

User's Guide



# N150 Wireless Outdoor PoE Access Point

TEW-715APO

## Contents

<b>Product Overview .....</b>	<b>3</b>
Package Contents .....	3
Features .....	3
<b>Product Hardware Features.....</b>	<b>4</b>
Application Diagram .....	5
Creating a Network.....	6
Wireless Performance Considerations .....	6
<b>Getting Started .....</b>	<b>7</b>
Connect wireless devices to your access point.....	8
Steps to improve wireless connectivity .....	8
<b>Configuration .....</b>	<b>9</b>
Access the management page .....	9
<b>System Modes .....</b>	<b>10</b>
<b>Bridge Mode .....</b>	<b>10</b>
AP Mode .....	11
Wireless Client Mode.....	13
Bridge Mode .....	16
AP Repeater Mode.....	18
<b>Router Mode.....</b>	<b>20</b>
AP Mode .....	21
Wireless Client Mode.....	23
Bridge Mode .....	26
AP Repeater Mode.....	28
<b>Wireless Networking and Security .....</b>	<b>30</b>

How to choose the type of security for your wireless network .....	30
Secure your wireless network .....	31
Wireless access control .....	33
<b>Advance Settings .....</b>	<b>33</b>
Change your IP address .....	33
Configure your Internet connection .....	34
Setting time .....	35
Advance wireless settings.....	35
Change your login password .....	36
<b>Access Control .....</b>	<b>37</b>
Source IP Filtering.....	37
Destination IP Filtering .....	37
Source Port Filtering .....	37
Destination Port Filtering .....	38
Port Forwarding.....	38
Open a device on your network to the Internet.....	39
DMZ.....	39
UDP Pass through .....	39
Configure your log .....	39
View your log.....	39
Ping Watchdog .....	40
Ping Watchdog .....	40
WDS Data Rate Test.....	40
Antenna Alignment.....	41
Speed Test .....	41
Remote Mangement .....	41
Coovachili .....	43

Upgrade Firmwre.....	43
Backup and restore your router configuration settings .....	44
Reset to factory defaults .....	45
Certificate configuration settings .....	45
Device Information .....	45
Associated Information .....	46
Statistics.....	47
ARP Table.....	47
Bridge Table.....	47
DHCP Clients .....	48
Network Activity .....	48
<b>Additional hardware installation .....</b>	<b>48</b>
Ground wire.....	48
Using the optional external antenna .....	49
Pole mounting .....	49
<b>Access Point Management Page Structure .....</b>	<b>50</b>
<b>Technical Specifications.....</b>	<b>51</b>
<b>Troubleshooting.....</b>	<b>52</b>
<b>Appendix .....</b>	<b>53</b>
Internet service types .....	55

## Product Overview



## Package Contents

In addition to the access point, the package includes:

- TEW-715APO
- CD-ROM (User's Guide)
- Multi-Language Quick Installation Guide
- Mounting hardware
- Power Adapter (12V, 1A)
- PoE Injector
- Grounding Wire

If any package contents are missing or damaged, please contact the retail store, online retailer, or reseller/distributor from which the product was purchased.

## Features

TRENDnet's N150 Wireless Outdoor PoE Access Point, model TEW-715APO, provides high speed building-to-building networking with its built in dual polarization directional 8dBi antenna for distances up to 6 miles (10 km)\*. Install an omni-directional antenna (with a N-Type connector), such as TRENDnet's TEW-AO080 to provide blanket outdoor wireless coverage over a large area. A range of applications are facilitated with Access Point, Wireless Client, WDS, Bridge, CPE, and Repeater mode support.

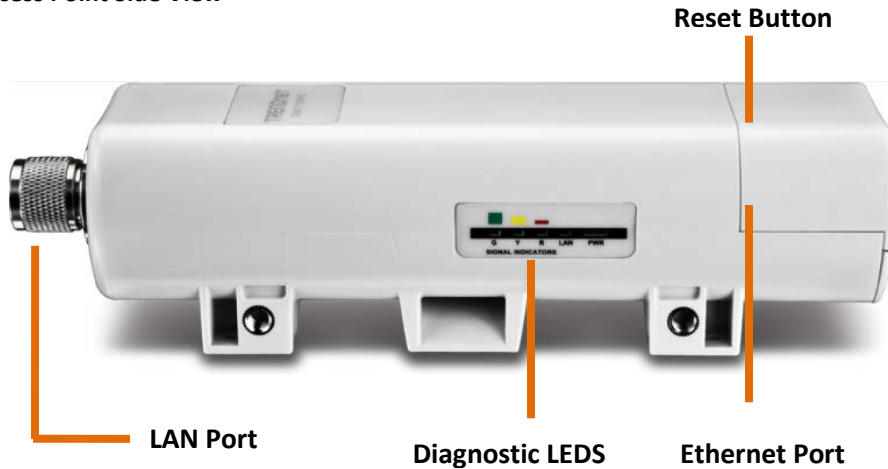
A durable IP-55 rated outdoor enclosure protects the device from inclement weather. Power for this unit is supplied by an included PoE injector, resulting in equipment and installation cost savings. Additional features include SNMP (v2c, v3), Spanning Tree, real time network activity tables, WPA/WPA2 encryption, MAC address filters, 16 virtual AP profiles, 802.1Q, 802.1X, mounting hardware, and GPS coordinate support.

- 1 x 10/100Mbps Auto-MDIX LAN port
- 1 x reset button
- 1 x Reverse N-type connector for optional antenna configuration
- LED indicators: Power, WLAN, LAN
- Internal high powered 8Bi patch antenna directional antenna
- Rugged IP55 rated weather proof housing
- PoE compliant device
- High speed data rates of up to 150Mbps based on IEEE 802.11n technology
- Compliant with IEEE 802.11b/g standards
- Supports Access Point (AP), Wireless Distribution System (WDS)/Bridge, Customer Premises Equipment (CPE), and AP + Repeater modes
- Multiple SSID or Virtual Access Points with Layer 2 VLAN wireless client isolation
- Access restriction with MAC filtering
- Universal Plug and Play (UPnP) for auto discovery and support for device configuration of Internet applications
- Complete wireless security with WPA/WPA2-RADIUS, WPA /WPA2-PSK, and WEP
- Wi-Fi Multimedia (WMM) Quality of Service (QoS) data prioritization
- Easy setup via Web browser using the latest versions of Internet Explorer, FireFox, and Safari
- Supports SNMP (v2c and v3), Telnet, SSH, and HTTP/HTTPS management
- Surface mounting hardware
- Electrical ground cable
- 3-year limited warranty

\*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.

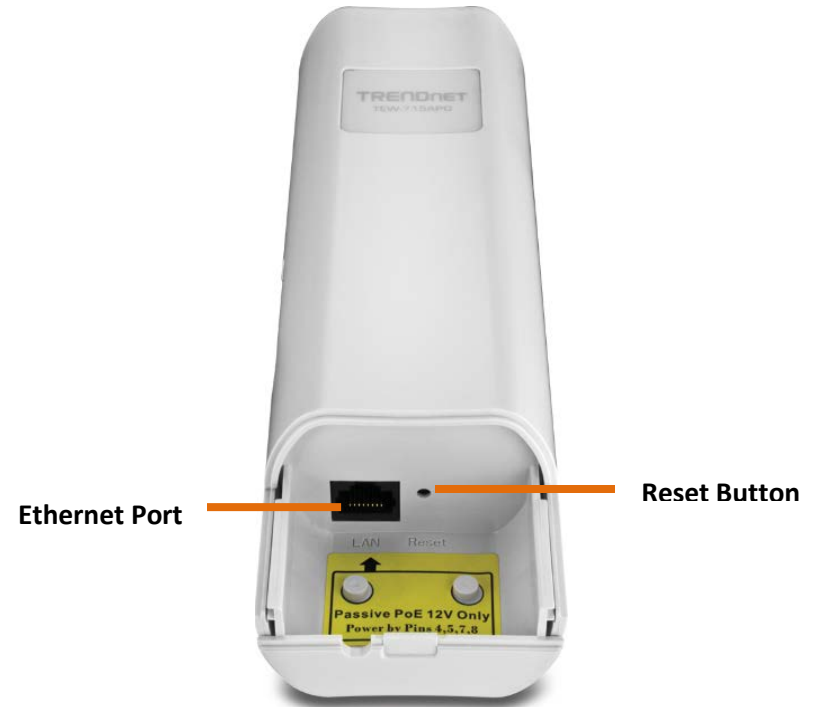
## Product Hardware Features

### Access Point Side View



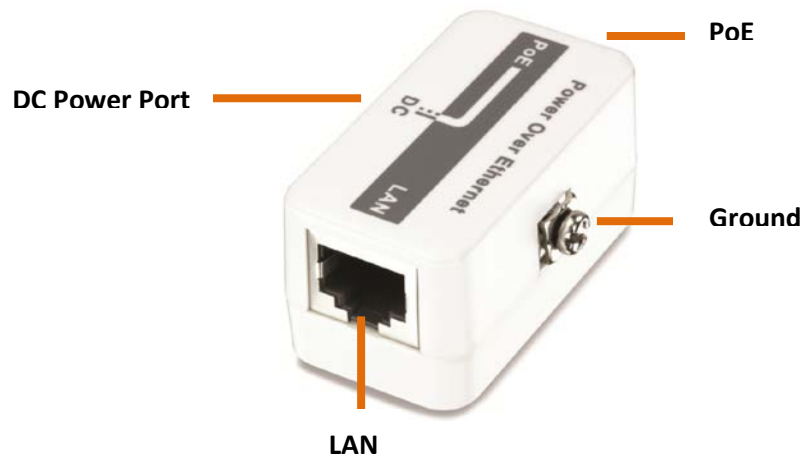
- **External Antenna (optional):** N-Type connector for the option to connect an external antenna and not use the built in antenna.
- **Diagnostic LEDs:** Provides device status.
  - **Wireless Signal: Blinks green during wireless network activity.**
    - **Green (Good), Yellow (Moderate), Red (Poor)**
  - **LAN: Blinks green during network activity**
  - **Power: Solid green when the device has power**
- **Ethernet port:** 1x 10/100Mbps Auto-MDIX port. Connect the side marked "PoE" of PoE adapter to this port. Depending on the mode settings applied, the Ethernet port can function as the network WAN port or LAN port. *Note: To access the Ethernet port, remove the bottom cap.*
- **Reset button:** Press and hold the reset button for 15seconds to reset the unit back the factory default settings. *Note: To access the reset button, remove the bottom cap*

### Access Point Front View with Bottom Cap Removed



- **Ethernet port:** 1x 10/100Mbps Auto-MDIX port. Connect the side marked "PoE" of PoE adapter to this port. Depending on the mode settings applied, the Ethernet port can function as the network WAN port or LAN port
- **Reset button:** Press and hold the reset button for 15seconds to reset the unit back the factory default settings.

## PoE Adapter View



- **PoE:** Provides power to the access point. Connect this side to the access point Ethernet port.
- **DC Power port:** Powers up the PoE adapter.
- **LAN:** Provides network connectivity to the access point and your network. Connect this side to your router or network.
- **Ground:** Provides extra grounding connection to protect the access point.

Application Diagram

The access point is mounted a pole which is connected to the provided PoE adapter and then connected to your network switch or router. Wireless signals from the access point are broadcasted to each creating a Bridge/WDS connection, thereby providing network connection between both networks.

## Creating a Network

What is a network?

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

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

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

### **How to set up a home network**

1. For a network that includes Internet access, you'll need:
  - Computers/devices with an Ethernet port (also called network port) or wireless networking capabilities.
  - A modem and Internet service to your home, provided by your ISP (modem typically supplied by your ISP).
  - A router to connect multiple devices to the Internet.
2. Make sure that your modem is working properly. Your modem is often provided by your Internet Service Provider (ISP) when you sign up for Internet service. If your modem is not working contact your ISP to verify functionality.
3. Set up your router. See "How to setup your router" below.
4. To connect additional wired computers or wired network devices to your network, see "Connect additional wired devices to your network" on page 11.
5. To set up wireless networking on your router, see "Wireless Networking and Security" on page 12.

## Wireless Performance Considerations

There are a number of factors that can impact the range of wireless devices.

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.

## Getting Started

For a typical wireless setup at home or office when using the access point in AP mode, please do the following:

### Hardware Installation

1. Remove the bottom cap.



2. Plug a Network cable to the Ethernet port.



3. Slide the bottom cover back to the unit.



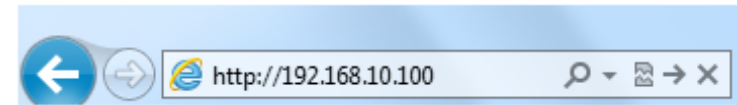
4. Plug an Ethernet cable to the access point and plug the other end of the cable to the side of the PoE adapter marked **PoE**.
5. Take another Ethernet cable and plug it on the side of the PoE adapter marked **LAN**, plug the other end of the cable to your network.



6. Verify that the following LED indicators on the access point: Power (Solid Green), LAN (Solid/Blinking Green) and WLAN (Blinking Green).



7. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to <http://192.168.10.100>. The access point will prompt you for a password.



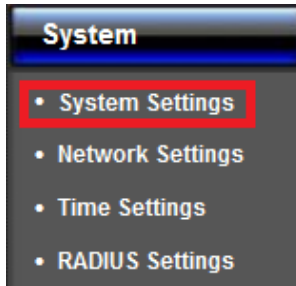
8. Enter the default user name and password and then click **Login**.

Default System Password: **admin**

LOGIN PASSWORD	
User Name:	<input type="text" value="admin"/>
Password:	<input type="password"/>
<input type="button" value="Login"/> <input type="button" value="Reset"/>	



9. Click the System button on the left side and then System Settings.

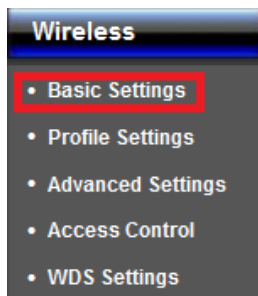


10. Select **Bridge** in the Mode drop down menu.

Device Settings	
Device Name:	TEW-715APO (max. 15 characters and no spaces)
Network Mode:	Bridge

11. Click **Apply** button to save your setting.

12. Once the configuration is saved. Click the Wireless button on the left side and then Basic Settings.



13. Select AP in the Operation Mode pull down menu.

14. Enter your desired network name (SSID) of your wireless network in the Wireless Network Name and click **Apply** to save settings.

