Online Help

1 Getting Help

2 Management Page Overview

3 Connection

4 SMS

5 SD Card

6 Settings

7 Appendixes

1 Getting Help

If the device is not operating normally, you can try the following methods to get help:

- See **Help** on the web management page.
- Restart the device.
- Restore the factory defaults.
- Contact your service provider.

Back Top

2 Management Page Overview

2.1 Accessing the Management page

Procedure

1. Start the Internet browser and enter **http://192.168.1.1** in the address bar.
2. Enter the password, and then click **Login**

   The default password is **admin**.

Back Top

2.2 Device Status

The following table lists the status information of the device.

Item	Status
SIM	● ▮▯: The card is valid. ● ▯: The SIM card does not exist or the PIN code is not verified or the SIM card is corrupted.
Internet	● 🌐: The dial-up connection is established. ● 🌐: The dial-up connection is not established.
WLAN	● 🖵: The WLAN is established. ● 🖵: The WLAN is not established.
Battery	The battery power level from weak to strong is shown as follows: 🔋 🔋 🔋 🔋 🔋
SIG	The signal strength from weak to strong is shown as follows: 📶 📶 📶 📶 📶 📶

Back Top

3 Connection

3.1 Viewing the Connection Status

Procedure

1. Click **Connection**.
2. View the basic connection status.
    1. **Connection Status**
    2. **WAN Status**
    3. **WLAN Status**
3. Click **Advanced...** on the right area of the page to view the detailed status.
    1. Click **Refresh** to view the current status on the advanced status page.
    2. Click **Back** to return to the previous page.

Back Top

3.1.1 Viewing the Traffic Statistics

Prerequisite

NOTE:
The statistical data of the traffic is for your reference only. The actual traffic information is for billing purpose is based on the traffic data collected by the service provider.

Procedure

1. Click **Connection**.
2. Click **Advanced...** in the **Connection Status** area.
3. View the traffic statistics.
4. Click **Clear History** to reset the current statistic to zero.

Back Top

3.2 Accessing the Internet

Procedure

1. Click **Connection**.
2. Connect to the Internet.
    1. If **Connection Mode** is **Manual**, click **Connect / Disconnect** to connect to or disconnect from the network.
    2. If **Connection Mode** is **Auto**, refresh the page to view the current network connection status.
3. Wait for several minutes. If the connection is successful, you can use the Internet service.

Back Top

4 SMS

4.1 Creating and Sending a Message

Procedure

1. Click **SMS > Write SMS**.
2. Enter the message content.
3. Enter the recipient number.
4. After the message is completed, you can choose the following options:
    1. **Send:** To send the message.
    2. **Save:** To save the message as a draft.

Back Top

4.2 Viewing a Message

Inbox stores the received messages. **Sent** stores the sent messages, including both the messages sent successfully and unsuccessfully. **Drafts** store the drafts of messages.

Procedure

1. Click **SMS > Inbox/Sent/Drafts**. The state of a SMS message in Inbox is represented by the following icons:
    1. ✉: The memory is full.
    2. ✉: An unread message.
    3. ✉: A read message.
2. On the SMS page, you can choose the following options.
    1. Turn a page and view messages.
    2. Refresh the current storage status.
    3. Mark or unmark all messages.
    4. Delete the marked message(s).
3. After you click one message in the message list, the detail of the message is displayed. You can choose the following options.
    1. Read the contents.
    2. Reply to the message.
    3. Forward the message.
    4. Delete the message.

Back Top

4.3 SMS Settings

Procedure

1. Click **SMS> SMS Settings**.
2. View or edit the **SMS Center Number.**

NOTE:

1. The information of SMS center number is provided with the SIM card. When the SIM card is inserted, the information is changed automatically.
2. If the information is null or you delete the information by accident, contact your service provider.

3. Select **SMS Save Mode** to save the messages in the SIM card or the device.
4. Click **Apply** to save the settings.

Back Top

5 SD Card

5.1 SD Card Settings

Procedure

1. Click **SD Card**.
2. Set the **SD Card Sharing Mode**.
    1. **Web Share Mode:** You can access the SD card only on the Web management page.
    2. Select **Enable/Disable** to turn **SD Card Sharing** on or off.
    3. Set **File to Share:**
        1. **Entire SD Card:** All files stored in the SD card can be accessed.
        2. **Custom Setting:** Specified files can be accessed
    4. Set **Access Type:**
        1. **Read Only:** You can view the shared files only.
        2. **Read/Write:** You can manage the shared files.
    5. **USB Access Only:** You can access the SD card only as a removable disk by connecting device with USB cable.
3. Click **Apply**.

