TEW-430APB

54Mbps 802.11g Wireless Access Point

User's Guide

TRENDnet®

TRENDware, USA

What's Next in Networking

Regulatory notes and statements

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions, however, are far much less than the electromagnetic energy emissions from wireless devices (e.g. mobile phones). Wireless LAN devices are safe for use, meeting frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

·On board of airplanes, or

·In an explosive environment, or

·In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user’s authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

USA-FCC (Federal Communications Commission) statement

This device complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause interference, and

2. This device must accept any interference, including interference that may cause undesired operation of this device.

FCC Radio Frequency Exposure statement

This Wireless LAN radio device has been evaluated under FCC Bulletin OET 65 and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices.

The radiated output power of this Wireless LAN device is far below the FCC radio frequency exposure limits. Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation is minimized.

When nearby persons have to be kept to ensure RF exposure compliance, in order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antennas and the user should not be less than 20 cm.

FCC 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. If not installed and used in accordance with the instructions, it 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 and correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.

2. Increase the distance between the equipment and the receiver.

3. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

4. Consult the dealer or an experienced radio/TV technician for help.

Export restrictions

This product or software contains encryption code that may not be exported or transferred from the US of Canada without an approved US Department of Commerce export license.

Safety Information

Your device contains a low power transmitter. When device is transmitted it sends out radio frequency (RF) signal.

CAUTION: To maintain compliance with FCC’s RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body, and used on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1, EN 301 489-17 and EN 55024 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328-2 has been conducted. These are considered relevant and sufficient.

CE in which Countries where the product may be used freely:

Germany, UK, Italy, Spain, Belgium, Netherlands, Portugal, Greece, Ireland, Denmark, Luxembourg, Austria, Finland, Sweden, Norway and Iceland.

France: The use of other channels that the channel 10 through 13 is prohibited by law.

TABLE OF CONTENT

ABOUT THIS GUIDE

Congratulations on your purchase of this IEEE 802.11g Wireless LAN Access Point. This manual helps to feature the innovating wireless technology that can help you build a wireless network easily! This manual contains detailed instructions in operation of this product. Please keep this manual for future reference.

With a WLAN (IEEE 802.11g) Access Point, a mobile computer can share data with another mobile computer in a wireless way. Easy-to-use utilities are bundled with WLAN Access Point for configuration and monitoring purposes.

WLAN networking can wirelessly transmit and receive data, minimizing the need for wired connections, at a speed of up to eleven megabit per second. With WLAN networking, you can locate your PC wherever you want without wires and cables.

WLAN networking provides users with an access to real-time information anywhere in their organization. The mobility provides productivity and service, which are not available under wired networks.

Purpose

This manual discusses how to install the WLAN Access Point.

Overview of this User’s Guide

Introduction. Describes the WLAN Access Point and its features.

Unpacking and Setup. Helps you get started with the basic installation of the WLAN Access Point.

Hardware Installation. Describes the LED indicators of the AP.

Software Installation. Tells how to setup the driver and the utility setting.

Technical Specifications. Lists the technical (general, physical and environmental) specifications of the WLAN Access Point.

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Access Point.

Unpacking

Open the box of the Access Point and carefully unpack it. The box should contain the following items:

- One Wireless Access Point
- One External Power Adapter
- One Quick Installation Guide
- One CD-Rom (User's guide)

If any item is found missing or damaged, please contact your local reseller for replacement.

Setup

The setup of the Wireless Access Point can be performed using the following steps:

- Locate an optimum location for the Wireless LAN Access Point (AP). The best place for your AP is usually the center of your wireless network, in line of sight to all of your mobile stations.
- Visually inspect the Ethernet RJ45 port connector and make sure that it is fully plugged into the system's Ethernet switch/hub port.
- Fix the direction of the antennas. Try to place the AP in a position that can best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.
- Visually inspect if the Power Adapter was fully plugged to the device power jack.

HARDWARE INSTALATION

LED Indicator

The figure below shows the LED Indicator of the Wireless LAN Access Point.

PWR/Power

This indicator lights green when the Access Point receives power. Otherwise, it turns off.

LAN (Link/ACT)

This indicator lights green when the LAN port is connected to a 100Mbps Ethernet station, the indicator blinks green while transmitting or receiving data on the 100Mbps Ethernet network.

WLAN (Link)

This indicator always blinks green while the wireless AP is always broadcasting packets.

Rear Panel

The figure below shows the rear panel of the Access Point

Ethernet

Ethernet uplink port with auto-sensing for connecting to either 10/100Mbps Fast Ethernet connections, connect this port to switch/hub.

Reset

The Reset function is to reset the setting back to factory default setting, once you press the "RESET" button within 10 seconds, the LED of the WLAN will turn off. And when the Access Point is ready, the WLAN LED will start blinking.

And the other function is when the AP is locked; press the reset button to unlock it.

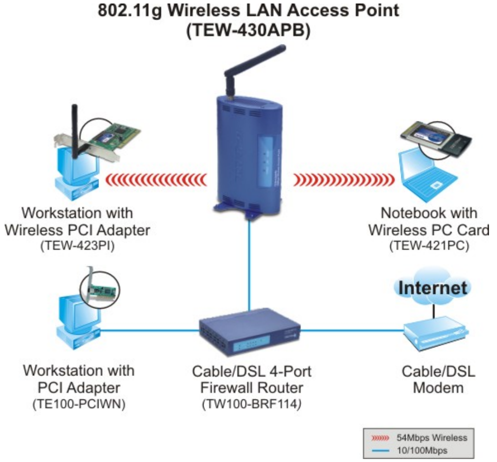
DC Power

Connect the Power Adapter DC plug to the AP's power jack.

Antenna

This is a detachable antenna. It can be replaced with high-gain antenna to extend wireless connectivity.

Hardware connections



Connect to the Switch/Hub

1. Plug in one end of the RJ45 network cable to the Switch/Hub port,
2. Plug in the other end of the RJ45 network cable to the Wireless Access Point.

Check the installation

The control LEDs of the Access Point are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected, the Power, LAN and WLAN port link LEDs of the Internet Broadband Router will light up indicating a normal status.
2. If the LAN Port's Link indicator does not light up then check if the RJ-45 cable is firmly fed into the RJ45 port. While the LAN is linked up to the Switch/Hub, the LAN port's LED will light up.

CONFIGURING THE WIRELESS LAN ACCESS POINT

The Wireless Access Point has a Web GUI interface for configuration. The AP can be configured through the Web Browser. A network manager can manage, control and monitor the AP from the local LAN. This section indicates how to configure the AP to enable its functions.

Login to the Wireless AP through WLAN

Before configuring the Wireless AP through WLAN, make sure that the SSID, Channel and the WEP was set properly.

The default setting of the Wireless AP that you will use:

SSID: default

Channel: 6

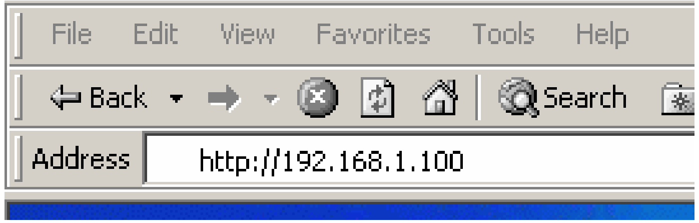
WEP Encryption: disable

Login

Before you configure this device, note that when the AP is configured through an Ethernet connection, make sure the manager PC must be set on the same **IP network**. For example, when the default network address of the default IP address of the AP is ***192.168.1.100***, then the manager PC should be set at 192.168.1.x (where x is a number between 1 and 254), and the default subnet mask is 255.255.255.0.

Open Internet Explorer 5.0 or above Web browser.

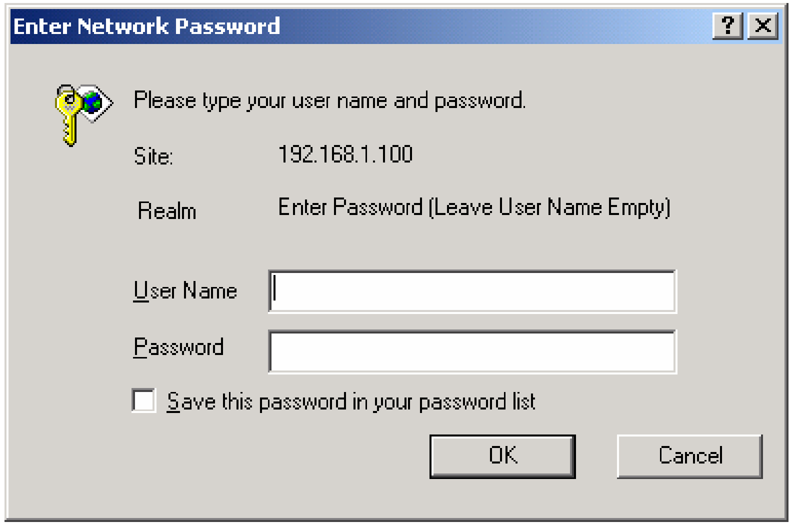
Enter IP address ***http://192.168.1.100*** (the factory-default IP address setting) to the address location.



Address http://192.168.1.100

When there is a screen to enter the Network password, type in the password you entered before. There is no need to enter any password when you first login the AP because the default setting is without a password.

Type a name or leave the username dialog box empty to login. The system will check only the password that was set in the system before.



Enter Network Password

Please type your user name and password.

Site: 192.168.1.100

Realm Enter Password (Leave User Name Empty)

User Name

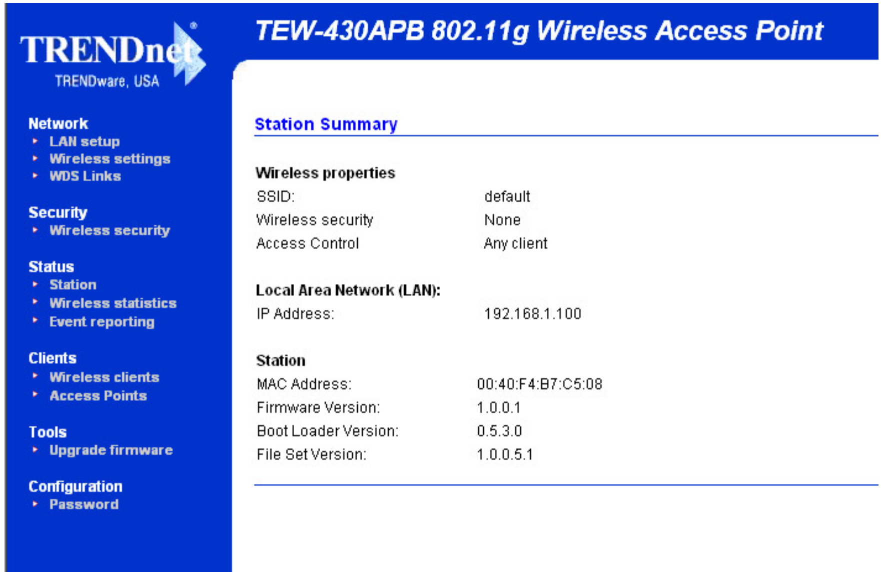
Password

□ Save this password in your password list

Main Screen of the Access Point

The screen will show the station summary of the AP when you login to the AP.

There are six main functions included in the left side of the main screen: Network, Security, Status, Clients, Tools and Configuration. Point the selections in the left side of the menu screen.



TEW-430APB 802.11g Wireless Access Point

Station Summary

Wireless properties

SSID:	default
Wireless security	None
Access Control	Any client

Local Area Network (LAN):

IP Address:	192.168.1.100

Station

MAC Address:	00:40:F4:B7:C5:08
Firmware Version:	1.0.0.1
Boot Loader Version:	0.5.3.0
File Set Version:	1.0.0.5.1

Network

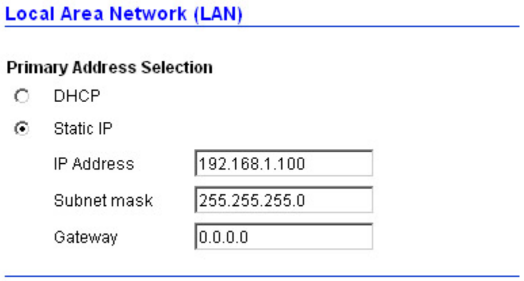
The Network Function can configure the LAN Setup, Wireless settings and WDS Links of the Access Point.

I. LAN Setup

The LAN Setup function can configure the basic LAN setting:

DHCP: Click on the DHCP for dynamic IP address allocation from the Server PCs.

Static IP: Click on the Static IP to fill up the IP Address, Subnet Mask and Gateway from the Networking Manager.



Local Area Network (LAN)

Primary Address Selection

○ DHCP

● Static IP

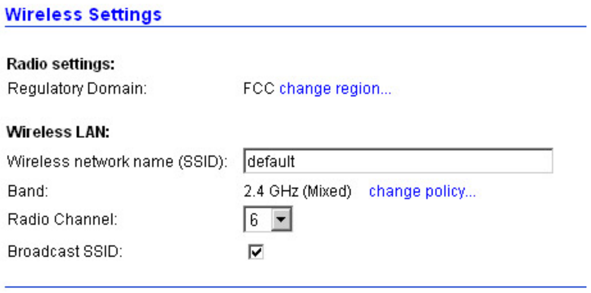
IP Address: 192.168.1.100

Subnet mask: 255.255.255.0

Gateway: 0.0.0.0

II. Wireless Settings

The Wireless Settings contain two settings, Radio Setting and Wireless LAN Setting.



Wireless Settings

Radio settings:

Regulatory Domain: FCC change region...

Wireless LAN:

Wireless network name (SSID): default

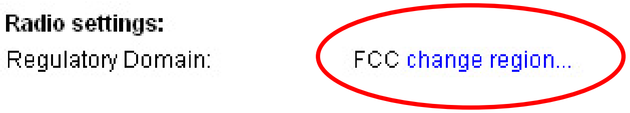
Band: 2.4 GHz (Mixed) change policy...

Radio Channel: 6

Broadcast SSID: ☑

Radio Settings: to configure the Regulatory Domain settings.

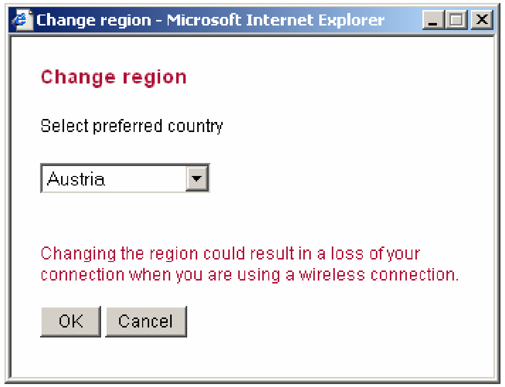
- **Regulatory Domain:** this is the channel selection of each country regulatory domain, select the country where you are using this Wireless Device, users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of these countries.



Radio settings:

Regulatory Domain: FCC change region...

Click on the change region and a window will pop out, select the region in which you are using this AP.



Change region

Select preferred country

Austria

Changing the region could result in a loss of your connection when you are using a wireless connection.

Wireless LAN Settings: to configure the wireless networking settings.

- **Wireless Network Name (SSID):** It is an ASCII string up to 32 characters used to identify a WLAN that prevents the unintentional merging of two co-located WLANs. The SSID value must be the same in all stations and AP in the extended WLAN.
- **Band:** you can select to change the radio band to mixed mode, G-only or B-only, a window will pop out to change the policy; it may result in a loss of the connection when you are using wireless connection.

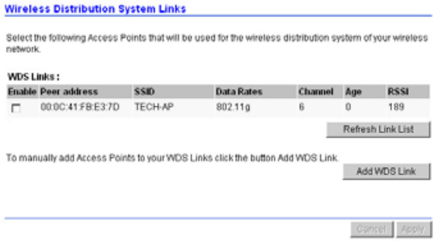
  Mixed mode: choosing this mode may allow users using both 802.11g and 802.11b.

  G-only: choosing this mode may allow users using only 802.11g.

  B-only: choosing this mode may allow users using only 802.11b.
- **Radio Channel:** there are 14 channels available due to different Regulatory Domain. The channels differ from country to country; select the channel to be used.
- **Broadcast SSID:** when enable this function, this AP will broadcast the SSID to the stations; if the function was disable, the stations must know the AP SSID in advance.

III. WDS Links

WDS (Wireless Distribution System) uses wireless media to communicate with other APs. When you enter the screen of the WDS, a list of other APs will appear. Click enable in the left side of the screen, and click apply to add the AP to your WDS Link, or click the “Add WDS Link” button to add the APs that you need to add.



Wireless Distribution System Links

Select the following Access Points that will be used for the wireless distribution system of your wireless network.

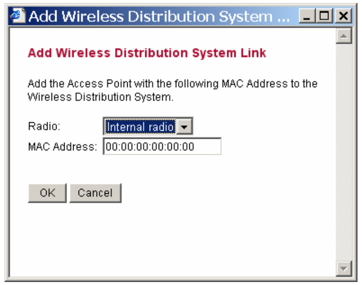
WDS Links :

Enable	Peer address	SSID	Data Rates	Channel	Age	RSSI
□	00:0C:41:FB:E3:7D	TECH-AP	802.11g	6	0	189

To manually add Access Points to your WDS Links click the button Add WDS Link.

This WDS Link will scan only other APs channel within the range of 3 channels among your AP radio channel. There are two other ways to connect to the APs that are not listed in the WDS Link.

1. Click the “Add WDS Link” button, a window will pop out, type in the MAC address of the AP that you need to communicate.
2. Change your AP radio channel within the range of 3 channels to scan the AP that you want to connect.



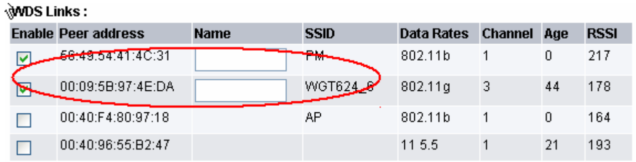
Add Wireless Distribution System Link

Add the Access Point with the following MAC Address to the Wireless Distribution System.

Radio: Internal radio

MAC Address: 00:00:00:00:00:00

After the AP is linked, type a name to identify the AP you are linking, unclick the enable box to remove the WDS Link that you set before.



WDS Links :

Enable	Peer address	Name	SSID	Data Rates	Channel	Age	RSSI
☑	56:49:54:41:4C:31		PM	802.11b	1	0	217
☑	00:09:5B:97:4E:DA		WGT624_6	802.11g	3	44	178
□	00:40:F4:80:97:18		AP	802.11b	1	0	164
□	00:40:96:55:B2:47			11 5.5	1	21	193

In Addition, make sure you configure all WDS APs to work on the same radio channel and in the same WEP key.

Security

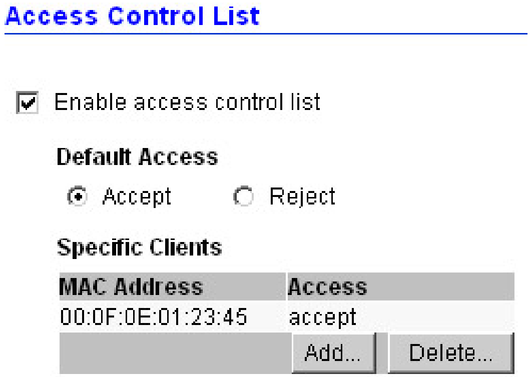
This function is used to protect wireless communication from eavesdropping. A secondary function of encryption is to prevent unauthorized access to a wireless network, and it can be achieved by using the Encryption function.

This AP provides three modes for Security Encryption, WPA, 802.1x and WEP.

I. Access Control List

Access Control function allows clients whose MAC addresses in the list will be able to connect to this Access Point. When this function is activated, no wireless clients can connect to the Access Point unless they are listed in the Access Control list.

- **Default Access:** selecting **Accept** will allow clients on the list to connect to this AP, and select **Reject** to disconnect the clients on the list.
- **Specific Clients:** add the MAC addresses of the clients that you want to connect or disconnect to this AP.



Access Control List

☑ Enable access control list

Default Access

● Accept ○ Reject

Specific Clients

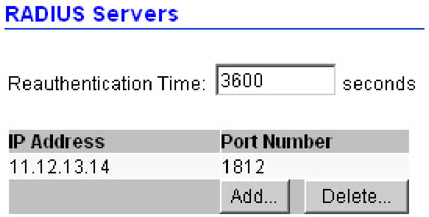
MAC Address	Access
00:0F:0E:01:23:45	accept

II. Radius Server

A RADIUS server is used to authenticate the connection for clients and return authentication key parameters to the users to connect to the wireless network.

RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.

Re-authentication Time: type in how long the seconds that you want to re-authenticate the client.

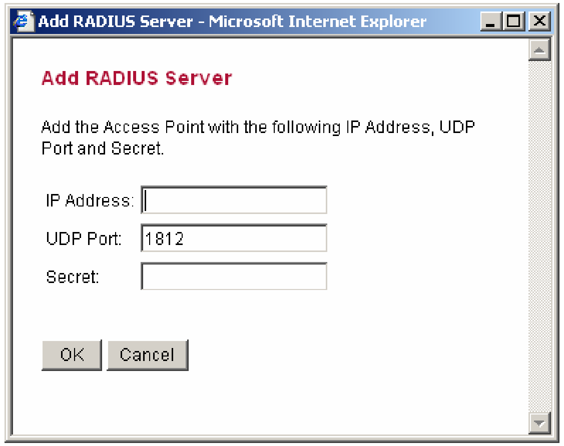


RADIUS Servers

Reauthentication Time: 3600 seconds

IP Address	Port Number
11.12.13.14	1812

Click “Add” to add the Radius Server IP Address, Server UDP port and Secret. The secret is a key between the AP and the Radius Server.



Add RADIUS Server

Add the Access Point with the following IP Address, UDP Port and Secret.

IP Address:

UDP Port: 1812

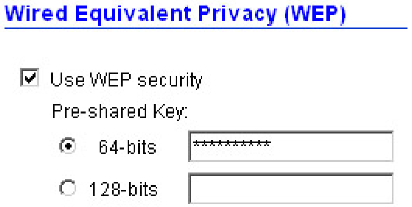
Secret:

III. Wired Equivalent Privacy (WEP)

WEP encryption implementation was not put in place with the 802.11 standard. This means that there are about as many methods of WEP encryption as there are providers of wireless networking products. In addition, WEP is not completely secure. One piece of information still not encrypted is the MAC address, which hackers can use to break into a network by spoofing (or faking) the MAC address.

When choosing the encryption to WEP mode, click the “Use WEP Security” to enable the WEP security function, here are some of the following settings:

- **64-bits:** selecting the 64bit, you must type 10 values in the following range (0~F, hexadecimal).
- **128-**bits: selecting the 128bit, you must type 26 values in the following range (0~F, hexadecimal).



Wired Equivalent Privacy (WEP)

☑ Use WEP security

Pre-shared Key:

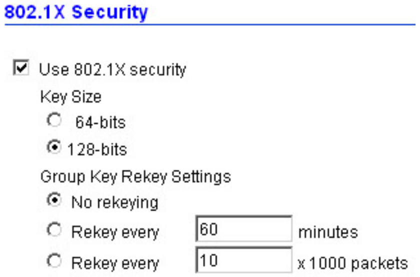
● 64-bits ***********

○ 128-bits

IV. 802.1x Security

To address the shortcomings of WEP for authentication, the industry is working towards solutions based on the 802.1x specification, which is based on the Extensible Authentication Protocol (EAP). EAP was designed with flexibility in mind, and it has been used as the basis for a number of network authentication extensions.

Click to enable the 802.1x security function.



802.1X Security

☑ Use 802.1X security

Key Size

○ 64-bits

● 128-bits

Group Key Rekey Settings

● No rekeying

○ Rekey every 60 minutes

○ Rekey every 10 x 1000 packets

- **Key Size:** selecting the 64bit or 128-bit for the key size of the 802.1x security.
- **Group Key Setting:**

No Rekeying: the client will not need to re-key the password to authenticate with the Radius Server.

Rekeying Time: type in the time for clients to re-key the password for authentication and security.

Rekeying packets: type in the numbers of packets in which the manager wants to control every client to re-key the password when the number of every 1000 packets was transmitted.

V. Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption.

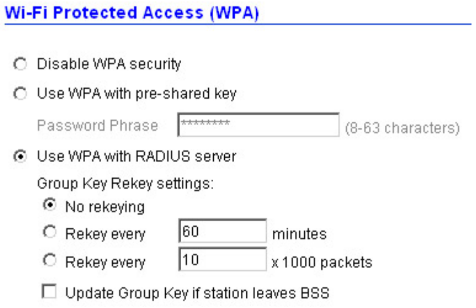
- **Disable WPA Security:** to disable the WPA security.
- **Use WPA with Pre-Shared Key:** type in 8 ~ 63 characters inside the dialog box to have the WPA password between the AP and the clients.
- **Use WPA with Radius Server:** the authentication between the Radius Server, the AP and the clients using the Group Key Re-key Settings.

No Rekeying: the clients will not need to re-key the password to authenticate with the Radius Server.

Rekeying Time: type in the time for when the manager want clients to re-keying the password for authentication and security.

Rekeying packets: type in the numbers of packets in which the manager want to control every client to re-key the password when the number of every 1000 packets was transmitted.

- **Update Group Key:** to update the password when the station or the client leaves the Networking Group (BSS, Basic Service Set).



Wi-Fi Protected Access (WPA)

○ Disable WPA security

○ Use WPA with pre-shared key

Password Phrase ******** (8-63 characters)

● Use WPA with RADIUS server

Group Key Rekey settings:

● No rekeying

○ Rekey every 60 minutes

○ Rekey every 10 x 1000 packets

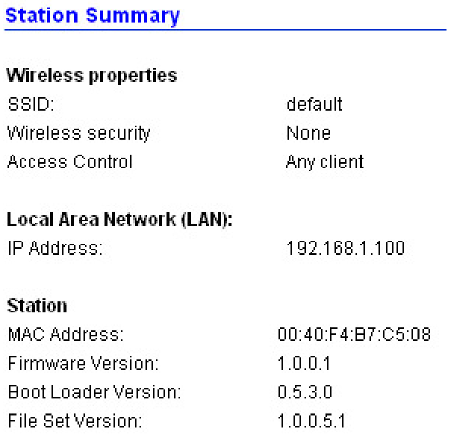
□ Update Group Key if station leaves BSS

Status

This function will show the statistics of the Station, Wireless Statistics and Event Reporting.

I. Station

This screen will show the status summary of the system.



Station Summary

Wireless properties

SSID:	default
Wireless security	None
Access Control	Any client

Local Area Network (LAN):

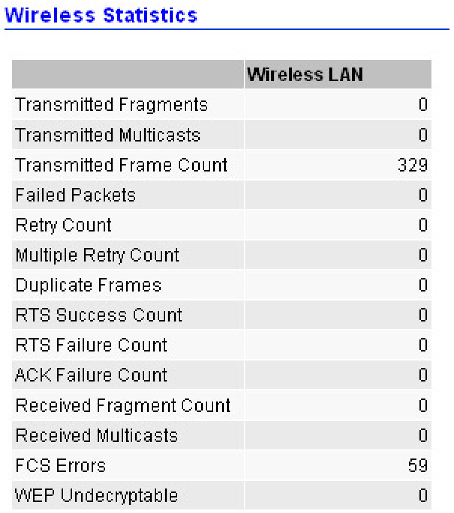
IP Address:	192.168.1.100

Station

MAC Address:	00:40:F4:B7:C5:08
Firmware Version:	1.0.0.1
Boot Loader Version:	0.5.3.0
File Set Version:	1.0.0.5.1

II. Wireless Statistics

This screen shows the statistics of the wireless AP.

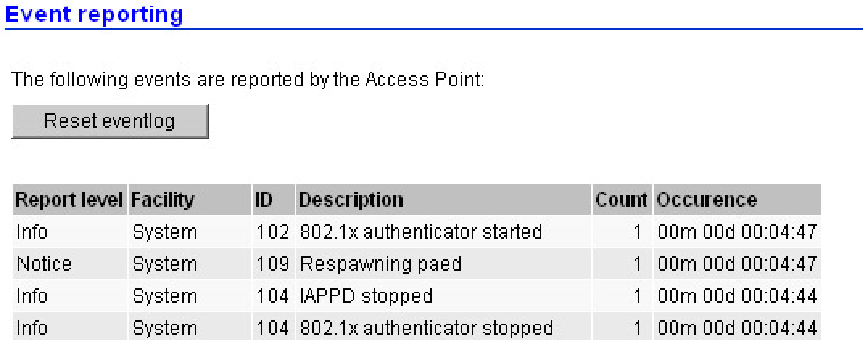


Wireless Statistics

	Wireless LAN
Transmitted Fragments	0
Transmitted Multicasts	0
Transmitted Frame Count	329
Failed Packets	0
Retry Count	0
Multiple Retry Count	0
Duplicate Frames	0
RTS Success Count	0
RTS Failure Count	0
ACK Failure Count	0
Received Fragment Count	0
Received Multicasts	0
FCS Errors	59
WEP Undecryptable	0

III. Event Report

This screen shows the event happened on the AP, press “Reset Event Log” to clear the record of the event happened.



Event reporting

The following events are reported by the Access Point:

Reset eventlog

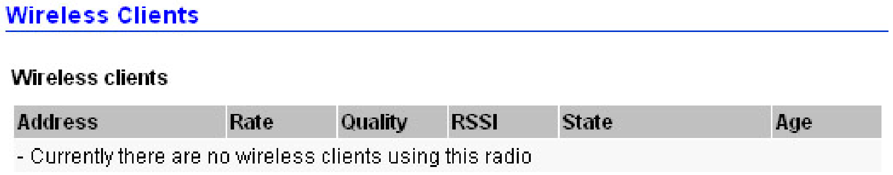
Report level	Facility	ID	Description	Count	Occurence
Info	System	102	802.1x authenticator started	1	00m 00d 00:04:47
Notice	System	109	Respawning paed	1	00m 00d 00:04:47
Info	System	104	IAPPD stopped	1	00m 00d 00:04:44
Info	System	104	802.1x authenticator stopped	1	00m 00d 00:04:44

Clients

This function shows the list of the wireless surrounded this AP.

I. Wireless Clients

This function shows the list of the wireless clients that connected to this AP.



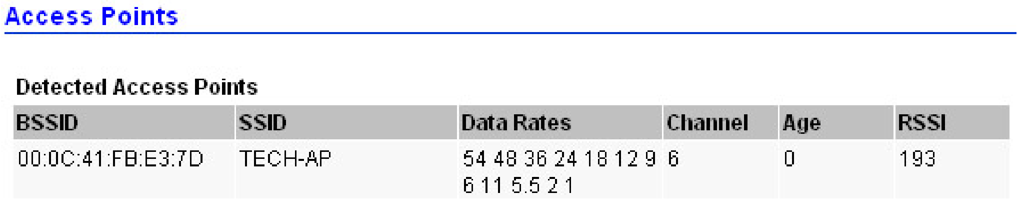
Wireless Clients

Wireless clients

Address	Rate	Quality	RSSI	State	Age
- Currently there are no wireless clients using this radio					

II. Access Points

This function shows the list of the Wireless Access Point that this AP can connect with, this is the list that you can use for WDS Links, refer to WDS Links on page 9.



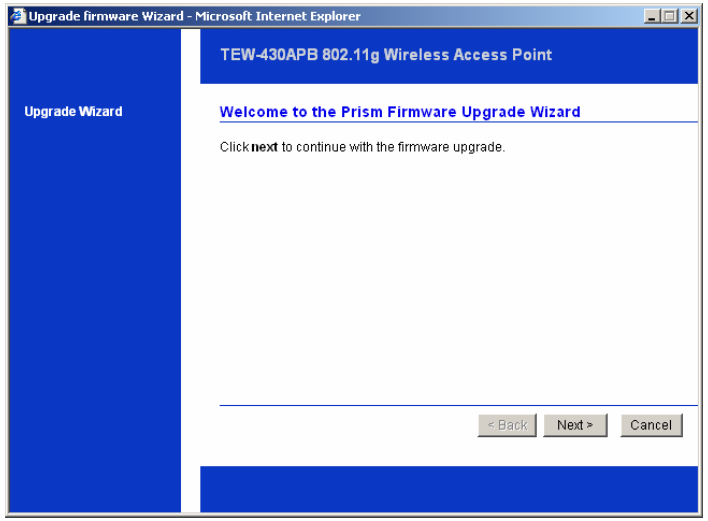
Access Points

Detected Access Points

BSSID	SSID	Data Rates	Channel	Age	RSSI
00:0C:41:FB:E3:7D	TECH-AP	54 48 36 24 18 12 9 6 11 5.5 2 1	6	0	193

Tools

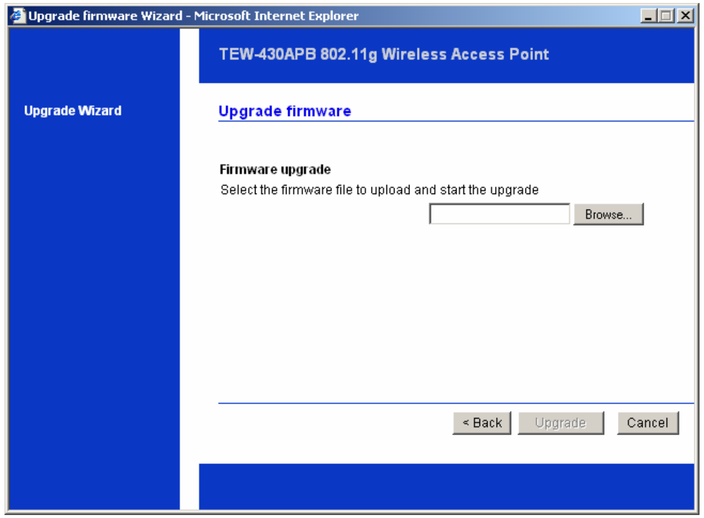
This function will help you to upgrade the firmware of the AP, press the "Upgrade Firmware" button in the left side of the menu screen and a window will pop out.


Upgrade firmware Wizard - Microsoft Internet Explorer
TEW-430APB 802.11g Wireless Access Point
Upgrade Wizard
< Back
Next >
Cancel

Welcome to the Prism Firmware Upgrade Wizard

Click **next** to continue with the firmware upgrade.

Press "Next ".

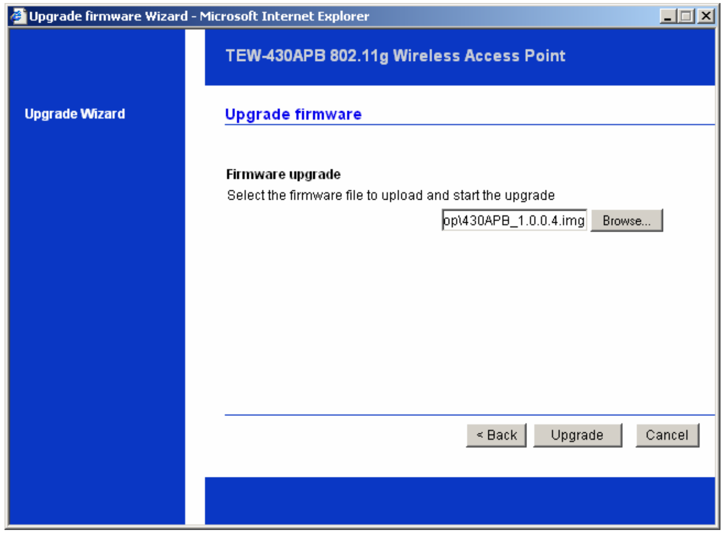

Upgrade firmware Wizard - Microsoft Internet Explorer
TEW-430APB 802.11g Wireless Access Point
Upgrade Wizard
Browse...
< Back
Upgrade
Cancel

Upgrade firmware

Firmware upgrade

Select the firmware file to upload and start the upgrade

Type the firmware file that you need to upgrade inside the box, or press the "Browse" button to find the firmware file location.


Upgrade firmware Wizard - Microsoft Internet Explorer
TEW-430APB 802.11g Wireless Access Point
Upgrade Wizard
Browse...
< Back
Upgrade
Cancel

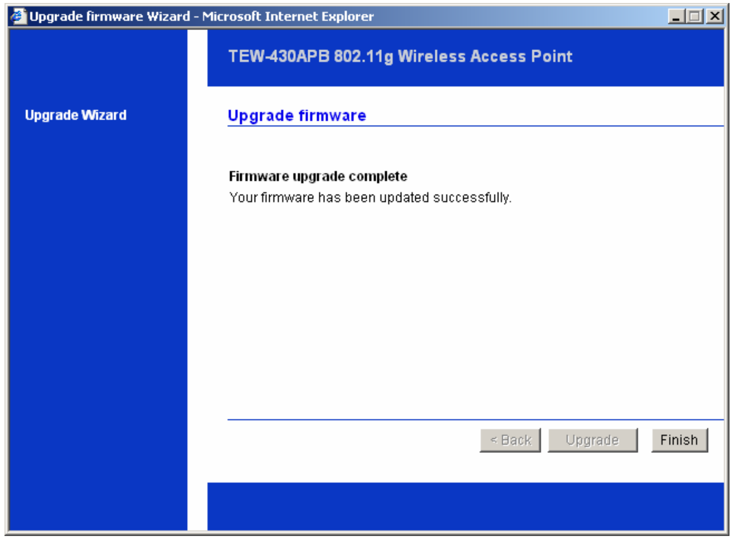
Upgrade firmware

Firmware upgrade

Select the firmware file to upload and start the upgrade

op\430APB_1.0.0.4.img

When finish uploading the file to the AP, ***do not power off the AP until the finish screen appears.***


Upgrade firmware Wizard - Microsoft Internet Explorer
TEW-430APB 802.11g Wireless Access Point
Upgrade Wizard
< Back
Upgrade
Finish

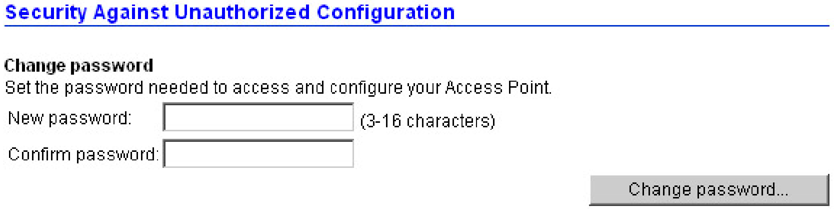
Upgrade firmware

Firmware upgrade complete

Your firmware has been updated successfully.

I. Change Password

This function will help you to configure the password of the AP, type in the new password inside the New password and Confirm password dialog box, and press the “Change password” button to activate this function.



Security Against Unauthorized Configuration

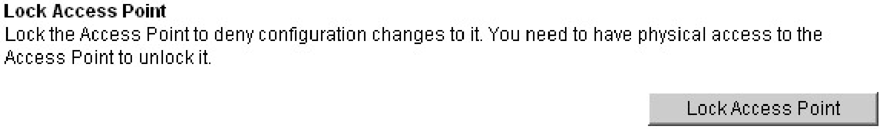
Change password
Set the password needed to access and configure your Access Point.

New password: (3-16 characters)

Confirm password:

II. Lock Access Point

Lock the Access Point to deny configuration changes to it. You need to have physical access to the Access Point to unlock it, press the reset button on the rear panel of the AP to unlock.



Lock Access Point
Lock the Access Point to deny configuration changes to it. You need to have physical access to the Access Point to unlock it.

TECHNICAL SPECIFICATIONS

General	
Standards	Standard: IEEE 802.11g IEEE 802.3u 10/100BASE-TX Fast Ethernet
Signal Type:	OFDM (Orthogonal Frequency Division Multiplexing)
Modulation:	QPSK / BPSK / CCK / OFDM
LED Indicators:	Power, LAN (Link/Activity), WLAN (Link)
Frequency Range	2412 ~ 2484 MHz ISM band (channels 1 ~ 14)
Frequency Band:	2.4 GHz
Channel:	1 ~ 11 Channels (US, Canada, China) 1 ~ 13 Channels (Europe) 1 ~ 14 Channels (Japan)
Data Encryption:	64 bit / 128 bit WEP Encryption, WPA
Data Transfer Rate	Fast Ethernet: 100Mbps Wireless: Up to 54Mbps (with Automatic Scale Back)
Receiver Sensitivity	54Mbps: Typical -68dBm @10% PER 1Mbps: Typical -81dBm @8% PER
Transmit Power	802.11g: Minimum 12dBm typically 802.11b: Minimum 15dBm typically
Transmission Range:	Outdoor: 100~300M (depends on environment) Indoor: 50~100M (depends on environment)
Network Cables	10BASET: 2-pair UTP Cat. 3,4,5 (100 m), EIA/TIA- 568 100-ohm STP (100 m)
Interface	1 x 10/100Mbps RJ45 port
Antenna:	1 x 2dBi Diversity Antenna
Physical and Environmental	
DC inputs	DC 5V, 1.2A
Power Consumption	6W (Max)
Temperature	Operating: 0° ~ 40° C, Storage: -10° ~ 70° C
Humidity	Operating: 10% ~ 90%, Storage: 5% ~ 90%
Dimensions	124 x 86 x 40 mm (4.9 x 3.4 x 1.6 inches) (without antenna)
EMI:	FCC Class B, CE Mark B,

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.

Wireless Products – 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, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW 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 DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 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.

Technical Support

You can find the most recent driver/firmware/software and user documentations on the **TRENDware website**. **TRENDware** provides **FREE technical support** for all customers for the duration of the warranty period on this product.

TRENDware Technical Support
Tel: +1-310-626-6252
Fax: +1-310-626-6267

E-mail: support@trendware.com
www.TRENDnet.com

Monday ~ Friday, 7:30AM ~ 6:00PM Pacific Standard Time
(Except holidays)

TRENDnet®

TRENDware, USA

What's Next in Networking

Product Warranty Registration

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

TRENDware International, Inc.
3135 Kashiwa Street
Torrance, CA 90505

http://www.TRENDNET.com