User's Guide

TRENDnet®

Dual Band Wireless Access Point

TEW-821DAP

Table of Contents

Product Overview

TRENDnet's AC1200 Dual Band PoE Access Point, model TEW-821DAP, supports Access Point (AP), Wireless Distribution System (WDS) Bridge, AP + WDS, Client Bridge, and Repeater mode functionality. A convenient wireless scan feature streamlines the WDS setup process. Multiple SSIDs are supported for each band. The web-based management page allows you to configure your Access Point easily.

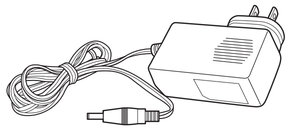
Features

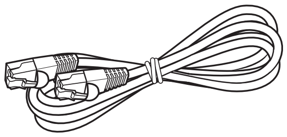
- Compatible with IEEE 802.11ac technology:
    - ◆ 2TX/2RX wireless speed up to 866Mbps data rate
- Compatible with IEEE 802.11n high rate standard to provide wireless speed of 300Mbps data rate
- Compatible with IEEE 802.11g high rate standard to provide wireless speed of 54Mbps data rate
- Compatible with IEEE 802.3at PoE
- Simultaneously transmit both 2.4 GHz and 5 GHz wireless networks
- IEEE 802.11b/g/n/ac Infrastructure operating modes
- 1 x 10/100/1000Mbps Gigabit Ethernet port with PoE function
- Supports Multiple Input Multiple Output(MIMO) technology with 2TX/2RX(11a/b/g/n/ac)
- Allow auto fallback data rate for optimized reliability, throughput and transmission range
- Supports wireless data encryption with 64/128-bit WEP standard for security
- Supports enhance security for WPA-PSK, WPA2-PSK, WPA and WPA2
- Advance wireless security of up to WPA2-RADIUS
- Web-based configuration tools and management via WEB Browser
- Supports WPS (Wi-Fi Protected Setup Specification Windows)
- Supports statistics information
- Supports Wireless Distribution System (WDS) for wireless network bridging

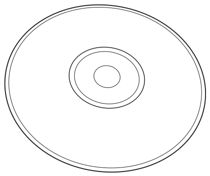
Package Content

Check if your package contains the following items. If any item is missing or appears damaged, contact your dealer.

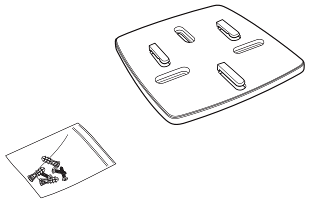
Access Point


Power Adapter (12V, 1A)


RJ-45 Ethernet cable

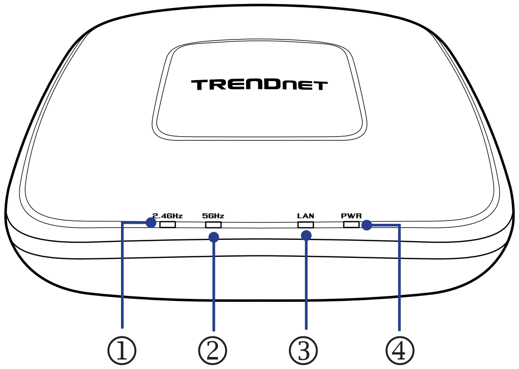

CD-ROM (User's Guide)

Quick Start Guide


Mounting kit
(incl. bracket + screws)

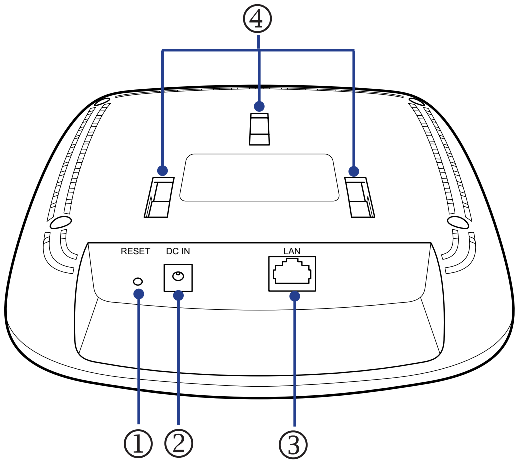
Hardware Overview

Front View



No.	Item	Description
1	2.4G LED	The indicator turns on solid green when the wireless is enabled on your access point. This LED blinks green during data transmission.
2	5G LED	The indicator turns on solid green when the wireless is enabled on your access point. This LED blinks green during data transmission.
3	LAN LED	The indicator turns on solid green when the wireless is enabled on your access point. This LED blinks green during data transmission.
4	POWER LED	A solid green light indicates a proper connection to the power supply.

Rear View



No.	Item	Description
1	Reset Button	Use a sharp tool to press and hold this button for 10 seconds to reset the access point.
2	Power connector	Connect the power adapter from your access point power port to an available power outlet.
3	LAN Port	Connect the Ethernet cable (also called network cables) from your access point to your router and wired network devices.
4	Mounting holes	Attach the mounting plate here.

Wireless Considerations

Connection Performance

A number of factors affect the performance of wireless connection. Consider the following guidelines to ensure high-range and stable connectivity.

- ✓ 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.

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

Security Checklist

Wireless networks are easy to install and convenient to use. However, wireless network signals can also be intercepted easily.

To prevent unauthorized users from connecting to your wireless network, follow the guidelines below.

- ✓ **Change the default wireless network name**

  Your device has a default Service Set Identifier (SSID) which is the wireless network name. Change the SSID with a unique name to identify your network. The SSID can be up to 32 characters in length.

- ✓ **Change the default password**

  Your device has a default password. You have to enter this password to change your network settings. Change the password to prevent unauthorized users from hacking into your network and changing the settings.

- ✓ **Enable MAC address filtering**

  Your device supports Media Access Control (MAC) address filtering. You can assign a MAC address on each computer that you want to connect to your wireless network. When MAC address filtering is enabled, only the computers with the specified MAC addresses are allowed access.

- ✓ **Enable encryption**

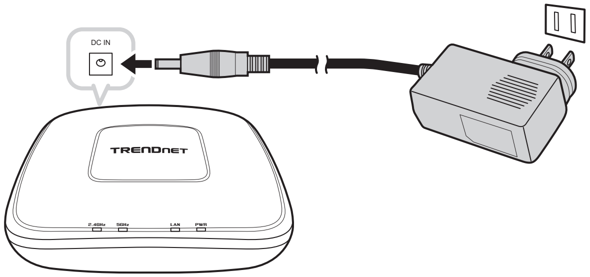
  Your device supports Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access (WAP/WPA2) encryption. To ensure a high level of security, enable the highest security encryption and use strong passphrases, avoid using words that can be found in the dictionary.

Installation

Make sure that all devices are powered off before starting installation.

Connect the Power

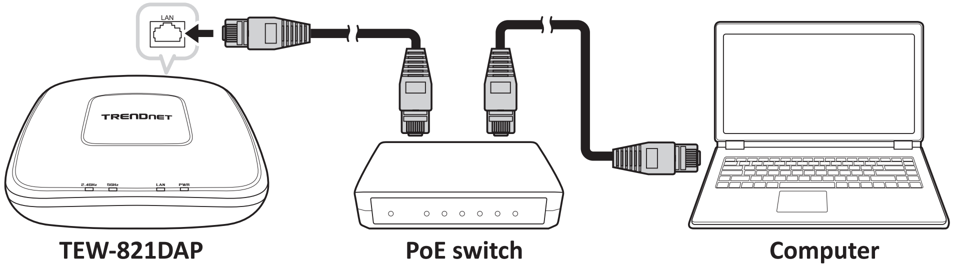
1 Connect the power adapter to the power port of your access point.
2 Plug the power adapter to a power outlet.
The access point powers up automatically.



Note: Use only the supplied power adapter. Using other power adapters may cause damage to the device.

Connect the Computer

1 Connect one end of the first RJ-45 cable to the Ethernet port of your access point.
2 Connect the other end of the first RJ-45 cable to the PoE switch.
3 Connect one end of the second RJ-45 cable to the PoE switch.
4 Connect the other end of the second RJ-45 cable to the LAN port of your computer.



Check the Connections

To ensure that all devices are properly connected, check the LED indicators on the front of your access point. For basic installation, the following LED must be lit:

✓ Power LED

✓ LAN LED

✓ 2.4G LED

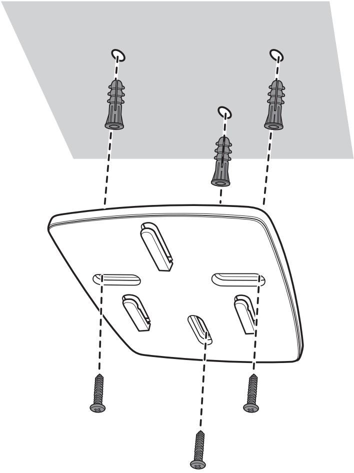
✓ 5G LED

The lighted LED indicators vary depending on the type of connection that you make. Refer to "Front View" on page 6 for more information on LED indicators.

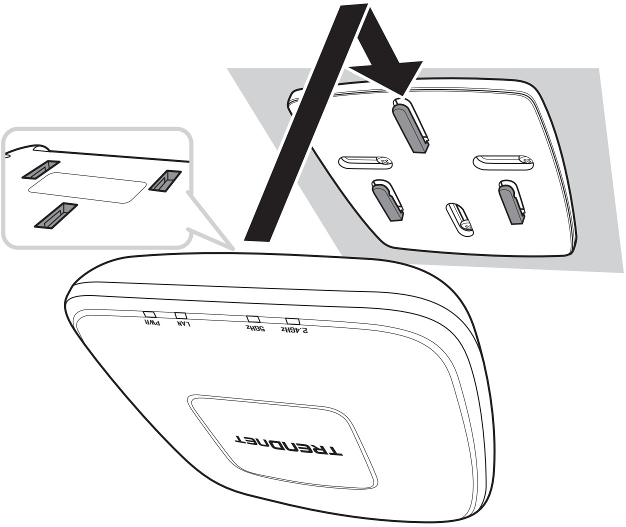
Ceiling Mounting

To ceiling mount the access point, do the following:

1. Drill three small holes on the mounting location and insert the plastic washers into the holes.
2. Then place the three supplied screws into the three holes at the ceiling bracket, and secure them into the holes on the ceiling.



3. Align and hook the TEW-821DAP to the ceiling bracket, and then push down to secure it into place.



Initial Setup

Configure the Computer

Below are procedures on how to configure your computer according to the operating system you are using:

Windows 7/8/8.1

1 Click **Start** > **Control Panel** > **Network and Sharing Center** > **Change Adapter Settings**.
2 Right-click the **Local Area Connection** icon.
3 Click **Properties**. Then click **Internet Protocol Version 4 (TCP/IPv4)**.
4 Select **Use the following IP address**.
5 Enter the required *IP address* and *Subnet mask*.
6 Click **OK**.

Windows Vista

1 Click **Start** > **Control Panel** > **Network and Internet** > **Manage Network Connections**.
2 Right-click the **Local Area Connection** icon, and then click **Properties**.
3 Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
4 Select **Use the following IP address**.
5 Enter the required *IP address* and *Subnet mask*.
6 Click **OK**.

Windows XP/2000

1 Click **Start** > **Control Panel**. Then double-click the **Network Connections** icon.
2 Right-click the **Local Area Connection** icon, and then click **Properties**.
3 Click **Internet Protocol (TCP/IP)**, and then click **Properties**.
4 Select **Use the following IP address**.
5 Enter the required *IP address* and *Subnet mask*.
6 Click **OK**.

Log in to Management Page

Default Settings

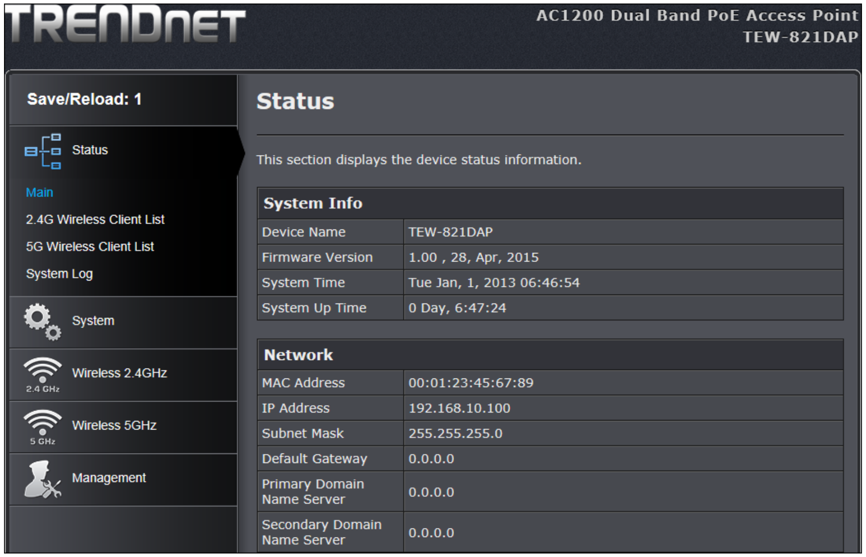
Before accessing the web-based management page, configure the IP address and subnet mask of your computer to the following:

Management IP:	**192.168.10.x**
Subnet mask:	**255.255.255.0**
Administrator name:	**admin**
Administrator password:	**admin**
Default SSID:	**(printed on pre-set label)**
Default SSID passphrase:	**(printed on pre-set label)**

Access the Management Page

1 Open your web browser and do one of the following:
- enter the URL/domain name http://tew-821dap, or
- enter the IP address http://192.168.10.100.

2 Enter the default user name and password, select your preferred language, and then click **Login**.
The main screen appears.



Status

This section displays the device status information.

System Info	
Device Name	TEW-821DAP
Firmware Version	1.00 , 28, Apr, 2015
System Time	Tue Jan, 1, 2013 06:46:54
System Up Time	0 Day, 6:47:24

Network	
MAC Address	00:01:23:45:67:89
IP Address	192.168.10.100
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary Domain Name Server	0.0.0.0
Secondary Domain Name Server	0.0.0.0

Note:

- *If you have changed the password in the Setup Wizard, you will need to login using the new password.*
- *User name and Password are case sensitive.*

Setup Wizard

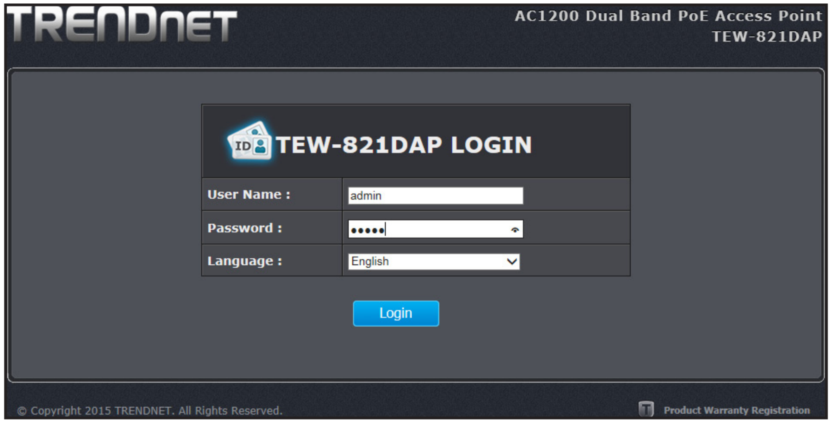
Setup wizard is provided as part of the web configuration utility. It sets up the basic administrator password and management IP address.

1 Open your web browser (i.e. Internet Explorer, Firefox, Safari, Chrome, or Opera) and enter http://192.168.10.100. Your access point will prompt you for a user name and password.

http://192.168.10.100/

Note: You can also access the device using the following URL/domain name: http://tew-821dap.

2 Enter the default user name and password, select your preferred language, and then click **Login**.
Default User Name: Admin
Default Password: admin



AC1200 Dual Band PoE Access Point
TEW-821DAP

TEW-821DAP LOGIN

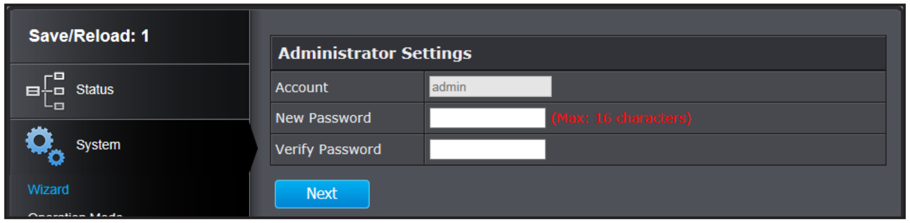
User Name : admin
Password : •••••
Language : English

TRENDNET
Login
© Copyright 2015 TRENDNET. All Rights Reserved.
Product Warranty Registration

Note: User name and Password are case sensitive.

3 Click **System** > **Wizard**. The following screen will appear.

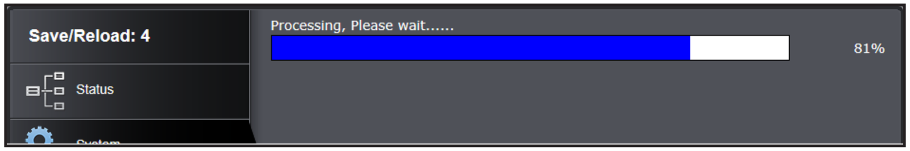
4 Enter your new administrator password and then click **Next** to continue.



Administrator Settings

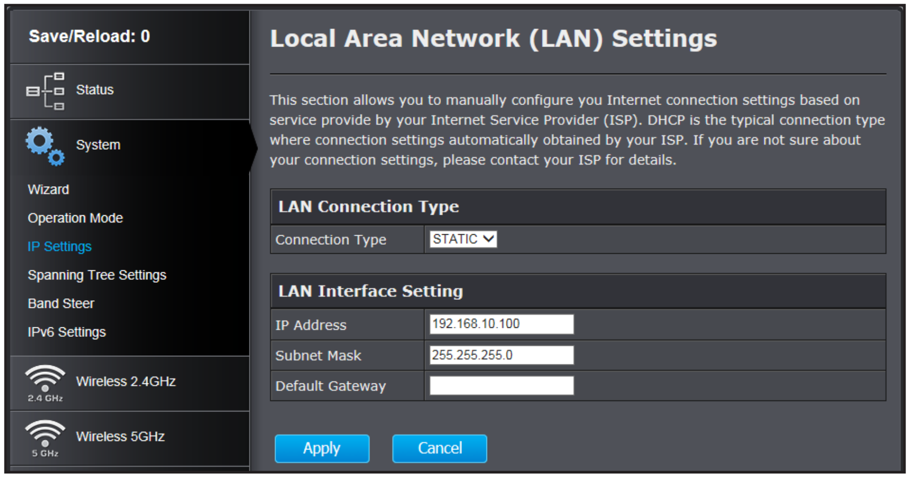
Account: admin
New Password: (Max: 16 characters)
Verify Password:

5 TEW-821DAP will apply password change and the Local Area Network (LAN) Settings page opens.



Processing, Please wait......
81%

6 Set the Connection Type as "STATIC". Enter the management IP address for this TEW-821DAP. 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-821DAP on network. Click **Apply**.



Local Area Network (LAN) Settings

This section allows you to manually configure you Internet connection settings based on service provide by your Internet Service Provider (ISP). DHCP is the typical connection type where connection settings automatically obtained by your ISP. If you are not sure about your connection settings, please contact your ISP for details.

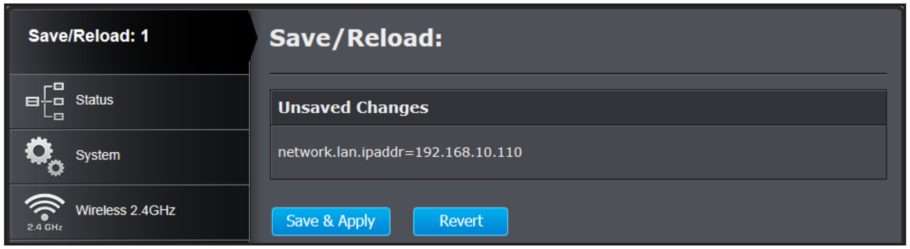
LAN Connection Type

Connection Type: STATIC

LAN Interface Setting

IP Address: 192.168.10.100
Subnet Mask: 255.255.255.0
Default Gateway:

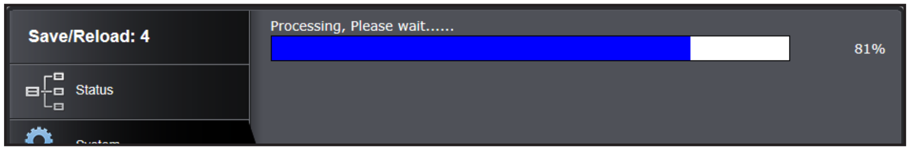
7 Click **Save** & **Apply**.



