of your secondary DNS (Domain Name System) server for Internet domain name resolution to be distributed to DHCP clients. If the primary DNS server cannot be reached, the secondary DNS server will be used. This parameter is optional. (e.g. 8.8.4.4)
- **Local domain name** – Enter a domain name to distribute to DHCP clients. This parameter is optional. (e.g. trendnet.com)

Below is a reference of the additional DHCP Server/Relay settings if you choose to make other configuration changes to these sections.

DHCP Server/Relay

General Setup	Advanced Settings
	DHCP mode <input type="text" value="Enable"/> <small>🔗 DHCP disable/enable/relay.</small>
	Start <input type="text" value="101"/> <small>🔗 Lowest leased address as offset from the network address.</small>
	End <input type="text" value="199"/> <small>🔗 Highest leased address as offset from the network address.</small>
	Leasetime <input type="text" value="24h"/> <small>🔗 Expiry time of leased addresses, range 2m ~ 999999h (m = minut</small>
	WINS server <input type="text"/> <small>🔗 WINS(Windows Internet Name Service) server.</small>
	Primary DNS server <input type="text"/> <small>🔗 Primary DNS(Domain Name System) server.</small>
	Secondary DNS server <input type="text"/> <small>🔗 Secondary DNS(Domain Name System) server.</small>
	Local domain name <input type="text"/> <small>🔗 Local domain name.</small>

Advanced Settings

- **Dynamic DHCP** – Checking this option enables the DHCP server to distribute IPv4 address settings dynamically to clients. If this option is unchecked, IPv4 address settings will only be assigned to DHCP clients with a static DHCP reservation. Typically, this parameter does not need to be modified.
- **Log Queries** – Checking this option will enable generate logging to internal or syslog of any DNS queries. Typically, this parameter does not need to be modified.

Add static DHCP reservations

Network > LAN

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click **LAN**.
3. Under the Static Leases section, click **Add**.

Static Leases

Hostname	MAC-Address	IPv4-Address
This section contains no values yet		
<input type="button" value="ADD"/>		

4. Enter the parameters for the static DHCP reservation and click **Apply** to save and commit the changes.

Note: The network device or computer the reservation is created will need to release and renew the IPv4 address settings in order to obtain the new IP address settings.

- **Hostname** – Enter a name for the DHCP reservation. (e.g. *trendnetpc*)
- **MAC-Address** – Enter the MAC (Media Access Control) address of the computer or network device to assign to the reservation. You can also click the drop-down list to select from a list of network devices detected by the router that have been assigned IPv4 address settings through DHCP. (e.g. *AA:BB:CC:DD:EE:FF*)
- **IPv4-Address** – Enter the IPv4 address to assign to the computer or network device for the reservation. You can also click the drop-down list to select from list o of network devices detected by the router through DHCP. (e.g. *192.168.50.150*)

Static Leases

Hostname	MAC-Address	IPv4-Address
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="ADD"/>		

Add static host name entries

Network > LAN

The router can be used for host name to IP address resolution of computers or network devices on your local network similar to a WINS server however, entries will not dynamically populate and each entry must be manually entered. For clients to resolve the manually entered static entries, DHCP clients must use the router LAN IPv4 address as the WINS server.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click **LAN**.
3. Under the Host Entries section, click **Add**.
4. Enter the parameters for the static host name entry and click **Apply** to save and commit the changes.
 - **Hostname** – Enter the host name. (e.g. *trendnetpc*)
 - **IPv4-Address** – Enter the IPv4 address to resolve to host name. (e.g. *192.168.50.150*)

Host Entries

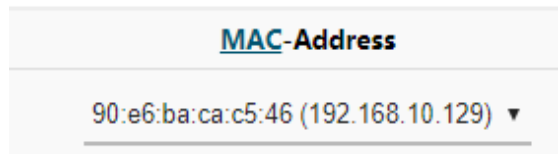
Hostname	IP Address
<input type="text"/>	<input type="text"/>
<input type="button" value="ADD"/>	

Add static ARP entries

Network > LAN


ARP (Address Resolution Protocol) is the protocol responsible for resolve IP addresses to hardware MAC addresses. Typically, ARP entries are dynamically learned and refreshed in the ARP table however, in the case where your application requires static ARP entries to always be present in the router ARP table, you can manually enter and add them to the router. (ex. applications: WoL (Wake on LAN) or Wake on WAN)

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click **LAN**.
3. Under the Static ARP section, click the **MAC-Address** drop-down list to select a MAC address from the list or select custom to manually enter a MAC address (format example: aa:bb:cc:dd:ee:ff).



A screenshot of a web interface showing a dropdown menu titled "MAC-Address". The selected option is "90:e6:ba:ca:c5:46 (192.168.10.129)" with a downward arrow on the right.

4. Click the **IPv4-Address** drop-down list and select the IPv4 address to assign to the MAC address ARP table entry or select custom to manually enter an IPv4 address (format example: 192.168.10.129)



A screenshot of a web interface showing a dropdown menu titled "IPv4-Address". The selected option is "192.168.10.129" with a downward arrow on the right.

5. Click **Apply** to save and commit the changes.



A blue rectangular button with the word "APPLY" in white capital letters.

Note: You can specify additional static ARP entries by clicking **Add**. Delete existing entries by clicking the **Delete** button next to the entry to be removed.



Configure WAN1 / WAN2 interfaces for Internet connectivity

Network > WAN1/WAN2

By default, the WAN configuration is set to use WAN1 as the primary connection for Internet connectivity and failover to WAN2 secondary if there is fault in connectivity to WAN1. This section will explain how to set up the WAN1 or WAN2 interfaces for Internet connectivity to your ISP (Internet Service Provider).

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click **WAN1** or **WAN2**.
3. Under the Common Configuration section, click the **Protocol** drop-down list and select the Internet connection provided by your ISP.

Common Configuration

The screenshot shows the 'Common Configuration' section of the WAN1/WAN2 interface settings. The 'Protocol' dropdown menu is expanded, showing the following options: Static address, DHCP client (highlighted), PPTP, PPPoE, and L2TP. Other visible settings include:

- Status:** Uptime: 0h 22m 14s, MAC-Address: 3C:8C:F8:F3:85:B4, RX: 592.08 KB (1975 Pkts.), TX: 285.74 KB (1414 Pkts.), IPv4: 10.10.10.83/26
- Dual WAN priority:** Primary (with a note: "The interface with lower gateway metric has higher priority.")
- Hostname to send when requesting DHCP:** (field is empty)

4. Complete all of the fields required by your ISP and click **Apply** to save and commit the changes.

Below is a reference of the additional WAN settings if you choose to make other configuration changes to these sections.

General Setup

- **Status – LAN Interface (br-lan)**
 - **Uptime** – Displays the amount time the WAN1/WAN2 interface has been up and continuously running. This time will reset if the router is powered off or router is rebooted.
 - **MAC-Address** – Displays the current MAC address assigned to the WAN1/WAN2 interface.
 - **Rx** – Displays the total amount of data received by the WAN1/WAN2 interface in MB (# of packets) since the start of the currently displayed uptime.
 - **Tx** – Displays the total amount of data transmitted by the WAN1/WAN2 interface in MB (# of packets) since the start of the currently displayed uptime.
 - **IPv4:** Displays the current IPv4 address settings assigned to the WAN1/WAN2 interface.
- **Dual WAN priority** – Displays the current priority assignment for the selected WAN interface. The WAN priority settings can be configured under Network > Multiple WAN. By default, the WAN configuration is set to use WAN1 as the primary connection for Internet connectivity and failover to WAN2 secondary if there is fault in connectivity to WAN1.
- **Hostname to send when requesting DHCP** – If your ISP requires to send specific hostname with the DHCP request for Internet connectivity, enter the required host name in the field. Applies to DHCP client/PPTP/L2TP WAN protocols.
- **WAN mode** – Applies to PPTP/L2TP WAN protocols.
 - **DHCP client** – Using this option will set the WAN to obtain IP address settings automatically from your ISP for Internet connectivity.
 - **Static IP** – Using this option will require you to manually enter the WAN IP settings required by your ISP for Internet connectivity.
- **Connect mode** – Applies to PPPoE/PPTP/L2TP WAN protocols.
 - **Keep alive** – This option will keep the connection on at all times.
 - **On demand** – This option will automatically disconnect after the max. idle time is reached and will automatically re-establish connection when Internet access is used.

- **Access concentrator / Service name** – Optional parameters required only if ISP requires for Internet connectivity. Applies to PPPoE WAN protocol.
- **MPPE support**– Optional parameter (applies Microsoft Point-to-Point Encryption) required only if ISP requires for Internet connectivity. Applies to PPTP WAN protocol.
- **Use DNS servers advertised by peer**- If checked, automatically obtains DNS service IP address settings from your ISP. If unchecked, allows you to specify custom DNS server IP addresses. Applies to PPPoE/PPTP/L2TP WAN protocols.

Advanced Settings

- **Bring up on boot** – The parameter is enabled to bring the WAN1/WAN2 interface up during device boot. Typically, this parameter does not need to be modified.
- **Use builtin IPv6-management** – Enables/disables IPv6 protocol on the WAN1/WAN2 interface. Typically, this parameter does not need to be modified.
- **Enable IPv6 negotiation on PPP link** – Enables/disables IPv6 when using the PPPoE/L2TP WAN protocols. Typically, this parameter does not need to be modified.
- **Use broadcast flag** – Optional parameter if your ISP may requires that DHCP requests from your device be sent as broadcasts or unicasts for IP address settings for Internet access.
- **Use default gateway** – This parameter automatically created a default gateway route in the device routing table to access the Internet through the selected WAN interface. If unchecked, the default gateway route for Internet access must be entered in manually in the device routing table settings. Typically, this parameter does not need to be modified.
- **Use gateway metric** – This parameter is the route priority value assigned to the default gateway route. Range: 0-9999, 0 being the highest priority. Typically, this parameter does not need to be modified.
- **Use DNS servers advertised by peer**- If checked, automatically obtains DNS service IP address settings from your ISP. If unchecked, allows you to specify custom DNS server IP addresses. Applies to the DHCP client WAN protocol.
- **Client ID to send when requesting DHCP** – Optional parameter only required if your ISP requires a specific client ID to be sent when requesting IP address settings for Internet access. Applies to DHCP client WAN protocol.

- **Vendor Class to send when requesting DHCP** – Optional parameter only required if your ISP requires a specific vendor class to be sent when requesting IP address settings for Internet access. Applies to DHCP client WAN protocol.
- **Override MAC address** – Optional parameter used to change the WAN interface MAC address if you are experiencing issues obtaining IP address settings from your ISP. This parameter is more commonly known as MAC address cloning where you can assign a LAN computer MAC address to the WAN interface. Applied to DHCP client WAN protocol.
- **Override MTU** – The default MTU (maximum transfer unit) or frame size is set to 1500 bytes. This parameter allows you to assign a new MTU size. For PPPoE/PPTP/L2TP WAN protocols, if you experience issues accessing SSL/HTTPS secure websites, you can try lower the MTU value to 1492 to decrease the amount of packet errors. Typically, this parameter does not need to be modified.

WAN VLAN Tagging

Some ISPs require VLAN tag assignment of a specific VLAN ID when for Internet access or other services. You can follow the steps below to assign a specific VLAN ID to the WAN interface.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click **VLAN**.
3. Under the **VID**, you can enter the **VID** required by your ISP and set the WAN interface to tagged or untagged. Click **Apply** to save and commit the changes.

2	WAN1 Untagged ▼
3	WAN2 Untagged ▼

IPv6 settings

Network > IPv6

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

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

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

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click on **IPv6**.

3. Review the IPv6 Internet Connection settings and enter information settings specified by your ISP. Complete all of the fields required by your ISP and click **Apply** to save and commit the changes.

Note: Please contact your ISP for IPv6 service availability.

Select the IPv6 WAN connection type provided by your ISP.

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

Virtual LANs (VLANs)

Network > VLAN

Your router supports port-based 802.1Q VLANs as well inter-VLAN routing. VLANs can be assigned different IP address interfaces in which the router can route between VLAN IP subnets.

Create a port-based VLAN

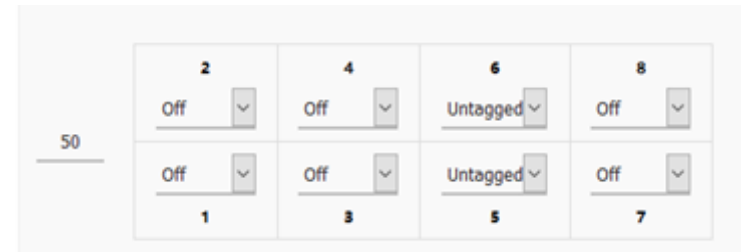
1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click **VLAN**.
3. Before assigning which untagged and tagged VLAN member ports are assigned to a new VLAN, the ports must be set to Off in the default VLAN VID: 1 (LAN). Also, click the Inter VLAN Routing drop-down list and select **Enabled** to enable communication between the LAN and other VLAN interfaces. Click **Apply** to save and commit the changes. *Example: We will remove ports 5-8 from the default VLAN VID: 1 (LAN) interface so these ports can be re-assigned as untagged member ports of new VLANs in example below.*

VID	Ports				Network
1	<div style="text-align: center;">2</div> Untagged <input type="button" value="v"/> Untagged <input type="button" value="v"/> 1	<div style="text-align: center;">4</div> Untagged <input type="button" value="v"/> Untagged <input type="button" value="v"/> 3	<div style="text-align: center;">6</div> Off <input type="button" value="v"/> Off <input type="button" value="v"/> 5	<div style="text-align: center;">8</div> Off <input type="button" value="v"/> Off <input type="button" value="v"/> 7	Inter VLAN Routing Enabled <input type="button" value="v"/> IP Address 192.168.10.1 Subnet Mask 255.255.255.0

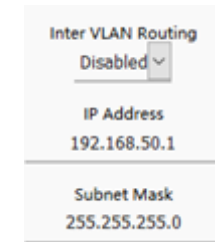
4. To create a new 802.1Q VLAN, under the VLANs section, click **Add**.



5. Under **VID**, enter the VLAN ID to assign to the new VLAN (4-4094, VLAN IDs 1-3 are reserved for use with the default LAN, WAN1, WAN2 interfaces) and set the untagged VLAN member ports. *Example: In the example below, we will create a new VLAN with VLAN ID: 50 and assign ports 5 & 6 as untagged member ports.*



6. Enter the VLAN IP interface configuration under **IP Address** and **Subnet Mask**. *Example: In the example below, we will enter the VLAN 50 interface IP address as 192.168.50.1 and subnet mask 255.255.255.0.*



7. Under DHCP Server, click the **Mode** drop-down list and select **Enabled** to enable the DHCP server on the VLAN. Click **Apply** to save and commit the changes.

Example: In the example below, we will enable the DHCP server on VLAN 50 and leave IP address range and lease defaults. This will assign a DHCP IP range of 101-199 to ensure any devices connected to this VLAN obtain IP address information via DHCP.

Mode: **Enabled** ▾

Start
101

End
199

Leasetime
12h

If following the port-based VLAN configuration example, any computers or devices connecting to ports 5 & 6 will obtain 192.168.50.x/255.255.255.0 address settings and use the VLAN 50 IP interface 192.168.50.1 as the Internet gateway and gateway to other local IP subnets.



VLAN 50
IP: 192.168.50.1
Mask: 255.255.255.0

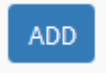
Create a port-based VLAN with 802.1Q tagging

Your router supports 802.1Q VLAN tagging/trunking to other 802.1Q VLAN devices such as managed switches.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click **VLAN**.
3. Under VLAN VID:1 (LAN), click the Inter VLAN Routing drop-down list and select **Enabled** and click **Apply** to commit and save the changes.

VID	Ports				Network
1	2 Untagged ▾	4 Untagged ▾	6 Untagged ▾	8 Untagged ▾	Inter VLAN Routing Enabled ▾ IP Address 192.168.10.1 Subnet Mask 255.255.255.0
	1 Untagged ▾	3 Untagged ▾	5 Untagged ▾	7 Untagged ▾	

4. To create a new 802.1Q VLAN, under the VLANs section, click **Add**.



5. Under **VID**, enter the VLAN ID to assign to the new VLAN (4-4094, VLAN IDs 1-3 are reserved for use with the default LAN, WAN1, WAN2 interfaces) and set the tagged VLAN member port. *Example: In the example below, we will create a new VLAN with VLAN ID: 50 and assign port 8 as a tagged VLAN member port.*

The screenshot shows a configuration table for VLAN 50. The table has two rows and four columns. The columns are labeled 2, 4, 6, and 8 at the top. The rows are labeled 1, 3, 5, and 7 at the bottom. In the top row, port 2 is 'Off', port 4 is 'Off', port 6 is 'Off', and port 8 is 'Tagged'. In the bottom row, all ports (1, 3, 5, 7) are 'Off'.

50	2 Off	4 Off	6 Off	8 Tagged
	1 Off	3 Off	5 Off	7 Off

6. Enter the VLAN IP interface configuration under **IP Address** and **Subnet Mask**.
Example: In the example below, we will enter the VLAN 50 interface IP address as 192.168.50.1 and subnet mask 255.255.255.0.

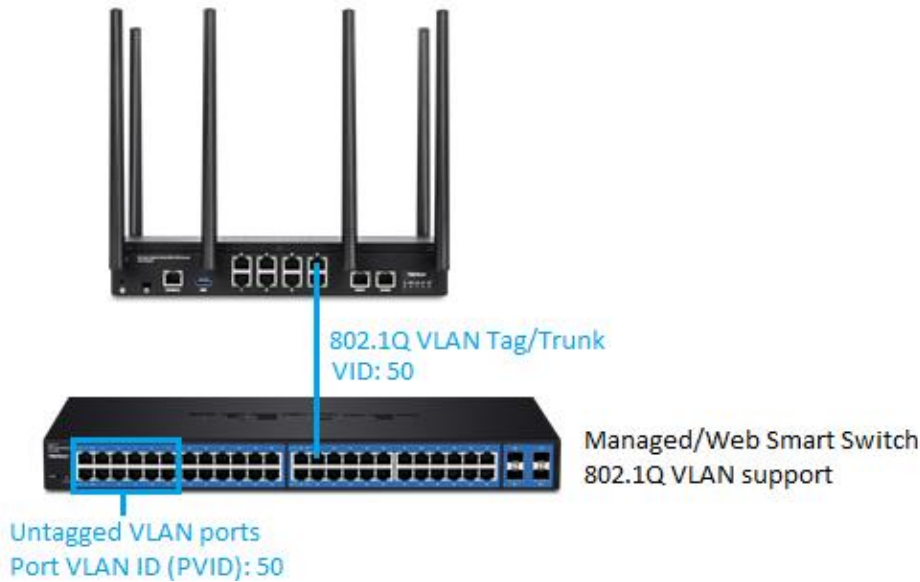
The screenshot shows the 'Inter VLAN Routing' configuration. The 'Inter VLAN Routing' dropdown is set to 'Disabled'. Below it, the 'IP Address' is set to 192.168.50.1 and the 'Subnet Mask' is set to 255.255.255.0.

7. Under DHCP Server, click the **Mode** drop-down list and select **Enabled** to enable the DHCP server on the VLAN. Click **Apply** to save and commit the changes.

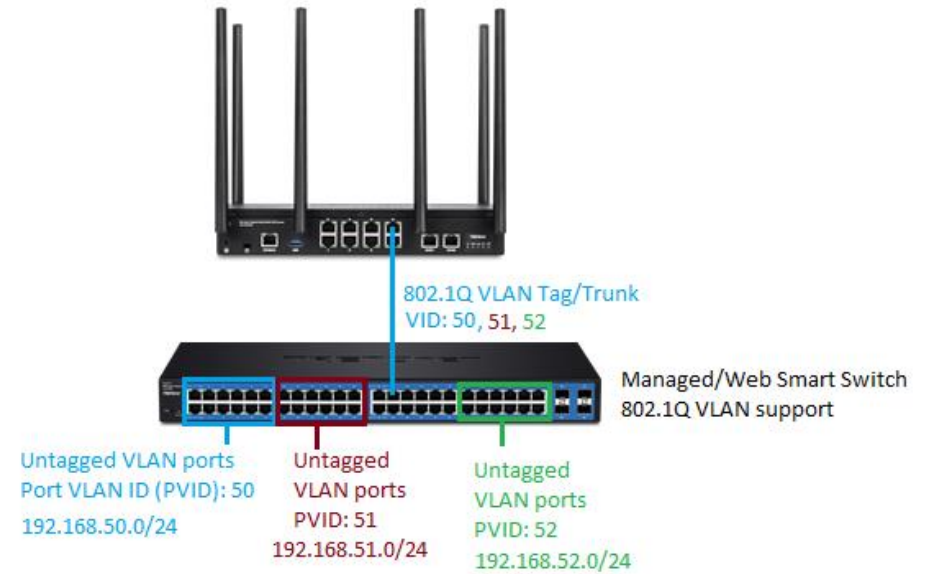
Example: In the example below, we will enable the DHCP server on VLAN 50 and leave IP address range and lease defaults. This will assign a DHCP IP range of 101-199 to ensure any devices connected to this VLAN obtain IP address information via DHCP.

The screenshot shows the DHCP Server configuration. The 'Mode' dropdown is set to 'Enabled'. The 'Start' IP address is 101 and the 'End' IP address is 199. The 'Leasetime' is set to 12h.

If following the 802.1Q VLAN configuration example, a managed/web smart switch with 802.1Q VLAN support can be connected and pass VLAN 50 traffic between the router and switch. Any computers or devices connecting to the untagged VLAN ports (PVID: 50) on the managed/web smart will obtain 192.168.50.x/255.255.255.0 address settings and use the VLAN 50 IP interface 192.168.50.1 as the Internet gateway and gateway to other local IP subnets. Additional VLANs can be created on the router and switch in which 802.1Q VLAN traffic can pass through the same single 802.1Q VLAN tag/trunk link.



Example below of multiple VLANs configured and passing traffic through the same 802.1Q VLAN tag/trunk link.



Assigning VLAN IDs to Wireless SSIDs

Your router supports assigning specific VLAN IDs to wireless SSIDs to extend VLAN traffic manageability and control to your router wireless network. By default, primary and multiple SSIDs are assigned to the LAN (VLAN 1) IP network.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click **VLAN**.
3. Under VLAN VID:1 (LAN), click the Inter VLAN Routing drop-down list and select **Enabled** and click **Apply** to commit and save the changes.

VID	Ports	Network																
1	<table border="1"> <tr> <td>2</td> <td>4</td> <td>6</td> <td>8</td> </tr> <tr> <td>Untagged</td> <td>Untagged</td> <td>Untagged</td> <td>Untagged</td> </tr> <tr> <td>1</td> <td>3</td> <td>5</td> <td>7</td> </tr> <tr> <td>Untagged</td> <td>Untagged</td> <td>Untagged</td> <td>Untagged</td> </tr> </table>	2	4	6	8	Untagged	Untagged	Untagged	Untagged	1	3	5	7	Untagged	Untagged	Untagged	Untagged	<div style="border: 2px solid red; padding: 2px;">Inter VLAN Routing Enabled</div> <p>IP Address 192.168.10.1</p> <p>Subnet Mask 255.255.255.0</p>
2	4	6	8															
Untagged	Untagged	Untagged	Untagged															
1	3	5	7															
Untagged	Untagged	Untagged	Untagged															

4. To create a new 802.1Q VLAN, under the VLANs section, click **Add**.



5. Under **VID**, enter the VLAN ID to assign to the new VLAN (4-4094, VLAN IDs 1-3 are reserved for use with the default LAN, WAN1, WAN2 interfaces) and set the tagged VLAN member port. *Example: In the example below, we will create a new VLAN with VLAN ID: 50 and assign port 8 as a tagged VLAN member port.*

50	2	4	6	8
	Off	Off	Off	Tagged
	Off	Off	Off	Off
	1	3	5	7

6. Enter the VLAN IP interface configuration under **IP Address** and **Subnet Mask**. *Example: In the example below, we will enter the VLAN 50 interface IP address as 192.168.50.1 and subnet mask 255.255.255.0.*

Inter VLAN Routing
Disabled

IP Address
192.168.50.1

Subnet Mask
255.255.255.0

7. Under DHCP Server, click the **Mode** drop-down list and select **Enabled** to enable the DHCP server on the VLAN. Click **Apply** to save and commit the changes.

Example: In the example below, we will enable the DHCP server on VLAN 50 and leave IP address range and lease defaults. This will assign a DHCP IP range of 101-199 to ensure any devices connected to this VLAN obtain IP address information via DHCP.

