HT851W USERS GUIDE

Content

Safety Precautions

Read the safety precautions carefully to ensure the correct and safe use of your wireless device.

	Do not switch on your device when the device use is prohibited or when the device use may cause interference or danger.
	Follow the rules or regulations in hospitals and health care facilities. Switch off your device near medical apparatus.
	Switch off your device in an aircraft. The device may cause interference to control signals of the aircraft.
	Switch off your device near high-precision electronic devices. The device may affect the performance of these devices.
	Do not attempt to disassemble your device or its accessories. Only qualified personnel are allowed to service or repair the device.
	Do not place your device or its accessories in containers with strong electromagnetic field.
	Do not place magnetic storage media near your device. Radiation from the device may erase the information stored on them.
	Do not put your device in a high-temperature place or use it in a place with flammable gas such as a gas station.
	Keep your device and its accessories away from children. Do not allow children to use your device without guidance.
	Use approved batteries and chargers only to avoid explosion.
	Observe the laws or regulations on device use. Respect others' privacy and legal rights when using your device.

It is recommended that the equipment only be used in the environment where temperature is between 0℃ and 45℃ and humidity is between 10% to 90%. Keep the equipment in the environment where temperature is between 0℃ and 45℃ or humidity is between 10% to 90%.

1 Overview

HT851W is positioned as a terminal device that interconnects with wireless fix-line phone. It provides circuit switched voice service by through connect fix-line phone as well as integrated functions of router. The products are therefore offered high-speed Internet data access service for LAN/WLAN via wired/wireless WAN. Besides, the product also provides network sharing service via access to File Server and Printer server by USB. The products meet demands on both voice calling and Internet accessing in special situation such as in remote area, no access to fix-line network and temporary office.

1.1 Introduction
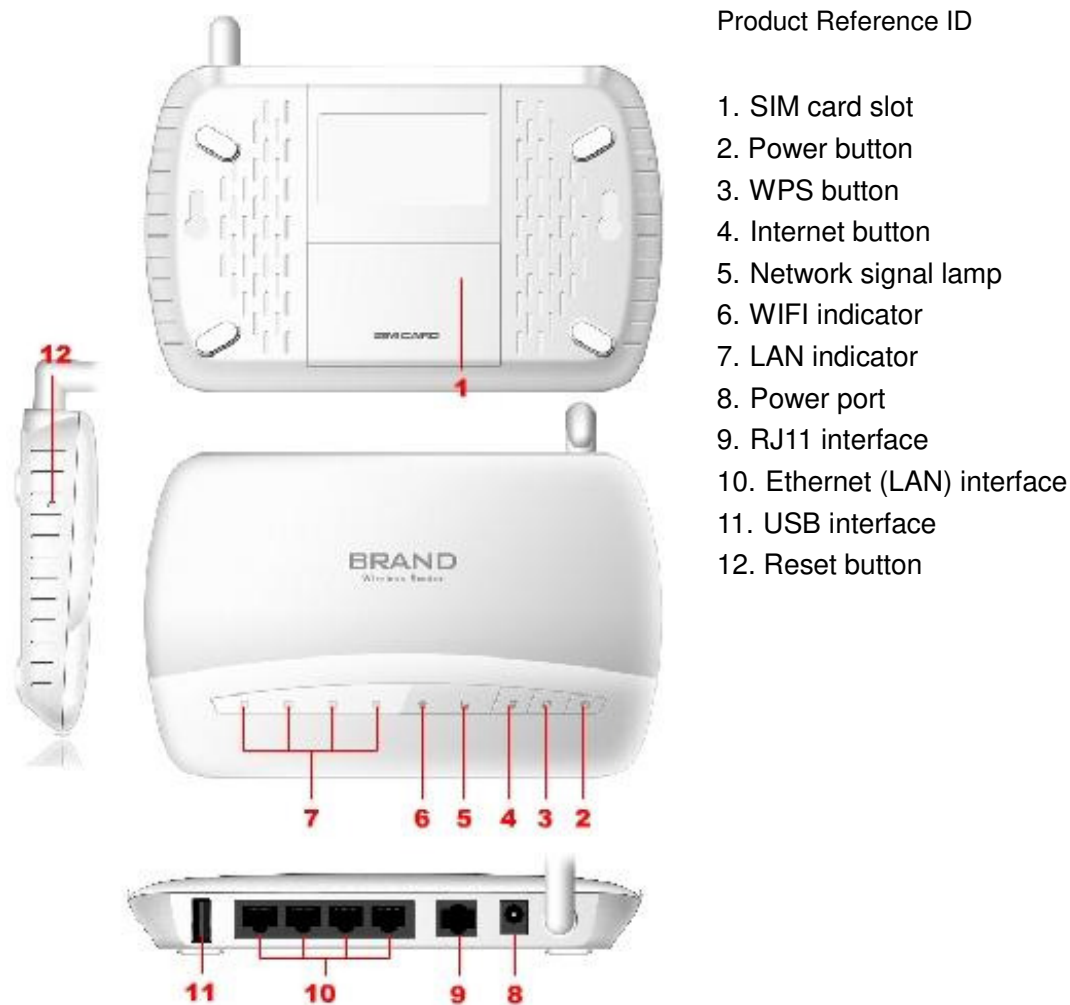
Product Reference ID

1. SIM card slot
2. Power button
3. WPS button
4. Internet button
5. Network signal lamp
6. WIFI indicator
7. LAN indicator
8. Power port
9. RJ11 interface
10. Ethernet (LAN) interface
11. USB interface
12. Reset button

Interface Specification

ITEM	INTRODUCTION
SIM card slot	Insert SIM card
Power button	Start-up/Shutdown device
WPS button	Establish/Disconnect WPS connection
Internet button	Connect/Disconnect Internet access
Network signal indicator	Indicate network connection status
WIFI indicator	Indicate WLAN connection status.
LAN indicator	Accessing LAN when LAN indicator is blinking
Power Interface	Connect power adapter
RJ11 interface	Connect voice device via phone line with RJ11 connector
Ethernet (LAN) interface	Connect PC or Laptop via Ethernet cable with RJ45 connector
USB interface	Connect USB Printer/USB stick
Reset button	Restore settings to factory default , restart router

1.2 System Requirements

Item		Description
Operating System	Windows	Windows7/VISTA/XP(SP2 and higher)
	Mac	X 10.4.9 or higher, but no higher than X10.6.0
Browser	Internet Explorer	6/7/8
	Safari	3/4/5

2 Device Installation

2.1 Hardware Installation

Before you want to use your device, please follow the quick steps below to power up your network:

1. Insert SIM card into SIM slot；

2. Connect Power adapter；

3. Hold the Power button to power on;

4. Connect FWT with your terminal device。

5. Four RJ45 connectors of the device are used to built wired LAN；

Alternative, user also can choose built-in 3G module connect to the Internet via 3G network。