Unsaved Changes

network.lan.ipaddr=192.168.10.110

8 TEW-821DAP will apply IP address change and then reboot. Login, using the new IP address and/or new password.

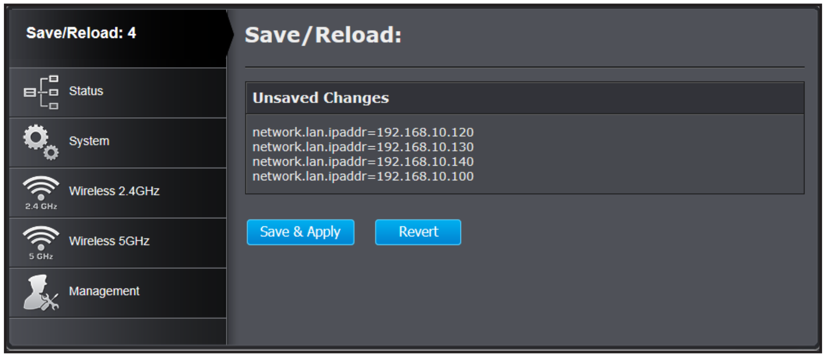


Processing, Please wait......

81%

Save / Reload

The TEW-821DAP 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 & Apply**. 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.



Unsaved Changes

network.lan.ipaddr=192.168.10.120
network.lan.ipaddr=192.168.10.130
network.lan.ipaddr=192.168.10.140
network.lan.ipaddr=192.168.10.100

Access Point Mode Management Page Structure

Status

- Main
- 2.4G Wireless Client List
- 5G Wireless Client List
- System Log

System

- Wizard
- Operation Mode
- IP Settings
- Spanning Tree Settings
- Band Steer
- IPv6 Settings

Wireless 2.4GHz

- Wireless Network
- Wireless MAC Filter
- Wireless Advanced Settings
- WPS

Wireless 5GHz

- Wireless Network
- Wireless MAC Filter
- Wireless Advanced Settings
- WPS

Management

- Administration
- Management VLAN
- Wireless Traffic Shaping
- SNMP Settings
- Backup/Restore Settings
- Upload Firmware
- Time and Date Settings
- Schedule
- CLI Settings
- Log
- Diagnostics
- LED Control

Client Bridge/AP Repeater Mode Management Page Structure

Status

- Main
- 2.4G Wireless Client List
- 5G Wireless Client List
- System Log

System

- Wizard
- Operation Mode
- IP Settings
- Spanning Tree Settings
- Band Steer
- IPv6 Settings

Wireless 2.4GHz

- Wireless Network
- Wireless Advanced Settings

Wireless 5GHz

- Wireless Network
- Wireless Advanced Settings

Management

- Administration
- Management VLAN
- Wireless Traffic Shaping
- SNMP Settings
- Backup/Restore Settings
- Upload Firmware
- Time and Date Settings
- Schedule
- CLI Settings
- Log
- Diagnostics
- LED Control

Basic System Configurations

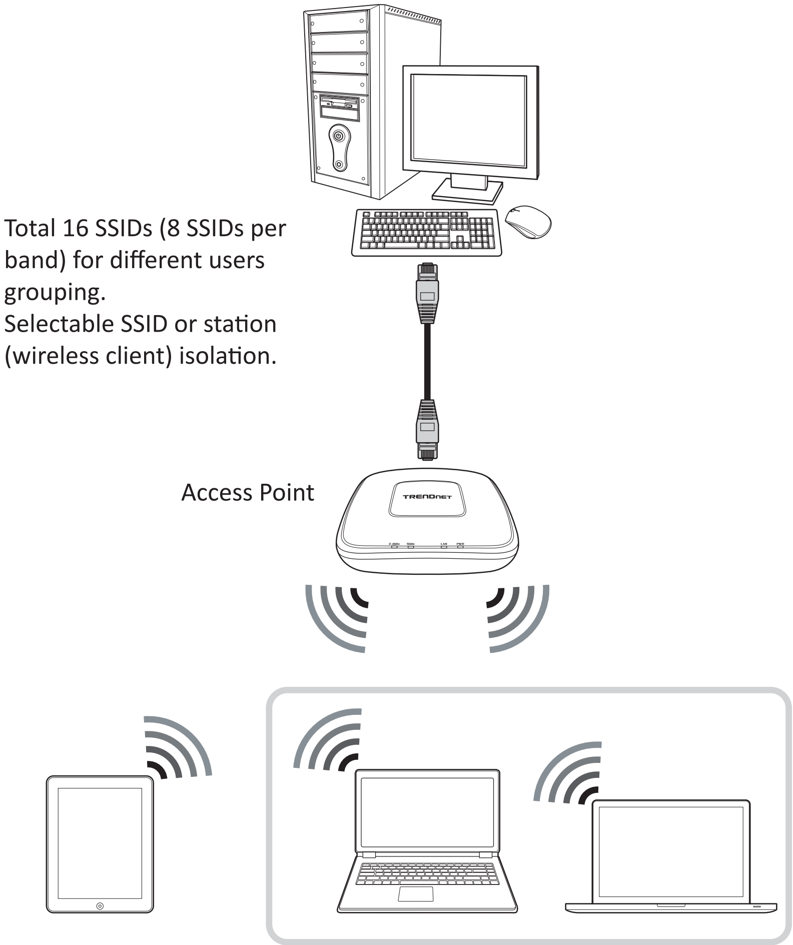
There are four operating modes provided by TEW-821DAP, Access Point, Client Bridge, WDS and Repeater. Configure the TEW-821DAP to different operation mode which service the best in your network.

Access Point Mode

This is the default operation mode. TEW-821DAP 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.

Note: This device has dual band wireless capability allowing the access point to broadcast a wireless network name on two separate bands, 2.4GHz and 5GHz. Wireless clients can connect to your access on either band depending on the wireless band supported by your wireless client. The 2.4GHz band is more commonly used and supported for general applications such as Internet access and web browsing. The 5GHz band is less commonly used and supported which can be more useful for higher or stable bandwidth application requirements such as media streaming as this band may be less likely affected by neighboring wireless networks operating on the 5GHz band.

- Total 16 SSIDs (8 SSIDs per band) for different users grouping.
- Selectable SSID or station (wireless client) isolation.



Multiple SSID

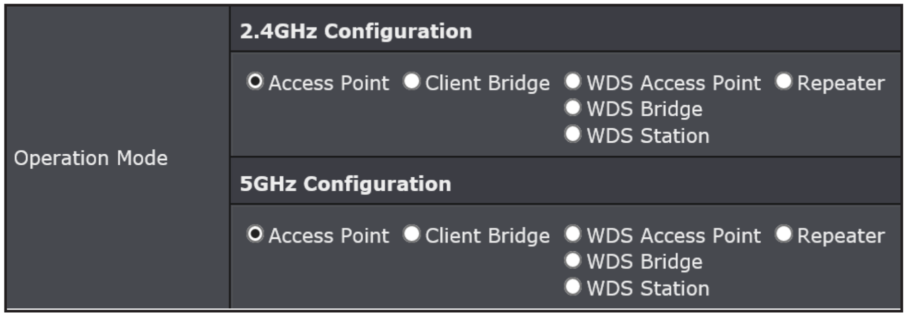
SSID/STA isolation

Configuring the Device as Access Point

System > Operation Mode

Note: By default, the device function is set to Access Point mode.

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).
2 Click **System** > **Operation Mode**.
3 In *Operation Mode* section, select **Access Point**.



Operation Mode	**2.4GHz Configuration**
	● Access Point ○ Client Bridge ○ WDS Access Point ○ Repeater ○ WDS Bridge ○ WDS Station
	5GHz Configuration
	● Access Point ○ Client Bridge ○ WDS Access Point ○ Repeater ○ WDS Bridge ○ WDS Station

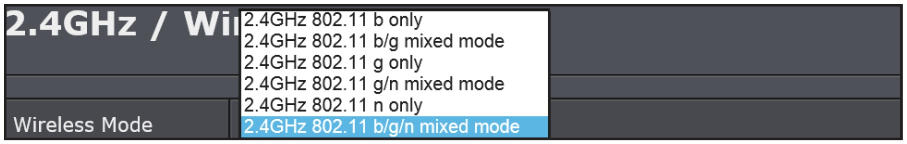
4 Click **Apply** to save changes.

Note: To discard the changes, click **Cancel**.

Using Access Point Mode

Wireless 2.4GHz or Wireless 5GHz > Wireless Network

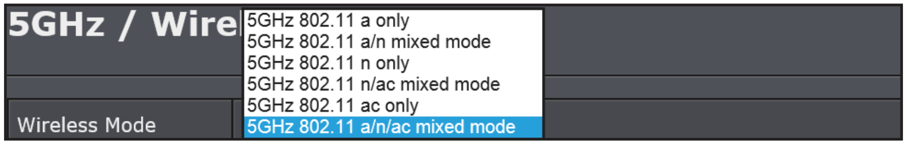
1 Log into your access point management page (refer to "Log in to Management Page" on page 10).
2 Configure the following settings, click **Apply** when finished.
- **Wireless Mode:** Choose between N only, G only, B only, B/G mixed, or B/G/N mixed mode. The rule of the thumb is to choose single mode if your devices all work in the same mode. Mixed mode increases compatibility, but sometimes lowers the data speed.



2.4GHz / Wi

Wireless Mode: 2.4GHz 802.11 b only / 2.4GHz 802.11 b/g mixed mode / 2.4GHz 802.11 g only / 2.4GHz 802.11 g/n mixed mode / 2.4GHz 802.11 n only / 2.4GHz 802.11 b/g/n mixed mode (selected)

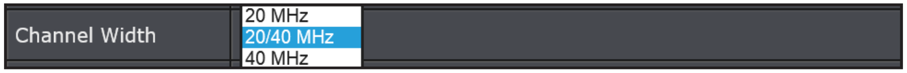
or



5GHz / Wire

Wireless Mode: 5GHz 802.11 a only / 5GHz 802.11 a/n mixed mode / 5GHz 802.11 n only / 5GHz 802.11 n/ac mixed mode / 5GHz 802.11 ac only / 5GHz 802.11 a/n/ac mixed mode (selected)

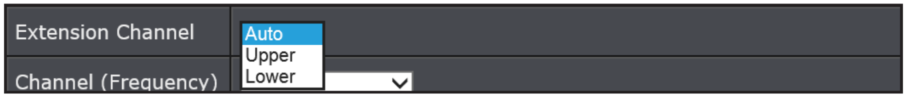
- **Channel Width**: Select the appropriate channel width for your wireless network.



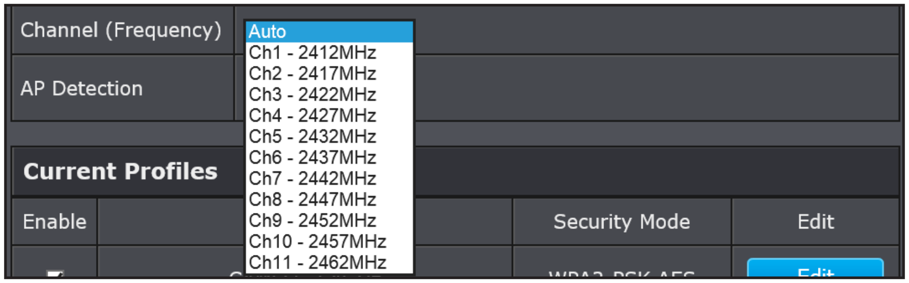
Channel Width: 20 MHz / 20/40 MHz (selected) / 40 MHz

  - 20 MHz: This mode operates using a single 20MHz channel for wireless devices connecting at 802.11n on both 2.4GHz and 5GHz. This setting may provide more stability than **Auto 20/40MHz** for connectivity in busy wireless environments where there are several neighboring wireless networks in the area.
  - Auto 20/40MHz: When **Auto 20/40MHz** is active, this mode is capable of providing higher performance only if the wireless devices support the channel bandwidth settings. Enabling **Auto 20/40MHz** typically results in substantial performance increases when connecting an 802.11n client.
  - The 40 MHz channel width allows for twice the usable radio spectrum to transmit data, doubling performance compared to a normal 20 MHz channel width.

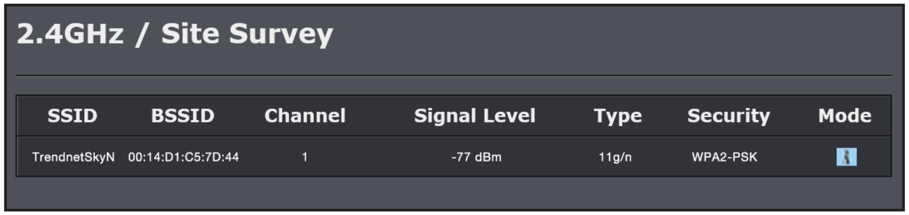
- **Extension Channel:** When you choose manual channel selection and 20/40MHz or 40MHz in channel width, you can choose which neighbour channel you want to combine, upper channel or lower channel, or auto to let the device to decide.



- **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.)



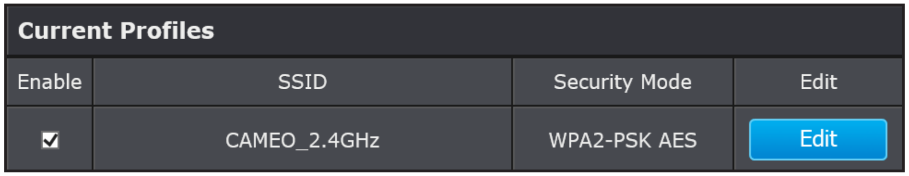
- **AP Detection:** Before you setup your TEW-821DAP wireless settings, you may want to know what signal are currently broadcasting. Click **Scan** to do a site survey and list the running access points around you.



2.4GHz / Site Survey

SSID	BSSID	Channel	Signal Level	Type	Security	Mode
TrendnetSkyN	00:14:D1:C5:7D:44	1	-77 dBm	11g/n	WPA2-PSK	

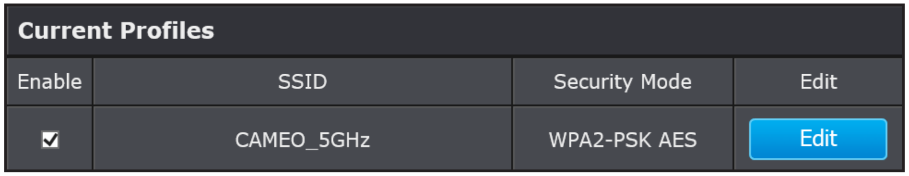
- **Current Profile:** General setups options for your 2.4GHz / 5GHz wireless connection. You can setup up to eight SSIDs for different groups of users. Do any of the following:
  - Click the **Enable** checkbox to enable the wireless profile.
  - Click **Edit** to modify the settings and after modifications are done, click **Apply**.



Current Profiles

Enable	SSID	Security Mode	Edit
☑	CAMEO_2.4GHz	WPA2-PSK AES	Edit

or



Current Profiles

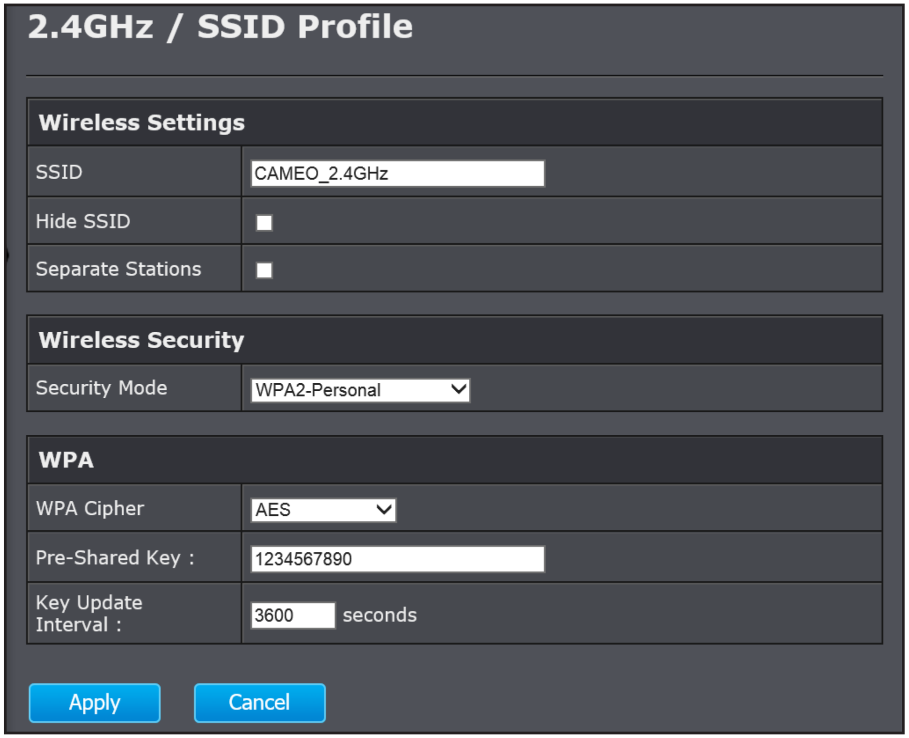
Enable	SSID	Security Mode	Edit
☑	CAMEO_5GHz	WPA2-PSK AES	Edit

Wireless Settings:

- **SSID:** Select the human readable SSID to be easily identified. You can choose any combination with 1 to 32 letters.
- **Hide SSID:** Select this checkbox to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
- **Separate Stations:** 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 WEP-OPEN, WEP-SHARED, WEP-AUTO, WPA-Personal, WPA2-Personal, WPA2-Personal Mixed, WPA-Enterprise, WPA2-Enterprise Mixed. Please see more in "Wireless Networking and Security" on page 17.



2.4GHz / SSID Profile

Wireless Settings

SSID	CAMEO_2.4GHz
Hide SSID	□
Separate Stations	□

Wireless Security

Security Mode	WPA2-Personal

WPA

WPA Cipher	AES
Pre-Shared Key :	1234567890
Key Update Interval :	3600 seconds

Wireless Networking and Security

Tips to Improve Wireless Reception

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

- Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
  - ✓ For the widest coverage area, install your access point near the center of your home, and near the ceiling, if possible.
  - ✓ 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.
  - ✓ 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.
  - ✓ Place the access point in a location away from other electronics, motors, and fluorescent lighting.
  - ✓ 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.
- Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.
- Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.
- Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.

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

Choose the Security Type for Wireless Network

Setting up wireless security is very important. Leaving your wireless network open and unsecure could expose your entire network and personal files to outsiders. TRENDnet recommends reading through this entire section and setting up wireless security on your new 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 802.11 b 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.*

Security Standard	WEP	WPA	WPA2
Compatible Wireless Standards	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g (802.11n devices will operate at 802.11g to connect using this standard)	IEEE 802.11a/b/g/n
Highest Performance Under This Setting	Up to 54Mbps	Up to 54Mbps	Up to 300Mbps
Encryption Strength	Low	Medium	High
Additional Options	Open System or Shared Key, HEX or ASCII, Different key sizes	TKIP or AES, Preshared Key or RADIUS	TKIP or AES, Preshared Key or RADIUS
Recommended Configuration	Open System ASCII 13 characters	TKIP Preshared Key 8-63 characters	AES Preshared Key 8-63 characters

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

Secure your Wireless Network

Wireless 2.4GHz or Wireless 5GHz > Wireless Network

After you have determined which security type to use for your wireless network (refer to "Choose the Security Type for Wireless Network" on page 18), you can set up wireless security.

