

User's Guide

TRENDnet[®]



Gigabit Multi-WAN VPN Business Router

TWG-431BR

Table of Contents

Product Overview	1
Package Contents	1
Features	1
Product Hardware Features.....	3
Applications	5
Router Installation	1
Desktop Hardware Installation	1
Rack Mount Hardware Installation	1
Basic Installation and Configuration	2
Basic Router Settings.....	7
Access your router management page.....	7
Saving and applying router configuration changes	7
Change your administrator password	8
Set your router date and time	8
Create time schedules	9
Change LAN IPv4 address settings.....	10
Configure LAN IPv4 DHCP server settings.....	11
Add static DHCP reservations	13
Configure WAN interfaces for Internet connectivity	14
IPv6 settings.....	15
Virtual LANs (VLANs).....	16
Static routes.....	18
Dynamic routing protocols	19
Bandwidth Control.....	23
Dynamic DNS	25
Wake on LAN (WoL).....	26

USB Mode	27
Firewall & security settings	28
Virtual server/Port forwarding	28
IP filtering	29
MAC filtering.....	31
IM/P2P application filtering.....	32
DMZ Host.....	34
Multiple WAN Configuration	35
Multiple WAN Management Settings.....	35
Web Management System (Router Limits™)	38
Setup your router with Router Limits.....	38
Router Limits Content Management	40
Virtual Private Networking (VPN)	43
Creating a Virtual Private Network (VPN).....	43
PPTP VPN Server	44
Setting up the PPTP VPN server	44
Setting up the PPTP VPN client (Windows).....	46
L2TP VPN Server	47
Setting up the L2TP VPN server without IPsec encryption	47
Setting up the L2TP VPN server with IPsec encryption (PSK).....	49
Setting up the L2TP VPN client (Windows) with IPsec encryption (PSK)	50
IPsec (Internet Protocol Security).....	52
Setting up IPsec site-to-site VPN (PSK)	52
Setting up IPsec server VPN (PSK).....	57
Secure Socket Layer VPN (SSL) / OpenVPN	58
SSL VPN Server Setup.....	58
SSL VPN Client Setup (Windows)	59
High Availability.....	63

Configuring a high availability cluster	63	SNMP Settings	73
Router Maintenance and Monitoring67		Check the router status information	74
Managing access to the router management interface	67	View routing table and ARP entries.....	75
Diagnostic tools	68	View your router logging.....	75
Backup and restore your router configuration settings	69	Configure router logging settings and setup external syslog server	75
Reboot your router	69	SMTP Email Notification	76
Scheduled automatic reboot	70	Technical Specifications 77	
Console access	71	Troubleshooting 79	
Router Default Settings	71	Appendix 80	
Reset your router to factory defaults	71		
Upgrade your router firmware	72		

Product Overview



TWG-431BR

Package Contents

In addition to your router, the package includes:

- Quick Installation Guide
- RJ-45 to RS-232 console cable (1.5m / 5 ft.)
- Power adapter (12V DC, 1A)
- 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 Gigabit Multi-WAN VPN Business Router, model TWG-431BR, features internet WAN load balancing, a network fail-safe backup, and encrypted Virtual Private Network (VPN) access for remote users. Improve peak-network-loading performance and eliminates network downtime with the use of the VPN router's multiple WAN ports. Smooth network loading, minimize network downtime, and allow employees to access your network from the Internet—all with a single router. The VPN router features advanced management, high availability, QoS, VLAN, VPN, and other capabilities to ensure optimal performance, scalability, and protection of your network. Advanced SPI, NAT and SNAT protects against Internet attacks.

The TWG-431BR comes fully integrated with Router Limits' comprehensive web management system, designed to give users more control over the activity on their network. Manage screen time, filter content, track web use and browsing history, as well as device level controls and more. Router Limits' software is also available for mobile devices, providing you better management of your connected network.

Multi-WAN

Supports up to four separate WAN internet connections for load-balancing or fault-tolerance modes

VPN Router

The VPN router 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

High Availability

Create a high availability network by grouping two or more routers on the network for redundancy

Ports

5 x Gigabit ports, 1x Console port

Rack Mount Design

Sturdy metal housing with rack mount brackets included

Online Firmware Updates

Automatic notification of firmware updates

Management

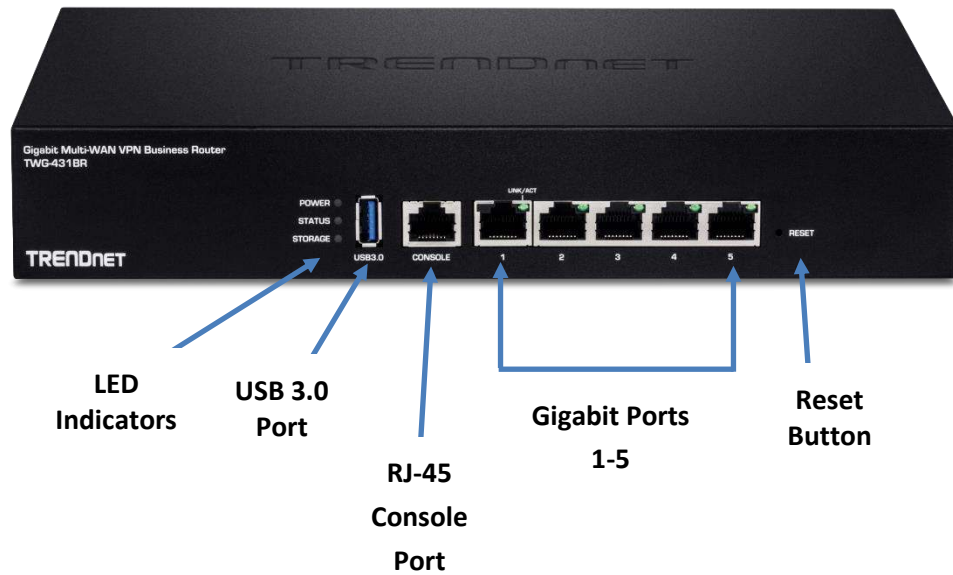
Supports web browser (HTTP, HTTPS), CLI, SSH and Telnet management

Content Filtering

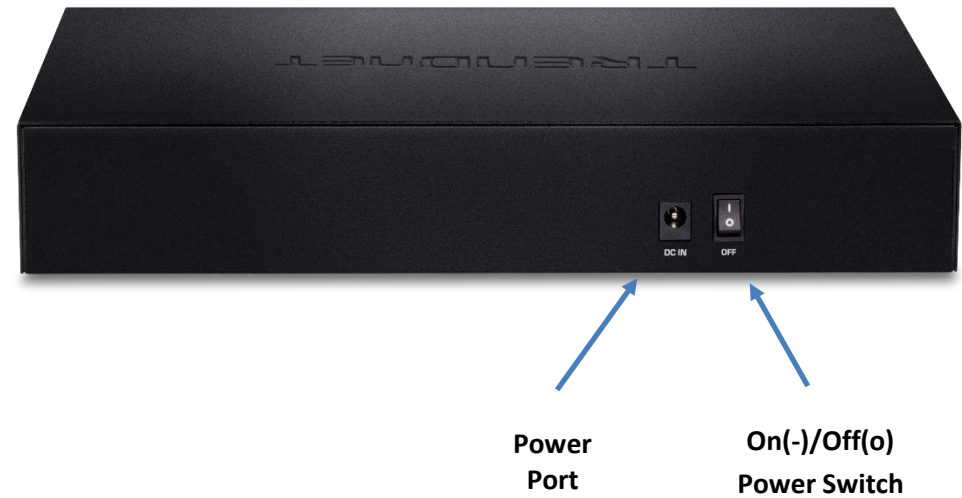
Manage screen time, filter content, track web use and browsing history, as well as device level controls and more. Advanced web content filtering service powered by Router Limits™

Product Hardware Features

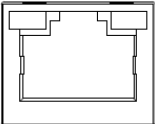
Front Panel View



Rear Panel View



LED Indicators

LED	Description
Power	Solid Green – Device is ready and receiving power. Off – Device is not powered or not ready.
Status	Refer to USB mode section for functionality.
Storage	Refer to USB mode section for functionality.
Gigabit Ports 1-5 LED 	LED r Solid Green – Port is connected at 10Mbps/100Mbps/1Gbps link speed. Blinking Green - Data activity/transmission on port. Off – Port is disconnected or no link.

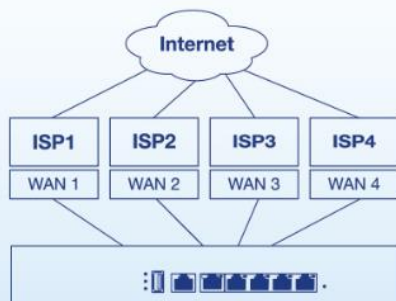
Port/Button Description

Ports/Buttons	Description
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: 57600 / 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 for configuration backup and export logging. (FAT32/NTFS format only)
Gigabit Ports 1-5	By default, port 1 is configured as the LAN port and ports 2-5 are configured as WAN ports. The ports can operate in two modes, 1 x LAN / 4 x WAN or 4 x LAN / 1 x WAN. By default, management access to the GUI and command line interface via default LAN IP address: 192.168.10.1 / 255.255.255.0 The WAN port(s) connect your ISP(s) equipment for Internet connectivity such as modem. By default, WAN1 (port 2) is configured as the primary WAN interface and all WAN interfaces are configured in load balance mode.
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

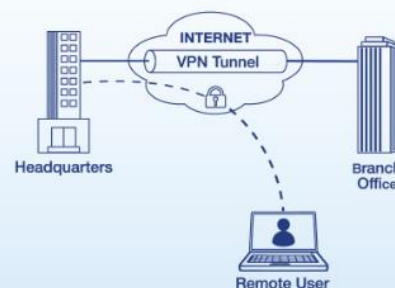
Multi-WAN

Connect up to four separate WAN internet connections to efficiently load-balance traffic by distributing network traffic to the best available link.



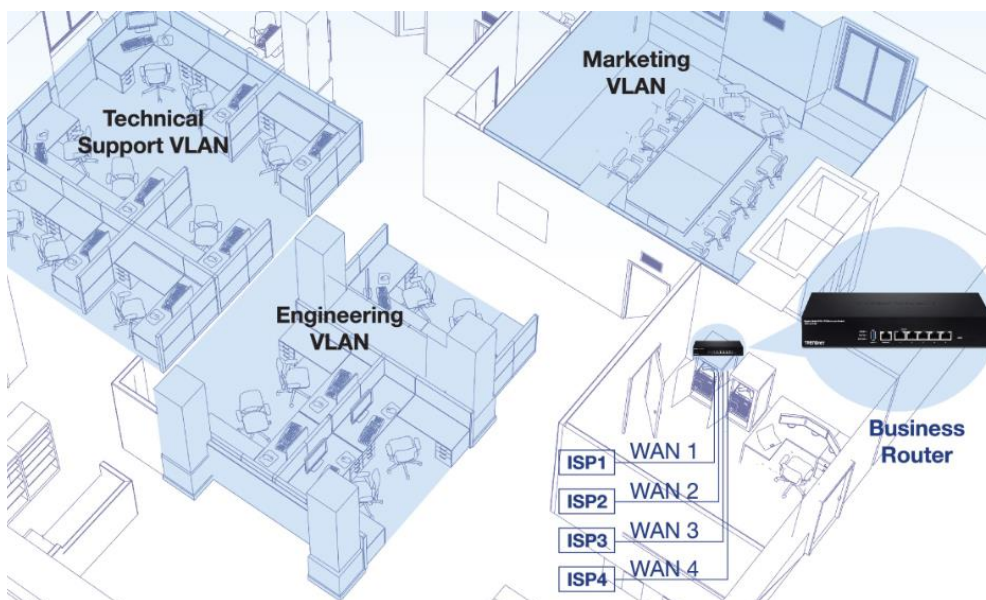
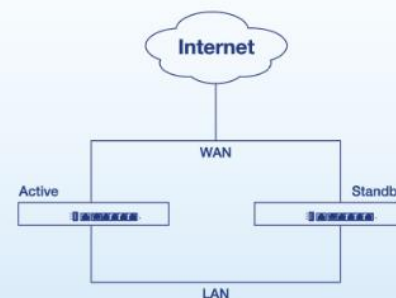
VPN Router

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



High Availability

Group multiple TWG-431BR VPN routers together to create a high availability network with router redundancy to minimize downtime.



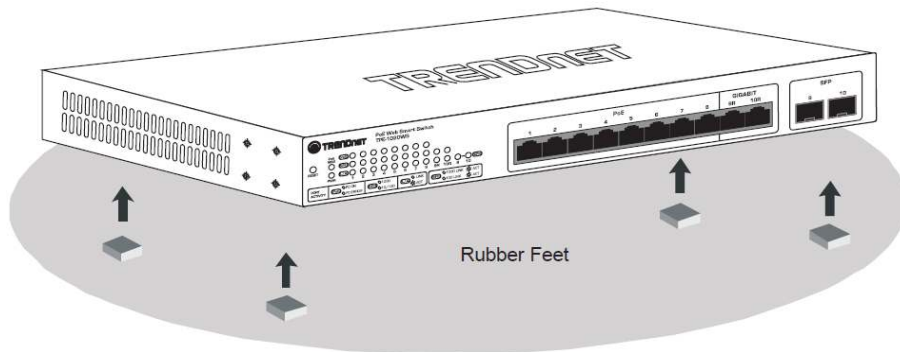
Router Installation

Desktop Hardware Installation

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

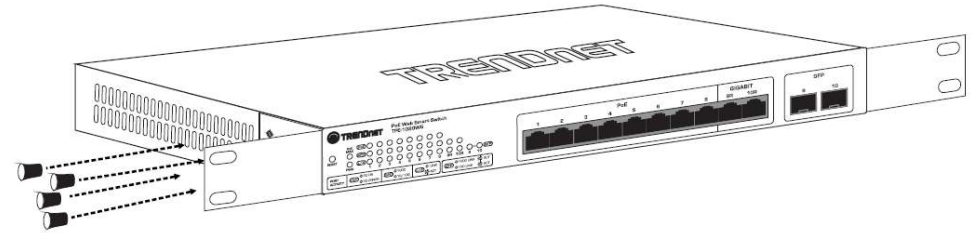
Note: The router model may be different than the one shown in the example illustrations.

- 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.

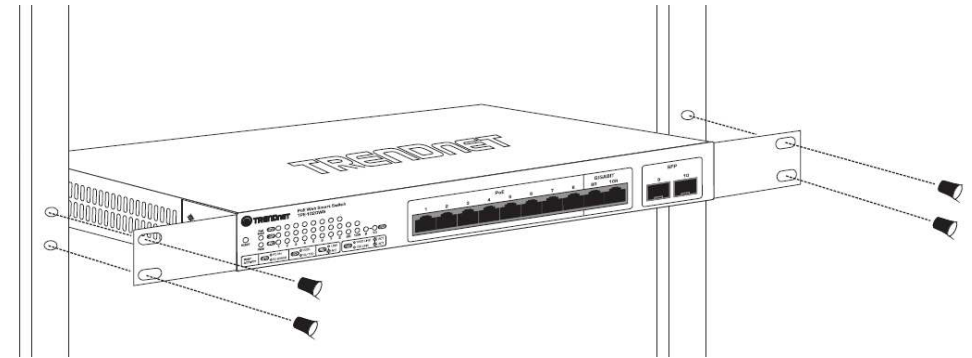


Rack Mount Hardware Installation

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.

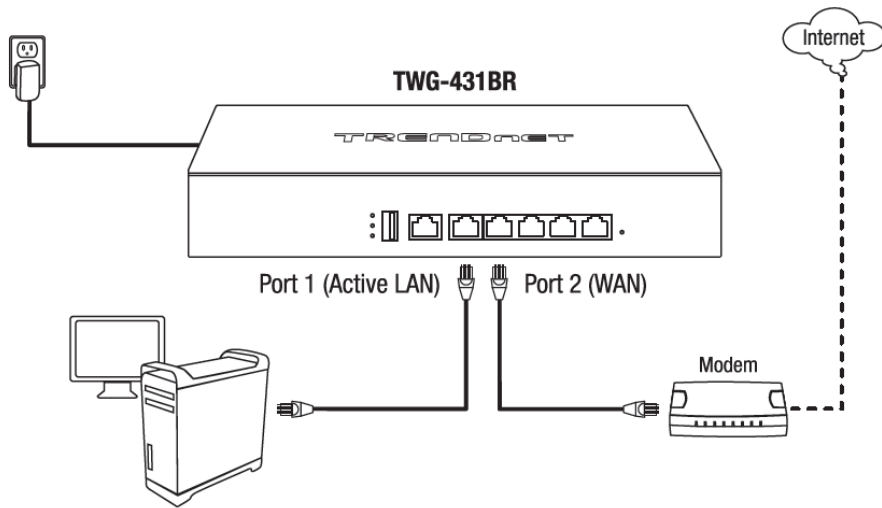


Note: The look of the router may be different than what is actually displayed.

Basic Installation and Configuration

IMPORTANT NOTE: The default mode for the interfaces is 1 x LAN / 4 x WAN. In this mode, NAT throughput/performance will have a performance limitation of 200Mbps per WAN interface.

1. Connect a network cable from the Port 2 WAN1 of your router to your modem.
2. Connect a network cable from Port 1 (Active LAN) your router to your computer.
3. 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.



4. After you have the unit powered on and have connected your computer into the Active LAN port, open your web browser and type the IP address of the router in the address bar, then press **Enter**. The default IP address is 192.168.10.1.