Mode: **Enabled** ▾

Start
101

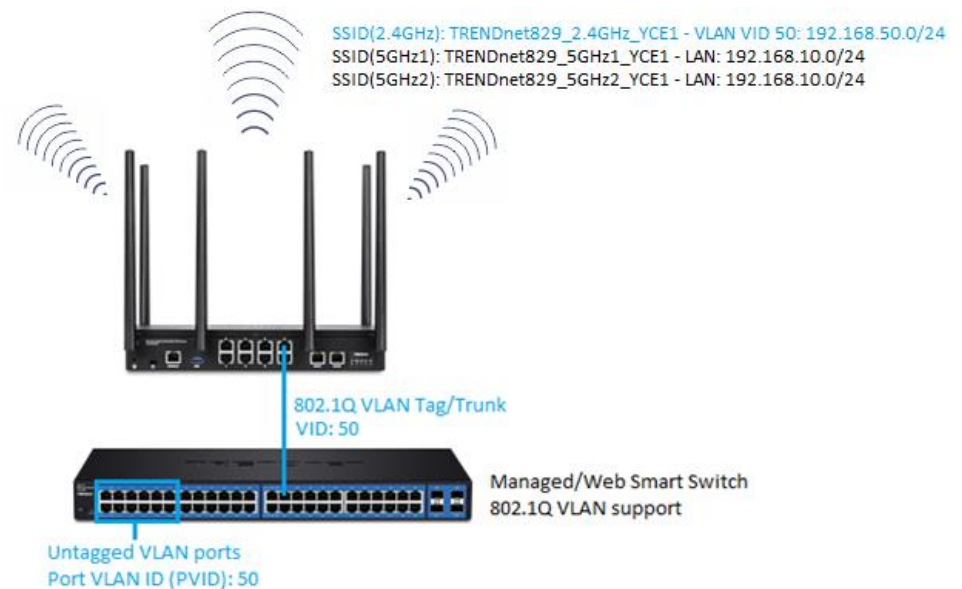
End
199

Leasetime
12h

8. Under Reassign SSID to VLAN, next to the SSID you would like to assign the new VLAN ID, click the **Network/VID** drop-down list and select the VLAN ID. Click **Apply** to save and commit the changes.

SSID	Network/VID
TRENDnet829_2.4GHz_YCE1	50 ▾
TRENDnet829_5GHz2_YCE1	LAN ▾
TRENDnet829_5GHz1_YCE1	LAN ▾

If following the 802.1Q VLAN configuration example, a managed/web smart switch with 802.1Q VLAN support can be connected and pass VLAN 50 traffic between the router and switch and 2.4GHz wireless SSID. Any computers or devices connecting to the untagged VLAN ports (PVID: 50) on the managed/web smart will obtain 192.168.50.x/255.255.255.0 address settings and use the VLAN 50 IP interface 192.168.50.1 as the Internet gateway and gateway to other local IP subnets. Any wireless computers or devices connecting to the 2.4GHz wireless SSID will also obtain 192.168.50.x/255.255.255.0 address settings while connecting to 5GHz1 or 5GHz2 SSIDs will remain on the LAN network. Additional VLANs can be created on the router and switch in which 802.1Q VLAN traffic can pass through the same single 802.1Q VLAN tag/trunk link. Multiple SSIDs will appear in this section when enabled and configured. Guest network SSID does not apply.



Below is a reference of the additional VLAN settings if you choose to make other configuration changes to these sections.

- **VID** – The VLAN ID assigned to a specific VLAN.
- **Ports 1-8** – Configure port VLAN membership settings.
 - **Untagged** – Default setting. Sets port membership as untagged and allows connectivity to network devices such as computers. The router will use the internal port VLAN ID (PVID) to forward VLAN traffic accordingly to these ports based on their untagged VLAN membership.
 - **Tagged** – Sets port membership as tagged and used for VLAN tag or trunk links to other VLAN aware devices such as managed switches or access points.
 - **Off** – Removes port membership from a specific VLAN.
- **Inter VLAN Routing** – Allows communication between local network interfaces/IP subnets such as the LAN and VLAN interfaces.
- **IP Address/Subnet Mask** – The IP address and subnet mask assigned to a specific VLAN interface.
- **Mode** – Configures the DHCP server settings for a specific VLAN interface.
 - **Disabled** – Disables DHCP on a specific VLAN interface.
 - **Enabled** – Enables the internal DHCP server on a specific VLAN interface. Allows you to set the IP address range/pool, lease time, WINS/DNS servers, and local domain name for the DHCP server.
 - **Relay** – Enables DHCP relay on a specific VLAN interface and forwards DHCP requests on the VLAN interface to an external DHCP server IP address (e.g. 192.168.50.20).

Application layer gateway (ALG)

Network > 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 8).
2. Click on **Network** and click on **ALG**.
3. Review the applications. Click **Apply** to save and commit the changes.

File Transfer Protocol (FTP)

Trivial File Transfer Protocol (TFTP)

Simple Network Management Protocol (SNMP)

Session Initiation Protocol (SIP)

Real Time Streaming Protocol (RTSP)

Internet Relay Chat (IRC)

H.323 Protocol

PPTP Passthrough

L2TP Passthrough

IPSec Passthrough

UPnP and NAT-PMP

Services > UPnP

UPnP (Universal Plug and Play) and NAT-PMP (NAT Port Mapping Protocol) 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 and NAT-PMP is disabled on your router by default and should only be enabled 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 8).
2. Click on **Services** and click on **UPnP / NAT-PMP**.
3. Under the **UPnP / NAT-PMP** section, check the **Enable UPnP / NAT-PMP functionality** option. Click **Apply** to save and commit the changes.

UPnP / NAT-PMP settings

Enable UPnP / NAT-PMP functionality

Note: When UPnP/NAT-PMP is enabled, you can check the currently open connections in the UPnP/NAT-PMP entries table..

UPnP / NAT-PMP entries

Protocol	External Port	Client Address	Client Port
There are no active redirects.			

Static routes

Network > 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 this 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 IP networks. In order to communicate between the two separate networks, static routing needs to be configured.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click on **Routing**.
3. Review the Routing section. Click **Add** to add the new static route. Click **Apply** to save and commit the changes.
 - **Interface** – Select the interface to assign the route.
 - **Target Host-IP or Network:** Enter the IP network address of the destination network for the route. (e.g. 192.168.20.0)
 - **IP4-Netmask:** Enter the subnet mask of the destination network for the route.(e.g. 255.255.255.0)
 - **IPv4-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 0-9999, the lowest number 0 being the highest priority.

Interface	Target Host-IP or Network	IPv4-Netmask	IPv4-Gateway	Metric	MTU
LAN	192.168.20.0	255.25.255.0	192.168.10.2	0	1500

You can check the current routing table under **Status > Routes** under **Active IPv6-Routes**.

Dynamic routing protocols

Network > 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.

Routing Information Protocol (RIP)

Network > Routing > RIP

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click on **Routing**, and click on the **RIP** tab.
3. Review the RIP Routing section. To save changes to this section, click **Apply** to command save your changes.

- **RIP enable:** Check the option to enable the RIP dynamic routing protocol globally on the router.

In the **Overview** table, you can enable and configure RIP for each interface by clicking **Edit** next to the interface.

Key mode	
md5	EDIT
md5	EDIT
md5	EDIT

RIP details for LAN

RIP enable	<input checked="" type="checkbox"/>
Send version	Version 2 ▾
Receive version	Version 2 ▾
Key authentication	<input type="checkbox"/>
Key string	123
Plain text password	<input type="checkbox"/>

- **RIP enable:** Check the option to enable RIP on the specified interface.
- **RIP version:** Click the drop-down list and select the appropriate RIP 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.
- **Redistribute:** Select the method used to redistribute dynamic routing information. The **Kernel** option should be left on as this option advertises/announces that the router can provide network routing information using RIP. The **OSPF** option allows the router to learn new routing information using the RIPv1/2 protocols and redistribute the routing information using OSPF protocol.
- **Send version** – Select the RIP protocol version to send.
- **Receive version** – Select the RIP protocol version to receive.
- **Authentication** – Enables MD5 authentication on all RIP messages sent and received.
- **Key string** – If authentication is enabled, enter the authentication key string/password to use for RIP messages sent and received.
- **Plain text password** – This option will set the password to be send in clear text instead of using the MD5 hash. This setting is not recommended.

You can check the current routing table under **Status > Routes** under **Active IPv6-Routes**.

OSPF (Open Shortest Path First)

Network > Routing > OSPF

1. Log into your router management page (see "[Access your router management page](#)" on page 8).

2. Click on **Network**, click on **Routing**, and click on the **OSPF** tab.

3. Review the OSPF Routing section. To save changes to this section, click **Apply** to commit and save your changes.

In the **Overview** table, you can enable and configure RIP for each interface by clicking **Edit** next to the interface.

- **OSPF enable:** Check the option to enable OSPF dynamic routing globally on the router.
- **Router ID:** Enter the OSPF router ID.

Area	
0	EDIT
0	EDIT
0	EDIT

OSPF details for LAN

OSPF enable	<input checked="" type="checkbox"/>
Network type	Broadcast ▼
Key authentication	<input type="checkbox"/>
Key string	123
Plain text password	<input type="checkbox"/>
Cost	15
	<small>🔍 1~65535</small>
Priority	1
	<small>🔍 0~255</small>
Area	0
	<small>🔍 ip or 0~4294967295</small>

- **OSPF enable:** Check the option to enable OSPF dynamic routing on the specified interface.
- **Network type:** Select the OSPF network type. Select only **Point to Point** or **Point to Multi-point** if connecting to your networking using PPP protocol, otherwise select **Broadcast**. If only exchanging OSPF routing information to one other device, select **Non-Broadcast** and enter in the **Neighbor** IP address at the bottom.
- **Key authentication** – Enables MD5 authentication on all OSPF messages sent and received.
- **Key string** – If authentication is enabled, enter the authentication key string/password to use for OSPF messages sent and received.
- **Plain text password** – This option will set the password to be send in clear text instead of using the MD5 hash. This setting is not recommended.
- **Cost** – Enter the OSPF cost value.
- **Priority** – Enter the OSPF priority value.
- **Area** - Enter the area id for OSPF.

You can check the current routing table under **Status > Routes** under **Active IPv6-Routes**.

Quality of Service (QoS)

Network > QoS

The router supports up to four QoS priority queues for traffic classification and priority.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click on **QoS**.
3. Under QoS settings, review the settings below. When complete, click **Apply** to save and commit your changes.

QoS Settings

- **Enable:** Check the enable option to **Enable QoS**.
- **Download speed (kbit/s):** Enter the maximum download speed provided by your ISP in kilobits per sec. It is important to set this value accurately.
Note: If your multiple mode is set to load balancing, you can combine the total download bandwidth of both WAN connections.
- **Upload speed (kbit/s):** Enter the maximum upload speed provided by your ISP in kilobits per sec. It is important to set this value accurately.
Note: If your multiple mode is set to load balancing, you can combine the total upload bandwidth of both WAN connections.
- **Calculate overhead** – Typically, when this option is unchecked/disabled, the overhead value will not be added to the upload and download speeds entered in the fields. When this option is checked/enabled, the total overhead calculation is included in the total upload/download speed specified to ensure the values entered are the absolute maximum value limits entered.
- **Default class** – When QoS is enabled, select the default priority class used for all other traffic when QoS after all specific QoS classification rules have been applied. You can typically set this to **Low** or **Medium**.

QoS Settings

Enable
 Download speed (kbit/s)
 Upload speed (kbit/s)
 Calculate overhead
 Default class

Classes – The QoS priority classes define the bandwidth maximum limits of total bandwidth that can be used and total bandwidth that can be shared for a particular class. *Note: Typically, you do not need to modify the QoS priority class percentage settings.*

- **Download link share bandwidth (%)** – This defines the guaranteed bandwidth % from the total download speed defined in the QoS settings. The class setting will attempt to guarantee this bandwidth % minimum limit is allocated.
- **Download max bandwidth (%)** – This defines the maximum bandwidth % allowable from the total download speed defined in the QoS settings. This class setting is the maximum bandwidth % limit that can be allocated above the link share bandwidth %.
- **Upload link share bandwidth (%)** – This defines the guaranteed bandwidth % from the total upload speed defined in the QoS settings. The class setting will attempt to guarantee this bandwidth % minimum limit is allocated.
- **Upload max bandwidth (%)** – This defines the maximum bandwidth % allowable from the total upload speed defined in the QoS settings. This class setting is the maximum bandwidth % limit that can be allocated above the link share bandwidth %.

Download link share bandwidth (%)
 Download max bandwidth (%)
 Upload link share bandwidth (%)
 Upload max bandwidth (%)

Classification Rules

Click **Add** to create a new QoS classification rule. When complete, click **Apply** to save and commit your changes.

- **Target** – Select the QoS priority class to apply to the rule.
- **Direction** – Select the direction of traffic in which to apply the QoS classification, Download (Inbound Traffic) or Upload (Outbound Traffic).
- **Source Host** – Click the drop-down list to select All (any IP address), a specific source host IP address from the list or select Custom to define a particular source IP address not listed.
- **Destination Host**– Click the drop-down list to select All (any IP address), a specific destination host IP address from the list or select Custom to define a particular destination IP address not listed.
- **Protocol** – Click the drop-down to select the type of traffic to apply the QoS classification rule. All/TCP/UDP/ICMP or custom to specify a particular protocol not listed.
- **Source Port (range)** – Enter the source port or source port range to apply the QoS classification rule.
- **Destination Port (range)** – Enter the source port or source port range to apply the QoS classification rule.
-

Classification Rules

Target	Direction	Source host	Destination host	Protocol	Source Port (range)	Destination Port (range)	Comment
Highest	Download	All	All	All	All	All	

Dynamic DNS

Services > Dynamic DNS

When using a dynamic IP/DHCP WAN type from your ISP where your public IP or Internet IP address always changes, dynamic DNS provides a method of accessing your router or network remotely over the Internet for devices such as IP cameras, storage, or computers hosted on the local LAN side of your router. Dynamic DNS services do this by assigning a custom hostname or DNS name for you to reference. Your router will send updates to the dynamic DNS service provider if the WAN or Internet IP address(es) change providing the emulation of a virtual fixed IP address that you can always reference to access your router over the Internet.

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*, *dyndns.org* etc.)
2. Log into your router management page (see "[Access your router management page](#)" on page 8).
3. Click on **Services** and click on **Dynamic DNS**.
4. Review the **DDNS** settings below. When complete, click **Apply** to save and commit your changes.
 - **Enabled** – Check the enabled option to enable dynamic DNS on the selected WAN interface.
 - **DDNS Provider [IPv4]:** Click the drop-down list Select your DDNS service.
 - **Host Name:** Enter the custom hostname or DNS name you created with DDNS account. (e.g. *trendnet.ddns.net*)
 - **Account:** The user name needed to login to your Dynamic DNS service account.
 - **Password:** This is the password to login to your Dynamic DNS service account.

WAN1 DDNS Settings

Basic Settings	Timer Settings	Log File Viewer
Enabled <input type="checkbox"/>		
DDNS Service provider [IPv4]	No-IP.com	
Hostname/Domain	yourhost.example.com	
	Replaces [DOMAIN] in Update-URL	
Username	your_username	
	Replaces [USERNAME] in Update-URL	
Password	••••••••••	
	Replaces [PASSWORD] in Update-URL	

Below is a reference of the additional Dynamic DNS settings if you choose to make other configuration changes to these sections.

Timer Settings

Allows you to configure a specified interval to force your router to send a DDNS update to your DDNS service provider.

Note: Please note that it is recommended not to set the interval too low and send updates too often as this may not meet the minimum requirements of your DDNS service provider client update policy.

- **Force Interval** – Enter a value in days, hours, or minutes.

Note: The smallest interval allowed is 10 minutes. Setting the value to 0 will force your router to send a DDNS update only once and will not resend any more DDNS updates for the specified WAN.

File sharing server

Services > Network Shares

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 Samba (SMB) file sharing protocol and is compatible with SMB/CIFS.

Note: Only FAT32 or NTFS file formats are supported, up to 4TB max. storage size.

After you have connected your USB storage device:

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Services** and click on **Network Shares**.
3. Review the settings below. When complete, click **Apply** to save and commit your changes.

Note: By default, the Samba server name is set to TEW-829DRU or the LAN IP address may also be used default LAN IP: 192.168.10.1. To change the Samba server name, you can modify this setting under Administrator > System and edit the Host Name setting.

Samba General Settings

- **Enable** – Check the enable option to enable Samba file sharing.
- **Description:** Enter a description for the server.
- **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.
- **Login Required** – Selecting **No** will not require computers to login when accessing the USB share. Select **Yes** will require computers to enter a user name and password when accessing the USB share and user account can be modified under the Samba Users list. This user account will have full read/write permissions on the USB share.

Samba

General Settings	
Enable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Description	TEW-829DRU
Workgroup	WORKGROUP
Login Required	<input type="radio"/> Yes <input checked="" type="radio"/> No

Samba Users

- **User Name:** Enter the user name to be used to access the USB share.
- **Password:** Enter the password to be used to access the USB share.

Shared Devices

- **Device Name:** Displays the USB storage device name.
- **Shared Name:** Displays the Samba share name used to access the USB share over the network.

Example: You can access the USB share by typing in the path [\\TEW-829DRU\usb_A1](#) or [\\<routerIPaddress>\usb_A1](#).



- **Size** – Displays the total size of the USB storage device.
- **Used** – Displays the storage space currently used on the USB storage device.
- **Available** – Displays the storage space currently available on the USB storage device.
- **Eject Device** – Clicking the **Eject** button will allow you to safely remove/dismount and disconnect the USB storage device.

Wake on LAN (WoL)

Services > Wake on LAN

Wake on LAN (WoL) is used to remotely wake up or turn on device that support the WoL feature from your router.

Note: In order for the WoL feature to work, the device must support the WoL and it must be enabled configured properly on the device.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Services** and click on **Wake on LAN**.
3. Review the settings below. When complete, click **Apply** to save and commit your changes.
 - **Host to wake up:** Click the drop-down list to select a computer/device from the list or manually enter the MAC address of the device. Clicking the **WAKE UP HOST INSTANTLY** button will immediately send a wake up message to the WoL device.
 - **Add new WoL schedule:** Allows you to select a schedule when to send a wake up message to the WoL device.

Wake-on-LAN (WoL)

Name	MAC Address	Run Time
<i>This section contains no values yet</i>		
Host to wake up	<input type="text"/>	<input type="button" value="WAKE UP HOST INSTANTLY"/>
<input checked="" type="radio"/> Choose the host to wake up or enter a custom MAC address to use		
Add new WoL schedule	<input type="text" value="New rule name"/>	<input type="button" value="ADD"/>

Wireless Networking and Security

Wireless Settings

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

This section covers the wireless settings of your router such as wireless network names (SSIDs), channels, 802.11 mode, and other wireless settings.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click on the wireless band you would like to configure **Wireless (2.4GHz or 5GHz1 or 5GHz2)**
3. Review the settings below. When complete, click **Apply** to save and commit your changes.

Primary SSID – This tab involves the configuration parameters for the primary SSID for a specific wireless band.

- **Device Configuration**
 - **General Setup**

- **Status** – Displays current information about the wireless radio/band such as SSID, BSSID/wireless MAC address, encryption, operating channel, transmit power, bitrate, and country/region.
- **Enable wireless radio** – This option is checked by default to enable the wireless radio/band. Unchecking this option will disable the wireless radio/band including all additional SSIDs configured on the specific band.
- **Turn off wireless radio by schedule** – Allows you to assign a time schedule when the band should be turned on and off.
- **Operating frequency** – By default, the operating channel is set to Auto to automatically scan and use the best channel available when the device is powered on. If you are encountering interference or connectivity issues on the current channel, you can select a different wireless channel for the band to operate.

Note: Modifying the channel settings will force currently connected wireless client devices to disconnect and reconnect to your router's wireless networks.

General Setup	Advanced Settings
<p>Status Mode: Master SSID: TRENDnet829_5GHz1_YCE1 BSSID: 3C:8C:F8:F3:85:B8 Encryption: WPA2 PSK (CCMP) Channel: 40 (5.200 GHz) Tx-Power: 24 dBm Bitrate: 1733.3 Mbit/s Country: US</p>	
<p>Enable wireless radio <input checked="" type="checkbox"/></p>	
<p>Turn off wireless radio by schedule Disable time schedule <input type="button" value="v"/></p>	
<p>Operating frequency Auto <input type="button" value="v"/></p>	

- **Advanced Settings**
 - **Mode** – By default, 802.11b/g/n and 802.11a/n/ac modes are configured to ensure the best compatibility with wireless client devices. These settings will allow all wireless client devices to connect to your router's wireless networks including devices that support older standards such as 802.11a/b/g.
Note: If older slower wireless client devices connect to your wireless network, this may reduce the speed and performance of all other wireless client devices connecting to the same wireless network.
 - **HT mode:** Select the appropriate channel width for your wireless network. For greater 2.4GHz performance/data rate capability, you can select **Auto 20/40MHz** (Options: 20MHz or Auto 20/40MHz). It is recommended to use the default channel bandwidth settings.
For greater 5GHz performance/data rate capability, you can 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 20/40MHz or 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.

General Setup	Advanced Settings
Mode	802.11a/n/ac
HT mode	Auto 20/40/80MHz

- **Interface Configuration**


- **General Setup**

- **ESSID** – This is wireless network name setting for the primary SSID band. This name will differentiate your wireless network from other neighboring wireless networks so you can identify and connect your wireless client devices. Enter the wireless network name to assign to the wireless band.
 - **Hide ESSID** – Checking this option will hide your wireless network name from being discovered by wireless client devices scanning for available wireless networks. This will not disable the wireless band or network and wireless client devices can still connect. It only hides the network name from being discovered.

General Setup	Wireless Security	MAC-Filter	Advanced Settings
ESSID		TRENDnet829_5GHz1_YCE1	
Hide ESSID		<input type="checkbox"/>	

- **Wireless Security** – Allows you to configure the wireless encryption/security for the wireless band. See the [“How to choose the type of wireless security”](#) and [“Secure your wireless network”](#) sections for details configuring wireless security.

General Setup	Wireless Security	MAC-Filter	Advanced Settings
Encryption		WPA2-PSK	
Cipher		Force CCMP (AES)	
Key		●●●●●●●●	

- **MAC-Filter** – This feature adds additional security to your wireless band by allowing you to enter a list of specific MAC addresses that can either be allowed to connect (**Allow listed only**) or blocked (**Deny listed**) from connecting to your wireless network. This feature must be specified on each wireless band.
 - **MAC-Address Filter**
 - **Disable** - Disables MAC address filtering on the wireless band.
 - **Allow listed only (Whitelist)** – Sets the MAC filter action to allow only the MAC addresses listed and deny all others on the wireless band.
 - **Deny listed (Blacklist)** – Sets the MAC filter action to deny only the MAC addresses listed and allow all others on the wireless band.
 - **MAC-List** – Enter the MAC addresses to allow or deny. For each additional MAC address entries, click  . (e.g. a1:b2:c3:d4:e5:f6)

General Setup	Wireless Security	MAC-Filter	Advanced Settings
MAC-Address Filter		Deny listed	▼
MAC-List		+	

Advanced Settings

- **Separate Clients** – By default, this option is left unchecked and allows all wireless client devices that are connected to the same wireless SSID to communicate with other wireless client devices. Checking this option will block communication between wireless client devices connecting with other wireless client devices. This feature is also known as L2 isolation or L2 client isolation.
- **WMM Mode** – This feature enables Wi-Fi Multimedia QoS prioritization for wireless client devices that support WMM using the default priority level settings. Unchecking this option will disable WMM QoS on the wireless band.
- **Enable HT20/40 coexistence** – Applies to 2.4GHz band only. This option is enabled by default to ensure connection stability on the 2.4GHz band. When this option is enabled, the radio will attempt to operate at the higher 40MHz channel width mode if there are not too many neighboring wireless networks. If the current wireless environment is too busy the radio will automatically operate at the lower 20MHz channel width mode. Unchecking this option forces the radio to operate at the higher 40MHz channel which cause instability if there are too many neighboring 2.4GHz wireless networks.

Interface Configuration

General Setup	Wireless Security	MAC-Filter	Advanced Settings
Separate Clients		<input type="checkbox"/>	Prevents client-to-client communication
WMM Mode		<input checked="" type="checkbox"/>	
Enable HT20/HT40 coexistence		<input checked="" type="checkbox"/>	

Multiple SSID - This tab involves the configuration parameters for the additional SSIDs for a specific wireless band. Up to 7 additional SSIDs can be created per wireless band. You can view a summarized list of the current operating SSID and channels under Status > Overview in the Wireless section.