Also，WIFI of HT851W can be used to build WLAN，RJ11connector can connect fix-line phone to provides voice service via Circuit Switched (CS) Domain。USB connector can be used to connect USB printer or USB stick to provides network print service and network store function。
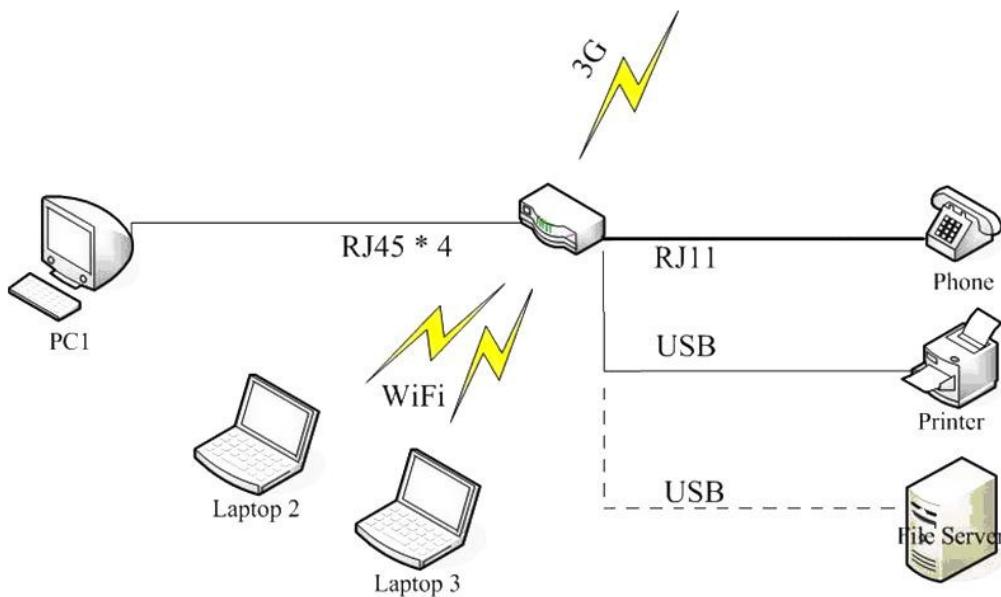
When 3G Only Internet connection is applied, the device is connected to the Internet through the built-in 3G Modem, All of the four RJ45 connectors will be used to build wired LAN network. At the same time, network sharing function can be achieved through WLAN for any terminal devices that support WiFi. Voice service is provided via CS domain by connect fix-line phone to

build-in RJ11 connector. USB connector is used to connect external USB printer or USB stick in order to provide network print and storage functions.

2.2 Startup

➢   Power up the device

    After all installation is complete, hold the power button over 2 second to power up the device.

➢   Restart the device

    Some configurations may take effect after system reboot. The device will reboot automatically once these configurations to be modified. After reboot the webpage will be automatically redirected to Homepage and need you to re-login for further changes。

➢   Shutdown the device

    Hold the power button over 2 second when the device is powered on, the device will automatically shutdown.

3 Quick Setup
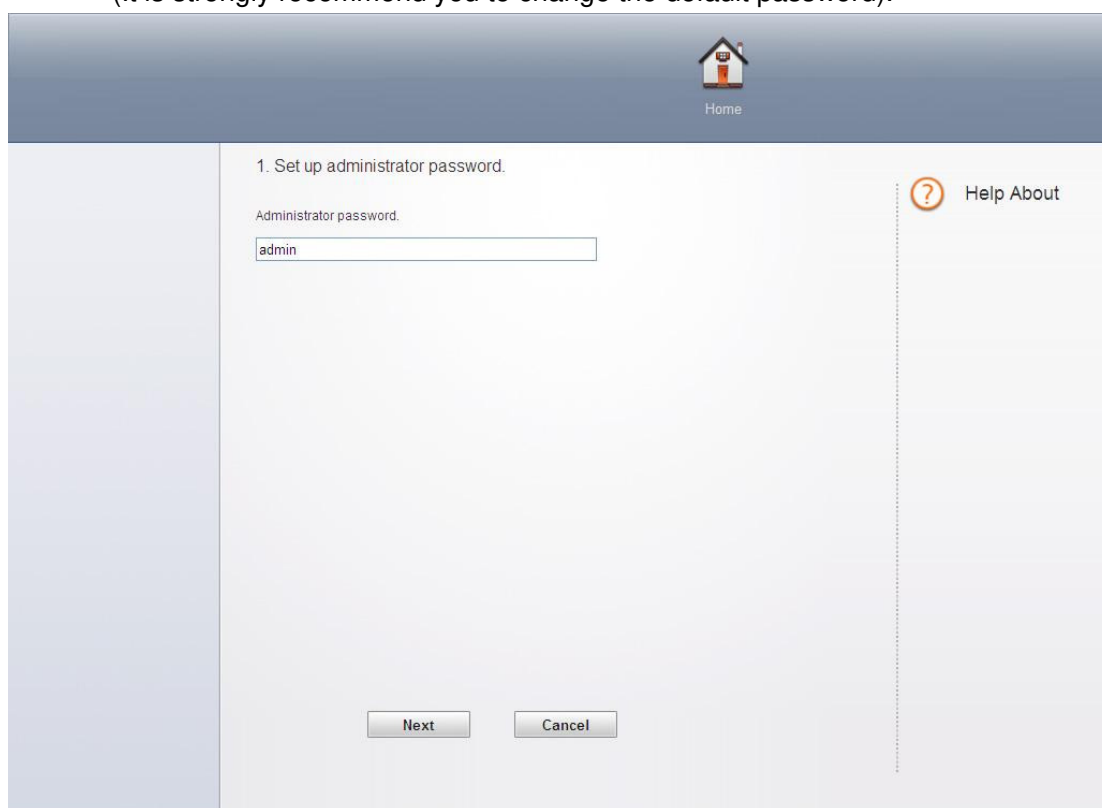
Use the instructions in this guide to help you connect the device, set it up, and configure it to work.

Login page

Open Web browser and enter "http：//192.168.100.1" into address bar then press Enter to access configuration page. If you are first time access to the configuration page, quick installation page is appeared to let you quickly and easily configure it to work. In these setup you can make follow configurations：

➢ Set your administrator password and press 'Next', the default password is 'admin'. (It is strongly recommend you to change the default password).

➢ Enter into APN configuration page，select Use the current APN and then press 'Next'.

> ➢ Enter into WIFI security configuration，you can modify network name(SSID) and security settings for WIFI, press 'Finish' once you finish quick setup guide.

