

User's Guide



3G Mobile Wireless Router

TEW-716BRG

Contents

Product Overview	3
Package Contents	3
Features	3
Product Hardware Features.....	4
Application Diagram	5
Basic Router Setup	6
Creating a Home Network	6
Router Installation	7
Wireless Networking and Security	9
How to choose the type of security for your wireless network	9
Secure your wireless network	10
Connect wireless devices to your router	11
Connect wireless devices using WPS	11
Basic wireless settings	12
Steps to improve wireless connectivity	14
Access Control Filters	14
Access control basics	14
MAC address filters	14
Domain Filters	15
URL Filters	15
Packet Outbound/Inbound Filters.....	16
Advanced Router Setup.....	18
Access your router management page.....	18

Change your router login password	18
Set your router date and time	18
Manually configure your Internet connection	19
Change your router IP address	20
Set up the DHCP server on your router	20
Set up DHCP reservation	21
Enable/disable UPnP on your router	21
Enable/disable DoS (Denial of Service) Prevention	22
Allow/deny ping requests to your router from the Internet	22
Identify your network on the Internet	22
Allow remote access to your router management page	23
Open a device on your network to the Internet.....	23
DMZ.....	23
Virtual Server	24
Special Applications	25
Prioritize traffic using QoS (Quality of Service)	26
Create schedules	26
Router Maintenance & Monitoring	27
Reset your router to factory defaults	27
Router Default Settings	28
Backup and restore your router configuration settings	28
Upgrade your router firmware	29
Restart your router	29
Check connectivity using the router management page	30
Check the router system information	30
View your router log	31

View wireless devices connected to your router..... 32

View NAT activity of your router 32

Configure your router log 33

Enable SNMP on your router 34

Add static routes to your router 34

Enable dynamic routing on your router 35

Router Management Page Structure36

Technical Specifications.....37

Troubleshooting.....38

Appendix39

Product Overview

TEW-716BRG



Package Contents

In addition to your router, the package includes:

- TEW-716BRG
- Multi-Language Quick Installation Guide
- CD-ROM (User's Guide)
- USB power cable
- Power Adapter (5V, 1.2A).

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 3G Mobile Wireless Router, model TEW-716BRG, shares a single Internet connection from a compatible USB 3G modem provider (such as Sprint™, AT&T™, or Verizon™) with multiple users.

Compatible with USB dongles from every mobile provider, this compact router shares an Internet connection anywhere there is a 3G* mobile signal. No installation is required with auto-recognized modems; simply plug and go.

The router can be powered directly from a laptop's USB ports, eliminating the search for an electrical outlet. The device also features a built in hanging hook allowing users to neatly hang the TEW-716BRG on the back of a laptop screen while working. The TEW-716BRG makes it easy to share a single Internet connection while at the airport, job site, carpooling, or even while on vacation.

- USB 2.0 port (3G dongle Internet)
- USB power port
- Hanging clip neatly hangs the TEW-716BRG on the back of most laptop screens
- High-speed data rates of up to 150Mbps based on IEEE 802.11n*
- Compliant with IEEE 802.11b/g standards
- Works with UMTS/HSPA, WCDMA (HSDPA), CDMA2000 (EV-DO), and TD-SCDMA mobile networks**
- Third party wireless 3G dongles connects to ISPs such as AT&T™, Sprint™, T-Mobile™, or Verizon™***
- Powered by computer's USB ports for easy portability or by an optional electrical adapter
- Advanced wireless encryption of up to WPA2-PSK
- Built-in antennas provide high-speed performance and expansive wireless coverage
- Quality of Service (QoS) prioritization controls
- Advanced Firewall protection with Network Address Translation (NAT), Stateful Packet Inspection (SPI), and DoS (Denial of Service) Attacks
- Static and Dynamic RIP V1/2 routing support
- Access restriction with internet Access Control by URL, Domain, packet type, and MAC address
- Universal Plug and Play (UPnP) for auto discovery and support for device configuration of Internet applications

- Easy setup via web browser using Internet Explorer 6.0 or above, Firefox 2.0 or above, Chrome, Opera, Safari
- One touch wireless connection to wireless clients using the WPS button
- Easy setup installation wizard with built-in WAN auto detection
- 3-year limited warranty

*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.

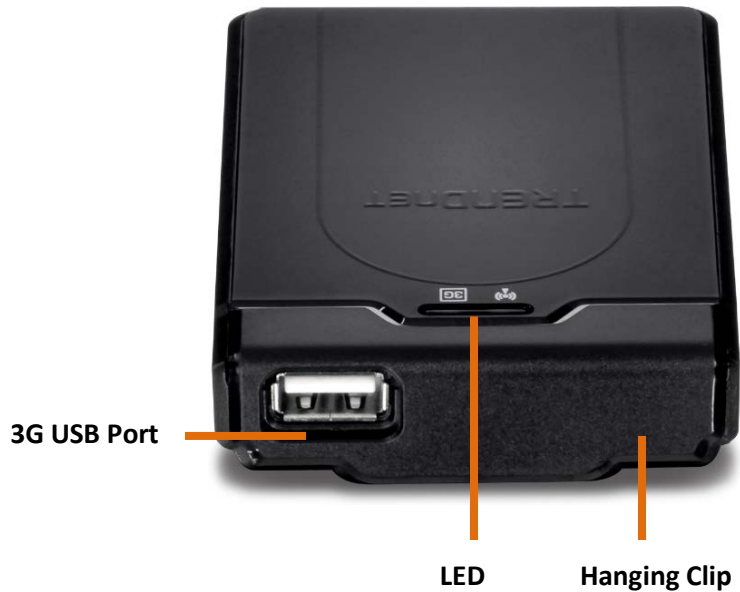
Product Hardware Features

Bottom View



- **Power Port:** Connect the included power adapter from your router power port and to an available power outlet.
- **On/Off Power Switch:** Push the router On/Off power switch to turn your router "On" (Inner position) or "Off" (Outer position).
- **WPS/Reset Button:** Press and hold this button for 3 seconds to activate WPS Push Button Configuration (PBC) or Press and hold for 10 seconds to reset the router back to factory default settings.

Top View



- **3G USB Port:** Plug your USB 3G Dongle to connect to your 3G network
- **3G LED** – This LED indicator is solid green when your router is connected to your 3G network. The LED indicator will be blinking green while data is transmitted or received through the router.
- **WLAN (Link/Activity) LED:** This LED indicator is blinking green when the wireless is “On” and functioning properly on your router. This LED indicator will be blinking green rapidly while data is transmitted or received by your wireless clients or wireless network devices connected to your router.
- **Hanging Clip:** Remove the hanging clip from the router to use as a hanging clip to most monitors. Press the button on the back of the router to release the hanging clip and rotate the clip around and clip back to the router.

Application Diagram

The 3G Mobile Wireless Router is installed and is connected to the 3G wireless network. Wireless signals from the router are broadcasted to wireless clients such as laptops (with wireless capability) thereby providing Internet access.

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.**

2. Make sure that your modem is working properly. Your modem is often provided by your Internet Service Provider (ISP) when you sign up for Internet service. If your modem is not working contact your ISP to verify functionality.
3. Set up your router. See "How to setup your router" below.
4. To connect additional wired computers or wired network devices to your network, see "[Connect wireless devices to your router](#)" on page 11.
5. To set up wireless networking on your router, see "[Secure your wireless network](#)" on page 10.

How to setup your router

Refer to the Quick Installation Guide or continue to the next section "[Router Installation](#)" on page 7 for more detailed installation instructions.

