



Wireless-B/G USB Adapter SWM9001

User Manual

Copyright

SCI is a registered trademark of **SCI** Incorporated.

Copyright © 2012 **SCI** Incorporated. All rights reserved.

No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

SCI Incorporated reserves the right to make changes in technical and product specifications without provisional notification.



This module is limited to OEM installation only and must not be sold to end-users.

OEM integrators must be instructed to ensure that the end-user has no manual instructions to remove or install the device.

The end-user can not remove or install this module to any other devices.



Contents

1. About This Manual	4
1.1 Software Installation	4
1.2 Hardware Installation	8
1.3 Uninstallation	8
2. Network Connections and Wireless Security	8
2.1 Viewing Wireless Networks in Your Area.....	8
2.2 Joining a Network	9
2.3 Profile Manager	10
3.About Your Smart Wizard.....	20
3.1 Diagnosis.....	20
3.2 Adapter Information	21
3.3 Advanced Statistics Page	21
3.4 card log.....	22
3.5 Operation of the task bar	23
4. Standards and Regulatory Compliance.....	24
4.1 Standards and certification	24
4.2 FCC certification requirements.	24
4.3 FCC RF exposure requirements.....	27



1. About This Manual

This Manual describes how to install, configure the Wireless-B/G USB Adapter SWM9001.

1.1 Software Installation

Install the Device

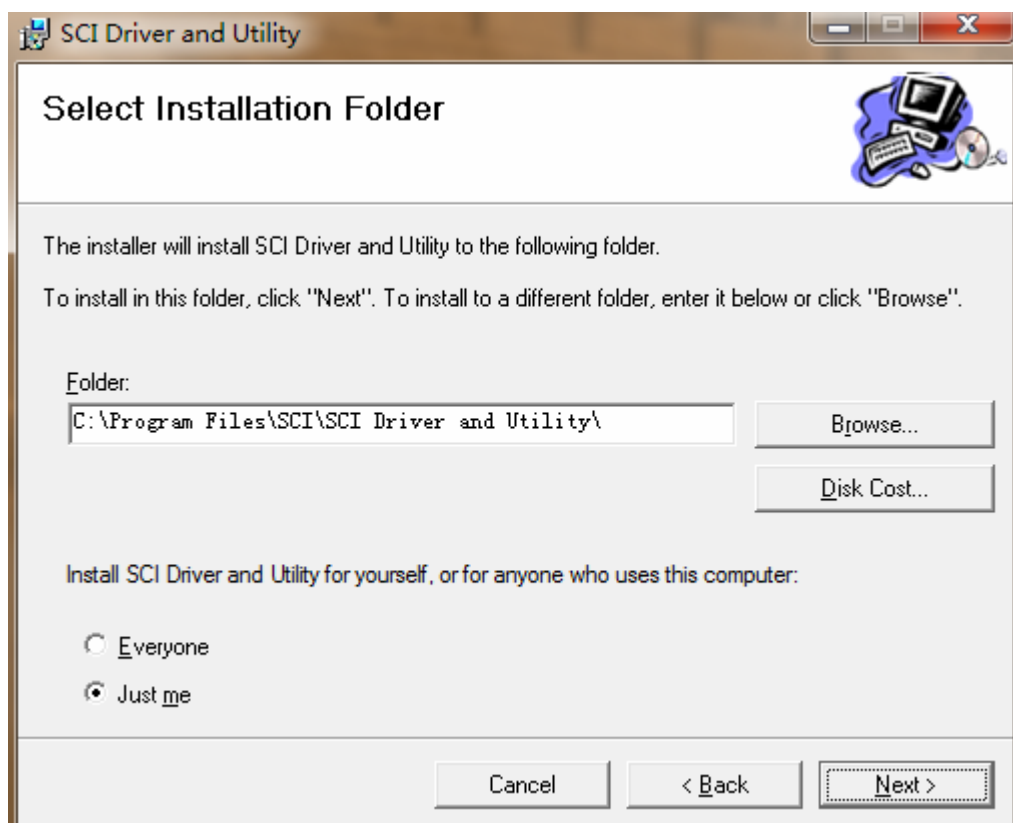
1. Make sure the Computer is turned off. Remove the expansion slot cover from the computer.
2. Carefully slide the 802.11 b/g dongle into the slot. Push evenly and slowly and ensure it is properly seated.
3. After device has been connected to you computer, turn on your computer. Windows will detect the new hardware and then automatically copy all the files needed for networking.

2.2 Install the Driver & Utility

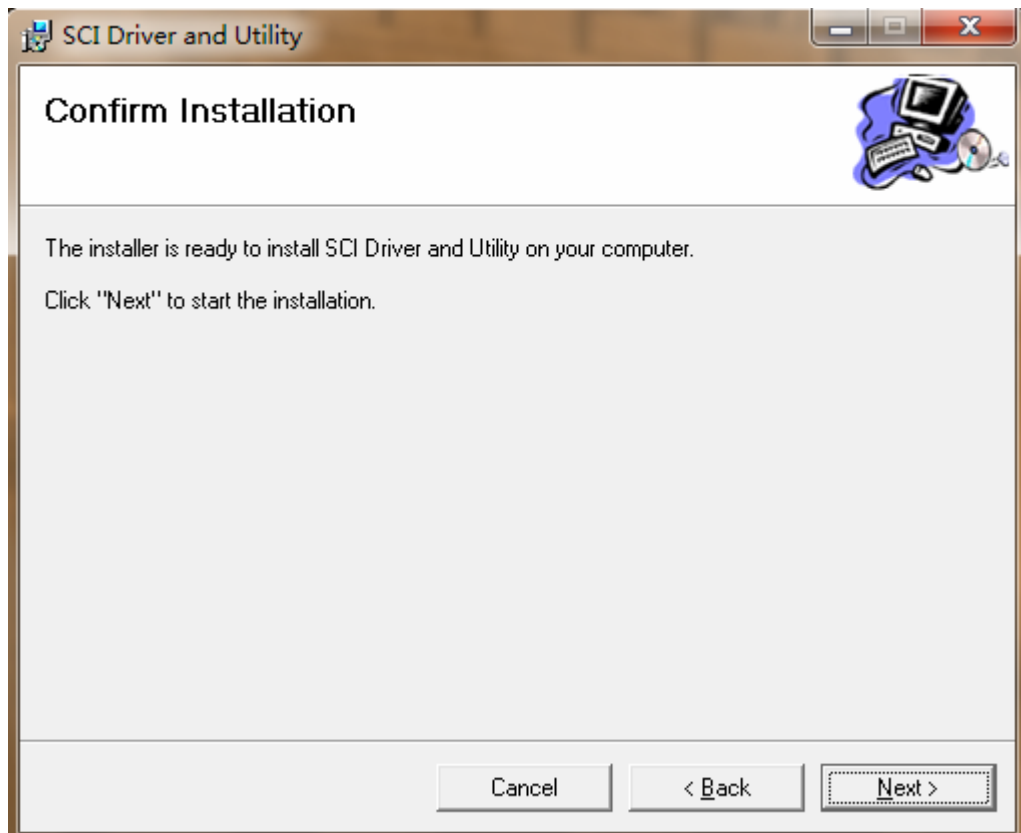
1. Insert the SCI CD. If the Welcome page does not open, double click Autorun.exe on the CD.
2. The welcome screen appears, then click “Next” to continue.



