i503W Indoor Station

User Manual

V1.0

Table of Contents

Foreword

Introduction

This manual introduces the installation, functions and operations of the indoor station (hereinafter referred to as "the Device"). Please read carefully before using the Device, and keep the manual for future reference.

Symbol Conventions

The symbols that might be found in this guide are defined as follows.

Symbol	Description
⚠ DANGER	Indicates a hazardous situation that, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, could result in property damage, data loss, performance degradation, or unexpected results.
TIP	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Changes	Release Date
V1.0	First release.	January 2026

About the Manual

- The Manual is for reference only. Slight differences might be found between the manual and the Device.
- We are not liable for losses incurred due to operating the Device in ways that are not in compliance with the manual.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Safety Instructions

Read all safety instructions carefully before installing or using the Device. Failure to follow these instructions may result in personal injury, equipment damage, or property loss.

- Use only the power adapter specified for this product. If a power adapter from another manufacturer must be used due to special circumstances, ensure that its rated voltage and current meet the product specifications, and that it is certified by recognized safety authorities. Using an incompatible or uncertified power adapter may result in fire or electric shock.
- Do not bend, twist, stretch, pull, bundle, place heavy objects on, or pinch the power cord. A damaged power cord may cause fire or electric shock.
- Before using the product, ensure that the ambient temperature and humidity meet the operating requirements specified for the Device. If the product is moved from an air-conditioned environment to a warmer or more humid environment, condensation may form on the surface or inside the device. In this case, allow the Device to dry naturally before powering it on.
- Do not disassemble or repair the product unless you are authorized technical service personnel. Improper disassembly or repair may result in electric shock, fire, or other hazards, and will void the product warranty.
- Do not insert metal objects, such as pins or wires, into the ventilation openings or slots of the Device. Contact between metal objects and internal electrical components may cause electric shock or injury. If any foreign object enters the Device, stop using it immediately and contact technical support.
- Keep plastic packaging bags out of the reach of children. Plastic bags may cause suffocation if placed over the head and block the nose and mouth.
- Do not continue to charge or use a battery that is swollen or leaking. Dispose of the battery properly, as it poses a fire risk.
- Use the product strictly in accordance with the instructions provided in this manual. Prolonged improper operation may result in device damage or safety hazards.

Chapter 1 Product Introduction

1.1 Overview

The i503W is a compact indoor station with a 2.8-inch display. It supports battery-powered operation, remote door unlocking, and home broadcasting for simple, secure, and efficient communication in homes and offices.

NOTE

- The manual serves as a reference guide for the better comprehension and operation of the Device.
- The manual may not reflect the latest software version. For assistance, you can refer to the Device's built-in help interface or download the latest user manual from the Fanvil official website.

1.2 Specification

Table 1-1 Product specification

Model	**i503W**
Applications	Residential communities, offices, villas
Display	2.8-inch IPS color display, resolution 320 × 240 pixels
Casing Material	ABS + PC
Button	5 programmable physical buttons
Speaker	5 W multimedia speaker
Battery Capacity	2600 mAh (typical capacity); 2470 mAh (rated capacity)
Wi-Fi	2.4 GHz / 5 GHz, Wi-Fi 6
Power Supply	5 VDC, 2 A
Operating Temperature	−20 °C to +60 °C (−4 °F to +140 °F)
Storage Temperature	−30 °C to +70 °C (−22 °F to +158 °F)

Operating Humidity	10% to 90% (RH)
Product Dimension	129.5 mm × 59.6 mm × 67.5 mm (5.10" × 2.35" ×2.66") (L × W × H)

1.3 Packing List

Figure 1-1 Packing list

NOTE

The removable battery is pre-installed inside the Device.

Chapter 2 Getting Started

2.1 Button Introduction

The Device is equipped with five physical buttons on the top.

Figure 2-1 Top view

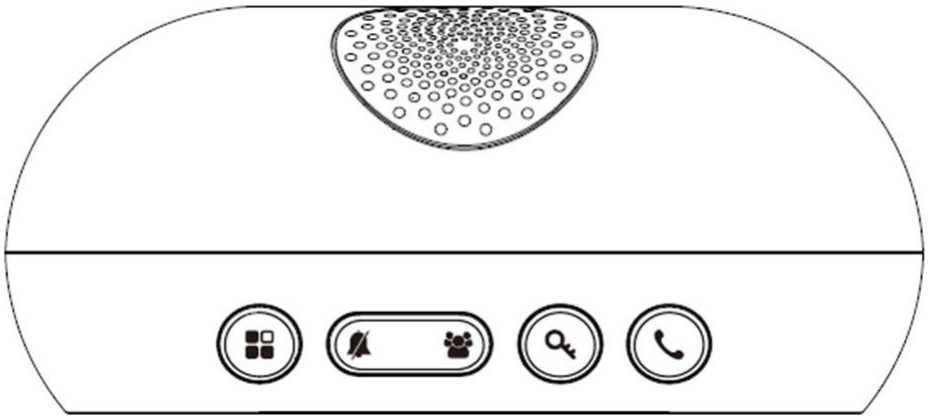


Table 2-1 Button description

Icon	Description
	• Press on the home screen to go to the menu screen. • On the home screen, press and hold for 3 seconds to power off the Device; press and hold for 10 seconds to restart the Device. • Press and hold for 3 seconds to power on the Device.
	Press to enable or disable the DND mode. In this mode, the Device rejects all incoming calls.
	Press to call indoor stations on the same network.
	Press to unlock the door.
	Press to answer an incoming call or hang up the current call.

2.2 Setup Wizard

When powering on the Device for the first time or after a factory reset, you follow the setup wizard to configure language, time zone, Wi-Fi, auto-discovery, and app registration.

Procedure

1. Press and hold to power on the Device.

   After powered on, the screen displays illustrations for the five physical buttons. Press any button to continue through the introduction.

Table 2-2 Button illustration

2. Select the language and time zone.
3. Configure Wi-Fi.

   After configuration, the Device can communicate with door phone or the App. For details, see *2.2.1 Configuring Wi-Fi*.

4. Configure auto-discovery.

   The Device automatically discovers other kit devices on the same network. For details, see *2.2.2 Auto Discovery*.

