# Table of Contents

## Product Overview
- Package Contents ................................................. 1
- Features .......................................................... 1
- Front Panel ....................................................... 3
- Mounting Holes .................................................. 3
- Connectors ......................................................... 3
- Product Preset Information ..................................... 4
- Mounting Accessories .......................................... 4

## Hardware Installation
- Mount on Wall or Ceiling ...................................... 5
- Mount on T-Bar .................................................... 5
- Wireless Performance Considerations ...................... 6

## Operation Modes
- Access Point ...................................................... 6
- Client Bridge ..................................................... 7
- Repeater .......................................................... 7
- Wireless Distribution System ................................. 8

## System configuration
- System Management and Default Settings .................. 9
- Log-in System Management for the First Time ............ 9

## Setup Wizard .................................................. 12
- Save/Reload ...................................................... 13
- Status ............................................................ 14
- System ........................................................... 19
- 2.4G Wireless ................................................... 23
- 5G Wireless ..................................................... 33
- Management ...................................................... 42

## Appendix
- WDS Frequent Asked Questions ............................... 53
- Federal Communication Commission Interference Statement .... 54
- Europe – EU Declaration of Conformity ........................ 55
- RoHS ............................................................. 55
- Limited Warranty ............................................... 57
Product Overview

**Features**
TRENDnet’s N600 Dual Band PoE Access Point, model TEW-753DAP, is a feature rich business class access point with proven concurrent 300 Mbps dual band wireless technology. A variety of installation scenarios are supported with Access Point, WDS AP, WDS Bridge, and Repeater modes. Save installation time and costs with PoE.

**Quick Setup**
Get up and running in minutes with the intuitive guided setup

**Low Profile**
Off white low profile smoke detector shape blends into most environments

**Power over Ethernet (PoE)**
Save installation time and costs with a PoE (Optional power port for non-PoE installations)

**LED Control**
Disable diagnostic LEDs to further reduce visual attention

**Concurrent Dual Band**
Proven concurrent 300 Mbps* dual band wireless n

**Gigabit Port**
Gigabit port maintains high performance connection to network

**Wireless Coverage**
Increased coverage with MIMO technology

**Backward Compatible**
Compatible older wireless g devices

---

**Package Contents**

TEW-753DAP package includes:

- TEW-753DAP
- Multi-Language Quick Installation Guide
- CD-ROM (User’s Guide)
- Network cable (1.5 m/5 ft.)
- Power adapter (12 V DC, 1.25 A)
- Installation 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.
Operation Modes
Independently set each band to Access Point, WDS AP, WDS Bridge, WDS Station, Client Bridge or Repeater mode

IPv6
IPv6 support

AP Scan
Integrated wireless scan function helps optimize wireless setup

SSIDs
Up to 8 SSIDs per band (16 total) with isolation support

Traffic Shaping
Allocate bandwidth to each wireless SSID

System Logs
Eight system log filters aid network troubleshooting

Spanning Tree
Configurable spanning tree controls

SNMP
Extend network monitoring to this device with SNMP support

Encrypted Wireless
Support for encryption up to WPA2

VLAN Management
Up to eight SSIDs per band with VLAN management support

Network Access
Create MAC filter tables to reduce network access risk

*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.
Front Panel

- **Reset Button**
  - Push and hold for 2 seconds to reset TEW-753DAP
  - Push and hold for more than 10 seconds to reset configuration to factory default

- **Power LED**
  - OFF: Powered off or LED display is disabled
  - ON: Powered on

- **Network LED**
  - Orange: 10/100
  - Green: Giga bit
  - OFF: No network connected through Ethernet port (PoE) or LED display has been disabled
  - ON: Network connected through Ethernet port (PoE)
  - Flashing: Network activities are detected on Ethernet (PoE) port

- **Wireless LED**
  - Orange: 2.4GHz
  - Green: 5GHz
  - OFF: No wireless network connection or LED display is disabled
  - Flashing: Wireless network activities are detected

Mounting Holes

- **Mounting holes**
- **Kensington security slot**

Connectors

- **Gigabit PoE Port**
- **DC Power 12V DC 1.25A (Optional)**
**Product Preset Information**

There are two preset product labels comes with the package. The first label is located on plastic wrapping of TEW-753DAP. The second label is located on the bottom of the TEW-753DAP. You can find default SSID, wireless key, administrator account, and administrator password there. The default static management IP is 192.168.10.100.

**Mounting Accessories**

The mounting accessories are provided for easier hardware installation, including two sets of T-Bar clips, two sets of screws, and a set of spacers.

- 15/16” T-Bar Clips
- 9/16” T-Bar Clips
- P2.6 * 10 Screws
- P2.6 * 25 Screws
- Spacers
Hardware Installation

Mount on Wall or Ceiling
Use two P3.5 pan head screws to hold the TEW-753DAP. The distance between mounting points is 2 3/4” (7cm)

Mount on T-Bar
Two additional bronze screw holes are provided for T-Bar mounting. Use two P2.6 screws to secure the TEW-753DAP on T-Bar clip and then clip on the T-Bar.
Wireless Performance Considerations

There are a number of factors that can impact the range of wireless devices. Adjust your wireless devices so that the signal is traveling in a straight path, rather than at an angle. The more material the signal has to pass through the more signal you will lose. 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.

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

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

Any device operating on the 2.4GHz frequency will cause interference. Devices such as 2.4GHz cordless phones or other wireless remotes operating on the 2.4GHz frequency can potentially drop the wireless signal. Although the phone may not be in use, the base can still transmit wireless signal. Move the phone’s base station as far away as possible from your wireless devices.

Adjust the wireless power setting on your AP if you have more than one AP covering a large area. Covering only the neighbor hop APs in wireless range is a good design. Covering more than neighbor APs will experience wireless interference and slow down the communication.

Operation Modes

There are four operating modes provided by TEW-753DAP, Access Point, Client Bridge, WDS and Repeater. Configure the TEW-753DAP to different operation mode which service the best in your network.

Access Point

This is the default operation mode. TEW-753DAP service wireless end points in this mode. You can setup local or remote wireless authentication, setup up to 8 sets of SSIDs in 2.4GHz band and 5GHz band, total 16 SSIDs and separate SSID or STA traffic.

• Total 16 SSIDs (8 SSIDs per band) for different users grouping
• Selectable SSID or station (wireless client) isolation
Client Bridge
When Client Bridge mode is set to 2.4GHz or 5GHz interface of TEW753DAP, this interface functions as a wireless client connecting to any AP dynamically (channels and encryptions). The interface bridges the traffic to the Ethernet and the other wireless interface.

- Connects to any 802.11 wireless AP
- Connects two networks wirelessly

Repeater
When Repeater Mode is selected, the selected wireless interface functions as a wireless repeater and is able to repeat the wireless signal of an access point. This feature is used to expand your existing wireless network on places your current access point is unable to reach. Make sure all the settings on selected interface of the TEW-753DAP matches the wireless access points you want to repeat in same wireless settings including SSID, channel and wireless encryption settings.
**Wireless Distribution System**

**Deploy ONLY multiple TEW-753DAPs in a single DS (distribution system). WDS may not work with other products due to its non-standard nature.**

WDS mode is a non-standard extension to the IEEE 802.11 standard to allow transparent Ethernet bridging on the station and to implement seamless hand-over for wireless clients roaming between different access points. Transparent bridge is also one of the requirements to some layer 2 services such as DHCP and 802.1X authentication. Because the WDS implementation is different from product to product, not all WDS enabled products are interoperable. You have to use multiple TEW-753DAP to build your mesh wireless DS or transparent bridge.

You can set up TEW-753DAP on different WDS modes for your different network planning.

**WDS Bridge:** In this mode, the selected interface wirelessly communicates with other WDS bridges to make a wireless backbone. You can make a simple mesh network with these WDS bridges. To build a WDS link, you have to list the neighbor’s BSSID (the MAC address) as the next hop packet forwarding. Your neighbor, vice versa, has to list your BSSID (the MAC Address) as its next hop. Make sure all access points are configured with the same SSID as a single DS (distribution system), wireless channel and wireless encryption settings have to be the same as well.