In this part, 9 options in total include the first option 'None' are available to you to choose any one of them which you would like to use for. See in detail below:
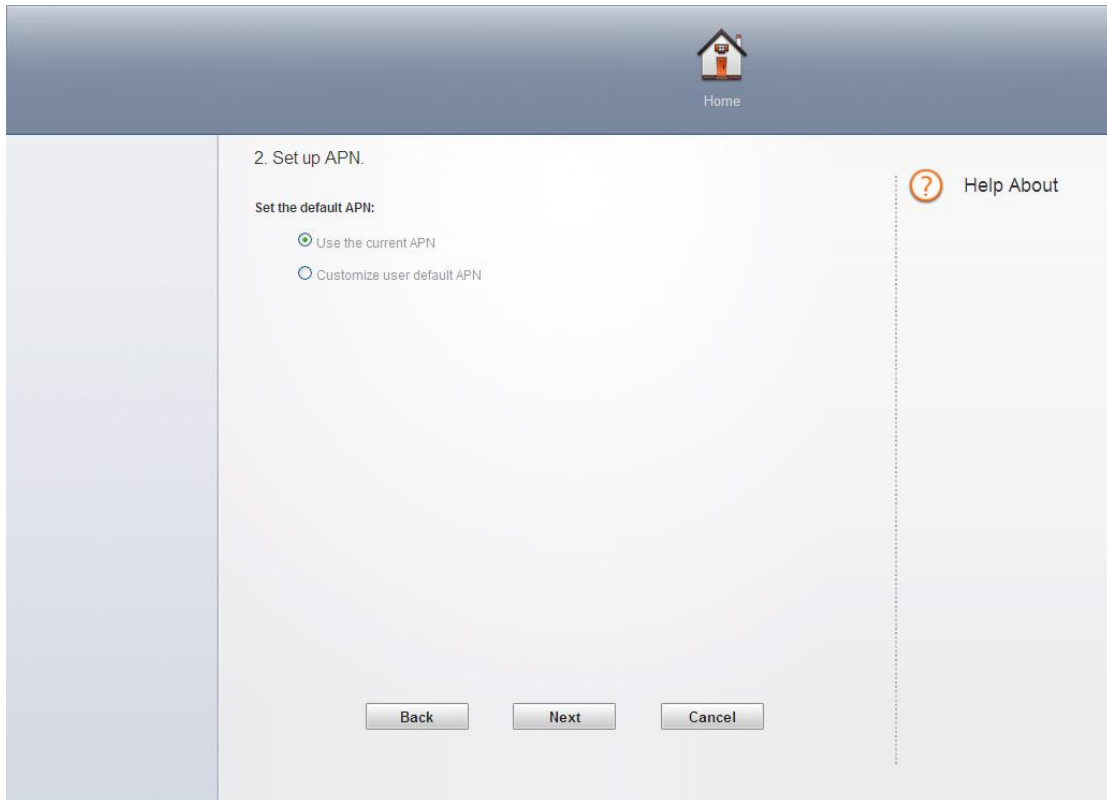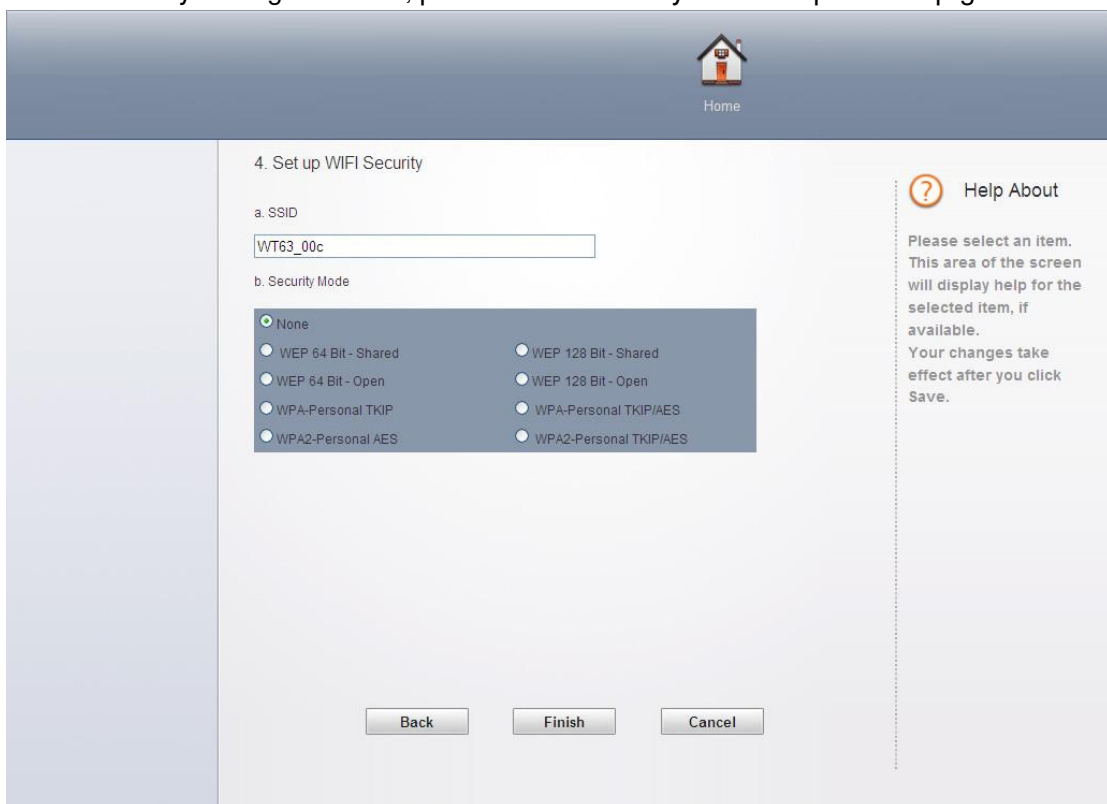
➢ **None:** Not security. It is not recommended since anyone can access your device and use your internet connection.

➢ **WEP 64 Bit - Shared**: Lower security. Works with older and newer Wi-Fi devices. Recommended only if your devices don't support WPA or WPA2. Shared WEP uses the same key for encryption and authentication which is considered to be less secure than open WEP. 10 HEX characters needed.

➢ **WEP 128 Bit - Shared**: Lower security. Works with older and newer Wi-Fi devices. Recommended only if your devices don't support WPA or WPA2. Shared WEP uses the same key for encryption and authentication which is considered to be less secure than open WEP. 26 HEX characters needed.

➢ **WEP 64 Bit - Open**: Lower security. Works with older and newer Wi-Fi devices. Recommended only if your devices don't support WPA or WPA2. Open WEP uses the key only for encryption. 10 HEX characters needed.