General Setup

- **Enabled** – Checking this option will enable the additional SSID on the specific wireless band. Before checking Enabled, click the Multiple SSID drop-down and select which index number SSID to configure.
- **Multiple SSID** – Click the drop-down to select the index number SSID to configure, then check Enabled.
- **ESSID** – This is wireless network name setting for the additional SSID band. This name will differentiate your wireless network from other neighboring wireless networks so you can identify and connect your wireless client devices. Enter the wireless network name to assign to the additional SSID.
- **Hide ESSID** – Checking this option will hide your wireless network name from being discovered by wireless client devices scanning for available wireless networks. This will not disable the additional SSID and wireless client devices can still connect. It only hides the network name from being discovered.
- **Turn off wireless radio by schedule** – Allows you to assign a time schedule when the band should be turned on and off.

General Setup

Enabled	<input type="checkbox"/>
Multiple SSID	SSID 1. ▼
ESSID	_____
Hide ESSID	<input type="checkbox"/>
Turn off wireless radio by schedule	Disable time schedule ▼


- **Wireless Security** – Allows you to configure the wireless encryption/security for the additional SSID. See the [“How to choose the type of wireless security”](#) and [“Secure your wireless network”](#) sections for details configuring wireless security.

Wireless Security

Encryption No Encryption 

- **Advanced Settings**
 - **Separate Clients** – By default, this option is left unchecked and allows all wireless client devices that are connected to the same wireless SSID to communicate with other wireless client devices. Checking this option will block communication between wireless client devices connecting with other wireless client devices. This feature is also known as L2 isolation or L2 client isolation.
 - **WMM Mode** – This feature enables Wi-Fi Multimedia QoS prioritization for wireless client devices that support WMM using the default priority level settings. Unchecking this option will disable WMM QoS on the additional SSID.

Advanced Settings

Separate Clients
 Prevents client-to-client communication

WMM Mode

How to choose the type of wireless security

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

- **WPA:** This encryption is significantly more robust than the older WEP legacy technology. Much of the older 802.11g hardware was been upgraded (with firmware/driver upgrades) to support this encryption standard. Total wireless speeds under this encryption type however are limited to 54Mbps.
- **WPA/WPA2 Mixed Mode:** 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. 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. There are two cipher types available which are Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). AES should be used whenever possible to ensure the highest level of security.

- WPA-PSK/WPA2-PSK vs. WPA-EAP/WPA2-EAP:** WPA & WPA2 support two security mechanisms, one using a pre-shared key (PSK) and the other using extensible authentication protocol (EAP). PSK is much easier to setup and configure and requires manually specifying the encryption key/pre-shared key (PSK) required for all wireless client devices to connect to your wireless network. EAP requires the use of an external authentication server and complex configuration to setup authentication and authorization your wireless client devices outside the scope of the router. Several types of EAP that can be configured from secured password + certificate that require more in-depth knowledge of security configuration.

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.

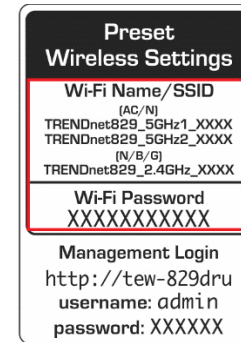
Security Standard	WPA	WPA2
Compatible Wireless Standards	802.11a/b/g (802.11ac/802.11n devices will operate at 802.11g/802.11a to connect using this standard)	802.11a/b/g/n/ac
Highest Performance Under This Setting	Up to 54Mbps	Highest data rate supported by wireless device
Encryption Strength	Medium	High
Additional Options	TKIP or AES, Preshared Key or RADIUS	TKIP or AES, Preshared Key or RADIUS
Recommended Configuration	TKIP Preshared Key 8-63 characters	AES Preshared Key 8-63 characters

Note: It is recommended to use WPA2 CCMP (AES) encryption whenever possible as it the most secure option and supports the highest data rates supported by the wireless network device.

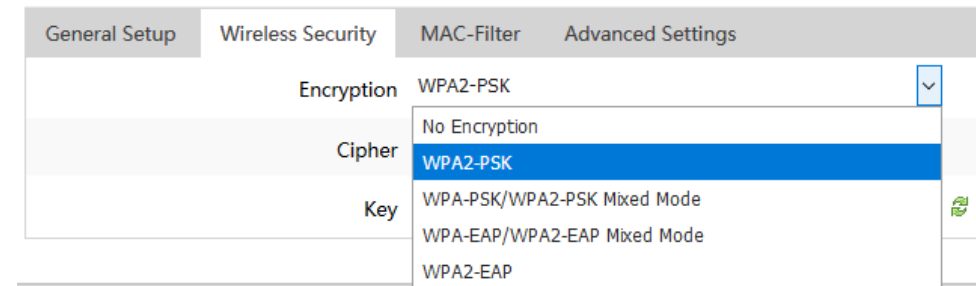
Secure your wireless network

Network > Wireless 2.4GHz / 5GHz1 / 5GHz2

By default, your router is pre-configured with wireless network names (SSIDs) and a wireless encryption key using WPA2-PSK (AES). 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. The following sections involve changing the default wireless security settings and encryption key.




- Log into your router management page (see “[Access your router management page](#)” on page 8).
- Click on **Network** and click on the wireless band you would like to configure, **Wireless 2.4GHz / 5GHz1 / 5GHz2**.
- Under Interface Configuration and in the Wireless Security tab, click on the **Encryption** drop-down list to select your wireless security type.



Selecting WPA2-PSK, WPA-PSK / WPA2-PSK Mixed Mode

(WPA2-PSK recommended):

In the **Security Mode** drop-down list, select **WPA2-PSK** or **WPA-PSK / WPA2-PSK Mixed Mode**. Review the settings below. When complete, click **Apply** to save and commit your changes.

General Setup	Wireless Security	MAC-Filter	Advanced Settings
	Encryption	WPA2-PSK	▼
	Cipher	Force CCMP (AES)	▼
	Key	●●●●●●●●	

The following section outlines options when selecting **WPA2-PSK**, or **WPA-PSK / WPA2-PSK Mixed Mode**.

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


Key: Enter the pre-shared key or passphrase. (8-63 alphanumeric characters (a,b,c,?,*,/,1,2, etc.)

Note: This is the wireless password, pre-shared key, or passphrase wireless client devices will use to connect to your wireless network.

Selecting WPA2-EAP, WPA-EAP / WPA2-EAP Mixed Mode

The following section outlines options when selecting **WPA2-EAP** or **WPA-EAP / WPA2-EAP Mixed Mode** (EAP or RADIUS). This security type is also known as EAP (Extensible Authentication Protocol) or RADIUS (Remote Authentication Dial-In User Service). Review the settings below. When complete, click **Apply** to save and commit your changes.

Note: This security type requires an external RADIUS server, Pre-Shared Key only requires you to create a wireless password, pre-shared key, or passphrase.

General Setup	Wireless Security	MAC-Filter	Advanced Settings
	Encryption	WPA-EAP/WPA2-EAP Mixed Mode	▼
	Cipher	Force TKIP and CCMP (AES)	▼
	Radius-Authentication-Server	<hr/>	
	Radius-Authentication-Port	1812	 Default 1812
	Radius-Authentication-Secret	<hr/>	

- **Cipher:** Select a Cipher Type to use.
 - When selecting **WPA-EAP / WPA2-EAP Mixed Mode** security, it is recommended to use **Force TKIP and CCMP (AES)**.
 - When selecting **WPA2-EAP** security, it is recommended to use **Force CCMP (AES)**.
- **Radius-Authentication-Server:** Enter the IP address of the RADIUS server. (e.g. 192.168.10.250)
- **Radius-Authentication-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 port used for the RADIUS service.
- **Radius-Authentication-Secret:** Enter the shared secret used to authorize your router with your RADIUS server.

Guest Network

Network > Guest Network

Creating an isolated and separate wireless guest network on each wireless band 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 8).
2. Click on **Network** and click on **Guest Network**.
3. Review the settings below. When complete, click **Apply** to save and commit your changes.

First, choose the wireless band guest network you would like to configure, **Wireless 2.4GHz Guest Network / 5GHz1 Guest Network / 5GHz2 Guest Network**.

- **Enable/Disable Guest Network** – Selecting **Enable** turns on the wireless guest network and selecting **Disable** turns off the wireless guest network for the specific wireless band.
- **Network Name(SSID)** - This is wireless network name setting for the guest network. This name will differentiate your wireless network from other neighboring wireless networks so you can identify and connect your wireless client devices. Enter the wireless network name to assign to the wireless guest network.
- **Wireless Security** – Allows you to configure the wireless encryption/security for the wireless band. See the "[How to choose the type of wireless security](#)" and "[Secure your wireless network](#)" sections for details configuring wireless security.
Note: You can only select WPA2-PSK or WPA-PSK / WPA2-PSK Mixed Mode. EAP security cannot be applied to the wireless guest networks.

Enable/Disable Guest Network	Disable	▼
Network Name(SSID)	TRENDnet829_2.4GHz_guest	
Security Mode	No Encryption	▼

Guest DHCP – The wireless guest networks are assigned to a different IP address subnet from the router LAN network for isolation.

- **IPv4 Address** – Enter the IP address interface for the wireless guest network. The IP address subnet should be different from any other LAN or VLAN IP networks configured on your router.
Note: The guest network IP address subnet only supports a class C subnet, subnet mask 255.255.255.0.
- **Start** – Enter the starting value of DHCP IPv4 address range for the wireless guest network. (e.g. If your guest network IPv4 address is 192.168.20.1, entering 120 will define the first IP address of the DHCP pool is 192.168.20.120)
- **End** – Enter the ending value of DHCP IPv4 address range. (e.g. If your LAN IPv4 address is 192.168.20.1, entering 200 will define the last IP address of the DHCP pool is 192.168.20.200)
- **Lease Time** – Enter the lease time in hours (h) or minutes (m) DHCP clients will hold their IP address settings before automatically requesting a new lease (IP address settings) from the internal DHCP server. (e.g. To specify 24 hours, enter 24h. To specify 480 minutes, enter 480m.)
- **Separate Clients** – This option allows all wireless client devices that are connected to the guest network wireless SSIDs to communicate with other wireless client devices. Checking this option will block communication between wireless client devices connecting with other wireless client devices. This feature is also known as L2 isolation or L2 client isolation.

Guest DHCP

IPv4 address	192.168.20.1
Start	101
	🔗 Lowest leased address as offset from the network address.
End	199
	🔗 Highest leased address as offset from the network address.
Leasetime	1h
	🔗 Expiry time of leased addresses, range 2m ~ 999999h (m = minutes, h = hours).
Separate Clients	<input checked="" type="checkbox"/>
	🔗 Prevents client-to-client communication

WiFi client bridge mode

Administrator > Device 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 LAN switch ports (1-8). 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 LAN switch ports (1-8). 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.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).

2. Click on **Administrator** and click on **Device Mode**.

Note: After changing the device mode to client bridge, the router will keep the existing static LAN IP address. By default, the static LAN IP address: 192.168.10.1 / 255.255.255.0.

3. After the device completely apply the configuration changes and reboots, click **Network** and click **Site Survey** to scan for available wireless networks.

Network

Site Survey

4. Select the WiFi network to connect to in the list by clicking on the Select button next to the WiFi network name or SSID and click **Connect**.

Note: If you do not find your WiFi network in the list, you can click Rescan to scan again for networks.

Wireless Network Site Survey

Select	Wireless Network Name
<input type="radio"/>	TRENDnet828_2.4GHz_0QNU
<input checked="" type="radio"/>	TRENDnet828_5GHz_0QNU
<input type="radio"/>	TRENDnet740_LKLS

CONNECT

5. If the network selected network requires a WiFi password/key, enter the key under **WiFi Key/Password** and click **Apply** to save and commit your changes.

Note: The router keep the existing static LAN IP address settings after you have connected to a WiFi network.

Wireless Security

Security Mode WPA2 Personal ▼
WiFi Key/Password

APPLY

Connect wireless devices using WPS

Network > 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 Hide ESSID option to enabled under Network > Wireless 2.4GHz / Wireless 5GHz1 / Wireless 5GHz2 sections.

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

- Virtual Push Button Configuration (PBC) method (Recommended)
 - PIN (Personal Identification Number) Method - located in router management page
- Note:** Refer to your wireless client device documentation for details on the operation of WPS.

PBC (Software/Virtual Push Button)

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 8).
2. Click on **Network** and click on **WPS**.
3. To add a wireless device to your network, under WPS Method, next to Push Button, click the **PBC Start** button. Then push the WPS button on the wireless device (consult wireless client device's User's Guide for length of time) you are connecting to your router.

Push Button



4. The WPS LED on the front panel will flash repeatedly when the WPS process is activated. The WPS LED will flash for approximately 2 minutes.

5. Wait for the status of the wireless client device to indicate that connection was successful.

PIN (Personal Identification Number)

If your wireless client 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 8).
 2. Click on **Network** and click on **WPS**.
 3. To add a wireless device to your network, in the **Station PIN** field, enter the 8-digit numeric PIN number of the wireless client device and click **ADD ENROLLEE**.
- Note:** You may need to initiate the WPS PIN on your wireless device first when using this method. Refer to your wireless client device documentation for details on the operation of WPS.

Station PIN _____

ADD ENROLLEE

CANCEL

4. Wait for the status of the wireless client device to indicate that the connection was successful.

Below is a reference of the additional settings if you choose to make other configuration changes to these sections. Review the settings below. When complete, click **Apply** to save and commit your changes.

WPS Configuration

- **Enable** – Check this option to enable WPS or uncheck to disable WPS.
- **Band Trigger** – Click the drop-down list to select which wireless band to trigger and activate for WPS connectivity. Select the wireless band and click **Apply** first before initiating WPS connection to a wireless client device.
- **External Registrar Enable** – By default, the router functions in WPS registrar mode. In WPS client connectivity, one device functions as a registrar and the other functions as an enrollee. Checking this option will allow the router to function enrollee mode instead of registrar mode. For security purposes, it is recommended to leave this settings unchecked/disabled.

WPS Configuration

Enable

Band Trigger All Band

External Registrar Enable

WPS Method

- **Push Button**
 - **PBC Start/PBC Again** – Clicking this button will activate WPS.
 - **PBC Stop** – Clicking this button will stop the WPS process.
- **Station PIN** – Enter the wireless client device 8 digit WPS PIN number and click **ADD ENROLLEE** to activate WPS via PIN.
- **Device PIN** – This displays the router current WPS PIN. Wireless client devices may have the ability to enter the PIN of the wireless router/access point you would like to connect. Instead of entering the wireless client device PIN under station PIN, you can enter the router device PIN in the wireless client device to activate WPS via PIN method.

WPS Status

- **Current Status** – Displays the current WPS process status.

- **Network Name(SSID)** – Displays the current wireless network name for each wireless band.
- **Security** – Displays the current security used on each wireless band.
- **Status** – Displays the current configuration status of WPS on the router.

WPS Method

Push Button PBC START PBC STOP

Station PIN ADD ENROLLEE CANCEL

Device PIN **66266709**

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.

Firewall & security settings

General settings

Network > Firewall > General Settings

The general firewall settings do not typically require any additional configuration settings as this controls the global actions for packet flow/filtering NAT to and from the router as well as through the router. Zones are defines as one or more interfaces that serve as source or destination interfaces used to forward traffic.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click on **Firewall**, and click on the **General Settings** tab.
3. Review the settings below. When complete, click **Apply** to save and commit your changes.

General Settings

- **Drop invalid packets** – By default, this function is disabled and will allow the router to respond to any packets received on any interface whether the packet is invalid or not. Enabling this function will set the router to drop all packets found to be invalid without any response to the sender which can increase security and prevent denial of service (DoS) attacks.
- **Input** – This setting defines the global action of how to handle traffic destined for the router inbound on an interface in a specific zone.
- **Output** - This setting defines the global action of how to handle traffic originating from the router outbound on an interface in a specific zone.
- **Forward** – This setting defines the global action of how to handle traffic passing between interfaces in a specific zone.
 - **Reject** – When packet reaches the router, drops packet and sends a response to sender indicating that a port is unreachable.
 - **Drop** – When packet reaches the router, drops packet without any response to the sender.
 - **Accept** – When packet reaches the router, allows a packet to traverse the router

General Settings

Drop invalid packets

Input	Accept	▼
Output	Accept	▼
Forward	Drop	▼

WAN Ping Respond

- **Enable** – By default, this function is disabled to prevent the WAN port interfaces from responding to ping/ICMP requests. Enabling this option will set your WAN port interfaces to respond ping/ICMP requests from the Internet.

WAN Ping Respond

Enable

Port forwarding rules

Network > Firewall > Port Forward

Port forwarding rules allow to create inbound rules from the WAN interfaces/Internet to your internal computers or devices for specific services/protocols such as a file server (FTP), IP camera, web server (HTTP/HTTPS), or remote access, etc.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click on **Firewall**, and click on the **Port Forward** tab.
3. Review the settings below. When complete, click **Add** to add the new entry to the list and **Apply** to save and commit your changes.

- **Name** – Enter a name for the new port forwarding rule.

Name

New port forward

- **Protocol** – Click the drop-down list to select the protocol for the service to allow: **TCP**, **UDP**, **TCP+UDP**, or **Other**.

Protocol

TCP+UDP

- **External Interface** – Click the drop-down list to select the external WAN interface(s) to allow: **WAN1**, **WAN2**, or **WAN1+WAN2**. For example, choosing WAN1 will only allow the port forward to work on inbound connection requests on WAN1 only and inbound connections requests on WAN2 will be denied.

External Interface

WAN1

- **External Port** – Enter the external port number for the service to allow.
Note: You can also enter a consecutive range of ports in the following format: 80-90

External port

- **Internal IP address** – Click the drop-down list to select a device from the list or enter the local/internal IP address of the device to forward the port/protocol service.

Internal IP address

- **Internal Port** – Enter the internal port number for the service to allow.
Note: You can also enter a consecutive range of ports in the following format: 80-90
Typically, the internal port or port range is same as the external port or port range.

Internal port

- **Schedule** – Allows you to select a schedule when the port forwarding rule should be enabled or disabled.

Schedule

Disable time schedule

Note: To restrict access to source IP address, after you have created the port forward rule, click **Edit** on the port forwarding entry in the list and enter the IP address in **Source IP address** field, then click **Apply**.

EDIT **DELETE**

Source IP address

 Only match incoming traffic from this IP or range.

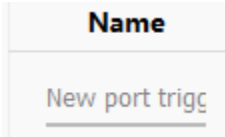
Port trigger rules

Network > Firewall > Port Trigger

Port triggering is typically used for applications that require a range of ports to be dynamically opened on request to an internal device on your network. The router will wait for a request on a specific port or range of ports (trigger port) from a device on your network and once a request is detected by your router, the router will forward a port or range of ports (match port) to the device on your network.

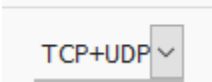
1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click on **Firewall**, and click on the **Port Forward** tab.
3. Review the settings below. When complete, click **Add** to add the new entry to the list and **Apply** to save and commit your changes.

- **Name** – Enter a name for the new port trigger rule.



- **Match Protocol** – Click the drop-down list to select the match port protocol for the service to allow: **TCP**, **UDP**, or **TCP+UDP**.

Match Protocol



- **Match Port** – Enter the match port number for the service to allow.
Note: You can also enter a consecutive range of ports in the following format: 80-90

Match port



- **Trigger Protocol** – Click the drop-down list to select the trigger port protocol for the service to allow: **TCP**, **UDP**, or **TCP+UDP**.

Trigger Protocol



- **Trigger Port** – Enter the match port number for the service to allow.
Note: You can also enter a consecutive range of ports in the following format: 80-90

Trigger port



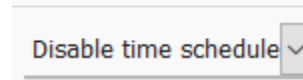
- **Internal Port** – Enter the internal port number for the service to allow.
Note: You can also enter a consecutive range of ports in the following format: 80-90
Typically, the internal port or port range is same as the external port or port range.

Internal port



- **Schedule** – Allows you to select a schedule when the port trigger rule should be enabled or disabled.

Schedule



IP filtering

Network > Firewall > IP Filtering

IP filtering allows you to restrict access to the Internet to specific IP addresses on your network. You can check the current IP addresses assigned to devices connected to your router under Status > Overview under the DHCP leases section. You can also lock the IP address assigned to specific devices connected to your router by [adding static DHCP leases or reservations](#).

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click on **Firewall**, and click on the **IP Filtering** tab.
3. Review the settings below. When complete, click **Add** to add the new entry to the list and **Apply** to save and commit your changes.

- **Name** – Enter a name for the new IP filtering rule.

Name

- **Src IP** – This is the source IP address or device IP address to filter. Click the drop-down list to select a device from the list or enter the local/internal IP address of the device to filter or restrict.

Src IP

- **Dst IP** – This is the destination IP address for the IP filtering rule. Since the IP filtering rule only applies to outbound Internet access, this will need to be a public Internet IP. You can leave this setting blank to set the rule to apply to any public Internet IP address.

Dst IP

- **Protocol** – Click the drop-down list to select the protocol for the service to restrict: **All, TCP, UDP, TCP+UDP, or ICMP.**

Protocol

- **Src Port** – This is the source port number. Enter the source port number for the service to restrict.

Note: You can also enter a consecutive range of ports in the following format: 80-90

Src Port

- **Dst Port** – This is the destination port number. Enter the destination port number for the service to restrict.

Note: You can also enter a consecutive range of ports in the following format: 80-90

Dst Port

- **Schedule** – Allows you to select a schedule when the IP filter rule should be enabled or disabled.

Schedule

MAC filtering

Network > Firewall > MAC Filtering

Every network device has a unique, 12-digit MAC (Media Access Control) address. MAC filtering allows you to restrict access to the Internet to specific MAC addresses on your network. MAC filtering in this section applies to both wired and wireless devices. To create MAC filtering rules on your wireless network only, go to the [Wireless Settings](#) section under MAC-filter. You can check the current MAC addresses of devices connected to your router under Status > Overview under the DHCP leases section.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click on **Firewall**, and click on the **MAC Filtering** tab.
3. Check the **Enable** option to enable MAC filtering and select **Mode**.

Note: Please make sure to add the MAC addresses in the list first before clicking Apply.


- **Enable** – Check this option to enable MAC filtering.
- **Mode** – Select the mode used for MAC filtering.
 - **Deny Mode (Blacklist)** – Sets the MAC filter action to deny only the MAC addresses listed and allow all others access to the Internet.
 - **Allow Mode (Whitelist)** – Sets the MAC filter action to allow only the MAC address listed and deny all others access to the Internet.

Important Note: Please make sure to add the MAC addresses in this list before applying the setting especially in Allow mode.

MAC Filtering Mode

Enable

Mode Deny Mode Allow Mode

 In allow mode, only allowed MAC Address can access the network

4. Review the settings below. When complete, click **Add** to add the new entry to the list and **Apply** to save and commit your changes.

- **Name** – Enter the name for the MAC filter rule.
- **MAC Address** – Click the drop-down list to select a device from the list or enter the MAC address manually. (e.g. a1:b2:c3:d4:e5:f6)
- **Schedule** – Allows you to select a schedule when the MAC filter rule should be enabled or disabled.

MAC Filtering List

Name	MAC Address	Schedule
This section contains no values yet		
Add New MAC Filtering Rule:		
Name	MAC Address	Schedule
New mac filtering rule	<input type="text"/>	Disable time schedule <input type="text"/>
		<input type="button" value="ADD"/>

Denial of service (DoS) prevention

Network > Firewall > DoS Prevention

The router supports prevention against common denial of service (DoS) attacks. Malicious users use denial of service attacks to temporarily or permanently disrupt the availability of services from network resource such as your router. Typically, DoS attacks are achieved by flooding a specific network resource by excessively sending unnecessary requests which can cause the network device or resource to stop functioning.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click on **Firewall**, and click on the **DoS Prevention** tab.
3. Review the settings below. When complete, **Apply** to save and commit your changes.

Choose the DoS prevention type to enable, TCP SYN flood, UDP flood, or ICMP flood.

- **Enable** – Check this option to enable DoS prevention.
- **Rate (times per second)** – This value limits the amount of packets that can be received by the router per second for a specific session.
- **Burst** – This value limits the total amount of packets that can be received and stored in buffer memory for a specific session.