5. Download and register the App for communication.

   For details, see *2.2.3 Downloading and Registering Fanvil Link App*.

2.2.1 Configuring Wi-Fi

Network configuration is required for the Device before communicating with the App or other devices. A QR code for Wi-Fi connection will display on the screen when you have selected language and time zone.

Procedure

1. Open the camera or the QR code scanner on your mobile phone, and then point it to the QR code on the Device.

   When the QR code is recognized, the phone will prompt **Join WLAN Network "i503W_xxxxxx"?**.

2. Tap **Join**.

   After a few seconds, the phone will go to the Wi-Fi configuration interface.

> **NOTE**
>
> You can also go to **Settings** > **WLAN** on your mobile phone, and then select **i503W_xxxxxx** to go to the Wi-Fi configuration interface.

3. Configure Wi-Fi.
   - Select a Wi-Fi from the list

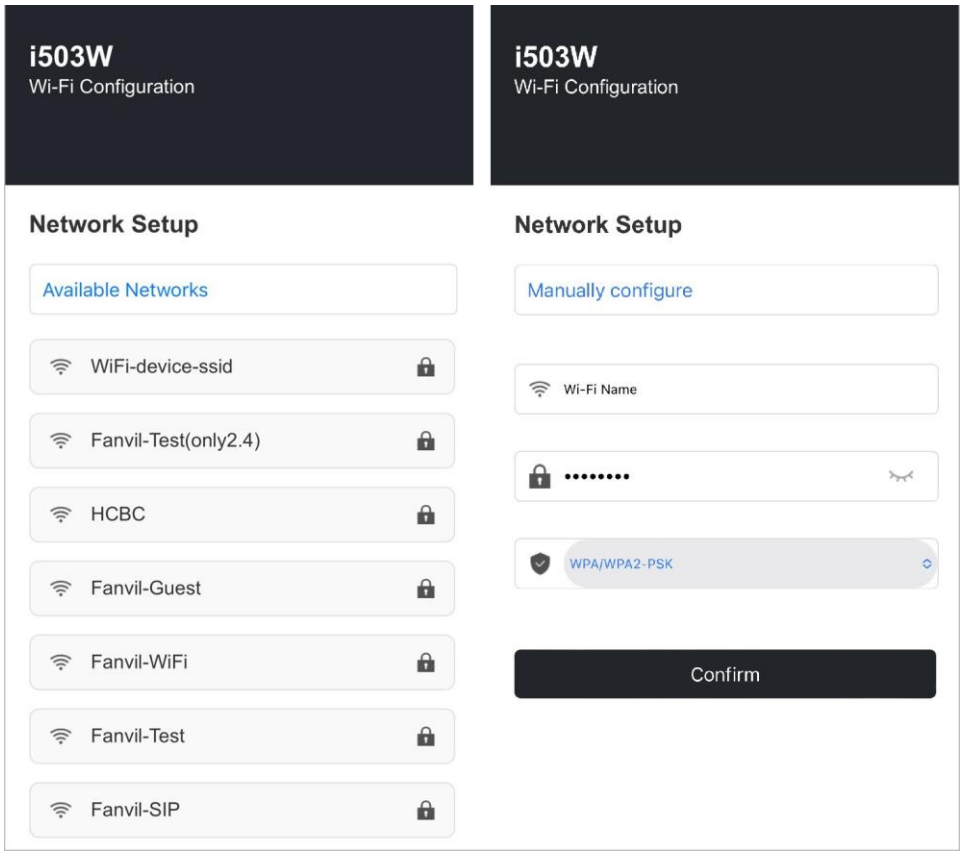
     Select a Wi-Fi from the **Available Networks** list, enter the password, and then tap **Confirm**. The Device displays **Connecting**. After a few seconds, the Device displays **Connect Success**.

   - Add a Wi-Fi manually

     1. Tap **Available Networks**, and then select **Manually configure**.
     2. Enter the Wi-Fi name and password, and then tap **Confirm**.

        The Device displays **Connecting**. After a few seconds, the Device displays **Connect Success**.

Table 2-3 Wi-Fi configuration interfaces



2.2.2 Auto Discovery

The Device can automatically discover other devices in the kit, which can be bound to the Fanvil Link App.

NOTE

Ensure that these devices are powered on and on the same network segment as the Device.

2.2.3 Downloading and Registering Fanvil Link App

Procedure

1. Open the camera or the QR code scanner on your mobile phone, and then scan the QR code on the Device to download the Fanvil Link app.

   NOTE

   You can also download the app from App Store, Google Play, or the Fanvil official website.

2. Open the app, and then tap on the login screen to scan the QR code on the Device.

   The app will display the account registration screen.

3. Register with your phone number or email address, and then set and confirm the login password.

   After setting the password, you will see the home screen of the app.

2.3 Selecting Language

The default language is English. You can select the desired language in the setup wizard, on the Device or via the web interface.

Procedure

- In the setup wizard

  After a factory reset, select the desired language in the setup wizard, and then press the **OK** or **Next** button.

- On the Device

  1. On the Device's home screen, press the button, select **Language**, and then press the **OK** button.
  2. Select the desired language, and then press the **OK** button.

     The screen displays **Config OK!** in the set language.

- Via the web interface

  You can log in to the Device's web interface using a mobile phone or computer. Ensure that your mobile phone and computer are on the same network segment as the Device.

  - Log in on a mobile phone

    1. On the Device's home screen, press the button, select **Settings**, and then press the **OK** button.

2. Open the camera or the QR code scanner on your mobile phone, and then point it to the QR code on the Device.

   The phone will go to the Device's login screen.

3. Enter the username and password, and then tap **Login**.

   > **NOTE**
   >
   > The username and password are both **admin**.

4. Tap **System** on the Device's webpage, and then select the language.

   The Device's screen displays **Config OK!** in the set language.

- Log in on a computer

  1. Log in to the Device's webpage. For details, see *2.7 Web Login*.
  2. Select the language from the drop-down list in the top-right corner.

     The Device's screen displays **Config OK!** in the set language.

2.4 Home Screen

The home screen is set as the start screen of the Device.

Figure 2-4 Home screen

Figure 2-2 Description of home screen

NO.	Description
1	Displays battery level, network connection status, and other system statuses.
2	Displays date and time.

