

User's Guide



AC1750 Dual Band Wireless Router

TEW-812DRU

Table of contents

Product Overview4

Package Contents 4

Features 4

Product Hardware Features.....5

Application Diagram 6

Wireless Performance Considerations 7

Basic Router Setup7

Creating a Home Network 7

Router Installation 8

Connect additional wired devices to your network..... 13

Wireless Networking and Security13

How to choose the type of security for your wireless network 13

Secure your wireless network 15

Connect wireless devices to your router 16

Connect wireless devices using WPS 16

Wireless 2.4GHz wireless settings 17

Wireless 2.4GHz Guest Network..... 19

Wireless 5GHz wireless settings 19

Wireless 5Hz Guest Network 20

2.4GHz Wireless Distribution System (WDS) 21

5GHz Wireless Distribution System (WDS) 21

Steps to improve wireless connectivity 22

Wireless 2.4GHz Advanced settings 22

Wireless 5GHz Advanced settings 23

Access Control Filters24

Access control basics 24

LAN Client Filter24

URL Filter.....24

MAC Filters.....25

Advanced Router Setup 26

Access your router management page..... 26

Using the Configuration Menu 26

Change your router login password 27

Change your router device name 27

Manually configure your Internet connection 27

Clone a MAC address..... 28

Change your router IP address 28

Set up the DHCP server on your router 29

Set up IPv6 on your router 30

Set your router date and time 30

Set schedules 31

QoS (Quality of Service)..... 31

Open a device on your network to the Internet..... 32

DMZ32

Virtual Server33

Special Applications34

Gaming.....35

Add static routes to your router 36

Enable/disable UPnP on your router 37

Identify your network on the Internet 37

Share Files..... 38

Samba38

FTP39

Administrator > File Sharing39

Remotely check router status.....	40	Dynamic DHCP List.....	52
Print Share Utility Installation	40	2.4GHz Wireless Station List	53
Windows Installation	40	5GHz Wireless Station List	53
MAC OS X Installation	41	QoS Wireless Station List	54
Launching the Utility	42	Management Page Structure.....	55
Utility Main Window	42	Technical Specifications	56
Configure Server	43	Troubleshooting	57
Connect.....	44	Appendix	58
Disconnect	44		
Sending a Request to Connect.....	44		
Connect to a Printer.....	46		
Auto-Connect Printer.....	46		
Connect to a Scanner.....	46		
Router Maintenance & Monitoring.....	47		
Reset your router to factory defaults	47		
Router Default Settings	47		
Backup and restore your router configuration settings	48		
Reboot your router	48		
Upgrade your router firmware	49		
Remotely check router status.....	49		
View your router log	50		
Router Status	50		
Check the router system information.....	50		

Product Overview



Package Contents

In addition to the access point, the package includes:

- TEW-812DRU AC1750 Dual Band Wireless Router
- CD-ROM (Utility and User's Guide)
- Multi-Language Quick Installation Guide
- Network cable Ethernet Cable (1.5m / 5ft.)
- Power Adapter (12V, 2A)

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 AC1750 Dual Band Wireless Router, model TEW-812DRU, produces the ultimate wireless experience with gigabit wireless speeds. Manage two wireless networks—the 1300 Mbps Wireless AC band for the fastest wireless available and the 450 Mbps Wireless N band to connect common wireless devices. The TEW-812DRU can easily handle the demands of multiple HD streams in a busy connected home.

Plug in a USB flash or NAS drive to share HD videos and music across the network. Gigabit ports on the back of the router maintain high speed wired connections. Create a secure isolated guest network for guest internet access. Beamforming technology directs the strongest signal to each connected device. Multiple-MIMO technology enables communication with multiple devices simultaneously. Wi-Fi Protected Setup (WPS) connects other WPS supported wireless adapters at the touch of a button. Manage access to websites and file types with advanced access controls.

- 4 x 10/100/1000 Mbps Auto-MDIX LAN ports
- 1 x 10/100/1000 Mbps Internet port
- 1 x USB 2.0 port for USB share (storage and printing***)
- 1 x Wi-Fi Protected Setup (WPS) button
- On / off power switch (EU version)
- Simultaneously transmit both 2.4 GHz and 5 GHz wireless networks
- Compliant with the latest draft 802.11ac wireless technology*
- Backwards compatible with IEEE 802.11n/b/g/a wireless standards
- High-speed data rates of up to 1.3Gbps with 802.11ac* and 450Mbps with 802.11n on both 2.4GHz and 5GHz band**
- IPv6 (Internet Protocol v6) support
- FTP and Samba USB storage support
- Share USB peripheral devices over the network including; flash drives, external hard drives and printers***
- Printer Control Center utility supports Windows 8 (32/64-bit), 7 (32/64-bit), Vista (32/64-bit), Windows XP (32/64-bit), and Mac OS X 10.6/10.7/10.8 operating systems
- Compatible with most popular cable / DSL Internet Service Providers using Dynamic / Static IP, PPPoE, L2TP, and PPTP connection
- Firewall protection with Network Address Translation (NAT)

- Wireless Distribution System (WDS) support for wireless network bridging
- Advance wireless security of up to WPA2-RADIUS
- Wi-Fi Multimedia (WMM) and configurable WAN Quality of Service (QoS) support
- Guest network support (3x per wireless band) with Internet access restriction
- Internet Access Control with MAC, URL, Service Type, and IP Range filtering
- Internet Access Control Rule Scheduling: schedule access to websites, online video games, Internet cameras and more for specific times throughout the week
- One touch wireless connection using the WPS button
- Easy setup via Web browser using the latest versions of Internet Explorer, FireFox, Safari, and Chrome
- Virtual server and Application Level Gateway (ALG) services for special Internet applications
- Universal Plug and Play (UPnP) for auto discovery and support for device configuration of Internet applications
- 3-year limited warranty

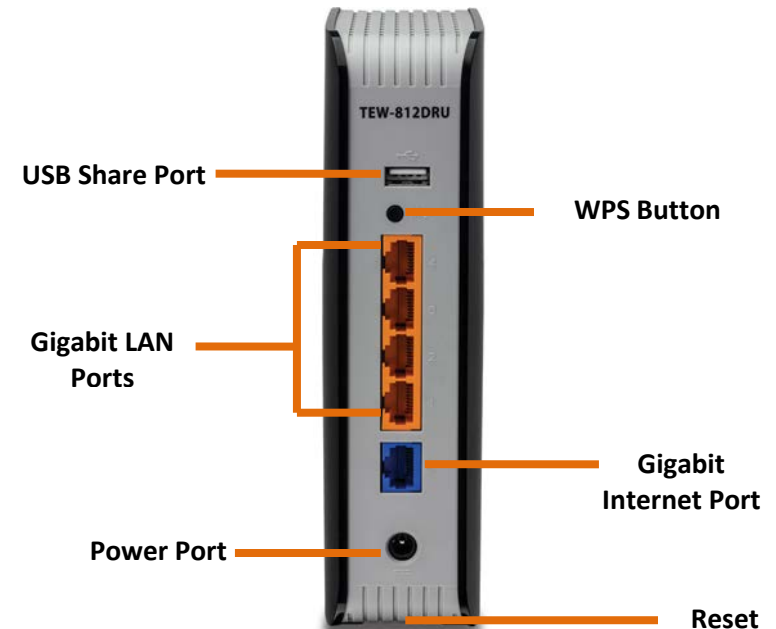
*For maximum performance of up to 1.3 Gbps use with a 1.3 Gbps 802.11ac wireless adapter

**Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions

*** Printer Control Center utility installation required for each computer in order to access the printer

Product Hardware Features

Rear View



- **USB Share Port:** Connect USB Storage device to share files through the network or connect a USB printer to provide network printing through the network (utility required for print sharing).
- **WPS (Wi-Fi Protected Setup)** – Push and hold this button for 5 seconds to activate WPS.
- **Gigabit LAN ports:** 4x Gigabit ports. Connect Ethernet cables (also called network cables) from your router LAN ports to your wired network devices.
- **Gigabit Internet port:** Gigabit port. Connect an Ethernet cable from your router WAN port to your modem.
- **Power port:** Connect the included power adapter from your router power port and to an available power outlet.
- **Reset (located in the bottom):** Press and hold this button for 10 seconds to reset your router to default settings

Front View



- **USB:** This indicator turns green indicating a USB device is connection.
- **WPS LED:** This indicator is turned on and blinks when WPS is activated. The LED will turn off automatically once WPS is completed.
- **Wireless (Link/Activity) LED:** This turns green when a 2.4GHz client is connected and turns blue when a 5GHz client is connected. If both types of wireless clients are connected the LED will be blue. The LED will blinks during data transmission.
- **Internet LED** -This LED indicator is solid green when the gigabit Internet port is connected. Otherwise if this LED indicator is off, there is no power to your router.
- **WAN (Link/Activity) LED** – This LED indicator is solid green when your router WAN port is physically connected to the modem Network port (also called network port) successfully with a Network cable. The LED indicator will be
- **Power LED:** This LED turns on when the unit is powered on.

Application Diagram

The router's gigabit Internet port is connected to your Internet modem connected which is connected to the Internet. Wireless signals from the router are broadcasted to wireless clients such as laptops (with wireless capability), TVs or media bridges thereby providing Internet access.

Wireless Performance Considerations

There are a number of factors that can impact the range of wireless devices.

1. Adjust your wireless devices so that the signal is traveling in a straight path, rather than at an angle. The more material the signal has to pass through the more signal you will lose.
2. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
3. Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.
4. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.
5. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.
6. Any device operating on the 2.4GHz frequency will cause interference. Devices such as 2.4GHz cordless phones or other wireless remotes operating on the 2.4GHz frequency can potentially drop the wireless signal. Although the phone may not be in use, the base can still transmit wireless signal. Move the phone's base station as far away as possible from your wireless devices.

If you are still experiencing low or no signal consider repositioning the wireless devices or installing additional access points. The use of higher gain antennas may also provide the necessary coverage depending on the environment.

Basic Router Setup

Creating a Home Network

What is a network?

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

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

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

How to set up a home network

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

5. PPTP or Russian PPTP

Type (Dynamic IP or Static IP)

My IP Address: _____. _____. _____. _____.
(e.g. 215.24.24.129)Subnet Mask: _____. _____. _____. _____.
(e.g. 255.255.255.0)Gateway: _____. _____. _____. _____.
(e.g. 215.24.24.1)Server IP: _____. _____. _____. _____.
(e.g. 215.24.24.1)

PPTP Account: _____

PPTP Password: _____

Retype Password: _____

6. L2TP or Russia L2TP

Type (Dynamic IP or Static IP)

My IP Address: _____. _____. _____. _____.
(e.g. 215.24.24.129)Subnet Mask: _____. _____. _____. _____.
(e.g. 255.255.255.0)Gateway: _____. _____. _____. _____.
(e.g. 215.24.24.1)Server IP: _____. _____. _____. _____.
(e.g. 215.24.24.1)

L2TP Account: _____

L2TP Password: _____

Retype Password: _____

7. Russia PPPoE

Type (Dynamic IP or Static IP)

User Name: _____

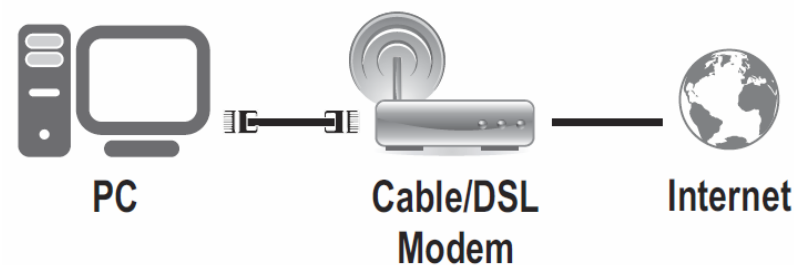
Password: _____

Verify Password: _____

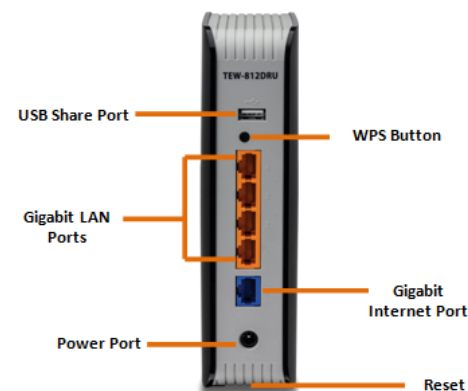
IP Address: _____. _____. _____. _____. (e.g. 215.24.24.129)

Hardware Installation

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

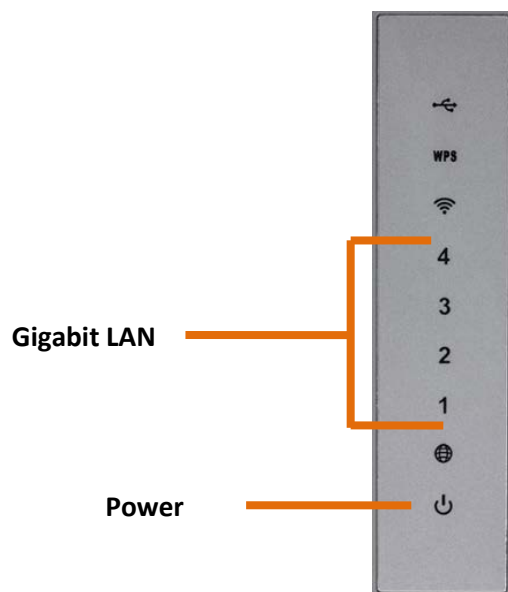


2. Turn off your modem.
3. Disconnect the Network cable from your computer to your modem.



4. Using a Network cable, connect the gigabit Internet port on the router to your modem.
5. Using another Network cable, connect your computer to one of the four gigabit LAN ports on the router.

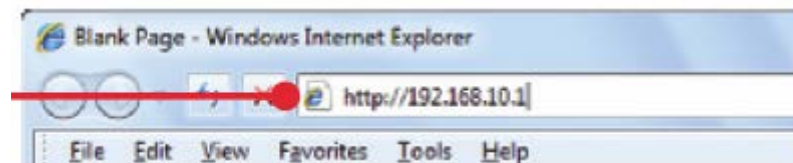
6. Plug in the power adapter, connect it to the router's power port, and then push the On/Off Power Switch to the "On" position (pushed in).
7. Turn on your modem.



8. Verify that the following front panel LED indicators on your router: Power (Solid Green), Gigabit LAN 1, 2, 3, or 4 (Solid/Blinking Green for ports for which devices are connected), WAN (Solid/Blinking Green).

Setup Wizard

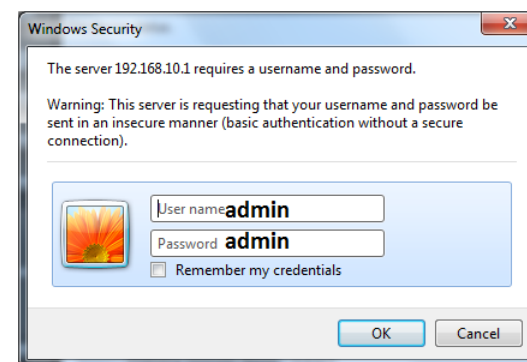
1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to <http://192.168.10.1>. Your router will prompt you for a user name and password.