Back Top

5.2 Web Sharing SD Card

5.2.1 Viewing Files

Procedure

1. Click **SD Card**.
2. View the shared files.

    NOTE:
    You can also click View MicroSD Files on the login page to access the SD card.
3. Click **Up** to return to the previous folder.

Back Top

5.2.2 Creating New Folders

When the **Write** permission of the **Web Share Mode** is enabled, you can create new folders in the SD card.

Procedure

1. Click **SD Card > New Folder**.
2. Input the new folder name.
3. Click **Ok** .

Back Top

5.2.3 Deleting Files

When the **Write** permission of the **Web Share Mode** is enabled, you can delete the files in the SD card.

Procedure

1. Click **SD Card**.
2. Select one or more files you need to clear.
3. Click **Delete Selected**.

Back Top

5.2.4 Uploading Files

When the **Write** permission of the **Web Share Mode** is enabled, you can upload files from the computer to the SD card.

Procedure

1. Click **SD Card**.
2. Click **Browse** to select a file from the computer.
3. Click **Upload**.

Back Top

5.3 Accessing SD Card via USB

When the **USB Access Only Mode** is enabled, you can access the SD card as a removable disk by connecting device with USB cable.

Procedure

1. Connect the device to a PC with the compatible data cable.
2. The PC detects and recognizes new hardware.
3. Enter **My Computer**; and then double click the **Removable Disk** mapped to the SD card.
4. View or manage the files stored in the SD card.

Back Top

6 Settings

6.1 Quick Setup

You can use the quick setup wizard to configure and maintain the basic parameters of the device.

Procedure

1. Click **Settings > Quick Setup** to access the welcome page.
2. Click **Next** to configure the parameters according to the onscreen instructions.
3. Click **Finish** to accept the settings.

Back Top

6.2 Dial-up Settings

6.2.1 Internet Connection

Procedure

1. Click **Settings > Dial UP > Mobile Connection**.
2. Select a profile from the established dial-up connection list. If the drop-down list is empty, you need to create a profile.
3. Select a dial-up connection mode.
    1. **Manual**: The device connects to the Internet after you click **Connect** on the connection page. For details, refer to"Accessing the Internet".
    2. **Auto**: The device automatically connects to the Internet when data transmission exists. When the duration of no data transmission exceeds **Max Idle Time**, the device disconnects the Internet connection.

       NOTE:
    3. **Max Idle Time**: The duration of the connection is in idle. In **Auto** mode, if no data is transmitted in this duration, the connection automatically disconnects.
4. Click **Apply**.

Back Top

6.2.2 Profile Management

Creating a Profile

Procedure

1. Click **Settings > Dial-up > Profile Management**.
2. Enter the profile information according to the onscreen instructions.The information is specific to your service provider. Please contact your service provider for the values.
3. Click **Save**.

Changing a Profile

Procedure

1. Click **Settings > Dial-up > Profile Management**.

2. Select a profile to be changed from the **Profile List** drop-down list. Relevant information is displayed in the corresponding text box.
3. Enter the profile information. The information is specific to your service provider. Please contact your service provider for the values.
4. Click **Save**.

Deleting a Profile

Procedure

1. Click **Settings > Dial-up > Profile Management**.
2. Select a profile to be deleted from the **Profile List** drop-down list.
3. Click **Delete**.

Back Top

6.2.3 Mobile Network Settings

Network Type and Band

Procedure

1. Click **Settings > Mobile Network Settings**.
2. Select a preferred network mode from the **Preferred Mode** list box.

   NOTE:
   1. If the service provider provides only the 2G service and the preferred mode is configured as 3G only, you cannot access the Internet.
   2. If the service provider provides only the 3G service and the preferred mode is configured as 2G only, you cannot access the Internet.
   3. If the service provider provides neither 3G nor 2G service, you cannot access the Internet regardless of the preferred mode.
   4. WCDMA Preferred means that the device will search for 3G network and then 2G network. You service provider may charge different rate for each different network connection so check with your service provider before using this setting.