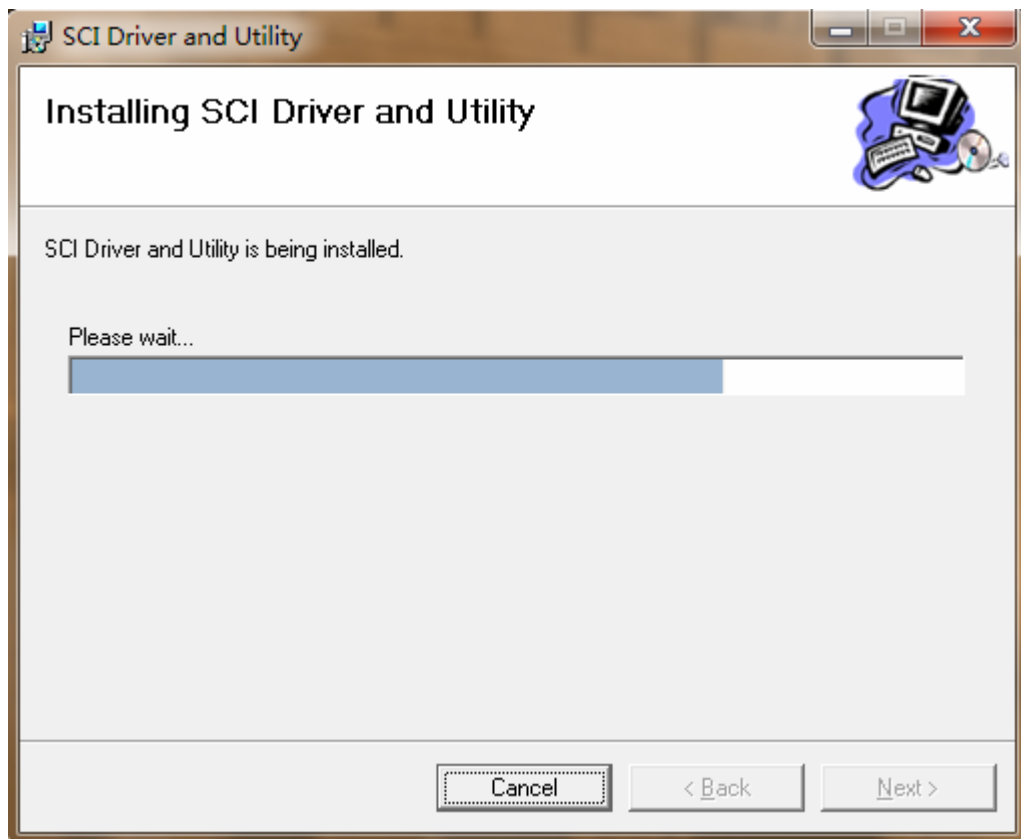
3. Select installation folder. If the folder is in the default path, click "Next".
Otherwise click "Browse" to choose the path of folder that you need.



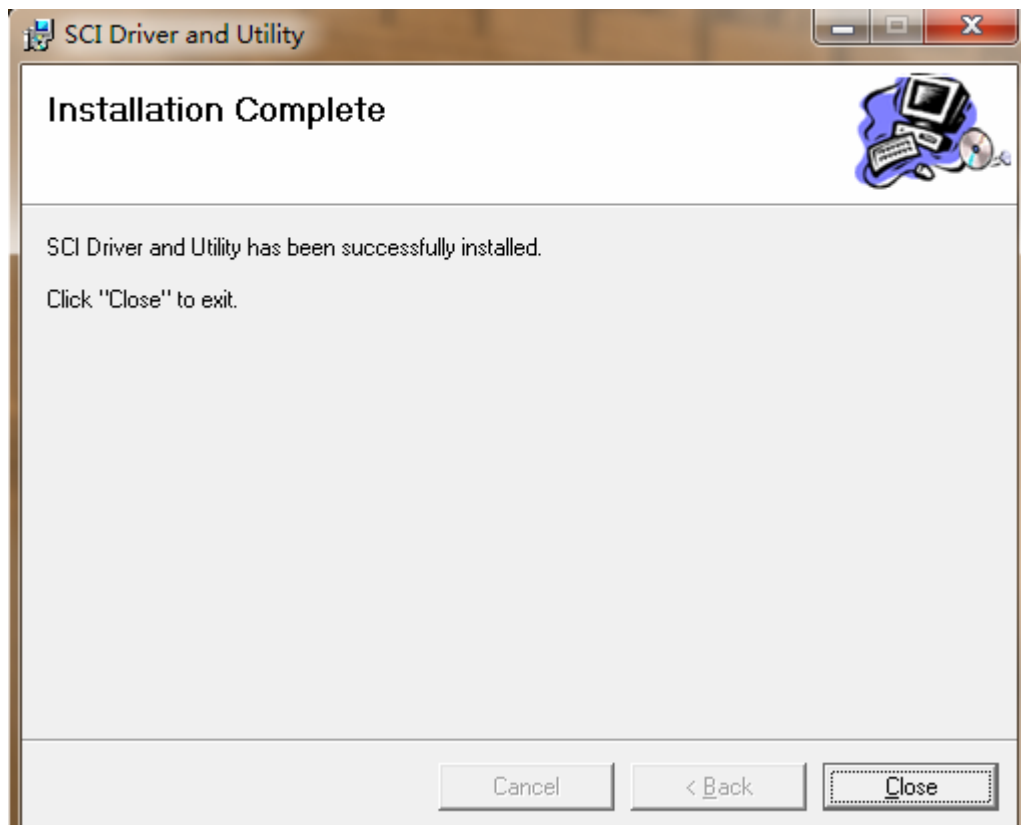
4. When you are prompted the following message, please click the “Next” to start the installation.



5. The installing SCI Driver & Utility window will open.



6. When the following screen appears, click "Close" to complete the software installation.





1.2 Hardware Installation

To verify if the device exists in your computer and is enabled, go to Start->Control Panel->System (Hardware)->Device Manager. Expand the network Adapters category. If the SWM9001 USB dongle is listed here, it means that your device is properly installed and enabled.

1.3 Uninstallation

You can remove the wireless adapter software in these two ways:











- Navigate the Windows Start menu to the SWM9001 USB 2.0 Adapter program group, select the uninstall option, and follow the screen prompts.
- Navigate the Windows Start menu to the Control Panel Add or Remove Program item, select the SWM9001 USB 2.0 Adapter option, and follow the screen prompts.

2. Network Connections and Wireless Security

This chapter explains how to use the Smart Wizard to connect to wireless networks and how to set up wireless security on your adapter if you are joining a secured wireless network.

2.1 Viewing Wireless Networks in Your Area

You can use the profile manager tab to view all available wireless networks in your area. Click the Scan tab to display the following screen. The screen shows the following information for each network scanned: Network Name (SSID), MAC Address, Mode, Security, Signal and Channel.

Network Name (SS...)	MAC Address	Network Type	Authentication	Encryption	Signal Str...	Chan...
 D-Link_DIR-600T	1c:bd:b9:f3:43:1b	Infrastructure	WPA2-Personal	AES	62%	1
 dlink123	00:26:5a:b0:53:76	Infrastructure	WPA2-Personal	AES	86%	6
 FAST_54M_8	54:e6:fc:7e:24:02	Infrastructure	Open	None	64%	1
 maxnet_ap1	00:24:b2:68:5e:80	Infrastructure	WPA2-Personal	AES	52%	1
 NWP-WLAN-8FA	e0:91:f5:03:c1:9d	Infrastructure	Open	WEP	69%	1
 NWP-WLAN-9FL	e0:91:f5:03:c3:fb	Infrastructure	Open	WEP	52%	6
 SEMI	f0:7d:68:91:e7:b6	Infrastructure	WPA2-Personal	AES	55%	11
 shcsz1	00:fd:07:a6:d9:a8	Infrastructure	WPA-Personal	TKIP	55%	3
 ufidawireless	00:13:46:de:83:67	Infrastructure	Open	WEP	52%	6
 wlan-g	00:14:a5:30:9c:6f	Infrastructure	Open	None	67%	1

Activate (A) Refresh OK



The access point supports WPS.



The access point supports WPA-Pi.



