



TRENDNET®



User's Guide

TEW-450APB

Contents

1. Overview	1
1.1 Product Feature	1
1.2 System Requirements	1
2. Getting Start.....	2
2.1 Know the Wireless Super G Access Point	2
2.2 Connect to the Wireless Super G Access Point	2
2.3 Quick Setup with Wizard.....	3
2.3.1 Access the Setting Menu	3
2.3.2 Setup with Wizard	4
3. Configuration through WEB Browser.....	7
3.1 Status.....	7
3.2 Basic Setting.....	8
3.3 IP Setting	12
3.4 Advanced Setting.....	13
3.5 Security.....	16
3.6 Tools	17
Glossary	19

1. Overview

1.1 Product Feature

- Compliance with IEEE 802.11g and 802.11b standards
- Highly efficient design mechanism to provide unbeatable performance
- Achieves data rates up to 54Mbps for 802.11g and 11Mbps for 802.11b with wide range coverage; high performance to deliver up to 108Mbps raw data rate for 802.11g
- Strong network security with WEP, WPA and 802.1X encryption
- Quick and easy setup with Web-based management utility

1.2 System Requirements

- Windows 98, 98SE, Millennium Edition (ME), 2000, XP and Vista operating systems
- Microsoft Internet Explorer 6 or higher
- At least one RJ-45 Ethernet network adapter installed.

2. Getting Start

2.1 Know the Wireless Super G Access Point

Ports:

- Power Receptor
- Reset Button
- RJ-45 Ethernet Port

LEDs:

- Power LED: ON when the unit is powered up
- LAN LED: ON indicates LAN connection; BLINK indicates LAN activity
- WLAN LED: ON indicates WLAN is working; BLINK indicates wireless activity.

2.2 Connect to the Wireless Super G Access Point

Build the Infrastructure Mode



In order to setup an Infrastructure wireless network such as the example shown above, you will need the following:

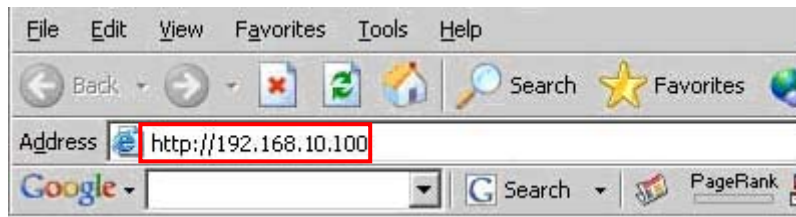
1. A broadband Internet connection.

2. ADSL or Cable modem provided by your ISP as part of the broadband connection installation.
3. A Router that connects to the ADSL/Cable modem for Internet connection sharing.
4. An Access Point to connect with the Router to form a wireless infrastructure network.
5. Wireless clients equipped with wireless networking devices such as wireless PC Card for wireless connection.

2.3 Quick Setup with Wizard

2.3.1 Access the Setting Menu

To access the configuration menu open a web browser window and type the IP address of this access point. The default IP is 192.168.10.100.



The below window will popup. Please enter the user name and password. The default User name and Password is “admin.”



Now, the main screen appears



2.3.2 Setup with Wizard

Setup wizard is provided as the part of the web configuration utility. Follow the step-by-step process to configure your Access Point by clicking on the “**Wizard**” button on the function menu. The following screen will appear. Please click “**Next**” to continue.



Step 1: Set Password

Set a desired password and then click “Next” to continue.



The screenshot shows the 'Set Password' screen of the 'Wireless Super G Access Point' setup wizard. The title is 'Wireless Super G Access Point' and the section is 'Set Password'. The instructions state: 'You may want to change the Administrator password of this Access Point to prevent authorized modification to the configuration settings. Enter your new password in the following text fields. Click Next to continue with setup or Exit to quit setup wizard.' There are two text input fields: 'Password' and 'Verify Password', both containing ten dots. At the bottom, there are three buttons: 'Back', 'Next', and 'Exit'.

Step2: Set WLAN Connection

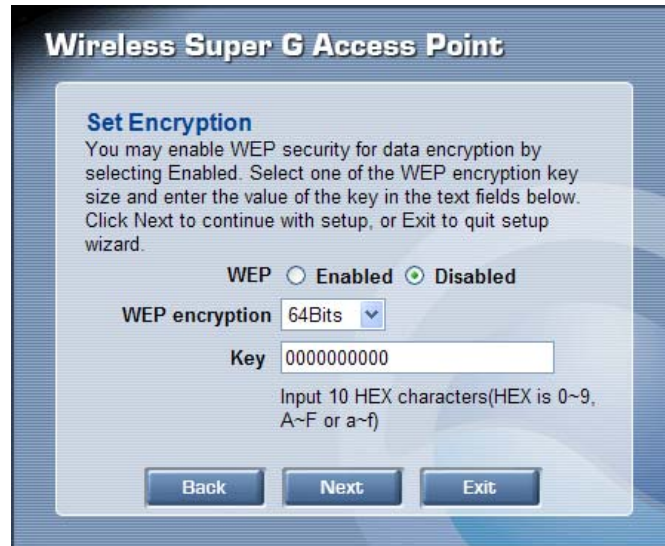
Enter an SSID for your access point and select a channel. Then, click “Next” to continue. The default SSID is **TRENDnet**.