Enable

Rate (times per second)

Burst

DMZ Host

Network > Firewall > DMZ Host

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 all ports 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 method and will open your local area network to greater threats from Internet attacks. It is recommended to use [port forwarding](#) instead to limit rules to specific ports/services only.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click on **Firewall**, and click on the **DMZ Host** tab.
3. Review the settings below. When complete, **Apply** to save and commit your changes.

- **Enable** – Check this option to enable DMZ host.
- **DMZ Host IP Address** - Enter the IP address you assigned to the computer or network device to expose to the Internet. (e.g. 192.168.10.250)

Enable

DMZ Host IP Address

One-to-One NAT

Network > Firewall > One-to-One NAT

If you have multiple static public WAN/Internet IP addresses assigned by your ISP, you can map the additional public IP addresses to a local computer or device on your network and allow all or specific ports or services similar to port forwarding but using different public IP addresses through your router. Please check with your ISP if you have multiple static public IP addresses available that can be used to map to devices on your local network.

Note: This feature will only work when using a static IP address WAN type/protocol.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click on **Firewall**, and click on the **One-to-One NAT** tab.
3. Review the settings below. When complete, click **Add** to add the new entry to the list and **Apply** to save and commit your changes.

- **Name** – Enter a name for the new one-to-one NAT rule.

Name

New one-to-oi

- **Private IP address** – Click the drop-down list to select a device from the list or enter the local/internal IP address of the device to forward the port/protocol service.

Private IP

▼

- **Public** – Enter the additional static public Internet IP address you would like to map to the local/internal IP address.

Public IP

- **External Interface** – Click the drop-down list to select the external WAN interface(s) to allow: **WAN1**, **WAN2**, or **WAN1+WAN2**. For example, choosing WAN1 will only allow the port forward to work on inbound connection requests on WAN1 only and inbound connections requests on WAN2 will be denied.

External Interface

WAN1 ▼

- **Forwarding Mode** - Select **DMZ** to forward all ports/protocols or **Port Forwarding** to specify which ports/protocols to allow.

Forwarding Mode

DMZ ▼

- **DMZ** – Selecting this option will set the rule to forward all ports/protocols to the device internal private IP address.
 - **Schedule** – Allows you to select a schedule when the port forwarding rule should be enabled or disabled.

Schedule Disable time schedule ▼

- **Port Forward** – Selecting this option will allow to set the specific ports/protocols to allow for the rule.
 - **Protocol** – Click the drop-down list to select the protocol for the service to allow: **TCP**, **UDP**, **TCP+UDP**, **ICMP**, or **Custom**.

Protocol TCP+UDP ▼

- **External Port** – Enter the external port number for the service to allow. **Note:** You can also enter a consecutive range of ports in the following format: 80-90

External Port

- **Internal Port** – Enter the internal port number for the service to allow. **Note:** You can also enter a consecutive range of ports in the following format: 80-90
Typically, the internal port or port range is same as the external port or port range.

Internal Port

- **Enable NAT Loopback** – Checking this option will allow devices to resolve the additional public static IP addresses from the local interfaces (e.g. LAN, VLAN). Unchecking this option will not allow to devices to resolve the additional public static IP addresses from the local interfaces. (e.g. LAN, VLAN)

Enable NAT Loopback

- **Schedule** – Allows you to select a schedule when the port forwarding rule should be enabled or disabled.

Schedule Disable time schedule



RADIUS Authentication

Network > Administrator > RADIUS

For additional security, the RADIUS authentication feature will allow you use an external RADIUS server to access the router management configuration page instead of using the internal administrator user account.

Note: This feature requires an external RADIUS authentication server to be set up and configured prior to enabling the feature on your router.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Administrator** and click on **RADIUS**.
3. Review the settings below. When complete, click **Apply** to save and commit your changes.

- **RADIUS Authentication** – Check this option to enable RADIUS authentication.
- **Server IP Address** – Enter the IP address of the external RADIUS server.
- **Server Port** – Enter the port used for the RADIUS service.
Note: The default port used for RADIUS server authentication is 1812.
- **Server Secret** – Enter the shared secret used to authorize the router for use with the external RADIUS server.
- **Confirm Secret** – Re-enter the shared secret for confirmation.
- **Timeout** – Enter the RADIUS server authentication timeout value in seconds. This is the number of seconds between transmissions for authentication requests.
Note: If you encounter issues with repeated authentication attempts, it is recommended to increase this value.
- **Retries** – Enter the number of retries allowed before RADIUS server will deny authentication requests for a specific user.
- **Allow local account login** – Checking this option will still allow login to the router configuration page using the internal administrator account.

RADIUS Authentication

Server IP Address 0.0.0.0

Server Port 1812

Server Secret 

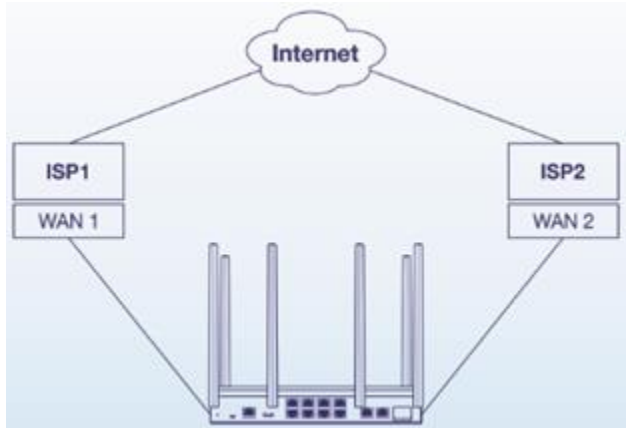
Confirm Secret 

Timeout 5

Retries 3

Allow local account login

Multiple WAN Configuration



Multiple WAN Management Settings

Network > Multiple WAN

The section provides an overview of the multiple WAN management settings and the dual WAN mode functionality.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network** and click on **Multiple WAN**.
3. Review the settings below. When complete, click **Apply** to save and commit your changes.

Note: Multiple WAN diagnostics can be used under Administrator > Diagnostics under the MWAN Interface Diagnostics section.

MWAN Status

- **Interface Live Status** – This section displays the current status of the WAN interfaces of your router. Tracking is enabled using physical link status and L2 based methods but the tracking status displayed refers to the status of IP based link tracking which can be configured under the Link Tracking section.


MWAN Status

Interface Live Status


WAN1 (eth0)
Online (tracking off)


WAN2 (eth2)
Online (tracking off)


Link Tracking – Allows you to setup WAN link tracking by pinging Internet IP addresses.

- **Enable Tracking** – Checking this option enables IP based WAN link tracking on the specific WAN interface.
- **Tracking IP** – Enter an Internet IP address to send ping requests used to verify the link status of a specific WAN interface. You can add additional IP address by clicking .
- **Ping Interval** – Click the drop-down list to set the time interval between consecutive ping requests.
- **Fail Count** – Click the drop-down list to set the maximum number of failed ping requests before interface status is considered to be down or failed.

Enable Tracking

Tracking IP 

Ping Interval 5 seconds 

Fail Count 3 

 Interface will be deemed down after this many failed ping tests

Default Traffic Rule

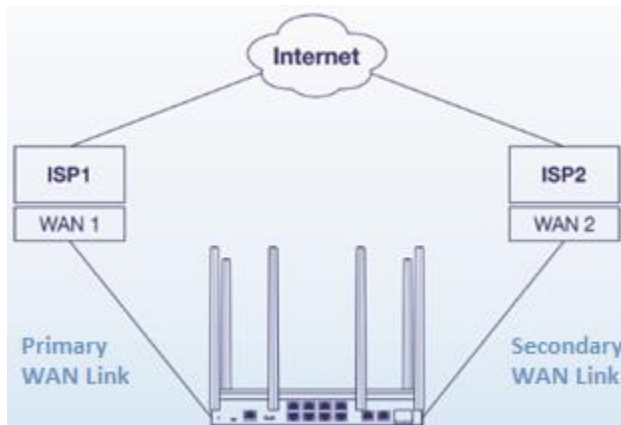
- **Policy** – This setting controls the default WAN mode for Internet connectivity access for all local interface such as LAN, wireless LAN, and VLAN interfaces.

Default Traffic Rule

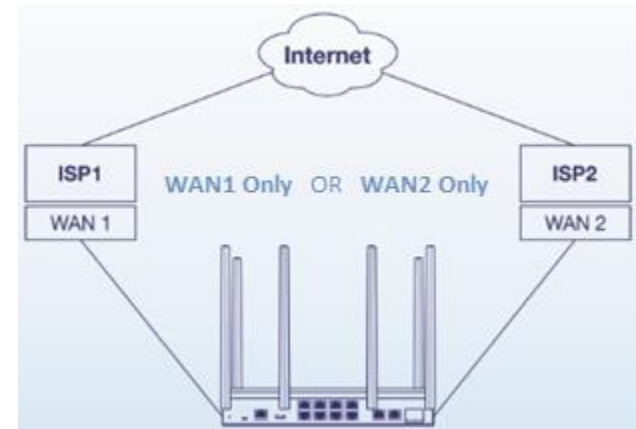
Here is the default traffic rule for all output traffic. You can also set specific rules in Traffic Rule page under Advanced tab

Policy **WAN1 (Failover to WAN2)**

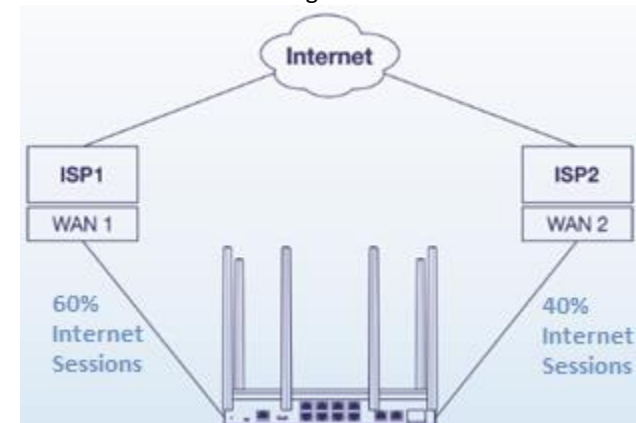
- **WAN1 (Failover to WAN2)** – This is the default WAN mode. In this mode, the primary WAN interface is set to WAN1 and secondary WAN interface is set to WAN2. All traffic will be routed only through WAN1 and will only route to WAN2 for Internet connectivity if the WAN1 primary interface link status fails. If WAN1 connectivity is restored, all Internet traffic will revert back to the primary WAN1 interface.
- **WAN2 (Failover to WAN1)** – In this mode, the primary WAN interface is set to WAN2 and secondary WAN interface is set to WAN1. All traffic will be routed only through WAN2 and will only route to WAN1 if the WAN2 primary fails or is disconnected. If WAN2 connectivity is restored, all Internet traffic will revert back to the primary WAN2 interface.



- **WAN1 (Fixed)** – In this mode, all Internet traffic will only be routed to the WAN1 interface. The WAN2 interface is not used.
- **WAN2 (Fixed)** – In this mode, all Internet traffic will only be routed to the WAN2 interface. The WAN1 interface is not used.



- **Load Balance** – In this mode, Internet traffic will be routed to both WAN1 and WAN2 interfaces based on weighted percentage. Traffic will be distributed to WAN1 and WAN2 based on the total of sessions and weighted % assignment. For example: If selecting a weight of 60% : 40% (WAN1:WAN2), 60% of all Internet sessions will be sent to WAN1 and the remaining 40% will be sent to WAN2.



- **Default (Use main routing table)** – Selecting this option will use the internal routing table to make routing decisions between WAN1 and WAN2 and allow you to device custom policies under the Advanced tab.

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. Web management filtering content services are offered for complimentary along with account sign up. Additional paid upgrades may be available. Services may be subject to change without notice.

Setup your router with Router Limits

Network > VPN

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Services** and click on **Router Limits™**.
3. Choose which mode to enable for Router Limits.
 - **Enabled without bandwidth monitoring** – Enables the standard Router Limits services.
 - **Enabled with bandwidth monitoring (reduces LAN > WAN performance)** – Enables Routers Limits functionality with the additional bandwidth monitoring function.

Note: Enabling the option with bandwidth monitoring will significantly decrease LAN to WAN performance.

Enabled without bandwidth monitoring

Enabled with bandwidth monitoring (reduces LAN > WAN performance)

APPLY

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

Current Status Ready

Pairing Code [REDACTED]

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..

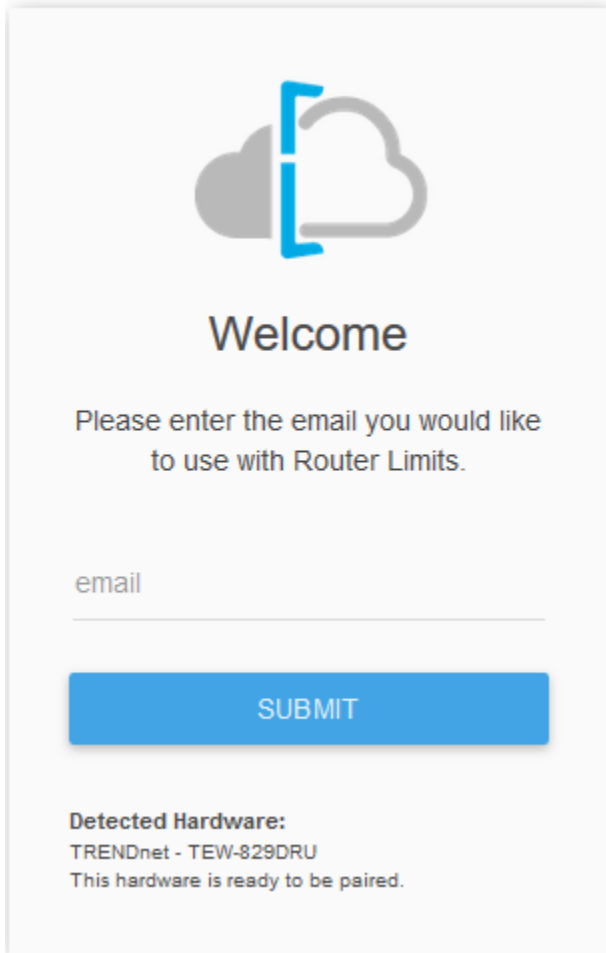
To use our service, you'll need hardware that is Router Limits Enabled.

Do you already have hardware?

Yes, activate my hardware

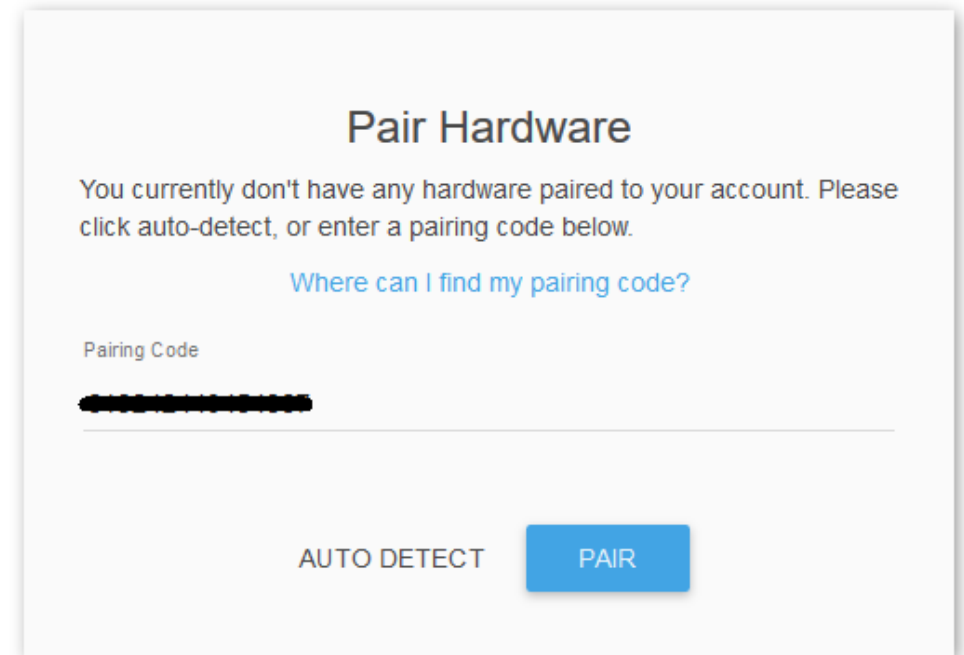
No, I need some

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 and a blue bracket. The text reads: 'Welcome', 'Please enter the email you would like to use with Router Limits.', and 'email' followed by a text input field. A blue 'SUBMIT' button is below the field. At the bottom, 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 is a 'Pairing Code' label and a text input field containing a blacked-out code. At the bottom are 'AUTO DETECT' and 'PAIR' buttons.

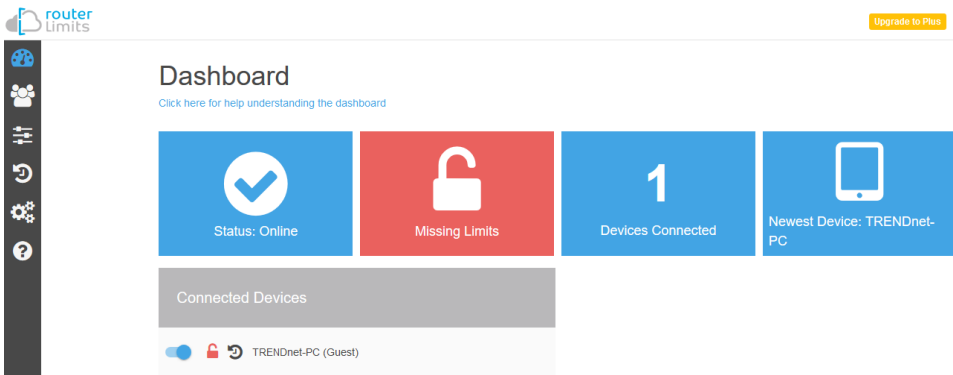
7. After your Router Limits account has been created and your router paired, you will automatically be brought to your web management dashboard. The Current Status on your router will display **Online** that the content management service is running and paired with your online account.

Current Status Online


Router Limits Content Management

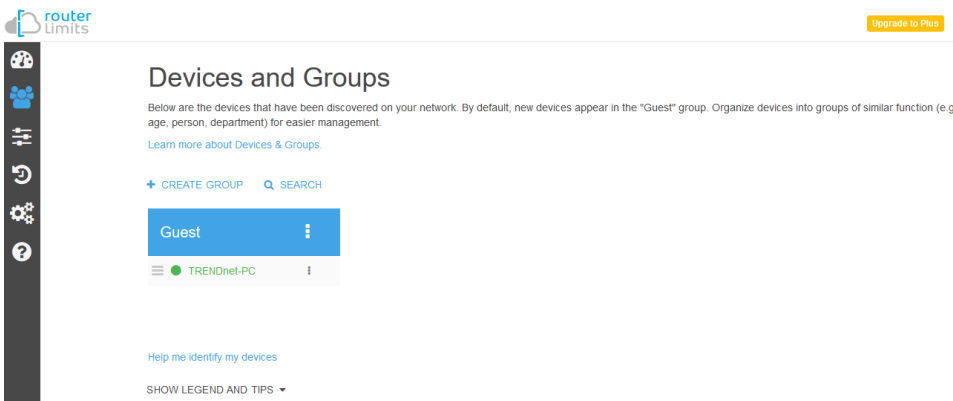
This section will provide a basic overview of the content management pages of your online Router Limits account.

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




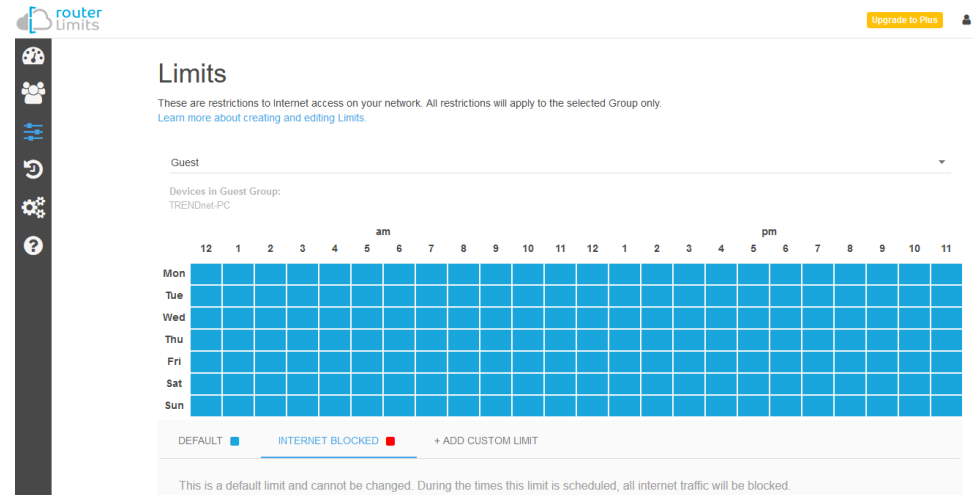
The screenshot shows the Router Limits Dashboard. At the top, there's a navigation bar with the Router Limits logo and an 'Upgrade to Plus' button. The main content area is titled 'Dashboard' and includes a link to help understanding the dashboard. Below this, there are four status cards: 'Status: Online' (green checkmark), 'Missing Limits' (red padlock), 'Devices Connected' (blue card with '1'), and 'Newest Device: TRENDnet-PC' (blue card with a device icon). A 'Connected Devices' section below shows a list with one device: 'TRENDnet-PC (Guest)'.

- 
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.



The screenshot shows the Router Limits 'Devices and Groups' page. It features a navigation bar with the Router Limits logo and an 'Upgrade to Plus' button. The main content area is titled 'Devices and Groups' and includes a link to learn more about devices and groups. Below this, there are buttons for '+ CREATE GROUP' and 'SEARCH'. A list of groups is shown, with 'Guest' selected. Under the 'Guest' group, one device is listed: 'TRENDnet-PC'. At the bottom, there are links for 'Help me identify my devices' and a 'SHOW LEGEND AND TIPS' dropdown.

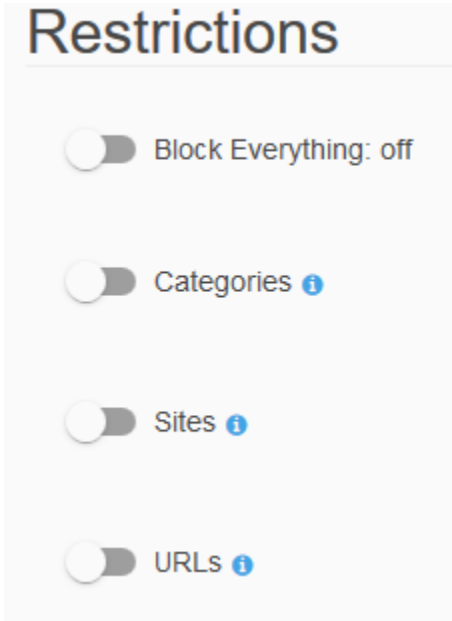
- 
Limits – Content filtering rules and scheduling are configured on this page. By default, all web content is allowed without restrictions. You can define new custom limits with a specific schedule along with a set of different restrictions or configuration options. Each template can be assigned to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



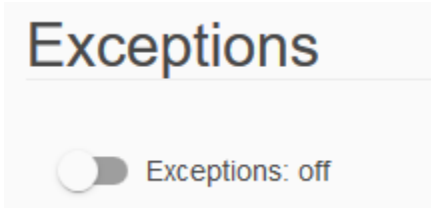
The screenshot shows the Router Limits 'Limits' page. It features a navigation bar with the Router Limits logo and an 'Upgrade to Plus' button. The main content area is titled 'Limits' and includes a link to learn more about creating and editing limits. Below this, there's a dropdown menu for the selected group, currently set to 'Guest'. Underneath, it says 'Devices in Guest Group: TRENDnet-PC'. A calendar grid shows the schedule for the selected group. The grid has columns for hours (12, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11) and rows for days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun). The grid is currently empty, indicating no custom limits are applied. Below the grid, there are buttons for 'DEFAULT', 'INTERNET BLOCKED', and '+ ADD CUSTOM LIMIT'. A note at the bottom states: 'This is a default limit and cannot be changed. During the times this limit is scheduled, all internet traffic will be blocked.'

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.