**WDS Access Point:** WDS AP is an outlet of a DS. Pairing with a WDS Station you can build a transparent bridge between two DS or from DS to STA. (See more information in “Appendix” on page 53)

**WDS Station:** Pair with WDS AP, you can build a transparent bridge for layer 2 requirements. (See more information in “Appendix” on page 53)
System configuration

System Management and Default Settings

If you have a brand new out of box TEW-753DAP or if you just reset TEW-753DAP to factory defaults by pressing and holding reset button for over 10 seconds, your TEW-753DAP has following settings:

Management IP : 192.168.10.100
Administrator name : admin
Administrator password : admin
Default SSID : (printed on pre-set label)
Default SSID passphrase : (printed on pre-set label)

Log-in System Management for the First Time

1. Power on your TEW-753DAP by connecting PoE cable to a PoE switch or plug-in the power adapter comes with the package. The power LED will turned on.

2. Search for available wireless connections in your computer’s network settings. The default SSID of the TEW-735AP is shown on the preset label. The default wireless security settings are set to WPA2 and the passphrase is printed on the preset label and device label.

Or,
Connect a network cable from your computer to the TEW-753DAP network port.
3. Open a web browser and type `http://tew-753DAP` to access web administration page.

If you have a static IP set on your PC, please open a web browser and enter `http://192.168.10.100` The TEW-735AP login page will appear.

Enter administrator login information (The default user name is `admin` and password is `admin`)

* Please reference the troubleshooting section if you cannot access administration web page.

4. Change your administration login password away from factory default setting. Click Next to continue.

5. Change the management IP address for the TEW-753DAP if necessary. Click Apply.
6 Click **Save/ Reload** on top of the menu and then click **Save & Apply**.

7 TEW-753DAP will apply password change and then reboot. Login again with your new password.

* Make sure you are still connecting to TEW-753DAP after reboot if you wireless connects to TEW-753DAP.
Setup Wizard

Setup wizard is provided as part of the web configuration utility. It sets up the basic administrator password and management IP address by clicking on the Wizard button on the function menu. The following screen will appear.

1. Enter your new administrator password and then click Next to continue.

2. Enter the management IP address for this TEW-753DAP. The default IP address is 192.168.10.100. Set it up in your network management subnet with a unique IP address. You can leave it set on default IP if you have only one TEW-753DAP on network. Click Apply.
3. Click **Save/ Reload** on top of the menu and then click **Save & Apply**.

![Save/Reload screenshot](image)

4. TEW-753DAP will apply password change and then reboot. Login again with your new password.

![Processing screenshot](image)

* Make sure you are still connecting to TEW-753DAP after reboot if you wireless connects to TEW-753DAP.

---

**Save/ Reload**

The TEW-753DAP is a commercial grade wireless access point. To make multiple network settings change at the same time and minimum the interruption of production network, all network configurations have to be changed in two stages.

When you change a network setting, the change command will be saved in a queue. When you finish all the setting changes, click **Save/Reload** on top of the listed menu. Review the list of commands on your change list. Click **Save & Apply** to apply the changes. If you want to cancel the changes, click **Revert**.

The number that follows **Save/ Reload** is a reminder that shows how many changes are in the queue waiting to be applied.
Status

Main status page shows TEW-753DAP’s basic information. Click Status then click Main to show the page.

### System Information

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Name of this device that is recognized by other network devices such as SNMP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet MAC Address</td>
<td>The MAC address of Ethernet Interface</td>
</tr>
<tr>
<td>2.4G Wireless MAC Address</td>
<td>The MAC address of each individual active SSID.</td>
</tr>
<tr>
<td>5G Wireless MAC Address</td>
<td>The MAC address of each individual active SSID.</td>
</tr>
<tr>
<td>Country</td>
<td>The country in which you are located.</td>
</tr>
<tr>
<td>Current Time</td>
<td>The current is important for schedule control and log accuracy.</td>
</tr>
<tr>
<td>Firmware version</td>
<td>Currently run firmware version</td>
</tr>
<tr>
<td>Management VLAN ID</td>
<td>The VLAN ID assigned to device management network. The default setting is untagged.</td>
</tr>
</tbody>
</table>
### LAN Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address</strong></td>
<td>IP address of the TEW-753DAP</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>Network range of IP address</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>The default route going further from TEW-753DAP subnet.</td>
</tr>
<tr>
<td><strong>Primary DNS</strong></td>
<td>Primary DNS server address</td>
</tr>
<tr>
<td><strong>Secondary DNS</strong></td>
<td>Secondary DNS server address</td>
</tr>
<tr>
<td><strong>DHCP Client</strong></td>
<td>DHCP client status. The IP address was statically set by default.</td>
</tr>
<tr>
<td><strong>Spanning Tree Protocol</strong></td>
<td>Spanning Tree Protocol is enabled or not.</td>
</tr>
<tr>
<td><strong>IPv6 IP Address</strong></td>
<td>The dual-stack IPv6 address of the TEW753DAP</td>
</tr>
<tr>
<td><strong>IPv6 Link-Local Address</strong></td>
<td>IPv6 link local address for auto-configuration</td>
</tr>
<tr>
<td><strong>IPv6 Default Gateway</strong></td>
<td>IPv6 default route going further from TEW-753DAP subnet.</td>
</tr>
<tr>
<td><strong>IPv6 Primary DNS</strong></td>
<td>Primary IPv6 DNS server address</td>
</tr>
<tr>
<td><strong>IPv6 Secondary DNS</strong></td>
<td>Secondary IPv6 DNS server address</td>
</tr>
<tr>
<td><strong>RX (packets)</strong></td>
<td>Received packets from Ethernet interface</td>
</tr>
<tr>
<td><strong>TX (packets)</strong></td>
<td>Transmitted packets from Ethernet interface</td>
</tr>
</tbody>
</table>

- **IP Address**: 10.10.10.100
- **Subnet Mask**: 255.255.255.0
- **Default Gateway**: 
- **Primary DNS**: 
- **Secondary DNS**: 
- **DHCP Client**: Disabled
- **Spanning Tree Protocol**: Disabled
- **IPv6 IP Address**: FE80::202:6FF:FE81:F706
- **IPv6 Link-Local Address**: FE80::202:6FF:FE81:F706
- **IPv6 Default Gateway**: 
- **IPv6 Primary DNS**: 
- **IPv6 Secondary DNS**: 
- **RX (Packets)**: 427,726 KB (2395 PKts.)
- **TX (Packets)**: 1,275,91 MB (1525 PKts.)
### Current Wireless Settings: 2.4GHz

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation Mode</strong></td>
<td>Shows which wireless mode the 2.4GHz interface is set to.</td>
</tr>
<tr>
<td><strong>Wireless Mode</strong></td>
<td>Shows which 802.11 wireless mode is set and running on the 2.4GHz interface.</td>
</tr>
<tr>
<td><strong>Channel Bandwidth</strong></td>
<td>Wireless Channel Bandwidth (20 or 40 MHz)</td>
</tr>
<tr>
<td><strong>Frequency/Channel</strong></td>
<td>Shows which 2.4GHz wireless channel (and frequency) is in use.</td>
</tr>
<tr>
<td><strong>Profile Settings</strong></td>
<td>Briefly shows wireless settings (SSID/Security/VID/802.1Q) on each SSID.</td>
</tr>
<tr>
<td><strong>Distance</strong></td>
<td>The distance setting for 2.4GHz wireless interface.</td>
</tr>
<tr>
<td><strong>RX (packets)</strong></td>
<td>Received packets by 2.4GHz wireless interface</td>
</tr>
<tr>
<td><strong>TX (packets)</strong></td>
<td>Transmitted packets from 2.4GHz wireless interface</td>
</tr>
</tbody>
</table>

### Current Wireless Settings: 5GHz

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation Mode</strong></td>
<td>Shows which wireless mode the 5GHz interface is set to.</td>
</tr>
<tr>
<td><strong>Wireless Mode</strong></td>
<td>Shows which 802.11 wireless mode is set and running on the 5GHz interface.</td>
</tr>
<tr>
<td><strong>Channel Bandwidth</strong></td>
<td>Wireless Channel Bandwidth (20 or 40 MHz)</td>
</tr>
<tr>
<td><strong>Frequency/Channel</strong></td>
<td>Shows which 5GHz wireless channel (and frequency) is in use.</td>
</tr>
<tr>
<td><strong>Profile Settings</strong></td>
<td>Briefly shows wireless settings (SSID/Security/VID/802.1Q) on each SSID.</td>
</tr>
<tr>
<td><strong>Distance</strong></td>
<td>The distance setting for 5GHz wireless interface.</td>
</tr>
</tbody>
</table>
### 2.4G Wireless Client List

This page shows all wireless clients connected to the 2.4GHz interface.