The screenshot shows the 'Set Wireless LAN Connection' screen of the 'Wireless Super G Access Point' setup wizard. The title is 'Wireless Super G Access Point' and the section is 'Set Wireless LAN Connection'. The instructions state: 'Enter the SSID of the wireless network, and select the frequency channel that this Access Point will operate in. Click Next to continue setup, or Exit to quit setup wizard.' There are two input fields: 'SSID' with the text 'TRENDnet' and 'Channel' with a dropdown menu showing '6'. At the bottom, there are three buttons: 'Back', 'Next', and 'Exit'.

Step 3: Set WEP Encryption

If you like to enable WEP, please click **“Enabled”**. Then, select the key size of WEP encryption and enter the key value in the key text box. Then click **“Next”** to continue.



The screenshot shows the 'Set Encryption' screen of the 'Wireless Super G Access Point' setup wizard. The title is 'Wireless Super G Access Point' and the sub-title is 'Set Encryption'. The instructions state: 'You may enable WEP security for data encryption by selecting Enabled. Select one of the WEP encryption key size and enter the value of the key in the text fields below. Click Next to continue with setup, or Exit to quit setup wizard.' There are two radio buttons for 'WEP': 'Enabled' (unselected) and 'Disabled' (selected). Below this is a dropdown menu for 'WEP encryption' set to '64Bits' and a text box for 'Key' containing '0000000000'. A note below the key box says 'Input 10 HEX characters(HEX is 0~9, A~F or a~f)'. At the bottom are three buttons: 'Back', 'Next', and 'Exit'.

Step 4: Restart

The Setup wizard is now completed. The new settings will be effective after the Access Point restarted. Please click **“Restart”** to reboot the Access Point. If you do not want to make any changes, please click **“exit”** to quit without any changes. You also can go back to modify the setting by clicking **“Back”**.