3. Select a band from the **Band** list box to search the network within the band.
4. Click **Apply**.

Searching the Network

Procedure

1. Click **Settings > Mobile Network Settings**.
2. Select the mode for searching the network.
   1. **Auto**: The device automatically searches for the available networks and then selects one to registers with.
   2. **Manual**: You need to manually search for the available networks and then selects one to registers with.
3. Click **Apply**.
4. In **Manual** mode, select the searched network and click **Log on**.

Back Top

6.2.4 PIN Management

NOTE:

1. If you are required to enter the PIN code, enter the correct one.
2. If you enter the wrong PIN code three times, the SIM card is locked. You need the PUK code to unlock the SIM card. If you enter wrong PUK code for ten times, the SIM card is locked permanently.
3. If you fail to enter the correct PIN or PUK code, the network-related functions are unavailable.
4. The default PIN code is 0000, if this doesn’t work or you forgot the new value after you changed it. Please contact your service provider for the PUK code.

Enabling or Disabling the PIN

Procedure

1. Click **Settings > Dial-up > PIN Code Management**.
2. Select **Enable/Disable** from the **PIN Code Management** list box.
3. Enter the correct PIN code.
4. Click **Apply**.

Changing the PIN

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

Procedure

1. Click **Settings > Dial-up > PIN Code Management**.
2. Select **Modify** from the **PIN Code Operation** list box.
3. Enter the current PIN code.
4. Enter the new PIN code and confirm it.
5. Click **Apply**.

Validating the PIN

When the PIN code protection is enabled, you need to enter the correct PIN code to validate whether the SIM card is valid after each restart.

Procedure

1. Click **Settings > Dial-up > PIN Code Management**.
2. Select **Validate** from the **PIN Code Operation** list box.
3. Enter the correct PIN code.
4. Click **Apply**.

Enabling or Disabling the PIN Auto Validation

When the PIN code protection is enabled, you can enable or disable the auto validate PIN code function. If **Auto Validation** is enabled, the PIN code is recorded and automatically validated after each restart. When the **Save PIN Code** check box is selected, the **Auto Validation** is enabled.

Procedure

1. Click **Settings > Dial-up > PIN Code Auto Validation**.
2. Select the **Enabled/Disabled** option button.
3. Enter the correct PIN code.
4. Click **Apply**.

Back Top

6.3 WLAN Settings

6.3.1 Enabling or Disabling the WLAN

Context

NOTE:
In **Connection**, you can configure the WLAN module by clicking **Turn On/Turn Off** button in the **WLAN** status area.

Procedure

1. Click **Settings > WLAN > WLAN Basic Settings**.
2. Set **WLAN Module:**.
    1. **On:** Enable the WLAN.
    2. **Off:** Disable the WLAN.
3. Click **Apply**.

Back Top

6.3.2 Configuring the WLAN SSID

The service set identifier (SSID) is used to identify a WLAN. A Client and the device can perform normal data communication only when they have the same SSIDs. To easily idenitify your own device among all the Wi-FI networks available, you can change it to a unique name. You can enter a character string as the SSID, such as MyHome.

Procedure

1. Click **Settings > WLAN > WLAN Basic Settings**.
2. Change the default **SSID** in the **(Name) SSID** textbox.
3. Click **Settings > WLAN > WLAN Advanced Settings**.
4. Enable/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 as long as he has the correct encryption information.
- **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.When the device is set at this mode, your computer needs to be configured to try to connect even when SSID is not broadcast.

NOTE:
To access the WLAN easily, you can select **Enabled** for **SSID Broadcast** when you configure the WLAN settings. After the settings, you can select **Disabled** to improve the WLAN security.

Back Top

6.3.3 Configuring WLAN Encryption

Procedure

1. Click **Settings > WLAN > WLAN Basic Settings**.
2. Configure the WLAN security key according to the onscreen instructions.

NOTE:
To access the WLAN easily, you can select **No Encryption** for the **Encryption Mode** when you set up a WLAN. It is not recommended that you select this option in daily use.

Back Top

6.3.4 Enabling or Disabling the Wi-Fi Auto Off

When the device is powered by the battery and no user accesses the WiFi network through the device for a period longer than the **WiFi Off Time**, the device will disable WiFi automatically. In this case, enable WiFi manually if you want to use this function again.

