Product Overview

TEW-814DAP

Features
TRENDnet’s high performance AC1200 Dual Band Wireless Access Point, model TEW-814DAP, supports Access Point (AP), Client, Repeater, Wireless Distribution System (WDS) Bridge, and WDS + AP modes. The TEW-814DAP generates concurrent 867 Mbps Wireless AC and 300 Mbps Wireless N networks. Embedded GREENnet technology reduces power consumption by up to 50%.

Multi-Mode Support
Supports Access Point (AP), Client, Repeater, Wireless Distribution System (WDS), and WDS + AP modes

One Touch Connection
Securely connect to the access point at the touch of the Wi-Fi Protected Setup (WPS) button

Multi Language
Multi Language Interface: English, Spanish, French, German, and Russian

Logs
Real time logs and statistics help trouble shooting

Encrypted Wireless
Support for wireless encryption of up to WPA2

Multiple SSIDs
Create up to four SSIDs per wireless band

Next Generation Wireless AC
802.11ac provides uninterrupted HD video streaming in a busy connected environment

Simultaneous Dual Band
High performance 867 Mbps Wireless AC + 300 Mbps Wireless N bands

Wireless Coverage

Package Contents
In addition to your access point, the package includes:

- TEW-814D0AP
- Multi-Language Quick Installation Guide
- CD-ROM (User’s Guide)
- Network cable (1.5 m/5 ft.)
- Power adapter (12 V DC, 1 A)

If any package contents are missing or damaged, please contact the retail store, online retailer, or reseller/distributor from which the product was purchased.
Extended wireless coverage with MIMO antenna technology

**Compatibility**
Compatible with legacy wireless devices

**Gigabit Port**
Gigabit LAN port maintains high performance connections to the wired network

**Energy Savings**
Embedded GREENet technology reduces power consumption by up to 50%

**IPv6**
IPv6 network support

**Targeted Beamforming**
Increased real-time performance by directing stronger wireless signals to your specific location

* 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 at least a 867MBps 802.11ac wireless clients

---

**Product Hardware Features**

**Rear View**

- **On/Off Power Button:** Press to turn the device on
- **10/100/1000 Mbps Ethernet/LAN Port:** Connect Ethernet cables (also called network cables) from your access point to your router and wired network devices.
- **Reset Button:** Press and hold this button for 10 seconds to reset the access point.
- **WPS Button (Wi-Fi Protected Setup):** Push and hold this button for 5 seconds to activate WPS. The Power LED will blink when WPS is activated.
• **Power LED:** The indicator is solid green when your access point is powered on. Otherwise if this LED indicator is off, there is no power to your access point. The indicator will also blink when WPS is activated. The LED will stop blinking and remain solid green automatically once WPS process is completed.

• **Wireless 2.4GHz:** This indicator solid green when wireless 2.4GHz is enabled and blinks during wireless during data transmission.

• **Wireless 5GHz:** This indicator solid green when wireless 5GHz is enabled and blinks during wireless during data transmission.

• **WPS:** This indicator blinks green when WPS is activated.

### Basic Access Point Setup

The first access point is installed near your modem/router (typically supplied by your ISP “Internet Service Provider”) and physically connected using one of your access point’s Ethernet LAN port. The access point is configured to create both 2.4GHz and 5GHz wireless networks for your wireless devices (TVs, game consoles, or media bridges).
Expanding a Home Network

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

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

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

How to expand a home network
The access point provides multiple modes to extend your current network.

The access point offers the following modes:

- Access Point (Default)
- WDS (also known as wireless bridge)
- Client (also known as wireless client adapter mode)

Where to find more help
In addition to this User’s Guide, you can find help below:

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

Basic Installation

1. Connect the power adapter to the access point and then to a power outlet. Connect your computer to one of the access point’s LAN port. Push the ON/OFF (EU version) switch on the TEW-814DAP to power up the access point.

2. Assign a static IP address to your computer’s network adapter in the subnet of 192.168.10.x (ex. 192.168.10.25) and a subnet mask of 255.255.255.0. (Please refer to the [Appendix](#) on page 49 on how to assign static IP address to your computer)


   **Note:** You can also access the device using the default IP address (192.168.10.100)

4. Enter the User Name and Password. By default
   
   - User Name: *admin*
   - Password: *admin*
5. The Wizard will start. Click Launch Wireless Setup Wizard to begin.

6. For security purposes you are required to enter a new password, verify and enter the new password, click Next to proceed.

7. Select Access Point Mode and then click Next.

7. For added security, we have pre-encrypted each TEW-814DAP with a unique Wi-Fi Name (SSID) and Wi-Fi Key. You can find these pre-configured settings on the labels at the side and bottom of the TEW-814DAP. You will use this information to connect wirelessly to the access point. To change the Wi-Fi key, please refer to Secure your Wireless Network on page 11. If the access point is reset, the Wi-Fi Key and Wi-Fi Name will also reset to factory defaults click Next. The side and bottom of the TEW-814DAP. You will use this information to connect wirelessly to the access point. To change the Wi-Fi key, please refer to Secure your Wireless Network.

8. Please wait while the settings are being applied. Setup is complete. Connect the access point to your router and connect your network ready devices to the access point’s LAN port.
Access your access point management page

Note: Your access point management page URL/domain name http://tew-814dap/ or default IP address http://192.168.10.100 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.

If you have changed the default IP address, you will need to ensure that your computer is configured with IP address settings in the same subnet as the as the access point in order to access the access point management page. (Ex. Access Point IP address changed to 192.168.0.100 / 255.255.255.0, example computer address 192.168.0.25 / 255.255.255.0).

1. Open your web browser and go to URL/domain name http://tew-814dap/ or IP address http://192.168.10.100. Your access point will prompt you for a user name and password.

2. By default, the user name is admin and password is admin. You can also find the Password on a sticker on the side of the access point and on the label on the bottom of the access point. Enter your Username and Password, select your preferred language, and then click Login.

   Note: If you have changed the password already such as in the Setup Wizard, you will need to login using the new password.

Default User Name: admin
Default Password: admin

Note: User Name and Password are case sensitive.

Choosing your device mode

Access Point (AP) Mode

By default, your access point functions in Access Point mode, creating a wireless network to allow wireless client devices to connect and access your network resources and access the Internet.

The diagram below shows your access point connected to one of your router LAN ports and functioning in Access Point mode allowing wireless clients (ex. laptops, game consoles, DVRs, Smart TVs, and mobile devices, etc.) to wirelessly connect to your access point to establish network and Internet connectivity.

Set the device to access point mode

Main > Device Mode

Note: By default, the device is set to function in access point mode.