2. Enter the default user name and password and then click Login.

Default User Name: **admin**

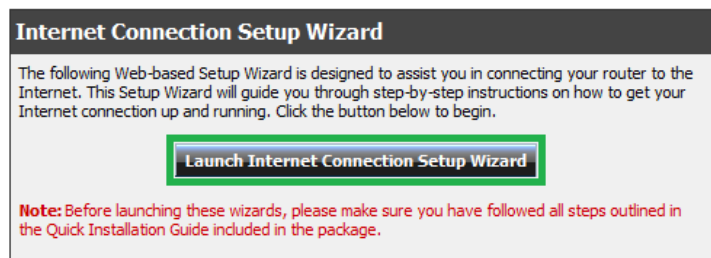
Default Password: **admin**



3. Click on the Administrator button and then Wizard button on the left side.



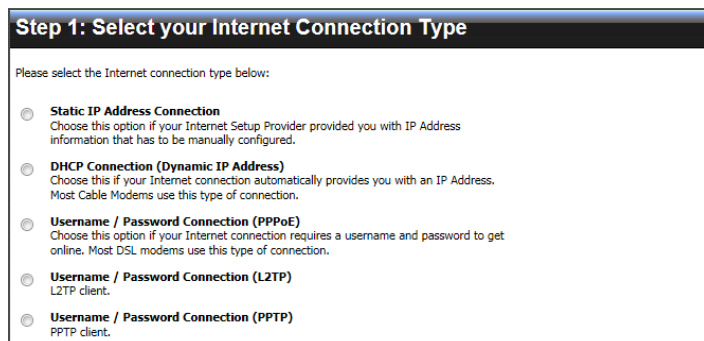
4. Click “Launch Internet Connection Setup Wizard” to setup your Internet connection on the router.



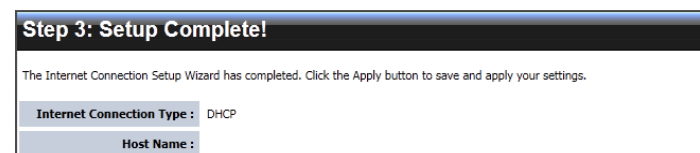
5. Click Next to begin the wizard



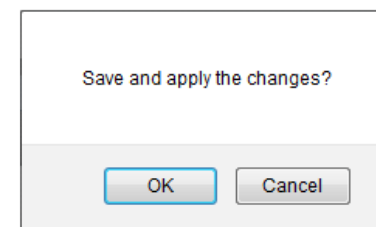
6. Select your Internet connection type and click Next to continue. Note: The most common Internet connection used is DHCP.



7. Verify if your settings are correct and click Apply to complete the Internet Setup Wizard.



8. Click OK to apply your settings.



9. The router will reboot once the process is completed.

The TEW-812DRU's wireless network is pre-encrypted with wireless security. These settings can be found on a sticker placed on the unit and the device label below the unit. If you would like to change those settings continue to the next step to launch the wireless security wizard.

1. Click the Wizard button again to run the Wireless Setup Wizard.



2. Click "Launch Wireless Security Setup Wizard".



Wireless Security Setup Wizard

For added security the TEW-812DRU's wireless network is pre-encrypted with its own unique network security key. Launch the Wireless Security Setup Wizard to change the existing encryption key.

Launch Wireless Security Setup Wizard

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the router.

3. Select which wireless network you would like to configure and click Next to begin.

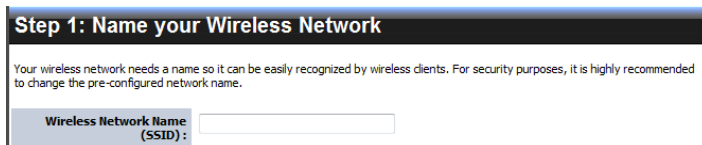


Welcome to the Wireless Security Setup Wizard

This wizard will guide you through a step-by-step process to set up your wireless network and make it secure.

- Please select which wireless interface you want to set up: Wireless 2.4GHz
- Step 1: Name your Wireless Network
- Step 2: Secure your Wireless Network
- Step 3: Set your Wireless Security Password

4. Enter the Wireless Network Name (SSID) you would like to assign your wireless network. This name will be used when connecting to your wireless network. Click Next to continue

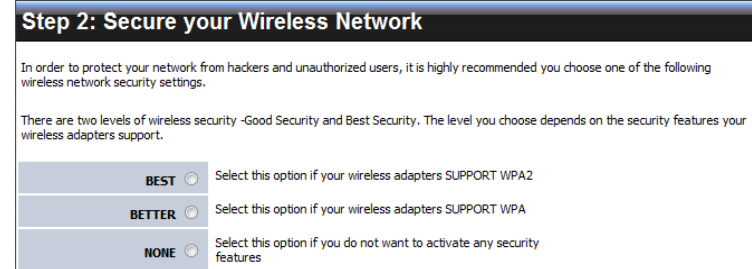


Step 1: Name your Wireless Network

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.

Wireless Network Name (SSID):

5. Select the type of wireless security to use. Click Next to continue. It is recommended to use a wireless security to protect your wireless network from any intruders.



Step 2: Secure your Wireless Network

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are two levels of wireless security -Good Security and Best Security. The level you choose depends on the security features your wireless adapters support.

BEST ☐ Select this option if your wireless adapters SUPPORT WPA2

BETTER ☐ Select this option if your wireless adapters SUPPORT WPA

NONE ☐ Select this option if you do not want to activate any security features

6. Enter the password or encryption key assigned to your wireless network. Click Next to continue.

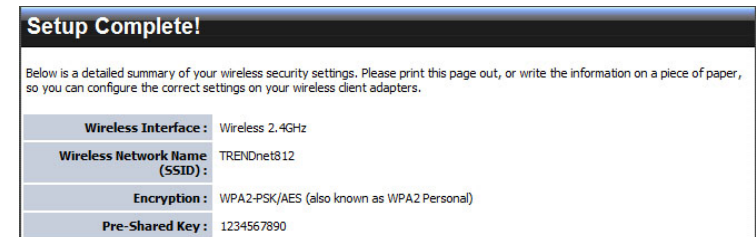


Step 3: Set your Wireless Security Password

You have selected your security level - you will need to set a wireless security password.

Wireless Security Password: (8 to 64 characters)

7. Verify your wireless settings are correct and click Apply.



Setup Complete!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

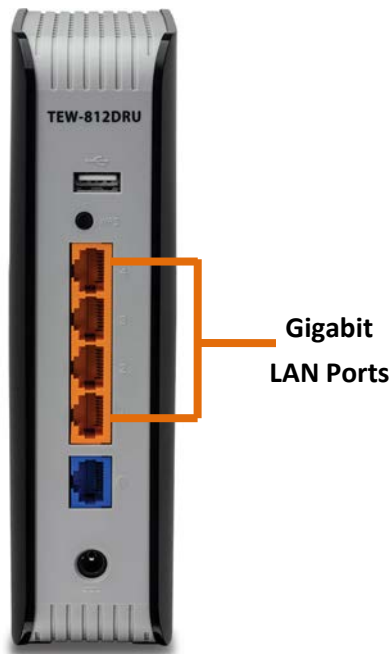
Wireless Interface:	Wireless 2.4GHz
Wireless Network Name (SSID):	TRENDnet812
Encryption:	WPA2-PSK/AES (also known as WPA2 Personal)
Pre-Shared Key:	1234567890

Note: Save your wireless settings in a location you can find easily, in case you forget the applied wireless settings.

Connect additional wired devices to your network

You can connect additional computers or other network enabled devices to your network by using Ethernet cables to connect them to one of the available LAN ports labeled 1,2,3,4 on your router. Check the status of the LED indicators (1, 2, 3, or 4) on the front panel of your router to ensure the physical cable connection from your computer or device.

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



Wireless Networking and Security

How to choose the type of security for your wireless network

Setting up wireless security is very important. Leaving your wireless network open and unsecure could expose your entire network and personal files to outsiders. TRENDnet recommends reading through this entire section and setting up wireless security on your new router.

There are a few different wireless security types supported in wireless networking each having its own characteristics which may be more suitable for your wireless network taking into consideration compatibility, performance, as well as the security strength along with using older wireless networking hardware (also called legacy hardware). It is strongly recommended to enable wireless security to prevent unwanted users from accessing your network and network resources (personal documents, media, etc.). In general, it is recommended that you choose the security type with the highest strength and performance supported by the wireless computers and devices in your network. Please review the security types to determine which one you should use for your network.

Wireless Encryption Types

- **WEP:** Legacy encryption method supported by older 802.11b/g hardware. This is the oldest and least secure type of wireless encryption. It is generally not recommended to use this encryption standard, however if you have old 802.11 b or 802.11g wireless adapters or computers with old embedded wireless cards(wireless clients), you may have to set your router to WEP to allow the old adapters to connect to the router.

Note: This encryption standard will limit connection speeds to 54Mbps.

- **WPA:** This encryption is significantly more robust than the WEP technology. Much of the older 802.11g hardware was been upgraded (with firmware/driver upgrades) to support this encryption standard. Total wireless speeds under this encryption type however are limited to 54Mbps.
 - **WPA-Auto:** This setting provides the router with the ability to detect wireless devices using either WPA or WPA2 encryption. Your wireless network will automatically change the encryption setting based on the first wireless device connected. For example, if the first wireless client that connects to your wireless network uses WPA encryption your wireless network will use WPA encryption. Only when all wireless clients disconnect to the network and a wireless client with WPA2 encryption connects your wireless network will then change to WPA2 encryption.

Note: WPA2 encryption supports 802.11n speeds and WPA encryption will limit your connection speeds to 54Mbps

- **WPA2:** This is the most secure wireless encryption available today, similar to WPA encryption but more robust. This encryption standard also supports the highest connection speeds. TRENDnet recommends setting your router to this encryption standard. If you find that one of your wireless network devices does not support WPA2 encryption, then set your router to either WPA or WPA-Auto encryption.

Note: Check the specifications of your wireless network adapters and wireless appliances to verify the highest level of encryption supported.

Below is brief comparison chart of the wireless security types and the recommended configuration depending on which type you choose for your wireless network.

Security Standard	WEP	WPA	WPA2
Compatible Wireless Standards	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g/n
Highest Performance Under This Setting	Up to 54Mbps	Up to 54Mbps	Up to 450Mbps (2.4Ghz) and 1.3Gbps (5Ghz) *
Encryption Strength	Low	Medium	High
Additional Options	Open System or Shared Key, HEX or ASCII, Different key sizes	TKIP or AES, Preshared Key or RADIUS	TKIP or AES, Preshared Key or RADIUS
Recommended Configuration	Open System ASCII 13 characters	TKIP Preshared Key 8-63 characters	AES Preshared Key 8-63 characters

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

Secure your wireless network

Wireless > Security

After you have determined which security type to use for your wireless network (see [“How to choose the security type for your wireless network”](#) on page 13), you can set up wireless security.

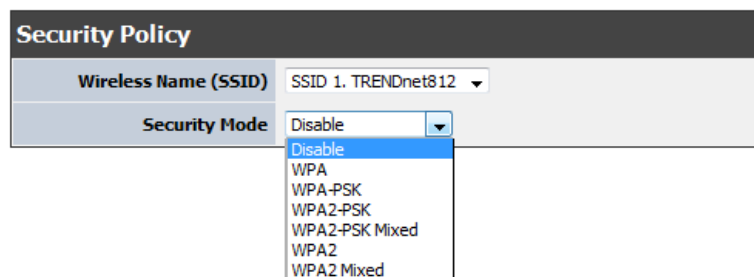
1. Log into your router management page (see [“Access your router management page”](#) on page 26).



2. Select the Wireless band you would like to configure



3. Click on **Security** section.



4. Click on the **Security Mode** drop-down list to select your wireless security type.

Selecting WEP:

If selecting **WEP** (Wired Equivalent Privacy), please review the WEP settings to configure and click **Apply** to save the changes. This security type is available only when **802.11 n-mode** is set to Off.

WEP	
Current Network Key	1 ▼
Network Key 1	
Network Key 2	
Network Key 3	
Network Key 4	

- **Current Network Key 1-4**
 - This is where you enter the password or key needed for a computer to connect to the router wirelessly
 - You can define up to 4 passwords or 4 keys. Only one key can be active at a given time. Most users simply define one key.
 - Choose a key index 1, 2, 3, or 4 and enter the key.
 - When connecting to the router, the client must match both the password and the Key number. (e.g. if you have activated Key 2 with a password of 12345, then the client must select: Key 2 (entering Key 1, 3, or 4 will block the ability to connect) and enter password 12345)
- **WEP Key** – Choose the key length **64-bit** or **128-bit**.

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

Selecting WPA-PSK, WPA2-PSK, or WPA2-PSK Mixed (WPA2-PSK recommended):

WPA	
WPA Encryption	AES ▼
WPA passphrase	•••••••• Click here to display
Network Key Rotation Interval	3600 (seconds)

The following section outlines options when selecting PSK (Preshared Key Protocol),

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

Selecting WPA, WPA2, or WPA2Mixed:

Radius Server	
RADIUS Server	
RADIUS Port	1812
RADIUS Key	

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

- Note:** This security type requires an external RADIUS server, PSK only requires you to create a passphrase.*
- **Radius Server:** Enter the IP address of the RADIUS server. (e.g. 192.168.10.250)
 - **Radius Port:** Enter the port your RADIUS server is configured to use for RADIUS authentication.
***Note:** It is recommended to use port 1812.*
 - **RADIUS Key:** Enter the shared secret used to authorize your router with your RADIUS server.

Connect wireless devices to your router

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

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

WEP Key Format	HEX	ASCII
Character set	0-9 & A-F, a-f only	Alphanumeric (a,b,c,?, *, /,1,2, etc.)
64-bit key length	10 characters	5 characters
128-bit key length	26 characters	13 characters

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

See the "[Appendix](#)" on page 58 for general information on connecting to a wireless network.

Connect wireless devices using WPS

WPS (Wi-Fi Protected Setup) is a feature that makes it easy to connect devices to your wireless network. If your wireless devices support WPS, you can use this feature to easily add wireless devices to your network.

***Note:** You will not be able to use WPS if you set the SSID Broadcast setting to Disabled.*

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

- Push Button Configuration (PBC) method
 - RECOMMENDED Hardware Push Button method—with an external button located physically on your router and on your client device
 - WPS Software/Virtual Push Button - located in router management page

- PIN (Personal Identification Number) Method - located in router management page
Note: Refer to your wireless device documentation for details on the operation of WPS.

Recommended Hardware Push Button (PBC) Method

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

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

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

PBC (Software/Virtual Push Button)

Wireless > WiFi Protected Setup

In addition to the hardware push button located physically on your router, the router management page also has push button which is a software or virtual push button you can click to activate WPS on your router.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).
2. Select the wireless band you would like to configure and click on **WPS**.



3. To add a wireless device to your network, simply push the WPS button on the wireless device (consult wireless device's User's Guide for length of time), you are

connecting, then in your router management page under WPS action click on the **Add Enrollee** button.