5. Enter the **User Name** and **Password**, and then click **OK**. By default:

User Name: **admin**

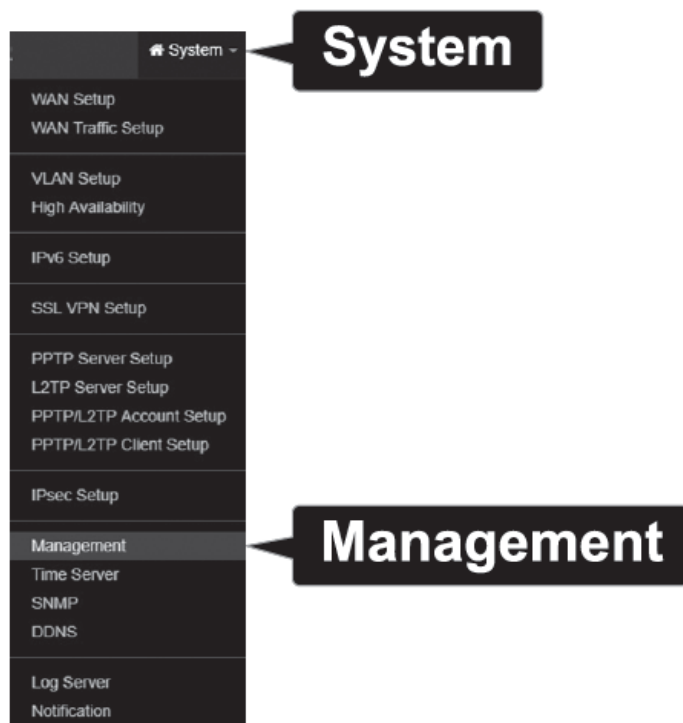
Password: **admin**



User name

Password

6. Click **System** at the top, then click **Management**.



7. In the Admin Password section, enter and confirm your new Admin Password.

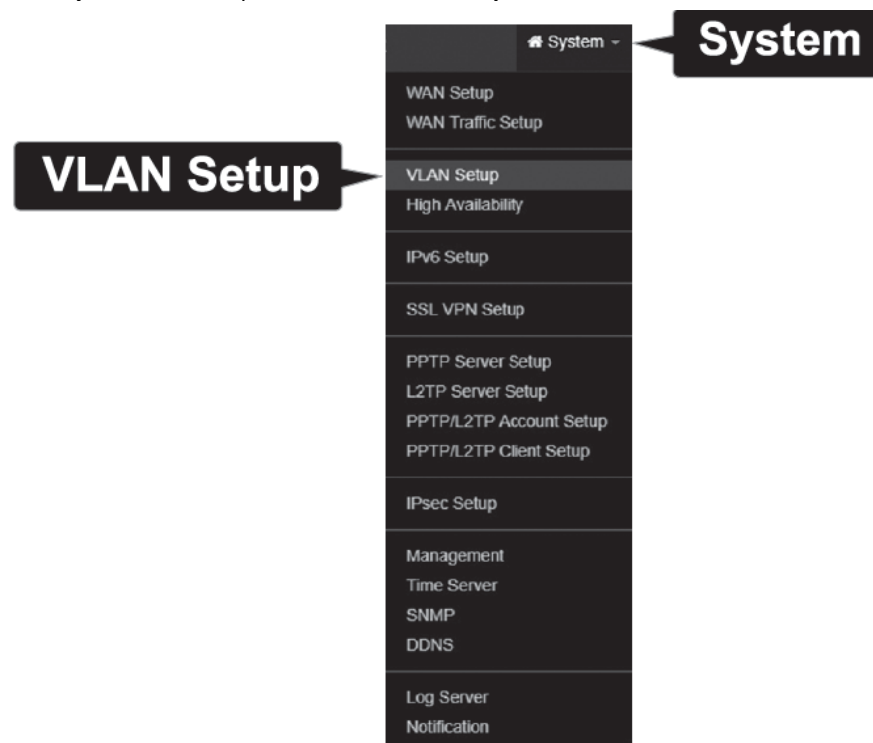
A screenshot of the 'Admin Password' section in the TRENDnet web interface. It features two input fields. The first field is labeled 'New Admin Password' and the second field is labeled 'Check Admin Password'. Both fields are empty and have a light gray border.

8. Click **Save** at the bottom of the page.

Note: After clicking **Save**, the changes you made to the router will not take effect until you reboot the unit. You can also make additional changes, then save and reboot after you completed all configuration changes. To save all configuration changes and reboot, click **Reboot** in the top right corner then click the **Reboot** button.

A large, dark gray button with the word 'Save' in white, sans-serif font.

9. Click **System** at the top, then click **VLAN Setup**.



10. By default, VLAN #1 refers to the LAN interface and the default IP address settings of the router.

#	VLAN Mode	Flag	IP Address	Netmask	Action
1	OK	Native	192.168.10.1	255.255.255.0	Network
2	OK	VLAN TAG: 101	192.168.20.1	255.255.255.0	Network
3	OK	VLAN TAG: 102	192.168.30.1	255.255.255.0	Network
4	OK	VLAN TAG: 103	192.168.40.1	255.255.255.0	Network
5	OK	VLAN TAG: 104	192.168.50.1	255.255.255.0	Network
6	OK	VLAN TAG: 105	192.168.60.1	255.255.255.0	Network
7	OK	VLAN TAG: 106	192.168.70.1	255.255.255.0	Network
8	OK	VLAN TAG: 107	192.168.80.1	255.255.255.0	Network

11. Under VLAN#1, click the **Network** button in the action column on the right.



12. Under IP setup, configure the router IP address settings, match the requirements of your network.

IP Setup

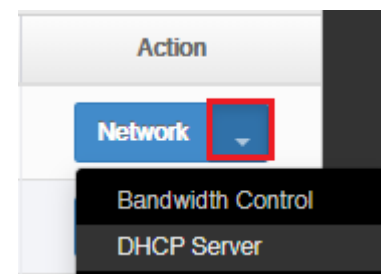
IP Address

192.168.10.1

Netmask

255.255.255.0

13. After you have configured the IP address settings, you need to configure the DHCP Pool to match the IP address settings. Under VLAN#1, click the arrow button in the Action column on the right then select **DHCP Server**.



14. In the DHCP Setup section, enter the desired IP address settings for your DHCP server.

DHCP Setup

Start IP

192.168.10.101

End IP

192.168.10.199

Netmask

255.255.255.0

Gateway

192.168.10.1

DNS1 IP

192.168.10.1

DNS2 IP

WINS IP

Domain

Lease Time

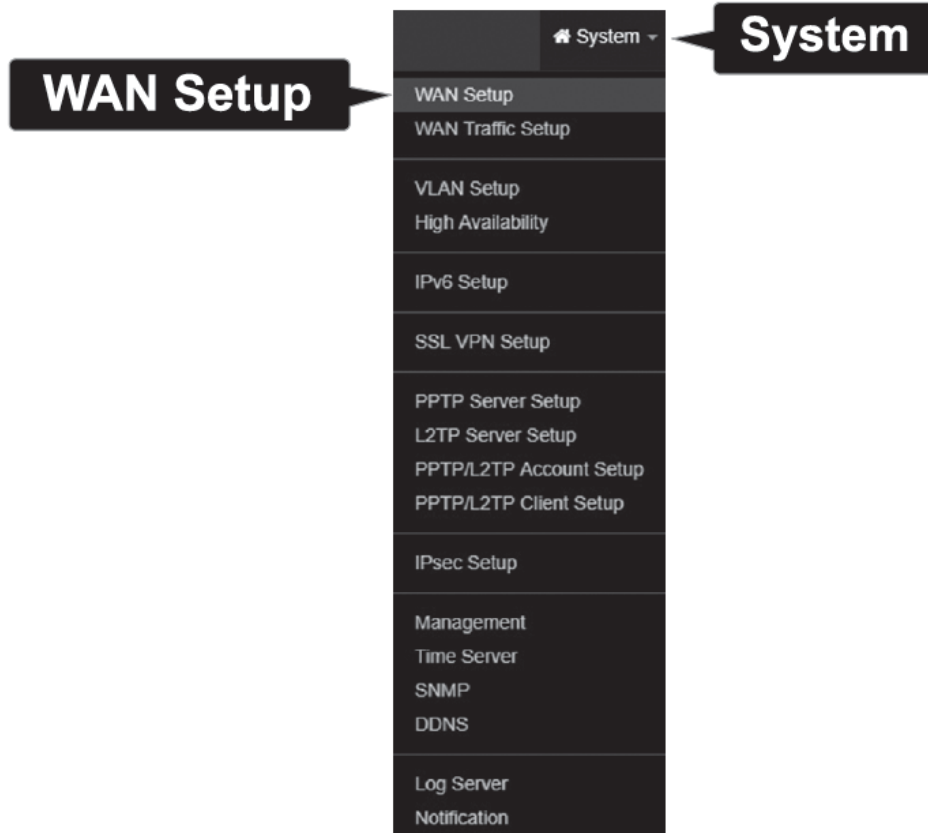
86400

15. Click **Save** at the bottom of the page.

Note: After click **Save**, the changes you made to the router will not take effect until you reboot the unit. You can also make additional changes, then save and reboot once you have completed all configuration changes. To save all configuration changes and reboot, click **Reboot** at the top right corner and click the **Reboot** button.

Save

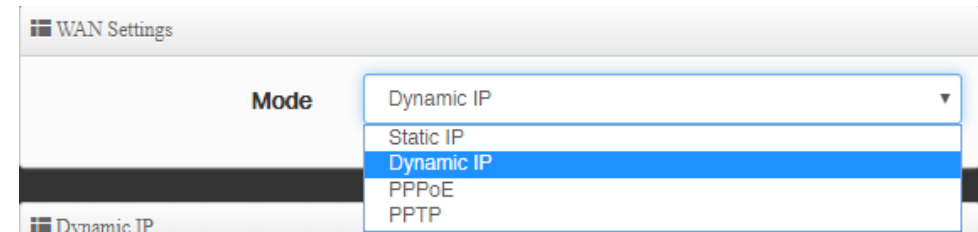
16. Click the **System** tab at the top, then click **WAN Setup**.



17. The WAN1 interface of the router is set to Dynamic IP (also known as DHCP) by default. To change the WAN1 Internet connection settings, click the Edit button in the column on the right.

WAN List			
#	Active	Mode	Edit
1	On	Dynamic IP	Edit
2	On	Dynamic IP	Edit
3	On	Dynamic IP	Edit
4	On	Dynamic IP	Edit

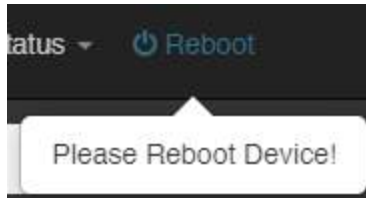
18. Under WAN settings, select the appropriate mode for your Internet connection **Dynamic IP**, **Static IP**, and **PPPoE**. If you are unsure of the connection mode, please contact your ISP.



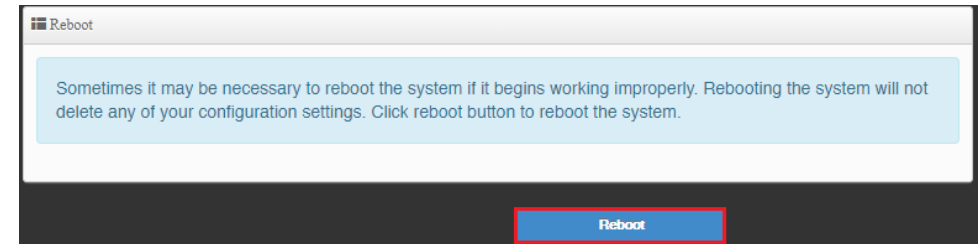
19. After you have selected the appropriate mode and entered your settings, click **Save** at the bottom of the page.

Save

20. After you save your changes, the device will prompt you to reboot in the top right corner.



21. Click **Reboot** in the top right corner, then click the **Reboot** button.



Basic Router Settings

Access your router management page

Note: Your router management page 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 IP address <http://192.168.10.1>. Your router will prompt you for a user name and password.



2. The default User Name and Password are below.

- User Name: **admin**
- Password: **admin**



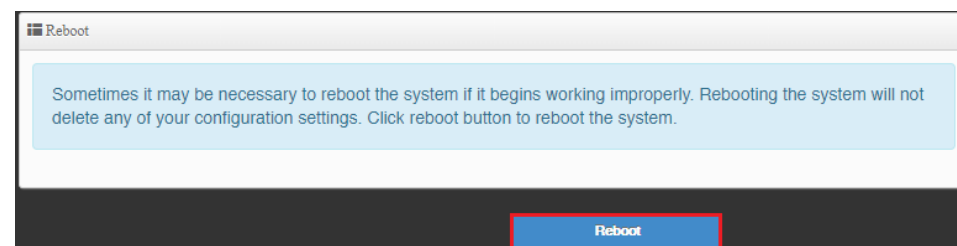
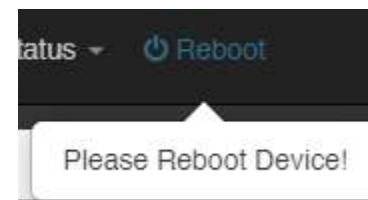
User name

Password

Saving and applying router configuration changes

In the router management page, you may apply multiple configuration and reboot to apply all configuration changes at one time. When apply configuration changes, a reboot prompt will appear at the top right corner.

You can continue to make additional configuration changes and when finished, you can click the Reboot prompt and reboot the router to apply configuration changes at the same time.



Change your administrator password

System > Management

By default, the administrator user name and password is configured to

- User Name: **admin**
- Password: **admin**

This section will allow you to change the default administrator password used to log into your router management page.

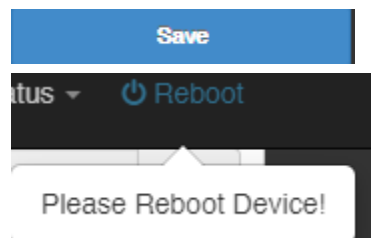
1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **System** and click on **Management**.
3. Enter the new administrator password in the **New Admin Password** and re-enter the new password in the **Check Admin Password** fields. Click **Save** and **Reboot** to commit the changes.

Admin Password

New Admin Password

Check Admin Password

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 default password.

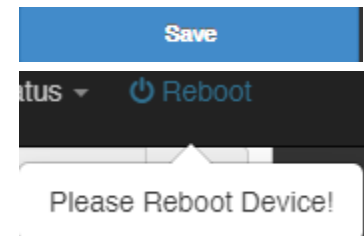


Set your router date and time

System > Time Server

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 7).
2. Click on **System** and click on **Time Server**.
3. Review the settings below. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



System Time

- **Local Time** – Displays the current device day, date, and time.
- **Mode**
 - **NTP Server** - Enables the NTP client to configure router to obtain time and date settings from an external network time server.
 - **Default NTP Server** – Click the drop-down list to select from an available list of time servers. You can select the **Customize** option to manually specify an NTP server.
 - **NTP Server** – The selected NTP server will displays in the list. If an NTP server is not available in the list, you can manually enter the domain name of the NTP server to obtain time and date settings.
 - **Time Zone** – Click the drop-down list to select the appropriate time zone.
 - **Daylight Savings Time** – Enable or disable daylight savings time depending on the time zone.

System Time

Local Time: 2019/12/06 12:58:06

Mode: ☒ NTP Server ☐ Manual

NTP Server

Default NTP Server: north-america.pool.ntp.org

NTP Server: north-america.pool.ntp.org

Time Zone: (GMT-08:00) Pacific Time (US & Canada)

Daylight Saving Time: ☐ Enable ☒ Disable

- **Manual** - This setting allows you to set the time and date settings manually. Click the drop-down lists to manually set the date and time settings.

System Time

Local Time: 2019/12/06 13:01:05

Mode: ☐ NTP Server ☒ Manual

User Setup

Date(Y/M/D): 2019 12 6

Time(H:M:S): 13 1 4 (GMT+8:00)

Create time schedules

Advanced > Time Policy

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 7).
2. Click on **Advanced** and click **Time Policy**.
3. Next to entry 1, click **Edit** next to the new schedule entry in the list.

Policy List			
#	Comment	Mode	Edit
1	Policy 1	On Schedule	Edit

- **Comment** – Enter a name for the new policy.
- **Mode**
 - **On Schedule** – The rules in which the policy is applied will be enabled/activated according to the defined schedule list.
 - **Out of Schedule** – The rules in which the policy is applied will be enabled/activated outside of the defined schedule list.

To defined a new schedule, click on **Create New Policy**.

- **Day of the Week** – Select which days when the schedule will be applied.
 - **Start Time** – Manually define a start time for the schedule.
 - **End Time** – Manually define an end time for the schedule.
- Note:** The time period is specified in 24 hour format.

Time Policy Rules

Day of Week

☒ Sun	☒ Mon	☒ Tue
☒ Wed	☒ Thu	☒ Fri
☒ Sat		

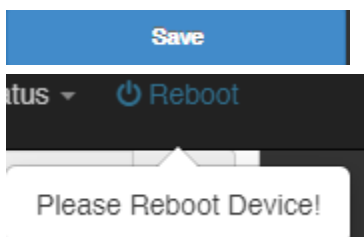
Start Time

00	00
----	----

End Time

23	59
----	----

Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



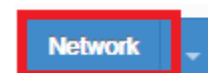
Change LAN IPv4 address settings

System > VLAN Setup > Network

Note: The default LAN interface IPv4 address settings is 192.168.10.1 / 255.255.255.0 and also assigned to LAN port 1 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. In the router configuration page, the LAN settings are set as VLAN1 settings.

Note: When changing the LAN IPv4 address, the DHCP server IP range does not change automatically. DHCP server settings must be changed manually.

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **System** and click **VLAN Setup**.
3. Under the VLAN1 section, click **Network**.



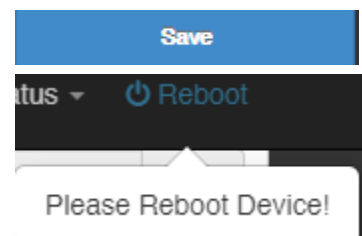
- **IP Address** – Enter the new LAN IPv4 address. (e.g. 192.168.50.1)
- **Netmask** – Enter the new LAN IPv4 subnet mask. (e.g. 255.255.255.0)

IP Setup

IP Address 192.168.10.1

Netmask 255.255.255.0

Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.

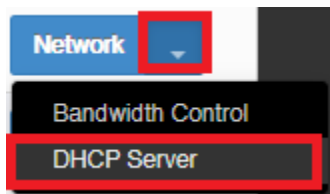


Configure LAN IPv4 DHCP server settings

System > VLAN Setup > DHCP Server

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 7).
2. Click on **System** and click **VLAN Setup**.
3. Under the VLAN1 section, click the drop-down list next to Network and click **DHCP Server**.



3. Under the DHCP Server/Relay section, you can modify or enter the new DHCP settings.

- **DHCP Service** – 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.
 - **DHCP 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 IP** – 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 IP** – 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)
- **Netmask** – Enter the subnet mask to assign to DHCP clients. The default subnet mask is 255.255.255.0.
- **DNS1 IP** – 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 (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)
- **DNS2 IP** – 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)
- **Domain – Local domain name** – Enter a domain name to distribute to DHCP clients. This parameter is optional. (e.g. trendnet.com)
- **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)

- **Lease Time** – Enter the lease time in seconds DHCP clients will hold their IP address settings before automatically requesting a new lease (IP address settings) from the internal DHCP server.

DHCP Service

Mode

☒ Enable ☐ Disable

DHCP Relay

☐ Enable ☒ Disable

DHCP Setup

Start IP

192.168.10.101

End IP

192.168.10.199

Netmask

255.255.255.0

Gateway

192.168.10.1

DNS1 IP

192.168.10.1

DNS2 IP

WINS IP

Domain

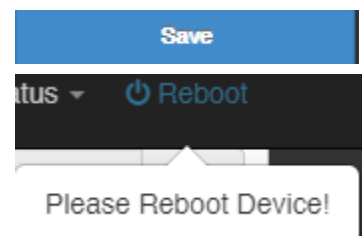
Lease Time

86400

DHCP Client List – Displays a list of the current DHCP clients/leases. Clicking **Fixed** will add the client information to the Static Lease IP Setup to be added as a static DHCP reservation.

DHCP Client List					
#	IP Address	MAC Address	Hostname	Expired	Action
1	192.168.10.101	1c:87:2c:ca:9b:62	DESKTOP-1UGCT5I	23:59:58	Fixed

Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



Add static DHCP reservations

System > VLAN Setup > DHCP Server

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **System** and click **VLAN Setup**.
3. Under the VLAN1 section, click the drop-down list next to Network and click **DHCP Server**.

