

User's Guide

TRENDNET[®]



Dual Band Wireless Access Point

TEW-814DAP

Table of Contents

Product Overview	4	Log in to the Management Page	10
Features	4	Access Point Mode Management Page Structure	11
Package Content	4	Client Bridge/AP Repeater Mode Management Page Structure ..	11
Hardware Overview	5	Selecting Device Mode	12
<i>Front View</i>	5	Access Point Mode	12
<i>Rear View</i>	5	<i>Configuring the Device as Access Point</i>	13
Wireless Considerations	6	<i>Using Access Point Mode</i>	13
<i>Connection Performance</i>	6	<i>Wireless Networking and Security</i>	14
<i>Security Checklist</i>	6	<i>Connect Wireless Devices to your Access Point</i>	17
Installation	7	<i>Connect Wireless Devices using WPS</i>	17
Connect the Power	7	<i>Configure Multiple SSID Settings</i>	18
Connect the Computer	7	<i>Configure User Limit Settings</i>	19
Check the Installation	7	<i>Advanced Wireless Settings</i>	19
Initial Setup	8	Wireless Bridge (WDS) Mode	20
Configure the Computer	8	<i>Planning for Wireless Bridging</i>	20
<i>Windows 7/8/8.1</i>	8	<i>Pure Wireless Bridge</i>	22
<i>Windows Vista</i>	8	<i>Wireless Bridge with Access Point Mode</i>	24
<i>Windows XP/2000</i>	8	<i>Creating a Wireless Bridge (WDS)</i>	26
Setup Wizard	8	<i>Additional WDS Options</i>	27

Client Bridge Mode	28	Reset to Factory Defaults	41
<i>Configuring the Device as Client Bridge</i>	29	Update System Firmware	42
<i>Using Client Bridge Mode</i>	29	System Reboot	42
AP Repeater Mode	30	Configure Syslog Server	43
<i>Configuring the Device as AP Repeater</i>	31	View System Information	43
<i>Using AP Repeater Mode</i>	31	<i>View the Device Information</i>	43
Advanced Settings	32	<i>View the Data Traffic Statistics</i>	44
Configure MAC Filter Settings	32	<i>View the Connected Wireless Clients</i>	44
Change the IP Address	33	<i>View the Wireless Connection Information</i>	44
Configure IPv6 Settings	34	View Events Log	45
Configure the DHCP Server	35	Appendix	46
Create Schedules	36	Federal Communication Commission Interference Statement	46
<i>Edit a Schedule</i>	36	Europe – EU Declaration of Conformity	46
Configure Email Settings	37	Specifications	48
Enable Ping Test	38		
Maintenance	38		
Change Login Password	38		
Change the Device Name	39		
Set the Date and Time	39		
Backup System Settings	40		

Product Overview

TRENDnet's AC1200 Dual Band Wireless Access Point, model TEW-814DAP, 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

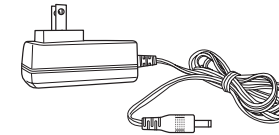
- Compatible with IEEE 802.11ac technology:
 - ◆ 2TX/2RX wireless speed up to 867Mbps data rate
 - ◆ Provides uninterrupted HD video streaming in a busy connected environment
- Compatible with IEEE 802.11n high rate standard to provide wireless speed of 300Mbps data rate
- Compatible with IEEE 802.11g high rate standard to provide wireless speed of 54Mbps data rate
- 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 WAN port for ADSL / Cable Modem with Auto MDI-X 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
- IPv6 network support
- Supports up to four SSIDs per wireless band
- Web-based configuration tools and management via WEB Browser
- Multi Language support (English, Spanish, French, German, and Russian)
- Supports WPS (Wi-Fi Protected Setup Specification Windows)
- Provides real time logs and statistics for efficient troubleshooting
- Embedded GREENnet technology, allowing to reduce power consumption up to 50%

Package Content

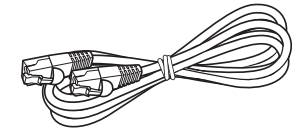
Check if your package contains the following items. If any item is missing or appears damaged, contact your dealer.



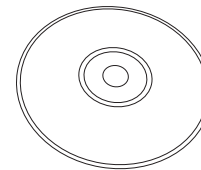
Access Point



Power Adapter (12V, 1A)



RJ-45 Ethernet cable



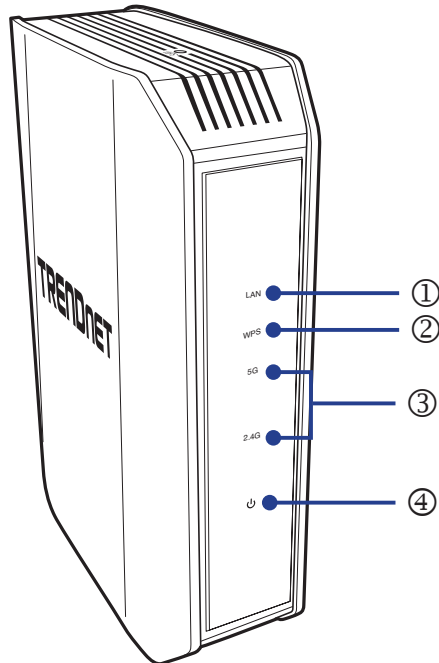
CD-ROM (User's Guide)



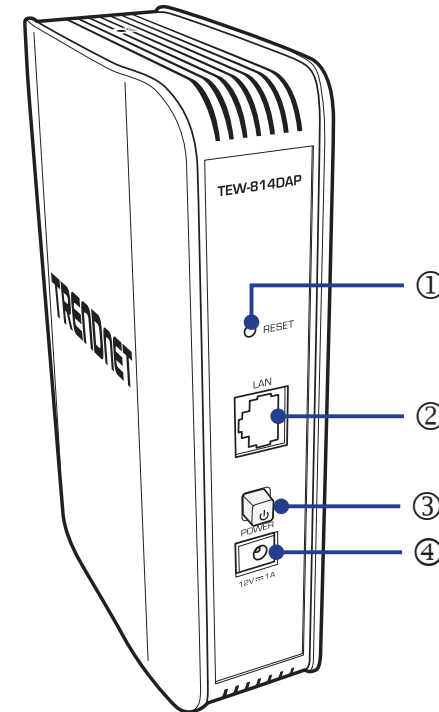
Quick Start Guide

Hardware Overview

Front View



Rear View



No.	Item	Description
1	LAN LED	The indicator turns on solid green when the wireless is enabled on your access point. This LED blinks green during data transmission.
2	WPS LED	The indicator will blink when the WPS function is activated. The LED will stop blinking and remain solid green automatically once the WPS process is completed.
3	5G/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.
4	POWER LED	A solid green light indicates a proper connection to the power supply.

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	LAN Port	Connect the Ethernet cable (also called network cables) from your access point to your router and wired network devices.
3	Power Button	Press this button to turn your access point on or off ("On" (Inner position) or "Off" (Outer position)).
4	Power Port	Connect the power adapter from your access point power port to an available power outlet.

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**

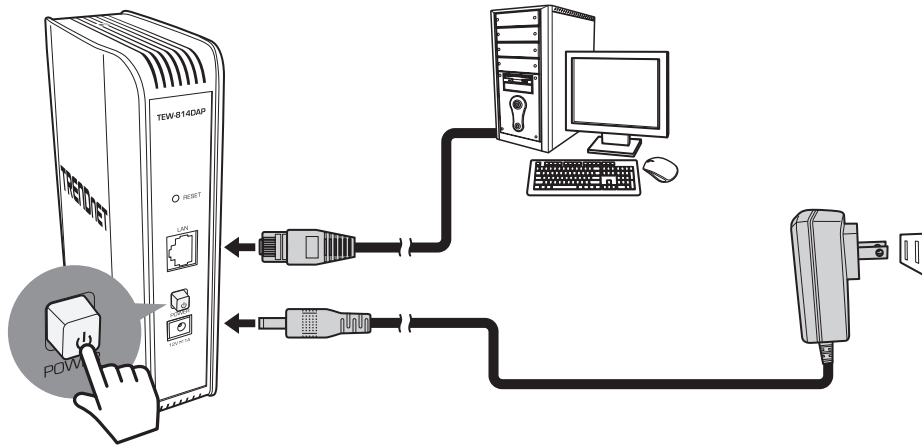
Your device has a default password. You have to enter this password to change your network settings. Change the password to prevent unauthorized users from hacking into your network and changing the settings.
- ✓ **Enable MAC address filtering**

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.
- 3 Push the **Power** button to turn your access point on.

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 RJ-45 cable to the Ethernet port of your access point.
- 2 Connect the other end of the RJ-45 cable to the Ethernet port of the computer.

Check the Installation

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 5](#) for more information about the LED indicators.

Initial Setup

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

IP address: 192.168.10.x

Subnet mask: 255.255.255.0

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**.

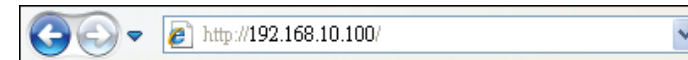
Windows XP/2000

- 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**.

Setup Wizard

With Setup Wizard, it will guide you through simple steps to help you connect your access point to the Internet and configure the device mode.

- 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.



- ↳ *Note:* You can also access the device using the following URL/domain name: <http://tew-814dap>.

- 2 Enter the default user name and password, select your preferred language, then click **Login**.

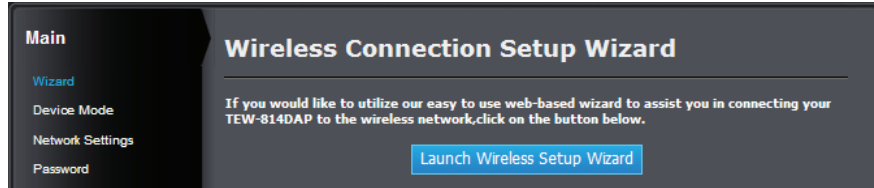
Default User Name: Admin

Default Password: admin

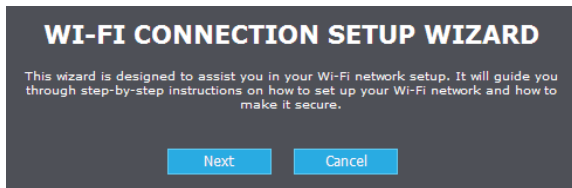
TEW-814DAP LOGIN	
User Name:	Admin
User Password:
Language:	English
<input type="button" value="Login"/>	

- ↳ *Note:* User name and Password are case sensitive.

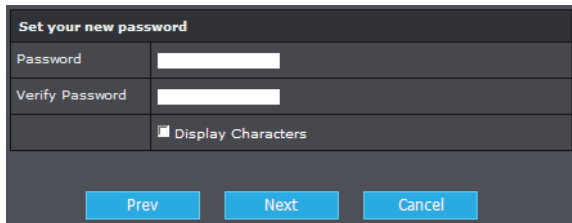
3 Click **Launch Wireless Setup Wizard** to configure your Internet connection on your access point.



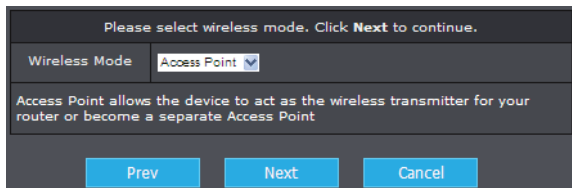
4 The *Setup Wizard* main page appears. Click **Next** to begin the wizard.



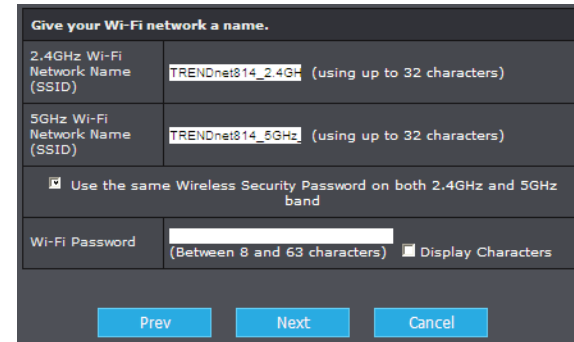
5 Set your new password and then click Next.



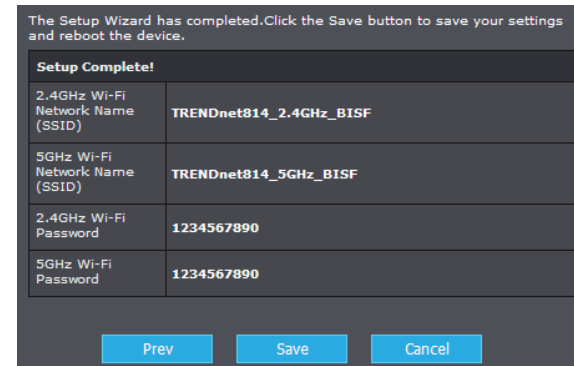
6 On *Wireless Mode*, select **Access Point** and then click **Next**.



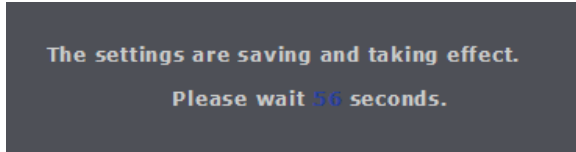
7 Enter the Wireless Network Name (SSID) you would like to assign your wireless network. Then enter the password or encryption key assigned to your wireless network. Click **Next** to continue.



