TOKO
Wireless Network Adapter
User's Guide

Adapter type
TMW1059 :Cardbus

FCC Compliance

This device complies with Part 15 of the FCC Rules. Operation is subject to 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.

This equipment has been tested and found to comply with the limits for a Class B Personal Computer and Peripheral, 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 dose 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 or more 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 equipment has been tested to comply with the limits for a Class B personal computer and peripheral, pursuant to Subpart B of Part 15 of FCC Rules. Only peripherals (computer input/output devices, terminals, printers, etc.) certified (DoC) or verified to comply with Class B limits may be attached to this equipment. Operation with non-certified (DoC) or non-verified personal computer and/or peripherals is likely to result in Interference to radio and TV reception. The connection of a unshielded equipment interface cable to this Equipment will invalidate the FCC Certification of this device and may cause interference levels which Exceed the limits established by FCC for equipment.

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

For portable devices without co-location condition (eg. notebook pc)

FCC RF Radiation Exposure Statement:

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This device was tested and complies with FCC RF Exposure (SAR) limits in typical laptop computer configurations and this device can be used in desktop or laptop computers with side mounted PCMCIA slots which can provide 8 mm separation distance from the antenna to the body of the user or a nearby person. Thin laptop computers may need special attention to maintain antenna spacing while operating. This device cannot be used with handheld PDAs (personal digital assistants). Use in other configurations may not ensure compliance with FCC RF exposure guidelines.

Table of Contents

1. Introduction

TOKO Wireless Network Adapter offers performance comparable to Ethernet Local Area Network (LAN) system, without the limitations of network cables. It allows you to connect your computer to a Local Area Network from anywhere within the wireless coverage area. It also enables you to roam throughout the network while remaining connected to the LAN.

Package Contents

Make sure the following materials are available before beginning:

- TMWTMW1059 Release CD, or electronic equivalent
- Wireless Network Adapter TMW1059

System Requirements

- Laptop PC containing:
  TMW1059 32-bit CardBus slot (or Desktop PC with PC Card-PCI adapter)
  128 MB memory or greater
  300 MHz processor or higher
- Microsoft Windows 2000/Windows Millennium Edition/Windows 98 Second Edition/Windows XP

Specifications

- Absolute Maximum Ratings

  Supply Voltage. . . . . -0.3V to 3.6V (Max)

  Storage Temperature * 2 . . . . –10℃ to 60℃

  * 2 All temperature references refer to ambient conditions.

- Operating Conditions

  Temperature Range . . . . . 0℃ TA 55℃

  Supply Voltage Range . . . . . 3.0V to 3.6V

  Caution: These are the absolute maximum ratings for the PC Card product. Exceeding these limits could cause permanent damage to the card.

- Electrical Specifications

Test Conditions: Supply Voltage (V CC) = 3.3V, Ambient Temperature (TA) = 25℃,Unless Otherwise Specified

PARAMETER	TEST CONDITIONS	MIN	TYP	MAX	UNITS
MECHANICAL	PCMCIA Type II Cardbus,with Antenna Extension				
CURRENT CONSUMPTION					
Continuous Transmit 11g Mode		–	570	615	mA
Continuous Transmit 11b Mode		–	500	550	mA
Continuous Receive 11g Mode		–	365	320	mA
Continuous Receive 11b Mode		–	300	320	mA
Cardbus LOGIC LEVELS					
Input HIGH Voltage		0.7Vcc	–	Vcc+0.2	V
Input LOW Voltage		0	–	Vcc/3	V
Output HIGH Voltage	Sourcing 1mA	Vcc-0.2	–	Vcc	V
Output LOW Voltage	Sinking 2mA	0	–	0.2	V
Input Leakage Current		-10	–	10	μA
Cardbus LOADING CAPACITANCE					
Input Capacitance		–	–	15	pF
Output Capacitance		–	–	15	pF
RF SYSTEM SPECIFICATIONS					
Center Frequency Range		2412	–	2462	MHz
IF Frequency		1740	–	1800	MHz
Antenna Gain		–	0	2.14	dBi
Transmitter Power Output 11g Mode		–	+15	–	dBm
Transmitter Power Output 11b Mode		–	+17	–	dBm
EIRP 11g Mode		–	+15	–	dBm
EIRP 11b Mode		–	+17	–	dBm
Receive Sensitivity	54Mbps, 10% PER	–	-68	–	dBm
	11Mbps, 8% PER	–	-85	–	dBm
Data Rate (Physical Layer) 11g Mode		–	6,12,18,24,36,48,54	–	Mbps
Data Rate (Physical Layer) 11b Mode		–	1, 2, 5.5,11	–	Mbps

2. Windows XP

This chapter describes the Windows XP driver installation.

Driver Installation (First Time Install)

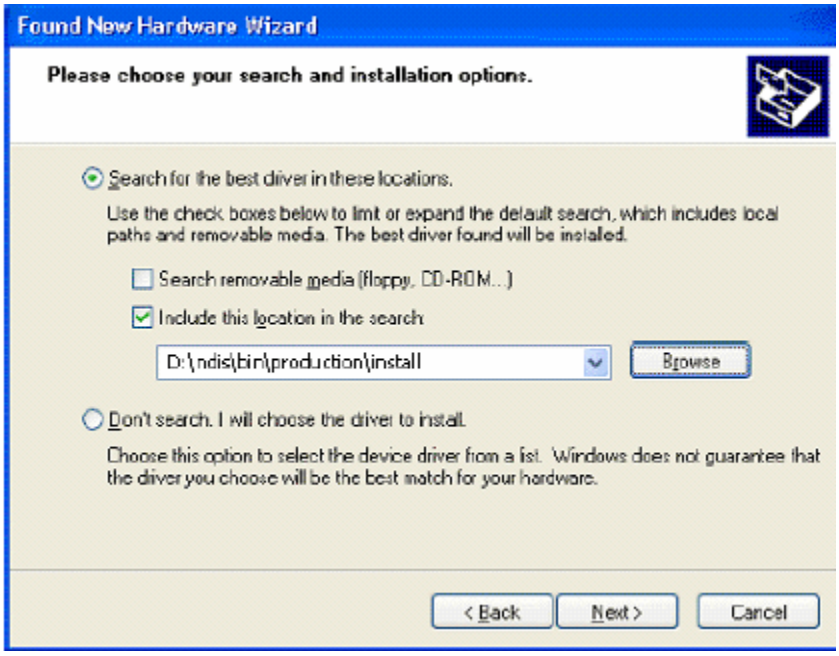
This section describes the first-time installation for the driver for Windows XP. For a previously installed driver, TOKO provides the InstallShield Wizard, which includes an application for upgrading the present driver and the Client Utility.

To install the NDIS Driver (first-time installation):

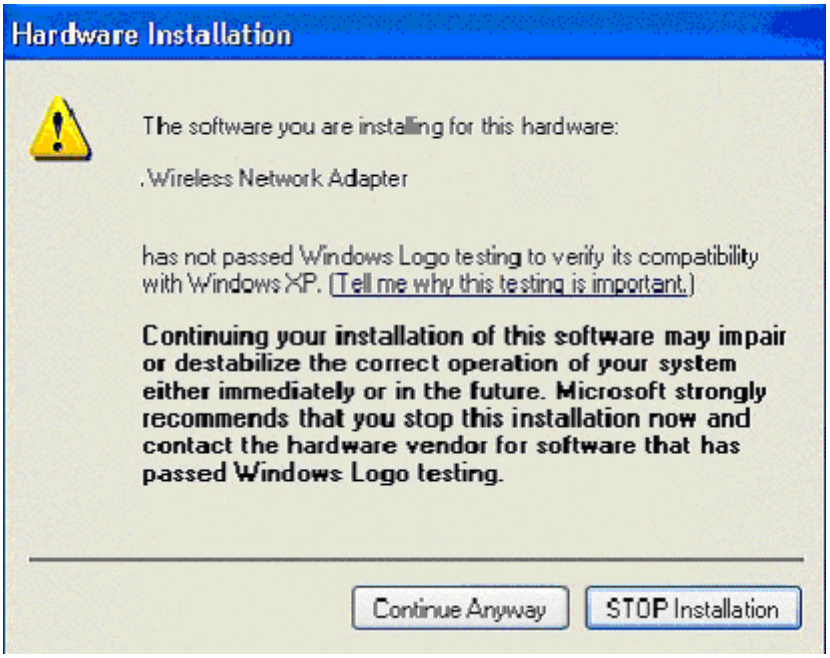
Insert the TOKO Wireless Network Adapter into a 32-bit CardBus slot(or miniPCI) and follow these steps to install the NDIS driver:

1. Wait for the Found New Hardware Wizard dialog box to appear. Choose "Install from a list or specific location (Advanced)," and click Next to continue.

2. Under "Search for the best driver in these locations," choose "Include this location in the search" and click Browse to find the location of the NDIS driver. When the location has been identified, click Next to continue.



3. The TOKO NDIS driver currently does not have a digital signature from Microsoft. Therefore, Windows XP shows a warning message. Click Continue Anyway to proceed with driver installation.



4. Click Finish to complete driver installation, and refer to 11 for device configuration.

Client Utility Installation and Driver Update

TOKO provides an InstallShield utility to upgrade the NDIS driver, if a previous release is installed, and to install the Client Utility.

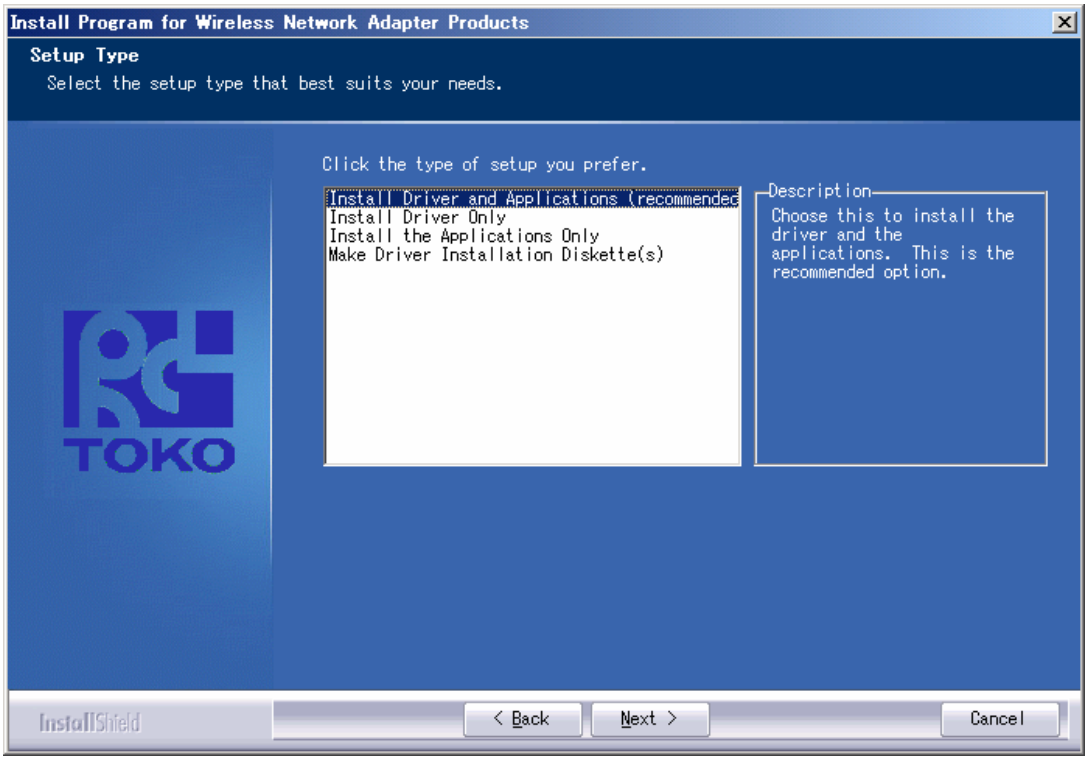
To install the Client Utility and upgrade the NDIS driver:

When an TOKO NDIS driver has been previously installed, insert the TOKO Wireless Network Adapter into a 32-bit CardBus slot(or miniPCI slot). Follow these steps to update the NDIS driver:

1. Open the InstallShield Wizard (**setup.exe**).
2. Click Next to continue.

3. Click Yes to accept the License Agreement.

   The Update Program Setup Type dialog will display.



4. The Setup Type page provides selections as summarized in Table 1-1.Choose the selection appropriate for your network.

Table 1-1. Setup Type Page Selections

Selection	Description
Install Driver and Client Utility	Recommended. Updates drivers and installs the Client Utility.
Install Driver Only	Installs TOKO NDIS driver only.
Install Application Only.	Installs Client Utility only.
Make Driver Installation Diskette(s)	Creates Client Utility installation diskettes.

5. Click Next to continue.
6. Choose the destination location. Click Next to continue.
7. Specify the program folder to store start icons.
8. Use the checkbox to enable the Client Utility tray icon and start the Client Utility when restarting the system. The tray icon will appear in the Windows System Tray.
9. If a previous release of the Client Utility is installed, make sure it is not currently running. Click Next to continue.

   If you are running a previous version of the Client Utility, a dialog box will appear requesting an exit from the program. Click OK and continue.

10. The TOKO NDIS evaluation driver currently does not have a digital signature from Microsoft, so Windows XP may show a warning message. Click Yes to proceed with driver installation.
1. Click Finish when the InstallShield Wizard is complete.

Driver and Client Utility Uninstallation

This section provides information about uninstallation procedures for TOKO software releases.

To uninstall the Client Utility and the NDIS driver:

Use the InstallShield Updater to uninstall the NDIS driver and Client Utility application and remove them from the Device Manager.

1. Open the InstallShield Wizard (setup.exe).
2. Click Next to continue.
3. Click Yes to accept the License Agreement.
4. On the Setup Type page, choose Uninstall Driver and Applications to uninstall drivers and Client Utility.

   Click Next to continue.

5. Click Finish when the InstallShield Wizard is complete.

Some files are left on the system to ease reinstallation. Use the following instructions to completely remove these files.

1. Go to the Start menu and choose Search For Files or Folders...
2. Enter oem*.inf in the “Search for files or folders named “field”, and enter TOKO in the “Containing text:” field.
3. Click Search Now.

A few files matching these criteria are possible, if previous drivers have not been removed properly.

4. Choose the files that have been found and delete them from the system.
5. To complete the uninstallation, remove the file ar5211.sys from the \WINNT\system32\drivers folder.

Device Configuration

Use the Client Utility to configure the device driver. The Client Utility provides extensive online help to aid in configuring the device.

the Client Utility by clicking the Start button and choosing Programs > Toko > Client Utility. The Client Utility tray icon is displayed in the right side of the Toolbar. Launch the Client Utility by double-clicking the tray icon, or by right-clicking the tray icon and selecting Launch Station Utility.

Windows XP Wireless Network Configuration

Windows XP provides Zero Configuration functionality that automatically tries to connect the STA to available wireless networks. This section explains how to set up and manage security configurations using both the Client Utility and Windows XP Zero Configuration.

For complete information on Zero Configuration, visit the following Microsoft web site:
http://www.microsoft.com/technet/prodtechnol/winxppro/reskit/prdc_mcc_kqmu.asp

Client Utility Security

The Client Utility allows connection profiles of:

- No security
  Link encryption/decryption is disabled, no keys are installed.

- Static key security
  Keys are installed at driver initialization and profile change events. All Atheros-supported encryption protocols are supported and the chosen keys can be 40-, 104-, or 128-bits.

- Dynamic key security
  Pre-configured keys will be installed, but the expectation is that protocols running outside the context of the Client Utility will be providing link security.

The LEAP protocol is also available, and is enabled by choosing Dynamic Security followed by LEAP username/password configuration. Note that LEAP is limited to 40-bit and 104-bit keys and it uses the WEP algorithm only.

Zero Configuration Security

The Windows XP Wireless Zero Configuration Service (WZCS) is an NT service that manages the wireless connection in a largely dynamic way. For infrastructure networks, the user must identify and minimally configure connection information. After this the service automatically switches to the active AP listed at the top of the Preferred Networks list.

Some of the details that must be provided to WZCS pertain to security:

- Key value, key length, and default key index
- Whether WZCS should allow keys to be provided from outside its context (that is, either from the Client Utility or from key distribution protocols like 802.1x)

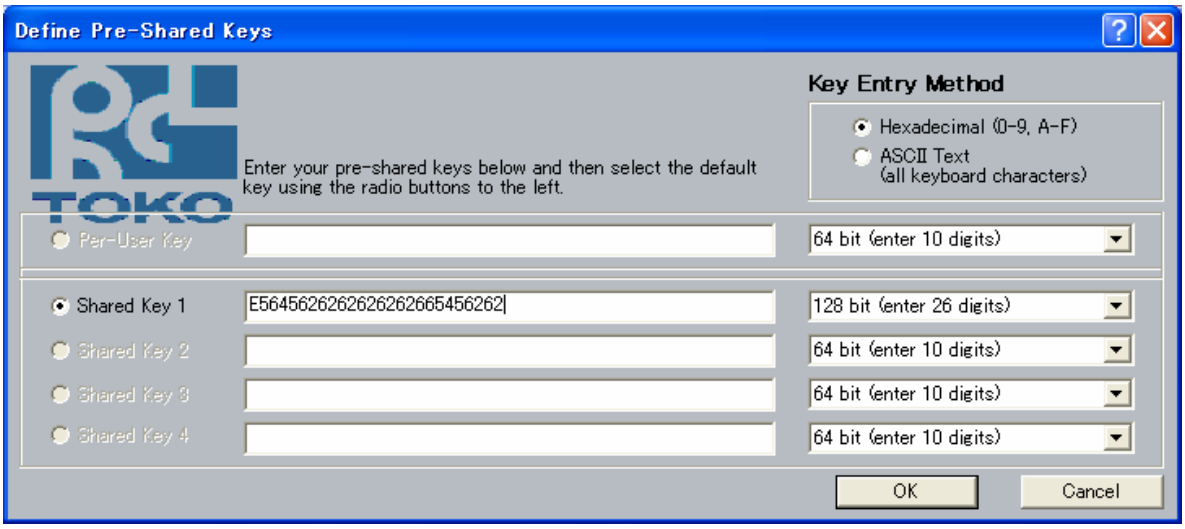
Interactions

Although it would appear that WZCS is the only service which actively manages the wireless connection, there are actually a number of details that should be understood to provide the proper configuration information. In general, if WZCS is active, it will override many of the security settings in the Client Utility .

First, LEAP and WZCS are basically incompatible. That is, when attempting to connect to an AP which is using LEAP, disable WZCS entirely. Without doing so, the WZCS will continually ask for status from the driver and may succeed in disabling the connection altogether.

The use of shared key authentication is not recommended since it actually lowers the level of security for the wireless network. Still, many networks require it, so the Client Utility allows the user to configure static keys even though the Dynamic Security option is chosen. When using the Microsoft 802.1x supplicant with operating systems other than Windows XP,

it is necessary to enter at least one key into the Client Utility static key configuration. For these other operating systems, there is no WZCS dynamically managing the connection, and therefore there is no entity to initialize the security settings. This must be performed by the Client Utility. Enter a dummy key into the Client Utility profile for this connection.



Because LEAP is implemented in the context of the wireless driver instead of in a distinct context like the 802.1x supplicant, it never needs the WZCS to provide it with dummy keys.

Sample Configuration

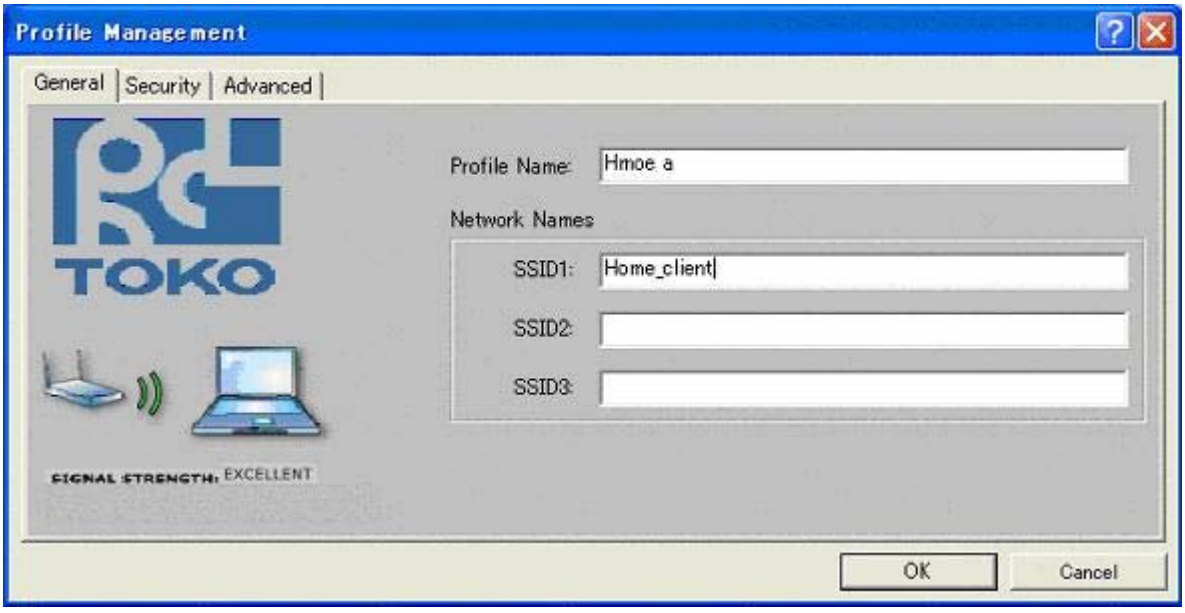
This section provides a sample configuration for WZCS configuration with Windows XP. This example configuration consists of three APs:

- AP-Static
  Static keys must be used with this network.
- AP-802.1x
  Provides keys through 802.1x; MAC-layer authentication is used.
- AP-LEAP
  Provides keys through the LEAP protocol.

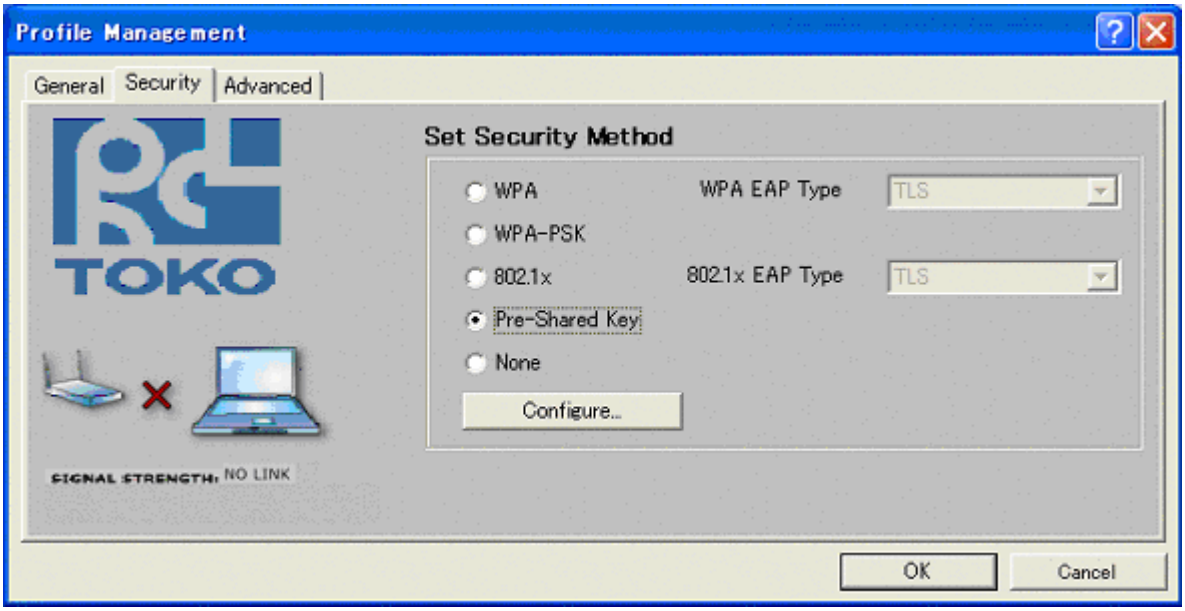
WZCS can be used to dynamically change the keys for the AP-Static and AP-802.1x networks, however WZCS cannot be used with AP-LEAP network.

Take the following steps to configure the Client Utility to use WZCS:

1. In the Client Utility's General Configuration tab, setup a new profile that supports dynamic keys, however program static keys corresponding to the requirements of the AP-Static network.

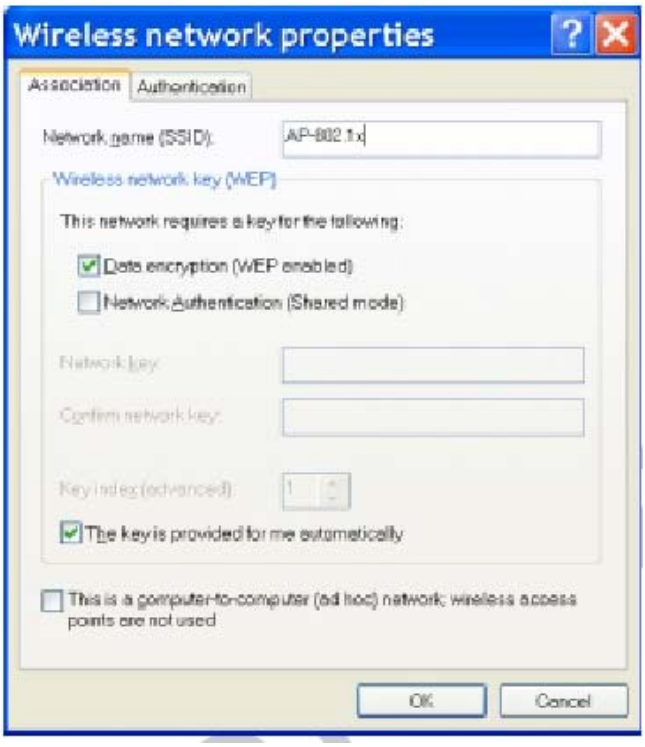


2. Under the Security tab, select the Encryption Type radio button to choose Use Dynamic Security.



3. Click on Define Static Encryption Keys and enter the keys for the APStatic network.
4. Choose Start->Network Connections to open the Network Connections panel.
5. Right click on the entry for the wireless device and choose View Available Wireless Networks.
6. Choose Advanced in the next dialog.
7. In the next panel, use the checkbox to select Use Windows to Configure My Wireless Networks Settings.
8. Setup the AP-802.1x network in the Wireless Network Properties dialog by pressing Configure.

9. Enter the security information for the network.



10. Select the Authentication tab.

11. Enter the remaining 802.1x configuration as required by the particular authentication services on the network.

12. Click OK to close the Authentication panel and go back to the WZCS profile management panel.

If the newly configured network is not at the top of the Preferred Networks list, then press the Move Up button until it is. Then click OK to close the panel.

13. Repeat the above procedures for the AP-Static network, but disable the settings related to 802.1x.
14. Click OK to close the WZCS panel.
15. Configure the AP-LEAP network with a completely separate Client Utility profile. To use this network, select that profile as well as disable WZCS as previously discussed.

WZCS connects to the active network listed in the highest position in the Preferred Networks list. For both the AP-Static and the AP-802.1x networks, the Client Utility-provided static keys are installed. In the AP-Static network, these provide the required keys. In the AP-802.1x network, they are installed and serve only to initialize the security data structures. After association, the 802.1x key distribution protocol provides the real key material.