➢ **WEP 128 Bit - Open**: Lower security. Works with older and newer Wi-Fi devices. Recommended only if your devices don't support WPA or WPA2. Open WEP uses the key only for encryption. 26 HEX characters needed.

➢ **WPA - Personal TKIP**: A strong security standard, supported by most Wi-Fi devices. 8 to 63 ASCII characters needed.

➢ **WPA - Personal TKIP/AES**: A strong security standard, supported by most Wi-Fi devices. 8 to 63 ASCII characters needed.

➢ **WPA2 - Personal AES**: A stronger, newer security standard. Limited to newer Wi-Fi devices. 8 to 63 ASCII characters needed.

➢ **WPA2 - Personal TKIP/AES**: A stronger, newer security standard. Limited to newer Wi-Fi devices. 8 to 63 ASCII characters needed.

➢ **WPA/WPA2 - Personal**: Wi-Fi devices that use either WPA or WPA2 can connect to the device. Supported by most Wi-Fi devices. 8 to 63 ASCII characters needed.

The length of your Wi-Fi password depends on the type that you've selected. Please note, make sure that your password is not easy to guess.

4 Advanced Settings

Advanced settings help you to configure Internet connection, Wireless LAN, Router, System setting, Voice and USB device. After making some modification, you should click "Save" to save all the settings or you can select "Cancel" to give up the modification.

4.1 Internet setting

Make sure SIM has been inserted before you start internet settings.

Network Settings

In the part of Network settings, you can configure the network mode and network selection.

In "Network mode" setting, you should select the rule for registering the network. The default selection is "3G Preferred".

The default Network Selection mode is "Automatic". When click "Manual", a network list will be activated, containing all searched networks. Having selected an available network from the list, FWT will register to the selected network.

Connection Settings

In the part of connection settings, you can configure the connect mode and profile.

This device supports two ways to connect to the internet, "Auto" and "Dial Demand". You can modify the mode in connection settings part in Internet,

➢ If "Auto" is selected, the automatic connection will be applied after reboot or input the Card again.
➢ If "Dial Demand" is selected, it will not connect to network until it detects the connection from LAN or Wi-Fi. And the device will disconnect automatically when there is no connection in a period of time (10 minutes default) after connecting.

And in the profile list, you will see the default and other APN configuration. An APN (Access Point Name) is a reference to the Internet access point on. Different APNs for the 2G and 3G networks may be required.

You can select other APN as default, edit or delete exist ones or create a new APN configuration (no more than 10 in the list).

Set the profile name, APN, username and password and select Auth. Type when you want to create a new APN profile .

Note: only input what you have received from your service provider and leave other fields empty.

PIN LOCK

You can lock the SIM with PIN to protect the device against unauthorized use and unlock it. The default PIN and PUK are provided by the operator or service provider. The current PIN status and the rest chances to input PIN and PUK are displayed in this page.

The old PIN is needed if you want to unlock SIM or set a new PIN. Select "Lock" and click "Save" button when you don't want to use the PIN.

Note: The PUK (an 8-digit code) is required when PIN is input incorrectly 3 times. If the PUK is wrongly input for continuously 10 times, the card will be damaged. Please contact the network service provider for details.

4.2 Wireless LAN settings

WLAN settings

This part allow you to turn on/off Wi-Fi; select Wireless Interface, set network name (SSID), Regulatory Domain, Wi-Fi Channel and enable/disable SSID Broadcast。

➢ **Wi-Fi Connection**: Enable Wi-Fi connection and select wireless interface (type of wireless) to connect to your network firstly if you want to use this function.

➢ **Wireless Interface**: Select "802.11g only" which can give you faster Wi-Fi speeds when you confirm all of the Wi-Fi devices that will be connected to your device support 802.11g, otherwise, select "802.11b/g compatible".

➢ **SSID**: This name is visible to other Wi-Fi-enabled devices, and is used to identify your Wi-Fi network. The length of the SSID must be 1-32 characters long including "_".

➢ **Regulatory Domain**: Select the domain for the Wi-Fi access point.

➢ **Channel**: Different domain has different channels. If your network has problems (possibly caused by other Wi-Fi networks in the vicinity using the same channel), change to another one.

➢ **SSID Broadcast**: Disable SSID broadcast in the access point or device to secure Wi-Fi detected as a "cloaked" network.

Advanced settings contain Beacon Period, RTS threshold and Fragmentation.

➢ **Beacon Period**: Beacon Period is the frequency of broadcast packets from the device which is used to synchronize wireless networks. Set lower value for finding and connecting to the device fast when higher value helps to save power.

➢ **RTS Threshold**: RTS Threshold is the maximum packet size (in bytes) that RTS/CTS (Request to Send/Clear to Send) handshaking is used for.

➢ **Fragmentation:** Fragmentation is the maximum packet size (in bytes). When exceed this, it will be fragmented into multiple packets before transmitted.

   Note: Change this value only if you're experiencing inconsistent data flow. Make only minor changes to this value.

Security

This part helps you configure the security of the wireless network.

Select an encryption mode in the list and set your password. If you select "None", any Wi-Fi-enabled device can connect with the WLAN without the password.

➢ **None:**   Not security. It is not recommended since anyone can access your device and use your internet connection.

➢ **WEP 64 Bit - Shared**: Lower security. Works with older and newer Wi-Fi devices. Recommended only if your devices don't support WPA or WPA2. Shared WEP uses the same key for encryption and authentication which is considered to be less secure than open WEP. 10 HEX characters needed.

➢ **WEP 128 Bit - Shared**: Lower security. Works with older and newer Wi-Fi devices. Recommended only if your devices don't support WPA or WPA2. Shared WEP uses the same key for encryption and authentication which is considered to be less secure than open WEP. 26 HEX characters needed.

➢ **WEP 64 Bit - Open**: Lower security. Works with older and newer Wi-Fi devices. Recommended only if your devices don't support WPA or WPA2. Open WEP uses the key only for encryption. 10 HEX characters needed.

➢ **WEP 128 Bit - Open**: Lower security. Works with older and newer Wi-Fi devices. Recommended only if your devices don't support WPA or WPA2. Open WEP uses the key only for encryption. 26 HEX characters needed.

➢ **WPA - Personal TKIP**: A strong security standard, supported by most Wi-Fi devices. 8 to 63 ASCII characters needed.

➢ **WPA - Personal TKIP/AES**: A strong security standard, supported by most Wi-Fi devices. 8 to 63 ASCII characters needed.

➢ **WPA2 - Personal AES**: A stronger, newer security standard. Limited to newer Wi-Fi devices. 8 to 63 ASCII characters needed.

➢ **WPA2 - Personal TKIP/AES**: A stronger, newer security standard. Limited to newer Wi-Fi devices. 8 to 63 ASCII characters needed.