2.5 Menu Screen

On the menu screen, you can configure function key, network, language, SIP account, and more. Press the button to go to the menu screen.

Table 2-3 Description of menu screen

Menu	Description
Function Key	Press the function key to trigger an action that you have assigned to it on the Device's webpage.
Network	View network information, including the network type, IP address, Wi-Fi SSID, and more.
Device	View device information, including the model, MAC address, software version, and hardware version.
Account	Check the registration status of the SIP line.
Settings	Set the network, language, and time zone on the mobile phone.
Wi-Fi QR Code	Configure Wi-Fi network on the mobile phone.
Language	Set the language for the Device.
Reboot System	Restart the Device.
Advanced Settings	Includes auto discovery, factory reset, and USB drive debugging. ⚠ **CAUTION** A factory reset will erase all configurations and saved data.

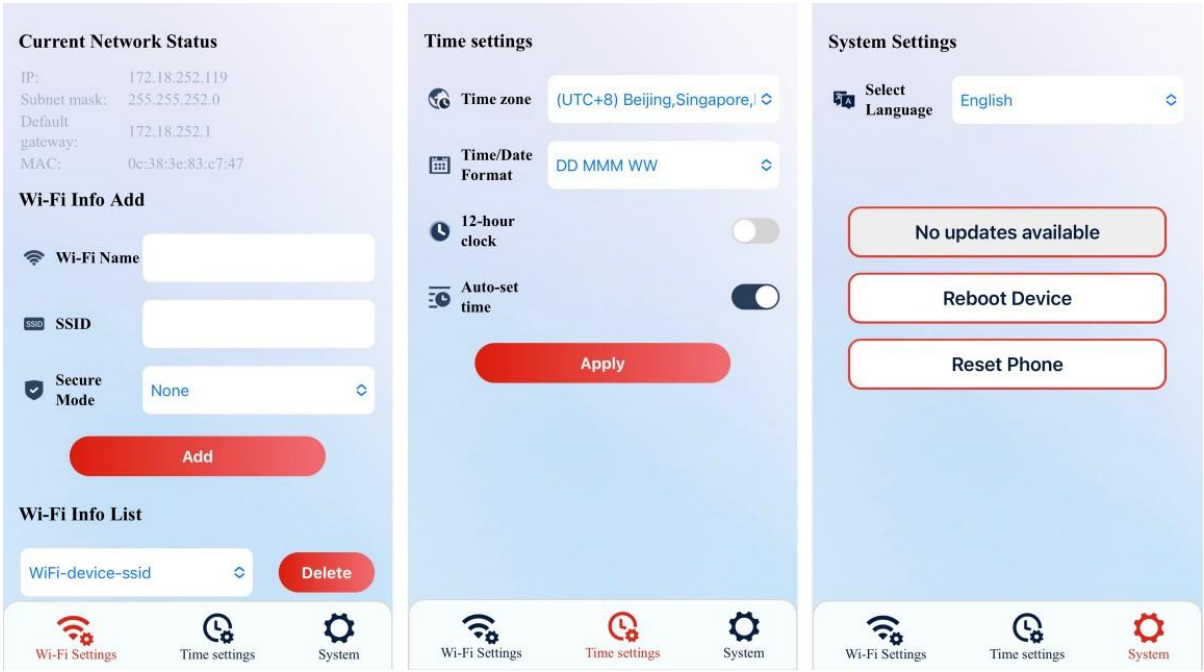
2.5.1 Function Keys

The Device's function keys can be configured for various actions via the web interface, such as speed dial and door unlock. After configuration, press the function key on the Device to trigger a configured action. For details, see *Chapter 13 Function Keys*.

2.5.2 Settings

There is a QR code on the **Settings** screen. Scan the QR code with your mobile phone to log in to the webpage and configure Wi-Fi, language, time zone, and more. For detailed information on login with a mobile phone, see *2.3 Selecting Language*.

Figure 2-5 Webpage interface on the mobile phone



2.5.3 Advanced Settings

- Auto discovery

  The Device is able to discover other devices on the same network. You can select the discovered devices and scan the QR code to bind them to the Fanvil Link App.

- Factory reset

  1. On the Device's home screen, press the button, select **Advanced**, and then press the **OK** button.

     The screen displays **Reset to Default?**

  2. Press the **OK** button to restore the Device to factory settings or press the **Cancel** button to cancel the operation.

- USB drive debugging

  Prerequisites

  Please ensure that you have inserted the USB.

  - **U-Disk Log Export**: Export the debugging logs.

- **U-Disk Config Update**: Update the configuration file.
- **U-Disk Wi-Fi Config Update**: Update Wi-Fi configuration.

2.6 Device Status

You can view device status on the Device or via the web interface.

- On the Device

  On the Device's home screen, press the button to go to the menu screen.

- Via the web interface

  On the Device's home page, select **System** > **Information**.

Table 2-4 Parameter description of device status

Access Method	Parameter	Description
On the Device	Network	Displays network type, IP address, Wi-Fi SSID, and more
	Device	Displays the model, MAC address, software version, and hardware version.
	Account	Displays the registration status of each SIP line.
Via the web interface	System Information	Displays device model, hardware and software versions, uptime, and more.
	Network	Displays MAC address, IP address, subnet mask, gateway, and more.
	SIP Accounts	Displays the name, number, and registration status of SIP line.

2.7 Web Login

2.7.1 Obtaining IP Address

You can find the Device's IP address on the Device or by using an IP scanner tool **(Device Manager**) on the computer.

Procedure

- On the Device

  On the Device's home screen, press the button, select **Network**, and then press **OK** to view its IP address (e.g., 192.168.1.100).

- IP scanner

  1. Go to our official website *https://fanvil.com*, and then select **Support** > **Download Center** > **Tools** > **IP Scanner**.
  2. Click to download the latest version of the tool.
  3. Open the tool, and then click **Rescan** to view the Device's IP address.

2.7.2 Logging in to the Webpage

Log in to the Device's webpage to view or configure parameters.

Prerequisites

You have obtained the IP address of the Device.