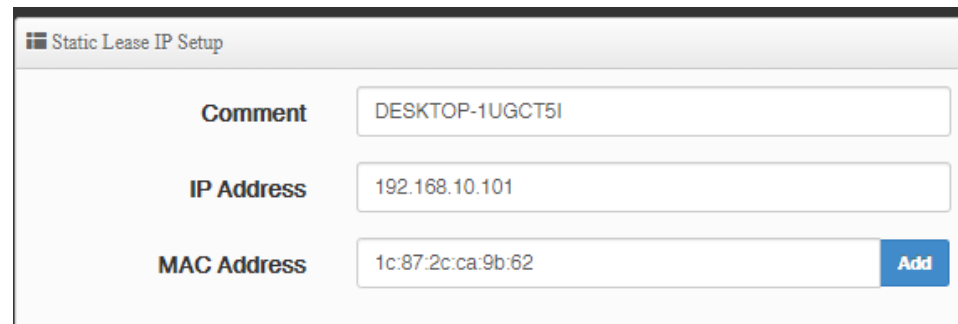
Static Leases

Hostname	MAC-Address	IPv4-Address
This section contains no values yet		
ADD		

4. In the **Static IP Lease Setup**, enter the parameters for the static DHCP reservation and click **Add** to add the static DHCP reservation to the list.

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.

- **Comment** – Enter a description or name for the DHCP reservation. (e.g. trendnetpc)
- **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 of network devices detected by the router through DHCP. (e.g. 192.168.50.150)
- **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)



Static Lease IP Setup

Comment: DESKTOP-1UGCT5I

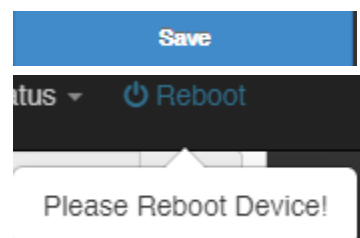
IP Address: 192.168.10.101

MAC Address: 1c:87:2c:ca:9b:62 [Add](#)



#	Comment	IP Address	MAC Address	Action
1	DESKTOP-1UGCT5I	192.168.10.101	1c:87:2c:ca:9b:62	Delete

5. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



Configure WAN interfaces for Internet connectivity

System > WAN Setup

By default, the WAN configuration is set to WAN load balance equally across all WAN interface and use WAN1 as the primary connection for Internet connectivity. WAN failover to the next active WAN interface if connection WAN1 fails. This section will explain how to set up the WAN interfaces for Internet connectivity to your ISP (Internet Service Provider).

IMPORTANT NOTE: The default mode for the interfaces is 1 x LAN / 4 x WAN. In this mode, NAT throughput/performance will have a performance limitation of 200Mbps per WAN interface.

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **System** and under **DNS**, enter primary and secondary IP addresses of the DNS servers provided by your ISP (Internet Service Provider), then click **Save**.

Note: Please note that the router will use one set of DNS servers for all WAN interfaces.

DNS

DNS1

DNS2

3. Under the WAN List next to **WAN1**, click **Edit**.

#	Active	Mode	Edit
1	On	Dynamic IP	Edit

4. Under the WAN Settings, click the **Mode** drop-down list and select the Internet connection provided by your ISP.

WAN Settings

Mode

- Dynamic IP
- Static IP
- Dynamic IP
- PPPoE
- PPTP

5. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.

Reboot

Please Reboot Device!

IPv6 settings

System > IPv6 Setup

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 7).
2. Click on **System** and click on **IPv6 Setup**.

3. Select **Enable**. Review the IPv6 Internet Connection settings and enter information settings specified by your ISP.

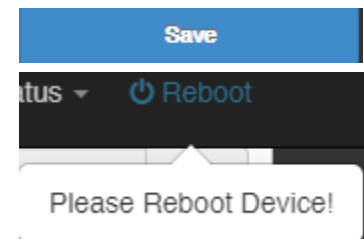
Note: Please contact your ISP for IPv6 service availability.

IPv6 Setup										
IPv6 DNS Server Setting										
IPv6 ☒ Enable ☐ Disable										
Primary DNS Server										
Secondary DNS Server										
WAN List										
WAN#	Connection Type	Link-Local Address	IPv6 Address	Prefix Length	Gateway Address	6to4 Relay	6rd Relay	IPv6 Prefix Length	IPv6 Prefix	
WAN1	Static	☐								
WAN2	Static	☐								
WAN3	Static	☐								
WAN4	Static	☐								
VLAN List										
VLAN#	WAN	DHCP-PD	IPv6 Address	Prefix Length	Autoconfiguration	DHCPv6(Start)	DHCPv6(End)	Lifetime		
VLAN1	WAN1	☐			Stateless Auto					

Select the IPv6 WAN connection type provided by your ISP.

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

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



Virtual LANs (VLANs)

System > VLAN Setup

Your router supports 802.1Q tagged VLANs as well inter-VLAN routing. VLANs can be assigned different IP address interfaces in which the router can route between VLAN IP subnets. The router supports up to 7 802.1Q tagged VLANs.

Note: The default VLAN must be assigned as Native to access the router management interface.

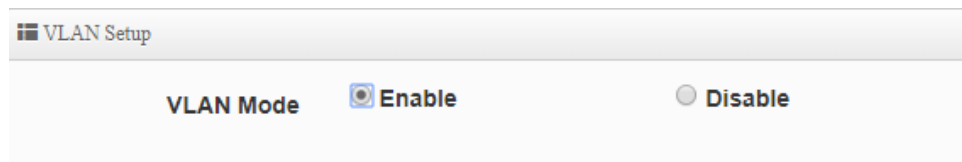
Enable an 802.1Q tagged VLAN

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 7).
2. Click on **System** and click **VLAN Setup**.
3. Under VLAN #2, click **Network**.

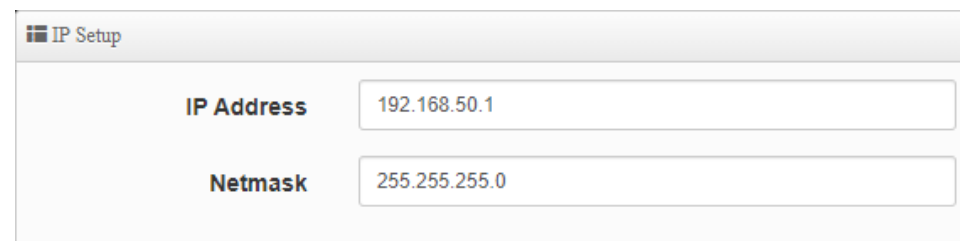


4. For the VLAN Mode, select **Enable**.

A screenshot of the 'VLAN Setup' page. The 'VLAN Mode' section shows two radio buttons: 'Enable' (selected) and 'Disable'.

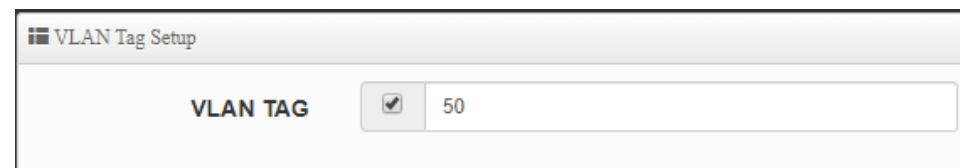
5. Under IP Setup, enter the **IP Address** and **Subnet Mask** for the new VLAN.

Ex: We will enter the interface IP address as 192.168.50.1 and subnet mask 255.255.255.0.

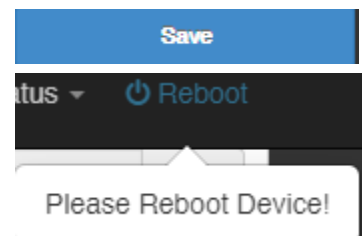
A screenshot of the 'IP Setup' page. It shows two input fields: 'IP Address' with the value '192.168.50.1' and 'Netmask' with the value '255.255.255.0'.

6. Under VLAN Tag Setup, enter the VLAN tag/VID of the new VLAN.

Ex: We will enter the tag/VID 50 for the new VLAN.

A screenshot of the 'VLAN Tag Setup' page. It shows a 'VLAN TAG' field with a checkmark icon and the value '50'.

7. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.

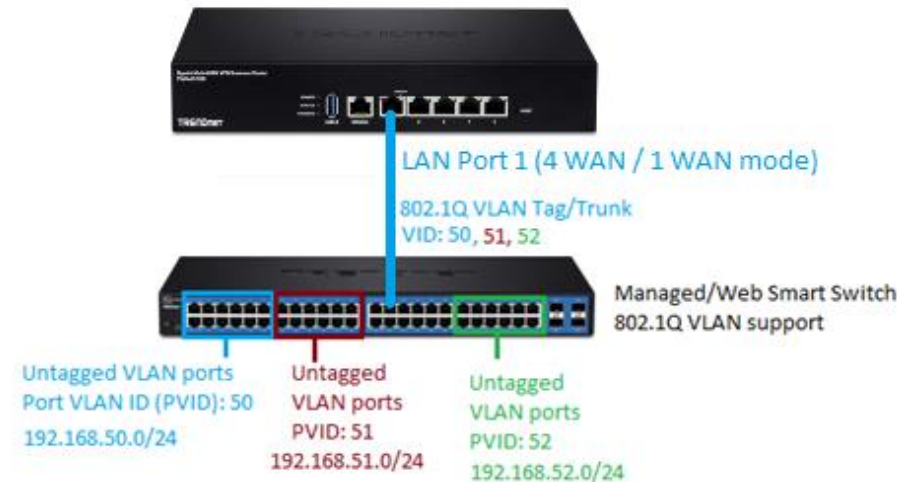


Note: If using multiple WAN mode, under Specify WAN Port, you can select which WAN to direct the outbound traffic for the VLAN.

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 switch 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.



Static routes

Advanced > IP Routing Rule Setup

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 7).

2. Click on **Advanced**, click on **IP Routing Rule Setup**, and next to the first entry, click **Edit**.

IP Routing Rule List						
#	Active	Destination Net/Mask	Via	OSPF	RIP	Edit
1	On/Active	-	-	On	Off	Edit

3. Review the Routing section.

- **Service:** Select Enable to enable the route or disable to disable the route.
- **Destination Net/Mask:** Enter the IP network address of the destination network for the route. (e.g. 192.168.150.0/24)
- **Via**
 - **Gateway:** This option configures that static route to an external IP network and specify the gateway IP address. If choosing this option, enter the Gateway IP address. (e.g 192.168.10.2)
 - **Interface:** This option configure an interface route. If choosing this option, click the drop-down list and select the interface.
- **Metric:** Enter the metric or priority of the route. The metric range is 1-255, the lowest number 1 being the highest priority.

IP Routing Rule Settings

Service

☒ Enable
 ☐ Disable

Destination Net/Mask

Via

☒ Gateway
 ☐ Interface

Gateway

Metric

1-255

OSPF

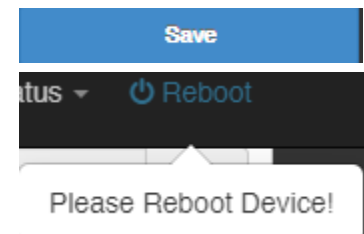
☐ Enable
 ☒ Disable

RIP

☐ Enable
 ☒ Disable

You can check the current routing table **Advanced > IP Routing Status**.

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



Dynamic routing protocols

Advanced > IP Routing Rule Setup

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)

Advanced > IP Routing Setup / Advanced > IP Routing Rule Setup

Note: The RIP version is RIP version 2.

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **Advanced** and click on **IP Routing Setup**.
3. Review the RIP Routing section. To save changes to this section, click **Apply** to command save your changes.
 - **Service:** Check **Enable** to enable the RIP version 2 routing protocol.
 - **Distribute OSPF over RIP:** If you are using both RIP and OSPF dynamic routing protocols at the same time, this option will distribute OSPF routes over RIP protocol to other RIP enabled devices.

RIP Settings

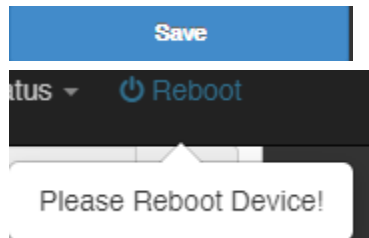
Service	☒ Enable	☐ Disable
Distribute OSPF over RIP	☐ Enable	☒ Disable

Under RIP Side (Devices) Settings, select the interface you would like to enable the RIP protocol.

RIP Side(Devices) Settings

WAN1	☐ Enable	☒ Disable
WAN2	☐ Enable	☒ Disable
WAN3	☐ Enable	☒ Disable
WAN4	☐ Enable	☒ Disable
VLAN1	☐ Enable	☒ Disable
VLAN2	☐ Enable	☒ Disable
VLAN3	☐ Enable	☒ Disable
VLAN4	☐ Enable	☒ Disable
VLAN5	☐ Enable	☒ Disable
VLAN6	☐ Enable	☒ Disable
VLAN7	☐ Enable	☒ Disable
VLAN8	☐ Enable	☒ Disable

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



5. Click on **Advanced**, click on **IP Routing Rule Setup**, and next to the first entry, and click **Edit**.

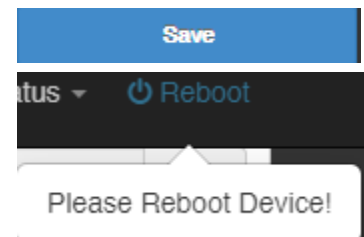
IP Routing Rule List						
#	Active	Destination Net/Mask	Via	OSPF	RIP	Edit
1	InActive			Off	Off	Edit

6. Review the Routing section.

- **Service:** Select Enable to enable the route or disable to disable the route.
- **Destination Net/Mask:** Enter the IP network address of the destination network for the route or network to distribute for the RIP/OSPF protocol (e.g. 192.168.150.0/24)
- **Via**
 - **Gateway:** This option configures that static route to an external IP network and specify the gateway IP address. If choosing this option, enter the Gateway IP address. (e.g 192.168.10.2)
 - **Interface:** This option configure an interface route. If choosing this option, click the drop-down list and select the interface.
- **Metric:** Enter the metric or priority of the route. The metric range is 1-255, the lowest number 1 being the highest priority.
- **RIP** – Selecting Enable will distribute the network route to other RIP enabled devices.
- **OSPF** – Selecting Enable will distribute the network route to other OSPF enabled devices.

You can check the current routing table **Advanced > IP Routing Status**.

6. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



OSPF (Open Shortest Path First)

Advanced > IP Routing Setup / Advanced > IP Routing Rule Setup

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **Advanced** and click on **IP Routing Setup**.
3. Review the OSPF Routing section.
 - **Service:** Check **Enable** to enable the OSPF routing protocol.
 - **Router ID:** Click the drop-down and select which interface IP to assign as the OSPF router ID.
 - **Distribute RIP over OSPF:** If you are using both RIP and OSPF dynamic routing protocols at the same time, this option will distribute RIP routes over OSPF protocol to other OSPF enabled devices.

OSPF Settings

Service
☒ Enable
☐ Disable

Router ID

VLAN1 ▼

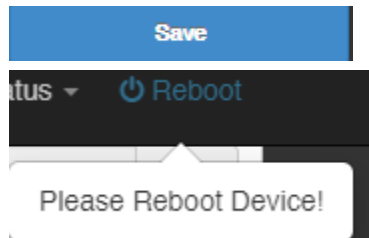
Distribute RIP over OSPF
☐ Enable
☒ Disable

Under OSPF network settings, check the network interfaces to enable OSPF and enter the Area ID.

OSPF Network Settings

WAN1 Area	☐	0
WAN2 Area	☐	0
WAN3 Area	☐	0
WAN4 Area	☐	0
VLAN1 Area	☐	0
VLAN2 Area	☐	0
VLAN3 Area	☐	0
VLAN4 Area	☐	0
VLAN5 Area	☐	0
VLAN6 Area	☐	0
VLAN7 Area	☐	0
VLAN8 Area	☐	0

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



5. Click on **Advanced**, click on **IP Routing Rule Setup**, and next to the first entry, and click **Edit**.

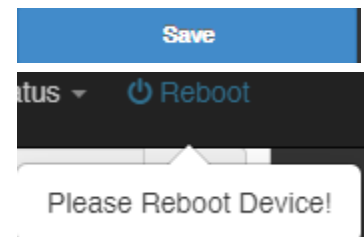
IP Routing Rule List						
#	Active	Destination Net/Mask	Via	OSPF	RIP	Edit
1	InActive			Off	Off	Edit

6. Review the Routing section.

- **Service:** Select Enable to enable the route or disable to disable the route.
- **Destination Net/Mask:** Enter the IP network address of the destination network for the route or network to distribute for the RIP/OSPF protocol (e.g. 192.168.150.0/24)
- **Via**
 - **Gateway:** This option configures that static route to an external IP network and specify the gateway IP address. If choosing this option, enter the Gateway IP address. (e.g 192.168.10.2)
 - **Interface:** This option configure an interface route. If choosing this option, click the drop-down list and select the interface.
- **Metric:** Enter the metric or priority of the route. The metric range is 1-255, the lowest number 1 being the highest priority.
- **RIP** – Selecting Enable will distribute the network route to other RIP enabled devices.
- **OSPF** – Selecting Enable will distribute the network route to other OSPF enabled devices.

You can check the current routing table **Advanced > IP Routing Status**.

6. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



Bandwidth Control

System > VLAN Setup > Bandwidth Control

1. Log into your router management page (see "[Access your router management page](#)" on page 7).

2. Click on **System**, click on **VLAN Setup**, click on the drop-down arrow next to Network and select **Bandwidth Control**.

Note: The bandwidth control setting is applied per VLAN interface. By default, VLAN1 is considered as the LAN interface of the router.

VLANList					
#	VLAN Mode	Flag	IP Address	Netmask	Action
1	On	Active	192.168.10.1	255.255.255.0	Network 

3. Under the Bandwidth Control settings, review the settings below.

- **Enable:** Enables the bandwidth control feature for the VLAN.

Total Bandwidth Control

- **Upload (Kbps):** Enter the maximum upload bandwidth you would like to allocate to the VLAN in kilobits per sec. It is important to set this value accurately.
Note: This should not be the total bandwidth allocated by your ISP but a portion you would like to allocate only for the selected VLAN.
- **Download (Kbps):** Enter the maximum download bandwidth you would like to allocate to the VLAN in kilobits per sec. It is important to set this value accurately.
Note: This should not be the total bandwidth allocated by your ISP but a portion you would like to allocate only for the selected VLAN.
Note: If you are using multi-WAN mode, you can combine the total download bandwidth of the WAN connections. Please note that performance throughput is limited of up to 200Mbps per WAN connection in multi-WAN mode.

Bandwidth Rules

In the rules list, review the settings below.

The rules will allow you to create specific bandwidth control limits based on a specific type of traffic or IP address or IP address range.

- **Active** – Enables the bandwidth control rule.
- **Rule Mode** – Click the drop-down list to select the specify the type of traffic you would like to apply the bandwidth rule.
- **Value 1/Value 2** – If selecting IP/Mask, IP Range Range, or Port, these fields will allow you to enter the specific IP network, range or ports to apply the bandwidth rule.
- **Upload (Kbps)** – Enter the maximum upload bandwidth to apply to the specified traffic.
- **Download (Kbps)** – Enter the maximum download bandwidth to apply to the specified traffic.
- **Comment** – Enter a description for the rule. (Optional)

Bandwidth Control

Mode ☒ Enable ☐ Disable

Total Bandwidth Control

Mode ☒ Enable ☐ Disable

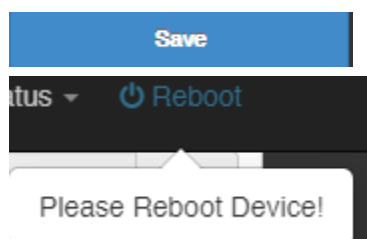
Upload Kbps

Download Kbps

QoS RuleList

#	Active	Rule Mode	Value1	Value2	Upload(Kbps)	Download(Kbps)	Comment
1	☒	ANY			1024	1024	
2	☒	ANY			1024	1024	
3	☒	ANY			1024	1024	
4	☒	ANY			1024	1024	
5	☒	ANY			1024	1024	
6	☒	ANY			1024	1024	
7	☒	ANY			1024	1024	
8	☒	ANY			1024	1024	
9	☒	ANY			1024	1024	
10	☒	ANY			1024	1024	

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



Dynamic DNS

System > DDNS

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.