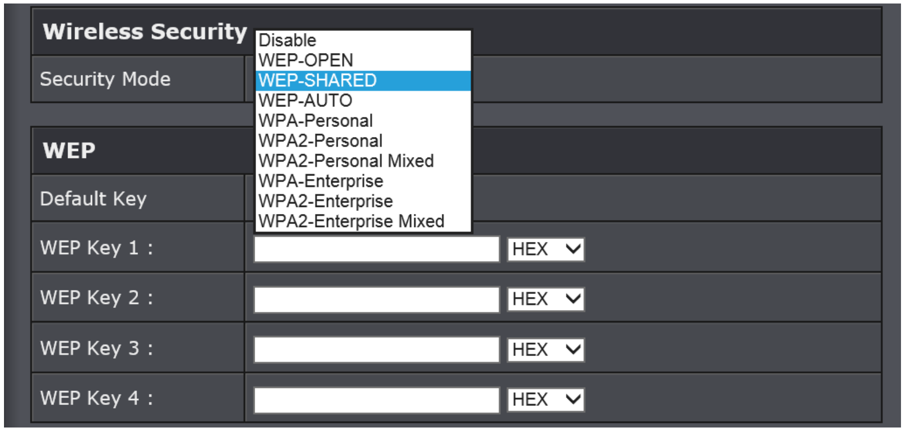
Note: By default, your access point is configured with a predefined wireless network name (SSID) and security key using WPA-Personal. The predefined wireless network name and security can be found on the sticker on the side of the access point or on the device label at the bottom of the access point.

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 In Current Profile section, click **Edit** next to the wireless profile to select the wireless security type.

3 In *Wireless Security* section, select the preferred Security Mode:

- Select between WPA-OPEN, WPA-SHARED, or WPA-AUTO. WPA-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. WPA-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 WPA-AUTO if you are not sure which authentication type is used. Click **Apply** to save the changes.



Wireless Security

Security Mode: WEP-SHARED

WEP

Default Key

WEP Key 1 : HEX

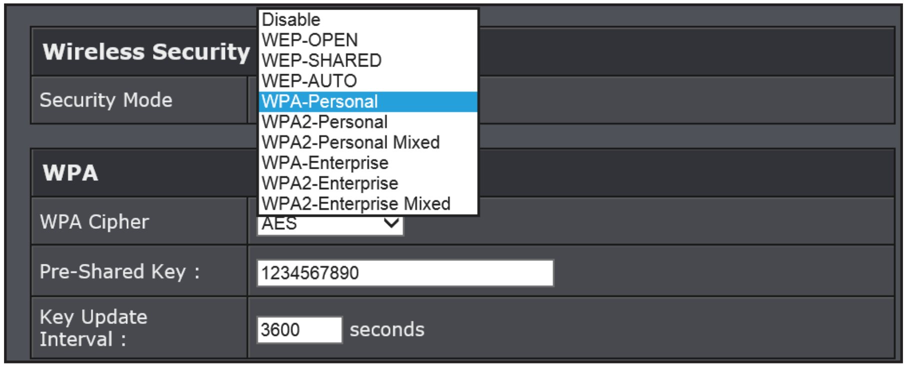
WEP Key 2 : HEX

WEP Key 3 : HEX

WEP Key 4 : HEX

- Default Key: You may choose one of your four different WEP keys from below.
- WEP Key 1 to 4: Enter the WEP key. This is the password or key that is used to connect your computer to this access point wirelessly. You can enter four different WEP keys.
- HEX / ASCII: 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.

- If the security type is set to **WPA-Personal**, review the WPA-Personal settings to configure and click **Apply** to save the changes.



Wireless Security

Security Mode: WPA-Personal

WPA

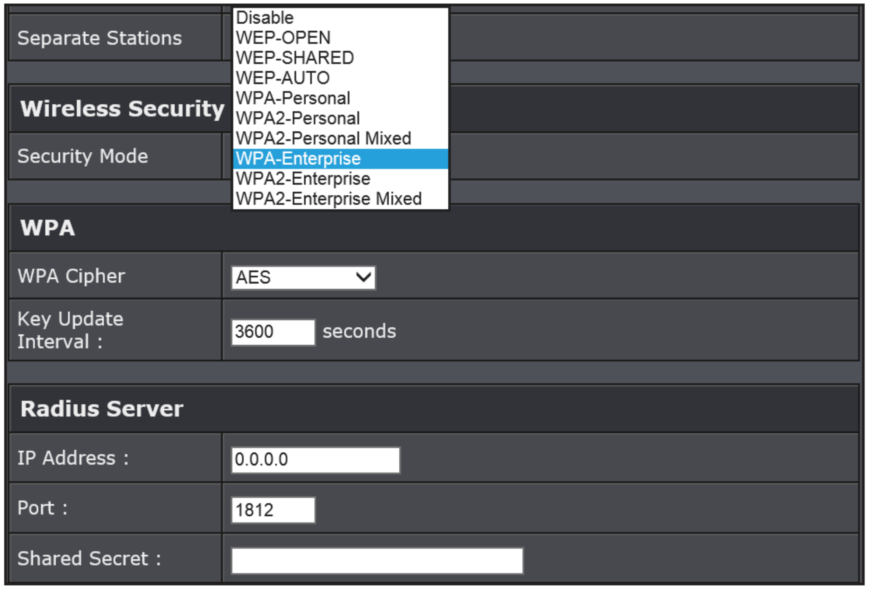
WPA Cipher: AES

Pre-Shared Key : 1234567890

Key Update Interval : 3600 seconds

- Security Mode: Select the WPA security type.
- WPA Cipher: Select 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. With the "TKIP and AES" option, the device negotiates the cipher type with the client, and uses AES when available.

- If the security type is set to **WPA-Enterprise**, review the WPA-Enterprise settings to configure and click **Apply** to save the changes. This security type is also known as EAP (Extensible Authentication Protocol) or Remote Authentication Dial-In User Service or RADIUS.



Separate Stations

Wireless Security

Security Mode: WPA-Enterprise

WPA

WPA Cipher	AES
Key Update Interval :	3600 seconds

Radius Server

IP Address :	0.0.0.0
Port :	1812
Shared Secret :	

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

- 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).
- IP Address: Enter the IP address of the RADIUS server. (i.e. 192.168.10.250)
- 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.
- 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.

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.

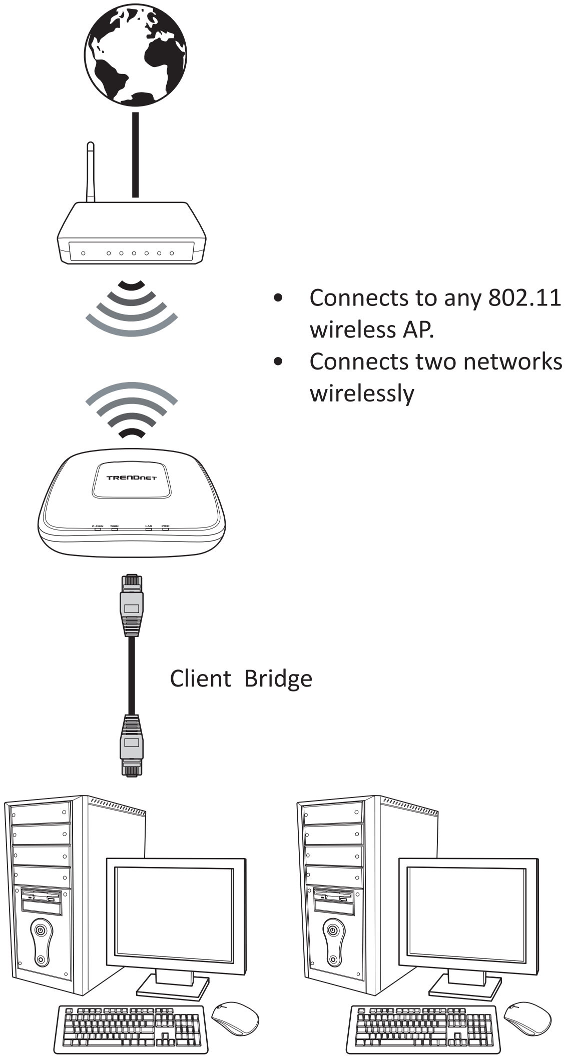
There are two methods the WPS feature can easily connect your wireless devices to your network.

- Push Button Configuration (PBC) method ("PBC (Software/Virtual Push Button)" on page 38).
- PIN (Personal Identification Number) method ("PIN (Personal Identification Number)" on page 39).

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

Client Bridge Mode

Client Bridge 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 the LAN port using an Ethernet cable to establish wired connectivity to your network. When using this mode, please note that Client Bridge mode can only function using one band at a time, 2.4GHz or 5GHz and other modes cannot be used simultaneously.



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

Configuring the Device as Client Bridge

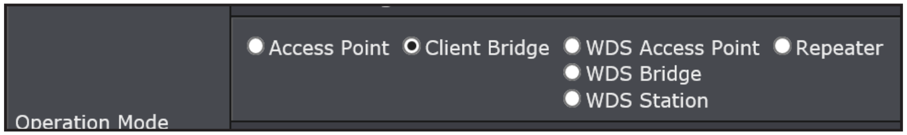
System > Operation Mode

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click **System** > **Operation Mode**.

3 In *Operation Mode* section, select **Client Bridge**.

Note: In the following example the Client Bridge mode is selected for 2.4GHz wireless profile.



Operation Mode

○ Access Point ● Client Bridge ○ WDS Access Point ○ Repeater
○ WDS Bridge
○ WDS Station

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

Note: To discard the changes, click Cancel.

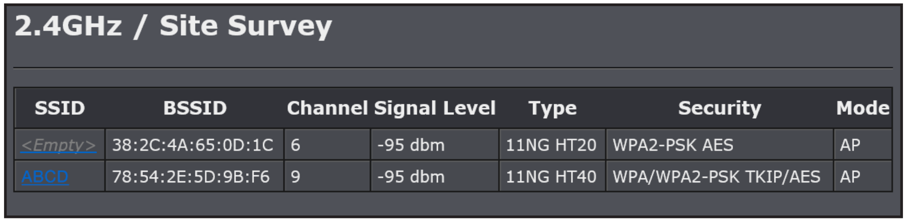
Using Client Bridge Mode

Wireless 2.4GHz or Wireless 5GHz > Wireless Network

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 In *Wireless 2.4GHz or Wireless 5GHz* > *Wireless Network* > *SSID* section, specify the static SSID manually or click *Wireless 2.4GHz or Wireless 5GHz* > *Wireless Network* > *Site Survey*.

3 The available networks are listed. Select a network to connect to.



2.4GHz / Site Survey

SSID	BSSID	Channel	Signal Level	Type	Security	Mode
<Empty>	38:2C:4A:65:0D:1C	6	-95 dbm	11NG HT20	WPA2-PSK AES	AP
ABCD	78:54:2E:5D:9B:F6	9	-95 dbm	11NG HT40	WPA/WPA2-PSK TKIP/AES	AP

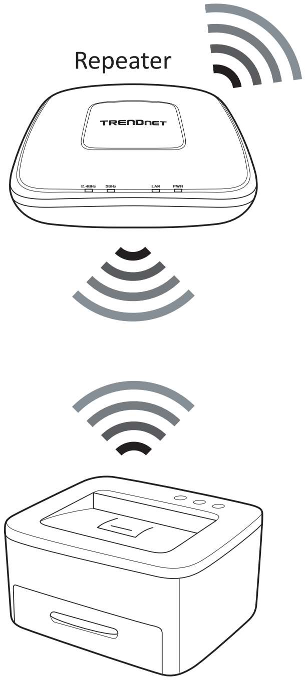
*Note: If you are unable to find your wireless network in the list, click **Refresh** to rescan for the available networks.*

4 Click on the SSID field to connect to the selected wireless network.

5 Click **Apply** to save the wireless network.

Repeater Mode

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-821DAP matches the wireless access points you want to repeat in same wireless settings including SSID, channel and wireless encryption settings.



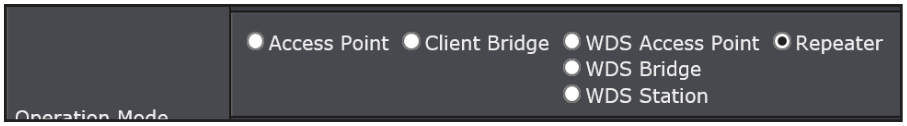
Configuring the Device as Repeater

System > Operation Mode

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click ***System > Operation Mode***.

3 In *Operation Mode* section, select **Repeater**.



Operation Mode

○ Access Point ○ Client Bridge ○ WDS Access Point ● Repeater
○ WDS Bridge
○ WDS Station

4 Click **Apply** to save changes or **Cancel** to discard the changes.

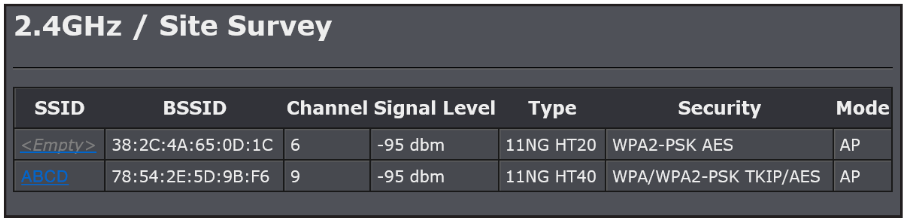
Using Repeater Mode

Wireless 2.4GHz or Wireless 5GHz > Wireless Network

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 In *Wireless 2.4GHz or Wireless 5GHz > Wireless Network > SSID* section, specify the static SSID manually or click *Wireless 2.4GHz or Wireless 5GHz > Wireless Network > Site Survey*.

3 The available networks are listed. Select a network to connect to.



2.4GHz / Site Survey

SSID	BSSID	Channel	Signal Level	Type	Security	Mode
<Empty>	38:2C:4A:65:0D:1C	6	-95 dbm	11NG HT20	WPA2-PSK AES	AP
ABCD	78:54:2E:5D:9B:F6	9	-95 dbm	11NG HT40	WPA/WPA2-PSK TKIP/AES	AP

*Note: If you are unable to find your wireless network in the list, click **Refresh** to rescan for the available networks.*

4 Click on the SSID field to connect to the selected wireless network.

5 Click **Apply** to save the wireless network.

Wireless Distribution System (WDS)

IMPORTANT: Deploy ONLY multiple TEW-821DAPs in a single DS (distribution system).
WDS may not work with other products due to its non-standard nature.

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 seamingless hand-over for wireless clients roaming between different access points. 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-821DAP, 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.

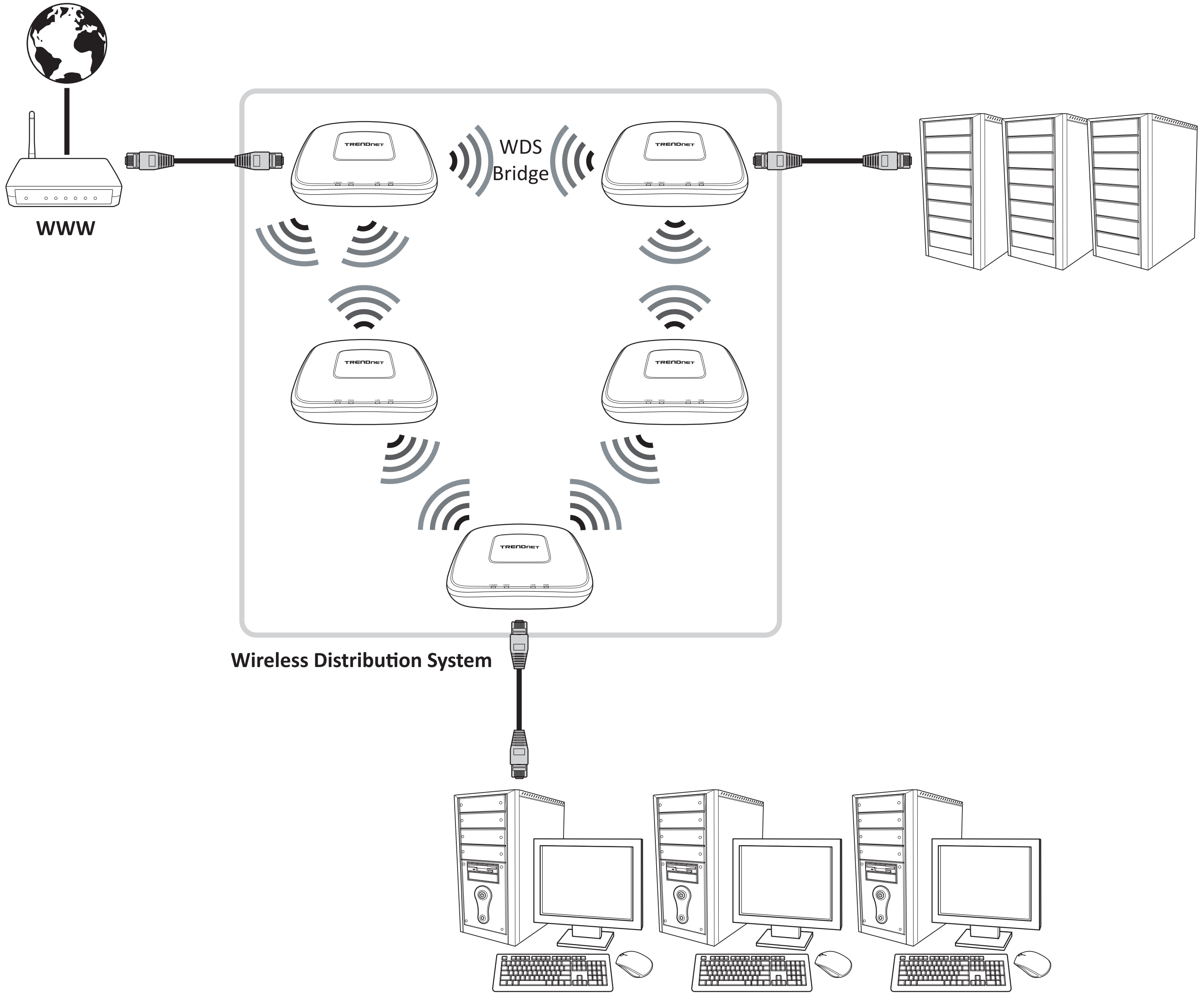
The 802.11 standard only uses three MAC addresses for frames transmitted between the Access Point and the Station. Frames transmitted from the station to the AP don't include the Ethernet source MAC address of the requesting host and response frames are missing the destination Ethernet MAC to address 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.

You have to use multiple TEW-821DAPs 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.

WDS Bridge

In this mode, the selected interface wirelessly communicate to 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 next hop packet forwarding. Your neig, 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.


WWW
WDS
Bridge
Wireless Distribution System

Creating a WDS Bridge

System > Operation Mode

Note: By default, your access point is configured with a predefined wireless network name (SSID) and security key using WPA-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.

To configure a WDS bridge between two TEW-821DAP access points:

- Make note of the wireless MAC address of both access points. Refer to "System Information" on page 28 for checking the status page.

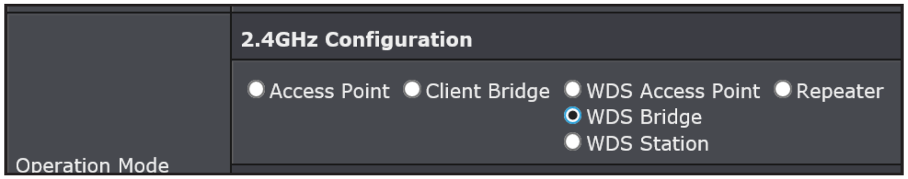
  Note: Please note that 2.4GHz and 5GHz bands will have two different MAC addresses. If using the 2.4GHz band wireless MAC address, please use the 2.4GHz wireless MAC address for all other WDS supported devices to bridge and if using the 5GHz band wireless MAC address, use the 5GHz wireless MAC address for all other WDS supported devices to bridge.

- Make sure the IP address on each WDS supported access is point is different and on the same IP network/subnet. Please refer to "Configure IP Settings" on page 30 for changing access point IP address.

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *System > Operation Mode*.