> **WPA/WPA2 - Personal**: Wi-Fi devices that use either WPA or WPA2 can connect to the device. Supported by most Wi-Fi devices. 8 to 63 ASCII characters needed.

The length of your Wi-Fi password depends on the type that you've selected.
Note: make sure that your password is not easy to guess.

MAC Filtering

MAC filtering is used to control specific MAC addresses to access.

> **No filtering**: All terminal devices are allowed to access the router via WIFI
> **Allow all in list**: Only devices in this list are allowed to access the router via WIFI
> **Block all in list**: All terminal devices are allowed to access the router via WIFI except ones in this list.

You can select to add new configuration in the list (no more than 10), edit or delete exist ones.

WPS

WPS (Wi-Fi Protected Setup) provide a more intuitive way of wireless configuration between your device and the wireless client. Please make sure that the Wi-Fi-enabled devices you want to connect support this function.

Enable WPS firstly before you want to use it.
    If you select the "PIN" way, input the client's PIN to the "Client PIN" frame.
If you select the "PBC" way, press the "WPS" button on wireless device in 120 seconds to establish WPS connection after you have pressed the "Wi-Fi/WPS" button on your device or clicked "Save".

Click "Save" to save your settings and start connecting when you select PIN or PBC way. You can also choose "No Connection" and click "Save" to save your settings without connecting.

4.3 Router Settings

LAN Settings

This part helps you set your internal network for the device which contains Router IP Address, Subnet Mask, Hostname, DHCP Server, DHCP IP Pool, and DHCP Lease Time.

> **Router IP Address**: The router's IP address on the LAN. The default setting is

"192.168.100.1".

➢ **Subnet Mask**: The router's internal LAN subnet mask. The default setting is "255.255.255.0".

➢ **Hostname**: User can access the device directly via entering the hostname in the address bar of the browser.

➢ **DHCP Server**: DHCP Server will automatically assign IP addresses to devices on the network. The default setting is "Enable".

➢ **DHCP IP Pool**: Set a range of IP addresses available to access.

➢ **DHCP Lease Time**: Amount of time that a Wi-Fi-enabled device can use its assigned IP address before it is required to renew the lease.

Static DHCP

With DHCP, IP addresses are assigned dynamically; devices typically don't have a permanent IP address. But sometimes you may want to assign a static IP address to a device, while still using DHCP for the rest of the devices on your network.
You may want to do this with, for example, a Web server, FTP server, media server.

➢ **Hostname**: the name of the device that you want to assign IP Address to.

➢ **MAC Address**: the MAC Address of the device that you want to assign IP Address to.

➢ **IP Address**: input the permanent IP Address that you want to assign to the device.

You can determine to enable it or not, and can also add new client and edit or delete existing ones.

IP Filtering

IP filtering is used to control specific IP addresses to access.

➢ Select "No Filtering" to disable this function.

➢ Select "Block all in the list" to deny IP addresses that you have set in the IP filtering list to access.

You can select to add new configuration in the list (no more than 10), edit or delete exist ones.

MAC Filter

MAC Filter function is applied to allow/deny specified computers in WLAN have permission to access WAN so that any WLAN users can access to the Internet via router under permission.

➢ Select "No Filtering" to disable this function.
➢ Select "Allow all in list" to allow all the devices in this list have permission to access the Internet via router
➢ Select "Block all in list" to deny all the devices to access the Internet via router
You can select to add new configuration in the list (no more than 10), edit or delete exist ones.

URL Filtering

URL filtering is used to control devices on the LAN access to specific URLs.

➢ Select "No Filtering" to disable this function.
➢ Select "Block all in the list" to deny all devices in the LAN to access the URLs that you have set in the URL filtering list.
You can select to add new configuration in the list (no more than 10), edit or delete exist ones.

Device List

The Device List lists the information about the device in the LAN including IP address, host name, MAC address and connect mode.

Port Forward

Port Forward is used to forward incoming traffic to specific ports or Internet addresses on your network.
Port Trigger
In computer network, an application makes connection to external computer by use specific port(trigger port), router forward external connection to internal port as you specified (trigger port)。

DMZ (Demilitarized Zone)

DMZ is a physical or logical sub-network that contains an organization's external services to a larger untrusted network, usually the Internet.
DDNS(Dynamic DNS)
DDNS (Dynamic DNS) is a service that maps Internet domain names to IP addresses. DDNS serves a similar purpose to DNS: DDNS allows anyone hosting a Web or FTP server to advertise a public name to prospective users.
VPN (Virtual Private Network)
A VPN is a virtual computer network which established a communication tunnel for two or more intranets over the existing network through a special encryption communication protocol.

Static Routing

Static Routing helps network administrator to manually configure routing information.

4.4 System setting

Basic settings

This part helps you configure System Language, Change Password and Firmware Upgrade

➢ **Change Password**: Input the new password; confirm it and click "Save" to finish the settings.
➢ **Language Select**: Select the language that you want to see during using the configuration.
➢ **Firmware Update**: Select the firmware file in your PC first and click "Update". It will update automatically. Please wait while the upgrade occurs; this may take several minutes.

Note: During installation of the update, do not turn off or unplug the device. And Your Wi-Fi and Internet connections won't be available.

System Log

In this page contains system log information .

➢ Click "Download" to download the log information to the local PC.
➢ Click "Refresh" to update the log information.
➢ Click "Clear" to delete all the log information.

Configuration

This part helps you Reset to factory default settings, Backup Settings or Restore Settings.

➢ Click "Reset" to reset the configuration to the factory settings.
➢ Click "Backup" to back up the configuration file to the local PC.
Click "Restore" to restore the settings from the configuration file backed up in the local PC.

Restart
➢ **Click "Restart" to reboot the device.**

4.5 Voice settings

The device provides one RJ11 connector to connect fix-line phone in order to offer voice service based on CS domain.

Call settings

DTMF and FSK selection

There are two kind of information transmission modes for display of incoming call：DTMF and FSK。User can choose the specific information transmission mode according to their own country or region.

Note：we recommend that please keep the distance over 1.5 meters between the device and external telephone or fax in order to avoid signal interference in voice quality made by device.

