108Mbps 802.11g MIMO Wireless miniPCI Module

User's Guide

Federal Communication Commission Interference Statement

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

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

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

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

This device is intended only for OEM integrators under the following conditions:

1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and
2) The transmitter module may not be co-located with any other transmitter or antenna.

As long as 2 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

IMPORTANT NOTE: In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users (for example : Access Point, Router…etc.). The final end product must be labeled in a visible area with the following: “Contains TX FCC ID: S9ZTEW610-611”.

TRENDnet declares that TEW610-611, (FCC ID: S9ZTEW610-611) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.

Manual Information That Must be Included

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the users manual of the end product which integrate this module.

The users manual for OEM integrators must include the following information in a prominent location “ IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements, the antenna 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.

Distance between two external antennas on housing is 15cm, and PLS refer to the following picture for antenna position.

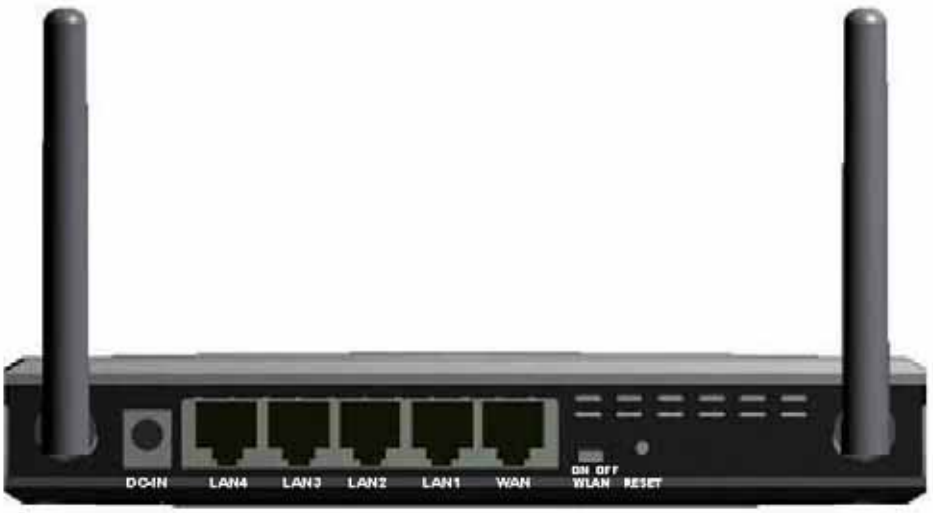


Table of Contents

Getting Started

This chapter introduces the module and prepares you to use the Wireless Utility.

About Your 802.11g WLAN MIMO mPCI

The Module is an IEEE 802.11b, and 802.11g compliant wireless LAN adapter. With the Module, you can enjoy wireless mobility within almost any wireless networking environment.
The following lists the main features of your Module.

- ✓ Your Module can communicate with other IEEE 802.11b/g compliant wireless devices.
- ✓ Automatic rate selection.
- ✓ Standard data transmission rates up to 54 Mbps.
- ✓ Proprietary Atheros transmission rates of 108 Mbps
- ✓ Offers 64-bit, 128-bit and 152-bit WEP (Wired Equivalent Privacy) data encryption for network security.
- ✓ Supports IEEE802.1x and WPA (Wi-Fi Protected Access).
- ✓ Low CPU utilization allowing more computer system resources for other programs.
- ✓ Support external antennas

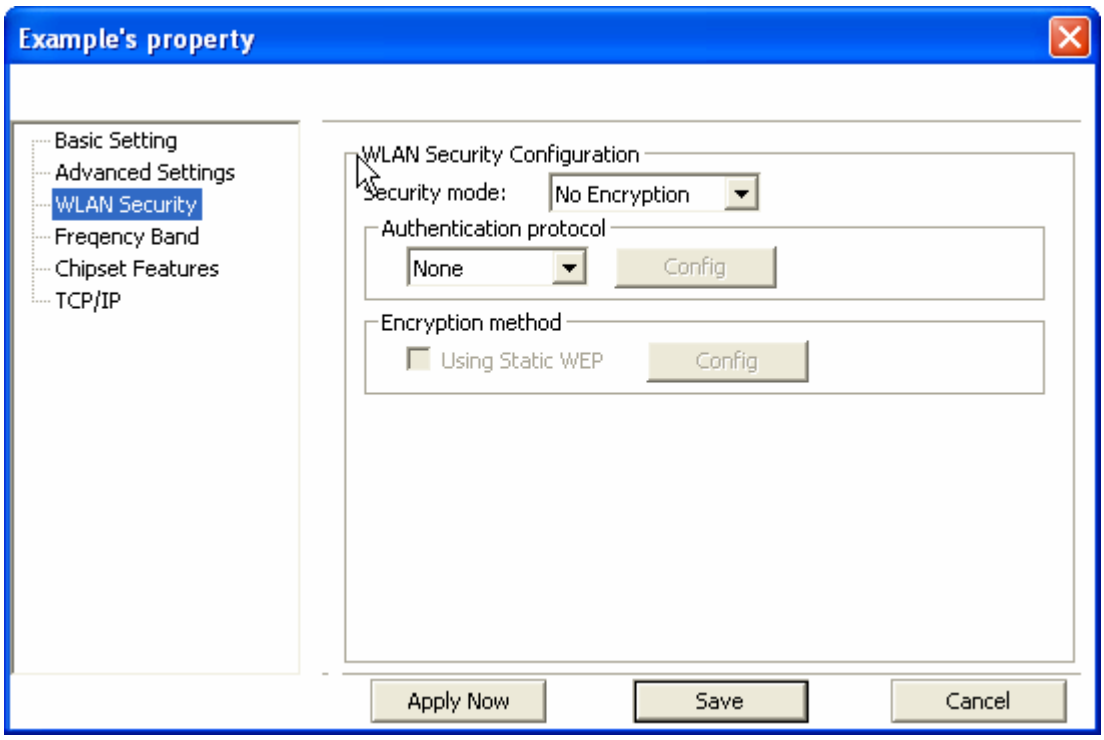
Configuring Wireless Security

This chapter covers the configuration of security options in the Wireless Utility.

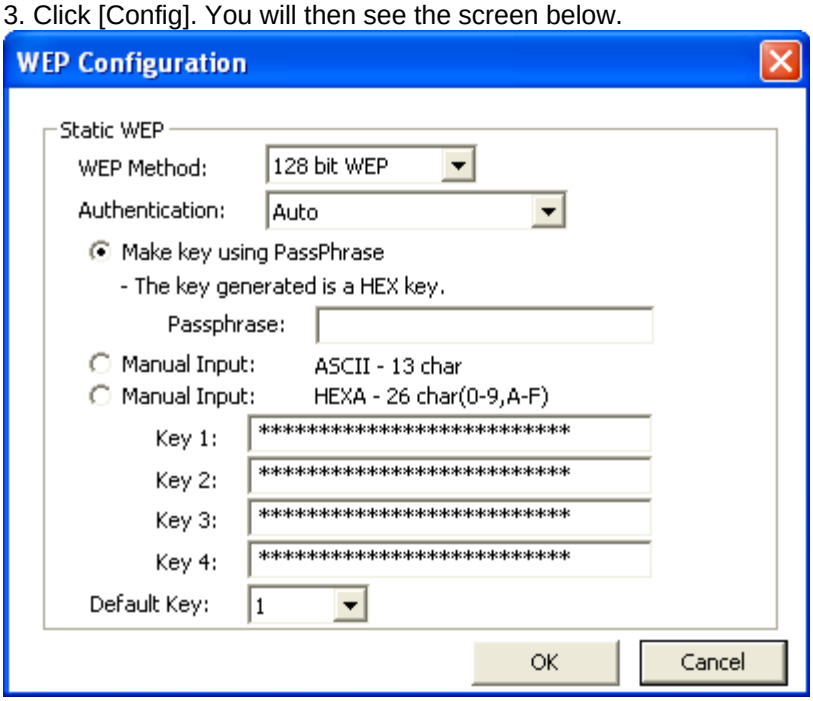
Configuring Security

You can configure your security settings at any time. Simply select the profile you wish to edit under the [Profile] tab, select [Properties] and then choose [WLAN Security]. You are also presented with the option to configure security during the profile creation process. Whether changing the security settings of an existing profile or creating a new profile, the steps to configure your security settings remain the same.

Configuring WEP


Example's property
Basic Setting
Advanced Settings
WLAN Security
Freqency Band
Chipset Features
TCP/IP
WLAN Security Configuration
Security mode:
No Encryption
Authentication protocol
None
Config
Encryption method
Using Static WEP
Config
Apply Now
Save
Cancel

1. Select [WEP] under [Security Mode]
2. Put a check mark next to [Using Static WEP]
3. Click [Config]. You will then see the screen below.



4. [WEP Method] Select the correct encryption level to match your access point. Either 64, 128, or 152-bit. The encryption level set her must match the encryption level used by your access point.

a. [Authentication] You can choose between Auto, Open System, and Shared. Please see section 2.5 for more information on the different types of authentication. For most installations choosing “Auto” is the best choice.
b. Enter the WEP key exactly as you did in your access point.

There are three ways of generating a WEP Key:

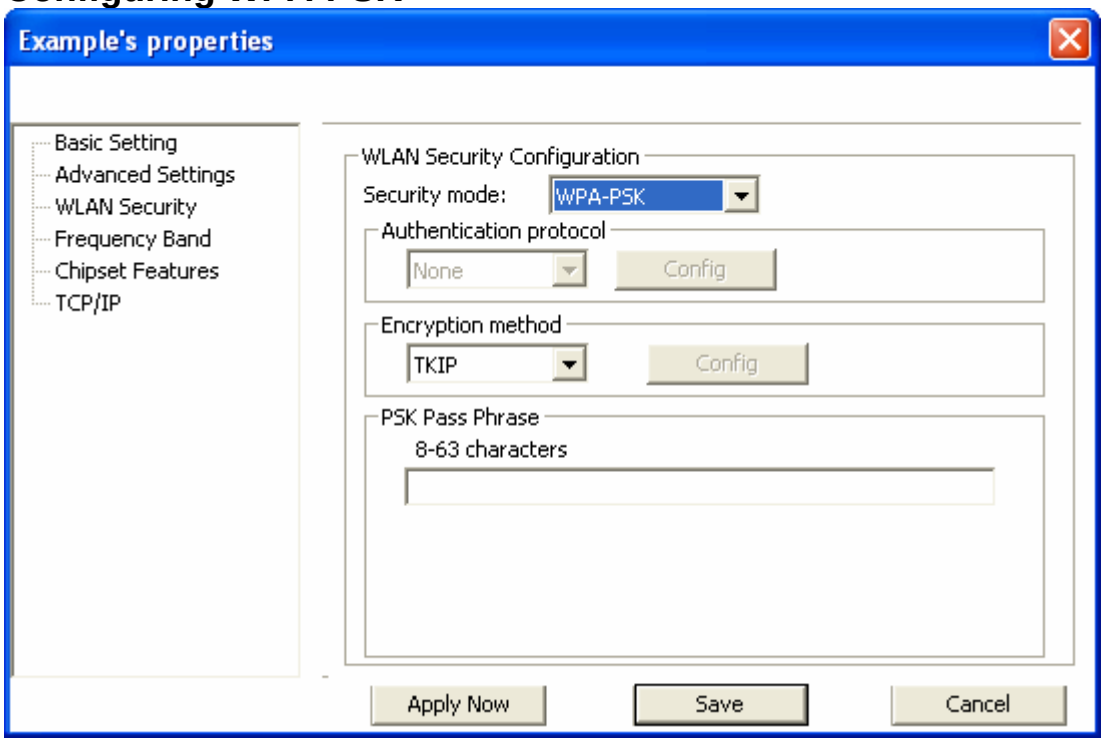
Make key using PassPhrase: a WEP Key is automatically generated as you type in any PassPhrase of your choice. Use this feature when you have used a PassPhrase to generate your WEP key on your access point.

Manual Input (ASCII): You generate your own WEP Key using ASCII characters (5 characters for 64-bit, 13 characters for 128-bit, 16 characters for 152-bit)

Manual Input (Hexadecimal): You generate your own WEP Key using hexadecimal characters (10 characters for 64-bit, 26 characters for 128-bit, 32 characters for 152-bit).

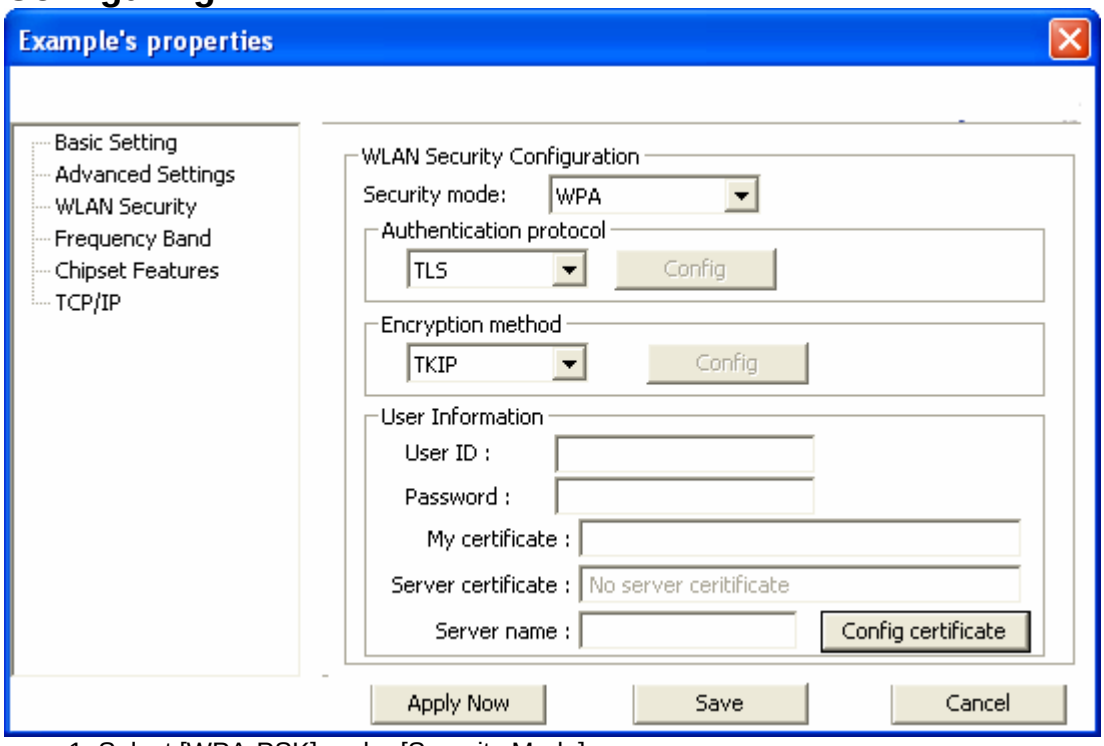
5. Click [OK] to save your settings and return to the previous screen.
6. If you want to use 802.1x authentication with WEP, you will need to configure your 802.1x settings. Please see section 4.5 for details on configuring 802.1x.

Configuring WPA-PSK



1. Select [WPA-PSK] under [Security Mode].
2. Select [Encryption method]. You can choose between TKIP or AES. Most access points use TKIP for WPA-PSK.
3. Under [PSK Pass Phrase] enter the same pass phrase used to configure WPA-PSK on your access point.

Configuring WPA



1. Select [WPA-PSK] under [Security Mode].
2. Select [Encryption method]. You can choose between TKIP or AES. Most access points use TKIP for WPA.
3. See section 4.5 for configuring 802.1x for WPA.

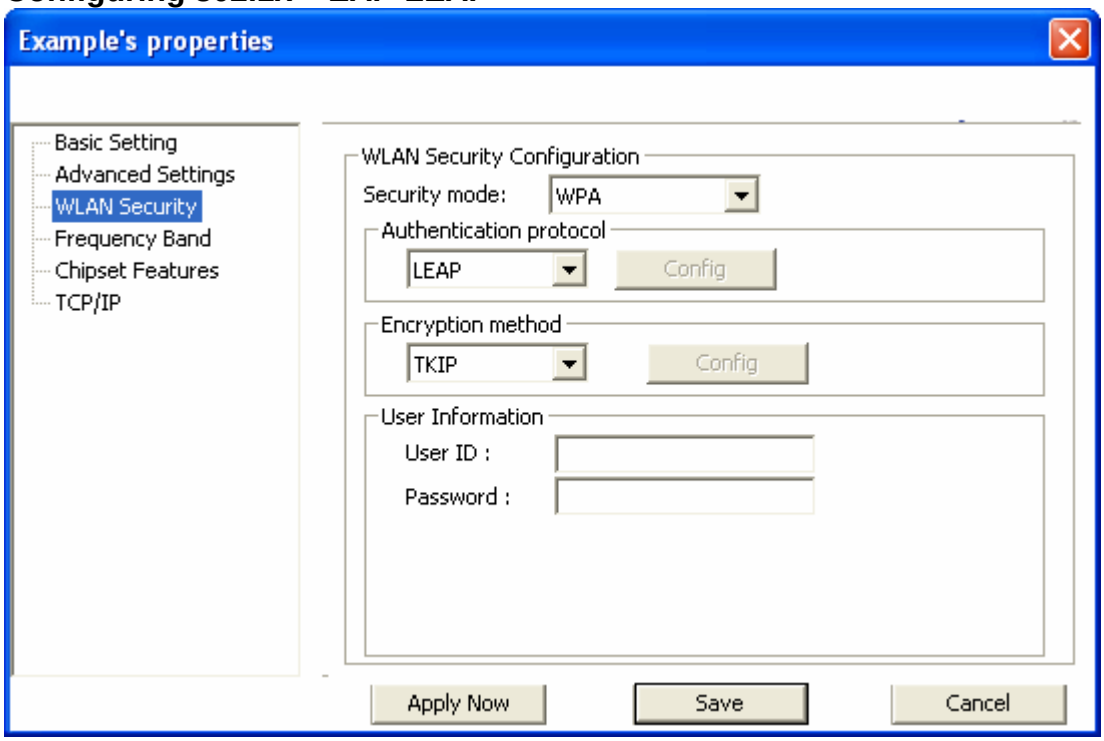
Configuring 802.1x

1. Choose the EAP method under [Authentication protocol].
2. Depending on the EAP method chosen the options under [User Information] will change.

Configuring 802.1x – EAP-MD5

1. EAP-MD5 is only a choice when use WEP. MD5 is not allowed for WPA.
2. Enter in unique User ID and Password under [User Information]

Configuring 802.1x – EAP-LEAP



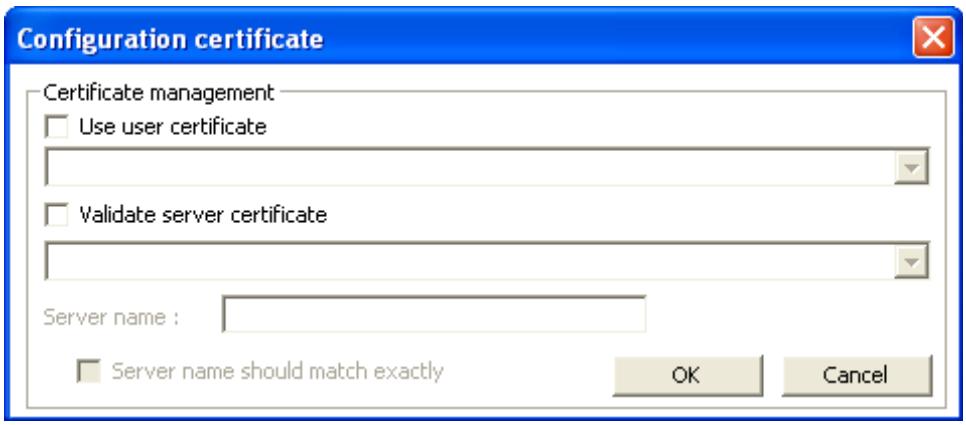
1. Enter in unique User ID and Password under [User Information]

Configuring 802.1x – EAP-PEAP

1. Click [Config] under [Authentication protocol]
2. Select inner PEAP protocol. You choices are [MS-CHAP v2] or [TLS].
3. Click [OK] to finish and return to the previous screen.
4. Enter in unique User ID and Password under [User Information].
5. If using a user6 or server certificate click [Config certificate]. The following window appears:

---

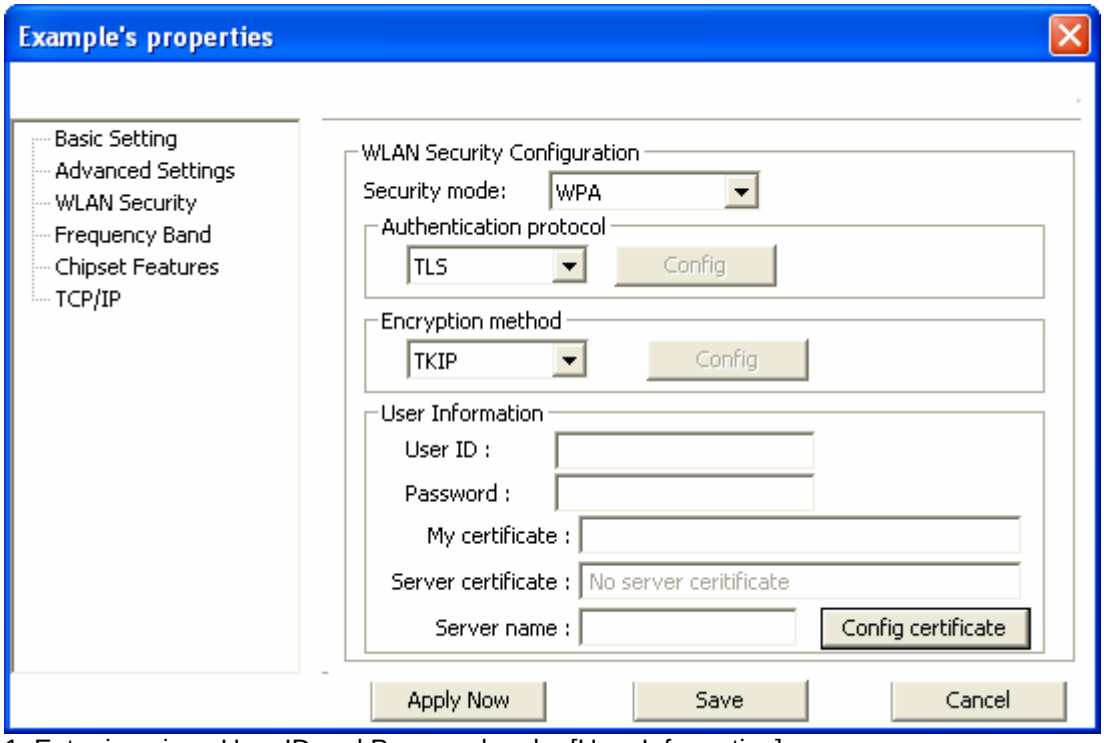
[6] You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.



[Use user certificate]: Put a check in the box to activate user certificate. Then select certificate from the pull down menu.
[Validate server certificate]: Put a check in the box to activate server certificate. Then select the certificate authority from the pull down menu.
[Server name]: Name of server used for 802.1x authentication.
[Server name should match exactly]: Check this box to force server name to match exactly the same in the certificate.

6. Click [OK] to finish and return to the previous screen.

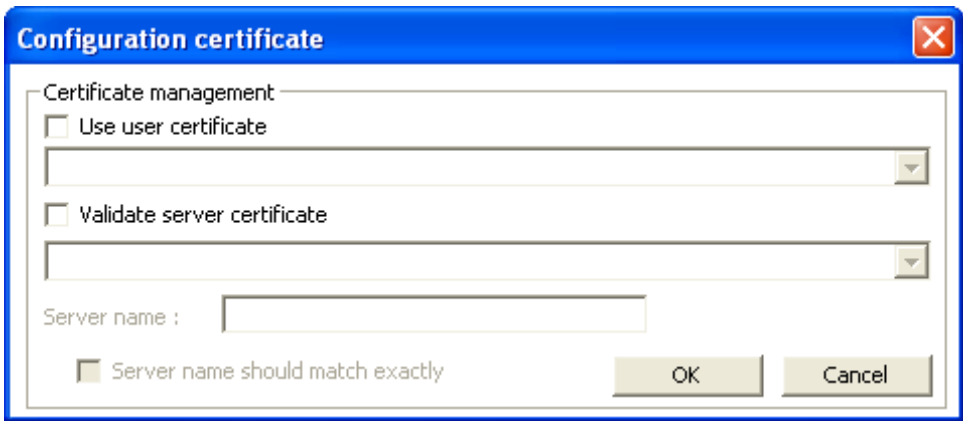
Configuring 802.1x – EAP-TLS



1. Enter in unique User ID and Password under [User Information].
2. TLS requires you to configure both a server and user7 certificate.
3. Click [Config certificate]. The following window appears:

---

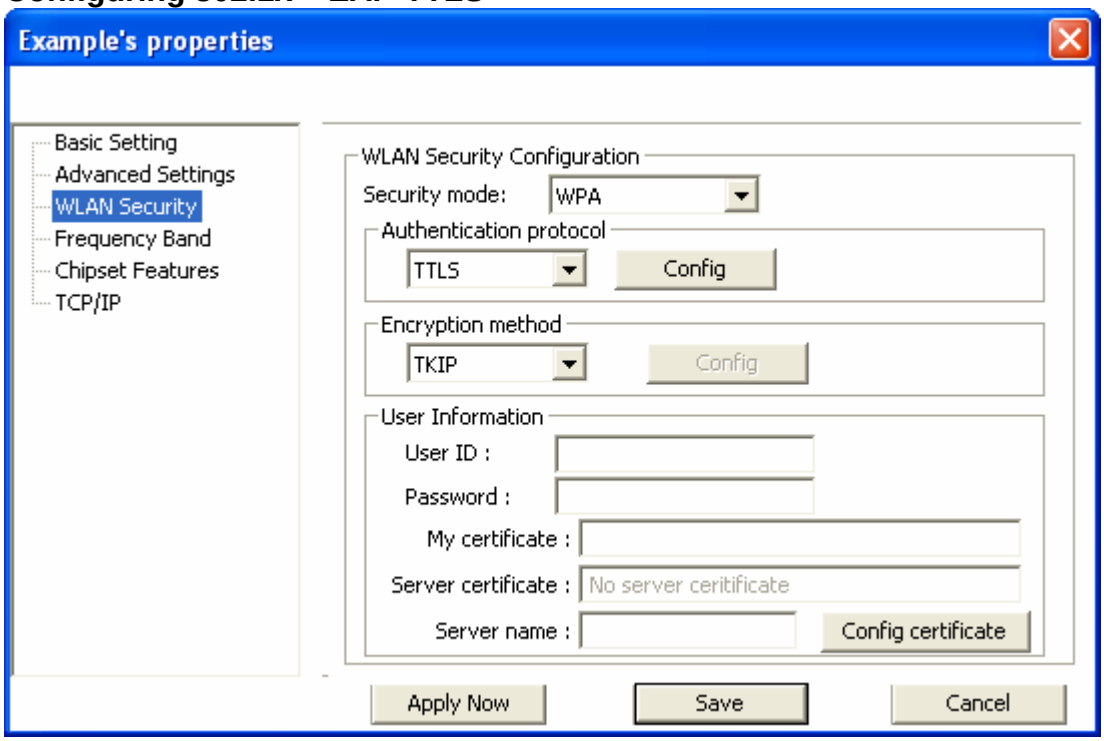
[7] You must first have a wired connection to a network and obtain the certificate(s) from a certificate authority (CA). Consult your network administrator for more information.



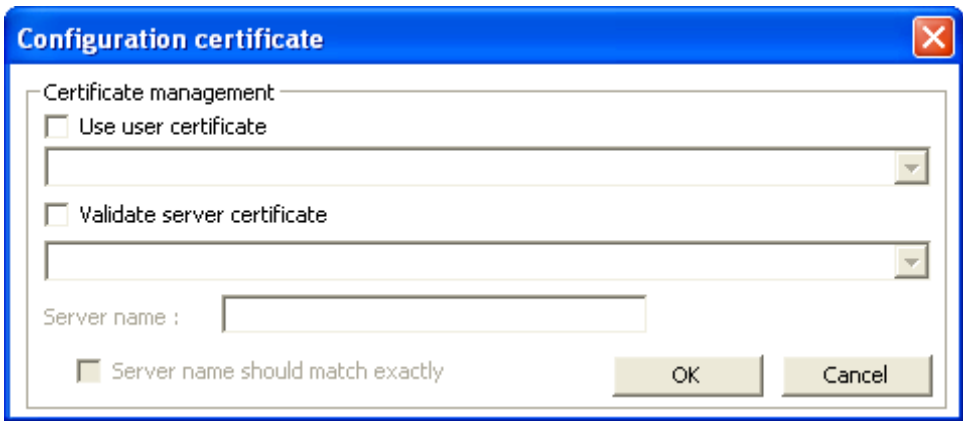
[Use user certificate]: Put a check in the box to activate user certificate. Then select certificate from the pull down menu.
[Validate server certificate]: Put a check in the box to activate server certificate. Then select the certificate authority from the pull down menu.
[Server name]: Name of server used for 802.1x authentication.
[Server name should match exactly]: Check this box to force server name to match exactly the name in the certificate.

4. Make selections and then click [OK] to finish and return to the previous screen.

Configuring 802.1x – EAP-TTLS



1. Enter in unique User ID and Password under [User Information].
2. Select inner TTLS protocol. You can choose between [PAP], [CHAP], [MS-CHAP], [MS-CHAPv2], or [MD5-Challenge].
3. Click [OK] to finish and return to the previous screen.
4. Click [Config certificate]. The following window appears:



[Use user certificate]: Put a check in the box to activate user certificate. Then select certificate from the pull down menu.
[Validate server certificate]: Put a check in the box to activate server certificate. Then select the certificate authority from the pull down menu.
[Server name]: Name of server used for 802.1x authentication.
[Server name should match exactly]: Check this box to force server name to match exactly the name in the certificate.

5. Make selections and then click [OK] to finish and return to the previous screen. Server certificate must be configured for TTLS to work.