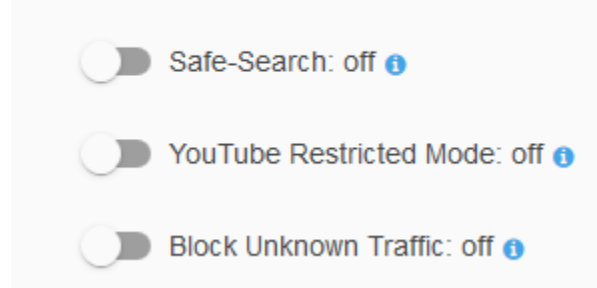
Exceptions – This setting allows you to configure exceptions and allow access.




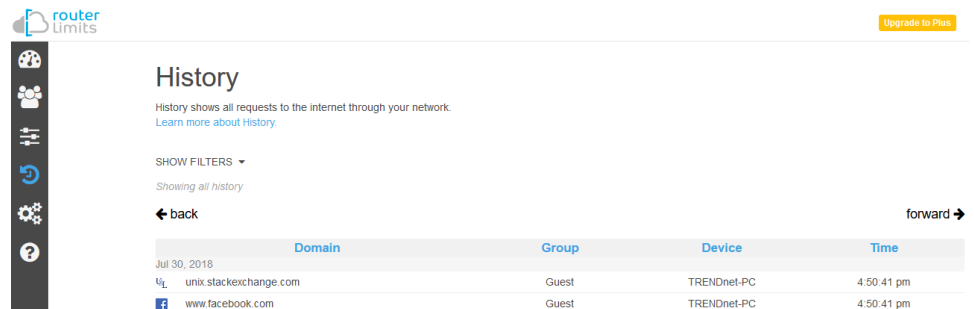
Options

- **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.



- **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

Virtual Private Networking (VPN)

Creating a Virtual Private Network (VPN)

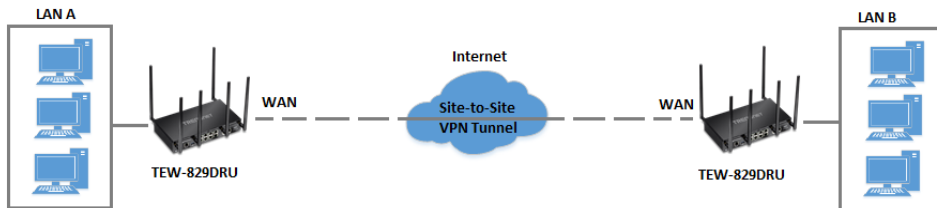
Network > VPN

What is a VPN?

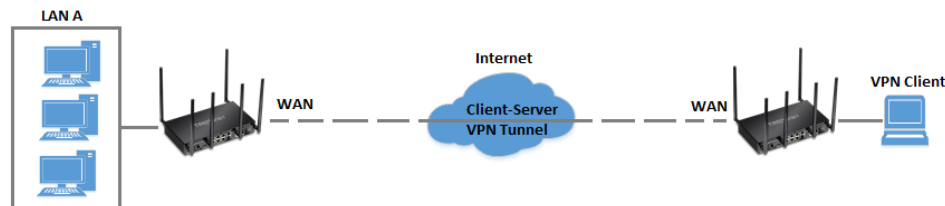
A VPN provides secure communications typically over the Internet by creating a secure tunnel between two or more VPN routers (gateways) also known as a site-to-site VPN or between a single client computer and a VPN router (gateway) also known as a client-server VPN.

On your router, the following types of tunnels can be created:

- **Site-to-Site VPN** – Connects two or more VPN routers (gateways) allowing the LAN network from each router to securely communicate to each other over the Internet. Tunneling Methods: IPsec



- **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: IPsec/SSL(OpenVPN)/PPTP/L2TP/L2TP with IPsec



Tunneling methods supported by your router:

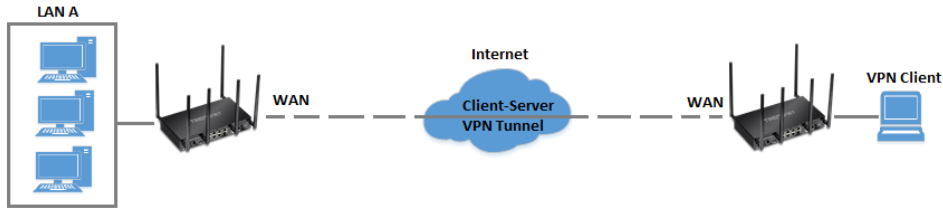
- **SSL (Secure Socket Layer) VPN** – This type of VPN can be used for Client-Server VPN only. There is support for both Layer 3 and Layer 7 network access with SSL VPN but your router only supports Layer 3 access. Additionally, your router utilizes the use of OpenVPN® for SSL VPN. The third party software client is available for free download using the following link for both Windows® and Linux operating systems <https://openvpn.net/index.php/open-source/downloads.html>.
- **IPsec (Internet Protocol Security) VPN** – This type of VPN can be used for either Site-to-Site VPN or Client-Server VPN, however, the most common application for this type is a Site-to-Site VPN. This type of VPN can provide highest degree of security. For a Client-Server VPN, typically, a third party VPN client software is required to be installed and configured and can be difficult when installing and configuring on VPN client computers. This VPN type can provide the highest degree of security.
- **PPTP (Point-to-Point Tunneling Protocol) VPN** – This type of VPN can be used for Client-Server VPN only however both server mode and client mode are supported on your router. Most computer operating systems already include a pre-installed PPTP VPN client software that can be easily configured which eliminates the need for an additional third party VPN client software to be purchased and installed. Since it provides less security overall than IPsec VPN, it is not recommended for a Site-to-Site VPN.
- **L2TP (Layer 2 Tunneling Protocol) VPN** – This type of VPN is very similar to PPTP VPN as it is most commonly used for a Client-Server VPN, pre-installed on most computer operating systems and easy to configure, and provides less overall security than IPsec VPN. Most of the current operating systems with L2TP VPN client software pre-installed use L2TP VPN in conjunction with IPsec VPN to improve the overall security provided. This router does not support the L2TP over IPsec VPN method.

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.

PPTP VPN Server

Network > VPN > PPTP Server

You can enable and configure the PPTP VPN server on your router to allow remote computers or mobile devices with PPTP VPN support to connect securely over the Internet and access the company LAN network.



Setting up the PPTP VPN server

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click **VPN**, and click the **PPTP Server** tab.
3. Under Service Setting, check the **Enable** option to enable the PPTP server.

Enable

4. In the **Local IP** field, enter the LAN IP address. (Default LAN IP: 192.168.10.1)

Note: Entering the LAN IP address as the Local IP of the PPTP server ensures your PPTP VPN clients are able to access the Internet and the router LAN network via full tunneling. If an IP address different from the LAN IP is entered, PPTP VPN clients will be allowed to access router LAN and not the Internet.

Local IP 192.168.10.1

5. In the **Client IP** field, enter an IP address range (within the same LAN IP subnet range) to assign to PPTP VPN clients. By default, the router LAN DHCP server pool is 192.168.10.101-192.168.10.199, therefore, we will assign a range that does not conflict with the DHCP server range such as 192.168.10.10-192.168.10.20.

Client IP 192.168.10.10-192.168.10.20

6. Click the **Authentication** drop-down list and select **MS-CHAPv2**.

Authentication MS-CHAPv2

7. Under the User Account section, enter a profile name for the new user account and click **Add**. (e.g. User1)

User1

ADD

8. Check the **Enable** option and enter a **User name** and **Password** for the new user account. (e.g. User name: user1 / Password: user1)

User Account

Profile	Enable	User name	Password
User1	<input checked="" type="checkbox"/>	<u>user1</u>	<u>.....</u>
		ADD	

9. Click **Apply** and the bottom of the page so save and commit the changes.

APPLY

SAVE

RESET

10. Click on the **Status > Overview** page and under the Network section, make note of your WAN IPv4 addresses to configure the PPTP VPN clients. You can also configure dynamic DNS to use a dynamic DNS hostname instead of dynamic WAN IP address.

Note: For the VPN client computer, you will require a third party PPTP VPN software to be installed configured matching the PPTP VPN settings on your router. Typically, PPTP VPN software is pre-installed with most operating systems. Please refer to your operating system or mobile device User's Guide/Manual for configuring the VPN settings.

Below is a reference of the additional PPTP VPN server settings if you choose to make other configuration changes to these sections.

- **Enable** – Check this option to enable the PPTP VPN server.
- **Local IP** – Enter an IP address for the PPTP VPN server. This should be the same as your LAN IPv4 address to allow both access to LAN network and Internet to VPN clients via full tunneling. (e.g. 192.168.10.1)
- **Client IP** – Enter the IP address pool to distribute to your PPTP VPN clients after they establish VPN connectivity. This should be in the same IPv4 subnet used as your Local IP address. If using the same as the router LAN IP address, make sure to assign a range different from your LAN DHCP server IP range. (e.g. 192.168.10.10-192.168.10.20)
- **MS-DNS 1** – Enter the IPv4 address of the primary DNS server to distribute to PPTP VPN clients after they establish VPN connectivity. This parameter is optional. (e.g. 8.8.8.8)
- **MS-DNS 2** – Enter the IPv4 address of the secondary DNS server to distribute to PPTP VPN clients after they establish VPN connectivity. This parameter is optional. (e.g. 8.8.4.4)
- **MS-WINS 1** – Enter the IPv4 address of the primary WINS server to distribute to PPTP VPN clients after they establish VPN connectivity. This parameter is optional. (e.g. 192.168.10.32)
- **MS-WINS 2** – Enter the IPv4 address of the secondary WINS server to distribute to PPTP VPN clients after they establish VPN connectivity. This parameter is optional. (e.g. 192.168.10.33)
- **Authentication** – Click the drop-down list and select the authentication protocol to use for PPTP VPN authentication, **PAP/CHAP/MS-CHAPv1/MS-CHAPv2**. It is strongly recommended to use **MS-CHAPv2** since it offers the highest degree of security from these options and is supported by most modern computers and mobile devices.

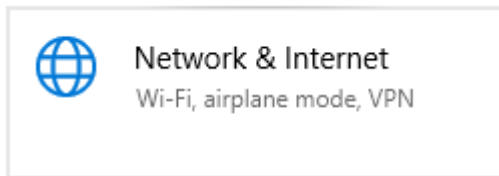
Setting up the PPTP VPN client (Windows)

Note: This procedure provides a basic example how to setup PPTP VPN and establish connectivity using a Windows® 10 client computer. If you are using a different operating system or mobile device, please refer to the user's guide/manual of the third party operating system or device on configuring PPTP VPN. The PPTP VPN settings must match with the settings configured on the router.

1. Click the Start button and click the Settings icon.



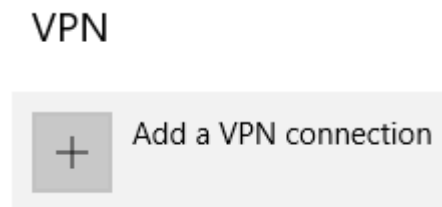
2. Click **Network & Internet**.



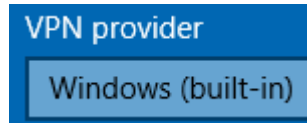
3. Click **VPN** in the left panel.



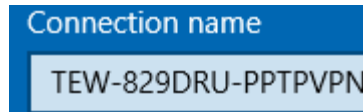
4. Under VPN, click **Add a VPN connection**.



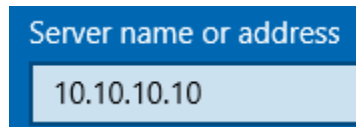
5. Click the **VPN provider** drop-down list and select **Windows (built-in)**.



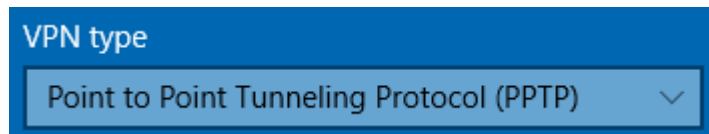
6. Enter a name in the **Connection name** field.



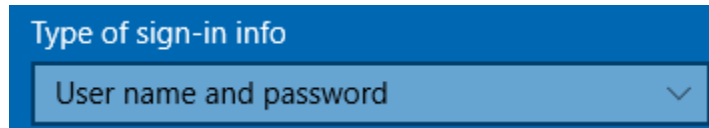
7. Enter the Internet WAN IP address, DNS, or dynamic DNS hostname of your router to connect over the Internet. In the example below, the Internet WAN IP address of the router is 10.10.10.10. In your router, you can check the WAN IP address under **Status > Overview**, under **Network** in the IPv4 status section.



8. Click the **VPN type** drop-down list and select **Point to Point Tunneling Protocol (PPTP)**.



9. Click the **Type of sign-in info** drop-down list and select **User name and password**.



10. You can choose to enter the account credentials in the fields provide for authentication or if not, you will be prompted when attempting to establish PPTP VPN connection to your TEW-829DRU router. Click **Save**.

User name (optional)


Password (optional)

11. Under **VPN**, the new VPN connection will be listed. Click **Connect**.


VPN

VPN

+ Add a VPN connection

 TEW-829DRU-PPTPVPN

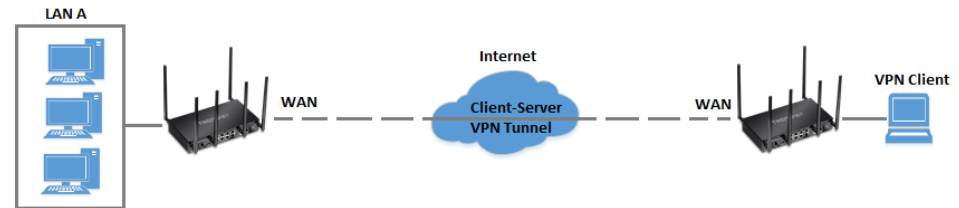
12. The status will display **Connected** if the PPTP VPN connection was successful.

 TEW-829DRU-PPTPVPN
 Connected

L2TP VPN Server

Network > VPN > L2TP Server

You can enable and configure the L2TP VPN server on your router to allow remote computers or mobile devices with L2TP support to connect securely over the Internet and access the company LAN network. It is strongly recommended to enable L2TP VPN server with IPsec instead of L2TP VPN only due to the higher degree of security offered and supported on most modern computers and mobile devices.



Setting up the L2TP VPN server without IPsec encryption

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click **VPN**, and click the **L2TP Server** tab.
3. Under Service Setting, check the **Enable** option to enable the L2TP server.
4. In the **Local IP** field, enter the LAN IP address. (Default LAN IP: 192.168.10.1)

Note: Entering the LAN IP address as the Local IP of the L2TP server ensures your L2TP VPN clients are able to access the Internet and the router LAN network via full tunneling. If an IP address different from the LAN IP is entered, L2TP VPN clients will be allowed to access router LAN and not the Internet.

Local IP 192.168.10.1

5. In the **Client IP** field, enter an IP address range (within the same LAN IP subnet range) to assign to L2TP VPN clients. By default, the router LAN DHCP server pool is 192.168.10.101-192.168.10.199, therefore, we will assign a range that does not conflict with the DHCP server range such as 192.168.10.10-192.168.10.20.

Client IP 192.168.10.10-192.168.10.20

6. Check the **Access LAN** option to ensure VPN clients can access the router LAN interface. **Note:** *If VLANs interfaces are created, they will available under Access vlan.*

Access Lan

7. Click the **Authentication** drop-down list and select **MS-CHAPv2**.

Authentication MS-CHAPv2

8. Under the User Account section, enter a profile name for the new user account and click **Add**. (e.g. User1)

User1

9. Check the **Enable** option and enter a **User name** and **Password** for the new user account. (e.g. User name: user1 / Password: user1)

User Account

Profile	Enable	User name	Password
User1	<input checked="" type="checkbox"/>	<u>user1</u>	<u>.....</u> 
<input type="button" value="ADD"/>			

10. Click **Apply** and the bottom of the page so save and commit the changes.



Setting up the L2TP VPN server with IPsec encryption (PSK)

1. Log into your router management page (see "[Access your router management page](#)" on page 8).

2. Click on **Network**, click **VPN**, and click the **L2TP Server** tab.

3. Under Service Setting, check the **Enable** option to enable the L2TP server.

Enable

4. In the **Local IP** field, enter the LAN IP address. (Default LAN IP: 192.168.10.1)

Note: Entering the LAN IP address as the Local IP of the L2TP server ensures your L2TP VPN clients are able to access the Internet and the router LAN network via full tunneling. If an IP address different from the LAN IP is entered, L2TP VPN clients will be allowed to access only the router LAN and not the Internet.

Local IP 192.168.10.1

5. In the **Client IP** field, enter an IP address range (within the same LAN IP subnet range) to assign to L2TP VPN clients. By default, the router LAN DHCP server pool is 192.168.10.101-192.168.10.199, therefore, we will assign a range that does not conflict with the DHCP server range such as 192.168.10.10-192.168.10.20.

Client IP 192.168.10.10-192.168.10.20

6. Check the **Access LAN** option to ensure VPN clients can access the router LAN interface. **Note:** If VLANs interfaces are created, they will available under Access vlan.

Access Lan

7. Remove any settings for **DNS Server 1 & 2**. These are optional parameters.

8. Click the **Authentication** drop-down list and select **MS-CHAPv2**.

Authentication MS-CHAPv2

9. Under the User Account section, enter a profile name for the new user account and click **Add**. (e.g. User1)

User1

10. Check the **Enable** option and enter a **User name** and **Password** for the new user account. (e.g. User name: user1 / Password: user1)

User Account

Profile	Enable	User name	Password
User1	<input checked="" type="checkbox"/>	<u>user1</u>	<u>.....</u> 
<input type="button" value="ADD"/>			

11. Click **Apply** and the bottom of the page so save and commit the changes.

12. Click on **Network**, click **VPN**, and click the **IPsec** tab.

13. Under Overview, enter a tunnel name and click **Add**. (e.g. L2TPwIPsec)

L2TPwIPsec

143. Click the **Connection type** drop-down list and select **Remote Access (Roadwarrior)**.

Connection type Remote Access (Roadwarrior) ▼

14. Click the **Authentication type** drop-down list and select **L2TP/IPSec PSK**.

Authentication type L2TP/IPSec PSK

15. In the **Local** field enter the local WAN1 IP address and click **Apply**. (e.g. 10.10.10.10)

Local 10.10.10.10
 ⓘ Can be IP or FQDN, e.g.:192.168.123.109

APPLY

16. Under Authentication Key, enter the **Pre-Shared Key** (PSK) for the IPsec VPN tunnel and click **Apply**. (e.g. 1234567890)

Authentication Key

Pre-Shared key 

APPLY

Note: For the VPN client computer, you will require a third party L2TP with IPsec VPN software to be installed configured matching the L2TP with IPsec VPN settings on your router. Typically, L2TP with IPsec VPN software is pre-installed with most operating systems. Please refer to your operating system or mobile device User's Guide/Manual for configuring the VPN settings.

Below is a reference of the additional L2TP VPN server settings if you choose to make other configuration changes to these sections.

- **Enable** – Check this option to enable the L2TP VPN server.
- **Local IP** – Enter an IP address for the L2TP VPN server. This should be different from your LAN IPv4 address and any other VLAN IPv4 addresses you are using on your router. (e.g. 192.168.0.1)
- **Client IP** – Enter the IP address pool to distribute to your L2TP VPN clients after they establish VPN connectivity. This should be in the same IPv4 subnet used as your Local IP address. (e.g. 192.168.0.100-192.168.0.254)
- **Access lan** - Checking this option will allow L2TP VPN clients to access the router LAN IPv4 interface network.
- **Access vlan** – If VLAN IPv4 interfaces are created on your router, they will be displayed and you can allow L2TP VPN clients access to specific VLAN interfaces.
- **DNS Server 1** – Enter the IPv4 address of the primary DNS server to distribute to L2TP VPN clients after they establish VPN connectivity. This parameter is optional. (e.g. 8.8.8.8)
- **DNS Server 2** – Enter the IPv4 address of the secondary DNS server to distribute to L2TP VPN clients after they establish VPN connectivity. This parameter is optional. (e.g. 8.8.4.4)
- **Authentication** – Click the drop-down list and select the authentication protocol to use for L2TP VPN authentication, **PAP/CHAP/MS-CHAPv1/MS-CHAPv2**. It is strongly recommended to use **MS-CHAPv2** since it offer the highest degree of security from these options and is supported by most modern computers and mobile devices.

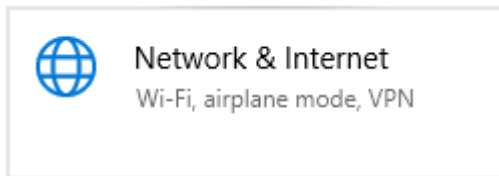
Setting up the L2TP VPN client (Windows) with IPsec encryption (PSK)

Note: This procedure provides a basic example how to setup L2TP with IPsec VPN and establish connectivity using a Windows® 10 client computer. If you are using a different operating system or mobile device, please refer to the user's guide/manual of the third party operating system or device on configuring L2TP with IPsec VPN. The L2TP with IPsec VPN settings must match with the settings configured on the router.

1. Click the Start button and click the Settings icon.



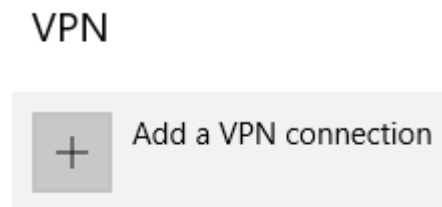
2. Click **Network & Internet**.



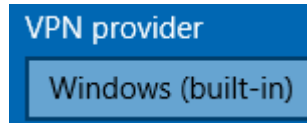
3. Click **VPN** in the left panel.



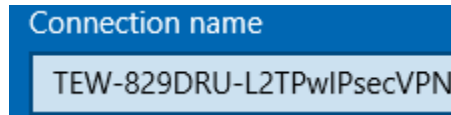
4. Under VPN, click **Add a VPN connection**.



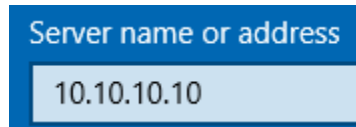
5. Click the **VPN provider** drop-down list and select **Windows (built-in)**.



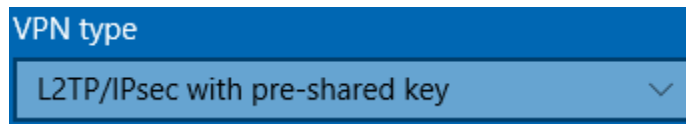
6. Enter a name in the **Connection name** field.



7. Enter the Internet WAN IP address, DNS, or dynamic DNS hostname of your router to connect over the Internet. In the example below, the Internet WAN IP address of the router is 10.10.10.10. In your router, you can check the WAN IP address under **Status > Overview**, under **Network** in the IPv4 status section.



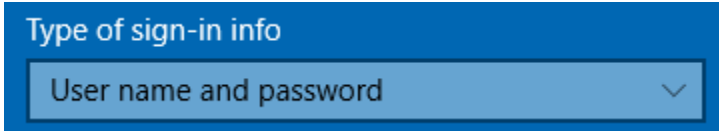
8. Click the **VPN type** drop-down list and select **L2TP/IPsec with pre-shared key**.



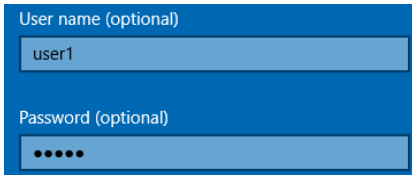
9. Enter the IPsec pre-shared key (PSK).



10. Click the **Type of sign-in info** drop-down list and select **User name and password**.



10. You can choose to enter the account credentials in the fields provide for authentication or if not, you will be prompted when attempting to establish PPTP VPN connection to your TEW-829DRU router. Click **Save**.



11. Under **VPN**, the new VPN connection will be listed. Click **Connect**.

VPN

VPN

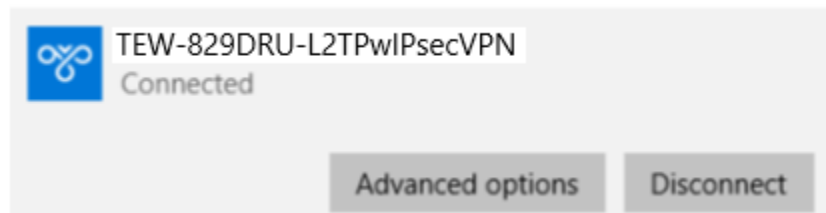


Add a VPN connection



TEW-829DRU-L2TPwIPsecVPN

12. The status will display **Connected** if the PPTP VPN connection was successful.

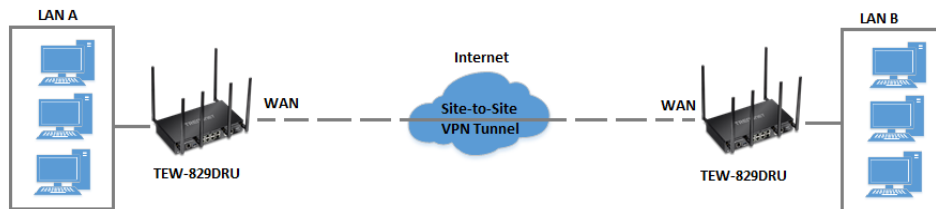


IPsec (Internet Protocol Security)

Setting up IPsec site-to-site VPN (PSK)

Network > VPN > IPsec

To configure and IPsec site-to-site VPN tunnel with pre-shared key (PSK) between two routers:



- Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through your router and make note of the WAN (Internet) IP assigned to both routers under the **Status > Overview** page.