Procedure

1. Open a web browser on your computer (such as Chrome, Edge, Safari).
2. Enter the Device's IP address in the browser's address bar, and then press the Enter key.
3. Enter username and password, select the language, and then click **Login**.

NOTE

- Ensure that the computer and the Device are on the same network segment.
- The default username and password are both **admin**.
- Click the checkbox on the right to synchronize the set language to the Device.

Chapter 3 Basic Calling Features

3.1 Making Calls

The Device supports configuring speed dial numbers on the function keys, allowing you to quickly make a call to the configured number on the Device.

Prerequisites

You have configured the number via the Device's web interface. For details, see *Chapter 13 Function Keys*.

Procedure

1. On the Device home screen, press the button, select **Function Key,** and then press the **OK** button.
2. Select the desired number.
3. Press the **OK** button.

   The Device calls the selected number.

3.2 Answering Calls

When the Device receive an incoming call, press the **Answer** button to answer the incoming call. Press the **End** button to hang up the current call.

3.3 Rejecting Calls

You can reject a call manually or by enabling DND.

3.3.1 Rejecting a call manually

Press the **Reject** button to reject an incoming call.

3.3.2 DND

You can enable the do not disturb (DND) mode on the Device or via the web interface. After enabled, the Device automatically rejects an incoming call.

Procedure

- On the Device
  1. On the Device's home screen, Press the button.

The screen displays **Do you want to enable DND?**.

2. Press the **OK** button to enable DND.

   The screen displays **DND enabled**.

3. Press the button again to exit the DND mode.

   The screen displays **DND disabled**.

- Via the web interface

1. On the Device's home page, select **Device Settings** > **Features** > **DND Settings**.
2. Select **Device** or **Line** from the DND option, select ☐ to enable DND timer, and then set the time interval.
3. Click **Apply**.

3.4 Ending Calls

If you want to end the current call, press the **End** button to hang up.

3.5 Adjusting Volume

- During a call, press the **Vol.+** button to turn up the volume.
- During a call, press the **Vol.−** button to turn down the volume.

3.6 One-Touch Family Call

In a home environment, family members in different rooms may need to communicate with one another. The one-touch family call feature allows the user to call all supported devices at once by pressing the button. When a one-touch family call is initiated, devices in different rooms automatically answer the call, enabling real-time voice communication throughout the home.

Chapter 4 Advanced Calling Features

4.1 Holding and Resuming Calls

During a call, you can put the call on hold to temporarily mute audio in both directions.

- On the call screen, press the **Hold** button to put the call on hold.
- On the call screen, press the **Hold** button to resume the call.

4.2 Call Forwarding

Call forwarding is a feature that redirects incoming calls to another number. You can configure call forwarding individually for each line via the web interface.

There are three types of call forwarding:

- **Unconditional forwarding**: All incoming calls are forwarded to the configured number.
- **Busy forwarding**: When the user is busy (on another call), incoming calls are forwarded to the configured number.
- **No-Answer forwarding**: If the user does not answer within a set timeout period, incoming calls are forwarded to the configured number.

Procedure

1. On the Device's home page, select **Line** > **SIP** > **Basic Settings**.
2. Select the line from the **Line** drop-down list.
3. Select ☐ to enable the desired forwarding type, and then enter the target number for forwarding.
4. Click **Apply**.

4.3 Intercom

The Intercom function allows for instant and hands-free audio communication between devices. When Intercom mode is enabled, the device can automatically answer incoming intercom calls.

4.3.1 Making Intercom Calls

To quickly make an intercom call, you need to configure the function key via the web interface. After configuration, you can make an intercom call on the **Function Key** screen of the Device.

Procedure

1. On the Device's home page, select **Function Key** > **Function Key**.
2. Select **Memory Key** from the **Type** drop-down list, and then select **Intercom** from the **Subtype** drop-down list.
3. Configure the line, name, and number.
4. Click **Apply**.

4.3.2 Answering Intercom Calls

You can enable the intercom function and configure parameters via the web interface. After enabled, the Device automatically answers incoming intercom calls.

Procedure

1. On the Device's home page, select **Device Settings**> **Features** > **Intercom Settings**.
2. Configure the parameters.
3. Click **Apply**.

Table 4-1 Parameter description of intercom

Parameter	Description
Enable Intercom	When enabled, the Device will automatically answer incoming calls that contain the specific SIP `Call-Info` header indicating an intercom request.
Enable Intercom Mute	Enables or disables the mute function during an intercom call.
Enable Intercom Tone	Plays an alert tone when an intercom call is received.
Enable Intercom Barge	When enabled, if the current call is not an intercom call, the Device automatically answers the new intercom call; if the current call is an intercom call, the Device rejects the new intercom call.

4.4 Multicast

The Multicast function enables efficient one-to-many audio broadcasting. A source server sends an RTP stream once to a specific multicast group address, and all devices configured to listen to that address will receive and play the stream simultaneously. You can configure multicast parameters via the web interface.

Procedure

1. On the Device's home page, select **Device Settings** > **MCAST**.
2. Configure the parameters.
3. Click **Apply**.

Table 4-2 Parameter description of multicast

Parameter	Description
SIP Priority / Intercom Priority	Defines the call priority when a multicast call is received during an existing call.
Mcast Listening Renew Time	The waiting time before the Device attempts to re-listen to the multicast stream after an interruption.
Multicast Tone	When enabled, a short beep tone plays before the multicast audio starts.
Enable Page Priority	When enabled, if two multicast streams arrive simultaneously, the device will answer the one with the higher priority.
Enable Prio Chan	When enabled, a connection is established only if both the port and channel match. Channel 24 is the highest priority, and channel 0 indicates not matching the channel.
Enable Emer Chan	When enabled, Channel 25 is given the highest priority.
Name	Set a name for the multicast.
Host:port	Enter the server address and port of the multicast.
Channel	0–25. • 24: priority channel • 25: emergency channel

MCAST Dynamic	Multicast configuration can be delivered dynamically via SIP NOTIFY messages. After receiving such a message, the Device automatically adds the configuration to its system to start listening to the specified multicast stream, or removes the configuration to stop listening.

4.5 SIP Hotspot

The SIP hotspot function creates a simple virtual SIP extension group. One device serves as the hotspot server (Device A), registering a main SIP account with the service provider. Other devices serve as hotspot clients (Device B and Device C), sharing this SIP account.