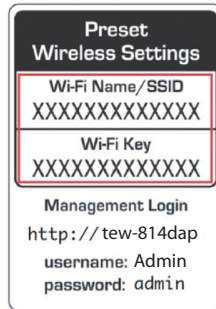
8 Verify your wireless settings are correct and click **Save** to save your settings.



9 The system will reboot once the process is completed. Please wait while the settings are being applied.



Note: You can also find the default wireless settings information on the label on the bottom of the access point.



Log in to the Management Page

- 1 Open your web browser and do one of the following:
 - enter the URL/domain name <http://tew-814dap>, or
 - enter the IP address <http://192.168.10.100>.
- 2 Enter the user name and password and then click **Login**. The main screen appears.



- 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.

Access Point Mode Management Page Structure

Main	Wireless	Status	Access	Tools
<ul style="list-style-type: none"> • Wizard • Device Mode <ul style="list-style-type: none"> ◆ Access Point ◆ AP Repeater ◆ Client Bridge • Network Settings <ul style="list-style-type: none"> ◆ LAN IPV4 Connection Type ◆ Dynamic IP (DHCP) LAN Connection Type • Password <ul style="list-style-type: none"> ◆ Device Name ◆ Password • Time • IPv6 	<ul style="list-style-type: none"> • Basic <ul style="list-style-type: none"> ◆ Wireless Mode ◆ 2.4GHz Wireless Network & Security Settings ◆ 5GHz Wireless Network & Security Settings • Advanced <ul style="list-style-type: none"> ◆ Advanced Wireless Settings • WPS (Wi-Fi Protected Setup) <ul style="list-style-type: none"> ◆ Wi-Fi Protected Setup ◆ Pin Settings ◆ Add Wireless Station 	<ul style="list-style-type: none"> • Device Info • Logs • Statistics • Wireless Client • IPv6 	<ul style="list-style-type: none"> • MAC Filter • Multi SSID • User Limit 	<ul style="list-style-type: none"> • Upload Firmware • Settings Management <ul style="list-style-type: none"> ◆ Save Configuration Settings ◆ Restore Configuration Settings ◆ Restore Factory Default Settings ◆ System Reboot • Ping Test • Schedule • Email Settings • Syslog • Logout

Client Bridge/AP Repeater Mode Management Page Structure

Main	Wireless	Status	Tools
<ul style="list-style-type: none"> • Wizard • Device Mode <ul style="list-style-type: none"> ◆ Access Point ◆ AP Repeater ◆ Client Bridge • Network Settings <ul style="list-style-type: none"> ◆ LAN IPV4 Connection Type ◆ Dynamic IP (DHCP) LAN Connection Type • Password <ul style="list-style-type: none"> ◆ Device Name ◆ Password • Time • IPv6 	<ul style="list-style-type: none"> • Site Survey 	<ul style="list-style-type: none"> • Device Info • Logs • Statistics • Wireless Client • IPv6 	<ul style="list-style-type: none"> • Upload Firmware • Settings Management <ul style="list-style-type: none"> ◆ Save Configuration Settings ◆ Restore Configuration Settings ◆ Restore Factory Default Settings ◆ System Reboot • Ping Test • Schedule • Email Settings • Syslog • Logout

Selecting Device Mode

The access point offers the following modes:

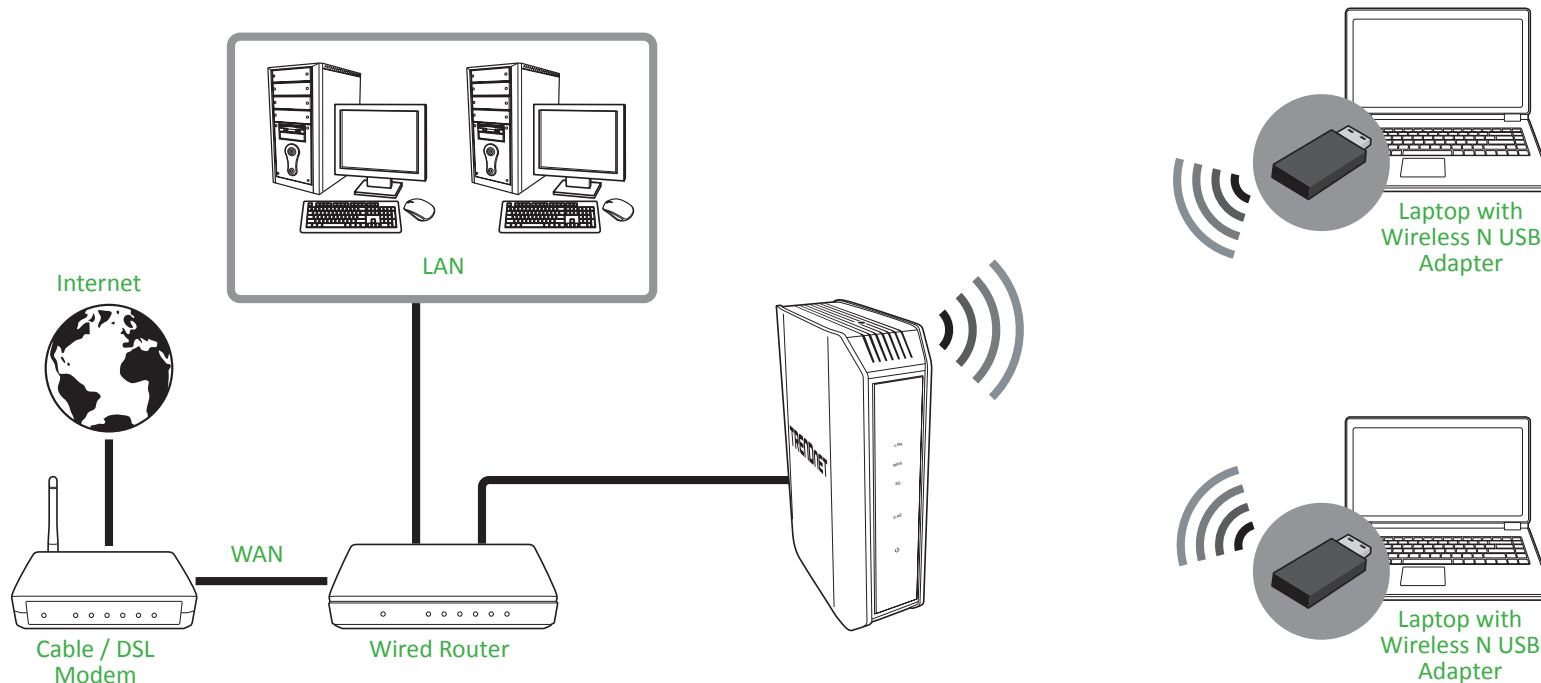
- Access Point (Default)
- Wireless Bridge (also known as WDS mode)
- Wireless Client Bridge
- Wireless AP Repeater

Access Point Mode

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

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

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.

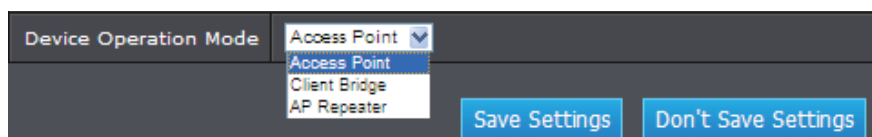


Configuring the Device as Access Point

Main > Device 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 the Management Page” on page 10).
- 2 Click **Main > Device Mode**.
- 3 On *Device Operation Mode*, select **Access Point**.



- 4 Click **Save Settings** to save changes.

Note: To discard the changes, click Don't Save Settings.

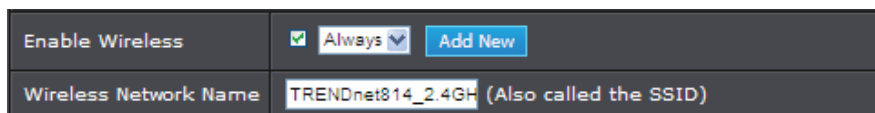
Using Access Point Mode

Wireless > Basic > 2.4GHz Wireless Network Settings or 5GHz Wireless Network Settings

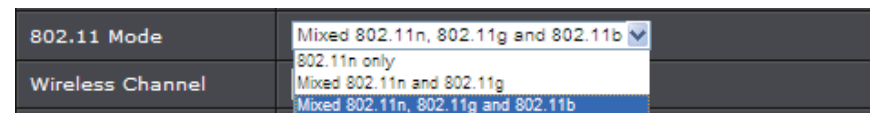
- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Wireless > Basic > 2.4GHz Wireless Network Settings or 5GHz Wireless Network Settings**.
- 3 Configure the following settings, click **Save Settings** when finished.

- **Enable Wireless:** Check the option to enable the wireless network/band or uncheck to disable.
 - Click **Add New** to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule. (Refer to “Create Schedules” on page 36).

Note: It is recommended to leave this setting checked.

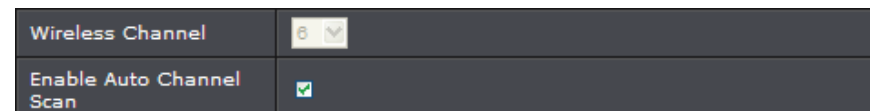


- **Wireless Network Name (SSID):** Enter the wireless name (SSID) for your wireless network. This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. By default, the access point's wireless name is unique to the device. If you choose to change the SSID, change it to a name that you can easily remember.
- **802.11 Mode:** Select the appropriate transmission mode. When applying the 802.11 Mode setting, please keep in mind the following:



- ✓ Wireless devices that support 802.11n are backwards compatible and can connect wirelessly at 802.11g, 802.11b, or 802.11a.
- ✓ Connecting at 802.11b, 802.11g, or 802.11a will limit the capability of your 802.11n supported wireless devices from obtaining higher performance and data rates.
- ✓ Allowing 802.11b, 802.11g, or 802.11a devices to connect to an 802.11n capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11n.
- ✓ Wireless devices that only support 802.11b, 802.11g, or 802.11a will not be able to connect to a wireless network that is set to 802.11n only mode.
- ✓ Wireless devices that only support 802.11b will not be able to connect to a wireless network that is set to 802.11g only mode.

- **Wireless Channel:** Uncheck the **Enable Auto Channel Scan** option to manually set the channel on which the access point will broadcast. Click the drop-down list and select the desired channel for wireless communication. The goal is to select the channel that is least used by neighboring wireless networks.



- **Enable Auto Channel Scan:** Check this option to set your access point to scan for which wireless channels to use automatically.

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

Channel Width	Auto 20/40MHz
Visibility Status	Auto 20/40MHz visible

- ↳ *Note: Please note that this setting may provide more stability than the higher channel bandwidth settings such as 20/40MHz (Auto) for connectivity in busy wireless environments where there are several wireless networks in the area.*
- 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.
- **Visibility Status:** Give you option to hide you wireless network name.

Visibility Status	<input checked="" type="radio"/> Visible <input type="radio"/> Invisible
-------------------	--

- Visible: Select this option to allow the wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your access point.
- Invisible: Select this option to turn off the ability for wireless devices to find your network. It is still possible for wireless devices to be configured to connect to your wireless network. Disabling this setting will disable WPS functionality.

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

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

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

Wireless Encryption Types

- **WEP:** Legacy encryption method supported by older 802.11b/g hardware. This is the oldest and least secure type of wireless encryption. It is generally not recommended to use this encryption standard, however if you have old 802.11 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 > Basic > 2.4GHz Wireless Security Setting or 5GHz Wireless Security Setting

After you have determined which security type to use for your wireless network (refer to "Choose the Security Type for Wireless Network" on page 15), 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 the Management Page" on page 10).
- 2 Click **Wireless > Basic > 2.4GHz Wireless Security Setting** or **5GHz Wireless Security Setting**.
- 3 On *Security Mode*, select your wireless security type.
 - If the security type is set to **WEP** (Wired Equivalent Privacy), review the WEP settings to configure and click **Save Settings** to save the changes.

2.4GHz Wireless Security Setting	
Security Mode	WEP
WEP Encryption	64 bit (10 hex digits)
WEP Key 1	<input type="text"/> <input type="checkbox"/> Display Characters
Authentication	Both

- WEP Encryption: Choose the key length 64-bit or 128-bit.
 - Note:* It is recommended to use 128-bit because it is more secure to use a key that consists of more characters.
- WEP Key 1: Enter the WEP key. This is the password or key that is used to connect your computer to this access point wirelessly.
- Authentication: Select the authentication type.
 - Note:* It is recommended to use Both which includes both Open and Shared. Open is known to be more secure than Shared Key.

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

2.4GHz Wireless Security Setting	
Security Mode	WPA-Personal
WPA Mode	AUTO (WPA or WPA2)
Cipher Type	TKIP and AES
Pre-Shared Key	<input type="text"/> <input type="checkbox"/> Display Characters

- WPA Mode: Select the WPA security type.
- Cipher Type: 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 **Save Settings** to save the changes. This security type is also known as EAP (Extensible Authentication Protocol) or Remote Authentication Dial-In User Service or RADIUS.

2.4GHz Wireless Security Setting	
Security Mode	WPA-Enterprise
WPA Mode	AUTO (WPA or WPA2)
Cipher Type	TKIP and AES
RADIUS Server IP Address	<input type="text"/>
RADIUS Server Port	<input type="text"/>
RADIUS Server Shared Secret	<input type="text"/> <input type="checkbox"/> Display Characters
<input type="button" value="Advanced"/>	

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

- RADIUS Server IP Address: Enter the IP address of the RADIUS server. (i.e. 192.168.10.250)
- RADIUS Server Port: Enter the port your RADIUS server is configured to use for RADIUS authentication.
 - ↳ *Note: It is recommended to use port 1812 which is typical default RADIUS port.*
- RADIUS Server Shared Secret: Enter the shared secret used to authorize your access point with your RADIUS server.
- Advanced: Click this option to set up an additional backup 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.

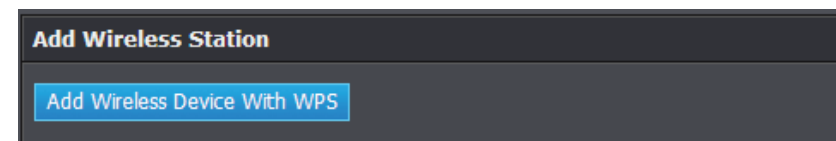
- Push Button Configuration (PBC) method
- PIN (Personal Identification Number) method

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

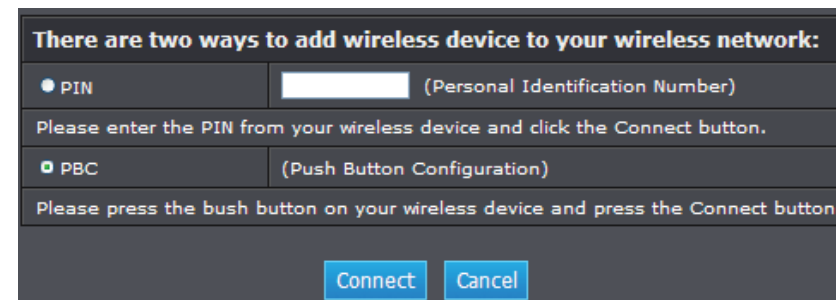
PBC (Software/Virtual Push Button)

Wireless > Wi-Fi Protected Setup

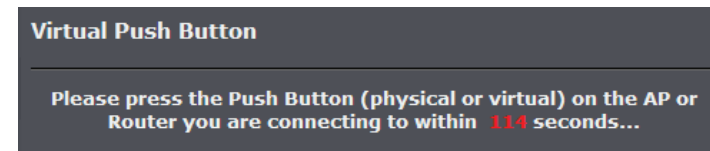
- 1 Log into your access point management page (refer to "Log in to the Management Page" on page 10).
- 2 Click **Wireless > Wi-Fi Protected Setup**.
- 3 On the **Add Wireless Station** section, click **Add Wireless Device With WPS** to add a wireless device to your network.



- 4 Select **PBC** and click **Connect**. Then push the WPS button on the wireless device (consult wireless device's User's Guide for length of time) you are connecting to your network.



- 5 Wait for your access point to finish the WPS process.

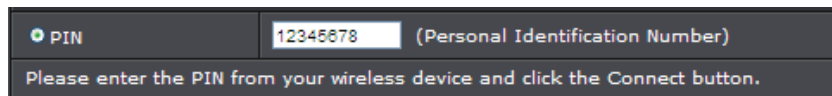


PIN (Personal Identification Number)

Wireless > Wi-Fi Protected Setup

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

- 1 Log into your access point management page (refer to "Log in to the Management Page" on page 10).
- 2 Click **Wireless > Wi-Fi Protected Setup**.
- 3 Click **Add Wireless Device With WPS** to add a wireless device to your network.
- 4 Select **PIN** and enter the 8-digit numeric PIN number of the wireless client device. Then click **Connect**.

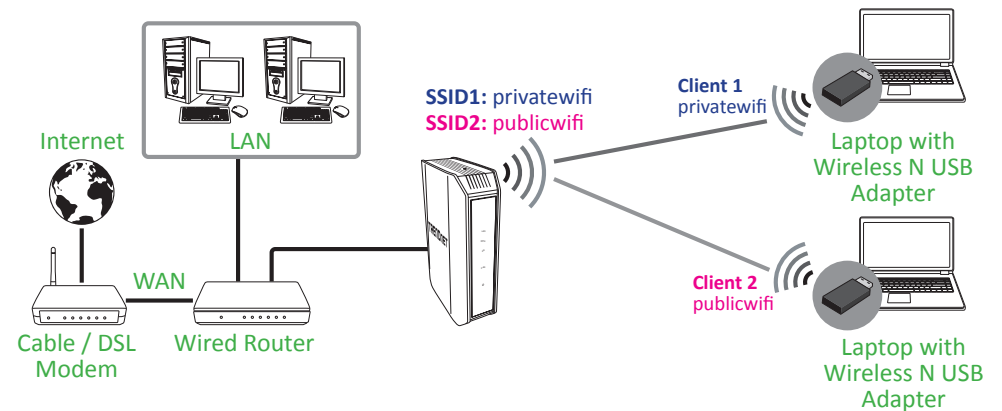


- 5 Wait for your access point to finish the WPS process.

Configure Multiple SSID Settings

Access > Multi-SSID

The multiple SSID feature allows you to broadcast up to 3 additional SSIDs (or wireless network names) per band (2.4GHz and 5GHz). When wireless devices are searching for available wireless networks to connect to, the SSIDs (or wireless network names) will appear as separate and different wireless networks. Each SSID can be configured each with a different SSID (or wireless network name), security type and additional settings for wireless devices to connect. You can use the multiple SSID feature to setup guest wireless accounts with a different security type to keep your primary wireless network security information private.



- 1 Log into your access point management page (refer to "Log in to the Management Page" on page 10).
- 2 Click **Access > Multi-SSID > Multi-SSID 2.4G** or **Multi-SSID 5G**.

Multi-SSID 2.4G	
Multi-SSID Index	SSID1
Enable SSID	<input checked="" type="checkbox"/>
Wireless Network Name	TRENDnet814_2.4Gh (Also called the SSID)
Security Mode	None

- 3 On *Multi-SSID Index*, select the SSID to configure.
 - 4 Check the **Enable SSID** option to enable the selected SSID.
 - 5 In the **Wireless Network Name** field, enter the wireless name (SSID) to broadcast for the additional SSID.
 - 6 On *Security Mode*, select the wireless security type for the selected SSID. Refer “[Secure your Wireless Network](#)” on page 16 for details on configuring wireless security.
 - 7 To save changes, click **Save Settings**. Repeat these steps 2-7 to configure the additional SSIDs.
- ⚠ *Note: To verify that the multiple SSIDs are active, using a wireless device, scan for available wireless networks and check if the wireless device is able to discover the SSIDs. To check connectivity, using a wireless device, connect to these SSIDs using the wireless security types you have configured.*

Configure User Limit Settings

Access > User Limit

The multiple SSID feature allows you to set a limit upon the number of wireless clients. Using this features, you can prevent scenarios where the device in your network shows performance degradation because it is handling heavy wireless traffic.

- 1 Log into your access point management page (refer to “[Log in to the Management Page](#)” on page 10).
- 2 Click **Access > User Limit > 2.4Ghz User Limit Settings** or **5Ghz User Limit Settings**.

2.4Ghz User Limit Settings	
Enable User Limit	<input type="checkbox"/>
User Limit (2 - 32)	<input type="text" value="0"/>

- 3 Check the **Enable User Limit** option to enable this function.
- 4 In the **User Limit** field, set the maximum number of wireless clients.
- 5 Click **Save Settings** to save changes.

Advanced Wireless Settings

Wireless > Advanced

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

- 1 Log into your access point management page (refer to “[Log in to the Management Page](#)” on page 10).
- 2 Click **Wireless > Advanced**.

Advanced Wireless Settings	
Transmit Power	<input type="text" value="100%"/>
WMM Enable	<input checked="" type="checkbox"/>
Short GI	<input checked="" type="checkbox"/>
IGMP Snooping	<input type="checkbox"/>
WLAN Partition	<input type="checkbox"/>
HT 20/40 Coexistence	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

- 3 Configure the following settings, click **Save Settings** when finished.
 - **Transmit Power:** Adjust the wireless transmit power to a lower setting. In busy wireless environments, lowering the transmit power may improve better performance and connectivity and decrease interference with neighboring wireless networks.
 - **WMM Enable:** Check to enable the Wi-Fi Multimedia option that improves the user experience for audio, video, and voice applications by prioritizing data traffic.
 - **Short GI:** Check to enable a short (400ns) guard interval function.
 - **IGMP Snooping:** Check to enable the IGMP protocol.
 - **WLAN Partition:** Check to enable WLAN partition function that prevents associated wireless clients from communicating with each other.
 - **HT 20/30 Coexistence:** Select **Enable** to enable this feature.

Wireless Bridge (WDS) Mode

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

There are 2 types of WDS modes:

- WDS (pure WDS) – Strictly for establishing wireless bridging only and will not function in access point simultaneously, allowing wireless client devices such as computers, game consoles, mobile phones, etc. to connect in order to access network resources from multiple groups of network devices as well as the Internet.
- WDS+AP - Allows the device to establish wireless bridging and function as access point simultaneously, allowing wireless client devices such as computers, game consoles, mobile phones, etc. to connect to the access point in order to access network resources from multiple groups of network devices as well as the Internet. Refer to [“Wireless Bridge with Access Point Mode” on page 24](#) for details on this mode.

Planning for Wireless Bridging

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

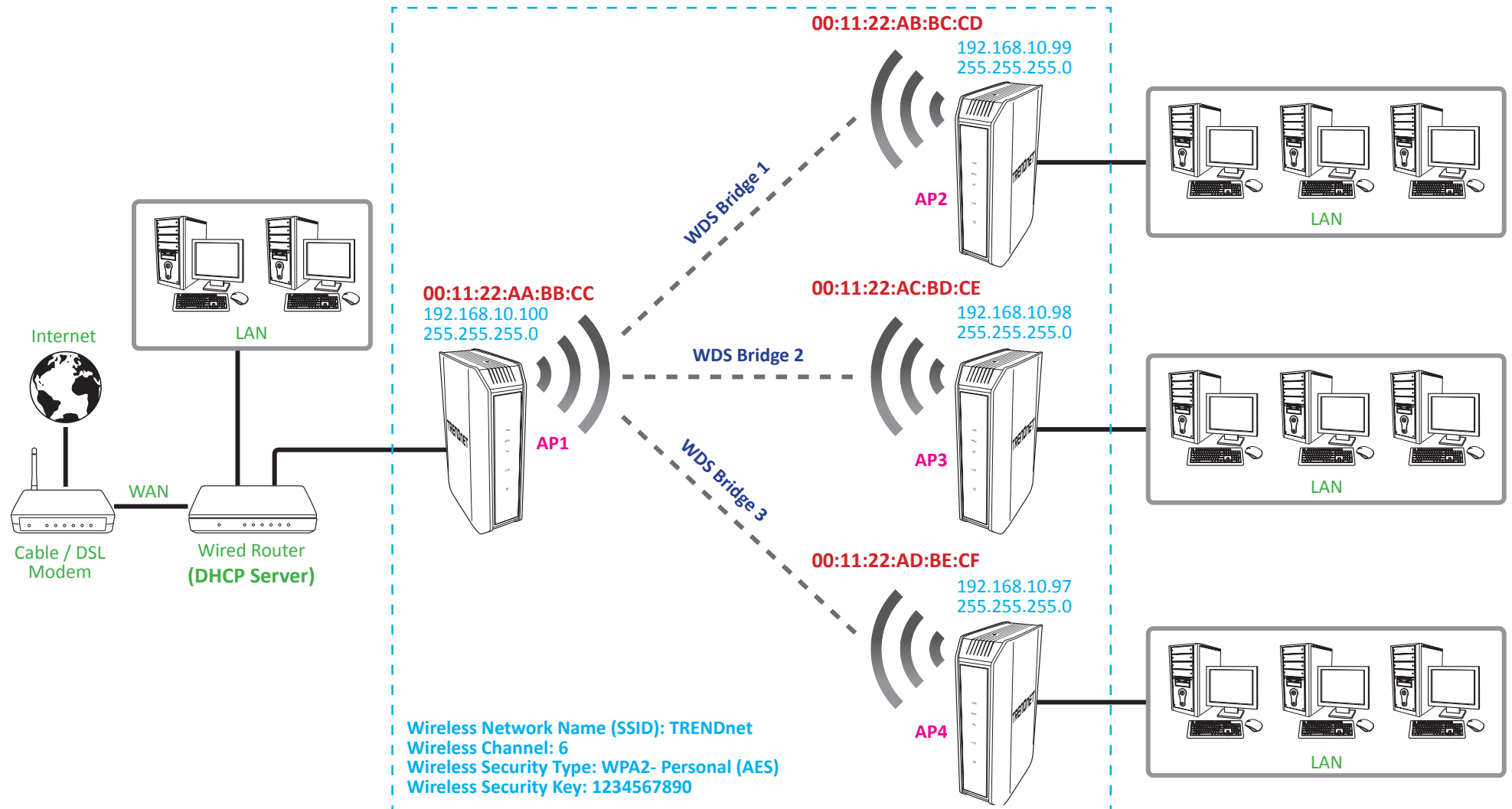
Before configuring WDS, please ensure the following items first:

- 1 Choose which band to use for bridging (2.4GHz or 5GHz). If all of your WDS supported devices do not the 5GHz band, you may need to choose the 2.4GHz.
- 2 Make sure different IP addresses are assigned to each WDS supported wireless device used for bridging. (ex. 192.168.10.100,192.168.10.99,192.168.10.98, etc.) to avoid IP address conflicts. Refer to [“Change the IP Address” on page 33](#) for changing the access point IP address.
- 3 Please ensure that only one DHCP server is assigning IP addresses on your network to avoid IP address conflicts. Typically, most routers used in a home environment include a built-in DHCP server (typically enabled by default) to assign IP addresses to local client devices automatically. Please make sure that only one device on your network has DHCP server enabled and disabled on all others to avoid IP address conflicts.
- 4 WDS bridging requires all WDS supported devices to use the same wireless network name (SSID), wireless channel, and wireless security settings on all WDS supported wireless devices. Refer to [“Using Access Point Mode” on page 13](#) to configure wireless network name (SSID) and wireless channel settings. Refer to [“Wireless Networking and Security” on page 14](#) to configure wireless security settings.
- 5 You will require the wireless MAC address of each WDS supported device. On any network, each network device has a unique 6-digit MAC (Media Access Control) address. For each WDS supported device, all of the remote wireless MAC addresses of the other WDS supported device you are bridging. (For example, in diagram on the next page, AP1 needs to enter the remote MAC addresses of AP2, AP3, and AP4. AP2 needs to enter the remote MAC address of AP1 only, AP3 and AP4 also need to enter the remote MAC address of AP1 only). You can find the wireless MAC address of the access point in the management page under Status > Device Info.

Note: Please note that 2.4GHz and 5GHz bands will have two different MAC addresses.

The diagram below illustrates an example of the parameters configured when planning for WDS bridging.

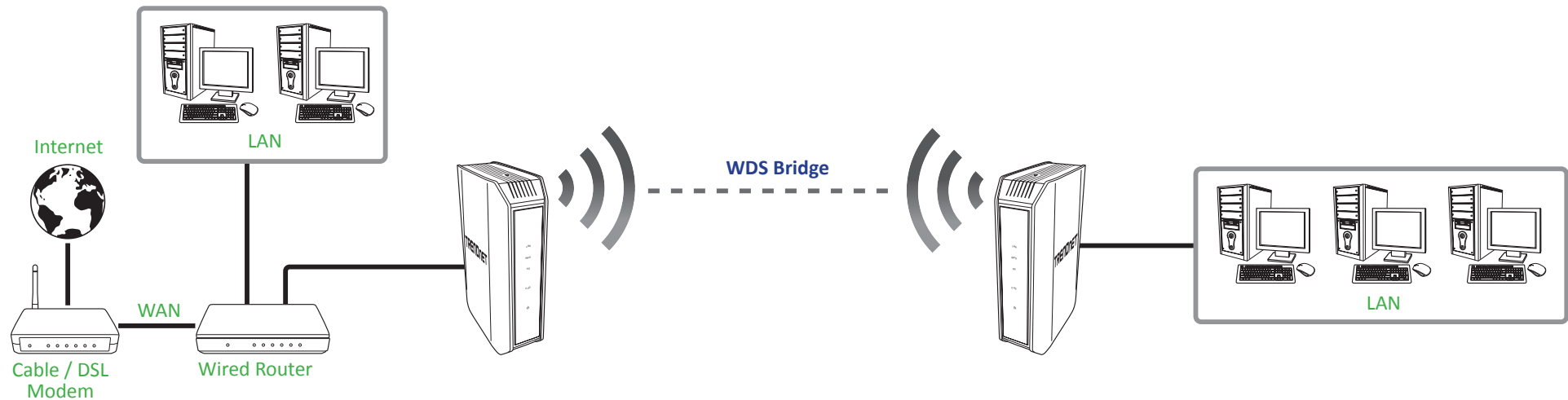
- ✓ Each WDS supported access point is configured with a different IP address (blue) to prevent IP address conflict.
- ✓ The “wired router” is the only single DHCP server (green) providing automatic IP address assignment for all client devices in the network.
- ✓ The WDS parameters required to match on all WDS supported access points in order to establish WDS wireless bridging is configured (blue).
- ✓ The wireless MAC of all devices is noted (red).



Pure Wireless Bridge

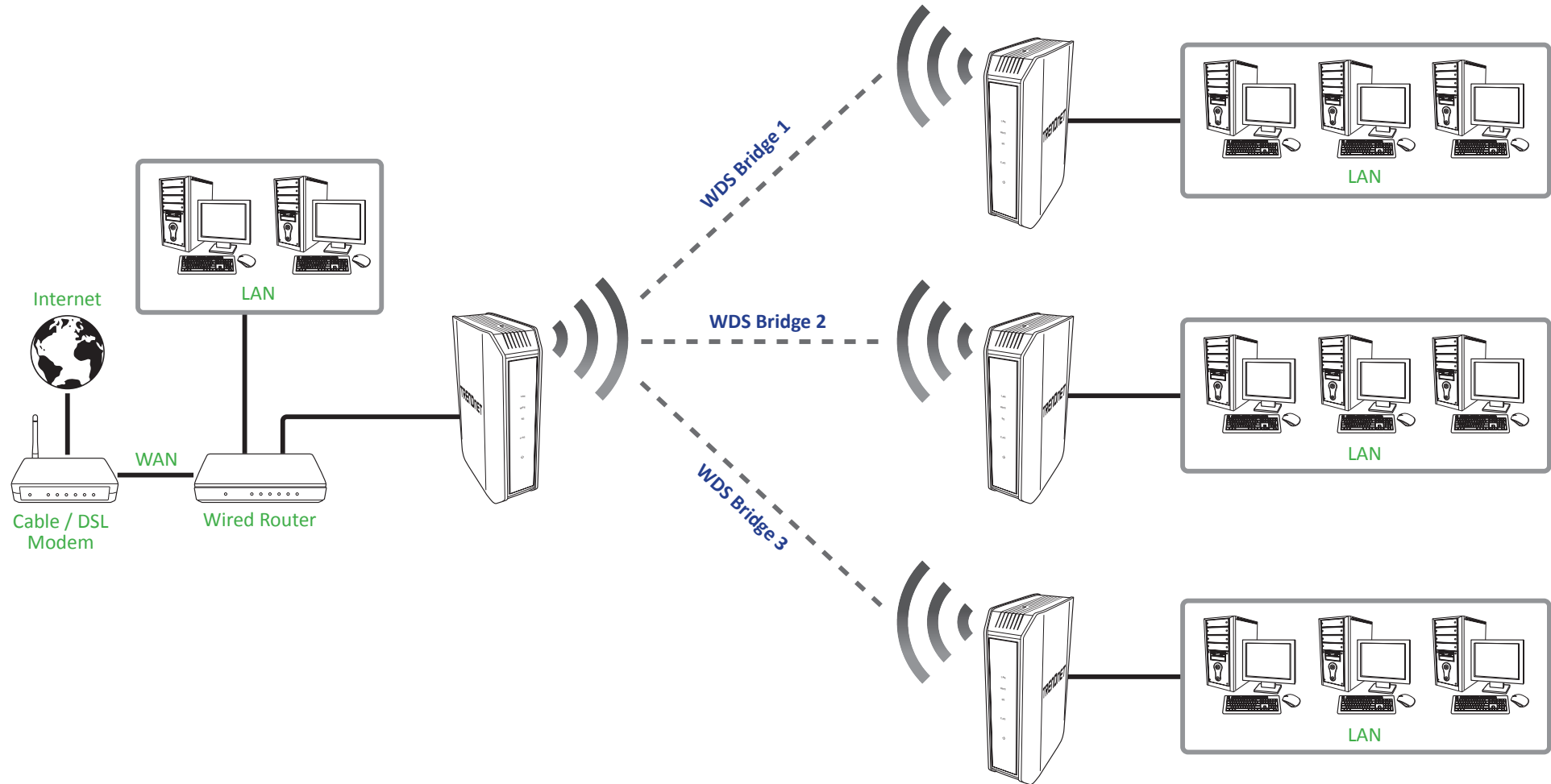
This mode configures the device to operate as a point-to-point or point-to-multipoint WDS wireless bridge to wirelessly bridge to other WDS capable access points or routers. This mode does not operate as an access point simultaneously to allow wireless client devices to connect, only WDS bridge mode.

The diagram below illustrates examples of pure WDS.



Note: You can create up to four WDS bridge connections on each wireless band (2.4GHz and 5GHz). WDS (Wireless Distribution System) is not currently standardized and may not connect to different model wireless routers or access points, therefore, when using WDS, it is recommended to use the same model and version for wireless bridging.

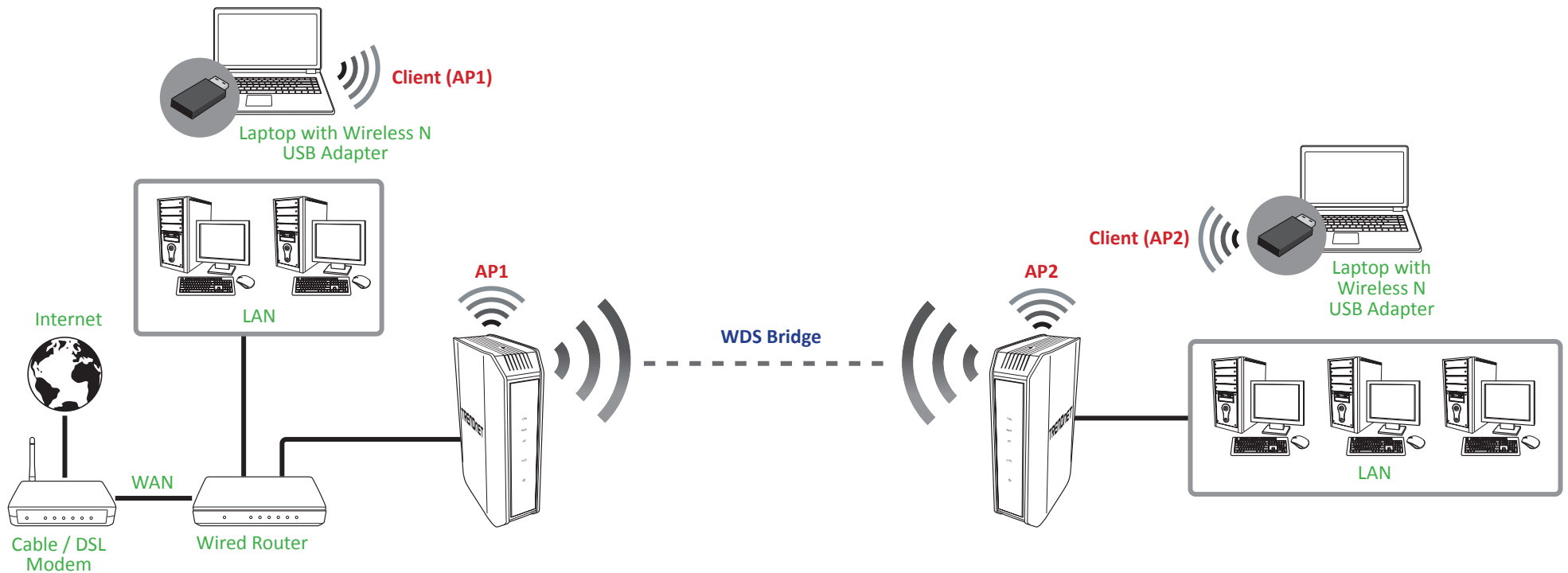
The diagram below illustrates an example of multiple WDS wireless bridge links.



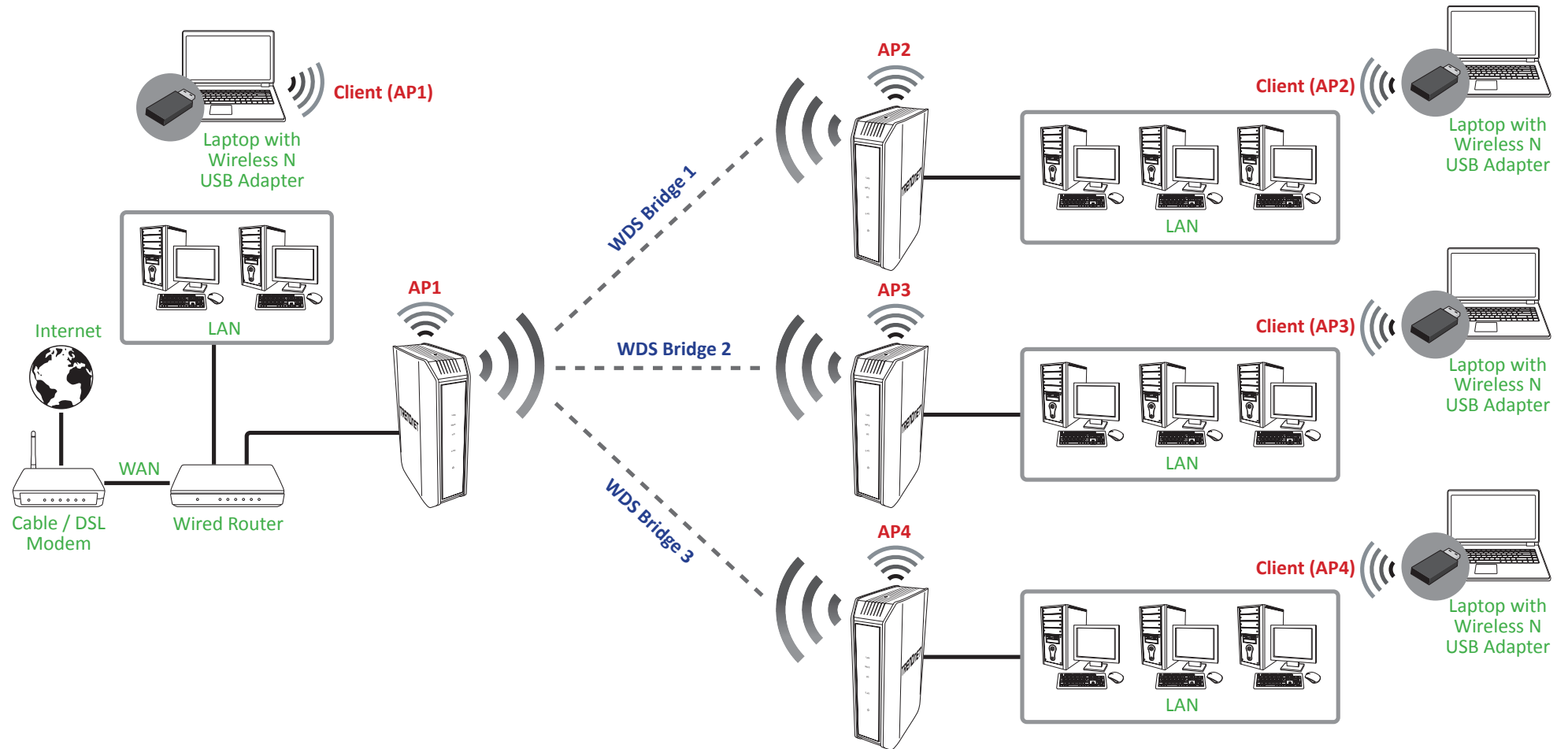
Wireless Bridge with Access Point Mode

This mode configures the device to operate as both an access point to allow wireless client devices to connect and at the same time as a point-to-point or point-to-multipoint WDS wireless bridge to wirelessly bridge to other WDS capable access points or routers. Unlike Access Point and WDS modes, this mode allows the device to operate in both modes at the same time.

Note: You can create up to four WDS bridge connections on each wireless band (2.4GHz and 5GHz). WDS (Wireless Distribution System) is not currently standardized and may not connect to different model wireless routers or access points, therefore, when using WDS, it is recommended to use the same model and version for wireless bridging.



The diagram below illustrates an example of multiple WDS wireless bridge links with access point functionality.

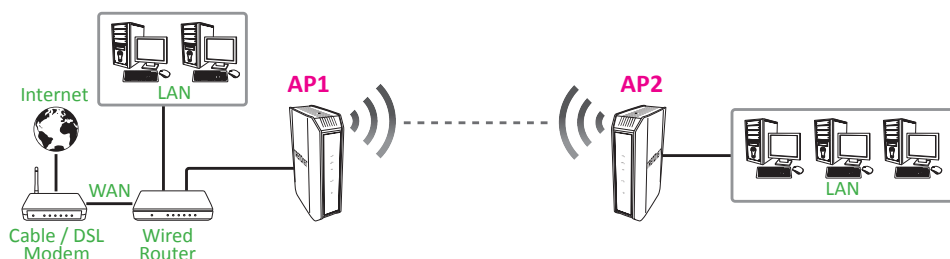


Creating a Wireless Bridge (WDS)

Wireless > Basic

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



- Make note of the wireless MAC address of both access points. Refer to “View the Device Information” on page 43 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.

Example:

AP1 (Access Point 1) 2.4GHz Wireless MAC Address: 00:11:22:AA:BB:C1

AP1 (Access Point 1) 5GHz Wireless MAC Address: 00:11:22:AA:BB:C2

AP2 (Access Point 2) 2.4GHz Wireless MAC Address: 00:11:22:AA:BB:C3

AP2 (Access Point 2) 5GHz Wireless MAC Address: 00:11:22:AA:BB:C4

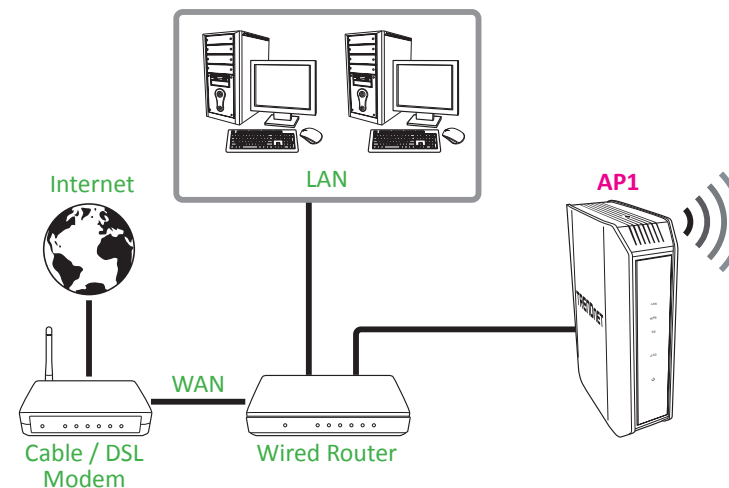
- Make sure the IP address on each WDS supported access is point is different and on the same IP network/subnet. Refer to “Change the IP Address” on page 33 for changing access point IP address.

Example:

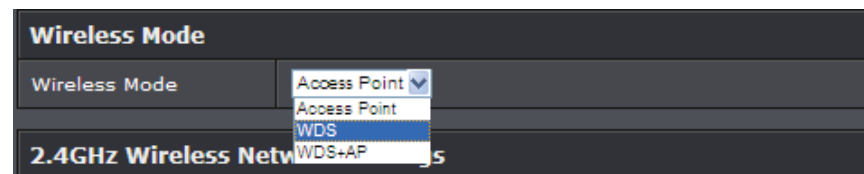
AP1 (Access Point 1) IP Address Settings: 192.168.10.100 / 255.255.255.0

AP2 (Access Point 2) IP Address Settings: 192.168.10.99 / 255.255.255.0

Access Point Configuration (i.e. AP1)



- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Wireless > Basic**.
- 3 On *Wireless Mode*, select one of the WDS options.



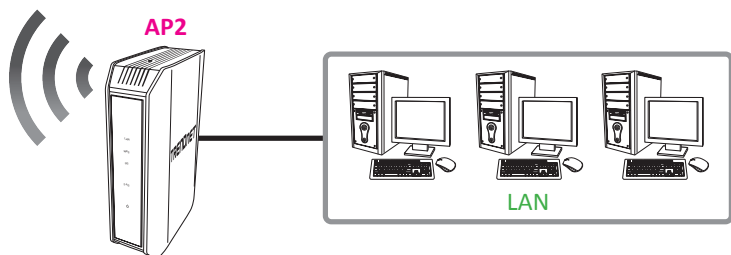
- **WDS:** Select this option to establish wireless bridging only without broadcasting your wireless network name for client devices to connect. Refer to “Wireless Bridge (WDS) Mode” on page 20 for details on this mode.
 - **WDS+AP:** Select this option to establish wireless bridging and broadcast your wireless network name for client devices to connect simultaneously. Refer to “Wireless Bridge with Access Point Mode” on page 24 for details on this mode.
- 4 On the **BRIDGE setting** section, configure the following bridge settings and click **Save Settings** when finished.

BRIDGE setting	
Bridge Band	<input checked="" type="radio"/> 2.4GHz <input type="radio"/> 5GHz
802.11 Mode	Mixed 802.11n, 802.11g and 802.11b
Wireless Channel	6
Channel Width	Auto 20/40MHz
Remote AP Mac:	1. <input type="text"/> 2. <input type="text"/>
	3. <input type="text"/> 4. <input type="text"/>
	5. <input type="text"/> 6. <input type="text"/>
	7. <input type="text"/> 8. <input type="text"/>
Bridge Security	None

- **Bridge Band:** Specify the wireless band type.
- **802.11 Mode:** Select the appropriate transmission mode.
- **Wireless Channel:** Set the channel on which the access point will broadcast.
- **Channel Width:** Select the appropriate channel width for your wireless network.
- **Remote AP Mac:** Enter the wireless MAC address of the remote WDS supported access point or router.
- **Bridge Security:** Select the wireless security type. Refer to “Wireless Networking and Security” on page 14 for details on configuring wireless security settings.

Note:

- To configure other access points, repeat step 1~4 and enter the specific wireless MAC address of the remote WDS supported access point or router.



- This device can support up to 4 wireless WDS bridges per band (2.4GHz and 5GHz).

Additional WDS Options

Lazy WDS

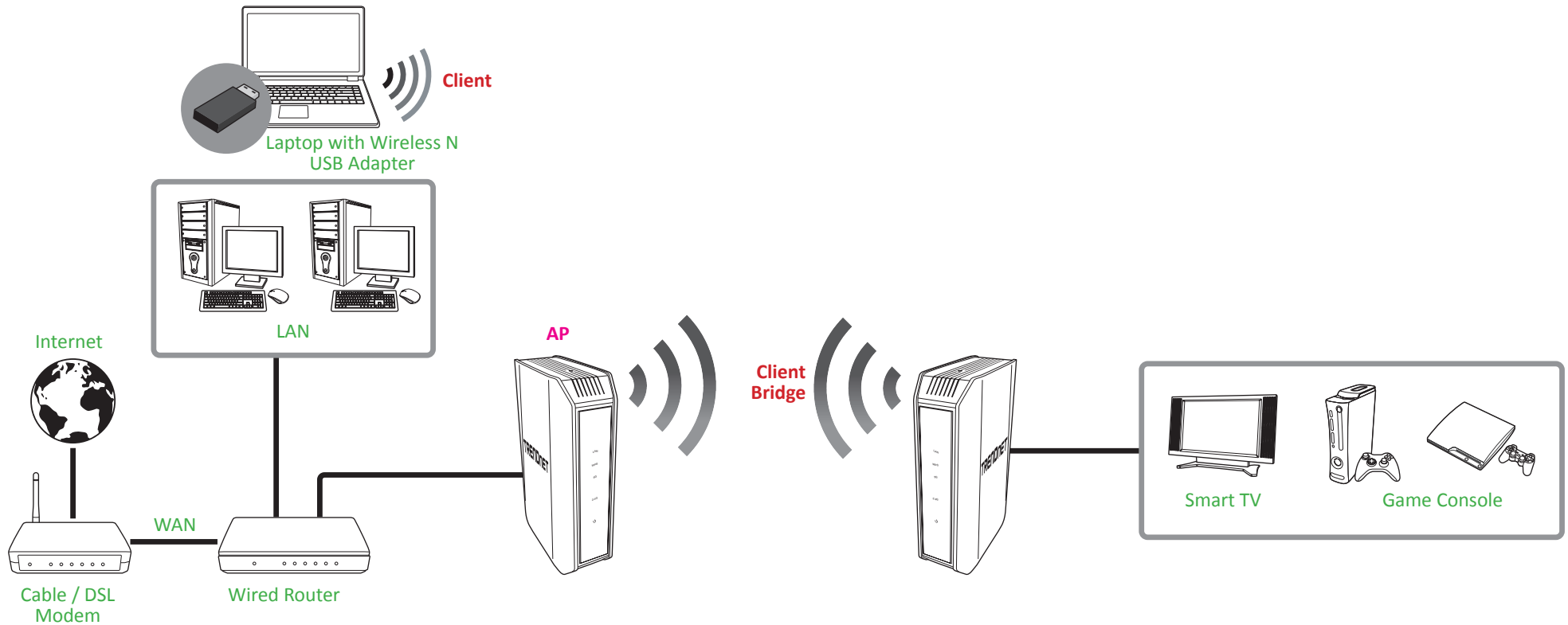
Note: This option is only available when using Wireless Bridge with Access Point.

This option simplifies the configuration of MAC address in WDS by only requiring one side of a WDS bridge to add remote wireless MAC addresses. For example, if the wireless MAC address of AP2 has been added to AP1, the wireless MAC address of AP1 does not need to be added to AP2. On AP2, you would need to simply enable **Lazy WDS** to establish the bridge connection.

Lazy WDS	<input type="checkbox"/>
----------	--------------------------

Client Bridge Mode

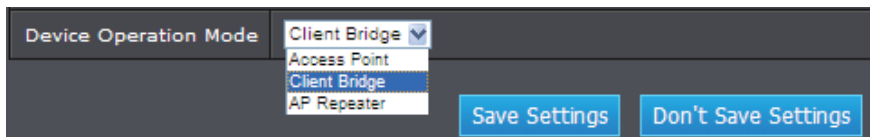
Client Bridge mode allows the device to act as a wireless client device to connect to your wireless network and bridge the wireless connection from the wireless network to the LAN port located on the back of the device. Client devices with wired network capability such as in a media or entertainment 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.



Configuring the Device as Client Bridge

Main > Device Mode

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Main > Device Mode**.
- 3 On *Device Operation Mode*, select **Client Bridge**.



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

Note: To discard the changes, click **Don't Save Settings**.

Using Client Bridge Mode

Wireless > Site Survey

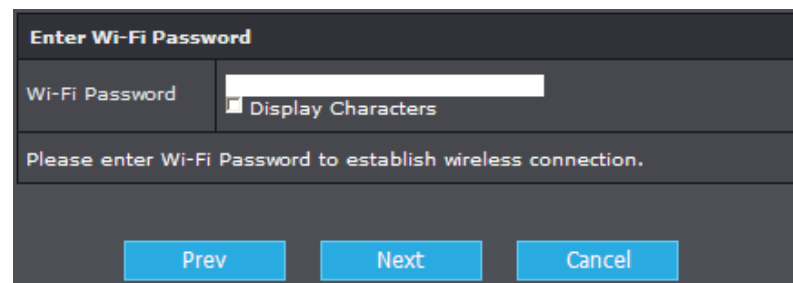
- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Wireless > Site Survey**.
- 3 The available networks are listed. Select a network to connect to.

SITE SURVEY RESULT						
SSID	BSSID	Channel	Type	Encryption	Signal	Select
TRENDnet_5GHz	c0:a0:bb:6e:08:e0	149 (A+N+AC)	AP	WPA2-PSK (aes)	100	<input type="radio"/>
TRENDnet_2.4GHz	c0:a0:bb:6e:08:de	6 (B+G+N)	AP	WPA2-PSK (aes)	99	<input type="radio"/>
HP-Print-71-Officejet 6700	38:ea:a7:4c:84:71	6 (B+G)	AP	None	34	<input type="radio"/>
XXXXX	b8:a3:86:50:9b:80	11 (B+G+N)	AP	WPA2-PSK (aes)	24	<input type="radio"/>

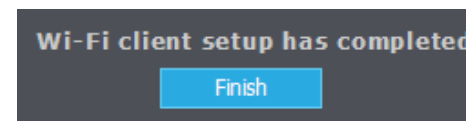
Buttons: Rescan, Next, Cancel

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

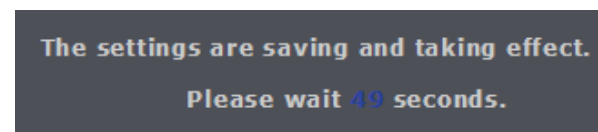
- 4 Click **Next** to connect to the selected wireless network.
- 5 If your wireless network requires wireless security, you will be prompted to enter your wireless key. Enter your Wireless Key required to connect to your existing wireless network and click **Next**.



- 6 Click **Finish** to save the settings.

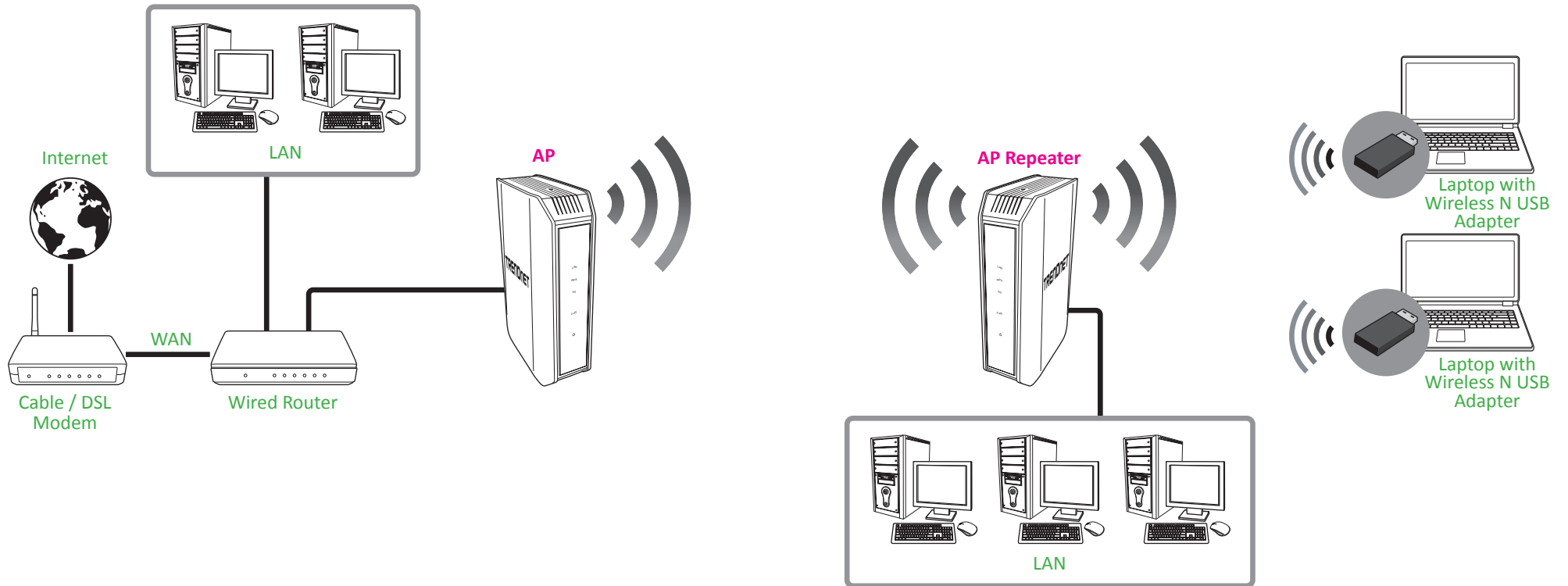


- 7 Wait for the device to apply the settings.



AP Repeater Mode

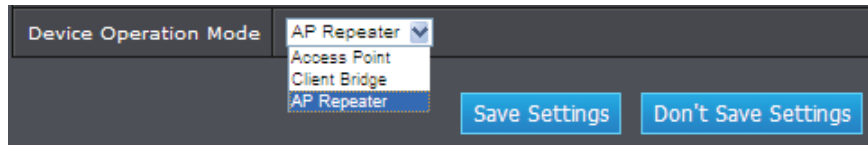
Wireless AP repeater mode allows the device to extend the range of an existing wireless network. The existing wireless signal can be broadcasted from your wireless router or other access point. In addition, other network enabled devices can connect to your network using the Ethernet LAN ports. The functionality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



Configuring the Device as AP Repeater

Main > Device Mode

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Main > Device Mode**.
- 3 On *Device Operation Mode*, select **AP Repeater**.



- 4 Click **Save Settings** to save changes.

Note: To discard the changes, click **Don't Save Settings**.

Using AP Repeater Mode

Wireless > Site Survey

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Wireless > Site Survey**.
- 3 The available networks are listed. Select a network to connect to.

SITE SURVEY RESULT						
SSID	BSSID	Channel	Type	Encryption	Signal	Select
dlink-08DE-5GHz	c0:a0:bb:6e:08:e0	48 (A+N+AC)	AP	WPA2-PSK (aes)	93	<input type="radio"/>
dlink-08DE	c0:a0:bb:6e:08:de	6 (B+G+N)	AP	WPA2-PSK (aes)	90	<input type="radio"/>
XXXXX	b8:a3:86:50:9b:80	11 (B+G+N)	AP	WPA2-PSK (aes)	28	<input type="radio"/>
HP-Print-71-Officejet 6700	38:ea:a7:4c:84:71	6 (B+G)	AP	None	21	<input type="radio"/>
Angel Note	e8:99:c4:b9:42:28	1 (B+G+N)	AP	WPA2-PSK (aes)	15	<input type="radio"/>

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

- 4 Click **Next** to connect to the selected wireless network.
- 5 If your wireless network requires wireless security, you will be prompted to enter your wireless key. Enter your Wireless Key required to connect to your existing wireless network and click **Next**.
- 6 In the **Wireless Network Name (SSID)** field, enter the wireless name for the extended network.

Please enter the settings for the extended network

Wireless Network Name (SSID)

Give your network a name, using up to 32 characters.

Use the same Network Name for the Extended Network

Note: To use the same name as the repeater network, check **Use the same Network Name for the Extended Network** checkbox.

- 7 Click **Save** to save the settings.

Setup Complete!

Repeater Network Name **LG..Zura**

Wi-Fi Password **azurah0124**

Extender Network Name **Home 1**

- 8 Wait for the device to apply the settings.

Advanced Settings

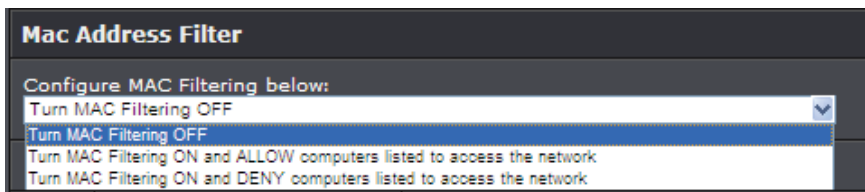
This section will guide you through configuring several advanced settings.

Configure MAC Filter Settings

Access > 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 the Management Page](#)” on page 10).
- 2 Click **Access > MAC Filter**.
- 3 On *Configure MAC Filtering below*, select one of the MAC filter function.



- **Turn MAC Filtering OFF:** Select this option to disable the MAC address filter.
- **Turn MAC Filtering ON and ALLOW computers listed to access the network:** 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.
- **Turn MAC Filtering ON and DENY computers listed to access the network:** 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 than to determine which MAC addresses you do not want to allow access.

- 4 Configure the following options:

	MAC Address	Schedule
<input checked="" type="checkbox"/>	00:00:00:00:00:00	Always <input type="button" value="Add New"/>
<input type="checkbox"/>	00:00:00:00:00:00	Always <input type="button" value="Add New"/>

- **MAC Address:** Check the box next to the entry to enable and in the *MAC Address* field, enter the MAC address of the devices you would like to filter. (i.e. 00:11:22:AA:BB:CC)
 - **Add New:** Click **Add New** to select the pre-defined schedule to apply. The filter will only be active during the time period defined in the pre-defined schedule. (Refer to “[Create Schedules](#)” on page 36).
- Note:* Before applying scheduling, please ensure your Time settings are configured correct and you have defined a schedule. Refer to [page 39](#) to configure the time settings and refer to [page 36](#) to create a schedule.

- 5 Click **Save Settings** to save changes.

Change the IP Address

Main > Network Settings

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

The default Access Point IP Address Settings: 192.168.10.100 / 255.255.255.0

- 1 Log into your access point management page (refer to "Log in to the Management Page" on page 10).
- 2 Click **Main > Network Settings**.
- 3 On *My LAN Connection is*, select the access point IP address settings.

LAN IPV4 CONNECTION TYPE	
Choose the IPv4 mode to be used by the Access Point.	
My LAN Connection is	<div style="border: 1px solid black; padding: 2px;"> Static IP <ul style="list-style-type: none"> Static IP Dynamic IP(DHCP) </div>

- **Dynamic IP (DHCP):** Choose the option to set the access point to automatically obtain IP address settings from a DHCP server.
- **Static IP:** Choose this option to manually configure the IP address settings of the access point.

Configure the following settings:

STATIC IP ADDRESS LAN CONNECTION TYPE	
Enter the IPv4 Address information.	
IP Address	192.168.10.100
Subnet Mask	255.255.255.0
Gateway Address	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0

- IP Address: Enter the new access point IP address. (i.e. 192.168.0.100)
- Subnet Mask: Enter the new access point subnet mask. (i.e. 255.255.255.0)

- Gateway Address: Enter the default gateway address of your network. This parameter is required for the access point to access Internet for functions such as e-mail notifications.
 - ↳ *Note: Typically, your network router IP address is used as the default gateway address to access the Internet (i.e. 192.168.10.1).*
- Primary DNS Server: Enter the primary DNS server address. This parameter is required for access point to resolve web addresses.
- Secondary DNS Server: Enter the secondary DNS server address. This parameter is required for access point to resolve web addresses.
 - ↳ *Note: Typically, your network IP address is used as the DNS server address.*

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

↳ *Note: You will need to access your access point management page using your new access point IP address. (i.e. Instead of using the default <http://192.168.10.100> your new access point IP address will use the following format using your new IP address [http://\(new.ipaddress.here\)](http://(new.ipaddress.here)) to access your access point management page. You can also use the default login URL <http://tew-814dap>.*

Configure IPv6 Settings

Main > IPv6

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 the Management Page” on page 10).
- 2 Click **Main > IPv6**.
- 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	<div style="border: 1px solid black; padding: 2px;"> Link-Local Only <ul style="list-style-type: none"> Link-Local Only Static IPv6 Autoconfiguration (SLAAC/DHCPv6) </div>
LAN IPv6 ADDRESS SETTINGS	

- **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	<input type="text"/>
Subnet Prefix Length	<input type="text" value="0"/>
Default Gateway	<input type="text"/>
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>

- **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.	
<input type="radio"/>	Obtain IPv6 DNS server address automatically
<input checked="" type="radio"/>	Use the following IPv6 DNS Servers
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>

- **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 **Save Settings** to save changes.

Configure the DHCP Server

Main > Network Settings

Your access point can be used as a DHCP (Dynamic Host Configuration Protocol) server to automatically assign an IP address to each computer or device on your network. The DHCP server is disabled by default on your access point. In most cases your network router has a built-in DHCP server that is typically enabled and used as your network DHCP server. If you already have a DHCP server on your network, leave this settings disabled.

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Main > Network Settings**.
- 3 Set the *My LAN Connection is* setting to **IP Static**.
- 4 On the **DHCP Server Setting** section, configure the following settings:

DHCP Server Settings	
Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.	
Enable DHCP Server	<input checked="" type="checkbox"/>
DHCP IP Address Range	192.168.10.10 to 192.168.10.20 (addresses within the LAN subnet)
Always Broadcast	<input type="checkbox"/>
Gateway	192.168.10.10
WINS	192.168.10.10
DNS	192.168.10.10
DHCP Lease Time	1 Hour

- **Enable DHCP Server:** Check the checkbox to enable the DHCP server.
- **DHCP IP Address Range:** Enter the starting IP address and ending IP address for the DHCP server range. (i.e.192.168.10.20 to 192.168.10.30)
 - ↳ *Note: The Start IP and End IP specify the range of IP addresses to automatically assign to computers or devices on your network.*
- **Always Broadcast:** Check the checkbox to enable the option. Enabling this option will cause the access point to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.

- **Gateway:** Enter the default gateway IP address to automatically assign to computers or devices on your network. (i.e. 192.168.10.1)
- **WINS:** Enter the WINS server IP address to automatically assign to computers or devices on your network.
- **DNS:** Enter the DNS server IP address to automatically assign to computer or devices on your network. (i.e. 192.168.10.1)
- **DHCP Lease Time:** Enter the DHCP lease time in minutes.

↳ *Note: The DHCP lease time is the amount of time a computer or device can keep an IP address assigned by the DHCP server. When the lease time expires, the computer or device will renew the IP address lease with the DHCP server, otherwise, if there is no attempt to renew the lease, the DHCP server will reallocate the IP address to be assigned to another computer or device.*

- 5 Click **Save Settings** to save changes.

Create Schedules

Tools > 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

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

Add Schedule Rule


Name	<input type="text"/>
Day(s)	<input checked="" type="radio"/> All Week <input type="radio"/> Select Day(s)
	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat
All Day - 24 hrs	<input type="checkbox"/>
Time format	24-hour ▾
Start Time	0 : 0 AM ▾ (hour:minute)
End Time	0 : 0 AM ▾ (hour:minute)
<input type="button" value="Add"/> <input type="button" value="Clear"/>	



- **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.
- **Time format:** Select the desired time format.

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

4 Click **Add** to create the schedule.

Edit a Schedule

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Tools > Schedule**.
- 3 On the **Schedule Rules List** section, click the  icon next to the schedule that you want to edit.

Schedule Rules List				
Name	Day(s)	Time Frame		
weekend	Sun Sat	All Day		

4 Adjust the necessary settings.

Add Schedule Rule

Name	<input type="text" value="weekend"/>
Day(s)	<input checked="" type="radio"/> All Week <input type="radio"/> Select Day(s)
	<input checked="" type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat
All Day - 24 hrs	<input type="checkbox"/>
Time format	24-hour ▾
Start Time	0 : 0 AM ▾ (hour:minute)
End Time	24 : 0 AM ▾ (hour:minute)
<input type="button" value="Update"/> <input type="button" value="Clear"/>	

5 Click **Update** 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.

Configure Email Settings

Tools > Email Settings

The email notification settings allow you to send the device log files via email for troubleshooting or monitoring purposes.

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Tools > Email Settings**.
- 3 Configure the following settings:

Enable	
Enable Email Notification	<input type="checkbox"/>
Email Settings	
From Email Address	<input type="text"/>
To Email Address	<input type="text"/>
Email Subject	<input type="text"/>
SMTP Server Address	<input type="text"/>
SMTP Server Port	<input type="text" value="0"/>
Enable Authentication	<input type="checkbox"/>
Account Name	<input type="text"/>
Password	<input type="password"/> <input type="checkbox"/> Display Characters
Verify Password	<input type="password"/> <input type="checkbox"/> Display Characters
<input type="button" value="Send Mail Now"/>	
Email Log When Full	
Email Log When Full	<input type="checkbox"/>

- **Enable Email Notification:** Check the option to enable email log notification.

- **From Email Address:** Enter the sender or source mail address. You can use this to easily identify the notification in your email inbox. (i.e. access point@trendnet.com)
 - ↳ *Note: This does not need to be real e-mail address, only used for identification purposes when checking your e-mail.*
 - **To Email Address:** Enter your e-mail address.
 - **Email Subject:** Enter the subject for your email.
 - **SMTP Server Address:** Enter the IP address (i.e. 10.10.10.10) or domain name (i.e. mail.trendnet.com) of your e-mail server.
 - **SMTP Server Port:** Enter the SMTP Port used by your e-mail server. (i.e. Default SMTP Server Port: 25)
 - **Enable Authentication:** Check this option if your e-mail server requires authentication. If enabled, enter the account name and password in the *Account Name* and *Password* fields.
 - ↳ *Note: If you are unsure of this setting, check with your e-mail service provider if authentication is required.*
 - **Account Name:** Enter the account name required for authentication by your SMTP mail server.
 - **Password:** Enter the password required for authentication by your SMTP mail server. Enter the password again in the *Verify Password* field.
 - **Send Mail Now:** Click this option to send an e-mail with the current access point log using your email settings.
 - **Email Logs When Full:** Check this option to configure the device to send log file email notifications when the internal device logging is full.
- 4 Click **Save Settings** to save the settings.

Enable Ping Test

Tools > Ping Test

The ping test enables you to determine whether an IP address or host is present on the Internet or not.

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Tools > Ping Test**.
- 3 In the *Host Name or IP address* or *Host Name or IPv6 address* field, enter the host name or IP address in the respective text box.

Ping Test	
Host Name or IP address	<input type="text"/> <input type="button" value="Ping"/>
IPv6 Ping Test	
Host Name or IPv6 address	<input type="text"/> <input type="button" value="Ping"/>

- 4 Click **Ping**.

*Note: The ping test result will be displayed on the **Ping Result** option.*

Ping Result
Success.

Maintenance

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

Main > Password

For security purposes, it is recommended to change the login password periodically.

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Main > Password**.
- 3 On the **Password** section, enter the new password in the *New Password* field.

Password	
New Password	<input type="text"/>
Verify Password	<input type="text"/>
<input type="checkbox"/> Display Characters	
<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>	

- 4 Enter the password again in the *Verify Password* field to confirm.
- 5 Click **Save Settings** to save the settings.

Change the Device Name

Main > Password

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-814dap>).

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Main > Password**.
- 3 On the **Device Name** section, enter the new device name to display on your network to identify the access point in the *Device Name* field.

Device Name	
Device Name allows you to configure this device more easily. You can enter " http://device name " into your web browser instead of IP address for configuration.	
Device Name	<input type="text" value="tew-814dap"/>

- 4 Click **Save Settings** to save the settings.

Set the Date and Time

Main > Time

Before you use the scheduling feature on your access point, ensure that your system time is configured correctly.

Note: The current device time and date information is displayed on the **Time** section.

Time	
Time	01/01/2014 07:44:11

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Main > Time**.
- 3 Configure the following settings:
 - **Enable NTP server:** Select this option to enable NTP server configuration.

Automatic Time Configuration																
Enable NTP server	<input checked="" type="checkbox"/>															
NTP Server	<input type="text"/> <input type="button" value="Update Now"/>															
Time Zone	(GMT-08:00) Pacific Time (US/Canada), Tijuana															
Enable Daylight Saving	<input checked="" type="checkbox"/>															
Daylight Saving Offset	+1:00															
Daylight Saving Dates	<table border="1"> <thead> <tr> <th></th> <th>Month</th> <th>Week</th> <th>Day of Week</th> <th>Time</th> </tr> </thead> <tbody> <tr> <td>DST Start</td> <td>Mar</td> <td>3rd</td> <td>Sun</td> <td>2 am</td> </tr> <tr> <td>DST End</td> <td>Nov</td> <td>2nd</td> <td>Sun</td> <td>2 am</td> </tr> </tbody> </table>		Month	Week	Day of Week	Time	DST Start	Mar	3rd	Sun	2 am	DST End	Nov	2nd	Sun	2 am
		Month	Week	Day of Week	Time											
DST Start	Mar	3rd	Sun	2 am												
DST End	Nov	2nd	Sun	2 am												

- **NTP server:** Specify an NTP server (i.e. *pool.ntp.org*) and click **Update Now** to sync the system's time with the NTP server.
- **Time Zone:** Select your time zone.
- **Enable Daylight Saving:** Select this option to enable the Daylight savings time.
- **Daylight Saving Offset:** Specify the daylight saving offset.
- **Daylight Saving Dates:** Specify a *DST Start* and *DST End* date and time when using the daylight savings time.

- **Date and Time:** Select this option if you would like to specify the time manually. You must specify the Year, Month, Day, Hour, Minute, and Second. Alternatively, click the **Copy Your Computer's Time Settings** to use the system time from the computer being used to access the Management page.

Set the Date and Time Manually						
Date and Time	Year	2014	Month	Jun	Day	20
	Hour	16	minute	30	second	27
<input type="button" value="Copy Your Computer's Time Settings"/>						

4 Click **Save Settings** to save the settings.

Backup System Settings

Tools > Settings Management

This option allows you to backup your access point configuration.

- 1 Log into your access point management page (refer to "Log in to the Management Page" on page 10).
- 2 Click **Tools > Settings Management**.
- 3 On the **Save Configuration Settings** section, click **Save** to save the current configuration to your computer.

Save Configuration Settings	
Save Settings	<input type="button" value="Save"/>

Note: Depending on your web browser settings, you may be prompted to open or save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: config.dat)

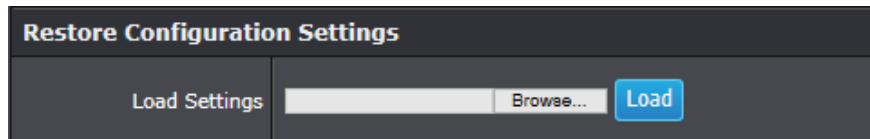


Load System Settings

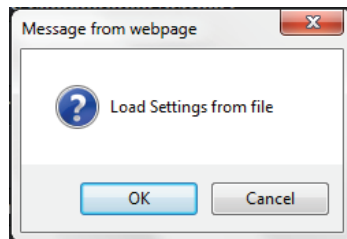
Tools > Settings Management

This option allows you to restore your access point configuration.

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Tools > Settings Management**.
- 3 On the **Restore Configuration Settings** section, click **Browse**.



- 4 Select the access point configuration file to restore and click **Load**.
- 5 A confirmation message appears on the screen. Click **OK** to restore the settings.



Reset to Factory Defaults

Tools > Settings Management

You may want to reset your access point to the factory default settings if you are encountering difficulties with your access point. Before you reset your access point to defaults, if possible, you should backup your access point configuration first, refer to “Backup System Settings” on page 40.

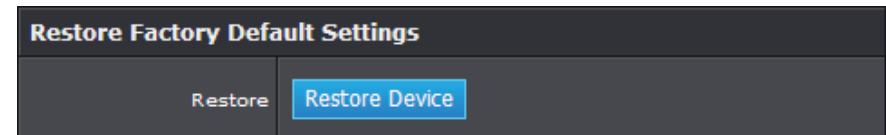
There are two methods that can be used to reset your access point to the factory default settings.

- Use the **Reset** button (refer to “Rear View” on page 5). Use this method if you are encountering difficulties with accessing your access point management page.

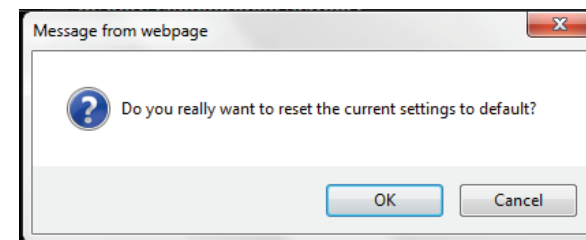
OR

- Via the Management Page

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Tools > Settings Management**.
- 3 On the **Restore Factory Default Settings** section, click **Restore Device**.



- 4 A confirmation message appears on the screen. Click **OK** to reset the current parameters to the factory default settings.



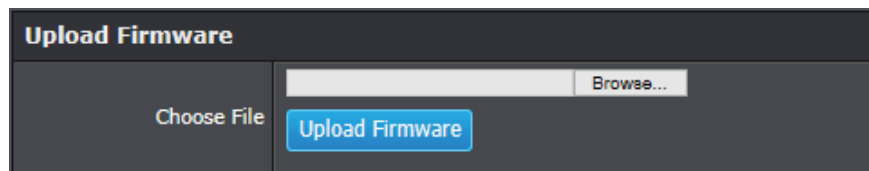
Update System Firmware

Tools > Upload Firmware

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

In addition, it is also important to verify if the latest firmware version is newer than the one your access point is currently running. To identify the firmware that is currently loaded on your access point, log in to the access point management page, then click on the Status > Device Info section (refer to “View the Device Information” on page 43). If there is a newer version available, also review the release notes to check if there were any new features you may want or if any problems were fixed that you may have been experiencing.

- 1 Download the latest firmware from TRENDnet web site and save it your computer.
- 2 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 3 Click **Tools > Upload Firmware**.
- 4 On the **Restore Configuration Settings** section, click **Browse** and select the firmware file (*.bin).



- 5 Click **Upload Firmware** to update the firmware to the latest version.

