D100 Wi-Fi/LAN Adapter

User Guide

Wonderful Communication, Mobile Life.

Welcome to D100 Wi-Fi/LAN Adapter

D100 Wi-Fi/LAN Adapter

User Guide

Notice

Copyright © 2008 Huawei Technologies Co., Ltd.

All Rights Reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks

and HUAWEI are trademarks of Huawei Technologies Co., Ltd. All other trademarks and trade names mentioned in this manual are the property of their respective holders.

Notice

The information in this manual is subject to change without notice. Every effort has been made in the preparation of this manual to ensure accuracy of the contents, but all statements, information, and recommendations in this manual do not constitute the warranty of any kind, expressed or implied.

Huawei Technologies Co., Ltd.

Address:

Administration Building, Huawei Technologies Co., Ltd., Bantian, Longgang District, Shenzhen, P. R. China

Postal Code: 518129

Website: http://www.huawei.com

Safety Precautions

Read the safety precautions carefully to ensure the correct and safe use of your wireless device. For detailed information, see "Warnings and Precautions."

Do not switch on your device when the device use is prohibited or when the device use may cause interference or danger.

Do not use your device while driving.

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 accessories only to avoid explosion.

Observe the laws or regulations on device use. Respect others' privacy and legal rights when using your device.

Table of Contents

Table of Contents 1

Quick Start 1

- Appearance 1
- Installation 1
- Viewing the Running Status 2
- Dial-up Access 3
- Restoring the Factory Defaults 3

Using the Management Page 4

- Log in to the Management Page 4
- Management Page Overview 4
- View Configuration Information 5
- Quick Setup 5
- Access the Internet 7

Configuring Your Computer 8

- Wireless Configuration 8
- Configuring the PC Network 9

Advanced Settings 10

- Overview 10
- System Management 10
- SIM/UIM Settings 11
- Mobile Network Settings 12
- Dial-up Settings 13
- DHCP Settings 14
- WLAN Settings 15

Security Settings (Optional) 19

- Firewall Switch 19
- LAN MAC Filter 19
- LAN IP Filter 19
- Virtual Server 20
- DMZ Settings 22
- UPnP Settings 22
- Remote Management 22

Troubleshooting 24

Safety Information 27

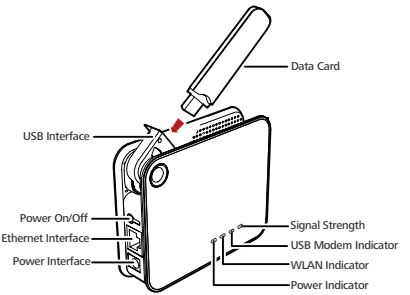
- Interference 27
- Medical Device 27
- Area with Inflammables and Explosives . 27
- Traffic Security 27
- Safety of Children 28
- Environment Protection 28
- WEEE Approval 28
- RoHS Approval 28
- Laws and Regulations bservance 28
- Care and Maintenance 28
- Emergency Call 29
- Body Worn Operation 29
- Regulatory Information 29

Abbreviations 31

1 Quick Start

Note The supported functions and displayed appearance are subject to your product purchased. Pictures are posted for illustration purpose only. Please refer to the product for actual appearance. For details of your product selection, consult your service provider.

Appearance



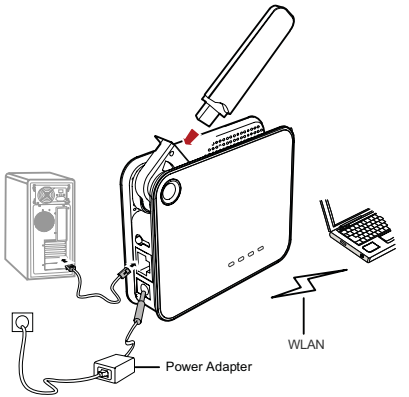
Installation

Step 1: Connect with the data card through the USB interface.

Note Use the specified data card to connect with the device.

Step 2: Connect to a PC through an Ethernet cable or WLAN.

- If the indicator of the Ethernet interface connecting with a network cable is on, the PC lineate connection is successful. The Ethernet cable cannot be longer than 100 meters (328 feet). To achieve better effect, use the shielded cable.
- Whether the PC wireless connection is successful, please check your PC connected through WLAN. For details, please see “Configuring Your Computer”.
- If connect your device to one PC with the Ethernet cable and other PCs with WLAN simultaneously, you have constructed a LAN and can share the local resources.



Step 3: Connect with the power adapter.

