

MERCUSYS®

MW150US 150Mbps Wireless N Nano USB Adapter



FCC 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 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 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.
- 2) This device must accept any interference received, including interference that may cause undesired operation.

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

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment has been SAR-evaluated for use in hand. SAR measurements are based on a 5mm spacing from the body and that compliance is achieved at that distance.

CE Mark Warning

CE1588

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

- (1) This device may not cause interference, and
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil est conforme aux normes CNR exemptes de licence d'Industrie Canada. Le fonctionnement est soumis aux deux conditions suivantes:

- (1) cet appareil ne doit pas provoquer d'interférences et
- (2) cet appareil doit accepter toute interférence, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

Industry Canada Statement

Complies with the Canadian ICES-003 Class B specifications.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

This device complies with RSS 210 of Industry Canada. This Class B device meets all the requirements of the Canadian interference-causing equipment regulations.

Cet appareil numérique de la Classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Déclaration d'exposition aux radiations: Le produit est conforme aux limites d'exposition pour les appareils portables RF pour les Etats-Unis et le Canada établies pour un environnement non contrôlé.

Le produit est sûr pour un fonctionnement tel que décrit dans ce manuel. La réduction aux expositions RF peut être augmentée si l'appareil peut être conservé aussi loin que possible du corps de l'utilisateur ou que le dispositif est réglé sur la puissance de sortie la plus faible si une telle fonction est disponible.



Продукт сертифіковано згідно з правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

Safety Information

- When product has power button, the power button is one of the way to shut off the product; when there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don't disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.
- This product can be used in the following countries:

AT	BG	BY	CA	CZ	DE	DK	EE
ES	FI	FR	GB	GR	HU	IE	IT
LT	LV	MT	NL	NO	PL	PT	RO
RU	SE	SK	TR	UA			

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **150Mbps Wireless N Nano USB Adapter**

Model No.: **MW150US**

Trademark: **MERCUSYS**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC, Directives 2006/95/EC, Directives 1999/519/EC, Directives 2011/65/EU

The above product is in conformity with the following standards or other normative documents:

ETSI EN 300 328 V1.7.1: 2006

ETSI EN 301 489-1 V1.9.2:2011 & ETSI EN 301 489-17 V2.1.1:2009

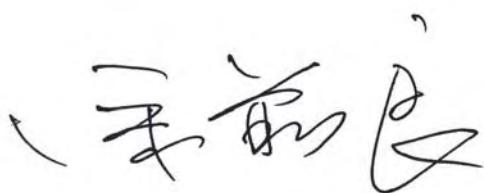
EN 60950-1:2006+A11: 2009+A1:2010+A12:2011

EN 62311:2008

The product carries the CE Mark:

CE1588

Person responsible for marking this declaration:



Tu Qianliang

Manager of International Product Department

Date of issue:2013

MERCUSYS TECHNOLOGIES CO., LTD.

3rd Floor, Building R1-B,, No. 23, Gaoxin 4th Road, South Hi-Tech Park, Nanshan, Shenzhen,
P.R.China

Package Contents

The following contents should be found in your box:

- One MW150US 150Mbps Wireless N Nano USB Adapter
- Quick Installation Guide
- One Resource CD for MW150US, including:
 - MERCUSYS Wireless Configuration Utility (MWCU) and Drivers
 - User Guide
 - Other Helpful Information

NOTE:

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact your distributor.

Conventions

The Adapter or MW150US, or device mentioned in this User Guide stands for MW150US 150Mbps Wireless N Nano USB Adapter without any explanations.

Parameters provided in the pictures are just references for setting up the product, which may differ from the actual situation.

You can set the parameters according to your demand.

CONTENTS

Package Contents	I
Conventions	I
Chapter 1. Introduction.....	1
1.1 Overview of the product.....	1
1.2 Features.....	1
1.3 LED Status.....	2
Chapter 2. Installation Guide.....	3
2.1 Hardware Installation	3
2.2 Software Installation.....	3
2.2.1 Overview.....	3
2.2.2 Software Installation	3
Chapter 3. Connect to a Wireless Network	8
3.1 To connect using MWCU	8
3.2 To connect using WPS	12
3.2.1 PBC (Push Button Configuration) method	13
3.2.2 PIN method.....	14
3.3 To connect using Windows built-in wireless utility	17
3.3.1 In Windows 7	17
3.3.2 In Windows Vista	19
3.3.3 In Windows XP	21
Chapter 4. Management.....	24
4.1 Profile.....	24
4.1.1 Add a profile	24
4.1.2 Modify a profile	26
4.1.3 Delete a profile.....	27

4.2	Advanced.....	27
4.3	About	28
Chapter 5.	AP Mode	29
Chapter 6.	Uninstall Software	32
6.1	Uninstall the utility software from your PC	32
6.2	Uninstall the driver software from your PC.....	33
Appendix A:	Specifications	36
Appendix B:	Glossary	37

Chapter 1.

Introduction

1.1 Overview of the product

The adapter is designed to provide a high-speed and unrivaled wireless performance for your notebook and PC. With a faster wireless connection, you can get a better Internet experience, such as downloading, gaming, video streaming and so on.

The MW150US's auto-sensing capability allows high packet transfer rate of up to 150Mbps for maximum throughput. It has good capability on anti-jamming; it can also interoperate with other wireless (802.11b/g/n) products. The adapter supports WEP, WPA and WPA2 encryption to prevent outside intrusion and protect your personal information from being exposed.

The Quick Setup Wizard guides you step-by-step through the installation process; the MERCUSYS Wireless Configuration Utility helps you create a wireless connection immediately.

With unmatched wireless performance, reception, and security protection, the MW150US is the best choice for easily adding or upgrading wireless connectivity.

1.2 Features

- IEEE802.11b, IEEE802.11g, IEEE802.11n standards
- Supports WPA/WPA2 data security, IEEE802.1x authentication, TKIP/AES encryption, WEP encryption
- Make use of IEEE 802.11n wireless technology to provide a wireless data rate of up to 150Mbps
- Supports automatically adjust to lower speeds due to distance or other operating limitations
- Provides USB interface
- Supports Ad-Hoc and Infrastructure modes
- Good capability on anti-jamming
- Supports roaming between access points when configured in Infrastructure mode
- Easy to configure and provides monitoring information
- Supports Windows XP, Windows Vista and Windows 7

1.3 LED Status

Status	Working Status
Off	The driver has not been installed.
Flashing Slowly	The driver has been installed but there is no data being transmitted or received.
Flashing Quickly	There is data being transmitted or received.

Chapter 2.

Installation Guide

2.1 Hardware Installation

Plug the Adapter directly to the USB port on your computer.

The prompted “**Found New Hardware Wizard**” screen will pop up when the adapter is installed correctly. Click **Cancel**.

2.2 Software Installation

2.2.1 Overview

The Adapter’s Setup Wizard will guide you through the Installation procedure. The Setup Wizard will install the MERCUSYS Wireless Configuration Utility (MWCU) and drivers.

When you install the hardware before installing the software, the system will prompt “Found New Hardware Wizard”, click **Cancel**, and run the Setup Wizard program on the CD.

2.2.2 Software Installation

NOTE:

The Setup steps for Windows XP/Vista/7 are similar with each other. The following instructions take Windows 7 for example.

1. Insert the Resource CD into the CD-ROM drive. Open the CD from **My Computer**. Choose **Network Adapter** and open the folder named **MW150US**. Then double-click **Setup.exe** to start the installation.