Operation Mode:	AP	Site Survey
Wireless Network Name(SSID):	TRENDnet715	(more...)

## Connect wireless devices to your access point

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

- Wireless Laptop computers
- Network media players
- Wireless IP cameras
- Smart Phones
- Gaming Consoles
- Internet enabled TVs

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

See the "Appendix" on [page 53](#) for general information on connecting to a wireless network.

## Steps to improve wireless connectivity

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

1. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
  - a. For the widest coverage area, install your router near the center of your home, and near the ceiling, if possible.
  - b. Avoid placing the router on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), and masonry walls.

- c. Any obstruction can weaken the wireless signal (even non-metallic objects), so the fewer obstructions between the router and the wireless device, the better.
  - d. Place the router in a location away from other electronics, motors, and fluorescent lighting.
  - e. Many environmental variables can affect the router's performance, so if your wireless signal is weak, place the router in several locations and test the signal strength to determine the ideal position.
2. Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.
  3. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.
  4. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.

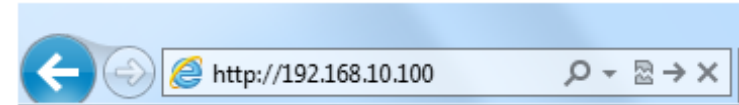
If possible, upgrade wireless network interfaces (such as wireless cards in computers) from older wireless standards to 802.11n. If a wirelessly networked device uses an older standard, the performance of the entire wireless network may be slower. If you are still experiencing low or no signal consider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

## Configuration

### Access the management page

**Note:** The access point's default management page <http://192.168.10.100> is accessed through the use of your Internet web browser (e.g. Internet Explorer, Firefox, Chrome, Safari, Opera) and will be referenced frequently in this User's Guide.

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to <http://192.168.10.100>. The access point will prompt you for a password.



2. Enter the default user name and password and then click **Login**.

Default System Password: **admin**

LOGIN PASSWORD	
User Name:	<input type="text" value="admin"/>
Password:	<input type="password"/>
<input type="button" value="Login"/> <input type="button" value="Reset"/>	

## System Modes

The TEW-715APO access point supports two different types of system modes. Please verify carefully on which mode you would like the device to operate in to proper installation.

- **Bridge Mode:** The device operates as an access point with no WAN/Internet configuration. Below list the supported wireless modes when bridge is selected as the device system mode.
  - **AP Mode:** Creates a wireless network to your existing network. Device Ethernet port serves as a LAN (Local Area Network) port of the device
  - **Wireless Client:** Connects to any existing wireless network (similar to a wireless adapter). Device Ethernet port serves as a LAN (Local Area Network) port of the device
  - **Bridge:** Creates a wireless bridge connection with another access point. Ethernet port serves as a LAN (Local Area Network) port of the device
  - **AP Repeater:** Repeats the wireless signal of an existing wireless network. Device Ethernet port serves as a LAN (Local Area Network) port of the device
- **Router Mode:** The device operates similar to a wireless router with WAN/Internet configuration. Below list the supported wireless modes when bridge is selected as the device system mode.
  - **AP Mode:** Creates a wireless network with your device (similar to a wireless router). Device Ethernet port serves as a WAN (Wide Area Network) or Internet port.
  - **Wireless Client:** Connects to any existing wireless network (similar to a wireless adapter) in which the wireless network the device is connecting to serves as your Internet connection. Ethernet port serves as a LAN (Local Area Network) port of the device and the wireless settings is based on your ISP (Internet Service Provider) connection.
  - **Bridge:** Creates a wireless network with your device (similar to a wireless router). Device Ethernet port serves as a WAN (Wide Area Network) or Internet port.
  - **AP Repeater:** Creates a wireless network with your device (similar to a wireless router). Device Ethernet port serves as a WAN (Wide Area Network) or Internet port.

## Bridge Mode

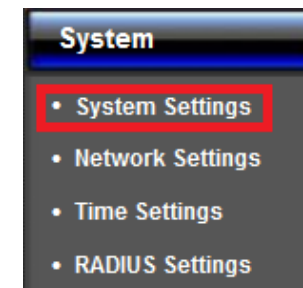
Below describes the configuration settings when the TEW-715APO System Mode is set to **Bridge**. In this setting the Ethernet port of the TEW-715APO serves as a LAN (Local Area Network) connection.

### Configuration

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Your access point will prompt you for a user name and password.



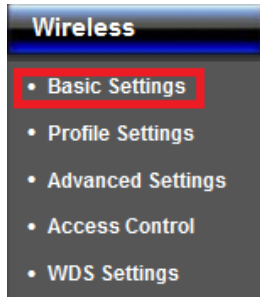
3. Enter the default user name and password and then click Login.  
 Default User Name: **admin**  
 Default Password: **admin**
4. Click the System button on the left side and then System Settings.



5. Select **Bridge** in the Mode drop down menu.
6. Click Apply button to save your setting.

Device Settings	
Device Name:	TEW-715APO (max. 15 characters and no spaces)
Network Mode:	Bridge

7. Click the Wireless button on the left side and then Basic Settings.



8. Select the mode you would like to apply Operation Mode pull down menu.

- **AP Mode:** Creates a wireless network to your existing network. Device Ethernet port serves as a LAN (Local Area Network) port of the device
- **Wireless Client:** Connects to any existing wireless network (similar to a wireless adapter). Device Ethernet port serves as a LAN (Local Area Network) port of the device
- **Bridge:** Creates a wireless bridge connection with another access point. Ethernet port serves as a LAN (Local Area Network) port of the device
- **AP Repeater:** Repeats the wireless signal of an existing wireless network. Device Ethernet port serves as a LAN (Local Area Network) port of the device

## AP Mode

Wireless > Basic



This section outlines available management options when the device System Setting is set to **Bridge** and the wireless Operation Mode is set to **AP**. Click **Apply** to save any changes.

Disable Wireless LAN Interface	
Operation Mode:	AP <input type="button" value="Site Survey"/>
Wireless Network Name(SSID):	715715TRENDnet <input type="button" value="(more...)"/>
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
802.11 Mode:	802.11B/G/N
HT protect:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Frequency/Channel:	2437MHz (6)
Extension Channel:	Lower Channel 2417MHz (2)
40MHz Center Frequency:	2427MHz (4)
Channel Mode:	40 MHz
Antenna:	<input checked="" type="radio"/> Internal (8 dBi) <input type="radio"/> External (N-Type)
Maximum Output Power (per chain):	12 <input type="range" value="26"/> 26 dBm
Data Rate:	Auto
Extension Channel Protection:	None

- **Disable Wireless LAN Interface:**

- **Check/Off:** turns off wireless networking on your router.
- **Unchecked/On:** turns on the wireless networking on your router (by default it is enabled).

**Note:** *It is recommended to leave the wireless setting to **On** unless you do not plan on connecting any wireless computers or devices to your network.*

- **Operation Mode:** Select the mode you want the access point to operate in.

- **AP:** refer to pagexxxx for additional information.
- **Wireless Client:** refer to page xxx for additional information
- **Bridge:** refer to page xxx for additional information
- **AP Repeater:** refer to page xxx for additional information to operate the device as an access point.

- **Wireless Network Name (SSID):** 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 broadcast TRENDnet715 as the wireless network name. If you choose to change the SSID, change it to a name that you can easily remember. You can click more to configure additional SSID. Please refer to pagexxxx

- **Broadcast SSID:**

- **Enable:** Access point will broadcast the your wireless network name (SSID), making it easier for wireless clients to find the wireless network.
- **Disable:** Access point will not broadcast the wireless network name (SSID) and wireless clients will have to manually enter the wireless network to connect.

- **802.11 Mode:** If all of the wireless devices you want to connect with this Access Point can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate mode. If you have some devices that use a different transmission mode, choose the appropriate mode.

- **802.11b/g mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will allow both wireless b and wireless g client to connect and access point, at 54Mbps for wireless g and share access at the same time. Although the wireless b/g operates in the 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless n/g @ 54Mbps) to connect and access at the same time.
- **802.11b/g/n mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will only allow the use of wireless g client devices to

connect and access point, 54Mbps for wireless g and up to 300Mbps\* for wireless n and share access at the same time. Although the wireless b/g/n operates in the same 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless b/g/n) to connect and access at the same time.

- **HT protect:** Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.
- **Frequency (Channel):** To manually set the channel on which the router will broadcast, uncheck **Auto Channel**, then 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.
- **Extension channel:** When 20/40 channel bandwidth has been chosen, you should select extension channel to get higher throughput.
- **Channel Mode:** Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.
- **Antenna:** By default, IEEE 802.11b/g/n Wireless CPE uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from "Internal (8 dBi)" to "External (N-Type)". When **External (N-Type)** is selected, an Antenna Gain bar will appear to allow you specify the gain of the external antenna. The antenna gain calculates the TX power back off needed to remain in compliance with regulations. Please refer to [External Antenna](#) installation on page 49.
  - You are able to choose "External (N-Type)" only when you have well done installing the external antenna; otherwise, it might damage IEEE 802.11b/g/n Wireless CPE itself.
  - The maximum output power will vary depending on the country selected in order to comply with the local regulation.
  - The output power here is counted from the RF single chain only not including the 8dBi internal antenna.
- **Maximum Output power:** Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly.
- **Data Rate:** Usually "**Auto**" is preferred. Under this rate, the IEEE 802.11b/g/n Wireless CPE will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

- **Extension Channel Protection:** This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

Wireless > Profile

This section outlines available management options under the Profile Settings of the Wireless button. This access point supports multiple SSID, you can set an additional of 16 SSID for your wireless network.

#	Profile Name	SSID	Security	Vlan ID	Enable
1	TEW715	715715TRENDnet	WPA2 with Radius	0	Always Enabled
2	Profile2	TRENDnet715	Open System	0	<input type="checkbox"/>
3	Profile3	TRENDnet715	Open System	0	<input checked="" type="checkbox"/>
4	Profile4	TRENDnet715	Open System	0	<input type="checkbox"/>

- Select **Always Enabled** option and click the Profile Name you would like to configure.

**Basic Settings**

Profile Name:

Wireless Network Name (SSID):

Broadcast SSID:  Enabled  Disabled

Wireless Separation:  Enabled  Disabled

WMM Support:  Enabled  Disabled

Max. Station Num.:  (0-32)

The following section outlines options to configure the basic settings of the multiple SSID.

- **Profile Name:** Enter the profile name of the network name you are configuring.
- **Wireless Network Name (SSID):** This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you.

- **Broadcast Network Name (SSID):**
  - **Enabled** allows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your router.
  - **Disabled** turns 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.
- **Wireless Separation:**
  - Enabled separates all wireless clients connected to this SSID, clients cannot communicate with each other.
  - Disabled allows all wireless clients connect to this SSID to communicate with each other
- **WMM:** Wi-Fi Multimedia is a Quality of Service (QoS) feature which prioritizes audio and video data packets. This feature requires the wireless device to also support WMM. Click **Enabled (recommended)** or **Disabled** to turn this feature on or off on your router.
- **Max. Station Num.:** Select this option to limit the amount of clients who can connect to this SSID.
  - Enter the amount of clients you would like to limit.

**Wireless Client Mode**

Wireless > Basic



This section outlines available management options when the device System Setting is set to **Bridge** and the wireless Operation Mode is set to **Wireless Client**. Click **Apply** to save any changes.

Disable Wireless LAN Interface	
Operation Mode:	Wireless Client <input type="button" value="Site Survey"/>
Wireless Network Name(SSID):	TRENDnet715
Lock AP MAC:	
802.11 Mode:	802.11B/G/N
Channel Mode:	40 MHz
Antenna:	<input checked="" type="radio"/> Internal (8 dBi) <input type="radio"/> External (N-Type)
Maximum Output Power (per chain):	<input type="text" value="12"/> <input type="text" value="26"/> dBm
Data Rate:	Auto
Extension Channel Protection:	None
<input type="checkbox"/> Enable MAC Clone:	00:19:70:79:fd:33

- **Disable Wireless LAN Interface:**

- **Check/Off:** turns off wireless networking on your router.
- **Unchecked/On:** turns on the wireless networking on your router (by default it is enabled).

**Note:** It is recommended to leave the wireless setting to **On** unless you do not plan on connecting any wireless computers or devices to your network.

- **Operation Mode:** Select the mode you want the access point to operate in.
  - **AP:** refer to pagexxx for additional information.
  - **Wireless Client:** refer to page xxx for additional information
  - **Bridge:** refer to page xxx for additional information
  - **AP Repeater:** refer to page xxx for additional information to operate the device as an access point.
- **Site Survey:** Click to scan and select available wireless networks.
- **Wireless Network Name (SSID):** This acronym stands for Service Set Identifier and is the name of your wireless network. You can manually enter the wireless network you want to connect to or click "Site Survey" option to scan for available wireless networks around you. Please refer to pagexxx
- **Lock AP MAC:** Enter the MAC address of the access point you are connected.

- **802.11 Mode:** If all of the wireless devices you want to connect with this Access Point can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate mode. If you have some devices that use a different transmission mode, choose the appropriate mode.
  - **802.11b/g mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will allow both wireless b and wireless g client to connect and access point, at 54Mbps for wireless g and share access at the same time. Although the wireless b/g operates in the 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless n/g @ 54Mbps) to connect and access at the same time.
  - **802.11b/g/n mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will only allow the use of wireless g client devices to connect and access point, 54Mbps for wireless g and up to 300Mbps\* for wireless n and share access at the same time. Although the wireless b/g/n operates in the same 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless b/g/n) to connect and access at the same time.
- **Channel Mode:** Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.
- **Antenna:** By default, IEEE 802.11b/g/n Wireless CPE uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from "Internal (8 dBi)" to "External (N-Type)". When **External (N-Type)** is selected, an Antenna Gain bar will appear to allow you specify the gain of the external antenna. The antenna gain calculates the TX power back off needed to remain in compliance with regulations. Please refer to [External Antenna](#) installation on page 49.
  - You are able to choose "External (N-Type)" only when you have well done installing the external antenna; otherwise, it might damage IEEE 802.11b/g/n Wireless CPE itself.
  - The maximum output power will vary depending on the country selected in order to comply with the local regulation.
  - The output power here is counted from the RF single chain only not including the 8dBi internal antenna.
- **Maximum Output power:** Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly.
- **Data Rate:** Usually "Auto" is preferred. Under this rate, the IEEE 802.11b/g/n Wireless CPE will automatically select the highest available rate to transmit. In

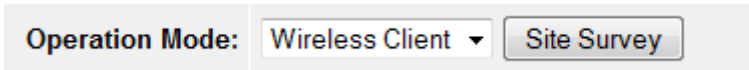
some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

- **Extension Channel Protection:** This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.
- **Enable MAC Clone:** Available only under wireless client mode, it hides the MAC address of the AP while displays the one of associated wireless client or the MAC address designated manually.