4.6 USB Device Applications

Display property information of plugged USB device via USB cable

USB device is connected printers

    If you want to connect a USB printer with WT6309, connect the printer to the USB device port, and then add the printer to your PC as the following steps (the example is shown on windows XP OS):
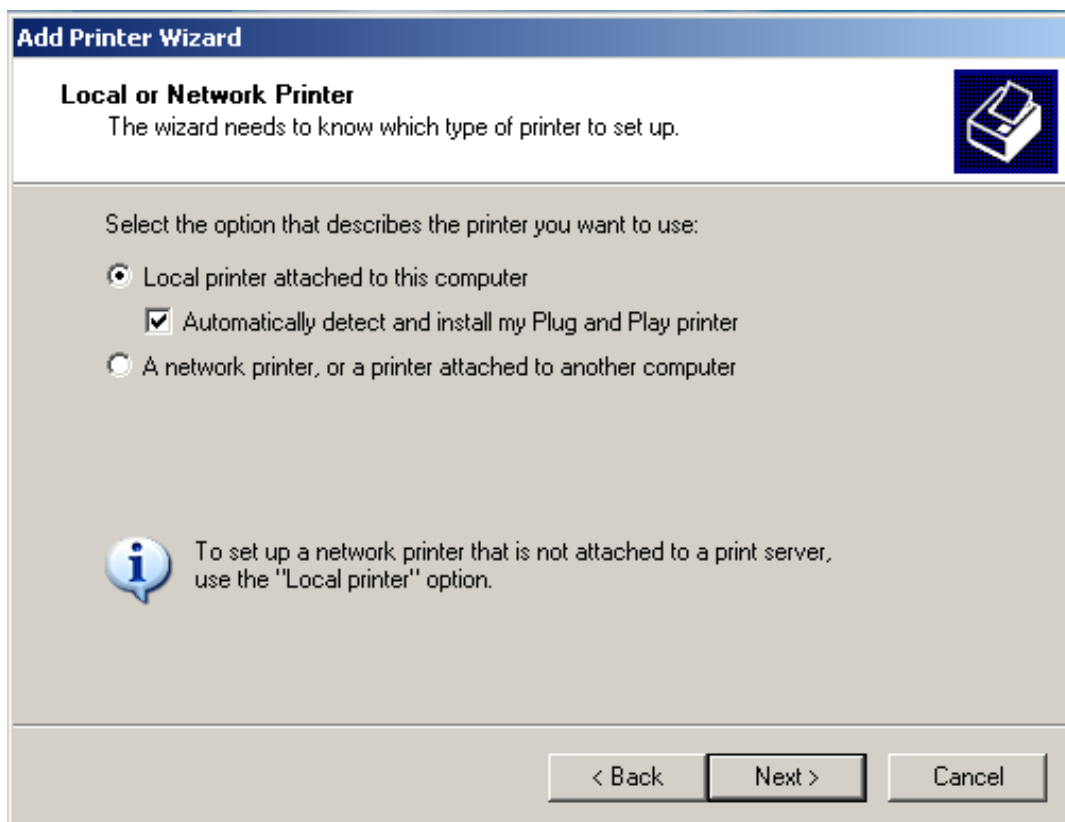
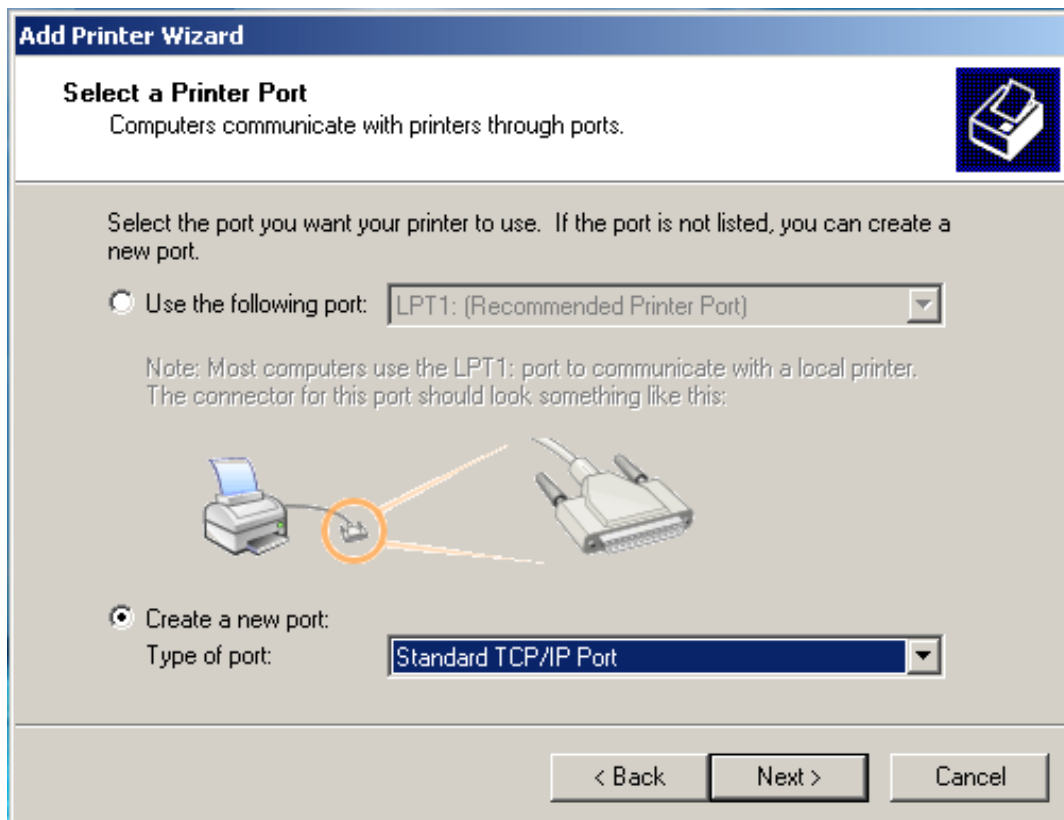➢   Enter the "Control Panel", and select "Printers and Faxes"
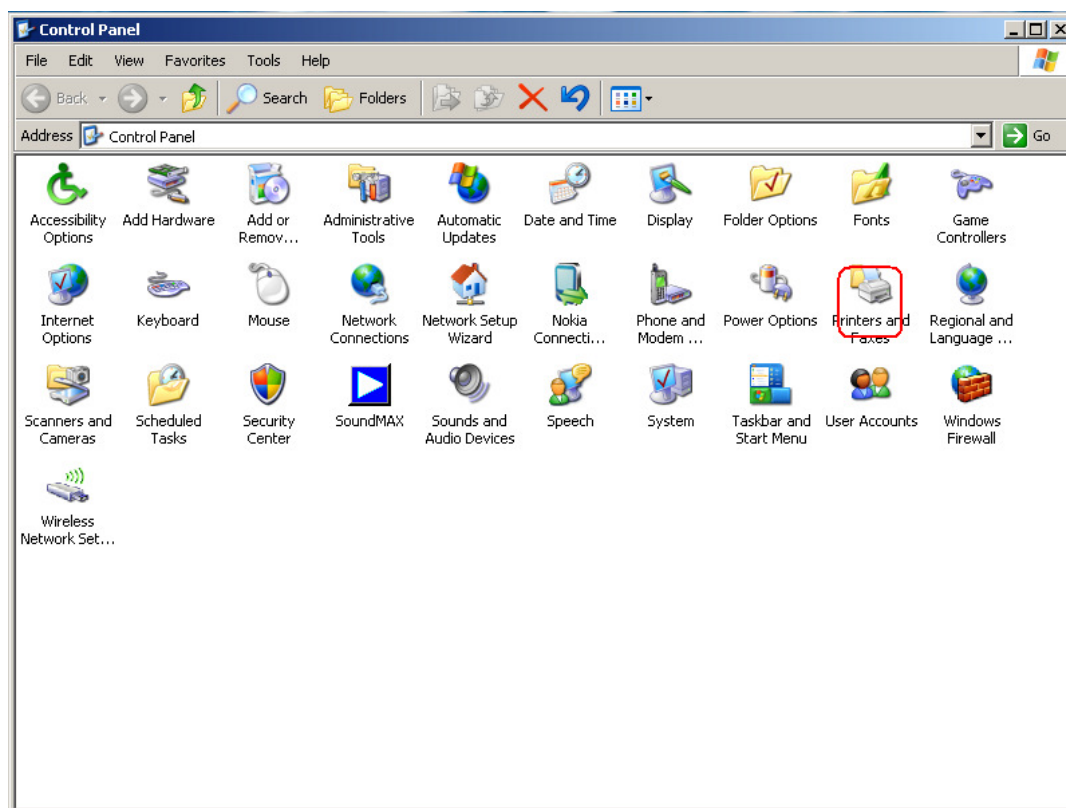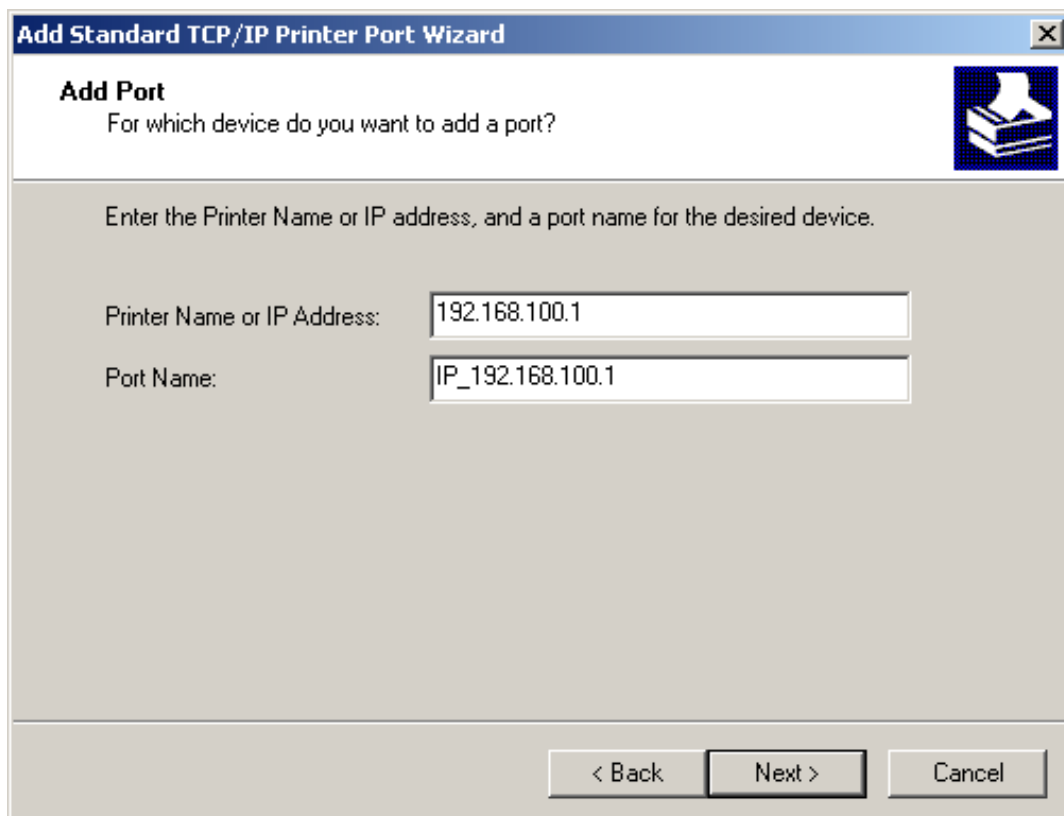

➢   Select the "Add a printer" and click "Next"
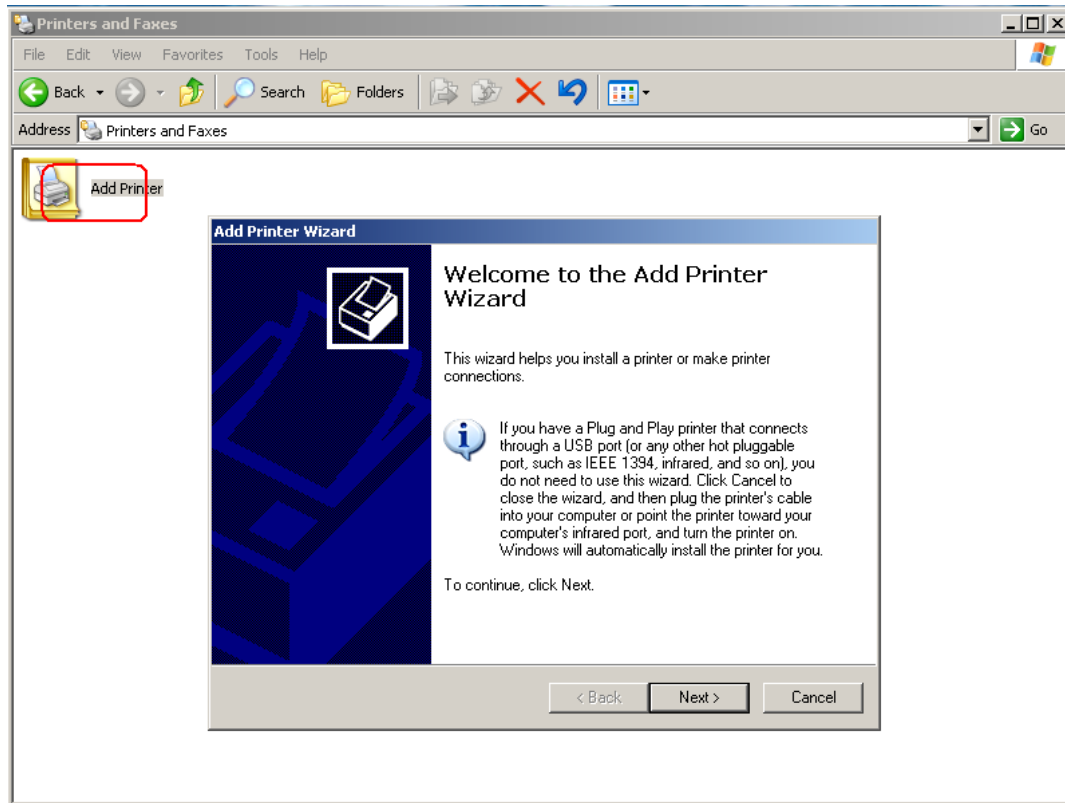
➢ Select "Add a local printer" and click "Next"

> Select "Create a new port"→"Standard TCP/IP Port" and click "Next"

> Input "192.168.100.1" into "Printer Name or IP address". Then click the "Next".