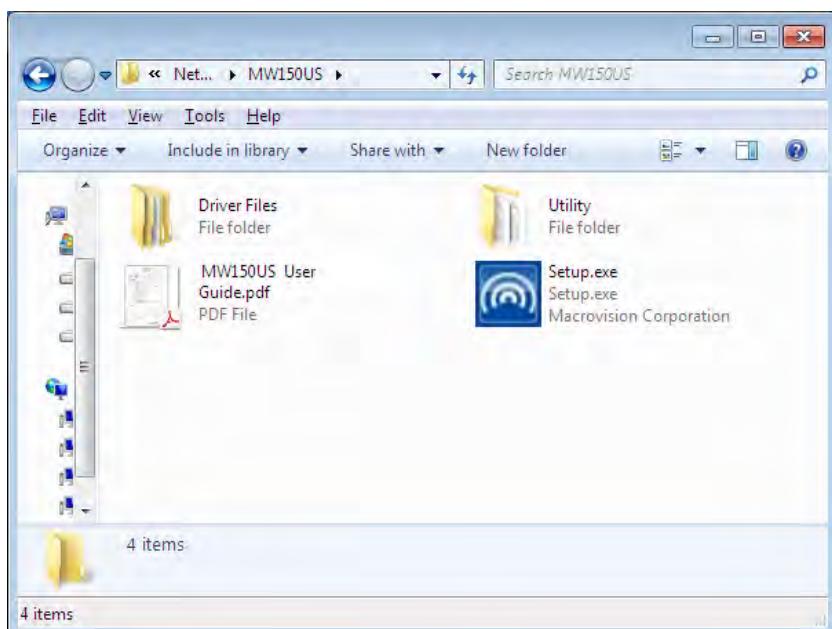


Figure 2-1

Chapter 2 – Installation Guide

2. The InstallShield Wizard window will appear. Click **Next** to continue.

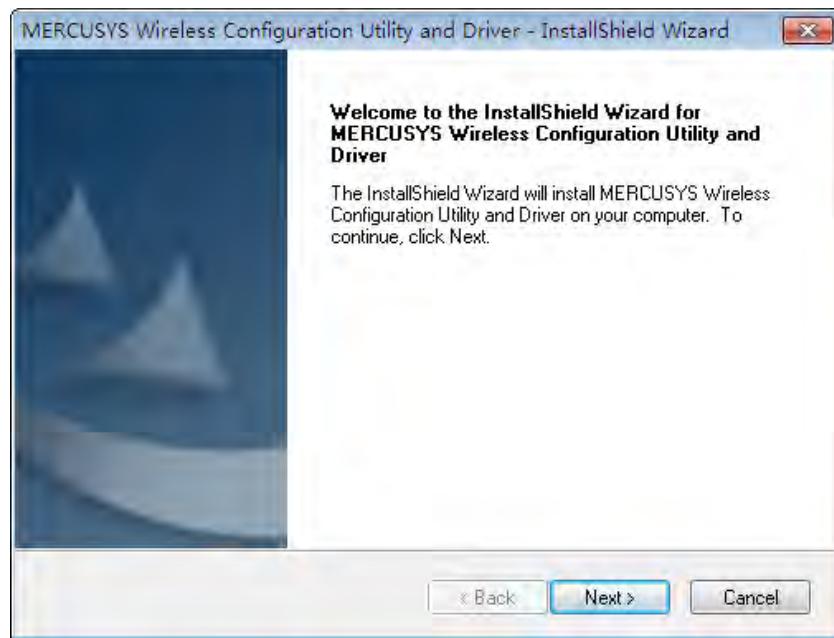


Figure 2-2

3. Select **Install MERCUSYS Wireless Configuration Utility and Driver** and then click **Next**.

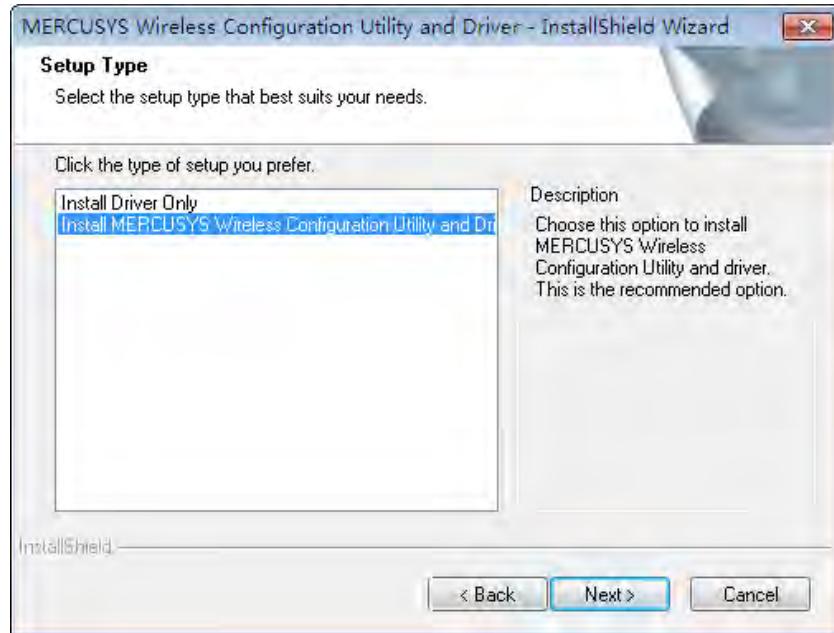


Figure 2-3

4. Click **Change...** to specify the destination location or you can leave it default.

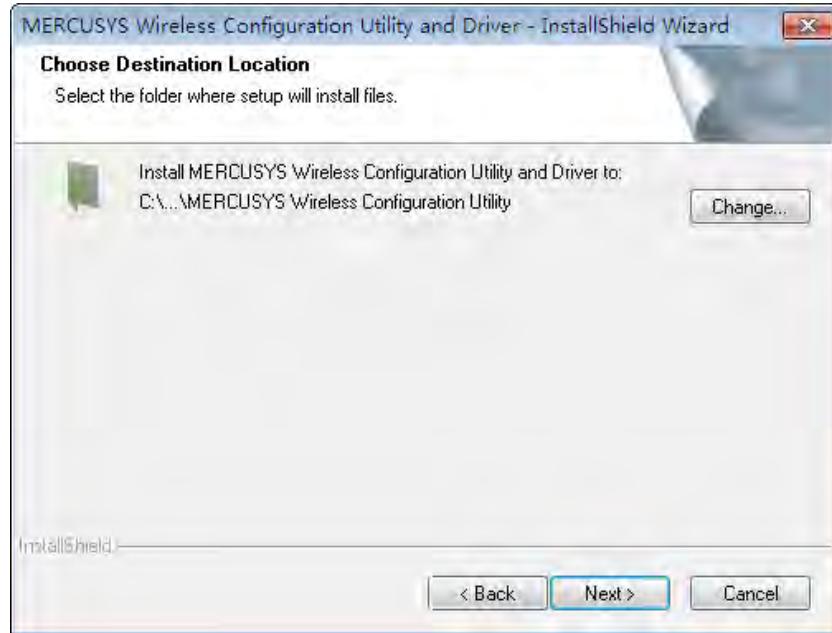


Figure 2-4

5. Click **Install** to install the driver and utility for your adapter.

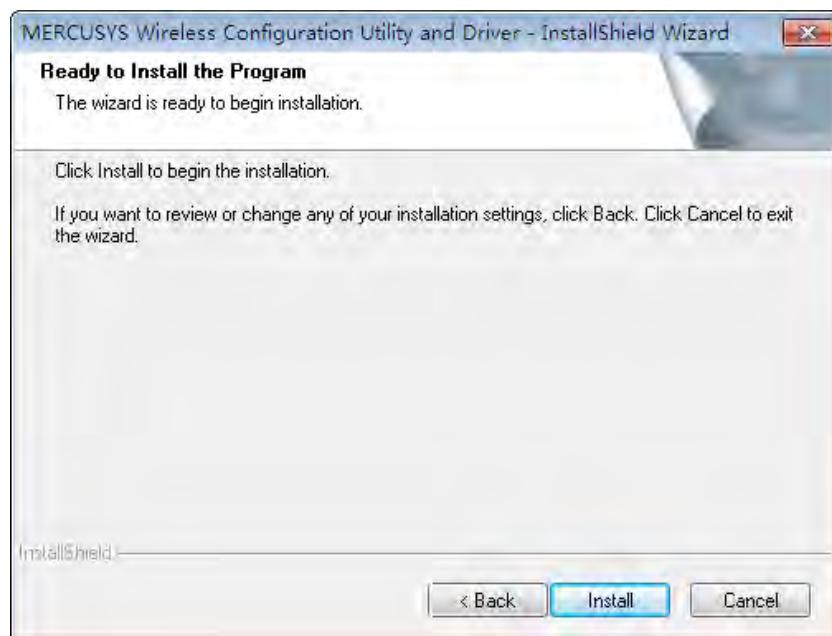


Figure 2-5

6. The installation of the driver and utility may take 1~2 minutes.

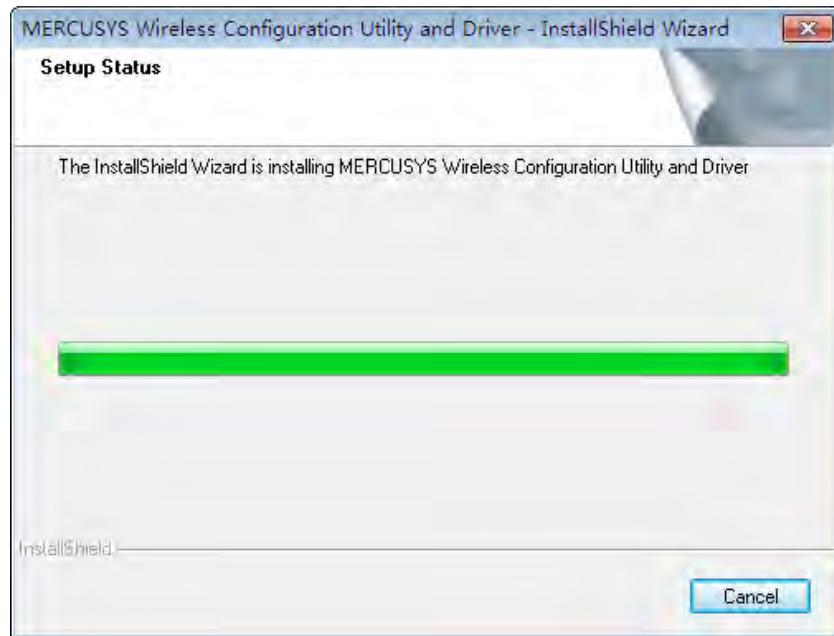


Figure 2-6

7. The following screen will then appear. Click **Finish** to complete the setup.

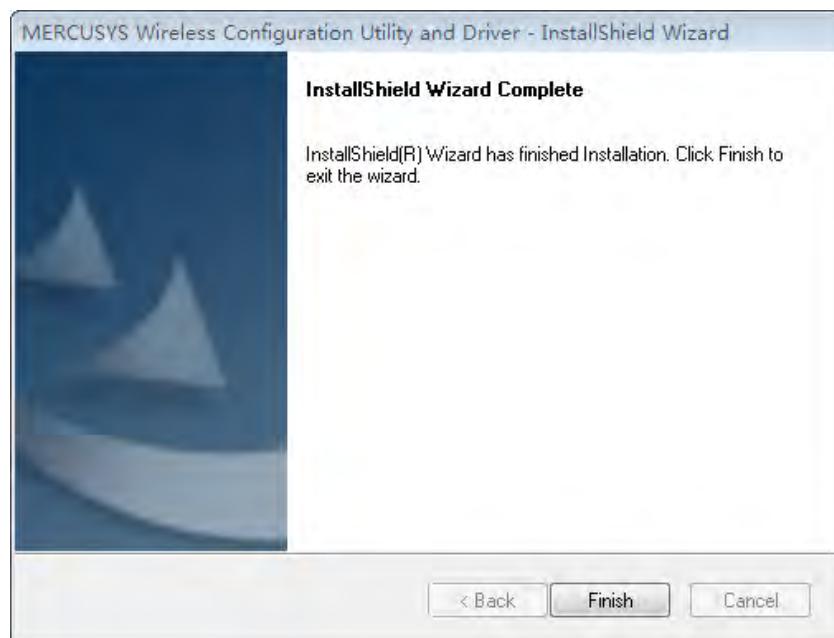


Figure 2-7

8. After installation, the utility configuration page will automatically pop up as shown in the following figure and the icon  will appear in your system tray. To connect to a network, please refer to [Chapter 3 Connect to a Wireless Network](#).

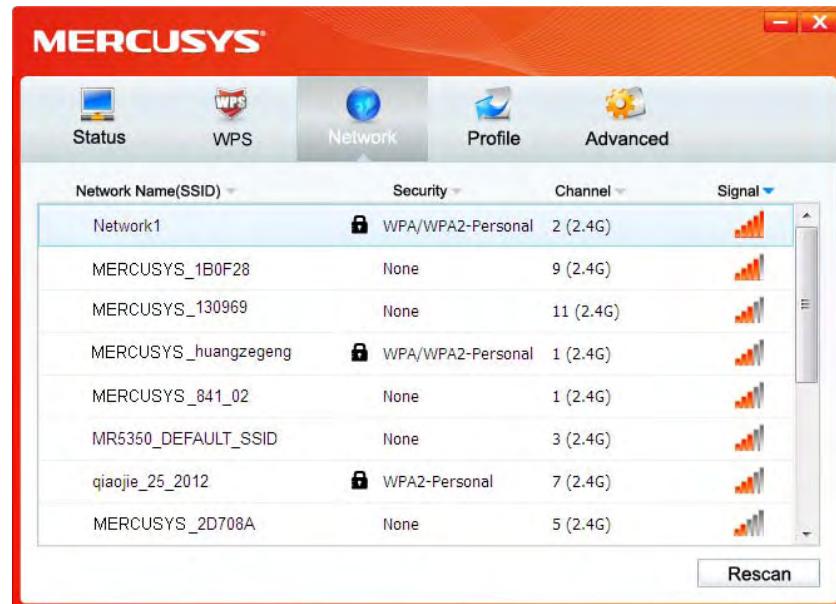


Figure 2-8

Chapter 3.

Connect to a Wireless Network

With both the hardware and software successfully installed into your computer, you can quickly connect to a wireless network using one of the following methods.

- Method One:

To connect using MWCU

MW150US uses the MERCUSYS Wireless Configuration Utility (MWCU) as the management software. The utility provides you an easy interface to connect to a network and to change any settings related to the wireless adapter.

- Method Two:

To connect using WPS

By this method, you can connect to your network quickly on the condition that your router or access point supports WPS function.

- Method Three:

To connect using Windows built-in wireless utility

Windows users may use the built-in wireless utility to connect to a wireless network. For specific operations, please go to [To connect using Windows built-in wireless utility](#).

3.1 To connect using MWCU

1. After installation, the utility configuration page will automatically pop up on the screen. If the utility page does not pop up, you can also launch the utility by double-clicking on the  icon on your desktop or the  icon in your system tray.

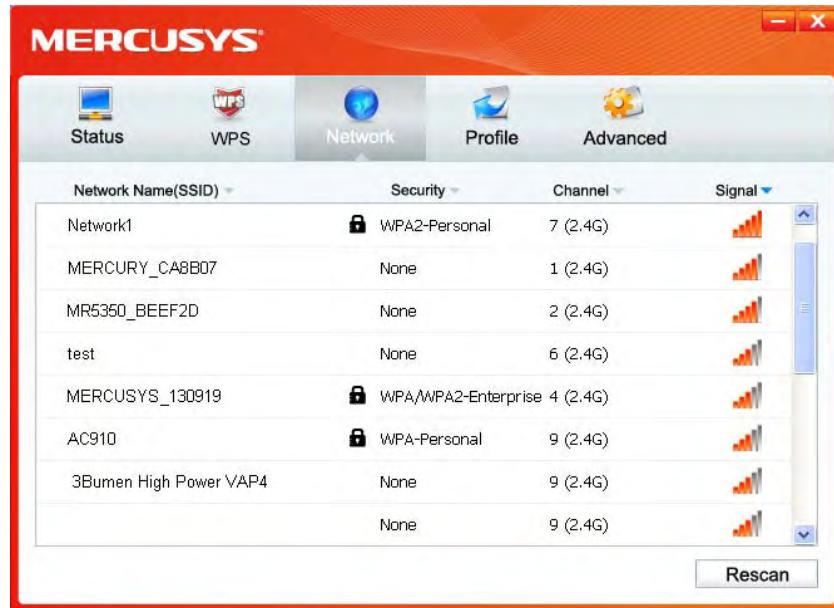


Figure 3-1

2. The **Network** page will display all wireless networks that are available in your area. To connect to a network, simply highlight the wireless network name and click **Connect**. **SSID** (Service Set Identifier) is the name of the wireless network. The adapter will automatically connect to your target network next time if you tick **Connect automatically**.

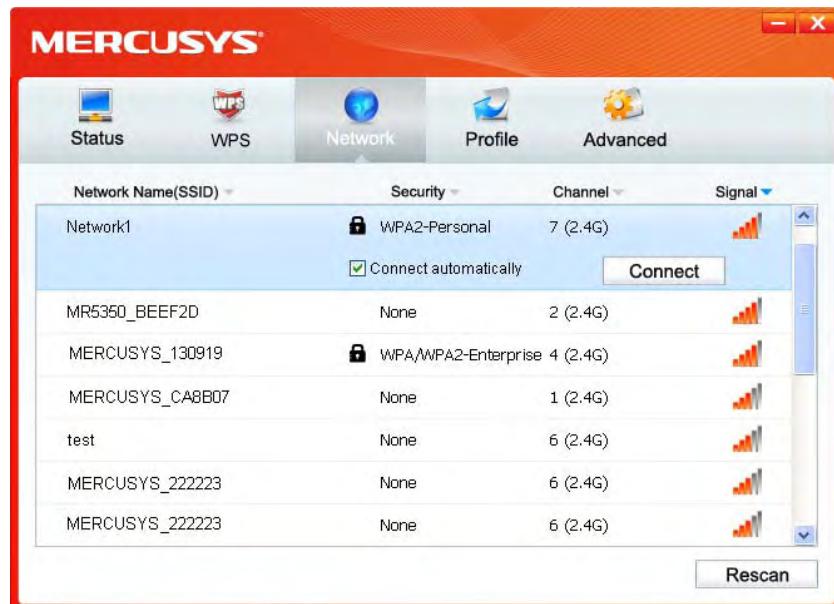


Figure 3-2

3. You will be prompted different windows when you choose wireless network of different security types.
 - 1) Wireless network of **WPA/WPA2-Personal**

If you selected a wireless network of the security type WPA/WPA2-Personal, you will be

prompted to enter the password in the security key field, as shown in Figure 3-3. Or you can push the **WPS** button on your Router (if it features the WPS function) to quickly build a connection without entering the security key (password).



Figure 3-3

NOTE:

The security key (password) can be found on the configuration page of your Router or Access Point.

2) Wireless network of **WPA/WPA2-Enterprise**

If you selected a wireless network of the security type WPA/WPA2-Enterprise, you will be prompted to choose a type of authentication, either **certificate** or **password**. With **Certificate** as your authentication, you need to select one specific certificate from the drop-down list, as shown in Figure 3-4. With **Password** as your authentication, you should enter the right user name and password in the corresponding field, as shown in Figure 3-4.



Figure 3-4



Figure 3-5

3) Wireless network of **None**

If you selected a wireless network of **None** (that is, no security is set.), you can get directly connected to this network without any further configuration.

4. Please wait a few minutes for the connection process.

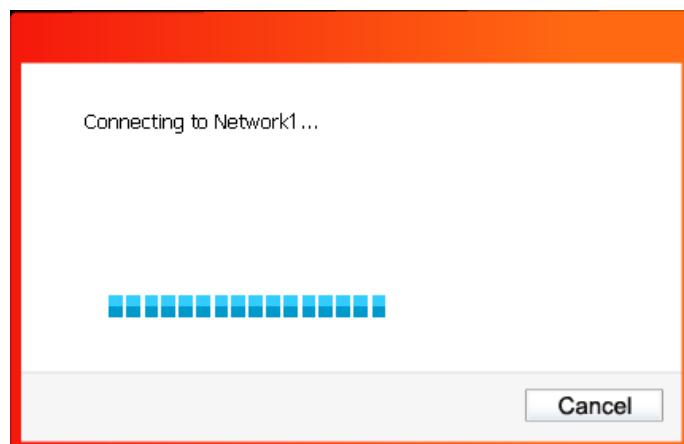


Figure 3-6

5. You have now successfully connected to your network. Click **Close** to enjoy the Internet.

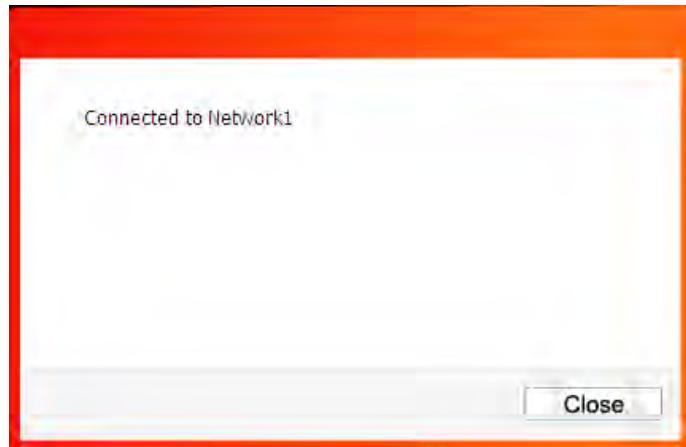


Figure 3-7

6. To view more information about the network currently connected, click **Status** in the tools section and the page will display information such as the network type, channel and wireless mode.

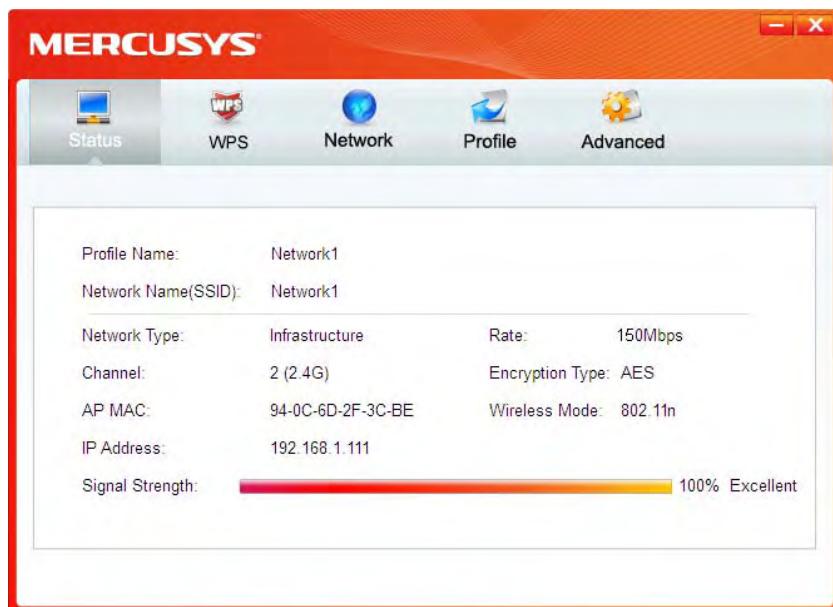


Figure 3-8

3.2 To connect using WPS

WPS (Wi-Fi Protected Setup) function allows you to add a new wireless device to an existing network quickly.

If the wireless router supports WPS, you can establish a wireless connection between wireless card and router using either Push Button Configuration (PBC) method or PIN method. Three WPS connection methods are listed in the following parts.

3.2.1 PBC (Push Button Configuration) method

1. Press the WPS/RESET button on the back panel of the router.



2. Open MWCU and click **WPS** tab. Select **Push the button on my access point or wireless router** and then click **Connect**.

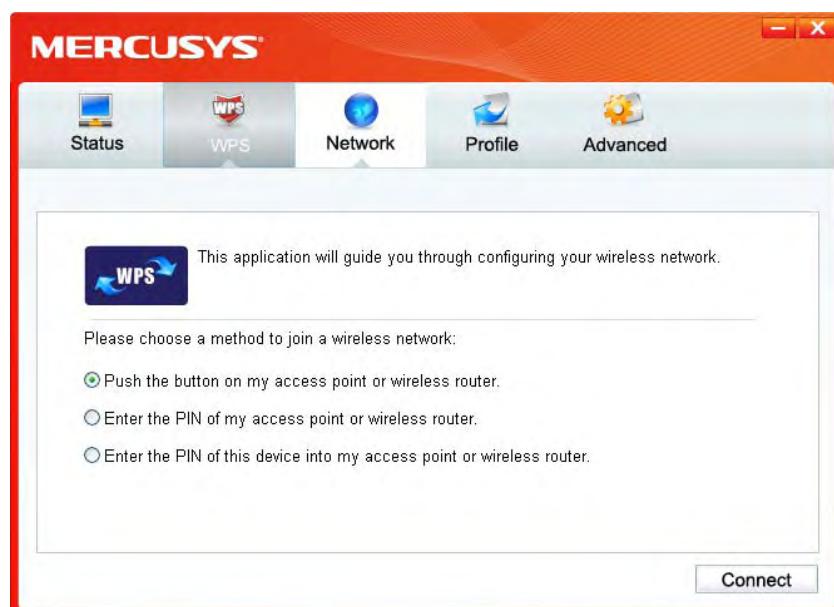


Figure 3-9

3. The adapter will be connecting to the target network.



Figure 3-10

4. When the following window appears, you have successfully connected to the network.



Figure 3-11

3.2.2 PIN method

There are two ways to configure the WPS by PIN method:

- 1) Enter the PIN from your AP device.
- 2) Enter a PIN into your AP device.

Following are detailed configuration procedures of each way.

3.2.2.1. Enter the PIN from your AP device

1. Open MWCU and click **WPS** tab. Select **Enter the PIN of my access point or wireless router**. In the empty field beside PIN, enter the PIN labeled on the bottom of the router (here takes 13492564 for example). If you have generated a new PIN code for your router, please enter the new one instead. Click **Connect** to continue.

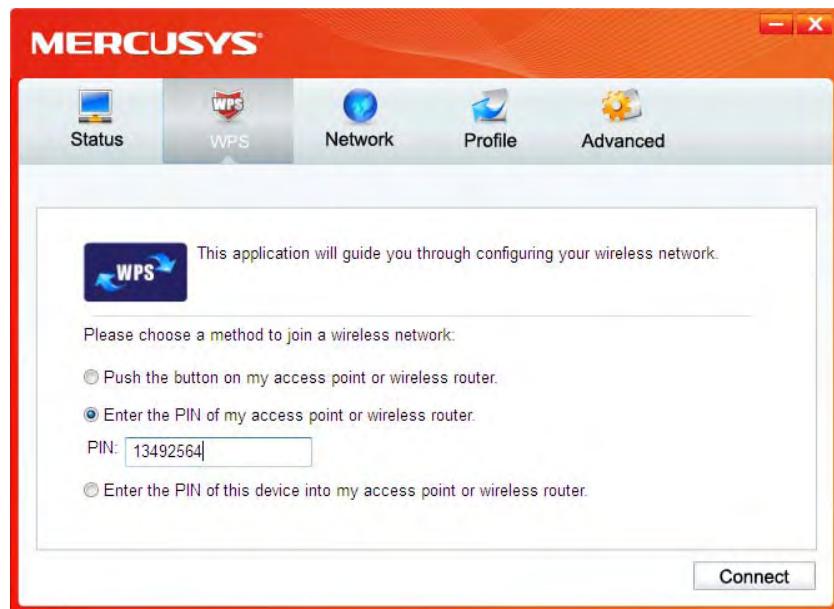


Figure 3-12

2. The adapter will be connecting to the target network.



Figure 3-13

3. When Figure 3-11 appears, you have successfully connected to the network.

3.2.2.2. Enter a PIN into your AP device

1. Open MWCU and click **WPS** tab. Select **Enter the PIN of this device into my access point or wireless router**. In the field beside PIN, you will see the PIN value of the adapter which is randomly generated. Click **Connect** to continue.

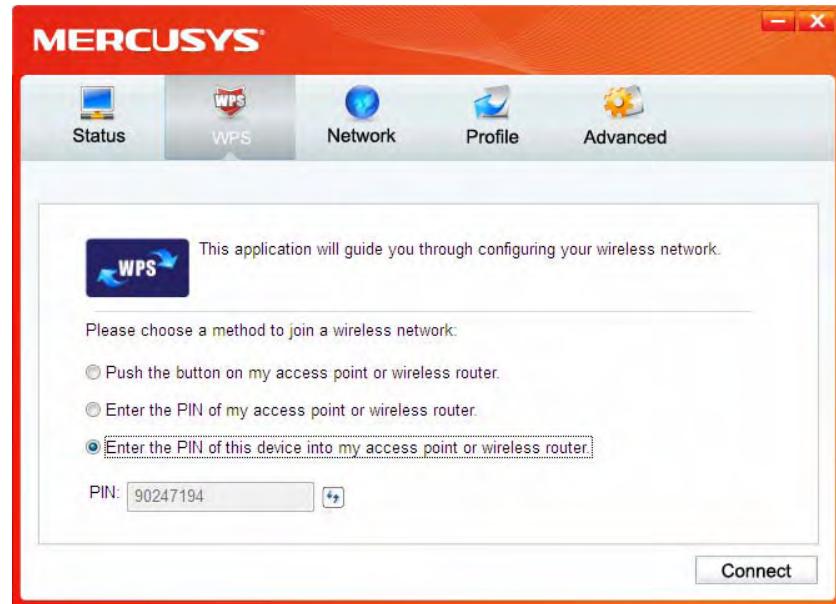


Figure 3-14

2. Open your router's Web-based Utility and click WPS link on the left of the main menu. Then click **Add device** and the following figure will appear. Enter the PIN value of the adapter in the empty field beside PIN and then click **Connect**.



Figure 3-15

3. When **Connect successfully** appears on the screen, the WPS configuration is complete. Or you can view the adapter's utility page to see whether the connection has been successful as shown in Figure 3-17.



Figure 3-16



Figure 3-17

3.3 To connect using Windows built-in wireless utility

3.3.1 In Windows 7

Windows 7 users may use the built-in wireless utility. Follow the steps below.

1. Left-click the wireless icon  in your system tray (lower-right corner). The utility will display any available wireless networks in your area. Highlight the wireless network (displayed using the SSID) to be connected and then click **Connect**.

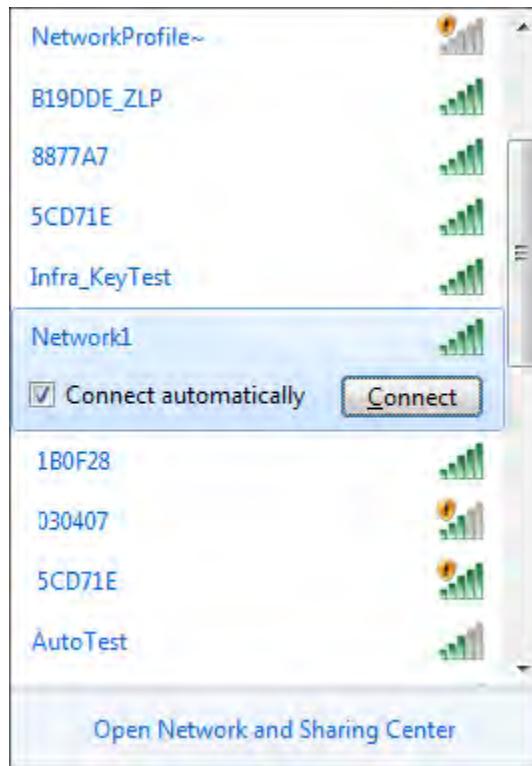


Figure 3-18

2. If the network you would like to connect is security-enabled, enter the same security key or passphrase that is on your router. Or push the WPS button on the router or access point (You will be prompted to push the button on the window if WPS function is supported as shown in the figure below). If the network to be connected is not secure, the connection will be built without entering a key.



Figure 3-19

3. You have now successfully connected to the network.



Figure 3-20

3.3.2 In Windows Vista

Windows Vista users may use the built-in wireless utility. Follow the steps below.

1. Open the wireless utility by right-clicking on the wireless computer icon in your system tray as shown in the figure below. Select **Connect to a network**.

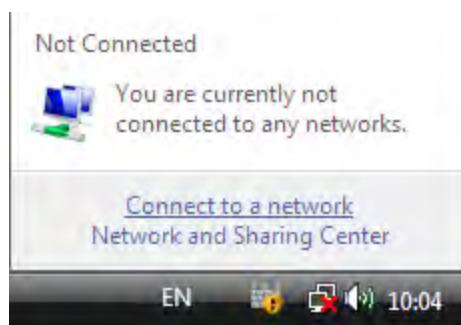


Figure 3-21

2. The utility will display any available wireless networks in your area. Highlight the wireless network you would like to connect and then click **Connect**.

Chapter 3 –Connect to a Wireless Network

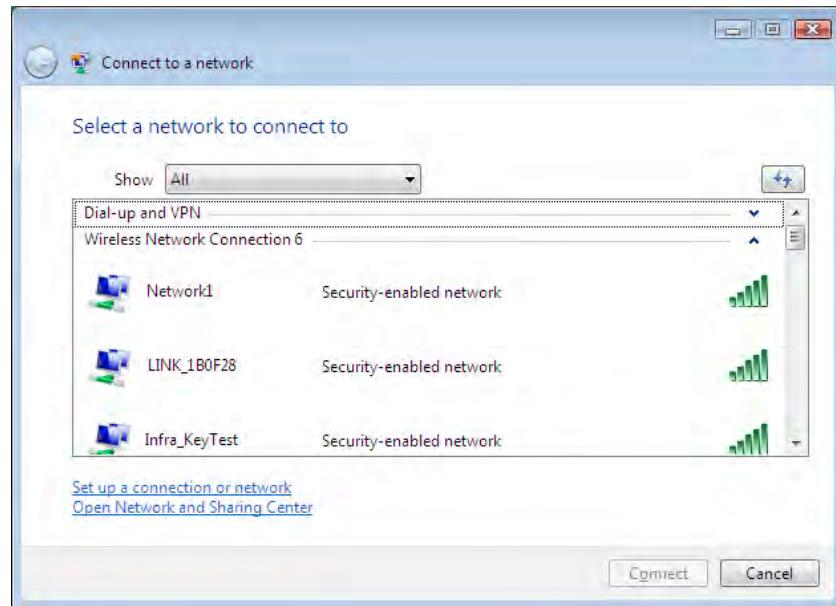


Figure 3-22

3. If the network you would like to connect is security-enabled, enter the same security key or passphrase that is on your router. If the network to be connected is not secure, the connection will be built without entering a key.

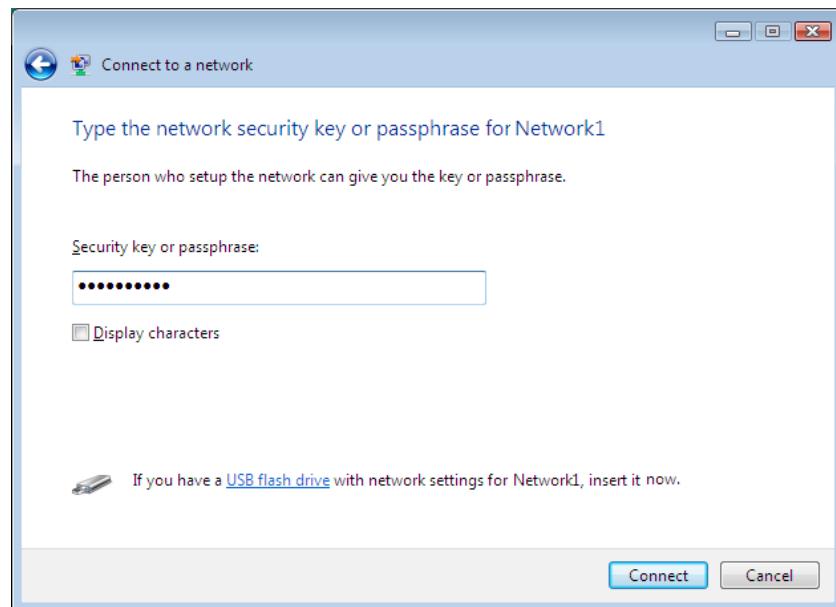


Figure 3-23

4. You have now successfully connected to the network.

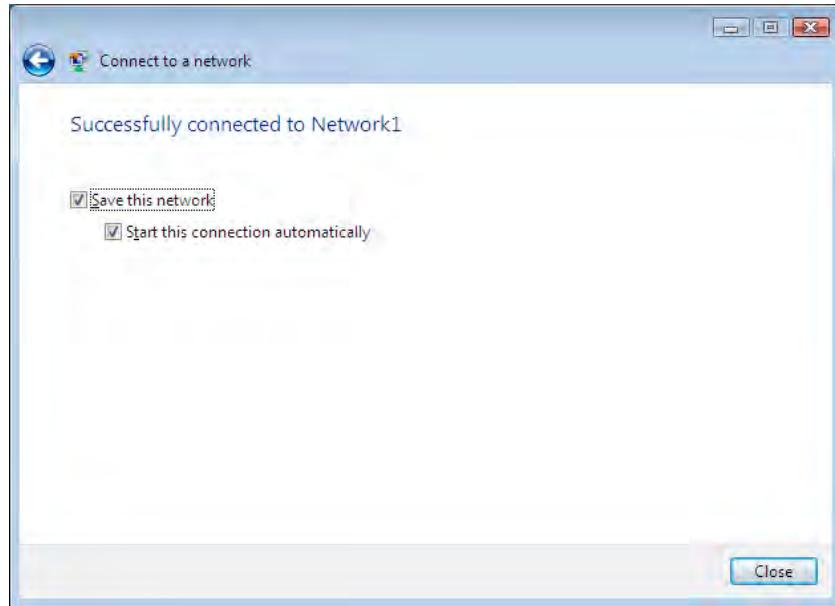


Figure 3-24

3.3.3 In Windows XP

Windows XP users may use the built-in wireless utility. Follow the steps below.

1. Right-click on the utility icon in your system tray (lower-right corner). Select **Switch to Windows wireless configuration tool**.

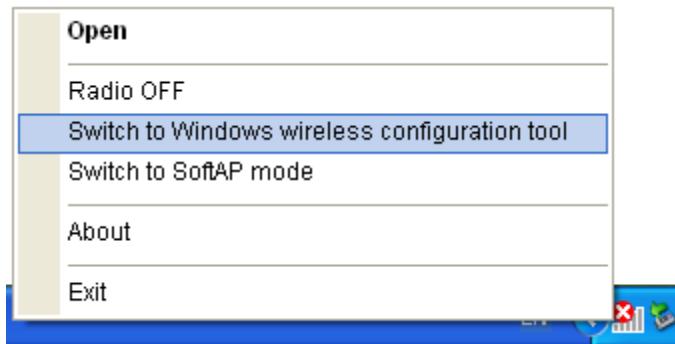


Figure 3-25

Or double-click the utility icon to load the utility configuration page. Click **Advanced** in the tools section and then select **Use Windows wireless configuration tool** in the figure shown below. Click **OK** when Figure 3-27 appears to continue.



Figure 3-26



Figure 3-27

2. Right-click on the wireless computer icon in your system tray (lower-right corner). Select **View Available Wireless Networks**.



Figure 3-28

3. The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

Chapter 3 –Connect to a Wireless Network

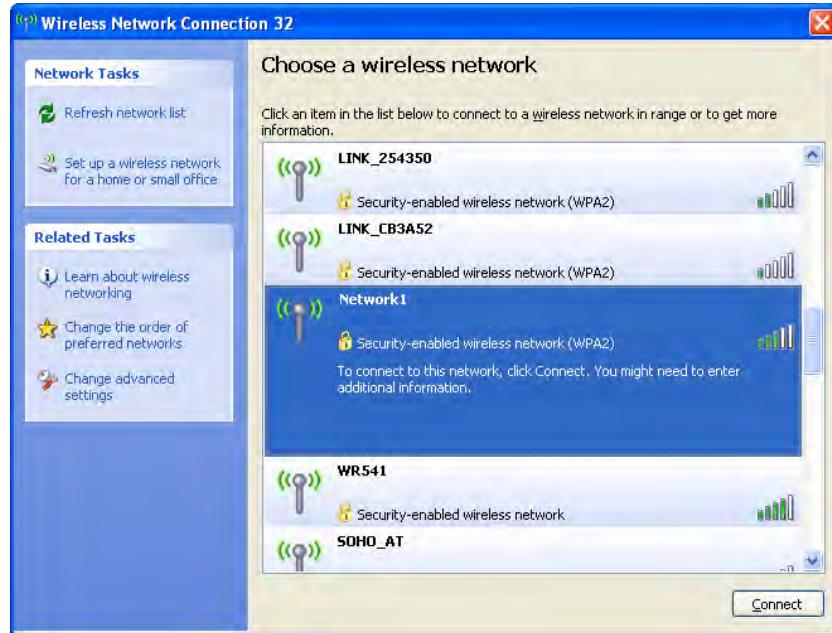


Figure 3-29

4. If the network is security-enabled, you will be prompted to enter the key as shown below. If not, you will connect to the network directly without entering a key.



Figure 3-30

Chapter 4.

Management

This section will show you how to configure your MW150US adapter using the MERCUSYS Wireless Configuration Utility (MWCU).

The MW150US adapter uses the MERCUSYS Wireless Configuration Utility as the management software. The utility provides users with an easy interface to change any settings related to the adapter. Double-clicking on the  icon on your desktop will start the utility.

4.1 Profile

Your wireless networks may vary in different places like home, office or coffee shop. With **Profile** management, you can easily save and manage various networks to be connected, saving you the trouble of having to repeat the same configurations. Click **Profile** in the tools section, the following page will appear.

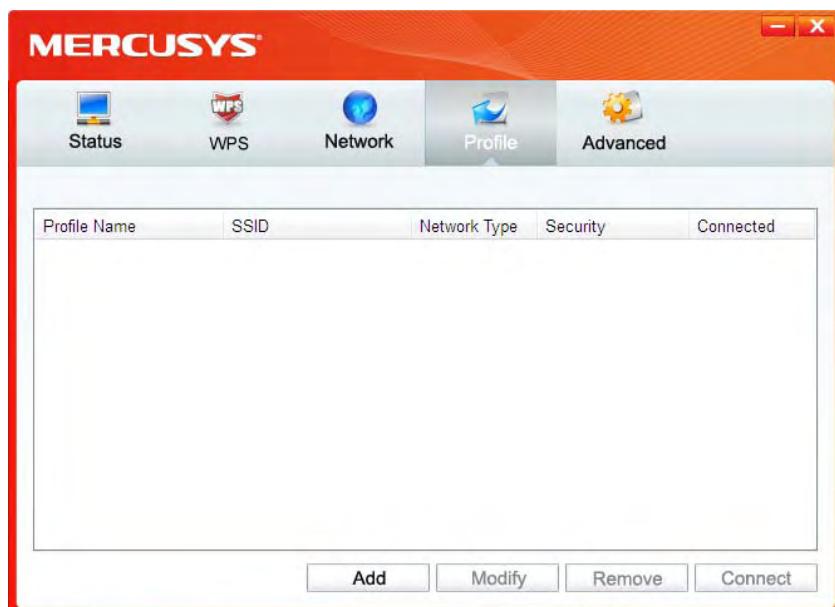


Figure 4-1

4.1.1 Add a profile

To add a profile, click the **Add** button on the bottom of the screen. Then the configuration window will appear.

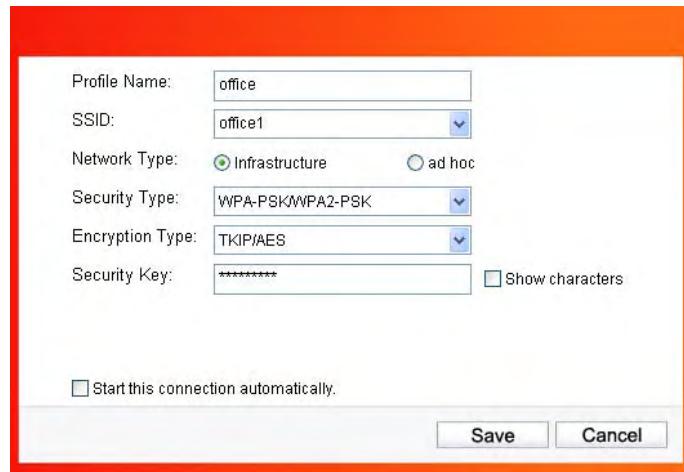


Figure 4-2



Figure 4-3

The following items can be found on the screen.

- **Profile Name:** Enter a name for your profile (e.g. office1 and office2). The same name is not allowed. Please also note that no space is allowed between words.
- **SSID:** Select the target network from the drop-down list.
- **Network Type:** Select the network type. If you are connecting to a wireless router or access point, select **Infrastructure**. If you are connecting to another wireless client such as an adapter, select **ad-hoc**.
- **Security Type:** Select the security type from the list. Four options are available: **WPA/WPA2**, **WPA-PSK/WPA2-PSK**, **WEP** and **None**. The security type should be the same as on your router or access point, otherwise, you will not be able to build a successful connection.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key must be the exact same key entered on your wireless router or access point. None stands for no security. It is recommended to enable WPA-PSK/WPA2-PSK on your wireless router or access point before configuring your wireless adapter.

NOTE:

You will see Figure 4-2 if you selected the security type **WPA-PSK/WPA2-PSK**; while, if you selected the security type **WPA/WPA2** (-Enterprise), Figure 4-3 will be displayed.

- **Encryption Type:** From the drop-down menu, select the encryption type that is the same as on your router or access point.
- **Security Key:** Enter the passphrase exactly as it is on your wireless router or access point. Click the **Show characters** box to see the passphrase. Unchecking it will hide it.
- **Authentication:** Select a type of authentication, either certificate or password.
- **Certificate:** If you select certificate as your Authentication, then you need to specify your certificate from the drop-down list here.
- **Start this connection automatically:** check this box to automatically connect to this network next time.
- **Save:** Click **Save** to save your settings.

Complete the above settings, the Profile page should look like the following figure. To connect to a desired network, just highlight the network you would like to connect to and click the **Connect** button on the bottom of the window.

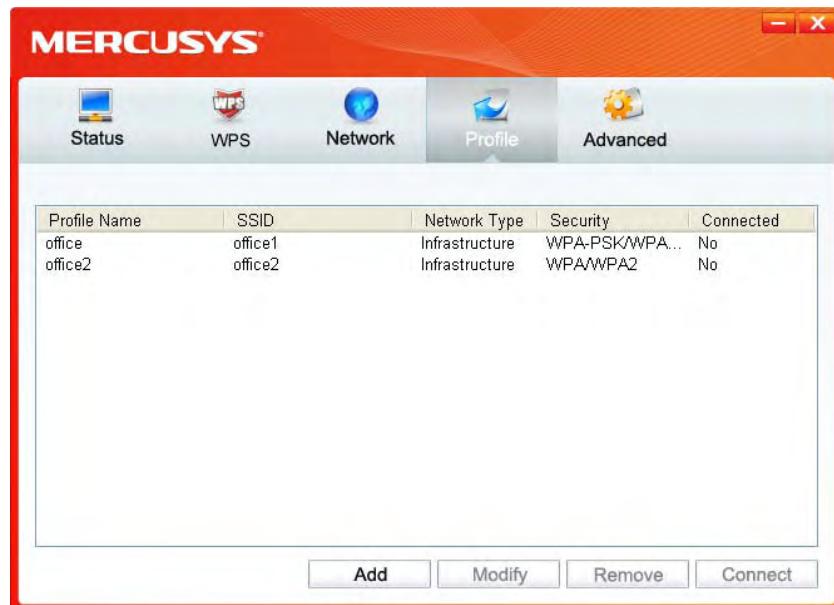


Figure 4-4

4.1.2 Modify a profile

You may edit an existing profile by clicking the **Modify** button from the Profile page. For instance, you may like to change the profile name from Home to Home1 or you may want to specify another SSID for profile Home. After all the changes, click **Save** to make the changes take effect.

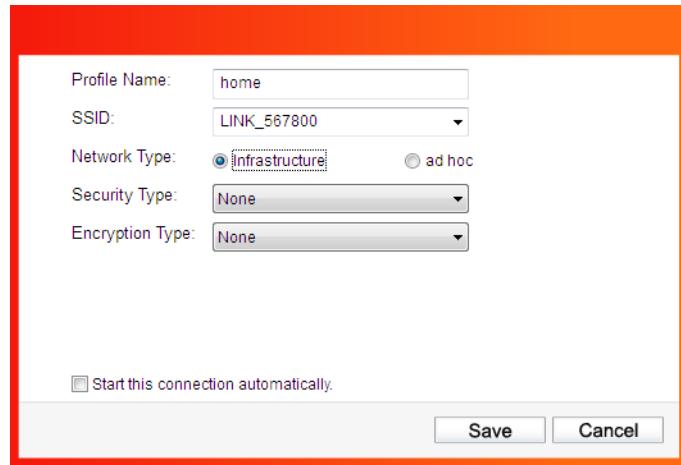


Figure 4-5

4.1.3 Delete a profile

To delete an existing profile, highlight the profile name and click **Remove** on the bottom of the screen or press the Delete button on your keyboard. When the following figure appears, click **OK** to continue.

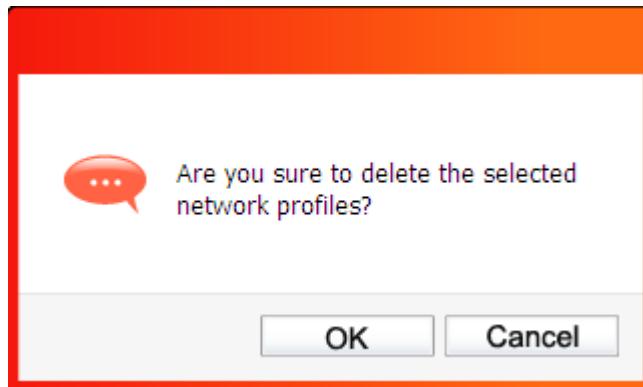


Figure 4-6

4.2 Advanced

The following configurations can be made on the **Advanced** page:

- 1) To select wireless configuration tool. (This option is available only in Windows XP.)

Here you can decide which tool to use, either the MERCUSYS Wireless Configuration Utility (MWCU) or the Windows wireless configuration tool. This option is available only in Windows XP.

- 2) To switch to another wireless network adapter.

Here you can switch to another adapter installed in your computer. The adapters successfully installed in your computer will be listed in the drop-down menu if the adapters are supported by this utility.

- 3) To switch to SoftAP mode.

Once enabled, the adapter will be able to work as an AP.

- 4) To change the power save mode. The default option is **OFF**.



Figure 4-7

4.3 About

The About screen gives you information about the Driver and Utility versions of the adapter. Right-click on the  icon in your system tray and select **About** from the list.



Figure 4-8

Chapter 5. AP Mode

In Soft AP mode, the adapter will work as an AP.

Suppose that only one computer in your house can access the Internet for various reasons like only one WLAN port is available on your wired broadband router, however, other wireless-capable devices also want to share the Internet. Then the adapter can be configured as an AP under the Soft AP mode, saving you the trouble of having to get a separate access point or a router.

With this feature, a computer can use a single physical wireless adapter to connect as a client to a hardware access point while at the same time acting as a software AP allowing other wireless-capable devices to connect to it.

To switch to this mode, right-click on the utility icon in your system tray and select **Switch to SoftAP mode**.

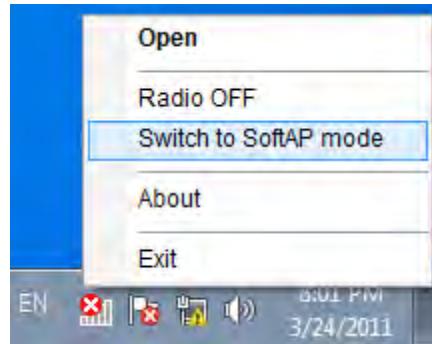


Figure 5-1

Or from the **Advanced** page of the utility, tick **ON** under the SoftAP mode as shown in the following figure. Click **OK** when prompted to confirm the setting.

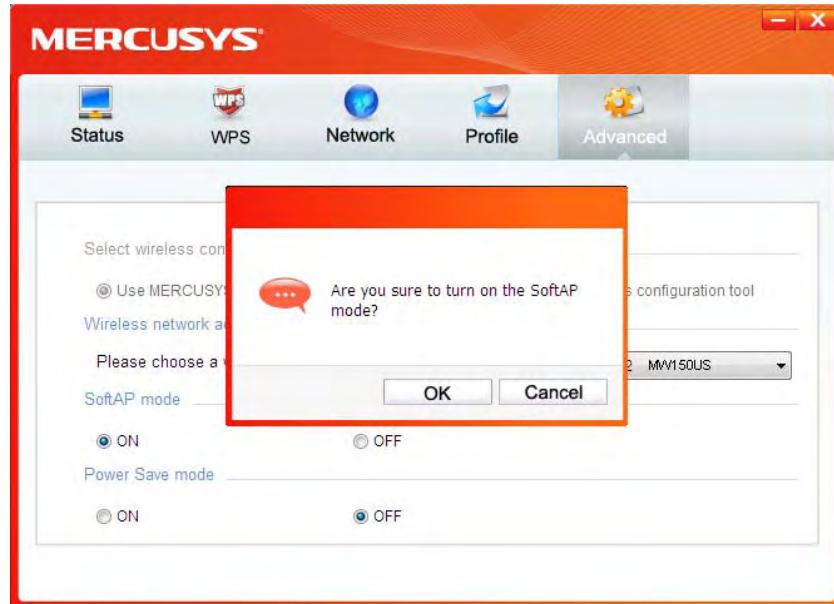


Figure 5-2

The **Soft AP** icon should then appear beside **Advanced** icon in the utility.



Figure 5-3

- **Soft AP mode:** Select to enable or disable the function.
- **Internet Connecting Share(ICS):** Specify a connection through which devices connected to your AP can access the Internet.
- **SSID:** Enter the name for your soft AP (for example, Jone) so that others can know which AP is yours when trying to connect to it. The default name (SSID) is "SoftAP".
- **Security Type:** The security type here is set to be WPA2-PSK which is based on 802.11i and uses Advanced Encryption Standard instead of TKIP. It was designed to improve the

Chapter 5 – AP Mode

security features of WEP. WPA2-PSK uses a passphrase or key to authenticate your wireless connection. You needn't make any configuration here.

- **Encryption Type:** The encryption type here is set to be AES.
- **Security Key:** Enter the Key in the field to make your AP security enabled. It is recommended that you specify another key instead of the default key 12345678. Only by entering the corresponding key can other computers establish a successful connection with your AP.
- **IP Address:** Here displays the IP address of the SoftAP.

Chapter 6.

Uninstall Software

6.1 Uninstall the utility software from your PC

1. On the Windows taskbar, click the **Start** button, click **All programs**→**MERCUSYS**, and then click **Uninstall-MERCUSYS Wireless Configuration Utility**.

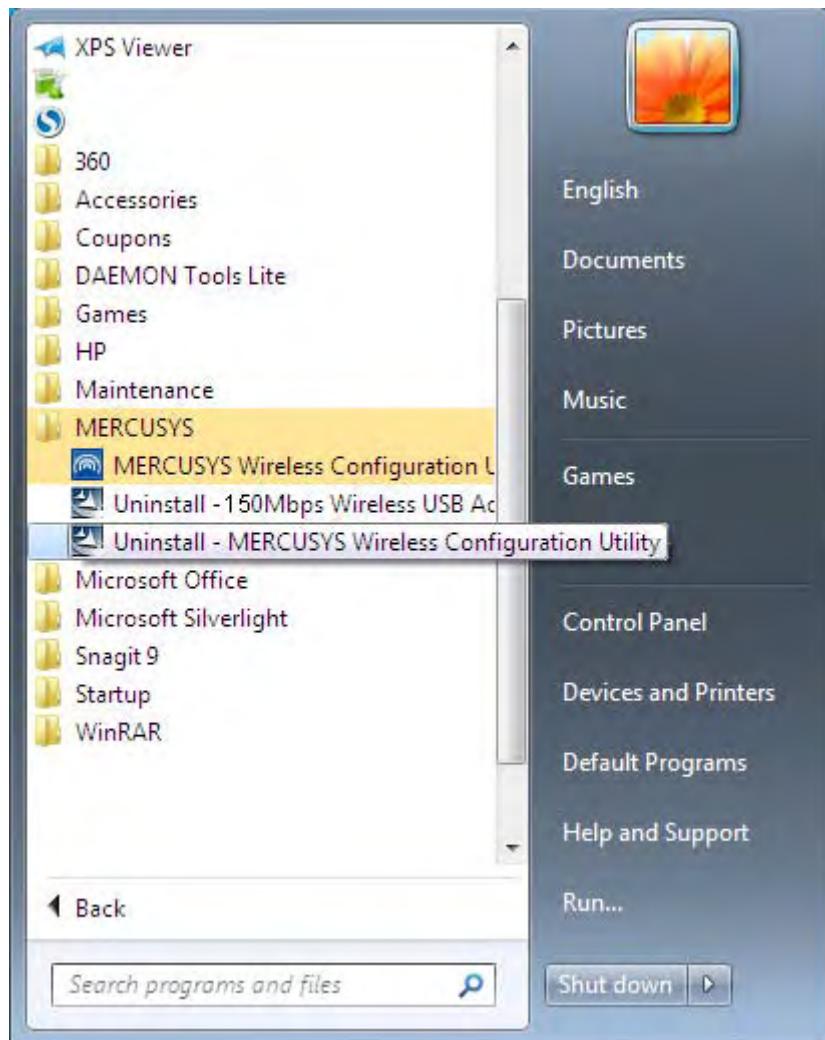


Figure 6-1 Uninstall Utility

2. Follow the Install Shield Wizard to uninstall the utility software from your PC.

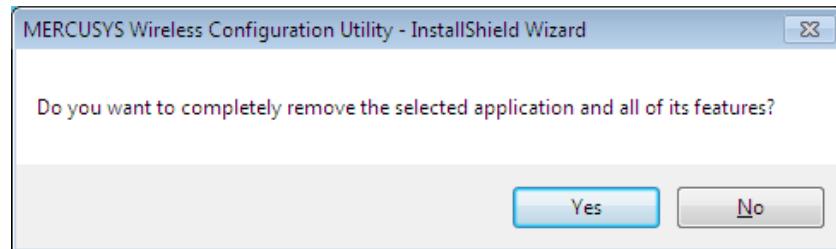


Figure 6-2

3. Click **Finish** when the figure below appears.

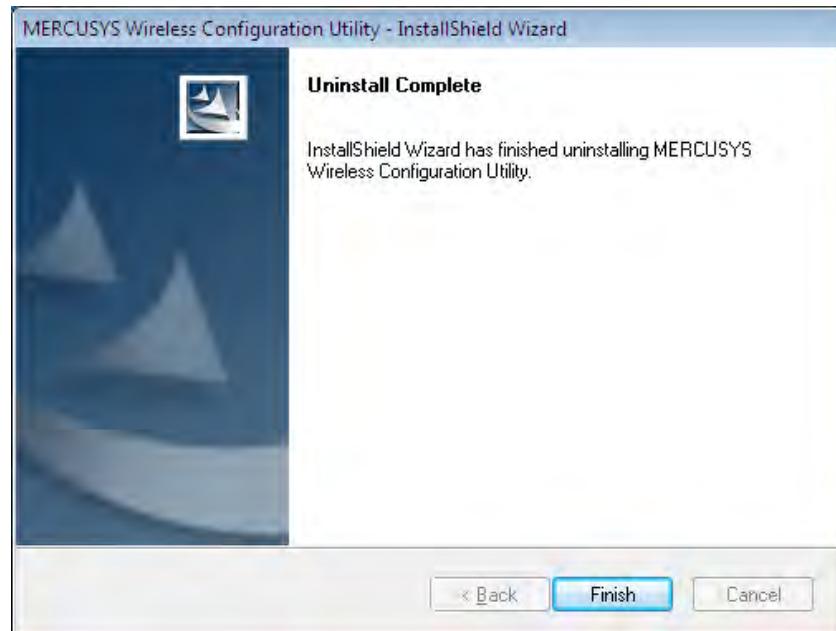


Figure 6-3

6.2 Uninstall the driver software from your PC

1. On the Windows taskbar, click the **Start** button, click **All programs**→**MERCUSYS**, and then click **Uninstall-150Mbps Wireless USB Adapter Driver**.

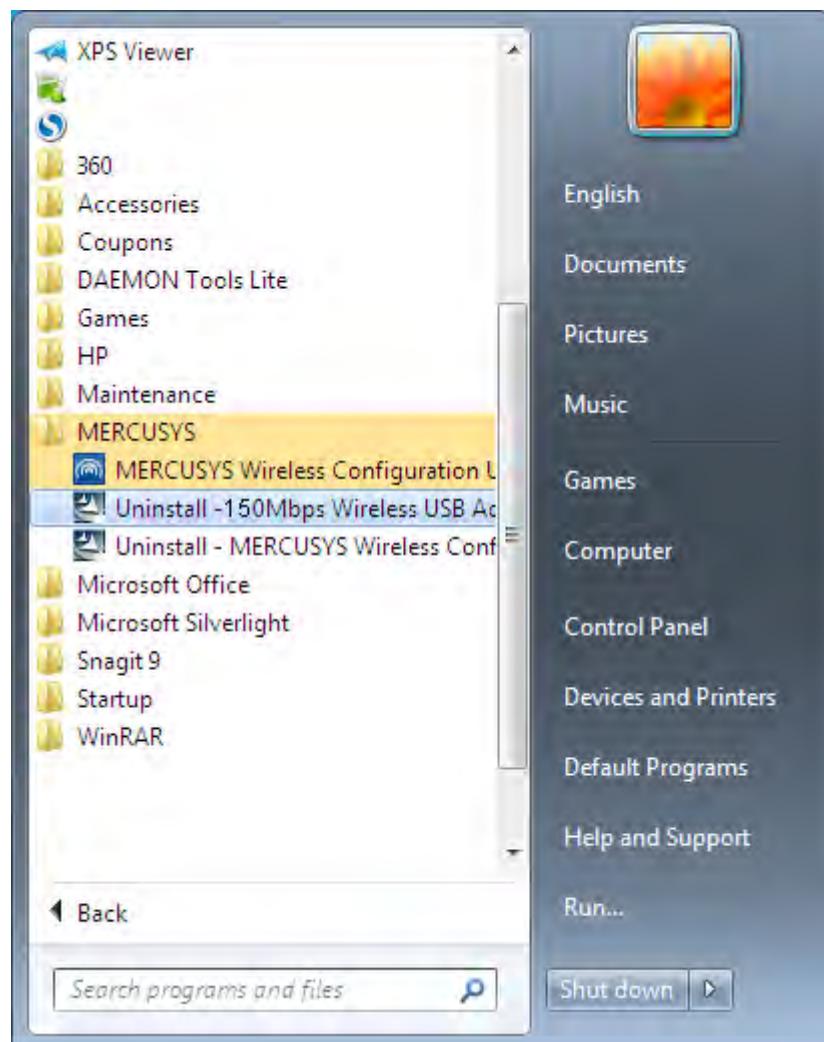


Figure 6-4 Uninstall Driver

2. Follow the Install Shield Wizard to uninstall the driver software from your PC.

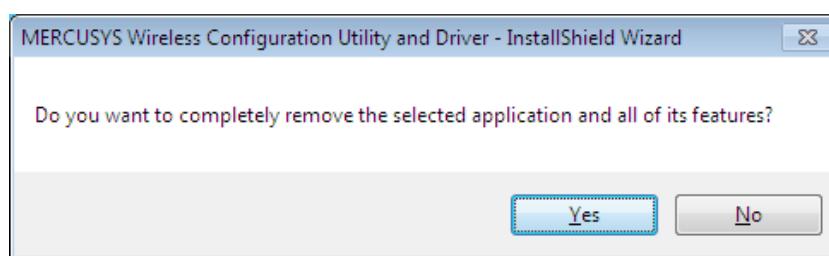


Figure 6-5

Chapter 6 – Uninstall Software

4. Click **Finish** when the figure below appears.

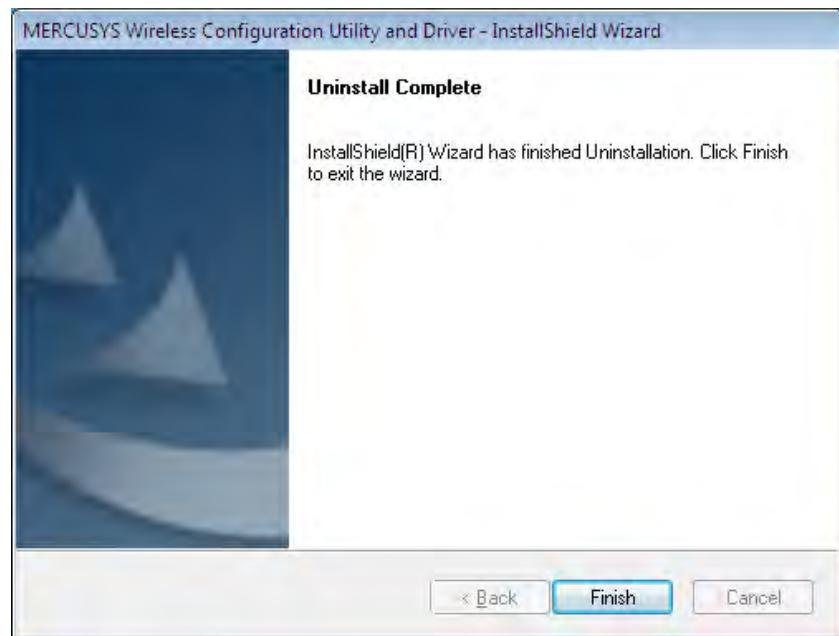


Figure 6-6

Appendix A: Specifications

Normal	
Interface	USB 2.0 Interface
Standards	IEEE802.11b; IEEE802.11g; IEEE802.11n
Operating System	Windows XP / Windows Vista / Windows 7
Radio Data Rate	11b: 1/2/5.5/11Mbps 11g: 6/9/12/18/24/36/48/54Mbps 11n: Up to 150Mbps
Modulation	11b: CCK,QPSK,BPSK; 11g: OFDM; 11n: QPSK, BPSK, 16-QAM, 64-QAM;
Media Access Protocol	CSMA/CA with ACK
Data Security	WPA/WPA2,WPA/WPA2,WPA-PSK/WPA2-PSK
Frequency	2.412 ~ 2.462GHz
Spread Spectrum	Direct Sequence Spread Spectrum (DSSS)
Safety & Emissions	FCC, CE

Environmental and Physical	
Operating Temperature	0°C~40°C (32°F~104°F)
Storage Temperature	-40°C~70°C (-40°F~158°F)
Working Humidity	10% - 90% RH, Non-condensing
Storage Humidity	5% - 90% RH, Non-condensing

* Only 2.412GHz~2.462GHz is allowed to be used in USA, which means only channel 1~11 is available for American users to choose.

Appendix B: Glossary

- **802.11b** - The 802.11b standard specifies a wireless product networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g** - specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **802.11n** - 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC)^[3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **Ad-hoc Network** - An ad-hoc network is a group of computers, each with a Wireless Adapter, connected as an independent 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.
- **DSSS - (Direct-Sequence Spread Spectrum)** - DSSS generates a redundant bit pattern for all data transmitted. This bit pattern is called a chip (or chipping code). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the receiver can recover the original data without the need of retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers. However, to an intended receiver (i.e. another wireless LAN endpoint), the DSSS signal is recognized as the only valid signal, and interference is inherently rejected (ignored).
- **FHSS - (Frequency Hopping Spread Spectrum)** - FHSS continuously changes (hops) the carrier frequency of a conventional carrier several times per second according to a pseudo-random set of channels. Because a fixed frequency is not used, and only the transmitter and receiver know the hop patterns, interception of FHSS is extremely difficult.
- **Infrastructure Network** - An infrastructure network is a group of computers or other devices, each with a Wireless Adapter, connected as an 802.11 wireless LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infrastructure wireless network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at a corporation scale, or when it is necessary to connect the wired and wireless networks.

Appendix B - Glossary

- **Spread Spectrum** - Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).
- **SSID** - A **Service Set Identification** is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. See *also* Wireless Network Name and ESSID.
- **WEP** - **(Wired Equivalent Privacy)** - A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.
- **Wi-Fi** - A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standards group promoting interoperability among 802.11b devices.
- **WLAN** - **(Wireless Local Area Network)** - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.
- **WPA** - **(Wi-Fi Protected Access)** - A wireless security protocol use TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. **MERCUSYS®** is a registered trademark of MERCUSYS TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from MERCUSYS TECHNOLOGIES CO., LTD. Copyright © 2013 MERCUSYS TECHNOLOGIES CO., LTD. All rights reserved.

<http://www.mercusys.com>