A rectangular button with a light gray border and the text 'Add Enrollee' in a dark font.

PIN (Personal Identification Number)

Wireless > WiFi Protected Setup

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

1. Log into your router management page (see "[Access your router management page](#)" on page 26).
2. Select the wireless band you would like to configure and click on **WPS**.
3. Next to **Station PIN**, enter the WPS PIN of the wireless device you are connecting and click the **Add Enrollee** button.

A rectangular input field with a light gray border and the text 'Station PIN' in a dark font to its left.

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

Wireless 2.4GHz wireless settings

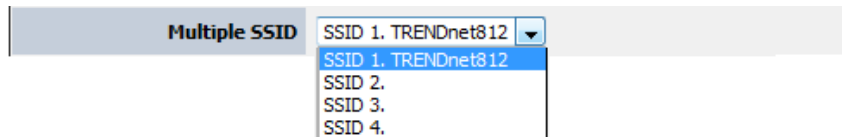
2.4GHz Wireless > Basic

This section outlines available management options for your router's 2.4GHz wireless network.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).
2. Click on **Wireless 2.4GHz** and click on **Basic**.

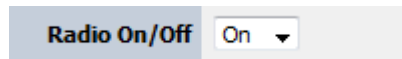


3. To save changes to this section, click **Apply** when finished.

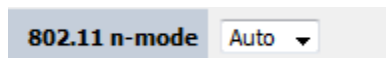


- **Multiple SSID:** Select which SSID you would like to configure. The Wireless Name (SSID) will be blank if additional SSID's have not been configured. This router supports 3 additional SSIDs.

Note: You will need to use one of the additional SSIDs to configure as your guest network. Please refer to Wireless 2.4GHz Guest Network section for more details.



- **Radio On/Off:**
 - **On:** Turns on wireless radio
 - **Off:** Turns off wireless radio.

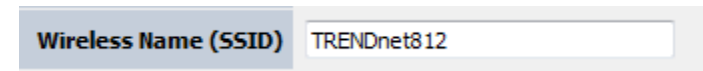


- **802.11 n-mode**
 - **Auto:** Select this option if you have non 802.11n wireless clients (802.11b/g).
 - **Off:** Router will only operate in 802.11n mode only, non 802.11n wireless clients will not be able to connect when this option is selected.

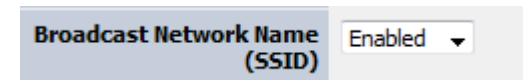
When applying the 802.11 mode setting, please keep in mind the following:

- Wireless devices that support 802.11n are backwards compatible and can connect wirelessly at 802.11g or 802.11b.

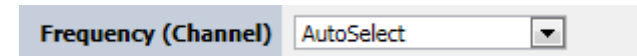
- Connecting at 802.11b or 802.11g will limit the capability of your 802.11n supported wireless devices from obtaining higher performance and data rates.
- Allowing 802.11b or 802.11g devices to connect to an 802.11n capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11n.
- Wireless devices that only support 802.11b or 802.11g will not be able to connect to a wireless network that is set to 802.11n only mode.
- Wireless devices that only support 802.11b will not be able to connect to a wireless network that is set to 802.11g only mode.



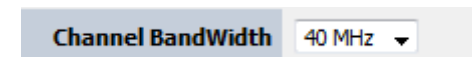
- **Wireless Name (SSID):** This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. By default, the router's wireless name is unique to the device. the wireless network name. If you choose to change the SSID,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



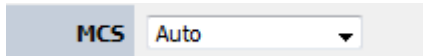
- **Broadcast Network Name (SSID):**
 - **Enabled** allows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your router.
 - **Disabled** turns off the ability for wireless devices to find your network. It is still possible for wireless devices to be configured to connect to your wireless network.



- **Frequency (Channel):** To manually set the channel on which the router will broadcast, uncheck **Auto Channel**, then click the drop-down list and select the desired Channel for wireless communication. The goal is to select the Channel that is least used by neighboring wireless networks.



- **Channel Bandwidth:** Select the channel bandwidth you would like the router to operate in. For greater performance, select **40MHz**.



- **MCS:** Select the speed you would like your wireless network to operate. For best results select Auto.

Wireless 2.4GHz Guest Network

2.4GHz Wireless > Guest Network

This section outlines how to setup your wireless network on the 2.4GHz wireless band and available management options. Multiple SSID feature has to be used to configure your wireless guest network.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Wireless 2.4GHz** and click on **Guest Network**.

Guest Network	
Wireless Name (SSID)	SSID 1. TRENDnet8124283
Network Bridge	LAN
Internet Access Only	Off

3. Review the Guest Network section, click **Apply** when finished.

- **Wireless Name (SSID):** Select from the pull down menu the wireless name (SSID) you would like to assign as your guest network.
- **Network Bridge:** Select which option you would like to assign the selected SSID

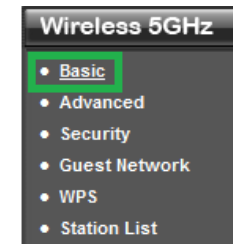
- o **LAN:** Select this option to have the selected SSID operate in your local network
- o **Guest:** Select this option to have the selected SSID operate as your guest network.
- **Internet Access Only:** Select On if you want to give your guest network access to the Internet only and not to your local network.

Wireless 5GHz wireless settings

5GHz Wireless > Basic

This section outlines available management options for your router's 2.4GHz wireless network.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).
2. Click on **Wireless 2.4GHz** and click on **Basic**.



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

Multiple SSID	
SSID 1. TRENDnet812ac	▼
SSID 1. TRENDnet812ac	
SSID 2.	
SSID 3.	
SSID 4.	

- **Multiple SSID:** Select which SSID you would like to configure. The Wireless Name (SSID) will be blank if additional SSID's have not been configured. This wireless router supports 3 additional SSIDs

Radio On/Off	
On	▼

- **Radio On/Off:**
 - o **On:** Turns on wireless radio
 - o **Off:** Turns off wireless radio.

802.11 n-mode Auto ▼

- **802.11 mode**

- o **Auto:** Select this option if you have non 802.11n wireless clients (802.11b/g).
- o **Off:** Router will only operate in 802.11n mode only, non 802.11n wireless clients will not be able to connect when this option is selected.

When applying the 802.11 mode setting, please keep in mind the following:

- Wireless devices that support 802.11n are backwards compatible and can connect wirelessly at 802.11g or 802.11b.
- Connecting at 802.11b or 802.11g will limit the capability of your 802.11n supported wireless devices from obtaining higher performance and data rates.
- Allowing 802.11b or 802.11g devices to connect to an 802.11n capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11n.
- Wireless devices that only support 802.11b or 802.11g will not be able to connect to a wireless network that is set to 802.11n only mode.
- Wireless devices that only support 802.11b will not be able to connect to a wireless network that is set to 802.11g only mode.

Wireless Name (SSID) TRENDnet812ac

- **Wireless Name (SSID):** This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. By default, the router wireless name is unique to the device. If you choose to change the SSID, change it to a name that you can easily remember.

Broadcast Network Name (SSID) Enabled ▼

- **Broadcast Network Name (SSID):**
 - o **Enabled** allows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your router.
 - o **Disabled** turns off the ability for wireless devices to find your network. It is still possible for wireless devices to be configured to connect to your wireless network.

Frequency (Channel) AutoSelect ▼

- **Frequency (Channel):** To manually set the channel on which the router will broadcast, uncheck **Auto Channel**, then click the drop-down list and select the desired Channel for wireless communication. The goal is to select the Channel that is least used by neighboring wireless networks.

Channel BandWidth 80 MHz ▼

- **Channel Bandwidth:** Select the channel bandwidth you would like the router to operate in. For greater performance, select **80MHz**.

MCS Auto ▼

- **MCS:** Select the speed you would like your wireless network to operate. For best results select Auto.

Wireless 5Hz Guest Network

5GHz Wireless > Guest Network

This section outlines how to setup your wireless network on the 5GHz wireless band and available management options. Multiple SSID feature has to be used to configure your wireless guest network.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Wireless 5GHz** and click on **Guest Network**.

Guest Network	
Wireless Name (SSID)	SSID 1. TRENDnet8124283
Network Bridge	LAN
Internet Access Only	Off

3. Review the Guest Network section, click **Apply** when finished.

- **Wireless Name (SSID):** Select from the pull down menu the wireless name (SSID) you would like to assign as your guest network.
- **Network Bridge:** Select which option you would like to assign the selected SSID
 - o **LAN:** Select this option to have the selected SSID operate in your local network
 - o **Guest:** Select this option to have the selected SSID operate as your guest network.
- **Internet Access Only:** Select On if you want to give your guest network access to the Internet only and not to your local network.

2.4GHz Wireless Distribution System (WDS)

Wireless > Basic

WDS or Wireless Distribution System allows your router to establish a wireless bridge connection to another access point. To use this feature the access point you want to connect has to also support WDS mode. This feature is available on both 2.4GHz and 5GHz wireless band.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).

Wireless 2.4GHz	
• Basic	
• Advanced	
• Security	
• Guest Network	
• WPS	
• Station List	

2. Click on **Wireless 2.4GHz** and click on **Basic**.

Wireless Distribution System(WDS)	
AP MAC Address	

3. Under **Wireless Distribution System (WDS)** enter the MAC address of the access point you would like the router to WDS to. You will also have to enter the MAC address of the router into the access point to establish the WDS or bridge connection. This wireless router supports up to 4 WDS connections.
4. Log into your access point and enter the MAC address of your router. Please see the access point's user manual for more information on how to configure WDS mode.
5. To save changes to this section, click **Apply** when finished.

5GHz Wireless Distribution System (WDS)

Wireless > Basic

WDS or Wireless Distribution System allows your router to establish a wireless bridge connection to another access point. To use this feature the access point you want to connect has to also support WDS mode. This feature is available on both 2.4GHz and 5GHz wireless band.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).

Wireless 5GHz	
• Basic	
• Advanced	
• Security	
• Guest Network	
• WPS	
• Station List	

2. Click on **Wireless 5GHz** and click on **Basic**.

Wireless Distribution System(WDS)	
AP MAC Address	

- Under **Wireless Distribution System (WDS)** enter the MAC address of the access point you would like the router to WDS to. You will also have to enter the MAC address of the router into the access point to establish the WDS or bridge connection. This wireless router supports up to 4 WDS connections.
- Log into your access point and enter the MAC address of your router. Please see the access point's user manual for more information on how to configure WDS mode.
- To save changes to this section, click **Apply** when finished.

Steps to improve wireless connectivity

There are a number of factors that can impact the range of wireless devices. Follow these tips to help improve your wireless connectivity:

- Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
 - For the widest coverage area, install your router near the center of your home, and near the ceiling, if possible.
 - Avoid placing the router on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), and masonry walls.
 - Any obstruction can weaken the wireless signal (even non-metallic objects), so the fewer obstructions between the router and the wireless device, the better.
 - Place the router in a location away from other electronics, motors, and fluorescent lighting.
 - Many environmental variables can affect the router's performance, so if your wireless signal is weak, place the router in several locations and test the signal strength to determine the ideal position.
- Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through

less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.

- Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.
- Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.

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

Wireless 2.4GHz Advanced settings

Wireless > Advanced

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

Advanced Wireless	
Beacon Interval	100 ms (range 20 - 1000, default 100)
DTIM	3 (range 1 - 255, default 3)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
Short Preamble	Disabled ▾
XPress™ Technology	On ▾

- Beacon Interval:** A beacon is a management frame used in wireless networks that transmitted periodically to announce the presence and provide information about the router's wireless network. The interval is the amount time between each beacon transmission.

Default Value: 100 milliseconds (range: 25-1000)

- **DTIM:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.
- **Fragment Threshold:** Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value of 2346 bytes. Setting the Fragmentation value too low may result in poor performance.
- **RTS Threshold** – The Request To Send (RTS) function is part of the networking protocol. A wireless device that needs to send data will send a RTS before sending the data in question. The destination wireless device will send a response called Clear to Send (CTS). The RTS Threshold defines the smallest data packet size allowed to initiate the RTS/CTS function.
Default Value: 2347 (range: 1-2347)
- **Short Preamble:** Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Xpress™ Technology:** Is frame bursting technology built by Broadcom to improve wireless performance. It is recommended to leave this feature On.

Wireless 5GHz Advanced settings

Wireless > Advanced

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

Advanced Wireless		
Beacon Interval	100	ms (range 20 - 1000, default 100)
DTIM	3	(range 1 - 255, default 3)
Fragment Threshold	2346	(range 256 - 2346, default 2346)
RTS Threshold	2347	(range 1 - 2347, default 2347)
Short Preamble	Disabled ▾	
XPress™ Technology	On ▾	

- **Beacon Interval:** A beacon is a management frame used in wireless networks that transmitted periodically to announce the presence and provide information about the router's wireless network. The interval is the amount time between each beacon transmission.
Default Value: 100 milliseconds (range: 25-1000)
- **DTIM:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.
- **Fragment Threshold:** Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value of 2346 bytes. Setting the Fragmentation value too low may result in poor performance.
- **RTS Threshold** – The Request To Send (RTS) function is part of the networking protocol. A wireless device that needs to send data will send a RTS before sending the data in question. The destination wireless device will send a response called Clear to Send (CTS). The RTS Threshold defines the smallest data packet size allowed to initiate the RTS/CTS function.
Default Value: 2347 (range: 1-2347)
- **Short Preamble:** Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

- **Xpress™ Technology:** Is frame bursting technology built by Broadcom to improve wireless performance. It is recommended to leave this feature On.

Access Control Filters

Access control basics

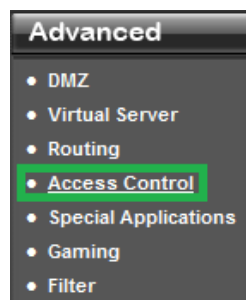
Advanced > Access Control

LAN Client Filter

Advanced > Access Control

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

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Advance**, click on **Access Control**.

LAN Client Filter Function Enabled ▼

3. Select **Enable** to enable LAN Client Filter Function.

LAN Client Filter Rules						
LAN IP Address Range		Protocol	Destination Port Range		Schedule	Enabled
	-	TCP ▼		-	Always ▼	☐
	-	TCP ▼		-	Always ▼	☐
	-	TCP ▼		-	Always ▼	☐
	-	TCP ▼		-	Always ▼	☐
	-	TCP ▼		-	Always ▼	☐
	-	TCP ▼		-	Always ▼	☐

4. Review the settings under **LAN Client Filter Rules** section

- **IP Range** – Enter the IP address or IP address range to apply the protocol (e.g. 192.168.10.20-192.168.10.20 or 192.168.10.20-192.168.10.30).

Note: The filter will not be applied to IP addresses outside of the range specified. You can leave the field blank to enable the rule for the entire LAN clients.

- **Protocol:** Select the protocol you would like to apply the rule to.
- **Port Range:** Enter the port or port range to apply the protocol.
- **Enabled:** Selecting **Enable** turns on the filter
- **Schedule:** Select the defined schedule you would like to have the rule to be applied. (see "[Set Schedule](#)" section on page 31).
- **Policy Name:** Enter a name for the Protocol/IP Filter.