<table>
<thead>
<tr>
<th>SSID : #</th>
<th>Shows the SSID that clients are associated with and their client number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address :</td>
<td>MAC address of wireless client</td>
</tr>
<tr>
<td>TX (Bytes) :</td>
<td>Transmitting data statistics</td>
</tr>
<tr>
<td>RX (Bytes) :</td>
<td>Receiving data statistics</td>
</tr>
<tr>
<td>RSSI (dBm) :</td>
<td>Received Signal Strength Indication: Signal strength of this wireless client</td>
</tr>
<tr>
<td>Kick and Ban :</td>
<td>Click this button to send this client to MAC address filter list. Click OK when you see this prompt. <em>(Save/Reload is required to apply change.)</em></td>
</tr>
</tbody>
</table>

**Refresh :** Click this button to refresh the list.
### 5G Wireless Client List

This page shows all wireless clients connected to the 2.4GHz interface.

<table>
<thead>
<tr>
<th>SSID</th>
<th>MAC Address</th>
<th>TX (Bytes)</th>
<th>RX (Bytes)</th>
<th>RSSI(dBm)</th>
<th>Kick and Ban</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID1</td>
<td>00:17:0c:00:17:0c</td>
<td>9904</td>
<td>35380</td>
<td>-38</td>
<td>Kick and Ban</td>
</tr>
<tr>
<td>SSID2</td>
<td>00:23:6c:00:23:6c</td>
<td>9940</td>
<td>57300</td>
<td>-22</td>
<td>Kick and Ban</td>
</tr>
</tbody>
</table>

- **SSID:** Shows the SSID that clients are associated with and their client number.
- **MAC Address:** MAC address of wireless client
- **TX (Bytes):** Transmitting data statistics
- **RX (Bytes):** Receiving data statistics
- **RSSI(dBm):** Received Signal Strength Indication: Signal strength of this wireless client
- **Kick and Ban:** Click this button to send this client to MAC address filter list. Click OK when you see this prompt. (*Save/Reload* is required to apply change.)

**Refresh:** Click this button to refresh the list

### System Log

This page allows users to view a running log of the access point’s system statistics, events and activities.

- **Choose a filter to quickly find the desired log.**
- **Refresh:** Click this button to refresh the log
- **Clear:** Click this button to clear the log
System

Operation Mode
Choose the mode that best suits your network: Access Point, Client Bridge, WDS, and Repeater. Either one of the wireless interfaces can be uses in bridge mode (Client Bridge, WDS Bridge, WDS Station, or Repeater), but not both. Select the country in which you are located and then select the operation mode for 2.4GHz and 5GHz wireless configurations. Click Apply to save the change. (Save/Reload is required for this change take effect.)

Access Point
This is the default operation mode for both the 2.4GHz and 5GHz wireless interfaces. Wireless clients, known as wireless stations (STAs), can wirelessly associate with these interfaces and connect to the Internet via the Ethernet port.

Client Bridge
The wireless interface works like a wireless station (STA), just like the wireless interface on a regular computer. The interface can connect to an AP dynamically (channels and encryption). The assigned wireless interface bridges the traffic to the Ethernet and the other TEW-753DAP wireless interface.

Repeater
In this mode, the wireless interface repeats wireless signal and packets for backbone communication as well as a client access. This feature is used to expand your existing wireless network to areas that your current access point is unable to reach. Make sure all of the settings of the wireless interface matches to your root or connecting wireless access points, same SSID, channel and wireless encryption settings.
**WDS (Wireless Distribution System)**
Wireless Distribution System, WDS, creates a wireless backbone link between multiple access points that are part of the same wireless network. This allows a wireless network to be expanded using multiple access points without the need for a wired backbone. TEW-753DAP WDS operation has three sub modes: WDS Access Point, WDS Bridge, or WDS Station

**WDS Access Point**
The wireless interface connects to other WDS bridge enable devices for backbone communication and provides wireless connection to clients (STAs) at the same time.

**WDS Bridge**
The wireless interface connects *ONLY* to other WDS bridge enabled devices and local networks (the other wireless interface and Ethernet interface) as a wireless backbone bridge.

**WDS Station**
The wireless interface connects to other WDS bridge enabled devices for backbone communication and connects to other wireless access points at the same time. Use this mode to pair with the next hop access point as a WDS network outlet.

* Only one bridge can be setup on 2.4GHz or 5GHz band, but not both.
IP Settings
The TEW-753DAP has a static IP (192.168.10.100) set for management purposes. You can change this IP address to fit your network plan or manage multiple TRENDnet access points. You can also set the TEW-753DAP to DHCP client to accept an IP dynamically.

<table>
<thead>
<tr>
<th>IP Network Setting</th>
<th>Select “Obtain an IP address automatically (DHCP)” or “Specify an IP address”. If you select specify an IP address, you have to enter the following information manually. If DHCP is selected, then the IP address is received automatically from the external DHCP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Specify an IP address</td>
</tr>
<tr>
<td>IP Subnet Mask</td>
<td>Specify a subnet mask for the IP address</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Default route for the TEW-753DAP</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>Primary DNS server address</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>Secondary DNS server address</td>
</tr>
<tr>
<td>Use Link Local Address</td>
<td>Check this to use link local address</td>
</tr>
<tr>
<td>IPv6 IP Address</td>
<td>Specify an IPv6 dual-stack address</td>
</tr>
<tr>
<td>IPv6 Subnet Prefix Length</td>
<td>Specify a subnet range for the IPv6 address</td>
</tr>
<tr>
<td>IPv6 Default Gateway</td>
<td>Default route for IPv6</td>
</tr>
<tr>
<td>IPv6 Primary DNS</td>
<td>Primary IPv6 DNS server address</td>
</tr>
<tr>
<td>IPv6 Secondary DNS</td>
<td>Secondary IPv6 DNS server address</td>
</tr>
</tbody>
</table>
Spanning Tree
The TEW-753DAP is designed for end point access as well as backbone connection. To avoid network looping, you can enable 802.1d spanning tree protocol.

<table>
<thead>
<tr>
<th>Spanning Tree Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spanning Tree Status</strong>: Enable or disable 802.1d spanning tree protocol to avoid network looping</td>
</tr>
<tr>
<td><strong>Bridge Hello Time</strong>: The time between each bridge protocol data unit (BPDU). Default: 2 sec.</td>
</tr>
<tr>
<td><strong>Bridge Max Age</strong>: Maximum time a BPDU kept in bridge. Default: 20 sec.</td>
</tr>
<tr>
<td><strong>Bridge Forward Delay</strong>: The time to be spent in listen and learning state. Default: 4 sec.</td>
</tr>
<tr>
<td><strong>Priority</strong>: Priority number for root bridge selection. (MAC number is listed on Status &gt; Main page)</td>
</tr>
</tbody>
</table>

Apply: Click this button to apply the change
Cancel: Click this button to cancel the change

Band Steer
In the office, the 2.4GHz is always crowded than 5GHz. There are fewer non-overlapping channels and more legacy devices in 2.4GHz compare to the 5GHz band. The TEW-753DAP is equipped with 2.4GHz and 5GHz wireless interfaces. When your client device can work on both 2.4GHz and 5GHz wireless, Band Steer will choose 5GHz as primary band over 2.4GHz. Traffic will mainly stays on 5GHz in stead of 2.4GHz. To setup band steer, you have to setup the same SSIDs on both the 2.4GHz and the 5GHz interfaces. Then check **Enable** on this page. Then click **Save**.