Note: In multi-WAN mode, you can configure a DDNS service for each WAN interface.

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 7).
3. Click on **System** and click on **DDNS**.
4. Next to one of the entries, click **Edit**. Review the **DDNS** settings below.
 - **Active** – Check the enabled option to enable the dynamic DNS entry.
 - **Provider:** Click the drop-down list Select your DDNS service.
 - **WAN:** Click the drop-down list and select the WAN interface for the DDNS service.

Note: To ensure resolvability, it is recommended to assign each DDNS entry to a specific WAN interface.

 - **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.
- **Interval** – This specified the time interval between each DDNS update sent the DDNS service provided. Please refer to your DDNS service provider requirements.

DDNS List					
#	Active	Provider	WAN	Hostname	Edit
0	InActive	dyndns	Auto		Edit

DDNS Setup

Active

☒ Enable
 ☐ Disable

Provider

no-ip ▼

WAN

WAN1 ▼

Hostname

Username

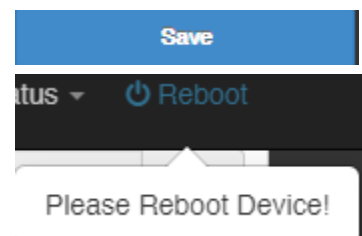
Password

Interval

10

Minute

5. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



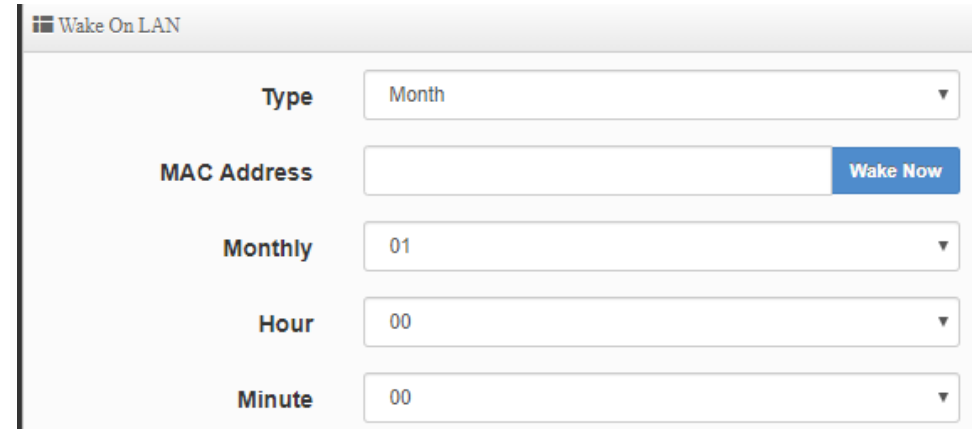
Wake on LAN (WoL)

System > Management

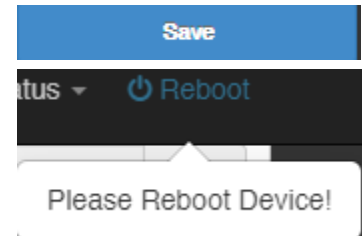
Wake on LAN (WoL) is used to remotely wake up or turn on device that support the WoL feature from your router.

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 7).
2. Click on **System** and click on **Management**.
3. Under Wake On LAN, review the settings below.
 - **Type:** Clicking the drop-down list allows you to specify a schedule when to send to a WoL message to wake up your WoL device. Daily, Weekly, Monthly.
 - **MAC Address:** Enter the MAC address of the WoL device. Clicking the **WAKE NOW** button will immediately send a wake up message to the WoL device.
 - **Monthly/Weekly:** If selecting to specify a schedule under Type, monthly will allow you to choose which day every month and weekly will allow you to choose which day every week.
 - **Hour/Minute:** Specify the hour and minute (24-hour format).
Note: If setting a schedule, please make sure the router time settings are setup correctly under System > Time Server.



4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



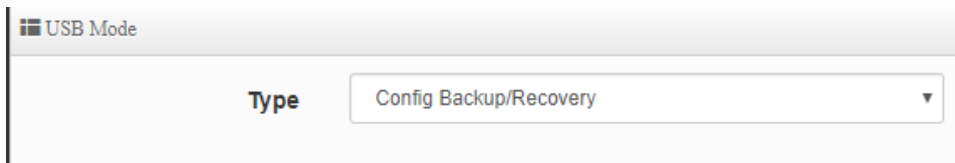
USB Mode

System > Management

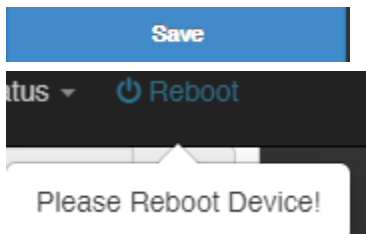
The USB port provides either of the two modes, export logging or backup configuration.

Note: The mode must be set in the router management interface first and the reset is used to initiate the function after the USB storage device has been connected. The default mode is backup configuration.

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **System** and click on **Management**.
3. Under USB mode, review the settings below.
 - **Type:**
 - **Config Backup/Recovery:** Sets the USB mode to backup router configuration.
 - **Export Log to CSV:** Sets the USB mode to export logging to .csv file.



4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



5. To initiate the function, connect the USB storage device to USB port.

6. Using a paper clip, push and hold the reset button and release when **POWER**, **STATUS**, **STORAGE** LEDs start flashing.

Note: Do not hold the reset button 10 seconds or longer or the router will reset to factory defaults.

7. All LEDs will turn off and **POWER/STORAGE** LEDs will turn back on to indicate that USB mode is ready.

8. Using a paper clip, push and hold the reset button for 6 seconds and release. **STORAGE LED** will remain on and **STATUS** will start flashing indicating write to USB. When writing to USB has completed, **STORAGE** and **STATUS** LED will turn off.

Note: Do not hold the reset button 10 seconds or longer or the router will reset to factory defaults.

Firewall & security settings

Virtual server/Port forwarding

Advanced > Virtual Server

Virtual Server/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 7).
2. Click on **Advanced** and click on **Virtual Server**.
3. Review the settings below. Click **Edit** to on the new entry in the list and click **Save**.

- **Active** – Select **Enable** to enable the virtual server/port forwarding rule.

Active ☒ **Enable** ☐ **Disable**

- **Comment** – Enter a name or description for the virtual server/port forwarding rule.

Comment

- **Protocol** – Select the protocol for the port or service **TCP** or **UDP**.

Protocol ☒ **TCP** ☐ **UDP**

- **Interface** – Click the drop-down list to select the external WAN interface(s) to allow: **ALL WAN, WAN1/2/3/4, WAN**. 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. Choosing ALL WAN will allow will enable the rule on all WAN interfaces.

Interface WAN1

- **Public Port** – Enter the external/public port number for the service to allow.

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

Public Port (min:1, max:65535 or Range xxxxx:xxxxx)

- **Private IP address** – Enter the local/internal IP address of the device to forward the port/protocol service.

Private IP Address

- **Private Port** – Enter the internal/private port number for the service to allow.

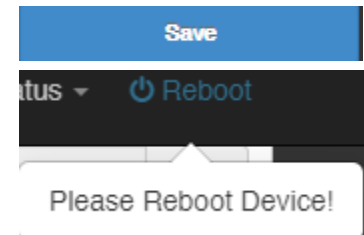
Note: You can also enter a consecutive range of ports in the following format: 80:90
Typically, the internal port or port range is same as the external port or port range.

Private Port (min:1, max:65535 or Range xxxxx:xxxxx)

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

Schedule Always

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



IP filtering

Advanced > IP Filter

IP filtering allows you to restrict access to the Internet to specific IP addresses on your network. This section also functions as a firewall rule section for inbound/outbound IP traffic. You can check the current IP addresses assigned to devices connected to your router under System > VLAN Setup > DHCP Server 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 7).
2. Click on **Advanced** and click on **IP Filter**.
3. Review the settings below. Click **Edit** to on the new entry in the list and click **Save**.

IP Filter Rules

- **Active** – Select Enable to enable the IP filtering rule.
- **Comment** – Enter a name or description for the new IP filtering rule.

IP Filter Rules

Active ☒ Enable ☐ Disable

- **Policy** – Specifies whether the IP filter rule will allow or deny the traffic. Deny or Pass.
- **Protocol** – Click the drop-down list to select the protocol for the service to filter: **All**, **TCP**, **UDP**, or **ICMP**.
- **Schedule** – Allows you to select a schedule when the IP filter rule should be enabled or disabled.

IP Filter Rules

Policy ☒ Deny ☐ Pass

Protocol TCP ▼

Listen ☒ Enable ☐ Disable

Schedule Always ▼

Source Rule

- **Self** – If enabled, specifies the traffic source is the router. If the origination of the source traffic is not the router and another device IP address, select disabled.
- **Source Address/Mask** – This is the source IP address or device IP address or network to filter. (ex: 192.168.10.0/24, 192.168.10.120/32)
- **Source IP Group** – Click the drop-down the select an IP address or IP address range group. You can create predefined IP address groups under Advanced > IP Group.
- **Source Port** – Enter the source port for the IP filter. If you did not create and select a port group, you can manually enter it here.
- **Source Port Group** – Click the drop-down the select a predefined port or port range group. You can create predefined port groups under Advanced > Port Group.
- **Interface** – Click the drop-down list to select the source interface for the IP filter.

Source Rule

Self ☐ Enable ☒ Disable

Source Address/Mask

Source IP Group

Source Port

Source Port Group

Interface

Destination Rule

Self ☐ Enable ☒ Disable

Destination Address/Mask

Destination IP Group

Destination Port

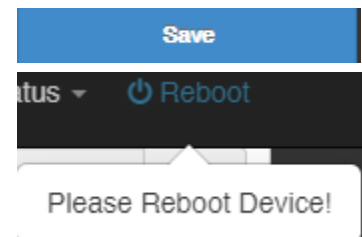
Destination Port Group

Interface

Destination Rule

- **Self** – If enabled, specifies the traffic destination is the router. If the origination of the destination traffic is not the router and another device IP address, select disabled.
- **Destination Address/Mask** – This is the destination IP address or device IP address or network to filter. (ex: 192.168.10.0/24, 192.168.10.120/32)
- **Source IP Group** – Click the drop-down the select an IP address or IP address range group. You can create predefined IP address groups under Advanced > IP Group.
- **Destination Port** – Enter the destination port for the IP filter. If you did not create and select a port group, you can manually enter it here.
- **Destination Port Group** – Click the drop-down the select a predefined port or port range group. You can create predefined port groups under Advanced > Port Group.
- **Interface** – Click the drop-down list to select the destination interface for the IP filter.

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



MAC filtering

Advanced > Access Control

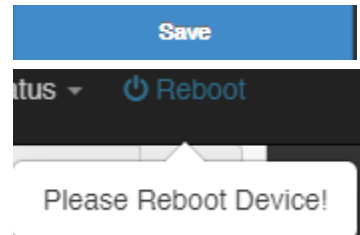
Every network device has a unique, 12-digit MAC (Media Access Control) address. MAC filtering allows you to restrict access to the Internet to specific MAC addresses on your network. You can check the current MAC addresses of devices connected to your router under System > VLAN Setup > DHCP Server under 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](#). The access control section can also be used to filter other outbound traffic by IP address, URL/keyword filter, and IM/P2P applications.

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **Advanced** and click on **Access Control**.
3. Review the settings below.
 - **Active** – Select Enable to enable the access control rule.
 - **Comment** – Enter the name or description for the access control rule.
 - **Protocol** – Click the drop-down list to select the protocol for the service to filter: **ANY, TCP, UDP, ICMP, Content Filter, Domain Filter, IP P2P, or IM.**
 - **Schedule** – Allows you to select a schedule when the access control rule should be enabled or disabled.
 - **MAC Address** – Enter the MAC address you would like to filter or deny traffic and click **Add** to add to the list. (e.g. a1:b2:c3:d4:e5:f6)

The screenshot shows the 'Access Control Rules' configuration page. At the top, there are radio buttons for 'Active', 'Enable' (selected), and 'Disable'. Below this are input fields for 'Comment', a dropdown for 'Protocol' (set to 'UDP'), and a dropdown for 'Schedule' (set to 'Always'). A section titled 'MAC Address Setup' contains a 'MAC Address' input field and an 'Add' button. Below that is a 'MAC Address List' table with columns for '#', 'MAC Address', and 'Action'.

#	MAC Address	Action
-	-	-

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



Note: Additionally, you can specify a specific IP address/range, port, and local interface to apply the access control rule. This can be a different IP address/range and does not need to be same as the IP address(es) of the MAC addresses added to the list.

IM/P2P application filtering

Advanced > Access Control

You can deny access to a list of predefined IM/P2P applications outbound and filter by MAC and/or IP address. You can check the current MAC addresses of devices connected to your router under System > VLAN Setup > DHCP Server 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](#). The access control section can also be used to filter other outbound traffic by IP address, URL/keyword filter, and IM/P2P applications.

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **Advanced** and click on **Access Control**.
3. Review the settings below.
 - **Active** – Select Enable to enable the access control rule.
 - **Comment** – Enter the name or description for the access control rule.
 - **Protocol** – Click the drop-down list to select the protocol for the service to filter: **ANY, TCP, UDP, ICMP, Content Filter, Domain Filter, IP P2P, or IM**. Select IP P2P or IM to select from a list of predefined applications.
 - **Schedule** – Allows you to select a schedule when the access control rule should be enabled or disabled.
 - **MAC Address** – Enter the MAC address you would like to filter or deny traffic and click **Add** to add to the list. (e.g. a1:b2:c3:d4:e5:f6)
Note: You can filter by MAC address or IP address.

Access Control Rules

Active

☒ Enable☐ Disable

Comment

Protocol

IP P2P

Schedule

Always

- **Local IP Address** – Enter the IP address range to apply the access control rule. (ex.: 192.168.10.20 – 192.168.10.30)
- **Local Port** – Enter the source/local port. (Optional for IP P2P/IM)
- **Comment** – Enter the name or description for the access control rule.
- **Destination IP Address** – Enter the destination IP address range for the access control rule. If left empty, this means any. (ex.: 10.10.10.20 – 10.10.10.30)
- **Destination Port** – Enter the destination port. (Optional for IP P2P/IM)
- **Interface** – Click the drop-down to select the local interface to apply the access control rule.
- **IP/P2P or IM Setup** – Select from the list of predefined P2P/IM applications to apply the access control rule.

IP Address Setup

Local IP Address

 -

Local Port

Destination IP Address

 -

Destination Port

Interface

IP P2P Setup

eDonkey/eMule/Overnet

☒ Enable☐ Disable

Direct Connect

☐ Enable☒ Disable

Kazaa

☐ Enable☒ Disable

Gnutella

☐ Enable☒ Disable

BitTorrent

☐ Enable☒ Disable

AppleJuice

☐ Enable☒ Disable

WinMX

☐ Enable☒ Disable

SoulSeek

☐ Enable☒ Disable

Ares

☐ Enable☒ Disable

IM Setup

WhatsApp

☐ Enable☒ Disable

Skype

☐ Enable☒ Disable

Facebook

☐ Enable☒ Disable

LINE

☐ Enable☒ Disable

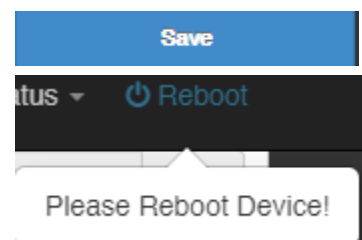
QQ

☐ Enable☒ Disable

WeChat

☐ Enable☒ Disable

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



DMZ Host

System > WAN Setup

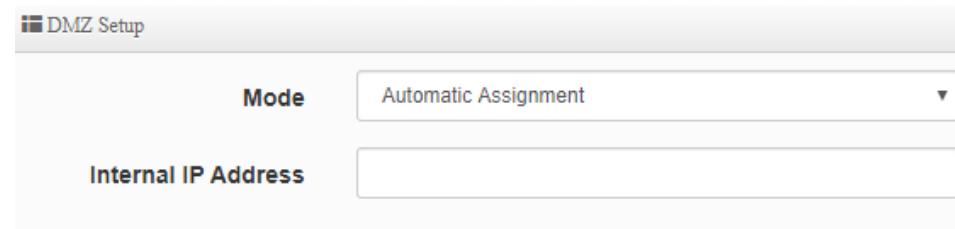
You may want to expose a specific computer or device on your network to the Internet to allow anyone to access it. Your router includes the DMZ (Demilitarized Zone) feature that makes all the ports and services available on the WAN/Internet side of the router and forwards all ports to a single IP address (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. If using multi-WAN mode, you can assign a DMZ host for each WAN interface.

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **System**, click on **WAN Setup**, and next to the WAN interface you would like to assign a DMZ host, click **Edit**.

WAN List			
#	Active	Mode	Edit
1	On	Dynamic IP	Edit

3. Under DMZ Setup, click the **Mode** drop-down list and select **Automatic Assignment**.

- **Internal 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)

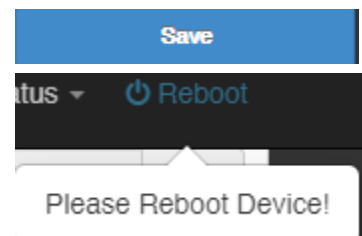


DMZ Setup

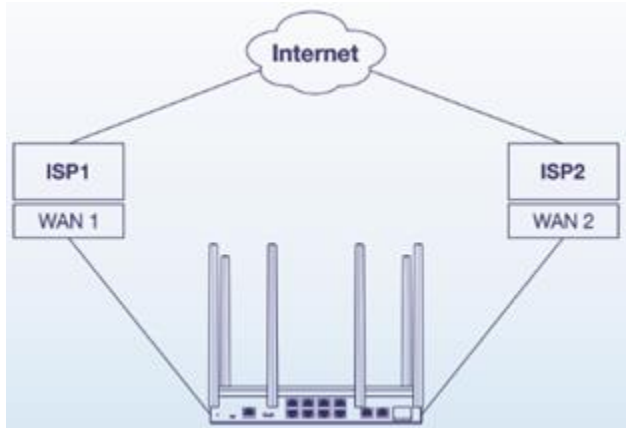
Mode: Automatic Assignment

Internal IP Address:

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



Multiple WAN Configuration



Multiple WAN Management Settings

System > WAN Setup / System > WAN Traffic Setup

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

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **System** and click on **WAN Setup**.