Procedure

1. Click **Settings > WLAN > WLAN Advanced Settings**.
2. Select **On/Off** to enable or disable the **WiFi Auto Off**.
3. Enter the **WiFi Off Time**, if the **WiFi Auto Off** is enabled.

Back Top

6.3.5 Selecting the Country and Channel

Procedure

1. Click **Settings > WLAN > WLAN Advanced Settings**.
2. Select **Country** and **Channel**.

NOTE:
- Different countries have different standards on channel usage.
- If you do not know which channel to select, select **Auto** and the device can automatically search for the channel.

Back Top

6.3.6 Enabling or Disabling the AP Isolation

Procedure

1. Click **Settings > WLAN > WLAN Advanced Settings**.
2. Select **On/Off** to enable or disable the **AP Isolation**.

- **On:** The Clients connecting to the device cannot communicate with each other.
- **Off:** The Clients connecting to the device can communicate with each other.

Back Top

6.3.7 Configuring the 802.11 Mode

Procedure

1. Click **Settings > WLAN > WLAN Advanced Settings**.
2. Select **802.11 Mode**.

- **802.11b:** Only allow the Clients supporting 802.11b standard to access the device. The wireless speed is up to 11 Mbps.
- **802.11g:** Only allow the Clients supporting 802.11g standard to access the device. The wireless speed is up to 54 Mbps.
- **802.11b/g:** Allow the Clients compatible with 802.11b or 802.11g standard to access the device.

NOTE:
For the 802.11 standard your Client supports, you can contact the service provider of your Client.

Back Top

6.3.8 Configuring the Transmission Rate

Procedure

1. Click **Settings > WLAN > WLAN Advanced Settings**.
2. Select **Rate**.

NOTE:
Select **Auto**, the device automatically searches for the transmission rate.

Back Top

6.3.9 Establishing the WPS Connection

WiFi Protected Setup (WPS) is a standard for easy and secure establishment of a wireless network. Traditionally, you would have to manually enter a wireless network name (SSID), and then manually enter a security key on both the access point and client to prevent unwanted access to your wireless network. With WPS, you do not need to know the SSID and security key. It will automatically configure the SSID and security key for the access point and the WPS enabled client devices on the network.

Procedure

1. Click **Settings > WLAN > WPS Settings**.
2. Enter the **WPS PIN:** of the WPS client device on the network.
3. Click **Apply**.

Back Top

6.3.10 WLAN MAC Filter

You can control and manage the Clients accessing the WLAN, and improve the WLAN security performance.

Procedure

1. Click **Settings > WLAN> WLAN MAC Filter**.
2. Select **MAC Restrict Mode**.
    1. **Disabled**: The MAC address filter function is disabled.
    2. **Allow**: The Clients with addresses in the **MAC Address** list are allowed to connect with the device over the WLAN.
    3. **Deny**: The Clients with addresses in the **MAC Address** list are not allowed to connect with the device over the WLAN.
3. Enter **MAC Address** in the list. The device can perform the access control over the Clients whose **MAC Address** are in the list.
4. Click **Apply**.

Example

To locate the **MAC Address** in the Windows OS:

1. Choose **Start** > **Run**, and then enter **cmd**.
2. The command window is displayed. Enter **ipconfig/all**, and then press **Enter**.
3. The MAC address is displayed as the **Physical Address**.

If your computer is connected to the device already, go to Connection > Advanced (in WLAN Status section) and you will see the information for the connected devices which includes the MAC address. This may be simpler if you have multiple computers running different OS.

Back Top

6.4 DHCP Settings

6.4.1 Enabling the DHCP Server

If the DHCP (Dynamic Host Configuration Protocol) server is enabled, the device can automatically assign IP addresses to the Clients connected to it.

Procedure

1. Click **Settings > DHCP**.
2. Enter the **IP Address** of the device (default: 192.168.1.1).
3. Enter the **Subnet Mask** of the device (default: 255.255.255.0).
4. Select **Enabled** option button.
5. Enter the **Start IP Address/End IP Address**.

    NOTE:
    1. The **Start IP Address** must be smaller than or equal to the **End IP Address**.
    2. The minimum range is a single IP address.

6. Enter the **DHCP Lease Time**. The value is in seconds.

    NOTE:
    1. The DHCP server automatically assigns an IP address to each Client connected to the LAN that utilizes DHCP to obtain its networking information. When the leased time expires, the DHCP server checks whether the Client is connected to the LAN. If the Client is disconnected from the LAN, the server assigns the IP address to another Client. Thus, the IP address is not wasted.

7. Click **Apply**.

Example

1. IP Address of the device: 192.168.1.1
2. Start IP Address: 192.168.1.XXX (2<=XXX<=254)
3. End IP Address: 192.168.1.YYY (XXX<=YYY<=254)

NOTE:

1. 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.
2. If the **DHCP Server** is enabled, you need to configure the Clients to obtain IP address and DNS server automatically. For details, see " 6.4.3 Configure the Client (Take PC for Example)".

Back Top

6.4.2 Disabling the DHCP Server

If the DHCP server is disabled, you must manually assign IP addresses for Clients connected to the device.

Procedure

1. Click **Advanced Settings > DHCP Settings**.
2. Select **Disabled** option button.
3. Click **Apply**.

NOTE:
If the **DHCP Server** is disabled, you need to manually configure the IP address and DNS server of the Clients. For details, see " 6.4.3 Configure the Client (Take PC for Example)".

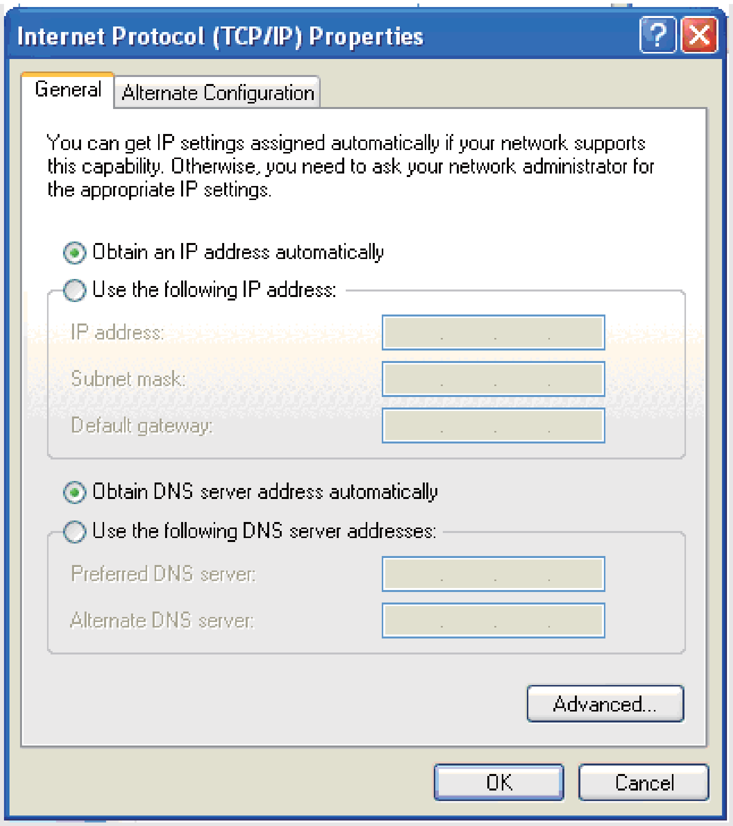
Back Top

6.4.3 Configure the Client (Take a Windows XP PC for Example)

Procedure

1. Select **Start > Control Panel > Network Connections > Wireless Network Connection**.
2. Right-click the **Network Connection** icon and select **Properties**.
3. Select **Internet Protocol (TCP/IP)**, 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** .

Example



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

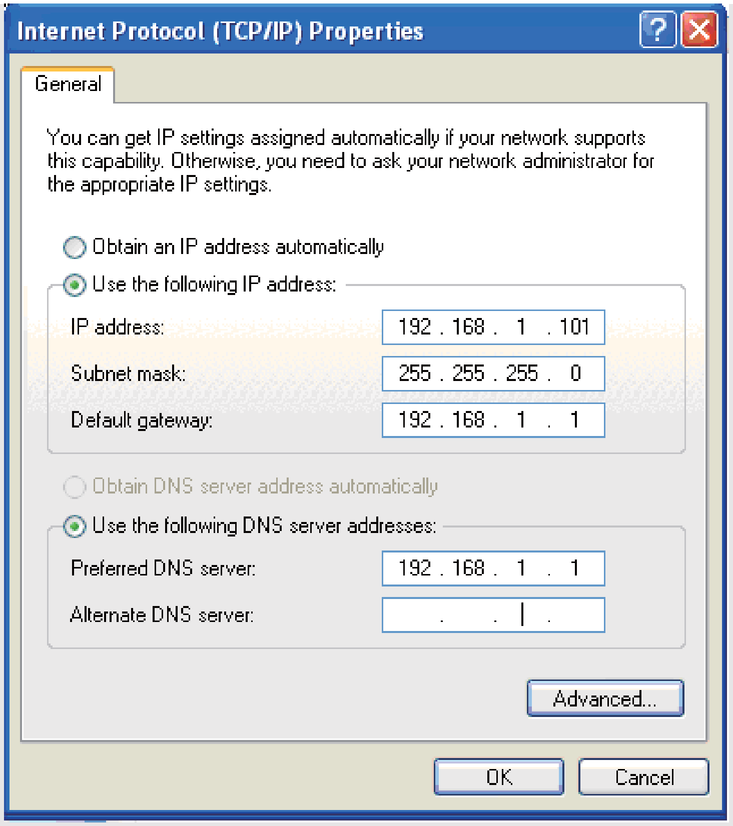
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

You can also enter the IP addresses and DNS server manually.

- **IP Address**: 192.168.1.XXX(2<=XXX<=254)
- **Subnet Mask**: 255.255.255.0
- **Default Gateway**: 192.168.1.1
- **DNS Server:** Enter the default gateway (192.168.1.1) or contact your service provider.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 101

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1

Alternate DNS server: . . .

Back Top

6.5 Security Settings

6.5.1 Firewall Switch

Your device has built-in firewall that controls the incoming and outgoing data flow and protects your computer from illegal intrusion.

Procedure

1. Click **Settings> Security > Firewall Switch**.
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 and the WAN port ping function are available.

Back Top

6.5.2 LAN IP Filter

You can configure the device to block specific IP addresses of the Internet service so that these services cannot be accessed by specific Clients in the local network. Please note that assignment of the same IP address to the Client is not guaranteed if DHCP is used by the Client to obtain its IP address from the device. For this filter to work correctly on subsequent restart, the Client should be using a static IP address.

Procedure

1. Click **Settings > Security > LAN IP Filter**.
2. Configure the information as required.
3. Click **Ok** to save the settings.
4. Click **Apply** to validate the settings.

- Click **Edit** to modify the selected items in the list.
- Click **Delete** to remove the selected items in the list.

Example

To prevent the Client (192.168.1.101) from accessing the Internet address www.huawei.com (10.82.48.26), comfigure the following filter rule:

- **Protocol**:TCP

  NOTE:
  The protocol of Web service is TCP. If you do not know the protocol, you can select **Both**. Then the device automatically searches for the protocol.

- **Status**:On

  NOTE:
  If you want to establish the filter and enable it later, you can select **Off**.

- **LAN IP Address:** 192.168.1.101

  NOTE:
  To locate the LAN IP address in the Windows OS:

  1. Select **Start** > **Run**, and then enter **cmd**.
  2. The command window is displayed. Enter **ipconfig**, and then press **Enter**.
  3. The IP address is displayed.

- **WAN IP Address:** 10.82.48.26

  NOTE:
  To locate the WAN IP address in the Windows OS:

  1. Select **Start** > **Run**, and then enter **cmd**.
  2. The command window is displayed. Enter **ping www.huawei.com**, and then press **Enter**.
  3. The **WAN IP Address** is displayed as the **10.82.48.26**.

- **LAN Port**/ **WAN Port**: 80

  NOTE:
  The default port of the Web service is 80. For the port and protocol, you can contact the service provider or access the official website of the Internet service.

Back Top

6.5.3 Virtual Server

Your device supports the virtual server to enable external users to access WWW, FTP, or other services provided by a specific Client in the LAN.

Procedure

1. Click **Settings > Security > Virtual Server**.
2. Configure the information as required. The virtual server should be configured with a static IP address and not rely on DHCP since the IP address assigned to a Client by the DHCP server is not guaranteed to be the same on every request.

   NOTE:
   You can also add a virtual server by selecting a port from the **Common Port** list. The parameters will be set as the default values. If required, you can change them.

3. Click **Ok** to save the settings.
4. Click **Apply** to validate the settings.

- Click **Edit** to modify the selected items in the list.
- Click **Delete** to remove the selected items in the list.