Warning

- To avoid electrical devices from interfering by the wireless signal, place electrical devices one meter away from the device.
- Do not put the data card in the slot and please turn the USB interface connected with the data card upright when the device is running.

The device can be placed horizontally or vertically on a table. Place the device on a higher place or near the window, so it can receive stronger signals.

Step 4: Power On/Off.

Press the **Power** key to switch on the device; press and hold the **Power** key to switch off the device.

Viewing the Running Status

Indicator	Status
Power	Steady on and in yellow green: the device is switched on successfully.
Modem	Steady on and in yellow green: the data card is connected successfully.

Indicator	Status
Signal	• Steady on and in yellow green: signal strength is strong; • Blinking in yellow green: signal strength is weak; • Off: the card does not exist or the PIN code is not verified or the signal is inexistent.
WLAN	• Steady on and in yellow green: WLAN is enabled; • Blinking in yellow green: data is transmitting.

Dial-up Access

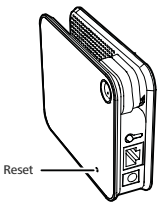
By default, the device dials up to access the Internet as required. You can directly use the network services such as web browsing, and receiving or sending emails.

If you need to configure the other device-related parameters, you need to access the device management page (http://192.168.1.1). For details, please see the following chapters.

Note Make sure that the data card is connected to the device, or else you cannot use the Internet service and some management pages are unavailable.

Restoring the Factory Defaults

If you need to reconstruct the network or you forget the changes of some parameters, you can choose to restore factory defaults and reconfigure the device.



Reset: Press and hold it to restore the factory defaults.

Note After this operation, all configurations are restored to the defaults.

2 Using the Management Page

Log in to the Management Page

1 Start the Internet browser and enter the address http://192.168.1.1 in the address bar.

2 Select a user type, enter the password, and then click Login.

- **Admin**: This user type is authorized to view and change the configurations. The default password is **admin**.
- **User**: This user type is authorized to view only the basic status information. The default password is **user**.

Note To avoid the configuration conflict, only one user is allowed to log in to the management page at a time.

Management Page Overview

Operation Functions

The following table shows the main operations in the management page.

Item	Description
Basic Status	Displays the parameter configuration status of the device.
Quick Setup	Quickly configures the device.
Connection	Displays the network connection status and connects to the network.
Advanced Settings	Configures the advanced settings.
Security (Optional)	Configures the security settings.
Logout	Log out of the management page.

Device Status

The following table shows the status information of the device.

Item	Green icon	Red icon
SIM/UIM	The card is valid.	The card is not inserted or is invalid.
WAN	The PPP dial-up connection is established.	The PPP dial-up connection is not established.

Item	Green icon	Red icon
WCDMA	The WCDMA network is available.	The WCDMA network is unavailable.
	Note If the device is registered with other network modes, the corresponding network connection status is displayed.	
SIG	The signal strength from weak to strong is shown as follows:	

View Configuration Information

On the configuration page, you can view the current parameter configuration information and the network connection status.

1. Click **Basic Status**.
2. Click **Advanced** on the right part of the page to view the advanced status.
3. Click **Refresh** to view the current status on the advanced status page.

Quick Setup

You can use the quick setup wizard to configure and maintain the basic parameters of the device. Click **Quick Setup** to access the welcome page. Click **Next** to configure the PPP profile settings.

Configuring PPP Profile Settings

- **Profile Name**: Enter a profile name when the text box is empty.
- **Dial-up Number/PPP User Name/PPP Password**: Enter these three parameters provided by the internet service provider (ISP). The dial-up number is used to initiate the network call; the PPP user name and PPP password is used to obtain the service authorization provided by the ISP.
- **APN/IP Address**: Select the mode for obtaining the access point name (APN) and IP address. If the carrier provides the relevant parameters, select **Static** and enter their values. Otherwise, select **Dynamic** and the device automatically obtains them.

Configuring PPP Dial-up Settings

PPP Connection: Select the dial-up access mode.

- **Auto**: The device automatically connects to the Internet and does not disconnect when no data is transmitted.

- **On Demand**: The device automatically connects to the Internet when data transmission exists. When the duration of no data transmission exceeds the maximum idle time, the device disconnects the Internet connection.
- **Manual**: The device connects to the Internet after you click Connect on the connection page. For details, see "Accessing the Internet."

PPP Authentication: This service is provided by your ISP. For details, consult your ISP.