<table>
<thead>
<tr>
<th>Band Steer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Band Steering</strong>: Enable</td>
</tr>
</tbody>
</table>

Save: Click this button to save the change. *(Save/Apply is required to apply changes.)*
Cancel: Click this button to cancel the change
2.4G Wireless

Wireless Network
General setups options for your 2.4GHz wireless connection. You can setup up to eight SSIDs for different groups of users.

<table>
<thead>
<tr>
<th>Network Mode</th>
<th>Network Mode: Choose between N only, G only, B only, B/G mixed, or B/G/N mixed mode. The rule of the thumb is to choose single mode if your devices all work in the same mode. Mixed mode increases compatibility, but sometimes lowers the data speed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel HT Mode</td>
<td>Channel HT Mode: The latest 802.11 protocol can combine channels for better wireless performance. You can choose fixed 20MHz or 40MHz, or automatically select 20MHz or 40MHz channels.</td>
</tr>
<tr>
<td>Extension Channel</td>
<td>Extension Channel: When you choose manual channel selection and 20/40MHZ or 40MHz in channel HT mode, you can choose which neighbor channel you want to combine, upper channel or lower channel.</td>
</tr>
<tr>
<td>Channel / Frequency</td>
<td>Channel / Frequency: If you want to setup fixed channel, choose a channel number to switch your radio frequency. Otherwise, check auto to select the channel automatically which is selected by default. (When you choose 20/40MHZ or 40MHz channel HT mode, the channel selection list is shorter. Four marginal channels are reserved for channel expansion.)</td>
</tr>
</tbody>
</table>
### Current Profile

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID (1 - 8)</td>
<td>The wireless network name setup for this SSID.</td>
</tr>
<tr>
<td>Security</td>
<td>Wireless security type setup for this SSID.</td>
</tr>
<tr>
<td>VID</td>
<td>VLAN id for this SSID</td>
</tr>
<tr>
<td>Enable</td>
<td>Check this box to enable this SSID</td>
</tr>
<tr>
<td>Edit</td>
<td>Click Edit to change the settings for this SSID</td>
</tr>
</tbody>
</table>

*(Save/Apply is required to apply changes.)*

---

### AP Detection

Before you setup your TEW-753DAP wireless settings, you may want to know what signal are currently broadcasting. Click Scan to do a site survey and list the running access points around you.

**2.4GHz / Site Survey**

<table>
<thead>
<tr>
<th>BSSID</th>
<th>Basic SSID. This is strictly unique SSID to identify a wireless access point, WAP. It is also the MAC address of the wireless interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>Service Set Identifier. This SSID is human readable and performs as ESSID to setup wireless groups.</td>
</tr>
<tr>
<td>Channel</td>
<td>2.4GHz wireless channel number</td>
</tr>
<tr>
<td>Signal Level</td>
<td>The signal strength from the access point.</td>
</tr>
<tr>
<td>Type</td>
<td>The 802.11 wireless mode this access point provides.</td>
</tr>
<tr>
<td>Security</td>
<td>Which wireless security was set to use.</td>
</tr>
<tr>
<td>Mode</td>
<td>This wireless source works on infrastructure mode or ad hoc mode.</td>
</tr>
</tbody>
</table>

**Go Back**: Click this button to go back
**SSID Settings**
Click **Edit** one the SSID you want to edit. The following setup window will appear.

*Wireless Settings*
- **SSID**: Select the human readable SSID to be easily identified. You can choose any combination with 1 to 32 letters.
- **Suppressed SSID**: Check this box to suppress SSID broadcasting. Your wireless network name is broadcast to anyone within wireless signal range. When this box is checked, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.
- **Station Separation**: If you enable station separation, wireless clients (a.k.a. STAs) associated with this SSID cannot communicate to each other directly even if they are in the same wireless group.

*Wireless Security*
- **Security Mode**: Choose between Disabled, WEP, WPA-PSK, WPA2-PSK or WPA-PSK Mixed for your wireless security.
- **(SSID 1 Only)**
- **Security Mode**: Choose between Disabled, WPA-PSK, WPA2-PSK or WPA-PSK Mixed for your wireless security.
- **Security Mode**: Choose between Disabled, WPA-PSK, WPA2-PSK or WPA Mixed for your wireless security.
**WEP (Wired Equivalent Privacy)**
This is a minimum and legacy type of wireless security. Only SSID 1 can be set with WEP wireless security mode.

<table>
<thead>
<tr>
<th>Wireless Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Mode</td>
</tr>
<tr>
<td>Auth Type</td>
</tr>
<tr>
<td>Input Type</td>
</tr>
<tr>
<td>Key Length</td>
</tr>
<tr>
<td>Default Key</td>
</tr>
<tr>
<td>Key1</td>
</tr>
<tr>
<td>Key2</td>
</tr>
<tr>
<td>Key3</td>
</tr>
<tr>
<td>Key4</td>
</tr>
</tbody>
</table>

**Auth Type :** Select Open System or Shared Key. **Open System** allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. **Shared Key** sends an unencrypted challenge text string to any device attempting to communicate with the AP. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. It is recommended to select **Auto** if you are not sure which authentication type is used.

**Key Type :** Select your key format to be in hexadecimal or ASCII codes. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember.

**Key Length :** Select a 64-bit, 128-bit, or 152-bit WEP key length from the drop-down list

**Default Key :** You may choose one of your four different WEP keys from below

**Key 1-4 :** You can enter four different WEP keys

**Save:** Click this button to save the changes
**Cancel :** Click this button to cancel the change
**WPA-PSK, WPA2-PSK, Mixed WPA-PSK**
This group of wireless security settings use the preshared key, PSK, stored on you TEW-753DAP to secure your wireless connections. WPA2 is currently the most advanced wireless encryption. Choose this option if all of your devices support WPA2. Otherwise choose WPA or WPA & WPA2 mixed.

**Encryption:**
Select TKIP, AES, or Both. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.

**Passphrase:**
The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format or hexadecimal numbers at both ends of the wireless connections. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

**Group Key Update Interval:**
Specify how often the wireless key should be renegotiated. Shorter time intervals are more secure, but cause more overhead. (Default: 3600 seconds/1 hour)
**WPA, WPA2, Mixed WPA**

This group of wireless security settings uses remote key services, RADIUS, to secure your wireless connections. WPA2 is currently the most advanced wireless encryption. Choose this option if all of your devices support WPA2. Otherwise choose WPA or WPA & WPA2 mixed.

### WPA Type:
Select TKIP, AES, or Both. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.

### RADIUS Server:
IP address of RADIUS server

### RADIUS Port:
RADIUS service port number. Default: 1812

### RADIUS Secret:
RADIUS service shared secret to authenticate this credential agent.

### Group Key Update Interval:
Specify how often the wireless key should be renegotiated. Shorter time intervals are more secure, but cause more overhead. (default: 3600 seconds/1 hour)

### Radius Accounting:
Enable or disable RADIUS accounting service

**Apply**: Click this button to apply the changes

**Cancel**: Click this button to cancel the change
MAC Filter
Set up a list of clients and policies that allow only the clients on the list to associate with this AP or to reject clients on the list from associating with this AP. Set up the list with MAC addresses. A MAC address is a unique ID assigned by the manufacturer of the network adapter. Enter a MAC address and click Add to add it to the list. Click Delete to remove an entry. Select your ACL Mode and then click Apply. (You can also go to the wireless client list and click Kick and Ban to add a client to the list.)

ACL (Access Control List) Mode:

Choose “Disabled” to disable the MAC filter.
Choose “Deny MAC in the List” to allow clients that aren’t on the list to associate with the TEW-753DAP’s 2.4GHz wireless interface.
Choose “Allow MAC in the List” to deny clients that aren’t on the list to associate with the TEW-753DAP’s 2.4GHz wireless interface.

Click Kick and Ban in the wireless client list to add a MAC entry to the MAC filter list.
Wireless Advanced Settings
Fine tune your wireless settings on this page.

2.4GHz / Wireless Advanced Settings

Data Rate:
Choose a fixed data rate for 802.11b and g mode and MCS number for 802.11n, or choose Auto for automatic rate adapting. The default setting is Auto.

Transmit Power:
Wireless signal transmission power. Setting transmission power to an appropriate value can make your multiple AP deployment easier. The default value is 18 dBm. Valid settings are between 11 and 18 (both FCC and CE).

RTS/CTS Threshold:
Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and to prevent hidden nodes from degrading the performance. Specify a value between 1 and 2346. The default value is 2346.

Distance:
Set the distance between the TEW-753DAP and other access points or wireless clients. Low speed/long range settings may be a priority for longer range connections. Valid settings are between 1 and 30. The default value is 1 Km.

Aggregation:
Combine short packets and send them together. Enabling packet aggregation will increase data throughput. However, it may cause jitters or delays in real-time communication.
WMM Parameters

<table>
<thead>
<tr>
<th>AC</th>
<th>Access Category: best effort (AC_BE), background (AC_BK), video (AC_VI), and voice (AC_VO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWmin</td>
<td>Minimum contention window</td>
</tr>
<tr>
<td>CWmax</td>
<td>Maximum contention window</td>
</tr>
<tr>
<td>AIFSN</td>
<td>The Arbitration Inter-Frame Spacing Number specifies a wait time for data frames</td>
</tr>
<tr>
<td>TXOP Limit</td>
<td>Transmission Opportunity Limit : The limit of the interval of time between the access point having the right to initiate transmissions and the transmission start time.</td>
</tr>
</tbody>
</table>

**Client Limit**

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Limit the number of clients connected to the 2.4GHz interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Check this box to enable maximum client limitation</td>
</tr>
<tr>
<td>Max Client</td>
<td>The maximum number of clients that can connect to the TEW-753DAP's 2.4GHz interface is 127. The valid numbers are from 1 to 127. The default value is 127.</td>
</tr>
</tbody>
</table>

**WPS**

WPS is one way to connect a wireless client to the TEW-753DAP. You don’t have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both the wireless client and the TEW-753DAP, and WPS will do the rest for you.

Only the first SSID (SSID 1) supports WPS pairing. There are two types of WPS: WPS via Push Button and WPS via PIN code are supported. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start WPS pairing, and click the **Start to Process** button in this page under **WPS via Push Button** to start WPS pairing.

If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the access point.

WPS is disabled by default. To enable it, you have to click **Enable** and then **Apply**. Go **Save/Apply** to apply the changes. Then come back to this page to start your WPS session.
## System Configuration

### 2.4GHz / WPS Setting

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WPS</strong></td>
<td>Enable the WPS feature</td>
</tr>
<tr>
<td><strong>WPS Current Status</strong></td>
<td>Displays the current status of the WPS configuration. Press <strong>Release Configuration</strong> to release previous settings.</td>
</tr>
<tr>
<td><strong>Self Pin Code</strong></td>
<td>Displays PIN code of TEW-753DAP</td>
</tr>
<tr>
<td><strong>SSID</strong></td>
<td>Displays the SSID for WPS pairing. Only the first SSID (SSID 1) can proceed with WPS pairing.</td>
</tr>
<tr>
<td><strong>Authentication Mode</strong></td>
<td>Displays the authentication mode of SSID 1</td>
</tr>
<tr>
<td><strong>Passphrase Key</strong></td>
<td>Current passphrase. Click the check box to reveal the passphrase.</td>
</tr>
<tr>
<td><strong>WPS Via Push Button</strong></td>
<td>Click on the <strong>Start to Process</strong> button if you would like to enable WPS through the Push Button instead of the PIN. After pressing this button you will be required to press the WPS on the client device within two minutes. Click the <strong>OK</strong> button in the dialog box</td>
</tr>
<tr>
<td><strong>WPS via PIN</strong></td>
<td>Specify a PIN, a unique number that can be used to add the router to an existing network or to create a new network. Then click the <strong>Start to Process</strong> button</td>
</tr>
</tbody>
</table>

**Table:**

- **WPS Current Status**: Displays the current status of the WPS configuration. Press **Release Configuration** to release previous settings.
- **Self Pin Code**: Displays PIN code of TEW-753DAP.
- **SSID**: Displays the SSID for WPS pairing. Only the first SSID (SSID 1) can proceed with WPS pairing.
- **Authentication Mode**: Displays the authentication mode of SSID 1.
- **Passphrase Key**: Current passphrase. Click the check box to reveal the passphrase.
- **WPS Via Push Button**: Click on the **Start to Process** button if you would like to enable WPS through the Push Button instead of the PIN. After pressing this button you will be required to press the WPS on the client device within two minutes. Click the **OK** button in the dialog box.
- **WPS via PIN**: Specify a PIN, a unique number that can be used to add the router to an existing network or to create a new network. Then click the **Start to Process** button.
5G Wireless

Wireless Network
General setups for your 5GHz wireless connection. You can setup up to eight SSIDs for different groups of users.

- **Network Mode**: Choose between N only, a only, or A/N mixed mode. The rule of the thumb is to choose single mode if your devices all work in the same mode. Mixed mode increases compatibility, but sometimes lowers the data speed.

- **Channel HT Mode**: The latest 802.11 protocol can combine channel for better wireless performance. You can choose fixed 20MHz or 40MHz, or automatically select 20MHz or 40MHz channels.

- **Extension Channel**: Not applicable in 5GHz wireless

- **Channel / Frequency**: If you want to setup fixed channel, choose a channel number to switch your radio frequency. Otherwise, check auto to select the channel automatically, which is selected by default.

**Current Profile**

- **SSID (9 - 16)**: The wireless network name setup for this SSID.
- **Security**: Wireless security type setup for this SSID.
- **VID**: VLAN id for this SSID
- **Enable**: Check this box to enable this SSID
- **Edit**: Click Edit to change the settings for this SSID. (Save/Apply is required to apply changes.)
**AP Detection**

Before you setup your TEW-753DAP wireless settings, you may want to know what signals are currently broadcasting. Click Scan to do a site survey and list the running access points around you.

### 5GHz / Site Survey

<table>
<thead>
<tr>
<th>BSSID</th>
<th>SSID</th>
<th>Channel</th>
<th>Signal Level</th>
<th>Type</th>
<th>Security</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:14:D1:98:B2:16</td>
<td>Wally World_5GHz</td>
<td>36</td>
<td>-58 dBm</td>
<td>11a/n</td>
<td>WPA2</td>
<td></td>
</tr>
<tr>
<td>00:14:D1:DC:70:34</td>
<td>602gr_5-et</td>
<td>48</td>
<td>-50 dBm</td>
<td>11a/n</td>
<td>WPA2</td>
<td></td>
</tr>
<tr>
<td>00:14:D1:A3:FA:55</td>
<td>TRENDnetSSID2ac0921</td>
<td>149</td>
<td>-66 dBm</td>
<td>11a/n</td>
<td>WPA2</td>
<td></td>
</tr>
</tbody>
</table>

- **BSSID**: Basic SSID. This is a strictly unique SSID to identify a wireless access point, WAP. It is also the MAC address of the wireless interface.
- **SSID**: Service Set Identifier. This SSID is human readable and performs as ESSID to setup wireless groups.
- **Channel**: 5GHz wireless channel number
- **Signal Level**: The signal strength from the access point.
- **Type**: The 802.11 wireless mode this access point provides.
- **Security**: Which wireless security was set to use.
- **Mode**: This wireless source works on infrastructure mode or ad hoc mode.