3. Review the settings below.

- **WAN Port** – The router can operate in two modes.
 - **4 WAN / 1 LAN Port:** 4 WAN (Ports 2-5) / 1 LAN (Port 1) or multi-WAN mode.
Note: Please note that performance throughput is limited of up to 200Mbps per WAN connection in multi-WAN mode.
 - **1 WAN / 4 LAN Port:** 1 WAN (Ports 1) / 4 LAN (Ports 2-5)
Note: Please note that the 4 LAN ports function as a 4-port LAN switch with a single IP interface, not as 4 individual LAN interface ports.
- **Primary Port** – In multi-WAN mode, this setting configures the primary WAN port used for Internet connectivity.
- **NAT Engine (1 WAN / 4 LAN Port Mode Only)** – When this setting is enabled, NAT hardware acceleration is enabled providing maximum NAT throughput/performance. It is recommended to leave this setting enabled.

WAN Port

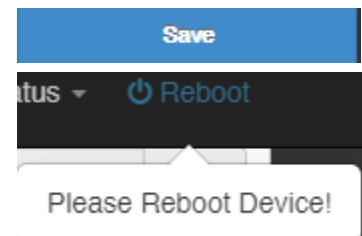
WAN Port

4 WAN / 1 LAN Port

Primary Port

WAN1

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



5. If the router is configured in multi-WAN mode, click on **System** and click on **WAN Traffic Setup** to configure the load balance settings.

Note: For WAN failover, the router will use the primary WAN port configured under System > WAN setup as the primary WAN port for Internet connectivity and failover to the next available active WAN link if the primary WAN link fails.

- **Mode** – Select the load balance mode for the multiple WAN interfaces to operate.
 - **Assign Weight** – This mode will allow you to configure a percentage assignment for each WAN interface.
 - **Connection Mode** – Select the mode for the router to determine how to send sessions out multiple WAN interfaces.
 - **Source IP based** – In this mode, if a device sends traffic through the router and forwarded to a specific WAN interface, the router will attempt to keep all future sessions originating from that device (source IP) on the same WAN interface.
 - **Source-Destination IP based** – In this mode, if a device sends traffic through the router to a specific destination IP address and forwarded to a specific WAN interface, the router will attempt to keep all future sessions originating from that device (source IP) along with same destination IP address on the same WAN interface.
 - **Per session** – In this mode, the router will randomly choose which WAN interface to forward the traffic based on each session. This may cause connectivity/stability issues with some applications or devices.

Load Balance Mode

Mode Assign Weight ▼

Connection Mode Source IP Based ▼

- **WAN Weight** – The weight is distributed as percentage across all WAN interfaces. Enter a number 1-10 to assign the WAN weight. The higher

the number/percentage, the more the router will utilize the WAN for more traffic and sessions.

Assign Weight

WAN1 Weight	10	25%
WAN2 Weight	10	25%
WAN3 Weight	10	25%
WAN4 Weight	10	25%

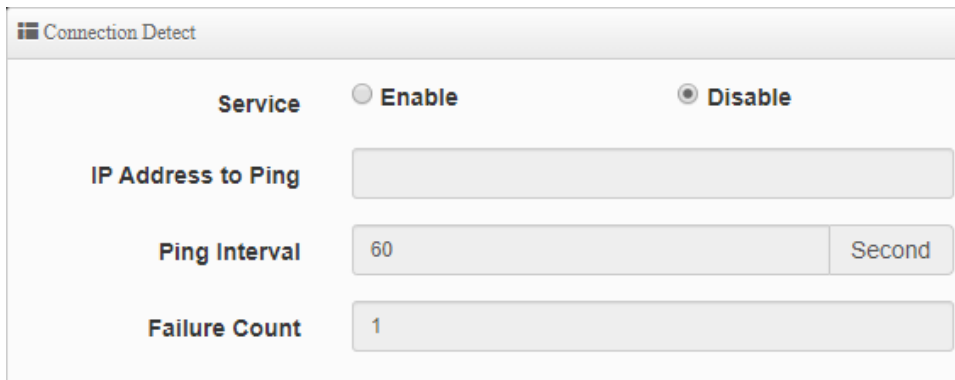
- **Line Speed Weight** – The mode allows you to specify the max. bandwidth allocated for each WAN interface.
 - **Line Speed Weight** – Enter the upload and download bandwidth for each WAN interface in Kbps.

Line Speed Weight

WAN1 (U/D)kbps	1024000	1024000
WAN2 (U/D)kbps	1024000	1024000
WAN3 (U/D)kbps	1024000	1024000
WAN4 (U/D)kbps	1024000	1024000

Connection Detect – Allows you to setup WAN link tracking by pinging Internet IP addresses instead of physical link detection.

- **Service** – Selecting Enable enables connection detection by IP address.
- **IP Address to Ping** – Enter an Internet IP address to send ping requests used to verify the Internet link status.
- **Ping Interval** – Click the drop-down list to set the time interval between consecutive ping requests in seconds.
- **Failure 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.



Connection Detect

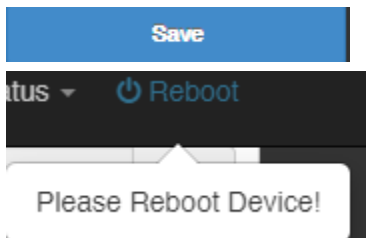
Service ☐ Enable ☒ Disable

IP Address to Ping

Ping Interval Second

Failure Count

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



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

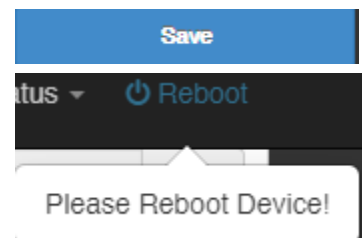
Advanced > Router Limits

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **Advanced** and click on **Router Limits™**.
3. Click the **Router Limits Mode** drop-down list and 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.

Router Limits Mode	Disable Disable Enable Enable with bandwidth monitoring (reduces LAN>WAN performance)
Status	

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



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

Router Limits Mode	Enable
Status	ready
Pairing Code	162093132352629

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...

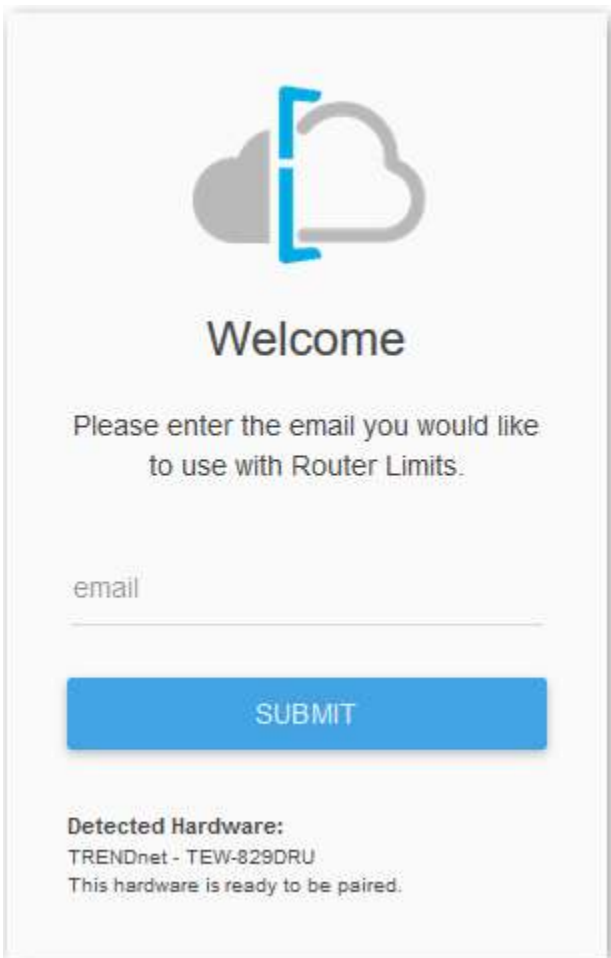
To use our service, you'll need hardware that is Router Limits Enabled.

Do you already have hardware?

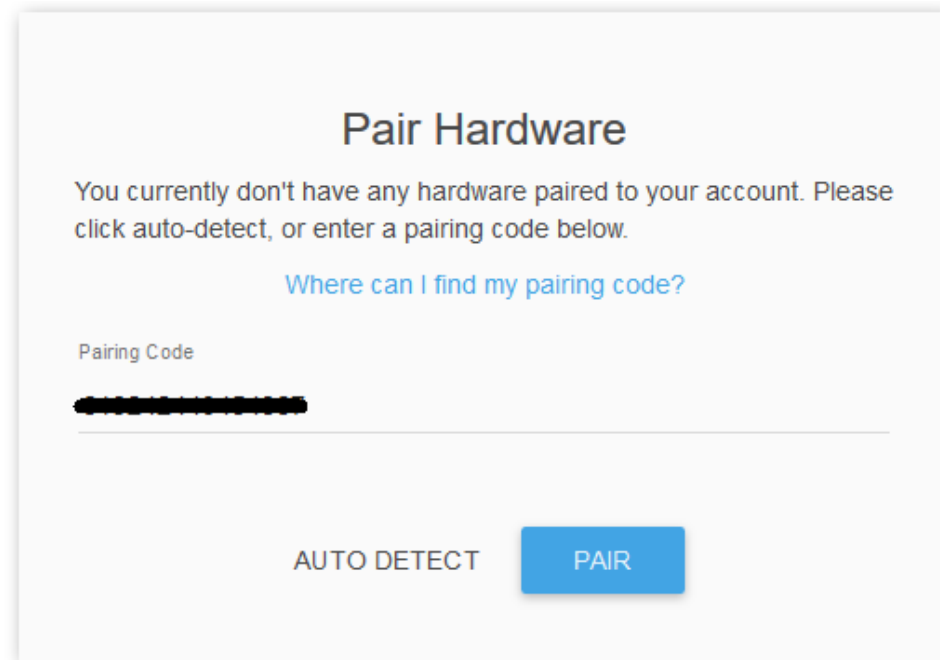
Yes, activate my hardware

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.

A screenshot of the 'Welcome' page for Router Limits. At the top is a logo consisting of a grey cloud with a blue bracket-like shape inside. Below the logo, the word 'Welcome' is centered in a large, bold, black font. Underneath, a message reads: 'Please enter the email you would like to use with Router Limits.' Below this is a text input field with the placeholder text 'email'. A large blue button with the word 'SUBMIT' in white capital letters is positioned below the input field. At the bottom, a section titled 'Detected Hardware:' shows 'TRENDnet - TEW-829DRU' and the message '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**.

A screenshot of the 'Pair Hardware' page. The title 'Pair Hardware' is centered at the top in a large, bold, black font. Below the title, a message reads: 'You currently don't have any hardware paired to your account. Please click auto-detect, or enter a pairing code below.' Underneath this is a link in blue text: 'Where can I find my pairing code?'. Below the link is a text input field with the placeholder text 'Pairing Code'. A large blue button with the word 'PAIR' in white capital letters is positioned to the right of the input field. To the left of the 'PAIR' button is a link in blue text: 'AUTO DETECT'.

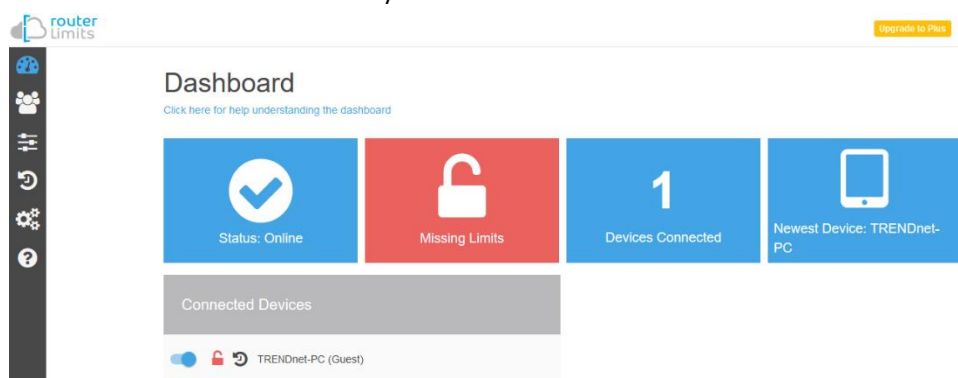
7. After your Router Limits account has been created and your router paired, you will automatically be brought to your web management dashboard. The Current Status on your router will display **Online** that the content management service is running and paired with your online account.

Current Status Online

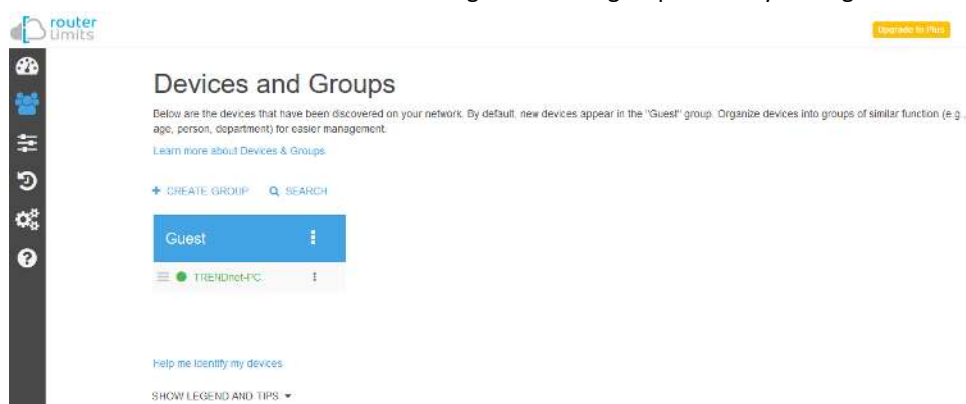
Router Limits Content Management

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.



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



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



Restrictions

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

Restrictions

☐ Block Everything: off

☐ Categories ⓘ

☐ Sites ⓘ

☐ URLs ⓘ

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

Exceptions

☐ Exceptions: off

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

☐ Safe-Search: off ⓘ

☐ YouTube Restricted Mode: off ⓘ

☐ Block Unknown Traffic: off ⓘ



- **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.

router limits [Upgrade to Plus](#)

History

History shows all requests to the Internet through your network.
[Learn more about History.](#)

SHOW FILTERS ▾
Showing all history

← back forward →

	Domain	Group	Device	Time
Jul 30, 2018				
14	unix.stackexchange.com	Guest	TRENDnet-PC	4:50:41 pm
f	www.facebook.com	Guest	TRENDnet-PC	4:50:41 pm



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

Settings

[Learn more about Settings.](#)

Router Information	Locale
Status: PROTECTING	Timezone
IP Address: 74.62.173.130	America/Los_Angeles
Pairing Code: 619242440454867	
Client Version: 2.13.2	SAVE
Interfaces:	
Name: br-lan	
MAC: 3C:8C:F8:F3:85:D6	
IP: 192.168.10.1	



- **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

System > PPTP Server Setup

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 7).
2. Click on **System** and click **PPTP Server Setup**.
3. For the Mode, select the **Enable** option to enable the PPTP server.

PPTP Server

Mode ☒ **Enable** ☐ **Disable**

4. In the **Local IP Address** field, enter an IP address other than the LAN IP address.
(Default LAN IP: 192.168.10.1) (e.g. 192.168.80.1)

Note: Entering an IP address different from 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 the LAN IP address is entered, PPTP VPN clients will be allowed to access router LAN and not the Internet.

Local IP Address 192.168.80.1

5. In the **Remote Start/End IP Address** fields, enter an IP address range (within the same Local IP Address subnet range) to assign to PPTP VPN clients.

In this example, we assigned 192.168.80.1 as the Local IP Address for the PPTP server so we will assign a range such as 192.168.80.10-192.168.80.20.

Remote Start IP Address

192.168.80.10

Remote End IP Address

192.168.80.20

6. Click **Save** at the bottom.

Save

7. Click on **System**, click on **PPTP/L2TP Account Setup**, and click **Create Account**.

Account List				
#	Username	PPTP Support	L2TP Support	Action

Create Account

8. Under Account Setup, enter the **User Name** and **Password** for the PPTP account.
(e.g. User1)

Account Setup

User Name User1

Password

9. Under Routing Rule, enter the Local Subnet the remote PPTP VPN clients will be allowed to access, for example, the default LAN IP subnet (e.g. 192.168.10.0/24) and for the Remote Subnet, enter the IP subnet assigned to PPTP VPN clients configured under System > and PPTP Server Setup. (e.g. 192.168.80.0/24)
click **Add** to add to the Routing Rule List.

Note: For remote PPTP VPN clients to access additional Local subnets, add additional routing rules for the other IP subnets.

Routing Rule

Local Subnet

192.168.10.0/24

Remote Subnet

192.168.80.0/24

Add

Routing Rule List

#	Local Subnet	Remote Subnet	Action
1	192.168.10.0/24	192.168.80.0/24	Delete

10. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.

Save

Status Reboot

Please Reboot Device!

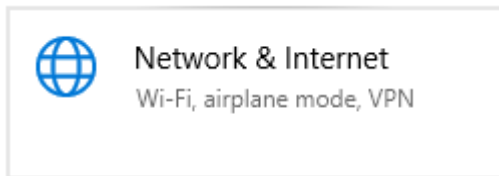
Setting up the PPTP VPN client (Windows)

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.



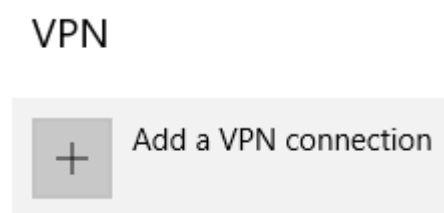
2. Click **Network & Internet**.



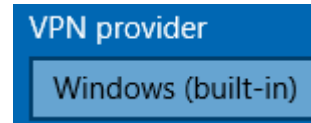
3. Click **VPN** in the left panel.



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



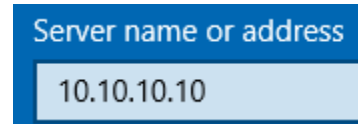
5. Click the **VPN provider** drop-down list and select **Windows (built-in)**.



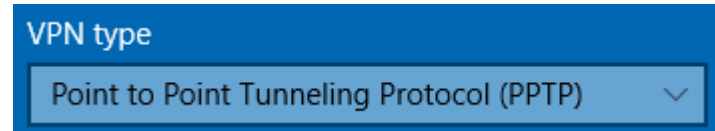
6. Enter a name in the **Connection name** field.



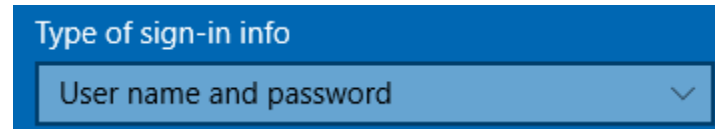
7. Enter the Internet WAN IP address, DNS, or dynamic DNS hostname of your router to connect over the Internet. In the example below, the Internet WAN IP address of the router is 10.10.10.10. In your router, you can check the WAN IP address under **Status > Overview**, under **WAN**.



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 TWG-431BR router. Click **Save**.

User name (optional)
user1

Password (optional)
.....

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

Connect Advanced options Remove

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

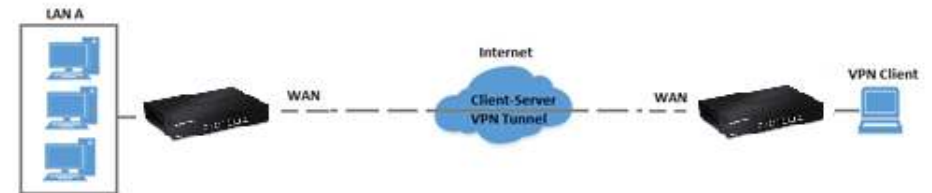
Connected

Advanced options Disconnect

L2TP VPN Server

System > L2TP Server Setup

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 7).
2. Click on **System** and click **L2TP Server Setup**.
3. For the Mode, select the **Enable** option to enable the L2TP server.