- **Incoming calls**: When the Device A receives an incoming call, all devices (Devices A, B, and C) in the hotspot group ring simultaneously. Once any one device answers, the ringing on all devices stops, and the remaining devices hang up.
- **Outgoing calls:** When any client device (Device B or Device C) makes an outgoing call, it uses the SIP account of the hotspot server (Device A).

NOTE

Extension numbers:

- The hotspot server is automatically assigned extension 0.
- Hotspot clients are automatically assigned extensions starting from 1 (incrementally).
- Devices within the same hotspot can call each other using these extensions (e.g., extension 1 dials extension 0).

You can configure SIP hotspot for the SIP server and SIP client via the web interface.

Procedure

- SIP server
  1. On the Device's home page, select **Line** > **SIP Hotspot**.
  2. Configure the parameters.
  3. Click **Apply**.
- SIP client

  Select the **Mode** as **Client**, and then the Device will be automatically configured as a SIP client.

Table 4-3 Parameter description of SIP hotspot

Parameter	Description
Enable Hotspot	Select **Enabled** from the drop-down list to enable the hotspot function.
Mode	• **Hotspot**: The Device serves as the SIP server. • **Client**: The Device serves as the SIP client.
Monitor Type	Includes **Broadcast** and **Multicast**. Defines how server and clients discover and communicate. Server and clients must be set to the same monitor type. Select **Multicast** allows reducing broadcast traffic.
Monitor Address	The IP address used for the communication between server and clients. Required only if **Monitoring Type** is **Multicast**. The system uses the WAN port's broadcast address when **Broadcast** is selected.
Local Port	The port for hotspot communication, which must be identical between server and clients.
Name	Set a unique name for the hotspot server to prevent conflicts in networks with multiple hotspots.
Line Settings	Select desired SIP line to enable SIP hotspot.

4.6 Text Message

If the SIP server supports short message service (SMS), the Device will receive notifications for incoming text messages. A new message alert will display on the Device's home screen.

Procedure

1. When the Device notifies a new message, press any button to open the inbox.
2. Select the unread message, and then press the **View** button to view the message.

Chapter 5 Door Unlock

The device can be bound to door phones via auto-discovery. You can then:

- Unlock a single door.
- Unlock multiple doors (if multiple devices are bound).
- Unlock the door for a device during a call.

5.1 Door Unlock on the Home Screen

5.1.1 Unlocking the Door

- For one door phone: Press the button to directly unlock the door.
- For multiple door phones: Prees the button to go to the **Door Access List**, select the desired device, and then press the **OK** button to unlock the door.

5.1.2 Configuring Door Unlock

You can add door phones via the web interface, including third-party devices or those on a different network.

Procedure

1. On the Device's home page, select **Application** > **Open the Door** > **Door Unlock Settings**.
2. Configure the name, IP address (or URL), username, and password of the door phone.
3. Click **Apply**.
4. On the Device's home screen, press the button to go the access control list.

NOTE

- For Fanvil door phones, enter the door phone's IP address or URL.
- For the third-party door phones, enter the door phone's URL.

5.2 Door Unlock on the Call Screen

5.2.1 Unlocking the Door

You can press the **Open** button to unlock the door for the door phone that is on a call with the Device.

5.2.2 Configuring Door Unlock

Procedure

1. On the Device's home page, select **Application** > **Doorphone Settings**.
2. Click **Add**, configure the parameters, and then click **OK**.
3. Click **Apply**.

Table 5-1 Parameter description of door unlock

Parameter	Description
Title	Set a custom name for the door phone.
Number	The IP address or SIP number of the door phone. Use IP address only for direct IP calls.
Line	Select the SIP line. **Auto** by default.
Password & Access Code	The password to remotely unlock the door, which must match the door release password configured on the door phone.

Chapter 6 Preview and Monitoring

6.1 Video Preview for Incoming Calls

Video preview allows you to see video from a door phone or a bound IP camera before answering the call. You can enable this function by configuring **SIP Video Preview** via the web interface.

Procedure

- SIP Line
  1. On the Device's home page, select **Line** >**SIP** > **Advanced Settings**.
  2. Click **Enable Preview**, and then select the **Preview** Mode.
     - **Preview18x**: Standard SIP video preview.
     - **Preview2XX**: Use only with Fanvil door phones.
  3. Click **Apply**.
- Direct IP dialing
  1. On the Device's home page, select **Line** > **Basic Settings** > **SIP P2P Settings**
  2. Click **Enable Preview**, and then select the **Preview** Mode.
     - **Preview18x**: Standard SIP video preview.
     - **Preview2XX**: Use only with Fanvil door phones.
  3. Click **Apply**.

Chapter 7 Phonebook

7.1 Adding Blocklist

The blocklist is used to reject calls from specific numbers. When numbers added to the blocklist call the Device, the system automatically rejects the call, and a missed call record will be displayed on the Device.

You can configure the blocklist via the web interface.

Procedure

1. On the Device's home page, select **Phonebook** > **Call List** > **Restricted Incoming Calls**.
2. Click **Add,** and then configure **Number**, **Line**, and **Number/Prefix**.
3. Click **OK**.

7.2 Adding Allowlist

The Device supports an incoming call allowlist. When a number is added to the allowlist, calls from this number can still be received even when DND or call forwarding is enabled. Calls from numbers not on the allowlist will be automatically rejected or forwarded.

The configuration of allowlist is similar to that of blocklist. For details, see *7.2 Adding Blocklist*.

7.3 Configuring Restricted Outgoing Calls

The Device allows outgoing call restrictions. Calls to restricted numbers are blocked, and the Device plays a call restriction tone and displays a pop-up notification. You can configure the function via the web interface.

Procedure

1. On the Device's home page, Select **Phonebook** > **Call List** > **Restricted Outgoing Calls**.
2. Click **Add**, and then configure **Number**, **Line**, and **Number/Prefix**.
3. Click **OK**.

Chapter 8 Call Logs

Call logs allow you to view and delete all incoming, outgoing, forwarded, and missed calls on the Device or via the web interface.

Procedure

- View call logs

  The Device can store up to 1,000 call records.