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on Main, click on Device Mode.
3. Click the **Device Operation Mode** drop-down list and select **Access Point**.

### Wireless Network

- **Mode**: Select the mode you would like to set the wireless band to operate.
  - **Access Point**: Select this option to create a wireless network.
  - **WDS**: Select this option to have the device establish a WDS (wireless bridge) connection with another access point.
  - **WDS + AP**: Select this option to create a wireless network and have the device establish a WDS (wireless bridge) connection with another access point.

- **Enable Wireless**: Select from the pull down menu the schedule of when to enable the wireless signal. Select **Always** for always on or click **Add New** to create a new schedule.

- **Wireless Name**: 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 access point’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.

- **802.11 Mode**: Select the 802.11 mode you would like to the wireless band to operate on.
  - **802.11a only**: Select this option if you only have 802.11a wireless devices.
  - **802.11n only**: Select this option if you only have 802.11n wireless devices.
  - **Mixed 802.11n and 802.11a**: Select this option if you will be using both 802.11n and 802.11a wireless devices.
  - **802.11ac only**: Select this option if you only have 802.11ac wireless devices.

4. To save changes, click **Save Settings**.

**Using access point mode**

*Wireless > Basic*

1. Log into your access point management page (see “**Access your access point management** page” on page 8).
2. Click on **Wireless**, click on **Basic** scroll down to **Wireless Network Settings** (2.4GHz or 5GHz)
3. Review the settings, click **Save Settings** when finished.
• **Mixed 802.11n and 802.11ac:** Select this option if you have both 802.11n and 802.11 ac wireless clients.

• **Mixed 802.11ac, 802.11n and 802.11a:** Default setting, select this option if you are uncertain what your wireless devices support.

  - **Wireless Channel:** 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. Select **Enable Auto Channel Scan** to have the access point select the operating channel.

  - **Channel Width:** Select the appropriate channel width for your wireless network. This setting only applies to 802.11n. For greater 802.11n performance, select **Auto 20/40/80MHz** (Options: 20MHz or 20/40MHz (Auto)). It is recommended to use the default channel bandwidth settings.

  - **Visibility Status:** Select **Visible** to allow your wireless network to be visible or **Invisible** to prevent your wireless network to be seen.

**Wireless Networking and Security**

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

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

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

**Wireless Encryption Types**

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

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

- **WPA:** This encryption is significantly more robust than the WEP technology. Much of the older 802.11g hardware was been upgraded (with firmware/driver upgrades) to support this encryption standard. Total wireless speeds under this encryption type however are limited to 54Mbps.

  - **WPA-Auto:** This setting provides the access point with the ability to detect wireless devices using either WPA or WPA2 encryption. Your wireless network will automatically change the encryption setting based on the first wireless device connected. For example, if the first wireless client that connects to your wireless network uses WPA encryption your wireless network will use WPA encryption. Only when all wireless clients disconnect to the network and a wireless client with WPA2 encryption connects your wireless network will then change to WPA2 encryption.

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

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

  **Note:** Check the specifications of your wireless network adapters and wireless appliances to verify the highest level of encryption supported. Below is brief comparison chart of the wireless security types and the recommended configuration depending on which type you choose for your wireless network.

<table>
<thead>
<tr>
<th>Security Standard</th>
<th>WEP</th>
<th>WPA</th>
<th>WPA2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Compatible Wireless Standards</strong></td>
<td>IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)</td>
<td>IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)</td>
<td>IEEE 802.11a/b/g/n</td>
</tr>
<tr>
<td><strong>Highest Performance</strong></td>
<td>Up to 54Mbps</td>
<td>Up to 54Mbps</td>
<td>Up to 300Mbps</td>
</tr>
</tbody>
</table>
Secure your wireless network

Wireless > Basic

After you have determined which security type to use for your wireless network (see “How to choose the security type for your wireless network” on page 10), you can set up wireless security.

Note: By default, your access point is configured with a predefined wireless network name (SSID) and security key using WPA2-Personal. The predefined wireless network name and security can be found on the sticker on the side of the access point or on the device label at the bottom of the access point.

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

### Secure your wireless network

<table>
<thead>
<tr>
<th>Under This Setting</th>
<th>Encryption Strength</th>
<th>Additional Options</th>
<th>Recommended Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Open System or Shared Key, HEX or ASCII, Different key sizes</td>
<td>Open System ASCII 13 characters</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>TKIP or AES, Preshared Key or RADIUS</td>
<td>TKIP Preshared Key 8-63 characters</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>TKIP or AES, Preshared Key or RADIUS</td>
<td>AES Preshared Key 8-63 characters</td>
</tr>
</tbody>
</table>

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on Wireless, and click on Security.

#### Selecting WEP:

If selecting WEP-OPEN or WEP-SHARED (Wired Equivalent Privacy), please review the WEP settings to configure and click Save Settings to save the changes.

*Note: WEP encryption is available when 802.11 n-mode is set to Off, 802.11n does not support WEP encryption. In addition, when WEP encryption is selected WPS feature will be disabled.*
Network Key: Select the Key number you would like to use and enter the WEP key. This is the password or key that is used to connect your computer to this access point wirelessly.

Selecting WPA-Personal

In the Security Mode drop-down list, select WPA-Personal; Please review the WPA-Personal settings to configure and click Apply to save the changes.

<table>
<thead>
<tr>
<th>WEP Key Format</th>
<th>HEX</th>
<th>ASCII</th>
</tr>
</thead>
<tbody>
<tr>
<td>Character set</td>
<td>0-9 &amp; A-F, a-f only</td>
<td>Alphanumeric (a,b,C,?, /,1,2, etc.)</td>
</tr>
<tr>
<td>64-bit key length</td>
<td>10 characters</td>
<td>5 characters</td>
</tr>
<tr>
<td>128-bit key length</td>
<td>26 characters</td>
<td>13 characters</td>
</tr>
</tbody>
</table>

Security Mode: Select WPA-Personal
WPA Mode: Select WPA2 Only, WPA Only or Auto (WPA or WPA2). It is recommended to select WPA2 Only, but if you are not certain you can select Auto.
Cipher Type: Select AES when using WPA2 only, TKIP when using WPA Only. You can select TKIP and AES when using Auto (WPA or WPA2)
Pre-Shared Key: Enter the security password. This is the password or key that is used to connect your computer to this access point wirelessly.

Selecting WPA Enterprise:

The following section outlines options when selecting WPA (EAP or RADIUS). This security type is also known as EAP (Extensible Authentication Protocol) or Remote Authentication Dial-In User Service or RADIUS.

Note: This security type requires an external RADIUS server, Pre-Shared Key only requires you to create a passphrase.