L2TP Server

Mode ☒ Enable ☐ Disable

4. In the **Local IP Address** field, enter an IP address other than the LAN IP address. (Default LAN IP: 192.168.10.1) (e.g. 192.168.80.1)

Note: Entering an IP address different from 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 the LAN IP address is entered, L2TP VPN clients will be allowed to access router LAN and not the Internet.

Local IP Address 192.168.80.1

5. In the **Remote Start/End IP Address** fields, enter an IP address range (within the same Local IP Address subnet range) to assign to L2TP VPN clients.

In this example, we assigned 192.168.80.1 as the Local IP Address for the L2TP server so we will assign a range such as 192.168.80.10-192.168.80.20.

Remote Start IP Address

192.168.80.10

Remote End IP Address

192.168.80.20

6. Click **Save** at the bottom.

Save

7. Click on **System**, click on **PPTP/L2TP Account Setup**, and click **Create Account**.

Account List				
#	Username	PPTP Support	L2TP Support	Action
				Create Account

8. Under Account Setup, enter the **User Name** and **Password** for the L2TP account.
(e.g. User1)

Account Setup

User Name User1

Password

9. Under Routing Rule, enter the Local Subnet the remote L2TP VPN clients will be allowed to access, for example, the default LAN IP subnet (e.g. 192.168.10.0/24) and for the Remote Subnet, enter the IP subnet assigned to L2TP VPN clients configured under System > and L2TP Server Setup. (e.g. 192.168.80.0/24)

click **Add** to add to the Routing Rule List.

Note: For remote L2TP VPN clients to access additional Local subnets, add additional routing rules for the other IP subnets.

Routing Rule

Local Subnet 192.168.10.0/24

Remote Subnet 192.168.80.0/24 **Add**

Routing Rule List			
#	Local Subnet	Remote Subnet	Action
1	192.168.10.0/24	192.168.80.0/24	Delete

10. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.

Save

Status **Reboot**

Please Reboot Device!

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 7).

2. Click on **System** and click **L2TP Server Setup**.

3. For the Mode, select the **Enable** option to enable the L2TP server.

L2TP Server

Mode ☒ **Enable** ☐ **Disable**

4. In the **Local IP Address** field, enter an IP address other than the LAN IP address. (Default LAN IP: 192.168.10.1) (e.g. 192.168.80.1)

Note: Entering an IP address different from 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 the LAN IP address is entered, L2TP VPN clients will be allowed to access router LAN and not the Internet.

Local IP Address 192.168.80.1

5. In the **Remote Start/End IP Address** fields, enter an IP address range (within the same Local IP Address subnet range) to assign to L2TP VPN clients.

In this example, we assigned 192.168.80.1 as the Local IP Address for the L2TP server so we will assign a range such as 192.168.80.10-192.168.80.20.

Remote Start IP Address 192.168.80.10

Remote End IP Address 192.168.80.20

6. Under L2TP Over IPsec Settings, for the Mode, select **Enable**.

L2TP Over IPsec Settings

Mode ☒ **Enable** ☐ **Disable**

7. Enter the **Pre-shared Key** for IPsec encryption.

Pre-shared Key

8. Click the **WAN ID** drop-down list to select the correct WAN interface for the L2TP over IPsec server.

WAN ID WAN1

9. Click **Save** at the bottom.

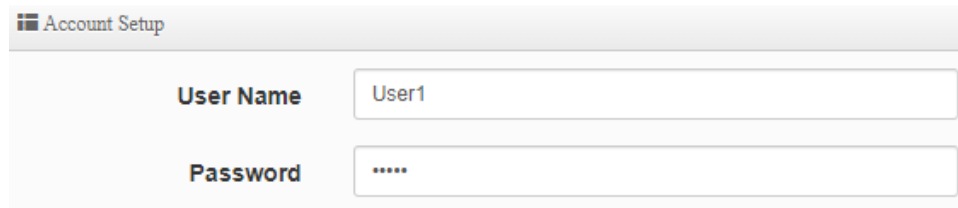
Save

10. Click on **System**, click on **PPTP/L2TP Account Setup**, and click **Create Account**.

#	Username	PPTP Support	L2TP Support	Action
-	-	-	-	-

11. Under Account Setup, enter the **User Name** and **Password** for the L2TP account.

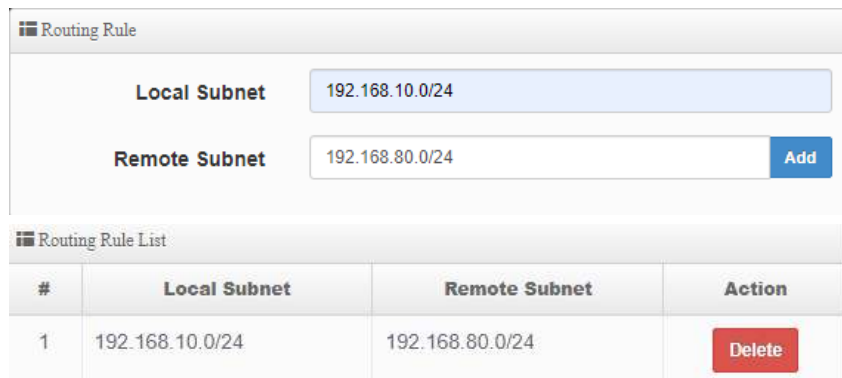
(e.g. User1)



12. Under Routing Rule, enter the Local Subnet the remote L2TP VPN clients will be allowed to access, for example, the default LAN IP subnet (e.g. 192.168.10.0/24) and for the Remote Subnet, enter the IP subnet assigned to L2TP VPN clients configured under System > and PPTP Server Setup. (e.g. 192.168.80.0/24)

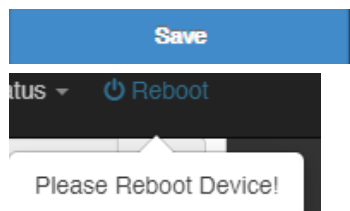
click **Add** to add to the Routing Rule List.

Note: For remote L2TP VPN clients to access additional Local subnets, add additional routing rules for the other IP subnets.



#	Local Subnet	Remote Subnet	Action
1	192.168.10.0/24	192.168.80.0/24	Delete

13. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



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.

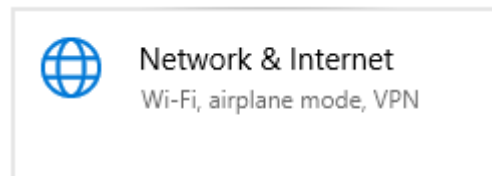


Start Button



Settings icon

2. Click **Network & Internet**.

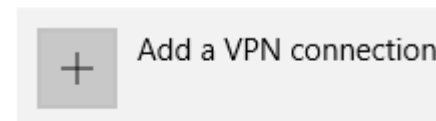


3. Click **VPN** in the left panel.

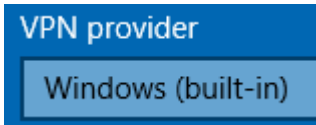


4. Under VPN, click **Add a VPN connection**.

VPN



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



VPN provider

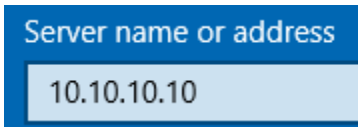
Windows (built-in)

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



Connection name

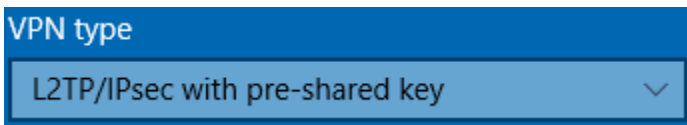
7. Enter the Internet WAN IP address, DNS, or dynamic DNS hostname of your router to connect over the Internet. In the example below, the Internet WAN IP address of the router is 10.10.10.10. In your router, you can check the WAN IP address under **Status > Overview**, under **Network** in the IPv4 status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



Server name or address

10.10.10.10

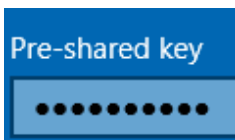
8. Click the **VPN type** drop-down list and select **L2TP/IPsec with pre-shared key**.



VPN type

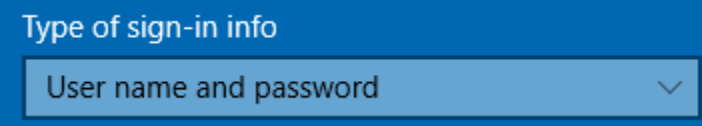
L2TP/IPsec with pre-shared key

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



Pre-shared key

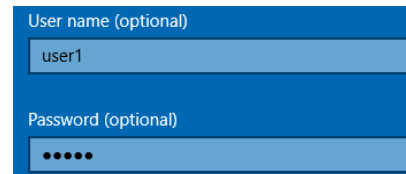
10. Click the **Type of sign-in info** drop-down list and select **User name and password**.



Type of sign-in info

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 L2TP with IPsec VPN connection to your TWG-431BR router. Click **Save**.



User name (optional)

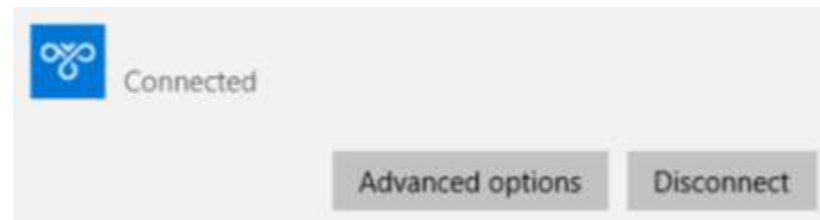
user1

Password (optional)

.....

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

12. The status will display **Connected** if the L2TP with IPsec VPN connection was successful.



Connected

Advanced options Disconnect

IPsec (Internet Protocol Security)

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

System > IPsec Setup

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.

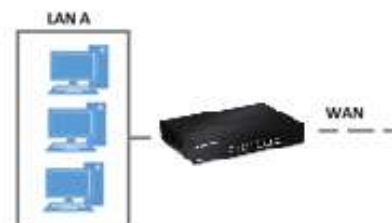
Note: Changing the LAN IP address of your router will change the LAN IP network of your router.

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



- Log into your router management page (see "[Access your router management page](#)" on page 7).
- Click on **System** and click **IPsec Server Setup**.
- Under IPsec List, click **Create New IPsec**.

IPsec List							Create New IPsec
#	Active	WAN	Mode	Local Subnet	Remote Subnet	Action	
1	-	-	-	-	-	-	-

- For the Service, select **Enable**.

IPsec Service

Service ☒ Enable ☐ Disable

- Click the Mode drop-down list and select **LAN-to-LAN**.

Mode LAN-to-LAN ▼

6. For the **Local ID Type**, select **IP Address**.

Local ID Type ☒ **IP Address** ☐ **FQDN**

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

Local Subnets 192.168.10.0/24

8. For the **Remote ID Type**, select **IP Address**.

Remote ID Type ☒ **IP Address** ☐ **FQDN**

9. In the **Remote Subnets** field, enter the remote LAN IP subnet. (e.g. 192.168.100.0/24)
You can add additional local subnets if needed. (e.g. 192.168.100.0/24,192.168.120.0/24)

Remote Subnets 192.168.100.0/24

10. In the **Remote Host** 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 Host 10.10.10.20

11. Enter the **Pre-Shared Key** (PSK) for the IPsec VPN tunnel. (e.g. 1234567890)

Pre-shared Key 1234567890

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

IPsec Settings	
Mode	LAN-to-LAN
Local ID Type	☒ IP Address ☐ FQDN
Local ID	
Router A Local Subnets LAN IP Network	192.168.10.0/24
Local Nexthop	0.0.0.0
Remote ID Type	☒ IP Address ☐ FQDN
Remote ID	
Router B Remote Subnets LAN IP Network	192.168.100.0/24
Remote Nexthop	0.0.0.0
Router B Remote Host WAN IP Address	10.10.10.20
Pre-shared Key	1234567890

12. For the **DPD** setting, select **Enable**.

DPD ☒ **Enable** ☐ **Disable**

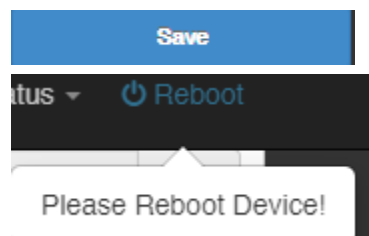
13. For the IKE Policy, **IKE Mode: Main**, **IKE Authentication: SHA1**, and **DH Group: DH2**.

IKE Mode	☒ Main ☐ Aggressive
IKE Authentication	SHA1 ▼
Encryption	3DES ▼
DH Group	DH2 ▼

14. For the IPsec Policy, **ESP Authentication: SHA1**, and **Perfect Forward Secrecy: Enable/DH Group: DH2**.

Security Protocol	ESP ▼
ESP Authentication	SHA1 ▼
ESP Encryption	3DES ▼
Perfect Forward Secrecy	☒ Enable ☐ Disable
DH Group	DH2 ▼

15. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



VPN Router B Configuration



1. Log into your router management page (see "[Access your router management page](#)" on page 7).

2. Click on **System** and click **IPsec Server Setup**.

3. Under IPsec List, click **Create New IPsec**.

IPsec List						
#	Active	WAN	Mode	Local Subnet	Remote Subnet	Action
1	-	-	-	-	-	-

Create New IPsec

4. For the Service, select **Enable**.

IPsec Service

Service ☒ Enable ☐ Disable

5. Click the Mode drop-down list and select **LAN-to-LAN**.

Mode LAN-to-LAN ▼

6. For the **Local ID Type**, select **IP Address**.

Local ID Type ☒ IP Address ☐ FQDN

7. In the **Local Subnets** field, enter the local LAN IP subnet. (e.g. 192.168.100.0/24).
You can add additional local subnets if needed. (e.g. 192.168.10.0/24,192.168.120.0/24)

Local Subnets 192.168.100.0/24

8. For the **Remote ID Type**, select **IP Address**.

Remote ID Type ☒ IP Address ☐ FQDN

9. In the **Remote Subnets** field, enter the remote LAN IP subnet. (e.g. 192.168.10.0/24)
You can add additional local subnets if needed. (e.g. 192.168.10.0/24,192.168.20.0/24)

Remote Subnets 192.168.10.0/24

10. In the **Remote Host** 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 Host 10.10.10.10

11. Enter the **Pre-Shared Key (PSK)** for the IPsec VPN tunnel. (e.g. 1234567890)

Pre-shared Key 1234567890

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

IPsec Settings

Mode	LAN-to-LAN
Local ID Type	☒ IP Address ☐ FQDN
Local ID	
Router B Local Subnets LAN IP Network	192.168.100.0/24
Local Nexthop	0.0.0.0
Remote ID Type	☒ IP Address ☐ FQDN
Remote ID	
Router A Remote Subnets LAN IP Network	192.168.10.0/24
Remote Nexthop	0.0.0.0
Router A Remote Host WAN IP Address	10.10.10.10
Pre-shared Key	1234567890

12. For the DPD setting, select **Enable**.

DPD ☒ Enable ☐ Disable

13. For the IKE Policy, **IKE Mode: Main**, **IKE Authentication: SHA1**, and **DH Group: DH2**.

IKE Mode	☒ Main ☐ Aggressive
IKE Authentication	SHA1
Encryption	3DES
DH Group	DH2

14. For the IPsec Policy, **ESP Authentication: SHA1**, and **Perfect Forward Secrecy: Enable/DH Group: DH2**.

Security Protocol	ESP
ESP Authentication	SHA1
ESP Encryption	3DES
Perfect Forward Secrecy	☒ Enable ☐ Disable
DH Group	DH2

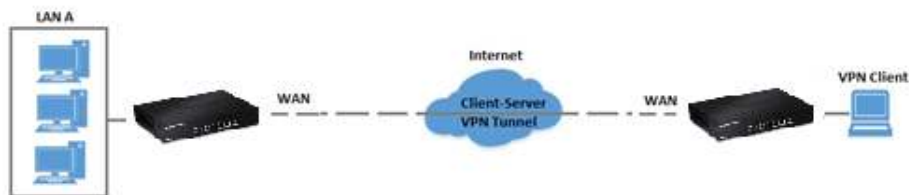
15. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.

Save

Status ☒ Reboot

Please Reboot Device!

Setting up IPsec server VPN (PSK)



1. Log into your router management page (see "[Access your router management page](#)" on page 7).

2. Click on **System** and click **IPsec Setup**.

3. Under IPsec List, click **Create New IPsec**.

IPsec List						
#	Active	WAN	Mode	Local Subnet	Remote Subnet	Action
1	-	-	-	-	-	-

Create New IPsec

4. For the Service, select **Enable**.

IPsec Service

Service ☒ **Enable** ☐ **Disable**

5. Click the Mode drop-down list and select **Client-to-LAN**.

Mode Client-to-LAN

6. For the Local ID Type, select **IP Address**.

Local ID Type ☒ **IP Address** ☐ **FQDN**

7. In the **Local Subnets** field, enter the local LAN IP subnet. (e.g. 192.168.100.0/24).

You can add additional local subnets if needed. (e.g. 192.168.10.0/24,192.168.120.0/24)

Local Subnets

192.168.100.0/24

8. For the Remote ID Type, select **IP Address**.

Remote ID Type

☒ **IP Address**

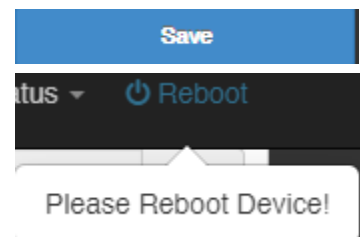
☐ **FQDN**

9. Enter the **Pre-Shared Key** (PSK) for the IPsec VPN tunnel. (e.g. 1234567890)

Pre-shared Key

1234567890

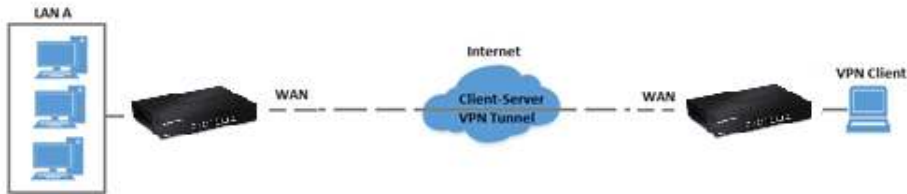
10. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



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.

Secure Socket Layer VPN (SSL) / OpenVPN

System > SSL VPN Setup



SSL VPN Server Setup

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **System** and click on **SSL VPN Server Setup**.
3. For the Mode, select **Enable**.



4. Click **Save** at the bottom.

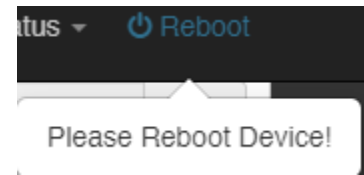


5. Wait the router to generate a new OpenVPN key. This may take up to 2 minutes.

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.



6. Then click **Reboot** at the top right to commit the changes.



7. Next to Client configuration files, 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

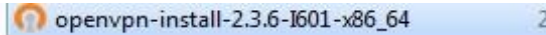
Below is a reference of the additional SSL VPN settings if you choose to make other configuration changes to these sections.

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

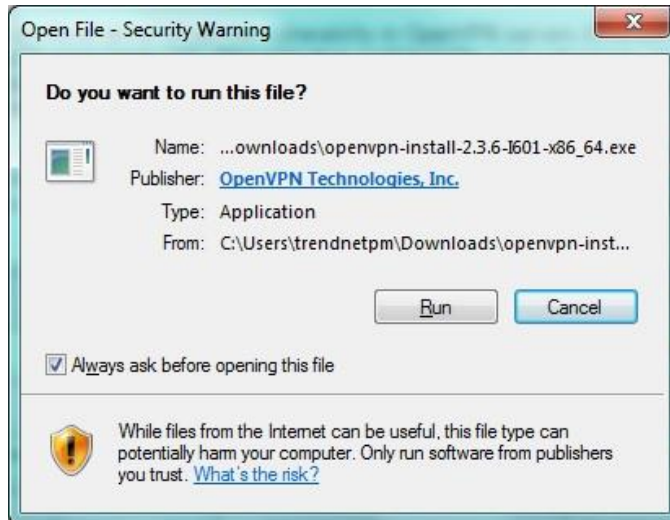
- **OpenVPN Protocol** – Used to change the default protocol. UDP or TCP.
- **Port** – Used to change the default SSL VPN server port number.
- **Subnet**– Used to change the default IP address subnet and IP address range to distribute to SSL VPN clients.
- **Subnet Mask**– Used to change the default IP subnet mask to distribute to SSL VPN clients.

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.



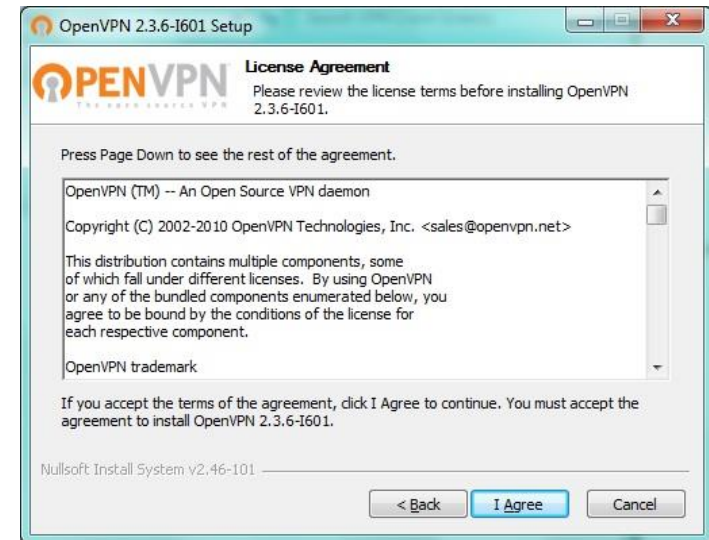
4. If prompted to run the file, click **Run**.



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



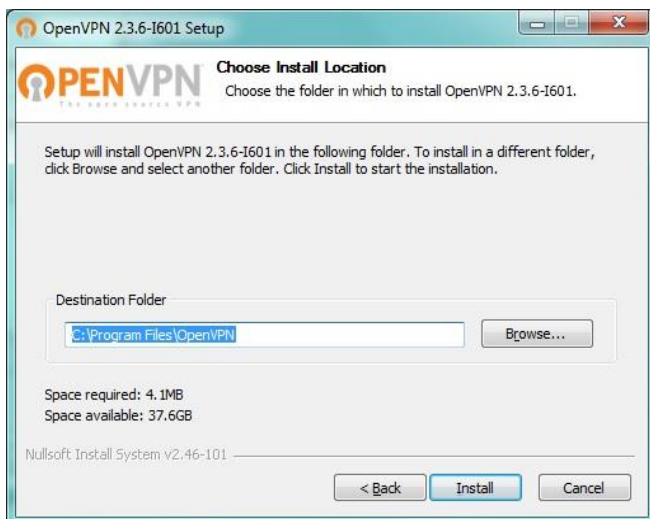
6. At the license agreement window, review the license agreement and click **I Agree**.



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



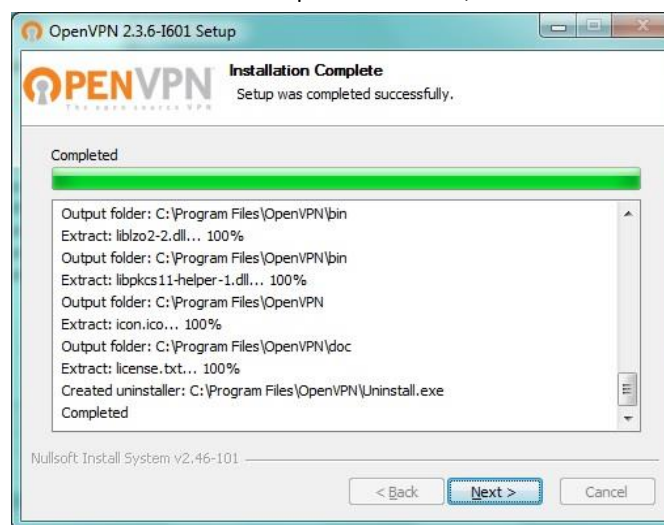
8. At the install location window, click **Install**.



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



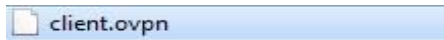
10. At the installation completion window, click **Next**.



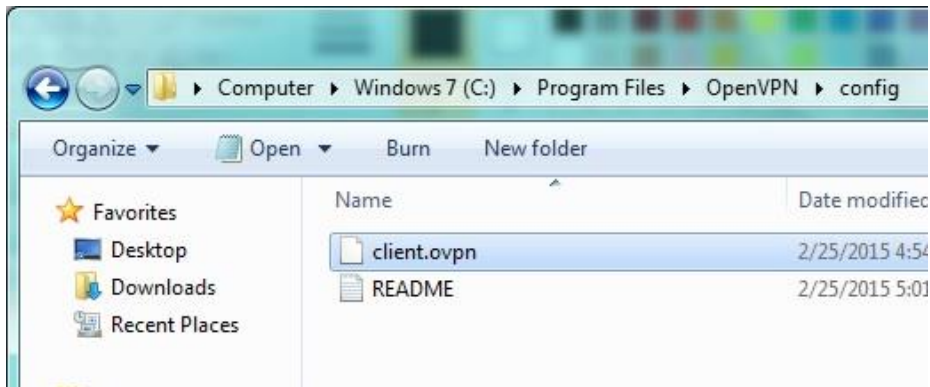
11. Make sure to uncheck the “Show Readme” and “Start OpenVPN GUI” options and click **Finish**.



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



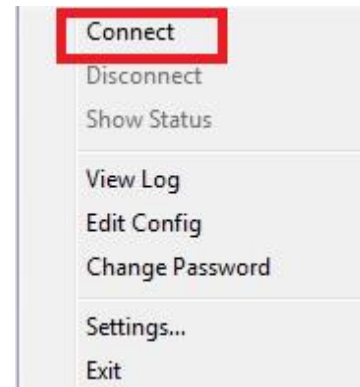
13. Double-click on the OpenVPN GUI shortcut on your desktop to start the OpenVPN Client software.



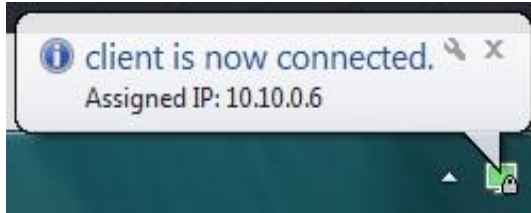
14. The OpenVPN system tray icon will appear in the bottom right corner. Right-click the icon to display the configuration menu.



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**.

High Availability

Configuring a high availability cluster

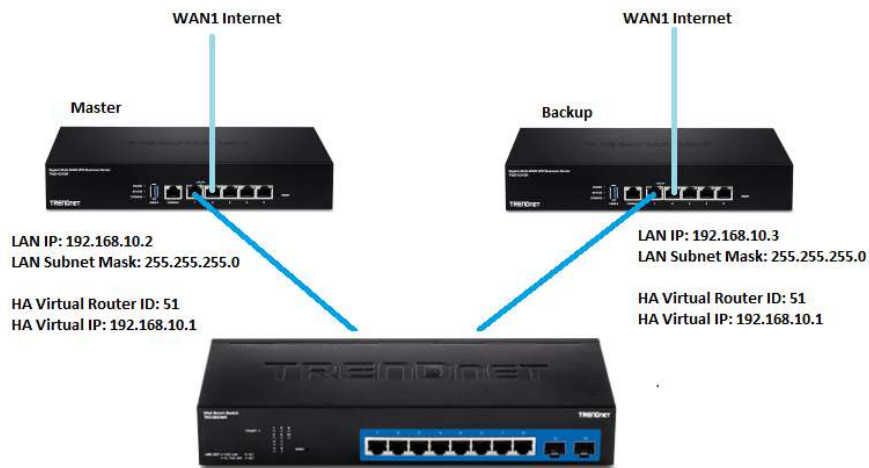
System > High Availability

What is high availability?

High availability allows you to configure multiple TWG-431BR routers to backup routers as fault tolerance in case the primary router fails. The TWG-431BR 1 master and 5 standby in a high availability cluster.

In the example below, we will use 2 TWG-431BR routers in a high availability cluster. Both router LAN interfaces are connected to the same LAN side switch. Assuming both routers have different WAN IP Internet connections possibly to the same ISP or different ISPs, the example below will explain how to configure LAN side High Availability.

Important Note: Configure the routers for HA configuration first before connecting them to the network.



Router 1 Master HA Configuration

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click **System** and click on **WAN Setup** and under **DNS**, enter the **DNS1** and **DNS2** server IP addresses to ensure DNS can be resolved for LAN/VLAN2 devices, then click **Save** at the bottom.

DNS

DNS1 8.8.8.8

DNS2 8.8.4.4

3. Click **System** and click on **VLAN Setup**.

4. Under **VLAN1** in the list, click on **Network**.

#	VLAN Mode	Flap	IP Address	Netmask	Action
1	On	None	192.168.10.1	255.255.255.0	Network

5. Change the **IP Address** to **192.168.10.2** and click **Save** at the bottom of the page.

IP Setup

IP Address 192.168.10.2

Netmask 255.255.255.0

6. Click on **System** and click on **High Availability**.

7. For the **Service**, select **Enable** and click **Save** at the bottom.

Note: Please note that the state of the high availability setup is set to Master by default.

The screenshot shows two configuration sections. The top section, titled 'Service', has a radio button for 'Enable' selected. The bottom section, titled 'High Availability Setup', has a radio button for 'Master' selected. Below this, there are three input fields: 'Virtual Router ID' with the value '51', 'Priority' with the value '100', and 'Advert Interval' with the value '1' and a unit dropdown set to 'Seconds'.

Service	
Service	☒ Enable ☐ Disable

High Availability Setup	
State	☒ Master ☐ Backup
Virtual Router ID	51
Priority	100
Advert Interval	1 Seconds

8. In the Virtual IP Setup list, under **VLAN1**, click on **Edit**.

The screenshot shows a table with one row for 'VLAN1'. The 'Status' column shows 'Off'. The 'Edit' button in the 'Action' column is highlighted with a red box.

VLAN	Status	Action
VLAN1	Off	Edit

9. For the **Service**, select **Enable**.

The screenshot shows the 'Service' configuration section with the 'Enable' radio button selected.

Service	
Service	☒ Enable ☐ Disable

10. Under Virtual IP Settings, for the **Virtual IP**, enter **192.168.10.1** and enter an 8 character password in the **Password** field.

The screenshot shows the 'Virtual IP Settings' page. The 'Virtual IP' field contains '192.168.10.1'. The 'Authentication Type' has 'PASS' selected. The 'Password' field contains '12345678'.

Virtual IP Settings	
Virtual IP	192.168.10.1
Authentication Type	☒ PASS ☐ AH
Password	12345678

11. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.

The screenshot shows a 'Save' button and a 'Reboot' button. A tooltip message 'Please Reboot Device!' is displayed over the 'Reboot' button.

[Save](#) [Reboot](#)

Please Reboot Device!

Router 2 Backup HA Configuration

1. Log into your router management page (see "[Access your router management page](#)" on page 7).

2. Click **System** and click on **WAN Setup** and under **DNS**, enter the **DNS1** and **DNS2** server IP addresses to ensure DNS can be resolved for LAN/VLAN2 devices, then click **Save** at the bottom.

DNS

DNS1

DNS2

3. Click **System** and click on **VLAN Setup**.

4. Under **VLAN1** in the list, click on **Network**.

#	VLAN Mode	Flap	IP Address	Netmask	Action
1	On	Stable	192.168.10.1	255.255.255.0	Network

5. Change the **IP Address** to **192.168.10.2** and click **Save** at the bottom of the page.

IP Setup

IP Address

Netmask

6. Click on **System** and click on **High Availability**.

7. For the **Service**, select **Enable**. Under High Availability Setup, for the **State**, click **Backup** and click **Save** at the bottom.

Note: Please note that the state of the high availability setup is set to Master by default. The Virtual Router ID must be the same for all routers configured in the same high availability cluster.

Service

Service ☒ **Enable** ☐ **Disable**

High Availability Setup

State ☐ **Master** ☒ **Backup**

Virtual Router ID

Priority

Advert Interval **Seconds**

8. In the Virtual IP Setup list, under **VLAN1**, click on **Edit**.

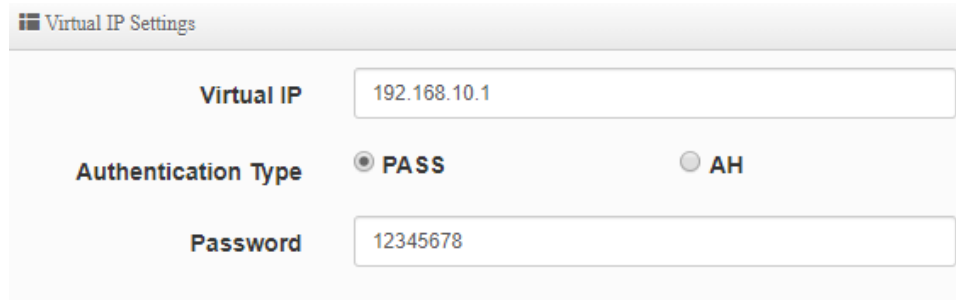
VLAN1	Off	Edit
--------------	------------	-------------

9. For the **Service**, select **Enable**.

Service

Service ☒ **Enable** ☐ **Disable**

10. Under Virtual IP Settings, for the **Virtual IP**, enter **192.168.10.1** and enter an 8 character password in the **Password** field.



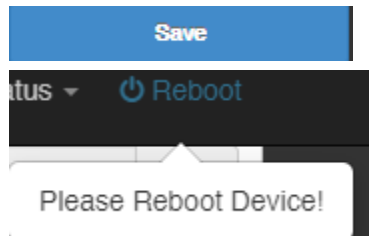
Virtual IP Settings

Virtual IP 192.168.10.1

Authentication Type ☒ PASS ☐ AH

Password 12345678

11. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



12. Connect the routers to the network and verify the high availability configuration by testing Internet connectivity from the LAN/VLAN1 side switch and disconnecting the LAN/VLAN1 link on the master router from the network.

Router Maintenance and Monitoring

Managing access to the router management interface

System > 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/VLAN1 interface.

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click **System** and click on **Management**.
3. Review the settings below.

Login Methods

- **HTTP** – By default HTTP access is enabled using the default HTTP port 80. The default management port can be modified. Please note that modifying the port will affect HTTP access from all allowed interfaces.
- **HTTPS** – Checking this option will enable secure HTTPS (SSL) access to the router management page on the selected local interfaces. The default HTTPS management port can be modified. Please note that modifying the port will affect HTTPS access from all allowed interfaces.
- **Telnet** – Checking this option will enable command line interface access via Telnet on the selected local interfaces. The default Telnet management port can be modified. Please note that modifying the port will affect Telnet access from all allowed interfaces.
- **SSH** – Checking this option will enable secure command line interface access via SSH (Secure Shell) on the selected local interfaces. . The default SSH management port can be modified. Please note that modifying the port will affect SSH access from all allowed interfaces.
- **Host Key Footprint** – The RSA key used for SSH management can be randomly generated to a new key by clicking **Generate Key**.

Login Methods

HTTP	☒	80	Port
HTTPS	☐	443	Port
Telnet	☐	23	Port
SSH	☐	22	Port

Host Key Footprint

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAA

Generate Key

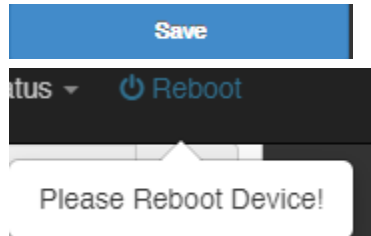
Management Access

By default, management access is only allowed through the LAN/VLAN1 interface. Select **Enable** for the other interfaces to allow local/remote management access.

Management Access

VLAN1	☒ Enable	☐ Disable
VLAN2	☐ Enable	☒ Disable
VLAN3	☐ Enable	☒ Disable
VLAN4	☐ Enable	☒ Disable
VLAN5	☐ Enable	☒ Disable
VLAN6	☐ Enable	☒ Disable
VLAN7	☐ Enable	☒ Disable
VLAN8	☐ Enable	☒ Disable
WAN1	☐ Enable	☒ Disable
WAN2	☐ Enable	☒ Disable
WAN3	☐ Enable	☒ Disable
WAN4	☐ Enable	☒ Disable

10. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



Diagnostic tools

Maintenance > Network Utility

This section includes network utilities (ping and traceroute) for testing connectivity and troubleshooting.

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **Maintenance** and click on **Network Utility**.

3. Review the settings below.

Network Utilities

- **Ping Utility** – This tool conducts a basic ping/connectivity test to a host IP address or domain name.
 - **IP/Domain** – Enter the destination IP or domain name to test connectivity.
 - **Times** – Enter the number of ping requests to send and click **Ping** to start the ping test.

 Ping Utility

IP/Domain

Times **Ping**

- **Traceroute** – This tool conducts a test to check the routing path taken to reach a specific destination host IP address or domain name.
 - **Destination Host** – Enter the host IP address test connectivity.
 - **Max. Hops** – Enter the max number of hops for the traceroute and click **Start** to start the traceroute test.

 Traceroute

Destination Host **Start**

Max. Hops **Stop**

Backup and restore your router configuration settings

Maintenance > Profile Setting

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 7).
2. Click on **Maintenance**, then click on **Profile Setting**.
3. Next to Save Settings To PC, click **Save**.

Save Settings To PC

Save

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: *config.bin*)

To restore your router configuration:

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **Maintenance**, then click on **Profile Setting**.
3. Next to Load Settings From PC, click **Choose File** or **Browse**.

Load Settings From PC

Choose File No file chosen

Upload

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

Reboot your router

Maintenance >

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 7).
2. Click on **Maintenance** then click on **Reboot**.
3. On the page, click **Reboot**.