➢ Select "Custom", click "Settings"

➢ Set the settings like what is shown in following picture, and then click "OK"

Select the right vendor and the right type of printer you used. In this example, we use the HP LaserJet 3055 form HP. Then click "Next".
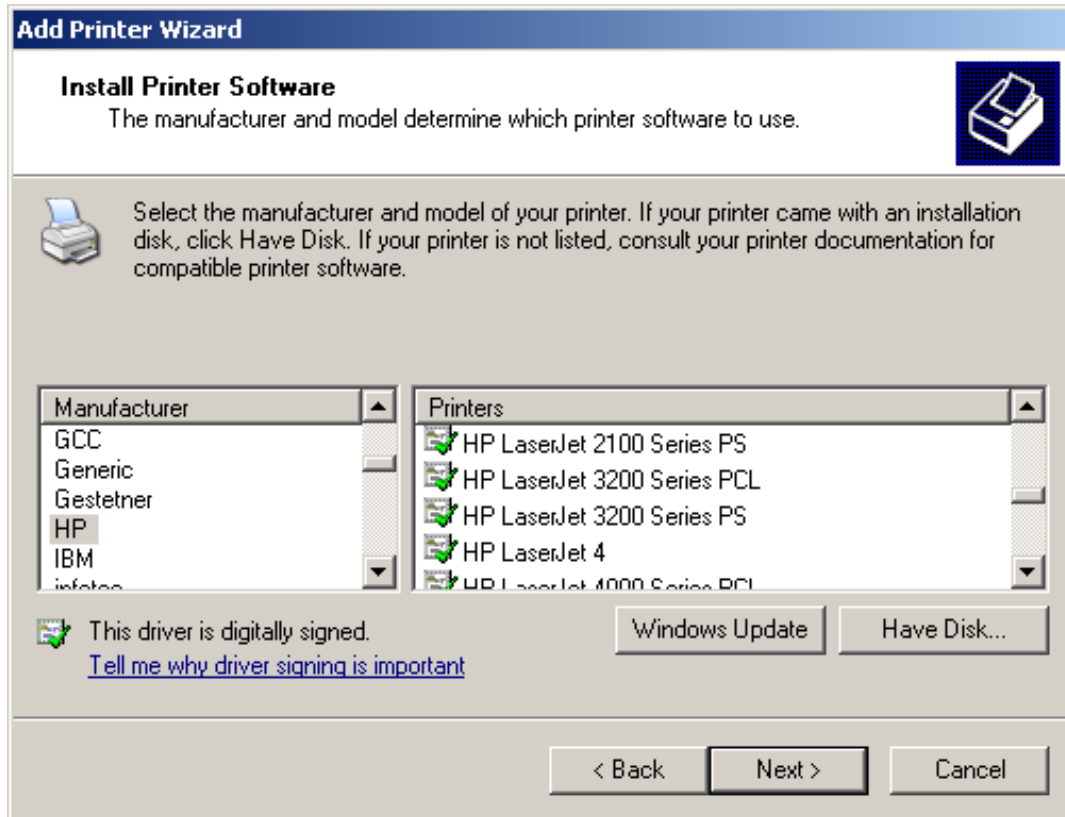
➢ Follow the windows guide until finish.

5 Warning and Precautions

Electronic Device

Turn off your device near high-precision electronic devices. The wireless device may affect the performance of these devices. Such devices include hearing aids, pacemakers, fire alarm system, automatic gates, and other automatic devices can be affected. If you are using an electronic medical device, consult the device manufacturer to confirm whether the radio wave affects the operation of this device.

Hospital

Pay attention to the following points in hospitals or health care facilities:

➢ Do not take your wireless device into the operating room, intensive care unit, or coronary care unit.

➢ Do not use your wireless device at places for medical treatment where wireless device use is prohibited.

Storage Environment

➢ Do not place magnetic storage media such as magnetic cards and floppy disks near the wireless device. Radiation from the wireless device may erase the information stored on them.

➢ Do not put your wireless device and other accessories in containers with strong magnetic field, such as an induction cooker and a microwave oven. Otherwise, circuit failure, fire, or explosion may occur.

➢ Do not leave your wireless device in a very hot or cold place. Otherwise, malfunction of the products, fire, or explosion may occur.

➢ Do not subject your wireless device to serious collision or shock. Otherwise, wireless device malfunction, overheat, fire, or explosion may occur.

Children Safety

➢ Put your wireless device in places beyond the reach of children. Do not allow children to use the wireless device without guidance.

➢ Do not allow children to put the device in mouth.

➢ Do not allow children to touch the small fittings. Otherwise, suffocation or gullet jam can be caused if children swallow the small fittings.

Operating Environment

➢ The wireless device is not water-resistant. Keep it dry. Protect the wireless device from water or vapor. Do not touch the wireless device with a wet hand. Otherwise, short-circuit and malfunction of the product or electric shock may occur.

➢ Do not use the wireless device in dusty, damp and dirty places or places with magnetic field. Otherwise, malfunction of the circuit may occur.

➢ On a thunder stormy day, do not use your wireless device outdoors.

23

➢ The wireless device may interfere with nearby TV sets, radio and PCs.

➢ In accordance with international standards for radio frequency and radiation, use wireless device accessories approved by the manufacturer only.

Cleaning and Maintenance

➢ Before you clean or maintain the wireless device, turn off it and disconnect it from the power. Otherwise, electric shock or short-circuit may occur.

➢ Do not use any chemical detergent, powder, or other chemical agent (such as alcohol and benzene) to clean the device. Otherwise, part damage or a fire can be caused. You can clean the device with a piece of soft antistatic cloth that is a little wet.

➢ Do not scratch the shell of the wireless device. Otherwise, the shed coating may cause skin allergy. Once it happens, stop using the device at once and go to see a doctor.

➢ If the wireless device or any of its fittings does not work, turn to the local authorize service center for help.

FCC Regulations:

●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.

●This device 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 radiated 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.

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

●The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

‣ RF Exposure Information

This device meets the government's requirements for exposure to radio waves.

This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government.

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment, In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm(8 inches) during normal operation.