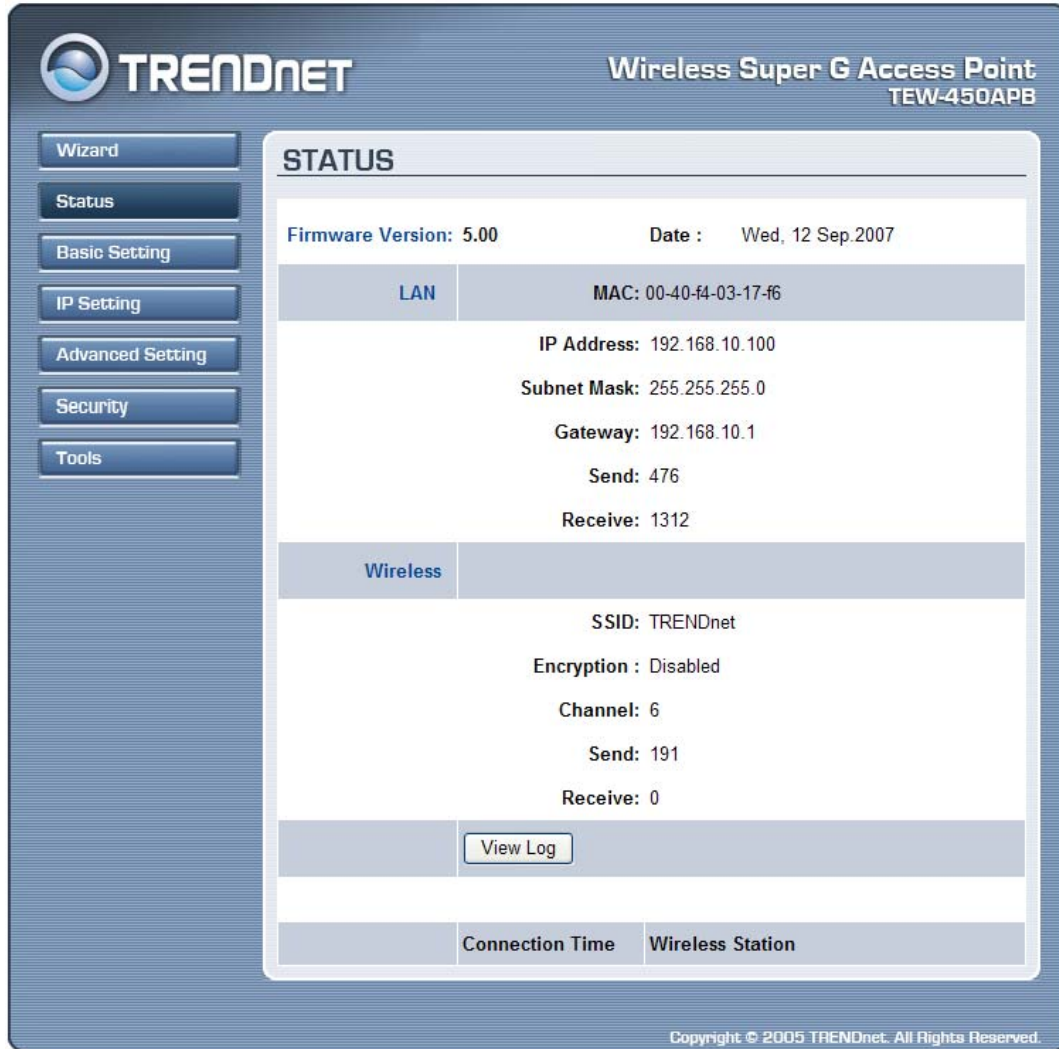


The screenshot shows the 'Set Completed' screen of the 'Wireless Super G Access Point' setup wizard. The title is 'Wireless Super G Access Point' and the sub-title is 'Set Completed'. The instructions state: 'The Access Point setup is now completed. If you want to change any setup settings, click Back to go back to the previous pages. Click Restart to reboot the Access Point for the new settings to take effect.' At the bottom are three buttons: 'Back', 'Restart', and 'Exit'.

3. Configuration through WEB Browser

3.1 Status

The status page shows you the following information.



Firmware Version: Shows the current firmware version.

LAN: Shows the Mac address, IP address (default: 192.168.10.100), Subnet Mask, Gateway Address. The current LAN traffic calculated in terms of number of packets sent and received by AP through wired connection is also displayed.

Wireless: Shows the Mac address, current ESSID, the status of Encryption Function (Enable or Disable), the current using channel. The current wireless traffic calculated in terms of number of packets sent and received by AP through wireless communication is also displayed.

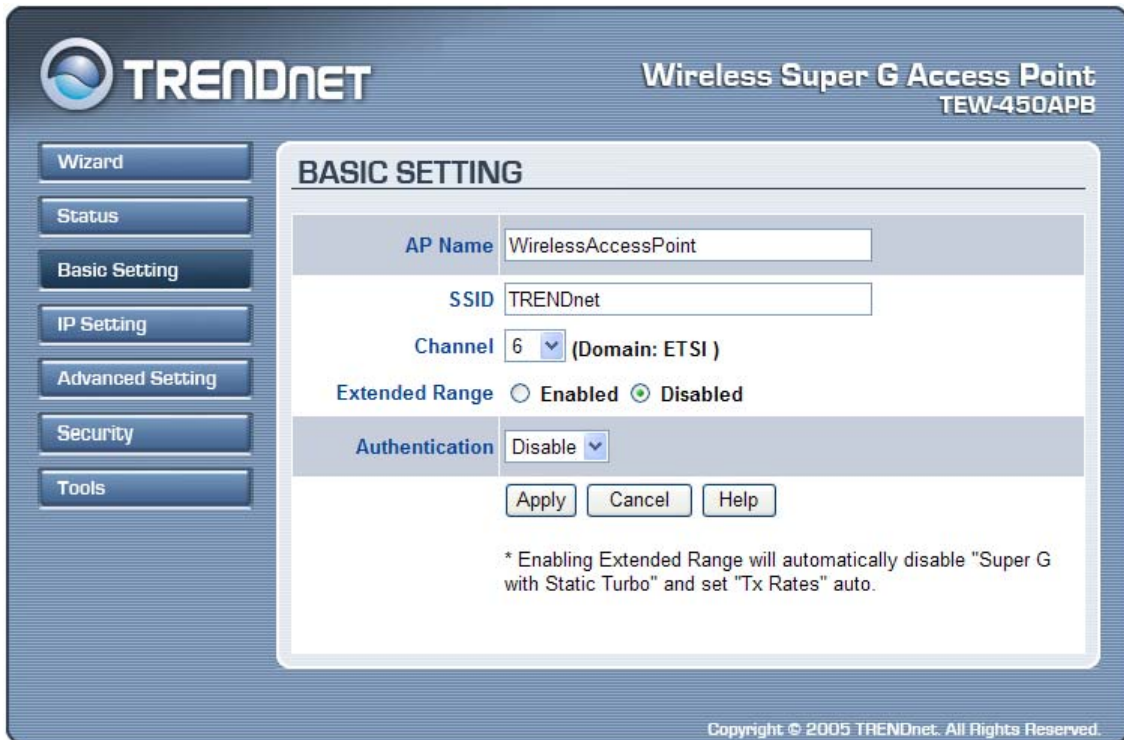
View Log: Upon clicked, the page will change to log page. The log page records every event and the time that it happens.



You may clear the entries recorded in the log by clicking the “**Clear Log**” button, and refresh the screen to show the latest log entries by clicking the “**Refresh**” button.

3.2 Basic Setting

This page allows you to change the wireless settings.



AP Name: The name of the AP, which can be used to identify the Access Point among the all the Access Points in the wireless network.

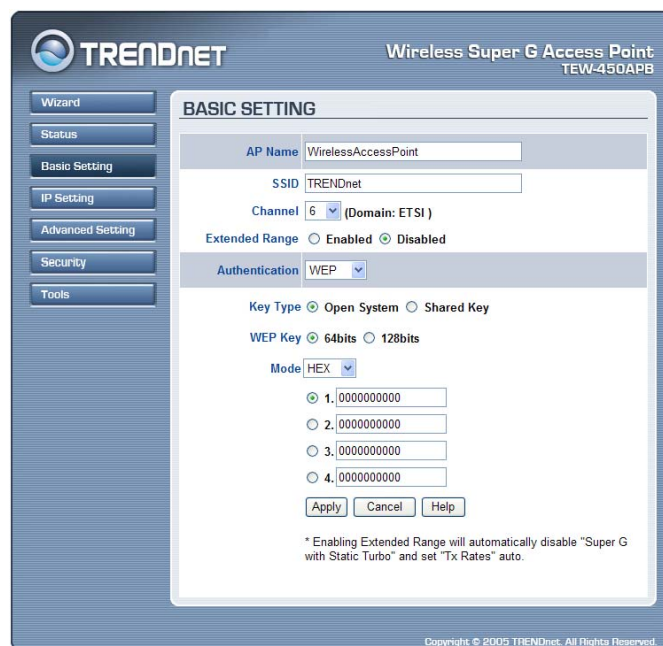
SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Channel: The channel that AP will operate in. You can select the channel range of 1 to 11 for North America (FCC) domain and 1 to 13 for European (ETSI) domain.

Extended Range: When you enable this function, AP will reduce data rate with a long distance.

Authentication Type: The authentication type default is set to disable. There are four options: Disable, WEP, WPA, and WPA2.

WEP Encryption:



Key Type: Open System or Shared Key; the Open System allows public access to the router via wireless communications; the Shared Key requires the user to set a WEP key to exchange data with other wireless clients that have the same WEP key.

WEP Key: Select the WEP encryption key length of 64bits or 128bit.

Mode: Select the key mode in ASCII or HEX

Key 1 ~ Key 4: Enables user to create an encryption scheme for Wireless LAN transmissions. Manually enter a set of values for each key. Select a key to use by clicking the radio button next to the key.

Apply: For the changes made to any of the items above to be effective, click “**Apply**”. The new settings are now been saved to Access Point and will be effective once the Access Point restarts.

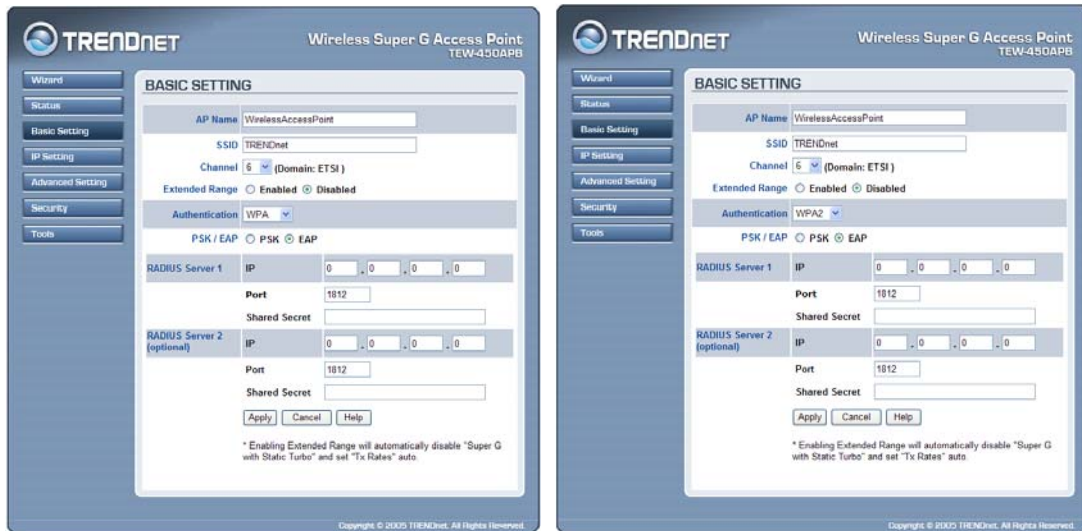
Note: When WEP security is enabled, all the wireless clients that wish to connect to the Access Point must also have WEP enabled with the identical WEP Key value entered.

WPA-PSK / WPA2-PSK:



If WPA-PSK or WPA2-PSK is selected, please set the PSK key in the passphrase field. The length should be 8 characters at least.

WPA / WPA2:



If WPA or WPA2 is selected, the below screen is shown. Please set the length of the encryption key and the parameters for the RADIUS server.

RADIUS Server 1:

Enter the IP address and the Port number to be used by the Primary Radius Server, enter the Shared Secret, which is used by the Radius Server.

RADIUS Server 2: (optional)

Enter the IP address and the Port number to be used by the Secondary Radius Server, enter the Shared Secret, which is used by the Radius Server.

Press **Apply** button to save the new settings and the Access Point will be restart to activate the new settings.

3.3 IP Setting

This page allows you to configure the IP and DHCP settings of the Access Point.

The screenshot displays the 'IP SETTING' configuration page for a Trendnet Wireless Super G Access Point (TEW-450APB). The interface includes a sidebar with navigation options: Wizard, Status, Basic Setting, IP Setting (selected), Advanced Setting, Security, and Tools. The main content area is titled 'IP SETTING' and contains the following configuration options:

- LAN IP:** Radio buttons for 'Obtain IP Automatically' and 'Fixed IP' (selected).
- Address:** Input fields for IP address: 192, 168, 10, 100.
- Subnet Mask:** Input fields for subnet mask: 255, 255, 255, 0.
- Gateway:** Input fields for gateway: 192, 168, 10, 1.
- DHCP Server:** Radio buttons for 'On' and 'Off' (selected).
- IP Range:** Fields for 'From' (192, 168, 10, 101) and 'To' (192, 168, 10, 200).
- DNS Server:** Input fields for DNS server: 192, 168, 10, 1.

At the bottom of the configuration area, there are three buttons: 'Apply', 'Cancel', and 'Help'. A copyright notice 'Copyright © 2005 TRENDnet. All Rights Reserved.' is visible at the bottom right of the page.

The default IP address of this access point is 192.168.10.100 with the subnet mask of 255.255.255.0. You can type in other values for IP Address, Subnet Mask and Gateway and click “**Apply**” button for the changes to be effective.

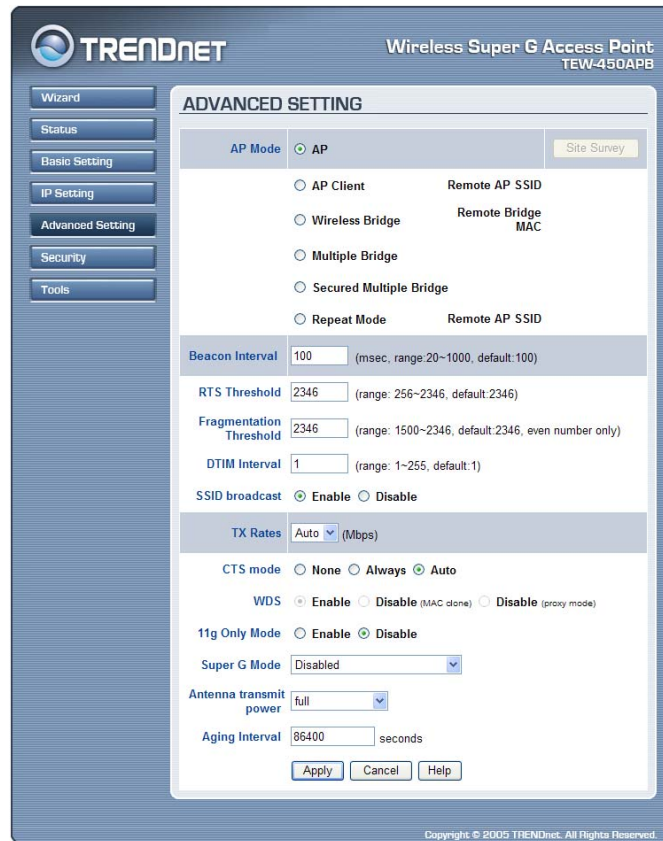
You can also set the Access Point to obtain the IP from a DHCP server, but it is not recommended. Select the option “Obtain IP Automatically” and click “**Apply**” button for the changes to be effective.

DHCP Server: It is not recommended to enable the DHCP Server if you have a DHCP server running in your LAN network because it could cause IP address conflict. Enable the DHCP server function by selecting the option “On”, and enter the IP range.

Click “**Apply**” for the changes to be effective.

3.4 Advanced Setting

This page contains advanced wireless options.



AP Mode: Select one of the AP operating modes for different application of Access Point:

1. **AP** mode: The normal Access Point operating mode which forms a wireless ESS network with its wireless clients.
2. **AP Client** mode: Acts as an Ethernet-to-Wireless Bridge, which allows a LAN or a single computer station to join a wireless ESS network through it. You must make sure SSID and Channel is set the same as that AP you wish to connect.

Remote AP SSID: key in the remote Access Point's SSID that you wish to connect.

Wireless Bridge mode: A pair of APs operating under Bridge mode to act as the bridge that connect two Ethernet networks or Ethernet enabled clients together. You must make sure that the SSID and Channel is set the same as that AP you wish to connect.

Remote Bridge MAC filed: key in the **Mac address** key in Wireless (not LAN) MAC address of remote AP in Bridge mode.

3. **Multiple Bridge mode:** Configure to the multiple bridge mode; these APs will be a LAN to LAN wireless Ethernet bridge between two or more separated Ethernet LAN segments.
4. **Secured Multiple Bridge mode:** When there are three APs joined to the WDS group, one of the AP in WDS mode will be the Master, the other two APs will be the Slave, all of the APs in the WDS group must use the same wireless channel and the same security setting, the Master need to fill all the Slave's MAC address in the "Remote AP Mac" list, the maximum of one Master can join eight Slave to be one WDS group
5. **Repeat Mode:** It is able to extend the effective range and coverage of the wireless network. Please make sure the SSID is the same as that AP you want to extend.

Note: All APs have to use the same **Channel** and **SSID** in order to set a Multiple Bridge network.

Beacon Interval: To set the period of time in milliseconds that AP sends out a beacon. Default is 100 milliseconds.

RTS Threshold: To set the size of RTS/CTS packet size. Default is 2346 bytes.

Fragmentation Threshold: To set the number of bytes used for the fragmentation boundary for directed messages. Default is 2346 bytes.

DTIM Interval: This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the access point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. Access point clients hear the beacons and awaken to receive the broadcast and multicast messages. Default value is 1.

SSID Broadcast Enable / Disable: When SSID Broadcast is enabled, all wireless clients will be able to communicate with the access point. For security purposes, you may want to disable SSID broadcast to allow only those wireless clients with the AP SSID to communicate with the access point.

TX Rates (MBps): Select one of the wireless communications transfer rates, measured in megabytes per second, based upon the speed of wireless adapters connected to the WLAN.

CTS Mode (clear to send): None- disable CTS function. Always- Regardless of wireless environment (11b or 11g), platform will always transfer 11b packet. Auto- AP soon detected the wireless environment and decided the transmission packet, either 11b or 11g.

WDS (Wireless Distribution System): For AP Client mode and Repeater mode. It will add client quantity at the back when you enable this function.

11g Only Mode: If selected the Enable, only allow 802.11g WLAN client communicate with this WLAN Router

Super G mode: From the drop list, if you want to use Super-G™ to enhance the speed, there are three options on Super-G™ mode: *Super G without turbo*; *Super G with Dynamic turbo* and *Super G with Static turbo*. The turbo mode indicates the combination of two channels to enhance the throughput. Super G without turbo indicates that it is on Super G mode without the channel's combination. Dynamic turbo is able to automatically detect if any 'Super-G™ based' product is available. If no, the connection is via 'normal' G. Static turbo means it will not go back to 'normal' G once it starts.

Antenna Transmit Power: Adjust the power of the antenna transmission by selecting from the dropping list.

Aging Interval: To limited STA connect timing.

3.5 Security

This page allows you to configure the security features supported by this Access Point.

TRENDNET Wireless Super G Access Point
TEW-450APB

Wizard
Status
Basic Setting
IP Setting
Advanced Setting
Security
Tools

SECURITY

Password Administrator ID:

AP Password New:

Confirm:

MAC Filter Enabled Disabled

Only deny PCs with MAC listed below to access device

Only allow PCs with MAC listed below to access device

1~10

MAC 1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
MAC 2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
MAC 3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
MAC 4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
MAC 5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
MAC 6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
MAC 7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
MAC 8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
MAC 9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
MAC 10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Copyright © 2005 TRENDnet. All Rights Reserved.

Administrator id: Allow you change the administrator user id.

Password: Allow you to change the new login password. Follow the steps below:

1. Enter the new password in the “**AP Password New:**” field.
2. Enter the new password again in the “**Confirm**” field.
3. Click “**Apply**”

MAC Filter: MAC Filter function controls the MAC of the network devices that are listed in this table for access authorization or denial. When MAC Filter is enabled, by selecting the “**Enabled**” radio box, select one of two choices:

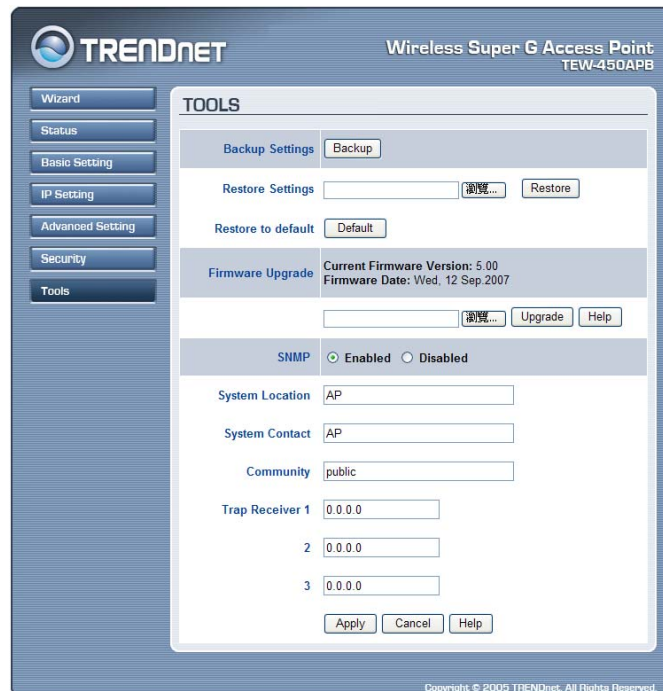
- Only deny PCs with MAC listed below to access device
- Only allow PCs with MAC listed below to access device

The maximum number of MAC addresses that can be stored is 50. You can browse through the MAC address saved by selecting the drop-down box.

For any changes made in the security page, click “**Apply**” for the changes to be effective.

3.6 Tools

Four functions are provided in this page, Backup, Restore Settings, Restore default settings and Firmware Upgrade.



Backup Settings: Click on “**Backup**” button, which will open a FileSave Dialog box, where you get to save all the current settings and configurations to a file.

Restore Settings: Click on the “**Browse**” button to open a FileOpen Dialog box, where you get to select the file, which you save previous settings and configurations. Upon selecting the saved file, click “**Restore**” and complete the restore process when the access point re-operates after it restarts.

Restore to default: Click on “**Default**” button to restore the access point back to its manufacture default settings.

Firmware Upgrade: Click on the “**Browse**” button to open a File Open Dialog box, where you get to select the firmware file, which you download from the web for the latest version. Upon selecting the firmware file, click “**Upgrade**” and complete the firmware upgrade process when the Access Point re-operates after it restarts.

SNMP: Enable or disable the SNMP function of the AP.

Glossary

Access Point: An internetworking device that seamlessly connects wired and wireless networks.

Ad-Hoc: An independent wireless LAN network formed by a group of computers, each with a network adapter.

AP Client: One of the additional AP operating modes offered by 54Mbps Access Point, which allows the Access Point to act as an Ethernet-to-Wireless Bridge, thus a LAN or a single computer station can join a wireless ESS network through it.

ASCII: American Standard Code for Information Interchange, ASCII, is one of the two formats that you can use for entering the values for WEP key. It represents English letters as numbers from 0 to 127.

Authentication Type: Indication of an authentication algorithm which can be supported by the Access Point:

1. Open System: Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any station that requests authentication with this algorithm may become authenticated if 802.11 Authentication Type at the recipient station is set to Open System authentication.

2. Shared Key: Shared Key authentication supports authentication of stations as either a member of those who knows a shared secret key or a member of those who does not.

Backbone: The core infrastructure of a network, which transports information from one central location to another where the information is unloaded into a local system.

Bandwidth: The transmission capacity of a device, which is calculated by how much data the device can transmit in a fixed amount of time expressed in bits per second (bps).

Beacon: A beacon is a packet broadcast by the Access Point to keep the network synchronized. Included in a beacon are information such as wireless LAN service area, the AP address, the Broadcast destination addresses, time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

Bit: A binary digit, which is either 0 or 1 for value, is the smallest unit for data.

Bridge: An internetworking function that incorporates the lowest 2 layers of the OSI network protocol model.

Browser: An application program that enables one to read the content and interact in the World Wide Web or Intranet.

BSS: BSS stands for “Basic Service Set”. It is an Access Point and all the LAN PCs that associated with it.

Channel: The bandwidth which wireless Radio operates is divided into several segments, which we call them “Channels”. AP and the client stations that it associated work in one of the channels.

CSMA/CA: In local area networking, this is the CSMA technique that combines slotted time -division multiplexing with carrier sense multiple access/collision detection (CSMA/CD) to avoid having collisions occur a second time. This works best if the time allocated is short compared to packet length and if the number of situations is small.

CSMA/CD: Carrier Sense Multiple Access/Collision Detection, which is a LAN access method used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is quiet (senses the carrier). If it is not, it waits a random amount of time before retrying. If the network is quiet and two devices access the line at exactly the same time, their signals collide. When the collision is detected, they both back off and wait a random amount of time before retrying.

DHCP: Dynamic Host Configuration Protocol, which is a protocol that lets network administrators manage and allocate Internet Protocol (IP) addresses in a network. Every computer has to have an IP address in order to communicate with each other in a TCP/IP based infrastructure network. Without DHCP, each computer must be entered in manually the IP address. DHCP enables the network administrators to assign the IP from a central location and each computer receives an IP address upon plugged with the Ethernet cable everywhere on the network.

DSSS: Direct Sequence Spread Spectrum. DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Dynamic IP Address: An IP address that is assigned automatically to a client station in a TCP/IP network by a DHCP server.

Encryption: A security method that uses a specific algorithm to alter the data transmitted, thus prevent others from knowing the information transmitted.

ESS: ESS stands for "Extended Service Set". More than one BSS is configured to become Extended Service Set. LAN mobile users can roam between different BSSs in an ESS.

ESSID: The unique identifier that identifies the ESS. In infrastructure association, the stations use the same ESSID as AP's to get connected.

Ethernet: A popular local area data communications network, originally developed by Xerox Corp., that accepts transmission from computers and terminals. Ethernet operates on a 10/100 Mbps base transmission rate, using a shielded coaxial cable or over shielded twisted pair telephone wire.

Fragmentation: When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium.

Fragmentation Threshold: The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages. The purpose of "Fragmentation Threshold" is to increase the transfer reliability thru cutting a MAC Service Data Unit (MSDU) into several MAC Protocol Data Units (MPDU) in smaller size. The RF transmission can not allow to transmit too big frame size due to the heavy interference caused by the big size of transmission frame. But if the frame size is too small, it will create the overhead during the transmission.

Gateway: a device that interconnects networks with different, incompatible communication protocols.

HEX: Hexadecimal, HEX, consists of numbers from 0 – 9 and letters from A – F.

IEEE: The Institute of Electrical and Electronics Engineers, which is the largest technical professional society that promotes the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession. The IEEE fosters the development of standards that often become national and international standards.

Infrastructure: An infrastructure network is a wireless network or other small network in which the wireless network devices are made a part of the network through the Access Point which connects them to the rest of the network.

ISM Band: The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4GHz, in particular, is being made available worldwide.

MAC Address: Media Access Control Address is a unique hex number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

Multicasting: Sending data to a group of nodes instead of a single destination.

Multiple Bridge – One of the additional AP operating modes offered by 54Mbps Access Point, which allows a group of APs that consists of two or more APs to connect two or more Ethernet networks or Ethernet enabled clients together. The way that multiple bridge setups is based on the topology of Ad-Hoc mode.

Node: A network junction or connection point, typically a computer or workstation.

Packet: A unit of data routed between an origin and a destination in a network.

PLCP: Physical layer convergence protocol

PPDU: PLCP protocol data unit

Preamble Type: During transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. Two different preambles and headers are defined as the mandatory supported long preamble and header which interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999, and an optional short preamble and header. At the receiver, the PLCP preamble and header are processed to aid in demodulation and delivery of the PSDU. The optional short preamble and header is intended for application where maximum throughput is desired and interoperability with legacy and non-short-preamble capable equipment is not consideration. That is, it is expected to be used only in networks of like equipment that can all handle the optional mode. (IEEE 802.11b standard)

PSDU: PLCP service data unit

Roaming: A LAN mobile user moves around an ESS and enjoys a continuous connection to an Infrastructure network.

RTS: Request To Send. An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit.

RTS Threshold: Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this “Hidden Node Problem”. If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Subnet Mask: The method used for splitting IP networks into a series of sub-groups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

TCP/IP: Transmission Control Protocol/ Internet Protocol. The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network, i.e. intranet or internet. When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

Throughput: The amount of data transferred successfully from one point to another in a given period of time.

WEP: Wired Equivalent Privacy (WEP) is an encryption scheme used to protect wireless data communication. To enable the icon will prevent other stations without the same WEP key from linking with the AP.

Wireless Bridge – One of the additional AP operating modes offered by 54mpbs Access Point, which allows a pair of APs to act as the bridge that connects two Ethernet networks or Ethernet enabled clients together.

Limited Warranty

TRENDware 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-450APB – 3 Years Warranty

If a product does not operate as warranted above during the applicable warranty period, TRENDware shall, at its option and expense, repair the defective product or part, deliver to customer an equivalent product or part to replace the defective item, or refund to customer the purchase price paid for the defective product. All products that are replaced will become the property of TRENDware. Replacement products may be new or reconditioned.

TRENDware 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 TRENDware 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 TRENDware office within the applicable warranty period for a Return Material Authorization (RMA) number, accompanied by a copy of the dated proof of the purchase. Products returned to TRENDware must be pre-authorized by TRENDware with RMA number marked on the outside of the package, and sent prepaid, insured and packaged appropriately for safe shipment.

WARRANTIES EXCLUSIVE: IF THE TRENDWARE PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDWARE'S OPTION, REPAIR OR REPLACEMENT. 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. TRENDWARE NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDWARE'S PRODUCTS.

TRENDWARE 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 TRENDWARE 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 TRENDWARE'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.

AC/DC Power Adapter, Cooling Fan, Cables and Power Supply carry 1 Year Warranty



TRENDNET®

Customer Support

Visit www.trendnet.com/support

Email:

support@trendnet.com



Europe (Germany • France • Italy • Spain • Switzerland • UK)

Toll Free Telephone: +00800 60 76 76 67

English/Espanol - 24/7

Francais/Deutsch - 11am-8pm, Monday - Friday MET

Worldwide

Telephone: +[31] (0) 20 504 05 35

English/Espanol - 24/7

Francais/Deutsch - 11am-8pm, Monday - Friday MET

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