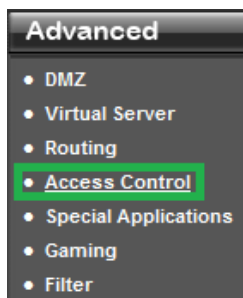
5. Click **Apply** to save settings.

URL Filter

Advanced > Access Control

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

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



- Click on **Advance**, click on **Access Control**.

Webs URL Filter Function Enabled ▾

- Select **Enable** on the pull down menu of **Web URL Filter Function**.

Webs URL Filter Rules				
LAN IP Address Range		URL	Schedule	Enabled
	-		Always ▾	☐
	-		Always ▾	☐
	-		Always ▾	☐
	-		Always ▾	☐

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

- IP Range** – Enter the IP address or IP address range to apply URL Filter (e.g. 192.168.10.20-192.168.10.20 or 192.168.10.20-192.168.10.30).

Note: The filter will not be applied to IP addresses outside of the range specified. You can leave the field blank to enable the rule for the entire LAN clients.

- URL:** Enter the URL you would like deny access. **Port Range:** Enter the port or port range to apply the protocol.
- Schedule:** Select the defined schedule you would like to have the rule to be applied. (see “[Set Schedule](#)” section on page 31).
- Enabled:** Selecting **Enable** turns on the filter

MAC Filters

Wireless > Security

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

- Log into your router management page (see “[Access your router management page](#)” on page 26).
- Click on **Wireless**, click on **Security**.

 A screenshot of the 'Wireless MAC Filter' settings page. It shows a 'Filter Mode' dropdown set to 'Disabled'. Below it is a table with four rows for MAC addresses, each with three input fields.

- Review the MAC Filter options. Click **Apply** to save settings.

- Filter Mode:** Select the mode applied to t listed MAC addresses.

- o **Allow** computers/devices with MAC addresses listed below to access the local network, web management, and the Internet.
- o **Deny** computers/devices with MAC addresses listed below to access the local network, web management, and the Internet

Note: MAC filter can be configured to allow access to the listed MAC address and deny all others unlisted or vice versa. The recommended function is to choose to only allow access to the MAC addresses listed and deny all others unlisted because it is easier to determine the MAC addresses of devices in your network then to determine which MAC addresses you do not want to allow access.

- Mac Address:** Enter the Mac address you would like to apply on the filter mode.

Advanced Router Setup

Access your router management page

Note: Your router management page <http://192.168.10.1> is accessed through the use of your Internet web browser (e.g. Internet Explorer, Firefox, Chrome, Safari, Opera) and will be referenced frequently in this User's Guide.

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to <http://192.168.10.1>. Your router will prompt you for a user name and password.



2. Enter the default user name and password and then click **Login**.

Default User Name: **admin**

Default Password: **admin**

Using the Configuration Menu

Whenever you want to configure your TEW-812DRU you can access the Configuration Menu by opening the Web-browser and typing in the IP Address of the TEW-812DRU.

- Open the Web browser.
- Type in the current **IP Address** of the AP (i.e. <http://192.168.10.1>)
- Type **admin** in the **User Name** field.
- The **Password** is **admin**.
- Click **Login In**.



When you log into the unit the initial screen you will see is the status page that provides system information and network configurations.

System Info	
Firmware Version	0.0.9.0, Dec 19, 2012
System Time	Sun Jan 1 00:27:14 2012
System Up Time	00:27:21

Internet Configurations	
Connected Type	PPPoE
WAN IP Address	68.167.159.22
Subnet Mask	255.255.255.255
Default Gateway	192.168.29.251
Primary Domain Name Server	64.105.132.251
Secondary Domain Name Server	64.105.172.27
Connect Disconnect	

LAN	
MAC Address	00:11:E0:04:49:3D
IP Address	192.168.10.1
Subnet Mask	255.255.255.0

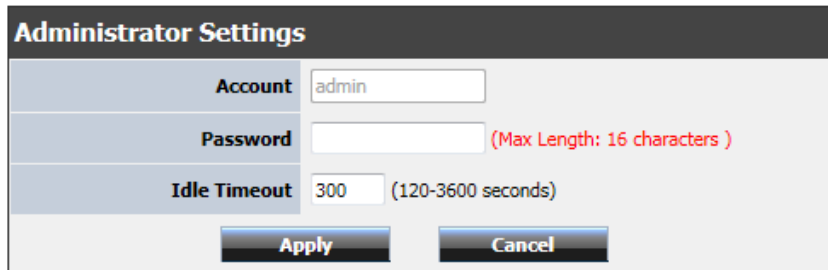
2.4GHz Wireless	
MAC Address	00:11:E0:04:49:3F
Channel	11
Network Name (SSID) / Security Mode	TRENDnet8124283/WPA2-PSK
Multiple SSID1 / Security Mode	
Multiple SSID2 / Security Mode	
Multiple SSID3 / Security Mode	

5GHz Wireless	
MAC Address	00:11:E0:04:49:3E
Channel	149
Network Name (SSID) / Security Mode	TRENDnet812ac4283/WPA2-PSK
Multiple SSID1 / Security Mode	
Multiple SSID2 / Security Mode	
Multiple SSID3 / Security Mode	

Change your router login password

Administrator > Management

1. Log into your router management page (see "[Access your router management page](#)" on page 26).
2. Click on **Administrator**, and click on **Management**.



The screenshot shows the 'Administrator Settings' form. It has three input fields: 'Account' with 'admin' entered, 'Password' which is empty and has a red note '(Max Length: 16 characters)', and 'Idle Timeout' with '300' entered and a note '(120-3600 seconds)'. At the bottom are 'Apply' and 'Cancel' buttons.

3. Under the **Administrator Settings** section, in the **Password** field, enter the new password
4. Enter the idle timeout time (in seconds) of when you would want to have log in prompt to appear.
5. To save changes, click **Apply**.

Note: If you change the router login password, you will need to access the router management page using the User Name "admin" and the new password instead of the default password "admin".

Change your router device name

Administrator > Management

1. Log into your router management page (see "[Access your router management page](#)" on page 26).
2. Click on **Administrator**, and click on **Management**.



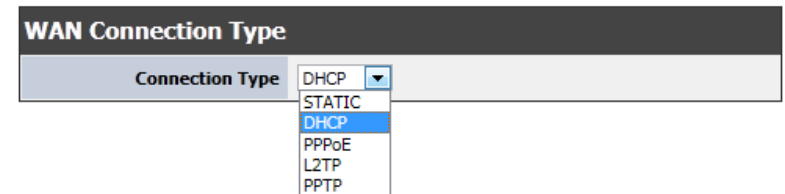
The screenshot shows the 'Device Name Settings' form. It has a 'Device Name' field with 'TEW-639GR' entered. At the bottom are 'Apply' and 'Cancel' buttons.

3. Under the **Device Name Settings** section, in the **Device Name** field, enter the new device name to show up on your network as reference to the router.
4. To save changes, click **Apply**.

Manually configure your Internet connection

Network > WAN Setting

1. Log into your router management page (see "[Access your router management page](#)" on page 26).
2. Click on **Network**, and click on **WAN Setting**.



The screenshot shows the 'WAN Connection Type' form. It has a 'Connection Type' dropdown menu with 'DHCP' selected. The dropdown list is open, showing options: DHCP, STATIC, DHCP, PPPoE, L2TP, and PPTP.

3. In the **Connection Type** drop-down list, click the type of Internet connection provided by your Internet Service Provider (ISP).
4. Complete the fields required by your ISP.
5. Complete the optional settings only if required by your ISP.
6. To save changes, click **Apply**.

Note: If you are unsure which Internet connection type you are using, please contact your ISP. **Note:** If your ISP requires a host name to be specified, you can specify it under Main > LAN & DHCP Server, in the **Host Name** field. To save changes, click **Apply** at bottom of the page.

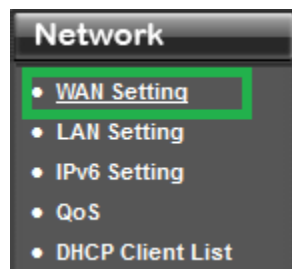
Clone a MAC address

Network > WAN Setting

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

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

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Network**, and click on **WAN Settings**.

MAC Address

3. Next to MAC Address field. Enter the MAC address of your computer.
4. To save changes, click **Apply**.

Change your router IP address

Network > LAN Setting

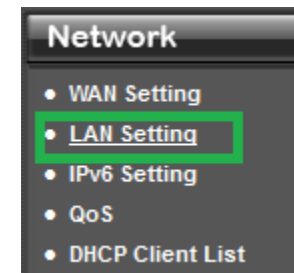
In most cases, you do not need to change your router IP address settings. Typically, the router IP address settings only needs to be changed, if you plan to use another router in your network with the same IP address settings, if you are connecting your router to an existing network that is already using the IP address settings your router is using, or if you are experiencing problems establishing VPN connections to your office network through your router.

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

Default Router IP Address: 192.168.10.1

Default Router Network: 192.168.10.0 / 255.255.255.0

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Network**, and click on **LAN Setting**.

LAN Interface Setting		
Configured Networks	Internal Network	Guest Network
MAC Address	00:11:E0:04:49:3D	00:00:00:00:00:00
IP Address	192.168.10.1	192.168.20.1
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.10.1	192.168.20.1

3. In **LAN Interface Setting** section enter the Internal Network section review the below settings to apply.

- **IP Address:** Enter the new router IP address. (e.g. 192.168.200.1)
- **Subnet Mask:** Enter the new router subnet mask. (e.g. 255.255.255.0)
- **Default Gateway:** Enter the new router default gateway IP address. (e.g. 192.168.200.1)

Note: The DHCP address range will change automatically to your new router IP address settings so you do not have to change the DHCP address range manually to match your new router IP address settings.

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

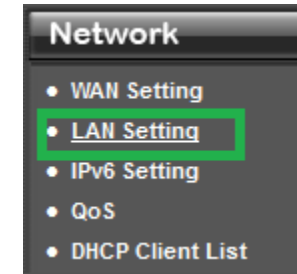
Note: You will need to access your router management page using your new router IP address to access the router management page. (e.g. Instead of using the default <http://192.168.10.1> using your new router IP address will use the following format using your new router IP address [http://\(new.router.ipaddress.here\)](http://(new.router.ipaddress.here)) to access your router management page.

Set up the DHCP server on your router

Network > LAN Setting

Your router can be used as a DHCP (Dynamic Host Configuration Protocol) server to automatically assign an IP address to each computer or device on your network. The DHCP server is enabled by default on your router. If you already have a DHCP server on your network, or if you do not want to use your router as a DHCP server, you can disable this setting. It is recommended to leave this setting enabled.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Network**, and click on **LAN Setting**.

DHCP Server Setting		
Configured Networks	Internal Network	Guest Network
DHCP Server	Enabled	Enabled
DHCP Start IP	192.168.10.100	192.168.20.100
DHCP End IP	192.168.10.150	192.168.20.150
DHCP Lease Time	86400 (seconds)	86400 (seconds)

3. In **Internal Network** section review the below settings. Click **Apply** to save settings.

- **DHCP Server:** Enable or Disable the DHCP server.
- **Start IP:** Changes the starting address for the DHCP server range. (e.g. 192.168.10.20)
- **End IP:** Changes the last address for the DHCP server range. (e.g. 192.168.10.30)
Note: The Start IP and End IP specify the range of IP addresses to automatically assign to computers or devices on your network.
- **DHCP Lease Time** – Click the drop-down list to select the lease time.
Note: The DHCP lease time is the amount of time a computer or device can keep an IP address assigned by the DHCP server. When the lease time expires, the computer or device will renew the IP address lease with the DHCP server, otherwise, if there is no attempt to renew the lease, the DHCP server will reallocate the IP address to be assigned to another computer or device.

Set up IPv6 on your router

Network > IPv6 Setting

Your router support IPv6 protocol. Which is the latest Internet Protocol standards.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Network**, and click on **IPv6 Setting**.

WAN IPv6 Setting	
WAN Network Prefix	2001:db0:1:0::/64

3. In **WAN IPv6 Setting** section, enter your IPv6 settings provided by your ISP (Internet Service Provider) to configure your router's IPv6 WAN settings. Click **Apply** to save settings.

LAN IPv6 Setting		
Configured Networks	Internal Network	Guest Network
Mode	Disabled	Disabled
LAN Network Prefix	2001:db8:1:0::/64	
DNS Server		
6to4 subnet ID	0	0

4. In **LAN IPv6 Setting** section, enter your IPv6 settings you would like to apply to your LAN (Local Area Network). Click **Apply** to save settings.

- **Mode**

- o **Disabled:** IPv6 will be disabled when this option is selected
- o **6to4 Only:** 6to4 is provided as a transitional mechanism for migrating from IPv4 to IPv6. It allows IPv6 packets to be transmitted over an IPv4 network through the automatic tunneling technology and routes traffic between 6to4 and IPv6 networks.
- o **Native IPv6 only:** Native IPv6 refers to a network where IPv6 is the only transport protocol.
- o **6to4 + Native IPv6:** Supports 6to4 and Native IPv6 simultaneously.
- **LAN Network Prefix:** Enter the LAN Network Prefix here. This can be based on ULA (Unique Local Address).
- **DNS server:** IPv6 DNS address will be provided by your local ISP.
- **6to4 subnet ID:** Specifies, in hexadecimal notation, a subnet ID other than 0

Set your router date and time

Main > Time

1. Log into your router management page (see "[Access your router management page](#)" on page 26).
2. Click on **Administrator**, and click on **Time**.

NTP Settings	
Enable NTP Server	☒
NTP Server	pool.ntp.org
Time Zone	(GMT-11:00) Midway Island, Samoa
NTP synchronization	300 (1~300) Minute

3. Select **Enable NTP Server**, to use a NTP server for the time settings. Or you can manually set the time settings by not selecting **NTP Server** option.
 - **NTP Server:** Select the NTP server you would like to use.
 - **Time Zone:** Select the your time zone.
 - **NTP synchronization:** Enter the time interval of when your router will sync with the NTP server.



Date and Time Settings

Date And Time

Year: 2012, Month: Jan, Day: 01

Hour: 01, Minute: 09, Second: 21

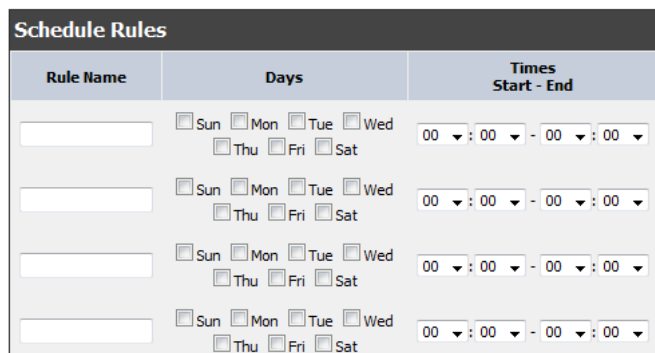
- To manually set the time settings. Select from the pull down menu the year, month and time you would like to apply on the router.
- To save changes, click **Apply**.

Set schedules

Advanced > Schedule

Your router has features Virtual Server rules and Access Controls that can turn on or off through schedules.

