User's Guide

TRENDNET®

AC2200 WiFi Mesh Router
AC2200 WiFi Mesh Router System

TEW-830MDR / TEW-830MDR2K

Table of Contents

Product Overview

TEW-830MDR

TEW-830MDR2K

Package Contents

TEW-830MDR package includes:

- TEW-830MDR
- Quick Installation Guide
- Network cable 0.5m (1.6 ft.)
- Power adapter (12V DC, 1.5A)
- Wall mount screws

TEW-830MDR2K package includes:

- 2 x TEW-830MDR
- Quick Installation Guide
- 2 x Network cable 0.5m (1.6 ft.)
- 2 x Power adapter (12V DC, 1.5A)
- Wall mount screws

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 AC2200 WiFi Mesh Router System is designed to blanket your home or small office in seamless WiFi coverage. The AC2200 WiFi Mesh Router System provides ample coverage for up to a 4,000 square foot home. For larger homes, simply add additional AC2200 WiFi Mesh Routers to the system for expanded WiFi coverage.

The WiFi mesh router system uses an intuitive app-based installation process, making setup a breeze using our TRENDnet WiFi Mesh app. In minutes, you'll have your AC2200 WiFi Mesh Router System up and running providing whole home WiFi coverage.

Our WiFi mesh router system also supports cutting-edge content filtering powered by Router Limits™. Router Limits' innovative tools offer an enhanced user experience for device-level scheduling and filtering capabilities. By offering access to these advanced web content filtering and productivity tools, the mesh router system allows you to take control of the Internet, whether it be for your business or your home.

Mesh Made Simple

The WiFi mesh router system uses an intuitive app-based installation process, making setup a breeze using our TRENDnet WiFi Mesh app

Whole Home WiFi Coverage

The AC2200 WiFi Mesh Router System provides ample coverage for up to a 4,000 square foot home. For larger homes, simply add additional AC2200 WiFi Mesh Routers to the system for expanded WiFi coverage

Router Limits

Router Limits' innovative tools offers an enhanced user experience for device-level scheduling and filtering capabilities. Offering access to these advanced web content filtering and productivity tools allows you to take control of your Internet, whether it be for business or home

Airtime Fairness

This smart WiFi feature calculates and determines which clients have priority over others. Clients that are faster and closer to the Mesh Router will have the highest priority while clients that are slower and farther away will have lower priority, freeing up WiFi resources

Band Steering

With band steering technology, the mesh router system alleviates network congestion by automatically directing wireless devices from the 2.4GHz band to the 5GHz band

Targeted Beamforming

Beamforming increases real-time performance by directing stronger wireless signals to your specific location. Beamforming improves wireless range, reception, and throughput

Monitoring

The TRENDnet WiFi Mesh app allows you to monitor each WiFi mesh router and connection status of network devices

Parental Controls

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

Guest Network

Create an isolated WiFi network for guest internet access

IPv6
IPv6 network support

Gigabit Ports

1 x Gigabit WAN Port, 1 x Gigabit LAN Port

USB 3.0 Share Port

Share content across the network with the USB 3.0 share port on each mesh router

*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials, and other conditions. For maximum performance of up to 867Mbps, use with an 867Mbps 802.11ac wireless adapter. For maximum performance of up to 400Mbps, use with a 400Mbps 802.11n wireless adapter. Multi-User MIMO (MU-MIMO) requires the use of multiple MU-MIMO enabled wireless adapters.

Product Hardware Features

Rear View
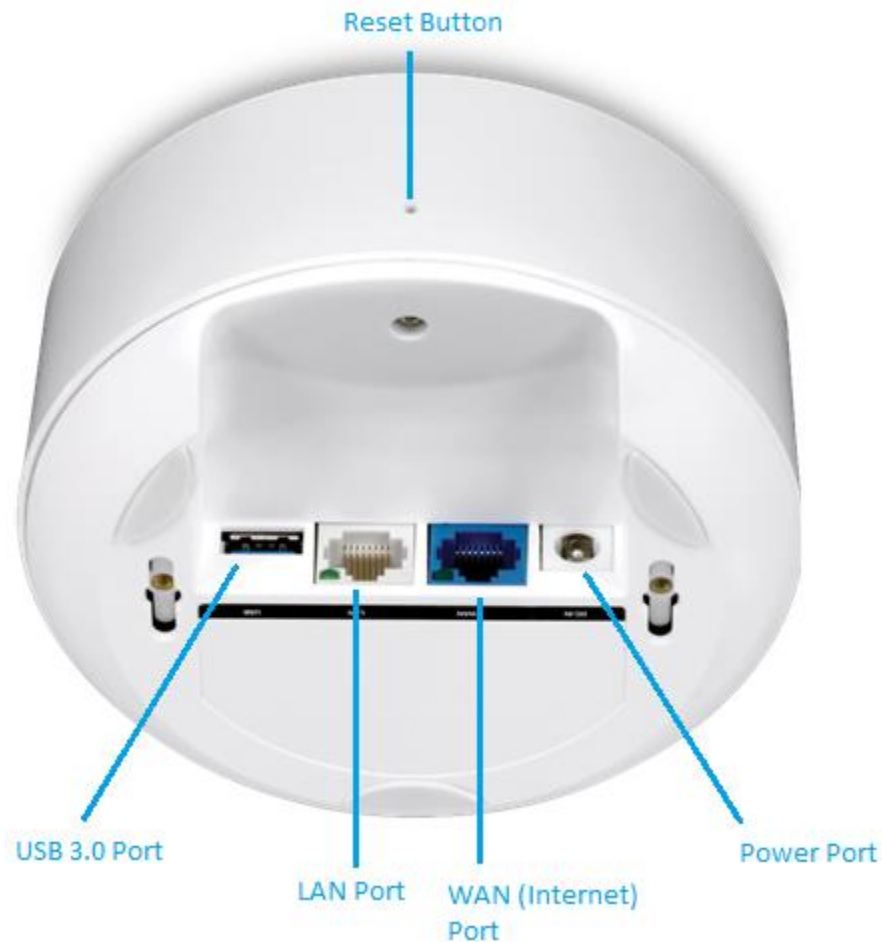
| Item	Description
USB 3.0 Port	Connect USB storage devices to share over the network via Windows® SMB/CIFS, Samba.
Gigabit LAN Port (White)	Connect an Ethernet cable (also called network cable) from your router LAN ports to your wired network device such as a computer.
Gigabit WAN/Internet Port (Blue)	Connect an Ethernet cable from your router Internet port to your modem.
On/Off Power Switch	Push the router On/Off power switch to turn your router "On" (Inner position) or "Off" (Outer position).
Power Port	Connect the included power adapter from your router power port and to an available power outlet.
Reset Button	Using a pen or paperclip, push and hold the reset button for 15 seconds and release to reset the router.

Front View

LED Indicator

LED Indicator	Description
Orange	**Blinking** – Device is ready for initial setup. **Blinking Rapidly** – Indicates WiFi connection was successful during initial setup. *Note: The LED will change from white to orange after device powers on when device is at factory default settings.*
White	**Blinking** – Device is applying configuration settings. **Solid** – Device is operating normally.
Blue	**Blinking** – Devices are pairing to WiFi mesh network. *Note: Additional device LED may blink between orange and blue during pairing process and red after pairing is completed*

Red	**Blinking** – Issue detected (Mesh device disconnect, lost Internet connection, etc.) **Blinking Rapidly** – Device is resetting to factory default. *Note: Using a paperclip, push and hold the reset button for 10 seconds or more and release to initiate a reset to factory defaults.*

Application Diagram
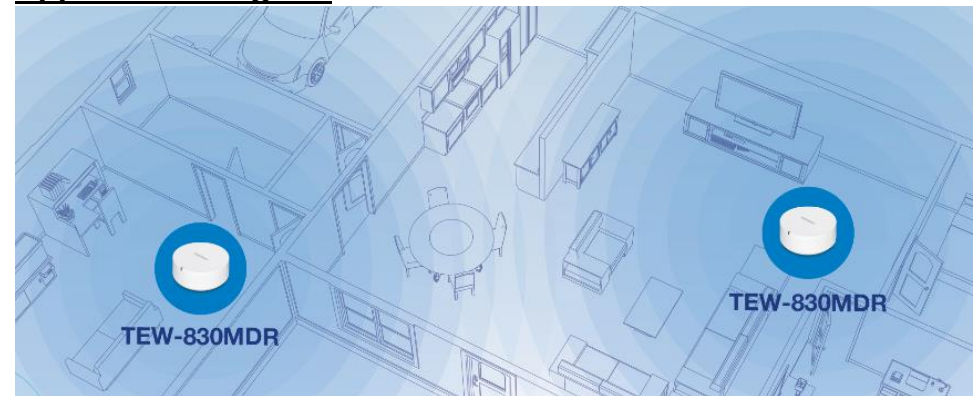
Mesh Made Simple
The WiFi mesh router system uses an intuitive app-based installation process, making setup a breeze using our TRENDnet WiFi Mesh app.

Router Limits
Router Limits' innovative tools offer an enhanced user experience for device-level scheduling and filtering capabilities. Offering access to these advanced web content filtering and productivity tools allows you to take control of your Internet, whether it be for business or home.

Airtime Fairness
This smart WiFi feature calculates and determines which clients have priority over others. Clients that are faster and closer to the mesh router will have the highest priority, while clients that are slower and farther away will have lower priority, freeing up valuable WiFi resources.

Initial Setup

<u>Creating a Home Network</u>

What is a network?

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

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

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

How to set up a home network

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

2. Make sure that your modem is working properly. Your modem is often provided by your Internet Service Provider (ISP) when you sign up for Internet service. If your modem is not working contact your ISP to verify functionality.

3. Set up your router. See "How to setup your router" below.

4. To connect additional wired computers or wired network devices to your network, see "Connect additional wired devices to your network" on page 9.

5. To set up wireless security on your router, see "Wireless Networking and Security" on page 18.

How to setup your router

Refer to the Quick Installation Guide or continue to the next section "Router Installation" on page 6 for more detailed installation instructions.

Where to find more help

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

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

Router Installation

Before you Install

Many Internet Service Providers (ISPs) allow your router to connect to the Internet without verifying the information fields listed below. Skip this section for now and if your router cannot connect to the Internet using the standard installation process, come back to this page and contact your ISP to verify required ISP specification fields listed below.

1. Obtain IP Address Automatically (Dynamic IP/DHCP)
Host Name:_____ (Optional, if required by ISP for Compatibilty)
Primary DNS Server Address: _____. _____._____._____ (Optional)
Secondary DNS Servers Address : _____. _____._____._____ (Optional)
MTU:_____ (Default: 1500, change if required by ISP)
MAC Address: ___:___:___:___:___:___ Clone your PC MAC Address (Optional)

2. Static IP/Fixed IP address
IP Address: _____. _____._____._____ (e.g. 215.24.24.129)
Subnet Mask: _____. _____._____._____
Default Gateway IP Address: _____. _____._____._____
Primary DNS Server Address: _____. _____._____._____
Secondary DNS Servers Address : _____. _____._____._____ (Optional)
MTU:_____ (Default: 1500, change if required by ISP)
MAC Address: ___:___:___:___:___:___ Clone your PC MAC Address (Optional)

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

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

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

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

Hardware Installation

1. Connect your modem to the mesh router Internet port (blue and connect the included power adapter.

Note: If you purchased a mesh network kit with multiple units, you can choose any of the units to set up first as the master. The router may take up to one minute to boot up. When the router LED changes form white to orange, this indicates that the router is ready for setup. For the initial setup, do no power on any other units except the single unit to be setup as master.
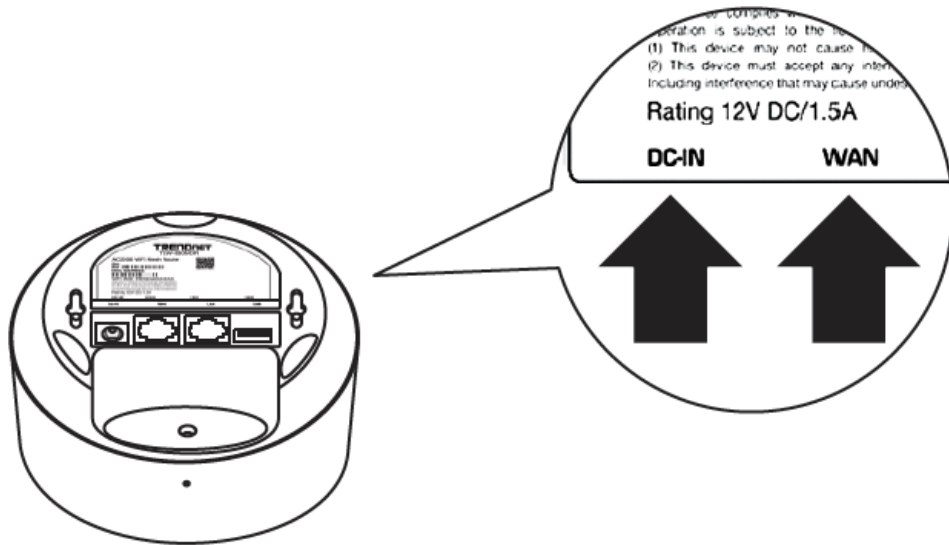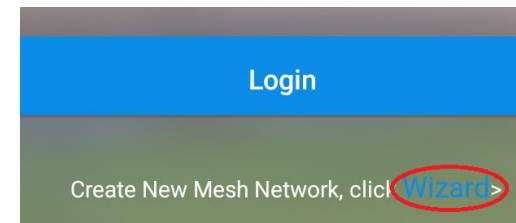

2. Using your mobile device, download and install the TRENDnet Mesh mobile app by scanning the appropriate QR code below for y our mobile device.

3. After the app installation is complete, open the **TRENDnet Mesh** app.

4. Click on the blue text link **Wizard** at the bottom of the screen to start the router setup wizard and follow the steps to complete the setup.

5. When reaching the final step, if setting up one router only, tap **Connect to TRENDnet Mesh now** at the bottom of the screen to connect to the router with the new settings and login. Otherwise, if you are connecting additional mesh units to your WiFi mesh network, tap **Add more devices** and follow the remaining steps to add the new mesh unit to your WiFi mesh network.

Note: The additional unit may take up to one minute to boot up. When the unit LED changes from white to orange, this indicates that the unit is ready for setup. Please make sure that the location of the additional unit is within at least 3m (9.84 ft.) range of the master router for initial setup.