Identifies whether the wireless network uses security settings such as WPA2-PSK, WPA-PSK, or WEP.

2.2 Joining a Network

After installation you can use the **Scan** button on the profile manager tab to view available networks and select the one that you want and then click Active tab to join the network.

How you join the network depends on whether it uses wireless security, and whether it supports WPS.

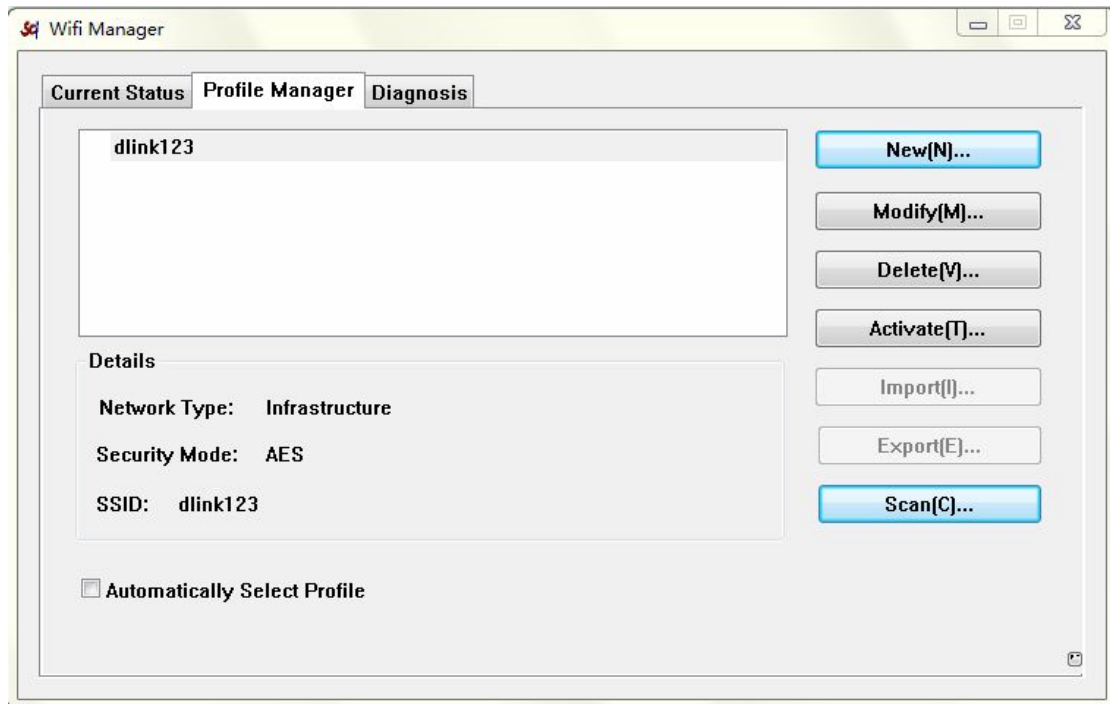
(1)Open network: This network does not use any wireless security. Select the network and click Active tab.

(2)Secured network: To join a secured wireless network, select it and click Active tab. You are prompted to enter the pass phrase or key.

(3)Secured network with WPS: The network uses wireless security and supports WPS.

2.3 Profile Manager

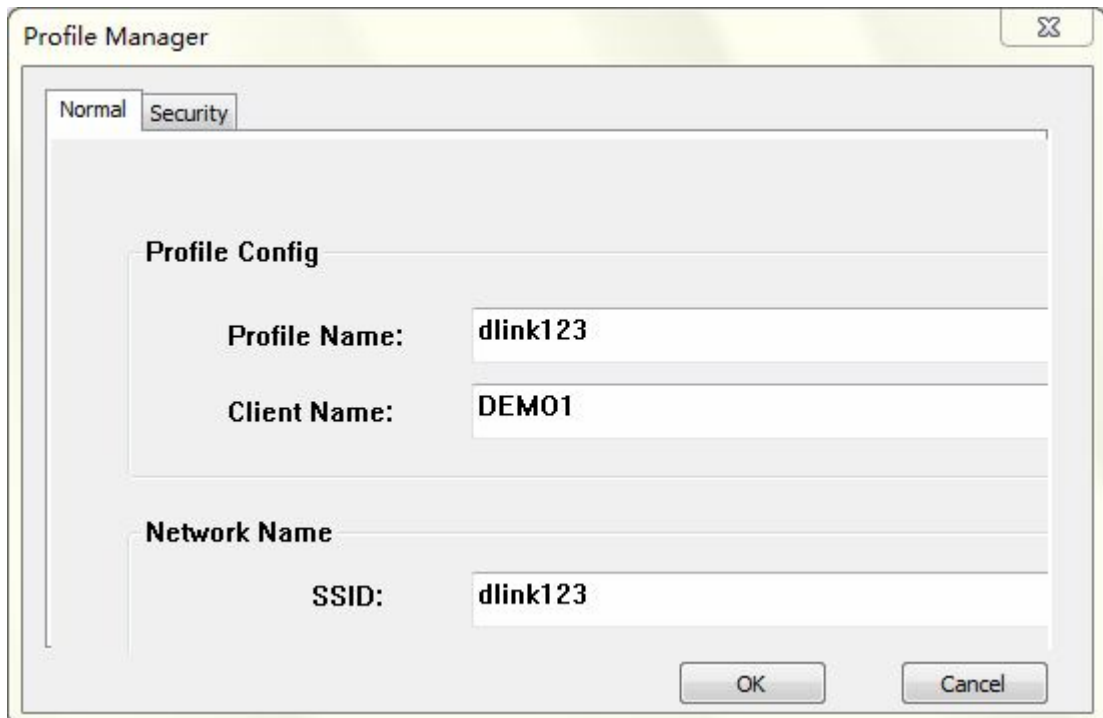
Profile can book keeping your favorite wireless setting among your home, office, and other public hot-spot. You may save multiple profiles, and activate the correct one at you preference. The Profile Manager enables you to New, Modify, Delete, Activate Import and export Profiles.



There are two special profile names: Default Settings and Security settings

(1) Default Settings

The profile named Default automatically scans for any wireless network. You cannot change this profile name.

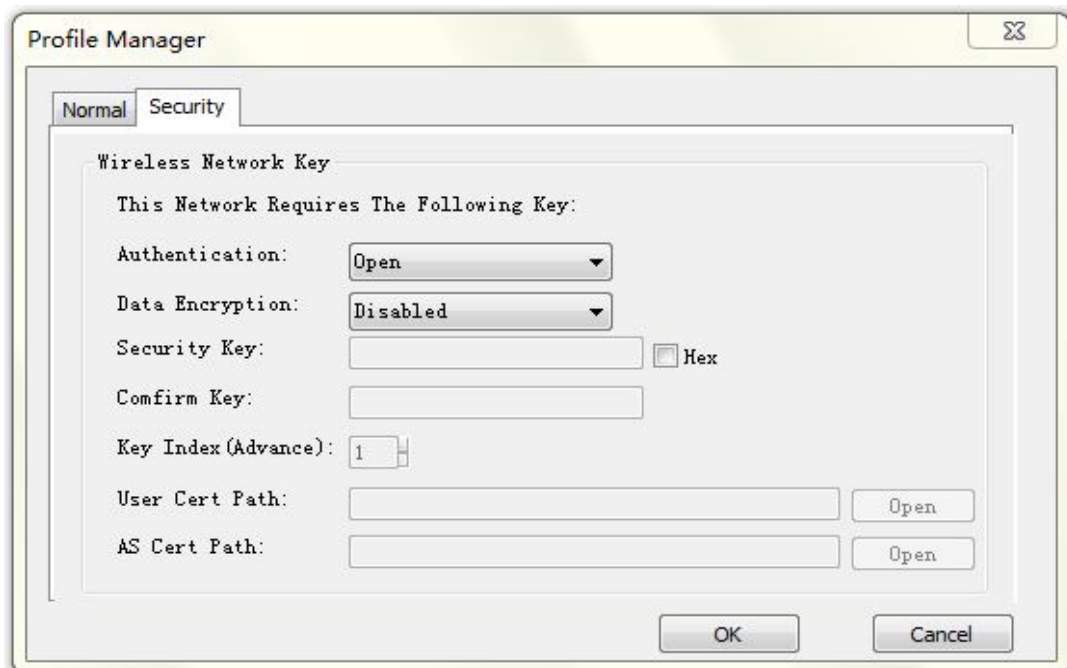


Normal Tab:

Profile Config	Profile Name	This name is unique with the same name as the network.
	Client Name	The name of the client computer.
Network Name	802.11 wireless network's name.	