- Log into your router management page (see "[Access your router management page](#)" on page 26).
- Click on **Administrator**, and click on **Time**.



Rule Name	Days	Times Start - End
	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat	00 : 00 - 00 : 00
	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat	00 : 00 - 00 : 00
	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat	00 : 00 - 00 : 00
	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat	00 : 00 - 00 : 00

- Review the Schedule settings. Click **Apply** to save settings.
 - Rule Name:** Enter a name for the schedule you would like to apply.
 - Days:** Select the days you would like the rule to be applied or select **All Week** to enable the rule all week.

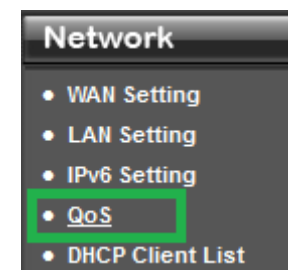
- Start/End Time:** Select the start and end time you would like the schedule to follow.

QoS (Quality of Service)

Network > QoS

QoS involves prioritization of network traffic. QoS can be targeted at a network interface, toward a given server or router's performance, or in terms of specific applications.

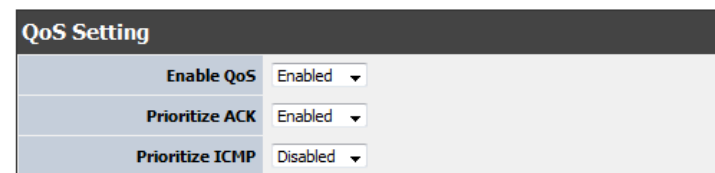
- Log into your router management page (see "[Access your router management page](#)" on page 26).



Network

- WAN Setting
- LAN Setting
- IPv6 Setting
- **QoS**
- DHCP Client List

- Click on **Network**, and click on **QoS**.
- Review the QoS settings.



QoS Setting

Enable QoS: Enabled

Prioritize ACK: Enabled

Prioritize ICMP: Disabled

- Enable QoS:** Enable or Disable the Quality of service through the router.
- Prioritize ACK:** Enable or disable ACK prioritization.
- Prioritize ICMP:** Enable or disable ICMP prioritization.

Traffic Class Setting

Default Traffic Class Highest ▾

3. Select the traffic class you would like to configure for your QoS rule.

Inbound Class Setting

Inbound Classes (% Max Input BW)			
BW Max Inbound		1500	Kbit/s
%BW			
Highest	0	0	Kbit/s
High	0	0	Kbit/s
Medium	0	0	Kbit/s
Low	0	0	Kbit/s
Lowest	0	0	Kbit/s

4. Review the **Inbound Class Setting** section.

- **BW Max Inbound:** Enter the maximum download speed of your ISP (Internet Service Provider).
- **Highest/High/Medium/Low/Lowest:** Enter the download speeds you would like to apply on each state of download speeds. This setting is similar to setting the priority speeds of each class

Outbound Class Setting

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

5. Review the **Outbound Class Setting** section. These fields would automatically populate when Inbound Class is configured, but setting allows you make any fine adjustments. Click **Apply** to save settings.

- **BW Max Inbound:** Enter the maximum upload speed of your ISP (Internet Service Provider).
- **Highest/High/Medium/Low/Lowest:** Enter the upload speeds you would like to apply on each state of download speeds. This setting is similar to setting the priority speeds of each class

QoS Rule Add

Add QoS Rule (Outbound)	
IP/MAC Address Filter	Any ▾ Address:
Protocol Filter	Any ▾
Port Filter	Any ▾ Port List:
Class Assigned	Highest ▾
Description	
Add Rule	

6. Review the **QoS Rule** settings.

- **IP/MAC Address Filter:** Select from the pull down menu the IP address or MAC you would like to apply and enter the IP address of MAC address.
- **Protocol Filter:** Select the protocol you would like to apply on the QoS Rule.
- **Port Filter:** Select the port from the pull down menu you would like to assign on the QoS rule and enter the port.
- **Class Assigned:** Select from the pull down menu the class you applied on the previous section you would like to assign the QoS rule.
- **Description:** Enter the QoS description that best describes the rule.

7. Click **Add Rule** to save the settings.

Open a device on your network to the Internet

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

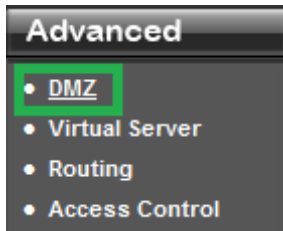
DMZ

Advanced > DMZ

You may want to expose a specific computer or device on your network to the Internet to allow anyone to access it. Your router includes the DMZ (Demilitarized Zone) feature that makes all the ports and services available on the WAN/Internet side of the router and forwards them to a single IP address (computer or network device) on your network. The DMZ feature is an easy way of allowing access from the Internet however, it is a very **insecure** technology and will open local area network to greater threats from Internet attacks.

It is strongly recommended to use **Virtual Server** (also called port forwarding, see "[Virtual Server](#)" on page 33) to allow access to your computers or network devices from the Internet.

1. Make the computer or network device (for which you are establishing a DMZ link) has a static IP address. Signing up for a Dynamic DNS service (outlined in [Identify Your Network](#) section pg.37) will provide identification of the router's network from the Internet.
2. Log into your router management page (see "[Access your router management page](#)" on page 26).



3. Click on **Advanced**, and click on **DMZ**.

A screenshot of the 'DMZ Settings' form. It has two sections: 'DMZ Settings' with a dropdown menu set to 'Enabled', and 'DMZ IP Address' with an empty text input field.

4. Select Enable in the **DMZ Settings** section.
5. Enter the IP address you assigned to the computer or network device to expose to the Internet.
6. To save changes, click **Apply**.

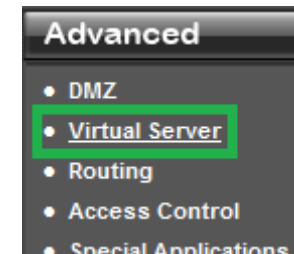
Virtual Server

Advanced > Virtual Server

Virtual Server (also called port forwarding) allows you to define specific ports (used or required by a specific application) and forward them to a single IP address (a computer or device) on your network. Using this feature is more secure compared to using DMZ (see "[DMZ](#)" on page 32) in which DMZ forwards all ports instead of only specific ports used by an application. An example would be forwarding a port to an IP camera (TRENDnet IP cameras default to HTTP TCP port 80 for remote access web requests) on your network to be able to view it over the Internet. To open several ports please refer to "[Gaming](#)" section on page 35.

Since most ISPs constantly change your home IP address, to be able to access the Virtual Server port(s) from the Internet it is recommended to setup Dynamic DNS service (outlined in [Identify Your Network](#) section pg.37).

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Advanced**, and click on **Virtual Server**.

A screenshot of the 'Virtual Server' configuration page. The 'Virtual Server Function' section has a dropdown menu set to 'Enabled'.

3. Select Enable in the Virtual Server Function section.

Virtual Server Rules					
Protocol	Public Port	LAN IP Address	Private Port	Schedule	Enabled
TCP ▼				Always ▼	☐
TCP ▼				Always ▼	☐
TCP ▼				Always ▼	☐
TCP ▼				Always ▼	☐
TCP ▼				Always ▼	☐

4. Review the virtual server settings. Click **Apply** to save settings.

- **Protocol:** Select the protocol required for your device. **TCP** or **UDP**.

Note: Please refer to the device documentation to determine which ports and protocols are required. You should assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.

- **Public Port:** Enter the port number used to access the device from the Internet.
- **LAN IP Address:** Enter the IP address of the device to forward the port (e.g. 192.168.10.101).
- **Schedule:** Select the defined schedule you would like to have the rule to be applied (see "[Set Schedule](#)" section on page 31).

Note: The **Public Port** can be assigned a different port number than the **Private Port** (also known as port redirection), however it is recommended to use the same port number for both settings. Please refer to the device documentation to determine which ports and protocols are required.

- **Enabled:** Selecting **Enabled** turns on the virtual server and unchecking disabled the rule..

Example: To forward TCP port 80 to your IP camera

1. Setup DynDNS service (see [Identify Your Network](#) section pg.38).
2. Access TRENDnet IP Camera management page and forward Port 80 (see product documentation)
3. Make sure to configure your network/IP camera to use a static IP address.

Note: You may need to reference your camera documentation on configuring a static IP address.

4. Log into your router management page (see "[Access your router management page](#)" on page 26).
5. Click on **Advanced**, and click on **Virtual Server**.
6. Click **Enabled** to turn on this virtual server.
7. Next to **Name**, you can enter another name for the virtual server, otherwise, leave the default name.
8. Next to **LAN Server**, enter the IP address assigned to the camera. (e.g. 192.168.10.101)
9. Next to **Protocol**, make sure **TCP** is selected in the drop-down list.
10. The **Private Port** and **Public Port**, make sure port number **80** is configured for both settings.
11. To save the changes, click **Add**.

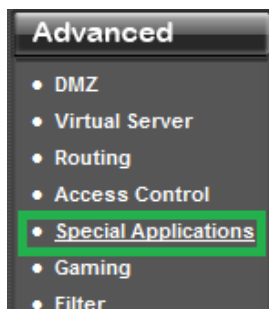
Special Applications

Advanced > Special Application

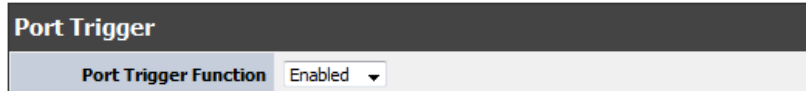
Special applications (also called port triggering) is typically used for online gaming applications or communication applications that require a range of ports or several ports to be dynamically opened on request to a device on your network. The router will wait for a request on a specific port or range of ports (or trigger port/port range) from a device on your network and once a request is detected by your router, the router will forward a single port or multiple ports (or incoming port/port range) to the device on your network. This feature is not typically used as most devices and routers currently use UPnP (Universal Plug and Play) to automatically configure your router to allow access for applications. See "[Enable/disable UPnP on your router](#)" on page 37.

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

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Advanced**, and click on **Special Application**.



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

Port Trigger Rules						
Match Protocol	Match Port Range		Trigger Protocol	Trigger Port Range		Enabled
TCP ▼		-	TCP ▼		-	☐
TCP ▼		-	TCP ▼		-	☐
TCP ▼		-	TCP ▼		-	☐
TCP ▼		-	TCP ▼		-	☐
TCP ▼		-	TCP ▼		-	☐

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

- **Match Protocol:** Select the protocol to be forwarded to the device. **TCP** or **UDP**.
- **Match Port:** Enter the ports or port range to be forwarded to the device. (e.g. 2000-2038 ,2200-2210).
- **Trigger Protocol:** Select the protocol requested by the device. **TCP** or **UDP**.
- **Trigger Port:** Enter the ports or port range requested by the device. (e.g. 554-554 or 6112-6112).

Note: Please refer to the device documentation to determine which ports and protocols are required.

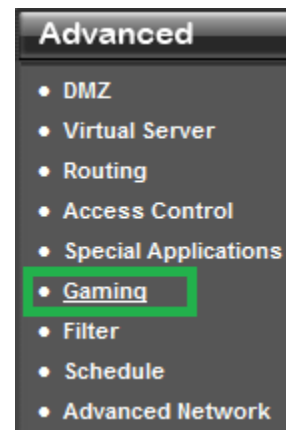
- **Schedule:** Select the defined schedule you would like to have the rule to be applied (see "[Set Schedule](#)" section on page 31).
- **Enabled:** Selecting **Enabled** turns on the virtual server and selecting unchecking disables the rule.

Gaming

Advanced > Gaming

Gaming allows you to define multiple ports (used or required by a specific application or game) and forward them to a single IP address (a computer or device) on your network. Using this feature is more secure compared to using DMZ (see "[DMZ](#)" on page 32) in which DMZ forwards all ports instead of only specific ports used by an application. Since most ISPs constantly change your home IP address, to be able to access the Virtual Server port(s) from the Internet it is recommended to setup Dynamic DNS service (see "[Identify your network over the Internet](#)" section on page 37).

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Advanced**, and click on **Gaming**.

Gaming

Gaming Function Enabled ▾

3. Click on **Enabled** under **Gaming Function** section.

Gaming Rules

LAN IP Address	TCP Ports	UDP Ports	Schedule	Enabled
	-	-	Always ▾	☐
	-	-	Always ▾	☐
	-	-	Always ▾	☐
	-	-	Always ▾	☐

3. Review the virtual server settings. Click **Apply** to save settings.

- **LAN IP Address:** Enter the IP address of the device to forward the port (e.g. 192.168.10.101).
 - **TCP Ports to Open:** Enter the TCP port you would like to set.
 - **UDP Ports to Open:** Enter the UDP port you would like to set.
- Note:** Please refer to the device documentation to determine which ports and protocols are required. You should assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.
- **Schedule:** Select the defined schedule you would like to have the rule to be applied (see [“Set Schedule”](#) section on page 31).
 - **Enabled:** Selecting **Enabled** turns on the virtual server and selecting unchecking disables the rule.

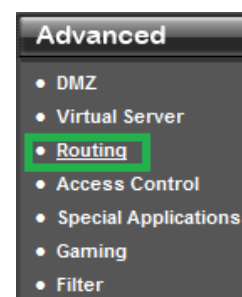
Add static routes to your router*Advanced > Routing*

You may want set up your router to route computers or devices on your network to other local networks through other routers. Generally, different networks can be determined by the IP addressing assigned to those networks. Generally speaking and for the case of an example, your network may have 192.168.10.x IP addressing and another network may have 192.168.20.x IP addressing and because the IP addressing of these two networks are different, they are separate networks. In order to communicate

between the two separate networks, static routing needs to be configured. Below is an example diagram where routing is needed for devices and computers on your network to access the other network.

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

1. Log into your router management page (see [“Access your router management page”](#) on page 26).



2. Click on **Advanced**, and click on **Routing**.

WAN Static Routes

IP Address	Subnet Mask	Gateway	Metric

3. Review the **WAN Static Routes** section. Click **Apply** to save settings.

- **IP Address:** Enter the IP network address of the destination network for the route. (e.g. 192.168.20.0)
- **Subnet Mask:** Enter the subnet mask of the destination network for the route.(e.g. 255.255.255.0)
- **Gateway:** Enter the gateway to the destination network for the route. (e.g. 192.168.10.2)

- **Metric:** Enter the metric or priority of the route. The metric range is 1-15, the lowest number 1 being the highest priority. (e.g. 1)

LAN Static Routes			
IP Address	Subnet Mask	Gateway	Metric

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

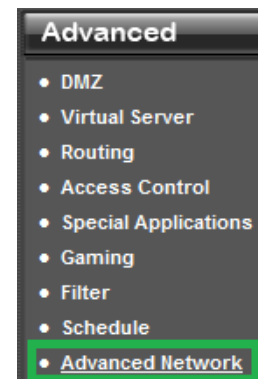
- **IP Address:** Enter the IP network address of the destination network for the route. (e.g. 192.168.20.0)
- **Subnet Mask:** Enter the subnet mask of the destination network for the route. (e.g. 255.255.255.0)
- **Gateway:** Enter the gateway to the destination network for the route. (e.g. 192.168.10.2)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

Enable/disable UPnP on your router

Advanced > Advanced Network

UPnP (Universal Plug and Play) allows devices connected to a network to discover each other and automatically open the connections or services for specific applications (e.g. instant messenger, online gaming applications, etc.) UPnP is enabled on your router by default to allow specific applications required by your computers or devices to allow connections through your router as they are needed.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Advanced**, and click on **Advanced Network**.