3 On *Operation Mode* section, select **WDS Bridge**.



2.4GHz Configuration

Operation Mode: ○ Access Point ○ Client Bridge ○ WDS Access Point ○ Repeater ● WDS Bridge ○ WDS Station

4 Click **Apply** to save changes or **Cancel** to discard the changes.

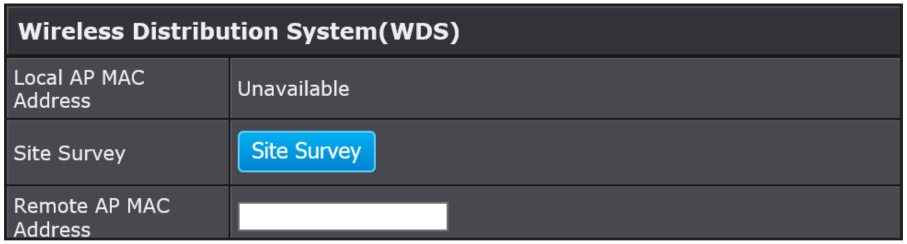
Using a WDS Bridge

Wireless 2.4GHz or Wireless 5GHz > WDS Link Settings

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 In *Wireless 2.4GHz or Wireless 5GHz > Wireless Link Settings > Remote AP MAC Address* section, do on of the following:

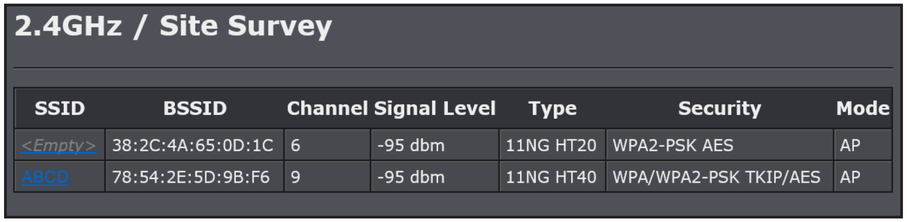
- Specify the remote AP MAC address manually, and click **Apply** or
- Click *Wireless 2.4GHz or Wireless 5GHz > Wireless Link Settings > Site Survey*.



Wireless Distribution System(WDS)

Local AP MAC Address	Unavailable
Site Survey	Site Survey
Remote AP MAC Address	

3 The available networks are listed. Select a network to connect to.



2.4GHz / Site Survey

SSID	BSSID	Channel	Signal Level	Type	Security	Mode
<Empty>	38:2C:4A:65:0D:1C	6	-95 dbm	11NG HT20	WPA2-PSK AES	AP
ABCD	78:54:2E:5D:9B:F6	9	-95 dbm	11NG HT40	WPA/WPA2-PSK TKIP/AES	AP

*Note: If you are unable to find your wireless network in the list, click **Refresh** to rescan for the available networks.*

4 Click on the SSID field to connect to the selected wireless network.

5 Click **Apply** to save the wireless network.

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.

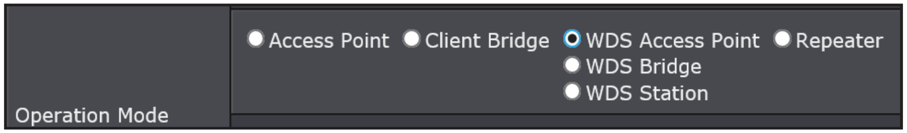
Creating a WDS Access Point

System > Operation Mode

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *System > Operation Mode*.

3 On *Operation Mode* section, select **WDS Access Point**.



Operation Mode: ○ Access Point ○ Client Bridge ● WDS Access Point ○ Repeater ○ WDS Bridge ○ WDS Station

4 Click **Apply** to save changes or **Cancel** to discard the changes.

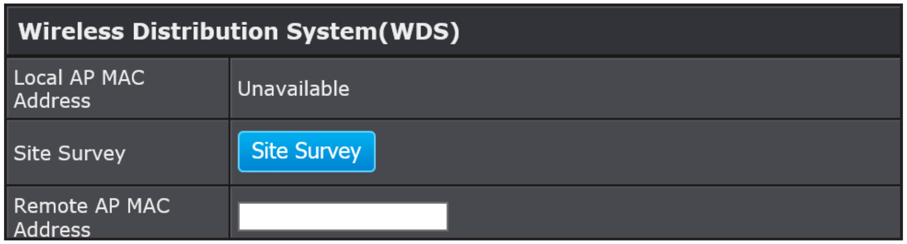
Using a WDS Bridge

Wireless 2.4GHz or Wireless 5GHz > WDS Link Settings

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 In *Wireless 2.4GHz or Wireless 5GHz* **>** *Wireless Link Settings* **>** *Remote AP MAC Address* section, do one of the following:

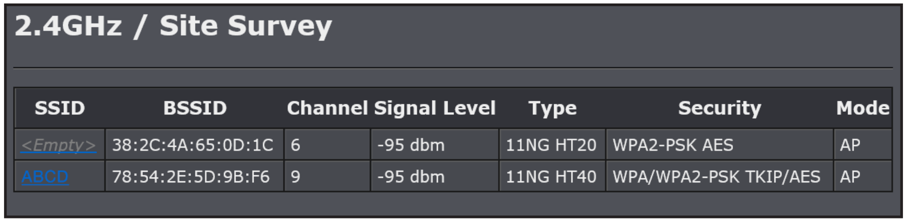
- Specify the remote AP MAC address manually and click **Apply** or
- Click *Wireless 2.4GHz or Wireless 5GHz > Wireless Link Settings > Site Survey*.



Wireless Distribution System(WDS)

Local AP MAC Address	Unavailable
Site Survey	Site Survey
Remote AP MAC Address	

3 The available networks are listed. Select a network to connect to.



2.4GHz / Site Survey

SSID	BSSID	Channel	Signal Level	Type	Security	Mode
<Empty>	38:2C:4A:65:0D:1C	6	-95 dbm	11NG HT20	WPA2-PSK AES	AP
ABCD	78:54:2E:5D:9B:F6	9	-95 dbm	11NG HT40	WPA/WPA2-PSK TKIP/AES	AP

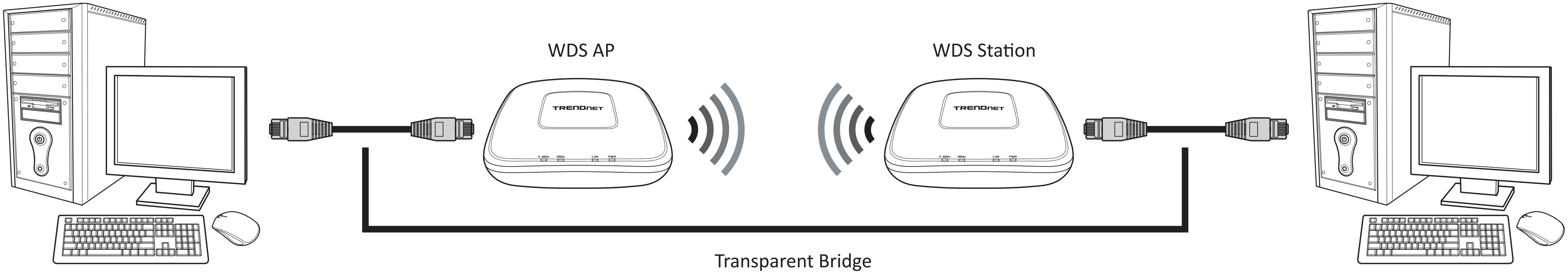
Note: If you are unable to find your wireless network in the list, click ***Refresh*** *to rescan for the available networks.*

4 Click on the SSID field to connect to the selected wireless network.

5 Click **Apply** to save the wireless network.

WDS Station

Pair with WDS AP, you can build a transparent bridge for layer 2 requirements.



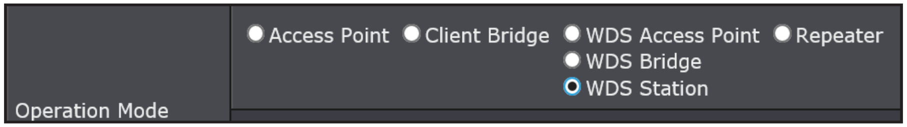
Creating a WDS Station

System > **Operation Mode**

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *System > Operation Mode*.

3 On *Operation Mode* section, select **WDS station**.



Operation Mode	○ Access Point ○ Client Bridge ○ WDS Access Point ○ Repeater ○ WDS Bridge ● WDS Station

4 Click **Apply** to save changes or **Cancel** to discard the changes.

Using a WDS Station

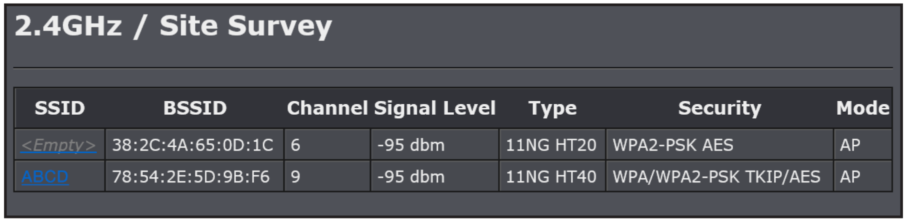
Wireless 2.4GHz or **Wireless 5GHz** > **Wireless Network**

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 In *Wireless 2.4GHz or Wireless 5GHz > Wireless Network > SSID* section, do one of the following:

- Specify the static SSID manually and click **Apply** or
- Click *Wireless 2.4GHz or Wireless 5GHz > Wireless Network > Site Survey*.

3 The available networks are listed. Select a network to connect to.



2.4GHz / Site Survey

SSID	BSSID	Channel	Signal Level	Type	Security	Mode
<Empty>	38:2C:4A:65:0D:1C	6	-95 dbm	11NG HT20	WPA2-PSK AES	AP
ABCD	78:54:2E:5D:9B:F6	9	-95 dbm	11NG HT40	WPA/WPA2-PSK TKIP/AES	AP

Note: If you are unable to find your wireless network in the list, click ***Refresh*** *to rescan for the available networks.*

4 Click on the SSID field to connect to the selected wireless network.

5 Click **Apply** to save the wireless network.

View System Status

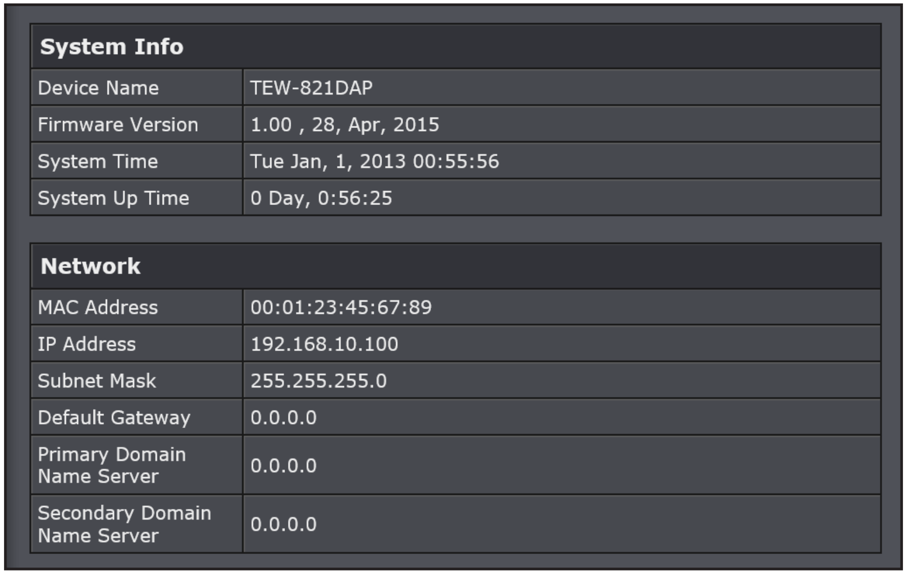
System Information

Status > **Main**

View the device information, and LAN and Wireless LAN configuration.

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *Status > Main*.

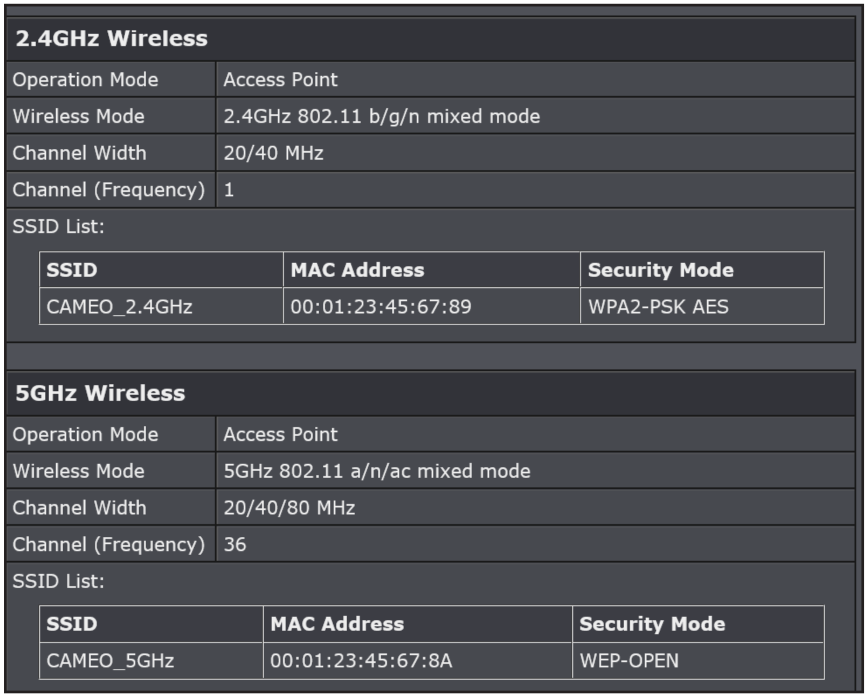


System Info	
Device Name	TEW-821DAP
Firmware Version	1.00 , 28, Apr, 2015
System Time	Tue Jan, 1, 2013 00:55:56
System Up Time	0 Day, 0:56:25

Network	
MAC Address	00:01:23:45:67:89
IP Address	192.168.10.100
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary Domain Name Server	0.0.0.0
Secondary Domain Name Server	0.0.0.0

- In the *System Info* section:
  - Device Name: Display name of this device that is recognized by other network devices such as SNMP.
  - Firmware Version: Display currently run firmware version.
  - System Time: Display the current time is important for schedule control and log accuracy.
  - System Up Time: Display how long the system has been running without reboot.

- In the *Network* section:
  - MAC Address: Display the MAC address of the access point.
  - IP Address: Display address of the TEW-821DAP.
  - Subnet Mask: Display network range of IP address.
  - Default Gateway: Display the default route going further from TEW-821DAP subnet.
  - Primary Domain Name Server: Display primary domain server address.
  - Secondary Domain Name Server: Display secondary domain server address.



2.4GHz Wireless

Operation Mode	Access Point
Wireless Mode	2.4GHz 802.11 b/g/n mixed mode
Channel Width	20/40 MHz
Channel (Frequency)	1

SSID List:

SSID	MAC Address	Security Mode
CAMEO_2.4GHz	00:01:23:45:67:89	WPA2-PSK AES

5GHz Wireless

Operation Mode	Access Point
Wireless Mode	5GHz 802.11 a/n/ac mixed mode
Channel Width	20/40/80 MHz
Channel (Frequency)	36

SSID List:

SSID	MAC Address	Security Mode
CAMEO_5GHz	00:01:23:45:67:8A	WEP-OPEN

- On the *2.4GHz / 5GHz Wireless* section:
  - Operation Mode: Display which wireless mode the 2.4GHz / 5GHz interface is set to.
  - Wireless Mode: Display which 802.11 wireless mode is set and running on the 2.4GHz / 5GHz interface.
  - Channel Width: Wireless Channel Bandwidth.
  - Channel (Frequency): Display which 2.4GHz / 5GHz wireless channel (and frequency) is in use.
  - SSID List: Display information on SSID, MAC address, and security mode.

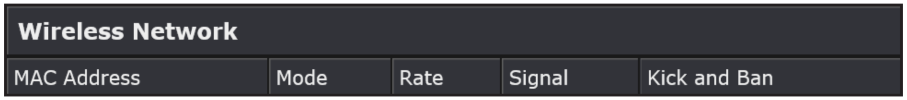
2.4G Wireless Client List

Status > 2.4G Wireless Client List

To view all wireless clients connected to the 2.4GHz interface, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *Status > 2.4G Wireless Client Lis***t**.
The list of connected wireless clients is displayed on the screen.



Wireless Network

MAC Address	Mode	Rate	Signal	Kick and Ban

3 Click **Kick and Ban** to send this client to MAC address filter list.

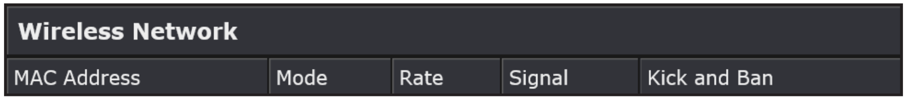
5G Wireless Client List

Status > 5G Wireless Client List

To view all wireless clients connected to the 5GHz interface, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *Status > 5G Wireless Client List*.
The list of connected wireless clients is displayed on the screen.



Wireless Network

MAC Address	Mode	Rate	Signal	Kick and Ban

3 Click **Kick and Ban** to send this client to MAC address filter list.

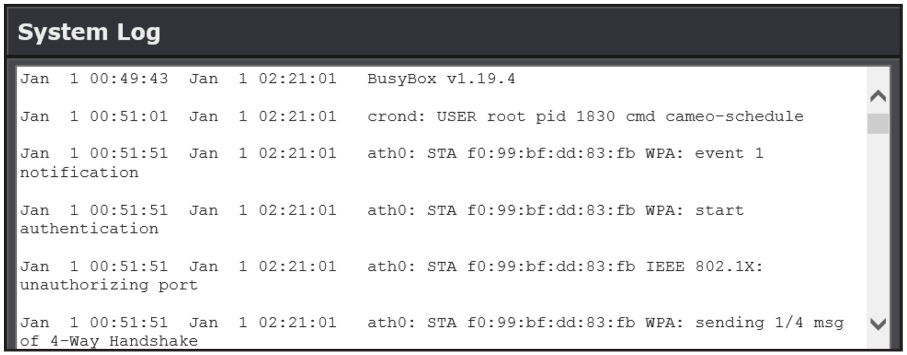
System Log

Status > System Log

To view a running log of the access point's system statistics, events and activities, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *Status > System Log*.



System Log

```
Jan  1 00:49:43  Jan  1 02:21:01   BusyBox v1.19.4

Jan  1 00:51:01  Jan  1 02:21:01   crond: USER root pid 1830 cmd cameo-schedule

Jan  1 00:51:51  Jan  1 02:21:01   ath0: STA f0:99:bf:dd:83:fb WPA: event 1
notification

Jan  1 00:51:51  Jan  1 02:21:01   ath0: STA f0:99:bf:dd:83:fb WPA: start
authentication

Jan  1 00:51:51  Jan  1 02:21:01   ath0: STA f0:99:bf:dd:83:fb IEEE 802.1X:
unauthorizing port

Jan  1 00:51:51  Jan  1 02:21:01   ath0: STA f0:99:bf:dd:83:fb WPA: sending 1/4 msg
of 4-Way Handshake
```

Configure IP Settings

Status > IP Settings

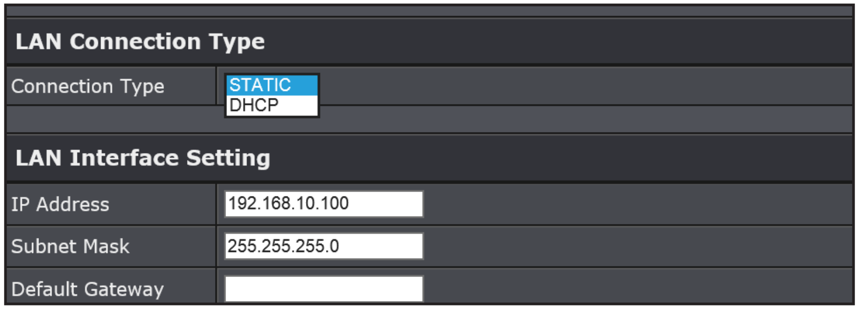
The TEW-821DAP has a static IP (192.168.10.100) set for management purposes. You can change this IP address to fit your network plan or manage multiple TRENDnet access points. You can also set the TEW-821DAP to DHCP client to accept an IP dynamically.

Note: You can change the IP settings also using the System > Wizard menu.

To start changing the IP settings, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *System > IP Settings*.



LAN Connection Type

Connection Type	STATIC DHCP

LAN Interface Setting

IP Address	192.168.10.100
Subnet Mask	255.255.255.0
Default Gateway	

3 Modify the following *LAN Connection Type* field:

- **Connection Type:** Choose one of the following:
  - Static to manually configure the IP address settings of the access point.
  - DHCP to set the access point to automatically obtain IP address settings from a DHCP server.

4 Modify any of the following *LAN Interface Setting* fields:

- **IP Address:** Specify an IP address.
- **Subnet Mask:** Specify a subnet mask for the IP address.
- **Default Gateway**: Default route for the TEW-821DAP.