Example:

VPN Router A WAN1 (Internet) IP Address: 10.10.10.10

VPN Router B WAN1 (Internet) IP Address: 10.10.10.20

- Make sure the LAN IP network on each VPN router is a different IP subnet.

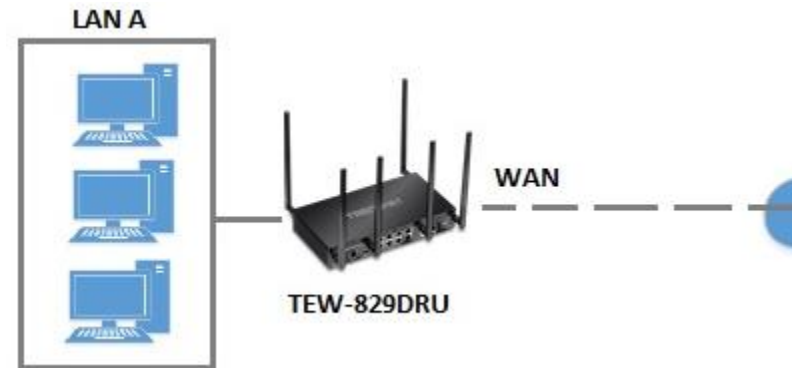
Note: Changing the LAN IP address of your router will change the LAN IP network of your router.

Example:

VPN Router A LAN IP Settings: 192.168.10.1 / 255.255.255.0

VPN Router B LAN IP Settings: 192.168.100.1 / 255.255.255.0

VPN Router A Configuration



1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click **VPN**, and click the **IPsec** tab.
3. Under Overview, enter a tunnel name and click **Add**. (e.g. Tunnel1)

Tunnel1

4. Click the Connection type drop-down list and select **Site-to-Site**.


Connection type **Site-to-Site**


5. Click the Authentication type drop-down list and select **IPSec IKEv2 PSK**.

Authentication type **IPSec IKEv2 PSK**

6. In the **Local** field, enter the local WAN1 IP address. (e.g. 10.10.10.10) This can also be a domain name (ex: dynamic DNS host name)


Local 10.10.10.10
Can be IP or FQDN, e.g.:192.168.123.109


7. In the **Local subnet** field, enter the local LAN IP subnet. (e.g. 192.168.10.0/24) You can add additional local subnets by click the add icon  (e.g. 192.168.20.0/24)

Local subnet 192.168.10.0/24 
If you want to use split tunnel(It is only for IKEv2), set the access subnet. e.g.:192.168.10.0/24
 If you want to redirect to Internet, set the local subnet as 0.0.0.0/0



8. In the **Remote** field, enter the remote WAN1 IP. (e.g. 10.10.10.20) This can also be a domain name (ex: dynamic DNS host name)

Remote 10.10.10.20
Can be IP or FQDN, e.g.:192.168.123.10.

9. In the **Remote subnet** field, enter the remote LAN IP subnet. (e.g. 192.168.100.0/24) and click **Apply**. You can add additional local subnets by click the add icon  (e.g. 192.168.120.0/24)


Remote subnet 192.168.100.0/24 
e.g.:192.168.20.0/24
APPLY

Based on the example, the network settings will be the following:

Router A WAN1 IP Address	Local	<u>10.10.10.10</u>
		<small>Can be IP or FQDN, e.g.:192.168.123.109</small>
	Local ID	<u></u>
		<small>e.g.:C=TW, O=peer1, CN=vpn.peer1.org, C:Country Code, ST:State or Province Name, L:Local Name, O:O</small>
Router A LAN IP Network	Local subnet	<u>192.168.10.0/24</u> 
		<small>If you want to use split tunnel(It is only for IKEv2), set the acc If you want to redirect to Internet, set the local subnet as 0.0.0.0/0</small>
Router B WAN1 IP Address	Remote	<u>10.10.10.20</u>
		<small>Can be IP or FQDN, e.g.:192.168.123.10.</small>
	Remote ID	<u></u>
		<small>e.g.:C=TW, O=peer2, CN=vpn.peer2.org, C:Country Code, ST:State or Province Name, L:Local Name, O:O</small>
Router B LAN IP Network	Remote subnet	<u>192.168.100.0/24</u> 
		<small>e.g.:192.168.20.0/24</small>

10. Under Authentication Key, enter the **Pre-Shared Key** (PSK) for the IPsec VPN tunnel and click **Apply**. (e.g. 1234567890)

Authentication Key

Pre-Shared key 
APPLY

VPN Router B Configuration



1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click **VPN**, and click the **IPsec** tab.
3. Under Overview, enter a tunnel name and click **Add**. (e.g. *Tunnel1*)

Tunnel1

4. Click the Connection type drop-down list and select **Site-to-Site**.


Connection type Site-to-Site ▼


5. For the Authentication type drop-down list and select **IPSec IKEv2 PSK**.

Authentication type IPSec IKEv2 PSK ▼

6. For the **Local** field, enter the local WAN1 IP address. (e.g. *10.10.10.20*) This can also be a domain name (ex: dynamic DNS host name)


Local 10.10.10.20
 ⓘ Can be IP or FQDN, e.g.:192.168.123.109

7. For the **Local subnet** field, enter the local LAN IP subnet. (e.g. *192.168.100.0/24*) You can add additional local subnets by click the add icon  (e.g. *192.168.120.0/24*)

Local subnet 192.168.100.0/24 
 ⓘ If you want to use split tunnel(It is only for IKEv2), set the access subnet. e.g.:192.168.10.0/24
 If you want to redirect to Internet, set the local subnet as 0.0.0.0/0

8. For the **Remote** field, enter the remote WAN1 IP. (e.g. *10.10.10.10*) This can also be a domain name (ex: dynamic DNS host name)

Remote 10.10.10.10
 ⓘ Can be IP or FQDN, e.g.:192.168.123.10.

9. For the **Remote subnet** field, enter the remote LAN IP subnet. (e.g. *192.168.10.0/24*) and click **Apply**. You can add additional local subnets by click the add icon  (e.g. *192.168.20.0/24*)

Remote subnet 192.168.10.0/24
 ⓘ e.g.:192.168.20.0/24

Based on the example, the network settings will be the following:

Router B WAN1 IP Address	Local	10.10.10.20
		<small>Can be IP or FQDN, e.g.:192.168.123.109</small>
	Local ID	
		<small>e.g.:C=TW, O=peer1, CN=vpn.peer1.org, C:Country Code, ST:State or Province Name, L:Local Name, O:</small>
Router B LAN IP Network	Local subnet	192.168.100.0/24
		<small>If you want to use split tunnel(It is only for IKEv2), set the ac If you want to redirect to Internet, set the local subnet as 0.0.0</small>
Router A WAN1 IP Address	Remote	10.10.10.10
		<small>Can be IP or FQDN, e.g.:192.168.123.10.</small>
	Remote ID	
		<small>e.g.:C=TW, O=peer2, CN=vpn.peer2.org, C:Country Code, ST:State or Province Name, L:Local Name, O:</small>
Router A LAN IP Network	Remote subnet	192.168.10.0/24
		<small>e.g.:192.168.20.0/24</small>

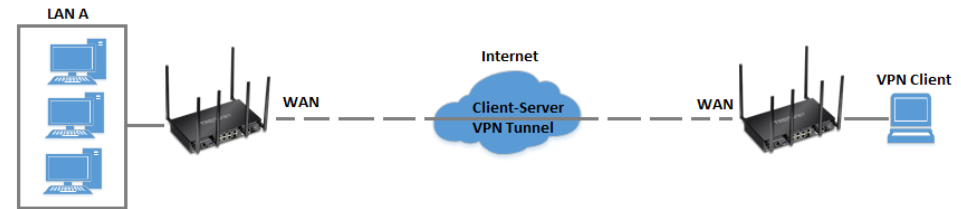
10. Under Authentication Key, enter the **Pre-Shared Key** (PSK) for the IPsec VPN tunnel and click **Apply**. (e.g. 1234567890)

Authentication Key

Pre-Shared key

APPLY

Setting up IPsec server VPN (PSK with xAUTH)



1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click **VPN**, and click the **IPsec** tab.
3. Under Overview, enter a tunnel name and click **Add**. (e.g. *IPsec_Server*)

IPsec_Server **ADD**

4. Click the Connection type drop-down list and select **Remote Access (Roadwarrior)**.

Connection type **Remote Access (Roadwarrior)**


5. For the Authentication type drop-down list and select **IPSec XAUTH PSK**.

Authentication type **IPSec XAUTH PSK**


6. For the **Local** field, enter the local WAN1 IP address. (e.g. 10.10.10.10) This can also be a domain name (ex: dynamic DNS host name)

Local

 Can be IP or FQDN, e.g.:192.168.123.109

7. In the **Local subnet** field, enter the local LAN IP subnet. (e.g. 192.168.10.0/24) You can add additional local subnets by click the add icon  (e.g. 192.168.20.0/24)

Local subnet

 If you want to use split tunnel(It is only for IKEv2), set the access subnet. e.g.:192.168.10.0/24
If you want to redirect to Internet, set the local subnet as 0.0.0.0/0

8. In the **Assign IP range** field, enter the IP address subnet to assign the IPsec VPN client devices upon connectivity and click **Apply**. (e.g. 192.168.30.0/24). The IP address range/subnet should be different from the local LAN IP subnets and also different from the remote client side.

Assign IP range

 e.g.:192.168.30.0/24

APPLY

9. Under Authentication Key, enter the **Pre-Shared Key** (PSK) for the IPsec VPN tunnel. (e.g. 1234567890)

Authentication Key

Pre-Shared key



10. Under XAUTH Account, enter the **User name** and **Password** for the account, then click **Add**. Click **Apply** to save and commit the changes.

New user Name

Password

ADD

APPLY

Note: For the VPN client computer, you will require a third party IPsec VPN software to be installed configured matching the IPsec VPN settings on your router. Please refer to your third party IPsec VPN User's Guide/Manual for configuring the VPN settings.

Below is a reference of the additional IPsec VPN settings if you choose to make other configuration changes to these sections.

- **Certificate List** – Used for IPsec tunnels requiring the RSA authentication type. You can create or import IPsec certificates under Administrator > Certificate Management.
- **Local ID/Remote ID** – This parameter is only required for IPsec tunnels with the RSA authentication type. If not using RSA, this additional parameter can be added for extra security in identification of the IPsec peers. (e.g. *Local ID assigned CN=vpnsite1.trendnet.com and Remote ID CN=vpnsite2.trendnet.com*)
- **Authentication Key** – This is the PSK (pre-shared key) used for IPsec tunnels requiring the PSK authentication type.
- **XAUTH Account** – This parameter provides an additional layer of security by requiring a user name and password for authentication of the IPsec tunnel and required for IPsec XAUTH PSK tunnel type.
- **EAP Account** – This parameter provides an additional layer of security by requiring a user name and password for authentication of the IPsec tunnel and required for IPsec IKEv2 RSA EAP_MS_CHAPv2 tunnel type.

Phase 1 settings

- **Phase 1 auto configure** – Checking this option automatically configures the IPsec Phase 1 parameters for the tunnel. Unchecking this option allows you to manually set the IPsec Phase 1 parameters.
 - **Cipher algorithm** – The encryption/cipher algorithm used for IPsec phase 1. AES 256-bit offers the highest degree security.
 - **Hash algorithm** – The authentication/hash algorithm used for IPsec phase 1. SHA2 256-bit offers highest degree of security.
 - **DH exchange** – The Diffie-Hellman group used for IPsec phase 1 key exchange. Group 14 (2048 bit) offers the highest degree of security.

Phase 2 settings

- **Phase 2 auto configure** – Checking this option automatically configures the IPsec Phase 2 parameters for the tunnel. Unchecking this option allows you to manually set the IPsec Phase 2 parameters.
 - **Transform algorithm** – The encryption/cipher algorithm used for IPsec phase 2. AES 256-bit offers the highest degree security.
 - **Hash algorithm** – The authentication/hash algorithm used for IPsec phase 2. SHA2 256-bit offers highest degree of security.

- **PFS exchange** – The Perfect Forward Secrecy group used for IPsec phase 2. PFS adds additional security to the IPsec tunnel by forcing re-negotiation of phase 1 keys for every new pair of phase 2 SAs (security associations) established. Group 14 (2048 bit) offers the highest degree of security.
- **DPD (Dead Peer Detection)** – DPD implements a keep alive/monitoring function to the IPsec tunnel to check if IPsec peers are still active and responding.
 - **DPD action** - Sets the action when IPsec peers do not respond to DPD messages within the DPD delay interval. **Clear** will automatically close the IPsec connection and will not attempt to re-negotiate the connection, **Hold** will keep the connection and will attempt to re-negotiate the connection on-demand only when new traffic is sent through the tunnel, **Restart** will immediately force re-negotiation of the connection.
 - **DPD delay** – Sets the time interval when DPD messages are sent to IPsec peers to check the alive status.
 - **DPD timeout** – Sets the maximum timeout interval when IPsec connections are completely deleted due to inactivity.

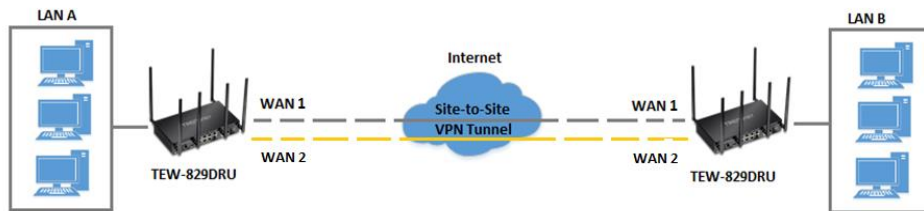
Setting up IPsec site-to-site VPN Failover (PSK)

Note: IPsec VPN failover is only supported on firmware 1.0.0.33 or above. This configuration will only work when multiple WAN configuration is set to WAN1 (Failover to WAN2), WAN2 (Failover to WAN1), Load Balance (weight cannot be set to 50%:50%).

Network > VPN > IPsec

VPN failover configuration allows you to add redundancy/fault tolerance to your IPsec VPN tunnel connectivity.

To configure and IPsec site-to-site VPN tunnel failover with pre-shared key (PSK) between two routers:



- Ensure that your router is connected to the Internet and computers and devices are able to access the Internet through the WAN1 and WAN2 interfaces on your router and make note of the WAN1 and WAN2 IP addresses assigned to both routers under the **Status > Overview** page. In this example, we will assume the following static IP WAN info. and LAN IP settings below.

Example:

VPN Router A WAN1 (Internet) IP Address: 10.10.10.85 / 255.255.255.192

VPN Router A WAN2 (Internet) IP Address: 10.10.10.130 / 255.255.255.192

VPN Router B WAN1 (Internet) IP Address: 172.16.0.1 / 255.255.255.192

VPN Router B WAN1 (Internet) IP Address: 172.16.0.62 / 255.255.255.192

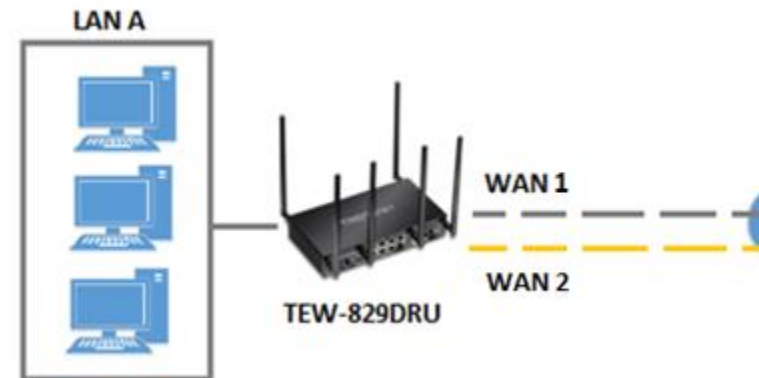
- Make sure the LAN IP network on each VPN router is a different IP subnet.
Note: Changing the LAN IP address of your router will change the LAN IP network of your router.

Example:

VPN Router A LAN IP Settings: 192.168.200.1 / 255.255.255.0

VPN Router B LAN IP Settings: 192.168.210.1 / 255.255.255.0

VPN Router A Configuration



1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click **Firewall**, and click the **General Settings** tab.
3. Check the **Enable** under WAN Ping Respond and click **Apply** to save and commit the configuration changes.

WAN Ping Respond

Enable

4. Click on **Network** and click on **Multiple WAN**.

5. Under the Link Tracking section, check **Enable Tracking** on both **WAN1** and **WAN2**, and enter an IP address or IP addresses on the Internet to check for connectivity and quickly determine if the WAN interface is up or down (e.g. 8.8.8.8). Set the **Ping Interval** to **3 seconds**, and **Fail Count** to **1** for both **WAN1** and **WAN2** and click **Apply** to save and commit the configuration changes.


Link Tracking

Link Tracking is used to determine if the link is up or down by ping the tracking IP. Disable link tracking implies to assume interface is always on

WAN1

Enable Tracking	<input checked="" type="checkbox"/>
Tracking IP	8.8.8.8 
Ping Interval	3 seconds ▼
Fail Count	1 ▼
<small>ⓘ Interface will be deemed down after this many failed ping tests</small>	

WAN2

Enable Tracking	<input checked="" type="checkbox"/>
Tracking IP	8.8.8.8 
Ping Interval	3 seconds ▼
Fail Count	1 ▼
<small>ⓘ Interface will be deemed down after this many failed ping tests</small>	

6. Click on **Network**, click **VPN**, and click the **IPsec** tab.

7. Under Overview, enter a tunnel name and click **Add**. (e.g. Tunnel1)

Tunnel1	ADD
---------	------------

8. Click the Connection type drop-down list and select **Site-to-Site**.

Connection type	Site-to-Site ▼
-----------------	----------------

9. Click the Failover drop-down list and select **Enable**.


Failover	Enable ▼
----------	----------

10. Click the Authentication type drop-down list and select **IPSec IKEv2 PSK**.


Authentication type	IPSec IKEv2 PSK ▼
---------------------	-------------------

11. In the **Local** field, enter the local WAN1 IP address. (e.g. 10.10.10.85) This can also be a domain name (ex: dynamic DNS host name)

Local	10.10.10.85
-------	-------------

12. Click  to add an additional IP address and enter the local WAN2 IP address (e.g. 10.10.10.130).


Local	10.10.10.85 
	10.10.10.130 

13. In the **Local subnet** field, enter the local LAN IP subnet. (e.g. 192.168.200.0/24) You can add additional local subnets by click the add icon  (e.g. 192.168.20.0/24)

Local subnet	192.168.200.0/24
--------------	------------------

14. In the **Remote** field, enter the remote WAN1 IP address. (e.g. 172.16.0.1) This can also be a domain name (ex: dynamic DNS host name)

Remote	172.16.0.1
--------	------------

15. Click  to add an additional IP address and enter the remote WAN2 IP address (e.g. 172.16.0.80).

Remote	172.16.0.1	
	172.16.0.80	

16. In the **Remote subnet** field, enter the remote LAN IP subnet. (e.g. 192.168.210.0/24) and click **Apply**. You can add additional local subnets by click the add icon (e.g. 192.168.30.0/24)

Remote subnet	192.168.210.0/24	
---------------	------------------	--

APPLY

Based on the example, the network settings will be the following:

Local	10.10.10.85	Router A WAN1 IP Address	
	10.10.10.130	Router A WAN2 IP Address	
	Can be IP or FQDN, e.g.:192.168.123.109		
Local ID	e.g.:C=TW, O=peer1, CN=vpn.peer1.org, C:Country Code, ST:State or Province Name, L:Local Name, O:Organization		
Local subnet	192.168.200.0/24	Router A LAN IP Network	
	If you want to use split tunnel(It is only for IKEv2), set the access subnet. If you want to redirect to Internet, set the local subnet as 0.0.0.0/0		
Remote	172.16.0.1	Router B WAN1 IP Address	
	172.16.0.80	Router B WAN2 IP Address	
	Can be IP or FQDN, e.g.:192.168.123.10.		
Remote ID	e.g.:C=TW, O=peer2, CN=vpn.peer2.org, C:Country Code, ST:State or Province Name, L:Local Name, O:Organization		
Remote subnet	192.168.210.0/24	Router B LAN IP Network	
	e.g.:192.168.20.0/24		

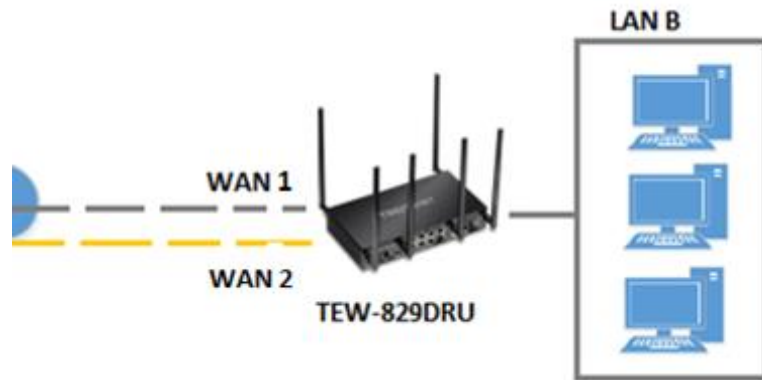
17. Under Authentication Key, enter the **Pre-Shared Key** (PSK) for the IPsec VPN tunnel and click **Apply**. (e.g. 1234567890)

Authentication Key

Pre-Shared key	
----------------	-------	--

APPLY

VPN Router B Configuration



1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Network**, click **Firewall**, and click the **General Settings** tab.
3. Check the **Enable** under WAN Ping Respond and click **Apply** to save and commit the configuration changes.

WAN Ping Respond

Enable

4. Click on **Network** and click on **Multiple WAN**.

5. Under the Link Tracking section, check **Enable Tracking** on both **WAN1** and **WAN2**, and enter an IP address or IP addresses on the Internet to check for connectivity and quickly determine if the WAN interface is up or down (e.g. 8.8.8.8). Set the **Ping Interval** to **3 seconds**, and **Fail Count** to **1** for both **WAN1** and **WAN2** and click **Apply** to save and commit the configuration changes.

Link Tracking

Link Tracking is used to determine if the link is up or down by ping the tracking IP. Disable link tracking implies to assume interface is always on

WAN1

Enable Tracking

Tracking IP

Ping Interval

Fail Count

Interface will be deemed down after this many failed ping tests

WAN2

Enable Tracking

Tracking IP

Ping Interval

Fail Count

Interface will be deemed down after this many failed ping tests

6. Click on **Network**, click **VPN**, and click the **IPsec** tab.

7. Under Overview, enter a tunnel name and click **Add**. (e.g. Tunnel1)

8. Click the Connection type drop-down list and select **Site-to-Site**.

Connection type

9. Click the Failover drop-down list and select **Enable**.


Failover

10. Click the Authentication type drop-down list and select **IPSec IKEv2 PSK**.


Authentication type IPSec IKEv2 PSK

11. In the **Local** field, enter the local WAN1 IP address. (e.g. 172.16.0.1) This can also be a domain name (ex: dynamic DNS host name)

Local 172.16.0.1

12. Click  to add an additional IP address and enter the local WAN2 IP address (e.g. 172.16.0.80).


Local 172.16.0.1 
172.16.0.80 

13. In the **Local subnet** field, enter the local LAN IP subnet. (e.g. 192.168.210.0/24) You can add additional local subnets by click the add icon  (e.g. 192.168.30.0/24)


Local subnet 192.168.210.0/24

14. In the **Remote** field, enter the remote WAN1 IP address. (e.g. 172.16.0.1) This can also be a domain name (ex: dynamic DNS host name)

Remote 10.10.10.85

15. Click  to add an additional IP address and enter the remote WAN2 IP address (e.g. 172.16.0.80).







Remote 10.10.10.85
10.10.10.130

16. In the **Remote subnet** field, enter the remote LAN IP subnet. (e.g. 192.168.200.0/24) and click **Apply**. You can add additional local subnets by click the add icon  (e.g. 192.168.20.0/24)

Remote subnet 192.168.200.0/24 

APPLY

Based on the example, the network settings will be the following:

Local	172.16.0.1	Router B WAN1 IP Address	
	172.16.0.80	Router B WAN2 IP Address	
<small>Can be IP or FQDN, e.g.:192.168.123.109</small>			
Local ID	<small>e.g.:C=TW, O=peer1, CN=vpn.peer1.org, C:Country Code, ST:State or Province Name, L:Local Name, O:Organization Na</small>		
Local subnet	192.168.210.0/24	Router B LAN IP Network	
<small>If you want to use split tunnel(It is only for IKEv2), set the access subnet. e.g If you want to redirect to Internet, set the local subnet as 0.0.0.0/0</small>			
Remote	10.10.10.85	Router A WAN1 IP Address	
	10.10.10.130	Router A WAN2 IP Address	
<small>Can be IP or FQDN, e.g.:192.168.123.10.</small>			
Remote ID	<small>e.g.:C=TW, O=peer2, CN=vpn.peer2.org, C:Country Code, ST:State or Province Name, L:Local Name, O:Organization Na</small>		
Remote subnet	192.168.200.0/24	Router A LAN IP Network	
<small>e.g.:192.168.20.0/24</small>			

17. Under Authentication Key, enter the **Pre-Shared Key** (PSK) for the IPsec VPN tunnel and click **Apply**. (e.g. 1234567890)

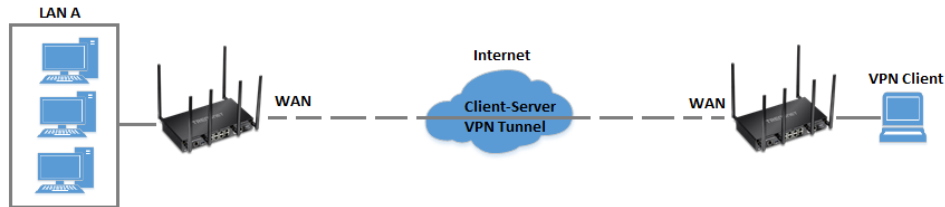
Authentication Key

Pre-Shared key 

APPLY

Secure Socket Layer VPN (SSL) / OpenVPN

Network > VPN > OpenVPN



SSL VPN Server Setup

1. Log into your router management page (see "[Access your router management page](#)" on page 8).

2. Click on **Administrator** and click **Certificate Management**.

3. Enter a name for the certificate to use for SSL VPN and click **Add**. (e.g. *SSL-VPN*)

SSL-VPN

4. Click the **Used for** drop-down list and select **OpenVPN**.

Used for OpenVPN

5. In the **Country Code** field, enter the two letter country code. (e.g. *US*)

Country Code US

6. In the **State or Province Name** field, enter the full name of the state or province. (e.g. *California*)

State or Province Name California

7. In the **Local Name** field, enter the city name. (e.g. *Torrance*)

Local Name Torrance

8. In the **Organization Name** field, enter your company name (e.g. *TRENDnet*)

Organization Name TRENDnet

9. In the **Org. Unit** field, enter the section, group, or department. (e.g. *IT*)

Org. Unit IT

10. In the **Email Address** field, enter the email address used for the certificate. (e.g. tew-829dru@trendnet.com)

Email Address tew-829dru@trendnet.com

11. In the **Validity Days** field, enter the number of days the certificate will be valid and click **Apply** to save and commit the changes.. (e.g. *100*)

Validity Days 100

12. Click on **Network**, click **VPN**, and click the **OpenVPN** tab.

13. Check the **Enable** option to enable the SSL VPN server.

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.

Enable

14. In the **Certificate List** drop-down list, select the name of the OpenVPN certificate you created and click **Apply** to save and commit the changes. (e.g. *SSL-VPN*)

Certificate List SSL-VPN ▼

15. Next to Client configuration file, click **Export** to download the configuration files for the VPN client computer.

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

Folder paths for SSL VPN client configuration files:

Windows: C:\Program Files\OpenVPN\config

Linux: /etc/openvpn

Below is a reference of the additional SSL VPN settings if you choose to make other configuration changes to these sections.

Note: Changing any settings will require you to export a new client configuration file.

- **Port** – Used to change the default SSL VPN server port.
- **Server** – Used to change the default IP address subnet and IP address range to distribute to SSL VPN clients.
- **Proto** – Used to change the default protocol. UDP or TCP.
- **Connect Type** – Changing this setting will change the access level of your SSL VPN clients.
 - **LAN Access** – This setting will allow your SSL VPN clients access to your LAN network and the Internet.
 - **Internet Redirect** – This setting will allow your SSL VPN clients access only the Internet only via full tunneling but no access to your LAN network
- **Cipher** – Select the cipher/encryption algorithm used for SSL VPN client connections. AES-256-CBC offers the highest degree security.
- **Auth** – The authentication/hash algorithm used for SSL VPN client connections. SHA256 offers highest degree of security.
- **Enable client authentication** – Checking this option will require additional security by means of user name and password authentication in addition to the standard encryption/authentication protocols. You will need to add a user name and password under **Client Authentication Account**.

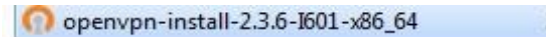
SSL VPN Client Setup (Windows)

1. Make sure to copy or move the configuration files downloaded from your router to the VPN client computer and that your client computer has access to the Internet.

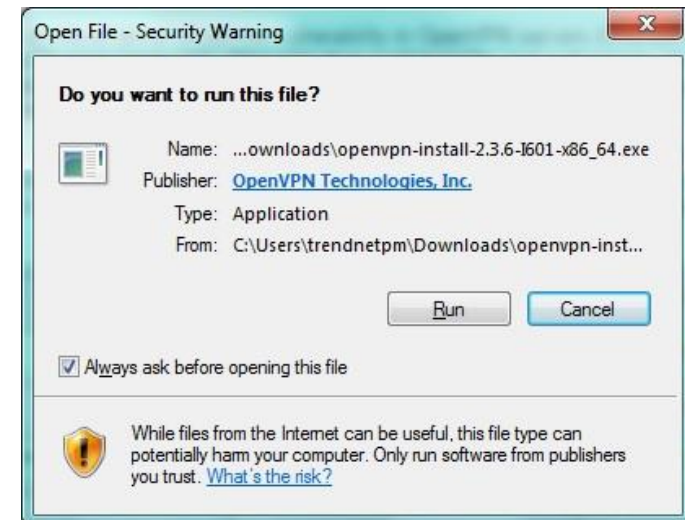
2. Download the appropriate OpenVPN software version for your operating system from the following URL: <https://openvpn.net/index.php/open-source/downloads.html>

Note: Please note there is also a link in the description in the router management page under *Advanced > Setup > VPN*.

3. Once you have downloaded the software, navigate to the location where you downloaded the file and double click to start the installation.

 openvpn-install-2.3.6-I601-x86_64

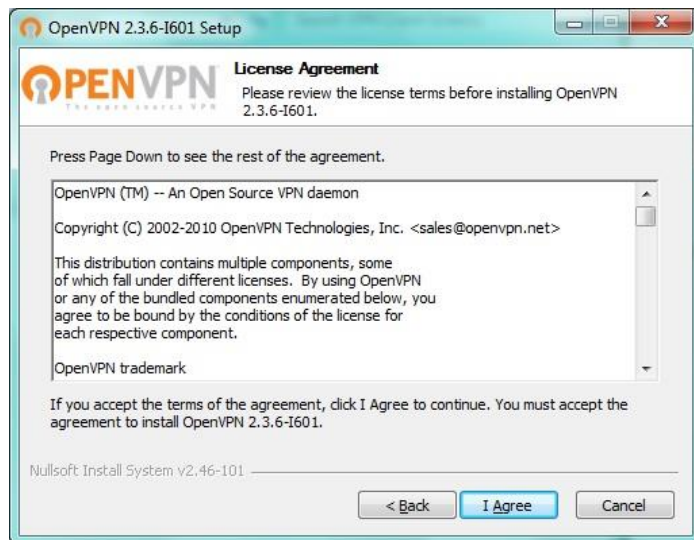
4. If prompted to run the file, click **Run**.



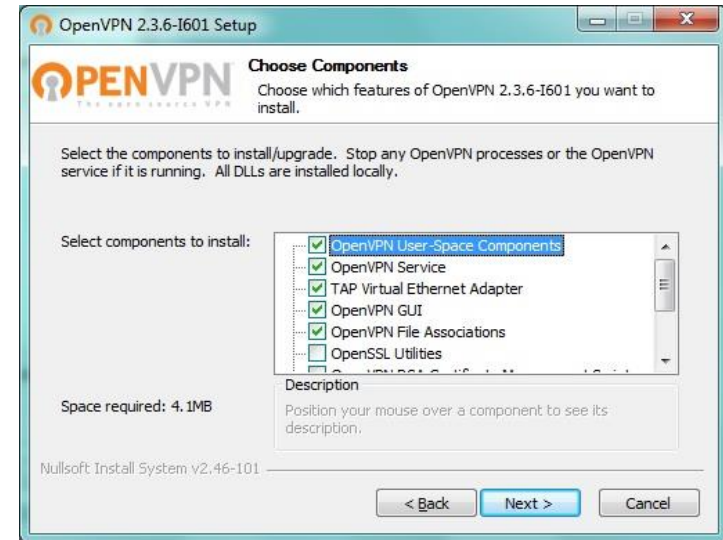
5. At the installation window, click **Next**.



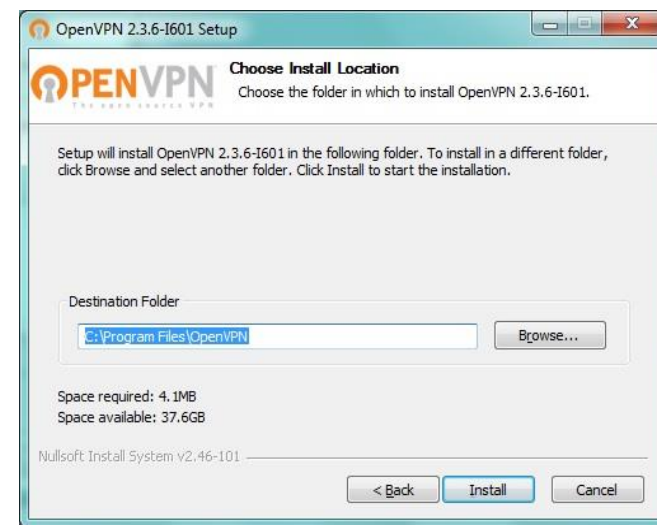
6. At the license agreement window, review the license agreement and click **I Agree**.



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



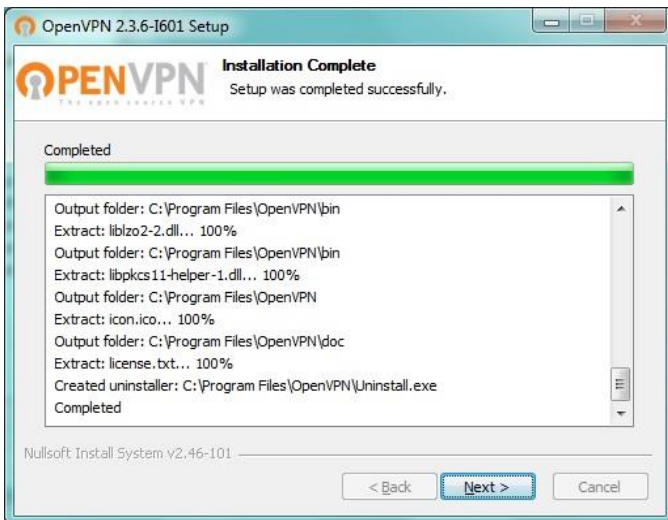
8. At the install location window, click **Install**.



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



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



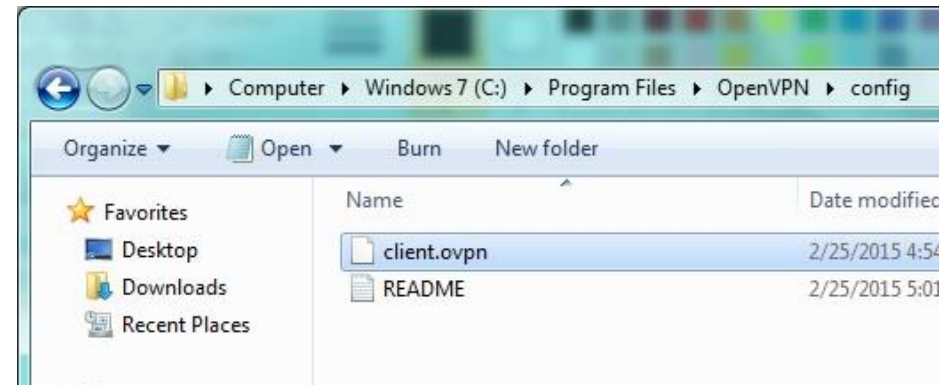
11. Make sure to uncheck the "Show Readme" and "Start OpenVPN GUI" options and click **Finish**.



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



C:\Program Files\OpenVPN\config



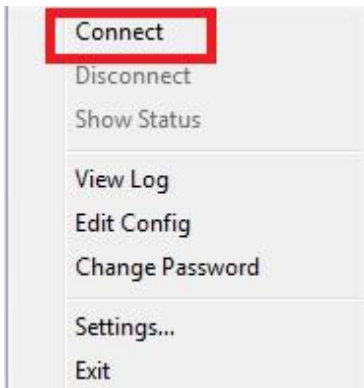
13. Double-click on the OpenVPN GUI shortcut on your desktop to start the OpenVPN Client software.



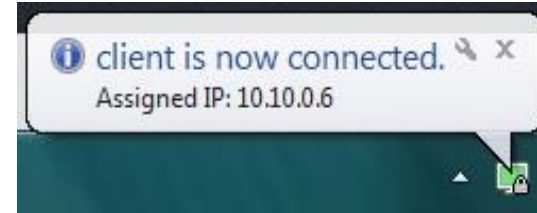
14. The OpenVPN system tray icon will appear in the bottom right corner. Right-click the icon to display the configuration menu.



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**.

Certificate Management

Administrator > Certificate Management


The certificate management allows you to create, import, and export security certificates used for IPsec RSA and SSL VPN (OpenVPN) identification and authentication in IPsec RSA or SSL VPN (OpenVPN) configuration.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Administrator** and click on **Certificate Management**.
3. Under Local Certificates, enter a name for the certificate and click **Add**. (e.g. *IPsecVPN* or *OpenVPN*)
4. Click the **Used for** drop-down list and select the appropriate VPN method the certificate will be used for, **IPsec** or **OpenVPN**.
5. Review the settings below. When complete, click **Apply** to save and commit your changes. After you have created the appropriate VPN certificate, the certificate will be available under the IPsec or Open VPN configuration settings under Network > VPN.

IPsec – Below are the parameters you can set for the certificate. The only required parameters for an IPsec RSA certificate are Common Name (Server), Common Name (Client), and Valid Days.

- **Certificate Name** – Enter the name for the certificate.
- **Used for** – Click the drop-down list and select **IPsec**.
- **Country Code** – Enter the 2 letter country code for the certificate. (e.g. US)
Note: Setting this parameter is optional for IPsec VPN RSA.
- **State or Province Name** – Enter the name of the state or province for the certificate. (e.g. California)
Note: Setting this parameter is optional for IPsec VPN RSA.
- **Local Name** – Enter the name of the city for the certificate. (e.g. Torrance)
Note: Setting this parameter is optional for IPsec VPN RSA.
- **Organization Name** – Enter the company name for the certificate (e.g. TRENDnet)
Note: Setting this parameter is optional for IPsec VPN RSA.
- **Org. Unit** – Enter the department or group name for the certificate (e.g. IT)
Note: Setting this parameter is optional for IPsec VPN RSA.
- **Email Address** – Enter the email address contact for the certificate (e.g. xxxxx@trendnet.com)
Note: Setting this parameter is optional for IPsec VPN RSA
- **Common Name (Server)** – Enter the host + domain name of first site/IPsec tunnel endpoint. (e.g. site1.ipsecvpn.local)
Note: Setting this parameter is required for IPsec VPN RSA
- **Common Name (Client)** – Enter the host + domain name of the second site/IPsec tunnel endpoint. (e.g. site2.ipsecvpn.local)
Note: Setting this parameter is required for IPsec VPN RSA
- **Valid Days** – Enter the amount of days the certificate will be valid before expiration. The first day will be set as the day the certificate was created. (e.g. 100)
Note: Setting this parameter is required for IPsec VPN RSA
- **SAN (Server)** – Enter the IP address, email, or domain name of the SAN (storage array network server) of the first site/IPsec tunnel endpoint. (e.g. 192.168.10.20)
Note: Setting this parameter is optional for IPsec VPN RSA.
- **SAN (Client)** – Enter the IP address, email, or domain name of the SAN (storage array network server) of the second site/IPsec tunnel endpoint. (e.g. 192.168.100.20)
Note: Setting this parameter is optional for IPsec VPN RSA
- **Password** – Enter the import/export password for the certificate.
Note: Setting this parameter is optional for IPsec VPN RSA.

Certificate Name

Used for 

Country Code
2 letter code

State or Province Name
Full name

Local Name
eg, city

Organization Name
eg, company

Org. Unit
eg, section

Email Address


Common Name (Server)
The Common Name is typically composed of Host + Domain Name.
 *Must be filled for IPSEC.

Common Name (Client)
The Common Name is typically composed of Host + Domain Name.
 *Must be filled for IPSEC.

Validity Days
Between 1-3650

SAN(Server)
Specifies additional subject identities for server, can be IP, Email, DNS.


SAN(Client)
Specifies additional subject identities for client, can be IP, Email, DNS.

Password 
Set import/export password for .p12

OpenVPN – Below are the parameters you can set for the certificate. All parameters are required for the SSL VPN (OpenVPN) certificate.

- **Certificate Name** – Enter the name for the certificate.
- **Used for** – Click the drop-down list and select **OpenVPN**.
- **Country Code** – Enter the 2 letter country code for the certificate. (e.g. US)
- **State or Province Name** – Enter the name of the state or province for the certificate. (e.g. California)
- **Local Name** – Enter the name of the city for the certificate. (e.g. Torrance)
- **Organization Name** – Enter the company name for the certificate (e.g. TRENDnet)
- **Org. Unit** – Enter the department or group name for the certificate (e.g. IT)
- **Email Address** – Enter the email address contact for the certificate (e.g. xxxxx@trendnet.com)
- **Valid Days** – Enter the amount of days the certificate will be valid before expiration. The first day will be set as the day the certificate was created. (e.g. 100)

Certificate Name

Used for 

Country Code
2 letter code

State or Province Name
Full name

Local Name
eg, city

Organization Name
eg, company

Org. Unit
eg, section

Email Address

Validity Days
Between 1-3650

Router Maintenance and Monitoring

Managing access to the router management interface

Administrator > Access Management

This section will allow you to restrict access router management access to specific interfaces. By default, management access to the web interface (HTTP) is restricted only to the LAN interface.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Administrator** and click on **Access Management**.
3. Review the settings below. When complete, click **Apply** to save and commit your changes.

Local Access Management

- **Limit access by interface** – Checking this option will allow you to select specific local interfaces (e.g. LAN, VLAN) that are allowed access to the router management interface.
 - **Allowed interfaces** – The available local interfaces will be in this section. (e.g. Selecting LAN will only allow management access from the LAN and all other VLAN interfaces will be denied.)
- **Enable HTTPS** – Checking this option will enable secure HTTPS (SSL) access to the router management page on the selected local interfaces.
- **Enable Telnet** – Checking this option will enable command line interface access via Telnet on the selected local interfaces.
- **Enable SSH** – Checking this option will enabled secure command line interface access via SSH (Secure Shell) on the selected local interfaces.

Local Access Management

Limit access by interface

Allowed interfaces LAN

Enable HTTP

Port

Enable HTTPS

Enable Telnet

Enable SSH

Remote Access Management

- **Limit access by interface** – Checking this option will allow you to select specific WAN interfaces (e.g. WAN1, WAN2) that are allowed access to the router management interface over the Internet.
 - **Allowed interfaces** – The WAN1 and WAN2 interfaces will be in this section. (e.g. Selecting WAN1 will only allow management access from the WAN1 interface and will deny management access on the WAN2 interface.)
- **Enable HTTPS** – Checking this option will enable secure HTTPS (SSL) access to the router management page on the selected WAN interfaces.
- **Enable Telnet** – Checking this option will enable command line interface access via Telnet on the selected WAN interfaces.
- **Enable SSH** – Checking this option will enabled secure command line interface access via SSH (Secure Shell) on the selected WAN interfaces.

Remote Access Management

Limit access by interface

Enable HTTP

Enable HTTPS

Diagnostic tools

Administrator > Diagnostics

This section includes network tools and utilities for testing connectivity and troubleshooting.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Administrator** and click on **Diagnostics**.
3. Review the settings below.

Network Utilities

- **Ping** – This tool conducts a basic ping/connectivity test to a host IP address or domain name. After selecting and entering all of the required parameters, click **PING** to start the connectivity test and the results will appear at the bottom of the page.
 - **Interface** – Select the interface used to run the connectivity test.
 - **Default** – Uses the internal loopback interface to conduct the connectivity test.
 - **WAN1/WAN2** – You can select either WAN1 or WAN2 to conduct the connectivity test through a specific WAN interface for troubleshooting.
 - **Protocol** – Select the IP protocol version for the connectivity test, IPv4 or IPv6.
 - **Host** – Enter the host IP address or domain name to test connectivity.
- **Traceroute** – This tool conducts a test to check the routing path taken to reach a specific destination host IP address or domain name. After selecting and entering all of the required parameters, click **TRACEROUTE** to start the connectivity test and the results will appear at the bottom of the page.
 - **Interface** – Select the interface used to run the connectivity test.
 - **Default** – Uses the internal loopback interface to conduct the connectivity test.

- **WAN1/WAN2** – You can select either WAN1 or WAN2 to conduct the connectivity test through a specific WAN interface for troubleshooting.
 - **Protocol** – Select the IP protocol version for the connectivity test, IPv4 or IPv6.
 - **Host** – Enter the host IP address or domain name to test connectivity.
- **Nslookup** – This tool conducts a test to check domain name resolution to an IP address. After entering in the domain name to resolve, click **NSLOOKUP** to start the resolution test and the results will appear at the bottom of the page.
 - **Host** – Enter the host IP address or domain name to test resolution.

Network Utilities

Ping	Traceroute	Nslookup
Interface: Default	Interface: Default	
Protocol: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	Protocol: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	Host: trendnet.com
Host: 192.168.10.180	Host:	
PING	TRACEROUTE	NSLOOKUP

MWAN Interface Diagnostics – This section allows to conduct connectivity testing on the multi-WAN configuration.

- **Interface** – Select the WAN interface to conduct testing.
 - **Ping Default Gateway** – This will conduct a ping connectivity test to the default gateway IP address of the selected WAN interface.
 - **Ping Tracking IP** – This will conduct a ping connectivity test to the tracking IP configured under Network > Multiple WAN in the Link Tracking section for the selected WAN interface.
 - **Check IP Rules** – This will display the current IP rules configured for the selected WAN interface.
 - **Check Routing Table** – This will display the current default route configured for the selected WAN interface.

MWAN Interface Diagnostics

Check the interface status via Multiple WAN Management (MWAN). IPv4 Only.

Interface: WAN1

PING DEFAULT GATEWAY
PING TRACKING IP
CHECK IP RULES
CHECK ROUTING TABLE

Backup and restore your router configuration settings

Administrator > Backup / Flash Firmware

You may have added many customized settings to your router and in the case that you need to reset your router to factory defaults, 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:

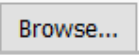

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Administrator**, then click on **Backup / Flash Firmware**
3. Next to Download backup, click **Generate Archive**.

Download backup: 

4. Depending on your web browser settings, you may be prompted to save the configuration file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: *backup-TEW-829DRU-YYYY-MM-DD.dat*)

To restore your router configuration:

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Administrator**, then click on **Backup / Flash Firmware**.
3. Next to Restore backup, click **Browse** or **Choose File**.

Restore backup:  No file selected. 

4. A separate file navigation window should open.
5. Select the router configuration file to restore and click **Upload Archive** (Default Filename: *backup-TEW-829DRU-YYYY-MM-DD.dat*). If prompted, click **Yes** or **OK**.
6. Wait for the router to restore settings.