3. Next to **UPnP**, select **Enable** or **Disable** on the pull down menu to turn the feature on or off on your router.

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

4. Click **Apply**, to save settings.

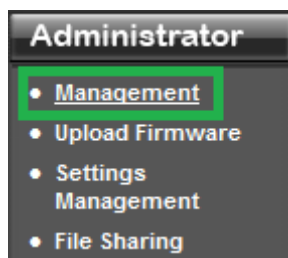
Identify your network on the Internet

Administrator > Management

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

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

1. Sign up for one of the DDNS available service providers list under **Server Address**. (e.g. dyndns.com, etc.)
2. Log into your router management page (see "[Access your router management page](#)" on page 26).



3. Click on **Administrator** and click on **Management**.

A screenshot of the 'DDNS Settings' form. It has a dark header with the title 'DDNS Settings'. Below the header, there are four rows of settings: 'Dynamic DNS Provider' with a dropdown menu showing 'None', 'Host Name' with a text input field, 'Account' with a text input field, and 'Password' with a text input field. At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

4. Review the **DDNS Settings** section. Click **Apply** to save settings.
 - **Dynamic DNS Provider:** Select your DDNS service.
 - **Host Name:** Personal URL provided to you by your Dynamic DNS service provider (e.g. www.trendnet.dyndns.biz)
 - **User Name:** The user name needed to log in to your Dynamic DNS service account
 - **Password:** This is the password to gain access to Dynamic DNS service (NOT your router or wireless network password) for which you have signed up to.

Share Files

Administrator > File Sharing

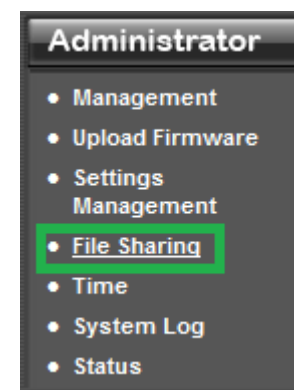
Your router's USB port can be used to share files through the network when a USB storage device is connected on the back USB port. The router supports both FTP and SAMBA (SMB) filing sharing protocols.

Samba

Administrator > File Sharing

Samba is a network protocol that allows you to access shared files through your network. In order to share files, you will need to plug in a USB storage device on the USB port on the back of the router. You can access these files under your network map or by typing [\\routerIPaddress](#) on your browser's address bar. Please follow the below steps to configure the router's Samba settings

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Administrator**, and click on **File Sharing**.

Samba Server Information	
Server Status	Enabled ▾
Server Name	TEW812DRU_SMB
Workgroup	WORKGROUP
Description	

3. Review the setting on **Samba Server Information** section. Click **Apply** to save settings

- **Server Status:** Select enable or disable for the feature.
- **Server Name:** Enter the name of your server.
- **Workgroup:** Enter the work group of your server.
- **Description:** Enter a description of the server.

Administrator	
User Name	admin
Password	admin

4. Review the administrator settings required for your **Samba server**. Click **Apply** to save settings. Administrator will have read and write access to files. To define user accounts continue to the next step.

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

User Account List			
User Name	Password	Permission	Enabled
		Read Only ▾	☐
		Read Only ▾	☐
		Read Only ▾	☐
		Read Only ▾	☐
		Read Only ▾	☐

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

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

FTP

Administrator > File Sharing

FTP (File Transfer Protocol) is used to access shared files through the Internet. In order to share files, you will need to plug in a USB storage device on the USB port on the back of the router. Signing up for a Dynamic DNS service (outlined in [Identify Your Network](#) section pg.38) will provide identification of the router's network from the Internet. You can access your shared files by typing ex. <ftp://router'sWANIPaddress> or <ftp://myDDNSservice> Please follow the steps below to configure the router's FTP settings

1. Log into your router management page (see "[Access your router management page](#)" on page 26).

Administrator
• Management
• Upload Firmware
• Settings Management
• File Sharing
• Time
• System Log
• Status

2. Click on **Administrator**, and click on **File Sharing**.

FTP Server Information	
Server Status	Enabled ▾
Language(Codepage)	Traditional Chinese ▾

3. Review the setting on **Samba Server Information** section. Click **Apply** to save settings

- **Server Status:** Select enable or disable for the feature.
- **Language:** Select your language.

Administrator	
User Name	admin
Password	admin

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

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

User Account List			
User Name	Password	Permission	Enabled
		Read Only ▼	☐
		Read Only ▼	☐
		Read Only ▼	☐
		Read Only ▼	☐
		Read Only ▼	☐

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

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

Remotely check router status

Advanced > Advanced Network

For remote troubleshooting purposes, you may want to check your routers status in a remote location.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).
2. Click on **Administrator**, and click on **Management**.

Remote Management	
Remote Control (via WAN)	Enable ▼
Remote Port	8080
Apply Reset	

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

- **Remote Control:** Select enable or disable for the feature.
- **Port:** Enter the port to assign remote access to the router. It is recommended to leave this setting as 8080.

***Note:** If you have configured port 8080 for another configuration section such as virtual server or special application, please change the port to use.
(Recommended port range 1024-65534)*

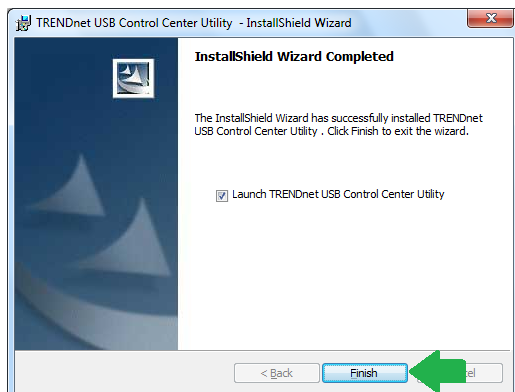
Print Share Utility Installation

Windows Installation

1. For each computer that requires access to USB printer, insert the **Utility CD-ROM** into your computer's CD-ROM Drive.



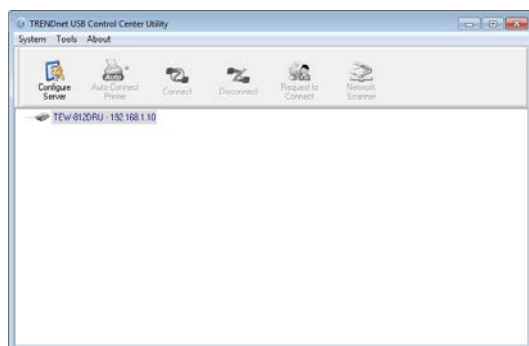
2. Click **Install Utility**



3. Follow the installation instructions and click **Finish** when prompted. Make sure to click **Launch TRENDnet USB Control Center Utility** to run the utility.



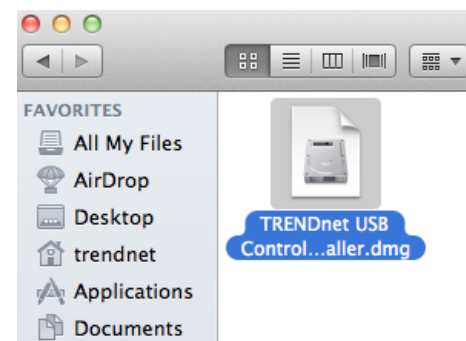
4. Double click on the **TRENDnet USB Control Center Utility** icon



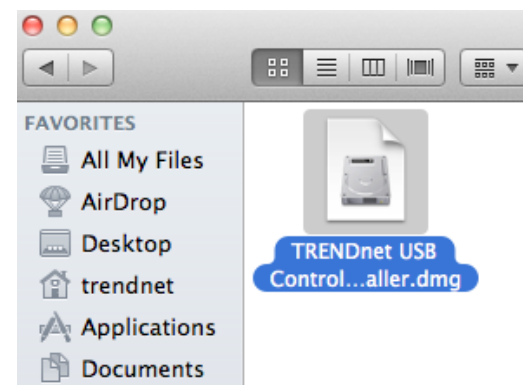
5. The utility will automatically detect your router and USB printer.

MAC OS X Installation

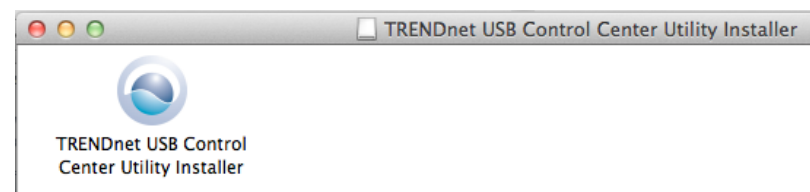
1. Insert the included CD-ROM into your computer's CD-ROM drive.



2. Open the CD contents and locate the "TRENDnet USB Control Center Utility Installer" (.dmg) file. Double-click the file.



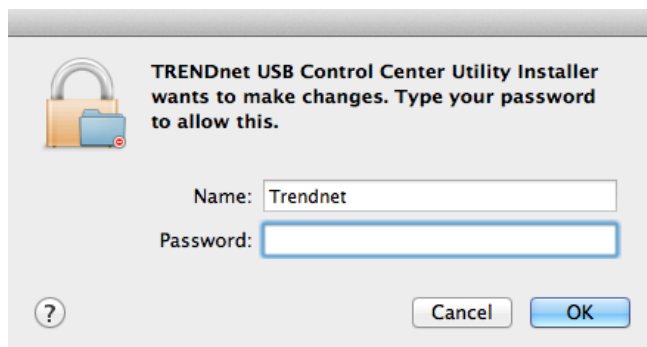
3. Double-click the file in the window.



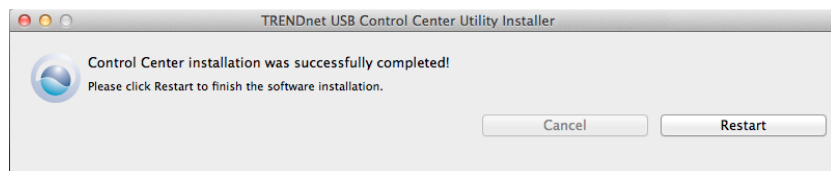
4. You will be prompted to install the utility. Click **Install** to start the installation.



5. You will be prompted for your password to allow the installation. Enter your password and click **OK**.



6. Once the installation is completed. Click **Restart** to restart your computer.



7. Run the TRENDnet USB Control Center Utility. The utility will automatically find your router and USB printer.

Launching the Utility

Windows OS

Upon completing the software installation, a desktop shortcut is automatically created. You double click the icon to start the utility or open the utility if it is already running.



If the utility is already running and you attempt to close the window, it will continue to run in the background and you will find the icon in your notification area if the utility is still running. To close and exit the utility and exit the application, you can right-click the notification icon and select **Exit** or click **System > Exit** in the utility main window, however, it is recommended to keep this utility running in the background.

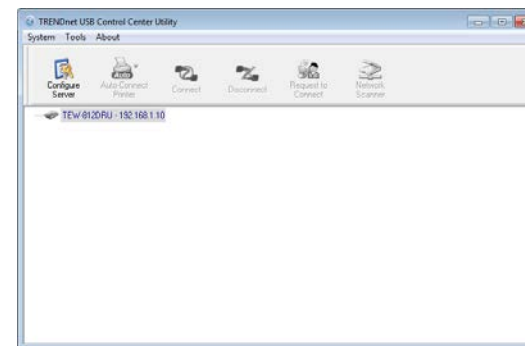


MAC OS X

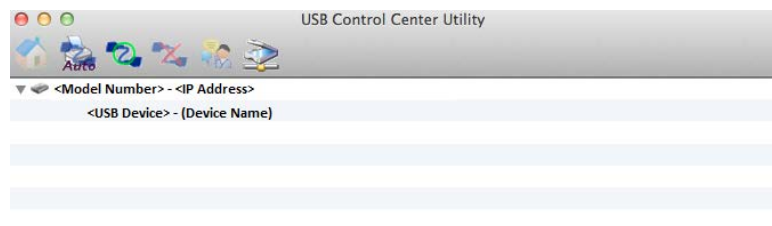
Upon completing the software installation, a desktop shortcut is automatically created. Double-click the icon to start the utility. Closing the utility will exit the application.

Utility Main Window

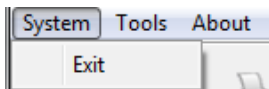
In the utility window, you will see the model name and IP address of your print server listed. When USB devices are connected, they will be listed under the model name and IP address of the print server.



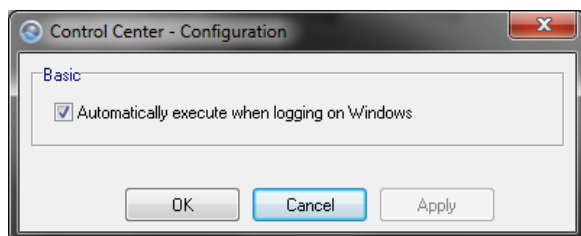
Windows OS



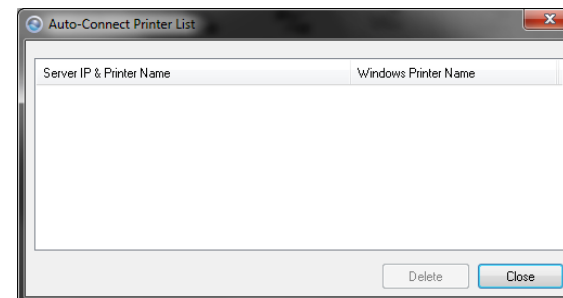
MAC OS X Utility

Menu Items (*Windows Only*)

- **System** - Clicking **Exit** will close the utility and exit the application.
- **Tools**



- o **Configuration** – Checking the option **Automatically execute when logging on Windows** will automatically start the utility when you log on. Unchecking the option will disable the utility from automatically starting when logging on.



- o **Auto-Connect Printer List** – Provides a list of printers installed on your computer. Select the printer you would like to assign to the Auto-Connect printer list. If you would like to delete printers from this listing, select the printer in the list and click **Delete**. Click **Close** to close the window.
- **About**
 - o **About** – Displays the software/driver version and support contact information.

Configure Server

Select the print server you would like to configure in the utility window.

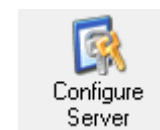
Windows OS

..... <Model Number> - <IP Address>

MAC OS X

..... <Model Number> - <IP Address>

1. Clicking the **Configure Server** button will open the router's management page in your web browser.



Windows OS



MAC OS X

Connect

To connect your computer to a USB device, select the USB device in the list, then click the **Connect** button to connect your computer to the USB device.

Note: The utility will only allow one computer to connect to one USB device at any given time, therefore, a computer must disconnect from the USB device first before another computer can connect to it.



Windows OS



MAC OS X

To verify if you are connected to the USB device, a message will appear next to the USB device displaying a message that the USB device is “Manually connected by <your computer name>”.

Windows OS

<Mass Storage or Printer> - (Name of device) (Manually connected by <your computer name>)

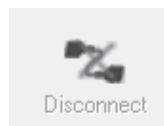
MAC OS X

<USB Device> - (Device Name) (Manually Connected by <your computer name>)

Disconnect

To disconnect your computer from a USB device, select the USB device in the list, then click the **Disconnect** button to disconnect your computer to the USB storage device or printer.

Note: The utility will only allow one computer to connect to one USB device at any given time, therefore, a computer must disconnect from the USB device first before another computer can connect to it.



Windows OS



MAC OS X

To verify if you disconnected from the USB device, the status message next to the message will not show any status message.

<Mass Storage or Printer> - (Name of device)

Windows OS

<Model Number> - <IP Address>

MAC OS X

If another computer is currently connected to the USB device you are trying to connect your computer to, you will not be able to connect to it. To verify if another computer is connected to the device, a message will appear next to the USB device displaying a message that the USB device is “Manually connected by <another computer name>”.

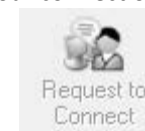
<Mass Storage or Printer> - (Name of device) (Manually connected by <another computer name>)

Windows OS

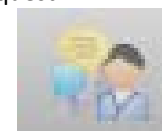
<USB Device> - (Device Name) (Manually Connected by <another computer name>)

MAC OS X

If a USB device is currently being used by another computer, click the **Request to Connect** button to send a request to the computer that is currently connected to the USB device. The computer that is currently connected to USB device will be prompted to “Accept” or “Reject” the your connection request.



Windows OS



MAC OS X

Sending a Request to Connect

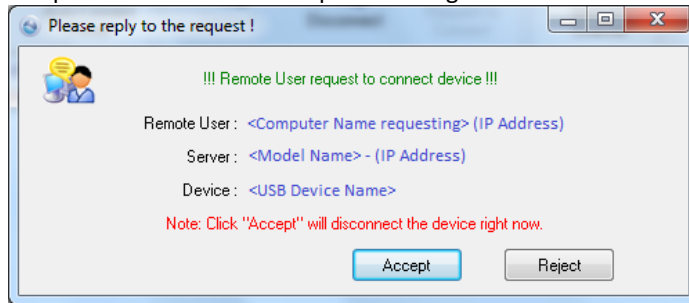
You can send a request to connect to the computer that is currently connected to the USB device you would like to establish connection too.



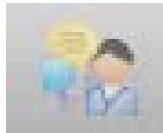
Windows OS

To send t a request to connect to a USB device, click the **Request to Connect** button.

The remote computer will receive the request message below.



- **Accept:** Clicking this option will disconnect your computer from the device and allow the requesting computer to connect to the USB device.
- **Reject:** Clicking this option will disregard the request and your computer will not be able to connect to the USB



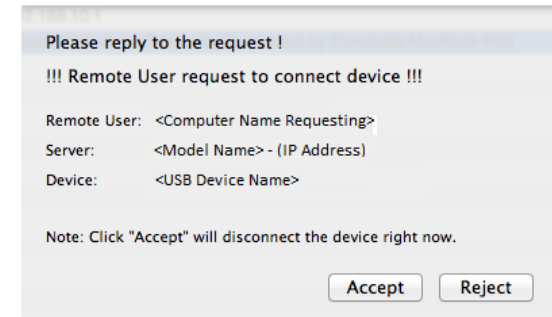
MAC OS X

To send a request to connect to a USB device, click the **Request to Connect** button.

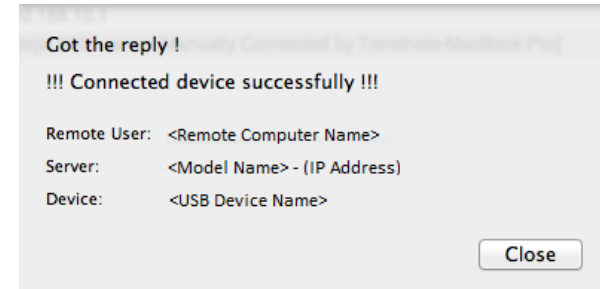
The local computer sending the request will show the status message below.



The remote computer will receive the request message below.

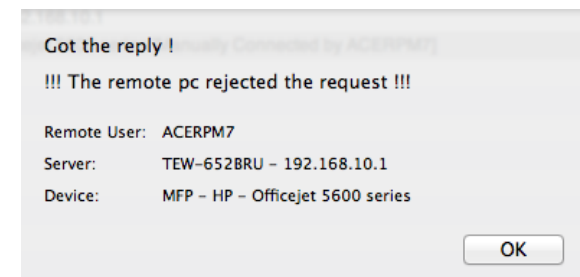


- **Accept:** Clicking this option will disconnect your computer from the device and allow the requesting computer to connect to the device.



If the remote computer accepts the request, the local computer will display the message below. Click **Close** to close the message.

- **Reject:** Clicking this option will disregard the request.



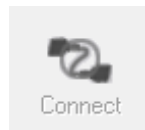
If the remote computer rejects the request, the local computer will display the message below. Click OK to close the message.

Connect to a Printer

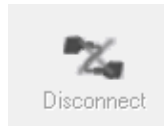
Note: This function applies to stand-alone USB printers or USB multi-function printers. It is required that the printer drivers are installed before your computer is able to print. Please ensure the printer drivers are installed. If the printer drivers are not installed, please refer to your printer manufacturer website or documentation on where to download and how to install the printer drivers. Before installing the printer drivers, connect your computer to the printer using the USB utility first. Some printers may require that the printer is directly connected to the computer in order to complete the driver installation.

Once the printer drivers are installed properly on your computer,

1. Select the printer listed in the utility.



2. Click **Connect** to connect your computer to the printer.
3. Once your computer is connected, you can send print jobs to the printer.



4. After you have finished printing, click Disconnect, to make the printer available to other computers on your network that use the printer, or, you can use the Auto-Connect Printer Feature.

Auto-Connect Printer

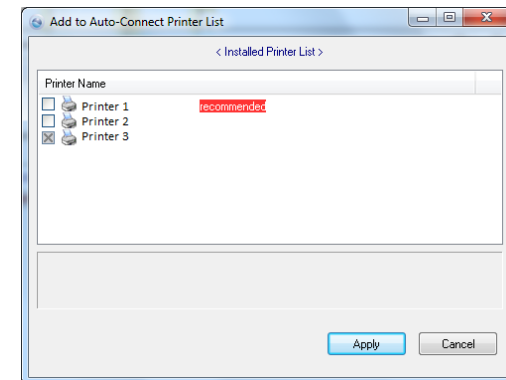
When a USB printer is connected and selected in the main window, clicking this option allows you to enable/disable the auto connect feature to a selected printer in the Auto-Connect printer list. When your computer attempts to print, the Auto-Connect feature will automatically connect your computer to the set Auto-Connect printer assigned in the utility. Once the print job from your computer is completed, it will automatically disconnect to make the printer available to other computers on your network.

Note: It is recommended to enable this feature on all computers that will need to connect to the USB printer. Enabling the Auto-Connect Printer feature will avoid the

complexity of having to manually connect and disconnect from the printer for each computer when multiple computers are sending print jobs to the USB printer.



1. Click **Auto-Connect Printer**.
2. Select the assigned printer to use as the auto connect printer by checking the box.

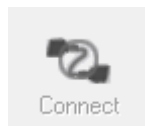


3. When you are finished, click **Apply**.

Connect to a Scanner

Note: This function applies to stand-alone USB scanners or USB scanners included with multi-function printers. It is required that the scanner drivers are installed before your computer is able to scan. Please ensure the scanner drivers are installed. If the scanner drivers are not installed, please refer to your printer manufacturer website or documentation on where to download and how to install the scanner drivers. Before installing the scanner drivers, connect your computer to the printer using the USB utility first. Some scanners may require that the scanner is directly connected to the computer in order to complete the driver installation.

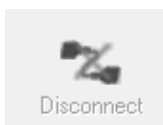
1. Select the scanner or multi-function printer with scanning capability listed in the utility.



- Click **Connect** to connect your computer to the scanner.



- Once your computer is connected, you can receive scanned files from the scanner.



- After you have finished printing, click **Disconnect**, to make the scanner available to other computers on your network that use the scanner.

Router Maintenance & Monitoring

Reset your router to factory defaults

Administrator > Settings Management

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting. Before you reset your router to defaults, if possible, you should backup your router configuration first, see [“Backup and restore your router configuration settings”](#) on page 48.

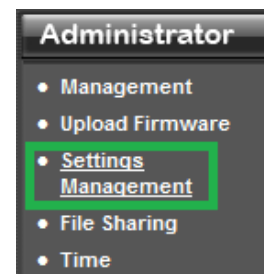
There are two methods that can be used to reset your router to factory defaults.

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

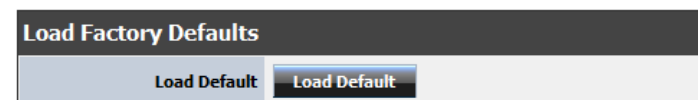
OR

- **Router Management Page**

- Log into your router management page (see [“Access your router management page”](#) on page 26).



- Click on **Administrator** and click on **Settings Management**.



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

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	192.168.10.100-192.168.150
Wireless 2.4GHz	Enabled
Wireless 2.4GHz Encryption	Please refer to wireless sticker or device label
Wireless 5Ghz	Enabled
Wireless 5GHz Encryption	Please refer to wireless sticker or device label

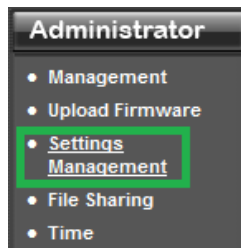
Backup and restore your router configuration settings

Administrator > Settings Management

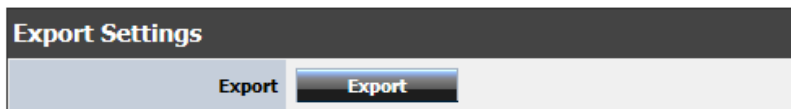
You may have added many customized settings to your router and in the case that you need to reset your router to default, all your customized settings would be lost and would require you to manually reconfigure all of your router settings instead of simply restoring from a backed up router configuration file.

To backup your router configuration:

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



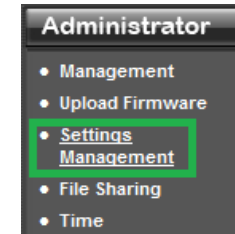
2. Click on **Administrator** and click on **Settings Management**.



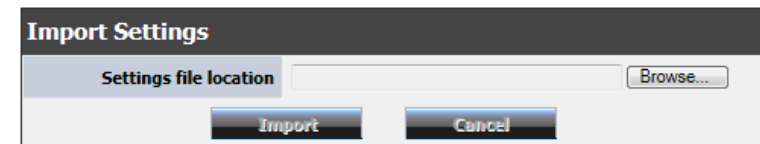
3. Under **Export Settings** section, click **Export**.
4. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: .cfg)

To restore your router configuration:

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



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



3. Under **Import Settings**, next to **Settings file location**, depending on your web browser, click on **Browse** or **Choose File**.
4. A separate file navigation window should open.
5. Select the router configuration file to restore and click **Load**. (Default Filename: *cfg.bin*). If prompted, click **Yes** or **OK**.
6. Wait for the router to restore settings.

Reboot your router

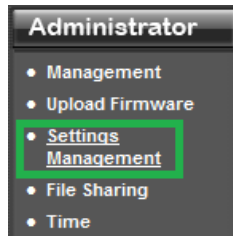
Administrator > Settings Management

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

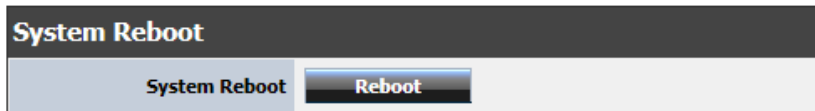
There are two methods that can be used to restart your router.

- **Turn the router off** for 10 seconds using the router On/Off switch (EU version only) located on the rear panel of your router or disconnecting the power port, see "[Product Hardware Features](#)" on page 5.
Use this method if you are encountering difficulties with accessing your router management page. This is also known as a hard reboot or power cycle.
OR
- **Router Management Page** – This is also known as a soft reboot or restart.

1. Log into your router management page (see "[Access your router management page](#)" on page 27).



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



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

Upgrade your router firmware

Administrator > Settings Management

TRENDnet may periodically release firmware upgrades that may add features or fix problems associated with your TRENDnet router model and version. To check if there is a firmware upgrade available for your device, please check your TRENDnet model and version using the link. <http://www.trendnet.com/downloads/>

In addition, it is also important to verify if the latest firmware version is newer than the one your router is currently running. To identify the firmware that is currently loaded on your router, log in to the router, click on the Administrator section and then on the Status. The firmware used by the router is listed at the top of this page. If there is a newer version available, also review the release notes to check if there were any new features you may want or if any problems were fixed that you may have been experiencing.

1. If a firmware upgrade is available, download the firmware to your computer.
2. Unzip the file to a folder on your computer.

Please note the following:

- Do not interrupt the firmware upgrade process. Do not turn off the device or press the Reset button during the upgrade.
- If you are upgrade the firmware using a laptop computer, ensure that the laptop is connected to a power source or ensure that the battery is fully charged.
- Disable sleep mode on your computer as this may interrupt the firmware upgrade process.
- Do not upgrade the firmware using a wireless connection, only using a wired network connection.
- Any interruptions during the firmware upgrade process may permanently damage your router.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).
2. Click on **Administrator** and click on **Upload Firmware**.



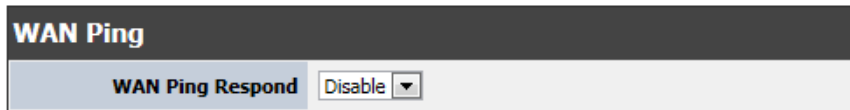
3. Depending on your web browser, in the **Upload Firmware** section, click **Browse** or **Choose File**.
4. Navigate to the folder on your computer where the unzipped firmware file (.bin) is located and select it.
5. Click **Upgrade**. If prompted, click **Yes** or **OK**.

Remotely check router status

Advanced > Advanced Network

For remote troubleshooting purposes, you may want to check your routers connectivity in a remote location. You can disable or enable your router to respond to ping request through the Internet.

1. Log into your router management page (see "[Access your router management page](#)" on page 27).
2. Click on **Advanced**, and click on **Advanced Network**.



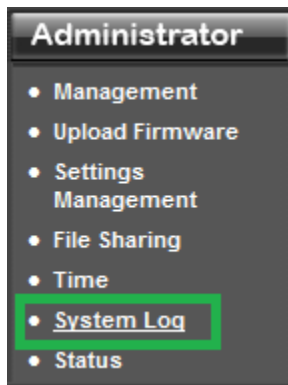
3. Next to **WAN Ping Respond**, select **Enable** or **Disable** on the pull down menu to turn the feature on or off on your router.

View your router log

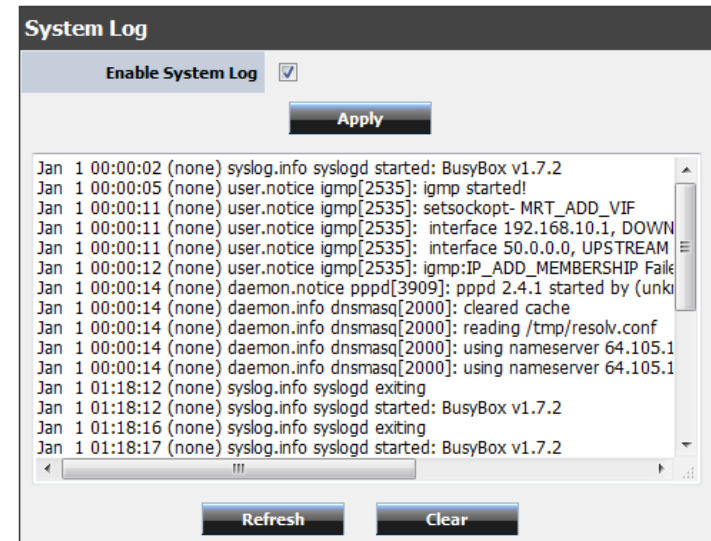
Administrator > System Log

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

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Administrator**, and click on **System Log**.



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

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

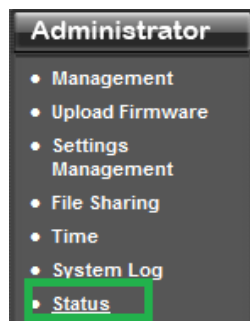
Router Status

Check the router system information

Administrator > Status

You may want to check the system information of your router such as WAN (Internet) connectivity, wireless and wired network settings, router MAC address, and firmware version.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



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

System Info

System Info	
Firmware Version	1.0.3.0, Jan 3, 2013
System Time	Wed Jan 16 12:41:03 2013
System Up Time	00:51:36

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

Internet Configurations

Internet Configurations	
Connected Type	PPPoE
WAN IP Address	68.167.159.22
Subnet Mask	255.255.255.255
Default Gateway	192.168.29.251
Primary Domain Name Server	64.105.132.251
Secondary Domain Name Server	64.105.172.27
Connect Disconnect	

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

LAN Information

LAN	
MAC Address	00:11:E0:04:49:3D
IP Address	192.168.10.1
Subnet Mask	255.255.255.0

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

2.4GHz Wireless LAN

2.4GHz Wireless	
MAC Address	00:11:E0:04:49:3F
Channel	11
Network Name (SSID) / Security Mode	TRENDnet8124283/WPA2-PSK
Multiple SSID1 / Security Mode	
Multiple SSID2 / Security Mode	
Multiple SSID3 / Security Mode	

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

5GHz Wireless LAN

5GHz Wireless	
MAC Address	00:11:E0:04:49:3E
Channel	149
Network Name (SSID) / Security Mode	TRENDnet812ac4283/WPA2-PSK
Multiple SSID1 / Security Mode	
Multiple SSID2 / Security Mode	
Multiple SSID3 / Security Mode	

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

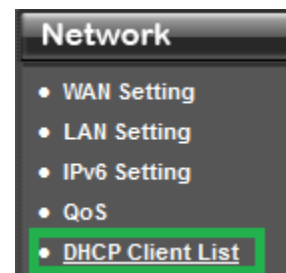
- **Network Name (SSID)/ Security Mode:** Displays the current wireless network name assigned to your router and the wireless security applied to the SSID

Dynamic DHCP List

Network > DHCP Client List

You can view the list of active lease entries for computers or devices that have been assigned IP addresses automatically from the DHCP server on your router.

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Network**, and click on **DHCP Client List**.

DHCP Clients				
Hostname	MAC Address	IP Address	Expires In	Network
	7C:ED:8D:AF:1A:06	192.168.10.100	Expired	Internal
	28:0D:FC:3D:25:EA	192.168.10.101	Expired	Internal
PM_Acer_Laptop	00:26:C6:2C:68:40	192.168.10.102	Expired	Internal
WDTVLive	00:90:A9:C4:17:2F	192.168.10.107	Expired	Internal

- **Host Name:** Displays the hostname of the connected client
- **MAC Address:** The MAC address of your client wireless or interface configuration.
- **IP Address:** Displays your router's current IP address.
- **Expires In:** Displays the time of when the client's IP address will automatically renew.
- **Network:** Displayed which network (Internal/Guest) that client is connected too.

2.4GHz Wireless Station List

Wireless > Station List

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

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Wireless**, and click on **Station List**

MAC Address	Association Time	Authorized	WMM Link	Power Save	APSD Default
00:90:A9:C4:17:2F	00:01:41	Yes	Yes	No	
00:14:D1:F2:98:61	00:02:25	Yes	Yes	No	
28:0D:FC:3D:25:EA	00:02:26	Yes	No	No	
7C:ED:8D:AF:1A:06	00:02:27	Yes	Yes	No	

- **MAC Address:** The current MAC address of your 2.4GHz wireless client.
- **Association Time:** Displays the time duration the client has been connected.
- **Authorized:** Displays if the connected client is authorized to connect.
- **WMM Link:** Determines if the wireless client is connected with WMM technology.
- **Power Save:** Displays if the connected client has power saving feature.
- **APSD Default:** Determines if APSD (Automatic Power Save Delivery) is enabled.

5GHz Wireless Station List

Wireless > Station List

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

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Wireless**, and click on **Station List**

MAC Address	Association Time	Authorized	WMM Link	Power Save	APSD Default
00:90:A9:C4:17:2F	00:01:41	Yes	Yes	No	
00:14:D1:F2:98:61	00:02:25	Yes	Yes	No	
28:0D:FC:3D:25:EA	00:02:26	Yes	No	No	
7C:ED:8D:AF:1A:06	00:02:27	Yes	Yes	No	

- **MAC Address:** The current MAC address of your 2.4GHz wireless client.
- **Association Time:** Displays the time duration the client has been connected.
- **Authorized:** Displays if the connected client is authorized to connect.
- **WMM Link:** Determines if the wireless client is connected with WMM technology.
- **Power Save:** Displays if the connected client has power saving feature.
- **APSD Default:** Determines if APSD (Automatic Power Save Delivery) is enabled.

QoS Wireless Station List

Wireless > Station List

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

1. Log into your router management page (see "[Access your router management page](#)" on page 26).



2. Click on **Wireless**, and click on **Station List**

QoS Rule List

Rule No.	Address Type	Address	Protocol	Port Filter	Port No.	Class	Description
----------	--------------	---------	----------	-------------	----------	-------	-------------

- **Rule no.** The QoS rule number.
- **Address Type:** Address applied to QoS rule.
- **Address:** Address assigned to QoS rule.
- **Protocol:** Protocol assigned to QoS rule
- **Port Filter:** Port filter assigned to QoS rule.
- **Post No.:** Port number assigned to QoS rule
- **Class:** Class assigned to QoS rule.
- **Description:** Description of QoS rule.

Management Page Structure

Network

- Internet Wizard
- Wireless Wizard

Network

- WAN Setting
 - Clone MAC Address
- LAN Setting
 - DHCP Reservation
- IPV6 Setting
- QoS
- DHCP Client List

Wireless 2.4GHz

- Basic
 - WDS
- Advanced
- Security
 - MAC Filter
- Guest Network
- WPS
- Station List

Wireless 2.4GHz

- Basic
 - WDS
- Advanced
- Security
 - MAC Filter
- Guest Network
- WPS

- Station List

Advanced

- DMZ
- Virtual Server
- Routing
- Access Control
- Special Applications
- Gaming
- Filter
- Schedule
- Advanced Network
 - UPnP
 - WAN Ping

Administrator

- Management
 - Password
 - DDNS
 - Remote Management
- Upload Firmware
- Settings Management
 - Export Settings
 - Import Settings
 - Load Factory Defaults
 - Reboot
- File Share
 - Samba
 - FTP
- Time
- System Log
- Status

Technical Specifications

Hardware	
Standards	Wired: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), IEEE 802.3ab (1000Base-T) Wireless: IEEE 802.11ac (draft 2.0), IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, 802.11a
Internet Protocol	IPv4 and IPv6
LAN	4 x 10/100/1000 Mbps Auto-MDIX
WAN	1 x 10/100/1000 Mbps Auto-MDIX
USB	1 x USB 2.0 Type-A (Storage / Printing)
WPS Button	Wi-Fi Protected Setup (WPS) connects with other WPS compliant devices
Reset Button	Reset unit back to factory default (press and hold for 10 seconds)
Network Protocols / Features	IGMP v1/2/3 proxy and snooping, Static and dynamic routing, UPnP, DHCP, server, Dynamic DNS (No-IP.com and DynDNS.com), NTP, IPsec / PPTP / L2TP VPN pass through, IPv6
Quality of Service	WMM and WAN (Configurable Upload / Download)
Control Center Utility OS Support	Windows: 8 (32/64-bit), 7 (32/64-bit), Vista (32/64-bit), XP (32/64-bit) Mac OS X: 10.4 / 10.5 / 10.6 / 10.7
Internet Connection Type	IPv6, Dynamic IP, Static (fixed) IP, PPPoE, PPTP, L2TP
Firewall	NAT, SPI, DMZ host, virtual servers, MAC / IP filters and URL filter
Management / Monitoring	Local / remote configuration, upgrade firmware, backup / restore configuration via web browser, internal system log, ping test tool
Supported	Internet Explorer 6.0 or above, Firefox 2.0 or above, Chrome, Opera,

Web Browser	Safari
LED Indicator	Power, LAN 1-4, WAN, 2.4GHz Wireless, 5GHz Wireless, WPS
Power Adapter	Input: 100 ~ 240 V, 50~60 Hz, 0.8 A Output: 12 V DC, 2 A external power adapter
Power Consumption	18 watts (max.)
Dimension (L x W x H)	48 x 155 x 180 mm (1.9 x 6.1 x 7.1 in)
Weight	395 g (14 oz)
Temperature	Operation: 0°~ 40°C (32°F~ 104°F) Storage: -20°~ 60°C (-4°F~140 °F)
Humidity	Max 90% (non-condensing)
Certifications	CE, FCC
Wireless	
Frequency	2.4 GHz: 2.412~2.462 (FCC) and 2.412~2.472 (ETSI) 5 GHz: 5.15 ~ 5.250 / 5.725~5.850 GHz (FCC) 5.15 ~ 5.250 (ETSI)
Antenna	2.4 GHz: 3 x 2 dBi PIFA internal 5 GHz: 3 x 2 dBi PIFA internal
Modulation	CCK, DQPSK, DBPSK, OFDM, BPSK, QPSK, 16/64/256-QAM
Data Rate	802.11a: up to 54 Mbps 802.11b: up to 11 Mbps 802.11g: up to 54 Mbps 802.11n: up to 450 Mbps (for both 2.4 & 5 GHz) 802.11ac: up to 1.3 Gbps
Security	64/128-bit WEP, WPA/WPA2-PSK, WPA/WPA2-RADIUS
Guest network	Up to 3 per wireless band
Access Control	MAC Address Filter (Up to 24 entries)

Output Power	802.11a: 12 dBm (typical) 802.11b: 16 dBm (typical) 802.11g: 15 dBm (typical) 802.11n: 12 dBm (typical) (for 2.4 & 5GHz) 802.11ac: 15 dBm (typical)
Receiving Sensitivity	802.11a: -68 dBm (typical) @ 54 Mbps 802.11b: -84 dBm (typical) @ 11 Mbps 802.11g: -72 dBm (typical) @ 54 Mbps 802.11n: -68 dBm (typical) @ 450 Mbps (for 2.4 & 5 GHz) 802.11ac: -55 dBm (typical) @ 1.3 Gbps
Channels	2.4 GHz: 1~11 (FCC), 1~13 (ETSI) 5 GHz: 36, 40, 44, 48, 149, 153, 157, 161 and 165 (FCC) 36, 40, 44, 48 (ETSI)

*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions.

Troubleshooting

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

Answer:

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

Windows 7

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

Windows Vista

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

Windows XP/2000

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

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

Q: I am not sure what type of Internet Account Type I have for my Cable/DSL connection. How do I find out?

Answer:

Contact your Internet Service Provider (ISP) for the correct information.

Q: The Wizard does not appear when I access the router. What should I do?

Answer:

1. Click on Wizard on the left hand side.
2. Near the top of the browser, "Pop-up blocked" message may appear. Right click on the message and select Always Allow Pop-ups from This Site.
3. Disable your browser's pop up blocker.

Q: I went through the Wizard, but I cannot get onto the Internet. What should I do?

Answer:

1. Verify that you can get onto the Internet with a direct connection into your modem (meaning plug your computer directly to the modem and verify that your single computer (without the help of the router) can access the Internet).
2. Power cycle your modem and router. Unplug the power to the modem and router. Wait 30 seconds, and then reconnect the power to the modem. Wait for the modem to fully boot up, and then reconnect the power to the router.
3. Contact your ISP and verify all the information that you have in regards to your Internet connection settings is correct.

Q: I cannot connect wirelessly to the router. What should I do?

Answer:

1. Double check that the WLAN light on the router is lit.
2. Power cycle the router. Unplug the power to the router. Wait 15 seconds, then plug the power back in to the router.
3. Contact the manufacturer of your wireless network adapter and make sure the wireless network adapter is configured with the proper SSID. The preset SSID is TRENDnet(model_number).
4. To verify whether or not wireless is enabled, login to the router management page, click on *Wireless*.
5. Please see "[Steps to improve wireless connectivity](#)" on page 22 if you continue to have wireless connectivity problems.

Appendix

How to find your IP address?

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

Command Prompt Method

Windows 2000/XP/Vista/7

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

MAC OS X

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

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

Graphical Method

MAC OS 10.6/10.5

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

MAC OS 10.4

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

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

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

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

Windows 7

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

Windows Vista

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

Windows XP/2000

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

MAC OS 10.4/10.5/10.6

- From the **Apple**, drop-down list, select **System Preferences**.
- Click the **Network** icon.
- From the **Location** drop-down list, select **Automatic**.
- 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**.
- 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.

- Restart your computer.

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

How to find your MAC address?

In Windows 2000/XP/Vista/7,

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

In MAC OS 10.4,

- Apple Menu > System Preferences > Network**
- From the **Show** menu, select **Built-in Ethernet**.
- On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

In MAC OS 10.5/10.6,

- Apple Menu > System Preferences > Network**
- Select **Ethernet** from the list on the left.
- Click the **Advanced** button.
- On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

How to connect to a wireless network using the built-in Windows utility?

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

Windows 7

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

Windows Vista

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

Windows XP

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

Federal Communication Commission Interference Statement

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

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

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

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

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

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

RoHS

This product is RoHS compliant.



Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- **EN60950-1:2006+A11: 2009**

Safety of Information Technology Equipment



- **EN 62311:2008**

- Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

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

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

- **EN 301 489-1 V1.8.1: (2008-04)**

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

- **EN 301 489-17 V2.1.1:(2009-05)**

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

- **EN 301 893 V1.5.1(2008-12)**

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

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

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

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of

2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

TEW-812DRU – 3 Years Warranty

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

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

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

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

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

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

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

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

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

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

PWP05202009v2

2013/01/16



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