Note:

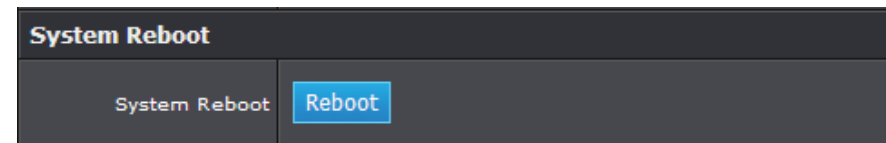
- Do not interrupt the firmware upgrade process. Do not turn off the device or press the Reset button during the upgrade process.
- Disable sleep mode on your computer as this may interrupt the firmware upgrade process.
- If you are upgrade the firmware using a notebook, ensure that the notebook is connected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

System Reboot

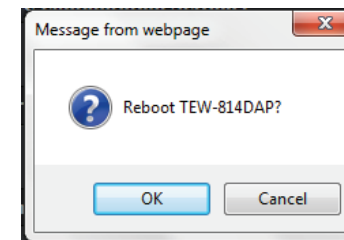
Tools > Settings Management

You may want to restart your access point if the system is not performing correctly.

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Tools > Settings Management**.
- 3 On the **System Reboot** section, click **Reboot**.



- 4 A confirmation message appears on the screen. Click **OK** to reboot the system.



Configure Syslog Server

Tools > Syslog

This option allows you to archive your log files to a Syslog Server.

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

System Logs	
Enable Logging To Syslog Server:	<input type="checkbox"/>
Syslog Server IP Address:	<input type="text"/>
<input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>	

- **Enable Logging To Syslog Server:** Select this option if you have a syslog server currently running on the LAN and want to send messages to it
 - **Syslog Server IP Address:** Enter the LAN IP address of the Syslog Server.
- 4 Click **Save Settings** to save the settings.

View System Information

View the Device Information

Status > Device Info

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

- 1 Log into your access point management page (refer to “Log in to the Management Page” on page 10).
- 2 Click **Status > Device Info**.

Device Information	
Firmware Version	1.01 , Wed, 04, Jun, 2014
Time	1/1/2014 2:47:25
LAN Information	
Device Mode	Access Point
MAC Address	D8:FE:E3:3E:AC:DC
Connection	Dynamic IP
IP Address	169.254.147.184
Subnet Mask	255.255.255.0
Gateway Address	0.0.0.0
WLAN 2.4GHz Information	
MAC Address	D8:FE:E3:3E:AC:DD
SSID	TRENDnet814_2.4GHz_BISF
Security Mode	WPA2 Mixed
Channel Width	Auto 20/40MHz
Channel	1

- On the **Device Information** section: Display the current firmware version and released date code.
- On the **LAN Information** section: Display the wired Ethernet Interface information such as the device mode, interface MAC address, IP address connection type, IP address settings including default gateway and Subnet Mask settings.

- On the **WLAN 2.4GHz/5GHz Information** section: Display the Access Point's wireless connection information, including the access point's wireless interface MAC address, the connection status, the SSID status, which channel is being used, and whether security is enabled or not.

View the Data Traffic Statistics

Status > Statistics

View information about the data traffic statistics on the amount of packets received and transmitted over the LAN, and wireless interface.

- Log into your access point management page (refer to "Log in to the Management Page" on page 10).
- Click **Status > Statistics**.

LAN STATISTICS			
Sent	24469	Received	11191
TX Packets Dropped	0	RX Packets Dropped	0
Collisions	0	Errors	0

2.4GHz WIRELESS STATISTICS			
Sent	3666	Received	10408
TX Packets Dropped	0	RX Packets Dropped	0
Collisions	0	Errors	0

5GHz WIRELESS STATISTICS			
Sent	122	Received	46540
TX Packets Dropped	0	RX Packets Dropped	0
Collisions	0	Errors	0

View the Connected Wireless Clients

Status > Wireless Client

View information about the devices connected to the wireless Access Point.

- Log into your access point management page (refer to "Log in to the Management Page" on page 10).
- Click **Status > Wireless Client**.

Number of Wireless Clients - 2.4GHz Band:	
Connected Time	MAC Address
---	None

Wireless Lan	
Connected Time	MAC Address
---	None

View the Wireless Connection Information

Status > IPv6

View information about all of your WAN and LAN connection details.

- Log into your access point management page (refer to "Log in to the Management Page" on page 10).
- Click **Status > IPv6**.

All of your IPv6 Internet and network connection details are displayed on this page.

IPv6 Connection Type	Link-Local Only
LAN IPv6 Address	None
IPv6 Default Gateway	None
LAN IPv6 Link-Local Address	fe80::dafe:e3ff:fe3e:acdc/64
Primary DNS Address	None
Secondary DNS Address	None

View Events Log

Status > Logs

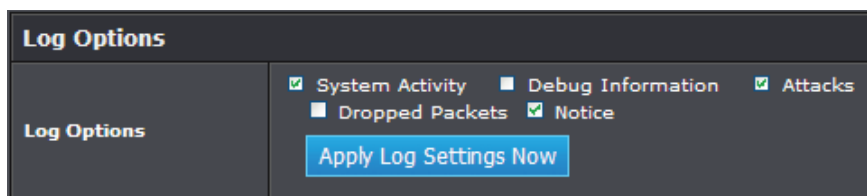
This device keeps a running log of events and activities occurring on the system.

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

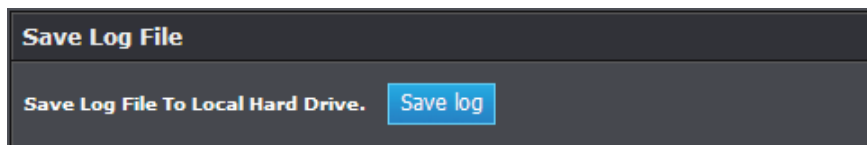
2 Click **Status > Logs**.

3 Do the following:

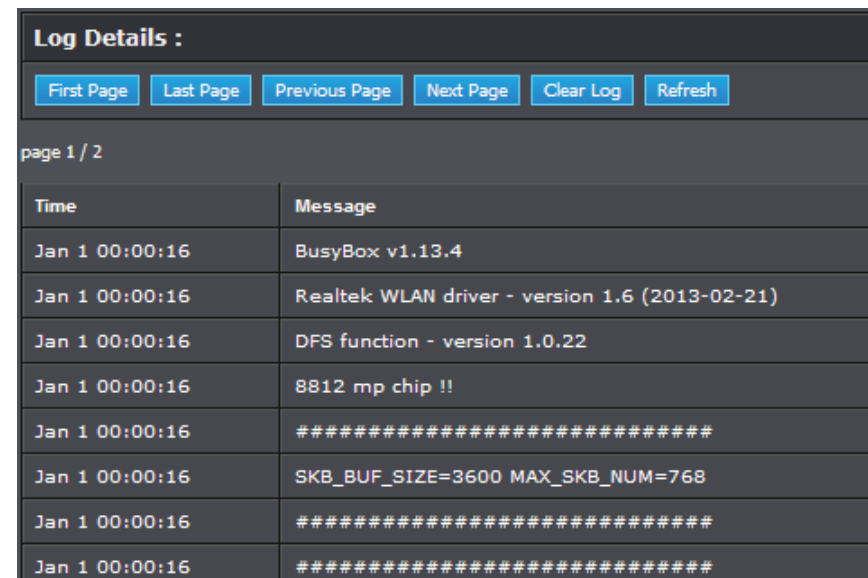
- On the **Log Option** section: Select the types of logs that can be viewed. Click **Apply Log Settings Now** to save the settings.



- On the **Save Log File** section: Click **Save log** to save the current log to your hard drive.



- On the **Log Details** section: View the log entries.
 - First Page: Click this button to view the first page of the log.
 - Last Page: Click this button to view the final page of the log.
 - Previous Page: Click this button to view the page just before the current page.
 - Next Page: Click this button to view the page just after the current page.
 - Clear Log: Click this button to delete the contents of the log and begin a new log.
 - Refresh: Click this button to refresh the screen to show the latest log entries.



Appendix

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.

Operations in the 5.15-5.25GHz band are restricted to indoor usage 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 50385 : 2002

Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

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.

 Český [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.
 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.
 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.
 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.
 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.
 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.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑΤRENDnet ΔΗΛΩΝΕΙ ΟΤΙ ΤΕW-814DAP ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK, 2006/95/EK, 2009/125/EK και.
 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.
 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.
 Latviski [Latvian]	AršoTRENDnetdeklarē, ka TEW-814DAP atbilstDirektīvas 1999/5/EK, 2006/95/EK, un 2009/125/EK būtiskajāmprasībām un citiemar to saistītajiemnoteikumiem.

 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.
 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.
 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.
 Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-814DAP megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv, a 2006/95/EK és a 2009/125/EK irányelv egyéb előírásainak.
 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.
 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.
 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.
 Slovenský [Slovak]	TRENDnettýmto vyhlasuje, že TEW-814DAP spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES, 2006/95/ES, a 2009/125/ES.
 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.
 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.

Specifications

Item	Specifications
Standards	<ul style="list-style-type: none"> IEEE 802.11b/g/n (Wireless LAN 2.4GHz) IEEE 802.11a/n/ac (Wireless LAN 5GHz) IEEE 802.3 u/z Auto negotiation
Radio Technology	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 866Mbps: Typical TBD @ 10% PER 300Mbps: Typical TBD @ 10% PER 54Mbps: Typical TBD @ 10% PER 11Mbps: Typical TBD @ 8% PER
Frequency	<ul style="list-style-type: none"> 2.4 GHz: 2.412 – 2.462 (FCC), 2.412 – 2.472 GHz (ETSI) 5 GHz: 5.180 – 5.240 + 5.745 – 5.825 (FCC), 5.180 – 5.725 GHz (ETSI)
Wireless Channel	<ul style="list-style-type: none"> 2.4 GHz: 1 - 11 (FCC), 1 - 13 (ETSI) 5 GHz: 36, 40, 44, 48, 149, 159, 157, 161, 165 (FCC), 36, 40, 44, 48 (ETSI)
Modulation	<ul style="list-style-type: none"> 802.11a/n: BPSK, QPSK, 16-QAM, 64-QAM sub carrier with OFDM 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256QAM with OFDM
Media Access Protocol	CSMA/CA with ACK

Item	Specifications
Wireless Output Power/ Receiving Sensitivity (per chain)	<ul style="list-style-type: none"> 802.11b: FCC: 24 dBm, CE: 17 dBm (max.)/ -84 dBm (typical) @ 11 Mbps 802.11g: FCC: 22 dBm, CE: 17 dBm (max.)/ -70 dBm (typical) @ 54 Mbps 802.11a: FCC: 20 dBm, CE: 22 dBm (max.)/ -73 dBm (typical) @ 54 Mbps 802.11n: FCC: 22 dBm, CE: 17 dBm (max.)/ -66 dBm (typical) @ 300 Mbps 2.4GHz 802.11n: FCC: 20 dBm, CE: 22 dBm (max.)/ -66 dBm (typical) @ 300 Mbps 5GHz 802.11ac: FCC: 20 dBm, CE: 22 dBm (max.)/ -56 dBm (typical) @ 867 Mbps
Antenna Type	Internal pcb antenna
Antenna Gain	<ul style="list-style-type: none"> 2.4 GHz: 2 dBi (max.) / 0 dBi (Avg.) internal 5 GHz: 2 dBi (max.) / 0 dBi (Avg.) internal
Protocol	TCP/IP
Operation Modes	<ul style="list-style-type: none"> Access Point (AP), Repeater AP+WDS Client
SSID	Up to 4 SSIDs per band (AP mode)
Hardware Interface	<ul style="list-style-type: none"> WAN: 1 x 10/100/1000Mbps Auto-MDIX Gigabit Ethernet port LED indicators WPS button On/Off power switch Power Jack
Supported Network Protocols	<ul style="list-style-type: none"> TCP/IP NAT PPPoE/PPTP/L2TP HTTP
DHCP Server/Client Network Management	Web base configuration utility via Ethernet
Access Control	Wireless encryption: <ul style="list-style-type: none"> WEP WPA/WPA2-PSK WPA/WPA2-RADIUS (AP mode) Access Control: <ul style="list-style-type: none"> MAC Filter

Item	Specifications
Range Coverage	<ul style="list-style-type: none"> Indoor: Up to 100 meters (depends on environment) Outdoor: Up to 300 meters (depends on environment)
Diagnostic LEDs	<ul style="list-style-type: none"> Power Internet (WAN port) 2.4G Wireless 5G Wireless WPS
Power Adapter	12VDC / 1A external power adapter
Power Consumption	<ul style="list-style-type: none"> Input: 100 - 200V AC, 50 - 60 Hz, 0.5A Output: 12V DC, 1A external power adapter Consumption: 8.8 Watts (maximum)
Operation Temperature	0 - 40°C (32 - 104°F)
Storage Temperature	-10 ~ 70°C
Operating Humidity	Maximum 95% no condensation
Certifications	<ul style="list-style-type: none"> FCC certificate for USA CE certificate for Europe
Dimensions (W x H x D)	180 x 155 x 48 mm (7.1 x 6.1 x 1.9 in.)
Weight	340g (12 oz.)
Warranty	3 years limited warranty

**For maximum performance up to 867 Mbps, use with a 867 Mbps 802.11ac wireless client. Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions.*

TRENDnet[®]

Product Warranty Registration

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

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA

Copyright ©2014. All Rights Reserved. TRENDnet.