

3G ROUER USER GUIDE



PO Box 561

Hull

East Yorkshire

HU9 9JZ

08458620226

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°C and 50°C and humidity is between 10% to 90%. Keep the equipment in the environment where temperature is between -10°C and 70°C or humidity is between 10% to 90%.

Content

Safety Precautions	1
1. Overview	3
1.1 Introduction	3
1.2 System Requirements	5
2. Quick Start	6
2.1 Connect the Device	6
2.2 Basic Tasks	7
3. Quick Setup	10
4. Advanced Settings	12
4.1 Wireless LAN Settings	12
4.2 Internet Settings	14
4.3 Router Settings	15
4.4 NAT Settings	16
4.5 Application	17
4.6 System Settings	18
5 Warning and Precautions	19

1. Overview

3G Hotspot provides a simple way to use 3G connect to the Internet with any Wi-Fi-enabled device and to fulfill needs of sharing your internet connection during outside home.

1.1 Introduction

Indicator Description

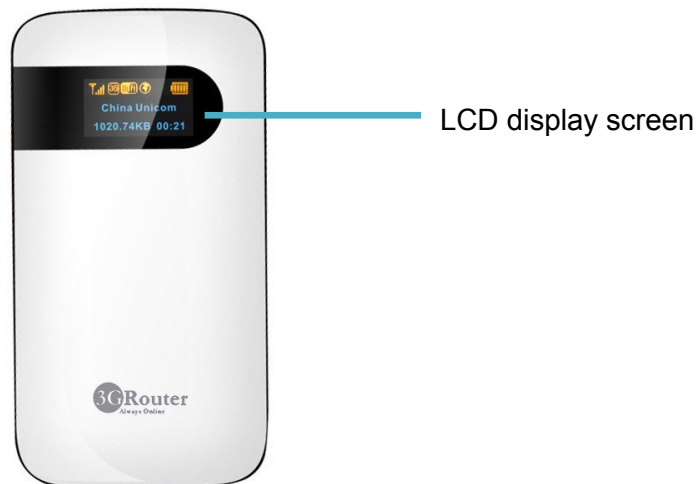


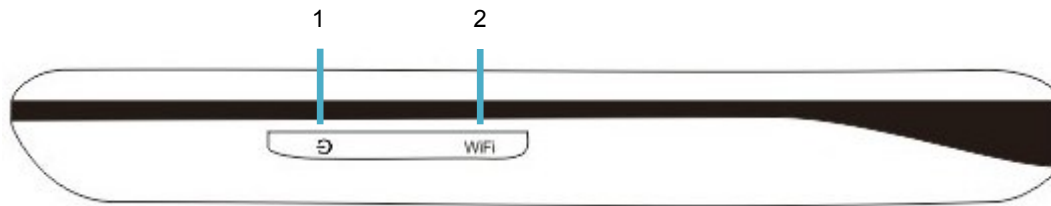
Fig 1.1

LCD Status Information

Category	Icon Display
Signal Strength	 From no signal to excellent signal
Network Status	 2G Connected  UMTS Connected
Data Connection	 Network is connected
User	  the number of Wi-Fi users
Battery	     Battery status
Others	  Power adapter only

Button Description

➤ Right side



➤ Left side

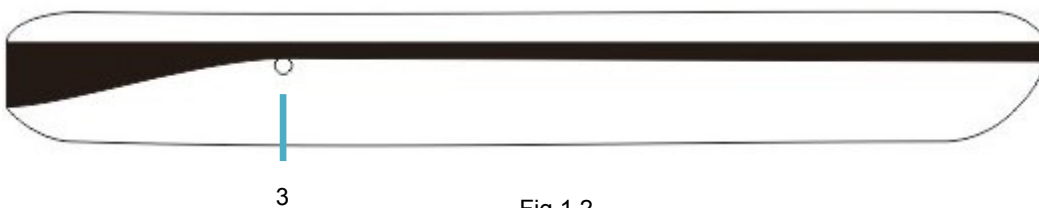


Fig 1.2

1. Power

- Press and hold the power button more than 2 seconds to power on/off.

2. WiFi

Turn on/off WPS.

- When Wi-Fi is on, press and hold for about Four seconds until the LCD display to activate the WPS.

3. Reset

- Long press(more than 3 seconds)reset button to restore factory settings.