**Go Back**: Click this button to go back
### SSID Settings
Click **Edit** for the SSID you want to edit. The following setup window will appear.

#### Wireless Settings
- **SSID**: Select the human readable SSID to be easily identified. You can choose any combination with 1 to 32 letters.
- **Suppressed SSID**: Check this box to suppress SSID broadcasting. Your wireless network name is broadcast to anyone within wireless signal range. When this box is checked, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.
- **Station Separation**: If you enable station separation, wireless clients (a.k.a. STAs) associated with this SSID cannot communicate to each other directly, even if they are in the same wireless group.

#### Wireless Security
- **Security Mode**: Choose between Disabled, WPA-PSK, WPA2-PSK or WPA-PSK mixed, WPA, WPA2 or WPA Mixed for your wireless security.
**WPA-PSK, WPA2-PSK, Mixed WPA-PSK**

This group of wireless security settings use the preshared key, PSK, stored on your TEW-753DAP to secure your wireless connections. WPA2 is currently the most advanced wireless encryption. Choose this option if all of your devices support WPA2. Otherwise choose WPA or WPA & WPA2 mixed.

### Encryption:
Select TKIP, AES, or Both. The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. Note that, if the bridge uses the AES option, the bridge can associate with the access point only if the access point is also set to use only AES.

### Passphrase:
The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format or hexadecimal numbers at both ends of the wireless connections. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

### Group Key Update Interval:
Specify how often the wireless key should be renegotiated. Shorter time intervals are more secure, but cause more overhead. (default: 3600 seconds/ 1 hour)
**WPA, WPA2, Mixed WPA**

This group of wireless security use remote key services, RADIUS, to secure your wireless connections. WPA2 is currently the most advanced wireless encryption. Choose this option if all of your devices support WPA2. Otherwise choose WPA or WPA & WPA2 mixed.
**Wireless MAC Filter**

Set up a list of clients and policies that allow only the clients on the list to associate with this AP or to reject clients on the list from associating with this AP. Set up the list with MAC addresses. A MAC address is a unique ID assigned by the manufacturer of the network adapter. Enter a MAC address and click **Add** to add it to the list. Click **Delete** to remove an entry. Select your **ACL Mode** and then click **Apply**. (You can also go to the wireless client list and click **Kick and Ban** to add a client to the list.)

### 5GHz / Wireless MAC Filter

**CAUTION:** When WPS is enabled, Wireless MAC Filter cannot be applied to the first SSID.

**ACL Mode:**
- **Disabled**
- **Allow MAC in the List**
- **Deny MAC in the List**

Choose “Disabled” to disable the MAC filter.

Choose “Deny MAC in the List” to allow clients that aren’t on the list to associate with the TEW-753DAP’s 5GHz wireless interface.

Choose “Allow MAC in the List” to deny clients that aren’t on the list from associating with the TEW-753DAP’s 5GHz wireless interface.

Click **Kick and Ban** in the wireless client list to add a MAC entry to MAC filter list.
Wireless Advanced Settings
Fine tune your wireless settings on this page.

**5GHz / Wireless Advanced Settings**

**Data Rate:**
Select different 802.11n Modulation and Coding Scheme (MCS) against particular wireless noise or select **auto** for the TEW-753DAP to select MCSs dynamically. Or, choose the speed you want in 802.11a mode.

**Transmit Power:**
Wireless signal transmission power. Setting transmission power to an appropriate value can make your multiple AP deployment easier. The default value is 18 dBm. Valid settings are between 11 and 18 (both FCC and CE).
### RTS/CTS Threshold
Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and to prevent hidden nodes from degrading the performance. Specify a value between 1 and 2346. The default value is 2346.

### Distance
Set the distance between the TEW-753DAP and other access points or wireless clients. Low speed/long range settings may be a priority for longer range connection. Valid settings are between 1 and 30. The default value is 1 Km.

### Aggregation
Combine short packets and send them together. Enabling packet aggregation will increase data throughput. However, it may cause jitters or delays in real-time communication.

<table>
<thead>
<tr>
<th>WMM Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Access Category: best effort (AC_BE), background (AC_BK), video (AC_VI), and voice (AC_VO)</td>
</tr>
<tr>
<td>CWmin</td>
<td>Minimum contention window</td>
</tr>
<tr>
<td>CWmax</td>
<td>Maximum contention window</td>
</tr>
<tr>
<td>AIFSN</td>
<td>The Arbitration Inter-Frame Spacing Number specifies a wait time for data frames</td>
</tr>
</tbody>
</table>

### TXOP Limit
Transmission Opportunity Limit: The limit of the interval of time between the access point having the right to initiate transmissions and the transmission start time.

### Client Limit
| Frequency | Limit the number of clients connected to the 5GHz interface |
| Enable | Check this box to enable maximum client limitation |
| Max Client | The maximum number of clients that can connect to the TEW-753DAP's 5GHz interface is 127. The valid numbers are from 1 to 127. The default value is 127. |

### WPS
WPS is one way to connect a wireless client to the TEW-753DAP. You don’t have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both the wireless client and the TEW-753DAP, and WPS will do the rest for you.

Only the first SSID (SSID 9) supports WPS pairing. There are two types of WPS: WPS via Push Button and WPS via PIN code are supported. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start WPS pairing, and click the Start to Process button in this page under **WPS via Push Button** to start WPS pairing.
If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the access point.

WPS is disabled by default. To enable it, you have to click Enable and then Apply. Go to Save/Apply to apply the changes. Then come back to this page to start your WPS session.

| **WPS** | Enable the WPS feature |
| **WPS Current Status** | Displays the current status of the WPS configuration. Press Release Configuration to release previous settings. |
| **Self Pin Code** | Displays PIN code of TEW-753DAP |
| **SSID** | Displays the SSID for WPS pairing. Only the first SSID (SSID 9) can proceed with WPS pairing. |
| **Authentication Mode** | Displays the authentication mode of SSID 9 |
| **Passphrase Key** | Current passphrase. Click the check box to reveal the passphrase. |
| **WPS Via Push Button** | Click on the Start to Process button if you would like to enable WPS through the Push Button instead of the PIN. After pressing this button you will be required to press the WPS on the client device within two minutes. Click the OK button in the dialog box |
| **WPS via PIN** | Specify a PIN, a unique number that can be used to add the router to an existing network or to create a new network. Then click the Start to Process button |
**Management**

**Administration**
Change the password required to log into the access point’s web-based management. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive. Enter your password and system information and then click **Apply** to save the change.

**Management VLAN Settings**
This feature is only available under Access Point or WDS AP mode and allows users to configure the 802.1q VLAN settings to for all wireless clients. A VLAN is a group of computers on a network whose software has been configured so that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN.

Enter the VLAN ID you want to tag to clients associated with specific SSIDs. Different SSIDs should be set with different VLAN IDs. Enable Virtual LAN service and click **Apply** to save the changes.

LAN VLAN MGMT is a special VLAN to manage the TEW-753DAP. Enabling management VLAN tagging will keep all services, for example DHCP server and client, in this VLAN.

### Management VLAN Settings
- **New Name:** The new administrator login name
- **Old Password:** Enter the current password for authentication allowing new password change.
- **New Password:** Enter your new password here.
- **Confirm Password:** Type your new password again for verification purposes
### 2.4G / 5G Current Profiles

<table>
<thead>
<tr>
<th>SSID (1 - 16)</th>
<th>Security</th>
<th>Isolation</th>
<th>VID</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRENDnet753_2.4GHz_5RL2</td>
<td>WPA2-PSK AES</td>
<td>1</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>None</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td>8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Security
- Wireless security set to the SSID

#### Isolation
- Packets are not tagged with a VLAN ID by default. Checking this box will tag the VLAN ID to the packets going through this SSID. Packets with different VLAN ID are recognized as if they are in the different network.

#### VID
- Virtual LAN ID

#### Enable
- Redundant control to enable or disable the particular SSID.

---

### Management VLAN ID

| No VLAN Tag | Management VLAN packets are not tagged by default. |
| Specified VLAN ID | Select this if you want to separate the management VLAN. Enabling tagging will redirect all services, including web management and DHCP, to a specific VLAN, specified in VLAN ID field. (1 ~ 4094) |

#### Apply
- Click this button to apply the changes. *(Save/Apply is required to apply changes.)*

#### Cancel
- Click this button to cancel the change.
Wireless Traffic Shaping
Traffic shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.

<table>
<thead>
<tr>
<th><strong>Enable Traffic Shaping</strong></th>
<th>Choose to enable or disable the traffic shaping feature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incoming Traffic Limit</strong></td>
<td>Set the traffic limitation going through Ethernet port. The default value is 10Mbps (10,000). The number can be set from 512 to 99,999,999. The traffic will be limited by this value and physical speed whichever is lower. (The TEW-753DAP Ethernet port is capable of 1Gbps, 1,000,000 kbps.)</td>
</tr>
</tbody>
</table>

2.4GHz / 5GHz Settings

<table>
<thead>
<tr>
<th><strong>Outgoing Traffic Limit</strong></th>
<th>Set the traffic limitation going through the wireless interface. The default value is 180Mbps (180,000). The number can be set from 512 to 99,999,999. The traffic will be limited by this value and physical speed whichever is lower. (The TEW-753DAP wireless interfaces are capable of 300 Mbps, 300,000 kbps for 2.4GHz and 5GHz respectively.)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total Percentage</strong></td>
<td>This value adds up all numbers in following 8 SSID percentage settings. This value may exceed 100, up to 800. The traffic limit of this wireless interface is calculated as: Outgoing Traffic Limit * Total Percentage.</td>
</tr>
</tbody>
</table>

| **SSID (1 - 8)** | Set the number you want to shape your traffic for clients connects to specific SSIDs by increasing or decreasing the value. The default value is 10 (%). The number can be set from 0 to 100. The traffic limit of this SSID is calculated as: Outgoing Traffic Limit * Total Percentage. |

<table>
<thead>
<tr>
<th><strong>Apply</strong></th>
<th>Click this button to apply the changes. (Save/Apply is required to apply changes.)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cancel</strong></td>
<td>Click this button to cancel the change</td>
</tr>
</tbody>
</table>
SNMP Settings
SNMP Settings allows you to assign the contact details, location, community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.

### SNMP Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>Choose to enable or disable the SNMP feature</td>
</tr>
<tr>
<td>Contact</td>
<td>Specify the contact details of the TEW-753DAP</td>
</tr>
<tr>
<td>Location</td>
<td>Specify the location of the TEW-753DAP</td>
</tr>
<tr>
<td>Community Name (Read Only)</td>
<td>Specify the password for access to the SNMP community for read only access</td>
</tr>
<tr>
<td>Community Name (Read/Write)</td>
<td>Specify the password for access to the SNMP community with read/write access</td>
</tr>
<tr>
<td>Trap Destination Address</td>
<td>Specify the IP address for the SNMP trap community</td>
</tr>
<tr>
<td>Trap Destination Community Name</td>
<td>Specify the name of SNMP trap community</td>
</tr>
<tr>
<td>SNMP v3</td>
<td>Select enable or disable SNMP v3 protocol</td>
</tr>
<tr>
<td>User Name</td>
<td>SNMP v3 manager user name</td>
</tr>
<tr>
<td>Auth Protocol</td>
<td>Choose the authentication method to verify the source of information: MD5, SHA, or None.</td>
</tr>
<tr>
<td>Auth Key</td>
<td>Specify the authentication key between 8 to 32 letters.</td>
</tr>
<tr>
<td>SNMP Manager IP</td>
<td>Specify the SNMP manager IP address</td>
</tr>
<tr>
<td>Priv Protocol</td>
<td>Choose the privacy key to encrypt SNMP messages: DES or None.</td>
</tr>
<tr>
<td>Priv Key</td>
<td>Specify the privacy key between 8 to 32 letters.</td>
</tr>
<tr>
<td>Engine ID</td>
<td>SNMPv3 engine ID</td>
</tr>
</tbody>
</table>

**Save/Apply**: Click this button to apply the changes.

**Cancel**: Click this button to cancel the change.
Backup / Restore Settings
This page allows you to save the current configurations. Click Backup to save your current configuration.

To load previously saved configurations, click Choose File to find the configuration file and then click Restore. The configuration file is encrypted with an Encryption Key. Enter your encryption key and then click Save to save the key to the TEW-753DAP. The new configuration file will be saved and encrypted with this new key.

In case you want to reset TEW-753DAP’s configurations back to factory defaults, click Factory Default in this page. All configurations will be set back to their original default settings.

Firmware Upgrade
TRENDnet may periodically release firmware upgrades that might add features or fix problems associated with your TRENDnet model and version. To find out 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/

1. If a firmware upgrade is available, download the firmware to your computer.
2. Unzip the file to a folder on your computer.
3. Log into the TEW-753DAP
4. Click on Management and then Firmware Upgrade
5. Click Choose File and navigate to the folder on your computer in which the unzipped firmware file (.bin) is.
6. Located and select it the firmware file.
7. Click Upload.
Time Settings
The accuracy of the system clock is important for scheduling and accurate logging. You can synchronize the system time with your computer, or automatically check the time accuracy with a network time server (NTP server).

**Manually Set Date and Time**
Choose this option to manually set your system clock. You can enter the time manually or you can copy the time from your computer by clicking **Synchronize with PC**. Click **Save/Apply** to change the system clock.

**Automatically Get Date and Time**
Choose this selection to get the time from a network time server automatically. Select the **Time Zone** of the country or region you are currently in. The TEW-753DAP will set its time based on your selection.

If you have a preferred NTP server, check the **User defined NTP Server** and Enter the NTP server IP address. Otherwise, leave it unchecked to use the TEW-753DAP’s default NTP server.

Check **Enable Daylight Saving** if your time zone has daylight savings. Enter the start time and end time of daylight savings.

When you finish your settings, click **Save/Apply** to change the system clock.
Schedule
Service schedule can be set up daily or weekly for power saving and security reasons. You can setup up to 50 schedule entries. Click **Add** to add a schedule entry. Select an entry and then click **Delete Selected** to delete the entries. Click **Reset** to remove the selections. Click **Delete All** to remove all entries. After schedule editing, click **Apply** to save your schedule. Check **Enabled Schedule Table** to make AP services work with the schedule.

### Schedule Table

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Service</th>
<th>Schedule</th>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>a1</td>
<td>Wireless Active (2.4GHz)</td>
<td>All Time * - Mon, Tue, Wed, Thu, Fri, Sat, Sun</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>b</td>
<td>Wireless Active (5GHz)</td>
<td>All Time * - Mon, Tue, Wed, Thu, Fri, Sat, Sun</td>
<td></td>
</tr>
</tbody>
</table>

- **Delete Selected**: Delete selected schedule
- **Delete All**: Click this button to clear the list
- **Reset**: Reset previous selections
- **Apply**: Click this button to apply the changes.
- **Cancel**: Click this button to cancel the change.
**CLI Settings**

To enable the Command Line Interface for batch management or advanced configuration, select CLI ON and then click **Save/Apply**.

Access the CLI interface using SSH with the administrator user name and password. For example (in Linux):

```bash
$ ssh admin@192.168.10.100
The authenticity of host '192.168.10.100' (192.168.10.100) can't be established.
Are you sure you want to continue connecting (yes/no)? yes
admin@192.168.10.100's password:
*** Hi admin, welcome to use cli(V-1.7.6) ***
------- Commands Help -------
  stat -- Status
  sys -- System
  wless2 -- 2.4G-Wireless
  wless5 -- 5G-Wireless
  mgmt -- Management
  tree -- Tree
  help -- Help
  reboot -- Reboot
tew-753dap>
```

**Log**

To keep your system operating history, you can setup local and remote loggings.

**Syslog**

Select **Enable** from the drop down list and then enter the log server IP address or URL. Then click **Save/Apply** to save the log to the log server.

**Local Log**

Select **Enable** from the drop down list and then click **Save/Apply** to save the log locally. You can view the log in **Status > System Log**.
Diagnosis
There are 3 network tools you can use on the TEW-753DAP: ping, traceroute, and speed test.

**PING**
Enter the Target IP / Domain Name, Ping Packet Size and Number of Pings and then click Start Ping to start the PING tool.

**Traceroute**
Enter the Traceroute Target and then click Start Traceroute to start the Traceroute tool.
**Speed Test**
Setup an iperf server. Enter the server address as the Target Address, Time Period, Check Interval and then click Start Speed Test to start the speed test tool. The default IPv4 test port is 5001 and the IPv6 test port is 5002.

### Diagnostics Results

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Operation Mode</th>
<th>IP Address</th>
<th>System MAC Address</th>
<th>Firmware Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device name of neighbor TEW-753DAP</td>
<td>Which operation mode the neighbor TEW-753DAP is running.</td>
<td>IP address of neighbor TEW-753DAP</td>
<td>System MAC address (LAN/2.4GHz wireless interface MAC address) of neighbor TEW-753DAP</td>
<td>Firmware version the neighbor TEW-753DAP is running.</td>
</tr>
</tbody>
</table>

**Device Discovery**
The TEW-753DAP can discover other TEW-753DAPs on neighboring wired or wireless network.

**Refresh** : Click this button to discover the neighboring devices.
LED Control
All LED indicators are turned on by default. You can turn any one of them or all of them on or off. Click the LED you want to turn on or off and then click Save/Apply to save and apply the changes.

<table>
<thead>
<tr>
<th>Power LED</th>
<th>OFF</th>
<th>Powered off or LED display is disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ON</td>
<td>Powered on</td>
</tr>
</tbody>
</table>

### Network LED
Orange: 10/100 Green: Giga bit
<table>
<thead>
<tr>
<th>OFF</th>
<th>No network connection detected through Ethernet port (PoE) or LED display has been disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON</td>
<td>Network connected through Ethernet port (PoE)</td>
</tr>
<tr>
<td>Flashing</td>
<td>Network activities are detected on Ethernet (PoE) port</td>
</tr>
</tbody>
</table>

### Wireless LED
Orange: 2.4GHz Green: 5GHz
| OFF       | No wireless network connection or LED display is disabled                                 |
| Flashing  | Wireless network activities are detected                                                   |

Logout
Logout from the management page. The TEW-753DAP allows only one management login at the same time. If you want to access the TEW-753DAP from different computer, remember to logout of the web management page first.
Appendix

WDS Frequent Asked Questions

What is WDS?
WDS stands for Wireless Distribution System, a non-standard extension to the IEEE 802.11 standard to allow transparent Ethernet bridging on the station and to implement seamless hand-over for wireless clients roaming between different access points.

Should I use WDS or not?
WDS links create transparent bridges facilitate layer 2 seamless communication. You don’t have to use WDS if you don’t need layer 2 services passing through TEW-753DAP, such as MAC filtering, and 802.1X authentication. You can simply use AP, Client Bridge, and Repeater mode to fit most of your network plan.

What problem WDS is resolving?
The 802.11 standard only uses three MAC addresses for frames transmitted between the Access Point and the Station. Frames transmitted from the station to the AP don’t include the Ethernet source MAC address of the requesting host and response frames are missing the destination Ethernet MAC to address the target host behind the client bridge.

WDS AP and WDS Station uses the 4 MAC address including complete source, destination, WDS AP, and WDS Station addresses. Data frame arriving WDS AP or WDS Station will be translated back to 802.3 data frame with real source address instead of WDS AP or WDS Station address. The 4 addresses design keeps the original data frame intact bridging to the other side transparently.

What should I have to build WDS network?
You have to use multiple TEW-753DAPs to build WDS AP - WDS Station pair or WDS bridge mesh groups. Different model with same or different brand name may NOT work together because of the different WDS implementation details.
Federal Communication Commission Interference Statement

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

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

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

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

FCC Radiation Exposure Statement:

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

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.
Europe – EU Declaration of Conformity
This device complies with the essential requirements of the R&TTE Directive 1999/5/EC, 2006/95/EC and 2009/125/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC, 2006/95/EC and 2009/125/EC:

Safety of Information Technology Equipment

EN50385 : 2002
Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)

EN 300 328 V1.7.1
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.9.2
Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V2.2.1
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

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

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

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

RoHS
This product is RoHS compliant.
<table>
<thead>
<tr>
<th>Language</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Czech</td>
<td>TRENDnet tímto prohlašuje, že tento TEW-753DAP je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES, 2006/95/ES, a 2009/125/ES.</td>
</tr>
<tr>
<td>Danish</td>
<td>Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-753DAP 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-753DAP 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>Spanish</td>
<td>Por medio de la presente TRENDnet declara que el TEW-753DAP cumple con los requisitos esenciales y otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE, 2006/95/CE, y 2009/125/CE.</td>
</tr>
<tr>
<td>Greek</td>
<td>ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ TRENDnet ΔΗΛΑΔΕΙ ΟΤΙ ΤΗΣ 1999/5ΕΚ, 2006/95ΕΚ, 2009/125ΕΚ.</td>
</tr>
<tr>
<td>Latvian</td>
<td>Ar šo TRENDnet deklarē, ka TEW-753DAP atbilst Direktīvām 1999/5EK, 2006/95EK, un 2009/125/EEK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.</td>
</tr>
<tr>
<td>Dutch</td>
<td>Hierbij verklaart TRENDnet dat het toestel TEW-753DAP in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG, 2006/95/EG, en 2009/125/EG.</td>
</tr>
<tr>
<td>Hungarian</td>
<td>Alulírott, TRENDnet nyilatkozom, hogy a TEW-753DAP megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv, a 2006/95/EK és a 2009/125/EK irányelv egyéb előírásainak.</td>
</tr>
<tr>
<td>Polish</td>
<td>Niniejszym TRENDnet oświadcza, że TEW-753DAP jest zgodny z zasadniczymi wymogami oraz pozostalymi stosownymi postanowieniami Dyrektywy 1999/5/WE, 2006/95/WE i 2009/125/WE.</td>
</tr>
<tr>
<td>Portuguese</td>
<td>TRENDnet declara que este TEW-753DAP está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE, 2006/95/CE e 2009/125/CE.</td>
</tr>
<tr>
<td>Slovenian</td>
<td>TRENDnet izjavlja, da je ta TEW-753DAP v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES, 2006/95/ES, a 2009/125/ES.</td>
</tr>
<tr>
<td>Slovak</td>
<td>TRENDnet týmto vyhlasuje, že TEW-753DAP splňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EF.</td>
</tr>
<tr>
<td>Swedish</td>
<td>Härdem intygar TRENDnet att denna TEW-753DAP står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG, 2006/95/EG och 2009/125/EG.</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.

- TEW-753DAP – 3 Years Warranty
- AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1 year warranty.

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

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

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

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

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER’S OR ANY THIRD PERSON’S MISUSE, 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 or http://www.trendnet.com Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please go to http://www.gnu.org/licenses/gpl.txt or http://www.gnu.org/licenses/lgpl.txt for specific terms of each license.
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 ©2013. All Rights Reserved. TRENDnet.