(2) Security settings

Security page displays key information, according to the different encryption method to choose a different configuration.



Security Tab:

Authentication	Authentication mode used within the network, including Unknown, WPA-PSK, WPA2-PSK, WPA and WPA2
Encryption	Identifies whether the wireless network uses security settings such as WEP, WPA2-PSK, or WPA-PSK.
Network Key	If WEP Authentication is Used, For 64-bit WEP, enter 10 hex digits (any combination of 0-9 or a-f). For 128-bit WEP, enter 26 hex digits. If WPA2-PSK or WPA-PSK Authentication is Used, Encryption key size must be 128-bit or 256-bit.
Confirm Network Key	The same as the network key you enter.
Key Index	Match with the group key
User Cert Path	Select the user certificate path

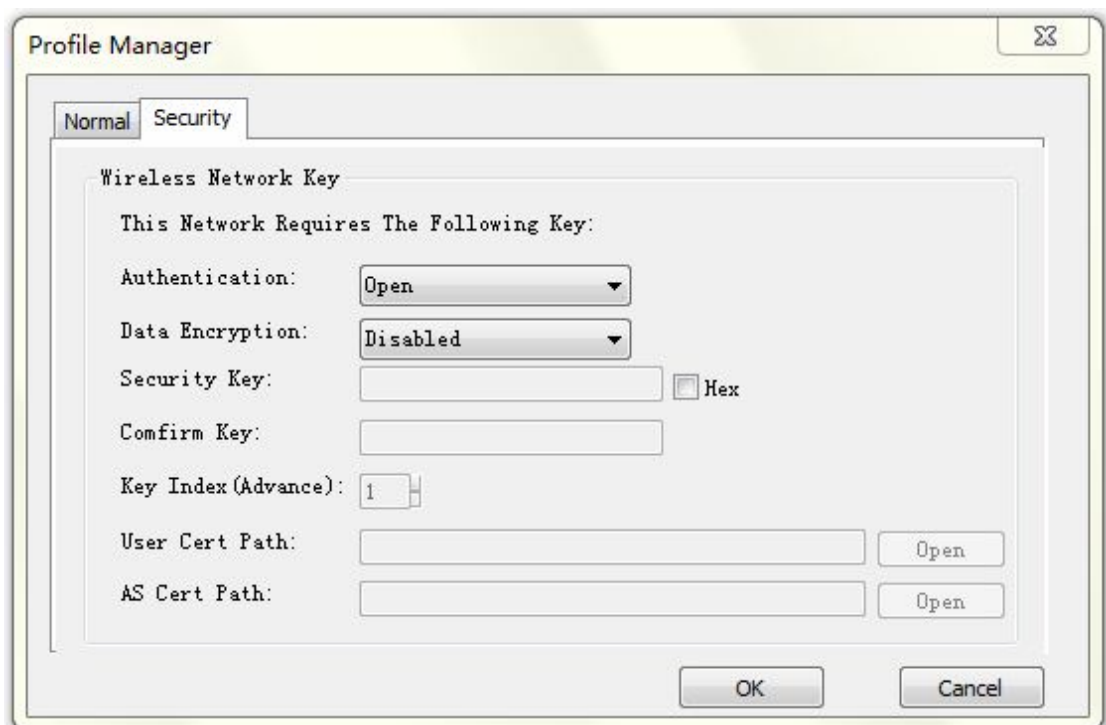
As Cert Path	Select the AS certificate path
---------------------	--------------------------------

Security page shows following config mode:

- **Wireless Security: Open**

Data Encryption: Disabled

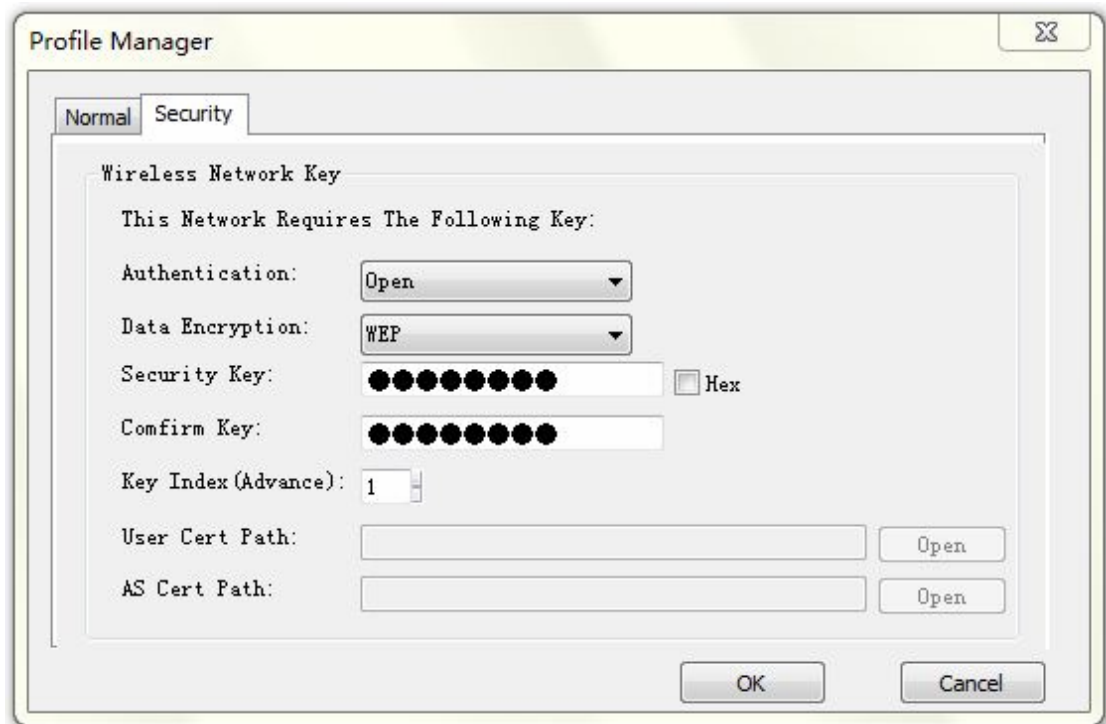
This network does not use any wireless security. Select the network and click Active tab.



- **Wireless Security: Open**

Data Encryption: WEP

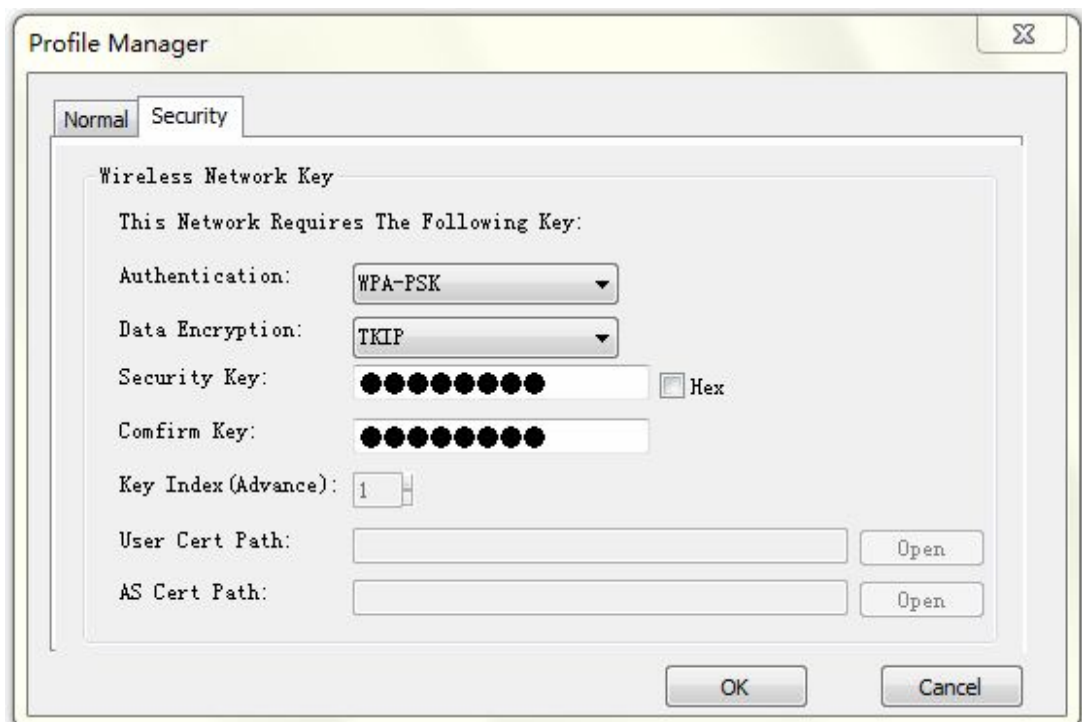
The wireless security features require key index and password to access the shared resources in the network.



- **Wireless Security: WPA-PSK**

Data Encryption: TKIP

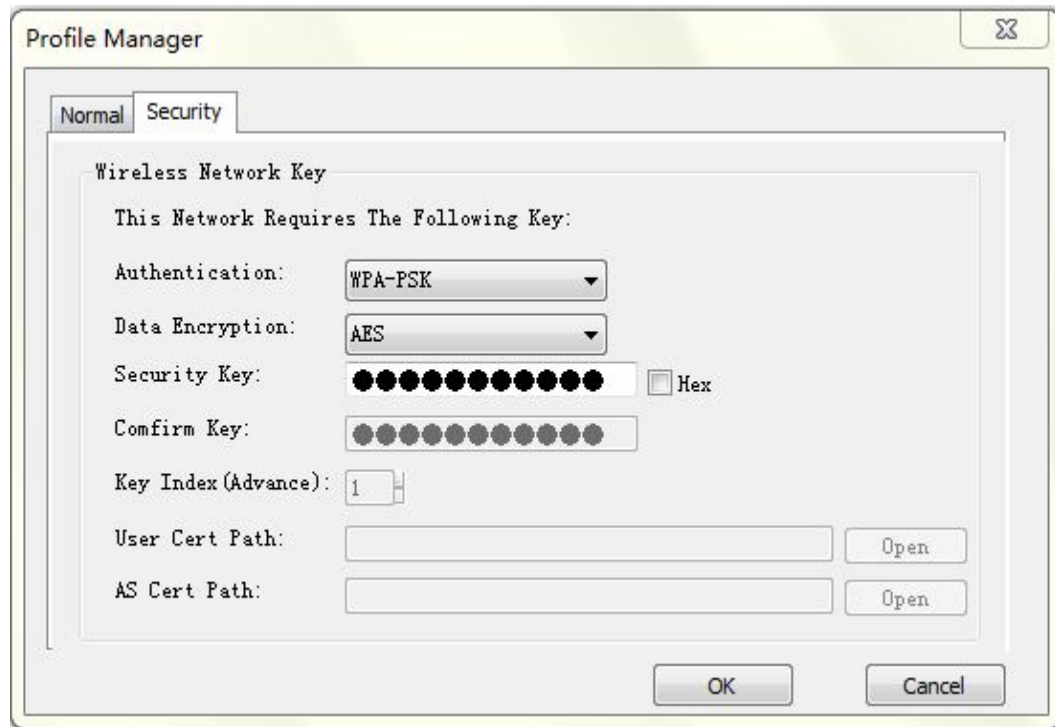
The wireless security features require password to access the shared resources in the network.



- **Wireless Security: WPA-PSK**

Data Encryption: AES

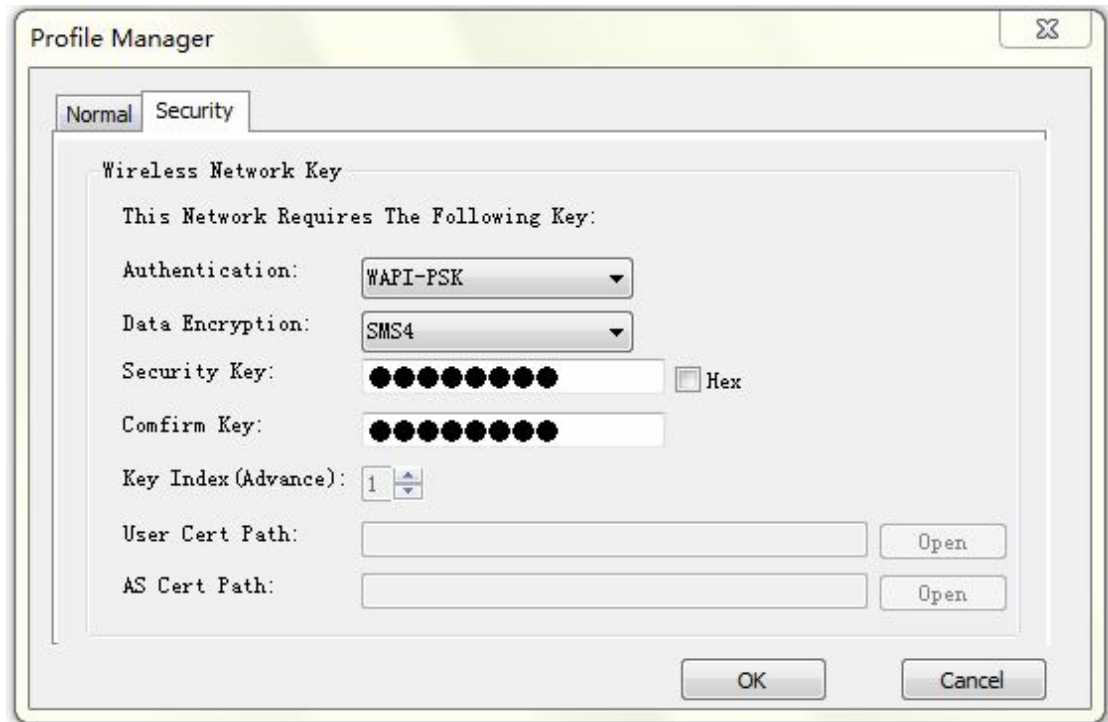
The wireless security features require password to access the shared resources in the network.



- **Wireless Security: WPA2-PSK**

Data Encryption: SMS4

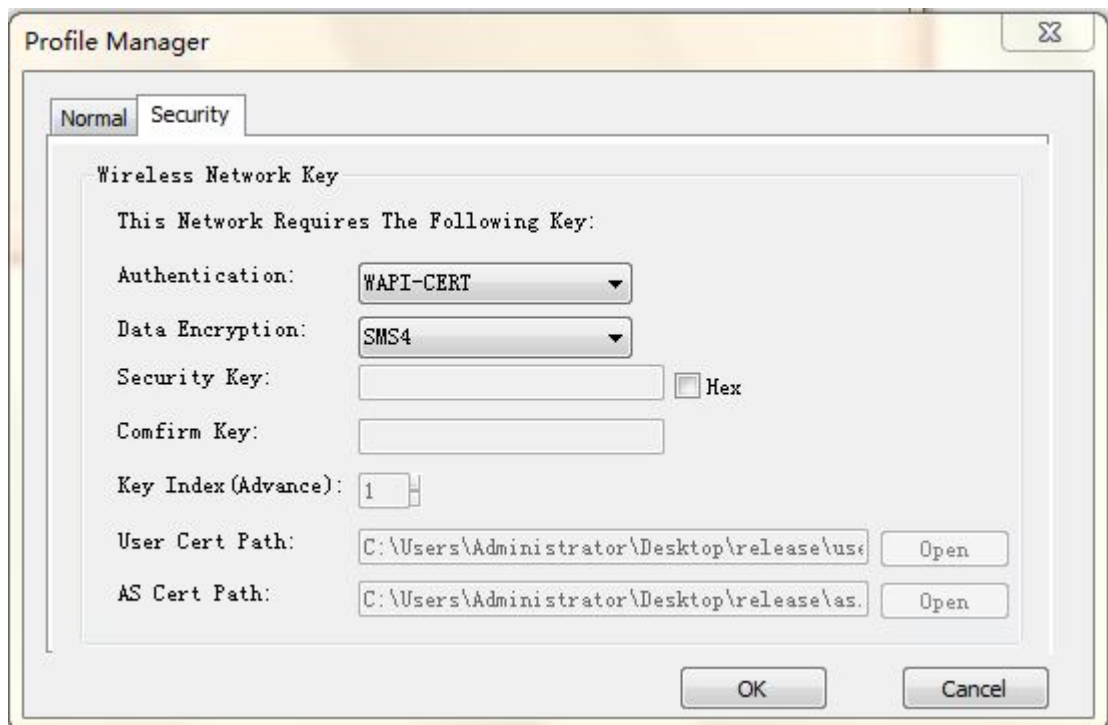
The wireless security features require password to access the shared resources in the network.



- **Wireless Security: WAPI-CERT**

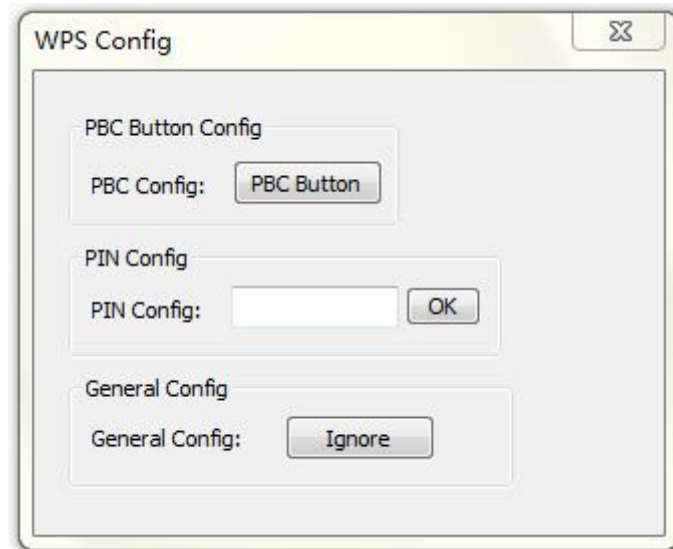
Data Encryption: SMS4

The wireless security features require the User cert and AS cert to access the shared resources in the network.



- **Config connection with WPS AP**

- The wireless USB adapter detects a network with WPS ,click the network .The **WPS Config** page:



The WPS configuration methods include: Pin Input Config (PIN) method, Push Button Config (PBC) method,

★ PIN Config method

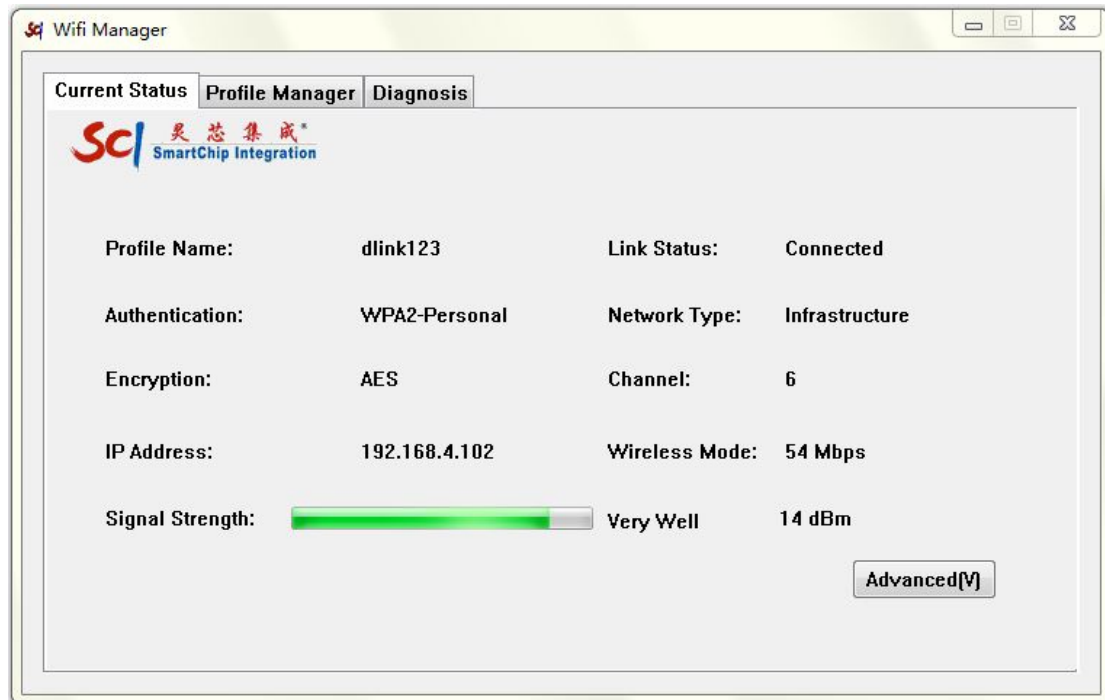
- ◆ Enter the PIN of the AP at the PIN Config Box on STA.
- ◆ Ping from Console to STA must succeed within 2 minutes

★ PBC Config method

- ◆ Push the PBC button on the AP
- ◆ Push the PBC button on the Sta.
- ◆ Ping from Console to STA must succeed within 2 minutes.

- If you don't use WPS config, please click Ignore button to enter the general config.

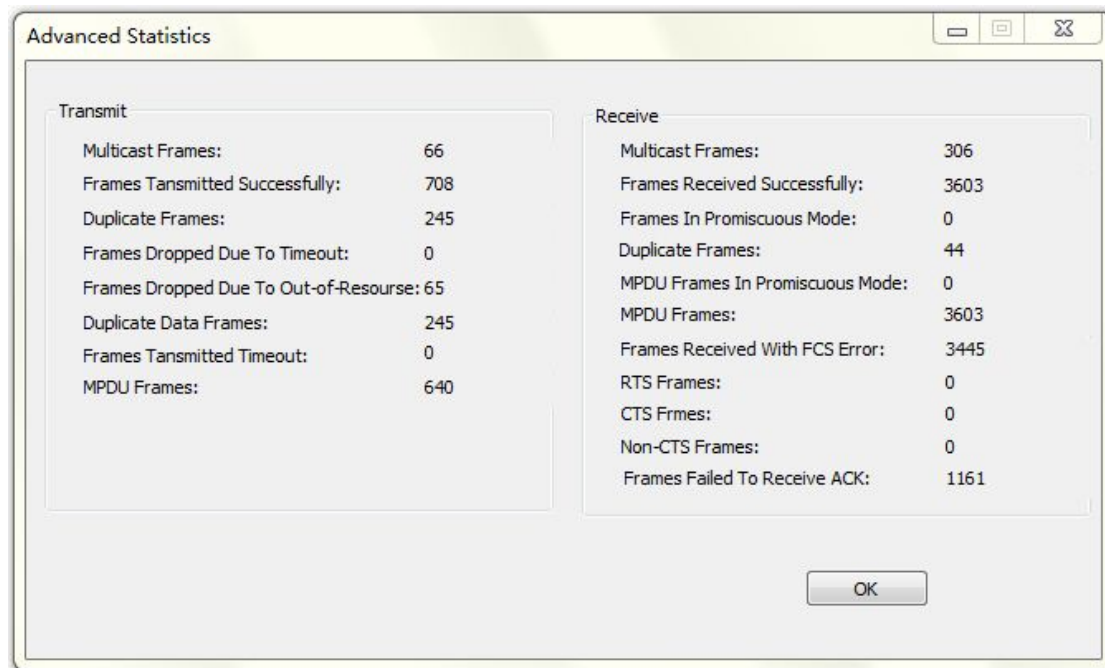
When the adapter has joined a network, click the Current Status tab to display the following screen:



The Current Status page shows your network connection and Internet connection:

Profile Name	You may enter a distinctive name of profile in this column.
Link Status	Shows the link Status.
Network Type	Network type in use, infrastructure for BSS.
Authentication	Authentication mode used within the network.
Encryption	Shows the encryption type currently in use.
Channel	Shows the channel currently in use.
Wireless Mode	AP support wireless mode. It may support 802.11b, 802.11g Wireless Mode.
IP Address	Shows the IP Address information.
Signal Strength	Shows the receiving signal strength of specified network.

Click the Advanced tab to view the following page:



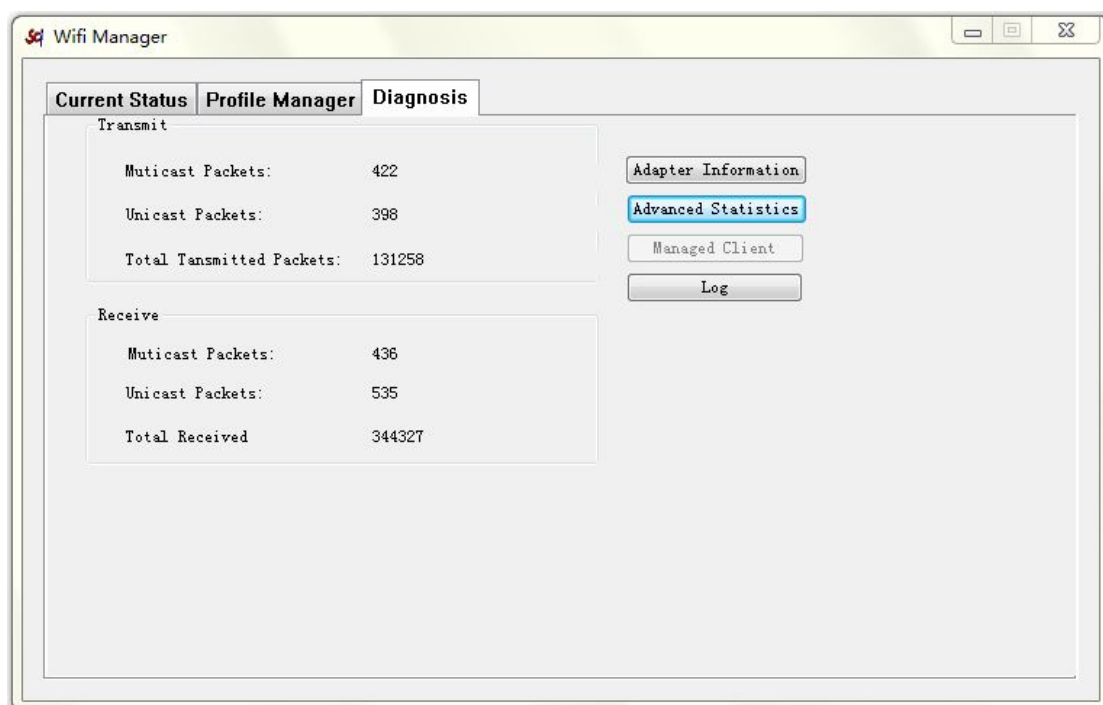
Advanced Statistics: The screen shows the following information for the device's details.

Network Name	The name assigned to a wireless network.
Authentication	Authentication mode used within the network..
Encryption	Shows the encryption type currently in use.
Wireless Mode	AP support wireless mode.
Authentication Type	There are four types of authentication modes support .They are open, shared, WPA-PSK and WPA system..
MIC	Whether MIC or not.
AP Name	Shows the name of the AP that wireless card connecting.
AP IP Address	Shows the IP address of the AP that wireless card connecting.
AP MAC Address	Shows the MAC address of the AP that wireless card connecting.

Signal Strength	Shows current signal strength.
Noise Strength	Shows the noise signal strength.
Packet Preamble	Shows 802.11 packet preamble
Receive	Shows the current receive rate.
Transmit	Shows the current transmit rate.
Channel	Shows the current channel in use.
Frequency	Shows the current signal frequency.
Channel Set	Shows the current signal frequency channel set.
Runtime	Shows the wireless card connection time.

3.About Your Smart Wizard

3.1 Diagnosis



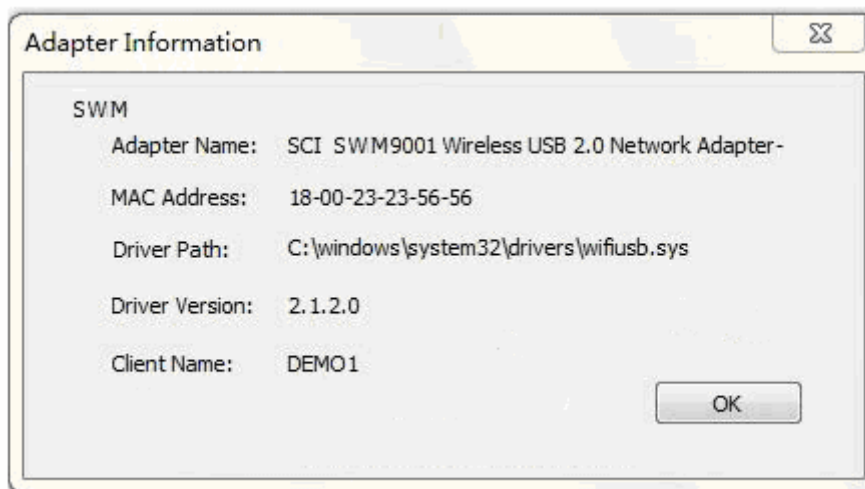
The following information is displayed in diagnosis page:

- Transmit and Receive Broadcast/Multicast packets

- Transmit and Receive Unicast packets
- total transmitted packets and receive packets

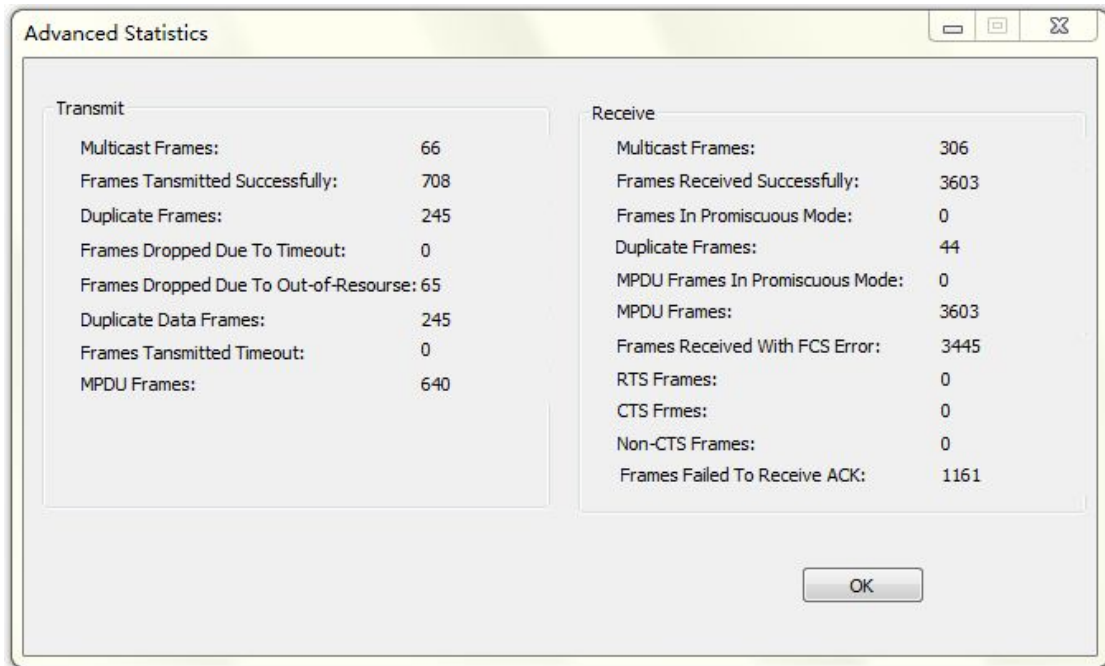
3.2 Adapter Information

The Adapter Information displays the current software version information:



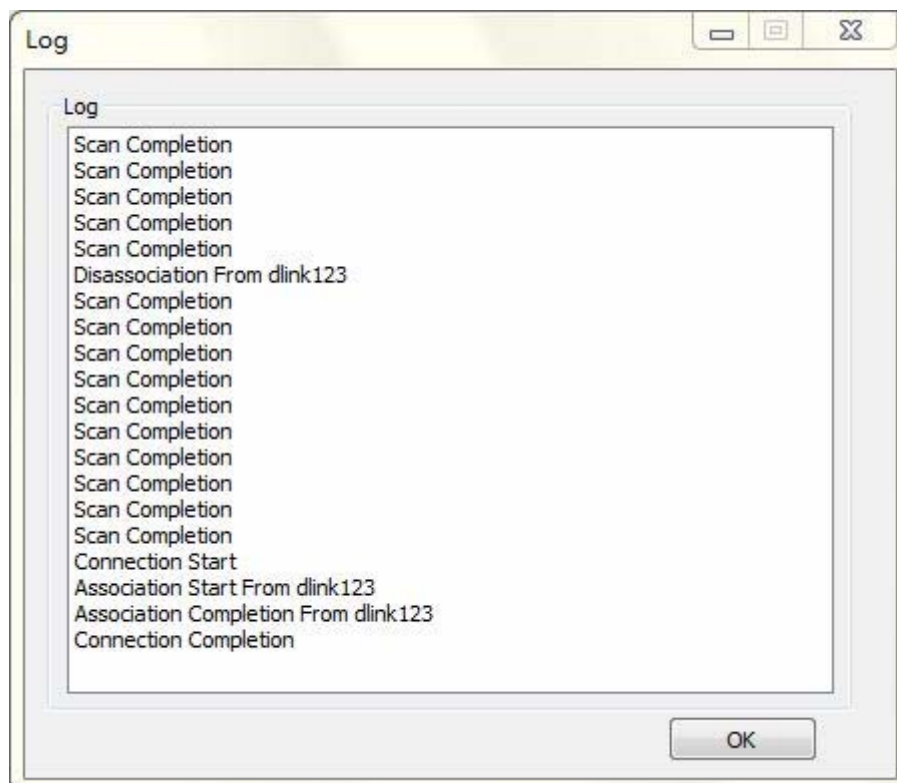
3.3 Advanced Statistics Page

The Statistics page provides real time and historical trend information on the data traffic and performance of your wireless adapter.




3.4 card log

On the diagnosis tab click the card log button to display the dialog box shown below:





3.5 Operation of the task bar

When you minimize SCI wireless device management application, the  icon appears on the desktop and in the lower right of the Windows task bar. You can either Right-click or double-click this icon on the desktop at any time, to use the Smart Wizard.

4. Standards and Regulatory Compliance

4.1 Standards and certification

The EUT conforms to the following standards and certification requirements:

802.11 b/g

FCC

- ☐ 47 CFR Part 1 - RF radiation exposure limits
- ☐ 47 CFR Part 2 - Equipment authorization
- ☐ 47 CFR Part C - WIFI

4.2 FCC certification requirements.

According to the definition of mobile and fixed device is described in Part 2.1091(b), this device is a mobile device.

And the following conditions must be met:

1. The EUT is a mobile device; maintain at least a 20 cm separation between the EUT and the user's body and must not transmit simultaneously with any other antenna or transmitter.
2. The device is only for fixed operation mode. (A Class II Change would be required for near-body Host applications.)



3. A label with the following statements must be attached to the host end product: This device contains Tx FCC ID: A7N-SWM9001.
4. To comply with FCC regulations limiting both maximum RF output power and human exposure to RF radiation, maximum antenna gain (including cable loss) must not exceed:
 - ☐ 802.11b band < 1.5 dBi
 - ☐ 802.11g band <1.5 dBi
5. This module must not transmit simultaneously with any other antenna or transmitter
6. The host end product must include a user manual that clearly defines operating requirements and conditions that must be observed to ensure compliance with current FCC RF exposure guidelines.

For portable devices, in addition to the conditions 3 through 6 described above, a separate approval is required to satisfy the SAR requirements of FCC Part 2.1093

If the device is used for other equipment that separate approval is required for all other operating configurations, including portable configurations with respect to 2.1093 and different antenna configurations.

For this device, OEM integrators must be provided with labeling instructions of finished products. Please refer to KDB784748 D01 v07, section 8. Page 6/7 last two paragraphs:

A certified modular has the option to use a permanently affixed label, or an electronic label. For a permanently affixed label, the module must be labelled with an FCC ID - Section 2.926 (see 2.2 Certification (labelling requirements) above). The OEM manual



must provide clear instructions explaining to the OEM the labelling requirements, options and OEM user manual instructions that are required (see next paragraph).

For a host using a certified modular with a standard fixed label, if (1) the module's FCC ID is not visible when installed in the host, or (2) if the host is marketed so that end users do not have straightforward commonly used methods for access to remove the module so that the FCC ID of the module is visible; then an additional permanent label referring to the enclosed module: "Contains Transmitter Module FCC ID: A7N-SWM9001" or "Contains FCC ID: A7N-SWM9001" must be used. The host OEM user manual must also contain clear instructions on how end users can find and/or access the module and the FCC ID.

The users manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

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 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.



4.3 FCC RF exposure requirements

1. Radiated transmit power must be equal to or lower than that specified in the FCC Grant of Equipment Authorization for FCC ID: A7N-SWM9001.
2. To comply with FCC regulations limiting both maximum RF output power and human exposure to RF radiation, maximum antenna gain (including cable loss) must not exceed:
 - ❑ 802.11b band < 1.5 dBi
 - ❑ 802.11g band < 1.5 dBi
3. This module must not transmit simultaneously with any other antenna or transmitter.
4. To ensure compliance with all non-transmitter functions the host manufacturer is responsible for ensuring compliance with the module(s) installed and fully operational. For example, if a host was previously authorized as an unintentional radiator under the Declaration of Conformity procedure without a transmitter certified module and a module is added, the host manufacturer is responsible for ensuring that after the module is installed and operational the host continues to be compliant with the Part 15B unintentional radiator requirements.