Where to find more help

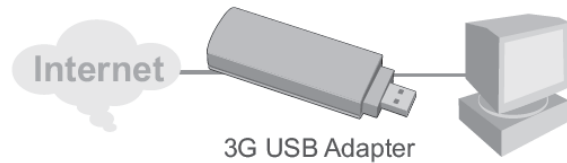
In addition to this User's Guide, you can find help below:

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

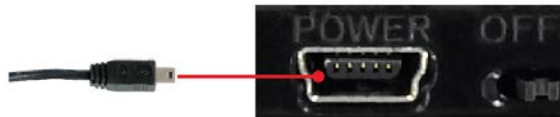
Router Installation

Hardware Installation

1. Verify that you have an Internet connection when connecting your computer directly to your 3G dongle.



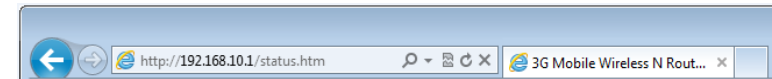
2. Connect the Mini-USB end of the power adapter to the TEW-716BRG and connect the power adapter to a power outlet.



3. Connect your 3G dongle to the USB port of the TEW-716BRG.



4. Move the power switch of the TEW-716BRG to the **On** position and verify that the LEDs are turned on.
5. Connect your computer wirelessly to the TEW-716BRG. The default SSID (Wireless Network Name) of the TEW-716BRG is **TRENDnet716**.
6. Open a web browser and type <http://192.168.10.1> in the address bar and then press Enter.



7. Enter the System Password and click **Login**. By default the System Password is **admin**.

System Password : (default: admin)

8. Select **Wizard** and click **Enter**.



6. You will be prompted to change the login password of your router. Complete the fields and click **Next**.



7. Select the time zone you would like to set on your router and click **Next**.



8. Verify the LAN IP address you would like to apply to the router and select the WAN type you will be using. Click **Next** to continue.



9. Select Automatic to have the router automatically detect your 3G WAN settings. Click **Next** to continue.



10. Enter the Network ID (SSID) you would like to assign to the router.

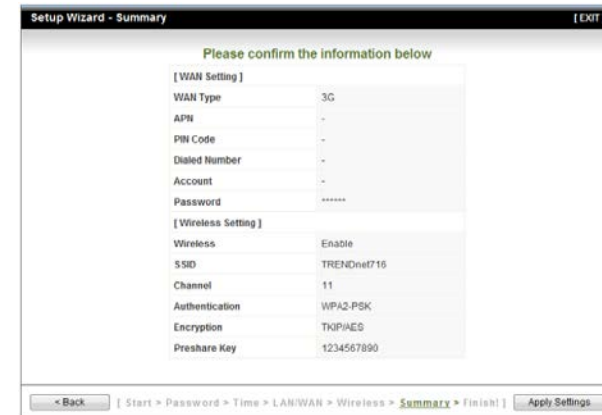


11. Select the wireless security settings you would like to apply to the router.



11. Verify your settings and click **Apply Settings**.

Note: Once the router reboots you will need to connect to the updated settings you have applied during the wizard (Network ID, Wireless Security, LAN IP).



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*
Encryption Strength	Low	Medium	High
Additional Options	Open System or Shared Key, HEX or ASCII, Different key sizes	TKIP or AES, Preshared Key or RADIUS	TKIP or AES, Preshared Key or RADIUS
Recommended Configuration	Open System ASCII 13 characters	TKIP Preshared Key 8-63 characters	AES Preshared Key 8-63 characters

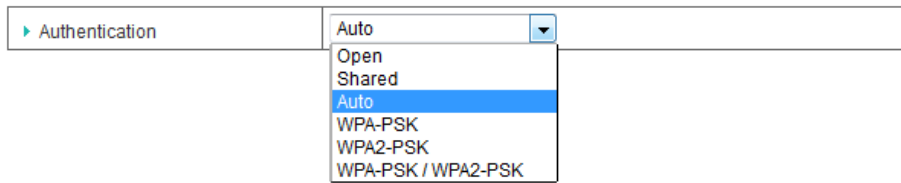
*Dependent on the maximum 802.11n data rate supported by the device (150Mbps, 300Mbps, or 450Mbps)

Secure your wireless network

Basic Setting > Wireless

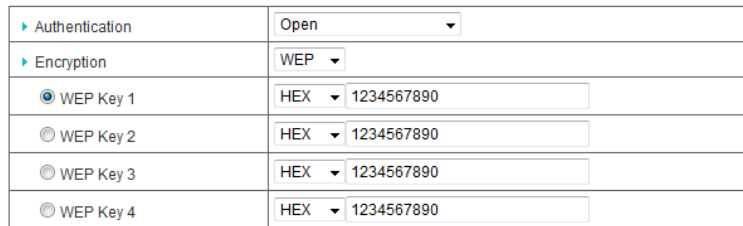
After you have determined which security type to use for your wireless network (see [“How to choose the security type for your wireless network”](#) on page 9), you can set up wireless security.

1. Log into your router management page (see [“Access your router management page”](#) on page 18).
2. Click on **Wireless**, and click on **Security**.
3. Click on the **Authentication** drop-down list to select your wireless security type.



Selecting WEP (Open/Shared):

If selecting **Open**, **Shared** or **Auto** Authentication you will be using WEP (Wired Equivalent Privacy) Encryption type. Please review the settings to configure and click **Save** to apply the changes.



- **Authentication:** Choose **Open**, **Shared** or **Auto**.
Note: It is recommended to use Open System because it is known to be more secure than Shared Key.
- **Encryption:** Select **WEP**
- **Mode** – Choose **HEX** or **ASCII**.

Note: It is recommended to use ASCII because of the much larger character set that can be used to create the key.

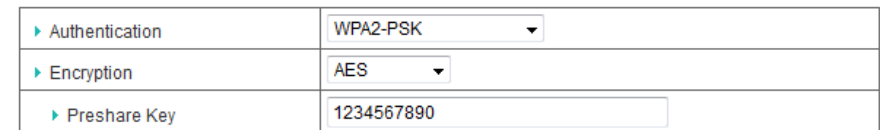
- **WEP Key** – Choose the key length **64-bit** or **128-bit**.

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

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

- **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)

Selecting WPA, WPA-Auto, or WPA2 (WPA2 recommended):



First, from the Authentication Type row, select **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK.WPA2-PSK**.

- The following section outlines options when selecting PSK (Preshared Key Protocol),**
- Select a Cipher Type. When selecting **WPA** security, it is recommended to use **TKIP**.
 - When selecting **WPA-Auto** security, it is recommended to use **AES**.
 - When selecting **WPA2** security, it is recommended to use **AES**.

Create your Wireless security Passphrase (password or key):

- **Passphrase** – Enter the passphrase. This is the password or key that is used to connect your computer to this router wirelessly
- **Confirmed Passphrase** – Re-enter the passphrase.
*Note: 8-63 alphanumeric characters (a,b,C,?, *, /,1,2, etc.)*

Connect wireless devices to your router

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

- Smart Phones
- Wireless Laptop computers

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.

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 4)

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

PBC (Software/Virtual Push Button)*Basic Settings > Wireless > WPS 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 18).
2. Click on **Basic Settings, Wireless**, and click on **WPS Setup** in the bottom.
3. To add a wireless device to your network, simply the 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 next to **Config Method**, select **Push Button**, click **Trigger** to start WPS authentication.

Wi-Fi Protected Setup	
Item	Setting
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ AP PIN	00762946 <input type="button" value="Generate New PIN"/>
▶ Config Mode	Registrar ▾
▶ Config Status	CONFIGURED <input type="button" value="Release"/>
▶ Config Method	Push Button ▾
▶ WPS status	NOUSED
<input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Cancel"/>	

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 18).
2. Click on **Basic Settings, Wireless**, and click on **WPS Setup** in the bottom.