Security Mode: Select WPA-Enterprise
WPA Mode: Select WPA2 Only, WPA Only or Auto (WPA or WPA2). It is recommended to select WPA2 Only, but if you are not certain you can select Auto.
Cipher Type: Select AES when using WPA2 only, TKIP when using WPA Only. You can select TKIP and AES when using Auto (WPA or WPA2)
RADIUS Server IP Address: Enter the IP address of the RADIUS server. (e.g. 192.168.10.250)
RADIUS Port: Enter the port your RADIUS server is configured to use for RADIUS authentication.
Note: It is recommended to use port 1812 which is typical default RADIUS port.
RADIUS server Shared Secret: Enter the shared secret used to authorize your access point with your RADIUS server.
Connect wireless devices to your access point

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 access point’s wireless network.

See the “Appendix” on page 44 for general information on connecting to a wireless network.

Connect wireless devices using WPS

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

**Note:** You will not be able to use WPS if you set the SSID Broadcast setting to Disabled or if you are using WEP security. Please note that WPS functionality will only be available when the Device Mode is set to Access Point mode under Main > Device Mode.

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

- Push Button Configuration (PBC) method
  - (RECOMMENDED) Hardware Push Button method—with an external button located physically on your access point and on your client device
  - WPS Software/Virtual Push Button - located in access point management page
- PIN (Personal Identification Number) Method - located in access point management page

**Note:** Refer to your wireless device documentation for details on the operation of WPS.

Recommended Hardware Push Button (PBC) Method

**Note:** It is recommended that a wireless key (passphrase or password) is created before connecting clients using the PBC method. By default your access point is preconfigured with a wireless encryption key. If no wireless key is defined when connecting via PBC, the access point will automatically create an encryption key that is 64 characters long. This 64 character key will then have to be used if one has to connect computers to the access point using the traditional connection method.

To add a wireless device to your network, simply push the WPS button on the wireless device you are connecting (consult client device User’s Guide for length of time), then push and hold the WPS button located on your access point for 3 seconds and release it. The WPS LED will blink to indicate WPS has been activated on your access point. (See “Product Hardware Features” on page 2)

For connecting additional WPS supported devices, repeat this process for each additional device.
PBC (Software/Virtual Push Button)

Wireless > Wi-Fi Protected Setup

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

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on Wireless, and click on Wi-Fi Protected Setup.
3. To add a wireless device to your network, click the Add Wireless Device with WPS button in the Add Wireless Station section.
4. Select PBC option and click Connect.
5. Then push the WPS button on the wireless device (consult wireless device’s User’s Guide for length of time) you are connecting.
6. Wait for your access point to finish the WPS process.

PIN (Personal Identification Number)

Wireless > Wi-Fi Protected Setup

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

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on Wireless, and click on Wi-Fi Protected Setup.
3. To add a wireless device to your network, enter the 8-digit numeric PIN number of the wireless client device and click Add Enrollee.
4. Select PIN option and click Connect.
5. Then press the PIN activation on your wireless device (consult wireless device’s User’s Guide for length of time) you are connecting.
6. Wait for your access point to finish the WPS process.
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 access point near the center of your home, and near the ceiling, if possible.
   b. Avoid placing the access point 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 access point and the wireless device, the better.
   d. Place the access point in a location away from other electronics, motors, and fluorescent lighting.
   e. Many environmental variables can affect the access point’s performance, so if your wireless signal is weak, place the access point 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.

Multiple SSID

Access > Multi-SSID

The multiple SSID feature allows you to broadcast up to additional SSIDs (or wireless network names). When wireless devices are searching for available wireless networks to connect to, the SSIDs (or wireless network names) will appear as separate and different wireless networks. Each SSID can be configured each with a different SSID (or wireless network name), security type and additional settings for wireless devices to connect. You can use the multiple SSID feature to setup guest wireless accounts with a different security type to keep your primary wireless network security information private.

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on Access, and click on Multi-SSID.
3. Click the Multi-SSID Index drop-down list and select the SSID to configure (SSID 1 is the primary SSID).
4. Review the settings, click **Apply** when finished.
   - **Enable SSID**: Select to enable the selected wireless network/band.
   - **Wireless Network Name**: 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.
   - **Security Mode**: Select the security type you would like to apply.

**Note**: To verify that the multiple SSIDs are active, using a wireless device, scan for available wireless networks and check if the wireless device is able to discover the SSIDs. To check connectivity, using a wireless device, connect to these SSIDs using the wireless security types you have configured.

**Advanced wireless settings**

**Wireless > Advanced**

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

- **Transmit Power: Beacon Interval**: A Select the percentage level of wireless transmit power you would like to have the access point operate in. Default Value: 100%
- **WMM Enable**: Select this option to enable WMM feature.
- **Short GI**: Select this option to enable Short guard interval feature.
- **IGMP Snooping**: Select this option to enable IGMP snooping feature.
- **WLAN Partition**: Select this option to disable the communication between connected clients.
- **HT20/40 Coexistence**: Select enable to allow the access point to support both 20MHz and 40MHz.
**Wireless Bridge**

Wireless bridging using WDS (Wireless Distribution System) allows the device to create a wireless bridge with other WDS supported wireless routers and access points configured in WDS mode to bridge groups of network devices together wirelessly. Network enabled devices can be plugged into the Ethernet LAN port. WDS is subset option of Access Point mode. There are 2 types of WDS modes,

- **WDS**: Strictly for establishing wireless bridging only and will not function in access point simultaneously, allowing wireless client devices such as computers, game consoles, mobile phones, etc. to connect in order to access network resources from multiple groups of network devices as well as the Internet. The diagram below illustrates examples of WDS.

- **WDS+AP**: Allows the device to establish wireless bridging and function as access point simultaneously, allowing wireless client devices such as computers, game consoles, mobile phones, etc. to connect to the access point in order to access network resources from multiple groups of network devices as well as the Internet. Please refer to the section Wireless Bridge (WDS) with Access Point (AP) Mode on page 19 for details on this mode.

**Note**: WDS (Wireless Distribution System) is not currently standardized and may not connect to different model wireless routers or access points, therefore, when using WDS, it is recommended to use the same model and version for wireless bridging.

---

© Copyright 2015 TRENDnet. All Rights Reserved.
The diagram below illustrates an example of multiple WDS wireless bridge links.
Access Point Mode with Wireless Bridge (WDS)

Wireless bridging using WDS (Wireless Distribution System) allows the device to create a wireless bridge with other WDS supported wireless routers and access points configured in WDS mode to bridge groups of network devices together wirelessly. Network enabled devices can be plugged into the Ethernet LAN port. WDS is subset option of Access Point mode.