Configuring WLAN Settings

(Name) SSID: Enter a name for your wireless local area network (WLAN).

- The service set identifier (SSID) is used to identify a WLAN. A PC and the wireless device can perform normal data communication only when they have the same SSIDs. To ensure the WLAN security, do not use the default SSID. You can enter a character string as the SSID, such as **MyHome**.

SSID Broadcast: Enable or disable the SSID broadcast.

- **Enabled**: The device broadcasts the SSID of the WLAN and users can easily access the WLAN. In this case, unauthorized users can also access the WLAN because the SSID is broadcasted.
- **Disabled**: The device does not broadcast the SSID of the WLAN. Before accessing the WLAN, a user must obtain the SSID of the WLAN. In this case, the WLAN security is improved.

Note For the convenience of users accessing the WLAN, you can select **Enabled** for SSID Broadcast when you configure the WLAN setting. After the setting, you can select **Disable** to improve the WLAN security.

Configuring the WLAN Encryption

To access the WLAN, you must set the wireless security key on your PC to be the same as that of the wireless device.

No Encryption

- For the convenience of users accessing the WLAN, you can select **NO ENCRYPTION** for the **Encryption mode** when you set up a WLAN. It is not recommended to select this option in daily use.

WPA-PSK/WPA2-PSK

- **WPA-PSK**: It is a 256-bit data encryption method that can automatically change the key.
- **WPA2-PSK**: It is a more secure version of WPA-PSK and it supports the IEEE 802.11 standard.
- **WPA Encryption Algorithm**: **TKIP, AES, TKIP+AES**.
- **WPA Pre-Shared Key**: You can enter a 64-character hexadecimal value or 8-63-character ASCII value as

the key. The ASCII value contains all characters that can be entered through the PC keyboard, and the hexadecimal value contains numbers of 0-9 and characters of A-F. For example, you can enter the ASCII value of 1234abcde as the key.

- **Network Key Rotation Interval**: It is used to set how long a network key is dynamically changed. By default, it is 0. To disable this function, you can set the value to 0 or null.

WEP

- Wireless Equivalent Privacy (WEP) is a 64-bit or 128-bit data encryption method. The 128-bit WEP encryption provides higher security level.
- **Network key 1**: You can enter 5 ASCII characters or 10-character hexadecimal numeral to form a 64-bit key. You can also enter 13 ASCII characters or 26-character hexadecimal numeral to form a 128-bit key.

Validating Quick Setup

The last page of the wizard displays all the settings you have configured.

- To accept the settings, click **Finish**.
- To change the settings, click **Back**.
- To quit the settings, click **Cancel**.

Accessing the Internet

1 Click **Connection**.

Note

- If you are required to enter the PIN code, enter the correct one. If you fail to enter the correct PIN or PUK code, the network-related functions are unavailable.
- The SIM/UIM card is supplied by the service provider. For details, contact your service provider.

2 If **PPP Connection** is **Auto** or **On Demand**, refresh the page to view the current network connection status.

3 If **PPP Connection** is **Manual,** click **Connect** / **Disconnect** to connect to or disconnect from the network.

4 Wait for several minutes, if you are prompted that the connection is successful, you can start the browser and enter the website address to access the Internet.

3 Configuring Your Computer

This takes the Windows XP operating system (OS) as an example to describe how to configure your computer. For other OSs, the configurations may be different and you need to configure them as required.

Wireless Configuration

The wireless configuration allows your PC to connect to the device through the wireless network. If you need only the Ethernet to connect your PC, you can skip this part.

Configuration Requirements

- To set up wireless network connection, your PC must be configured with the WLAN adapter that supports the IEEE 802.11 b/g protocol.
- If the encryption function is enabled, you need to ensure that all PCs connecting to the device use the same key as that of the device.
- For the use of WLAN adapter, refer to the WLAN adapter user guide provided by the manufacturer.
- For the encryption configurations, see "Configuring the WLAN Encryption Mode."
- For SSID parameters configuration, see "Configuring WLAN Settings."

Configuring the Wireless Network

1. Choose **Start > Control Panel > Network Connections > Wireless Network Connection**.
2. Click **Show Wireless Networks** to display the wireless network connection list.
3. Select the network connection that the SSID is the same as that of the device, and then click **Connect**.
4. If the encryption parameter is set for the device, the **Wireless Network Connection** dialog box is displayed and requires the network key and confirmation. The value you entered must be the same as the **WPA Pre-Shared Key** or **Network Key** of the device.