3. Next to **Config Method** select **PIN Code**, enter the WPS PIN of the wireless device you are connecting and click **Trigger**.

Wi-Fi Protected Setup	
Item	Setting
▶ WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
▶ AP PIN	00762946 <input type="button" value="Generate New PIN"/>
▶ Config Mode	Registrar ▾
▶ Config Status	CONFIGURED <input type="button" value="Release"/>
▶ Config Method	PIN Code ▾ <input type="text"/>
▶ WPS status	NOUSED
<input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Cancel"/>	

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.

Basic wireless settings*Basic Setting > Wireless*

This section outlines available management options under the Basic Wireless sub tab.

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Basic Settings** and click on **Wireless**.
3. To save changes to this section, click **Apply** when finished.

Wireless Setting [Help]	
Item	Setting
Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID(SSID)	TRENDnet716
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
Wireless Mode	B/G/N mixed
Authentication	Auto
Encryption	None
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WPS Setup..."/> <input type="button" value="Wireless Client List..."/>	

• Wireless Module

- **Enabled** turns on the wireless networking on your router (by default it is enabled).
- **Disabled** turns off wireless networking on your router.

Note: It is recommended to leave the wireless setting to **Enabled** unless you do not plan on connecting any wireless computers or devices to your network.

- **Network (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 broadcast TRENDnet716 as the wireless network name. If you choose to change the SSID, change it to a name that you can easily remember.

• SSID Broadcast

- **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.

- **Channel:** Select **Auto** to have the router automatically pick the clearest channel available. Or you can manually set the channel on which the router will broadcast, uncheck **Auto**, 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.

- **Wireless Mode:** Select the appropriate mode for your network.

- **2.4GHz 802.11b/g/n mixed mode** – Select this mode for the best compatibility. This mode allows older 802.11b and 802.11g wireless devices to connect to the router in addition to newer 802.11n devices.
- **2.4GHz 802.11b/g mixed mode** – This mode only allows devices to connect to the router using older and slow 802.11b or 802.11g technology and it thereby reduces the router's maximum speed to 54Mbps (typically not recommended).
- **2.4GHz 802.11n only mode** – This mode only allows newer 802.11n devices to connect to your router. This mode does ensure the highest speed and security for your network, however if you have older 802.11g wireless clients, they will no longer be able to connect to this router.

- **Encryption:** Select the wireless security you would like to apply to your router. Please refer to [Secure Your Wireless Network](#) section on page 10.

Note: Please check the specifications on your wireless devices for the highest wireless capability supported first before applying these settings. If you are unsure, it is recommended that you keep the default setting (2.4GHz 802.11b/g/n mixed mode) for the best compatibility.

Steps to improve wireless connectivity

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

1. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
 - a. For the widest coverage area, install your router near the center of your home, and near the ceiling, if possible.
 - b. Avoid placing the router on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), and masonry walls.
 - c. Any obstruction can weaken the wireless signal (even non-metallic objects), so the fewer obstructions between the router and the wireless device, the better.
 - d. Place the router in a location away from other electronics, motors, and fluorescent lighting.
 - e. Many environmental variables can affect the router's performance, so if your wireless signal is weak, place the router in several locations and test the signal strength to determine the ideal position.
2. Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.
3. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.
4. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.

If possible, upgrade wireless network interfaces (such as wireless cards in computers) from older wireless standards to 802.11n. 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.

Access Control Filters

Access control basics

MAC address filters

Security Setting > MAC Control

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 wired or wireless network.

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Access**, click on **Filter**, and click on **MAC Filters**.
3. Click Enable to enable MAC Address Control rule.
4. Select the type of restrictions you would like to apply to the MAC control rule.
 - **Connection control:** Check "Connection control" to enable the controlling of which wired and wireless clients can connect with this device. If a client is denied to connect with this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect with this device.
 - **Association control:** Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN.
4. Review the MAC Filter options and click **Save** to apply settings.
 - **MAC Address** – Enter the 12-digit MAC address.(e.g. *00-11-22-AA-BB-CC*)
 - **C or A:** Select which rule you would like to apply on the applied MAC address.

MAC Address Control [Help]			
Item	Setting		
▶ MAC Address Control	<input checked="" type="checkbox"/> Enable		
<input type="checkbox"/> Connection control	Wireless and wired clients with C checked can connect to this device; and allow ▾ unspecified MAC addresses to connect.		
<input type="checkbox"/> Association control	Wireless clients with A checked can associate to the wireless LAN; and allow ▾ unspecified MAC addresses to associate.		
DHCP clients -- select one -- <input type="button" value="Copy to"/> ID -- ▾			
ID	MAC Address	C	A
1	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Save"/> <input type="button" value="Undo"/>			

Domain Filters

Security Setting > Domain Filters

You may want to allow or block computers or devices on your network access to specific websites (e.g. www.trendnet.com, etc.), also called domains or URLs (Uniform Resource Locators). You may also enter a keyword (e.g. instead of complete URL to generally allow or block computers or devices access to websites that may contain the keyword in the URL or on the web page.

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Access**, click on **Filter**, and click on **Domain/URL Blocking**.
3. Review the Domain/URL blocking options and click **Save** to apply settings.

Domain Filter [Help]			
Item	Setting		
▶ Domain Filter	<input type="checkbox"/> Enable		
▶ Log DNS Query	<input type="checkbox"/> Enable		
▶ Privilege IP Addresses Range	From <input type="text"/>	To <input type="text"/>	
ID	Domain Suffix	Action	Enable
1	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
10	* (all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-
<input type="button" value="Save"/> <input type="button" value="Undo"/>			

- **Domain Filter:** Check if you want to enable Domain Filter.
- **Log DNS Query:** Check if you want to log the action when someone accesses the specific URLs.
- **Privilege IP Address Range:** Setting a group of hosts and privilege these hosts to access network without restriction.
- **Domain Suffix:** A suffix of URL can be restricted, for example, ".com", "xxx.com".
- **Action:** Select the action you would like to apply when someone is accessing the URL met the domain-suffix.
 - **Drop:** Select this action to block access
 - **Log:** Select this action to allow access but to log the access.

URL Filters

Security Setting > URL Filter

URL Blocking will block LAN computers to connect with pre-define Websites. The major difference between "Domain filter" and "URL Blocking" is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a **keyword**.

access to websites that may contain the keyword in the URL or on the web page.

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Access**, click on **Filter**, and click on **Domain/URL Blocking**.
3. Review the URL blocking options and click **Save** to apply settings.

URL Blocking [Help]		
Item	Setting	
▶ URL Blocking	<input type="checkbox"/> Enable	
ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

- **Enable:** Check to enable the feature.
- **URL:** If any part of the Website's URL matches the pre-defined word, the connection will be blocked.
For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".
- **Enable:** Check to enable the selected URL.

Packet Outbound/Inbound Filters

Security Setting > Packet Filters

You may want specify inbound or outbound access control to allow/deny sources (or Internet IP addresses) to your network from the Internet or from computers or devices on your network to the Internet. Firewall rules may allow for more granular control of specific inbound and outbound access between your network and the Internet. It is

recommended that these settings remain set to default unless you are knowledgeable about the effects of changing the firewall rule configuration. It is possible to have undesirable functionality from your router if these settings are improperly modified.

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Configuration** at the top of the page, click on **Security Setting**, and click on **Packet Filters**.

Outbound Packet Filter

You may want apply outbound packet filters to allow or deny access of specific traffic from computers or devices on your local network to the Internet.

To configure outbound packet filters:

Next to **Outbound Packet Filter**, check the **Enable** option to enable outbound filtering.

▶ Outbound Packet Filter	<input type="checkbox"/> Enable
--------------------------	---------------------------------

- Select **Allow all to pass except those match the following rules** to allow all traffic and deny only the filters specified in the list.
- Select **Deny all to pass except those match the following rules** to deny all traffic and allow only the filter specified in the list.

<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.
--

Review the outbound packet filter settings.

ID	Source IP	Destination IP : Ports	Protocol	Enable	Use rule#
1	<input type="text"/>	0.0.0.0 : <input type="text"/>	Both ▼	<input type="checkbox"/>	(0) Always ▼

- **Source IP** – Enter the source IP address or computer/device IP address on your local network to apply the filter. (e.g. 192.168.10.101)

- **Destination IP : Ports** – Enter the destination IP address of the computer/device located on the Internet and port number to apply the filter. To specify all port numbers, do not specify any value for **Ports** field. For specific port numbers, enter a port number or range within the range of 1-65535 (e.g. 21 or 21-30) in the **Ports** field.

Note: Typically, you can specify 0.0.0.0 for any destination IP address located on the Internet or enter the specific IP address. (e.g. 10.10.10.200)

- **Protocol** – Select the protocol type to filter. **TCP, UDP**, or you can select **Both** to choose both protocol types.
- **Enable** – Check the option to enable the filter.
- **Use rule#** - Click the drop-down list to select a pre-defined schedule. The filter will only be active during the time period defined in the pre-defined schedule.

Note: Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 51 to configure Time Settings and see page 65 to create a schedule.

To save changes, click **Save** at the bottom of the page.

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

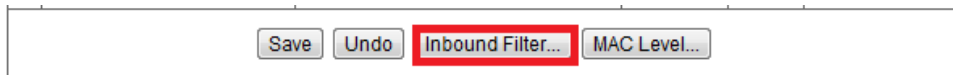
Clicking **MAC Level** will bring you to the **MAC Control** configuration page. See **MAC Control** section.

Inbound Packet Filter

You may want apply inbound packet filters to allow or deny access of specific traffic from the Internet to computers or devices on your local network.

To configure inbound packet filters:

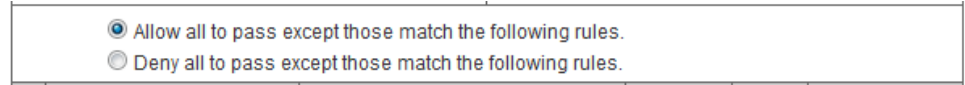
Click **Inbound Filter** at the bottom of the outbound packet filter page.



Next to **Inbound Packet Filter**, check the **Enable** option to enable inbound filtering.



- Select **Allow all to pass except those match the following rules** to allow all traffic and deny only the filters specified in the list.
- Select **Deny all to pass except those match the following rules** to deny all traffic and allow only the filter specified in the list.



Review the inbound packet filter settings.

ID	Source IP	Destination IP : Ports	Protocol	Enable	Use rule#
1	<input type="text"/>	0.0.0.0 : <input type="text"/>	Both ▾	<input type="checkbox"/>	(0) Always ▾

- **Source IP** – Enter the source IP address or computer/device IP address on your located on the Internet to apply the filter. (e.g. 192.168.10.101)
Note: Typically, you can specify 0.0.0.0 for any source IP address located on the Internet or enter the specific IP address. (e.g. 10.10.10.200)
- **Destination IP : Ports** – Enter the destination IP address of the computer/device located on your local network and port number to apply the filter. To specify all port numbers, do not specify any value for **Ports** field. For specific port numbers, enter a port number or range within the range of 1-65535 (e.g. 21 or 21-30) in the **Ports** field.
- **Protocol** – Select the protocol type to filter. **TCP, UDP**, or you can select **Both** to choose both protocol types.
- **Enable** – Check the option to enable the filter.
- **Use rule#** - Click the drop-down list to select a pre-defined schedule. The filter will only be active during the time period defined in the pre-defined schedule.
Note: Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. See page 51 to configure Time Settings and see page 65 to create a schedule.

To save changes, click **Save** at the bottom of the page.

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

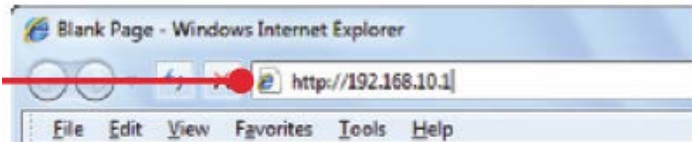
Clicking **MAC Level** will bring you to the **MAC Control** configuration page. See **MAC Control** section.

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. Next to Language, click the drop-down list to select your preferred language. Enter the default user name and password and then click **Login**.

Default Password: **admin**

System Password : (default: admin)

Change your router login password

Basic Setting > Change Password

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Basic Setting**, and click on **Change Password**.
4. To save changes, click **Apply**.

Change Password	
Item	Setting
▶ Old Password	<input type="text"/>
▶ New Password	<input type="text"/>
▶ Reconfirm	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

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".

Set your router date and time

Advanced Setting > System Time

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
 2. Click on **Advanced Setting**, and click on **System Time**.
 3. Review the system time settings and click **Save** to apply settings.
- Next to **Time Zone**, click the drop-down list to select your **Time Zone**.

System Time [Help]	
Item	Setting
▶ Time Zone	(GMT-08:00) Pacific Time (US & Canada)
▶ Auto-Synchronization	<input checked="" type="checkbox"/> Enable Time Server (RFC-868): Auto
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Sync with Time Server"/> <input type="button" value="Sync with my PC (Friday February 12, 2010 11:35:34)"/>	

- **Time Zone:** Select a time zone where this device locates.
- **Auto-Synchronization:** Check the "Enable" checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time.
- **Sync with Time Server:** Click on the button if you want to set Date and Time by NTP Protocol manually.
- **Sync with my PC:** Click on the button if you want to set Date and Time using PC's Date and Time manually.

Manually configure your Internet connection

Basic Setting > Network Setup

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Basic Setting**, and click on **Network Setup**.
3. In the **WAN Type** drop-down list, click the type of Internet connection provided by your Internet Service Provider (ISP).
4. Select **Manual** in the **Dial-Up Profile** section.
5. Complete the optional settings only if required by your ISP.
6. To save changes, click **Apply**.

Internet Setup [Help]	
▶ WAN Type	3G
▶ Dial-Up Profile	<input type="radio"/> Auto-Detection <input checked="" type="radio"/> Manual
▶ Country	Albania
▶ Telecom	Vodafone
▶ 3G Network	WCDMA/HSPA
▶ APN	<input type="text"/> (optional)
▶ PIN Code	<input type="text"/> (optional)
▶ Dialed Number	<input type="text"/>
▶ Account	test (optional)
▶ Password	<input type="password"/> (optional)
▶ Authentication	<input checked="" type="radio"/> Auto <input type="radio"/> PAP <input type="radio"/> CHAP
▶ Primary DNS	168.95.1.1 (optional)
▶ Secondary DNS	168.95.192.1 (optional)
▶ Connection Control	Connect-on-Demand ▶ Maximum Idle Time <input type="text"/> 300 seconds
▶ Keep Alive	<input checked="" type="radio"/> Disable <input type="radio"/> LCP Echo Request ▶ Interval <input type="text"/> seconds ▶ Max. Failure Time <input type="text"/> times <input type="radio"/> Ping Remote Host ▶ Host IP <input type="text"/> ▶ Interval <input type="text"/> seconds
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Reboot"/>	

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.

Change your router IP address

Basic Setting > Network Setup

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 18).
2. Click on **Basic Setting** and click on **Network Setup**.
3. Enter the router IP address settings and click **Save** to apply the settings.

LAN Setup	
Item	Setting
▶ LAN IP Address	192.168.123.254
▶ Subnet Mask	255.255.255.0

- **IP Address** – Enter the new router IP address.
(e.g. 192.168.200.1)
- **Subnet Mask** – Enter the new router subnet mask.
(e.g. 255.255.255.0)

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

Basic Setting > DHCP Server

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 18).
2. Click on **Basic Setting** and click on **DHCP Server**.
3. Review the DHCP Server settings.

DHCP Server [Help]	
Item	Setting
▶ DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ IP Pool Starting Address	101
▶ IP Pool Ending Address	200
▶ Lease Time	86400 Seconds
▶ Domain Name	

Save Undo More>> Clients List... Fixed Mapping...

- **DHCP Server** – Enable or Disable the DHCP server.
- **IP Pool Starting address:** Changes the starting address for the DHCP server range. (e.g. 192.168.10.20)
- **IP Pool Ending Address:** 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.
- **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.

- **Domain Name (Optional)** – Specifies a domain name to assign to computers or devices. (e.g. *trendnet.com*)

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

Dynamic DHCP 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.

DHCP Clients List					
IP Address	Host Name	MAC Address	Type	Lease Time	Select
<input type="button" value="Delete"/> <input type="button" value="Back"/> <input type="button" value="Refresh"/> <input type="button" value="Fixed Mapping"/>					

Set up DHCP reservation

Basic Setting > DHCP Server > Fixed Mapping

DHCP (Dynamic Host Configuration Protocol) reservation (also called Static DHCP) allows your router to assign a fixed IP address from the DHCP server IP address range to a specific device on your network. Assigning a fixed IP address can allow you to easily keep track of the IP addresses used on your network by your computers or devices for future reference or configuration such as virtual server (also called port forwarding, see "[Virtual Server](#)" on page 24) or special applications (also called port triggering, see "[Special Applications](#)" on page 25).

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Basic Setting**, click on **DHCP Server** and click on **Fixed Mapping**.
3. Review the DHCP reservation settings.

Fixed Mapping [Help]			
DHCP clients -- select one -- <input type="button" value="Copy to"/> ID -- --			
ID	MAC Address	IP Address	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

- **MAC Address:** Enter the MAC (Media Access Control) address of the computer or network device to assign to the reservation. (e.g. *00:11:22:AA:BB:CC*)
- **IP Address:** Enter the IP address to assign to the reservation. (e.g. *192.168.10.101*)
 - Note:** You cannot assign IP addresses outside of the DHCP range. The IP address is required to be within the DHCP IP address range (Start IP & End IP).
- **Enable:** Enable or Disable the DHCP reservation feature.

Enable/disable UPnP on your router

Forwarding Rules > Miscellaneous

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 18).

- Click on **Forwarding Rules** and click on **Miscellaneous**.
- Next to **UPnP**, click **Enabled** or **Disabled** 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.

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

Miscellaneous Items [Help]		
Item	Setting	Enable
▶ UPnP setting		<input checked="" type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

Enable/disable DoS (Denial of Service) Prevention

Security Setting > Miscellaneous

To provide additional security, your router offers DoS (Denial of Service) attack prevention to protect your network against well-known DoS attacks. You may want to enable the DoS feature for additional network security.

- Log into your router management page (see "[Access your router management page](#)" on page 18).
- Click on **Security Setting**, and click on **Miscellaneous**.
- To enable DoS prevention, next to **DoS Attack Detection**, check the **Enable** option.

▶ DoS Attack Detection	<input type="checkbox"/>
------------------------	--------------------------

- To save changes, click **Save** at the bottom of the page.

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

Allow/deny ping requests to your router from the Internet

Security Setting > Miscellaneous

To provide additional security, you may want to disable your router from responding to ping or ICMP (Internet Control Message Protocol) requests from the Internet. A ping is network communication test to check if a device with IP address is alive or exists on the network. By disabling this feature, you can conceal your router's IP address and existence on the Internet by denying responses to ping requests from the Internet.

- Log into your router management page (see "[Access your router management page](#)" on page 18).
- Click on **Security Setting**, and click on **Miscellaneous**.
- To deny ping requests from the Internet, next to **Discard PING from WAN side**, check the **Enable** option.

▶ Discard PING from WAN side	<input type="checkbox"/>
------------------------------	--------------------------

- To save changes, click **Save** at the bottom of the page.

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

Identify your network on the Internet

Advanced Setting > Dynamic DNS

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*, *no-ip.com*, etc.)
2. Log into your router management page (see "[Access your router management page](#)" on page 18).
3. Click on **Advance Setting** and click on **Dynamic DNS**.
4. Next to DDNS, click **Enabled**.
5. In the **Server Address** drop-down list, select the provider you selected, and enter your information in the fields.

Dynamic DNS [Help]	
Item	Setting
▶ DDNS	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
▶ Provider	DynDNS.org(Dynamic) ▼
▶ Host Name	<input type="text"/>
▶ Username / E-mail	<input type="text"/>
▶ Password / Key	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

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

Allow remote access to your router management page

Security Setting > Miscellaneous

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

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Security Setting** and click on **Miscellaneous**.
3. Select **Enable** and click **Save** to apply the settings.
 - **Remote IP Range** – It is recommended to leave this setting as *, to allow remote access from anywhere on the Internet.
Note: You can enter a specific range of Internet IP addresses that are allowed to access your router management page, all others will be denied.
 - **Port**– It is recommended to leave this setting as 8080.
Note: If you have configured port 8080 for another configuration section such as virtual server or special application, please change the port to use. (Recommended port range 1024-65534)

▶ Remote Administrator Host : Port	<input type="text"/>	/	<input type="text"/>	:	<input type="text"/>	<input type="checkbox"/>
------------------------------------	----------------------	---	----------------------	---	----------------------	--------------------------

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

Forwarding Rules > Miscellaneous

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 24) 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 (or you can use the DHCP reservation feature to ensure the device has a fixed IP address) (see "[Set up DHCP reservation](#)" on page 21).
 - A. Signing up for a Dynamic DNS service (outlined in the DDNS section) 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 18).
3. Click on **Forwarding Rules** and click on **Miscellaneous**.
4. Next to **DMZ Enable**, click **Enabled**.

▶ IP Address of DMZ Host	<input type="text"/>	<input type="checkbox"/>
--------------------------	----------------------	--------------------------

5. Next to **DMZ Host IP**, 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

Forwarding Rules > 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 23) 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.

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 DynDNS section).

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Forwarding Rules**, and click on **Virtual Server**.
To simplify configuration, there is a list of commonly used pre-defined virtual server entries to modify, otherwise, you can choose to manually add a new virtual server.

Virtual Server		[Help]
Well known services	-- select one --	Copy to ID --

3. Review the virtual server settings, click **Save** button to apply settings.

Virtual Server					[Help]
Well known services		-- select one --	Copy to	ID	--
ID	Service Ports	Server IP	Enable	Use Rule#	
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always	▼
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always	▼
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always	▼
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always	▼
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always	▼
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always	▼
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always	▼
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always	▼
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always	▼
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always	▼
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always	▼

- **Service Port:** Enter the port number required by your device. Refer to the connecting device's documentation for reference to the network port(s) required.
- **Server IP:** Enter the IP address of the device to forward the port (e.g. *192.168.10.101*).
 - Note:** 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.
- **Enabled** – Selecting **Enabled** turns on the virtual server and selecting **Disabled** turns off the virtual server.

Example: To forward TCP port 80 to your IP camera

1. Setup DynDNS service (See DynDNS section).
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 or you can use the DHCP reservation feature (see "[Set up DHCP reservation](#)" on page 21).

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 18).
5. Click on **Forwarding Rules**, and click on **Virtual Server**.
6. Enter **80** under **Service Port**.
7. Next to **Server IP**, enter the IP address assigned to the camera. (e.g. 192.168.10.101) Next to **Name**, you can enter another name for the virtual server, otherwise, leave the default name.
8. Select Enable to apply settings
9. To save the changes, click **Save**.

Special Applications

[Forwarding Rules](#) > [Special AP](#)

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 21.

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 18).
2. Click on **Access**, and click on **Special AP**.
3. Review the special application settings.

Special Applications [Help]			
Popular applications -- select one -- <input type="button" value="Copy to"/> ID --			
ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

- **Trigger** – Port or port range requested by the device.

Note: Please refer to the device documentation to determine which ports and protocols are required.
- **Incoming** – Port(s) forwarded to the device.
 - **Port Range** – Enter the ports or port range to be forwarded to the device. (e.g. 2000-2038,2069,2081,2200-2210).

Note: Please refer to the device documentation to determine which ports and protocols are required.
- **Enabled** – Selecting **Enabled** turns on the special application and selecting **Disabled** turns it off.

Note: To simplify configuration, there is a list of commonly used pre-defined special application entries to modify, otherwise, you can choose to manually add a new special application.

Prioritize traffic using QoS (Quality of Service)

Advanced Setting > QoS

You may want to prioritize outbound traffic for specific computers or devices on your network to have higher priority.

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **QoS**.
3. Next to **QoS Control**, check the **Enable** option.

▶ QoS Control	<input checked="" type="checkbox"/> Enable
---------------	--

4. Next to **Bandwidth of Upstream**, enter the maximum upload speed in kbps you have available from your ISP (Internet Service Provider).

Note: You can check your ISP for the maximum available upload speed you have available or you can run an Internet speed tests available on the Internet to determine the estimated value.

▶ Bandwidth of Upstream	<input type="text"/> kbps (Kilobits per second)
-------------------------	---

5. Review the QoS rule settings below.

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High ▾	<input checked="" type="checkbox"/>	(0) Always ▾

- **Local IP : Ports** – The IP address and port of the local device on your network.

(Port range to use: 1-65535)

Note: Typically, for the local device, it is recommended to specify all ports. To specify all ports, do not enter a value in the Port field.

- **Remote IP : Ports** – The IP address and port of the remote device on destination on the Internet. (Port range to use: 1-65535)

Note: You will need to specify the ports to apply QoS.

- **QoS Priority** – Choose from three priority queues to apply, **High**, **Normal**, and **Low**.
- **Enable** – Check the option to enable the QoS rule.
- **Use Rule#** – Allows you to specify a pre-defined schedule when the QoS rule is activated.

Note: To define a schedule, see the "Create schedules" section.

To save changes, click **Save** at the bottom of the page.

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

Create schedules

Advanced Setting > Scheduling

For additional security control, your router allows you to create schedules to specify a time period when a feature on your router should be activated and deactivated. Before you use the scheduling feature on your router, ensure that your router system time is configured correctly. See page 51 to configure the system time.

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

- Wireless
- Virtual Server
- Packet Filters
- QoS

To create a schedule to define a time period when a feature should be activated:

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **Scheduling**.
3. Next to **Schedule**, check the **Enable** option.

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

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

5. Next to a schedule entry, click **New Add**.

Rule#	Rule Name	Action
1		<input type="button" value="New Add"/>

6. Next to **Name of Rule #**, enter a name for the schedule.

▶ Name of Rule 1	<input type="text"/>
------------------	----------------------

7. Next to one of the entries, click **Week Day** and choose the day you would like to apply the schedule. In the **Start Time (hh:mm)** field, enter the start time. (e.g. 05:00) and in the **End Time (hh:mm)** field, enter the end time. (e.g.15:00).

Time Range: 00:00 (12:00AM) - 23:59 (11:59PM)

Note: Under *Week Day*, you can choose every day to apply the schedule to every day of the week.

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one --	<input type="text"/>	<input type="text"/>

8. To save changes, click **Save** at the bottom of the page.

9. Apply the schedule to one of the applicable features (Wireless, Virtual Server, Packet Filters, or QoS) in the drop-down list option **Use Rule#**.

Note: The feature will be activated during the time period specified in the schedule and deactivated during the time period not specified.

Router Maintenance & Monitoring

Reset your router to factory defaults

Toolbox > Reset to Default

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 36.

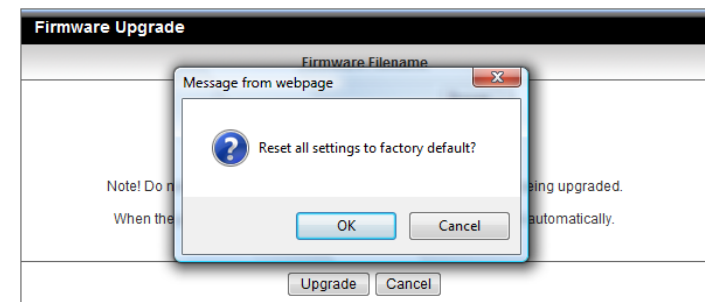
There are two methods that can be used to reset your router to factory defaults.

- **Reset Button** – Located on the rear panel of your router, see "[Product Hardware Features](#)" on page 4. Use this method if you are encountering difficulties with accessing your router management page.

OR

- **Router Management Page**

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Toolbox** and click on **Reset to Default**.



Router Default Settings

Administrator User Name	admin
Administrator Password	admin
Router IP Address	192.168.10.1
Router Subnet Mask	255.255.255.0
DHCP Server IP Range	192.168.10.101-192.168.199
Wireless	Enabled
SSID (wireless network name)	TRENDnet716
Wireless Security	None
Wireless Mode	B/G/N mixed
Channel	Auto

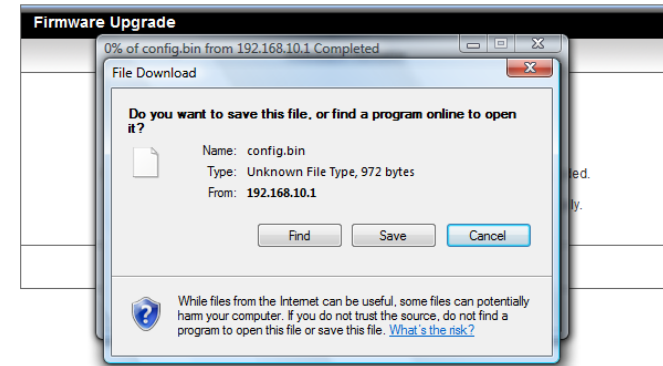
Backup and restore your router configuration settings

Toolbox > Backup Settings

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 18).
2. Click on **Toolbox** and click on **Backup Setting**.



Note: 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.bin)

To restore your router configuration:

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Toolbox** and click on **Firmware Upgrade**.
3. Click on **Browse** or **Choose File** and click **Upgrade** to restore settings.



Upgrade your router firmware

Toolbox > Firmware Upgrade

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 Status tab and then on the Device Information sub-tab. 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.

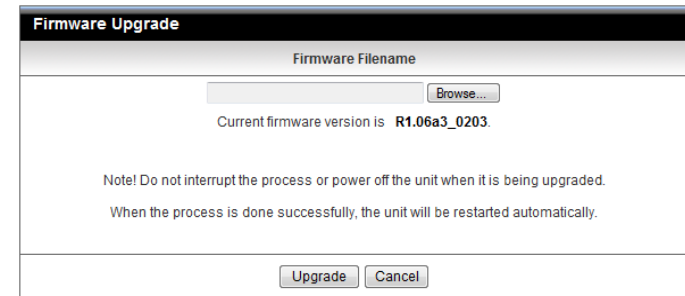
1. If a firmware upgrade is available, download the firmware to your computer.
2. Unzip the file to a folder on your computer.

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 18).
2. Click on **Toolbox** and click on **Firmware Upgrade**.

3. Click on **Browse** or **Choose File** and click **Upgrade** to restore settings.



Restart your router

Toolbox > Reboot

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

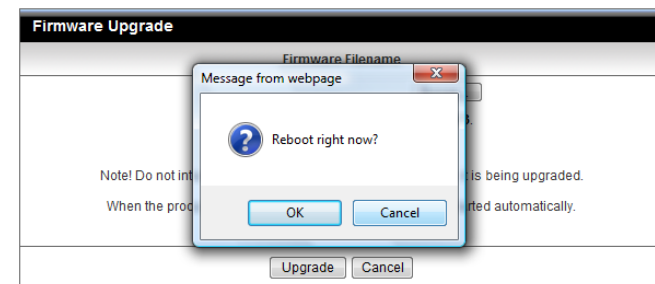
There are two methods that can be used to restart your router.

- **Turn the router off** for 10 seconds using the router On/Off switch located on the rear panel of your router, see "[Product Hardware Features](#)" on page 4.
Note: 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 18).
2. Click on **Toolbox** and click on **Reboot**.



Check connectivity using the router management page

Toolbox > Miscellaneous

For troubleshooting purposes, you may want to check your router connectivity using the ping (also known as a network connectivity test) test tool on your router management page.

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Toolbox** and click on **Miscellaneous**.
3. Enter in the IP address (e.g. *192.168.10.101*) or host name (e.g. *www.trendnet.com*) to test.
4. Click **Ping**.

Miscellaneous Items [Help]	
Item	Setting
▶ Domain Name or IP address for Ping Test	<input type="text"/> <input type="button" value="Ping"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Check the router system information

Status > Device Information

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 18).
2. Click on **Status** and click on **Device Information**.
3. Review the device information.

System Status

System Status [HELP]		
Item	Status	Sidenote
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0 , 0.0.0.0	
Connection Time	-	Connecting...

- **IP Address:** The current IP address assigned to your router 3G connection.
- **Subnet Mask:** The current subnet mask assigned to your router 3G connection.
- **Default Gateway:** The current gateway assigned to your router 3G connection.
- **DNS (Domain Name System)** – The current DNS address(es) assigned to your router port or interface configuration.
- **Connection Time:** The current connection time your router has been connected to your 3G network.

Wireless Modem Information

Wireless Modem Information		
Item	Status	Sidenote
Card Info	N/A	Supported Cards List
Link Status	Connecting...	
Signal Strength	N/A	
Network Name	N/A	

- **Card Info:** Displays your 3G adapter information.
- **Link Status:** Displays the status of your 3G connection.
- **Signal Strength:** Displays the signal strength of your 3G connection
- **Network Name:** Displays your 3G service provider.

Wireless Status

Wireless Status		
Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	TRENDnet716	
Channel	11	
Security	Auto	(None)

- **Wireless Mode:** Displays information of your wireless network.
- **SSID:** Displays the current wireless network name assigned to your router.
- **Channel:** Displays the current wireless channel your router is operating.
- **Security:** Displays the current wireless security configured on your router.

Statistics Information

Statistics Information		
Statistics of WAN	Inbound	Outbound
Octets	0	0
Unicast packets	0	0
Multicast packets	0	0

- **Octets:** Displays the amount of octets has passed through the router.
- **Unicast packets:** Displays the total amount of unicast packets that has gone through the router.
- **Multicast packets:** Displays the total amount of unicast packets that has gone through the router

View your router log

Status > 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 18).
2. Click on **Toolbox** and click on **System Info**.
3. Review the device log information.
 - **Time:** Displays the time of the log entry. If the time is inaccurate, make sure to set the router date and time correctly. (See "[Set your router date and time](#)" on page 18)
 - **Log:** Displays the log message.

System Log	
Time	Log
Dec 31 23:59:59	kernel: klogd started: BusyBox v1.3.2 (2010-10-28 11:58:12 CST)
Jan 1 00:00:00	commander: Ethernet port configuration: Configured as LAN
Jan 1 00:00:05	commander: Write AP PinCode into CSID_S_WLANAP_WPS_AP_PINCODE
Jan 1 00:00:08	udhcpd[1533]: udhcpd (v0.9.9-pre) started
Jan 1 00:00:08	udhcpd[1533]: Unable to open /var/run/udhcpd.leases for reading
Jan 1 00:00:09	init: Starting pid 1594, console /dev/ttyS1: '/bin/ash'
Jan 1 00:00:10	commander: STOP WANTYPE 3G
Jan 1 00:00:12	csman: img_len 290, sector_addr 3f0000, sector_size 2000
Jan 1 00:28:09	commander: CSID80190103 read err -61
Jan 1 00:30:16	commander: wps-action start
Jan 1 00:53:51	rlalert: fail to read pid file

Page: 1/1 (Log Number: 11)

Router Log Navigation

- **First Page:** Displays the first page of the log.
- **Last Page:** Displays the last page of the log.
- **Previous Page:** Display the log page previous to the current.
- **Next Page:** Displays the log page next to the current.
- **Clear Log:** Clears all logging
- **Refresh:** Refresh the log entries
- **Download:** Saves log entries to a file

View wireless devices connected to your router

Status > Client List

You may want to check the wireless devices connected to your router.

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Status** and click on **Client List**.

3. The table displays the amount time each wireless device has been connected and the MAC address of each wireless device.

Connected Time	MAC Address
01:06:31	7c:ed:8d:2e:9f:b3

View NAT activity of your router

Status > NAT Status

You may want to check the wireless devices connected to your router.

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Status** and click on **Client List**.
3. The table displays the TCP/UDP sessions of your router.

NAT Status					
ID	Protocol	Internal	NAT	External	Time-out
Page: 1/0 (Active Session Number: 0)					
<input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="First Page"/> <input type="button" value="Last Page"/> <input type="button" value="Refresh"/> <input type="button" value="Back"/>					

- **ID** – Displays the session number.
- **Protocol** – Displays the protocol used in the session established, TCP or UDP.
- **Internal** – Displays the internal IP address of the session and the local port number used in the session established.
- **NAT** – Displays the NAT IP used in the session established.
- **External** – Display the destination IP address and port of the session established.
- **Timeout** – Displays the TTL (Time to Live) of the session established.
- **Page: (Active Session Number:)** - Displays the current session page you are viewing and number of active sessions.

Configure your router log

Configuration > Advanced Setting > System Log

You may want send your router log to your e-mail address or to an external log server (also known as Syslog server) so you can check it periodically while away from home. You may also want to only see specific categories of logging.

Send router logs to an external log server

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **System Log**.
3. Next to **IP address for syslogd**, enter the IP address (e.g. 192.168.10.250) of the external log server to send router logging and check the **Enable** option.

Item	Setting	Enable
▶ IP address for syslogd	<input type="text"/>	<input checked="" type="checkbox"/>

3. Click **Save** to save the changes.

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

Clicking **View Log** will bring you to log page (Configuration > Toolbox > System Information). See the "View your router log" section.

Send router logs to your e-mail address

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **System Log**.
3. Review the e-mail log settings.

		Enable
▶ Setting of Email alert		<input checked="" type="checkbox"/>
• SMTP Server : port	<input type="text"/> : <input type="text"/>	
• SMTP Username	<input type="text"/>	
• SMTP Password	<input type="text"/>	
• E-mail addresses	<input type="text"/>	
• E-mail subject	<input type="text"/>	

- **SMTP Server : port** – Enter the IP address (e.g. 10.10.10.10) or domain name (e.g. mail.trendnet.com) of your e-mail server. Enter the port used by your e-mail service. (e.g. Default SMTP Server Port: 25)
- **SMTP Username** – Enter your account user name for your e-mail service.
- **SMTP Password** – Enter your password for your e-mail service.
- **E-mail addresses** – Enter the e-mail addresses to send the log file. (e.g. user1@trendnet.com, user2@trendnet.com)

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

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

5. Click **Email Log Now** to send an e-mail of the current router log using your email alert settings.

Clicking **View Log** will bring you to log page (Configuration > Toolbox > System Information). See the "View your router log" section.

Enable SNMP on your router

Advanced Setting > SNMP

SNMP (Simple Network Management Protocol) is a network management protocol used to monitor (read) and/or manage (write) multiple network devices on a network. This feature requires a preconfigured external SNMP server.

1. Log into your router management page (see "[Access your router management page](#)" on page 18).
2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **SNMP**.
3. Review the options for SNMP.

▶ Enable SNMP	<input type="checkbox"/> Local <input type="checkbox"/> Remote
▶ Get Community	<input type="text"/>
▶ Set Community	<input type="text"/>
▶ IP 1	<input type="text"/>
▶ IP 2	<input type="text"/>
▶ IP 3	<input type="text"/>
▶ IP 4	<input type="text"/>
▶ SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
▶ WAN Access IP Address	<input type="text"/>

- **Enable SNMP** – Check the **Local** option to allow SNMP access on the router wired LAN and wireless interfaces. Check the **Remote** option to allow SNMP access on the router WAN (Internet) interface.
- **Get Community** – Enter the community name to match the settings with the external SNMP server. This community will have SNMP read access only.
- **Set Community** – Enter the community name to match the settings with the external SNMP server. This community will have SNMP write access.
- **IP 1-4** – Enter up to four IP addresses of external SNMP servers. (e.g. 192.168.10.250)
- **SNMP Version** – Select the correct SNMP version to match the SNMP version of your external SNMP server(s), **V1** or **V2c**.
- **WAN Access IP Address** – You can specify a single IP address from the Internet to allow to connect your router using SNMP. (optional)

Note: When allowing Remote SNMP access, leaving this setting blank will allow access from any IP address from the Internet. It is recommended to specify an IP address if allowing Remote SNMP access.

4. To save changes, click **Save** at the bottom of the page.

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

Add static routes to your router

Advanced Setting > 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, 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 18).
2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **Routing**.
3. Next to **Static Routing**, check the **Enable** option to enable static routing.

▶ Static Routing	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
------------------	---

4. Review the static route settings.

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

- **Destination** – 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)
 - **Hop** – Enter the number of hops (routers) required to reach the destination network. The hop count range that can be specified is 0-99.
 - **Enable** – Check the option to enable the route and uncheck the option to disable the route.
5. To save changes, click **Save** at the bottom of the page.

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

Enable dynamic routing on your router

Advanced Setting > Routing

You may want set up your router to route computers or devices on your network to other local networks through other routers. If other routers support dynamic routing such as RIP (Routing Information Protocol), you can enable this feature on your router to automatically learn the required routes to reach those networks. It is required that the same dynamic routing protocol and version is also enabled on the other routers in order your router and the other routers to exchange information about the 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 18).
2. Click on **Configuration** at the top of the page, click on **Advanced Setting**, and click on **Routing**.
3. Select the appropriate dynamic routing protocol and version communicate with other routers.

▶ Dynamic Routing	<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2
-------------------	--

- **Disabled** – Disable sending and receiving or exchange of routing information dynamically between your router and other routers.
 - **RIPv1** - Enables sending and receiving or exchange of routing information dynamically between your router and other routers to build routes to your network and other networks using the RIP version 1 protocol.
 - **RIPv2** – Enables sending and receiving routing information dynamically between your router and other routers to build routes to your network and other networks using the RIP version 2 protocol.
4. To save changes, click **Save** at the bottom of the page.

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

Router Management Page Structure

Basic Setting

- Network Setup
 - LAN Setup
 - Internet Setup
- DHCP Server
- Wireless
 - Security
 - WPS
- Change Password

Forwarding Rules

- Virtual Server
- Special AP
- Miscellaneous
 - DMZ
 - UPnP

Security Setting

- Status
- Packet Filter
- Domain Filter
- URL Blocking
- MAC Control
- Miscellaneous
 - Administrator Time-Out
 - Remote Administrator
 - Discard WAN Ping

- DoS Attack Detection

Advanced Setting

- Status
- System Log
- Dynamic DNS
- QoS
- SNMP
- Routing
- System Time
- Scheduling

Toolbox

- System Info
- Firmware Upgrade
- Backup Setup
- Reset to Default
- Reboot
- Miscellaneous
 - Ping Test

Technical Specifications

Hardware	
Standards	IEEE 802.11b, IEEE 802.11g, Based on IEEE 802.11n technology USB: USB 2.0, USB 1.1
USB Port	1 x USB 2.0 port for 3G* USB adapter (Internet) 1 x USB 2.0 mini-Type B power port
WAN Connection Type	USB: 3G
Compatible Mobile Networks	UMTS/HSPA, WCDMA (HSDPA), CDMA2000 (EV-DO), and TD-SCDMA
Compatible USB Modems	List of compatible USB modems
Router/ Firewall	NAT, NAPT, and SPI Static / Dynamic Route (RIP v1/v2) UPnP, DMZ, Static/Dynamic Route support DoS protection, MAC/Packet/Domain and URL filtering (deny or allow).
Power Switch	On / off power switch
WPS / Reset Button	Wi-Fi Protected Setup (WPS) - Automated wireless connection push button (Hold for 3 seconds) Reset button - Factory Default (Hold for 20 seconds)
LED Indicator	Power / Wireless / WPS, USB (3G modem)
Power Adapter	Input: 100 ~240V AC, 50~60Hz 0.2A Output: 5V DC, 1.2A
Power Consumption	350mA (max.)
Dimension (L x W x H)	93 x 65 x 19.5 mm (3.66 x 2.56 x 0.77 in)
Weight	66 g (2.3 oz)

Temperature	Operation: 0°~ 40°C (32°F~ 104°F) Storage: -10°~ 70°C (14°F~158 °F)
Humidity	Max 95% (non-condensing)
Certifications	CE, FCC
Wireless	
Frequency	2.400 ~ 2.484GHz
Modulation	OFDM, DSSS, BPSK, QPSK, CCK
Data Rate	802.11b: up to 11 Mbps 802.11g: up to 54 Mbps 802.11n: up to 150 Mbps
Security	64/128-bit WEP, WPA/WPA2-PSK

*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 7.
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 5 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 3G dongle. How do I find out?

Answer:

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

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 to your 3G dongle (meaning plug your 3G dongle directly to your computer and verify that your single computer (without the help of the router) can access the Internet).
2. Power cycle your 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 14 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

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

Windows Vista

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

Windows XP/2000

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

MAC OS 10.4/10.5/10.6

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

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

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

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

f. Restart your computer.

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

How to find your MAC address?

In Windows 2000/XP/Vista/7,

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

In MAC OS 10.4,

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



In MAC OS 10.5/10.6,

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


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

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

Windows 7

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**.

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-716BRG – 3 Years Warranty

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

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

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

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

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

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

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

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

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

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

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

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

PWP05202009v2

2012/10/15



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