Connector Description

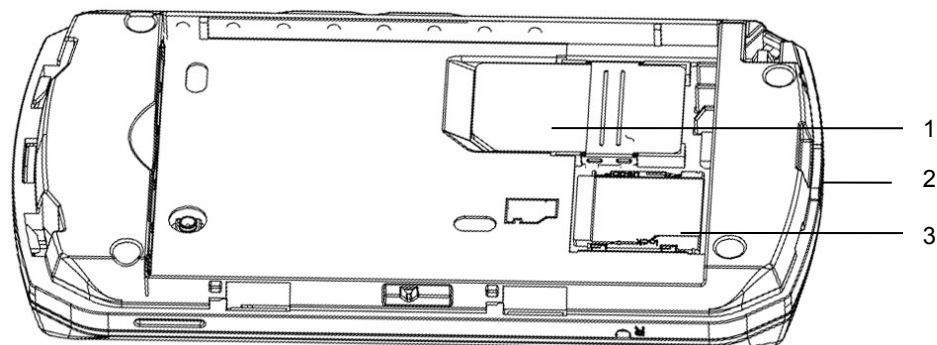


Fig 1.3

1. SIM Slot

A SIM can be inserted for connecting to the network.

2. Micro USB Connector

A terminal device can be connected via USB cable.

3. Micro SD Slot

A MicroSD card (maximum 16G supported) can be inserted for file transfer or storage. Please do as the following to insert them (Fig 1.4).

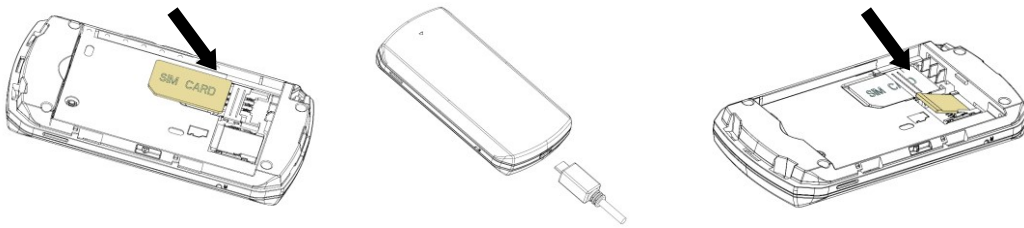


Fig 1.4

1.2 System Requirements

- CPU: Pentium 500MHz or above.
- Hard Disk: 50MB available space.
- Operating System: Windows7/VISTA/XP (SP2 and above), Mac OS X 10.4.9 and Later, Up to X10.6.0.
- Display Resolving Power: 800 × 600 pixels or above (1024 × 768 is recommended).
- Interface: Standard USB 2.0 interface.
- Web Browser: Internet Explorer 6/7/8, Safari3/4/5.
- One or more computing devices that support Wi-Fi (802.11b/g).

2. Quick Start

2.1 Connect the Device

Before you want to use the device, setup your device as following:

1. Insert SIM;
2. Insert MicroSD Card;
3. Insert the battery;
4. Hold the Power/Connect button to power on;
5. Connect this device to your terminal device.

If you want to go to internet, manage LAN, connect your terminal device to 3G Hotspot via USB or Wi-Fi:

- **Via USB:** If your terminal device (such as desktop) is Wi-Fi disabled, you can connect them via USB cable. After connected in the first time, driver will be installed automatically.
- **Via Wi-Fi:** It is better for you to connect the device to Wi-Fi-enabled devices through Wi-Fi, for which you don't need to install any driver.
-

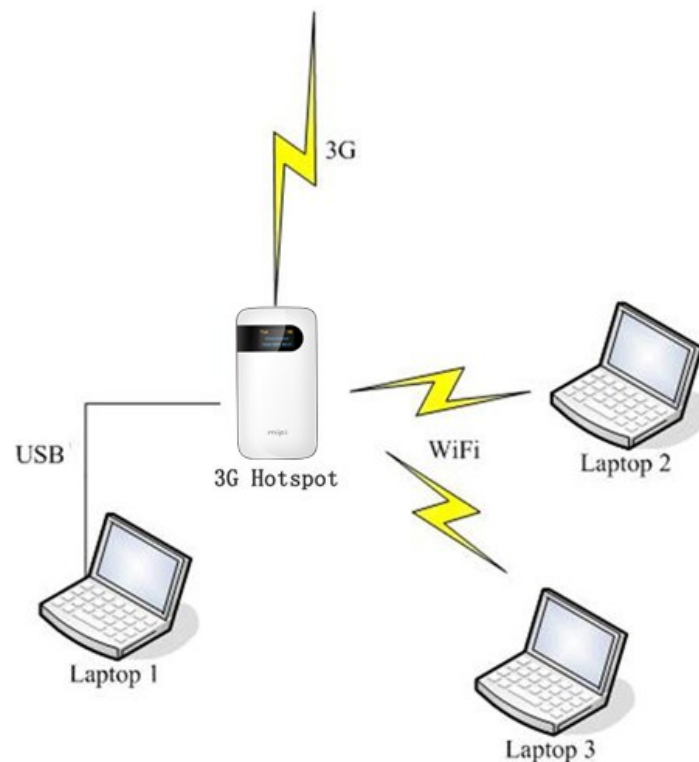


Fig 2.1

Note:

- If the computer's CDROM doesn't run automatically after the device has been connected with computer via USB cable and the driver has been installed into computer, you are therefore have to double click shortcut 'Swich Tool for 3G Hotspot' on Desktop have to be double clicked in order to let computer to be able to access Internet by use of device via USB cable.
- If automatic installation failed, please check whether the antivirus and security software is working. If it is, close it and reinstall.

2.2 Basic Tasks

Power On

Press and hold the power button more than 2 seconds.

If within thirty seconds, the device does not do any key operation, equipment to enter the 'Sleeping Mode'

Press any button or do some operation in the web UI to exit the sleeping mode.

Sleeping Mode

If you select “Auto” in “Power-Saving mode setting” (**Advanced Settings – System – Basic Settings**), when there is no data transmission (Internet, Wi-Fi, LAN containing), it will turn Sleeping Mode automatically.

When the device is in Sleeping Mode, the 3G modem radios, the Wi-Fi radio are off, and the LCD display will turn off. It works only when battery is live.

Log in to the Configuration Page

1. Open the browser, and then input the address <http://192.168.1.1>. The first time you do this after driver installed, a welcome page will display from which you have 3 choices as following (Fig 2.2.1):

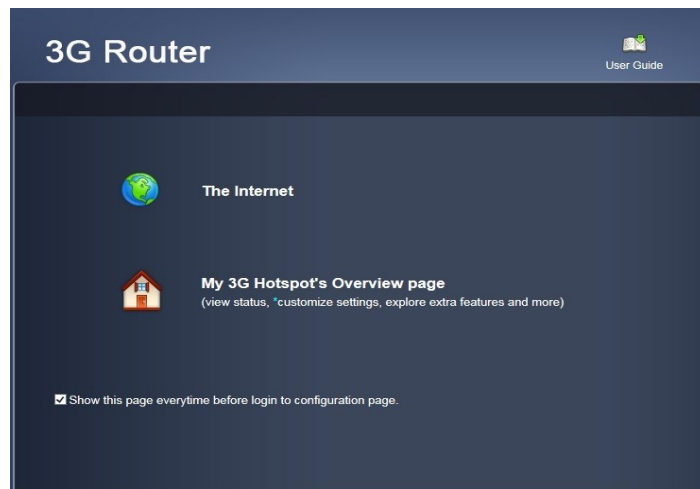


Fig 2.2.1

- **The Internet.** You will go to the internet directly without any setting modification.
- **My 3G Hotspot's Overview page.** Enter the configuration home page to view status, customize settings or explore extra features.

2. If you select the second option to the welcome page, you can overview the status of devices (Fig 2.2.2) in the home page. After login, you can go to advanced settings page to set the device, or go to admin setup.



Fig 2.2.2

Status Information

Category	Icon Display
Signal Strength	 From no signal to excellent
Connection Status	 Not Connected  WCDMA Unconnected  WCDMA Connected  UMTS Unconnected  UMTS Connected  HSUPA Unconnected  HSUPA Connected  GPRS Unconnected  GPRS Connected
Roaming or not	 Roaming On  Roaming Off 
User	 User number
MicroSD Card	 SD Security  SD Insecurity  SD Error  SD Disabled  SD Enabled  SD Card not detected
Battery	     Battery level from critical to full
Data Transmission	 No Transmission  Transmission
Others	 USB charging complete  Charged  Charging complete

Table 2.2

Restart

The device will restart and go back to home page automatically after some settings modification. And you need to re-log in.

Power Off

Press and hold the power button more than 2 seconds to power off the device.

3. Quick Setup

To quick setup your network, make sure you have logged in; the default password is “password”. Click “Admin Setup” to quick set your device after log in .

And you can do settings as following:

- **Create an administrator:** This password is used to log in to the home page, where you can view and customize your device settings. Your administrator password must be 1–20 characters long. If you forget this password, you need to reset the device to its default settings.
- **Name your Wi-Fi network (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 “_”.
Default SSID:3G_Router
- **Set up Wi-Fi security:** Select a security type and create a password for it. The recommended setting is WPA. Anyone can access your device and use your Internet connection if you disable this function.
Default Wi-Fi password:00000000
- **WPS:** Enable WPS (Wi-Fi Protected Setup) to set up Wi-Fi network and password automatically.

If you want to see all security types, click the link and you will find there are totally 10 options for you to choose in the Wi-Fi security type, the options are:

- **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.

After finish the setup, click "Submit" to save and apply all the settings, close pop dialogue and back to original interface. After reconnected to the network, click "Click here" and start to use .

4. Advanced Settings

Advanced settings help you to configure Wi-Fi, Internet, Router, NAT and System. 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 Wireless LAN Settings

WLAN Settings

Make sure SIM has been inserted before you start settings. And you can turn on/off Wi-Fi; select Wireless Interface, set SSID, Regulatory Domain, Channel, Max Number of Users and enable/disable SSID Broadcast in WLAN Settings.

- **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 (Channel 1~11 in FCC (US)/IC (Canada); Channel 1~13 in ETSI (Europe); Channel 1~13 in MKK (Japan)). If your network has problems (possibly caused by other Wi-Fi networks in the vicinity using the same channel), change to another one.
- **Max Number of Users:** Set the maximum number of Wi-Fi users. If your network has problems, you may want to decrease the number of Wi-Fi users allowed to connect to the device. The default and maximum value is “4”.
- **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 and Data Rate.

- **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.
- **Data Rate:** There are different options when you select different Wireless Interface. 802.11b Only: Auto, 1, 2, 5.5, and 11Mbps; 802.11g Only: Auto, 6, 9, 12, 18, 24, 36, 48, and 54Mbps; 802.11b/g Compatible: All above. Default setting is "Auto".

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.

MAC Filtering

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

- **No filtering:** All terminal devices are allowed to access the network.
- **Allow all in list:** Only devices in this list are allowed to access the network.
- **Block all in list:** All terminal devices are allowed to access the network 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.

4.2 Internet Settings

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 "Automatic".

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, 3G Hotspot 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 "Auto", "Manual" and "Dial Demand" way to connect to the internet. 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 "Manual" is selected, you can control the connection via clicking "Connect/Disconnect" in the home page.
- 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.

4.3 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 “192.168.1.1”.
- **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.

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.

4.4 NAT Settings

Application Settings

This part helps you configure UPnP .

- **UPnP:** UPnP (Universal Plug and Play) provides connectivity among consumer

electronics, intelligent appliances and mobile devices from many different vendors.

Note: When not required, it should be disabled since they may cause security risk.

4.5 Application

Sharing Settings

This product supports to share file via WEB browser.

Users can choose two sharing models,

- Web Share mode
- USB Access Only

Please make sure that your SD card is proper inserted into the card slot on the device.

Sharing

You can view the status information of SD card, while browsing the local file and create folders.

Upload a single file to the current directory of SD card, because the browser limitations, file name and share path does not exceed 150 characters.

Maximum size of uploaded file is 1.9G. But you can also upload files which larger than 1.9G under the USB mode.

SMS

This page provides you to manage SMSs which stored in both PC and (U)SIM.

Device: Display the contents of 'Inbox', 'Outbox' and 'Draft' stored in memory of the device. User can add, edit, delete, forward, send and other functions by click icon buttons on configuration page.

(U)SIM: Display the contents of 'Inbox' and 'Outbox' stored in (U) SIM card. Users can add, edit, delete, forward, send and other functions by click icon buttons on configuration page.

Settings: SMS center number setting and message storage location selection.

The device is able to automatically identify SMS center number from the (U) SIM card you used. You can also manually change this setting. Please contact with your service provider or network operator for detail of SMS center number.

Contacts

This page provides you to manage contact information which stored in both PC and (U)SIM.

Device: Display contact information stored in memory of the device. Users can add, edit, delete, search and other functions by click icon buttons on configuration page.

(U)SIM: Display contact information stored in (U) SIM card. Users can add, edit, delete, search and other functions by click icon buttons on configuration page.

Note:

The contact information can not to be recovered when deleted.

4.6 System Settings

Basic Settings

This part helps you configure System Language, Power-saving Mode, Change Password.

- **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.
- **Power-Saving Mode (Sleeping Mode):** When the device is in Sleeping Mode, the 3G modem radios, the Wi-Fi radio are off, and the power button is yellow and breathing. If you select "Auto", when there is no data transmission (Internet, Wi-Fi, LAN containing) in a time, it will turn into Sleeping Mode automatically. Selection "Off" to disable this function.

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.

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.

- 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.