5 Wait for a while after you enter the correct network key. The wireless connection icon displays in the status area in the lower right corner of the screen. Then, your PC can automatically connect to the device.

Configuring the PC Network

The recommended configurations of the PC are as follows:

- Obtain an IP address automatically.
- Deselect Use a proxy server for your LAN.

Confige the Network Connection

1 Choose **My Network Places > Properties > Local Area Connection**.

2 Right-click the **Local Area Connection** icon and select **Properties**.

3 In the **Local Area Connection Properties** dialog box, select **Internet Protocol (TCP/IP)** in the **This connection uses the following items** list box, and then click **Properties**.

4 In the **Internet Protocol (TCP/IP) Properties** dialog box, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and then click **OK**.

Disabling Proxy Settings

1 Start the Internet browser, and then choose **Tools > Internet Options**.

2 Select the **Connections** tab, and then click **LAN Settings**.

3 In the **LAN Settings** dialog box, deselect **Use a proxy server for your LAN**.

4 Advanced Settings

Overview

Click **Advanced Settings**, you can configure both the basic attributes and advanced parameters of the device, and also perform routine maintenance and management to the device.

The following table shows the functions of the shortcut icons.

Icon	Description
	Click to access the **System** page.
	Click to access the **SIM/UIM Settings** page.
	Click to access the **Mobile Network Settings** page.
	Click to access the **Dial-up Settings** page.
	Click to access the **DHCP Settings** page.
	Click to access the **WLAN Settings** page.

System Management

Click to access the **System** page.

Changing the Password

You can change the login password to prevent unauthorized users from logging in to the management page.

1 Click .

2 Enter the current password, and then enter the new password and confirm it..

3 Click **Modify**.

Upgrading the device

1 Click .

2 Enter the path or click **Browse** to select the software image file to be updated.

3 Click **Upgrade**.

Warning

- After the system is upgraded, the system automatically restarts. The whole process takes two to three minutes.
- The software programs for upgrading must come from the official website of Huawei or the official website of the carrier.
- Upgrading the software does not change the configuration of the client.

Restoring the Factory Defaults

If you need to reconstruct the network or you forget the changes of some parameters, you can choose to restore factory defaults and reconfigure the device.

Click to access the **Restore Defaults** page, and then click **Restore**.

Note After this operation, all configurations are restored to the defaults.

Restarting the Device

1 Click to access the **Reboot** page.

2 Click **Reboot**.

Viewing the Version Information

Click to access the **Version** page.

You can view the hardware version, software version, and the release time.

SIM/UIM Settings

Click to access the **SIM/UIM Settings** page.

When the device works in the ROM-SIM mode, the page is not available.

Enabling or Disabling the PIN Code

1 Click .

2 Select **Enable/Disable** in the **PIN Code Operation** list box.

3 Enter the correct PIN code.

4 Click **Apply**.

Changing the PIN Code

When the PIN code protection is enabled, you can reset the PIN code.

1 Click .

2 Select **Modify** in the **PIN Code Operation** list box.

3 Enter the current PIN code.

4 Enter the new PIN code and confirm it.

5 Click **Apply**.

Mobile Network Settings

Click to access the **Mobile Network Settings** page.

Configuring the Mode for Searching Network

1 Click .

2 Select the mode for searching the network.

- **Auto**: The device automatically searches the network and registers with it.
- **Manual**: You need to manually search the network and register with it.

3 Click **Apply**.

4 In Manual mode, select the searched network and click **Log on**.

Dial-up Settings

Click to access the **Dial-up Settings** page.

Configuring the PPP Settings

1 Click to access the **PPP Settings** page

2 Enter the correct parameters.

- **Profile List**: Select a profile from the established dial-up connection list. If the drop-down list is empty, you need to create a profile list.
- **PPP Connection**: Select the dial-up connection mode.
- **PPP Authentication**: The service is provided by your ISP. For details, consult your ISP.
- **PPP Max Idle Time**: The duration of the PPP connection is in idle. In **On Demand** mode, if no data is transmitted in this duration, the PPP connection automatically disconnects.
- **PPP MTU**: It is the maximum transmission unit (MTU) of the PPP connection. It is used to set the maximum number of bytes encapsulated in a single data frame.
- **PPP Max Dial Time**: Set the maximum waiting time when connecting to the Internet.

Managing the Profile List

Click to access the **Profile Settings** page.

◆ **Creating a Profile**

1 Enter the profile information in the text box according to the prompts.

2 Click **Save**.

◆ **Changing a Profile**

1 Select a profile to be changed in the **Profile List** drop-down list. Relevant information is displayed in the corresponding text box.