**Site Survey:**

The following section outlines how to utilize the site survey option in Wireless Client mode.

1. Log into the management page (see “[Access the management page](#)” on page 27).
2. Click on **Wireless** button and click on **Basic Settings**.
3. Select Wireless Client in the Operation Mode pull down menu and click **Apply**.
4. Click **Site Survey** button.



5. The access point will automatically scan for available access points.
6. Select the access point or wireless network you want to connect.

Select	SSID	Frequency/Channel	MAC Address	Wireless Mode	Signal Strength	Security
<input checked="" type="radio"/>	673ddwrt	2412MHz(1)	00:14:d1:e1:bc:56	802.11B/G/N	-52	WPA2
<input type="radio"/>	TRENDNETRMA-N	2442MHz(7)	00:14:d1:c3:bd:dd	802.11B/G/N	-68	WPA2
<input type="radio"/>	ArielCam	2417MHz(2)	00:50:18:60:13:10	802.11B/G/N	-61	WPA2

7. Click either Select AP , Select SSID or Scan option.
  - **Select AP:** Configures the access point based on the selected AP’s SSID and MAC address
  - **Select SSID:** Configures the access point based on the selected AP’s SSID only
  - **Scan:** Scans for available wireless networks.



8. Click Apply when you have selected the wireless network you want to connect with.
9. If your wireless network is configured with wireless security, click **Profile Settings**

**Basic Settings**

Profile Name:

Wireless Network Name (SSID):

WMM Support:  Enabled  Disabled

---

**Security Settings**

Network Authentication:

Data Encryption:

Key Type:

Default Tx Key:

WEP Passphrase:

Encryption Key 1:

Encryption Key 2:

Encryption Key 3:

Encryption Key 4:

- **Profile Name:** Enter the profile name you would like to assign to the wireless network.
- **Wireless Network Name (SSID):** Name of the wireless network you are connecting too.
- **WMM Support:** Is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type under AP mode only, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should also support it
- **Security Settings:** Select and configure the wireless security of your wireless network. Click **Apply** to save settings. Please refer to **Wireless Encryption Type** section on pagexxx



## Bridge Mode

Wireless > Basic



Bridge or Wireless Distribution System (WDS) or Bridge uses the WDS protocol that is not defined as the standard thus compatibility issues between equipment from different vendors may arise. Moreover, Tree or Star shape network topology should be used in all WDS use-cases (i.e. if AP2 and AP3 are specified as the WDS peers of AP1, AP2 should not be specified as the WDS peer of AP3 and AP3 should not be specified as the WDS peer of AP2 in any case). Mesh and Ring network topologies are not supported by WDS and should be avoided in all the use cases. This section outlines available management options when the device System Setting is set to **Bridge** and the wireless Operation Mode is set to **Bridge**. Click **Apply** to save any changes.

Disable Wireless LAN Interface	
Operation Mode:	Bridge <input type="button" value="Site Survey"/>
802.11 Mode:	802.11B/G/N
Frequency/Channel:	2437MHz (6)
Extension Channel:	Lower Channel 2417MHz (2)
40MHz Center Frequency:	2427MHz (4)
Channel Mode:	40 MHz
Antenna:	<input checked="" type="radio"/> Internal (8 dBi) <input type="radio"/> External (N-Type)
Maximum Output Power (per chain):	<input type="text" value="12"/> <input type="text" value="28"/> <input type="text" value="26"/> dBm
Data Rate:	Auto
Extension Channel Protection:	None

- **Disable Wireless LAN Interface:**

- **Check/Off:** turns off wireless networking on your router.
- **Unchecked/On:** turns on the wireless networking on your router (by default it is enabled).

**Note:** It is recommended to leave the wireless setting to **On** unless you do not plan on connecting any wireless computers or devices to your network.

- **Operation Mode:** Select the mode you want the access point to operate in.

- **AP:** refer to pagexxxx for additional information.
- **Wireless Client:** refer to page xxx for additional information
- **Bridge:** refer to page xxx for additional information
- **AP Repeater:** refer to page xxx for additional information to operate the device as an access point.

- **802.11 Mode:** If all of the wireless devices you want to connect with this Access Point can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate mode. If you have some devices that use a different transmission mode, choose the appropriate mode.

- **802.11b/g mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will allow both wireless b and wireless g client to connect and access point, at 54Mbps for wireless g and share access at the

same time. Although the wireless b/g operates in the 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless n/g @ 54Mbps) to connect and access at the same time.

- **802.11b/g/n mixed mode** (2.4GHz) - This wireless mode works in the 2.4GHz frequency range and will only allow the use of wireless g client devices to connect and access point, 54Mbps for wireless g and up to 300Mbps\* for wireless n and share access at the same time. Although the wireless b/g/n operates in the same 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless b/g/n) to connect and access at the same time.
- **Frequency (Channel):** To manually set the channel on which the router will broadcast, uncheck **Auto Channel**, then 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.
- **Extension channel:** When 20/40 channel bandwidth has been chosen, you should select extension channel to get higher throughput.
- **Channel Mode:** Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.
- **Antenna:** By default, IEEE 802.11b/g/n Wireless CPE uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from “Internal (8 dBi)” to “External (N-Type)”. When **External (N-Type)** is selected, an Antenna Gain bar will appear to allow you specify the gain of the external antenna. The antenna gain calculates the TX power back off needed to remain in compliance with regulations. Please refer to [External Antenna](#) installation on page 49.
  - You are able to choose “External (N-Type)” only when you have well done installing the external antenna; otherwise, it might damage IEEE 802.11b/g/n Wireless CPE itself.
  - The maximum output power will vary depending on the country selected in order to comply with the local regulation.
  - The output power here is counted from the RF single chain only not including the 8dBi internal antenna.
- **Maximum Output power:** Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly.
- **Data Rate:** Usually “Auto” is preferred. Under this rate, the IEEE 802.11b/g/n Wireless CPE will automatically select the highest available rate to transmit. In

some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

- **Extension Channel Protection:** This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

*Wireless >WDS Setting*

This section outlines the available management options under the WDS Settings of the Wireless button. WDS Settings is available only under Bridge and AP Repeater Mode.

<b>WDS Separation:</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>Local MAC Address:</b>	<input type="text" value="00:19:70:79:fd:33"/>
<b>Remote AP MAC Address 1:</b>	<input type="text" value="00:19:70:86:8c:80"/>
<b>Remote AP MAC Address 2:</b>	<input type="text"/>
<b>Remote AP MAC Address 3:</b>	<input type="text"/>
<b>Remote AP MAC Address 4:</b>	<input type="text"/>

- **WDS Separation:** Enable separates all configured WDS AP to communicate with each other.
- **Remote AP:** Enter the MAC address of the access point you want to WDS with. **Note:** You must enter the MAC address of every access point in the WDS network. Each wireless setting (SSID, channel, wireless encryption) must match on each access point in the WDS network.

## AP Repeater Mode

Wireless > Basic.



AP Repeater mode allows the access point to repeat a wireless signal of an existing wireless network. This section outlines available management options when the device System Setting is set to **Bridge** and the wireless Operation Mode is set to **AP Repeater**. Click **Apply** to save any changes.

**Note:** The access point's wireless settings must be configured with the exact wireless settings as the repeating signal (Network name, channel, wireless security, etc.)

Disable Wireless LAN Interface	
Operation Mode:	AP Repeater <input type="button" value="Site Survey"/>
Wireless Network Name(SSID):	TRENDnet715 <input type="button" value="(more...)"/>
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
802.11 Mode:	802.11B/G/N
HT protect:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Frequency/Channel:	2437MHz (6)
Extension Channel:	Lower Channel 2417MHz (2)
40MHz Center Frequency:	2427MHz (4)
Channel Mode:	40 MHz
Antenna:	<input checked="" type="radio"/> Internal (8 dBi) <input type="radio"/> External (N-Type)
Maximum Output Power (per chain):	<input type="range" value="26"/> 26 dBm
Data Rate:	Auto
Extension Channel Protection:	None

- **Disable Wireless LAN Interface:**
  - **Check/Off:** turns off wireless networking on your router.
  - **Unchecked/On:** turns on the wireless networking on your router (by default it is enabled).
- Note:** It is recommended to leave the wireless setting to **On** unless you do not plan on connecting any wireless computers or devices to your network.
- **Operation Mode:** Select the mode you want the access point to operate in.
  - **AP:** refer to pagexxx for additional information.
  - **Wireless Client:** refer to page xxx for additional information
  - **Bridge:** refer to page xxx for additional information
  - **AP Repeater:** refer to page xxx for additional information to operate the device as an access point.
- **Wireless Network Name (SSID):** This acronym stands for Service Set Identifier and is the name of your wireless network. You can manually enter the wireless network you want to repeat.
- **Broadcast SSID:**
  - **Enable:** Access point will broadcast the your wireless network name (SSID), making it easier for wireless clients to find the wireless network.

- **Disable:** Access point will not broadcast the wireless network name (SSID) and wireless clients will have to manually enter the wireless network to connect.
- **802.11 Mode:** If all of the wireless devices you want to connect with this Access Point can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate mode. If you have some devices that use a different transmission mode, choose the appropriate mode.
  - **802.11b/g mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will allow both wireless b and wireless g client to connect and access point, at 54Mbps for wireless g and share access at the same time. Although the wireless b/g operates in the 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless n/g @ 54Mbps) to connect and access at the same time.
  - **802.11b/g/n mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will only allow the use of wireless g client devices to connect and access point, 54Mbps for wireless g and up to 300Mbps\* for wireless n and share access at the same time. Although the wireless b/g/n operates in the same 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless b/g/n) to connect and access at the same time.
- **HT protect:** Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.
- **Frequency (Channel):** To manually set the channel on which the router will broadcast, uncheck **Auto Channel**, then 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.
- **Extension channel:** When 20/40 channel bandwidth has been chosen, you should select extension channel to get higher throughput.
- **Channel Mode:** Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.
- **Antenna:** By default, IEEE 802.11b/g/n Wireless CPE uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from "Internal (8 dBi)" to "External (N-Type)". When **External (N-Type)** is selected, an Antenna Gain bar will appear to allow you specify the gain of the external antenna. The antenna gain

- calculates the TX power back off needed to remain in compliance with regulations. Please refer to [External Antenna](#) installation on page 49.
- You are able to choose "External (N-Type)" only when you have well done installing the external antenna; otherwise, it might damage IEEE 802.11b/g/n Wireless CPE itself.
  - The maximum output power will vary depending on the country selected in order to comply with the local regulation.
  - The output power here is counted from the RF single chain only not including the 8dBi internal antenna.
- **Maximum Output power:** Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly.
  - **Data Rate:** Usually "Auto" is preferred. Under this rate, the IEEE 802.11b/g/n Wireless CPE will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.
  - **Extension Channel Protection:** This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

4. Click **Profile Settings** and select the Profile Name you want to configure.

#	Profile Name	SSID	Security	Vlan ID	Enable
1	TEW715	715715TRENDnet	WPA2 with Radius	<input type="text" value="0"/>	Always Enabled
2	Profile2	TRENDnet715	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
3	Profile3	TRENDnet715	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
4	Profile4	TRENDnet715	Open System	<input type="text" value="0"/>	<input type="checkbox"/>

5. Enter the configuration settings to match the access point to repeat and click **Apply** to save settings.

## Router Mode

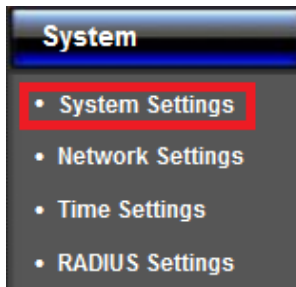
Below describes the configuration settings when the TEW-715APO System Mode is set to Router. In this configuration the Ethernet port of the TEW-715APO can serve as the WAN (Wide Area Network) or Internet port. Please verify your network configuration when using this mode. Please refer to [Internet Service Types](#) section in the Appendix to help determine your Internet settings.

### Configuration

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Your access point will prompt you for a user name and password.



3. Enter the default user name and password and then click Login.  
Default User Name: **admin**  
Default Password: **admin**
4. Click the System button on the left side and then System Settings.



5. Select **Router** in the System Mode drop down menu.
6. Click **Apply** button to save your setting.

Device Settings	
Device Name:	TEW-715APO (max. 15 characters and no spaces)
Network Mode:	Bridge

7. Click the Wireless button on the left side and then Basic Settings.



8. Select the mode you would like to apply Operation Mode pull down menu. Click **Apply** to save changes.
  - **AP Mode:** Creates a wireless network with your device (similar to a wireless router). Device Ethernet port serves as a WAN (Wide Area Network) or Internet port.
  - **Wireless Client:** Connects to any existing wireless network (similar to a wireless adapter) in which the wireless network the device is connecting to serves as your Internet connection. Ethernet port serves as a LAN (Local Area Network) port of the device and the wireless settings is based on your ISP (Internet Service Provider) connection.
  - **Bridge:** Creates a wireless network with your device (similar to a wireless router). Device Ethernet port serves as a WAN (Wide Area Network) or Internet port.
  - **AP Repeater:** Creates a wireless network with your device (similar to a wireless router). Device Ethernet port serves as a WAN (Wide Area Network) or Internet port.

## AP Mode

Wireless > Basic



When AP mode is selected a wireless network is created with your device (similar to wireless router). Device Ethernet port serves as a WAN (Wide Area Network) or Internet port. This section outlines available management options when the device System Setting is set to **Router** and the wireless Operation Mode is set to **AP**. Click **Apply** to save any changes.

Disable Wireless LAN Interface	
Operation Mode:	AP <input type="button" value="Site Survey"/>
Wireless Network Name(SSID):	715715TRENDnet <a href="#">(more...)</a>
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
802.11 Mode:	802.11B/G/N
HT protect:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Frequency/Channel:	2437MHz (6)
Extension Channel:	Lower Channel 2417MHz (2)
40MHz Center Frequency:	2427MHz (4)
Channel Mode:	40 MHz
Antenna:	<input checked="" type="radio"/> Internal (8 dBi) <input type="radio"/> External (N-Type)
Maximum Output Power (per chain):	<input type="range" value="26"/> 26 dBm
Data Rate:	Auto
Extension Channel Protection:	None

- **Disable Wireless LAN Interface:**
  - **Check/Off:** turns off wireless networking on your router.
  - **Unchecked/On:** turns on the wireless networking on your router (by default it is enabled).
- **Note:** It is recommended to leave the wireless setting to **On** unless you do not plan on connecting any wireless computers or devices to your network.
- **Operation Mode:** Select the mode you want the access point to operate in.
  - **AP:** refer to pagexxxx for additional information.
  - **Wireless Client:** refer to page xxx for additional information
  - **Bridge:** refer to page xxx for additional information
  - **AP Repeater:** refer to page xxx for additional information to operate the device as an access point.
- **Wireless Network Name (SSID):** 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 broadcast TRENDnet715 as

the wireless network name. If you choose to change the SSID, change it to a name that you can easily remember. You can click more to configure additional SSID.

Please refer to pagexxxx

- **Broadcast SSID:**
  - **Enable:** Access point will broadcast the your wireless network name (SSID), making it easier for wireless clients to find the wireless network.
  - **Disable:** Access point will not broadcast the wireless network name (SSID) and wireless clients will have to manually enter the wireless network to connect.
- **802.11 Mode:** If all of the wireless devices you want to connect with this Access Point can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate mode. If you have some devices that use a different transmission mode, choose the appropriate mode.
  - **802.11b/g mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will allow both wireless b and wireless g client to connect and access point, at 54Mbps for wireless g and share access at the same time. Although the wireless b/g operates in the 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless n/g @ 54Mbps) to connect and access at the same time.
  - **802.11b/g/n mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will only allow the use of wireless g client devices to connect and access point, 54Mbps for wireless g and up to 300Mbps\* for wireless n and share access at the same time. Although the wireless b/g/n operates in the same 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless b/g/n) to connect and access at the same time.
- **HT protect:** Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.
- **Frequency (Channel):** To manually set the channel on which the router will broadcast, uncheck **Auto Channel**, then 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.
- **Extension channel:** When 20/40 channel bandwidth has been chosen, you should select extension channel to get higher throughput.
- **Channel Mode:** Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.

- **Antenna:** By default, IEEE 802.11b/g/n Wireless CPE uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from "Internal (8 dBi)" to "External (N-Type)". When **External (N-Type)** is selected, an Antenna Gain bar will appear to allow you specify the gain of the external antenna. The antenna gain calculates the TX power back off needed to remain in compliance with regulations. Please refer to [External Antenna](#) installation on page 49.
  - You are able to choose "External (N-Type)" only when you have well done installing the external antenna; otherwise, it might damage IEEE 802.11b/g/n Wireless CPE itself.
  - The maximum output power will vary depending on the country selected in order to comply with the local regulation.
  - The output power here is counted from the RF single chain only not including the 8dBi internal antenna.
- **Maximum Output power:** Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly.
- **Data Rate:** Usually "**Auto**" is preferred. Under this rate, the IEEE 802.11b/g/n Wireless CPE will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.
- **Extension Channel Protection:** This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

Wireless > Profile

This section outlines available management options under the Profile Settings of the Wireless button. This access point supports multiple SSID, you can set an additional of 16 SSID for your wireless network.

#	Profile Name	SSID	Security	Vlan ID	Enable
1	TEW715	715715TRENDnet	WPA2 with Radius	0	Always Enabled
2	Profile2	TRENDnet715	Open System	0	<input type="checkbox"/>
3	Profile3	TRENDnet715	Open System	0	<input type="checkbox"/>
4	Profile4	TRENDnet715	Open System	0	<input type="checkbox"/>

- Select **Always Enabled** option and click the Profile Name you would like to configure.

**Basic Settings**

Profile Name:

Wireless Network Name (SSID):

Broadcast SSID:  Enabled  Disabled

Wireless Separation:  Enabled  Disabled

WMM Support:  Enabled  Disabled

Max. Station Num:  (0-32)

The following section outlines options to configure the basic settings of the multiple SSID.

- **Profile Name:** Enter the profile name of the network name you are configuring.
- **Wireless Network Name (SSID):** This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you.
- **Broadcast Network Name (SSID):**
  - **Enabled** allows wireless devices to search and discover your wireless network name (also called SSID) broadcasted by your router.
  - **Disabled** turns 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.

- **Wireless Separation:**
  - Enabled separates all wireless clients connected to this SSID, clients cannot communicate with each other.
  - Disabled allows all wireless clients connect to this SSID to communicate with each other
- **WMM:** Wi-Fi Multimedia is a Quality of Service (QoS) feature which prioritizes audio and video data packets. This feature requires the wireless device to also support WMM. Click **Enabled (recommended)** or **Disabled** to turn this feature on or off on your router.
- **Max. Station Num.:** Select this option to limit the amount of clients who can connect to this SSID.
  - Enter the amount of clients you would like to limit.

### Wireless Client Mode

Wireless > Basic



When Wireless Client is selected, the device connects to a wireless network (similar to a wireless adapter) in which the wireless network the device is connecting to serves as your Internet connection. The Ethernet port serves as a LAN (Local Area Network) port of the device and the wireless settings is based on your ISP (Internet Service Provider) connection. This section outlines available management options under the Basic Settings of the Wireless button when the Operation Mode is set to **AP Client** and will assist in setting up the access point. Click **Apply** to save any changes.



Disable Wireless LAN Interface	
Operation Mode:	Wireless Client <input type="button" value="Site Survey"/>
Wireless Network Name(SSID):	TRENDnet715
Lock AP MAC:	
802.11 Mode:	802.11B/G/N
Channel Mode:	40 MHz
Antenna:	<input checked="" type="radio"/> Internal (8 dBi) <input type="radio"/> External (N-Type)
Maximum Output Power (per chain):	<input type="text" value="12"/> <input type="text" value="26"/> dBm
Data Rate:	Auto
Extension Channel Protection:	None
<input type="checkbox"/> Enable MAC Clone:	00:19:70:79:fd:33

- **Disable Wireless LAN Interface:**

- **Check/Off:** turns off wireless networking on your router.
- **Unchecked/On:** turns on the wireless networking on your router (by default it is enabled).

**Note:** It is recommended to leave the wireless setting to **On** unless you do not plan on connecting any wireless computers or devices to your network.

- **Operation Mode:** Select the mode you want the access point to operate in.
  - **AP:** refer to pagexxx for additional information.
  - **Wireless Client:** refer to page xxx for additional information
  - **Bridge:** refer to page xxx for additional information
  - **AP Repeater:** refer to page xxx for additional information to operate the device as an access point.
- **Site Survey:** Click to scan and select available wireless networks.
- **Wireless Network Name (SSID):** This acronym stands for Service Set Identifier and is the name of your wireless network. You can manually enter the wireless network you want to connect to or click "Site Survey" option to scan for available wireless networks around you. Please refer to pagexxx
- **Lock AP MAC:** Enter the MAC address of the access point you are connected.

- **802.11 Mode:** If all of the wireless devices you want to connect with this Access Point can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate mode. If you have some devices that use a different transmission mode, choose the appropriate mode.
  - **802.11b/g mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will allow both wireless b and wireless g client to connect and access point, at 54Mbps for wireless g and share access at the same time. Although the wireless b/g operates in the 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless n/g @ 54Mbps) to connect and access at the same time.
  - **802.11b/g/n mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will only allow the use of wireless g client devices to connect and access point, 54Mbps for wireless g and up to 300Mbps\* for wireless n and share access at the same time. Although the wireless b/g/n operates in the same 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless b/g/n) to connect and access at the same time.
- **Channel Mode:** Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.
- **Antenna:** By default, IEEE 802.11b/g/n Wireless CPE uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from "Internal (8 dBi)" to "External (N-Type)". When **External (N-Type)** is selected, an Antenna Gain bar will appear to allow you specify the gain of the external antenna. The antenna gain calculates the TX power back off needed to remain in compliance with regulations. Please refer to [External Antenna](#) installation on page 49.
  - You are able to choose "External (N-Type)" only when you have well done installing the external antenna; otherwise, it might damage IEEE 802.11b/g/n Wireless CPE itself.
  - The maximum output power will vary depending on the country selected in order to comply with the local regulation.
  - The output power here is counted from the RF single chain only not including the 8dBi internal antenna.
- **Maximum Output power:** Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly.
- **Data Rate:** Usually "Auto" is preferred. Under this rate, the IEEE 802.11b/g/n Wireless CPE will automatically select the highest available rate to transmit. In

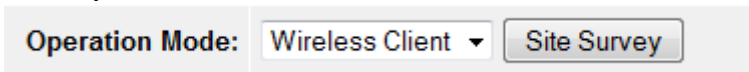
some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

- **Extension Channel Protection:** This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.
- **Enable MAC Clone:** Available only under wireless client mode, it hides the MAC address of the AP while displays the one of associated wireless client or the MAC address designated manually.

**Site Survey:**

The following section outlines how to utilize the site survey option in Wireless Client mode.

1. Log into the management page (see “[Access the management page](#)” on page 9).
2. Click on **Wireless** button and click on **Basic Settings**.
3. Select Wireless Client in the Operation Mode pull down menu and click **Apply**.
4. Click **Site Survey** button.



5. The access point will automatically scan for available access points.
6. Select the access point or wireless network you want to connect.

Select	SSID	Frequency/Channel	MAC Address	Wireless Mode	Signal Strength	Security
<input checked="" type="radio"/>	673ddwrt	2412MHz(1)	00:14:d1:e1:bc:56	802.11B/G/N	-52	WPA2
<input type="radio"/>	TRENDNETRMA-N	2442MHz(7)	00:14:d1:c3:bd:dd	802.11B/G/N	-68	WPA2
<input type="radio"/>	ArielCam	2417MHz(2)	00:50:18:60:13:10	802.11B/G/N	-61	WPA2

7. Click either Select AP , Select SSID or Scan option.
  - **Select AP:** Configures the access point based on the selected AP's SSID and MAC address
  - **Select SSID:** Configures the access point based on the selected AP's SSID only
  - **Scan:** Scans for available wireless networks.



8. Click Apply when you have selected the wireless network you want to connect with.
9. If your wireless network is configured with wireless security, click **Profile Settings**

**Basic Settings**

Profile Name:

Wireless Network Name (SSID):

WMM Support:  Enabled  Disabled

---

**Security Settings**

Network Authentication:

Data Encryption:

Key Type:

Default Tx Key:

WEP Passphrase:

Encryption Key 1:

Encryption Key 2:

Encryption Key 3:

Encryption Key 4:

- o **Profile Name:** Enter the profile name you would like to assign to the wireless network.
- **Wireless Network Name (SSID):** Name of the wireless network you are connecting too.
- **WMM Support:** Is a subset of 802.11e. It allows wireless communication to define a priority limit on the basis of data type under AP mode only, thus those time-sensitive data, like video/audio data, may own a higher priority than common one. To enable WMM, the wireless client should also support it
- **Security Settings:** Select and configure the wireless security of your wireless network. Click **Apply** to save settings. Please refer to **Wireless Encryption Type** section on pagexxx

## Bridge Mode

Wireless > Basic



When Bridge is selected a wireless network is created with your device (similar to a wireless router). Device Ethernet port serves as a WAN (Wide Area Network) or Internet port. This section outlines available management options under the Basic Settings of the Wireless button when the Operation Mode is set to **Bridge** and will assist in setting up the access point. Click **Apply** to save any changes.

Disable Wireless LAN Interface	
Operation Mode:	Bridge <input type="button" value="Site Survey"/>
802.11 Mode:	802.11B/G/N
Frequency/Channel:	2437MHz (6)
Extension Channel:	Lower Channel 2417MHz (2)
40MHz Center Frequency:	2427MHz (4)
Channel Mode:	40 MHz
Antenna:	<input checked="" type="radio"/> Internal (8 dBi) <input type="radio"/> External (N-Type)
Maximum Output Power (per chain):	12 <input type="range" value="26"/> 28 26 dBm
Data Rate:	Auto
Extension Channel Protection:	None

- **Disable Wireless LAN Interface:**
  - **Check/Off:** turns off wireless networking on your router.
  - **Unchecked/On:** turns on the wireless networking on your router (by default it is enabled).
- Note:** It is recommended to leave the wireless setting to **On** unless you do not plan on connecting any wireless computers or devices to your network.
- **Operation Mode:** Select the mode you want the access point to operate in.
  - **AP:** refer to page xxx for additional information.
  - **Wireless Client:** refer to page xxx for additional information
  - **Bridge:** refer to page xxx for additional information
  - **AP Repeater:** refer to page xxx for additional information to operate the device as an access point.
- **802.11 Mode:** If all of the wireless devices you want to connect with this Access Point can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate mode. If you have some devices that use a different transmission mode, choose the appropriate mode.
  - **802.11b/g mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will allow both wireless b and wireless g client to

connect and access point, at 54Mbps for wireless g and share access at the same time. Although the wireless b/g operates in the 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless n/g @ 54Mbps) to connect and access at the same time.

- **802.11b/g/n mixed mode** (2.4GHz) - This wireless mode works in the 2.4GHz frequency range and will only allow the use of wireless g client devices to connect and access point, 54Mbps for wireless g and up to 300Mbps\* for wireless n and share access at the same time. Although the wireless b/g/n operates in the same 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless b/g/n) to connect and access at the same time.
- **Frequency (Channel):** To manually set the channel on which the router will broadcast, uncheck **Auto Channel**, then 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.
- **Extension channel:** When 20/40 channel bandwidth has been chosen, you should select extension channel to get higher throughput.
- **Channel Mode:** Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.
- **Antenna:** By default, IEEE 802.11b/g/n Wireless CPE uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from "Internal (8 dBi)" to "External (N-Type)". When **External (N-Type)** is selected, an Antenna Gain bar will appear to allow you specify the gain of the external antenna. The antenna gain calculates the TX power back off needed to remain in compliance with regulations. Please refer to [External Antenna](#) installation on page 49.
  - You are able to choose "External (N-Type)" only when you have well done installing the external antenna; otherwise, it might damage IEEE 802.11b/g/n Wireless CPE itself.
  - The maximum output power will vary depending on the country selected in order to comply with the local regulation.
  - The output power here is counted from the RF single chain only not including the 8dBi internal antenna.
- **Maximum Output power:** Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly.
- **Data Rate:** Usually "Auto" is preferred. Under this rate, the IEEE 802.11b/g/n Wireless CPE will automatically select the highest available rate to transmit. In

some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.

- **Extension Channel Protection:** This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

#### Wireless >WDS Setting

This section outlines the available management options under the WDS Settings of the Wireless button.

**Note:** WDS Settings is available only under Bridge and AP Repeater Mode.

<b>WDS Separation:</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>Local MAC Address:</b>	<input type="text" value="00:19:70:79:fd:33"/>
<b>Remote AP MAC Address 1:</b>	<input type="text" value="00:19:70:86:8c:80"/>
<b>Remote AP MAC Address 2:</b>	<input type="text"/>
<b>Remote AP MAC Address 3:</b>	<input type="text"/>
<b>Remote AP MAC Address 4:</b>	<input type="text"/>

- **WDS Separation:** Enable separates all configured WDS AP to communicate with each other.
- **Remote AP:** Enter the MAC address of the access point you want to WDS with.
 

**Note:** You must enter the MAC address of every access point in the WDS network. Each wireless setting (SSID, channel, wireless encryption) must match on each access point in the WDS network.

## AP Repeater Mode

Wireless > Basic



When **Router** mode is applied as the system mode and the operation mode is set to **AP Repeater**, the access point serves as a wireless router. This section outlines available management options under the Basic Settings of the Wireless button when the Operation Mode is set to **Bridge** and will assist in setting up the access point. Click **Apply** to save any changes.

Disable Wireless LAN Interface	
Operation Mode:	AP Repeater <input type="button" value="Site Survey"/>
Wireless Network Name(SSID):	TRENDnet715 <input type="button" value="(more...)"/>
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
802.11 Mode:	802.11B/G/N
HT protect:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Frequency/Channel:	2437MHz (6)
Extension Channel:	Lower Channel 2417MHz (2)
40MHz Center Frequency:	2427MHz (4)
Channel Mode:	40 MHz
Antenna:	<input checked="" type="radio"/> Internal (8 dBi) <input type="radio"/> External (N-Type)
Maximum Output Power (per chain):	<input type="range" value="26"/> 26 dBm
Data Rate:	Auto
Extension Channel Protection:	None

- **Disable Wireless LAN Interface:**
  - **Check/Off:** turns off wireless networking on your router.
  - **Unchecked/On:** turns on the wireless networking on your router (by default it is enabled).
- Note:** It is recommended to leave the wireless setting to **On** unless you do not plan on connecting any wireless computers or devices to your network.
- **Operation Mode:** Select the mode you want the access point to operate in.
  - **AP:** refer to pagexxxx for additional information.
  - **Wireless Client:** refer to page xxx for additional information
  - **Bridge:** refer to page xxx for additional information
  - **AP Repeater:** refer to page xxx for additional information to operate the device as an access point.
- **Wireless Network Name (SSID):** This acronym stands for Service Set Identifier and is the name of your wireless network. You can manually enter the wireless network you want to repeat.
- **Broadcast SSID:**
  - **Enable:** Access point will broadcast the your wireless network name (SSID), making it easier for wireless clients to find the wireless network.

- **Disable:** Access point will not broadcast the wireless network name (SSID) and wireless clients will have to manually enter the wireless network to connect.
- **802.11 Mode:** If all of the wireless devices you want to connect with this Access Point can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate mode. If you have some devices that use a different transmission mode, choose the appropriate mode.
  - **802.11b/g mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will allow both wireless b and wireless g client to connect and access point, at 54Mbps for wireless g and share access at the same time. Although the wireless b/g operates in the 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless n/g @ 54Mbps) to connect and access at the same time.
  - **802.11b/g/n mixed mode (2.4GHz)** - This wireless mode works in the 2.4GHz frequency range and will only allow the use of wireless g client devices to connect and access point, 54Mbps for wireless g and up to 300Mbps\* for wireless n and share access at the same time. Although the wireless b/g/n operates in the same 2.4GHz frequency, it will allow the use of other 2.4GHz client devices (Wireless b/g/n) to connect and access at the same time.
- **HT protect:** Enable HT (High Throughput) protect to ensure HT transmission with MAC mechanism. Under 802.11n mode, wireless client can be divided into HT STA and Non-HT STA, among which the one with HT protect enabled gets higher throughput.
- **Frequency (Channel):** To manually set the channel on which the router will broadcast, uncheck **Auto Channel**, then 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.
- **Extension channel:** When 20/40 channel bandwidth has been chosen, you should select extension channel to get higher throughput.
- **Channel Mode:** Four levels are available: 5MHz, 10MHz, 20MHz and 40MHz. The last one can enhance data throughput, but it takes more bandwidth, thus it might cause potential interference.
- **Antenna:** By default, IEEE 802.11b/g/n Wireless CPE uses its built-in antenna for directional transmission; however, if you prefer to use an external antenna for your case-dependent applications, you can switch from "Internal (8 dBi)" to "External (N-Type)". When **External (N-Type)** is selected, an Antenna Gain bar will appear to allow you specify the gain of the external antenna. The antenna gain

calculates the TX power back off needed to remain in compliance with regulations. Please refer to [External Antenna](#) installation on page 49.

- You are able to choose "External (N-Type)" only when you have well done installing the external antenna; otherwise, it might damage IEEE 802.11b/g/n Wireless CPE itself.
- The maximum output power will vary depending on the country selected in order to comply with the local regulation.
- The output power here is counted from the RF single chain only not including the 8dBi internal antenna.
- **Maximum Output power:** Specify the signal transmission power. The higher the output power is, the wider the signal can cover, but the power consumption will be greater accordingly.
- **Data Rate:** Usually "Auto" is preferred. Under this rate, the IEEE 802.11b/g/n Wireless CPE will automatically select the highest available rate to transmit. In some cases, however, like where there is no great demand for speed, you can have a relatively-low transmit rate for compromise of a long distance.
- **Extension Channel Protection:** This is to avoid conflict with other wireless network and boost the ability of your device to catch all 802.11g transmissions. However, it may decrease wireless network performance. Compared to CTS-Self; the transmission amount of CTS-RTS is much lower.

4. Click **Profile Settings** and select the Profile Name you want to configure.

#	Profile Name	SSID	Security	Vlan ID	Enable
1	TEW715	715715TRENDnet	WPA2 with Radius	<input type="text" value="0"/>	Always Enabled
2	Profile2	TRENDnet715	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
3	Profile3	TRENDnet715	Open System	<input type="text" value="0"/>	<input type="checkbox"/>
4	Profile4	TRENDnet715	Open System	<input type="text" value="0"/>	<input type="checkbox"/>

5. Enter the configuration settings to match the access point to repeat and click **Apply** to save settings.

## Wireless Networking and Security

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

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

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 router to WEP to allow the old adapters to connect to the router. **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 router 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 router to this encryption standard. If you find that one of your wireless network devices does not support WPA2 encryption, then set your router 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
<b>Compatible Wireless Standards</b>	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
<b>Highest Performance Under This Setting</b>	Up to 54Mbps	Up to 54Mbps	Up to 450Mbps*
<b>Encryption Strength</b>	Low	Medium	High
<b>Additional Options</b>	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
<b>Recommended Configuration</b>	Open System ASCII 13 characters	TKIP Preshared Key	AES Preshared Key

		8-63 characters	8-63 characters
--	--	-----------------	-----------------

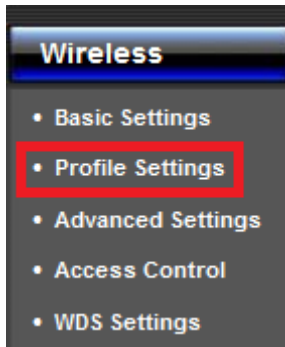
\*Dependent on the maximum 802.11n data rate supported by the device (150Mbps, 300Mbps, or 450Mbps)

## Secure your wireless network

Wireless > Profile Settings

After you have determined which security type to use for your wireless network (see "How to choose the security type for your wireless network" on page 12), you can set up wireless security.

1. Log into the management page (see "Access the management page" on page 9).
2. Click on **Wireless** button and click on **Profile Settings**.

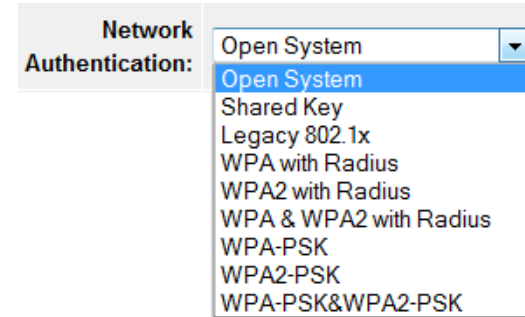


3. Click on the Profile name you would like to apply wireless security.

#	Profile Name	SSID	Security	Vlan ID	Enable
1	TEW715	715715TRENDnet	Open System	<input type="text" value="0"/>	Always Enabled



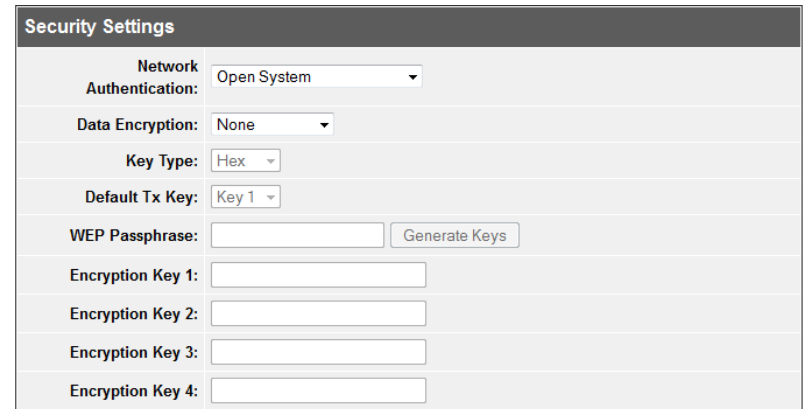
4. Select the wireless security on your wireless network from the **Network Authentication** pull down menu.



### Selecting WEP (Open System or Shared Key):

If selecting **WEP** (Wired Equivalent Privacy), please review the WEP settings to configure and click **Apply** to save the changes.

**Note:** It is recommended to use Open System because it is known to be more secure than Shared Key.



- **Data 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.

- **Key type:** Choose **HEX** or **ASCII**.

**Note:** It is recommended to use ASCII because of the much larger character set that can be used to create the key.

- **Key 1-4**



- This is where you enter the password or key needed for a computer to connect to the router wirelessly
- You can define up to 4 passwords or 4 keys. Only one key can be active at a given time. Most users simply define one key.
- Choose a key index 1, 2, 3, or 4 and enter the key.
- When connecting to the router, the client must match both the password and the Key number. (e.g. if you have activated Key 2 with a password of 12345, then the client must select: Key 2 (entering Key 1, 3, or 4 will block the ability to connect) and enter password 12345)
- **WEP Passphrase:** Enter a passphrase and click Generate key to have the access point generate your encryption key.

WEP Key Format	HEX	ASCII
Character set	0-9 & A-F, a-f only	Alphanumeric (a,b,C,?,*,/,1,2, etc.)
64-bit key length	10 characters	5 characters
128-bit key length	26 characters	13 characters

**Selecting WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK (WPA2-PSK recommended):**

The screenshot shows the 'Security Settings' form with 'Network Authentication' set to 'WPA2-PSK' and 'Data Encryption' set to 'AES'. The 'WPA Passphrase (Network Key)' field contains several asterisks.

**The following section outlines options when selecting PSK (Preshared Key Protocol).**

- **Data Encryption:** Select the cipher type to use.
  - **TKIP:** Recommended when using WPA-PSK security.
  - **AES:** Recommended when using WPA2-PSK or WPA-PSK & WPA2-PSK
- **WPA Passphrase** – Enter the passphrase.
  - This is the password or key that is used to connect your computer to this router wirelessly

**Selecting WPA, WPA2, or WPA & WPA2 with Radius:**

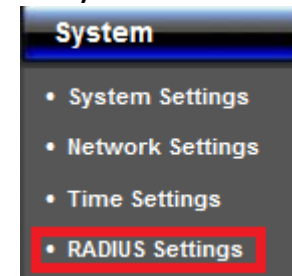
This is a duplicate of the screenshot above, showing the 'Security Settings' form with 'WPA2-PSK' authentication and 'AES' encryption.

**The following section outlines options when selecting Radius.**

*Note: Radius requires an external RADIUS server, PSK only requires you to create a passphrase.*

- **Data Encryption:** Select the cipher type to use.
  - **TKIP:** Recommended when using WPA-PSK security.
  - **AES:** Recommended when using WPA2-PSK or WPA-PSK & WPA2-PSK

Once you have selected the data encryption type. Click **Apply** to save settings and go to the **RADIUS Settings** section under **System** button on the left side.



**The following section outlines options to configure the access point's RADIUS settings.**

The screenshot shows the 'Authentication RADIUS Server' form with 'IP Address' set to '0.0.0.0', 'Port' set to '1812', and 'Shared Secret' field empty.

- **Radius Server** - Configure the RADIUS server settings.
    - **IP** – Enter the IP address of the RADIUS server. (e.g. 192.168.10.250)
    - **Port** – Enter the port your RADIUS server is configured to use for RADIUS authentication.
- Note: It is recommended to use port 1812.*

- **Shared Secret** – Enter the shared secret used to authorize your router

Global-Key Update	
every	<input type="text" value="3600"/> Seconds

- **Global-Key Update**
  - Enable this option to set the cache period based on seconds

## Wireless access control

*Wireless > Access Control*

The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adapter.

<b>Access Control Mode:</b>	<input type="text" value="Disable"/>
<b>MAC Address:</b>	<input type="text"/>

- **Access Control Mode:**
  - **Disable:** Access control is disabled
  - **Allow Listed:** Enter MAC address allowed to connect to the access point
  - **Deny List:** Enter MAC addresses to block connection to the access point.

## Advance Settings

### Change your IP address

*Basic Setting > Primary Setup*

In most cases, you do not need to change the access point's IP address settings. Typically, the access point IP address settings only needs to be changed, if you plan to use another access point in your network with the same IP address settings, if you are connecting the access point to an existing network that is already using the IP address settings your access point is using.

In addition, the 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. If you already have a DHCP server on your network, or if you do not want to use the access point as a DHCP server, you can disable this setting. This setting would be used when the access point's System settings is set to Router mode.

**Note:** If you are not encountering any issues or are not faced with one of the cases described above or similar, it is recommended to keep your router IP address settings as default.

**Note:** For VPN (Virtual Private Network) configuration, it is required that each router should have a different router or LAN IP address/network on each end of the VPN tunnel.

Default Router or LAN IP Address: 192.168.10.1 00

Default Router or LAN IP Network: 192.168.10.0 / 255.255.255.0

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **System**, and click on **Network Settings**.

LAN Settings	
IP Address :	192.168.10.100
Subnet Mask :	255.255.255.0
DHCP Server :	Disabled ▾
DHCP IP Address Range :	192.168.10.1 - 192.168.10.200
Lease Time :	7200 (15-44640 Minutes)
<input type="checkbox"/> Enable DHCP Relay	
DHCP Server IP :	0.0.0.0

- **IP Address:** Enter the new access point IP address. (e.g. 192.168.100.1)
- **Subnet Mask:** Enter the new access point subnet mask.(e.g. 255.255.255.0)
- **DHCP Server:** Enable or Disable the DHCP server on the access point.
- **DHCP IP Address Range:** Enter the IP address of the DHCP server to assign.
- **Lease Time:** Enter the lease time in seconds that DHCP client will hold their automatically assigned IP address before requesting a new IP address
- **Enable DHCP Relay:** Enable to forward DHCP requests and replies between clients and servers when they are not on the same physical subnet
- **DHCP Server IP:** Enter the DHCP IP address of the DHCP Relay

**Note:** The DHCP address range will change automatically to your new access point's IP address settings so you do not have to change the DHCP address range manually to match your new router IP address settings.

3. To save changes, click **Apply** at the bottom of the page.

**Note:** If you changed the IP address of the access point you will need to access the management page using the new IP address (e.g Instead of using the default <http://192.168.10.100> using your new router IP address will use the following format using your new router IP address [http://\(new.router.ipaddress.here\)](http://(new.router.ipaddress.here)) to access the management page.

## Configure your Internet connection

System > Network Settings

This section describes the features when setting the access points WAN settings. The access point supports DHCP, Static or PPPoE WAN types. Refer to [Internet Service Type](#) section in the Appendix for additional information on connection types. Before configuring this section, complete the settings in the [Router Mode](#) section to determine the type of networking you will be setting.

**Note:** This feature is only available when **Router** mode is applied in **System Settings**.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **System**, and click on **Network Settings**.
3. In the **WAN Access Type** drop-down list, select the type of Internet connection provided by your ISP (Internet Service Provider).

WAN Settings:	
WAN Access Type :	Static IP ▾
IP Address :	192.168.0.99
Subnet Mask :	255.255.255.0
Default Gateway :	192.168.0.254
DNS 1 :	0.0.0.0
DNS 2 :	0.0.0.0

4. Complete the fields required by your ISP.
5. Complete the optional settings only if required by your ISP.
6. To save changes, click **Save**.

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

## Setting time

System > Time Settings

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **System**, and click on **Time Settings**.

Current Time:	Yr 2010	Mon 1	Day 1	Hr 3	Mn 54	Sec 3
Time Zone Select:	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London					
<input type="checkbox"/> Enable NTP client update						
<input type="radio"/> NTP server:	192.5.41.41 - North America					
<input checked="" type="radio"/> Manual IP:	0.0.0.0					

### Manual configure time settings

1. Manually enter the date and time settings.
2. Next to **Time Zone Select**, select your time zone from the drop down menu. Click **Apply** to save settings.

### Time setting using a NTP server

1. Click **Enable NTP client update** option to obtain date and time settings from a NTP server.
2. Select one of the below options. Click **Apply** to save settings.
  - **NTP Server:** Select a NTP server to use.
  - **Manual IP:** Manually enter your NTP server.
2. You can also click **Enable NTP client update** option to obtain date and time settings from a NTP server.

## Advance wireless settings

Wireless > Advance Settings

This section outlines available management options under the Advance Settings of the Wireless button.

A-MPDU aggregation:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
A-MSDU aggregation:	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
Short GI:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
RTS Threshold:	2347	(1-2347)
Fragment Threshold:	2346	(256-2346)
Beacon Interval:	100	(20-1024 ms)
DTIM Interval:	1	(1-255)
Preamble Type:	<input type="radio"/> Long	<input checked="" type="radio"/> Auto
IGMP Snooping:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
RIFS:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Link Integration:	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
TDM Coordination:	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
Space In Meter:	1000	(0-15000 m)

- **A-MPDU/A-MSDU aggregation:** The data rate of your AP except wireless client mode could be enhanced greatly with this option enabled; however, if your wireless clients don't support A-MPDU/A-MSDU aggregation, it is not recommended to enable it.
- **Short GI:** Under 802.11n mode, enable it to obtain better data rate if there is no negative compatibility issue.
- **RTS Threshold:** The IEEE 802.11b/g/n Wireless CPE sends RTS (Request to Send) frames to certain receiving station and negotiates the sending of a data frame. After receiving an RTS, that STA responds with a CTS (Clear to Send) frame to acknowledge the right to start transmission. The setting range is 0 to 2346 in byte. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.

- **Fragment Threshold:** Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Leave it at its default of 2346 is recommended.
- **Beacon Interval:** Specify the frequency interval to broadcast packets. Enter a value between 20 and 1024.
- **DTIM Interval:** DTIM, which stands for Delivery Traffic Indication Message, is contained in the data packets. It is for enhancing the wireless transmission efficiency. The default is set to 1. Enter a value between 1 and 255.
- **Preamble Type:** It defines some details on the 802.11 physical layer. “Long” and “Auto” are available.
- **IGMP Snooping:** Available in AP/Router mode, IGMP snooping is the process of listening to IGMP network traffic. By enabling IGMP snooping, the AP will listen to IGMP membership reports, queries and leave messages to identify the ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups.
- **RIFS:** RIFS (Reduced Interframe Spacing) is a means of reducing overhead and thereby increasing network efficiency.
- **Link Integration:** Available under AP/Bridge/AP repeater mode, it monitors the connection on the Ethernet port by checking “Enabled”. It can inform the associating wireless clients as soon as the disconnection occurs.
- **TDM Coordination:** Stands for “Time-Division Multiplexing Technique”, this resource reservation control mechanisms can avoid packet collisions and send the packets much more efficiently allowing for higher effective throughput rates. This function is only available in AP/CPE mode. It is highly recommended to enable TDM coordination when there are multiple CPEs needed to connect to the AP in your application.
- **Space in Meter:** To decrease the chances of data retransmission at long distance, the IEEE 802.11b/g/n Wireless CPE can automatically adjust proper ACK timeout value by specifying distance of the two nodes.
- **Traffic Shaping:** Allows the administrator to specify the incoming and outgoing traffic limit by checking “Enable Traffic Shaping”. This is only available in Router mode.

■ Enable Traffic Shaping		
Incoming Traffic Limit:	<input type="text" value="102400"/>	kbit/s
Incoming Traffic Burst:	<input type="text" value="20"/>	kBytes
Outgoing Traffic Limit:	<input type="text" value="102400"/>	kbit/s
Outgoing Traffic Burst:	<input type="text" value="20"/>	kBytes

You can set the multiple SSID to a specific VLAN.

■ Enable 802.1Q VLAN	
Management VLAN ID:	<input type="text" value="0"/>

- **Enable:** Select this option to enable 802.1Q VLAN on the enabled multiple SSID.
- **Management VLAN:** Enter the VLAN ID to set on your network.

## Change your login password

*Basic Setting > Change Password*

1. Log into the management page (see “[Access the management page](#)” on page 9).
2. Click on **Management**, and click on **Password Settings**. Click **Apply** to save changes.

<b>Current Password:</b>	<input type="text"/>
<b>New Password:</b>	<input type="text"/>
<b>Confirm Password:</b>	<input type="text"/>

- **Current Password:** Enter the current password of the access point.
- **New Password:** Enter the new password
- **Confirm Password:** Re-enter the new password to confirm.

**Note:** If you change the login password, you will need to access the management page using the new password instead of the default password “admin”.

## Access Control

### Source IP Filtering

Firewall Setting > Src IP Filtering

The Source IP Filtering gives users the ability to restrict certain types of data packets from your local network to the access point. Use of such filters can be helpful in securing or restricting your local network. Please note that this feature is only available when access point System Mode is set to **Router**.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Firewall Settings**, and click on **Src IP Filtering**. Click **Apply** to save settings.

<input type="checkbox"/> <b>Enable Source IP Filtering</b>
<b>Local IP Address:</b> <input type="text"/>
<b>Comment:</b> <input type="text"/>

- **Enable Source IP Filtering:** Check this option to enable source IP filtering
- **Local IP Address:** Enter the IP address you would like to apply the IP filtering rule.
- **Comment:** Enter any notes you would like to add to distinguish the rule.

### Destination IP Filtering

Firewall Setting > Dst IP Filtering

The destination IP filtering gives you the ability to restrict the computers in LAN from accessing certain websites in WAN according to specified IP addresses. Please note that this feature is only available when access point System Mode is set to **Router**.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Firewall Settings**, and click on **Dst IP Filtering**. Click **Apply** to save settings.

<input type="checkbox"/> <b>Enable Destination IP Filtering</b>
<b>Destination IP Address:</b> <input type="text"/>
<b>Comment:</b> <input type="text"/>

- **Enable Destination IP Filtering:** Check this option to enable source IP filtering
- **Destination IP Address:** Enter the IP address you would like to apply the destinationIP filtering rule.
- **Comment:** Enter any notes you would like to add to distinguish the rule.

### Source Port Filtering

Firewall Setting > Src Port Filtering

The source port filtering enable you to restrict certain ports of data packets from your local network to Internet through the access point. Use of such filters can be helpful in securing or restricting your local network. Please note that this feature is only available when access point System Mode is set to **Router**.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Firewall Settings**, and click on **Src Port Filtering**. Click **Apply** to save settings.

<input type="checkbox"/> <b>Enable Source Port Filtering</b>
<b>Port Range:</b> <input type="text"/> - <input type="text"/>
<b>Protocol:</b> <input type="text" value="Both"/>
<b>Comment:</b> <input type="text"/>

- **Enable Destination IP Filtering:** Check this option to enable source IP filtering
- **Port Range:** Enter the range of ports you would like to apply the source port filtering.
- **Protocol:** Select the protocol you would like to filter. From UDP, TCP or Both (UDP and TCP).
- **Comment:** Enter any notes you would like to add to distinguish the rule.

## Destination Port Filtering

Firewall Setting > Dst Port Filtering

The destination port filtering enables you to restrict certain ports of data packets from your local network to Internet through the access point. Use of such filters can be helpful in securing or restricting your local network. Please note that this feature is only available when access point System Mode is set to **Router**.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Firewall Settings**, and click on **Dst Port Filtering**. Click **Apply** to save settings.

<input type="checkbox"/> Enable Destination Port Filtering	
Port Range:	<input type="text"/> - <input type="text"/>
Protocol:	<input type="text" value="Both"/>
Comment:	<input type="text"/>

- **Enable Destination IP Filtering:** Check this option to enable source IP filtering
- **Port Range:** Enter the range of ports you would like to apply the source port filtering.
- **Protocol:** Select the protocol you would like to filter. From UDP, TCP or Both (UDP and TCP).
- **Comment:** Enter any notes you would like to add to distinguish the rule.

## Port Forwarding

Firewall Setting > Port Forwarding

The destination port filtering enables you to restrict certain ports of data packets from your local network to Internet through the access point. Use of such filters can be helpful in securing or restricting your local network. Please note that this feature is only available when access point System Mode is set to **Router**.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Firewall Settings**, and click on **Port Forwarding**. Click **Apply** to save settings.

<input type="checkbox"/> Enable Port Forwarding	
IP Address:	<input type="text"/>
Protocol:	<input type="text" value="Both"/>
Port Range:	<input type="text"/> - <input type="text"/>
Comment:	<input type="text"/>

- **Enable Destination IP Filtering:** Check this option to enable source IP filtering
- **IP Address:** Enter the IP address of the device to forward the port. (e.g. *192.168.10.101*).
- **Protocol:** Select the protocol required for your device. **TCP**, **UDP**, or you can select **Both** to choose both TCP & UDP.
- **Port Range:** Enter the port number used to access the device from the Internet.
- **Comment:** Enter any notes you would like to add to distinguish the rule.

### Example: To forward TCP port 80 to your network/IP camera

1. Make sure to configure your network/IP camera to use a static IP address or you can use the DHCP reservation feature (see "Set up DHCP reservation" on page 55).

**Note:** You may need to reference your camera documentation on configuring a static IP address.

2. Log into the management page (see "[Access the management page](#)" on page 9).
3. Click on **Firewall Settings** on the side, click on **Port Forwarding**.
4. Under **IP Address**, enter the IP address assigned to the camera. (e.g. *192.168.10.101*)
5. To save changes, click **Save** at the bottom of the page.

## Open a device on your network to the Internet

### DMZ

Firewall Settings > DMZ Setting

You may want to expose a specific computer or device on your network to the Internet to allow anyone to access it. Your router includes the DMZ (demilitarized zone) feature that makes all the ports and services available on the WAN/Internet side of the router and forwards them to a single IP address (computer or network device) on your network. The DMZ feature is an easy way of allowing access from the Internet however, it is also very **insecure** method.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Firewall Settings**, and click on **DMZ Setting**. Click **Apply** to save settings.

<input type="checkbox"/> <b>Enable DMZ</b>
DMZ Host IP Address: <input type="text" value="0.0.0.0"/>

- **Enable DMZ:** Check this option to enable DMZ
- **DMZ Host IP Address:** Enter the IP address you would like to apply DMZ.

### UDP Pass through

Firewall Settings > UDP Pass through

You may want to expose a specific computer or device on your network to the Internet to allow anyone to access it. Your router includes the DMZ (demilitarized zone) feature that makes all the ports and services available on the WAN/Internet side of the router and forwards them to a single IP address (computer or network device) on your network. The DMZ feature is an easy way of allowing access from the Internet however, it is also very **insecure** method.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Firewall Settings**, and click on **UDP Pass through**. Click **Apply** to save settings.

<input type="checkbox"/> <b>Enable UDP Pass through</b>
---

- **Enable UDP Pass through:** Check this option to enable UDP Pass through

### Configure your log

Tool Settings > System Log

You may want send your router log to your e-mail address or to an external log server (also known as Syslog server) so you can check it periodically while away from home. You may also want to only see specific categories of logging.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Tools**, and click on **System Log**. Click **Apply** to save settings.

<input type="checkbox"/> <b>Enable Remote Syslog Server</b>
IP Address: <input type="text" value="0.0.0.0"/>
Port: <input type="text" value="514"/>

- **Enable Remote Syslog Server:** Check this option to enable DMZ
- **IP Address:** enter the IP address (e.g. 192.168.10.250) of the external log server to send
- **Port:** Enter the port used on your log server.

### View your log

Tool Settings > System Log



You may want send your router log to your e-mail address or to an external log server (also known as Syslog server) so you can check it periodically while away from home. You may also want to only see specific categories of logging.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Tools**, and click on **System Log**. Click **Apply** to save settings.

#	Time	Source	Message
1	2009-12-31 23:59:53	00:19:70:79:FD:33	WLAN service stopped.
2	2009-12-31 23:59:53	00:19:70:79:FD:33	WLAN service started.
3	2009-12-31 23:59:54	00:19:70:79:FD:33	WLAN service stopped.
4	2009-12-31 23:59:54	00:19:70:79:FD:33	WLAN service started.
5	2010- 1- 1 00:01:43	192.168.10.20	WEB: Authorized user "admin".

- **Time:** Displays the date and time of the log entry. If the time is inaccurate, make sure to set the router date and time correctly. (See "[Setting time](#)" on page 51)
- **Source:** Source of the log entry
- **Message:** Displays the log message.
- **Refresh:** Click to refresh the displayed log entries
- **Clear:** Click to clear all current log entries

## Ping Watchdog

### Ping Watchdog

*Tools > Ping Watchdog*

You may want to expose a specific computer or device on your network to the Internet to allow anyone to access it. Your router includes the DMZ (demilitarized zone) feature that makes all the ports and services available on the WAN/Internet side of the router and forwards them to a single IP address (computer or network device) on your

network. The DMZ feature is an easy way of allowing access from the Internet however, it is also very **insecure** method.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Tools**, and click on **Ping Watchdog**. Click **Apply** to save settings.

<input type="checkbox"/>	<b>Enable Ping Watchdog</b>
<b>IP Address to Ping:</b>	<input type="text" value="0.0.0.0"/>
<b>Ping Interval:</b>	<input type="text" value="300"/> seconds
<b>Startup Delay:</b>	<input type="text" value="120"/> seconds(>120)
<b>Failure Count To Reboot:</b>	<input type="text" value="300"/>

- **Enable Ping Watchdog:** Check this option to enable option
- **IP Address to Ping:** Enter the IP address of the remote unit to ping
- **Ping Interval:** Enter the time interval in seconds to ping the remote unit
- **Startup Delay:** Enter the startup delay time in seconds to prevent the reboot before the access point is initialized
- **Failure Count To Reboot:** Enter the count value of when the access point will reboot automatically

## WDS Data Rate Test

*Tool > Data Rate Test*

For troubleshooting purposes, you may want to check your WDS connectivity using the data rate test tool on your router management page. Please note that this option is only available when Bridge Mode is selected.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Tools**, and click on **Data Rate Test**.

	Index	MAC Address
⊙	1	00:19:70:86:8c:80

3. Select the WDS Node you would like to test.
4. Click **Start** to begin test and **Stop** to end test. If you cannot find your remote device click **Refresh**.

## Antenna Alignment

Tool > Antenna Alignment

Under Bridge mode, when the bridges are not easily visible from the location where the dish will be installed, the antenna alignment tool can help you evaluate the position of the unit and adjust the angle of the antenna more precisely. Keep it in mind that additional factors should be taken into account when your unit is installed. These factors include various obstacles (buildings, trees), the landscape, the altitude, transponder orientation, polarization, etc. To use the tool, select the desired remote access point and click "Start", the web page will display the measured signal strength, RSSI and transmit/receive packets. If the signal quality is not quite good, try to adjust the antenna and see if the quality improves or not. Please note that this option is only available when Bridge mode is enabled.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Tools**, and click on **Antenna Alignment**.

	Index	MAC Address
⊙	1	00:19:70:86:8c:80

3. Select the remote access point you are configuring.
4. Click **Start** to begin test. If you cannot find your remote device click **Refresh**.

## Speed Test

Tool > Speed Test

The speed test is to monitor the current data transmission (TX) and data reception (RX) rate with the remote access point. Enter the IP address of the remote access point, type in the user name/password and click "**Test**". The result will display in the bottom **STATUS**. You may test single TX/RX or bi-direction.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Tools**, and click on **Speed Test**.

Destination IP:	<input type="text"/>
User Name:	<input type="text"/>
Password:	<input type="text"/>
Direction:	Transmit ▾

- **Destination IP:** Enter the IP address of the remote access point
- **Username:** Enter the username of the remote access point
- **Password:** Enter the password information for the remote access point
- **Direction:** Select the direction you would like to test with the remote access point.

## Remote Management

Management > Remote Management

The access point provides a variety of remotes managements tools including Telnet, SNMP, FTP, SSH, HTTPS and exclusive WISE tool, making configuration more convenient and secure.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Management**, and click on **Remote Management**.

Management Privacy Mode		
<input checked="" type="radio"/> Normal <input type="radio"/> Secure <input type="radio"/> Customized		
<input checked="" type="checkbox"/> Telnet	<input checked="" type="checkbox"/> SNMP	<input checked="" type="checkbox"/> FTP
<input type="checkbox"/> SSH	<input type="checkbox"/> Force HTTPS	<input checked="" type="checkbox"/> WISE

3. Select the management mode you would like to use. Click **Apply** to save settings.

- **Normal:** Select this mode to activate Telnet, SNMP and FTP
- **Secure:** Select this mode to activate SSH, HTTPS, and WISE
- **Customized:** Select this mode to manually choose the management modes

4. If SNMP is one of the management tools you have selected. You will need to complete the below settings.

SNMP Settings	
Protocol Version:	V2 ▾
Server Port:	161
Get Community:	public
Set Community:	private
Trap Destination:	0.0.0.0
Trap Community:	public
Location:	

- **Protocol Version:** Select from the pull down menu the SNMP version to use.
- **Server Port:** Enter the your SNMP server port
- **Get Community:** Enter the password for the incoming Get and GetNext requests from the management station
- **Set Community:** Specify the password for the incoming Set requests from the management station.
- **Trap Destination:** Specify the IP address of the station to send the SNMP traps to.
- **Trap Community:** Specify the password sent with each trap to the manager.

To use SNMP V3, click the option “Configure SNMPv3 User Profile” to display the configuration settings.

<input checked="" type="checkbox"/> Enable SNMPv3Admin	
User Name:	SNMPv3Admin
Password:	••••••
Confirm Password:	••••••
Access Type:	Read/Write ▾
Authentication Protocol:	MD5 ▾
Privacy Protocol:	None ▾
<input checked="" type="checkbox"/> Enable SNMPv3User	
User Name:	SNMPv3User
Password:	••••••
Confirm Password:	••••••
Access Type:	Read Only ▾
Authentication Protocol:	MD5 ▾
Privacy Protocol:	None ▾

- **User Name:** Specify a user name for the SNMPv3 administrator or user. Only the SNMP commands carrying this user name are allowed to access the access point
- **Password:** Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access the access point
- **Confirm Password:** Input password again to confirm
- **Access Type:** Select “Read Only” or “Read and Write” accordingly.
- **Authentication Protocol:** Select an authentication algorithm. SHA authentication is stronger than MD5 but is slower.
- **Privacy Protocol:** Specify the encryption method for SNMP communication. None and DES are available.
  - **None:** No encryption is applied.
  - **DES:** Data Encryption Standard, it applies a 58-bit key to each 64-bit block of data.

## Coovachili

Management > Coovachili Settings

Coovachilli is a captive portal management which allows WLAN users to easily and securely access the Internet. Under Router mode, when Coovachilli is enabled, the IEEE 802.11b/g/n Wireless Access Point will force an HTTP client on a network to see a special web page (usually for authentication purposes) before using the Internet normally. At that time the browser is redirected to a web page which may require authentication. Captive portals are used at most Wi-Fi hotspots. Therefore, to use Coovachilli, you need to find Coovachilli service providers that have the additional services needed to make Coovachilli work.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Management**, and click on **CoovaChili Settings**.
3. Select Coovachilli Enable to turn on feature.

<input checked="" type="checkbox"/> Coovachilli Enable
--

4. Configure the settings below and click **Apply** to save settings.

RADIUS Settings	
Primary RADIUS Server:	radius1.coova.net
Secondary RADIUS Server:	radius2.coova.net
RADIUS Auth Port:	1812
RADIUS Acct Port:	1813
RADIUS Shared Secret:	.....
RADIUS NASID:	your-radius-nasid

### Radius Settings

- **Primary Radius Server:** Enter the name or IP address of the primary radius server
- **Secondary Radius Server:** Enter the name or IP address of the primary radius server if any.
- **Radius Auth Port:** Enter the port number for authentication

- **Radius Acct Port:** Enter the port number for billing
- **Radius Shared Secret:** Enter the secret key of the radius server
- **Radius NAS ID:** Enter the name of the radius server if any

RADIUS Administrative-User	
RADIUS Admin Username:	your-admin-username
RADIUS Admin Password:	.....

### Radius Administrative-User

- **Radius Admin Username:** Enter the username of the Radius Administrator
- **Radius Admin Password:** Enter the password of the Radius Administrator

Captive Portal	
UAM Portal URL:	https://www.coova.net/h
UAM Secret:	.....

### Captive Portal

- **UAM Portal URL:** Enter the address of the UAM portal server
- **UAM Secret:** Enter the secret password between the redirect URL and the Hotspot.

## Upgrade Firmwre

Management > Firmware Upload

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

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Management**, and click on **Firmware Upload**.

3. Click **Browse** and select the updated firmware file you want to load. Click **Upload** to load the firmware file.

**Note:** Any interruption during the firmware upgrade can damage your device.

## Backup and restore your router configuration settings

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

### To back up your configuration:

*Management > Configuration File*

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Management**, and click on **Configuration File**.

3. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: *config.bin*)
4. Save the configuration file to location on your computer.

### To restore your router configuration and upgrade firmware

*Management > Configuration File*

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Management**, and click on **Configuration File**.

3. Under **Load Settings from file**, click on **Browse** select your saved configuration file and click **Upload**.

### Reboot your access point

*Management > Configuration File*

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

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

- **Disconnect the power adapter** – Located on the rear panel of your router, see "Product Hardware Features" on page 4 .

Use this method if you are encountering difficulties with accessing your router management page. This is also known as a hard reboot or power cycle.

Disconnect the power adapter from the power port of your router for 10 seconds, then, plug the power adapter back into the power of your router. Wait for your router Status light to begin flashing.

OR

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

*Toolbox > Reboot*

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Management**, and click on **Configuration File**.

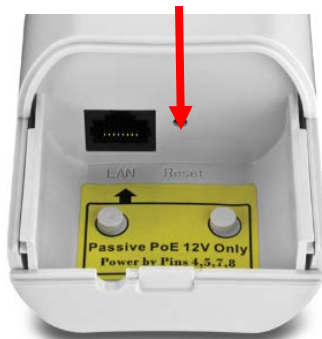
3. Click Yes or OK if prompted to your reboot your device.

## Reset to factory defaults

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting. Before you reset your router to defaults, if possible, you should backup your router configuration first, see “Backup and restore your router configuration settings” on page 70.

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

- **Reset Button** – Located on the bottom panel of the access point, cap must be removed to access reset button. Use this method if you are encountering difficulties with accessing your router management page. Push and hold this button for 15 seconds and release to reset your router to its factory defaults.



Bottom cap remove

OR

- **Router Management Page**

*Management > Configuration File*

1. Log into the management page (see “[Access the management page](#)” on page 9).
2. Click on **Management**, and click on **Configuration File**.

Reboot The Device:

3. You will be prompted to reset your router to factory defaults. Click **Yes** or **OK**.

## Certificate configuration settings

*Management > Certificate Settings*

Under Client mode, when EAP-TLS is used, the RADIUS server must know which user certificates to trust. The Server can trust all certificates issued by a given CA.

To import a user certificate, from Import User Certificates, click “**Browse**” and specify the location where the user certificate is placed. Click “**Import**”.

1. Log into the management page (see “[Access the management page](#)” on page 9).
2. Click on **Management**, and click on **Certificate Settings**.

Delete User Certificate:	<input type="text"/>	<input type="button" value="Delete"/>
Import User Certificates:	<input type="text"/> <input type="button" value="Browse..."/>	<input type="button" value="Import"/>

- **Delete User Certificate:** Select from the pull down menu the certificate would like to delete and deactivate. Press **Delete** to proceed.
- **Import User Certificate:** Click Browse and select the user certificate you want to load to the access point. Click **Import** to load the certificate.

## Device Information

*Status > Information*

Under Client mode, when EAP-TLS is used, the RADIUS server must know which user certificates to trust. The Server can trust all certificates issued by a given CA.

To import a user certificate, from Import User Certificates, click “**Browse**” and specify the location where the user certificate is placed. Click “**Import**”.

1. Log into the management page (see “[Access the management page](#)” on page 9).
2. Click on **Status**, and click on **Information**.

System Information	
Device Name	ap79fd33
Country/Region	United States
Firmware Version	1.02

### System Information

- **Device Name:** Name of device
- **Country/Region:** Applied country/region
- **Firmware Version:** Current firmware version of the access point.

WAN(Ethernet) Settings	
Connection Time	---
Access Type	Static IP <input type="button" value="Connect"/>
IP Address	192.168.10.100
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS1	0.0.0.0
DNS2	0.0.0.0
MAC Address	00:19:70:79:fd:33

### WAN Settings

Information is based on the mode settings applied to the access point and when System mode is to **Router**.

- **Connection Time:** Display time duration of when the WAN has established connection
- **Access Type:** Display the WAN connection type
- **IP Address:** Current assigned WAN IP address
- **Subnet Mask:** Assigned WAN Subnet Mask
- **Default Gateway:** Assigned WAN default gateway
- **DNS1/2:** Assigned WAN DNS IP address
- **MAC Address:** Displays the MAC address of the access points WAN port

LAN(Wireless) Settings	
IP Address	192.168.0.99
Subnet Mask	255.255.255.0
MAC Address	00:19:70:79:fd:33

### LAN Settings

Information is based on the **Wireless** mode setting applied to the access point.

- **IP Address:** LAN IP address of your access point
- **Subnet Mask:** Subnet Mask of your Local Area Network (LAN)
- **MAC Address:** Displays the MAC address of your access points Local Area Network (LAN)
- **Connection Time:** Display time duration of when the WAN has established connection
- **Access Type:** Display the WAN connection type
- **IP Address:** Current assigned WAN IP address
- **Subnet Mask:** Assigned WAN Subnet Mask
- **Default Gateway:** Assigned WAN default gateway
- **DNS1/2:** Assigned WAN DNS IP address

#### MAC Address:

- elect from the pull down menu the certificate would like to delete and deactivate. Press **Delete** to proceed.

## Associated Information

### *Status > Connections*

Open "**Connections**" in "**Status**" to check the information of associated wireless devices such as MAC address, signal strength, connection time, IP address, etc. All is read only. Click "**Refresh**" at the bottom to update the current association list. By clicking on the MAC address of the selected device on the web you may see more details including device name, connection time, signal strength, noise floor, ACK timeout, link quality, IP information, current data rate, current TX/RX packets.

1. Log into the management page (see "[Access the management page](#)" on page 27).
2. Click on **Status**, and click on **Connections**.

VAP Index	MAC Address	Signal Strength	Noise Floor	Connection Time	Last IP	Action
---	---	---	---	---	---	---

- **Refresh:** Click to refresh to view the current information

## Statistics

Status > Statistics

You may want to check the statistical received and transmit packets of the wired and wireless connections of the access point.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Status**, and click on **Statistics**.

	Received	Transmitted
<b>Wireless</b>		
Unicast Packets	0	0
Broadcast Packets	0	428
Multicast Packets	0	710
Total Packets	0	1138
Total Bytes	0	99854
<b>Ethernet</b>		
Total Packets	3839	5338
Total Bytes	471923	3426810

- **Refresh:** Click to refresh to view the current information

**Poll Interval:**  (0-65534) sec

- **Poll Interval:** Specify the refresh time interval in the box beside "**Poll Interval**" and click "**Set Interval**" to save settings. "**Stop**" helps to stop the auto refresh of network flow statistics.

## ARP Table

Status > ARP Table

You may want to view the access point's current ARP table.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Status**, and click on **ARP Table**.

IP Address	MAC Address	Interface
192.168.10.213	1C:C1:DE:0C:F6:38	br0

- **Refresh:** Click to refresh to view the current information

## Bridge Table

Status > Bridge Table

This page allows you to view any active bridge connections to the access point.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Status**, and click on **Bridge Table**.

MAC Address	Interface	Ageing Timer(s)
1c:c1:de:0c:f6:38	LAN	0.00
00:19:70:86:8c:80	Bridge	---

- **Refresh:** Click to refresh to view the current information



## DHCP Clients

Status > DHCP Clients

This page displays the access point's current DHCP clients.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Status**, and click on **DHCP Clients**.

IP Address	MAC Address	Time Expired(s)
None	---	---

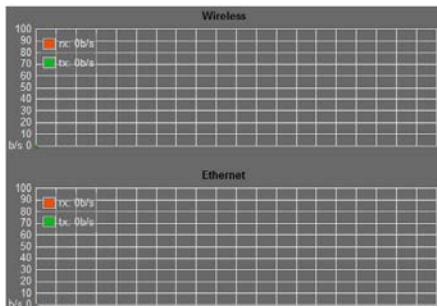
- **Refresh:** Click to refresh to view the current information

## Network Activity

Status > Network Activity

The network activities allows you to monitor the current Wireless and Ethernet TX/RX data traffic in graphical and numerical form on the Web of the Skyport. The chart scale and throughput dimension (Bps, Kbps, Mbps) changes dynamically according to the mean throughput value.

1. Log into the management page (see "[Access the management page](#)" on page 9).
2. Click on **Status**, and click on **Network Activity**.



- **Refresh:** Click to refresh to view the current information

## Additional hardware installation

### Ground wire

When placing your device out in an open area where lightning strikes can occur, it is advisable to ground it. This would protect your device from being damage and your network.

1. Loosen and remove the metal O-Ring connected below the optional external N-Type antenna connector



2. Place the grounding wire into the connector and tighten the O-Ring



3. Connect the end of the grounding wire to a grounding area. e.g Earth driven rod of grounded system.

## Using the optional external antenna

The access point offers the use of an optional external antenna. This allows you to use an Omni-Type antenna instead of the built in directional antenna.

**Note:** When using the optional external antenna, you must just the antenna settings on the access point to External N-Type. Please refer to the operation mode types you are using for additional information.

1. Remove the black rubber cap off the access point.



2. Connect and fasten tightly your N-Type antenna connector to the access point.



## Pole mounting

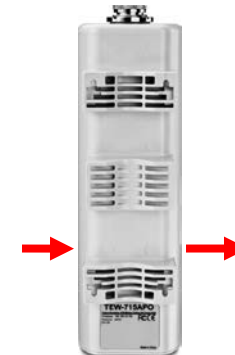
The access point comes with a pole mounting clamp that allows you to mount the device to a pole.

**Note:** The mounting clamp supports up to 63mm diameter.

1. Loosen the pole mounting clamp by turn the bolt in of the clamp counter clock wise



2. Insert one end of the clamp through the back (center section) of the access point.



3. Align the access point to the pole and tighten up the clamp till the access point is secured on the pole.



## Access Point Management Page Structure

### Status

- Information
- Connections
- Statistics
- ARP Table
- Bridge Table
- DHCP Client
- Network Activity

### System

- Device Settings
  - Mode
    - Router
    - Bridge
- GPS Coordinate Settings
- Network Settings
  - WAN Settings
  - LAN Settings
  - DHCP

- Time Settings
- RADIUS Settings

### Wireless

- Basic Settings
  - Operation Mode
    - AP
    - Wireless Client
    - Bridge
    - AP Repeater
- Profile Settings
- Advanced Settings
- Access Control
- WDS Settings

### Management

- Remote Settings
- CoovaChilli Settings
- Firmware Upload
- Configuration File

- Password Settings
- Certificate Settings

### Tools

- System Log
- Site Survey
- Ping Watchdog
- Data Rate Test
- Antenna Alignment
- Speed Test

### Firewall Settings

- Src IP Filtering
- Dst IP Filtering
- Src Port filtering
- Dst Port Filtering
- Port Forwarding
- UDP Pass Through
- DMZ Setting

## Technical Specifications

Hardware	
<b>Standards</b>	Wired: IEEE 802.3u Wireless: IEEE 802.11b, IEEE 802.11g, Based on IEEE 802.11n technology
<b>LED Indicator</b>	Power, LAN, WLAN
<b>Antenna</b>	8dBi directional antenna
<b>EXT (external antenna connector)</b>	N-Type Female connector (up to 15dBi)
<b>PoE</b>	12V 1 x 10/100Mbps RJ-45 PoE port, Passive only (non-802.3af compliant)
<b>Dimension (L x W x H)</b>	228 x 64 x 61 mm (9.0 x 2.5 x 2.4 in)
<b>Weight</b>	500g (17.6 oz)
<b>Power Consumption</b>	12 Watts (max.)
<b>Management</b>	Web browser (HTTP/HTTPS), SNMP (v2c and 3), Telnet, SSH
<b>Waterproof</b>	IP55 compliant
<b>Temperature</b>	Operating: -20° ~ 70°C (-4°F ~ 158°F) Storage: -30° ~ 80°C (-22°F ~ 176°F)
<b>Humidity</b>	Max. 95% (non-condensing)
<b>Power</b>	Passive PoE power injector DC Output: 12VDC, 1A Input: 100 –240V ~50/60Hz 1A
<b>Certifications</b>	CE, FCC
Wireless	
<b>Frequency</b>	FCC: 2.412 ~ 2.452 ETSI: 2.412 ~ 2.472
<b>Modes</b>	Access Point, CPE, Wireless Client AP, AP + Repeater

<b>Virtual Access Points</b>	16
<b>Associated Clients (max)</b>	32 (AP Mode), 32 (Repeater Mode)
<b>*Coverage</b>	10km line-of-sight
<b>Modulation Technique</b>	OFDM, BPSK, QPSK, CCK, DQPSK, DBPSK
<b>Data Rate (auto-fallback)</b>	802.11b: up to 11Mbps 802.11g: up to 54Mbps 802.11n: up to 135Mbps
<b>Security</b>	64/128/152-bit WEP, WPA /WPA2-PSK, WPA/WPA2-RADIUS for AP/CPE mode, WEP/WPA2-PSK for WDS mode MAC filter (32 entries)
<b>Output Power</b>	802.11b: 26dBm (typical) 802.11g: 24dBm (typical) 802.11n: 21dBm (typical)
<b>Receiving Sensitivity</b>	802.11b: -88dBm (typical) @ 11Mbps 802.11g: -73dBm (typical) @ 54Mbps 802.11n: -67dBm (typical) @ 150Mbps
<b>Channels</b>	FCC: 1~11 ETSI: 1~13

\*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.

## Troubleshooting

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

**Answer:**

1. Check your hardware settings again and that all cables are properly connected
2. Make sure the LAN and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set in the subnet class as the access point when accessing with a static IP address or [Obtain an IP address automatically](#) (see the steps below).
4. Press on the factory reset button for 15 seconds, the release.

### Windows 7

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

### Windows Vista

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

### Windows XP/2000

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

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

**Q: I am connected to the access point and able to pull DHCP from my network, but I cannot get onto the Internet. What should I do?**

**Answer:**

1. Verify that you can get onto the Internet with a direct connection into your router (meaning plug your computer directly to the router and verify that your single computer can access the Internet).
2. Power cycle your modem and router. Unplug the power to the modem and router. Wait 30 seconds, and then reconnect the power to the modem. Wait for the modem to fully boot up, and then reconnect the power to the router.
3. Contact your ISP and verify all the information that you have in regards to your Internet connection settings is correct.

**Q: I cannot connect wirelessly to the access point. What should I do?**

**Answer:**

1. Double check that the WLAN light on the router is lit.
2. Power cycle the access point. Unplug the power to the router. Wait 15 seconds, then plug the power back in to the router.
3. Contact the manufacturer of your wireless network adapter and make sure the wireless network adapter is configured with the proper SSID. The preset SSID is TRENDnet (*model\_number*).
4. Please see "Wireless Performance Consideration" if you continue to have wireless connectivity problems.

## Appendix

### How to find your IP address?

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

#### Command Prompt Method

##### **Windows 2000/XP/Vista/7**

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.
2. In the dialog box, type **cmd** to bring up the command prompt.
3. In the command prompt, type **ipconfig /all** to display your IP address settings.

##### **MAC OS X**

1. Navigate to your **Applications** folder and open **Utilities**.
2. Double-click on **Terminal** to launch the command prompt.
3. In the command prompt, type **ipconfig getifaddr <en0 or en1>** to display the wired or wireless IP address settings.

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

#### Graphical Method

##### **MAC OS 10.6/10.5**

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

##### **MAC OS 10.4**

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

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

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

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

#### **Windows 7**

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

#### **Windows Vista**

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

#### **Windows XP/2000**

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

#### **MAC OS 10.4/10.5/10.6**

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

In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Using DHCP** and click the **Apply Now** button.

In MAC 10.5, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.

In MAC 10.6, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.

f. Restart your computer.

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

### How to find your MAC address?

In Windows 2000/XP/Vista/7,

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

In MAC OS 10.4,

1. **Apple Menu > System Preferences > Network**
2. From the **Show** menu, select **Built-in Ethernet**.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.



In MAC OS 10.5/10.6,

1. **Apple Menu > System Preferences > Network**
2. Select **Ethernet** from the list on the left.
3. Click the **Advanced** button.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.


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

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

#### Windows 7

1. Open Connect to a Network by clicking the network icon ( or ) in the notification area.
2. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect**.
4. You may be prompted to enter a security key in order to connect to the network.
5. Enter in the security key corresponding to the wireless network, and click **OK**.

#### Windows Vista

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

#### Windows XP

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

## **Internet service types**

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

### **1. Obtain IP Address Automatically (DHCP)**

Host Name (Optional)

Clone Mac Address (Optional)

### **2. Fixed IP address**

WAN IP Address: \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_.  
(e.g. 215.24.24.129)

WAN Subnet Mask: \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_.  
(e.g. 255.255.255.0)

WAN Gateway IP Address: \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_.  
(e.g. 215.24.24.1)

DNS Server Address 1: \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_.  
(e.g. 209.17.172.20)

DNS Server Address 2: \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_.  
(e.g. 209.17.172.20)

### **3. PPPoE to obtain IP automatically**

User Name: \_\_\_\_\_

Password: \_\_\_\_\_

Verify Password: \_\_\_\_\_

### **4. PPPoE with a fixed IP address**

User Name: \_\_\_\_\_

Password: \_\_\_\_\_

Verify Password: \_\_\_\_\_

IP Address: \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_\_. (e.g. 215.24.24.129)



### Federal Communication Commission Interference Statement

---

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

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

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

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

#### FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To avoid the possibility of exceeding radio frequency exposure limits, you shall keep a distance of at least 100cm between you and the antenna of the installed equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

FCC NOTICE: To comply with FCC part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification.

It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly forbidden.

### Europe – EU Declaration of Conformity

---



### Copyright

---

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

Copyright 2006

### Trademark recognition

---

All product names used in this manual are the properties of their respective owners and are acknowledged.

### Limited Warranty

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

#### TEW-715APO – 3 Years Warranty

AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1 year warranty.

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

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

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

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

**WARRANTIES EXCLUSIVE:** IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

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

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

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

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

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

PWP05202009v2

2012/10/30



## 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