  - On the Device

    1. When the Device displays a missed call, press any button to go to the **Miss** screen.
    2. Press the **Up** or **Down** button to view all missed calls.

  - Via the web interface

    On the Device's home page, select **Call Logs** to view all calls.

    > **TIP**
    >
    > Select a call type from the drop-down list to view corresponding call records.

- Delete call logs

  1. On the Device's home page, select **Call Logs**.
  2. Select one or more records, and then click **Delete**. Click **Delete All** to delete all records.

Chapter 9 Device Functions

9.1 Time Plan

Time plan enables scheduling of automated device actions at a precise time or across a defined time range, allowing tasks like reboots or upgrades to be performed automatically.

NOTE

If the Device is on a call within the scheduled time period, restarting and upgrading will be skipped.

Procedure

1. On the Device's home page, select **Device Settings** > **Time Plan**.
2. Configure the parameters.
3. Click **Apply**.

Table 9-1 Parameter description of time plan

Parameter	Description
Name	Set a custom name for the action rule.
Type	The action to perform, including **Timed reboot**, **Timed upgrade**, **Timed forward**, and **Timed config**.
Repetition Period	Sets the recurrence pattern. • **No Repetition**: Executes once within the set time range. • **Daily**: Executes at the same time every day. • **Weekly**: Executes on the same weekday(s) every week. • **Monthly**: Executes on the same date every month.
Start Date	The date when the rule becomes active.
End Date	The date when the rule expires.
Effective Time	The effective time period for action execution.

9.2 Action Plan

Action plan is a Fanvil-defined technology that enables event-triggered control and linkage between Fanvil terminals and other devices. It allows the terminal to automatically execute predefined actions when specified events occur.

Procedure

1. On the Device's home page, select **Line** > **Action Plan**.
2. Configure the parameters.
3. Click **Apply**.

Table 9-2 Parameter description of action plan

Parameter	Description
Action	The action to perform when the rule is triggered. • **Video**: Displays video feed from a bound third-party camera during an incoming or active call. • **Mcast-Xfer**: Transfers the multicast. • **Mute**: Automatically mutes the Device. • **Answer**: Automatically answers the incoming call.
Number	The calling number that triggers this rule. Supports the same expression format as **Dial Plan**.
Type	• **Early**: Displays the video before the call is answered. • **Connected**: Displays the video after the call is answered.
Direction	• **Both**: For both incoming and outgoing calls. • **Incoming Call**: For the incoming calls only. • **Outgoing Call**: For the outgoing calls only.
Line	The SIP line to which this rule applies.
Username	The username for the RTSP authentication.
Password	The password for the RTSP authentication.
URL	(For **Video** action) The RTSP URL of the camera.
User Agent	User agent information.

9.3 System Maintenance

9.3.1 Managing System Configurations

Administrators can import, export, and clear device configurations, and restore the Device to factory settings in **System** > **Configurations**.

Table 9-3 Parameter description of system configurations

Operation	Description
Export configurations	Click to export the configuration file in .txt format.
Import configurations	Upload a previously saved configuration file to apply its settings to the Device.
Clear configurations	Clears SIP settings, auto-provisioning configurations, and shortcut keys.
Clear user data	Clears the local phonebook, call records, and blocklist and allowlist.
Reset Device	Erases all device data, including all configurations and database tables, restoring the device to its original state.

9.3.2 Upgrade

9.3.2.1 Upgrading Software Version

Procedure

1. On the Device's home page, select **System** > **Upgrade**.
2. Click **Select,** and then select a software version file.
3. Click **Upgrade**.

9.3.2.2 Upgrading Server

Places the upgrade .txt file and software on the corresponding server. When the device detects that the software on the server differs from its own version, it will prompt for an upgrade.

Procedure

1. On the Device's home page, select **System** > **Upgrade**.
2. Configure the parameters.

3. Click **Apply**.

Table 9-4 Parameter description of server upgrade

Parameter	Description
Upgrade Server	
Enable Auto Upgrade	When selected, the Device will periodically check the configured HTTP server for a new version.
Upgrade Server Address1	The URL of the main HTTP upgrade server.
Upgrade Server Address2	(Optional) The URL of a backup upgrade server.
Update Interval	The frequency at which the Device checks for new versions.
Firmware Information	
Current Software Version	The currently installed software version.
Server Firmware Version	The currently installed firmware version available on the server.
Upgrade	Becomes active when a newer version is detected. Click to upgrade to the new version.
New Firmware Information	Displays update information from the server's version file when available.

4. Place the firmware file (.z file) and a corresponding version information file on your HTTP server.
    - The version file must be named in this format: vendor_model_hwv1_0.txt
    - The .txt file must be UTF-8 encoded and contain the following information.

```
Version=2.12.0
Firmware=http://ip:port/xxx.z
BuildTime=2023.09.11 20:00
Info=TXT

Release Note:
Xxxxx
Xxxxx
Xxxxx
```

- When the update interval arrives, if new files are on the server, the device prompts the user who can then upgrade. The web UI also enables its upgrade button with release notes.

9.3.3 Auto-Provisioning

The Device supports four methods to obtain auto-provisioning parameters:

- **SIP plug-and-play (PnP)**
- **DHCP**
- **Static provisioning**
- **TR-069**

If all four methods are configured simultaneously, the Device will acquire the auto-provisioning parameters at startup according to the following procedure or priority: **SIP PnP** > **DHCP** > **TR-069** > **Static provisioning**

Supported protocols: FTP, TFTP, HTTP, and HTTPS

Procedure

1. On the Device's home page, select **System** > **Auto Provision**.
2. Configure the Parameters.
3. Click **Apply**.

Table 9-5 Parameter description of auto-provisioning

Parameter	Description
Basic Settings	
CPE Serial Number	Displays the serial number of the Device.

