



Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for TRENDNET TEW-453APB. You'll find the answers to all your questions on the TRENDNET TEW-453APB in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual TRENDNET TEW-453APB
User guide TRENDNET TEW-453APB
Operating instructions TRENDNET TEW-453APB
Instructions for use TRENDNET TEW-453APB
Instruction manual TRENDNET TEW-453APB



Copyright ©2005. All Rights Reserved. TRENDware International, Inc.



[You're reading an excerpt. Click here to read official TRENDNET TEW-453APB user guide](http://yourpdfguides.com/dref/3181063)
<http://yourpdfguides.com/dref/3181063>

Manual abstract:

.....
.....
.....

.....
.....
.....

.....
.....
.....

.... 6 Requirements.....

.....
.....

.....
.....
.....

.....
.....
.....

.....
.....
.....

. 6 Procedure

.....
.....

.....
.....
.....

.....
.....
.....

.....
.....
.....

.... 6 CHAPTER 3 ACCESS POINT SETUP

.....
.....

.....
.....
.....

.....
.....
.....
.....
.....
. 13 Security Profiles.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.. 15 Security Profile Screen...

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

.. 19 System Screen

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

. 35 Wireless Screens

.....

.....
.....
.....
.....

.....
.....
.....
.....
.....
.....
.....
.....

..... 37 Basic Settings Screen....

.....
.....
.....
.....
.....
.....

.....
.....
.....
.....

.....
.....

.... 37 Advanced Settings .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 40 CHAPTER 4 PC AND SERVER CONFIGURATION

.....
.....
.....

.....
.....
.....
.....

. 42 Overview

.....
.....
.....

.....
.....
.....
.....

.....

.....

.....

.....

.....

.....

.....

.... 45 802.

1x Client Setup on Windows XP

.....

.....

.....

.....

.....

.....

.....

.....

.. 55 Using 802.1x Mode (without WPA)

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.. 61 CHAPTER 5 OPERATION AND STATUS

.....

.....

.....

.....

.....

.....

.....

.....

..... 62 Operation

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....
. 69 Auto Config/Update

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 71 Config File.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 73 Syslog Log Settings.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 75 Rogue APs

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....
. 76 SNMP

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 77 Upgrade Firmware ..

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

..... 78 APPENDIX A SPECIFICATIONS .

.....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

. 79 Wireless Access Point....

.....
.....
.....
.....

.....
.....
.....

.....
.....
.....
.....

.....
.....
.....

... 79 APPENDIX B TROUBLESHOOTING

.....
.....
.....

.....
.....
.....
.....

... 83 Overview ..

.....
.....

.....
.....
.....

.....
.....
.....

.....
.....
.....

83 General Problems

.....

.....
.....
.....

.....
.....
.....

.....
.....
.....

... 83 APPENDIX C WINDOWS TCP/IP.....

.....
.....

.....
.....
.....
.....
.....
.....
.....
.....
.....

85 Overview

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

.. 85 Checking TCP/IP Settings - Windows 9x/ME:

.....
.....
.....
.....
.....
.....

... 85 Checking TCP/IP Settings - Windows NT4.0

.....
.....
.....
.....
.....
.....

..... 87 Checking TCP/IP Settings - Windows 2000...

.....
.....
.....
.....
.....
.....

... 89 Checking TCP/IP Settings - Windows XP ..

.....
.....
.....

.....
.....
.....
.....

. 91 i APPENDIX D ABOUT WIRELESS LANS.....

.....
.....
.....
.....
.....
.....
.....

..... 93 Overview

.....
.....
.....
.....
.....
.....

.....
.....
.....
.....
.....
.....

..... 93 Wireless LAN Terminology ...

.....
.....
.....
.....
.....
.....

.....
.....
.....
.....

..... 93 APPENDIX E COMMAND LINE INTERFACE .

.....
.....
.....
.....
.....
.....

... 96 Overview ..

The Wireless Access Point can login to your existing Radius Server (as a Radius client). Radius MAC Authentication. You can centralize the checking of Wireless Station MAC addresses by using a Radius Server. Rogue AP Detection. The Wireless Access Point can detect unauthorized (Rogue) Access Points on your LAN. Access Control.

The Access Control feature can check the MAC address of Wireless clients to ensure that only trusted Wireless Stations can use the Wireless Access Point to gain access to your LAN. Password - protected Configuration. Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings. · 2 Introduction Advanced Features · Auto Configuration. The Wireless Access Point can perform self-configuration by copying the configuration data from another Access Point.

This feature is enabled by default. · Auto Update. The Wireless Access Point can automatically update its firmware, by downloading and installing new firmware from your FTP server. Command Line Interface. If desired, the command line interface (CLI) can be used for configuration.

This provides the possibility of creating scripts to perform common configuration changes. · NetBIOS & WINS Support. Support for both NetBIOS broadcast and WINS (Windows Internet Naming Service) allows the Wireless Access Point to easily fit into your existing Windows network. Radius Accounting Support. If you have a Radius Server, you can use it to provide accounting data on Wireless clients. Syslog Support. If you have a Syslog Server, the Wireless Access Point can send its log data to your Syslog Server. SNMP Support. SNMP (Simple Network Management Protocol) is supported, allowing you to use a SNMP program to manage the Wireless Access Point.



[You're reading an excerpt. Click here to read official TRENDNET](#)

[TEW-453APB user guide](#)

<http://yourpdfguides.com/dref/3181063>

UAM Support.

The Wireless Access Point supports UAM (Universal Access Method), making it suitable for use in Internet cafes and other sites where user access time must be accounted for. WDS Support. Support for WDS (Wireless Distribution System) allows the Wireless Access Point to act as a Wireless Bridge. Both Point-to-Po the LAN cable to the powered Ethernet port on a suitable PoE Adapter. (24V DC, 500mA) 4. Connect the unpowered Ethernet port on the PoE adapter to your Hub or switch. 5. Connect the power supply to the PoE adapter and power up. 6. Check the LEDs on the Wireless Access Point to see it is drawing power via the Ethernet connection.

Figure 5: Using PoE (Power over Ethernet) Warning! Ensure the PoE power source (PoE Adapter) meets the IEEE 802.3af standards. Otherwise, the Access Point may be damaged. 7 Chapter 3 Access Point Setup This Chapter provides details of the Setup process for Basic Operation of your Wireless Access Point. 3 Overview This chapter describes the setup procedure to make the Wireless Access Point a valid device on your LAN, and to function as an Access Point for your Wireless Stations.

Wireless Stations may also require configuration. For details, see Chapter 4 - Wireless Station Configuration. The Wireless Access Point can be configured using either the supplied Windows utility or your Web Browser Setup using the Windows Utility A simple Windows setup utility is supplied on the CD-ROM. This utility can be used to assign a suitable IP address to the Wireless Access Point. Using this utility is recommended, because it can locate the Wireless Access Point even if it has an invalid IP address.

Installation 1. 2. 3. Insert the supplied CD-ROM in your drive. If the utility does not start automatically, run the SETUP program in the root folder. Follow the prompts to complete the installation. Main Screen Start the program by using the icon created by the setup program. The program then searches the network for all active Wireless Access Points and lists them as shown below. Figure 6: Management utility Screen 8 Access Point Setup Wireless Access Points The main panel displays a list of all Wireless Access Points found on the network. For each Access Point, the following data is shown: Name IP address MAC Address IEEE Standard FW Version Description This is the default name, as shown on a sticker on the base of the device.

The IP address for the Wireless Access Point. The hardware or physical address of the Wireless Access Point. The wireless standard or standards used by the Wireless Access Point (e.g. 802.11b, 802.11g) The current Firmware version installed in the Wireless Access Point. Any extra information for the Wireless Access Point, entered by the administrator. By default, this will be blank. Note: If the desired Wireless Access Point is not listed, check that the device is installed and ON, then update the list by clicking the Refresh button.

Buttons Refresh Detail Info Web Management Click this button to update the Wireless Access Point device listing after changing the name or IP Address. When clicked, additional information about the selected Access Point will be displayed. Use this button to connect to the Wireless Access Point's Webbased management interface. This will be grayed out if the current IP address is not valid on your LAN. Set IP Address Click this button if you want to change the IP Address of the Wireless Access Point.

This is required if the current IP address is not valid on your LAN. In that case, click this button, and enter an unused IP address from the IP address range used on your LAN. Exit Exit the Management utility program by clicking this button. 9 Wireless Access Point User Guide Setup Procedure 1. 2.

3. 4. 5. 6. Select the desired Wireless Access Point. Click the Set IP Address button. If prompted, enter the user name and password. The default values are admin for the User Name, and password for the Password. Ensure the IP address, Network Mask, and Gateway are correct for your LAN. Save any changes.

Click the Web Management button to connect to the selected Wireless Access Point using your Web Browser. If prompted, enter the User Name and Password again. Check the following screens, and configure as necessary for your environment. Use the on-line help if necessary. The later sections in this Chapter also provides more details about each of these screens. . . . 7. Access Control - MAC level access control. Security Profiles - Wireless security. System - Identification, location, and Network settings · Wireless - Basic & Advanced You may also wish to set the admin password and administration connection options. These are on the Admin Login screen accessed from the Management menu.

See Chapter 6 for details of the screens and features available on the Management menu. Use the Apply/Restart button on the menu to apply your changes and restart the Wireless Access Point. 8. Setup is now complete. Wireless stations must now be set to match the Wireless Access Point.

See Chapter 4 for details. 10 Access Point Setup Setup using a Web Browser Your Browser must support JavaScript. The configuration program has been tested on the following browsers: . . . Netscape V4.08 or later Internet Explorer V4 or later Setup Procedure Before commencing, install the Wireless Access Point in your LAN, as described previously. 1.

Check the Wireless Access Point to determine its Default Name. This is shown on a label on the base or rear, and is in the following format: SCxxxxx Where xxxxxx is a set of 6 Hex characters (0 ~ 9, and A ~ F). 2. Use a PC which is already connected to your LAN, either by a wired connection or another Access Point. . . . Until the Wireless Access Point is configured, establishing a Wireless connection to it may be not possible. 3. 4. If your LAN contains a Router or Routers, ensure the PC used for configuration is on the same LAN segment as the Wireless Access Point. Start your Web browser. In the Address box, enter "HTTP:// and the Default Name of the Wireless Access Point e.

g. HTTP://SC2D631A You should then see a login prompt, which will ask for a User Name and Password. Enter admin for the User Name, and password for the Password. These are the default values. The password can and should be changed. Always enter the current user name and password, as set on the Admin Login screen. 5. Figure 7: Password Dialog 6. You will then see the Status screen, which displays the current settings and status. No data input is possible on this screen.

See Chapter 5 for details of the Status screen. 11 Wireless Access Point User Guide 7. From the menu, check the following screens, and configure as necessary for your environment. Details of these screens and settings are described in the following sections of this chapter. . . . Access Control - MAC level access control.

Security Profiles - Wireless security. System - Identification, location, and Network settings 8.



[You're reading an excerpt. Click here to read official TRENDNET TEW-453APB user guide](http://yourpdfguides.com/dref/3181063)
<http://yourpdfguides.com/dref/3181063>

· Wireless - Basic & Advanced You may also wish to set the admin password and administration connection options. These are on the Admin Login screen accessed from the Management menu. See Chapter 6 for details of the screens and features available on the Management menu.

Use the Apply/Restart button on the menu to apply your changes and restart the Wireless Access Point. 9. Setup is now complete. Wireless stations must now be set to match the Wireless Access Point. See Chapter 4 for details. If you can't connect: It is likely that your PC's IP address is incompatible with the Wireless Access Point's IP address. This can happen if your LAN does not have a DHCP Server. The default IP address of the Wireless Access Point is 192.168.0.

228, with a Network Mask of 255.255.255.0. If your PC's IP address is not compatible with this, you must change your PC's IP address to an unused value in the range 192.168.0.1 ~ 192.168.0.

254, with a Network Mask of 255.255.255.0. See Appendix C - Windows TCP/IP for details for this procedure.

12 Access Point Setup Access Control This feature can be used to block access to your LAN by unknown or untrusted wireless stations. Click Access Control on the menu to view a screen like the following. Figure 8: Access Control Screen Data - Access Control Screen Enable Use this checkbox to Enable or Disable this feature as desired. Warning ! Ensure your own PC is in the "Trusted Wireless Stations" list before enabling this feature. Trusted Stations This table lists any Wireless Stations you have designated as "Trusted".

If you have not added any stations, this table will be empty. For each Wireless station, the following data is displayed: · · · Buttons Modify List To change the list of Trusted Stations (Add, Edit, or Delete a Wireless Station or Stations), click this button. You will then see the Trusted Wireless Stations screen, described below. To upload a list of Trusted Stations from a file on your PC, click this button. To download the current list of Trusted Stations from the Access Point to a file on your PC, click this button. Name - the name of the Wireless station. MAC Address - the MAC or physical address of each Wireless station. Connected - this indicates whether or not the Wireless station is currently associates with this Access Point. Read from File Write to File 13 Wireless Access Point User Guide Trusted Wireless Stations To change the list of trusted wireless stations, use the Modify List button on the Access Control screen. You will see a screen like the sample below.

Figure 9: Trusted Wireless Stations Data - Trusted Wireless Stations Trusted Wireless Stations Other Wireless Stations Name Address Buttons << Add a Trusted Wireless Station to the list (move from the "Other Stations" list). · · >> Select an entry (or entries) in the "Other Stations" list, and click the " << " button. Enter the Address (MAC or physical address) of the wireless station, and click the "Add " button. This lists any Wireless Stations which you have designated as "Trusted". This list any Wireless Stations detected by the Access Point, which you have not designated as "Trusted". The name assigned to the Trusted Wireless Station. Use this when adding or editing a Trusted Station. The MAC (physical) address of the Trusted Wireless Station. Use this when adding or editing a Trusted Station. Delete a Trusted Wireless Station from the list (move to the "Other Stations" list).

· · Select an entry (or entries) in the "Trusted Stations" list. Click the " >> " button. Select All Select None Select all of the Stations listed in the "Other Stations" list. De-select any Stations currently selected in the "Other Stations" list. 14 Access Point Setup Edit To change an existing entry in the "Trusted Stations" list, select it and click this button.

1. Select the Station in the "Trusted Station" list. 2. Click the "Edit" button. The address will be copied to the "Address" field, and the "Add" button will change to "Update".

3. Edit the address (MAC or physical address) as required. 4. Click "Update" to save your changes. To add a Trusted Station which is not in the "Other Wireless Stations" list, enter the required data and click this button. Clear the Name and Address fields. Add Clear Security Profiles Security Profiles contain the SSID and all the security settings for Wireless connections to this Access Point. · · Up to eight (8) Security Profiles can be defined. Up to four (4) Security Profiles can be enabled at one time, allowing up to 4 different SSIDs to be used simultaneously. Figure 10: Security Profiles Screen 15 Wireless Access Point User Guide Data - Security Profiles Screen Profile List All available profiles are listed.

For each profile, the following data is displayed: · Asterisk (*) If an asterisk is displayed before the name of the profile, this indicates that the profile is currently enabled. If not displayed, the profile is currently disabled. Profile Name The current profile name is displayed. [SSID] The current SSID associated with this profile. Security System The current security system (e.g. WPA-PSK) is displayed. [Band] The Wireless Band (2.4 GHz, 5GHz) for this profile is displayed. Profiles may be assigned to either or both Wireless Bands.

Enable - Enable the selected profile. Configure - Change the settings for the selected profile. Disable - Disable the selected profile. · · · · Buttons · · · Primary Profile 802.11b/g AP Mode Select the primary profile for 802.

11b and 802.11g (2.4 GHz band) AP mode. Only enabled profiles are listed. The SSID associated with this profile will be broadcast if the "Broadcast SSID" setting on the Basic screen is enabled.

Select the primary profile for 802.11b and 802.11g (2.4 GHz band) Bridge Mode. This setting determines the SSID and security settings used for the Bridge connection to the remote AP. 802.11b/g Bridge Mode Isolation None If this option is selected, wireless clients using different profiles (different SSIDs) are not isolated from each other, so they will be able to communicate with each other. If this option is selected, wireless clients using different profiles (different SSIDs) are isolated from each other, so they will NOT be able to communicate with each other. They will still be able to communicate with other clients using the same profile, unless the "Wireless Separation" setting on the "Advanced" screen has been enabled. This option is only useful if the hubs/switches on your LAN support the VLAN (802.

1Q) standard. When VLAN is used, you must select the desired VLAN for each security profile when configuring the profile.



[You're reading an excerpt. Click here to read official TRENDNET](#)

[TEW-453APB user guide](#)

<http://yourpdfguides.com/dref/3181063>

(If VLAN is not selected, the VLAN setting for each profile is ignored.) Click the Configure VLAN button to configure the IDs used by each VLAN. See below for further details. Isolate all Use VLAN 16 Access Point Setup VLAN Configuration Screen This screen is accessed via the Configure VLAN button on the Security Profiles screen. · · The settings on this screen will be ignored unless the Use VLAN option on the Security Profiles screen is selected. If using the VLAN option, these settings determine which VLAN traffic is assigned to. Figure 11: VLAN Configuration Data - VLAN Configuration Screen VLAN - Client Traffic Profile Each profile is listed, whether currently enabled or not. You can assign traffic from each profile (SSID) to a different VLAN if desired. To assign multiple profiles to the same VLAN, just enter the same VLAN ID for each profile. Enter the desired VLAN ID, as used on your network. IDs must be in the range 1 ~ 4095. These IDs must match the IDs used by other network devices. VLAN ID VLAN - AP Traffic No VLAN Tag Traffic generated by this AP will not have a VLAN tag (no VLAN ID).

17 Wireless Access Point User Guide Replicate... If selected, each packet generated by this AP will be sent over each active VLAN, as defined in the client VLAN table above. This requires that each packet be replicated (up to 8 times).

This has a detrimental effect on performance, so should only be used if necessary. If selected, you can enter the desired VLAN ID. Normally, this ID should be one of the client VLAN IDs defined above. Specified VLAN ID 18 Access Point Setup Security Profile Screen This screen is displayed when you select a Profile on the Security Profiles screen, and click the Configure button. Figure 12: Security Profile Screen Profile Data Enter the desired settings for each of the following: Profile Name SSID Wireless Band Enter a suitable name for this profile. Enter the desired SSID. Each profile must have a unique SSID. Select the wireless band or bands for this profile. If your Wireless Access Point only has a single band, then only 1 option is available. Security Settings Select the desired option, and then enter the settings for the selected method.

The available options are: · · · None - No security is used. Anyone using the correct SSID can connect to your network. WEP - The 802.11b standard. Data is encrypted before transmission, but the encryption system is not very strong. WPA-PSK - Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. The PSK (Pre-shared Key) must be entered on each Wireless station. The 256Bit encryption key is derived from the PSK, and changes frequently. WPA-802.

1x - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard. If this option is selected: 19 · Wireless Access Point User Guide · · · · This Access Point must have a "client login" on the Radius Server. Each user must have a "user login" on the Radius Server.

Each user's wireless client must support 802.1x and provide the login data when required. All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required. 802.

1x - This uses the 802.1x standard for client authentication, and WEP for data encryption. If possible, you should use WPA-802.1x instead, because WPA encryption is much stronger than WEP encryption. If this option is selected: · · · · This Access Point must have a "client login" on the Radius Server. Each user must have a "user login" on the Radius Server. Each user's wireless client must support 802.1x and provide the login data when required. All data transmission is encrypted using the WEP standard. You only have to select the WEP key size; the WEP key is automatically generated.

20 Access Point Setup Security Settings - None Figure 13: Wireless Security - None No security is used. Anyone using the correct SSID can connect to your network. The only settings available from this screen are Radius MAC Authentication and UAM (Universal Access Method). Radius MAC Authentication Radius MAC Authentication provides for MAC address checking which is centralized on your Radius server. If you don't have a Radius Server, you cannot use this feature. Using MAC authentication 1. Ensure the Wireless Access Point can login to your Radius Server. · Add a RADIUS client on the RADIUS server, using the IP address or name of the Wireless Access Point, and the same shared key as entered on the Wireless Access Point. Ensure the Wireless Access Point has the correct address, port number, and shared key for login to your Radius Server. These parameters are entered either on the Security page, or the Radius-based MAC authentication sub-screen, depending on the security method used.

· 2. 3. On the Access Point, enable the Radius-based MAC authentication feature on the screen below. Add Users on the Radius server as required. The username must be the MAC address of the Wireless client you wish to allow, and the password must be blank.

When clients try to associate with the Access Point, their MAC address is passed to the Radius Server for authentication. · · If successful, "xx:xx:xx:xx:xx:xx MAC authentication" is entered in the log, and client station status would show as "authenticated" on the station list table; If not successful, "xx:xx:xx:xx:xx:xx MAC authentication failed" is entered in the log., and station status is shown as "authenticating" on the station list table. · 21 Wireless Access Point User Guide Radius-based MAC authentication Screen This screen will look different depending on the current security setting. If you have already provided the address of your Radius server, you won't be prompted for it again. Otherwise, you must enter the details of your Radius Server on this screen.

Figure 14: Radius-based MAC Authentication Screen Data - Radius-based MAC Authentication Screen Enable ... Radius Server Address Radius Port Client Login Name Enable this if you wish to Radius-based MAC authentication. If this field is visible, enter the name or IP address of the Radius Server on your network. If this field is visible, enter the port number used for connections to the Radius Server. If this field is visible, it displays the name used for the Client Login on the Radius Server. This Login name must be created on the Radius Server. (Some Radius servers allow you to use the AP's IP address instead of this login name.) If this field is visible, it is used for the Client Login on the Radius Server.

Enter the key value to match the value on the Radius Server. If this field is visible, it is for the WEP key used to encrypt data transmissions to the Radius Server.



[You're reading an excerpt. Click here to read official TRENDNET TEW-453APB user guide](http://yourpdfguides.com/dref/3181063)
<http://yourpdfguides.com/dref/3181063>

Enter the desired key value in HEX, and ensure the Radius Server has the same value. If this field is visible, select the desired key index. Any value can be used, provided it matches the value on the Radius Server. Shared Key WEP Key WEP Key Index 22 Access Point Setup UAM UAM (Universal Access Method) is intended for use in Internet cafes, Hot Spots, and other sites where the Access Point is used to provide Internet Access. If enabled, then HTTP (TCP, port 80) connections are checked. (UAM only works on HTTP connections; all other traffic is ignored.) If the user has not been authenticated, Internet access is blocked, and the user is re-directed to another web page. Typically, this web page is on your Web server, and explains how to pay for and obtain Internet access.

To use UAM, you need a Radius Server for Authentication. The "Radius Server Setup" must be completed before you can use UAM. The required setup depends on whether you are using "Internal" or "External" authentication. · Internal authentication uses the web page built into the Wireless Access Point. External authentication uses a web page on your Web server.

Generally, you should use External authentication, as this allows you to provide relevant and helpful information to users. UAM authentication - Internal 1. Ensure the Wireless Access Point can login to your Radius Server. · Add a RADIUS client on RADIUS server, using the IP address or name of the Wireless Access Point, and the same shared key as entered on the Wireless Access Point. 2.

3. 4. 5. 6. Ensure the Wireless Access Point has the correct address, port number, and shared key for login to your Radius Server. These parameters are entered either on the Security page, or the UAM sub-screen, depending on the security method used. Add users on your RADIUS server as required, and allow access by these users. Client PCs must have the correct Wireless settings in order to associate with the Wireless Access Point. When an associated client tries to use HTTP (TCP, port 80) connections, they will be redirected to a user login page. The client (user) must then enter the user name and password, as defined on the Radius Server.

(You must provide some system to let users know the correct name and password to use.) If the user name and password is correct, Internet access is allowed. Otherwise, the user remains on the login page. · Clients which pass the authentication are listed as "xx:xx:xx:xx:xx:xx WEB authentication" in the log table, and station status would show as "Authenticated" on the station list table. · If a client fails authentication, "xx:xx:xx:xx:xx:xx WEB authentication failed" shown in the log, and station status is shown as "Authenticating" on the station list table. UAM authentication - External 1. Ensure the Wireless Access Point can login to your Radius Server. · Add a RADIUS client on RADIUS server, using the IP address or name of the Wireless Access Point, and the same shared key as entered on the Wireless Access Point. 2. Ensure the Wireless Access Point has the correct address, port number, and shared key for login to your Radius Server.

These parameters are entered either on the Security page, or the UAM sub-screen, depending on the security method used. On your Web Server, create a suitable welcome page. The welcome page must have a link or button to allow the user to input their user name and password on the uamlogin.htm page on the Access Point. 23 Wireless Access Point User Guide 3.

4. 5. 6. 7. 8.

On the Access Point's UAM screen, select External Web-based Authentication, and enter the URL for the welcome page on your Web server. Add users on your RADIUS server as required, and allow access by these users. Client PCs must have the correct Wireless settings in order to associate with the Wireless Access Point. When an associated client tries to use HTTP (TCP, port 80) connections, they will be redirected to the welcome page on your Web Server. They must then click the link or button in order to reach the Access Point's login page. The client (user) must then enter the user name and password, as defined on the Radius Server. (You must provide some system to let users know the correct name and password to use.) If the user name and password is correct, Internet access is allowed. Otherwise, the user remains on the login page. · Clients which pass the authentication are listed as "xx:xx:xx:xx:xx:xx WEB authentication" in the log table, and station status would show as "Authenticated" on the station list table.

· If a client fails authentication, "xx:xx:xx:xx:xx:xx WEB authentication failed" is shown in the log, and station status is shown as "Authenticating" on the station list table. UAM Screen The UAM screen will look different depending on the current security setting. If you have already provided the address of your Radius server, you won't be prompted for it again. Figure 15: UAM Screen Data - UAM Screen Enable Internal Web-based Authentication Enable this if you wish to use this feature. See the section above for details of using UAM. If selected, then when a user first tries to access the Internet, they will be blocked, and re-directed to the built-in login page. The logon data is then sent to the Radius Server for authentication. 24 Access Point Setup External Web-based Authentication Login URL Login Failure URL If selected, then when a user first tries to access the Internet, they will be blocked, and re-directed to the URL below. This needs to be on your own local Web Server. The page must also link back to the builtin login page on this device to complete the login procedure. Enter the URL of the page on your local Web Server you wish users to see when they attempt to access the Internet, but are not logged in. Enter the URL of the page on your local Web Server you wish users to see if their login fails. (This may be the same URL as the Login URL). Security Settings - WEP This is the 802.11b standard.

Data is encrypted before transmission, but the encryption system is not very strong. Figure 16: WEP Wireless Security 25 Wireless Access Point User Guide Data - WEP Screen WEP Data Encryption Select the desired option, and ensure your Wireless stations have the same setting: · Authentication 64 Bit Encryption - Keys are 10 Hex (5 ASCII) characters. 128 Bit Encryption - Keys are 26 Hex (13 ASCII) characters. 152 Bit Encryption - Keys are 32 Hex (16 ASCII) characters. Normally, you can leave this at "Automatic", so that Wireless Stations can use either method ("Open System" or "Shared Key"). If you wish to use a particular method, select the appropriate value "Open System" or "Shared Key". All Wireless stations must then be set to use the same method.



[You're reading an excerpt. Click here to read official TRENDNET](#)

[TEW-453APB user guide](#)

<http://yourpdfguides.com/dref/3181063>

Key Input Key Value Select "Hex" or "ASCII" depending on your input method. (All keys are converted to Hex, ASCII input is only for convenience.) Enter the key values you wish to use. The default key, selected by the radio button, is required. The other keys are optional. Other stations must have matching key values. Use this to generate a key or keys, instead of entering them directly.

Enter a word or group of printable characters in the Passphrase box and click the "Generate Key" button to automatically configure the WEP Key(s). The current status is displayed. Click the "Configure" button to configure this feature if required. The current status is displayed. Click the "Configure" button to configure this feature if required. Passphrase Radius MAC Authentication UAM 26 Access Point Setup Security Settings - WPA-PSK Like WEP, data is encrypted before transmission. WPA is more secure than WEP, and should be used if possible. The PSK (Pre-shared Key) must be entered on each Wireless station. The 256Bit encryption key is derived from the PSK, and changes frequently. Figure 17: WPA-PSK Wireless Security Data - WPA-PSK Screen WPA-PSK Network Key WPA Encryption Enter the key value.

Data is encrypted using a 256Bit key derived from this key. Other Wireless Stations must use the same key. Select the desired option. Other Wireless Stations must use the same method. · TKIP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are not encrypted.

TKIP + 64 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 64 bit WEP. TKIP + 128 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 128 bit WEP. AES - CCMP - CCMP is the most common sub-type of AES (Advanced Encryption System). Most systems will simply say "AES". If selected, both Unicast (point-to-point) and multicast (broadcast) transmissions are encrypted using . . . 27 Wireless Access Point User Guide AES.

· AES - CCMP + TKIP - Unicast (point-to-point) transmissions are encrypted using AES - CCMP, and multicast (broadcast) transmissions are encrypted using TKIP. Group Key Update Key Lifetime Update Group key when any membership terminates Radius MAC Authentication UAM This refers to the key used for broadcast transmissions. Enable this if you want the keys to be updated regularly. This field determines how often the Group key is dynamically updated. Enter the desired value. If enabled, the Group key will be updated whenever any member leaves the group or disassociates from the Access Point. The current status is displayed. This will always be "Disabled", because Radius MAC Authentication is not available with WPAPSK. The Configure button for this feature will also be disabled. The current status is displayed.

This will always be "Disabled", because UAM is not available with WPA-PSK. The Configure button for this feature will also be disabled. 28 Access Point Setup Security Settings - WPA-802.1x This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard. If this option is selected: . . . This Access Point must have a "client login" on the Radius Server. Each user must have a "user login" on the Radius Server. Normally, a Certificate is used to authenticate each user. See Chapter4 for details of user configuration.

Each user's wireless client must support 802.1x. All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required. Figure 18: WPA-802.

1x Wireless Security 29 Wireless Access Point User Guide Data - WPA-802.1x Screen WPA-802.1x Radius Server Address Radius Port Client Login Name Enter the name or IP address of the Radius Server on your network. Enter the port number used for connections to the Radius Server. @@The Radius Server must be configured to accept this login.

This is used for the Client Login on the Radius Server. Enter the key value to match the Radius Server. Select the desired option. Other Wireless Stations must use the same method. · TKIP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are not encrypted.

TKIP + 64 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 64 bit WEP. TKIP + 128 bit WEP - Unicast (point-to-point) transmissions are encrypted using TKIP, and multicast (broadcast) transmissions are encrypted using 128 bit WEP. AES - CCMP - CCMP is the most common sub-type of AES (Advanced Encryption System). Most systems will simply say "AES". If selected, both Unicast (point-to-point) and multicast (broadcast) transmissions are encrypted using AES.

AES - CCMP + TKIP - Unicast (point-to-point) transmissions are encrypted using AES - CCMP, and multicast (broadcast) transmissions are encrypted using TKIP. Shared Key WPA Encryption . . . Group Key Update Key Lifetime Update Group key when any membership terminates Radius Accounting This refers to the key used for broadcast transmissions. Enable this if you want the keys to be updated regularly. This field determines how often the Group key is dynamically updated. Enter the desired value. If enabled, the Group key will be updated whenever any member leaves the group or disassociates from the Access Point. @@If enabled, the port used by your Radius Server must be entered in the Radius Accounting Port" field. Update Report every ...

Radius MAC Authentication If Radius accounting is enabled, you can enable this and enter the desired update interval. This Access Point will then send updates according to the specified time period. The current status is displayed. This will always be "Disabled", because Radius MAC Authentication is not available with WPA802.1x.

The Configure button for this feature will also be disabled. 30 Access Point Setup UAM The current status is displayed. This will always be "Disabled", because UAM is not available with WPA-802.1x. The Configure button for this feature will also be disabled.

31 Wireless Access Point User Guide Security Settings - 802.1x This uses the 802.1x standard for client authentication, and WEP for data encryption. If possible, you should use WPA-802.1x instead, because WPA encryption is much stronger than WEP encryption. If this option is selected: . . . This Access Point must have a "client login" on the Radius Server. Each user must have a "user login" on the Radius Server.



[You're reading an excerpt. Click here to read official TRENDNET](http://yourpdfguides.com/dref/3181063)

[TEW-453APB user guide](http://yourpdfguides.com/dref/3181063)

<http://yourpdfguides.com/dref/3181063>

Normally, a Certificate is used to authenticate each user. See Chapter4 for details of user configuration. Each user's wireless client must support 802.

Ix. All data transmission is encrypted using the WEP standard. @@Enter the port number used for connections to the Radius Server. @@The Radius Server must be configured to accept this login. This is used for the Client Login on the Radius Server. Enter the key value to match the Radius Server. @@128 Bit - Keys are 26 Hex (13 ASCII) characters. @@... The key exchange will be negotiated. The most widely supported protocol is EAP-TLS.

@@@@@@@Enter the WEP key according to the WEP Key Size setting above.

Wireless stations must use the same key. Select the desired index value. Wireless stations must use the same key index. @@@@Click the Configure button to configure this feature if required. The current status is displayed.

@@If selected, the following data must be entered. @@Enter an unused IP address from the address range on your LAN. Subnet Mask - The Network Mask associated with the IP Address above. Enter the value used by other devices on your LAN. Gateway - The IP Address of your Gateway or Router.

Enter the value used by other devices on your LAN. DNS - Enter the DNS (Domain Name Server) used by PCs on your LAN. Enter a suitable name for this Access Point. If desired, you can enter a description for the Access Point. @@@@802.11b - if selected, only 802.11b connections are allowed.

@@802.11g - only 802.11g connections are allowed.

@@@@@However, this option is backwardcompatible with 802.11b and (standard) 802.11g. · Static Super 802.11g (108Mbps) - This uses Packet Bursting, FastFrame, Compression, and Channel Bonding (using 2 channels) to increase throughput. Because "Channel Bonding" is always used, this method is NOT compatible with 802.11b and (standard) 802.11g. Only clients supporting the "Atheros Super G" mode can connect at 108Mbps; they will always connect at this speed. Select this option only if all wireless stations support this "Atheros Super G" mode.

AP Mode Both Bridge mode and AP mode can be used simultaneously, unless AP mode is "Client/Repeater". Select the desired AP mode: · · · None (disable) - Disable AP mode. Use this if you want to act a Bridge only. Access Point - operate as a normal Access Point Client/Repeater - act as a client or repeater for another Access Point. If selected, you must provide the address (MAC address) of the other AP in the Repeater AP MAC Address field.

In this mode, all traffic is sent to the specified AP. Note: If using Client/Repeater mode, you cannot use Bridge Mode. Repeater AP MAC Address This is not required unless the AP Mode is "Client/Repeater". In this mode, you must provide the MAC address of the other AP in this field. You can either enter the MAC address directly, or, if the other AP is on-line and broadcasting its SSID, you can click the "Select AP" button and select from a list of available APs.

If Disabled, no SSID is broadcast. If enabled, you must select the security profile whose SSID is to be broadcast. This can be done the "Security Profiles" screen. The SSID will then be broadcast to all Wireless Stations. Stations can then detect this AP and adopt the correct SSID for connections to this Access Point. Broadcast SSID 38 Access Point Setup Bridge Mode Both Bridge mode and AP mode can be used simultaneously, unless AP mode is "Client/Repeater".

Select the desired Bridge mode: · · None (disable) - Disable Bridge mode. Use this if you want to act a AP only. Point-to-Point Bridge (PTP) - Bridge to a single AP. You must provide the MAC address of the other AP in the PTP Bridge AP MAC Address field.

Point-to-Multi-Point Bridge (PTMP) - Select this only if this AP is the "Master" for a group of Bridge-mode APs. The other Bridge-mode APs must be set to Point-to-Point Bridge mode, using this AP's MAC address. They then send all traffic to this "Master". · If required, you can specify the MAC addresses of the APs which are allowed to connect to this AP in PTMP mode. To specify the allowed APs: 1. Enable the checkbox "In PTMP mode, only allow specified APs".

2. Click the button "Set PTMP APs". 3. On the resulting sub-screen, enter the MAC addresses of the allowed APs.

PTP Bridge AP MAC Address In PTMP mode, only allow specified APs This is not required unless the Bridge Mode is "Point-to-Point Bridge (PTP)". In this case, you must enter the MAC address of the other AP in this field. This is only functional if using Point-to-Multi-Point Bridge (PTMP) mode. If enabled, you can specify the MAC addresses of the APs which are allowed to connect to this AP. To specify the allowed APs: 1.

Enable this checkbox 2. Click the button "Set PTMP APs". 3. On the resulting sub-screen, enter the MAC addresses of the allowed APs. Use this to open a sub-window where you can specify the MAC addresses of the APs which are allowed to connect to this AP.

This is only functional if using Point-to-Multi-Point Bridge (PTMP) mode and you have enabled the checkbox "In PTMP mode, only allow specified APs". · ·

Set PTMP APs Parameters Channel No If "Automatic" is selected, the Access Point will select the best available Channel. If you experience interference (shown by lost connections and/or slow data transfers) you may need to experiment with manually setting different channels to see which is the best. Current Channel No. This displays the current channel used by the Access Point. 39 Wireless Access Point User Guide Advanced Settings Clicking the Advanced link on the menu will result in a screen like the following. Figure 22: Advanced Settings Data - Advanced Settings Screen Basic Rate Basic Rate The Basic Rate is used for broadcasting. It does not determine the data transmission rate, which is determined by the "Mode" setting on the Basic screen. Select the desired option. Do NOT select the "802.

11g" or "OFDM" options unless ALL of your wireless clients support this. 802.11b clients will not be able to connect to the Access Point if either of these modes is selected. Options Wireless Separation If enabled, then each Wireless station using the Access Point is invisible to other Wireless stations. In most business situations, this setting should be Disabled. Enable this setting if you wish to use this mode, and your Wireless stations support this mode. Worldwide Mode (802.11d) 40 Access Point Setup Parameters Disassociated Timeout This determines how quickly a Wireless Station will be considered "Disassociated" with this AP, when no traffic is received. Enter the desired time period. Enter the preferred setting between 256 and 2346.

Normally, this can be left at the default value. Enter the preferred setting between 20 and 1000.



[You're reading an excerpt. Click here to read official TRENDNET](http://yourpdfguides.com/dref/3181063)

[TEW-453APB user guide](http://yourpdfguides.com/dref/3181063)

<http://yourpdfguides.com/dref/3181063>

Normally, this can be left at the default value. Enter the preferred setting between 256 and 2346. Normally, this can be left at the default value. Select the desired option. The default is "Long". The "Short" setting takes less time when used in a good environment. Select the desired power output. Higher levels will give a greater range, but are also more likely to cause interference with other devices.

If your Access Point has only 1 antenna, there is only 1 option available. If your Access Point has 2 antennae, select the option which gives the best results in your location. Fragmentation Beacon Interval RTS/CTS Threshold Preamble Type Output Power Level Antenna Selection 802.11b Protection Type Short Slot Time Protection Mode Select the desired option. The default is CTS-only. Enable or disable this setting as required. The Protection system is intended to prevent older 802.11b devices from interfering with 802.11g transmissions. (Older 802.

11b devices may not be able to detect that a 802.11g transmission is in progress.) Normally, this should be left at "Auto". Select the desired option. The default is 11 Mbps. Protection Rate 41 Chapter 4 PC and Server Configuration This Chapter details the PC Configuration required for each PC on the local LAN. 4 Overview All Wireless Stations need to have settings which match the Wireless Access Point. These settings depend on the mode in which the Access Point is being used. · · If using WEP or WPA-PSK, it is only necessary to ensure that each Wireless station's settings match those of the Wireless Access Point, as described below. For WPA-802.

1x and 802.1x modes, configuration is much more complex. The Radius Server must be configured correctly, and setup of each Wireless station is also more complex. Using WEP For each of the following items, each Wireless Station must have the same settings as the Wireless Access Point. Mode SSID (ESSID) On each PC, the mode must be set to Infrastructure.

This must match the value used on the Wireless Access Point. The default value is wireless Note! The SSID is case sensitive. Wireless Security · · · Each Wireless station must be set to use WEP data encryption. The Key size (64 bit, 128 bit, 152 bit) must be set to match the Access Point. The keys values on the PC must match the key values on the Access Point.

Note: On some systems, the key sizes may be shown as 40bit, 104bit, and 128bit instead of 64 bit, 128 bit and 152bit. This difference arises because the key input by the user is 24 bits less than the key size used for encryption. 42 PC and Server Configuration Using WPA-PSK For each of the following items, each Wireless Station must have the same settings as the Wireless Access Point. Mode SSID (ESSID) On each PC, the mode must be set to Infrastructure. This must match the value used on the Wireless Access Point. The default value is wireless Note! The SSID is case sensitive. Wireless Security On each client, Wireless security must be set to WPA-PSK. · · The Pre-shared Key entered on the Access Point must also be entered on each Wireless client. The Encryption method (e.g.

TKIP, AES) must be set to match the Access Point. 43 Wireless Access Point User Guide Using WPA-802.1x This is the most secure and most complex system. 802.1x mode provides greater security and centralized management, but it is more complex to configure. Wireless Station Configuration For each of the following items, each Wireless Station must have the same settings as the Wireless Access Point. Mode SSID (ESSID) On each PC, the mode must be set to Infrastructure. This must match the value used on the Wireless Access Point. The default value is wireless Note! The SSID is case sensitive. 802.

1x Authentication 802.1x Encryption Each client must obtain a Certificate which is used for authentication for the Radius Server. Typically, EAP-TLS is used. This is a dynamic key system, so keys do NOT have to be entered on each Wireless station. However, you can also use a static WEP key (EAP-MD5); the Wireless Access Point supports both methods simultaneously.

Radius Server Configuration If using WPA-802.1x mode, the Radius Server on your network must be configured as follow: · · It must provide and accept Certificates for user authentication. There must be a Client Login for the Wireless Access Point itself. · · · The Wireless Access Point will use its Default Name as its Client Login name. (However, your Radius server may ignore this and use the IP address instead.

) The Shared Key, set on the Security Screen of the Access Point, must match the Shared Secret value on the Radius Server. Encryption settings must be correct. 44 PC and Server Configuration 802.1x Server Setup (Windows 2000 Server) This section describes using Microsoft Internet Authentication Server as the Radius Server, since it is the most common Radius Server available that supports the EAP-TLS authentication method. The following services on the Windows 2000 Domain Controller (PDC) are also required: · · · · · dhcpd dns rras webserver (IIS) Radius Server (Internet Authentication Service) Certificate Authority Windows 2000 Domain Controller Setup 1. 2. Run dcpromo.exe from the command prompt. Follow all of the default prompts, ensure that DNS is installed and enabled during installation. Services Installation 1.

2. 3. Select the Control Panel - Add/Remove Programs. Click Add/Remove Windows Components from the left side. Ensure that the following components are activated (selected): · Certificate Services. After enabling this, you will see a warning that the computer cannot be renamed and joined after installing certificate services. Select Yes to select certificate services and continue World Wide Web Server. Select World Wide Web Server on the Internet Information Services (IIS) component. From the Networking Services category, select Dynamic Host Configuration Protocol (DHCP), and Internet Authentication Service (DNS should already be selected and installed). · · 45 Wireless Access Point User Guide Figure 23: Components Screen 4.

5. Click Next. Select the Enterprise root CA, and click Next. Figure 24: Certification Screen 6. Enter the information for the Certificate Authority, and click Next.

46 PC and Server Configuration Figure 25: CA Screen 7. 8. Click Next if you don't want to change the CA's configuration data. Installation will warn you that Internet Information Services are running, and must be stopped before continuing. Click Ok, then Finish.

DHCP server configuration 1. 2. Click on the Start - Programs - Administrative Tools - DHCP Right-click on the server entry as shown, and select New Scope. Figure 26: DHCP Screen 3. 4. 5. Click Next when the New Scope Wizard Begins. Enter the name and description for the scope, click Next.



[You're reading an excerpt. Click here to read official TRENDNET](http://yourpdfguides.com/dref/3181063)

[TEW-453APB user guide](http://yourpdfguides.com/dref/3181063)

<http://yourpdfguides.com/dref/3181063>

Define the IP address range. Change the subnet mask if necessary.

Click Next. 47 Wireless Access Point User Guide Figure 27: IP Address Screen Add exclusions in the address fields if required. If no exclusions are required, leave it blank. Click Next. 7. Change the Lease Duration time if preferred. Click Next. 8. Select Yes, I want to configure these options now, and click Next. 9. Enter the router address for the current subnet. The router address may be left blank if there is no router. Click Next. 10. For the Parent domain, enter the domain you specified for the domain controller setup, and enter the server's address for the IP address.

Click Next. 6. Figure 28: DNS Screen 11. If you don't want a WINS server, just click Next. 12.

Select Yes, I want to activate this scope now. Click Next, then Finish. 13. Right-click on the server, and select Authorize. It may take a few minutes to complete. 48 PC and Server Configuration Certificate Authority Setup 1. 2. Select Start - Programs - Administrative Tools - Certification Authority. Right-click Policy Settings, and select New - Certificate to Issue. Figure 29: Certificate Authority Screen 3.

Select Authenticated Session and Smartcard Logon (select more than one by holding down the Ctrl key). Click OK. Figure 30: Template Screen 4. 5. Select Start - Programs - Administrative Tools - Active Directory Users and Computers. Right-click on your active directory domain, and select Properties. 49 Wireless Access Point User Guide Figure 31: Active Directory Screen 6. Select the Group Policy tab, choose Default Domain Policy then click Edit. Figure 32: Group Policy Tab 7. Select Computer Configuration - Windows Settings - Security Settings - Public Key Policies, right-click Automatic Certificate Request Settings - New - Automatic Certificate Request.

50 PC and Server Configuration Figure 33: Group Policy Screen 8. 9. When the Certificate Request Wizard appears, click Next. Select Computer, then click Next. Figure 34: Certificate Template Screen 10.

Ensure that your certificate authority is checked, then click Next. 11. Review the policy change information and click Finish. 12. Click Start - Run, type cmd and press enter.

Enter secedit /refreshpolicy machine_policy This command may take a few minutes to take effect. 51 Wireless Access Point User Guide Internet Authentication Service (Radius) Setup 1. 2. Select Start - Programs - Administrative Tools - Internet Authentication Service Right-click on Clients, and select New Client. Figure 35: Service Screen 3. 4. 5. 6. 7. 8.

Enter a name for the access point, click Next. Enter the address or name of the Wireless Access Point, and set the shared secret, as entered on the Security Settings of the Wireless Access Point. Click Finish. Right-click on Remote Access Policies, select New Remote Access Policy. Assuming you are using EAP-TLS, name the policy eap-tls, and click Next. Click Add... If you don't want to set any restrictions and a condition is required, select Day-And-TimeRestrictions, and click Add..

. Figure 36: Attribute Screen 9. Click Permitted, then OK. Select Next. 10.

Select Grant remote access permission. Click Next. 52 PC and Server Configuration 11. Click Edit Profile..

. and select the Authentication tab. Enable Extensible Authentication Protocol, and select Smart Card or other Certificate. Deselect other authentication methods listed. Click OK. Figure 37: Authentication Screen 12. Select No if you don't want to view the help for EAP. Click Finish. 53 Wireless Access Point User Guide Remote Access Login for Users 1. 2.

3. Select Start - Programs - Administrative Tools- Active Directory Users and Computers. Double click on the user who you want to enable. Select the Dial-in tab, and enable Allow access. Click OK. Figure 38: Dial-in Screen 54 PC and Server Configuration 802.1x Client Setup on Windows XP Windows XP ships with a complete 802.1x client implementation. If using Windows 2000, you can install SP3 (Service Pack 3) to gain the same functionality. If you don't have either of these systems, you must use the 802.

1x client software provided with your wireless adapter. Refer to your vendor's documentation for setup instructions. The following instructions assume that: . . You are using Windows XP You are connecting to a Windows 2000 server for authentication. You already have a login (User name and password) on the Windows 2000 server. Client Certificate Setup 1.

Connect to a network which doesn't require port authentication. 2. Start your Web Browser. In the Address box, enter the IP address of the Windows 2000 Server, followed by /certsrv e.g http://192.

168.0.2/certsrv 3. You will be prompted for a user name and password. Enter the User name and Password assigned to you by your network administrator, and click OK. Figure 39: Connect Screen 4. On the first screen (below), select Request a certificate, click Next. 55 Wireless Access Point User Guide Figure 40: Wireless CA Screen 5. Select User certificate request and select User Certificate, the click Next. Figure 41: Request Type Screen 6.

Click Submit. 56 PC and Server Configuration Figure 42: Identifying Information Screen 7. A message will be displayed, then the certificate will be returned to you. Click Install this certificate. Figure 43: Certificate Issued Screen 8. . You will receive a confirmation message. Click Yes. 57 Wireless Access Point User Guide Figure 44: Root Certificate Screen 9. Certificate setup is now complete.

802.1x Authentication Setup 1. 2. 3. Open the properties for the wireless connection, by selecting Start - Control Panel Network Connections. Right Click on the Wireless Network Connection, and select Properties. Select the Authentication Tab, and ensure that Enable network access control using IEEE 802.1X is selected, and Smart Card or other Certificate is selected from the EAP type. Figure 45: Authentication Tab Encryption Settings The Encryption settings must match the APs (Access Points) on the Wireless network you wish to join. . Windows XP will detect any available Wireless networks, and allow you to configure each network independently.

58 PC and Server Configuration . Your network administrator can advise you of the correct settings for each network. 802.1x networks typically use EAP-TLS. This is a dynamic key system, so there is no need to enter key values. Enabling Encryption To enable encryption for a wireless network, follow this procedure: 1. Click on the Wireless Networks tab. Figure 46: Wireless Networks Screen 2. 3. Select the wireless network from the Available Networks list, and click Configure. Select and enter the correct values, as advised by your Network Administrator.

For example, to use EAP-TLS, you would enable Data encryption, and click the checkbox for the setting The key is provided for me automatically, as shown below. 59 Wireless Access Point User Guide Figure 47: Properties Screen Setup for Windows XP and 802.



[You're reading an excerpt. Click here to read official TRENDNET TEW-453APB user guide](http://yourpdfguides.com/dref/3181063)
<http://yourpdfguides.com/dref/3181063>