Reboot your router


Administrator > Reboot

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](#)" section.
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.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Administrator**, then click on **Reboot**.
3. Next to Reboots the operating system, click **Perform Reboot**.

Reboots the operating system: 

4. Wait for the device to reboot.

Scheduled automatic reboot

Administrator > Reboot > Setting

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 and you have already created a time schedule for this function.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Administrator**, click on **Reboot**, and click on **Setting** tab.
3. Click the Automatic reboot by schedule drop-down list and select the schedule used for the automatic device reboot function. Click **Apply** to save and commit the changes.

Automatic reboot by schedule Disable time schedule ▼
 ⓘ The start time of schedule rule will apply automatic reboot time

Console access

Using the includes RS-232 to RJ-45 console cable, you can access the router console command line interface management through the console port for debugging and troubleshooting if necessary.

You can access the command line interface management of router using the terminal emulation program settings below.

Baud Rate (bps)	115200
Data Bits	8
Parity Bits	None
Stop Bits	1
Hardware Flow Control	Off

Command Line Interface

The router firmware is based on OpenWRT which is based on Linux and command usage can be referenced from the web links below.

<https://busybox.net/downloads/BusyBox.html>

<https://wiki.openwrt.org/doc/howto/user.beginner.cli>

<https://wiki.openwrt.org/doc/uci>

Router Default Settings

Administrator User Name	admin
Administrator Password	Please refer to sticker or device label
Router Default URL	http://tew-829dru
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/5GHz1/5GHz2	Enabled
Wireless 2.4GHz/5GHz1/5GHz2 Network Name/Encryption	Please refer to sticker or device label
Wireless 2.4GHz/5GHz1/5GHz2 Guest Network	Disabled
WAN1/WAN2 Mode	WAN1 Primary / WAN2 Secondary Failover

Reset your router to factory defaults

Administrator > Backup / Flash Firmware

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

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

- **Reset Button** – Located on the rear panel of your router, see "[Product Hardware Features](#)". 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 8).
2. Click on **Administrator**, then click on **Backup / Flash Firmware**.
3. Next to Reset to defaults, click **Perform Reset**. When prompted to confirm this action, click **OK**.

Reset to defaults: **PERFORM RESET**

4. Wait for the router to settings to factory default.

Upgrade your router firmware

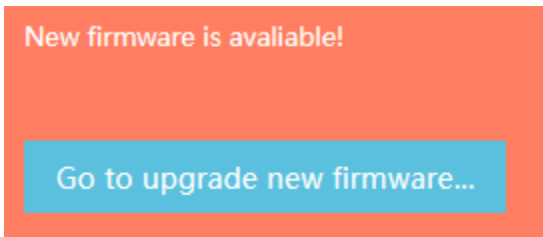
Administrator > Backup / Flash Firmware

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, check the Administrator > Backup / Flash Firmware under Online Firmware Upgrade or Status > Overview section under System.

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

When your router has detected a new firmware available online, a notification will appear at the top of the router management page. You can click the link or go to Administrator > Backup / Flash Firmware



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:	1.0.0.20, May 15, 2018
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**. At the verification page, click **Proceed**. Please wait for the online firmware upgrade procedure to complete successfully.

Note: The *Keep Settings* option will upgrade the firmware version and preserve your existing configuration settings. Unchecking the *Keep Settings* option will upgrade the firmware version and reset the device to factory defaults.

New Version:	1.0.0.21, MAY 17, 2018
Size:	24.72MB
	1. Initial Release
Release Note:	
Keep settings:	<input checked="" type="checkbox"/>
Error Message:	
	<input type="button" value="APPLY"/> <input type="button" value="CANCEL"/>

Flash Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the flash procedure.

Checksum: e5b3f68bc6f10e4881fa288a356410cd
Size: 24.72 MB
Configuration files will be kept.

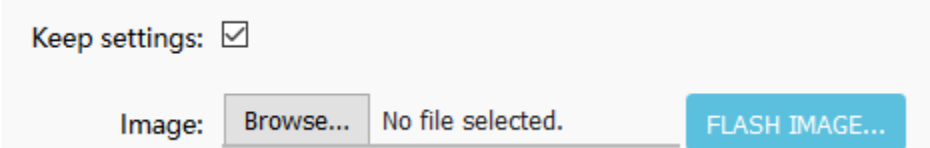
Manual Firmware Upgrade

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 8).
2. Click on **Administrator** and click on **Backup / Flash Firmware**.
3. Depending on your web browser, in the Flash new firmware image section, click **Browse** or **Choose File**.



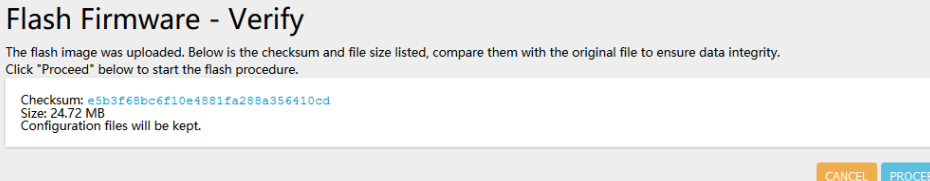
Keep settings:

Image: No file selected.

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

Note: The Keep Settings option will upgrade the firmware version and preserve your existing configuration settings. Unchecking the Keep Settings option will upgrade the firmware version and reset the device to factory defaults.

5. At the verification page, click **Proceed**. Please wait for the online firmware upgrade procedure to complete successfully.



Flash Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the flash procedure.

Checksum: e5b3f68bc6f10e4881fa288a356410cd
Size: 24.72 MB
Configuration files will be kept.


Ping Watchdog





Administrator > Ping Watchdog

The Ping Watchdog feature allows you configure your router to monitor connectivity to a specific host IP address. If connectivity is lost to the specified host IP address, the router will automatically initiate a device reboot in an automatic attempt to re-establish previously lost connectivity.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Administrator** and click on **Ping Watchdog**.
3. Review the settings below. When complete, click **Apply** to save and commit your changes.

Local Access Management

- **Enable** – Check this option to enable the ping watchdog feature.
- **Ping Host / Interface** – Enter the IP address to monitor and send ping requests to check connectivity.
 - Note:** You can additional host IP address entries to monitor by clicking  .
 - **ALL** – Check all local and WAN interfaces for the specified host IP address.
 - **WAN1** – Check only the WAN1 interface for the specified host IP address.
 - **WAN2** – Check only the WAN2 interface specified host IP address.
 - **Import Default Gateway** – Clicking this option will automatically attempt to copy both WAN interfaces default IP gateway to an available entry.
- **Ping Interval** – Enter interval time for the router to send ping and connectivity check. Ex: Setting the interval to 5 Minutes will configure to send a ping and check connectivity every 5 mintes.
- **Fail Count to Perform Reboot** – Once ping/connectivity check fails, this sets the maximum amount of attempts the router will attempt to check connectivity before initiating an automatic reboot.

Enable	<input checked="" type="checkbox"/>	
Ping Host / Interface	192.168.1.249	/ ALL 
	<input type="button" value="IMPORT DEFAULT GATEWAY"/>	<ul style="list-style-type: none"> ALL WAN1 WAN2
Ping Interval	5	Minutes 
	 Range: 5~1440 minutes or 1~24 hours	
Fail Count To Perform Reboot	1	
	 Range: 1~100	

Check the router status information

Status > Overview

You may want to check the system information of your router firmware, S/N, uptime, available memory, active connection, WAN interface information, wireless interface information, DHCP clients, connected wireless clients, dynamic DNS and active UPnP entries.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).

2. Click on **Status** and click on **Overview**.

- **System**

- **Hostname** – Displays the currently assigned hostname of the router. The name other network devices identify the router on the network.
- **Firmware Version** – Displays the currently loaded firmware version and date.
- **Serial Number** – Displays the device serial number.
- **Local Time** – Displays the current device time and date.
- **Uptime** – Displays the total amount of time the router has been up and running without reboot.
- **Load Average** – Displays the CPU load average of the device over the following time intervals. (one minute load avg., five minute load avg. fifteen minute load avg.)




System

Hostname	TEW-829DRU
Firmware Version	1.0.0.20, May 15, 2018
Serial Number	UM8ERJ1000405
Local Time	Sat May 19 11:03:20 2018
Uptime	0h 15m 24s
Load Average	5.54, 3.29, 1.43

- **Memory**

- **Total Available** – Displays the total amount of RAM memory available on the router regardless of usage.
- **Firmware Version** – Displays the total amount of free space RAM memory available on the router.
- **Buffered** – Displays the total amount of RAM memory used for buffer memory.




Memory

Total Available		80104 kB / 247288 kB (32%)
Free		67936 kB / 247288 kB (27%)
Buffered		12168 kB / 247288 kB (4%)

- **Network**

- **WAN1/WAN2** – Displays the current configuration of the WAN interfaces along with the IPv4/IPv6 address information and connected uptime.
- **Active Connections** – Displays the current amount of active Internet sessions.

Network

WAN1	IPv4 Status	Type: DHCP client Address: 10.10.10.80 Netmask: 255.255.255.192 Gateway: 10.10.10.126 DNS 1: 192.168.1.249 DNS 2: 8.8.8.8 Connected: 0h 9m 59s
	IPv6 Status	 Not connected
WAN2	IPv4 Status	Type: DHCP client Address: 10.10.10.84 Netmask: 255.255.255.192 Gateway: 10.10.10.126 DNS 1: 192.168.1.249 DNS 2: 8.8.8.8 Connected: 0h 9m 53s
	IPv6 Status	 Not connected
Active Connections		 54 / 32768 (0%)

- **DHCP/DHCPv6 Leases** – Displays the currently active DHCP and DHCPv6 address leases.

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
<i>There are no active leases.</i>			

DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining
<i>There are no active leases.</i>			

- **Wireless** – Displays the current configuration of the wireless bands such as SSID, Channel, Bitrate, BSSID (wireless MAC), encryption, and multiple SSID status.

Wireless

<p>Wireless 2.4GHz</p>	<p><i>Wireless 2.4GHz Network</i> SSID: TRENDnet829_2.4GHz_YCE1 Mode: Master Channel: 6 (2.437 GHz) Bitrate: 192 Mbit/s BSSID: 3C:8C:F8:F3:85:B7 Encryption: WPA2 PSK (CCMP) <i>Wireless 2.4GHz Guest Network : Disabled</i> <i>Wireless 2.4GHz Multiple Network (SSID 1) : Disabled</i> <i>Wireless 2.4GHz Multiple Network (SSID 2) : Disabled</i> <i>Wireless 2.4GHz Multiple Network (SSID 3) : Disabled</i> <i>Wireless 2.4GHz Multiple Network (SSID 4) : Disabled</i> <i>Wireless 2.4GHz Multiple Network (SSID 5) : Disabled</i> <i>Wireless 2.4GHz Multiple Network (SSID 6) : Disabled</i> <i>Wireless 2.4GHz Multiple Network (SSID 7) : Disabled</i></p>
------------------------	--

- **Associated Stations** – Displays the currently connect wireless client devices.

Associated Stations

MAC-Address	Band	Network	Signal	RX Rate	TX Rate
<i>No information available</i>					

- **Dynamic DNS** – Displays the current DDNS configuration for each WAN and status information.

Dynamic DNS

Configuration	Next Update	Hostname/Domain	Registered IP	Network
myddns1	Disabled	yourhost.example.com	No data	IPv4 / WAN1
myddns2	Disabled	yourhost.example.com	No data	IPv4 / WAN2

- **MWAN Interface Live Status** - Displays the current multiple WAN tracking and interface status.

MWAN Interface Live Status

WAN1 ([eth0](#))
Online (tracking off)

WAN2 ([eth2](#))
Online (tracking off)

- **Activate UPnP Redirects** – If UPnP is enabled, displays the currently active UPnP connections.

Active UPnP Redirects

Protocol	External Port	Client Address	Client Port
<i>There are no active redirects.</i>			

View routing table and ARP entries

Status > Routes

You may want to check the current routing table and ARP entry information for troubleshooting or monitoring purposes.

1. Log into your router management page (see "[Access your router management page](#)" on page 8).
2. Click on **Status** and click on **Routes**.

- **ARP** – Displays the router ARP table.

ARP

Network	IPv4-Address	MAC-Address
WAN1	10.10.10.84	3C:8C:F8:F3:85:B5
WAN2	10.10.10.80	3C:8C:F8:F3:85:B4
LAN	192.168.10.180	00:14:D1:15:31:C7
WAN1	10.10.10.126	00:24:14:E7:53:5B

- **Active IPv4-Routes** – Displays the current IPv4 active routing table.

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
WAN1	0.0.0.0/0	10.10.10.126	0	1
WAN2	0.0.0.0/0	10.10.10.126	0	2
WAN1	0.0.0.0/0	10.10.10.126	10	main
WAN2	0.0.0.0/0	10.10.10.126	20	main
WAN1	10.10.10.64/26		10	main
WAN2	10.10.10.64/26		20	main
WAN1	10.10.10.126		10	main
WAN2	10.10.10.126		20	main
VLAN4	192.168.4.0/24		0	main
LAN	192.168.10.0/24		0	main

- **Active IPv6-Routes** – Displays the current IPv6 active routing table.

Active IPv6-Routes

Network	Target	Source	Metric	Table
LAN	fd13:bee9:5f5::/64		1024	main
LAN	ff02::1		0	local
LAN	ff02::2		0	local
WAN2	ff02::1:2		0	local
WAN1	ff02::1:2		0	local
LAN	ff00::/8		256	local
VLAN4	ff00::/8		256	local
LAN	ff00::/8		256	local
WAN1	ff00::/8		256	local
WAN2	ff00::/8		256	local
LAN	ff00::/8		256	local
LAN	ff00::/8		256	local
LAN	ff00::/8		256	local

- **IPv6 Neighbors** – Displays currently discovered/detected IPv6 neighbor devices.

IPv6 Neighbours

Network	IPv6-Address	MAC-Address
---------	--------------	-------------

View your router logging

Status > System Log

Your router system 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 8).

2. Click on **Status** and click on **System Log**.

Note: The router system log will display the most recent entries in the list.

System Log

```
Sat May 19 10:49:37 2018 kern.warn kernel: [ 60.572214] ol_vdev_start_resp_ev for vap 0 (cb9c0000)
Sat May 19 10:49:37 2018 kern.warn kernel: [ 60.572437] su bfee 1 mu bfee 0 su bfer 1 mu bfer 1 impl bf 0 sounding dim 1
Sat May 19 10:49:37 2018 kern.warn kernel: [ 60.572463] wmi_unified_vdev_up_send for vap 0 (cb9c0000)
Sat May 19 10:49:37 2018 kern.warn kernel: [ 60.572484] _ieee80211_smart_ant_init: Smart Antenna is not supported
Sat May 19 10:49:37 2018 user.emerg syslog: Invalid command : obs_rx_rssi_th
Sat May 19 10:49:37 2018 user.emerg syslog: cat: can't open '/sys/class/net/ath2/address': No such file or directory
Sat May 19 10:49:37 2018 kern.warn kernel: [ 60.793106] wlan_vap_create : enter. devName=cb9c0000, opmode=IEEE80211_M_HOSTAP, flags=0x1
Sat May 19 10:49:37 2018 kern.warn kernel: [ 60.800866] wmi_unified_vdev_create_send: ID = 0 Type = 4, Subtype = 0 VAP Addr = 3c:8c:f6:f3:85:bb:
Sat May 19 10:49:37 2018 kern.warn kernel: [ 60.811122] su Dfee 0 mu bfee 0 su Dfer 0 mu bfer 0 impl bf 1 sounding dim 0
Sat May 19 10:49:37 2018 kern.warn kernel: [ 60.817410] _ieee80211_mbo_vattach:MBO Initialized
```

Configure router logging settings and setup external syslog server

Administrator > System > Logging

You can adjust specific log settings to set what type of logging is displayed in the system log and log buffer size.

1. Log into your router management page (see [“Access your router management page”](#) on page 8).

2. Click on **Administrator**, click on **System**, and click on the **Logging** tab.

- **System log buffer size** – You can increase or decrease the router buffer size. Enter the buffer size in KB.
- **External system log server** – This setting allows to send router logging to an external syslog server. Enter the IP address of the external syslog server.
- **External system log server port** – If sending logging to external syslog server, enter the syslog port to use. By default, the syslog port is 514.
- **Log output level** – This setting allows you to change the type of logging displayed in the internal system log of router displays under Status > System

Log. Debug displays all logging messages and selecting another log level type will only display those specific log messages along with any other levels above it.

- **Cron Log Level** – This setting allows you to change the type of logging send to the external syslog server.

System Properties

General Settings	Logging
System log buffer size	64 kiB
External system log server	0.0.0.0
External system log server port	514
Log output level	Debug
Cron Log Level	Normal

Technical Specifications

Standards

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x
- IEEE 802.3ab
- IEEE 802.1Q
- IEEE 802.1X
- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n (up to 400Mbps @ 256QAM)*
- IEEE 802.11ac (5GHz¹: up to 1733Mbps, 5GHz²: up to 867Mbps @ 256QAM)*

Device Interface

- 8 x Gigabit LAN ports
- 2 x Gigabit WAN ports (WAN failover / Load balancing)
- 1 x USB 3.0 (Samba)
- 1 x RJ-45 console port
- Power switch
- Reset button
- LED indicators

Performance

- NAT (LAN-to-WAN) throughput: 900Mbps
- Routing performance: 900Mbps
- Maximum concurrent sessions: 32,000
- Maximum number of VLANs: 8 (ID: 1-4094)
- IPsec VPN (AES-256/SHA-256/LAN-to-LAN) throughput: 90Mbps
- SSL VPN (OpenVPN®) Throughput (Blowfish/SHA-1/Bridge): 15Mbps

VPN

- SSL VPN Server (Up to 4 tunnels)
- OpenVPN Encryption: BF-CBC, AES-128-CBC, AES-256-CBC
- OpenVPN HMAC Authentication: SHA1, SHA256
- SSL VPN Certificate: RSA
- IPsec VPN Server / Site-to-Site (Up to 8 tunnels)
- IPsec Encryption: DES, 3DES, AES-128/256
- IPsec Authentication: MD5, SHA1, SHA2-256, Certificate: X.509v3
- IPsec Key Exchange: IKE: IKEv1/2, Main Mode, RSA, Pre-shared Key, DH Groups 1/2/5/14
- IPsec Protocols: ESP (Transport/Tunnel), PFS DH Groups 1/2/5/14, DPD, Local/Remote ID: IP Address, FQDN
- IPsec NAT Traversal
- IPsec VPN failover support
- PPTP/L2TP VPN Server (Up to 8 tunnels)
- L2TP with IPsec VPN Server (Up to 8 tunnels shared with L2TP)
- PPTP/L2TP Encryption: MPPE 40-bit, 128-bit, IPsec
- PPTP/L2TP Authentication: MS-CHAPv1/2

Networking

- WAN Modes: NAT, Classical Routing
- NAT Modes: NAT, PAT, One-to-One NAT
- WiFi client bridge mode
- ISP IPv4 WAN Modes: DHCP, Static IP, PPPoE, PPTP, L2TP
- ISP IPv6 WAN Modes: Static, Auto-configuration (SLAAC/DHCPv6), Link-Local, PPPoE
- VLAN ID assignment on WAN interface
- Routing: Static, RIPv1/v2, OSPFv2, routing policies (Up to 20 entries)
- Static ARP (Up to 32 entries)
- Inter-VLAN Routing (Up to 8 VLANs, 8 IP interfaces)
- SSID per VLAN assignment

- DHCP Server/Relay
- Dynamic DNS: dyn.com, no-ip.com
- WAN Failover
- WAN Load Balancing
- VPN passthrough: IPsec, PPTP, L2TP

Access Control

- Wireless encryption: WPA/WPA2-PSK, WPA/WPA2-RADIUS
- NAT, virtual server/port forwarding, port triggering, firewall traffic rules, DMZ host, UPnP/NAT-PMP, allow/deny ping on WAN interfaces
- ALG: PPTP/L2TP/IPsec VPN passthrough, FTP/TFTP/SIP/RTSP/IRC/H.323 passthrough
- MAC & IP filtering
- Custom scheduling for access control rules
- Wireless client isolation
- DoS prevention

Quality of Service

- User defined classification rules with 4 priority queues
- WMM

Management/Monitoring

- CLI (Console/Telnet/SSH) command line management
- HTTP/HTTPS web based management
- Scheduled automatic reboot
- Scheduled Wake-on-LAN (WoL)
- View ARP and routing table entries
- View CPU load, traffic/wireless usage, and NAT sessions
- Internal system logging
- Manual or online firmware upgrade and notification
- Backup and restore configuration
- Internal logging
- Ping watchdog
- Diagnostic tools: Built-in ping, traceroute, and ns-lookup network utilities

Frequency

- 2.412 - 2.472GHz
- 5.180 – 5.825GHz

Modulation

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

Media Access Protocol

- CSMA/CA with ACK

Antenna Gain

- 2.4GHz: 2 x 2.9 dBi (max.) / 5GHz: 4 x 4.4 dBi detachable/external

Wireless Output Power (max output power without antenna gain)

- 802.11a: FCC: 25 dBm (max.) / IC: 23 dBm (max.)
- 802.11b: FCC: 26 dBm (max.) / IC: 26 dBm (max.)
- 802.11g: FCC: 23 dBm (max.) / IC: 23 dBm (max.)
- 802.11n (2.4GHz): FCC: 23 dBm (max.) / IC: 23 dBm (max.)
- 802.11n (5GHz): FCC: 23 dBm (max.) / IC: 23 dBm (max.)
- 802.11ac: FCC: 23 dBm (max.) / IC: 23 dBm (max.)

Receiving Sensitivity (per chain)

- 802.11a: -70 dBm (typical) @ 54Mbps
- 802.11b: -83 dBm (typical) @ 11Mbps
- 802.11g: -70 dBm (typical) @ 54Mbps
- 802.11n (2.4GHz): -59 dBm (typical) @ 400Mbps
- 802.11n (5GHz): -59 dBm (typical) @ 800Mbps
- 802.11ac: -55 dBm (typical) @ 1733Mbps

Wireless Channels

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

Power

- Input: 100 – 240 V AC, 50 – 60 Hz, 1A
- Output: 12V DC, 3A external power adapter
- Max. Consumption: 17.4W

Operating Temperature

- 0° – 50° C (32° – 122° F)

Operating Humidity

- Max. 95% non-condensing

Certifications

- FCC
- IC

Dimensions

- 280 x 170 x 44.45mm (11 x 6.7 x 1.75 in.)
- Rack mountable 1U height

Weight

- 1.24kg (2.74 lbs.)

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 1.733Gbps, use with a 1.733Gbps 802.11ac wireless adapter. For maximum performance of up to 867Mbps, use with an 867Mbps 802.11ac wireless adapter. For maximum performance of up to 400Mbps, use with an 400Mbps 802.11n wireless adapter. Multi-User MIMO (MU-MIMO) requires the use of multiple MU-MIMO enabled wireless adapters.

Troubleshooting

Q: I typed <http://tew-829dru> 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.



IMPORTANT NOTE:

Radiation Exposure Statement:

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

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

Industry Canada Statement

INDUSTRY CANADA RADIATION EXPOSURE STATEMENT

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

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

This radio transmitter (IC: 6337A-TEW829DRU) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

This device has been designed to operate with cellular antennas having a maximum gain of 3 dBi. Antennas having a higher gain are strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

These devices have been designed to operate with WiFi antennas having a maximum gain of 5 dBi. Antennas having a higher gain are strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

DÉCLARATION D'INDUSTRIE CANADA

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

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

les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

NOTE IMPORTANTE (POUR L'UTILISATION DE DISPOSITIFS MOBILES): DÉCLARATION D'EXPOSITION AUX RADIATIONS

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

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

Le présent émetteur radio (IC: 6337A-TEW829DRU) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Ce dispositif a été conçu pour fonctionner avec une antenne cellulaire ayant un gain maximal de 3 dBi. Une antenne à gain plus élevé est strictement interdite par les règlements d'Industrie Canada. L'impédance d'antenne requise est de 50 ohms.

Ce dispositif a été conçu pour fonctionner avec une antenne WiFi ayant un gain maximal de 5 dBi. Une antenne à gain plus élevé est strictement interdite par les règlements d'Industrie Canada. L'impédance d'antenne requise est de 50 ohms.

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 DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

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

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

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

2019/09/18

TRENDnet[®]

Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet's website at <http://www.trendnet.com/register>

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA

Copyright ©2019. All Rights Reserved. TRENDnet.