2 Enter the profile information.

3 Click **Save**.

◆ **Deleting a Profile**

1 Select a profile to be deleted in the **Profile List** drop-down list.

2 Click **Delete**.

DHCP Settings

Click to access the **DHCP Settings** page, you can set the mode for assigning IP addresses in a LAN. DHCP automatically assigns IP addresses to the network devices. If you are using the DHCP server, you need to do the configurations on the PC connecting with the device. For details, see "Configuring the Network Connection".

- **IP Address**: The default IP address of the device is 192.168.1.1.
- **Subnet Mask**: The combination of the subnet mask and IP address enables the flexible sub netting. By default, the subnet mask is 255.255.255.0.
- **DHCP Server**: It is used to assign IP addresses dynamically. If the DHCP server is **Enabled**, it can automatically assign IP addresses for PCs. It is recommended to select **Enabled** for the DHCP server.
- **Start IP Address/End IP Address**: It is used to define the IP address range that the host can use during the IP address assignment. For example, in the network segment 192.168.1.0/24, the default IP address of the device is 192.168.1.1. The host IP address can range from 192.168.1.2 to 192.168.1.254. The minimum range is a single IP address.
- **DHCP Lease Time**: The DHCP server automatically assigns an IP address to each device connected to the network. When the leased time expires, the DHCP server checks whether the device is connected to the network. If the device is disconnected from the network, the server assigns the IP address to another device. Thus, the IP address is not wasted.

Note

- The **Start IP Address** must be smaller than or equal to the **End IP Address**.
- If the **DHCP Server** is **Enabled**, the configurations of **Start IP Address**, **End IP address,** and **DHCP Lease Time** are valid; otherwise, you cannot configure them.

WLAN Settings

Click to access the **WLAN Settings** page.

Enabling or Disabling the WLAN

1 Click to access the **WLAN Enable** page.

2 Select **Enable/Disable** to enable or disable the WLAN.

3 Click **Apply**.

WLAN Basic Settings

Click to access the **WLAN Basic Settings** page.

Selecting Interface IDs

- **Wireless Interface**: It refers to the SSID and MAC address, and is used to identify the wireless device.

SSID

- Entering a name (SSID) for your WLAN.
- Enabling or Disabling the **SSID Broadcast**.

Enabling or Disabling the AP Isolation

- **On**: The terminals (PCs) connecting to the device through the WLAN cannot communicate with each other.
- **Off**: The terminals (PCs) connecting to the device through the WLAN can communicate with each other.

Selecting a Country

- **Country**: It is used to identify the country. Different countries have different standards on channel usage.

Selecting a WLAN Channel

- **Channel:** It refers to the channel that the device works with. If you do not know which channel to select, select **Auto** and the device can automatically search for the channel.

Configuring the 802.11 Mode

There are four available modes, as shown in the following table.

Mode	Description
54g Auto	The WLAN has the best compatibility in this mode.

Mode	Description
54g Performance	The WLAN has the best performance in this mode.
54g LRS	If the device has difficulties in communicating with devices conforming to the IEEE 802.11b standards, select this mode.
802.11b Only	The device can only work in the low performance 802.11b standard network mode.
54g Only	The device can only work in the low performance 802.11g standard network mode.

Configuring the Transmission Rate

1. Select **Auto**, the device automatically searches the transmission rate.
2. Click **Apply** to submit the setting.

WLAN Advance Settings

Click to access the **WLAN Advance Settings** page.

A security key can protect your WLAN from illegal data attacking. The security key of your wireless device must be consistent with that of the PC.

Configuring the 802.11 Authentication

- **Open**: Open system authentication. A user accessing the WLAN can choose **WEP**, **WPA-PSK**, or **WPA2-PSK** key to pass the authentication or choose **No encryption** to skip the authentication.
- **Shared**: Shared key authentication. It can use only **WEP**. The user accessing the WLAN must use the **WEP** to authenticate.

Configuring the Encryption Mode

- There are four encryption modes: No Encryption, WPA-PSK, WPA2-PSK, and WEP. For details, refer to "Configuring the WLAN Encryption Mode."

Configuring the MAC Filter

Click to access the **WLAN MAC Filter** page.You can control and manage the clients accessing the WLAN, and improve the WLAN security performance.

MAC Restrict Mode

The following table shows the MAC address filter modes:

Parameter	Description
Disabled	The MAC address filter function is disabled.
Allow	The clients with addresses in the **MAC Address** list are allowed to connect with the device through the WLAN.
Deny	The clients with addresses in the **MAC Address** list are not allowed to connect with the device through the WLAN.

MAC Addresses

- Enter MAC addresses in the list. The device can perform the access control over the clients whose MAC addresses are in the list.

WLAN Bridge

Click to access the **WLAN Bridge** page.

- **Preamble Type**: It has two options: **Long** and **Short.** In the case that the client (PC) supports the **Short** type, the WLAN can have a better performance if it is **Short**.
- **MAX Associations Limit**: It refers to the maximum number of connections. It is used to set the maximum number of concurrent WLAN users on the device.
- **Mode**: It refers to the WLAN accessing mode. The device can work in two modes, as shown in the following table. The default value is **Access Point**.

Mode	Description
Wireless Bridge	It is used to connect two or more access points.
Access Point	The access points meeting the IEEE 802.11b/g standard or the wireless terminals can connect the wireless device.

WLAN Settings

- **Bridge Restriction**: It refers to the limitation to the peer MAC addresses. When it is **Disabled**, the device can access all the remote bridges; when it is **Enabled**, the device can only access the remote bridges that the addresses are in the address list.
- **Bridges**: It refers to the physical address of the remote peer bridge. The device supports the point-to-multipoint (PTM) bridge mode.
- **Peer MAC Address**: It refers to the physical address list of the remote peer bridges..
- **Link Status**: **Up** shows the successful connection and **Down** shows the failed connection.

5 Security Settings (Optional)

Click **Security**, you can configure the advanced security settings.

Firewall Switch

Your device has a true firewall that controls the incoming and outgoing data flow and protects your computer from illegal intrusion.

1 Click .

2 Select the **Enable the firewall (main switch of the firewall)** check box to enable the firewall.

Note

- Only when the **Enable the firewall** check box is selected, the other functions such as the IP address filter function, the MAC address filter function, and the WAN port ping function are available.
- When the **Enable LAN MAC address filter** check box is selected, the default filter rules are available.

3 Select other options as required, and then click **Apply**.

LAN MAC Filter

Your device supports MAC filtering based on a list of either denied or allowed computers. A common method to restrict network access is to specify the Media Access Control (MAC) address.

To locate the MAC address in the Windows OS, choose **Start > Run**, and then enter **cmd**.

The command window is displayed, enter **ipconfig /all**, and then press **Enter.**

The MAC address is displayed as the **Physical Address**.

1 Click .

2 Select **MAC Filter Mode**.

3 Enter the MAC addresses of the clients and click **Apply**.

LAN IP Filter

You can configure the device to block specific IP address so that they cannot be accessed from

computers in the local network.

Click to access the **LAN IP Filter** page.

Adding an IP Address

1. Select the protocol and status.
2. Enter the IP address and corresponding port to be blocked from accessing the LAN.
3. Click **Ok**.

Changing an IP Address

1. Click in the **Modification** column. The corresponding IP address filter is displayed.
2. Change the contents as required.
3. Click **Ok**.

Deleting an IP Address

Click in the **Modification** column.

The corresponding IP address filter is deleted.

Validating an IP Filter

1. Add a new IP address or select a record in the IP address filter table.
2. Select **On** for **Status**.
3. Click **Ok**.
4. Click **Apply**.

Virtual Server

Your device supports the virtual server to enable external computers to access WWW, FTP, or other services provided by the LAN.

Click to access the **Virtual Server** page.

Adding a Virtual Server

1. Select the protocol and status.
2. Enter values in the following text boxes:
   - **Name**: Enter a name to the service provided by the LAN.
   - **WAN Port**: Enter the WAN port of the LAN in which the computer provides services.
   - **IP Address**: Specify a computer in the LAN to provide services.
   - **LAN Port**: Enter the LAN port of the computer that provides services.
3. Click **Ok.**

You can also add a virtual server in the following way:

1. Select a port from the **Common Port** list. The Protocol, Status, Name, WAN Port, and LAN Port will be set as the default values. If required, you can change them.
2. Enter the IP Address.
3. Click **Ok**.

Changing a Virtual Server

1. Click in the **Modification** column. The relevant virtual server is displayed.
2. Change the contents as required.
3. Click **Ok**.

Deleting a Virtual Server

Click in the **Modification** column. The corresponding virtual server is deleted.

Validating a Virtual Server

1. Add a virtual server or select a record in the virtual server table.
2. Select **On** for **Status**.
3. Click **Ok**.

4 Click **Apply**.

DMZ Settings

If your PC cannot run network applications through the device, you can set the computer to access the Internet unlimitedly by configuring the IP address of the computer in the demilitarized zone (DMZ).

However, the DMZ computer is not protected by the firewall. It is vulnerable to attack and may also put other computers in the home network at risk.

1 Click .

2 Select **Enabled /Disabled** for **DMZ Status** to enable or disable the DMZ service.

3 Enter the local IP address of the computer that is specified as a DMZ host.

4 Click **Apply**.

Note Only one computer can be specified as a DMZ host at a time.

UPnP Settings

The Universal Plug and Play (UPnP) service allows other network users to control your device’ s network features to realize the intelligent interconnection.

1 Click .

2 Select **Enabled/Disabled** for **UPnP Status** to enable or disable the UPnP service

3 Click **Apply**.

Remote Management

The remote web management allows the access and control of the device either from the home network or from the Internet.

When you are on a trip, you can maintain your device through the remote web management service. It also

allows your ISP to help you solve the device problems from a remote location.

1. Click .
2. Select **Enabled /Disabled** for **Remote Status** to enable or disable the service.
3. Enter the IP address that can access and control your device.
4. Click **Apply**.

6 Troubleshooting

What to do if a PC in the LAN cannot access the Internet?

1. If the power indicator is off, you need to check whether the power adapter is normally connected.

2. If the modem indicator if off, you need to check whether the data card is connected normally.

3. If the signal strength indicator is off, you need to check whether the area is covered by the network.

4. If the area is covered by the network, you need to check whether the network mode is correct. For information about network mode, see "Mobile Network Settings".

5. If the indicator of the Ethernet interfaces blinks, the corresponding Ethernet interface is normally connected. If the indicator is off, you need to check and ensure that the related Ethernet connection is normal.

6. You must configure the correct PPP user name and PPP password when you access the Internet through the device. Check whether they are correct, and see "Configuring PPP Profile Settings" for details.

7. If the DHCP service is disabled and the PC obtains the IP address dynamically, the PC also cannot access the Internet. You can change the mode to manually assign an IP address. See "Configuring the Network Connection".

8. Check whether the driver of the network adapter is correctly installed.

9. If the preceding methods cannot solve the problem, please consult you service provider.

What to do if a PC in the WLAN cannot access the WLAN?

1. If interferences or shields near the device exist, you can adjust the position of the device. When the signal strength is strong, you can move to the next step.

2 Check and record the following data on the network adapter of your PC: SSID, WEP type, and key.

3 Check and record the following data on the device: SSID, WEP type, and key.

4 Compare the recorded data, the SSID on the network adapter should be ANY or be the same as that on the device. The WEP type and key on the network adapter and device should be the same. Otherwise, you need to change the data on the network adapter.

What to do if I forgot the IP address of the LAN interface?

If you forgot the IP address of the LAN interface, you can enter http://e.home and log in to the management page when the PC obtains the IP address automatically.

What to do if bridging between two devices is unsuccessful?

1 Make sure that the two devices work on the same channel. For details, see "Selecting a WLAN Channel".

2 Make sure that the MAC address of one device is in the peer MAC address list of the other device. For details, see "WLAN Bridge".

When the signal strength is normal, what to do if the downloading rate is low?

In this case, you need to set the value in the registry as follows:

1 Choose **Start > Run**.

2 Enter **regedit** in the **Open** text box and then click **OK**.

3 Select parameters in the following directory: **\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip**.

4 Choose **Edit > New > DWORD Value**.

5 Rename **New Value #1** to **TcpWindowSize**.

6 Right-click **TcpWindowSize** and then select **Modify**.

7 Select **Decimal** and enter **65535** in the **Value data** text box, and then click **OK**.

8 For the **DWORD Value** of **DefaultRcvWindow**, do the same operations as that of **TcpWindowSize**.

7 Safety Information

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

Interference

Do not use your wireless device if using the device is prohibited or when it cause danger or interference with electric devices.

Medical Device

- Do not use your wireless device and follow the rules and regulations set forth by the hospitals and health care facilities.
- Some wireless devices may affect the performance of the hearing aids. For any such problems, consult your service provider.
- If you are using an electronic medical device, consult the doctor or device manufacturer to confirm whether the radio wave affects the operation of this device.

Area with Inflammables and Explosives

To prevent explosions and fires in areas that are stored with inflammable and explosive devices, do not use your wireless device and observe the rules. Areas stored with inflammables and explosives include but are not limited to the following:

- Gas station
- Fuel depot (such as the bunk below the deck of a ship)
- Container/Vehicle for storing or transporting fuels or chemical products
- Area where the air contains chemical substances and particles (such as granule, dust, or metal powder)
- Area indicated with the "Explosives" sign
- Area indicated with the "Power off bi-direction wireless equipment" sign
- Area where you are generally suggested to stop the engine of a vehicle

Traffic Security

- Observe local laws and regulations while using the wireless device. To prevent accidents, do not use your wireless device while driving.
- RF signals may affect electronic systems of motor vehicles. For more information, consult the vehicle manufacturer.
- In a motor vehicle, do not place the wireless device over the air bag or in the air bag deployment area. Otherwise, the wireless device may hurt you owing to the strong force when the air bag inflates.

- Observe the rules and regulations of airline companies. When boarding, switch off your wireless device. Otherwise, the radio signal of the wireless device may interfere with the plane control signals.

Safety of Children

Do not allow children to use the wireless device without guidance. Small and sharp components of the wireless device may cause danger to children or cause suffocation if children swallow the components.

Environment Protection

Observe the local regulations regarding the disposal of your packaging materials, used wireless device and accessories, and promote their recycling.

WEEE Approval

The wireless device is in compliance with the essential requirements and other relevant provisions of the Waste Electrical and Electronic Equipment Directive 2002/96/EC (WEEE Directive).

RoHS Approval

The wireless device is in compliance with the restriction of the use of certain hazardous substances in electrical and electronic equipment Directive 2002/95/EC (RoHS Directive).

Laws and Regulations bservance

Observe laws and regulations when using your wireless device. Respect the privacy and legal rights of the others.

Care and Maintenance

It is normal that your wireless device gets hot when you use or charge it. Before you clean or maintain the wireless device, stop all applications and disconnect the wireless device from your PC.

- Use your wireless device and accessories with care and in clean environment. Keep the wireless device from a fire or a lit cigarette.
- Protect your wireless device and accessories from water and vapor and keep them dry.
- Do not drop, throw or bend your wireless device.
- Clean your wireless device with a piece of damp and soft antistatic cloth. Do not use any chemical agents

(such as alcohol and benzene), chemical detergent, or powder to clean it.
- Do not leave your wireless device and accessories in a place with a considerably low or high temperature.
- Use only accessories of the wireless device approved by the manufacture. Contact the authorized service center for any abnormity of the wireless device or accessories.
- Do not dismantle the wireless device or accessories. Otherwise, the wireless device and accessories are not covered by the warranty.

Emergency Call

This wireless device functions through receiving and transmitting radio signals. Therefore, the connection cannot be guaranteed in all conditions. In an emergency, you should not rely solely on the wireless device for essential communications.

Body Worn Operation

Important safety information regarding radiofrequency radiation (RF) exposure.

To ensure compliance with RF exposure guidelines the device must be used with a minimum of 1.5 cm separation from the body.

Failure to observe these instructions could result in your RF exposure exceeding the relevant guideline limits.

Regulatory Information

The following approvals and notices apply in specific regions as noted.

CE Approval (European Union)

The wireless device is approved to be used in the member states of the EU. The wireless device is in compliance with the essential requirements and other relevant provisions of the Radio and Telecommunications Terminal Equipment Directive 1999/5/EC (R&TTE Directive).

Federal Communications Commission Notice (United States): Before a wireless device model is available for sale to the public, it must be tested and certified to the FCC that it does not exceed the limit established by the government-adopted requirement for safe exposure.

FCC Statement

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 should be installed and operated with a minimum distance of 20 cm between the radiator and your body when using it via USB cable.

8 Abbreviations

3G	The Third Generation
AP	Access Point
APN	Access Point Name
CDMA	Code Division Multiple Access
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EDGE	Enhanced Data rates for GSM Evolution
GSM	Global System for Mobile communications
GPRS	General Packet Radio Service
HSPA	High Speed Packet Access
HSDPA	High Speed Downlink Packet Access
HSUPA	High Speed Uplink Packet Access
IP	Internet Protocol
LAN	Local Area Network
LED	Light Emitting Diode
NAT	Network Address Translation
POTS	Plain Old Telephone Service
UMTS	Universal Mobile Telecommunications System
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WCDMA	Wideband CDMA
WI-FI	Wireless Fidelity

Version:V100R001_01 Part Number:31018860