6. When setup is completed, tap **Login** to access the router management configuration.


7. Your WiFi mesh network setup is complete.

Note: If you have more than one unit connected to your WiFi mesh network, you can tap the additional units listed under the Connection Status to determine if the unit is installed within optimal range of the master router. If the range is indicated as too far or too close, you can physically move additional units to determine an optimal range and location through the app.
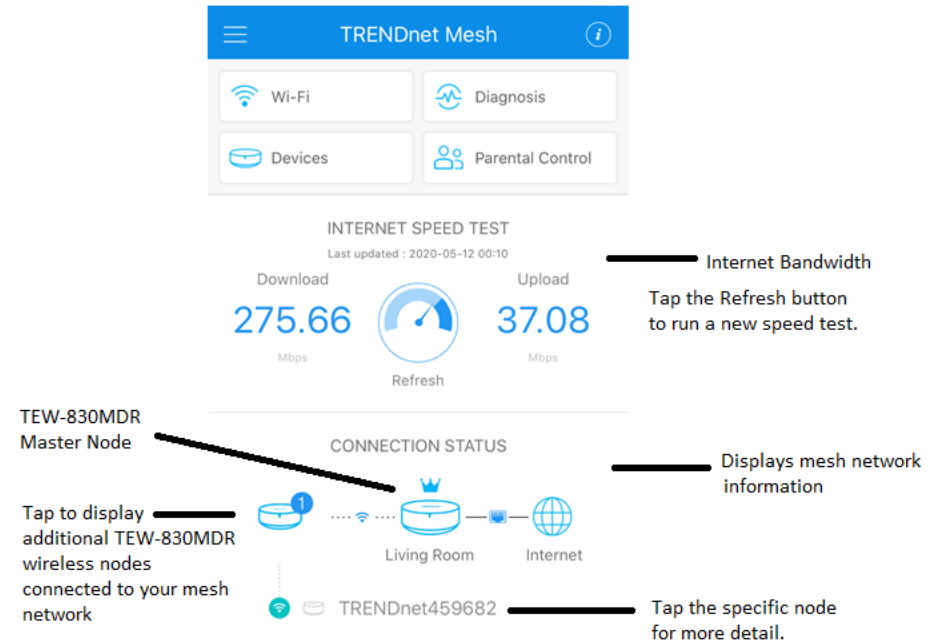
TRENDnet Mesh App Settings

At the login screen, enter the user name and password you created during initial setup and tap **Login**.
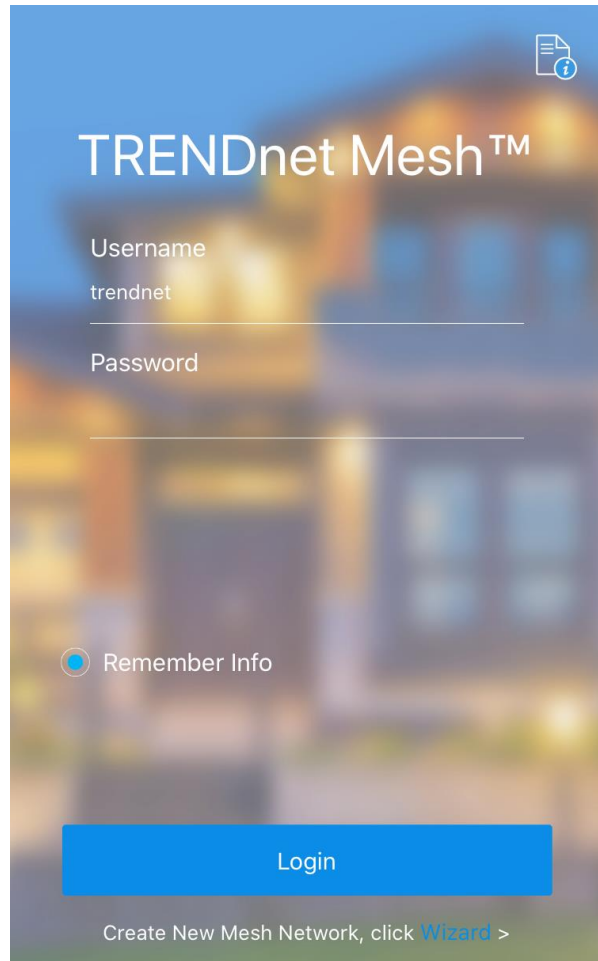
The main page displays the tested Internet bandwidth and any additional TEW-830MDR mesh nodes connected to your mesh network.

Devices

The crown at the top indicates that thsi is the master node

Tap the + symbol to add and setup an additional wireless node to your wireless mesh network.

Tap this icon to access additional functions of this wireless node.

You can manually change the name of the wireless node (ex: location of device)

Displays MAC address of wireless node

Displays IP address of wireless node

Displays the current number of wireless clients connected this wireless node.

For additional wireless, this will display the distance recommendation relative to the connectivity with the additional node and the mesh network.

Displays the current number of wireless clients connected to this wireless node as part of the wireless guest network.

Connection Info

Check the device's LED indicator or the app display to see your connection status.

Stable connection:
White LED / App Display:

Spotty connection:
Orange LED / App Display:

Disconnection:
Red LED / App Display:

Connection problem?

Be sure the devices are within 10 meters (30.28 ft) of each other

Devices / Node Advanced Settings

<	Advanced

TRENDnet459682

INTERNET SPEED TEST

Download: 172.50 Mbps

Upload: 37.78 Mbps

Tap Refresh to run an Internet speed test to the additional node.

Refresh

Last updated : 2020-05-12 23:36

LED Indicator: **Tap the LED indicator toggle to turn the LED indicator on the device.**

SAMBA: **Tap the SAMBA toggle to enable/disble file sharing on the device USB port.**

WPS: WPS   **Tap the WPS button to activate WPS on the device.**

Restart Device   **Tap the Restart Device button to reboot the device. This will only reboot the selected device, not all devices in mesh network.**

Factory Reset   **Tap the Factory Reset button to reset the device to factory defaults.**
Note: If you are under the Advanced settings of the Master node, this will reset all devices/nodes that are part of your mesh network.

WPS (WiFi Protected Setup)

WPS is a feature that allows you to easily connect wireless client devices to your wireless router or mesh network. If you wireless client devices support WPS, you can tap the WPS button on the app to activate the WPS pairing process on your TEW-830MDR, then push the WPS button on your wireless client device to connect. The pairing process may take up to 2 minutes to complete.

Samba

Samba is a network protocol that allows you to access shared files through your network. In order to share files, you will need to plug in a USB storage device on the USB port of the TEW-830MDR.

1. Plug in USB storage device into the USB port. Select the correct device in the app that you plugged the USB storage device and enable Samba.

2. Under Windows®, you can access the USB storage device on your computer under **Computer > Network > TRENDNETXXXXXX > sda1**.

Note: Each TEW-830MDR unit will be listed under Computer > Network section with the format TRENDNETXXXXXX (ex: TRENDNET459681, TRENDNET459682, etc.).

If your Windows® computer is not able to discover any network devices, you may not have network discovery and file sharing enabled, therefore, you may need to set the network to a private network and turn the feature on in Windows®
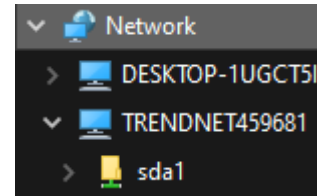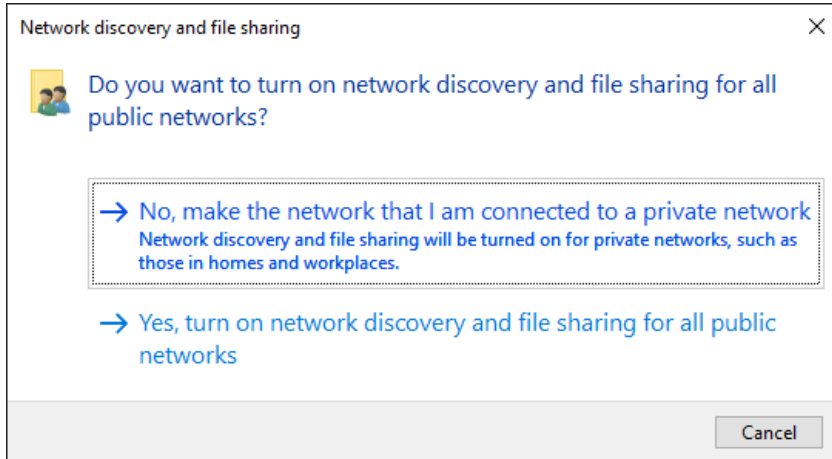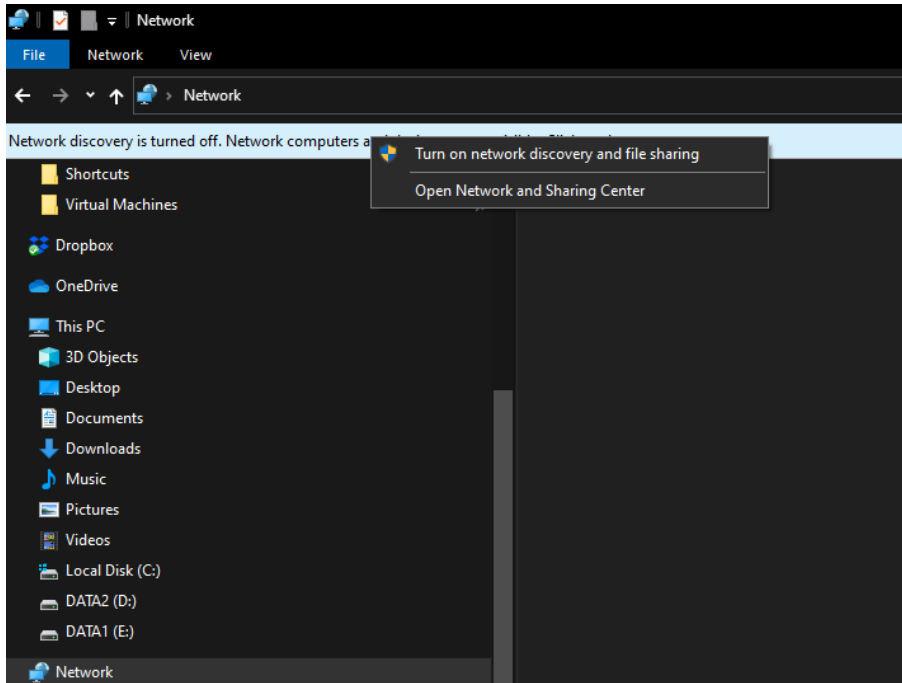
3. When prompted for a user name and password, enter the same user name and password you created during the initial app setup which is the same user name and password used to log into your router using the app.
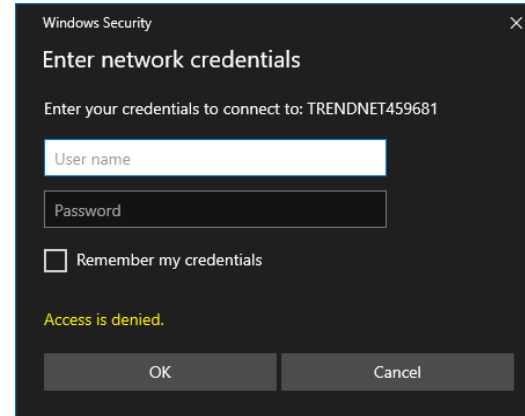
WiFi

Wi-Fi

Primary Wi-Fi

Wi-Fi Name(SSID):

You can manually change the WiFi Network Name/SSID of you wireless network.

TRENDnet6DA0FC

Wi-Fi Password:

You can manually change the WiFi Password/Key.

Encryption Type   WPA2/AES ›

Tap the Encryption Type setting to change the encryption type. WPA2/AES is recommeneded.

Advanced Settings   ›

Tap the Advanced Settings if you would like to set specific channel assignments for each band, channel width, and mesh backhaul mode.

Guest Wi-Fi

Guest Wi-Fi Name(SSID):

TRENDnet_GuestNetwork

Guest Wi-Fi Password:

Save   Tap Save to save the configuration changes.

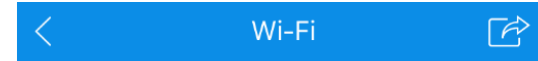**WiFi Guest Network**

Wi-Fi

TRENDnet6DA0FC

Wi-Fi Password:

Encryption Type   WPA2/AES ›

Advanced Settings   ›

Guest Wi-Fi

Tap the Guest Wi-Fi toggle to enable/disable the guest WiFi network.

Guest Wi-Fi Name(SSID):

Manually enter the WiFi Network Name/SSID of the guest WiFi network.

TRENDnet_GuestNetwork

Guest Wi-Fi Password:

Manually enter the WiFi Password/Key of the guest WiFi network. Note: WPA2/AES WiFi Password/Key must be 8-63 alphanumeric characters.

Encryption Type   WPA2/AES ›

Tap the Encryption Type setting to change the encryption type. WPA2/AES is recommended.

Save   Tap Save to save the configuration changes.

WiFi / Advanced Settings

Advanced

2.4 GHz

Channel   Auto

Bandwidth   20 MHz

5 GHz-1

Channel   Auto

Bandwidth   80 MHz

5 GHz-2

Channel   Auto

Bandwidth   80 MHz

Mesh Backhaul Mode   Dedicated

Save

Tap the Channel setting to set a specific channel to use for each band.

Tap the Bandwidth setting to set a specific bandwidth setting to use for each band.
2.4GHz: 20MHz, 40MHz, Auto 20/40MHz
5GHz: 20MHz, 40MHz, 80MHz
Note: It is recommended to use the default bandwidth settings for each band.

Tap the Mesh Backhaul Mode setting to specifically assign the mode for the 5GHz-2 mesh connectivity.

-Dedicated: Sets the 5GHz-2 band to only be used for mesh connectivity between nodes (Recommended).

-Shared: Sets the 5GHz-2 band to be shared for wireless client connections and mesh connectivity between nodes.

Tap Save to save the configuration changes.

Note: Increasing the bandwidth setting may allow you to obtain WiFi throughput however, depending on the WiFi environment and interference, this may negatively affect your WiFi connection stability.

Parental Controls

Tap the edit icon to drag and drop client devices between different groups.

Parental Control

Individual Users

User1
XX:XX:XX:XX:XX:XX   Online

User2
XX:XX:XX:XX:XX:XX   Online

Guest Network

List of currently connected client devices.