There are 2 types of WDS modes,

- **WDS+AP**: Allows the device to establish wireless bridging and function as access point simultaneously, allowing wireless client devices such as computers, game consoles, mobile phones, etc. to connect to the access point in order to access network resources from multiple groups of network devices as well as the Internet. The diagrams below illustrate examples of WDS with Access Point.

- **WDS**: Strictly for establishing wireless bridging only and will not function in access point simultaneously, allowing wireless client devices such as computers, game consoles, mobile phones, etc. to connect in order to access network resources from multiple groups of network devices as well as the Internet. Please refer to the section Wireless Bridge (WDS) Mode page 17 for details on this mode.

*Note:* WDS (Wireless Distribution System) is not currently standardized and may not connect to different model wireless routers or access points, therefore, when using WDS, it is recommended to use the same model and version for wireless bridging.
The diagram below illustrates an example of multiple WDS wireless bridge links with access point functionality.
Planning for Wireless Bridging (WDS)

Note: By default, the device is set to function in access point mode. WDS is a subset option of Access Point Mode. You must set your access point device mode to operate in Access Point first in order to configure WDS. Please ensure the Device Mode is set to Access Point under Main > Device Mode.

Before configuring WDS, please ensure the following items first:

1. Verify that all of your wireless devices support WDS.
2. Make sure different IP addresses are assigned to each WDS supported wireless device used for bridging. (ex. 192.168.10.100, 192.168.10.99, 192.168.10.98, etc.) to avoid IP address conflicts. See the section Change your access point IP address page 32 for changing the access point IP address.
3. Please ensure that only one DHCP server is assigning IP addresses on your network to avoid IP address conflicts. Typically, most routers used in a home environment include a built-in DHCP server (typically enabled by default) to assign IP addresses to local client devices automatically. Please make sure that only one device on your network has DHCP server enabled and disabled on all others to avoid IP address conflicts.
4. WDS bridging requires all WDS supported devices to use the same wireless network name (SSID), wireless channel, and wireless security settings on all WDS supported wireless devices. Refer to page 9 “Using access point mode” to configure wireless network name (SSID) and wireless channel settings. Refer to page 10 “Wireless Networking and Security” to configure wireless security settings.
5. You will require the wireless MAC address of each WDS supported device. On any network, each network device has a unique 6-digit MAC (Media Access Control) address. For each WDS supported device, all of the remote wireless MAC addresses of the other WDS supported device you are bridging. (Ex. In diagram on the next page, AP1 needs to enter the remote MAC addresses (red text) of AP2, AP3, and AP4. AP2 needs to enter the remote MAC address of AP1 only, AP3 and AP4 also need to enter the remote MAC address of AP1 only). You can find the wireless MAC address of the access point in the management page under Status > Device Information.
The diagram below illustrates an example of the parameters configured when planning for WDS bridging. Each WDS supported access point is configured with a different IP address (blue) to prevent IP address conflict. The “wired router” is the only single DHCP server (gray) providing automatic IP address assignment for all client devices in the network. The WDS parameters required to match on all WDS supported access points in order to establish WDS wireless bridging is configured (blue). The wireless MAC of all devices is noted (red).
Creating a Wireless Bridge (WDS)

Wireless > Basic

Note: Since wireless bridge (WDS) is a subset of Access Point mode, please make sure that Access Point mode is selected under Main > Device Mode for all access points. See page 9 “Set your device to access point mode.” This procedure can apply for both WDS and WDS+AP modes.

To configure a wireless bridge (WDS) between two TEW-814DAP access points:

- Make note of the wireless MAC address of both access points. See page XX for checking the status page.
  
  Example:
  
  **AP1 (Access Point 1) 5GHz Wireless MAC Address:** 00:11:22:AA:BB:C2
  
  **AP2 (Access Point 2) 5GHz Wireless MAC Address:** 00:11:22:AA:BB:C4
  
- Make sure the IP address on each WDS supported access point is different and on the same IP network/subnet. See page XX for changing access point IP address.
  
  Example:
  
  **AP1 (Access Point 1) IP Address Settings:** 192.168.10.100 / 255.255.255.0
  
  **AP2 (Access Point 2) IP Address Settings:** 192.168.10.99 / 255.255.255.0
1. Log into your access point management page (see “Access your access point management page” on page 7).
2. Click on Wireless, click on Basic.
3. Click the Mode drop-down list and select one of following WDS options.

- **WDS**: Select this option to establish wireless bridging only without broadcasting your wireless network name for client devices to connect. Please refer to the section Wireless Bridge (WDS) Mode page 17 for details on this mode.
- **WDS+AP (Recommended)**: Select this option to establish wireless bridging and broadcast your wireless network name for client devices to connect simultaneously. See page 23 for details. Please refer to the section Wireless Bridge (WDS) with Access Point (AP) Mode on page 19 for details on this mode.

4. Review the Bridge Setting section and press Save Settings.
• **802.11 n-mode**: Select the 802.11 mode you would like the wireless band to **operate on**.  
  Note: This device operates in 5GHz wireless mode, below options of 802.11n is based on 5GHz 802.11.  
  o **802.11a only**: Select this option if you only have 802.11a wireless devices.  
  o **802.11n only**: Select this option if you only have 802.11n wireless devices.  
  o **Mixed 802.11n and 802.11a**: Select this option if you will be using both 802.11n and 802.11a wireless devices.  
  o **802.11ac only**: Select this option if you only have 802.11ac wireless devices.  
  o **Mixed 802.11n and 802.11ac**: Select this option if you have both 802.11n and 802.11 ac wireless clients.  
  o **Mixed 802.11ac, 802.11n and 802.11a**: Default setting, select this option if you are uncertain what your wireless devices support.  

• **Wireless Channel**: 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 and the channel used must match on all WDS devices.  

• **Channel Width**: Select the appropriate channel width for your wireless network. This setting only applies to 802.11n. For greater 802.11n performance, select **Auto 20/40/80MHz** (Options: 20MHz or 20/40MHz (Auto)). It is recommended to use the default channel bandwidth settings and that similar setting is applied on all WDS devices.  

• **Remote AP Mac**: Enter the wireless MAC address of the remote WDS supported access point or router.  

• **Bridge Security**: Select and configure the wireless security to be used on the WDS connection. This setting must be applied on all WDS devices.
AP2 Configuration

1. Log into your access point management page (see "Access your access point management page" on page 9).
2. Click on Wireless, click on Basic.
3. Click the Mode drop-down list and select one of following WDS options.
   - **WDS**: Select this option to establish wireless bridging only without broadcasting your wireless network name for client devices to connect. Please refer to the section Wireless Bridge (WDS) Mode page 17 for details on this mode.
   - **WDS+AP (Recommended)**: Select this option to establish wireless bridging and broadcast your wireless network name for client devices to connect simultaneously. See page 23 for details. Please refer to the section Wireless Bridge (WDS) with Access Point (AP) Mode on page 19 for details on this mode.
4. Review the Bridge Setting section and press Save Settings.
• **802.11 n-mode**: Select the 802.11 mode you would like the wireless band to **operate on**.
  Note: This device operates in 5GHz wireless mode, below options of 802.11n is based on 5GHz 802.11.
  - **802.11a only**: Select this option if you only have 802.11a wireless devices.
  - **802.11n only**: Select this option if you only have 802.11n wireless devices.
  - **Mixed 802.11n and 802.11a**: Select this option if you will be using both 802.11n and 802.11a wireless devices.
  - **802.11ac only**: Select this option if you only have 802.11ac wireless devices.
  - **Mixed 802.11n and 802.11ac**: Select this option if you have both 802.11n and 802.11ac wireless clients.
  - **Mixed 802.11ac, 802.11n and 802.11a**: Default setting, select this option if you are uncertain what your wireless devices support.

• **Wireless Channel**: 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 and the channel used must match on all WDS devices.

• **Channel Width**: Select the appropriate channel width for your wireless network. This setting only applies to 802.11n. For greater 802.11n performance, select **Auto 20/40/80MHz** (Options: 20MHz or 20/40MHz (Auto)). It is recommended to use the default channel bandwidth settings and that similar setting is applied on all WDS devices.

• **Remote AP Mac**: Enter the wireless MAC address of the remote WDS supported access point or router.

• **Bridge Security**: Select and configure the wireless security to be used on the WDS connection. This setting must be applied on all WDS devices.

**Bridging additional WDS supported devices**

For a point-to-multipoint (hub and spoke) WDS configuration, the AP2 (spoke) configuration procedure in the previous section “Creating a Wireless Bridge” page 23 can be used when creating additional WDS bridges to AP1 (hub).

For multiple point-to-point wireless WDS bridge links, you can follow the entire configuration procedure in the previous section “Creating a Wireless Bridge” on page 23.

The TEW-814DAP can support up to 8 wireless WDS bridge connections.
**Client**

Client mode allows the device to act as a wireless client device to connect to your wireless network and bridge the wireless connection from the wireless network to the LAN port located on the back of the device. Client devices with wired network capability such as in a media or entertainment center (ex. Smart TV, Game Console, DVR, etc.) can connect to one of the available LAN port using an Ethernet cable to establish wired connectivity to your network.
Set the device to client bridge mode

Main > Device Mode

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click the Main and Device Mode. Next to Operation Mode select Client on the drop-down list.

![Device Mode](image)

4. To save changes, click Save Settings.

Configure Client mode

Wireless > Site Survey

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on Wireless and click on Site Survey.
3. Search for your wireless network to connect in the wireless network list. In the Select column, click the radio button to select your wireless network.

![Site Survey](image)

4. At the bottom, click Next to connect and copy the settings of the selected wireless network.
5. If your wireless network requires wireless security, you will be prompted to enter your wireless key. Enter your Wireless Key required to connect to your existing wireless network and click Connect.
6. Click **Finish** and wait for the device to apply the settings.

![](image)

7. To verify the access point has successfully copied the settings and connected to your device, it may take up to 1 minute for your device to verify and display the connection status.

**Link Status**

*Status > Link Status*

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click the **Status** and **Link Status** to view the connection status of your access point in client mode.

   **Note:** If the **Link Status** does not display any information after 1 min, please re-attempt the procedure.

<table>
<thead>
<tr>
<th>Connected Time</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>832 seconds</td>
<td>00:14:d1:b1:8c:ee</td>
</tr>
</tbody>
</table>

- **Connected Time:** Time duration of how long the access point has been connected.
- **MAC Address:** MAC address of the access point is connected
**Wireless Range Extender (AP Repeater)**

Wireless range extender or repeater mode allows the device to extend the range of an existing wireless network. The existing wireless signal can be broadcasted from your wireless router or other access point. In addition, other network enabled devices can connect to your network using the Ethernet LAN port. The functionality of this mode is similar to WDS with Access Point however, wireless range extender mode does not require the other wireless device to support repeater or WDS and can only function using one band at a time, 2.4GHz or 5GHz and other modes cannot be used simultaneously.
Set the device Repeater mode

Operation Mode

1. Log into your access point management page (see “Access your access point management page” on page 7).
2. Click the Main and Device Mode, next to Device Operation Mode section drop-down list select AP Repeater.

3. Select the Repeater Mode to use and click Apply.

Wireless > Site Survey

1. Log into your access point management page (see “Access your access point management page” on page 7).
2. Click on Wireless and click on Site Survey.
3. Search for your wireless network to extend or repeat in the wireless network list. In the Select column, click the radio button to select your wireless network.

4. At the bottom, click Next to connect and copy the settings of the selected wireless network.
5. If your wireless network requires wireless security, you will be prompted to enter your wireless key. Enter your Wireless Key required to connect to your existing wireless network and click Next.

6. You have the option to broadcast the selected wireless network name (SSID) or assign the access point a different wireless network name (SSID) of the repeated signal. To change the wireless network name uncheck the option.
Advanced Access Point Setup

MAC Address Filters

Access > MAC Filters

Every network device has a unique, 12-digit MAC (Media Access Control) address. Using MAC filters, you can allow or deny specific computers and other devices from using this access point’s wireless network. You can enter up to 24 MAC address entries.

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on Access, click on MAC Filters.
3. Review the MAC Filter options, click Save Settings to save settings.

Click the Configuring MAC Filtering below drop-down list to choose the MAC filter function.

- Turn MAC Filtering OFF: disables the MAC address filter.
- Turn MAC Filtering ON and ALLOW computers listed to access the network Only Allow computers/devices with MAC addresses listed to access the access point management page and the Internet. Deny all others. Turn MAC Filtering ON and DENY computers listed to access the network Only Deny computers/devices with MAC addresses listed to access to the access point management page and the Internet. Allow all others.

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

Before saving settings, add the MAC addresses to the MAC Table and configure the options first.

- **MAC Address:** Enter the MAC address of the devices you would like to filter. (e.g. 00:11:22:AA:BB:CC)

  **Note:** If you uncertain of the device MAC address, please refer to your computer or device documentation to find the MAC address.

- **Schedule:** Select from the pull down menu a schedule of when to apply the MAC filter rule, or click Add New to add a new schedule.

3. Review the User Limit options, click **Save Settings** to save settings.

- **Enable User Limit:** Select this option to turn on user limit feature
- **User Limit:** Enter the amount of users you would like to allow on your wireless network.

**Change your access point login password**

Main > Password

1. Log into your access point management page (see “**Access your access point management** page” on page 8).
2. Click on Main, and click on Password.
3. Under the Password section, in the Password field, enter the new password. Click **Save Settings** to apply changes.

  **Note:** If you change the access point login password, you will need to access the access point management page using the User Name “admin” and the new password.

**Change your device name**

Main > Password

1. Log into your access point management page (see “**Access your access point management** page” on page 8).
2. Click on **Main**, and click on **Password**.

3. Under the **Device Name Settings** section, in the **Device Name** field, enter the new device name to display on your network to identify the access point. Click **Save Settings** to apply changes.

**Note:** The access point’s device name is used to access the device using the URL feature. If changed the device name you will need to access your access point management page using your new access point IP address. *(e.g. Instead of using the default login URL [http://tew-814DAP](http://tew-814DAP))*

### IPv6 Connection Settings

**Main > 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**

1. Log into your access point management page (see “[Access your access point management page](#)” on page 8).
2. Click on **Main**, and click on **IPv6**.
3. Select the IPv6 connection type to assign IPv6 addressing to the access point.

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

**LAN IPv6 Address Settings**

Use this section to configure the internal network settings of your AP. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the web-based management interface.

**LAN IPv6 Link-Local Address:** Current IPv6 address applied to your access point.

### Change your access point IP address

**Main > Network Settings**

Typically, the access point IP address settings only needs to be changed when connecting the access point to your network and configuring to the device to be in the same IP network as your existing network.

Default Access Point IP Address Settings: 192.168.10.100 / 255.255.255.0

1. Log into your access point management page (see “[Access your access point management page](#)” on page 8).
2. Click on **Main**, and click on **Network Settings**.
3. Under **Connection Type**, click the drop-down list to select the access point IP address settings.
- **Dynamic IP (DHCP):** Choose the option to set the access point to automatically obtain IP address settings from a DHCP server.  
  *Note:* Typically, your network router has a built-in DHCP server.

- **Static IP:** Choose this option to manually configure the IP address settings of the access point.

  **Static IP Address LAN Connection Type**
  
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.10.100</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway Address</td>
<td>0.0.0</td>
</tr>
<tr>
<td>Primary DNS Server</td>
<td>0.0.0</td>
</tr>
<tr>
<td>Secondary DNS Server</td>
<td>0.0.0</td>
</tr>
</tbody>
</table>

- **IP Address:** Enter the new access point IP address. (e.g. 192.168.0.100)
- **Subnet Mask:** Enter the new access point subnet mask. (e.g. 255.255.255.0)
- **Gateway Address:** Enter the default gateway address of your network. This parameter is required for the access point to access Internet for functions such as e-mail notifications.  
  *Note:* Typically, your network router IP address is used as the default gateway address to access the Internet e.g. 192.168.10.1)

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

  *Note:* You will need to access your access point management page using your new access point IP address. (e.g. Instead of using the default http://192.168.10.100 your new access point IP address will use the following format using your new IP address http://(new.ipaddress.here) to access your access point management page. You can also use the default login URL http://tew-814DAP

Your access point can be used as a DHCP (Dynamic Host Configuration Protocol) server to automatically assign an IP address to each wireless device connected. The DHCP server settings can be accessed when access point is set to Static IP address and it is disabled by default.

- **Enable DHCP Server:** Select to enable DHCP server.
- **DHCP IP Address Range:** Enter the range of IP addresses to assign through the access point’s DHCP server.
- **Always Broadcast:** Select to enable the access point DHCP server.
- **Gateway:** Assign a gateway IP address to use.
- **WINS:** Assign a WINS IP address to use.
- **DNS:** Assign DNS IP address to use.
- **DHCP Lease Time:** Select the DHCP lease time allowed.

### Set your date and time

**Main > Time**

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on **Main**, and click on **Time**.
3. Review the Time settings. Click **Apply** to save settings.
• **Time**: Displays the current device time and date information.
• **Enable NTP Server**: Select this option to set your router date and time to synchronize with an NTP (Network Time Protocol) server address (e.g. pool.ntp.org). Enter the NTP server address next to Default NTP server, (e.g. pool.ntp.org). Click the **Time Zone** drop-down list to select the appropriate zone and you can optionally change your NTP Sync period.
• **NTP Server**: Enter the NTP server address you would like to use. Click **Update Now** to update time settings.
• **Enable Daylight Saving**: Check the option to configure the DST settings. Set the annual range when daylight saving is activated.

  **Note**: NTP servers are used for computers and other network devices to synchronize time across an entire network.

• **Manually set time**: Set your router date and time manually in the Date and Time Settings section. Click **Copy Your Computer’s Time Settings** if you would like to copy your computer’s time settings.

---

### Create schedules
**Tools > Schedule**

For additional security control, your router allows you to create schedules to specify a time period when a feature on your access point should be activated and deactivated.

1. Log into your access point management page (see "Access your access point management page" on page 8).
2. Click on **Main**, and click on **Time**.
3. Review the Schedule settings. Click **Apply** to save settings.

• **Name**: Enter a name for the schedule you would like to apply.
• **Days**: Check the days you would like the rule to be applied or select **All Week** to enable the rule all week.
• **Time format**: Select from the pull down menu the time format to use.
• **Start/End Time**: Select the start and end time you would like the schedule to follow.

**Note**: The schedule defined will define the time/day the feature will be activated.
Access Point Maintenance & Monitoring

Reset your Access Point to factory defaults
Tools > Settings Management
You may want to reset your access point to factory defaults if you are encountering difficulties with your access point and have attempted all other troubleshooting. Before you reset your access point to defaults, if possible, you should backup your access point configuration first, see “Backup and restore your access point configuration settings” on page 35.

There are two methods that can be used to reset your access point to factory defaults.
- **Reset Button** – Located on the rear panel of your access point, see “Product Hardware Features” on page 2. Use this method if you are encountering difficulties with accessing your access point management page.

  OR

- **Access Point Management Page**
  1. Log into your access point management page (see “Access your access point management page” on page 8).
  2. Click on **Tools** and click on **Settings Management**.
  3. Under Restore Factory Default Settings section, click **Restore Default**. When prompted to confirm this action, click **OK**.

<table>
<thead>
<tr>
<th>Access Point Default Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administrator User Name</strong></td>
</tr>
<tr>
<td><strong>Administrator Password</strong></td>
</tr>
<tr>
<td><strong>Access Point Default URL</strong></td>
</tr>
<tr>
<td><strong>Access Point IP Address</strong></td>
</tr>
<tr>
<td><strong>Access Point Subnet Mask</strong></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
</tr>
<tr>
<td><strong>Wireless</strong></td>
</tr>
<tr>
<td><strong>Wireless Network Name/Encryption</strong></td>
</tr>
<tr>
<td><strong>Wireless Multiple SSID</strong></td>
</tr>
</tbody>
</table>

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

To backup your access point configuration:
1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on **Tools** and click on **Settings Management**.
3. Next to **Save Settings** section, click **Save**.
4. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: config.bin)

To restore your access point configuration:
1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on Tools and click on Settings Management.
3. Next to Restore Configuration Settings, depending on your web browser, click on Browse or Choose File.
4. A separate file navigation window should open.
5. Select the access point configuration file to restore and click Load. (Default Filename: config.bin). If prompted, click Yes or OK.
6. Wait for the access point to restore settings.

Reboot your access point

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

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

- **Turn the access point off** for 10 seconds using the access point On/Off switch located on the rear panel of your access point or disconnecting the power port, see “Product Hardware Features” on page 2. Use this method if you are encountering difficulties with accessing your access point management page. This is also known as a hard reboot or power cycle.

- **Access Point Management Page** – This is also known as a soft reboot or restart.

4. Wait for the device to reboot.

Upgrade your access point firmware

Tools > Upload Firmware

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

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

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

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

3. Log into your access point management page (see “Access your access point management page” on page 8).

4. Click on **Tools** and click on **Upload Firmware**.

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

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

7. Click **Apply**. If prompted, click **Yes** or **OK**.

### Ping test

**Tools > Ping Test**

Your access point offers a ping test tool that allows you to use and verify connectivity.

1. Log into your access point management page (see “Access your access point management page” on page 8).

2. Click on **Tools**, and click on **Ping Test**.

3. Under Host Name or IP address section, enter the hostname (ie TRENDnet.com) or IP address (ie. 192.168.10.100) and click **Ping**.

### View your access point log

**Status > Log**

Your access point statistics can provide a quick overview of the access point’s status.

1. Log into your access point management page (see “Access your access point management page” on page 8).

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

3. Under **Log Options** section, select the log types you would like to be displayed.

4. Click **Apply Log Settings Now** to save settings.
First Page: Click to advance to the first log page
Last Page: Click to advance to the last log page
Previous Page: Click to view the previous log page
Next Page: Click to view the next log page
Clear Log: Click to clear all log entries
Refresh: Click to refresh log entries

5. To save log entries click Save Log button.

Email logs
Tools > Email settings
Your access point can email you log entries.
1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on Tools, and click on Email Settings.
3. Under Enable section, select the option to enable email logging.
4. Review the Email setting section and click Save Settings to Apply.

From Email Address: Enter the recipient email address to use
To Email Address: Enter the email address to send the logs
Email Subject: Enter the email subject to use when logs are sent
SMTP Server Address: Enter the SMTP server address of the email address used
SMTP Port: Enter the SMTP port used on the email address
Enable Authentication: Select this option to authenticate the email address
Account Name: Enter the account name used on the email address
Password: Enter the password of the email address used.

Wireless Client List
Status > Wireless Client
You can view the list of active wireless devices currently connected to your access point.
1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on Status, and click on Wireless Client.
Check the access point system information

You may want to check the system information of your access point such as IP address settings, access point mode, wireless and wired network settings, access point wireless MAC addresses, and firmware version.

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on Status and click on Device Info.

Device Info

- **Connected Time:** Displays the duration time of your wireless client
- **MAC Address:** Displays the current MAC address of your wireless client.

<table>
<thead>
<tr>
<th>Number Of Wireless Clients - 2.4GHz Band:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Time</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number Of Wireless Clients - 5GHz Band:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Time</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

**LAN Information**

- **Device Mode:** Current operating mode access point is set.
- **MAC Address:** Displays the current Ethernet wired interface MAC address.
- **Connection:** LAN IP set to the access point
- **IP Address:** The current IP address settings assigned to your access point.
- **Subnet Mask:** The current subnet mask assigned to your access point.
- **Default Gateway:** The current gateway assigned to your access point.

<table>
<thead>
<tr>
<th>LAN Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Mode</td>
</tr>
<tr>
<td>MAC Address</td>
</tr>
<tr>
<td>Connection</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Subnet Mask</td>
</tr>
<tr>
<td>Gateway Address</td>
</tr>
</tbody>
</table>

**2.4GHz Wireless**

- **MAC Address:** The MAC address of your access point’s 5GHz wireless LAN or interface configuration.
- **SSID:** Displays the SSID applied to the access point.
- **Security Mode:** Displays the wireless security type applied to your wireless network.
- **Channel Width:** Current operating channel width set on the access point.
- **Channel:** Displays the current 5GHz wireless channel your access point is operating.

<table>
<thead>
<tr>
<th>WLAN 2.4GHz Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
</tr>
<tr>
<td>SSID</td>
</tr>
<tr>
<td>Security Mode</td>
</tr>
<tr>
<td>Channel Width</td>
</tr>
<tr>
<td>Channel</td>
</tr>
</tbody>
</table>
5GHz Wireless

<table>
<thead>
<tr>
<th>WLAN 5GHz Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>D8:FE:E3:3E:AC:FC</td>
</tr>
<tr>
<td>SSID</td>
<td>814_mediatest5</td>
</tr>
<tr>
<td>Security Mode</td>
<td>WPA2</td>
</tr>
<tr>
<td>Channel Width</td>
<td>Auto 20/40/80MHz</td>
</tr>
<tr>
<td>Channel</td>
<td>153</td>
</tr>
</tbody>
</table>

- **MAC Address**: The MAC address of your access point’s 5GHz wireless LAN or interface configuration.
- **SSID**: Displays the SSID applied to the access point.
- **Security Mode**: Displays the wireless security type applied to your wireless network.
- **Channel Width**: Current operating channel width set on the access point.
- **Channel**: Displays the current 5GHz wireless channel your access point is operating.

IPv6 Status

**Status > IPv6**

You can view the current IPv6 status on your access point.

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on **Status**, and click on **IPv6**

<table>
<thead>
<tr>
<th>IPv6 Status</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Connection Type</td>
<td>Link-local Only</td>
</tr>
<tr>
<td>LAN IPv6 Address</td>
<td>NONE</td>
</tr>
<tr>
<td>IPv6 Default Gateway</td>
<td>NONE</td>
</tr>
<tr>
<td>LAN IPv6 Link-Local Address</td>
<td>fe80::de:43ff:fe3e:b04d/64</td>
</tr>
<tr>
<td>Primary DNS Address</td>
<td>NONE</td>
</tr>
<tr>
<td>Secondary DNS Address</td>
<td>NONE</td>
</tr>
</tbody>
</table>

- **IPv6 Connected Type**: Displays the IPv6 connection type assigned to your access point.
- **LAN IPv6 Address**: Displays the IPv6 IP address assigned to your access point.
- **IPv6 Default Gateway**: Displays the IPv6 default gateway assigned to your access point.
- **LAN IPv6 Link-Local Address**: Displays the link-local address of the access point.
- **Primary/Secondary IPv6 DNS Server**: Displays the IPv6 DNS server addresses assigned to your access point.

**View your access point statistics**

**Status > Statistics**

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

1. Log into your access point management page (see “Access your access point management page” on page 8).
2. Click on **Status**, and click on **Statistics**.

<table>
<thead>
<tr>
<th>LAN Statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sent</td>
<td>117228</td>
</tr>
<tr>
<td>TX Packets Dropped</td>
<td>0</td>
</tr>
<tr>
<td>Collisions</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wireless Statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sent</td>
<td>76700</td>
</tr>
<tr>
<td>TX Packets Dropped</td>
<td>0</td>
</tr>
<tr>
<td>Collisions</td>
<td>0</td>
</tr>
</tbody>
</table>
Access Point Management Page Structure

Main
- Wizard
- Device Mode
  - Access Point
  - Client
  - AP Repeater
- Network Settings
  - DHCP
  - Static
  - DHCP Server
- Password
  - Device Name
- Time
- IPv6

Wireless
- Basic
  - Access Point
  - WDS
  - WDS + AP
  - Security
- Advanced
- Security
  - MAC Filter
- WPS (Wi-Fi Protected Setup)

Access
- IPv6

Tools
- MAC Filter
- Multi-SSID
- User Limit
- Management
  - Password
- Upload Firmware
- Settings Management
  - Export settings
  - Restore settings
  - Load factory default
  - Reboot
- Ping Test
- Schedule
- Email Settings
- Syslog
- Logout
Troubleshooting

Q: I typed http://tew-814DAP in my Internet Browser Address Bar, but an error message says “The page cannot be displayed.” How can I access the access point management page?

Answer:
Assign your computer a static IP address in the subnet of 192.168.10.x (ex. 192.168.10.25) and access the access point using the default IP address 192.168.10.100. http://192.168.10.100

Q: I typed http://192.168.10.100 in my Internet Browser Address Bar, but an error message says “The page cannot be displayed.” How can I access the access point management page?

Answer:
1. Check your hardware settings again. See “Basic Installation” on page 5.
2. Make sure the LAN port you are connected to is on.
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 access point’s LAN port
5. Press on the factory reset button for 15 seconds, the release.

Windows 7
a. Go into the Control Panel, click Network and Sharing Center.
b. Click Change Adapter Settings, right-click the Local Area Connection icon.
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: The Wizard does not appear when I access the access point. What should I do?
Answer:
1. Click on Main and Wizard on the left hand side.
2. Near the top of the browser, “Pop-up blocked” message may appear. Right click on the message and select Always Allow Pop-ups from This Site.
3. Disable your browser’s pop up blocker.

Q: I cannot connect wirelessly to the access point. What should I do?
Answer:
1. Double check that the Wireless LED on the access point is on.
2. Power cycle the router. Unplug the power to the access point. Wait 15 seconds, then plug the power back in to the access point.
3. Contact the manufacturer of your wireless network adapter and make sure the wireless network adapter is configured with the proper SSID. The default predefined SSID is printed on the device label on the bottom or on the sticker on the side of the unit.
4. To verify whether or not wireless is enabled, login to the access point management page, click on Basic and Wireless.
5. Please see “Steps to improve wireless connectivity” on page 14 if you continue to have wireless connectivity problems.
Appendix

How to find your IP address?

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

Command Prompt Method

Windows 2000/XP/Vista/7/8
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 X 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 X 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.

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
a. Go into the Control Panel, click Network and Sharing Center.
b. Click Change Adapter Settings, right-click the Local Area Connection icon.
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 configure your network settings to use a static 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.

Windows 7/8
   a. Go into the Control Panel, click Network and Sharing Center.
   b. Click Change Adapter Settings, right-click the Local Area Connection icon.
   d. Then click Use the following IP address, and assign your network adapter a static IP address. 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 Use the following IP address, and assign your network adapter a static IP address. 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 Use the following IP address, and assign your network adapter a static IP address. 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.

How to find your MAC address?

In Windows 2000/XP/Vista/7/8,
   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**
1. Open Connect to a Network by clicking the network icon ( Rentals ) 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.
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 OK.

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

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

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

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24cm between the radiator & your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

RoHS
This product is RoHS compliant.
output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

<table>
<thead>
<tr>
<th>Language</th>
<th>Translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dansk [Danish]</td>
<td>Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-TEW-814DAP overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF, 2006/95/EF, og 2009/125/EF.</td>
</tr>
<tr>
<td>English</td>
<td>Hereby, TRENDnet, declares that this TEW-814DAP is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC, 2006/95/EC, and 2009/125/EC.</td>
</tr>
<tr>
<td>Español [Spanish]</td>
<td>Por medio de la presente TRENDnet declara que el TEW-814DAP cumple con los requisitos esenciales y las demás disposiciones aplicables o exigibles de la Directiva 1999/5/CE, 2006/95/CE, y 2009/125/CE.</td>
</tr>
<tr>
<td>Italiano [Italian]</td>
<td>Con la presente TRENDnet dichiara che questo TEW-814DAP è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE, 2006/95/CE e 2009/125/CE.</td>
</tr>
</tbody>
</table>
### Limited Warranty

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

<table>
<thead>
<tr>
<th>Product</th>
<th>Warranty Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>TEW-814DAP</td>
<td>3 Years Warranty</td>
</tr>
<tr>
<td>AC/DC Power Adapter, Cooling Fan, and Power Supply</td>
<td>1 year warranty</td>
</tr>
</tbody>
</table>

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

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

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual. Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

### WARRANTIES EXCLUSIVE

If the TRENDnet product does not operate as warranted above, the customer’s sole remedy shall be, at TRENDnet’s option, repair or replace. The foregoing warranties and remedies are exclusive and are in lieu of all other warranties, expressed or implied, either in fact or by operation of law, statutory or otherwise, including warranties of merchantability and fitness for a particular purpose. TRENDnet neither assumes nor authorizes any other person to assume for it any other liability in connection with the sale, installation maintenance or use of TRENDnet’s products.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER’S OR ANY THIRD PERSON’S MISUSE, 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").

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

© Copyright 2015 TRENDnet. All Rights Reserved.
Product Warranty Registration

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

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA

Copyright ©2015. All Rights Reserved. TRENDnet.