Reboot

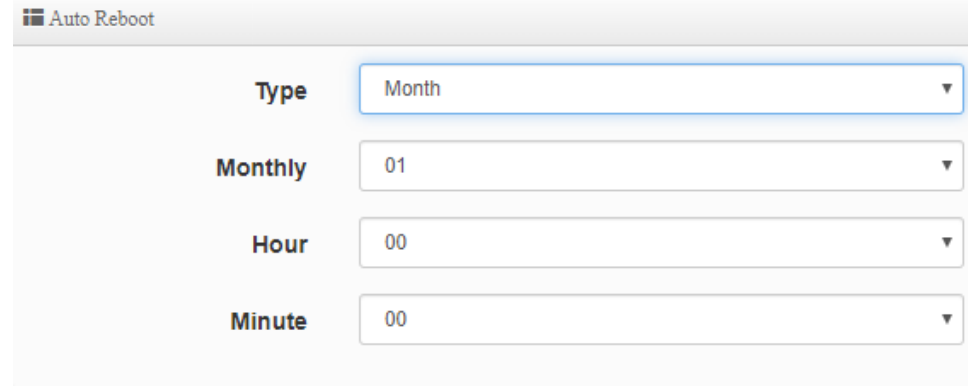
4. Wait for the device to reboot.

Scheduled automatic reboot

System > Management

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.

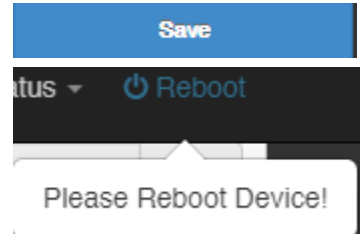
1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **System** and click on **Management**.
3. Click the Automatic reboot by schedule drop-down list and select the schedule used for the automatic device reboot function. Click **Apply** to save and commit the changes.
3. Under Wake On LAN, review the settings below.
 - **Type:** Clicking the drop-down list allows you to specify a schedule when to reboot the router. Daily, Weekly, Monthly.
 - **Monthly/Weekly:** If selecting to specify a schedule under Type, monthly will allow you to choose which day every month and weekly will allow you to choose which day every week.
 - **Hour/Minute:** Specify the hour and minute (24-hour format).
Note: If setting a schedule, please make sure the router time settings are setup correctly under System > Time Server.



Auto Reboot

Type	Month
Monthly	01
Hour	00
Minute	00

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



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)	57600
Data Bits	8
Parity Bits	None
Stop Bits	1
Hardware Flow Control	Off

Router Default Settings

Administrator User Name	admin
Administrator Password	admin
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
Default WAN Mode	4 WAN (Ports 2-5) / 1 LAN (Port 1)

Reset your router to factory defaults

Maintenance > Profile Setting

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 7).
2. Click on **Maintenance**, then click on **Profile Setting**.
3. Next to Reset to Factory Default, click **Default**. When prompted to confirm this action, click **OK**.

Reset To Factory Default

Default

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

Upgrade your router firmware

Maintenance > Upgrade 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>

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.

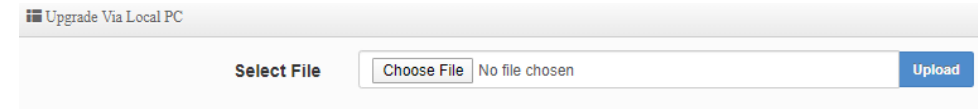
Please note the following:

- 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 7).

2. Click on **Maintenance** and click on **Upgrade Firmware**.

3. Depending on your web browser, in the Flash new firmware image section, click **Browse** or **Choose File**.



4. Navigate to the folder on your computer where the unzipped firmware file (webimg_TWG-431BR) is located, select it and click **Upload**. When prompted to confirm this action, click **OK**. Please wait for the online firmware upgrade procedure to complete successfully.

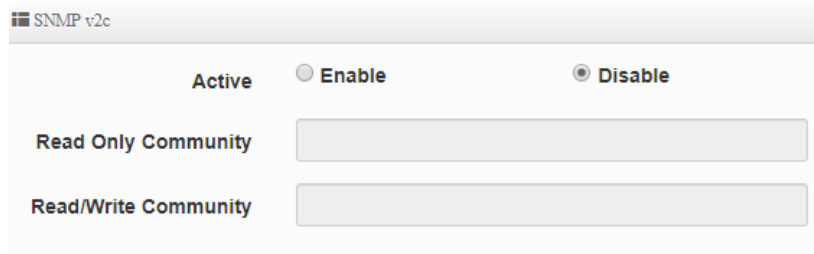
Note: The router also supports firmware upgrade from external sources such as TFTP (requires external TFTP server) or HTTP URL.

SNMP Settings

System > SNMP

The router also supports SNMP v1/2c/3 management and SNMP trap receivers. You can configure the SNMP management settings following the steps below.

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **System** and click on **Management**.
3. Review the settings below.

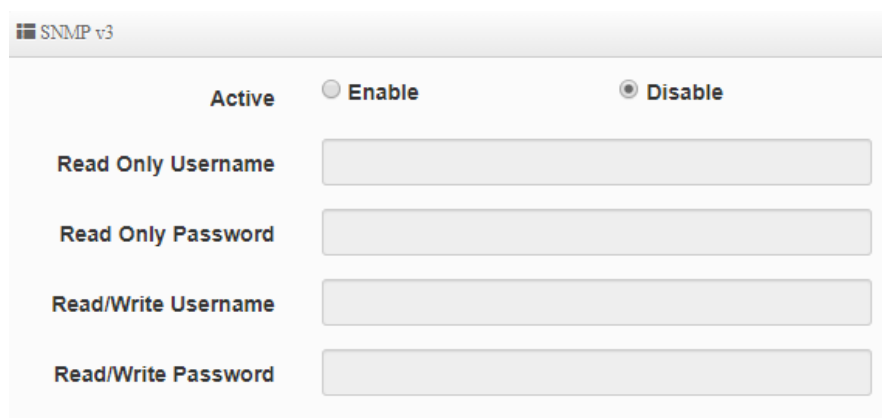


SNMP v2c

Active ☐ Enable ☐ **Disable** ☒

Read Only Community

Read/Write Community



SNMP v3

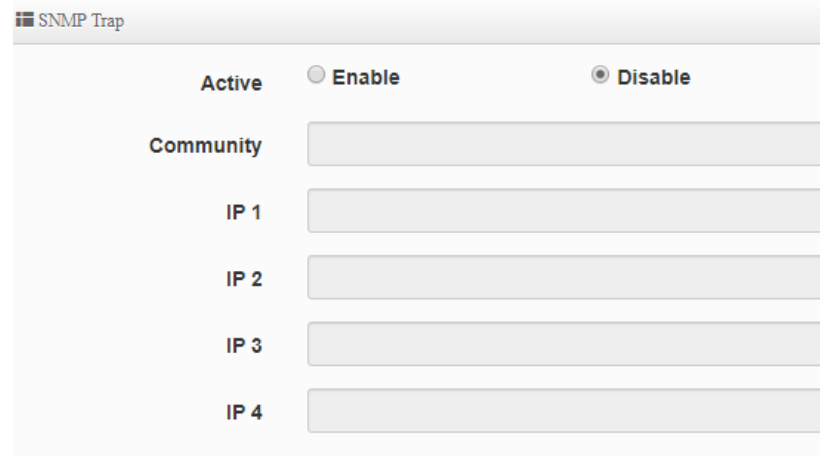
Active ☐ Enable ☐ **Disable** ☒

Read Only Username

Read Only Password

Read/Write Username

Read/Write Password



SNMP Trap

Active ☐ Enable ☐ **Disable** ☒

Community

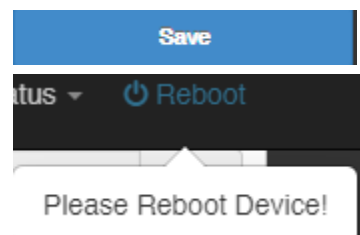
IP 1

IP 2

IP 3

IP 4

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.



Save

Status

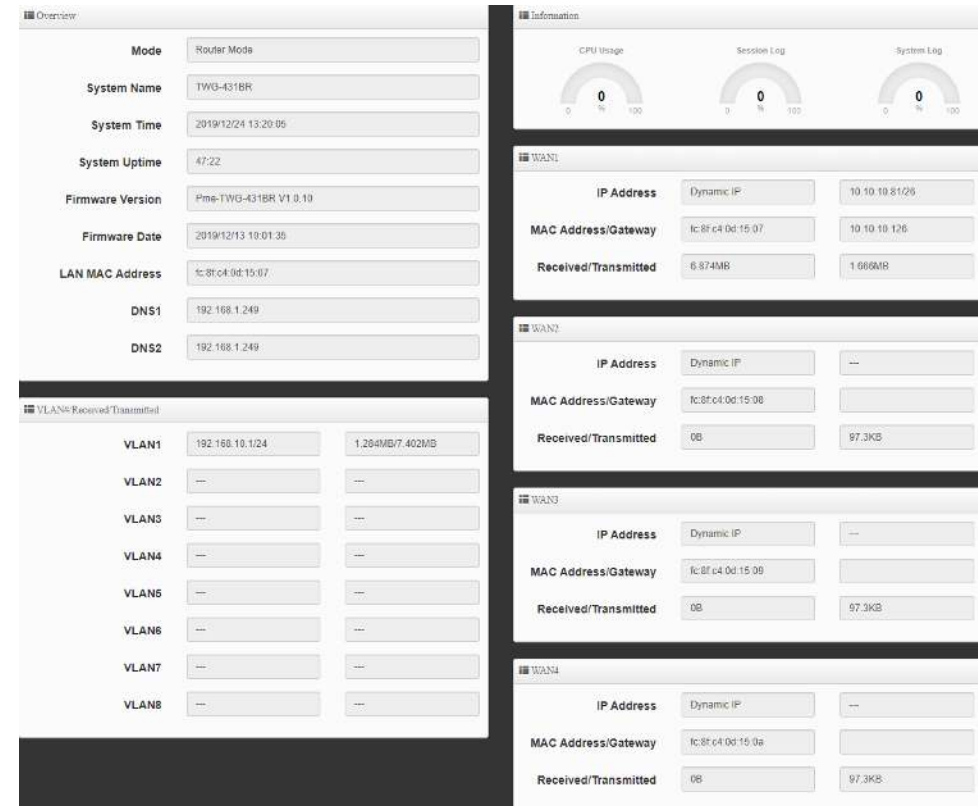
Please Reboot Device!

Check the router status information

Status > Overview

You may want to check the system information of your router firmware, CPU usage, system time, uptime, LAN/VLAN interface information, and WAN interface information.

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **Status** and click on **Overview**.
 - **CPU Usage** – The gauge displays the current CPU utilization.
 - **Session Log** – The gauge displays the current memory utilization for the session log.
 - **System Log** – The gauge displays the current memory utilization for the system log.
 - **Mode** – Displays the current operation mode of the router
 - **System Name** – Displays the current system name to the device. This can be modified under System > Management.
 - **System Time** – Displays the current router time.
 - **System Uptime** – Displays how long the router has been running without any interruptions or reboots.
 - **Firmware Version** – Displays the current firmware version of the router.
 - **Firmware Date** – Displays the firmware date.
 - **LAN MAC Address** – Displays the LAN MAC address.
 - **DNS1** – Displays the primary DNS server used by the router.
 - **DNS2** – Displays the secondary DNS server used by the router.
- **VLAN#** – Displays the VLAN IP interface and total data transmitted and received. If there is VLAN information displayed, the VLAN is currently enabled/active.
- **WAN#** - Displays the current WAN Mode, IP address, MAC address, default gateway, and total bytes transmitted and received through the interface.



View routing table and ARP entries

Advanced > IP Routing Status

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

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **Advanced** and click on **IP Routing Status**.

Type	Network	Netmask	Gateway	Interface	Metric
S*	0.0.0.0	0.0.0.0	10.10.10.126	WAN1	0
K	10.10.0.0	255.255.255.0	10.10.0.2		0
C	10.10.0.2	255.255.255.255			0
L	10.10.0.1	255.255.255.255			0
C	10.10.10.64	255.255.255.192		WAN1	0
L	10.10.10.81	255.255.255.255		WAN1	0
C	192.168.10.0	255.255.255.0		VLAN1	0
L	192.168.10.1	255.255.255.255		VLAN1	0

View your router logging

Status > Local 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 7).
2. Click on **Status** and click on **Local System Log**.

Note: You can click *Refresh* to refresh the current logging display or *clear* to completely delete all logging.

Time	Facility	Severity	Message
2019-12-24 12:32:52	System	Info	started: BusyBox v1.24.2
2019-12-24 12:32:52	System	Info	Change GUI settings(Socket) from (null)

Note: Logging memory usage can be configured under *Maintenance > Log Maintenance* and *System > Log Server* sections.

Configure router logging settings and setup external syslog server

System > Management

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **System** and click **Management**.
 - **Remote Server** – Check the option and enter the IP address of the external syslog server. This setting allows to send router logging to an external syslog server.
 - **Port** – If sending logging to external syslog server, enter the syslog port to use. By default, the syslog port is 514.

System Log Setup	
Remote Server	☐
Port	514 Port

SMTP Email Notification

System > SMTP

You can configure SMTP to send email notifications for monitoring purposes.

1. Log into your router management page (see "[Access your router management page](#)" on page 7).
2. Click on **System** and click on **SMTP**.
3. Review the settings below.

Note: You can configure the external SMTP server to use to send out email notifications from the router. In the receiver email list, you can enter all of the recipients for the email notifications.

SMTP Server Setup

SMTP1 Service ☒ Enable ☐ Disable

SMTP2 Service ☐ Enable ☒ Disable

Session Log Capacity 30 Minutes

System Log Capacity 30 Minutes

SMTP1 Server Setup

Sender From Test

SMTP Server

Port 25 Port

Encryption None

SMTP Authentication ☒ Enable ☐ Disable

Username

Password

Receiver E-Mail List

Create Receiver E-Mail

#	Receiver E-Mail	Event	Action
1			

4. Click **Save** at the bottom. Then click **Reboot** at the top right to commit the changes.

Save

Reboot

Please Reboot Device!

Technical Specifications

Standards

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x
- IEEE 802.3ab
- IEEE 802.1Q

Device Interface

- 5 x Gigabit ports (Modes: 4 WAN ports / 1 LAN port or 1 WAN port / 4 LAN ports)
- 1 x USB 3.0 port (Backup & Restore Configuration / Export Logging)
- 1 x RJ-45 console port
- Reset button
- LED indicators
- On/off switch

Performance

- NAT (LAN-to-WAN) throughput: 900Mbps*
- Routing performance: 900Mbps
- Maximum concurrent sessions: 50,000
- Maximum number of VLANs: 8 (ID: 1-4093)
- IPsec VPN (AES-256/SHA-256/LAN-to-LAN) throughput: 200Mbps
- SSL VPN Throughput (Blowfish/SHA-1/Bridge): 20Mbps

VPN

- SSL VPN Client-to-Site (Up to 30 tunnels)
- IPsec VPN Server / Site-to-Site (Up to 40 tunnels)
- PPTP/L2TP VPN Server (Up to 40 tunnels)
- L2TP with IPsec VPN Server (Up to 40 tunnels shared with L2TP)
- IPsec Encryption: 3DES, AES-128/192/256
- IPsec Authentication: MD5, SHA1, SHA256

- IPsec Key Exchange: IKE: Main Mode/Aggressive Mode, Pre-shared Key, DH Groups 1/2/5/14
- IPsec Protocols: ESP, PFS DH Groups 1/2/5/14, DPD, Local/Remote ID: IP Address, FQDN
- IPsec NAT Traversal
- SSL VPN Encryption: AES
- SSL VPN Certificate: RSA
- 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
- IPv4 WAN Modes: DHCP, Static IP, PPPoE, PPTP
- IPv6 WAN Modes: Static, Auto-configuration (SLAAC/DHCPv6), Link-Local, PPPoE, 6to4, 6rd
- Routing: Static, RIPv2, OSPFv1/2, distribute RIPv2 over OSPFv1/2, routing policies (Up to 20 entries)
- Inter-VLAN Routing (Up to 8 VLANs, 8 IP interfaces)
- DHCP Server/Relay
- Dynamic DNS: dyn.com, no-ip.com
- WAN Failover
- WAN Load Balancing: Assign weight by percentage or bandwidth, source IP based, source & destination IP based, session based
- High Availability: Supports 1 active-passive cluster up to a total of 6 units (1 master + 5 standby)
- VPN passthrough: IPsec, PPTP, L2TP

Access Control

- MAC address filtering (Up to 64 entries)
- IP address filtering: TCP, UDP, ICMP (Up to 64 entries)
- Content filtering: URL (HTTP only), Keyword, P2P, IM (Up to 64 entries)

- Virtual server/port forwarding (Up to 64 entries)
- Advanced web content filtering service powered by Router Limits™
- Scheduling: IP/MAC/Content filters, virtual server (Up to 10 entries)
- DMZ host

Quality of Service

- Bandwidth Control: applicable by IP network, IP range, TCP/UDP port, SIP, RTSP, RTP, web

Management/Monitoring

- CLI (Console/Telnet/SSHv2) command line management
- HTTP/HTTPS (SSL v2/3 TLS) web based management, upload custom SSL certificate
- SNMP v1, v2c, v3
- SNMP trap (Up to 4 receivers)
- Scheduled automatic reboot
- Scheduled Wake-on-LAN (WoL)
- Internal logging or send logging to external syslog server
- Manual or online firmware upgrade and notification
- Backup and restore configuration
- Diagnostic tools: Built-in ping & traceroute network utilities

MIB

- MIB II RFC 1213

Power

- Input: 100 – 240V AC, 50/60Hz, 0.5A
- Output: 12V DC, 1.5A external power adapter
- Max. consumption: 17.4W

MTBF

- 318,350 hours

Operating Temperature

- 0 – 50° C (32 – 122° F)

Operating Humidity

- Max. 80% non-condensing

Certifications

- CE
- FCC

Dimensions

- 265 x 185 x 44.45mm (10.4 x 7.28 x 1.75 in.)
- Rack mountable 1U height

Weight

- 1.1kg (2.44 lbs.)

Disclaimers

*Maximum NAT performance when using 1 WAN / 4 LAN mode. 4 WAN / 1 LAN mode has a limitation of up to 200Mbps per WAN interface.

Troubleshooting

Q: I typed `http://192.168.10.1` in my Internet Browser Address Bar, but an error message says “The page cannot be displayed.” How can I access the router management page?

Answer:

1. Check your hardware settings again. See “[Router Installation](#)” on page 8.
2. Make sure the LAN and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to Obtain an IP address automatically or DHCP (see the steps below).
4. Make sure your computer is connected to one of the router's LAN ports
5. Press on the factory reset button for 15 seconds, the release.

Windows 7/8/8.1

- 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: I went through the basic setup, 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.

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

RoHS

This product is RoHS compliant.

Europe – EU Declaration of Conformity

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

Safety EN 60950 : 2006 + A11: 2009 + A1: 2010 + A12: 2011 + A2: 2013

EMC EN 55032: 2012 + AC: 2013
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 55024: 2010
AS/NZS CISPR 32: 2013

This product is herewith confirmed to comply with the Directives.

Directive:

Low Voltage Directive 2014/35/EU
EMC Directive 2014/30/EU
RoHS Directive 2011/65/EU
WEEE Directive 2012/19/EU
REACH Regulation (EC) No. 1907/2006

Limited Warranty

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

Limited Warranty

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

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

Limited Lifetime Warranty

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

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

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

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

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

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

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

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

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

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

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

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

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

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW, TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN

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

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

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

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

PWP07172015v3

2022/04/05



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