Tap the "+" icon to create a group and client devices.
Note: This can simplify management as Parental control rules can be applied to a group of client devices instead of applying rules to each individual client device.

By default, a Guest Network group has already been created, you can move client devices from the Individual Users list to this group and apply parental control rules.

Rules List

Tap on Rules list to create new parental control rules for web filteirng and scheduling.

Tap to add a new Parental Control rule

Rules List

+ Add New Rule

Block User1   Save

Rule Name

Tap the Rule Name field and enter a name for the rule

Block User1

Tap Save to save configuration changes for the new rule.

Weekly Schedule

Disconnect Internet at a scheduled weekly time:

Tap the days that the schedule should be applied.

M   T   W   T   F   S   S

Tap the start time field to select the start time for the scheule.

from   12:15   to   12:30

Tap the Weekly Schedule function to apply the parental control rule based on the specified schedule. This function will block Internet access during the specified schedule.

Tap the end time field to select the end time for the schedule.

Web Filter

Set up keywords to block specific websites

○ Social Media

○ Search Engine

○ Video Media

○ Custom URL

Tap the Web Filter section to enable filtering and block based on the categories provided. Important Note: HTTPS/SSL websites are not supported.

Note: *If you are applying a scheduled rule, please ensure the device time settings are set correctly before applying the schedule rule.*

Tap Back to return to the main parental control page.

Rules List

+ Add New Rule

After the new rule is saved, the new rule will appear in the list.

Block User1

In the parental control list of client devices, tap the client device would like to apply the parental control rule. In this example, we'll select User1.

Parental Control   ✏ +

⊙ Individual Users   ∧

User1
XX:XX:XX:XX:XX:XX   Online

User2
XX:XX:XX:XX:XX:XX   Online

⊙ Guest Network   ∧

Rules List

User — Save

👥 User1 〉

QoS Setting

Set High Priority can get faster to access your network.

Normal ⌄

Set Rules

Select Rules from the List or add New Rule for the Group

Apply From Rule List — Tap to select a parental control rule to apply or create a new parental control rule.

Rules List — Save

Tap Save to save the configuration settings.

➕ Add New Rule

Tap the previously created example and make sure the check appears to ensure it has been selected.

✓ Block User1

User — Save

Tap Save to save the configuration changes.

👥 User1 〉

QoS Setting

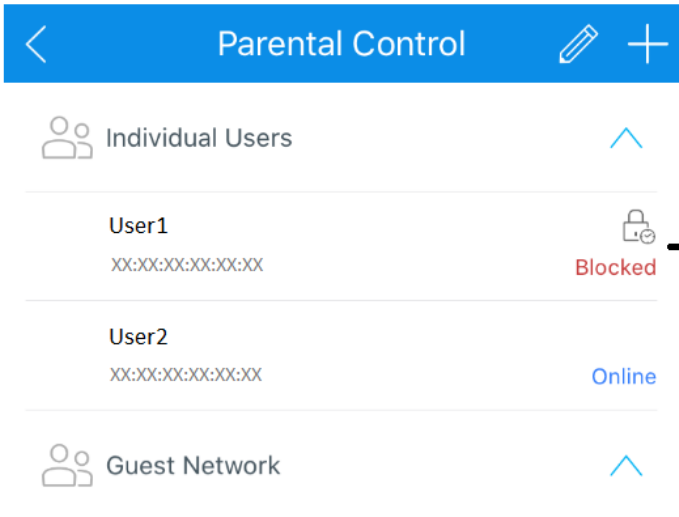Set High Priority can get faster to access your network.

Normal ⌄

Set Rules

Select Rules from the List or add New Rule for the Group

The new rule will be displayed in the list to indicate this rule has been applied to the client device.

Block User1

To verify that the client device is blocked during the specified schedule, the status will indicate that the client device is blocked.

To delete a rule, tap and hold the rule and prompt will appear if you would like to delete the rule.
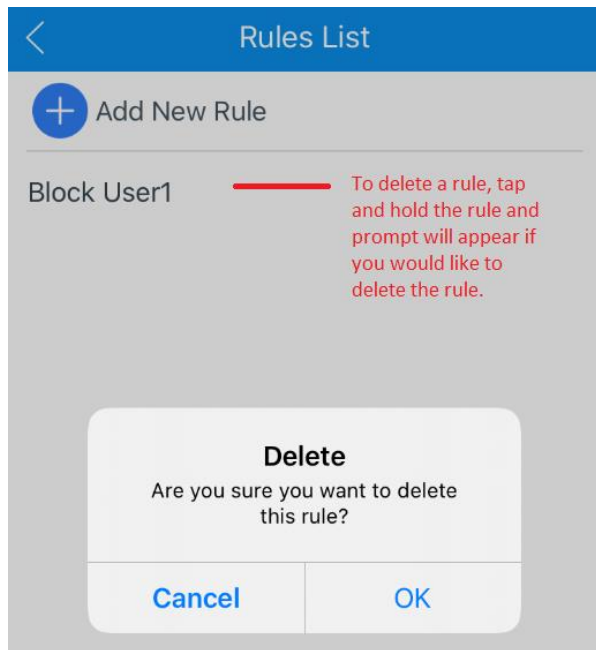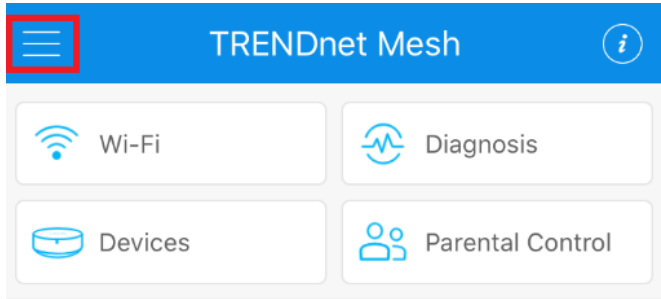
Parental Controls/QoS

For the QoS settings, you can prioritize traffic by setting specific clients to high priority. Tap Save to save the configuration settings.
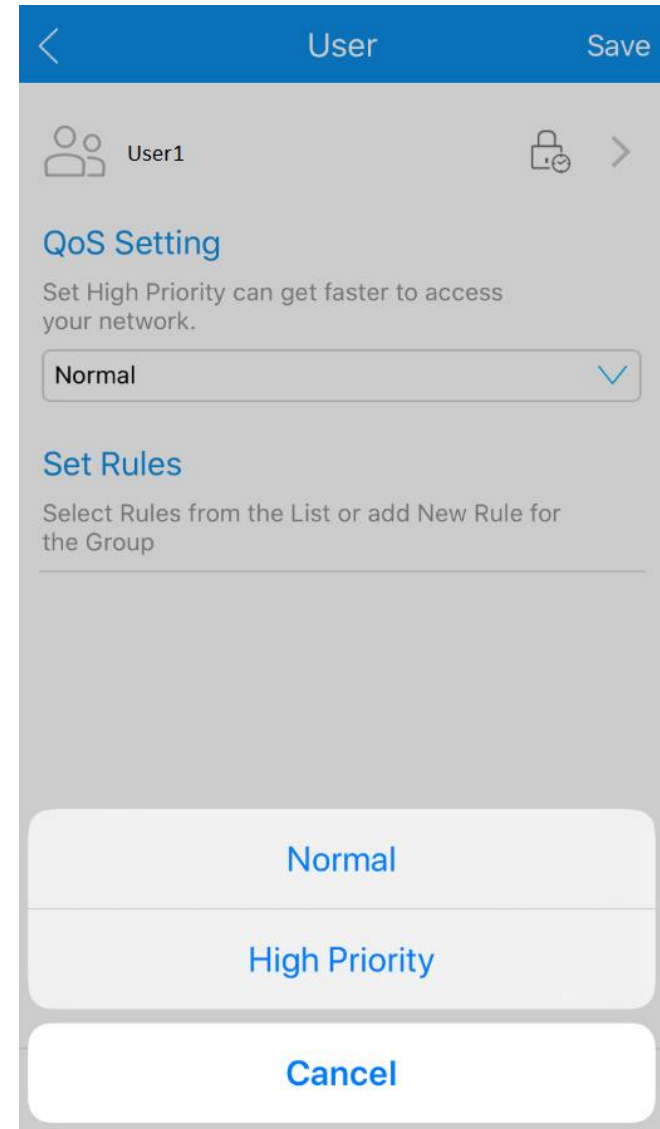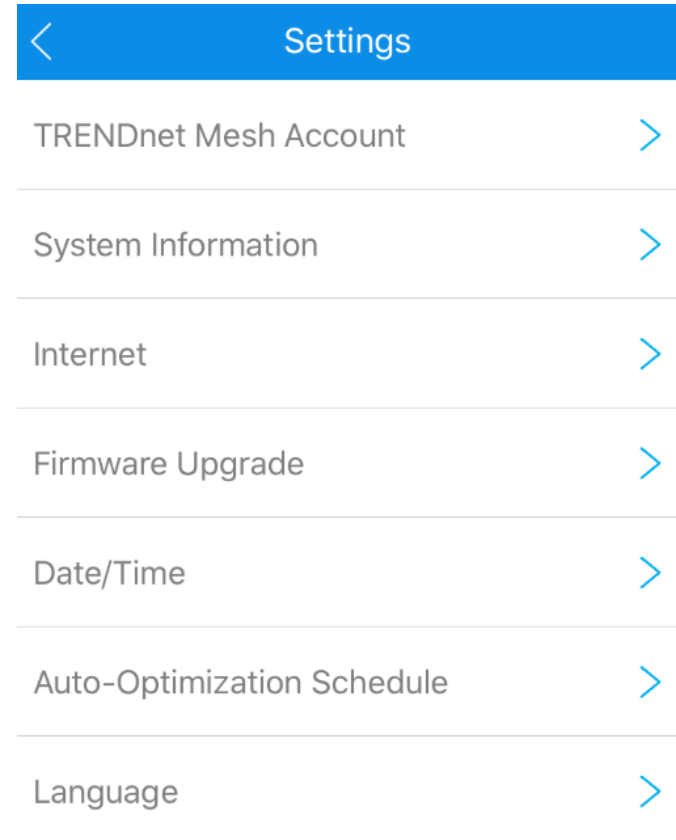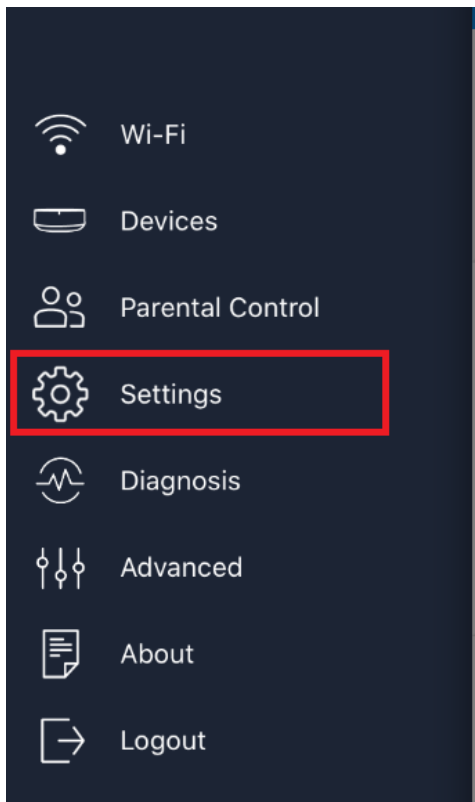
Settings

Tap the menu icon at the top left of the Home page.

When the menu appears, tap **Settings**.

Settings/TRENDnet Mesh Account

This page allows to change the User Name and Password used to log into your TEW-830MDR mesh network. Enter the new User Name, Current Password, and New Password, then tap Save to save the configuration settings.

< **TRENDnet Mesh Account**

Change TRENDnet Mesh Account

Username

trendnet

Current Password

New Password

Confirm New Password

Minimum of 8 characters

Save

Settings/System Information & Internet Information

This page will display your public Internet IP address (WAN) information provided by your ISP (Internet Service Provider)

< **System Information**

Internet Information   >

< **Internet Information**

Internet Type

DHCP

IP Address

10.10.10.30

Subnet Mask

255.255.255.192

Default gateway

10.10.10.62

Primary DNS

192.168.1.249

Secondary DNS

8.8.8.8

Settings/Internet

This page will allow you to configure your Internet configuration settings. Typically, DHCP is the most common however, if you are unsure, please contact your ISP (Internet Service Provider). If you have an existing Internet router, the master unit TEW-830MDR can function as a stand-alone wireless access point by selecting and applying the bridge mode setting and connecting the WAN port (blue) to one of the existing LAN ports of your existing Internet router.
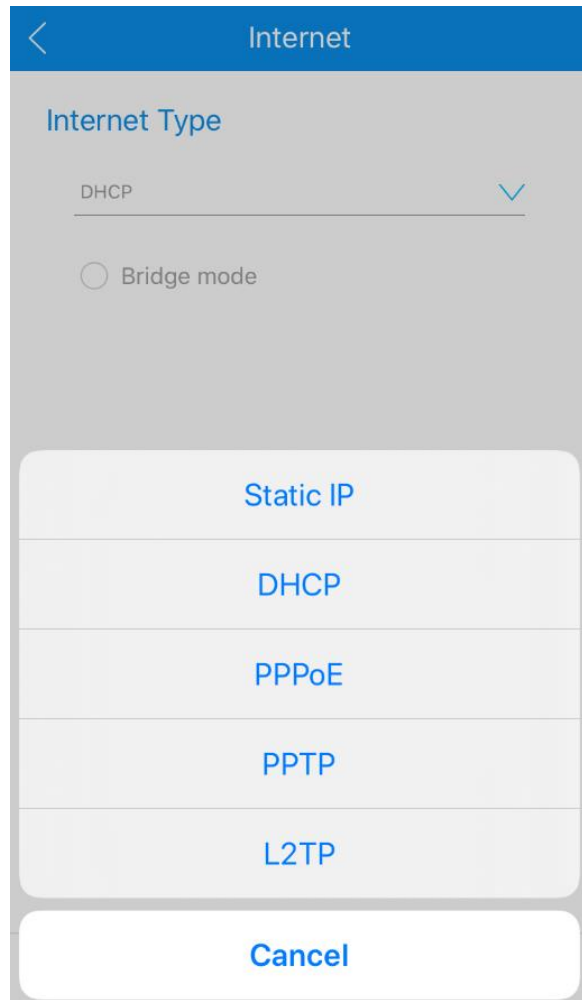
Settings/Firmware Upgrade

This page will check if there is an available firmware update online. You can also check the option to Auto Update which will automatically check if there is an update available online and initiate the firmware upgrade at 4:00am. If there is an update available and you would like to update manually, check all of the units listed in your mesh network and tap Next, then follow the remaining steps to upgrade the firmware.
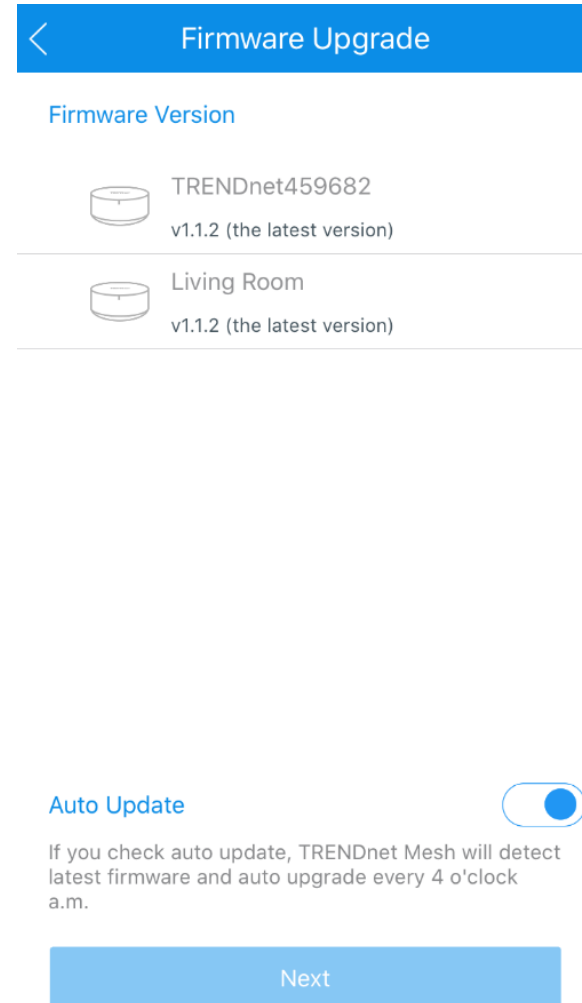
Settings/Date/Time

This page allows you to set the system/device time. Enabling auto detection will automatically pull time zone information from the Internet. Disable auto detection allows you to manually set your time zone. Tap Save to save your configuration settings.

Settings/Auto-Optimization Schedule

This page allows you to configure the auto-optimization schedule of the mesh system. To ensure optimal performance, the Mesh System, constantly collects signal information and adjusts some parameters. To apply the new configuration, a system reboot will be needed. Tap Save to save the configuration changes.

Settings/Language

This page allows you to set the app language settings. Tap Save to save the configuration settings.

Diagnosis
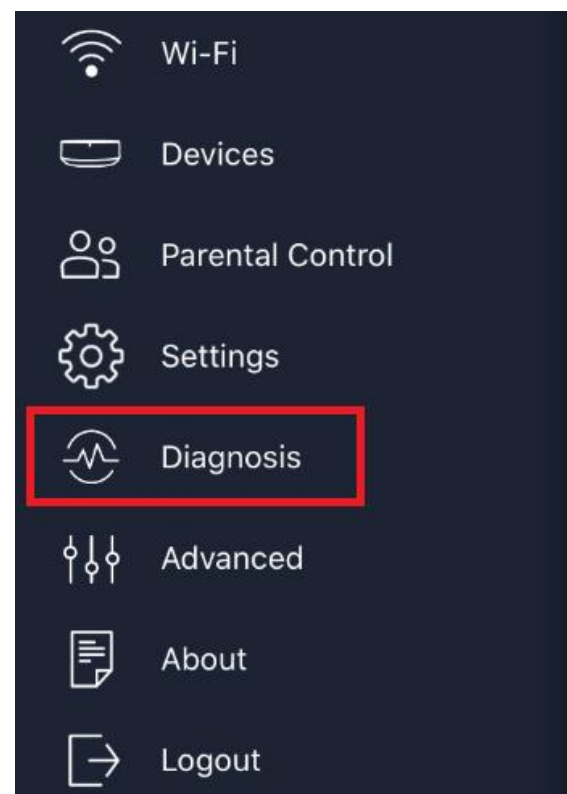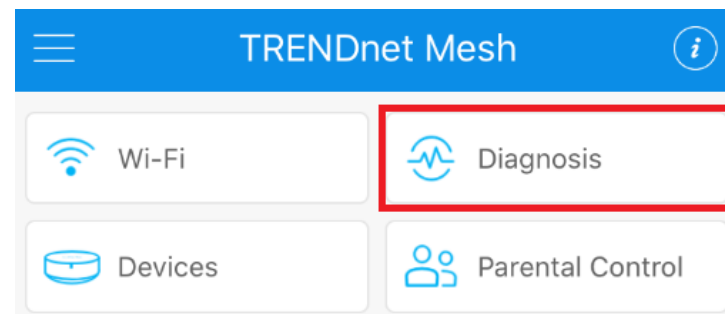
This page will provide an overall connection diagram of your mesh network units, Internet bandwidth, mesh network bandwidth, and indication if the range between the network units is optimal.

Tap Refresh to run a new Internet speed test.

Tap Run Test to run a new throughput test between the other mesh network unit to master unit

Advanced

Tapping the Advanced section will open the management interface of the router using the default web browser of your mobile device for additional configuration changes.

Important Note: For additional configuration changes, it is recommended that you use a computer to access the router management interface instead of mobile device.

TRENDnet Web GUI Settings

Access your router management web configuration page

Note: Your router management page URL/domain name http://tew-830mdr or IP address http://192.168.10.1 is accessed through the use of your Internet web browser (e.g. Internet Explorer®, Firefox®, Chrome™, Safari®, Opera™) and will be referenced frequently in this User's Guide.
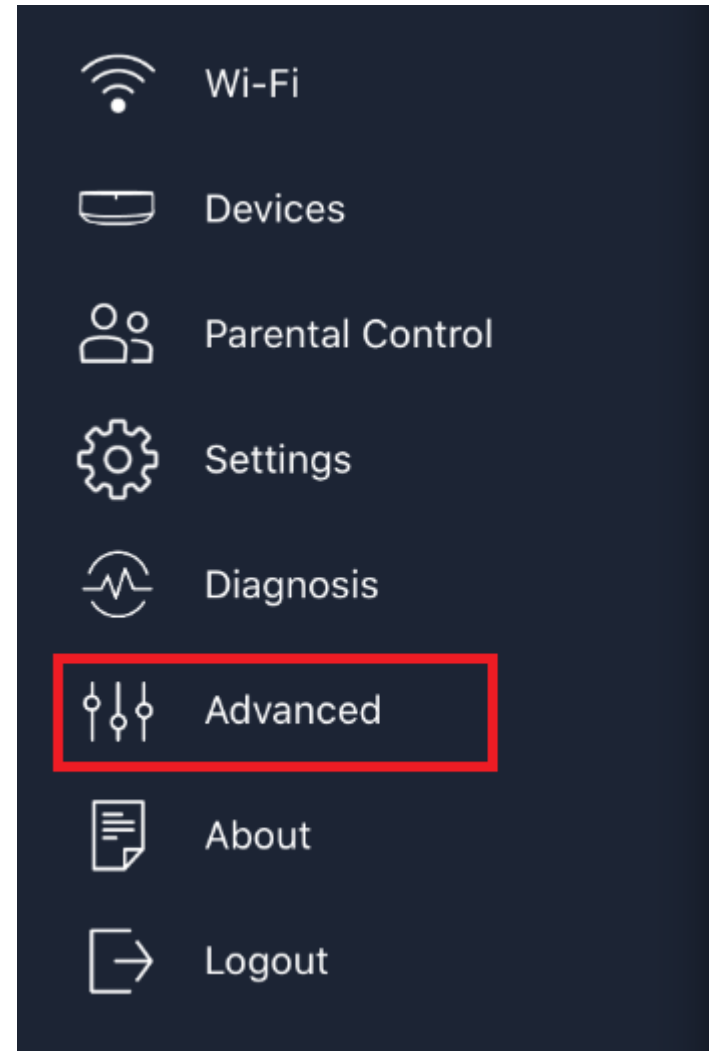
Note: The router management page can be accessed using a mobile device but it is recommended to use a computer web browser. You can access the router management page with a computer connected to your TEW-830MDR/TEW-830MDR2K WiFi mesh network or by connecting the computer to the wired LAN port (gray).

1. Open your web browser and go to URL/domain name https://tew-830mdr or default IP address https://192.168.10.1. Your router will prompt you for a user name and password.

2. You may receive a warning that the site may not be secure. Click More Information or Advanced (depending on your web browser) to choose alternative options to access the router management web configuration.

3. Enter the User Name and Password created during the initial app setup and click **Login.**

Note: User Name and Password are case sensitive.

Check the router system information

Home

This section displays a brief summary of the mesh network current status information such as WAN (Internet), wired (LAN), WiFi (Wireless) settings, firmware version, MAC address, mesh, and client devices.

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Home.**

System Information

- **Model Name** – Displays the model name of the device.
- **Operating Mode** – Displays the current mode the device is operating, Router or Bridge mode.

- **Time -** Displays the current day and time settings of the device.

System

Model Name	TEW-830MDR
Operation Mode	Router
Time	

WAN Internet Configuration

IPv4 WAN Status

- **Type:** Displays the current WAN IPv4 connection type applied.
- **Address** – The current IP address assigned to your router WAN interface.
- **Netmask** - The current subnet mask assigned to your router WAN interface.
- **Gateway** – The current gateway assigned to your router WAN interface.
- **DNS 1/2 (Domain Name System) Server** – The current DNS address(es) assigned to your router WAN interface.
- **Connected** – Displays the current uptime the WAN has been consistently connected without interruption.

IPv6 WAN Status

- **Type:** Displays the current WAN IPv6 connection type applied.
- **WAN IPv6 Link-Local Address** – The current Link Local IPv6 address and prefix assigned to your router WAN interface.
- **LAN IPv6 Link-Local Address –** Displays the current Link-Local IPv6 address and prefix assigned to your router LAN.

Note: The WAN status information displayed depending on your WAN connection type and settings.

WAN

IPv4 WAN Status	Type: DHCP Address: 10.10.10.22 Netmask: 255.255.255.192 Gateway: 10.10.10.62 DNS 1: 192.168.1.249 DNS 2: 8.8.8.8 Connected: 17h 46m 0s
IPv6 WAN Status	Type: Link-local only WAN IPv6 Link-Local Address : fe80::8adc:96ff:fe6d:a0ff/64 LAN IPv6 Link-Local Address : fe80::8adc:96ff:fe6d:a0fc/64

LAN Information

- **IPv4 LAN Status** - Displays your router's current LAN IP address.
- **IPv6 LAN Status** – Displays the current Link-Local IPv6 address and prefix assigned to your router LAN.

LAN

IPv4 LAN Status	192.168.10.1
IPv6 LAN Status	FE80::8ADC:96FF:FE6D:A0FC/64

───────────

Wireless Information

- **Wi-Fi Name (SSID):** Displays the current wireless network name or your wireless network.
- **Encryption:** Displays the current wireless network security mode of your wireless network.
- **Guest Wi-Fi Name (SSID)**: Displays the current wireless network name of your guest Wi-Fi network.
- **Encryption:** Displays the current wireless network security mode of your guest Wi-Fi network.
- **Status:** Displays the current status of your Wi-Fi guest network enabled or disabled.
- **2.4GHz 802.11B/G/N Wireless AP:** Displays the current Wi-Fi operating channel of the 2.4GHz wireless band and Wi-Fi MAC address/BSSID.
- **5GHz-1 802.11AC/N Wireless AP:** Displays the current Wi-Fi operating channel of the 5GHz-1 wireless band and Wi-Fi MAC address/BSSID.
- **5GHz-2 802.11AC/N Wireless AP:** Displays the current Wi-Fi operating channel of the 5GHz-2 wireless band and Wi-Fi MAC address/BSSID.
- **5GHz-2 802.11AC/N Wireless AP Mesh Backhaul Mode:** Displays the current mesh backhaul mode of the 5GHz-2 band. By default, this band set exclusively as dedicated mesh backhaul connection between other mesh nodes.

Wireless

Wi-Fi Name(SSID):	TRENDnet830
Encryption:	WPA2/PSK AES
Guest Wi-Fi Name(SSID):	TRENDnet_GuestNetwork
Encryption:	WPA2/PSK AES
Status:	Disable
2.4GHz 802.11 B/G/N Wireless AP	Channel: 10 (2.457 GHz) BSSID: XX:XX:XX:XX:XX:XX
5GHz-1 802.11 AC/N Wireless AP	Channel: 157 (5.785 GHz) BSSID: XX:XX:XX:XX:XX:XX
5GHz-2 802.11 AC/N Wireless AP	Channel: 40 (5.200 GHz) BSSID: XX:XX:XX:XX:XX:XX Mesh Backhaul Mode: Dedicated

Mesh Device List

Displays a list of the current node/mesh devices connected to your wireless network (The number of TEW-830MDR units connected to your wireless mesh network).

- **Model:** Displays the model number of the mesh node.
- **Location:** Displays the location name/description of each node. The location name/description was set during initial setup and can be changed manually.
- **MAC Address:** Displays the MAC address of each node/mesh device.
- **IP Address:** Displays the current IP address of each node/mesh device.
- **Firmware**: Displays the current firmware version of each node/mesh device.
- **Uptime:** Displays the current time each node/mesh device has been connected to the wireless mesh network without interruption.

Mesh Device List

Model	Location	MAC Address	IP Address	Firmware	Uptime
TEW-830MDR	TRENDnet459682	XX:XX:XX:XX:XX:XX	192.168.10.168	v1.1.4	15 hours 26 min 43 sec
TEW-830MDR	Living Room	XX:XX:XX:XX:XX:XX	192.168.10.1	v1.1.4	15 hours 26 min 35 sec

Mesh Connection Quality

The diagram displays the current network topology of your wireless network nodes/mesh devices and the connection quality (color coded) between each node.

Mesh Connection Quality

Living Room

TRENDnet459682

▬ Wired Connection   ▬ Too Close   ▬ Optimum Range   ▬ Too Far
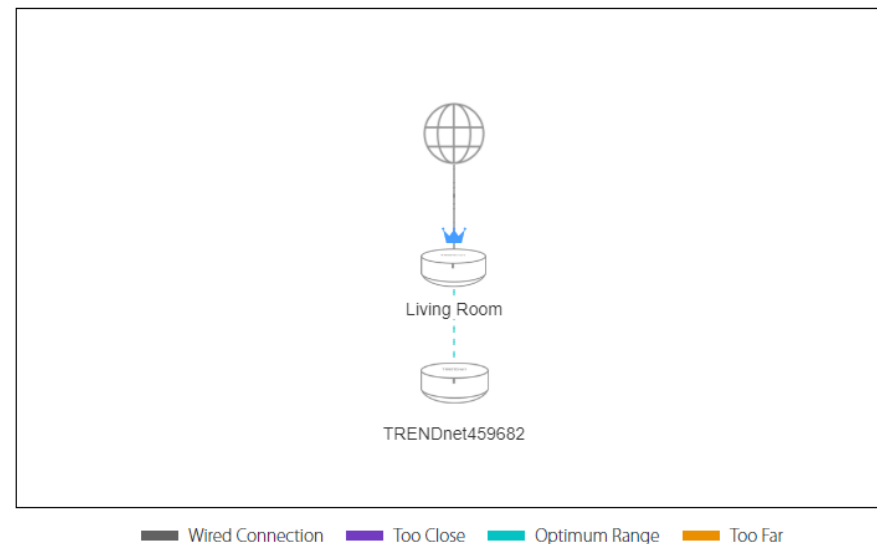
Client List

Displays a list of the client devices connected to your wireless mesh network, connection status, and which wireless node/mesh device each client is connected.

- **Device Name:** Displays the client device host name.
- **IPv4 Address:** Displays the current IPv4 address assigned to the client device.
- **Location:** Displays if the client device is currently connected via wired Ethernet cable or wireless including which wireless mesh node the client is connected.
- **Status:** Displays if the client device is currently online or offline.

Client List

Device Name	IPv4 Address	MAC Address	Location	Status	
CLIENT_DEVICE1	192.168.10.101	XX:XX:XX:XX:XX:XX	Wired connection	Online	●
CLIENT_DEVICE2	192.168.10.244	XX:XX:XX:XX:XX:XX	TRENDnet459682	Online	●
CLIENT_DEVICE3	192.168.10.227	XX:XX:XX:XX:XX:XX	N/A	Offline	○

Wireless Settings

WiFI > WiFi Settings

This section outlines available management options under the WiFi > WiFi Settings section.

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **WiFi** and click on **WiFi Settings**.

3. Under the Wireless Network section, review the settings below. To save changes to this section, click **Apply** at the bottom of the page.

- **Basic > WiFi Name (SSID)**: Enter the wireless name (SSID) for your wireless network. This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. By default, the router's wireless name is unique to the device. If you choose to change the SSID, change it to a name that you can easily remember. 2.4GHz, 5GHz-1, 5GHz-2 bands share the same wireless network name.
- **Basic > Hide WiFi Name:** Unchecked allows wireless client device to search and discover your wireless network name (also called SSID) broadcasted by your WiFi router/node/mesh device. Checked turns off the ability for wireless client devices to find your wireless network. It is still possible for wireless client devices to be manually configured to connect to your network. *Note: Disabling this settings will disable WPS functionality.*
- **Basic > Separate Clients:** When this option is checked, wireless client devices connected to your wireless network will be restricted from accessing other wireless client devices connected to your wireless network.

- **Security > Security Mode:** Click the drop-down list to select Disabled or WPA2/AES.
  - o **Disabled:** Not recommended. This setting will not require a key or password to access or your wireless network.
  - o **WPA2/AES (Default):** Enables security on your wireless network. This setting will require wireless client devices to enter a key/password/passphrase in order to connect to your wireless network.

  Note: **Key Format:** *8-63 alphanumeric characters (a,b,C,?,*, /,1,2, etc.)*

- **2.4GHz/5GHz 802.11 AC/B/G/N Wireless AP > Channel:** Selecting the **Auto** option will set your router to scan for the appropriate wireless channel to use automatically. Click the drop-down list and select the desired Channel for wireless communication. The goal is to select the Channel that is least used by neighboring wireless networks.
- **2.4GHz/5GHz 802.11 B/G/N Wireless AP > HT Mode:** Select the appropriate channel width for your wireless network. This setting only applies to 802.11n and 802.11ac. For greater 802.11n performance, select **20MHz/40MHz** or **40MHz** (Options: 20MHz, 20MHz/40MHz, 40MHz). It is recommended to use the default channel bandwidth settings 20MHz.
  For greater 802.11ac performance, select **80MHz** (Options: 20MHz, 40MHz, 80MHz). It is recommended to use the default channel width settings 80MHz.
  Note: Please note that the default settings may provide more stability than the higher channel bandwidth settings such as Auto 20/40/80MHz *for connectivity in busy wireless environments where there are several wireless networks in the area. It is recommended to keep the default settings.*
  - o **20 MHz** – This mode operates using a single 20MHz channel for wireless devices connecting at 802.11n on both 2.4GHz and 5GHz. This setting may provide more stability than 20MHz/40MHz, 40MHz, 80MHz for connectivity in busy wireless environments where there are several neighboring wireless networks in the area.

o **20/40MHz, 40MHz (2.4GHz)** or **40MHz, 80MHz (5GHz)** – When this setting is active, this mode is capable of providing higher performance only if the wireless devices support the channel width settings. Enabling 20/40MHz , 40MHz (2.4GHz) or 40MHz, 80MHz typically results in substantial performance increases when connecting an 802.11ac/n wireless client.

2.4GHz 802.11 B/G/N Wireless AP

| Channel | Auto |
| HT Mode | 20 MHz |

5GHz-1 802.11 AC/N Wireless AP

| Channel | Auto |
| HT Mode | 80 MHz (AC only) |

- **Advanced > Band Steering:** This setting controls how wireless clients are distributed between bands.
    o **Disabled** – Disables the band steering feature.
    o **Prefer 5GHz –** Selecting this option will automatically move 5GHz capable wireless clients if wireless clients initially connect to the 2.4GHz band. This option will still allow dual band (2.4GHz/5GHz) wireless clients to connect the 2.4GHz band.
    o **Force 5GHz (Default) –** Selecting this option will automatically move 5GHz capable wireless clients if wireless clients initially connect to the 2.4GHz band. This option will not allow dual band (2.4GHz/5GHz) wireless clients to connect the 2.4GHz band, only the 5GHz band.

o **Band Balance –** Selecting this option will automatically distribute wireless clients across 2.4GHz and 5GHz bands depending on connections per band and bandwidth usage.

Advanced

Band Steering	Force 5 GHz
	Disabled
	Prefer 5 GHz
	Force 5 GHz
	Band Balance

Force 5 G ... band steering is configured to ... not allow a dual band client to connect ... only if the client is not currently associated on the 2.4 GHz radio of this AP.

| Fast Roaming | ● Enabled ○ Disabled |
| Airtime Fairness | ● Enabled ○ Disabled |

Apply   **Cancel**
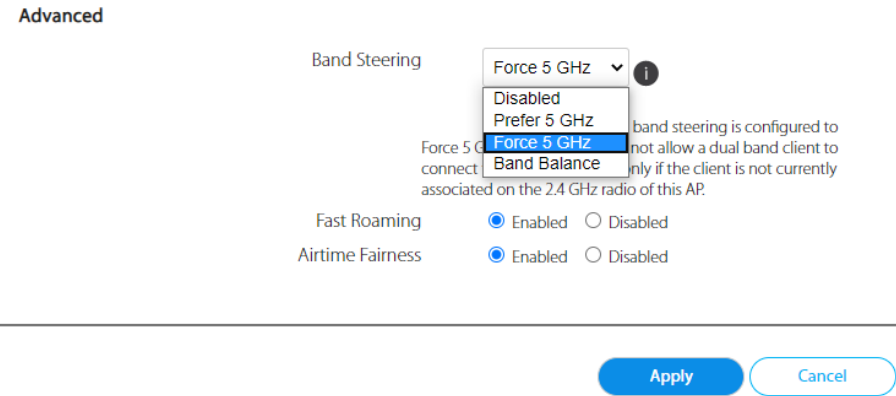
Guest Network

WiFi > Guest Network

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

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **WiFi** and click on **Guest Network**.

3. Under the Guest Network section, review the settings below. To save changes to this section, click **Apply** at the bottom of the page**.**

- **Basic > Guest Network:** This setting enables or disables the wireless guest network.
- **Basic > WiFi Name (SSID)**: Enter the wireless name (SSID) for your wireless guest network. This acronym stands for Service Set Identifier and is the name of your wireless guest network. It differentiates your wireless network from others around you. By default, the wireless guest network is disabled. If you choose to change the SSID, change it to a name that you can easily remember. The wireless guest network name is different from your primary wireless network name. 2.4GHz, 5GHz-1, 5GHz-2 bands share the same wireless guest network name.
- **Basic > Hide WiFi Name:** Unchecked allows wireless client device to search and discover your wireless guest network name (also called SSID) broadcasted by your WiFi router/node/mesh device. Checked turns off the ability for wireless client devices to find your wireless guest network. It is still possible for wireless client devices to be manually configured to connect to your network. *Note: Disabling this settings will disable WPS functionality.*

Guest Network

Basic

Guest Network	● Enabled ○ Disabled
Wi-Fi Name (SSID)	TRENDnet_GuestNetwork
Hide Wi-Fi Name	☐

- **Security > Security Mode:** Click the drop-down list to select Disabled or WPA2/AES.
  - **Disabled:** Not recommended. This setting will not require a key or password to access or your wireless guest network.
  - **WPA2/AES (Default):** Enables security on your wireless network. This setting will require wireless client devices to enter a key/password/passphrase in order to connect to your wireless guest network.
    Note: **Key Format**: *8-63 alphanumeric characters (a,b,C,?,*, /,1,2, etc.)*

Security

| Security Mode | WPA2 / AES ⌄ |
| Passphrase | ••••••••• 👁 |

Connect wireless devices to your router

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

- Gaming Consoles

- Internet enabled TVs

- Network media players

- Smart Phones

- Wireless Laptop computers

- Wireless IP cameras

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

See the "Appendix" on page 72 for general information on connecting to a wireless network.

Steps to improve wireless connectivity

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

1. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
   a. For the widest coverage area, install your router near the center of your home, and near the ceiling, if possible.

   b. Avoid placing the router on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), and masonry walls.

   c. Any obstruction can weaken the wireless signal (even non-metallic objects), so the fewer obstructions between the router and the wireless device, the better.

   d. Place the router in a location away from other electronics, motors, and fluorescent lighting.

   e. Many environmental variables can affect the router's performance, so if your wireless signal is weak, place the router in several locations and test the signal strength to determine the ideal position.

2. Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.

3. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.

4. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.

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

Change your router IP address

Interfaces > LAN

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 | Network: 192.168.10.0 / 255.255.255.0

1. Log into your router management page (see "Access your router management page" on page 23).
2. Click on **Interfaces** and click on **LAN**.
3. In the **General Setup** section under IPv4 Address, enter the new router IP address settings.
   - **IP Address:** Enter the new router IP address. (e.g. *192.168.200.1*)
     Note: The DHCP address range will change automatically to your new router IP address settings so you do not have to change the DHCP address range manually to match your new router IP address settings.

   - **DNS Type:** By default, the LAN IP address will be assigned to your client devices as the DNS server (**Dynamic**). If you would like to manually set your DNS server IP addresses, select **Static** and enter the new DNS server IP address settings in the primary and secondary DNS fields.

4. To save changes to this section, click **Apply** at the bottom of the page when finished.

Set up the DHCP server on your router

Interfaces > LAN

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 23).

2. Click on **Interfaces** and click on **LAN**.

3. In the **DHCP Server** section.
   - **DHCP Server:** Enable or Disable the DHCP server.
   - **Rebind Protection:** If enabled, the DHCP server will attempt to assign the same IP address to the same client device once the client device IP address lease expires. If disabled, the DHCP server may assign a different IP address from the start and end range IP address pool once the client IP address lease has expired.
   - **Start:** Changes the starting IP address for the DHCP server range. (*e.g. 100*)
   - **End:** Changes the ending address for the DHCP server range. (*e.g. 101*)
     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:** Changes the lease time for IP addresses issued to DHCP clients before renewal. (*e.g. One day*)
     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:** Enter a domain name to issue to DHCP clients.

DHCP Server

DHCP Server	● Enabled ○ Disabled
Rebind Protection	● Enabled ○ Disabled
Start	100 ⓘ
End	249 ⓘ
Lease Time	Half day ▼ ⓘ
Domain Name	

4. To save changes to this section, click **Apply** at the bottom of the page when finished.

Set up DHCP reservation

Interfaces > LAN

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 port forwarding (see "Port Forwarding" on page 42).

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Interfaces** and click on **LAN**.

3. In the **Static DHCP IP** section, click the ⊕ icon to add a static DHCP reservation.
   - **IP Address** – Enter the IP address to assign to the reservation. (e.g. 192.168.10.101)
   - **MAC Address** – Enter the MAC (Media Access Control) address of the computer or network client device to assign to the reservation. (e.g. *00:11:22:AA:BB:CC)*
   - **Comment** – Enter a comment, description, or name of the device you will assign the DHCP reservation.

Static DHCP IP

| IP Address	MAC Address	Comment	⊕
192.168.10.105	XX:XX:XX:XX:XX:XX	PC	⊖

4. To save changes to this section, click **Apply** at the bottom of the page when finished.

Note: You can delete a DHCP reservation entry by clicking ⊖ *icon next to the entry.*

Manually configure your Internet connection

Interfaces > WAN

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Interfaces** and click on **WAN**.

3. Under **IPv4 Connection Type** in **Protocol** drop-down list, select the type of Internet connection provided by your Internet Service Provider (ISP).

Protocol	DHCP ⌄
Operation Mode	Static address **DHCP** Br PPTP PPPoE L2TP
Hostname	
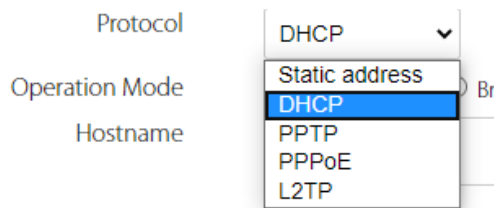
4. Complete the fields required by your ISP.

5. To save changes to this section, click **Apply** at the bottom of the page when finished.

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

IPv6 Settings

Interfaces > IPv6

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

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

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

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Interfaces** and click on **WAN6**.

.

3. Under **IPv6 Connection Type** in **Protocol** drop-down list, select the type of Internet connection provided by your Internet Service Provider (ISP).

Interfaces - WAN6

IPv6 Connection Type

Status
MAC Address: 88:DC:96:6D:A0:FF
RX: 422.86 MB (333141 Pkts.)
TX: 47.75 MB (206148 Pkts.)
IPv6: FE80:0:0:0:8ADC:96FF:FE6D:A0FF/64

Protocol
Link-local only ▾
Static IPv6
PPPoE
Autoconfiguration
6RD
Link-local only

WAN IPv6 Link-Local Address
LAN IPv6 Link-Local Address

4. Complete the fields required by your ISP.

5. To save changes to this section, click **Apply** at the bottom of the page when finished.

Note: *Please contact your ISP for IPv6 service availability.*

Select the IPv6 connection type provided by your ISP.

- Static IPv6
- PPPoE
- Autoconfiguration
- 6rd
- Link-Local Only

Add static routes

Interfaces > Routes

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

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

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Interfaces** and click on **Routes**.

3. In the **Static IPv4 Routes** section, click the ⊕ icon to add a new static route.
- **Destination LAN IP:** 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*)
- **Default Gateway:** Enter the gateway to the destination network for the route. (e.g. *192.168.10.2*)
- **Metric:** Enter the metric or priority of the route. The metric range is *1-256*, the lowest number *1* being the highest priority. (e.g. *1*)
- **Interface** – Select the interface to assign the route, LAN or WAN.

Routes

Static IPv4 Routes

Destination LAN IP	Subnet Mask	Default Gateway	Metric	Interface	⊕

| 192.168.2.0 | 255.255.255.0 | 192.168.10.2 | 500 | LAN ⌄ | ⊖ |

Note: *You can delete static route entry by clicking* ⊖ *icon next to the entry.*

4. To save changes to this section, click **Apply** at the bottom of the page when finished.

File Sharing

Storage > File Sharing

Samba is a network protocol that allows you to access shared files through your network. In order to share files, you will need to plug in a USB storage device on the USB port of the TEW-830MDR.

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Storage** and click on **File Sharing.** To save changes to this section, click **Apply** at the bottom of the page when finished.

- **Workgroup:** By default, the workgroup name is set to WORKGROUP which is the default name set in Windows®. You can manually change the workgroup name to a different name but make sure to set all computers and devices that will be accessing the USB file storage device on the network.
- **Description:** Enter a name description file sharing device. This parameter is optional.

Under the **Mesh List**, the all of the mesh nodes will be listed. File sharing/Samba can be enabled or disabled for each node.

File Sharing

Samba

Workgroup	WORKGROUP
Description (optional)	

Mesh List

Model	Location	MAC Address	IP Address	Status	
TEW-830MDR	TRENDnet459682	XX:XX:XX:XX:XX:XX	192.168.10.168	○ Enable	● Disable
TEW-830MDR	Living Room	XX:XX:XX:XX:XX:XX	192.168.10.1	● Enable	○ Disable

Apply   Cancel

4. Plug in USB storage device into the USB port.

5. Under Windows®, you can access the USB storage device on your computer under **Computer > Network > TRENDNETXXXXXX > sda1**.

Note: Each TEW-830MDR unit will be listed under Computer > Network section with the format TRENDNETXXXXXX (ex: TRENDNET459681, TRENDNET459682, etc.).

If your Windows® computer is not able to discover any network devices, you may not have network discovery and file sharing enabled, therefore, you may need to set the network to a private network and turn the feature on in Windows®
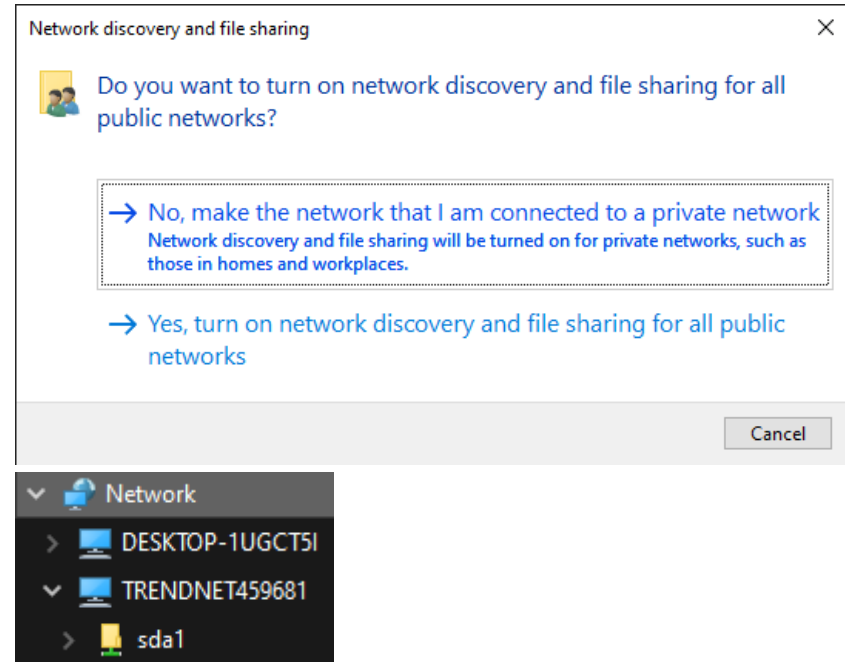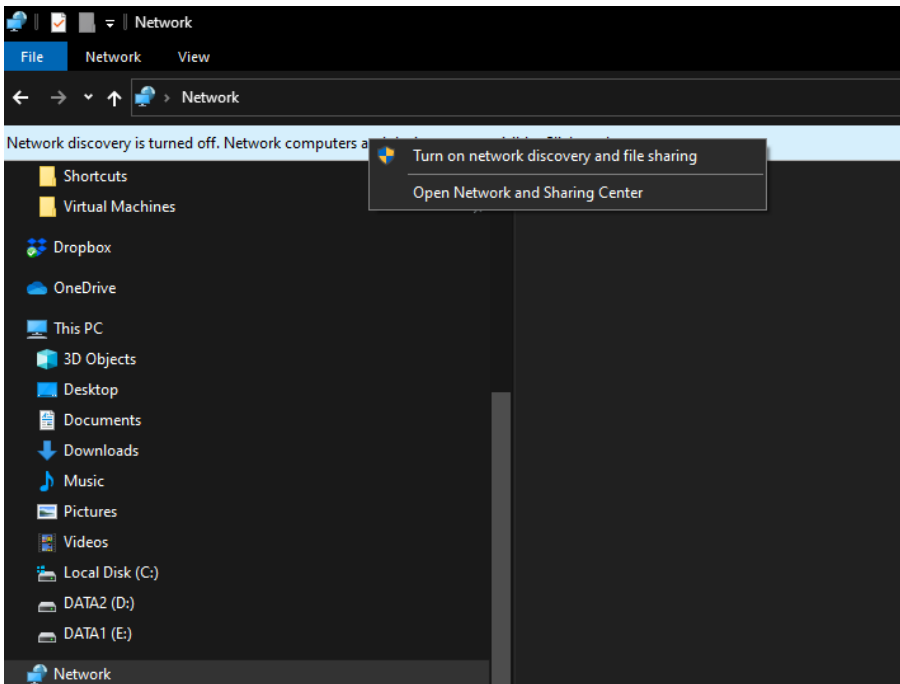
6. When prompted for a user name and password, enter the same user name and password you created during the initial app setup which is the same user name and password used to log into your router.

Firewall

Firewall > Firewall Settings

The firewall setting allows all of the specified incoming rules to function. By default, this setting is enabled and it is recommended to keep the default setting.

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Firewall** and **Firewall Settings.**

3. Under the Firewall section, select **Enabled** or **Disabled** to enable or disable the firewall functions. To save changes to this section, click **Apply** at the bottom of the page when finished.

Firewall

| Enable Or Disable Firewall Module Function | ● Enabled ○ Disabled |

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

Firewall > DMZ

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

It is strongly recommended to use **Port Forwarding** to allow access to your computers or network devices from the Internet.

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Firewall** and **DMZ.**

3. Under the DMZ section, check the **Enable DMZ** option to enable DMZ and enter the IP address the IP address you assigned to the computer or network device to expose to the Internet.

DMZ

| ☐ Enable DMZ | | |
| Local IP Address | | < | |

4. To save changes to this section, click **Apply** at the bottom of the page when finished.

Denial of Service (DoS)

Advanced > Firewall > DoS

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

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Firewall** and **DoS.**

3. Under the Denial of Service Feature section, check the DoS options to enable.

DoS

Denial of Service Feature					
Ping of Death	☐	20	Packet(s) burst	20	seconds
Discard Ping from WAN	☐				
Port Scan	☐				
Sync Flood	☐		Packet(s) burst		seconds

4. To save changes to this section, click **Apply** at the bottom of the page when finished.

Port Forwarding

Firewall > Port Forwarding

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 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 port fowarding port(s) from the Internet it is recommended to setup Dynamic DNS service (outlined in Identify Your Network).

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Firewall** and click on **Port Forwarding.**

3. Check the **Enable Port Forwarding** option to enable the port forwarding function. Review the port forwarding settings below. To save changes to this section, click **Apply** at the bottom of the page when finished.

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

- **Local IP:** Enter the IP address of the device to forward the port (e.g. *192.168.10.101).*
- **Local Port –** Enter the port number required by your device. Refer to the connecting device's documentation for reference to the network port(s) required.
- **Type**: Select the protocol required for your device. **TCP**, **UDP**
- **Public Port –** Enter the port number used to access the device from the Internet.

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

static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.

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

Port Forwarding

☐ Enable Port Forwarding

Local IP	Local Port	Type	Public Port	Comment
		Both ▾		⊕

Click the ⊕ icon to a new port forwarding rule.

Note: You can delete a port forwarding entry by clicking ⊖ icon next to the entry.

Example: To forward TCP port 80 to your IP camera

1. Setup DynDNS service (see Identify Your Network).

2. Access TRENDnet IP Camera management page and forward Port 80 (see product documentation)

3. Make sure to configure your network/IP camera to use a static IP address.
Note: You may need to reference your camera documentation on configuring a static IP address.

4. Log into your router management page (see "Access your router management page" on page 23).

5. Click on **Firewall** and click on **Port Forwarding.**

6. Check the **Enable Port Forwarding** option..

7. Enter the IP address assigned to the camera in the **Local IP** field. (e.g. *192.168.10.101*)

8. The **Local Port** and **Public Port**, enter port number **80** for both settings.

9. Make sure **TCP** is selected in the **Type** drop-down list.

10. To save changes to this section, click **Apply** at the bottom of the page when finished.

Identify your network on the Internet

Tools > DDNS

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

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

1. Sign up for one of the DDNS available service providers list under **Server Address**. (e.g. *no-ip.com,* etc.)

2. Log into your router management page (see "<u>Access your router management page</u>" on page 23).

3. Click on **Tools** and click on **DDNS**.

4. Review the **DDNS Settings** section. Click **Save Settings** to save settings.

- **Enabled:** Check the enabled option to enable the DDNS service.
- **Service:** Click the drop-down list Select your DDNS service.
- **Host Name:** Personal URL provided to you by your Dynamic DNS service provider (e.g. www.trendnet.dyndns.biz)
- **Username:** The user name needed to log in to your Dynamic DNS service account
- **Password:** This is the password to gain access to Dynamic DNS service for which you have signed up to. (NOT your router or wireless network password)

Dynamic DNS

Enabled	☐
Service	dyn.com ▾
Hostname	
Username	
Password	👁

5. To save changes to this section, click **Apply** at the bottom of the page when finished.

Allow remote access to your router management page

Tools > Web Management

You may want to make changes to your router from a remote location such at 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 23).

2. Click on **Tools** and click on **Web Management**.

3. Review the setting on the **Web Management** section. To save changes to this section, click **Apply** at the bottom of the page when finished.

- **HTTPS** – HTTPS access is enabled by default and is more secure than standard HTTP when accessing the router management page from a web browser. If disabling HTTPS, this will enable HTTP access.
- **Remote Access**
  - **Enabled:** Selecting enabled with allow remote access to the router management page from the Internet.
  - **Method:** All hosts will allow access from any public IP address on the Internet to access your router management. Specific host will restrict access to a single public IP address.
  - **Remote Port:** Enter the port to assign remote access to the router. It is recommended to leave this setting as 8080.

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

  - **HTTPS Port:** If using HTTPS for accessing your router management page, you can change the default HTTPS port used. If changing the default HTTPS port, you will need to specify the port when accessing the router management page. (ex: https://192.168.10.1:5000)

Web Management

HTTPS Settings

Enabled	● Enabled ○ Disabled

Remote Access

Enabled	● Enabled ○ Disabled
Method	● All Host ○ Specific Host
Port	8080
HTTPS Port	4430

Web Management System (Router Limits™)

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

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

Setup your router with Router Limits

Network > VPN

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Tools** and click on **Router Limits™.**

3. Select the mode to enable and click **Apply** at the bottom of the page when finished.

- **Enabled with bandwidth monitoring (reduces LAN > WAN performance):** This mode will allow you to monitor more bandwidth but will significantly decrease LAN > WAN performance.
- **Enabled without bandwidth monitoring:** This mode will enable the standard web content filtering service without bandwidth monitoring.

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

Router Limits System

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

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

5. At the welcome page, enter your email address to use for account creation and sign up and click **Submit.** Follow the remaining steps to create your Router Limits account.
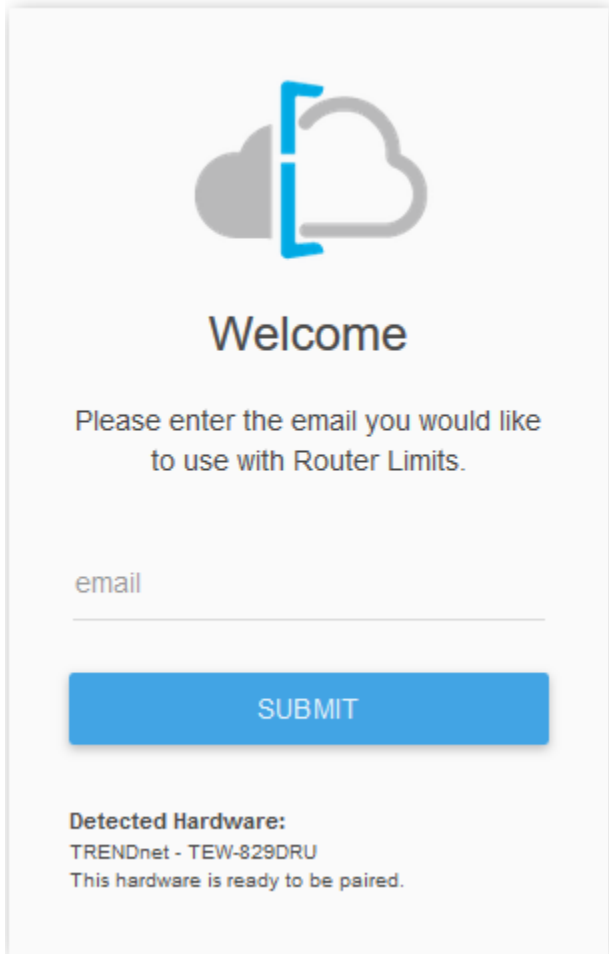
6. At the pair hardware page, the pairing code displayed should match the pairing code displayed in your router management page. If the pairing code does not match, you can click **Auto Detect** 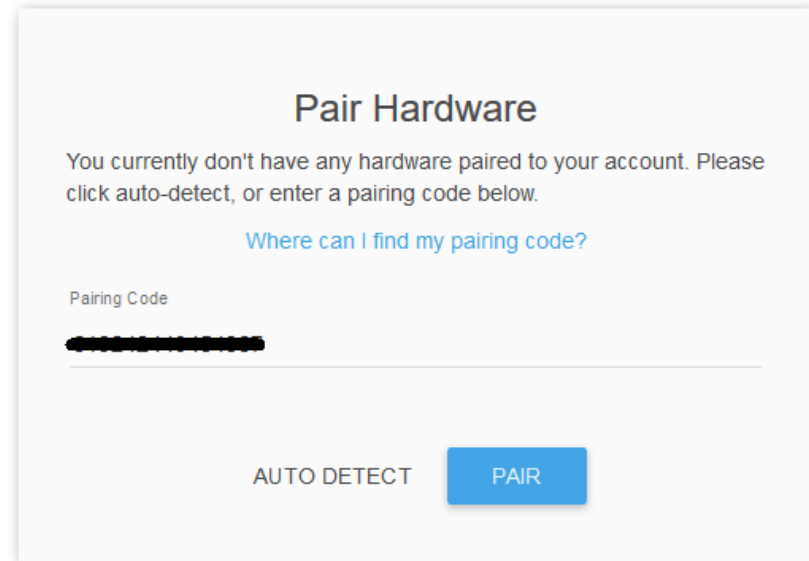to automatically copy the router pairing code into the field or you can manually enter the correct pairing code. After you have verified the correct pairing code is entered, click **Pair.**

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

Router Limits Content Management

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

- **Dashboard –** This page displays an overview of the service status and the devices connected to your network**.**
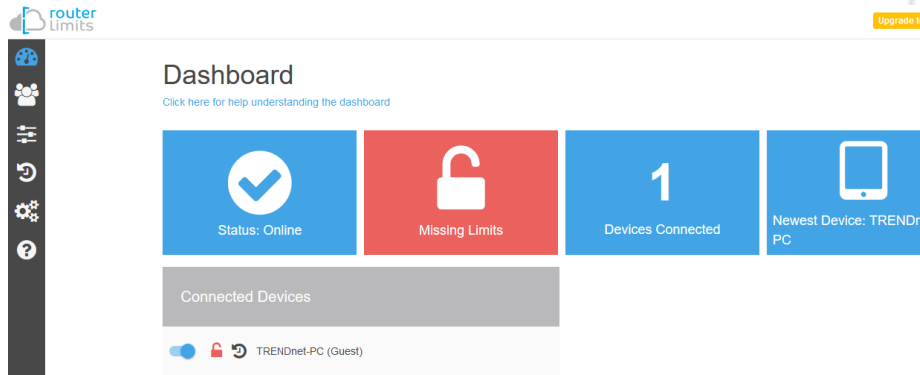
- **Devices and Groups –** This page displays the groups and devices assigned to each group. Content filters and scheduling can be assigned for each group. By default, new devices are assigned to the Guest group. New groups can be created and devices reassigned to new groups for easy management.
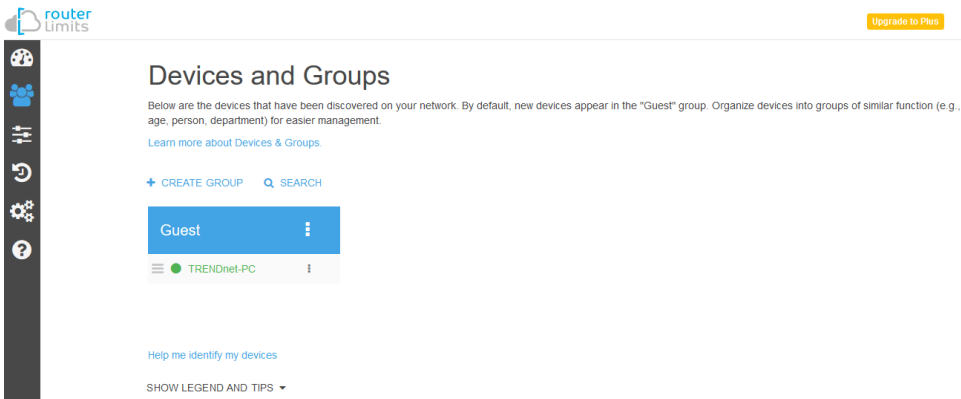
- **Limits –** Content filtering rules and scheduling are configured on this page. By default, all web content is allowed without restrictions. You can define new custom limits with a specific schedule along with a set of different restrictions or configuration options. Each template can be assigned to a specific group.
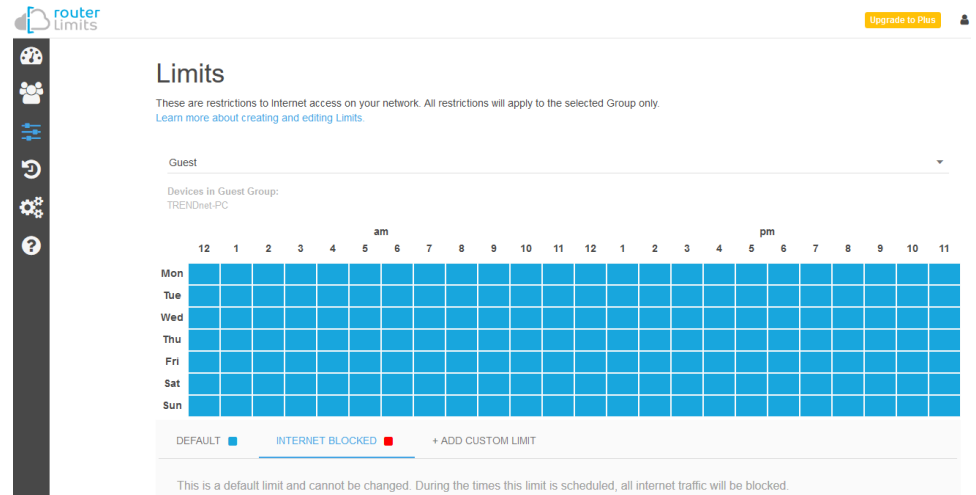
Restrictions

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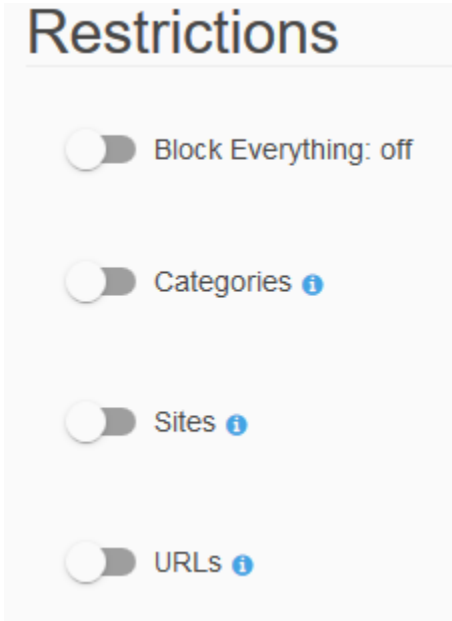
Exceptions – This setting allows you to configure exceptions and allow access.

Options

- o **Safe-Search –** Enables this setting enforces the use safe search to be enabled for Google and Bing search engines.
- o **YouTube Restricted Mode –** Enabling this setting enforces YouTube safety mode. (Currently not supported on mobile devices)
- o **Block Unknown Traffic –** Enabling this setting blocks all unknown IP addresses (specifically those used with VPN services or proxy services). It is recommended to leave this setting off unless explicitly required.
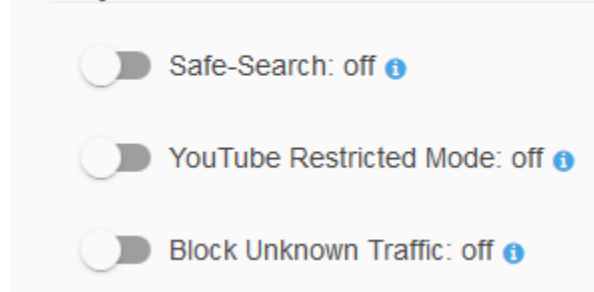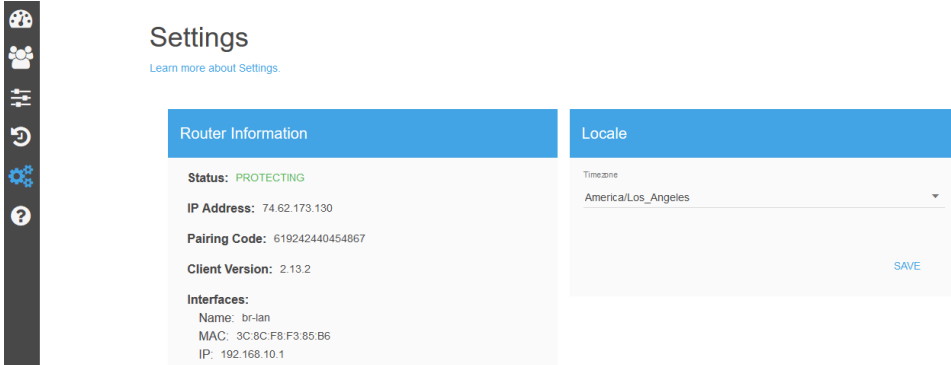
- • **History –** This page will display the Internet access history through your router. This page will also displays timestamps of when websites were accessed and which devices access each site.
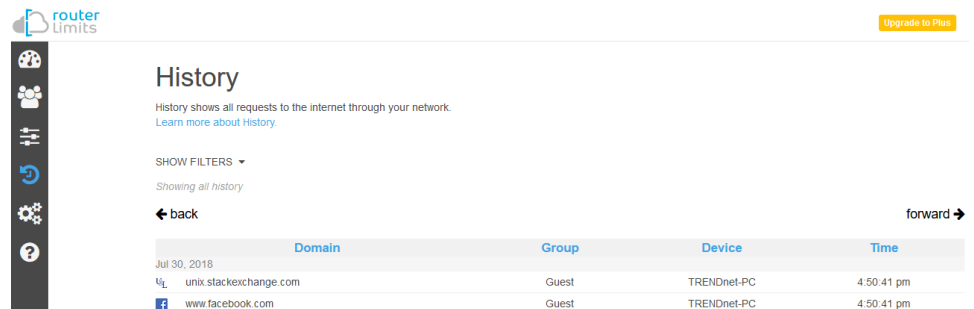
- ⚙️ **Settings –** This page will display the current status of service account and router as well as allow you to set the time zone settings.

Settings
Learn more about Settings.

Router Information

Status: PROTECTING

IP Address: 74.62.173.130

Pairing Code: 619242440454867

Client Version: 2.13.2

Interfaces:
   Name: br-lan
   MAC: 3C:8C:F8:F3:85:B6
   IP: 192.168.10.1

Locale

Timezone
America/Los_Angeles

SAVE

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

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

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

MANAGE ACCOUNT

Enable/disable UPnP on your router

Tools > UPnP

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 23).

2. Click on **Tools** and click on **UPnP**

3. Under the **UPnP** section, check the option to enable UPnP or uncheck to disable UPnP.

Universal Plug & Play

Enable UPnP Functionality   ⦿ Enable   ○ Disable

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

4. To save changes to this section, click **Apply** at the bottom of the page when finished.

Backup and restore your configuration settings

Tools > Backup / Restore

You may have added many customized settings to your router/mesh network and in the case that you need to reset your router/mesh network 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 23).

2. Click on **Tools** and click on **Backup / Restore.**

3. Next to Download Backup, click **Generate Archive**.

Download Backup: **Generate archive**

4. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default downloads folder. (Default Filename: *backup-TEW-830MDR-YYYY-MM-DD.tar.gz)*

To restore your router configuration:

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Tools** and click on **Backup / Restore.**

3. Next to Restore Backup, click **Browse** or **Choose File** (depending on your web browser).

Restore Backup: Choose File   No file chosen
                           Upload archive...

4. A separate file navigation window should open.

5. Select the configuration file to restore and click **Upload Archive**. (Default Filename: *backup-TEW-830MDR-YYYY-MM-DD.tar.gz)*. If prompted, click **Yes** or **OK**.

6. Wait for the router to restore settings.

Reboot your router / mesh network

Advanced > Administrator > Settings Management

You may want to restart your router/mesh network nodes if you are encountering difficulties 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 by disconnecting the power adapter connector located on the rear panel power port from the power port of your router/network node, see "Product Hardware Features" on page 2.
  Use this method if you are encountering difficulties with accessing your router management page. This is also known as a hard reboot or power cycle.
  OR
- **Router Management Page / TRENDnet Mesh App** – 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 23).

2. Click on **Tools** and click on **Reboot.**

3. To restart all mesh devices in the list, click **Restart All.**

To restart individual mesh devices in the list, next to the mesh node you would like to restart, click **Restart**

Restart

Restart mesh network   **Restart All**

Mesh List

Model	Location	MAC Address	IP Address	Action
TEW-830MDR	TRENDnet459682	XX:XX:XX:XX:XX:XX	192.168.10.168	**Restart**
TEW-830MDR	Living Room	XX:XX:XX:XX:XX:XX	192.168.10.1	**Restart**

Upgrade your router firmware

Tools > Firmware Upgrade

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

In addition, it is also important to verify if the latest firmware version is newer than the one your router is currently running. To identify the firmware that is currently loaded on your router, log in to the router, and you can check the Firmware version in the Mesh Device List or under Tools > Firmware. If there is a newer version available, also review the release notes to check if there were any new features you may want or if any problems were fixed that you may have been experiencing.

Online Firmware Upgrade (requires router/mesh network devices to be connected to Internet)

You can upgrade firmware via the TRENDnet Mesh app or web based router management page.

Note: *The TRENDnet Mesh app will allow you to enable auto upgrade which will upgrade the firmware for your mesh router and other mesh nodes automatically at 4:00am.*

1. Log into your router management page (see "Access your router management page" on page 23).

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

Online Firmware Check

        Current Version:1.1.4

Refresh

If a new firmware version is available, the details of the new version will automatically appear the about the new firmware. To start the online firmware upgrade process, click **Apply**. Please wait for the online firmware upgrade procedure to complete successfully.

Manual Firmware Upgrade

1. If a firmware upgrade is available, check the router model on our website http://www.trendnet.com/support   and download the firmware to your computer.

2. Unzip the file to a folder on your computer.

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

1. Log into your router management page (see "Access your router management page" on page 23).

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

3. Depending on your web browser, in the **Upload Firmware** section, click **Browse** or **Choose File**.

Firmware Upgrade - Upload

To upload a firmware image for upgrading your mesh devices.

Firmware image: Choose File | No file chosen   Upload

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

5. Click **Upload**. If prompted, click **Yes** or **OK**.

Reset your router to factory defaults

Advanced > Administrator > Settings Management

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting. Before you reset your router to defaults, if possible, you should backup your router configuration first, see "Backup and restore your router configuration settings" on page 59.

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

- **Reset Button** – Located on the side panel of your router, see "Product Hardware Features" on page 2. Use this method if you are encountering difficulties with accessing your router management page.

  OR

- **Router Management Page / TRENDnet Mesh App**

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Tools** and on click **Backup / Restore.**

3. Next to **Reset to Defaults**, click **Perform reset**. When prompted to confirm this action, click **OK**.

Note: This will reset all mesh network nodes to factory defaults.

Reset To Defaults: Perform reset

Router Default Settings

Administrator User Name	Created during initial app setup
Administrator Password	Created during initial app setup
Router Default URL	https://tew-830mdr
Router IP Address	192.168.10.1
Router Subnet Mask	255.255.255.0
DHCP Server IP Range	192.168.10.100-192.168.249
Wireless 2.4GHz & 5GHz	Enabled
Wireless 2.4GHz Network Name/Encryption	Created during initial app setup
Wireless 2.4GHz & 5GHz Guest Network	Disabled
USB SMB Settings	Disabled
USB SMB User Name	Same as Administrator
USB SMB Password	Same as Administrator

View your router log

Tools > System Logs

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 23).

2. Click on **Tools** and on click **System Logs.**

3. Check the **Enabled** or **Disabled** option to enable or disable logging. Then click **Apply**. The logging will display in the log window.

*Note: Clicking **Refresh** will refresh the page to ensure display of the most recent logging information. Click **Clear** will clear and delete all of the current logging information. Clicking the **Log Type** drop-down list will allow you to filter the logging to display only logging of specific severity/category.*

Advanced settings

The advanced settings provide can provide you with additional configuration options for setting up your wireless mesh network such as bridge mode operation and simultaneous wireless + wired mesh backhaul.

Bridge Mode Operation

Web based router management page: Interfaces > WAN

TRENDnet Mesh app: Settings > Internet

By default, the operation mode is set to Router Mode which performs network address translation (NAT) translating address between your single public Internet IP address (WAN) and private LAN IP network addresses. If you have an existing NAT router, you can set your mesh network to operate in **Bridge Mode** which will forward all traffic from your existing NAT router. If operating in Bridge Mode, for the master mesh node, connect the WAN port (blue) to one of your existing NAT router LAN ports. All of the mesh nodes and wireless will remain functioning from Router mode. You can also continue to pair additional mesh nodes to your mesh network.

Note: In order to change the operation mode, you will first need to setup and configure the mesh nodes using the initial TRENDnet Mesh app setup.

Web based router management page

1. Log into your router management page (see "Access your router management page" on page 23).

2. Click on **Interfaces** and click on **WAN.**

3. For the Operation Mode, click on **Bridge Mode**, then click **Apply**.

Interfaces - WAN

IPv4 Connection Type

Status — MAC Address: 88:DC:96:6D:A0:FF
RX: 1.30 GB (1060571 Pkts.)
TX: 115.52 MB (684716 Pkts.)
IPv4: 10.10.10.37/26

Protocol — DHCP

Operation Mode — ○ Router Mode ● Bridge Mode

Hostname

Wired Mesh Backhaul

The mesh nodes can simultaneously connect to each other both wirelessly and wired provide a wireless and wired mesh network backhaul for fault tolerance in case disconnection occurs between mesh nodes to create the wireless mesh network. There is no additional configuration needed.

After the initial setup app setup process is completed, connect the LAN (gray) port from the master router node, to your LAN network and connect the WAN (blue) port for the additional mesh nodes to your network LAN to create the wired mesh backhaul.

Note: Wired connection will take highest priority over wireless connection for mesh backhaul if connected. If wired connection is disconnected, the mesh connection will switch to wireless automatically.

Technical Specifications

Standards
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x
- IEEE 802.3ab
- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n (up to 400Mbps @ 256QAM)*
- IEEE 802.11ac (5GHz[1]: up to 867Mbps, 5GHz[2]: up to 867Mbps @ 256QAM)*

Device Interface
- 1 x Gigabit LAN port
- 1 x Gigabit WAN port
- 1 x USB 3.0 (Samba)
- Reset button
- LED indicator

Special Features
- Easily expand your WiFi mesh network coverage with additional TRENDnet WiFi mesh router
- Multi-User MIMO for increased bandwidth efficiency and better user experience*
- Seamless WiFi roaming
- Multi-Language app interface: English, Traditional Chinese, German, Italian, Swedish, French, Spanish, Dutch
- IPv6 support
- Samba support
- Implicit/Explicit Beamforming
- Band Steering

Access Control
- WiFi encryption: WPA/WPA2-PSK AES
- WiFi Guest network
- Hide WiFi Name/SSID
- Wireless client isolation

- NAT
- Port forwarding
- DMZ host
- UPnP
- DoS prevention
- Allow/deny WAN ping requests
- Parental controls (Set schedules for Internet access or filter by keyword or custom websites)
- Manage screen time, filter content, monitor bandwidth, and track browsing history with Router Limits™ web management system

Quality of Service
- Set client device priority (Normal/High priority)
- WMM

Internet Connection Types
- Dynamic IP (DHCP)
- Static IP (Fixed)
- PPPoE (Dynamic IP/Static IP)
- PPTP (Dynamic IP/Static IP)
- L2TP(Dynamic IP/Static IP)
- IPv6 (Static, Auto-configuration (SLAAC/DHCPv6), Link-Local, PPPoE, 6rd)

Management/Monitoring
- HTTP/HTTPS local/remote web-based management
- Internal system logging
- Mesh connection quality display
- Client device list
- Internet speed test
- Manual or online firmware upgrade and notification
- Backup and restore configuration
- Internal logging
- Restore to factory default
- Router/Bridge operation modes
- Static routes

Frequency
- 2.412 - 2.472GHz
- 5.180 – 5.825GHz

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

Media Access Protocol
- CSMA/CA with ACK

Antenna Gain
- 2.4GHz: 2 x 4.03 dBi (max.) / 5GHz: 4 x 5.64 dBi internal antennas

Receiving Sensitivity
- 802.11a: -73 dBm (typical) @ 54Mbps
- 802.11b: -90 dBm (typical) @ 11Mbps
- 802.11g: -76 dBm (typical) @ 54Mbps
- 802.11n (2.4GHz): -89 dBm (typical) @ 300Mbps
- 802.11n (5GHz): -86 dBm (typical) @ 300Mbps
- 802.11ac: -83 dBm (typical) @ 867Mbps

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

Power
- Input: 100 – 240V AC, 50/60Hz
- Output: 12V DC, 1.5A external power adapter
- Max. Consumption: 15.12W

Operating Temperature
- 0° – 40° C (32° – 104° F)

Operating Humidity
- Max. 90% non-condensing

Certifications
- FCC
- IC

Dimensions
- 126 x 126 x 60mm (4.96 x 4.96 x 2.36 in.) per unit

Weight
- 372g (13.1 oz.) per unit

Disclaimers
*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials, and other conditions. For maximum performance of up to 867Mbps, use with an 867Mbps 802.11ac wireless adapter. For maximum performance of up to 400Mbps, use with a 400Mbps 802.11n wireless adapter. Multi-User MIMO (MU-MIMO) requires the use of multiple MU-MIMO enabled wireless adapters.

Troubleshooting

Q: I typed http://tew-830mdr **in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the router management page?**
Answer:
Access the router using the default IP address 192.168.10.1.

http://192.168.10.1

Q: I typed http://192.168.10.1 in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the router management page?
Answer:
1. Check your hardware settings again. See "Router Installation" on page 8.
2. Make sure the LAN and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to *Obtain an IP address automatically* or *DHCP* (see the steps below).
4. Make sure your computer is connected to one of the router's LAN ports
5. Press on the factory reset button for 15 seconds, the release.
Windows 7/8/8.1/10

    a. Go into the **Control Panel**, click **Network and Sharing Center**.

    b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

    c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

    d. Then click **Obtain an IP address automatically** and click **OK**.

Windows Vista

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

Windows XP/2000

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

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

Q: I am not sure what type of Internet Account Type I have for my Cable/DSL connection. How do I find out?
Answer:
Contact your Internet Service Provider (ISP) for the correct information.

Q: I went through the Wizard, but I cannot get onto the Internet. What should I do?
Answer:
1. Verify that you can get onto the Internet with a direct connection into your modem (meaning plug your computer directly to the modem and verify that your single computer (without the help of the router) can access the Internet).
2. Power cycle your modem and router. Unplug the power to the modem and router. Wait 30 seconds, and then reconnect the power to the modem. Wait for the modem to fully boot up, and then reconnect the power to the router.
3. Contact your ISP and verify all the information that you have in regards to your Internet connection settings is correct.

Q: I cannot connect wirelessly to the router. What should I do?
Answer:
1. Double check that the LED on the router is lit (white) indicating that the router is operating normally without issue..
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.
4. Please see "Steps to improve wireless connectivity" on page 28 if you continue to have wireless connectivity problems.

Appendix

How to find your IP address?

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

Command Prompt Method

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

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.

2. In the dialog box, type *cmd* to bring up the command prompt.

3. In the command prompt, type *ipconfig /all* to display your IP address settings.

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.

2. Double-click on **Terminal** to launch the command prompt.

3. In the command prompt, type *ipconfig getifaddr <en0 or en1>* to display the wired or wireless IP address settings*.*

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

Graphical Method

MAC OS 10.6/10.5
1. From the Apple menu, select **System Preferences**.
2. In System Preferences, from the **View** menu, select **Network**.
3. In the Network preference window, click a network port (e.g., Ethernet, AirPort, modem). If you are connected, you'll see your IP address settings under "Status:"

MAC OS 10.4
1. From the Apple menu, select **Location**, and then **Network Preferences**.
2. In the Network Preference window, next to "Show:", select **Network Status**. You'll see your network status and your IP address settings displayed.

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

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

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

Windows 7/8/8.1/10
    a. Go into the **Control Panel**, click **Network and Sharing Center**.
    b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.
    c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.
    d. Then click **Obtain an IP address automatically** and click **OK**.

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

Windows XP/2000
    a. Go into the **Control Panel**, double-click the **Network Connections** icon
    b. Right-click the **Local Area Connection** icon and the click **Properties**.
    c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
    d. Then click **Obtain an IP address automatically** and click **OK**.

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

In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Using DHCP** and click the **Apply Now** button.
In MAC 10.5, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.
In MAC 10.6, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.
f. Restart your computer.

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

How to find your MAC address?

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

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

In MAC OS 10.4,

1. **Apple Menu > System Preferences > Network**

2. From the **Show** menu, select **Built-in Ethernet**.

3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

In MAC OS 10.5/10.6,

1. **Apple Menu > System Preferences > Network**

2. Select **Ethernet** from the list on the left.

3. Click the **Advanced** button.

3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

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

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

Windows 7/8/8.1/10

1. Open Connect to a Network by clicking the network icon (or) in the notification area.

2. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect.**

4. You may be prompted to enter a security key in order to connect to the network.

5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows Vista

1. Open Connect to a Network by clicking the **Start Button**. and then click **Connect To.**

2. In the **Show** list, click **Wireless**.

3. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect.**

4. You may be prompted to enter a security key in order to connect to the network.

5. Enter in the security key corresponding to the wireless network, and click **OK**.

Windows XP

1. Right-click the network icon in the notification area, then click **View Available Wireless Networks**.

2. In **Connect to a Network**, under **Available Networks**, click the wireless network you would like to connect to.

3. You may be prompted to enter a security key in order to connect to the network.

4. Enter in the security key corresponding to the wireless network, and click **Connect**.

Federal Communication Commission Interference Statement

The device complies with Part 15 of FCC Rules. Operation is subject to the following two

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

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

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

Operations in the 5.15-5.25GHz band are restricted to indoor use only.

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

IMPORTANT NOTE:

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

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

Industry Canada Statement

This device complies with ISED's licence-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d' ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Caution :

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

(iii) where applicable, antenna type(s), antenna models(s), and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 6.2.2.3 shall be clearly indicated.

Avertissement:

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

(iii) lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3, doivent être clairement indiqués.Radiation Exposure Statement:

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

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à plus de 20 cm entre le radiateur et votre corps.

Limited Warranty

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

Limited Warranty

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

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

Limited Lifetime Warranty

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PWP07172015v3   2021/07/16

TRENDNET®

Product Warranty Registration

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

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA