



TRENDNET[®]



User's Guide

TEW-637AP
3.01

Federal Communication Commission Interference Statement

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

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

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

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- **EN60950-1:2006**
Safety of Information Technology Equipment
- **EN50385 : (2002-08)**
- Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public
- **EN 300 328 V1.7.1: (2006-10)**
- Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- **EN 301 489-1 V1.8.1: (2008-04)**
- Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17 V1.3.2 (2008-04)**
- Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for 2,4 GHz wideband transmission systems, 5 GHz high performance RLAN equipment and 5,8 GHz Broadband Data Transmitting Systems
-

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

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

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



 Český [Czech]	<i>TRENDware</i> tímto prohlašuje, že tento TEW-637AP je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede <i>TRENDware</i> erklærer herved, at følgende udstyr TEW-637AP overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erkläre <i>TRENDware</i> , dass sich das Gerät TEW-637AP in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab <i>TRENDware</i> seadme TEW-637AP vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, <i>TRENDware</i> declares that this TEW-637AP is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente <i>TRENDware</i> declara que el TEW-637AP cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>TRENDware</i> ΔΗΛΩΝΕΙ ΟΤΙ ΤΕW-637ΑΡ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
 Français [French]	Par la présente <i>TRENDware</i> déclare que l'appareil TEW-637AP est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente <i>TRENDware</i>] dichiara che questo TEW-637AP è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
 Latvīski [Latvian]	Ar šo <i>TRENDware</i> deklarē, ka TEW-637AP atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
 Lietuvių [Lithuanian]	Šiuo <i>TRENDware</i> deklaruoja, kad šis TEW-637AP atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart <i>TRENDware</i> dat het toestel TEW-637AP in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, <i>TRENDware</i> jiddikjara li dan TEW-637AP jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, <i>TRENDware</i> nyilatkozom, hogy a TEW-637AP megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym <i>TRENDware</i>] oświadcza, że TEW-637AP jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	<i>TRENDware</i> declara que este TEW-637AP está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	<i>TRENDware</i> izjavlja, da je ta TEW-637AP v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
 Slovensky [Slovak]	<i>TRENDware</i> týmto vyhlasuje, že [typ zariadenia] spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	<i>TRENDware</i> vakuuttaa täten että TEW-637AP tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar <i>TRENDware</i> att denna TEW-637AP står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Contents

Package Contents	6
Minimum System Requirements	6
Introduction	7
Features	7
Hardware Overview	8
Hardware Overview	8
Installation Considerations	10
Getting Started	11
Using the Configuration Menu	18
Network	19
Network LAN Setting	19
Wireless	20
Wireless Basic	20
Wireless Advanced	23
MAC Filter	25
Security	26
WPS	29
Station List	29
Administrator	30
System Management	30
Upload Firmware	30
Settings Management	31
Status	31
Glossary	32
Specifications	40
Limited Warranty	41

Package Contents

- TEW-637AP
- Multi-Language Quick Installation Guide
- CD-ROM (Setup Wizard and User's Guide)
- 1 x network cable(0.6 m/ 2 ft.)
- Power adapter (12vDC 0.5A)



Using a power supply with a different voltage than the one included with your product will cause damage and void the warranty for this product.

Minimum System Requirements

Installation Requirements

- Web Browser: Internet Explorer (6 or higher) Mozilla or Safari.
- A computer with a network adapter or wireless adapter properly installed.
- CD-ROM drive
- A router with an available network LAN port.
- A RJ-45 network cable.

Introduction

The 300Mbps Wireless Easy-N-Upgrader™ upgrades your old, perfectly functioning router, to high speed wireless n. Enjoy up to 12 times the speed and 6 times the coverage of a wireless g network

Eliminate wireless dead spots, seamlessly surf the Internet and help the environment by not throwing away your old router. GREENwifi technology reduces energy consumption by up to 50%.

The compact 300Mbps Wireless Easy-N-Upgrader™ is designed around ease of use, performance and environmental friendliness. The latest in wireless encryption ensures wireless security. Advanced Multiple Input Multiple Output (MIMO) antenna technology eliminates wireless dead spots. Wireless Protected Setup (WPS) lets you integrate other WPS devices into your network quickly.

FEATURES

- 1x 10/100Mbps Ethernet port
- 1x Wi-Fi Protected Setup (WPS) button
- 2x 2dBi fixed antennas
- Compliant with IEEE 802.11n, IEEE 802.11g, & 802.11b standards
- High-speed data rates of up to 300Mbps with IEEE 802.11n*
- Compact high performance wireless n access point
- Up to 50% energy savings with GREENwifi technology
- A smaller and faster access point solution suitable for upgrading to wireless N
- Affordable wireless N device for easily migrating from wireless G and B networks
- Broadcast up to 4 SSIDs with different wireless encryption
- Supports Wireless Distribution System (WDS) to extend wireless network
- Wi-Fi Multimedia (WMM) Quality of Service (QoS) supported
- Improves the data transfer speed by working with existing wireless G and B Networks
- Wireless security support of up to WPA2-RADIUS
- Low Interference and high susceptibility guarantee reliable performance
- One-touch wireless security setup using the Wi-Fi Protected Setup (WPS) button
- Indoor coverage up to 100 meters (328ft.)*
- Outdoor coverage up to 300 meters (984ft.)*

HARDWARE OVERVIEW



Front View	<p>WLAN LED A solid light indicates that the wireless segment is ready. This LED blinks green during wireless data transmission.</p>
	<p>WPS LED This LED blinks green during WPS function is enabled.</p>
	<p>LAN LED A solid light indicates a connection to a Router on the LAN port. This LED blinks green during data transmission</p>
	<p>POWER LED A solid green light indicates a proper connection to the power supply</p>
	<p>WPS Button Press the button to enable WPS function.</p>



Rear View	<p>Auto MDI/MDIX 10/100Mbps LAN Ports This port automatically senses the cable type when connecting to Router.</p>
	<p>Reset Buttonressing the reset button restores the AP to its original factory default settings.</p>
	<p>Power Switch (EU version) On/off Switch</p>
	<p>DC-IN The DC power input connector is a single jack socket to supply power to the TEW-638APB. Please use the Power Adapter provided on the TEW-638APB package.</p>

INSTALLATION CONSIDERATIONS

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

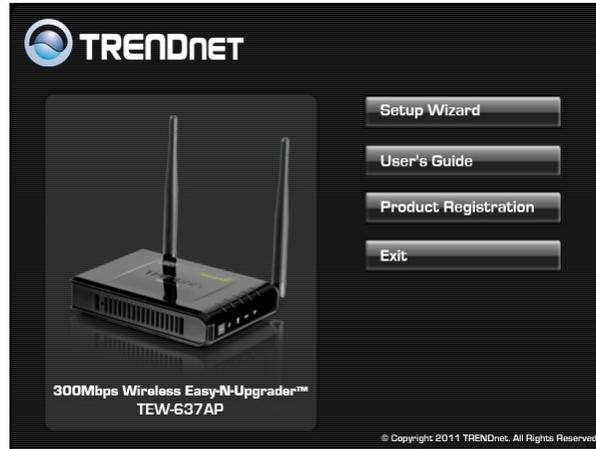
1. Adjust your wireless devices so that the signal is traveling in a straight path, rather than at an angle. The more material the signal has to pass through the more signal you will lose.
2. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position 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, please do the following:

1. Connect one end of the provided network cable into your computer's network port, and connect the other end of the provided network cable into the TEW-637AP's Ethernet port.
2. Plug the power adapter to outlay, and connect the power jack to the TEW-637AP.
3. Verify that the Power & Ethernet LEDs are lit.
4. Insert Setup Wizard CD into your CD-ROM drive.
5. The Welcome screen appears on your monitor. Click **Start** button.



6. Read the License Agreement and click **Next** to continue the installation.



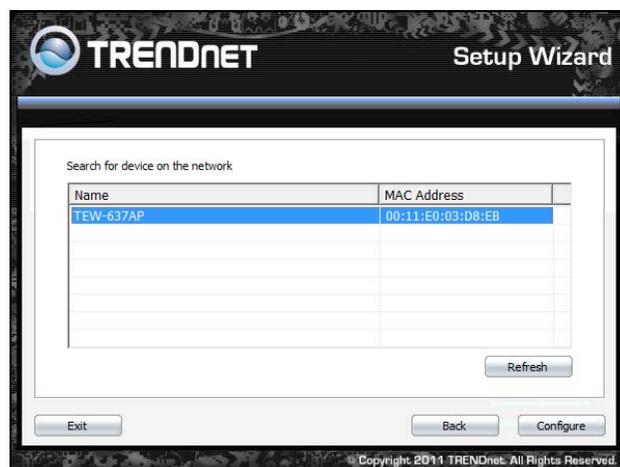
7. Connect an Ethernet cable from the LAN port on your Router to the LAN port on the TEW-638APB, click **Next button** to continue.



8. Plug in the power adapter of the TEW-638APB and plug in the device that you will be connecting together. Verify the Power & Ethernet LEDs are light. *EU Version please make sure the power switch is on the On position*



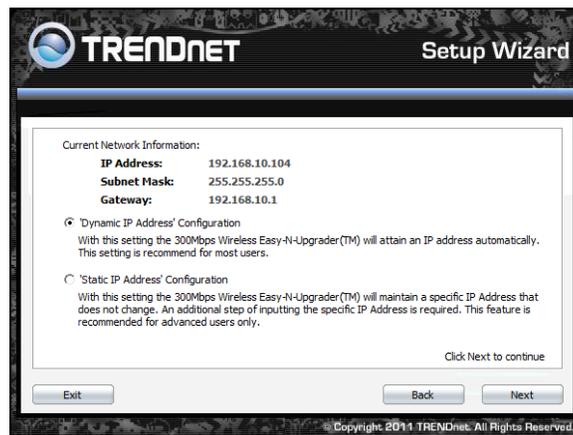
9. Your computer will detect TEW-637AP and the Device List screen appears on your monitor. Click **Configure** button to continue (default TEW-638APB IP Address is 192.168.10.100).
- 10.



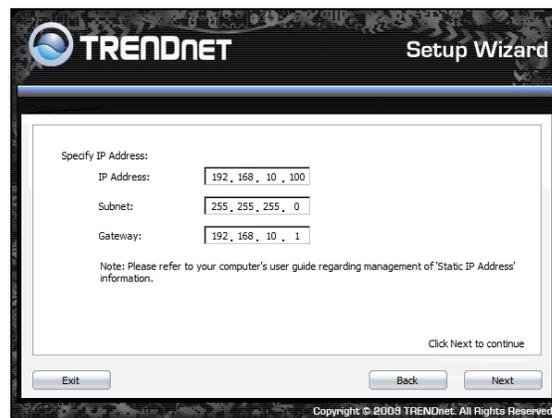
11. Enter password for the Access Point. The default password is “admin”. Click **Login** button to continue.



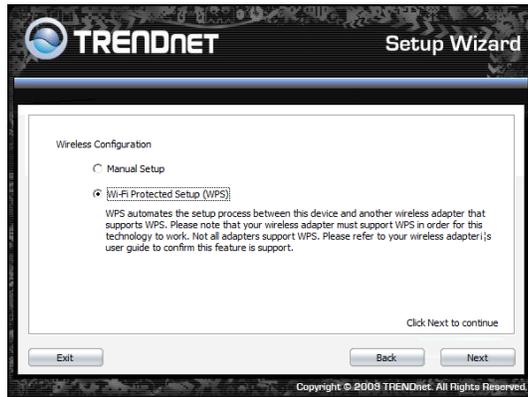
12. The default IP address is 192.168.10.100, you can choose to obtain network setting automatically, or set the IP address manually. After setting, click **Next** to continue.



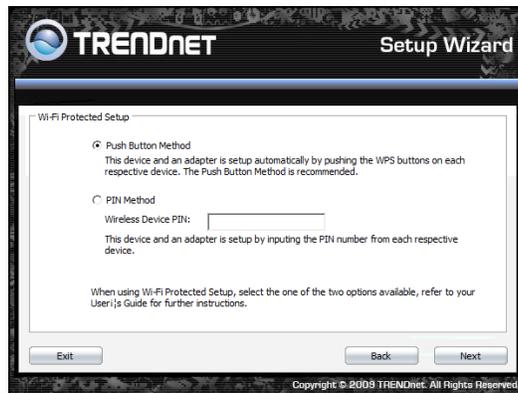
13. The default IP address is 192.168.10.100, you can choose to obtain network setting automatically, or set the IP address manually. After setting, click **Next** to continue.



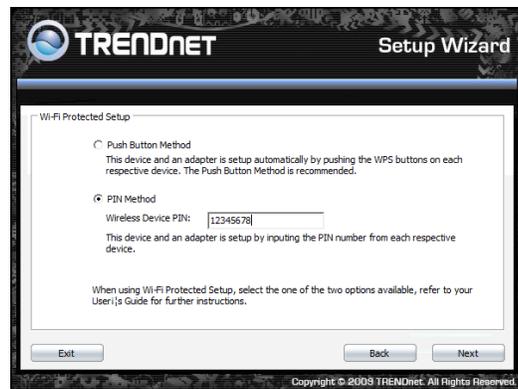
14. Select **Wi-Fi Protected Setup** to connect your wireless client device to this AP, and click **Next** button.



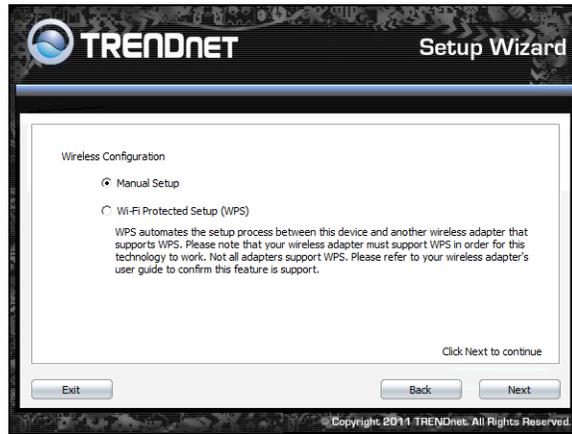
15. Use **Push Button Method**, click **Connect** button to continue. You also need to enable WPS function of the wireless client device to make connection.



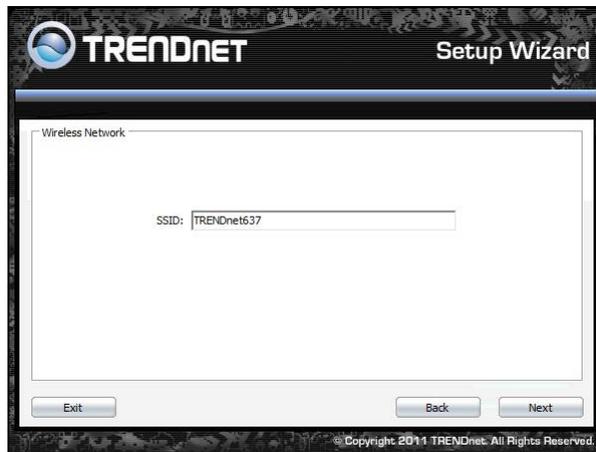
16. Use **PIN Method** and enter your wireless client PIN number on **Wireless Device PIN**, and then click **Connect** button to make wireless connection.



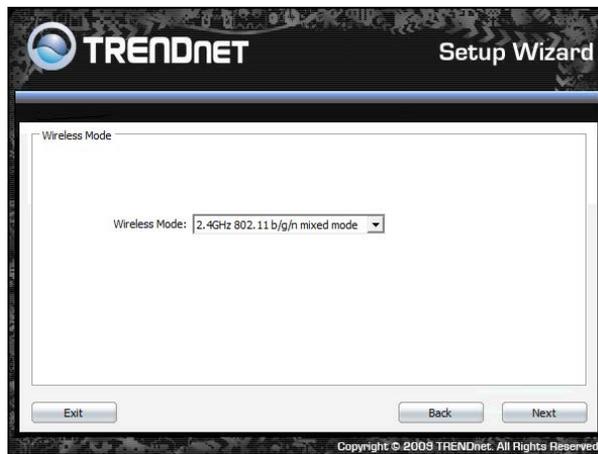
17. To set TEW-638APB security, select **Manual setup** and click **Next** button



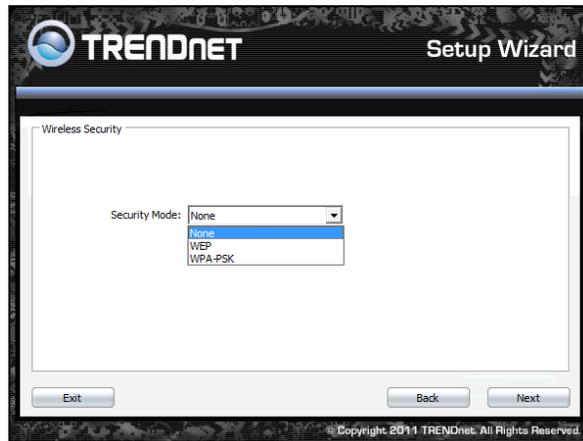
18. Enter **SSID** of TEW-638APB, click **Next** button.



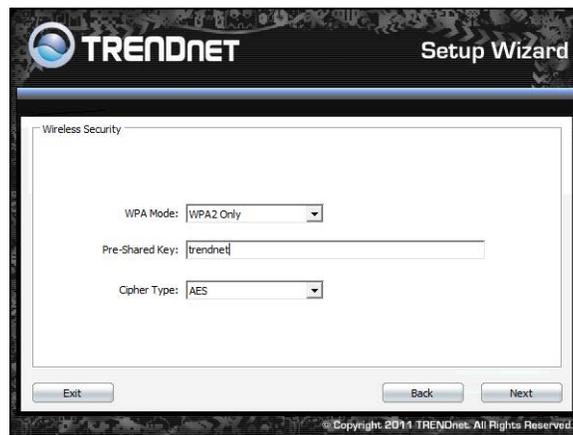
19. Choice Wireless Mode.



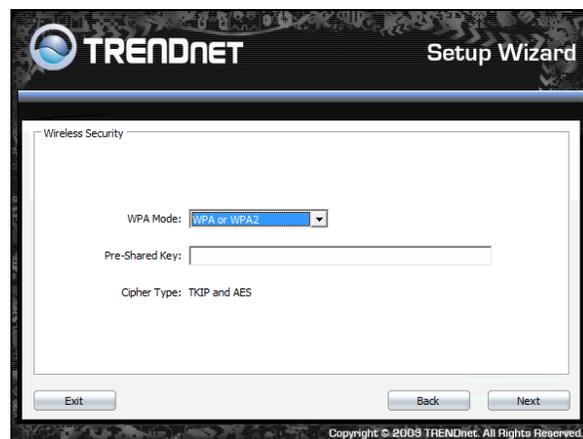
20. To disable **Security Mode**, select **None** and click **Next** button.



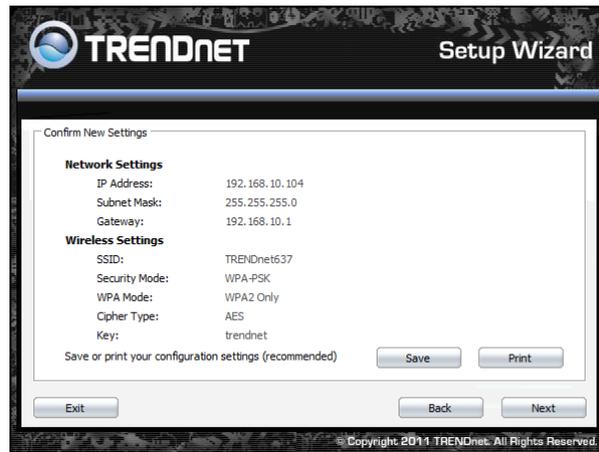
21. To use WEP security, select **WEP** and click **Next** button. Select **64-bit** or **128-bit** WEP key length, and enter your WEP key. For 64-bit encryption, enter 10 hexadecimal characters, For 128-bit encryption, enter 26 hexadecimal characters. Click **Next** to continue the setting.



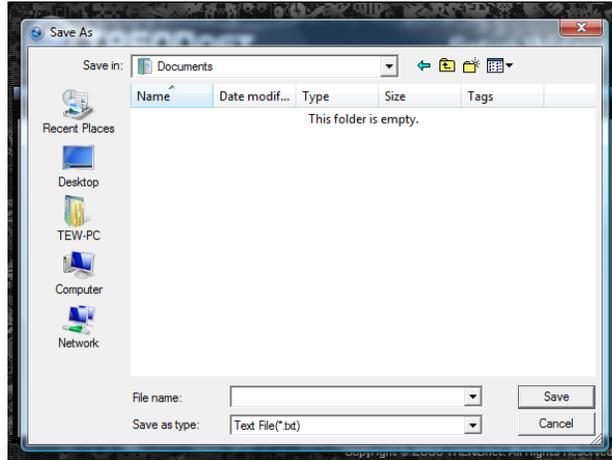
22. To use WPA or WPA2 security, select **WPA or WPA2** and click **Next** button. Select **WPA Mode: WPA Only, WPA2 Only, WPA or WPA2**, and set **Pre-Shared Key** by entering 8 ~ 63 characters. Click **Next** to continue the setting.



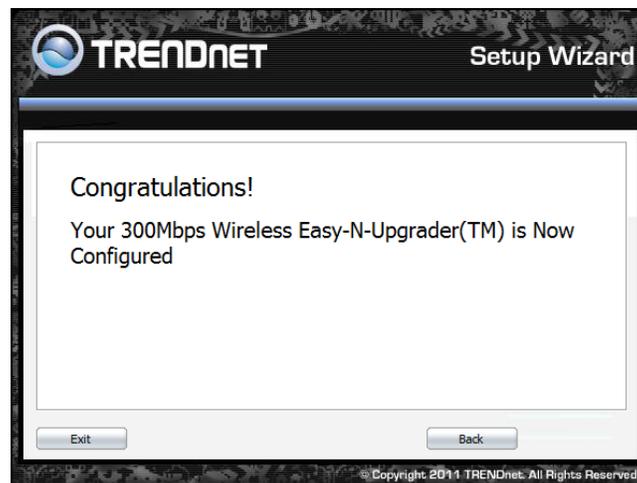
23. Confirm your new settings. It is recommended that you save or print your wireless settings with the **Save** or **Print** buttons. Once finished, click **Configure** to continue.



24. Save you setting to a text file in a desired location.



25. Congratulations you have configured you TEW-637AP.



Using the Configuration Menu

Whenever you want to configure your TEW-637AP, you can access the Configuration Menu by opening the Web-browser and typing in the IP Address of the TEW-637AP.

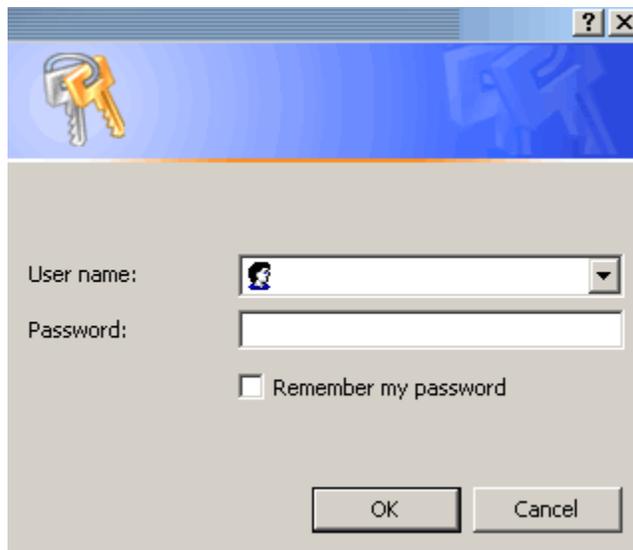
- Open the Web browser.
- Type in the current **IP Address** of the AP (i.e. <http://192.168.10.100>).



If you have changed the default IP Address assigned to the TEW-637AP, make sure to enter the correct IP Address.

NOTE

- Type **admin** in the **User Name** field.
- type the Password **admin**.
- Click **OK**.

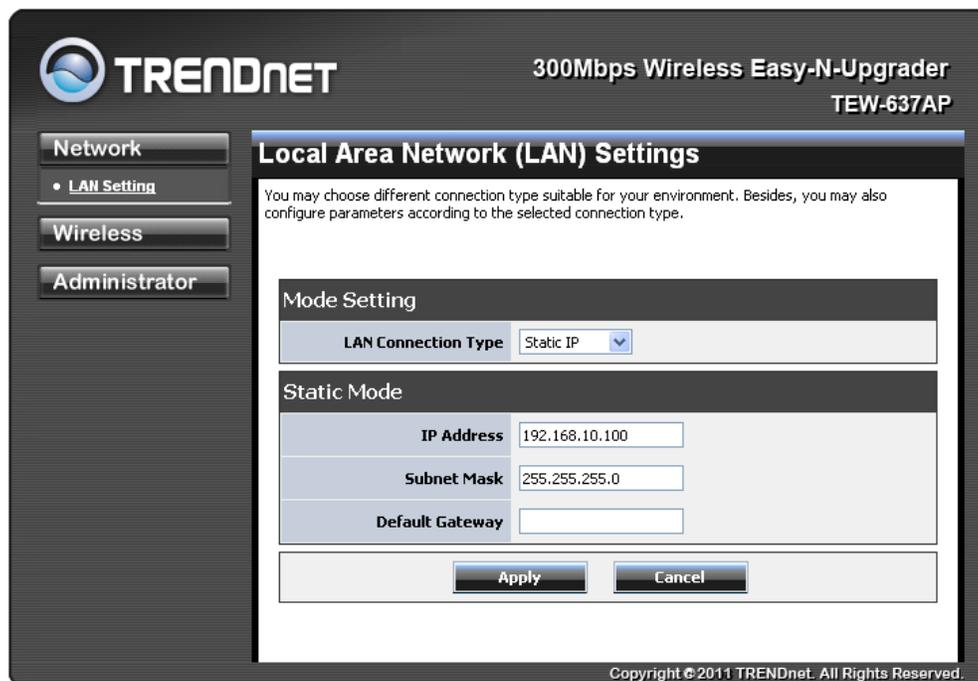


The screenshot shows a login dialog box with a blue header bar containing a key icon. The dialog has a 'User name:' label next to a text input field with a dropdown arrow. Below it is a 'Password:' label next to a text input field. A checkbox labeled 'Remember my password' is located below the password field. At the bottom, there are 'OK' and 'Cancel' buttons.

Network

The Network tab provides the following configuration options: LAN Setting.

NETWORK LAN SETTING



These are the settings of the LAN (Local Area Network) interface for the Access Point. The Access Point's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this Web-based management interface.

LAN Connection Type

Choose "**Static IP (fixed IP)**" if your router does not support DHCP or if for any other reason you need to assign a fixed address to the AP. In this case, you must also configure the following fields.

IP Address

The IP address of the AP on the local area network. Assign any unused IP address in the range of IP addresses available for the LAN. For example, 192.168.10.100.

Subnet Mask

The subnet mask of the local area network.

Default Gateway

The IP address of the router on the local area network.

Choose "**DHCP (Auto Config)**" if your router supports DHCP and you want the router to assign an IP address to the AP.

Wireless

The wireless section is used to configure the wireless settings for your Access Point. Note that changes made in this section may also need to be duplicated on wireless clients that you want to connect to your wireless network.

To protect your privacy, use the wireless security mode to configure the wireless security features.

The Wireless tab provides the following configuration options: Basic, Advanced, MAC Filter, Security, WPS and Station List.

WIRELESS BASIC

The screenshot shows the configuration interface for a TRENDnet 300Mbps Wireless Easy-N-Upgrader (TEW-637AP). The interface is divided into a left sidebar and a main content area. The sidebar includes tabs for Network, Wireless, and Administrator. The Wireless tab is active, showing a list of sub-options: Basic, Advanced, MAC Filter, Security, WPS, and Station List. The main content area is titled "Basic Wireless Settings" and contains the following configuration options:

- Wireless Network**
 - Repeater Mode Support: Enable Disable
 - Wireless Mode: 802.11 n only (dropdown)
 - Wireless Name(SSID): TRENDnet637 (text input)
 - Multiple SSID1: (text input)
 - Multiple SSID2: (text input)
 - Multiple SSID3: (text input)
 - Broadcast Network Name (SSID): Enable Disable
 - BSSID: 00:11:E0:03:D8:EB (text input)
 - Frequency (Channel): Auto (dropdown)
 - MCS: Auto (dropdown)
- Wireless Distribution System(WDS)**
 - WDS Mode: Disable (dropdown)
- HT Physical Mode**
 - Channel BandWidth: Auto 20/40MHz (dropdown)
 - Control Sideband: Upper (dropdown)

At the bottom of the configuration area are "Apply" and "Cancel" buttons. The footer of the page reads "Copyright © 2011 TRENDnet. All Rights Reserved."

Repeater Mode Support

Repeater Mode Support allows you to “repeat” a wireless signal from an existing access point.

Select the radio button to enable or disable. When enabled you have the option of defining the specific access point to repeat off of by entering in the remote access points or wireless router’s wireless MAC address into the “AP MAC Addr. (Optional)” field. You must also configure the TEW-637AP with the same SSID, channel and wireless encryption settings of the remote access point.



To repeat Wireless N Router's signal, enter its wireless MAC address into "AP MAC Addr." field

Wireless 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 "Only" mode. If you have some devices that use a different transmission mode, choose the appropriate "Mixed" mode.

Network Name (SSID)

When you are browsing for available wireless networks, this is the name that will appear in the list (unless Broadcast Network Name is set to Disable, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name.

Multiple SSID

This Access Point support multiple SSID function, you can assign three more SSID for this device.

Broadcast Network Name (SSID)

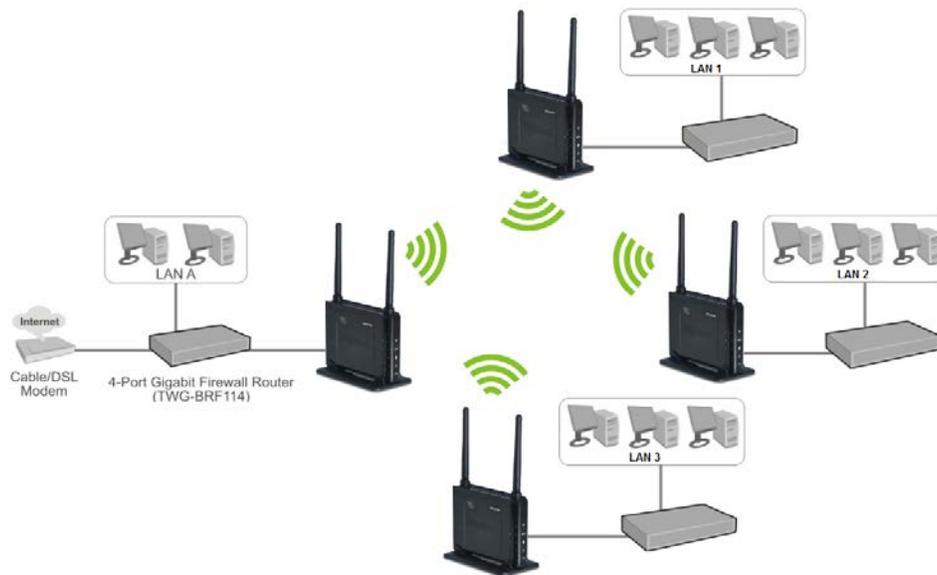
This option allows you to hide your wireless network. When this option is set to enable, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When this mode is disabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

Frequency (Channel)

A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

WDS Mode

When WDS is enabled, this access point functions as a wireless bridge and is able to wirelessly communicate with other access points via WDS links. A WDS link is bidirectional; both end points must support WDS and each access point must know the MAC Address of the other. Each access point will be configured with the remote access point's MAC address and vice versa. Make sure all access points are configured with the same SSID, channel and wireless encryption settings.



Operating Mode

If you have both 11g and 11n client devices included on your wireless network at the same time, you should choose **Mixed Mode**. And if you only have 11n client devices on your wireless network, you can choose **Green Field** to enjoy high throughput.

Channel Bandwidth

The "20/40" MHz option is usually best. The other option is available for special circumstances.

Guard Interval

Using "Auto" option can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

MCS

This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.

Reserve Direction Grant (RDG)

Disable or enable reserve direction grant. Default is enabled.

Extension Channel

When 20/40 channel bandwidth has been chosen, you should select extension channel to get higher throughput.

Aggregation MSDU (A-MSDU)

Disable or enable aggregation MSDU. Default is disabled.

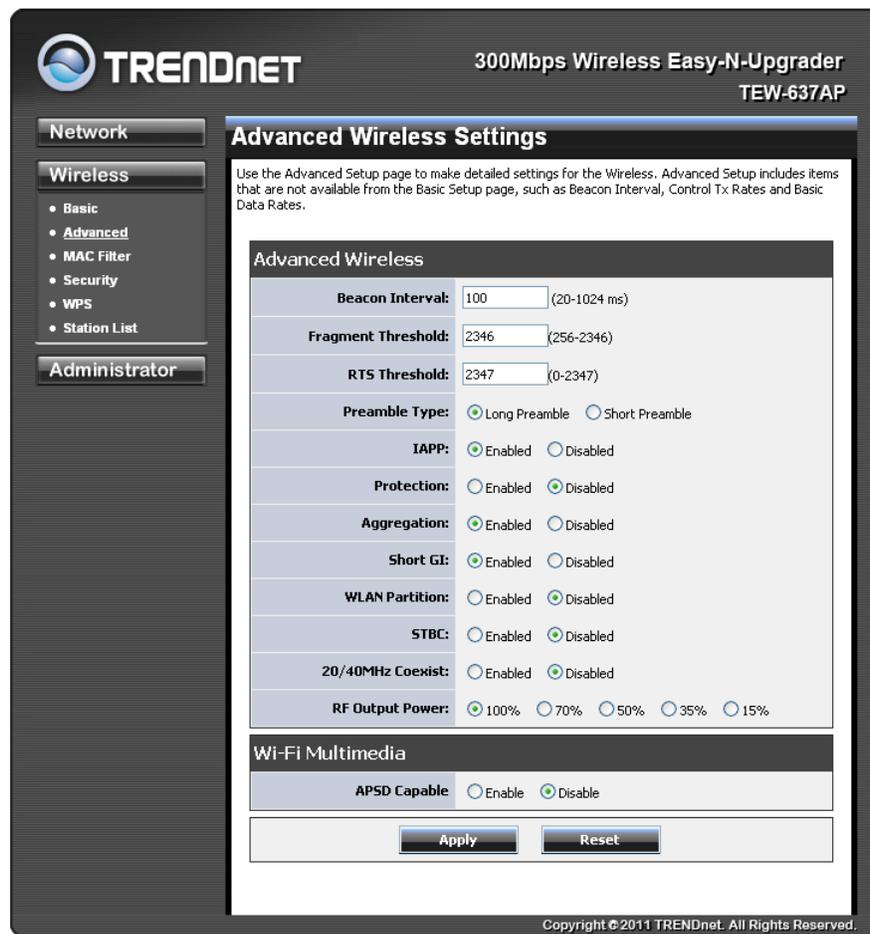
Auto Block ACK

Disable or enable auto block ACK. Default is enabled.

Decline BA Request

Disable or enable decline BA request. Default is disabled.

WIRELESS ADVANCED



Beacon Interval

Beacons are packets sent by a wireless Access Point to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.

Fragment Threshold

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

RTS Threshold

This setting should remain at its default value of 2347. If you encounter inconsistent data flow, only minor modifications to the value are recommended.

Preamble Type: Long Preamble / Short Preamble

The radio preamble is a section of data at the head of the Physical Layer Convergence Protocol that contains information that the device and client devices need when sending and receiving packets. The 18 byte ("long preamble") preamble is used to signal "here is a train of data coming" to the receiver. The 802.11b standard gives an option of reducing the size of the PLCP preamble to 9 bytes ("short preamble"), this significantly increases the throughput performance at higher data rates. One downside to the PLCP is that the PLCP preamble and header is always transmitted at 1Mbps, regardless of the transmission rate for the rest of the data. This means that the transfer time is constant at 192 Usec (microseconds) for the PLCP with long preamble. The short preamble version does a little better,

transmitting the shorter preamble at 1Mbps and the header at 2Mbps, shortening the transmit time to 96 Usec.

IAPP(Inter-Access Point Protocol)

IEEE 802.11F or Inter-Access Point Protocol is a recommendation that describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multivendor systems.

The protocol is designed for the enforcement of unique association throughout an Extended Service Set and for secure exchange of station's security context between the current AP and the new AP during the handoff period. Based on security level, communication session keys between Aps are distributed by a RADIUS server. The RADIUS server also provides a mapping service between AP's MAC address and IP address.

Protection

These protection mechanisms ensure that a STA that is a potential interferer defers any transmission for a known period of time. These mechanisms are used to ensure that non-ERP STAs do not interfere with frame exchanges using ERP PPDU between ERP STAs and that non-HT STAs do not interfere with frame exchanges using HT PPDU between HT STAs, thereby allowing non-ERP and/or non-HT STAs to coexist with ERP and/or HT STAs.

Frame aggregation

Frame aggregation is a feature of the IEEE 802.11e and 802.11n wireless LAN standards that increases throughput by sending two or more data frames in a single transmission. Every frame transmitted by an 802.11 device has a significant amount of overhead, including radio level headers, media access control (MAC) frame fields, interframe spacing, and acknowledgment of transmitted frames. At the highest data rates, this overhead can consume more bandwidth than the payload data frame. To address this issue, the draft 802.11n standard defines two types of frame aggregation: Mac Service Data Unit (MSDU) aggregation and MAC Protocol Data Unit (MPDU) aggregation. Both types group several data frames into one large frame. Because management information needs to be specified only once per frame, the ratio of payload data to the total volume of data is higher, allowing higher throughput.

MSDU aggregation

MSDU aggregation relies on the fact that most mobile access points and most mobile client protocol stacks use Ethernet as their "native" frame format. It collects Ethernet frames to be transmitted to a single destination and wraps them in a single 802.11n frame. This is efficient because Ethernet headers are much shorter than 802.11 headers.

MPDU aggregation

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

Guard interval

In telecommunications, guard intervals are used to ensure that distinct transmissions do not interfere with one another. These transmissions may belong to different users (as in TDMA) or to the same user (as in OFDM). The standard symbol guard interval used in 802.11 OFDM is 0.8 μ s. To increase data rate, 802.11n added optional support for a 0.4 μ s guard interval. This provides an 11% increase in data rate.

Short GI (Shorter guard interval)

The shorter guard interval results in a higher packet error rate when the delay spread of the channel exceed the guard interval and/or if timing synchronization between the transmitter and receiver is not precise. A scheme could be developed to work out whether a short guard interval would be of benefit a particular link. To reduce complexity, manufacturers typically only implement a short guard interval as a final rate adaptation step when the device is running at its highest data rate.

WLAN Partition

When two clients link to this AP, they won't be able to communicate with each other if the WLAN Partition is enabled.

STBC (Space Time Block Coding)

A transmitter diversity technique of spreading the transmit signal over multiple antennas to improve reception. STBC also incorporates FEC (Forward Error Correction) coding.

20/40MHz Coexist

The 20/40 BSS Coexistence element is used by STAs to exchange information that affects 20/40 BSS Coexistence.

RF Output Power

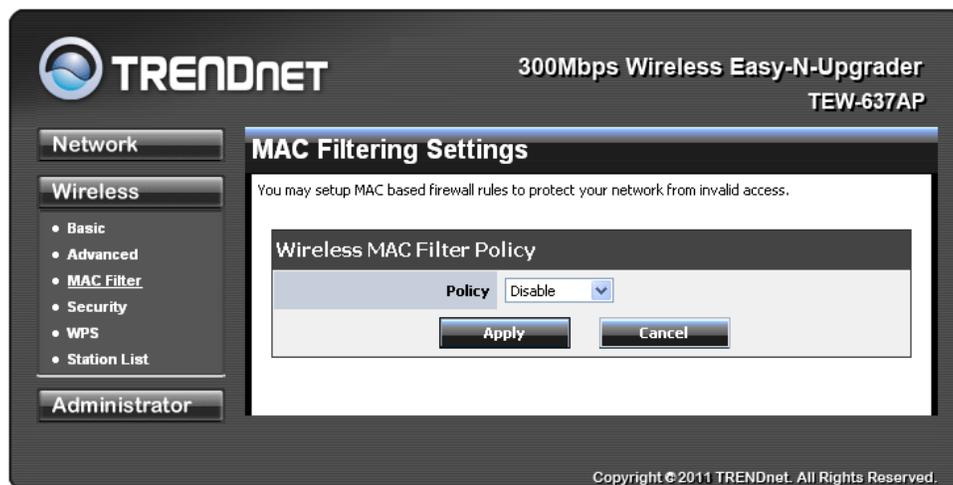
Switch the RF output power strength(%).

APSD Capable (Automatic Power Save Delivery)

Automatic power save delivery is a more efficient power management method than legacy 802.11 Power Save Polling. The literature includes an 802.11 Power Save Mode overview, an analysis of unscheduled and scheduled automatic power save delivery (APSD) and a comparison of APSD versus 802.11 Power Save Mode performance. Most newer 802.11 stations already support a power management mechanism similar to APSD. APSD is very useful for a VoIP phone, as data rates are roughly the same in both directions. Whenever voice data is sent to the access point, the access point is triggered to send the buffered voice data in the other direction. After that the VoIP phone enters a doze state until next voice data has to be sent to the access point.

MAC FILTER

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.



Wireless MAC Filtering

Choose the type of MAC filtering needed.

Turn MAC Filtering Disable:

When "Disable" is selected, MAC addresses are not used to control network access.

Add MAC Filtering Rule

Use this section to add MAC addresses to the list below.

MAC Address

Enter the MAC address of a computer that you want to control with MAC filtering. Computers that have obtained an IP address from the router's DHCP server will be in the DHCP Client List. Select a device from the drop down menu.

The rule of thumb:

In mixed mode, multicast key has to be TKIP, but unicast key can be different per stations. In WPA or WPA2 only mode, unicast and multicast key can be only AES for WPA2, and TKIP for WPA. (AES means the unicast and multicast key are all AES. TKIP/AES means multicast is TKIP. But unicast can be AES or TKIP, which depends on the peer.)

SECURITY



SSID choice

Choose the SSID which need to implement security.

Security Mode

Unless one of these encryption modes is selected, wireless transmissions to and from your wireless network can be easily intercepted and interpreted by unauthorized users.

WEP

Security Policy	
Security Mode	WEP

Wire Equivalence Protection (WEP)	
Authentication	<input type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto

WEP Key	
Key Length	64-bit
Key Format	Hex (10 characters)
WEP Key	*****

A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

Key Length	Hex	ASCII
64-bit	10 characters	5 characters
128-bit	26 characters	13 characters

WPA/WPA2-Personal and Enterprise

Both of these options select some variant of Wi-Fi Protected Access (WPA) -- security standards published by the Wi-Fi Alliance. The WPA Mode further refines the variant that the router should employ.

WPA/WPA2 Mode:

WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the router associates only with clients that also support WPA2 security.

Cipher Type:

The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. With the "TKIP and AES" option, the router negotiates the cipher type with the client, and uses AES when available.

Group Key Update Interval:

The amount of time before the group key used for broadcast and multicast data is changed.

WPA/WPA2-Personal

Security Policy	
Security Mode	WPA
WPA	
Auth. Mode	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)
WPA Algorithms	<input checked="" type="checkbox"/> TKIP <input type="checkbox"/> AES
Pass Phrase Format	Passphrase
Pass Phrase	••••••••

This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).

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

WPA/WPA2-Enterprise

Security Policy	
Security Mode	WPA
WPA	
Auth. Mode	<input checked="" type="radio"/> Enterprise (RADIUS) <input type="radio"/> Personal (Pre-Shared Key)
WPA Algorithms	<input checked="" type="checkbox"/> TKIP <input type="checkbox"/> AES
Radius Server	
IP Address	
Port	1812
Shared Secret	

This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.

Authentication Timeout: Amount of time before a client will be required to re-authenticate.

RADIUS Server IP Address: The IP address of the authentication server.

RADIUS Server Port: The port number used to connect to the authentication server.

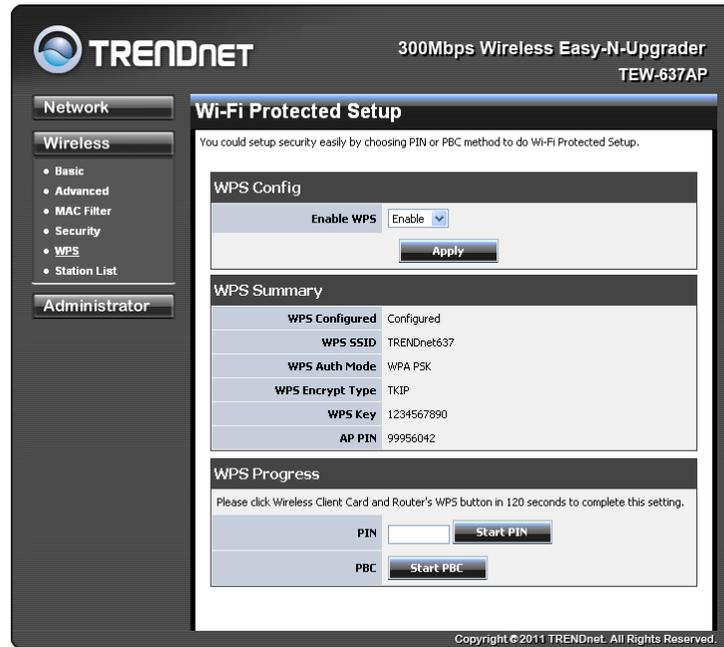
RADIUS Server Shared Secret: A pass-phrase that must match with the authentication server.

WPA/WPA2 mixed environment

For those WPA2 stations, they will use AES for unicast. For those WPA stations, they will use TKIP for unicast. But for multicast all WPA and WPA2 stations have to use the same key, and that will be TKIP, because WPA station only knows about TKIP, WPA2 is new standard, so it is defined to backward support TKIP on multicast.

WPS

You can setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

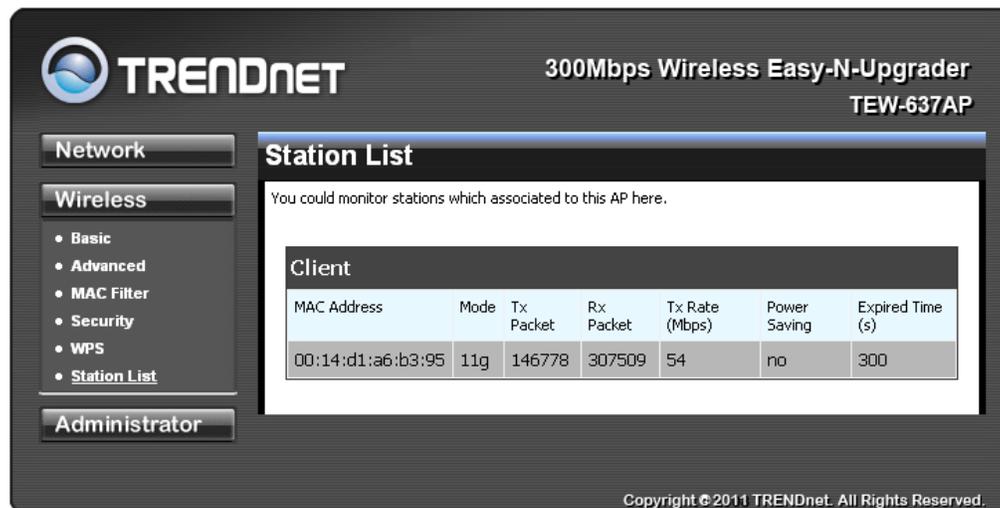


WPS mode

Two WPS modes can be selected – PIN & PBC. If PIN is selected, you should enter PIN code of your wireless client device to get wireless connection with this AP.

STATION LIST

You can monitor stations which associated to this AP.



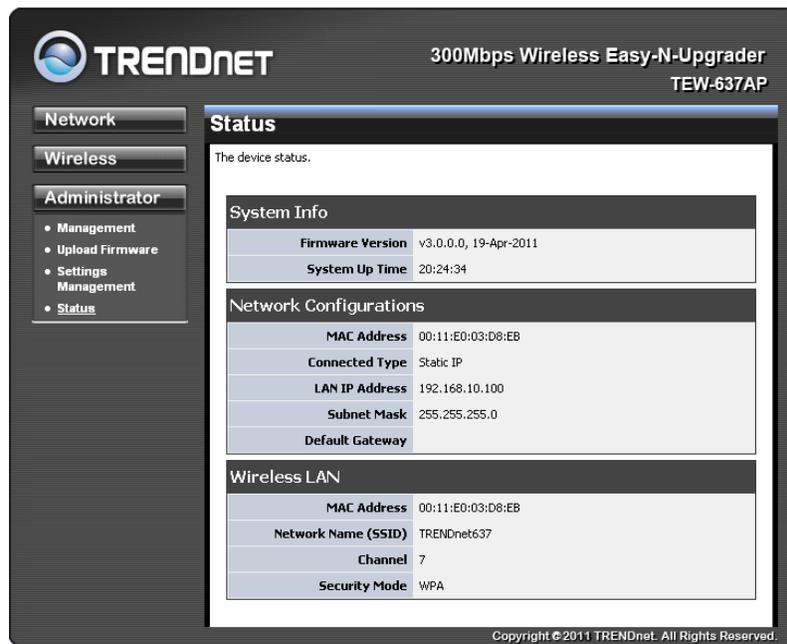
Administrator

This Administrator section is used to set password for access to the Web-based management, also provide function of firmware upgrade.

The Administrator tab provides the following configuration options: Management, Upload Firmware, Settings Management & Status.

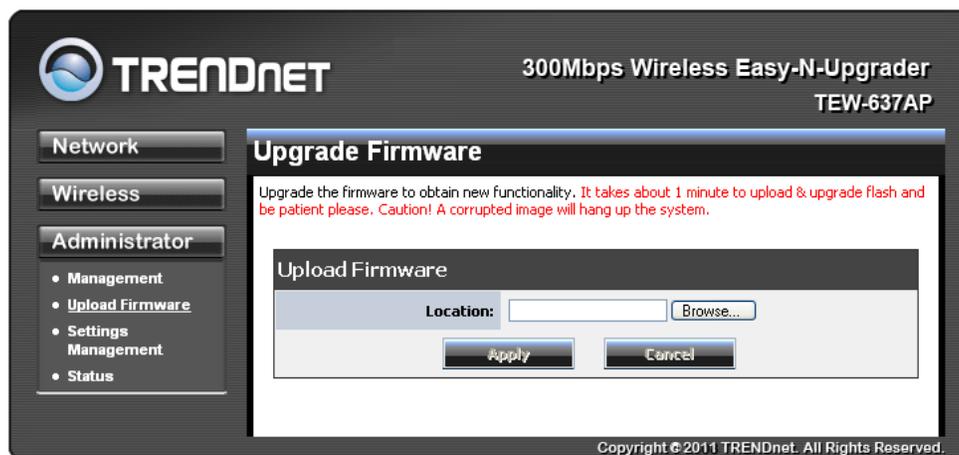
SYSTEM MANAGEMENT

At this page, you can configure administrator account and password.



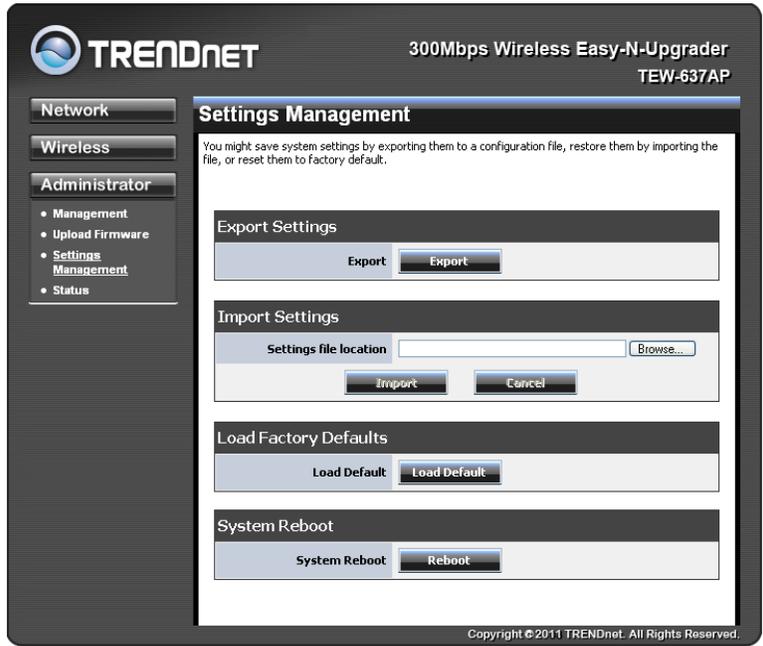
UPLOAD FIRMWARE

By assigning firmware location, you can upload firmware at this page.



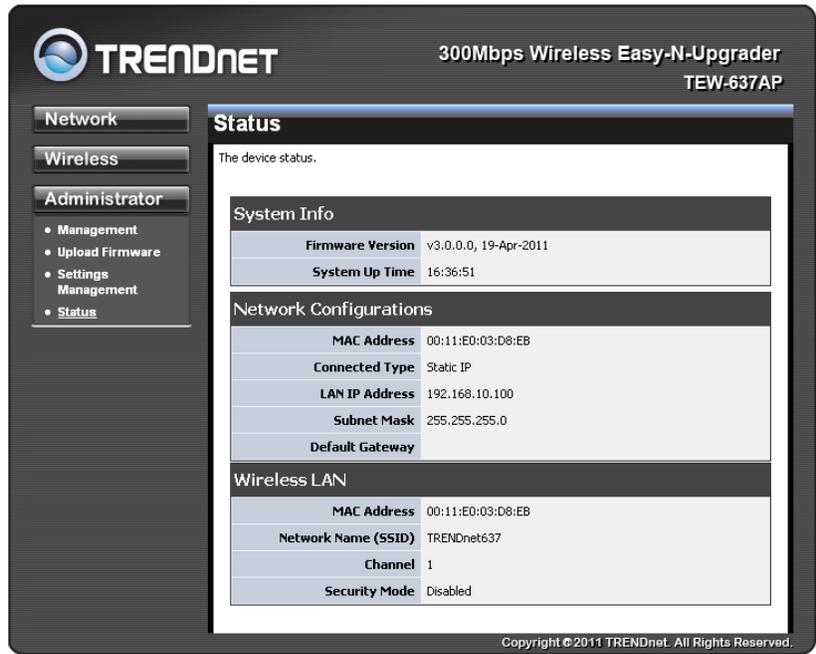
SETTINGS MANAGEMENT

You can save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default.



STATUS

You can check system information and network configurations on this page.



Glossary

A

Access Control List

ACL. This is a database of network devices that are allowed to access resources on the network.

Access Point

AP. Device that allows wireless clients to connect to it and access the network

Ad-hoc network

Peer-to-Peer network between wireless clients

Address Resolution Protocol

ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

Advanced Encryption Standard

AES. Government encryption standard

Alphanumeric

Characters A-Z and 0-9

Antenna

Used to transmit and receive RF signals.

ASCII

American Standard Code for Information Interchange. This system of characters is most commonly used for text files

Attenuation

The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication

To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

Automatic Private IP Addressing

APIPA. An IP address that that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

B

Backward Compatible

The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

Bandwidth

The maximum amount of bytes or bits per second that can be transmitted to and from a network device

Beacon

A data frame by which one of the stations in a Wi-Fi network periodically broadcasts network control data to other wireless stations.

Bit rate

The amount of bits that pass in given amount of time

Bit/sec

Bits per second

BOOTP

Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

Broadcast

Transmitting data in all directions at once

Browser

A program that allows you to access resources on the web and provides them to you graphically

C

CAT 5

Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

Client

A program or user that requests data from a server

Collision

When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie

Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

D

Data

Information that has been translated into binary so that it can be processed or moved to another device

Data-Link layer

The second layer of the OSI model. Controls the movement of data on the physical link of a network

dBd

Decibels related to dipole antenna

dBi

Decibels relative to isotropic radiator

dBm

Decibels relative to one milliwatt

Decrypt

To unscramble an encrypted message back into plain text

Default

A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

DHCP

Dynamic Host Configuration Protocol: Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that request them

Digital certificate:

An electronic method of providing credentials to a server in order to have access to it or a network

Direct Sequence Spread Spectrum

DSSS: Modulation technique used by 802.11b wireless devices

DNS

Domain Name System: Translates Domain Names to IP addresses

Domain name

A name that is associated with an IP address

Download

To send a request from one computer to another and have the file transmitted back to the requesting computer

Duplex

Sending and Receiving data transmissions at the same time

Dynamic IP address

IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

E

EAP

Extensible Authentication Protocol

Encryption

Converting data into cyphertext so that it cannot be easily read

Ethernet

The most widely used technology for Local Area Networks.

F

File server

A computer on a network that stores data so that the other computers on the network can all access it

File sharing

Allowing data from computers on a network to be accessed by other computers on the network with different levels of access rights

Firewall

A device that protects resources of the Local Area Network from unauthorized users outside of the local network

Firmware

Programming that is inserted into a hardware device that tells it how to function

Fragmentation

Breaking up data into smaller pieces to make it easier to store

FTP

File Transfer Protocol. Easiest way to transfer files between computers on the Internet

Full-duplex

Sending and Receiving data at the same time

G

Gain

The amount an amplifier boosts the wireless signal

Gateway

A device that connects your network to another, like the internet

Gbps

Gigabits per second

Gigabit Ethernet

Transmission technology that provides a data rate of 1 billion bits per second

GUI

Graphical user interface

H

Half-duplex

Data cannot be transmitted and received at the same time

Hashing

Transforming a string of characters into a shorter string with a predefined length

Hexadecimal

Characters 0-9 and A-F

Hop

The action of data packets being transmitted from one AP to another

Host

Computer on a network

HTTP

Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

HTTPS

HTTP over SSL is used to encrypt and decrypt HTTP transmissions

Hub

A networking device that connects multiple devices together

I

ICMP

Internet Control Message Protocol

IEEE

Institute of Electrical and Electronics Engineers

IGMP

Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent APs

IIS

Internet Information Server is a WEB server and FTP server provided by Microsoft

Infrastructure

In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

Internet

A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

Internet Explorer

A World Wide Web browser created and provided by Microsoft

Internet Protocol

The method of transferring data from one computer to another on the Internet

Internet Protocol Security

IPsec provides security at the packet processing layer of network communication

Internet Service Provider

An ISP provides access to the Internet to individuals or companies

Intranet

A private network

Intrusion Detection

A type of security that scans a network to detect attacks coming from inside and outside of the network

IP

Internet Protocol

IP address

A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

IPsec

Internet Protocol Security

IPX

Internetwork Packet Exchange is a networking protocol developed by Novel to enable their Netware clients and servers to communicate

ISP

Internet Service Provider

J**Java**

A programming language used to create programs and applets for web pages

K**Kbps**

Kilobits per second

Kbyte

Kilobyte

L**LAN**

Local Area Network

Latency

The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

LED

Light Emitting Diode

Legacy

Older devices or technology

Local Area Network

A group of computers in a building that usually access files from a server

LPR/LPD

"Line Printer Requestor"/"Line Printer Daemon". A TCP/IP protocol for transmitting streams of printer data.

L2TP

Layer 2 Tunneling Protocol

M**MAC address**

A unique hardware ID assigned to every Ethernet adapter by the manufacturer.

Mbps

Megabits per second

MDI

Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

MDIX

Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

MIB

Management Information Base is a set of objects that can be managed by using SNMP

Modem

A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

MPPE

Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

MTU

Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet

Multicast

Sending data from one device to many devices on a network

N**NAT**

Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

NetBEUI

NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

NetBIOS

Network Basic Input/Output System

Netmask

Determines what portion of an IP address designates the Network and which part designates the Host

Network Interface Card

A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

Network Layer

The third layer of the OSI model which handles the routing of traffic on a network

Network Time Protocol

Used to synchronize the time of all the computers in a network

NIC

Network Interface Card

NTP

Network Time Protocol

O

OFDM

Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.wireless g

OSI

Open Systems Interconnection is the reference model for how data should travel between two devices on a network

OSPF

Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other APs in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

P

Password

A sequence of characters that is used to authenticate requests to resources on a network

Personal Area Network

The interconnection of networking devices within a range of 10 meters

Physical layer

The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

Ping

A utility program that verifies that a given Internet address exists and can receive messages. The utility sends a control packet to the given address and waits for a response.

PoE

Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

Port

A logical channel endpoint in a network. A computer might have only one physical channel (its Ethernet channel) but can have multiple ports (logical channels) each identified by a number.

PPP

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

PPPoE

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

PPTP

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

Preamble

Used to synchronize communication timing between devices on a network

Q

QoS

Quality of Service

R

RADIUS

Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

Reboot

To restart a computer and reload it's operating software or firmware from nonvolatile storage.

Rendezvous

Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

Repeater

Retransmits the signal of an Access Point in order to extend it's coverage

RIP

Routing Information Protocol is used to synchronize the routing table of all the APs on a network

RJ-11

The most commonly used connection method for telephones

RJ-45

The most commonly used connection method for Ethernet

RS-232C

The interface for serial communication between computers and other related devices

RSA

Algorithm used for encryption and authentication

S

Server

A computer on a network that provides services and resources to other computers on the network

Session key

An encryption and decryption key that is generated for every communication session between two computers

Session layer

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

Simple Mail Transfer Protocol

Used for sending and receiving email

Simple Network Management Protocol

Governs the management and monitoring of network devices

SIP

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SOHO

Small Office/Home Office

SPI

Stateful Packet Inspection

SSH

Secure Shell is a command line interface that allows for secure connections to remote computers

SSID

Service Set Identifier is a name for a wireless network

Stateful inspection

A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass through the firewall

Subnet mask

Determines what portion of an IP address designates the Network and which part designates the Host

Syslog

System Logger -- a distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

T

TCP

Transmission Control Protocol

TCP/IP

Transmission Control Protocol/Internet Protocol

TCP Raw

A TCP/IP protocol for transmitting streams of printer data.

TFTP

Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

Throughput

The amount of data that can be transferred in a given time period

Traceroute

A utility displays the routes between you computer and specific destination

U**UDP**

User Datagram Protocol

Unicast

Communication between a single sender and receiver

Universal Plug and Play

A standard that allows network devices to discover each other and configure themselves to be a part of the network

Upgrade

To install a more recent version of a software or firmware product

Upload

To send a request from one computer to another and have a file transmitted from the requesting computer to the other

UPnP

Universal Plug and Play

URL

Uniform Resource Locator is a unique address for files accessible on the Internet

USB

Universal Serial Bus

UTP

Unshielded Twisted Pair

V**Virtual Private Network**

VPN: A secure tunnel over the Internet to connect remote offices or users to their company's network

VLAN

Virtual LAN

Voice over IP

Sending voice information over the Internet as opposed to the PSTN

VoIP

Voice over IP

W**Wake on LAN**

Allows you to power up a computer though it's Network Interface Card

WAN

Wide Area Network

WCN

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

WDS

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

Web browser

A utility that allows you to view content and interact with all of the information on the World Wide Web

WEP

Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

Wi-Fi

Wireless Fidelity

Wi-Fi Protected Access

An updated version of security for wireless networks that provides authentication as well as encryption

Wide Area Network

The larger network that your LAN is connected to, which may be the Internet itself, or a regional or corporate network

Wireless ISP

A company that provides a broadband Internet connection over a wireless connection

Wireless LAN

Connecting to a Local Area Network over one of the 802.11 wireless standards

WISP

Wireless Internet Service Provider

WLAN

Wireless Local Area Network

WPA

Wi-Fi Protected Access. A Wi-Fi security enhancement that provides improved data encryption, relative to WEP.

X

xDSL

A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

Y

Yagi antenna

A directional antenna used to concentrate wireless signals on a specific location

802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

Specifications

Hardware	
Standards	IEEE 802.11n, IEEE 802.11b, IEEE 802.11g, 802.3u and 802.3
Interface	1 x 10/100Mbps Auto-MDIX LAN port
CD Wizard OS Compatibility	Windows 7 (32/64-bit), Vista(32/64-bit), XP(32/64-bit), and 2000
LED Indicators	Power, LAN, WPS, and Wireless
Power Supply	12 V DC 0.5A external power adapter
Dimensions (LxWxH)	120 x 26 x 88 mm (4.7 x 1.0 x 3.4 in)
Weight	145 g (5.11oz)
Temperature	Operating: 0° ~ 40° C (32° ~ 104°F) Storage: -20° ~ 60°C (-4°~140°F)
Humidity	Max. 90% non-condensing
Wireless	
Module Technique	OFDM with BPSK ,DQPSK , CCK , BPSK, QPSK, 16/64QAM with OFDM
WDS	Enable/Disable Wireless Distribution System support
Antenna	2 x 2dBi external fixed dipole antennas
Frequency	2.412 -2.484GHz
Data Rate (Auto Fallback)	802.11n: up to 300Mbps 802.11g: up to 54Mbps 802.11b: up to 11Mbps
Output Power	802.11b: 18dBm (typical) @ 11Mbps 802.11g: 15dBm (typical) @ 54Mbps 802.11n: 11dBm (typical)@ 300Mbps
Receiving Sensitivity	802.11b: -84dBm (typical) @ 11mpbs 802.11g: -72dBm (typical) @ 54Mbps 802.11n: -68dBm (typical) @ 300Mbps
Encryption	64/128-bit WEP, WPA/WPA2 RADIUS, WPA/WPA2-PSK
Channels	1-11 (FCC) 1-13 (ETSI)

*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.

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-637AP – 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 DATA, 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



Product Warranty Registration

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