Example

To specify the Client (192.168.1.101) to provide a FTP service accessible by the external users, do as follows:

- **Common Port**: FTP (21)
- **Protocol**: TCP
- **Status**: On
- **Name**: My FTP server
- **LAN Port/ WAN Port**: 21
- **LAN IP Address**: 192.168.1.101

After the virtual server is established, the Internet users can access the FTP service.

1. Click **Basic Status** to get the **WAN IP Address** of the device.
2. The **WAN IP Address** of the device is displayed as the **IP Address** in the **WAN Status** area, such as 10.2.1.123.
3. Enter the FTP server address (ftp://10.2.1.123) in the Internet browser.
4. The device will pass the data traffic to port 21 to the Client which currently has the address 192.168.1.101.

   NOTE:
   The default port of the FTP service is 21. If the port is changed to 8021 that is not the default value, the external users must access the FTP server address (ftp://10.2.1.123:8021). The virtual service configuration has to be changed to specify port 8021 so that the device knows how to forward the request.

Back Top

6.5.4 Special Applications

Special applications can be used for dynamic port forwarding (commonly known as port triggering) configuration. Certain applications send their response back to connecting client through a specific port range only. The device needs to know the port range so it can forward the packets from the application back to the Client who initiate the request through the trigger port initially. When an application in the LAN intends to establish the TCP/UDP connection with a remote application, the firewall dynamically opens the required port range with this function. Please note only 1 Client can utilize the outbound trigger port at any one time since the device will not be able to route packets coming in through the opened port range to multiple Clients.

Procedure

1. Click **Settings > Security > Special Applications**.
2. Configure the information as required. The virtual server should be configured with a static IP address and not rely on DHCP since the IP address assigned to a Client by the DHCP server is not guaranteed to be the same on every request.

   NOTE:
   Your device is equipped with a list of **Special Applications**. To use any of these applications, you only need to select it from the **Common Port** list.

3. Click **Ok** to save the settings.
4. Click **Apply** to validate the settings.

- Click **Edit** to modify the selected items in the list.
- Click **Delete** to remove the selected items in the list.

Example

Consider a MSN Gaming Zone server that is accessed by the LAN Client using TCP protocol on port 47624. The gaming server responds by connecting the user using TCP on port 2400 when starting gaming sessions. In such a case, you must use dynamic port forwarding because this scenario conflicts with the following default firewall settings:

- The firewall blocks inbound traffic by default.
- The server can send a connection request to the device's IP address; however, the connection request cannot be sent back to the Client because the IP address of the Client is not a public address.

In order to solve this conflict, you need to define a dynamic port forwarding entry, which allows inbound traffic on TCP port 2400 when a LAN Client generates traffic to TCP port 47624. This will enable the reception of the inbound traffic from the gaming server, and the sending of the traffic to the LAN Client that has generated the outgoing traffic to TCP port 47624.

- **Common Port**: MSN Gaming Zone
- **Trigger Port**: 47624
- **Open Port**: 2300-2400, 28800-29000
- **Trigger Protocol**/**Open Protocol**: TCP
- **Status**: On
- **Name**: MSN Gaming Zone

NOTE:
For the **Trigger Port**, **Open Port**, **Trigger Protocol** and **Open Protocol**, you can contact the service provider or access the official Website of the **Special Applications**.

Back Top

6.5.5 DMZ Settings

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

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

Procedure

1. Click **Settings > Security > DMZ Settings**.
2. Select **Enabled/Disabled** for **DMZ Status** to enable or disable the DMZ service.
3. Enter the IP address of the Client that is specified as a DMZ host.
4. Click **Apply**.

NOTE:
Only one Client can be specified as a DMZ host at a time and it should be configured with a static IP address.

Back Top

6.5.6 SIP ALG Settings

The SIP (Session Initiation Protocol) is a protocol used to set up, change, or end the multimedia sessions. The ALG (Application-level gateway) can understand the SIP protocol used by the specific applications and make a protocol packet-inspection of traffic through it. If you need to use a SIP application you can enable the **SIP ALG**.

Procedure

1. Click **Settings > Security > SIP ALG Settings**.
2. Select **Enable SIP ALG** or not.
3. Input **SIP Port:** that is the port of the SIP server provided by the service provider.
4. Click **Apply** to save the settings.

Back Top

6.5.7 UPnP Settings

UPnP service (Universal Plug and Play) realizes the intelligent interconnection between any two UPnP devices through the port forwarding. The UPnP device can access the Internet dynamically and get the IP address automatically.

Procedure

1. Click **Security Settings > UPnP Settings**.
2. Select **Enable/Disable** for **UPnP Settings** to enable or disable the UPnP service.
3. Click **Apply**.

Prerequisite

To enable or disable the UPnP service of the Client (take a Windows XP PC for example):

1. Select **Start > Control Panel > Add/Remove Program > Add / Remove Windows Components**.
2. Select **Network Services** and then click **Details** in the **Windows Components Wizard to Install** dialog box.
3. Select **UPNP User Interface** to enable the UPnP service .
4. Click **Ok** .

Back Top

6.6 System Management

6.6.1 Viewing the Device Information

Procedure

1. Click **Settings > System > Device Information**.
2. View the device information.

Back Top

6.6.2 Viewing the Diagnosis Information

Procedure

1. Click **Settings > System > Diagnosis**.
2. View the diagnosis information.

Back Top

6.6.3 Parameters Backup or Recovery

Procedure

1. Click **Settings > System > Configuration**.
2. Backup or recover the configuration parameters.
   1. Backup parameters: Click **Backup** to export the configuration parameters to file.
   2. Recover parameters:
      1. Click **Browse** to select the exported configuration file.
      2. Click **Restore** to recover the configuration.

Back Top

6.6.4 Changing the Password

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

Procedure

1. Click **Settings > System > Modify Password**.
2. Enter the current password, and then enter the new password and confirm it.
3. Click **Modify**.

Back Top

6.6.5 Restoring the Factory Defaults

After this operation, all personal settings are deleted and all web-based management settings and parameters will be restored to their default values.

Procedure

1. Click **Settings > System > Restore Defaults.**
2. Click **Restore**.

NOTE:
After this operation, all personal settings are deleted and all web-based management settings and parameters will be restored to their default values.

Back Top

6.6.6 Restarting the Device

Procedure

1. Click **Settings > System > Reboot**.
2. Click **Reboot**.

Back Top

7 Appendixes

7.1 Abbreviations

2G	The Second Generation
3G	The Third Generation
AP	Access Point
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name Server
IP	Internet Protocol
MAC	Media Access Control
PIN	Personal Identification Number
SIM	Subscriber Identity Module
SSID	Service Set Identifier
TCP	Transmission Control Protocol

UDP	User Datagram Protocol
UPnP	Universal Plug and Play
USIM	UMTS Subscriber Identity Module
WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network
WiFi	Wireless Fidelity

Back Top

7.2 FAQ (Frequently Asked Questions)

What can I do if the Client connected with the AP(Access Point) cannot access the Internet?

1. Check and ensure that the Client is connected to the AP properly.
2. Check the power status to ensure that the device is powered on.
3. Check the signal strength to ensure that the area is covered by the network.
4. Check whether the network mode is correct. For information about the network mode, see "6.2.3 Mobile Network Settings".
5. You must configure the connection profile correctly when you access the Internet through the device. Check whether they are correct, and see "6.2.2 Profile Management" for details.
6. If the device still can not access the Internet after the DHCP service is disabled and the PC obtains the IP address dynamically, you can change the mode to manually assign an IP address. For details, see "6.4.3 Configuring the Client (Take Windows XP PC for Example)."
7. Check whether the network adapter of your Client is running properly.
8. If the problem still persists, consult you service provider for assistance.

What can I do if the Client cannot access the WLAN?

1. If interferences or shields near the device exist, you can adjust the position of the device.
2. Check and record the following data of your Client and your AP: SSID, WLAN encryption type, and key.
3. Use a computer to connect to the device using a USB cable and enter http://e5.home to access the web management interface.
4. Compare the recorded data. The SSID of the Client should be ANY or be the same as that of the AP. The WLAN encryption type and key of the Client and AP should be the same. Otherwise, you need to change the data either in the client or the device to match them.

What can I do if I forgot the default IP address of the management page?

1. If your computer can not connect to the device via Wi-Fi, connect to it by using a USB cable first.
2. You can then enter http://e5.home; and log in to the management page if your computer uses DHCP to obtain its IP address or.
3. On a Windows computer, bring up the command prompt and enter ipconfig. The gateway address is the address of the web management interface.

Back Top