5 Click **Apply** to save the LAN settings or **Cancel** to discard the changes.

Configure Spanning Tree

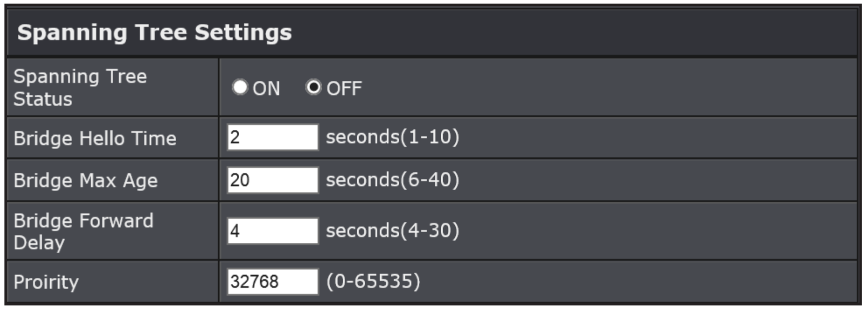
System > Spanning Tree Settings

The TEW-821DAP is designed for end point access as well as backbone connection. To avoid network looping, you can enable 802.1d spanning tree protocol.

To configure the spanning tree, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *System > Spanning Tree Settings*.



Spanning Tree Settings

Spanning Tree Status	○ ON ● OFF
Bridge Hello Time	2 seconds(1-10)
Bridge Max Age	20 seconds(6-40)
Bridge Forward Delay	4 seconds(4-30)
Proirity	32768 (0-65535)

3 Modify any of the following *Spanning Tree Settings* fields:

- **Spanning Tree Status:** Enable or disable 802.1d spanning tree protocol to avoid network looping.
- **Bridge Hello Time**: The time between each bridge protocol data unit (BPDU). Default: 2 sec.
- **Bridge Max Age**: Maximum time a BPDU kept in bridge. Default: 20 sec.
- **Bridge Forward Delay**: The time to be spent in listen and learning state. Default: 4 sec.
- Priority: Priority number for root bridge selection. (MAC number is listed on **Status** > **Main** menu).

4 Click **Apply** to save the spanning tree settings or **Cancel** to discard the changes.

Enable Band Steering

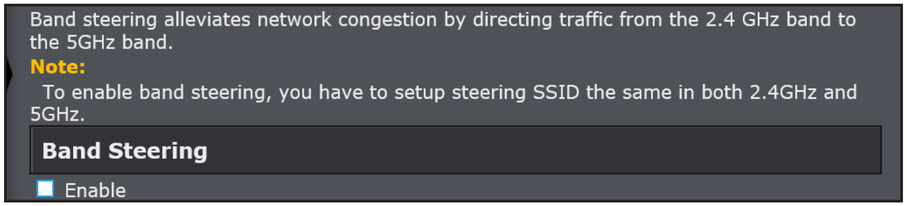
System > Band Steer

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.

To enable Band Steering, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *System > Band Steer*.



Band steering alleviates network congestion by directing traffic from the 2.4 GHz band to the 5GHz band.

Note:

To enable band steering, you have to setup steering SSID the same in both 2.4GHz and 5GHz.

Band Steering

□ Enable

3 Check **Enable** option to allow band steering.

4 Click **Save** to save the setting or **Cancel** to discard the changes.

IPv6 Settings

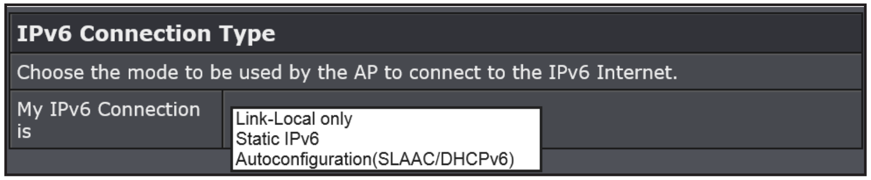
System > IPv6 Settings

Use this section if you are connecting this device to an IPv6 network and require this device to use IPv6 addressing. IPv6 is a updated IP addressing protocol which offers advanced capabilities and improvements over the more commonly used IP address standard (IPv4).

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *System > IPv6 Settings*.

3 Select the mode to be used by the access point to connect to an IPv6 network.



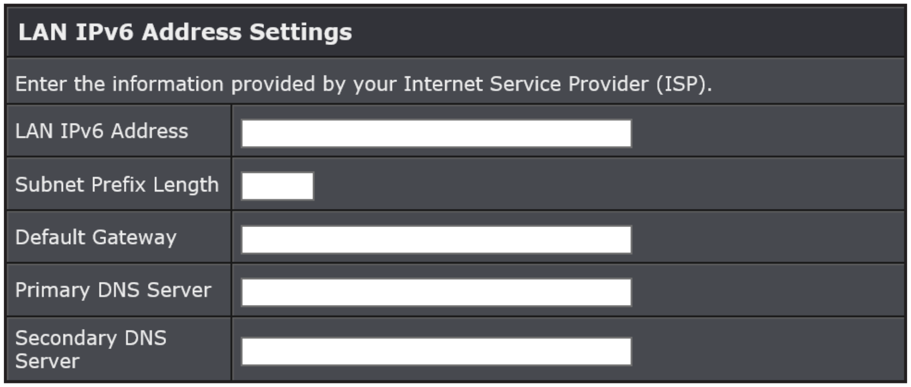
IPv6 Connection Type

Choose the mode to be used by the AP to connect to the IPv6 Internet.

My IPv6 Connection is: Link-Local only / Static IPv6 / Autoconfiguration(SLAAC/DHCPv6)

- **Link-Local Only**: The link-local address is used to communicate to neighboring IPv6 capable network devices that are connected to the same network segment. This is similar to the function automatic network IP addressing (APIPA) if a device cannot pull IPv4 address settings automatically from a network DHCP server.
- **Static IPv6**: Use this option to manually configure the IPv6 address settings of the device for connectivity to your IPv6 network.

  Configure the following settings:



LAN IPv6 Address Settings

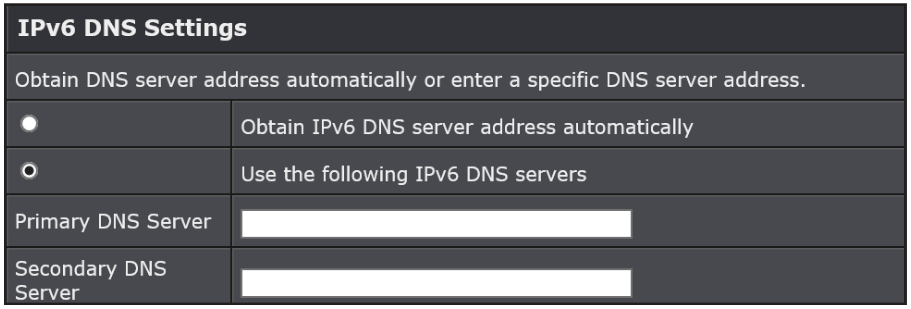
Enter the information provided by your Internet Service Provider (ISP).

LAN IPv6 Address	
Subnet Prefix Length	
Default Gateway	
Primary DNS Server	
Secondary DNS Server	

- ■ LAN IPv6 Address: Enter the static IPv6 address to assign to your device (i.e. 1234:5678:90ab:cdef::a or 1234:5678:90ab:cdef:0000:0000:0000:000a).
- ■ Subnet Prefix Length: Enter the IPv6 subnet prefix length(1-128, 64 is typically the standard prefix).
- ■ Default Gateway: Enter the IPv6 default gateway address (i.e. 1234:5678:90ab:cdef::1 or 1234:5678:90ab:cdef:0000:0000:0000:0001).
- ■ Primary DNS Server: Enter the primary IPv6 DNS server address (i.e. 1234:5678:90ab:cdef::1 or 1234:5678:90ab:cdef:0000:0000:0000:0001, 2001:4860:4860::8888 2001:4860:4860::8844).
- ■ Secondary DNS Server: Enter the secondary IPv6 DNS server address (i.e. 1234:5678:90ab:cdef::1 or 1234:5678:90ab:cdef:0000:0000:0000:0001, 2001:4860:4860::8888 2001:4860:4860::8844).

- **Autoconfiguration (SLAAC)/DHCPv6)**: Use this option to configure the device to obtain IPv6 address settings automatically from a DHCPv6 server on your network.

  Configure the following settings:



IPv6 DNS Settings

Obtain DNS server address automatically or enter a specific DNS server address.

○	Obtain IPv6 DNS server address automatically
●	Use the following IPv6 DNS servers
Primary DNS Server	
Secondary DNS Server	

- ■ Obtain IPv6 DNS server address automatically: Select this option to configure the device to obtain the IPv6 DNS server addresses automatically from the DHCPv6 server on your network.
- ■ Use the following IPv6 DNS Servers: Select this option to manually configure which IPv6 DNS server addresses the device will use.

4 Click **Apply** to save changes or **Cancel** to discard the changes.

Advanced System Configuration

This section will guide you through configuring several advanced settings.

Configure Wireless Network Settings

Basic Network Settings

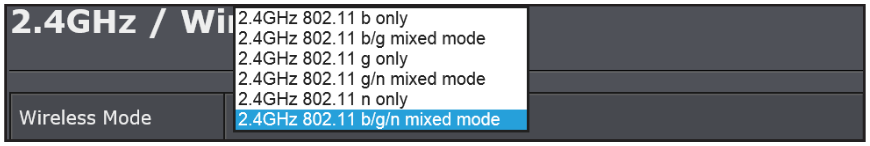
Wireless 2.4GHz > Wireless Network

General setups options for your 2.4GHz wireless connection. You can setup up to eight SSIDs for different groups of users.
To configure the basic network settings, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

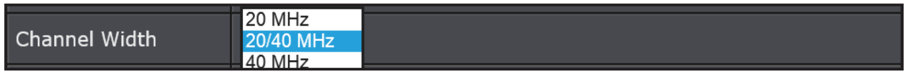
2 Click **Wireless 2.4GHz** > **Wireless Network**.

3 Select the network mode.


2.4GHz / Wi
Wireless Mode: 2.4GHz 802.11 b/g/n mixed mode
2.4GHz 802.11 b only
2.4GHz 802.11 b/g mixed mode
2.4GHz 802.11 g only
2.4GHz 802.11 g/n mixed mode
2.4GHz 802.11 n only
2.4GHz 802.11 b/g/n mixed mode

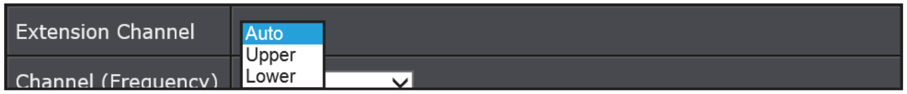
Note: Choose between N only, G only, B only, B/G mixed, G/N mixed, or B/G/N mixed mode. The rule of the thumb is to choose single mode if your devices all work in the same mode. Mixed mode increases compatibility, but sometimes lowers the data speed.

4 Select the channel width.


Channel Width: 20/40 MHz

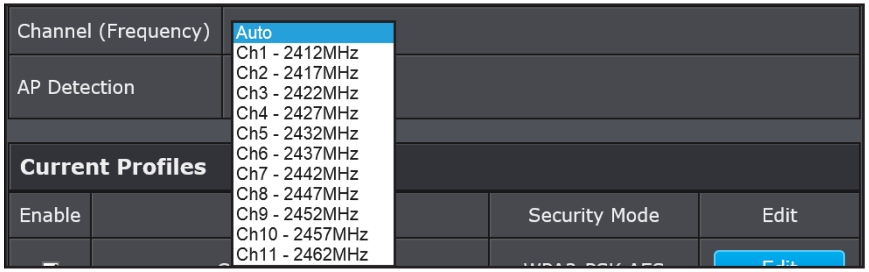
Note: The latest 802.11 protocol can combine channels for better wireless performance. You can choose fixed 20MHz or 40MHz, or automatically select 20MHz or 40MHz channels.

5 Select the extension channel.


Extension Channel: Auto
Channel (Frequency)

Note: 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.

6 Select the channel frequency.


Channel (Frequency): Auto
AP Detection
Current Profiles
Enable | Security Mode | Edit

Note: 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.)

7 Click **Apply** to save the changes or **Cancel** to discard the changes.

AP Detection

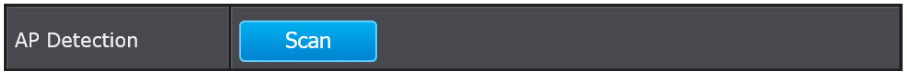
Wireless 2.4GHz > Wireless Network

Before you setup your TEW-821DAP wireless settings, you may want to know what signal are currently broadcasting.
To view the site survey and list the running access points around you, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

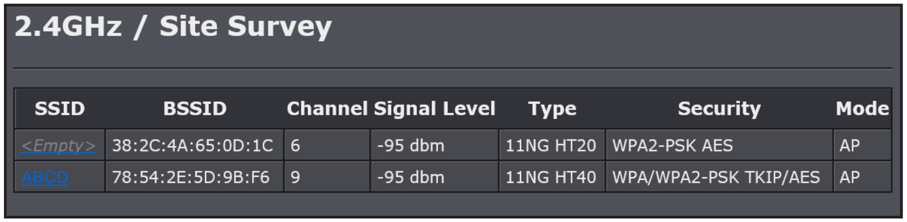
2 Click *Wireless 2.4GHz > Wireless Network.*

3 Click **Scan** next to the *AP Detection* field.



AP Detection	Scan

The site survey page opens.



2.4GHz / Site Survey

SSID	BSSID	Channel	Signal Level	Type	Security	Mode
<Empty>	38:2C:4A:65:0D:1C	6	-95 dbm	11NG HT20	WPA2-PSK AES	AP
ABCD	78:54:2E:5D:9B:F6	9	-95 dbm	11NG HT40	WPA/WPA2-PSK TKIP/AES	AP

In site survey you can see the following information:

- **SSID:** Service Set Identifier. This SSID is human readable and performs as ESSID to setup wireless groups.
- **BSSID**: Basic SSID. This is strictly unique SSID to identify a wireless access point, WAP. It is also the MAC address of the wireless interface.
- **Channel**: 2.4GHz 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.

4 Click **Refresh** to renew the information.

SSID Settings

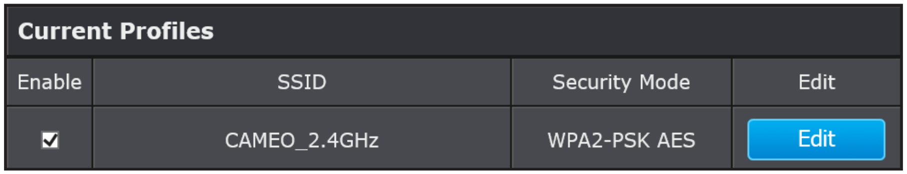
Wireless 2.4GHz > Wireless Network

To configure the SSID settings, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *Wireless 2.4GHz > Wireless Network*.

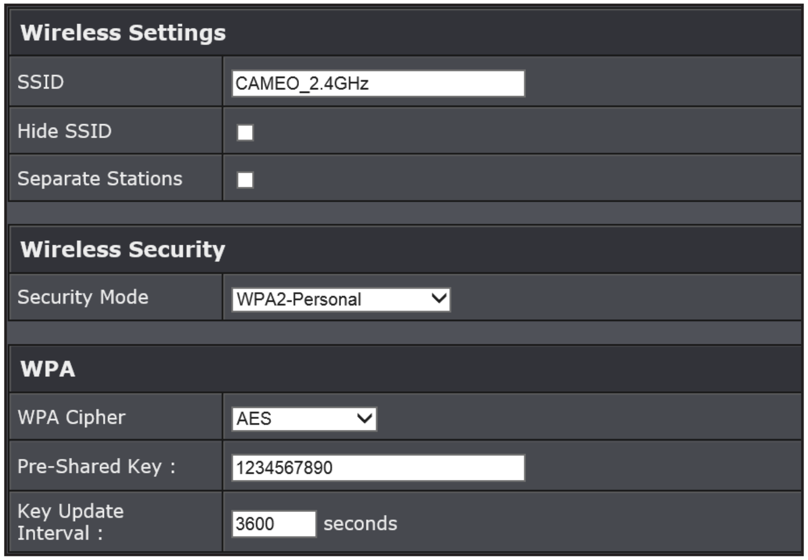
3 Select the profile from *Current Profile* section and click **Edit** next to the profile.



Current Profiles

Enable	SSID	Security Mode	Edit
☑	CAMEO_2.4GHz	WPA2-PSK AES	Edit

The SSID profile page opens.



Wireless Settings

SSID	CAMEO_2.4GHz
Hide SSID	□
Separate Stations	□

Wireless Security

Security Mode	WPA2-Personal

WPA

WPA Cipher	AES
Pre-Shared Key :	1234567890
Key Update Interval :	3600 seconds

4 Modify the following parameters:

- **SSID:** Select the human readable SSID to be easily identified. You can choose any combination with 1 to 32 letters .
- **Hide SSID**: Check this box to hide SSID broadcasting. Your wireless network name is broadcast to anyone within wireless signal range. When this is box is checked,

you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

- **Separate Stations:** 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.
- **Security Mode**: Please refer to

5 Click **Apply** to save the SSID information.

Configure MAC Filter Settings

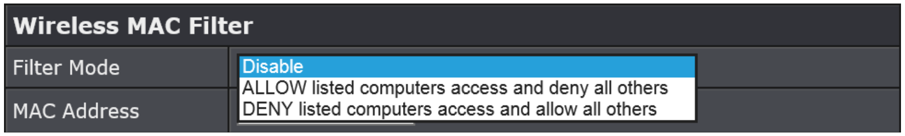
Wireless 2.4GHz > Wireless MAC Filter

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 (refer to "Log in to Management Page" on page 10).

2 Click **Wireless 2.4GHz** > **Wireless Network**.

3 On *Filter Mode below*, select one of the MAC filter function.



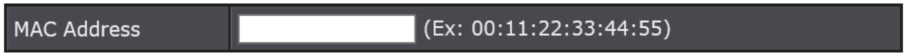
Wireless MAC Filter

Filter Mode	Disable ALLOW listed computers access and deny all others DENY listed computers access and allow all others
MAC Address	

- **Disable**: Select this option to disable the MAC address filter.
- **ALLOW listed computers access and deny all others**: Select this option to only allow computers/devices with MAC addresses listed to access the access point management page and the Internet. Deny all others.
- **DENY listed computers access and allow all others**: Select this option to only deny computers/devices with MAC addresses listed to access to the access point management page and the Internet. Allow all others.

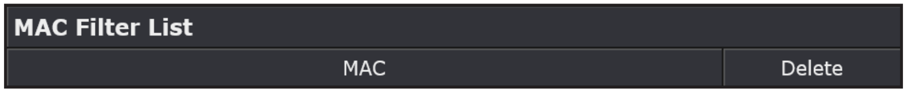
Note: MAC filter can be configured to allow access to the listed MAC address and deny all others unlisted or vice versa. The recommended function is to choose to only allow access to the MAC addresses listed and deny all others unlisted because it is easier to determine the MAC addresses of devices in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

4 Enter the MAC address you wish to allow or deny depending on the Filter Mode option. The MAC address needs to be filled in in the hexadecimal format. For example, 00:11:22:33:44:55.



MAC Address	(Ex: 00:11:22:33:44:55)

You can review the added MAC addresses in MAC Filter List table.



MAC Filter List

MAC	Delete

*Note: To remove the MAC address from the MAC Filter List, click **Delete** next to the chosen MAC address.*

5 Click **Apply** to save the changes or **Cancel** to discard the settings.

Configure Wireless Advanced Settings

Wireless 2.4GHz > Wireless Advanced Settings

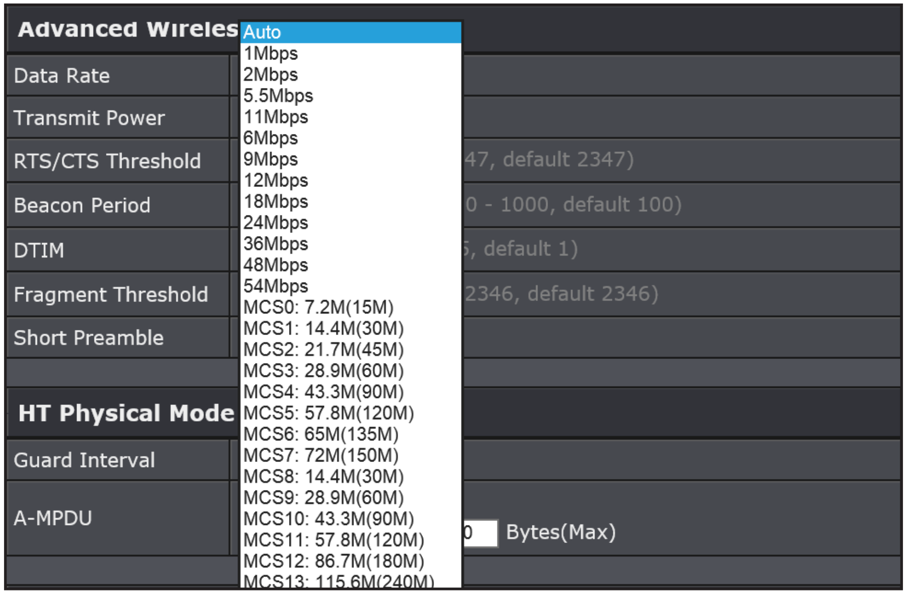
Fine tune your wireless settings on this page.

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

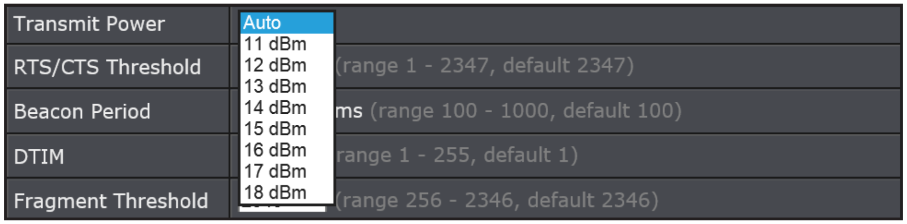
2 Click *Wireless 2.4GHz > Wireless Advanced Settings*.

3 In *Advanced Wireless* section, modify any of the following parameters:

- **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.

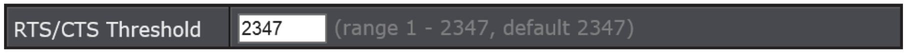


- **Transmit Power**: Wireless signal transmission power. Setting transmission power to an appropriate value can make your multiple AP deployment easier. The default value is 18 dBm. Valid settings are between 11 and 18 (both FCC and CE).



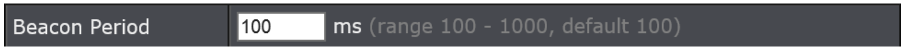
Transmit Power	Auto 11 dBm 12 dBm 13 dBm 14 dBm 15 dBm 16 dBm 17 dBm 18 dBm
RTS/CTS Threshold	(range 1 - 2347, default 2347)
Beacon Period	ms (range 100 - 1000, default 100)
DTIM	range 1 - 255, default 1)
Fragment Threshold	(range 256 - 2346, default 2346)

- **RTC/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.



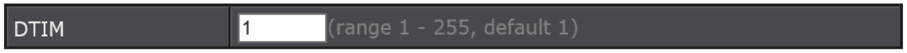
RTS/CTS Threshold	2347 (range 1 - 2347, default 2347)

- **Beacon Period**: Beacons are packets sent by the access point to synchronize wireless devices. Specify a Beacon Period value between 100 and 1000. The default value is set to 100 milliseconds.



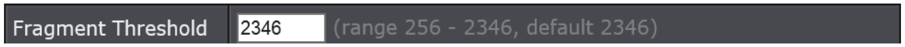
Beacon Period	100 ms (range 100 - 1000, default 100)

- **DTIM:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the access point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.



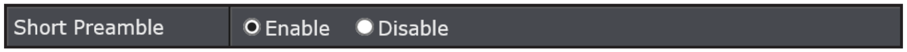
DTIM	1 (range 1 - 255, default 1)

- **Fragment Threshold**: This setting should remain at its default value of 2346. Setting the Fragmentation value too low may result in poor performance.



Fragment Threshold	2346 (range 256 - 2346, default 2346)

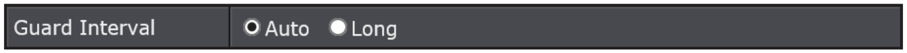
- **Short Preamble**: Disable this feature if you do not want the access point to use it at data transfer.



Short Preamble	○ Enable ○ Disable

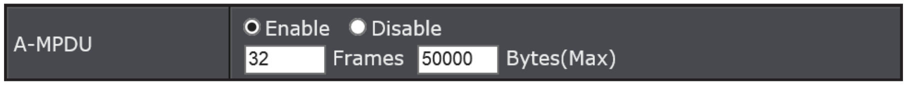
4 In *HD Physical Mode* section*,* modify any of the following parameters:

- **Guard Interval**: Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option between **Auto** and **Long** that works best for your installation.



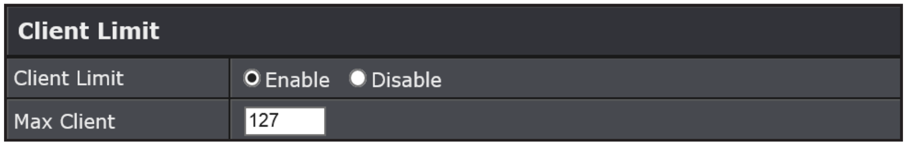
Guard Interval	○ Auto ○ Long

- **A-MPDU**: MPDU aggregation also collects Ethernet frames to be transmitted to a single destination, but it wraps each frame in an 802.11n MAC header. Normally this is less efficient than MSDU aggregation, but it may be more efficient in environments with high error rates, because of a mechanism called block acknowledgement. This mechanism allows each of the aggregated data frames to be individually acknowledged or retransmitted if affected by an error



A-MPDU	○ Enable ○ Disable 32 Frames 50000 Bytes(Max)

5 In *Client Limit* section*,* check **Enable** if you want to limit the number of clients and set the maximum number of clients that can connect to TEW-821DAP. If you do not want to use this feature, check **Disable**.



Client Limit

Client Limit	○ Enable ○ Disable
Max Client	127

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.

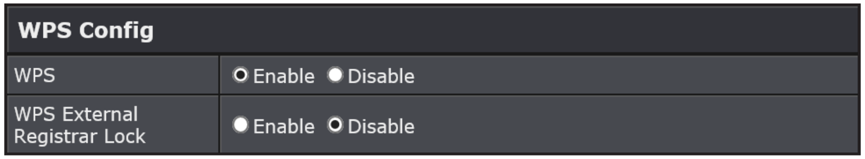
- Push Button Configuration (PBC) method
- PIN (Personal Identification Number) method

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

PBC (Software/Virtual Push Button)

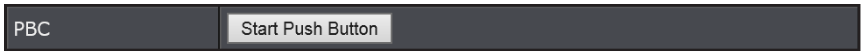
Wireless 2.4GHz > WPS

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).
2 Click *Wireless 2.4GHz > WPS*.
3 In *WPS Config* section enable the WPS feature.
4 Enable or disable the WPS External Registrar Lock.



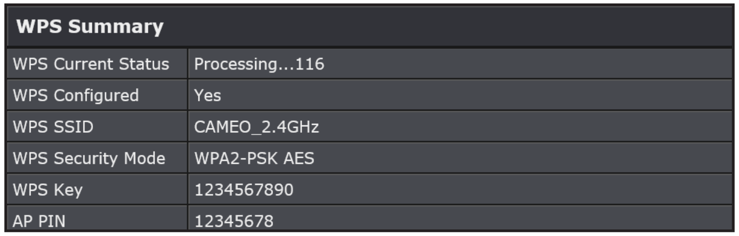
WPS Config	
WPS	◉ Enable ○ Disable
WPS External Registrar Lock	○ Enable ◉ Disable

5 In the *WPS Action* section, click **Start Push Button** to add a wireless device to your network.



PBC	Start Push Button

6 Wait for your access point to finish the WPS process.



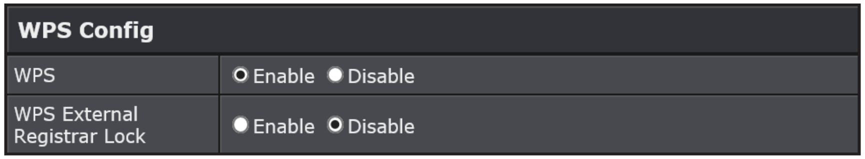
WPS Summary	
WPS Current Status	Processing...116
WPS Configured	Yes
WPS SSID	CAMEO_2.4GHz
WPS Security Mode	WPA2-PSK AES
WPS Key	1234567890
AP PIN	12345678

The procedure is complete when the *WPS Current Status in WPS Summary* section becomes "Idle".

PIN (Personal Identification Number)

Wireless 2.4GHz > WPS

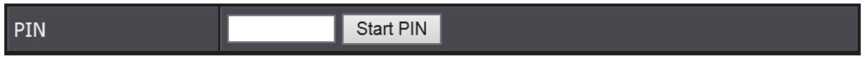
1 Log into your access point management page (refer to "Log in to Management Page" on page 10).
2 Click *Wireless 2.4GHz > WPS*.
3 In *WPS Config* section enable the WPS feature.
4 Enable or disable the WPS External Registrar Lock.



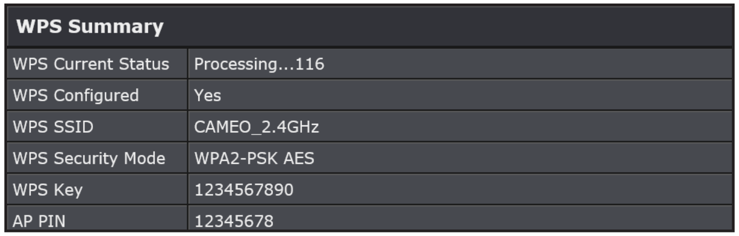
WPS Config	
WPS	● Enable ○ Disable
WPS External Registrar Lock	○ Enable ● Disable

5 In the *WPS Action* section, enter the 8-digit pin number and click **Start Push Button** to add a wireless device to your network.

Note: The PIN number is listed in WPS Summary > AP PIN.



6 Wait for your access point to finish the WPS process.



WPS Summary	
WPS Current Status	Processing...116
WPS Configured	Yes
WPS SSID	CAMEO_2.4GHz
WPS Security Mode	WPA2-PSK AES
WPS Key	1234567890
AP PIN	12345678

The procedure is complete when the WPS Current Status in *WPS Summary* section becomes back "Idle".

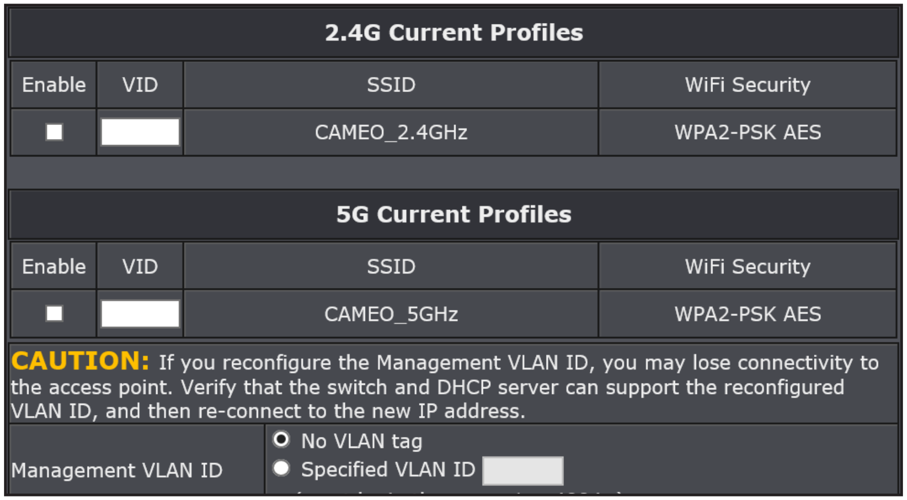
Configure Management VLAN Settings

Management > Management VLAN

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.

To configure the management VLAN settings, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).
2 Click *Management > Management VLAN*.



2.4G Current Profiles

Enable	VID	SSID	WiFi Security
□		CAMEO_2.4GHz	WPA2-PSK AES

5G Current Profiles

Enable	VID	SSID	WiFi Security
□		CAMEO_5GHz	WPA2-PSK AES

CAUTION: If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

Management VLAN ID: ● No VLAN tag ○ Specified VLAN ID

3 Configure or view any of the following parameters:

- **Enable:** Redundant control to enable or disable the particular SSID.
- **VID**: Virtual LAN 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).
- **SSID**: Showing the human readable SSID.
- **Wifi Security**: Wireless security set to the SSID.

4 Click **Apply** to save the management VLAN settings or **Cancel** to discard the changes.

Configure Traffic Shaping Settings

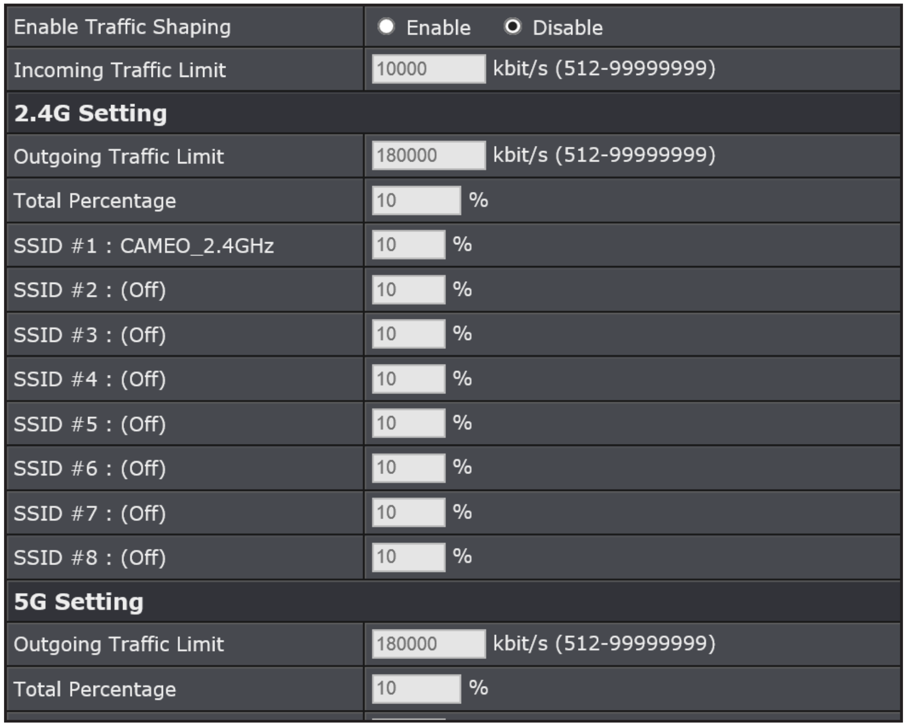
Management > Wireless Traffic Shaping

Traffic shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.

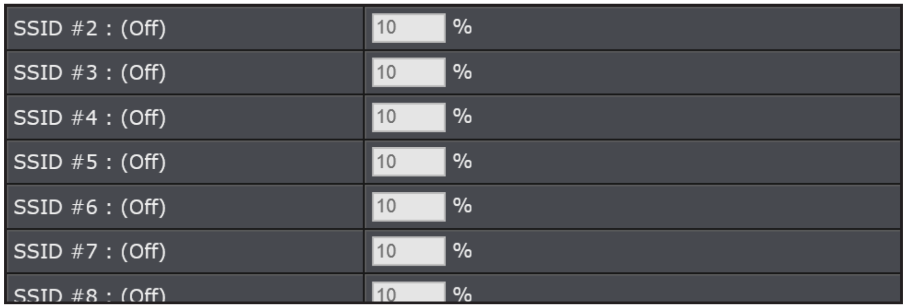
To configure the traffic shaping settings, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *Management > Wireless Traffic Shaping*.



Enable Traffic Shaping	○ Enable ● Disable
Incoming Traffic Limit	10000 kbit/s (512-99999999)
2.4G Setting	
Outgoing Traffic Limit	180000 kbit/s (512-99999999)
Total Percentage	10 %
SSID #1 : CAMEO_2.4GHz	10 %
SSID #2 : (Off)	10 %
SSID #3 : (Off)	10 %
SSID #4 : (Off)	10 %
SSID #5 : (Off)	10 %
SSID #6 : (Off)	10 %
SSID #7 : (Off)	10 %
SSID #8 : (Off)	10 %
5G Setting	
Outgoing Traffic Limit	180000 kbit/s (512-99999999)
Total Percentage	10 %



SSID #2 : (Off)	10 %
SSID #3 : (Off)	10 %
SSID #4 : (Off)	10 %
SSID #5 : (Off)	10 %
SSID #6 : (Off)	10 %
SSID #7 : (Off)	10 %
SSID #8 : (Off)	10 %

3 Configure any of the following parameters for 2.4G or 5G profile:

- **Outgoing Traffic Limit:** 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-821DAP wireless interfaces are capable of 300 Mbps, 300,000 kbps for 2.4GHz and 5GHz respectively.)
- **Incoming Traffic Limit**: 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-821DAP Ethernet port is capable of 1Gbps, 1,000,000 kbps.)
- **Total Percentage**: 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.
- **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.

4 Click **Apply** to save the changes or **Cancel** to discard the changes.

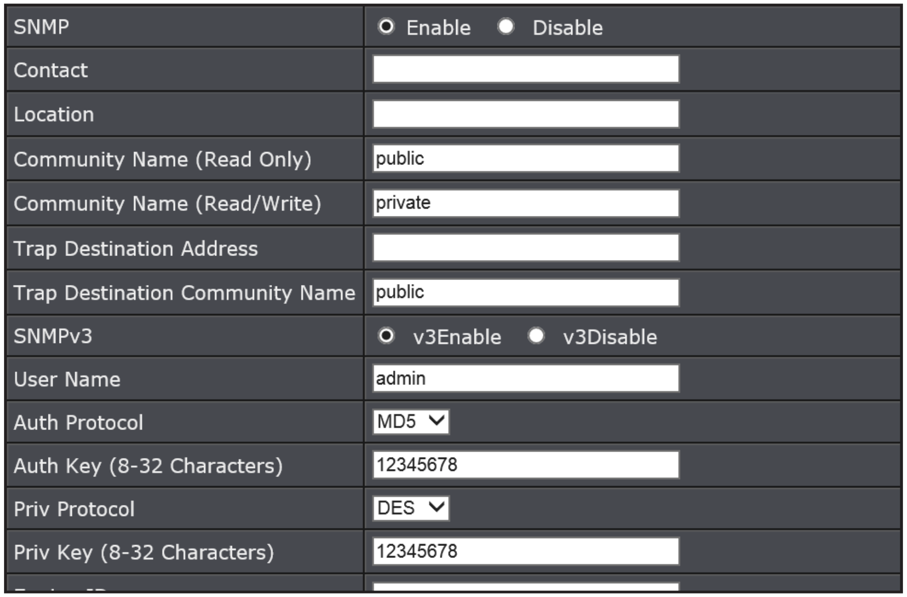
Configure SNMP Settings

Management > **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.

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

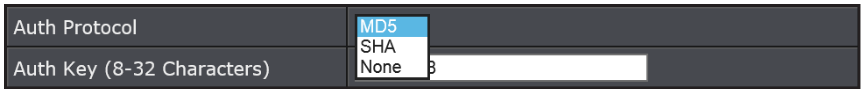
2 Click *Management > SNMP Settings*.



SNMP	○ Enable ● Disable
Contact	
Location	
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination Address	
Trap Destination Community Name	public
SNMPv3	○ v3Enable ● v3Disable
User Name	admin
Auth Protocol	MD5
Auth Key (8-32 Characters)	12345678
Priv Protocol	DES
Priv Key (8-32 Characters)	12345678

3 Configure or view any of the following parameters:

- **SNMP:** Choose to enable or disable the SNMP feature.
- **Contact**: Specify the contact details of the TEW-821DAP.
- **Location**: Specify the location of the TEW-821DAP.
- **Community Name (Read Only)**: Specify the password for access the SNMP community for read only access.
- **Community Name (Read/Write)**: Specify the password for access to the SNMP community with read/write access.
- **Trap Destination Address**: Specify the IP address for the SNMP trap community.
- **Trap Destination Community Name:** Specify the name of SNMP trap community.
- **SNMP v3:** Select enable or disable SNMP v3 protocol.
- **User Name**: SNMP v3 manager user name.
- **Auth Protocol:** Choose the authentication method to verify the source of information: MD5, SHA, or None.



Auth Protocol	MD5 SHA None
Auth Key (8-32 Characters)	

- **Auth Key (8-32 Characters):** Specify the authentication key between 8 to 32 letters.
- **Priv Protocol**: Choose the privacy key to encrypt SNMP messages: DES or None.
- **Priv Key (8-32 Characters)**: Specify the privacy key between 8 to 32 letters.
- **Engine ID**: SNMPv3 engine ID.

4 Click **Apply** to save the changes or **Cancel** to discard the changes.

Configure Schedule Settings

Management > Schedule

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

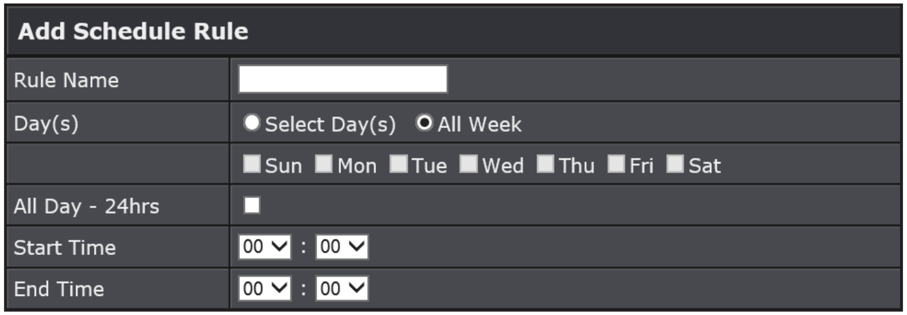
Note: You can apply a predefined schedule to the following features:

✓ *Wireless (2.4GHz and 5GHz)*
✓ *Wireless Multiple SSID (2.4GHz and 5GHz)*
✓ *MAC Filters*

Create a Schedule

To create a schedule, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).
2 Click *Management > Schedule*.
3 Configure the following settings:



Add Schedule Rule	
Rule Name	
Day(s)	○ Select Day(s) ● All Week
	□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
All Day - 24hrs	□
Start Time	00 : 00
End Time	00 : 00

- **Rule Name**: Enter a name for the schedule you would like to apply.
- **Day(s)**: Check **Select Day(s)** to select the days in the *Select Day(s)* section or select **All Week** to set the schedule for all days.
- **All Day – 24 hrs**: Check this box to have the schedule active the entire 24 hours on the days specified.
- **Start Time**: Select the activation time of the schedule.

- **End Time**: Select the deactivation time of the schedule.

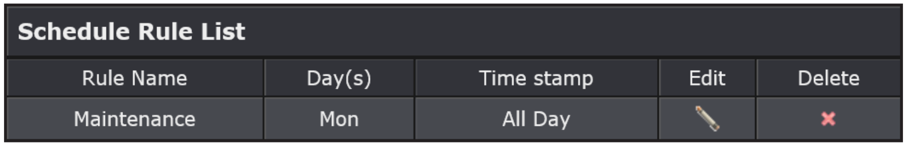
4 Click **Add** to create a schedule or **Clear** to discard the changes.

Edit a Schedule

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *Management > Schedule*.

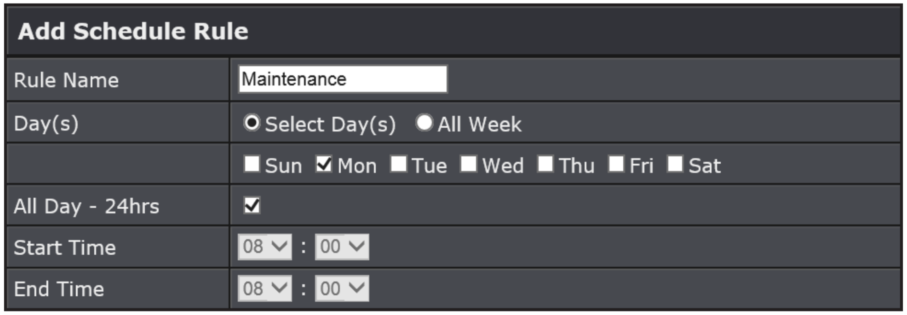
3 On the *Schedule Rules List* section, click the ✎ icon next to the schedule that you want to edit.



Schedule Rule List

Rule Name	Day(s)	Time stamp	Edit	Delete
Maintenance	Mon	All Day	✎	✖

4 Adjust the necessary settings.



Add Schedule Rule

Rule Name	Maintenance
Day(s)	● Select Day(s) ○ All Week
	□ Sun ☑ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
All Day - 24hrs	☑
Start Time	08 : 00
End Time	08 : 00

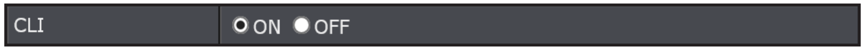
5 Click **Save** to save the settings.

Note: To delete a schedule, click the ✖ icon next to the schedule that you want to delete. A confirmation message appears on the screen. Click **Yes** *to confirm.*

Enable CLI

Management > CLI Settings

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



CLI	● ON ○ OFF

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

```
$ ssh admin@192.168.10.100
The authenticity of host '192.168.10.100
(192.168.10.100)' can't be established.
RSA key fingerprint is b2:41:6e:0f:4b:2a:f3:03:18:60:
0b:c4:eb:74:9d:9c.
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>
```

Management

This section will guide you how to change login password, update the firmware, export/import the system settings, restore the default settings, and other maintenance operations.

Change Login Password

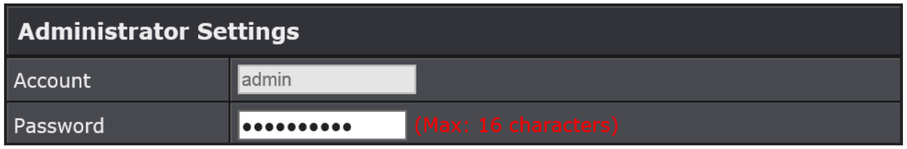
Management > Administration

For security purposes, it is recommended to change the login password periodically. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.
You can change the password in Management > Administration section or through the System > Wizard. The following instructions includes both options.

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

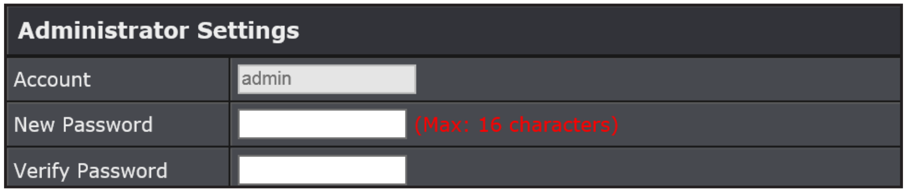
2 Click one of the following:

- *Management > Administration*



Administrator Settings	
Account	admin
Password	•••••••••• (Max: 16 characters)

- *System > Wizard*.



Administrator Settings	
Account	admin
New Password	(Max: 16 characters)
Verify Password	

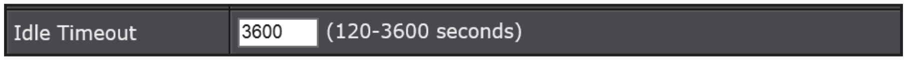
3 Do one of the following:
Management > Administration
a) Enter the new password in *Password* field.
b) Click **Apply** to save the modification.
System > Wizard
a) Enter the new password in New Password field.
b) To verify, enter the new password in *Verify Password* field.
c) Click **Next** to save the changes.

Modify Menu Timeout

Management > Administration

The menu idle timeout setting controls how long the connection can remain idle before the system forces the remote user to log in again.

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).
2 Click *Management > Administration*.
3 In *Administrator Setting* section modify the idle timeout in seconds.



Idle Timeout	3600 (120-3600 seconds)

4 Click **Apply** to save the idle timeout settings or **Cancel** to discard the modifications.

Change Device Name

Management > Administration

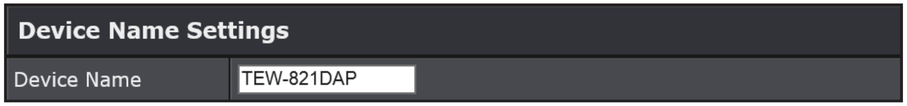
For easy access, you can also enter the Management page using the domain name (http://device name) based on the device name that you have configured in this section.

Note: By default, the domain name is the same as your access point model name (http://tew-821dap).

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *Management > Administration*.

3 On the *Device Name Settings* section, enter the new device name to display on your network to identify the access point in the *Device Name* field.



Device Name Settings

Device Name	TEW-821DAP

4 Click **Apply** to save the changes or **Cancel** to discard the changes.

Set Date and Time

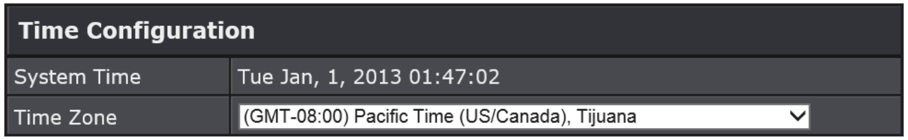
Management > Time and Date Settings

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).

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *Management* **>** *Time and Date Settings.*

3 View or modify the following settings in *Time Configuration* section:

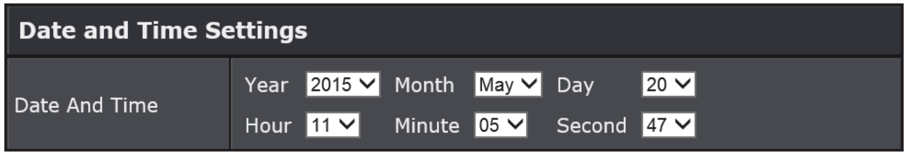


Time Configuration

System Time	Tue Jan, 1, 2013 01:47:02
Time Zone	(GMT-08:00) Pacific Time (US/Canada), Tijuana

- **System Time**: Current date and time.

Note: If you do not want to use the automatic time configuration (enable NTP server) then modify time manually in Date and Time Settings section.

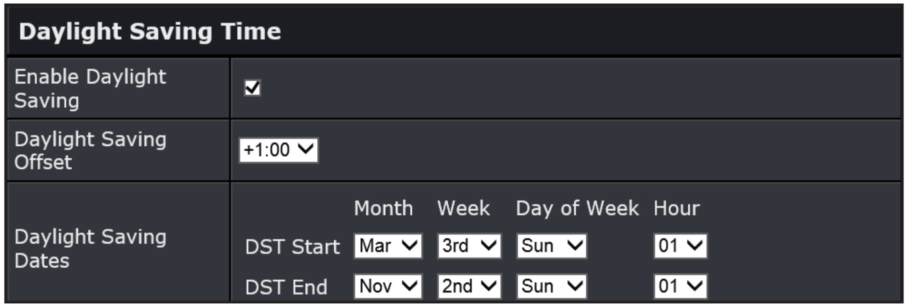


Date and Time Settings

Date And Time	Year	2015	Month	May	Day	20
	Hour	11	Minute	05	Second	47

- **Time Zone:** Select the time zone of the country or region you are currently in. The TEW-821DAP will set its time based on your selection.

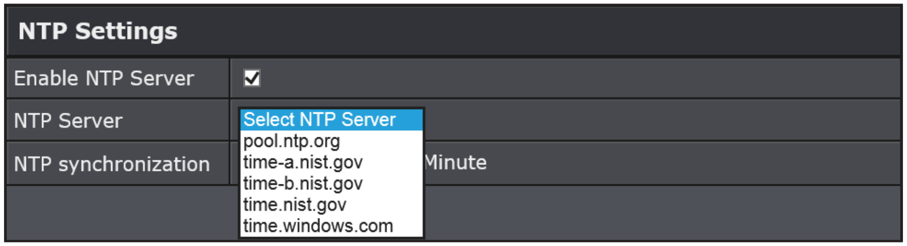
4 Check Enable Daylight Saving if your time zone has daylight savings. Enter the start time and end time of daylight savings.



Daylight Saving Time

Enable Daylight Saving	☑				
Daylight Saving Offset	+1:00				
Daylight Saving Dates		Month	Week	Day of Week	Hour
	DST Start	Mar	3rd	Sun	01
	DST End	Nov	2nd	Sun	01

5 If you have a preferred NTP server, check the Enable NTP Server and enter the NTP server IP address. Otherwise, leave it unchecked to use the TEW-821DAP's default NTP server.



NTP Settings

Enable NTP Server	☑
NTP Server	Select NTP Server pool.ntp.org time-a.nist.gov time-b.nist.gov time.nist.gov time.windows.com
NTP synchronization	Minute

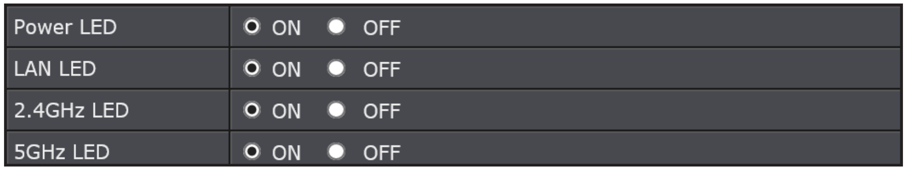
6 Click **Apply** to save the changes or **Cancel** to discard the changes.

Configure LED Indicators

Management > LED Control

All LED indicators are turned on by default. You can turn any one of them or all of them on or off.

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).
2 Click *Management > LED Control*.
3 Click the following LED to turn it on or off:



Power LED	○ ON ● OFF
LAN LED	○ ON ● OFF
2.4GHz LED	○ ON ● OFF
5GHz LED	○ ON ● OFF

- **Power LED:**
  - OFF: Powered off.
  - Solid Orange: System is under Power-ON booting process.
  - Solid Green: System is ON. (Booting process is done.)
- **Network LED (Orange: 10/100; Green: Giga bit):**
  - OFF: No link.
  - Solid green: The device's Ethernet port is connected to an active router or switch.
  - Blinking green: Data transmission.
- **Wireless LED (Orange: 2.4GHz; Green: 5GHz):**
  - OFF: No link.
  - Blinking green: Data transmission.

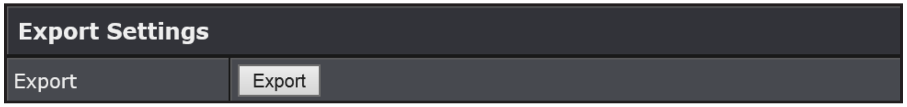
Backup / Restore System Settings

Management > Backup/Restore Settings

This page allows you to save the current configurations, load previously saved configurations, and reset TEW-821DAP's configurations back to factory defaults.

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).
2 Click *Management > Backup/Restore Settings.*
3 Do any of the following:

- Click **Export** to save the current configuration of the AP.

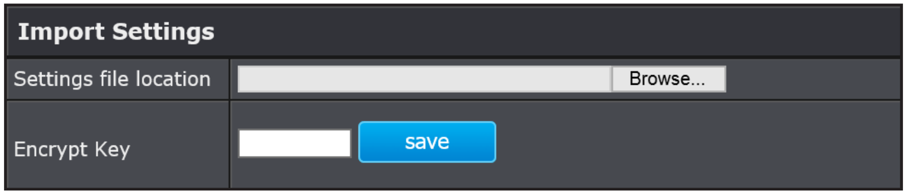


Export Settings

Export	Export

- To load a configuration file, do the following:

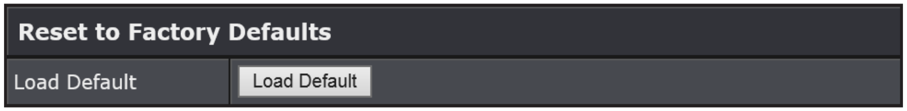
  a) Click **Browse** to load the configuration file.
  b) Enter the encryption key.
  c) Click Import.
  The new configuration file will be saved and encrypted with this new key.



Import Settings

Settings file location	Browse...
Encrypt Key	save

- Click **Load Default** if you want to reset TEW-821DAP's configurations back to factory defaults.



Reset to Factory Defaults

Load Default	Load Default

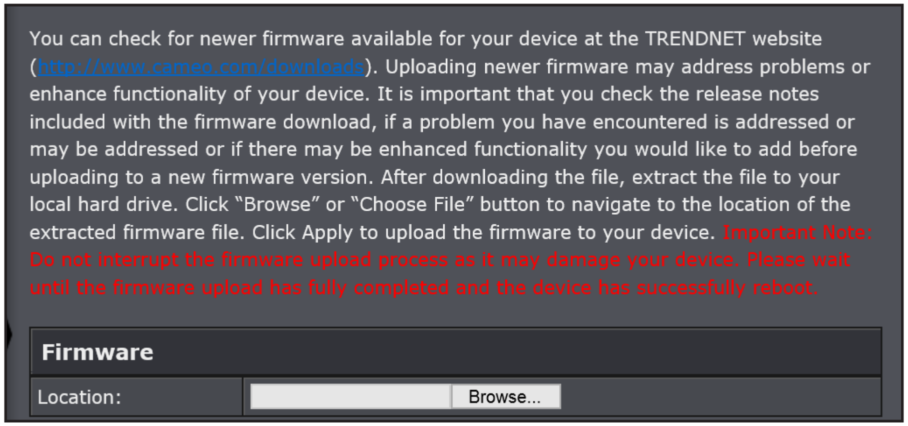
Update System Firmware

Management > **Upload Firmware**

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/

To update system firmware, do the following:

1 If a firmware upgrade is available, download the firmware to your computer.
2 Unzip the file to a folder on your computer.
3 Save the upgrade file on a flash disk.
4 Insert the flash disk into the AP.
5 Log into your access point management page (refer to "Log in to Management Page" on page 10).
6 Click *Management > Upload Firmware*.
7 Click **Browse** to load the upgrade file from your computer.
8 Click **Apply**.



You can check for newer firmware available for your device at the TRENDNET website (http://www.cameo.com/downloads). Uploading newer firmware may address problems or enhance functionality of your device. It is important that you check the release notes included with the firmware download, if a problem you have encountered is addressed or may be addressed or if there may be enhanced functionality you would like to add before uploading to a new firmware version. After downloading the file, extract the file to your local hard drive. Click "Browse" or "Choose File" button to navigate to the location of the extracted firmware file. Click Apply to upload the firmware to your device. Important Note: Do not interrupt the firmware upload process as it may damage your device. Please wait until the firmware upload has fully completed and the device has successfully reboot.

Firmware

Location:	

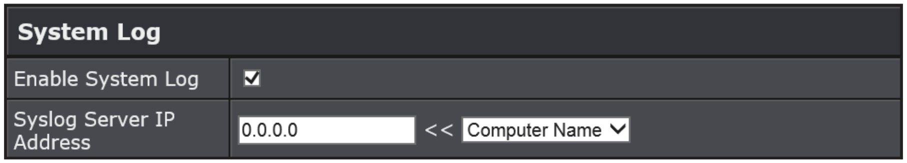
Configure System Log Server

Management > **Log**

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

To set up the remote loggings, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).
2 Click *Management > Log*.



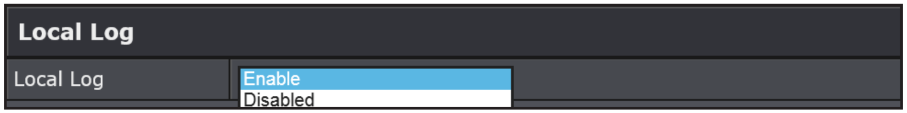
System Log

Enable System Log	☑
Syslog Server IP Address	0.0.0.0 << Computer Name

3 Check the Enable System Log checkbox.
4 Enter the log server IP address or URL.
5 Click **Apply** to save the settings.

To set up the local loggins, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).
2 Click *Management > Log*.



Local Log

Local Log	Enable Disabled

3 Select **Enable** to allow local logging.
You can view the log in *Status > System Log*.
4 Click **Apply** to save the settings.

Execute Diagnostics Test

Management > **Diagnostics**

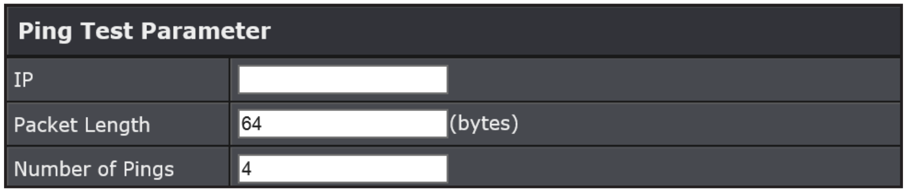
There are 2 network tools you can use on the TEW-821DAP: ping and traceroute.

To use ping test, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *Management > Diagnostics*.

3 Enter the following information:

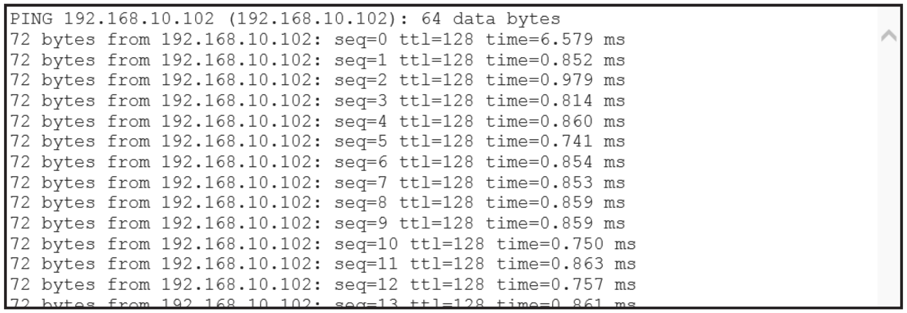


Ping Test Parameter	
IP	
Packet Length	64 (bytes)
Number of Pings	4

- Target IP address to the *IP* field.
- Ping packet size to the *Packet Length* field.
- Number of pings to the *Number of Pings* field.

4 Click **Ping** to start the test.

The result is displayed as shown on the following image:



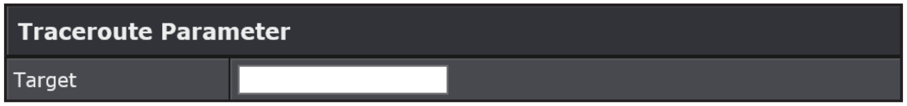
```
PING 192.168.10.102 (192.168.10.102): 64 data bytes
72 bytes from 192.168.10.102: seq=0 ttl=128 time=6.579 ms
72 bytes from 192.168.10.102: seq=1 ttl=128 time=0.852 ms
72 bytes from 192.168.10.102: seq=2 ttl=128 time=0.979 ms
72 bytes from 192.168.10.102: seq=3 ttl=128 time=0.814 ms
72 bytes from 192.168.10.102: seq=4 ttl=128 time=0.860 ms
72 bytes from 192.168.10.102: seq=5 ttl=128 time=0.741 ms
72 bytes from 192.168.10.102: seq=6 ttl=128 time=0.854 ms
72 bytes from 192.168.10.102: seq=7 ttl=128 time=0.853 ms
72 bytes from 192.168.10.102: seq=8 ttl=128 time=0.859 ms
72 bytes from 192.168.10.102: seq=9 ttl=128 time=0.859 ms
72 bytes from 192.168.10.102: seq=10 ttl=128 time=0.750 ms
72 bytes from 192.168.10.102: seq=11 ttl=128 time=0.863 ms
72 bytes from 192.168.10.102: seq=12 ttl=128 time=0.757 ms
72 bytes from 192.168.10.102: seq=13 ttl=128 time=0.861 ms
```

To use the traceroute test, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *Management > Diagnostics*.

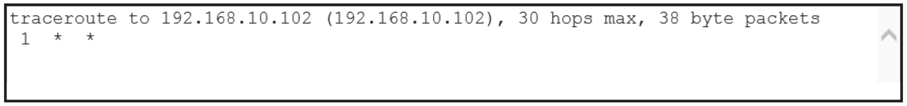
3 Enter the target machine IP address or domain name to the *Target* field.



Traceroute Parameter	
Target	

4 Click **Traceroute** to start the test.

The result is displayed as shown on the following image:



```
traceroute to 192.168.10.102 (192.168.10.102), 30 hops max, 38 byte packets
 1  *  *
```

System Reboot

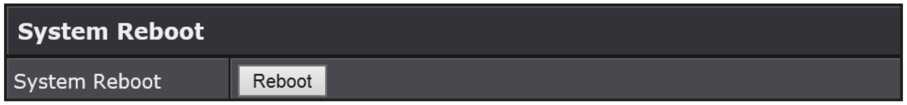
Management > Backup/Restore Settings

To reboot the AP, do the following:

1 Log into your access point management page (refer to "Log in to Management Page" on page 10).

2 Click *Management > Backup/Restore Settings.*

3 Click **Reboot**.



System Reboot

System Reboot

SmartConsole

Use SmartConsole to view and edit the main parameters of the devices, such as product name, IP address, MAC address, firmware version, etc.

Install the SmartConsole

To install the SmartConsole in your computer, do the following:

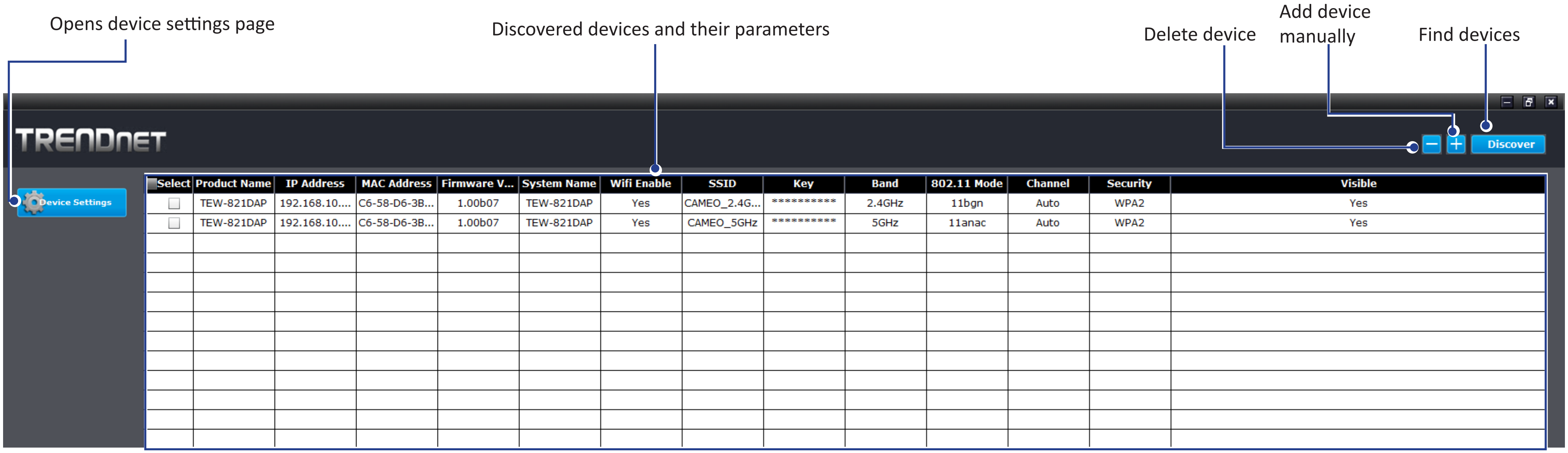
1 Download and install Adobe AIR software to your computer.

2 From the supplied CD, copy the SmartConsole program to the local disk of your computer.

3 Run "**AP Utility.exe**" in SmartConsole folder.
The program main screen opens. Please refer to the next section.

SmartConsole Overview

The following image displays the main page of the SmartConsole:



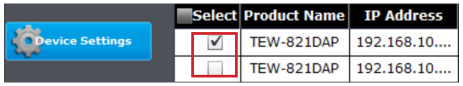
Select	Product Name	IP Address	MAC Address	Firmware V...	System Name	Wifi Enable	SSID	Key	Band	802.11 Mode	Channel	Security	Visible
□	TEW-821DAP	192.168.10....	C6-58-D6-3B...	1.00b07	TEW-821DAP	Yes	CAMEO_2.4G...	**********	2.4GHz	11bgn	Auto	WPA2	Yes
□	TEW-821DAP	192.168.10....	C6-58-D6-3B...	1.00b07	TEW-821DAP	Yes	CAMEO_5GHz	**********	5GHz	11anac	Auto	WPA2	Yes

Using the SmartConsole

To start using the SmartConsole, do the following:

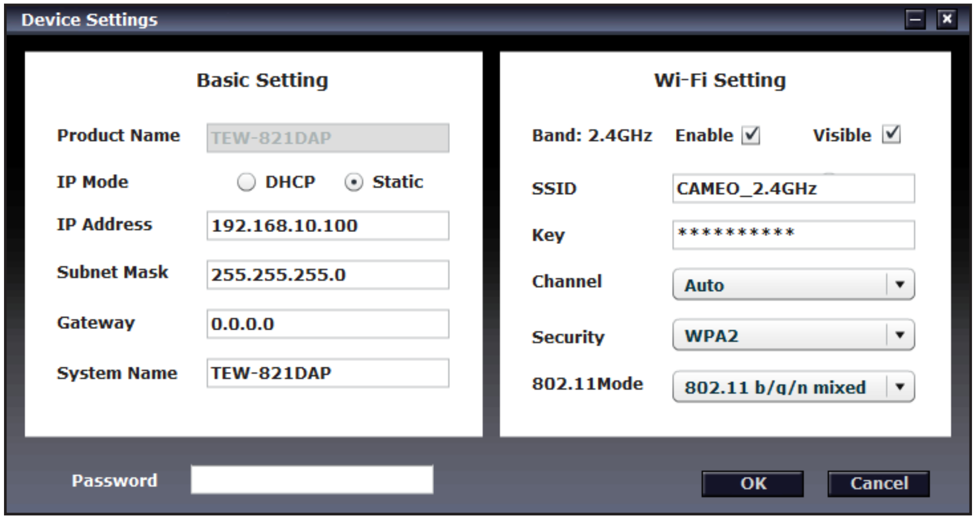
1 Click **Discover** (Discover) to let the system automatically discover all available devices in the network.

2 Click on the Select checkbox next to the device you wish to configure.



Select	Product Name	IP Address
☑	TEW-821DAP	192.168.10....
□	TEW-821DAP	192.168.10....

3 Click **Device Settings** (Device Settings) to open the selected device's settings page. The Device Settings page opens:



Device Settings

Basic Setting

Product Name: TEW-821DAP

IP Mode: ○ DHCP ● Static

IP Address: 192.168.10.100

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

System Name: TEW-821DAP

Wi-Fi Setting

Band: 2.4GHz Enable ☑ Visible ☑

SSID: CAMEO_2.4GHz

Key: **********

Channel: Auto

Security: WPA2

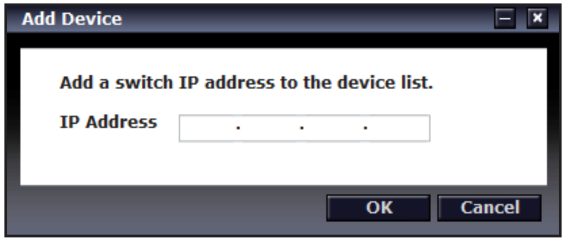
802.11Mode: 802.11 b/g/n mixed

Password:

4 Modify the basic / wi-fi settings and after finished, click **OK** to save the changes or **Cancel** to discard the changes.

5 Do any of the following:

- Repeat steps 1 to 4 to modify the settings of another device.
- Click + to insert the device connection parameters manually. Then click **OK** and repeat steps 2 to 4.

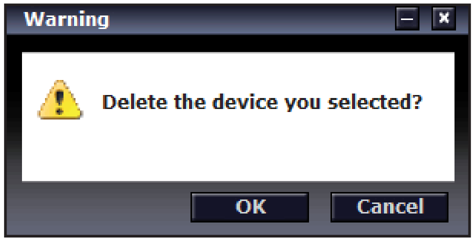


Add Device

Add a switch IP address to the device list.

IP Address: . . .

- Repeat step 2 and click — to delete the device from the list. Click OK to the confirmation message.



Warning

Delete the device you selected?

- Use — ❐ × to minimize, restore, or close the main page respectively.

Appendix

Specifications

Item	Specifications
Chipset	Qualcomm QCA9563+QCA9882
Standards	• EEE 802.11b/g/n Wireless LAN 2.4GHz • IEEE 802.11a/n/ac Wireless LAN 5GHz • IEEE 802.3/IEEE 802.3z Gigabit Ethernet • IEEE 802.3at PoE • ANSI/IEEE 802.3 Auto negotiation
Radio Technology	• IEEE 802.11g / IEEE 802.11n / IEEE 802.11a/n/ac Orthogonal Frequency Division Multiplexing (OFDM) • IEEE 802.11b: Direct Sequence Spread Spectrum (DSSS)
Transmission Rate	• 802.11ac: up to 867Mbps • 802.11an: up to 300Mbps • 802.11a: up to 54Mbps • 802.11n: up to 300Mbps • 802.11g: up to 54Mbps • 802.11b: up to 11Mbps
Receiver Sensitivity	• 11ac VHT80 MCS9: Typical - 51dBm @ 10% PER • 11ac VHT40 MCS9: Typical - 54dBm @ 10% PER • 11ac VHT20 MCS9: Typical - 57dBm @ 10% PER • 11a/n HT40 MCS7/15/23: Typical - 61dBm @ 10% PER • 11a/n HT20 MCS7/15/23: Typical - 64dBm @ 10% PER • 11a/g 54Mbps: Typical - 65dBm @ 10% PER • 11b 11Mbps: Typical - 83dBm @ 8% PER
Frequency	• 2.4GHz: 2412 ~ 2472 MHz ISM band (channels 1 ~ 13) • 5GHz: 5180 ~ 5825 MHz ISM band (channels 36 ~ 165)
Wireless Channel	• 2.4GHz: Channel 1 ~ 11(FCC), Channel 1 ~ 13(ETSI) • 5 GHz: 36, 40, 44, 48, 149, 153, 157, 161 and 165 (FCC), 36, 40, 44, 48(ETSI)
Modulation	• DBPSK/DQPSK/CCK for DSSS technique • BPSK/QPSK/16-QAM/64-QAM/256-QAM for OFDM technique
Media Access Protocol	CSMA/CA with ACK
Wireless Output Power/ Receiving Sensitivity (per chain)	**2.4G Mode** • FCC:23dBm, ETSI:10dBm (max) @ 802.11b • FCC:19dBm, ETSI:12Bm (max) @ 802.11g • FCC:19dBm, ETSI:12dBm (max) @ 802.11n HT20 • FCC:19dBm, ETSI:12dBm (max) @ 802.11n HT40 **5G Mode** • FCC:24dBm, ETSI:22dBm (max) @ 802.11a • FCC:24dBm, ETSI:22dBm (max) @ 802.11n HT20 / 802.11ac VHT20 • FCC:15dBm, ETSI:22dBm (max) @ 802.11ac VHT80
Antenna Type	• 2.4 GHz: 2 x 4dBi (Peak) PIFA Antenna's internal • 5 GHz: 2 x 4dBi (Peak) PIFA Antenna's internal
Antenna Gain	• 2.4 GHz: 2 dBi (max.) / 0 dBi (Avg.) internal • 5 GHz: 2 dBi (max.) / 0 dBi (Avg.) internal
Protocol	TCP/IP
Hardware Interface	• LAN: 1 x 10/100/1000Mbps Auto-MDIX Gigabit Ethernet port • Reset button • Power Jack
Operation Modes	• Access Point (AP), AP+WDS
SSID	Up to 4 SSIDs per band (AP mode)
Supported Network Protocols	• TCP/IP • HTTP
DHCP Server/Client Network Management	Web base configuration utility via Ethernet
Channel	• 2.4GHz: Channel 1 ~ 11(FCC), Channel 1 ~ 13(ETSI) • 5 GHz: 36, 40, 44, 48, 149, 153, 157, 161 and 165 (FCC), 36, 40, 44, 48(ETSI)
Security	• 64/128-bits WEP Encryption • WPA, WPA2 • WPA-PSK, WPA2-PSK • MAC address filtering

Item	Specifications
Range Coverage	• Indoor: Up to 100 meters (depends on environment) • Outdoor: Up to 300 meters (depends on environment)
Diagnostic LEDs	• Power • 2.4G Wireless • 5G Wireless • LAN
Power Adapter	12VDC / 1A external power adapter
Power Consumption	9.6 Watt
Operation Temperature	0 - 40°C (32 - 104°F)
Storage Temperature	-10 ~ 70°C
Operating Humidity	Maximum 10% ~ 95% 95%, no condensation
Certifications	• FCC certificate for USA • CE certificate for Europe
Dimensions (D x W x H)	187 x 187 x 46 mm (7.4 x 7.4 x 1.8 in.)
Weight	406g (12 oz.)
Warranty	3 years limited warranty

Federal Communication Commission Interference Statement

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.

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.

Operation of this device is restricted to indoor use only.

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

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

Country Code selection feature to be disabled for products marketed to the US/CANADA

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.
Regulation (EC) No. 1275/2008
Regulation (EC No. 278/2009
EN60950-1 : 2006 + A11 : 2009 + A1: 2010 + A12: 2011

Safety of Information Technology Equipment
EN 62311: 2008 :
Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz-300 GHz)

EN 300 328 V1.8.1 : (2012-06) Class B
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.9.2 : (2011-09)
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 : (2012-09)
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for 2,4 GHz wideband transmission systems, 5 GHz high performance RLAN equipment and 5,8 GHz Broadband Data Transmitting Systems

EN 301 893 V1.7.1 : (2012-06)
Broadband Radio Access Networks (BRAN);5 GHz high performance RLAN;Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive
This device is a 2.4/5G GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.
In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.
This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

Industry Canada Statement:

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions:

(1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil est conforme aux CNR exemptes de licence d'Industrie Canada. Son fonctionnement est soumis aux deux conditions suivantes:

(1) Ce dispositif ne peut causer d'interférences; et(2) Ce dispositif doit accepter toute interférence, y compris les interférences qui peuvent causer un mauvais fonctionnement de l'appareil.

Caution:

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

Avertissement:

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

Radiation Exposure Statement:

This equipment complies with IC 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.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

cs Česky [Czech]	TRENDnet tímto prohlašuje, že tento TEW-814DAP je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES, 2006/95/ES, a 2009/125/ES.
da Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-814DAP overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF, 2006/95/EF, og 2009/125/EF.
de Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TEW-814DAP in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG, 2006/95/EG und 2009/125/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEW814DAP vastavust direktiivi 1999/5/EÜ, 2006/95/EÜ ja 2009/125/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	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.
es Español [Spanish]	Por medio de la presente TRENDnet declara que el TEW-814DAP cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE, 2006/95/CE, 2009/125/CE y.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑTRENDnet ΔΗΛΩΝΕΙ ΟΤΙ TEW-814DAP ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ, 2006/95/ΕΚ, 2009/125/ΕΚ και.
fr Français [French]	Par la présente TRENDnet déclare que l'appareil TEW-814DAP est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE, 2006/95/CE, 2009/125/CE et.
it Italiano [Italian]	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.
lv Latviski [Latvian]	AršoTRENDnetdeklarē, ka TEW-814DAP atbilstDirektīvas 1999/5/EK, 2006/95/EK, un 2009/125/EK būtiskajāmprasībām un citiemar to saistītajiemnoteikumiem.

lt Lietuvių [Lithuanian]	Šiuo TRENDnet deklaruoja, kad šis TEW-814DAP atitinka esminius reikalavimus ir kitas 1999/5/EB, 2006/95/EB ir 2009/125/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEW-814DAP in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG, 2006/95/EG, en 2009/125/EG.
mt Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TEW-814DAP jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/KE, 2006/95/KE, u 2009/125/KE.
hu Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-814DAP megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv, a 2006/95/EK és a 2009/125/EK irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEW-814DAP jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/WE, 2006/95/WE i 2009/125/WE.
pt Português [Portuguese]	TRENDnet declara que este TEW-814DAP está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE, 2006/95/CE e 2009/125/CE.
sl Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEW-814DAP v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES, 2006/95/ES in 2009/125/ES.
sk Slovensky [Slovak]	TRENDnettýmtovyhlasuje, že TEW-814DAP spĺňazákladnépožiadavky a všetkypríslušnéustanoveniaSmernice 1999/5/ES, 2006/95/ES, a 2009/125/ES.
fi Suomi [Finnish]	TRENDnet vakuuttaa täten että TEW-814DAP tyyppinen laite on direktiivin 1999/5/EY, 2006/95/EY ja 2009/125/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar TRENDnet att denna TEW-814DAP 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.

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-821DAP – 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.

TRENDnet®

Product Warranty Registration

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

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA