

Netopia® 3-D Reach Utility User Guide

netopia®

BROADBAND WITHOUT BOUNDARIES™



Netopia® 3-D Reach Wireless Adapters

April 2007

Copyright

Copyright © 2007 Netopia, Inc.

Netopia and the Netopia logo are registered trademarks belonging to Netopia, Inc., registered U.S. Patent and Trademark Office. Broadband Without Boundaries and 3-D Reach are trademarks belonging to Netopia, Inc. All other trademarks are the property of their respective owners. All rights reserved.

Netopia, Inc. Part Number: 6161210-00-01

Table of Contents

Copyright	2
Netopia 3D Reach Utility Installation	3
For Microsoft Windows 98SE, ME, 2000	3
For Microsoft Windows XP	3
Macintosh Mac OS X 10.2 and higher and Linux drivers	3
Start the Netopia 3D REACH Utility	4
Site Survey	6
ADD/EDIT Profile	8
Encryption Setting WEP/TKIP/AES	10
802.1x Setting	12
CA Server	14
Profile	15
Link Status	17
Advanced	19
Country Channel List	21
About	25
Example: Adding a profile in the site survey page	26
Example: Adding a profile in the Profile page	31
Configure connection with WEP ON	39
Configure connection with WPA-PSK	43
Configure connection with WPA by 802.1x setting	47
Excursuses	61

Table of Contents

Netopia 3D Reach Utility Installation

For Microsoft Windows 98SE, ME, 2000

1. Insert the CD. The Setup utility will run automatically and load the driver for the Netopia 3D Reach Wireless PC Card.

When the installation is complete, a new Wireless communication icon will appear in your system tray in the Windows toolbar.

2. Click the Wireless icon to start the Netopia WLAN Utility. See [“Start the Netopia 3D REACH Utility”](#) on page 4.

For Microsoft Windows XP

1. Insert the CD. The Setup utility will run automatically and load the driver for the Netopia 3D Reach Wireless PC Card.

When the installation is complete, a new Wireless communication icon will appear in your system tray in the Windows toolbar.

2. Click the Wireless icon to start the Windows Zero Configuration Utility. Refer to Microsoft for documentation on the utility.

Macintosh Mac OS X 10.2 and higher and Linux drivers





The Netopia 3-D Reach Utility only supports Windows 98, 2K, ME, and XP. Additional driver support for other Operating Systems may be downloaded from the Ralink Support website at www.ralink.com.tw. These drivers have not been tested and are not supported by Netopia.

[Windows XP users only, Note:] When the Netopia 3D REACH Utility exits from the system, it will restore WZC to its initial state before starting Netopia 3D REACH Utility, for example, if WZC is stopped before the Netopia 3D REACH Utility started. WZC will stay stopped after the Netopia 3D REACH Utility terminated. If WZC is running before the Netopia 3D REACH Utility is started, it will be re-enabled after the Netopia 3D REACH Utility exited.



Figure 2-2 Netopia 3D REACH Utility icon

In addition, the small icon will change color to reflect the current wireless network connection status. The status is indicated as follows:

- : Indicates Connected and Signal Strength is Excellent/Good.
- : Indicates Connected and Signal Strength is Fair/Poor
- : Indicates Not Connected yet.
- : Indicates Wireless card or driver not ready.

Site Survey

Under the Site Survey tab, the system displays the information of surrounding Access Points from the results of the last scan. List information includes SSID, BSSID, Signal, Channel, Encryption Algorithm, and Network Type as shown in Figure 3-1.

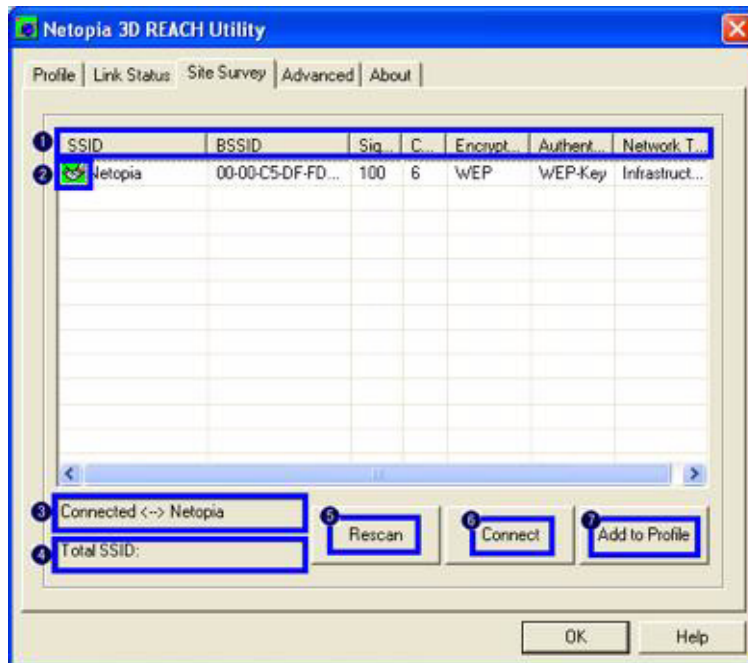


Figure 3-1 Detail information of site survey page


1 Definition of each field

1. SSID: Name of BSS or IBSS network.
2. BSSID: MAC address of Access Point or randomly generated from IBSS.
3. Signal: Received signal strength of specified network.
4. Channel: Channel in use.
5. Encryption: Encryption algorithm used within the BSS or IBSS. Valid value includes WEP, TKIP, AES, and Open.

6. Authentication: Authentication mode used within the network, including Open, WEP-Key, WPA-PSK and WPA.
7. Network Type: Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.

2 Connected network:

1. When the Netopia 3D REACH Utility is running, it will automatically select the best Access Point to which to connect.
2. If you want to connect to another Access Point, you can double click on the desired Access Point to make the connection.
3. If the desired network has encryption other than "Open", the Netopia 3D REACH Utility will display the security page and let you input the appropriate information to make the connection. Refer to section 4 on how to fill in the security information.

 This icon indicates the connection is successful.

3 Indicates the connection status; the connected network's SSID will show up here.

4 The numbers of SSID found in your surrounding wireless network.

5 Issue a rescan command to the wireless device to update information on the surrounding wireless network.

6 Command to connect to the selected wireless network.

7 Add the selected Access Point to the Profile setting. It will display the Profile page and save your setting to the profile setting.

ADD/EDIT Profile

1. System Configuration as shown in figure 3-2.

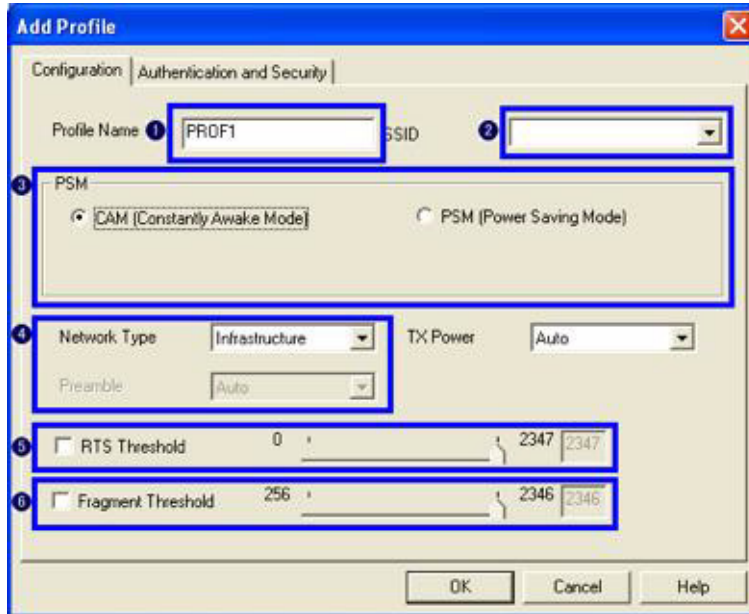


Figure 3-2 Profile system configuration

- 1 Profile Name: You can enter a name for this profile.
- 2 SSID: You can input the intended SSID name or use the pull down menu to select from the available Access Points.
- 3 Power Save Mode: You can choose CAM (Constantly Awake Mode) or Power Saving Mode.
- 4 Network Type: There are two types, infrastructure and 802.11 ad-hoc mode. Under ad-hoc mode, you can also choose the preamble type. The available preamble type includes short and long. Also, the channel field will be available for setup in ad-hoc mode.

- 5 RTS Threshold: You can adjust the RTS threshold number by sliding the bar or key directly to a value. The default value is 2347.
 - 6 Fragment Threshold: You can adjust the Fragment threshold number by sliding the bar or key directly to a value. The default value is 2346.
 - 7 Channel: Only available for setting under ad-hoc mode. You can choose the channel frequency for your ad-hoc network.
2. Authentication and Security settings are shown in figure 3-3. Detailed operations are explained in section 4.

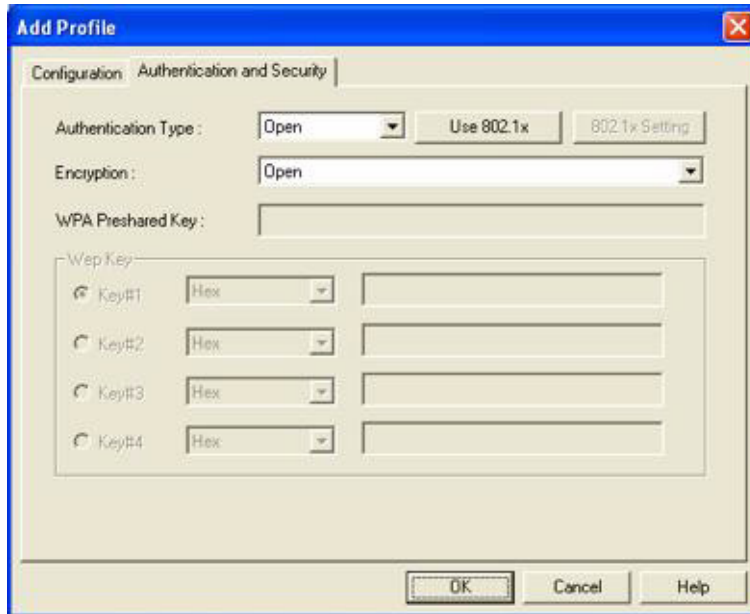


Figure 3-3 Profile Authentication and Security

Encryption Setting WEP/TKIP/AES

Authentication and Security settings, shown in figure 4-1.

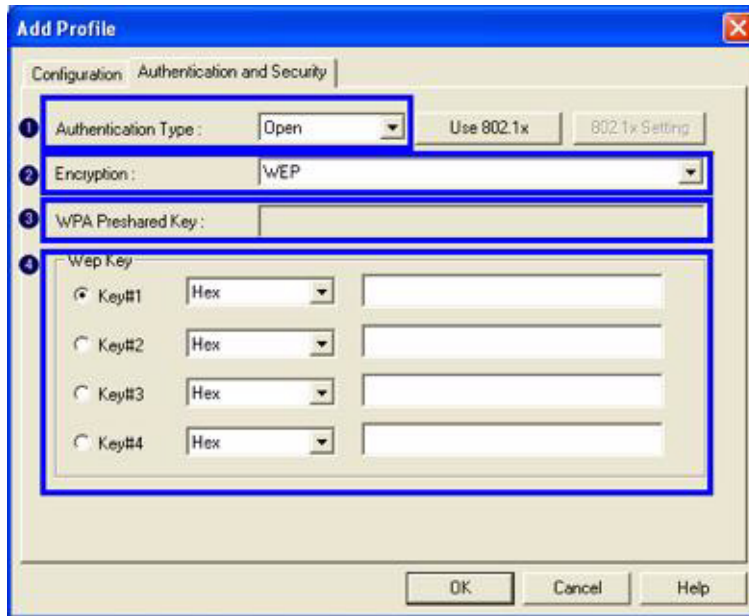


Figure 4-1 Authentication and Security setting

- 1 Authentication Type: Three types of authentication modes are supported by the Netopia 3D REACH Utility: Open, Shared, WPA-PSK and WPA system.
- 2 Encryption Type: For Open and Shared authentication mode, the selections of encryption type are None and WEP. For WPA and WPA-PSK authentication mode, the encryption types that are supported are TKIP and AES.
- 3 WPA Preshared Key: This is the shared key between the Access Point and the STA. For WPA-PSK authentication mode, this field must be filled in with between 8 and 32 characters.

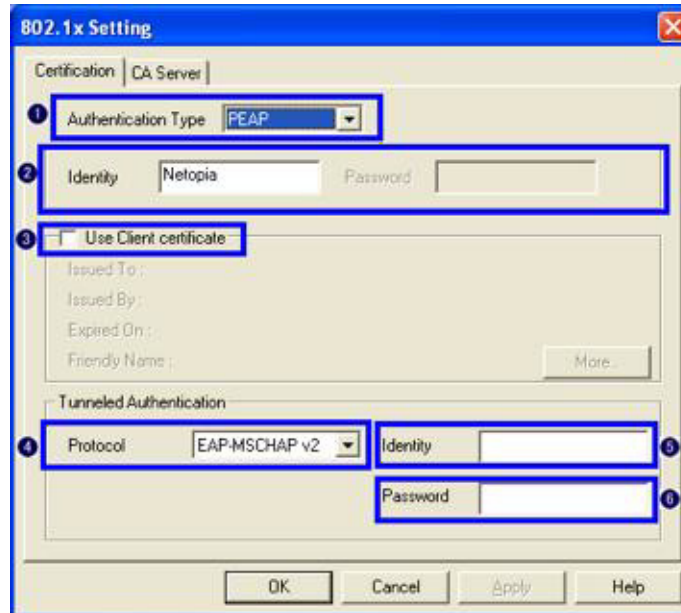
④ WEP Key: Only valid when using WEP encryption algorithm. The key must match the Access Point's key. There are several formats to enter the keys.

1. Hexadecimal`40bits: 10 Hex characters.
2. Hexadecimal`128bits: 32Hex characters.
3. ASCII`40bits: 5 ASCII characters.
4. ASCII`128bits: 13 ASCII characters.

See the examples in “Configure connection with WEP ON” on page 39, “Configure connection with WPA-PSK” on page 43, and “Configure connection with WPA by 802.1x setting” on page 47

802.1x Setting

802.1x is an authentication protocol for a “WPA” certificate to an authentication server. Shown as figure 14-14



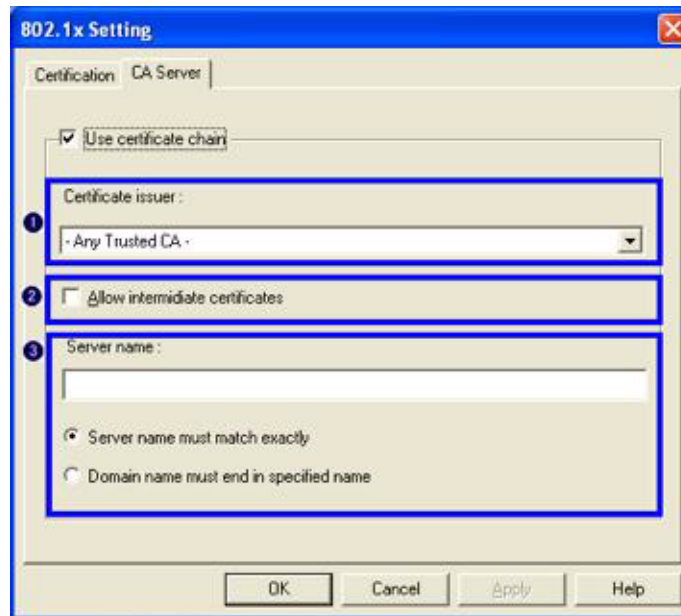
1 Authentication type:

1. PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authenticates data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
2. TLS/Smart Card: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.

3. **TLS: Tunneled Transport Layer Security.** This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
 4. **LEAP: Light Extensible Authentication Protocol.** It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.
 5. **MD5-Challenge: Message Digest Challenge.** Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.
-
2. **Identity and Password:** Identity and password for the server.
 3. **Use Client Certificate:** Client Certificate for server authentication.
 4. **Protocol:** Tunnel protocol, List information include "EAP-MSCHAP ", "EAP-MSCHAP v2", "CAHAP "and "MD5 ".
 5. **Tunnel Identity:** Identity for a tunnel.
 6. **Tunnel Password:** Password for a tunnel.

CA Server

Depending on the EAP in use, only the server or both the server and client may be authenticated and require a certificate. Server certificates identify a server, usually an authentication or RADIUS server to clients. Most EAPs require a certificate issued by a root authority or a trusted commercial Certificate Authority. Shown as the figure below.



- 1 Certificate issuer: Choose the server that issues certificates.
- 2 Allow intermediate certificates: Must be in the server certificate chain between the server certificate and the server specified in the Certificate issuer field.
- 3 Server name: Enter an authentication server root.

Profile

You can save your favorite wireless setting among your home, office, and other public hotspots in a Profile. You can save multiple profiles, and activate the correct one at your preference. Figure 5-1 shows the Profile page setting.

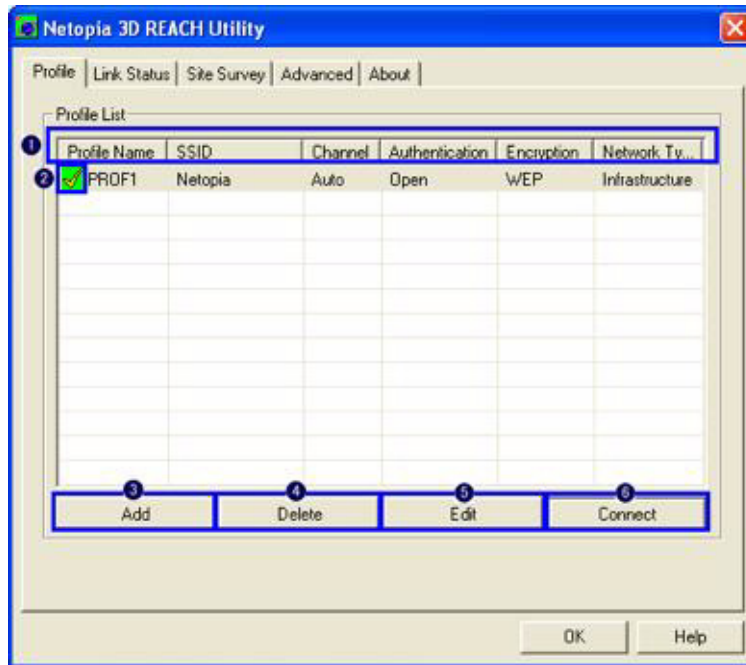


Figure 5-1 Profile page

- 1 Definition of each field:
 1. Profile: Name of profile, default preset to PROF* (* indicates 1, 2, 3, etc.).
 2. SSID: Access Point's or Ad-hoc's name.
 3. Channel: Channel in use.
 4. Authentication: Authentication mode.
 5. Encryption: Security algorithm in use.
 6. Network Type: Network's type, including Infrastructure and Ad-Hoc.

② Connection status

🟢 Indicates connection is successful on current activated profile.

🔴 Indicates connection failed on current activated profile.

③ Add a new profile.

④ Delete an existing profile.

⑤ Edit a Profile.

⑥ Activate selected profile.

Link Status

Figure 6-1 is the Link Status page; it displays detailed information about the current connection.

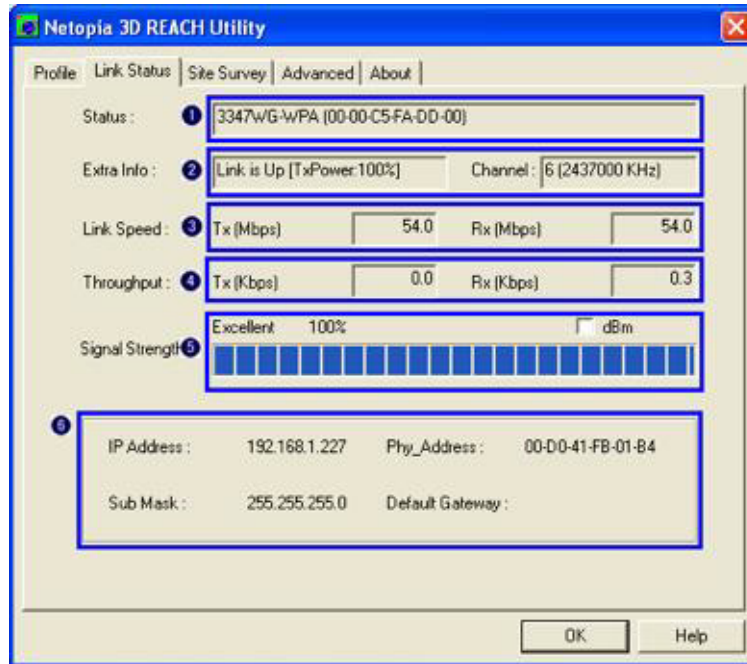


Figure 6-1 Link Status information

- ❶ Status: Current connection status. If there is no connection, it will show Disconnected. Otherwise, the connected SSID and BSSID will be shown here.
- ❷ Extra Info: Display link status and current channel in use.
- ❸ Link Speed: Display current transmit rate and receive rate.
- ❹ Throughput: Displays throughput (Tx: transmits and Rx: receives) in units of Kbits/sec.

5 Signal Strength: Reception signal strength; you can choose to display as a percentage or dBm format.

6 Displays wireless card's TCP/IP and physical address information.

Advanced

Figure 8-1 shows Advanced setting page of the Netopia 3D REACH Utility.

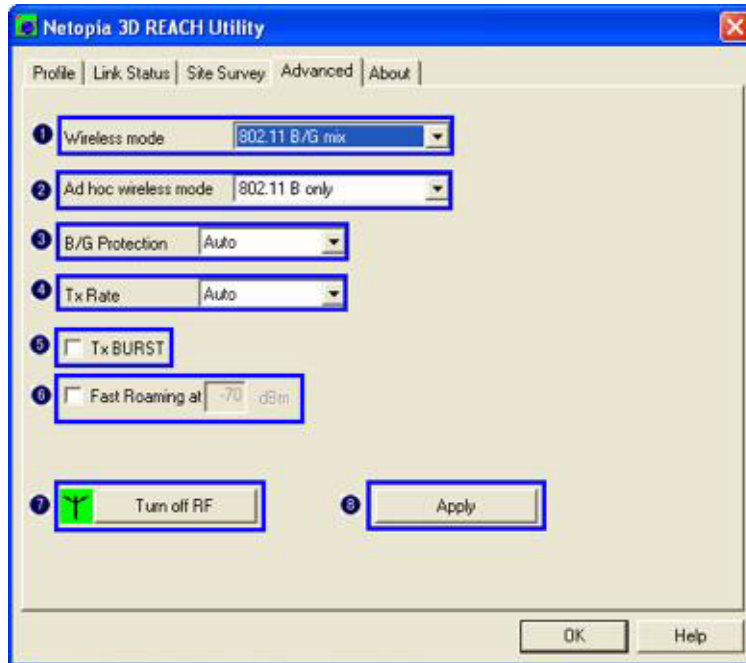


Figure 8-1 Advanced setting

1. Wireless mode: Select wireless mode. “802.11b only” and “802.11 B/G mix” modes are supported.
2. Ad hoc wireless mode: Select Ad hoc wireless mode. “802.11b only”, “802.11 B/G mixed”, and “802.11 G only” modes are supported.
3. B/G Protection: ERP protection mode of 802.11G definition. You can choose from Auto, On or Off.
 1. Auto: STA will dynamically change as Access Point announcement.
 2. On: Always send frames with protection.

3. Off: Always send frames without protection.

4 TX Rate: Manually force the Transmit using selected rate. Default is auto.

5 Tx Burst: Netopia 3D REACH Utility's proprietary frame burst mode.

6 Fast Roaming at: fast to roaming, setup by transmit power.

7 Turn radio ON/OFF for FAA requirement.



Radio On: Indicate to turn on radio.



Radio Off: Indicate to turn off radio.

8 Apply the above changes.

Country Channel List

Country channel list, channel classification and range.

Classification	Range	
0: FCC	CH1 ~	CH11
1: IC (Canada)	CH1 ~	CH11
2: ETSI	CH1 ~	CH13
3: SPAIN	CH10 ~	CH11
4: FRANCE	CH10 ~	CH13
5: MKK	CH14 ~	CH14
6: MKKI (TELEC)	CH1 ~	CH14
7: ISRAEL	CH3 ~	CH9

Country Name	Classification	Range
Argentina	0	CH1~11
Australia	2	CH1~13
Austria	2	CH1~13
Bahrain	2	CH1~13
Belarus	2	CH1~13
Belgium	2	CH1~13
Bolivia	2	CH1~13
Brazil	0	CH1~11
Bulgaria	2	CH1~13
Canada	0	CH1~11
Chile	2	CH1~13
China	2	CH1~13
Colombia	0	CH1~11
Costa Rica	2	CH1~13

Country Name	Classification	Range
Croatia	2	CH1~13
Cyprus	2	CH1~13
Czech Republic	2	CH1~13
Denmark	2	CH1~13
Ecuador	2	CH1~13
Egypt	2	CH1~13
Estonia	2	CH1~13
Finland	2	CH1~13
France	4	CH10~13
France2	2	CH1~13
Germany	2	CH1~13
Greece	2	CH1~13
Hong Kong	2	CH1~13
Hungary	2	CH1~13
Iceland	2	CH1~13
India	2	CH1~13
Indonesia	2	CH1~13
Ireland	2	CH1~13
Israel	7	CH3~9
Italy	2	CH1~13
Japan	6	CH1~14
Japan2	5	CH14~14
Japan3	2	CH1~13
Jordan	4	CH10~13
Kuwait	2	CH1~13
Latvia	2	CH1~13
Lebanon	2	CH1~13
Latvia	2	CH1~13
Lebanon	2	CH1~13
Liechtenstein	2	CH1~13
Lithuania	2	CH1~13

Country Channel List

Country Name	Classification	Range
Luxembourg	2	CH1~13
Macedonia	2	CH1~13
Malaysia	2	CH1~13
Mexico	0	CH1~11
Morocco	2	CH1~13
Netherlands	2	CH1~13
New Zealand	2	CH1~13
Nigeria	2	CH1~13
Norway	2	CH1~13
Panama	2	CH1~13
Paraguay	2	CH1~13
Peru	2	CH1~13
Philippines	2	CH1~13
Poland	2	CH1~13
Portugal	2	CH1~13
Puerto Rico	2	CH1~13
Romania	2	CH1~13
Russia	2	CH1~13
Saudi Arabia	2	CH1~13
Singapore	2	CH1~13
Slovakia	2	CH1~13
Slovenia	2	CH1~13
South Africa	2	CH1~13
South Korea	2	CH1~13
Spain	3	CH10~11
Sweden	2	CH1~13
Switzerland	2	CH1~13
Taiwan	0	CH1~11
Thailand	2	CH1~13
Turkey	2	CH1~13
United Arab Emirates	2	CH1~13

Country Name	Classification	Range
United Kingdom	2	CH1~13
United States of America	0	CH1~11
Uruguay	2	CH1~13
Venezuela	2	CH1~13
Yugoslavia	0	CH1~11

About

The About page displays the wireless card and driver version information as shown in figure 9-1.

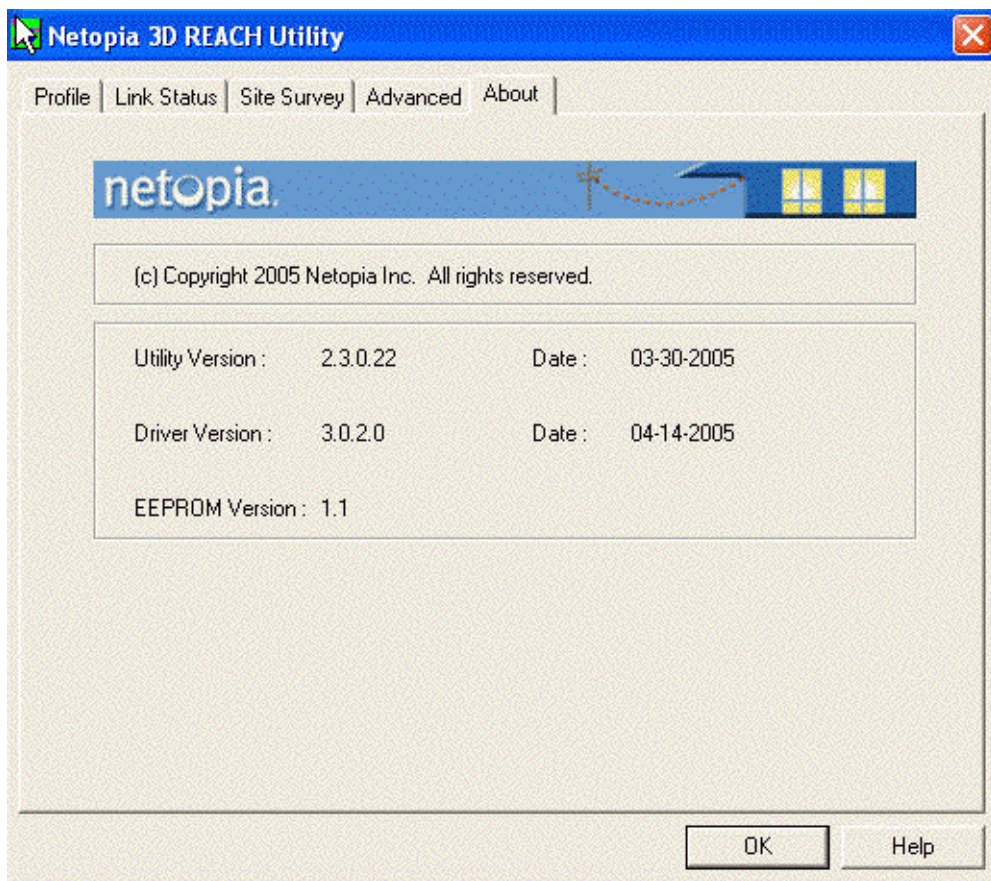
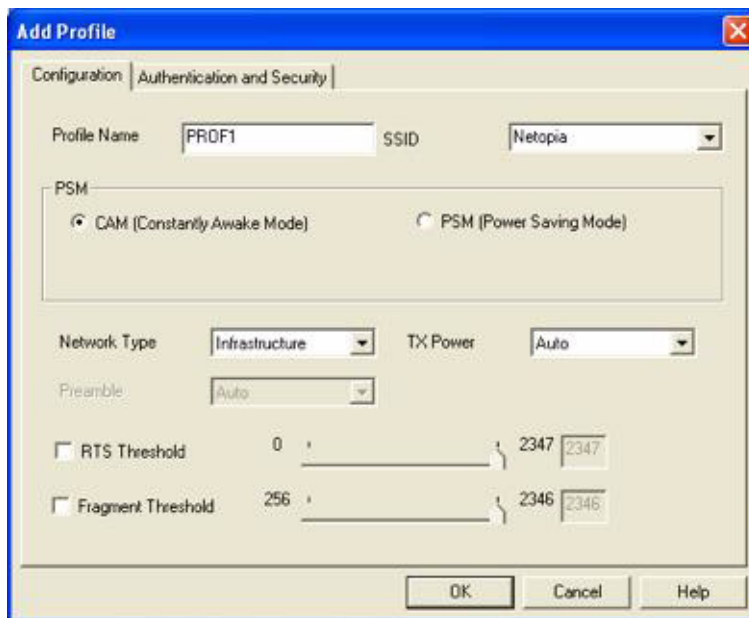


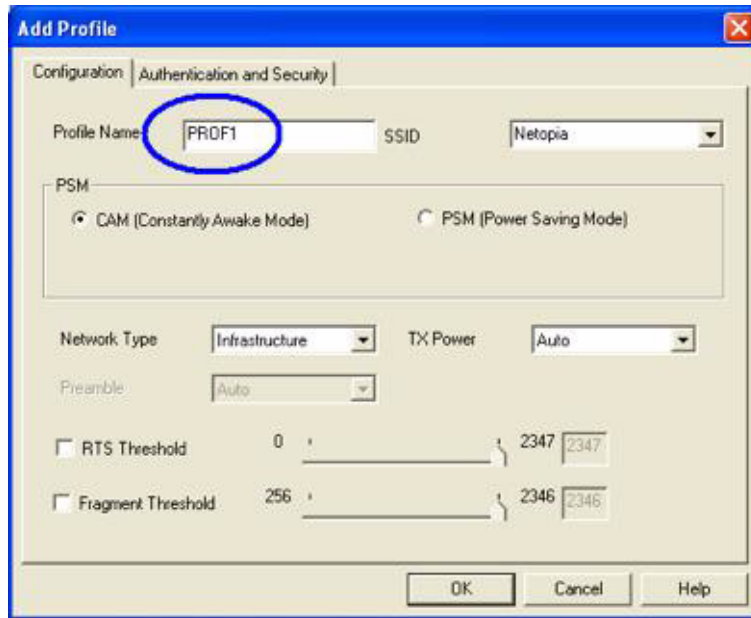
Figure 9-1 About Page

It displays the Configuration Utility Version, Driver Version, and EEPROM Version information.

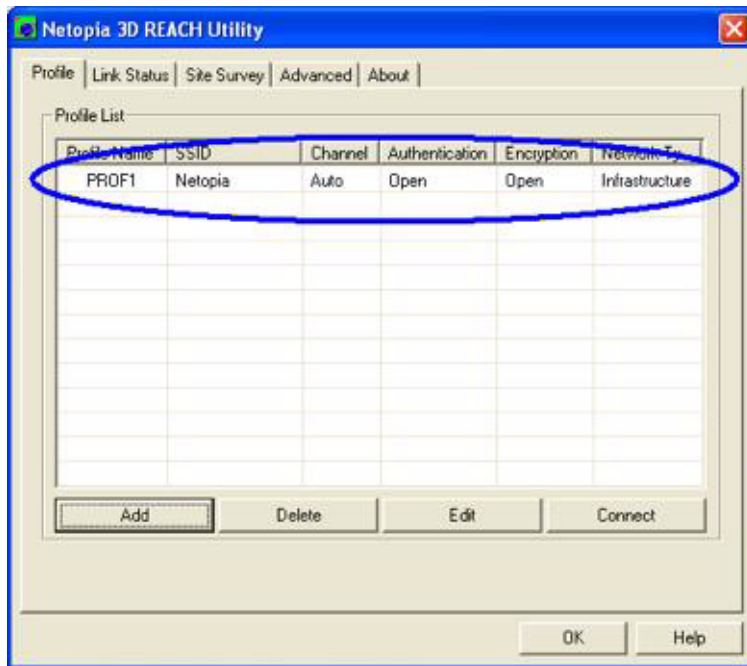
3. The Add Profile window appears.



4. Change the Profile Name to your preference (optional).

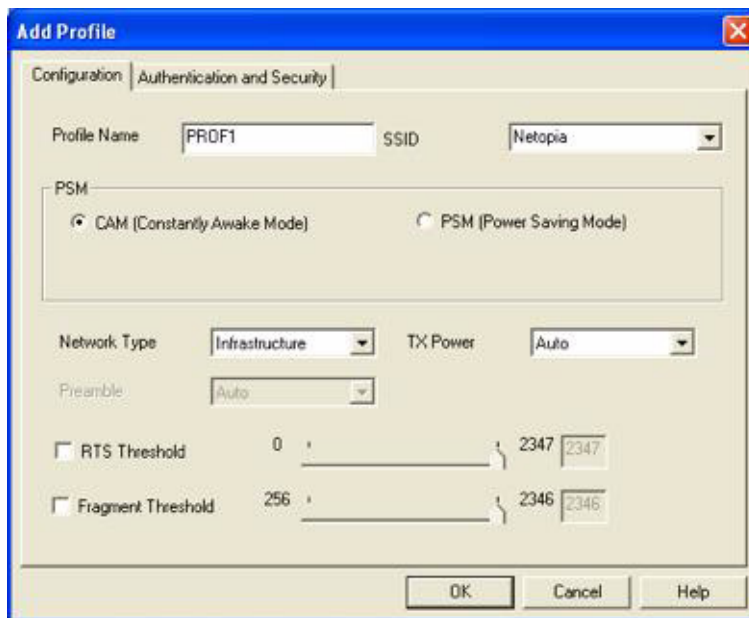


5. Click the OK button without changing any other values.

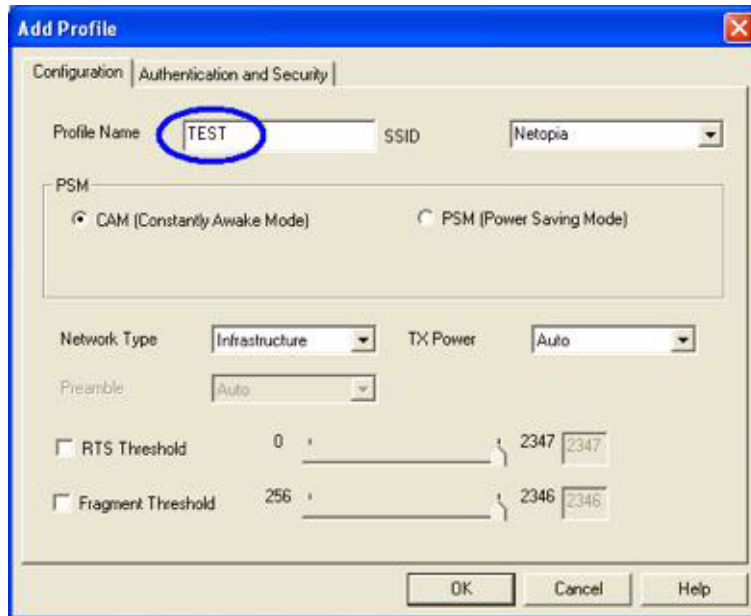


6. Follow the examples in the section “Configure connection with WEP ON” on page 39, the section “Configure connection with WPA-PSK” on page 43 or the section “Configure connection with WPA by 802.1x setting” on page 47 to set the authentication and security page.

2. The Add Profile page appears.

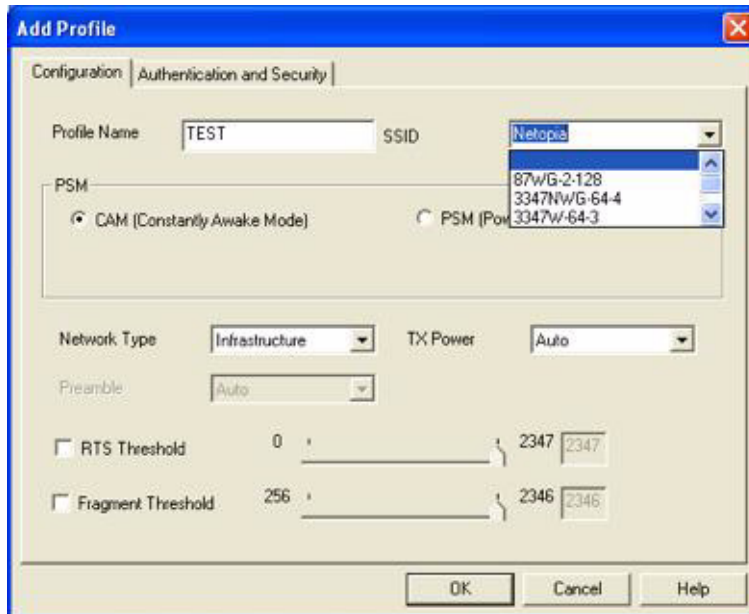


3. Change the Profile Name to your preference (optional).

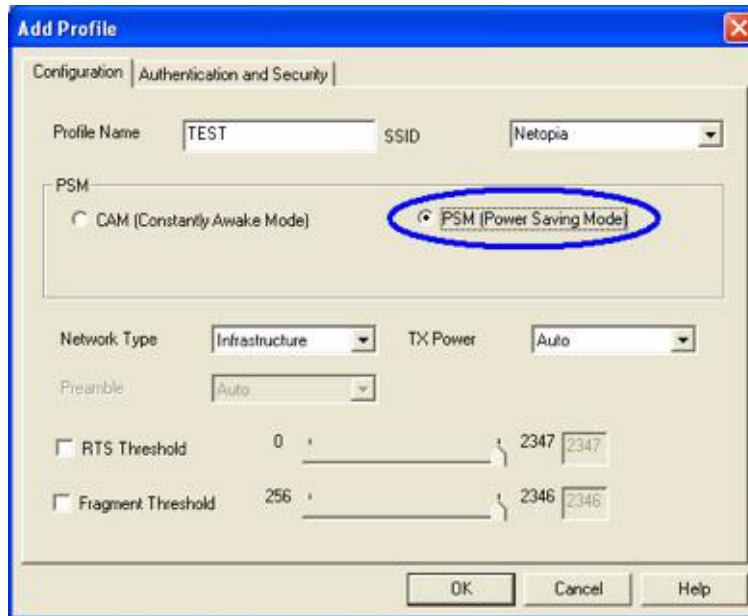


The screenshot shows a dialog box titled "Add Profile" with a blue title bar and a close button in the top right corner. The dialog is divided into two tabs: "Configuration" and "Authentication and Security". The "Configuration" tab is active. The "Profile Name" field contains the text "TEST" and is circled in blue. The "SSID" field is a dropdown menu currently showing "Netopia". Below these fields is a section for "PSM" (Power Saving Mode) with two radio buttons: "CAM (Constantly Awake Mode)" which is selected, and "PSM (Power Saving Mode)". Further down, there are three dropdown menus: "Network Type" set to "Infrastructure", "TX Power" set to "Auto", and "Preamble" set to "Auto". At the bottom, there are two checkboxes: "RTS Threshold" (unchecked) with a value of 0 and "Fragment Threshold" (unchecked) with a value of 256. To the right of these values are two small input boxes containing the numbers 2347 and 2346 respectively. At the very bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

- From the SSID pull-down menu select your desired Access Point. The Access Point list is generated from the results of the site survey.

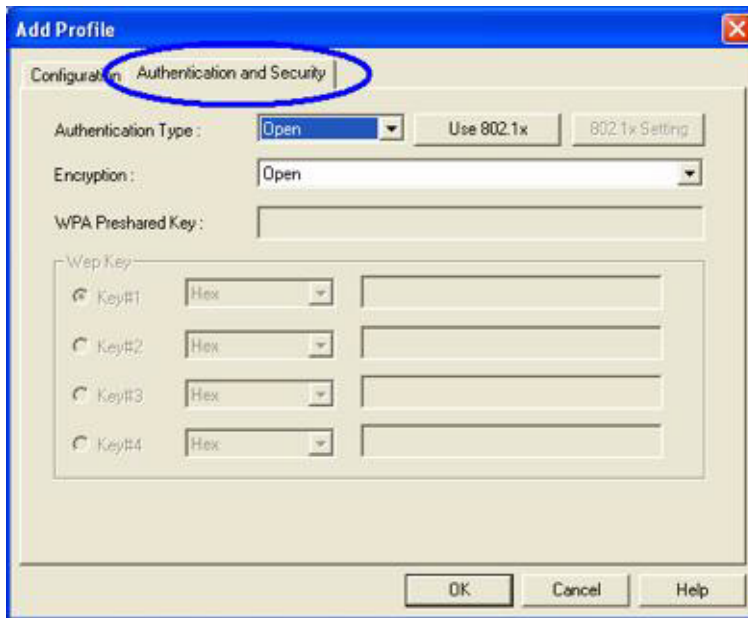


5. Set the desired Power Saving Mode (optional).



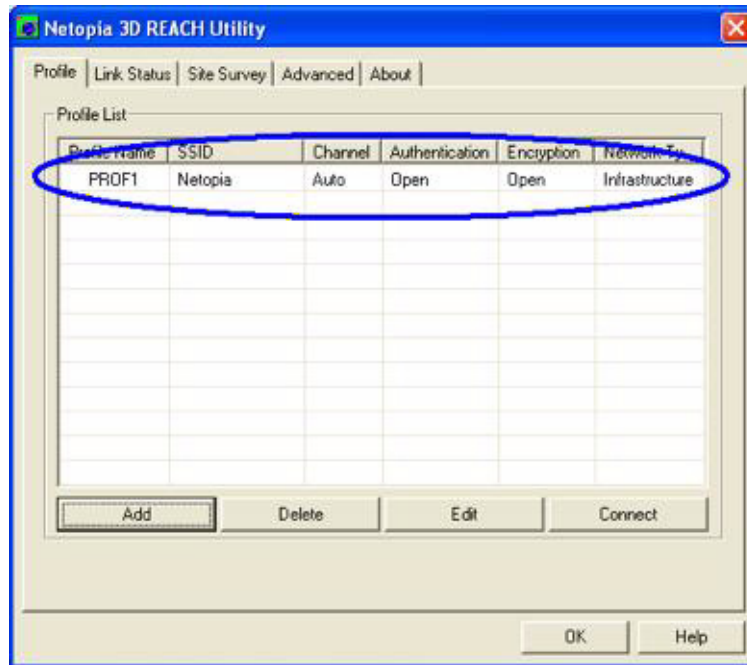
6. Click the Authentication and Security tab.

The Authentication and Security page appears.

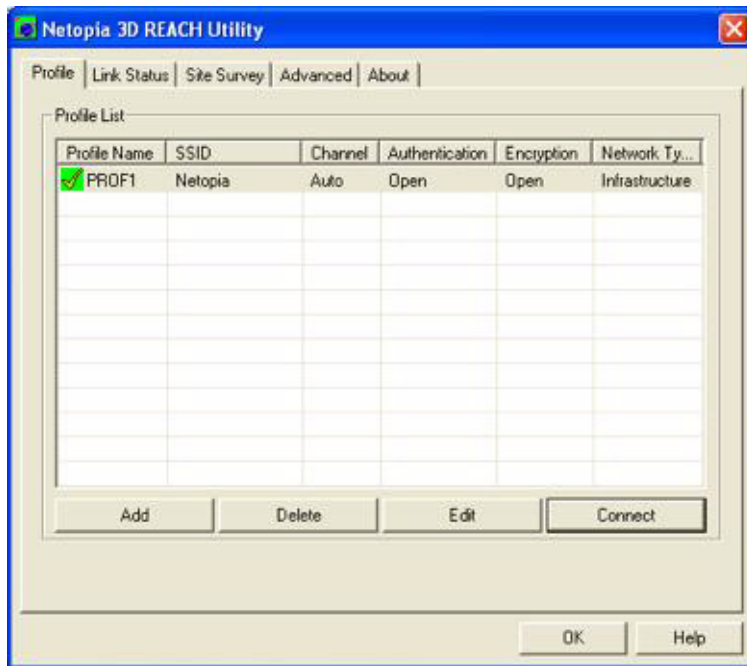


7. Click the OK button.

The created profile appears in the Profile List.



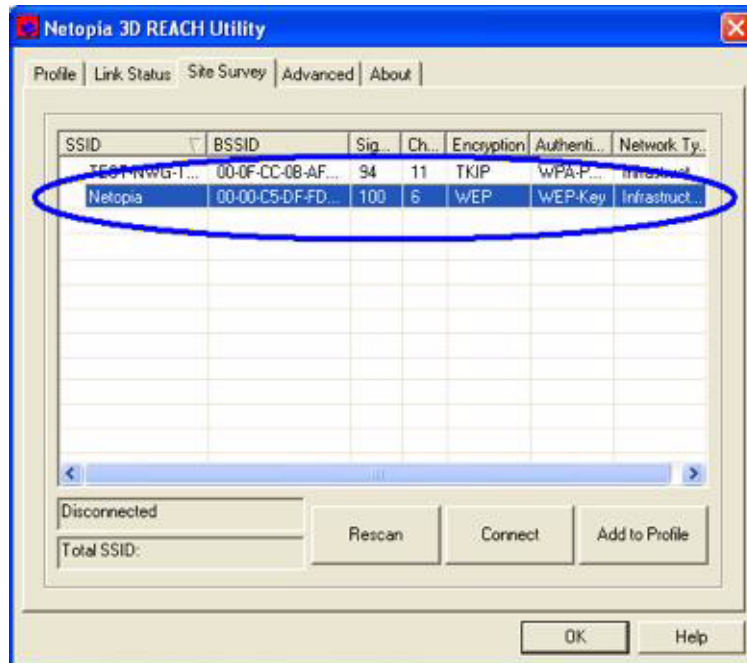
8. Click the Connect button to activate the profile setting.



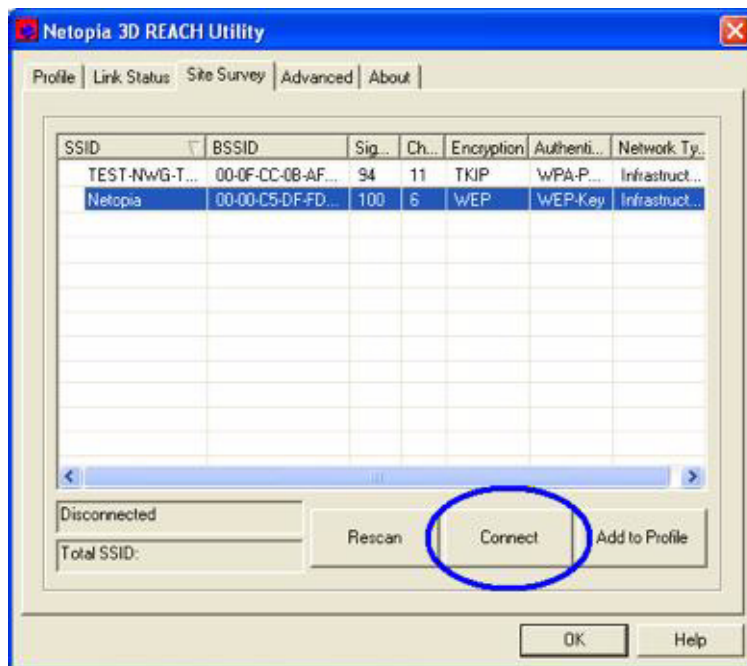
9. Follow the examples in the section “Configure connection with WEP ON” on page 39, the section “Configure connection with WPA-PSK” on page 43 or the section “Configure connection with WPA by 802.1x setting” on page 47 to set the authentication and security page.

Configure connection with WEP ON

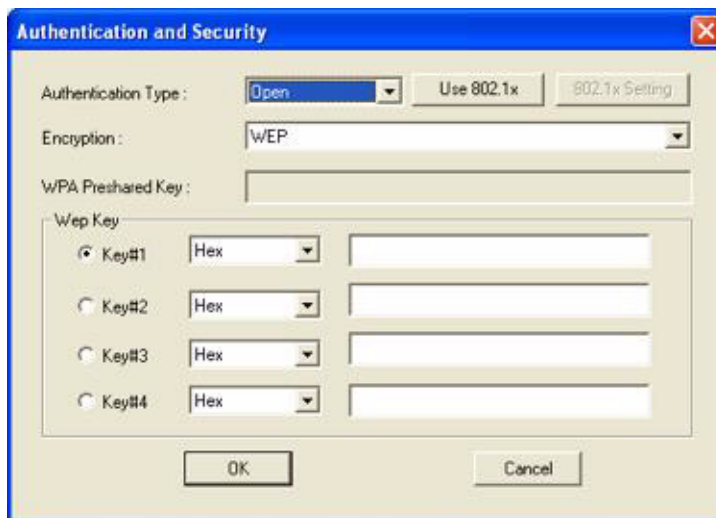
1. Select an Access Point with WEP encryption.



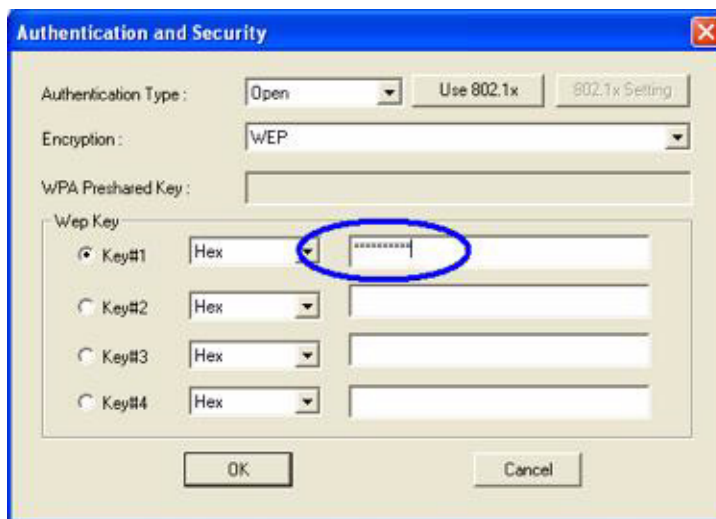
2. Click the Connect button or double-click on the intended network.



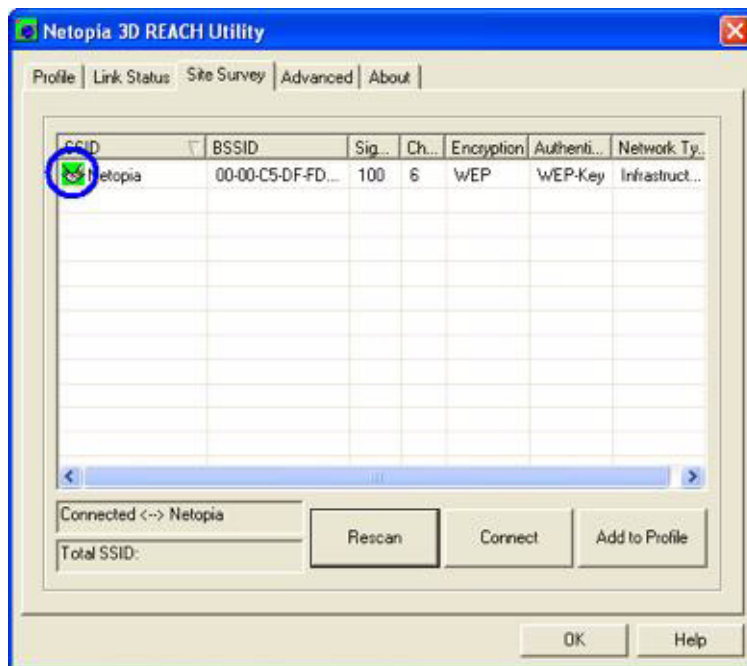
3. The Authentication and Security page appears.



4. Enter the proper key setting that matches your Access Point's.

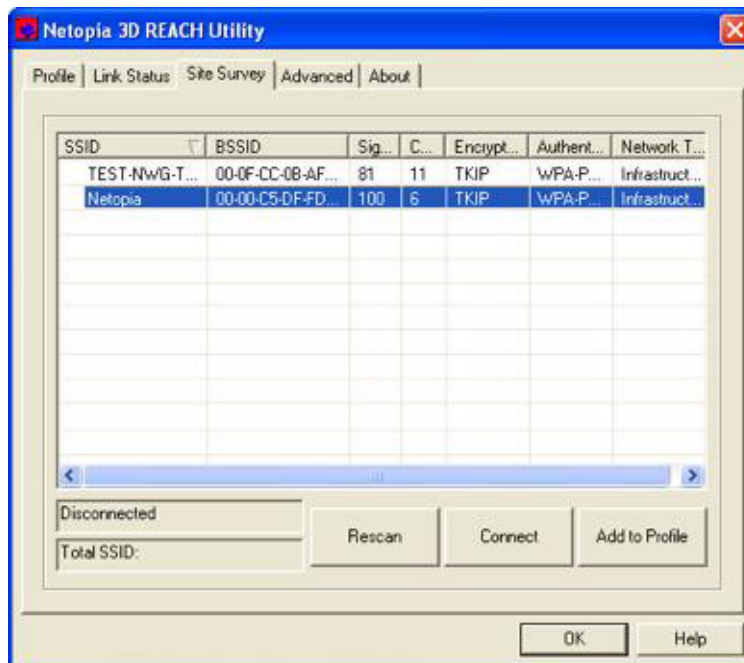


5. Click the OK button. An established connection will look like the figure below.

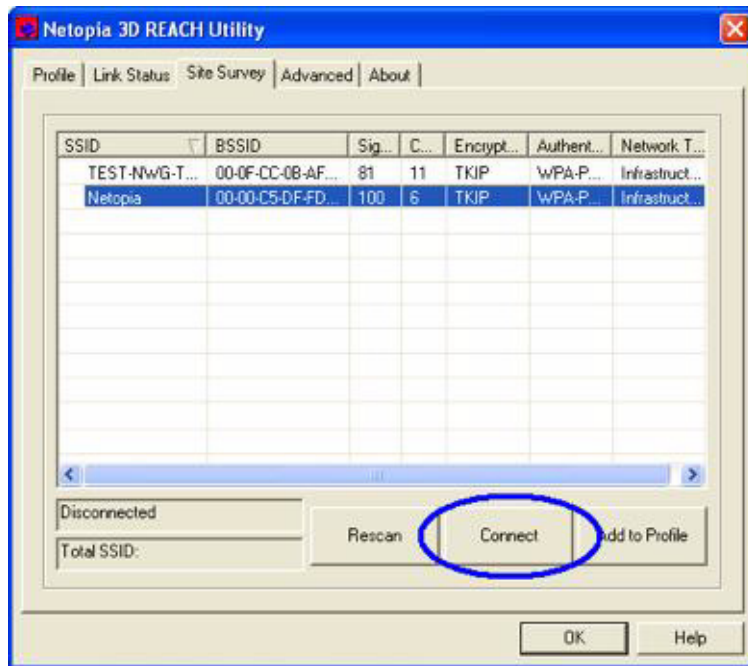


Configure connection with WPA-PSK

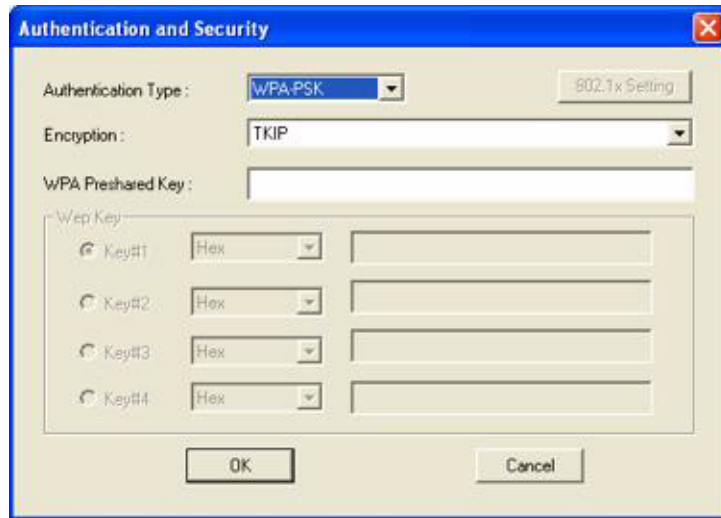
1. Select an Access Point with WPA-PSK authentication mode.



2. Click the Connect button or double click the intended network.

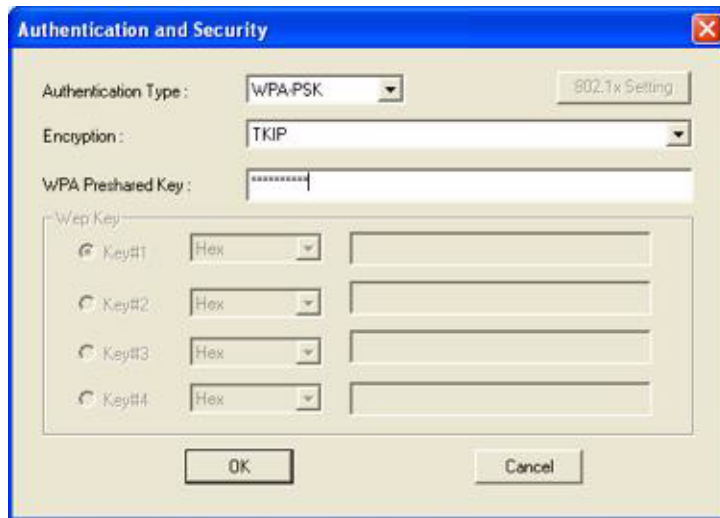


The Authentication and Security page appears.



3. The Authentication Type is WPA-PSK.

Select the correct encryption (TKIP or AES). Enter the WPA Preshared Key.



4. Click the OK button.

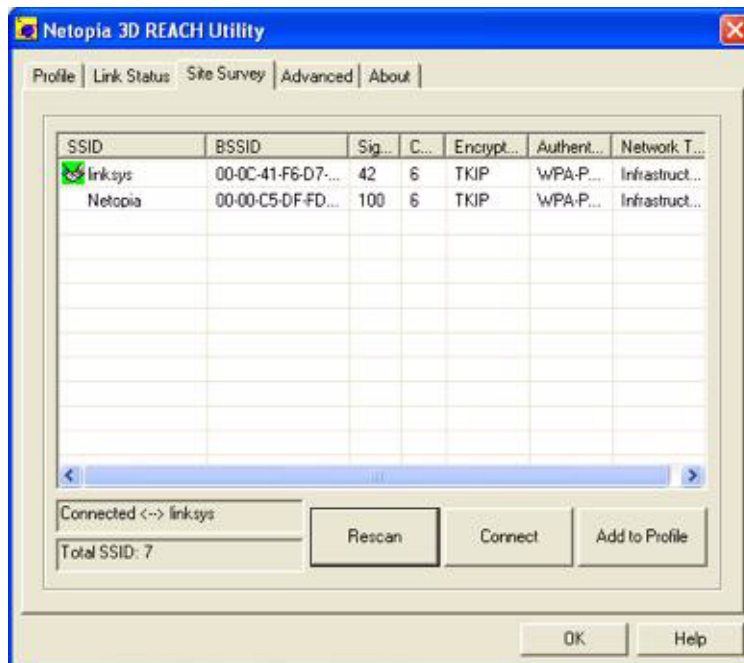


Warning:

If the WPA Preshared Key is entered incorrectly, the Access Point will be shown as connected, but you won't be able to exchange any data.

Configure connection with WPA by 802.1x setting

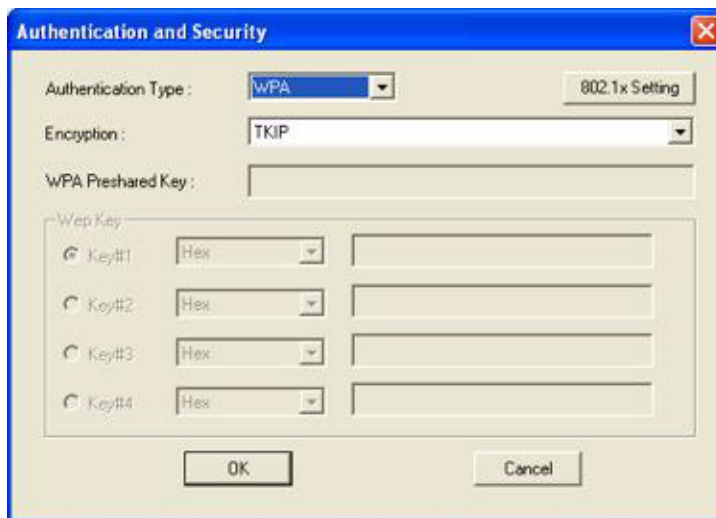
1. Select an Access Point with WPA authentication mode.



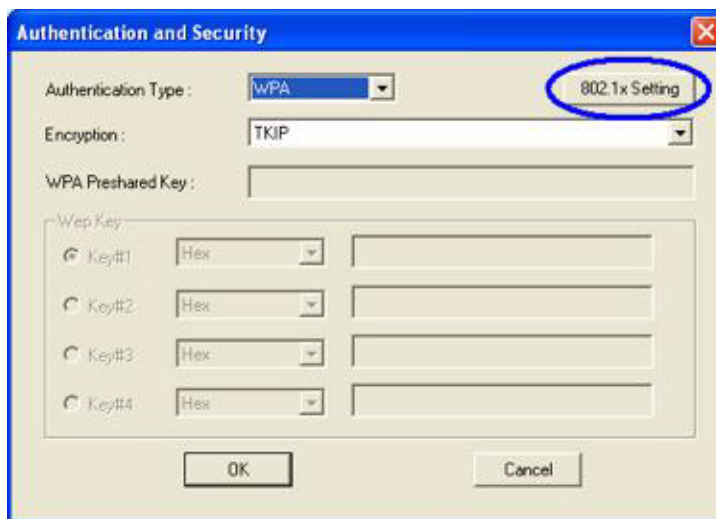
2. Click the Connect button or double-click the desired network.



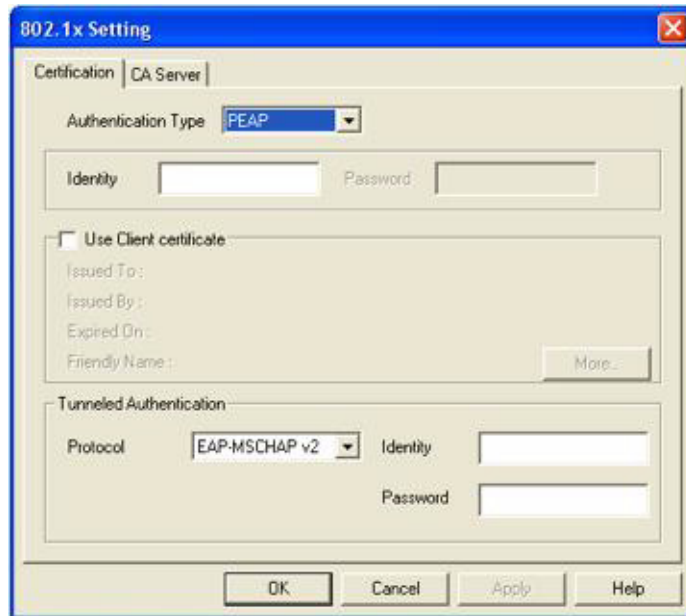
3. The Authentication and Security page appears.



4. Click the 802.1x Setting button.



5. The 802.1x Setting page appears.

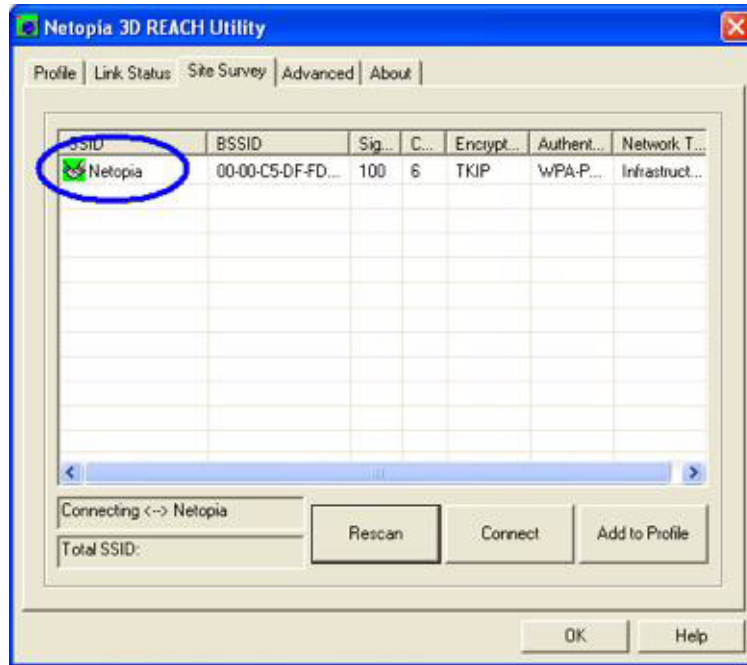


6. Authentication Type and setting method:

① PEAP:

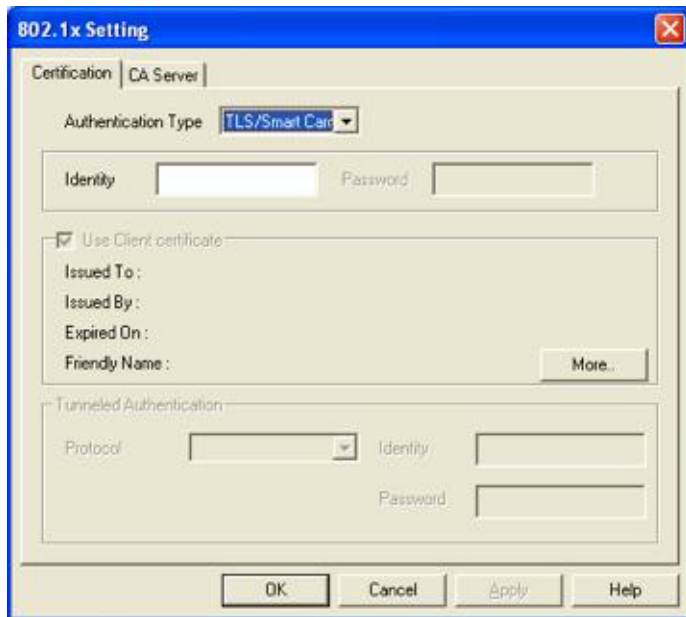
1. Authentication Type: choose PEAP, enter your identity (example: Netopia) in the Identity field. Tunneled Authentication: Protocol: choose EAP-MSCHAP v2, tunnel Identity is Netopia and tunnel Password is test. The setting is an example.

2. Click the OK button. The result will look like the figure below.

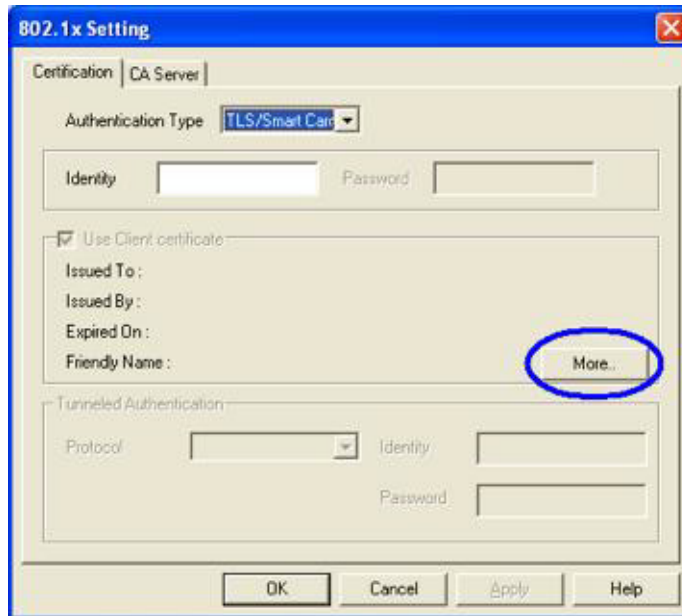


④ TLS / Smart Card:

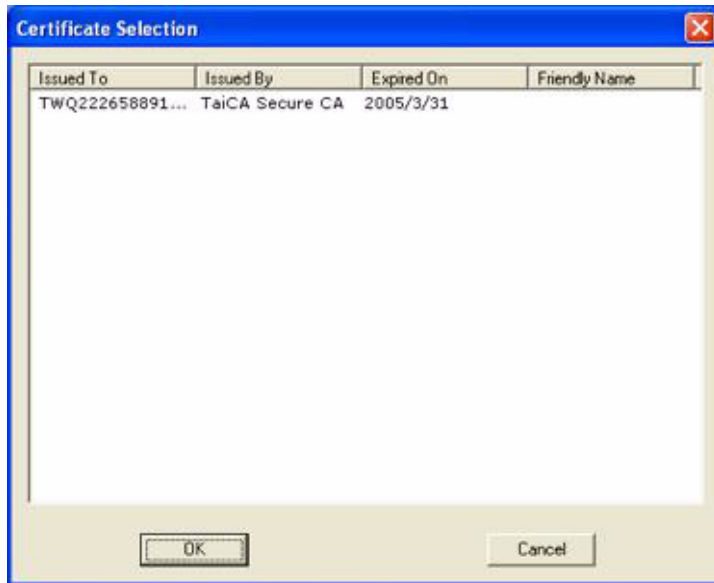
1. Authentication Type: choose TLS / Smart Card, TLS only needs an Identity that is Netopia for server authentication. The setting is an example.



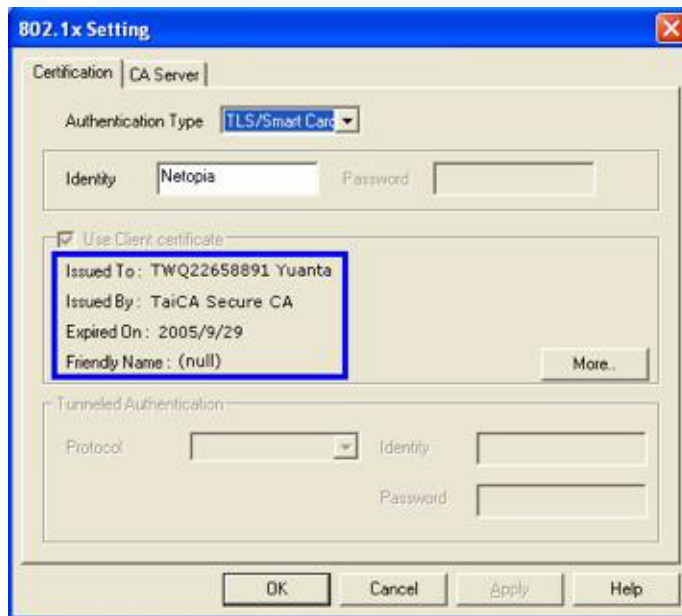
2. TLS must use a client certificate. Click the More button to choose a certificate.



3. The Certificate Selection page appears. Choose a certificate for server authentication.



4. To display certificate information in use see the client Certification page.

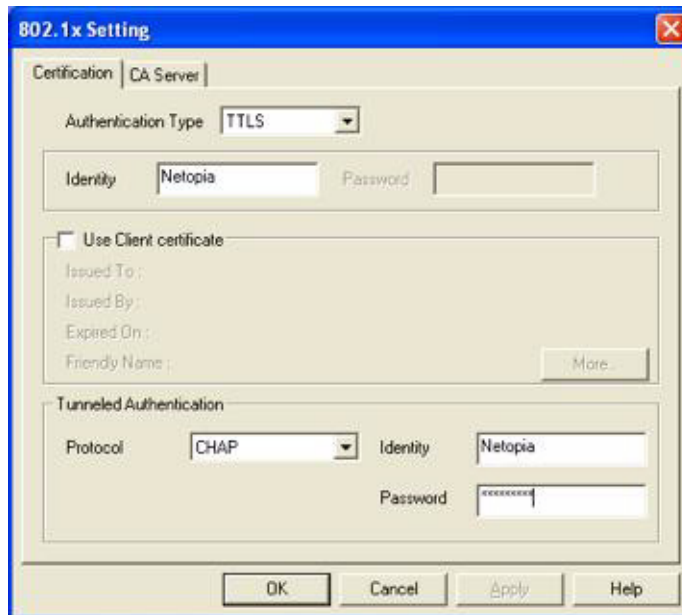


5. Click the OK button. The result will look like the figure below.



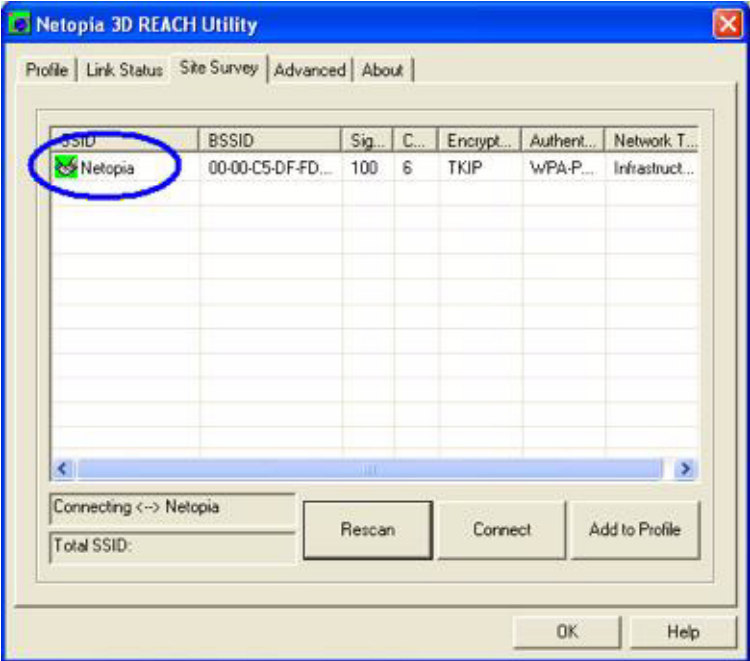
3 TTLS:

1. Authentication Type: choose TTLS; Identity is Netopia. For Tunnel Authentication Protocol choose CHAP, tunnel Identity is Netopia and tunnel Password is test. The setting is an example.



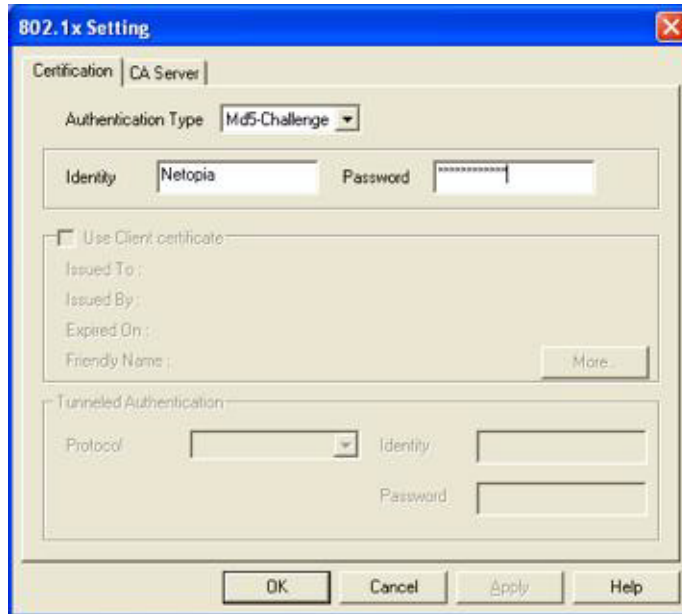
2. Click the OK button.

The result will look like the figure below.



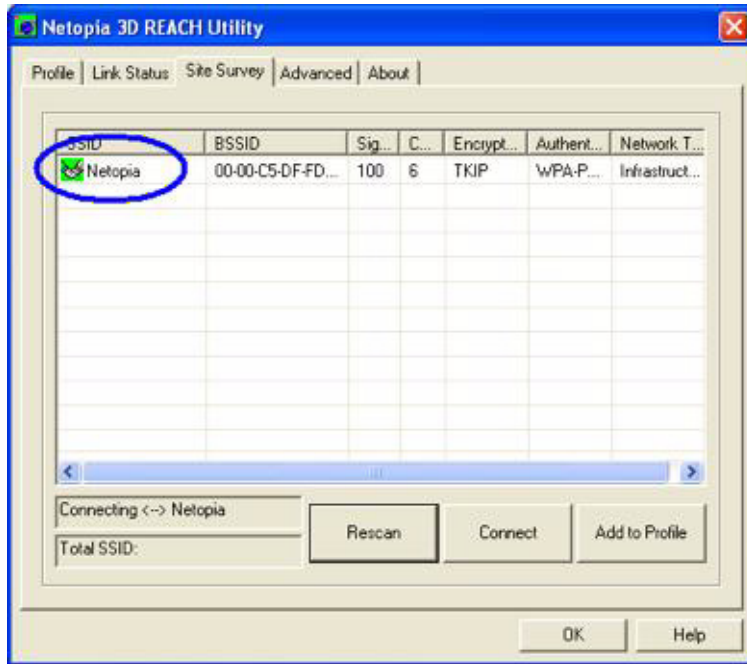
4 MD5:

1. Authentication Type: choose MD5; MD5 only needs identity and password - Netopia and test - for server authentication. The setting is an example.



2. Click the OK button.

The result will look like the figure below.



Excursuses

The above setting is a test platform by Netopia, inc. You can set the functions in accordance with the Access Point.

Acknowledgements:

“This product includes software developed by MDC and its licensors. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Netopia Part Number: 6161210-00-01