Authentication Name	The username for the FTP server. Not required for TFTP protocol. If using FTP and this field is left blank, the default is set to **anonymous**.
Authentication Password	Password for the FTP user.
Configuration File Encryption Key	If the configuration file to be upgraded is encrypted, enter its decryption key here.
General Configuration File Encryption Key	If the common configuration file to be upgraded is encrypted, enter its decryption key here.
Download Fail Check Times	The number of times the Device retries after a failed download. Default: 1.
Update Contact Interval	The preset interval at which the Device automatically downloads and updates the phonebook.
Save Auto Provision Information	Select ☐ to save the auto-provisioning information.
Download CommonConfig enabled	Select ☐ to download the common configuration file during automatic upgrading.
Enable Server Digest	If the Device uses Digest authentication to match configuration content, enabling this will trigger an update download whenever the configuration on the server is modified, or if the local configuration differs from the server's.
Display Provision Prompt	Settings for displaying upgrade prompt dialogs.

Provision Config Priority	Sets the priority between auto-provisioning and manual configuration.
DHCP Option	
Option Value	DHCP option used to obtain auto-provisioning parameters, supporting **Custom Option**, **Option 66**, and **Option 43**. **Disabled** is set by default.
Custom Option Value	The valid range for a custom option is 128 to 254. The custom option type must match the definition on the DHCP server.
Enable DHCP Option 120	Enables setting the SIP server address via DHCP Option 120.
DHCPv6 Option	
Option Value	DHCP option used to obtain auto-provisioning parameters, supporting **Custom Option**, **Option 66**, and **Option 43**. **Option 66** is set by default.
Custom Option Value	The valid range for a custom option is 128 to 254. The custom option type must match the definition on the DHCP server.
SIP Plug and Play (PnP)	
Enable SIP PnP	When enabled, the terminal will periodically send SIP SUBSCRIBE messages via multicast upon startup. Any compatible SIP server will respond with a SIP NOTIFY message containing the path to the auto-configuration or auto-provisioning server, from which the terminal can obtain the configuration file to download.
Server Address	The IP address of the PnP server.
Server Port	The port of the PnP server.
Transport Protocol	The transport protocol for PnP.
Update Interval	The interval (in hours) for checking updates.
Plug and Play	

Auto Discover	When enabled, the Device scans the LAN for door phones and indoor stations that have auto-discovery enabled and automatically configures them.
Device Name	The name of the Device.
Device Location	Devices in the same location can be discovered.
Static Server	
Server Address	The address of the FTP/TFTP/HTTP server. It can be an IP address (e.g., 192.168.1.1) or a domain name (e.g., ftp.domain.com). The system also supports specifying a subdirectory path (e.g., 192.168.1.1/ftp/Config/ or ftp.domain.com/ftp/config), meaning it will access the server at the given address or domain, with the file storage path under the specified subdirectory. A trailing slash is optional.
Configuration File Name	The name of the configuration file to download. For typical auto-provisioning, leave this field empty. The Device will then use its own MAC address as the filename to retrieve the file from the server.
Protocol Type	The server type: **FTP**, **TFTP**, **HTTP**, **and HTTPS**.
Update Interval	The interval (in hours) for checking updates.
Update Mode	The auto-update type. • **Disabled**: No update. • **Update After Reboot**: Update after the Device reboots. • **Update at Time Interval**: Updates at the specified interval.
Autoprovisioning Now	Click to start auto-provisioning.
TR069	
Enable TR069	Select ☐ to enable TR069.
ACS Server Type	Select the ACS server type. Supports **China Telecom**, **Common**, **China Unicom**, **eSight**, and **Reliance Jio**.
ACS Server URL	The URL of the ACS server.
ACS User	The username for ACS server authentication.

ACS Password	The password for ACS server authentication.
Enable TR069 Warning Tone	Select ☐ to enable TR069 prompt tone.
TLS Version	If "Auto Login" is selected, the Device will use the previously entered credentials to connect to the ACS server upon reboot without prompting for username and password.
INFORM Sending Period	The interval at which the Device periodically sends an INFORM message to the ACS server.
STUN Server Address	The address of the STUN server.
STUN Enable	Select ☐ to enable STUN.

Chapter 10 Preferences

You can configure date & time, screen and display, wallpaper, and other features on the Device or via the web interface.

10.1 Configuring Date & Time

Procedure

- On the Device
  1. On the Device home screen, press the button, select **Settings,** and then press the **OK** button.
  2. Scan the QR code on the screen to set date and time. For details, see *2.52 Settings*.
- Via the web interface
  1. On the Device's home page, select **Device Settings** > **Time/Date**.
  2. Configure the parameters.
  3. Click **Apply**.

Table 10-1 Parameter description of date & time

Parameter	Description
Network Time Server Settings	
Time Synchronized via SNTP	Enable time synchronization using the SNTP protocol.
Time Synchronized via DHCP	Enable time synchronization using the DHCP protocol.
Time Synchronized via DHCPv6	Enable time synchronization using the DHCPv6 protocol.
Primary Time Server	The address of the primary network time protocol (NTP) server.

Secondary Time Server	The address of the backup NTP server. The Device will attempt to synchronize with this server if the primary is unavailable.
Time zone	Select your local time zone.
Resync Period	The interval at which the Device re-synchronizes with the time server.
Time/Date Format	
12-hour clock	When enabled, displays time in a 12-hour format (AM/PM).
Time/Date Format	Set the display format for the date.
Daylight Saving Time Settings	
Location	Select your geographic location for automatic daylight saving time (DST) rules.
DST Set Type	• **Disabled**: DST adjustments are not applied. • **Manual**: Configure DST start and end times manually. • **Automatical**: DST rules are automatically applied based on the selected Location. When set to **Automatical**, the start and end parameters become read-only.
Fixed Type	Defines how the DST start/end dates are specified. • **By Date**: Set an exact calendar date (e.g., March 31). • **By Week**: Set a relative day (e.g., Second Sunday of March).
Offset	The amount of time to adjust the clock at the start and end of DST (e.g., +1 hour at the start, −1 hour at the end).
Start and End	• **By Date**: Configure **Month**, **Month day**, and **Hour**. • **By Week**: Configure **Month**, **Week**, **Weekday**, and **Hour**.
Manual Time Settings	Manually set the current date and time.

10.2 Screen and Display Settings

You can configure the brightness, wall paper, and other parameters on the Device.

10.2.1 Configuring Brightness and Backlight

The device enters backlight mode after a period of no operation. You can configure brightness and backlight via the web interface.

Procedure.

1. On the Device's home page, select **Device Settings** > **Advanced** > **Screen Configuration**.
2. Configure the parameters.
3. Click **Apply**.

Table 10-2 Parameter description of brightness and backlight

Parameter	Description
Backlight Active Level	The screen brightness level when the Device is active.
Backlight Inactive Level	The screen brightness level when the Device is idle.
Backlight Time	Screen backlight turns off after a period of inactivity.

10.2.2 Configuring Wallpaper

Procedure

1. Log in to the Device's web page, and then select **System** > **Upgrade** > **Background Upgrade**.
2. Click **Select** to select an image, and then click **Upload**.

The image format is as follows:

- Image Format: .bmp, .png, .jpg
- Resolution: 320 × 240
- Bit Depth: 24-bit

10.2.3 Configuring Boot Logo

Procedure

1. Log in to the Device's web page, and then select **System** > **Upgrade** > **Boot Logo Upgrade**.
2. Click **Select** to select an image, and then click **Upload**.

The image format is as follows:

- Image Format: .bmp
- Resolution: 320 × 240
- Bit Depth: 24-bit

10.3 Audio Settings

10.3.1 Selecting Ringtone

You can configure ringtone volume via the web interface.

Procedure

1. On the Device's home page, select **Device Settings** > **Media Settings** > **Media Settings**.
2. Selet a ringtone type from the **Default Ring Type** drop-down list.
3. Click **Apply**.

10.3.2 Adjusting Volume

You can adjust the device volume via the web interface.

1. On the Device's home page, select **Device Settings** > **Media Settings** > **Media Settings**.
2. Configure the volume parameters.
3. Click **Apply**.

Table 10-3 Parameter description of volume adjustment

Parameter	Description
Speakerphone Ring Volume	Volume for the incoming call ringtone and door open tone.
Speakerphone Volume	Volume for hands-free calls.

10.3.3 Configuring Alert Info

You can assign specific ringtones for calls containing Alert Info headers via the web interface.

Procedure

1. On the Device's home page, select **Device Settings** > **Media Settings** > **Alert Info Ring Settings**.
2. Configure the parameters.

3. Click **Apply**.

Table 10-4 Parameter description of alert information

Parameter	Description
Value	Defines a value for a specific ringtone type. When an incoming INVITE message contains an Alert Info header matching this value, the assigned ringtone plays.
Line	Enable the Alert Info rule on the selected SIP line.
Ringtone Type	Select a ringtone type for the Alert Info value.

10.3.4 Configuring Tones

You can configure various call tones via the web interface, such as call hold tone, call waiting tone, auto-answer tone.

Procedure

1. On the Device's home page, select **Device Settings** > **Features** > **Tone Settings**.
2. Configure the parameters.
3. Click **Apply**.

Table 10-5 Parameter description of tones configuration

Parameter	Description
Enable Holding Tone	Plays a tone when a call is placed on hold. It is enabled by default.
Enable Call Waiting Tone	Plays a tone when a second call arrives during an active call. It is enabled by default.
Play Dialing DTMF Tone	Plays a DTMF tone when pressing keys to dial.

Play Talking DTMF Tone	Plays a DTMF tone when pressing keys during a call. It is enabled by default.
Auto Answer Tone	Plays a prompt tone when a call is auto-answered.
Ring Back Tone	Set the ringback tone heard by the caller. You can configure custom ringback tone in **System** > **Upgrade** > **Ring Upgrade**.
Busy Tone	Set the fast busy tone indicating network congestion or failure. You can configure custom ringback tone in **System** > **Upgrade** > **Ring Upgrade**.

10.3.5 Uploading Ringtone

Procedure

1. On the Device's home page, select **Device Settings** > **Upgrade** > **Ring Upgrade**.
2. Click **Select** to select a ringtone file, and then click **Upload**.

Ringtone file specifications:

- Supported formats: .wav
- Maximum file size: 1 MB

Chapter 11 Network Settings

11.1 Wireless Network

The Device can be connected to Wi-Fi on the Device or via the web interface.

Procedure

- On the Device

  You can use the mobile phone to scan the QR code on the Device for Wi-Fi connection. For details, see *2.2.1 Configuring Wi-Fi*.

- Via the web interface

  1. On the Device's home page, select **Network** > **Wi-Fi Settings**.
  2. Select ☐ to enable the Wi-Fi function, and then click **Apply**.
  3. Configure **SSID**, **Secure Mode**, and **Password**.
  4. Click **Add**.

     The Connected Wi-Fi information displays in **Wi-Fi Info List**.

11.2 Network Mode

The network mode can be set to IPv4, IPv6, or both. You can configure it via the web interface.

Procedure

1. On the Device's home page, select **Network** > **Basic** > **Network Mode**.
2. Select the desired network mode from the drop-down list.
3. Click **Apply**.

Table 11-1 Parameter description of network mode

Parameter	Description
IPv4	Uses Internet Protocol version 4 only.
IPv6	Uses Internet Protocol version 6 only.
IPv4 & IPv6	Uses both protocols simultaneously.

11.3 Web Server

Configure the protocol and security for the Device's web management interface.

Procedure

1. On the Device's home page, select **Network** > **Service Port**.
2. Configure the parameters.
3. Click **Apply**.

Table 11-2 Parameter description of web server

Parameter	Description
Web Server Type	Select **HTTP** or **HTTPS**. A restart is required for changes to take effect.
Web Login Timeout	The period of inactivity before the web interface is logged out. The default value is 15 minutes.
Web auto login	If enabled, the browser automatically logs in to the web interface after a timeout. You do not need to enter username and password again.
HTTP Port	The TCP port for HTTP access. The default value is 80. Format: `http://device-ip:port`. For security, the port value can be custom.
HTTPS Port	The TCP port for HTTPS access. The default value is 443. Format: `http://device-ip:port`. For security, the port value can be custom.

11.4 VPN

- Virtual private network (VPN) creates a secure tunnel to a private network over the public Internet.
- The Device supports connecting to a VPN via L2TP and OpenVPN, and you can configure them via the web interface.

NOTE

Both L2TP and OpenVPN connections automatically reconnect after the Device restarts, unless manually disabled.

Procedure

- Configuring L2TP

1. On the Device's home page, select **Network** > **VPN**.
2. Select ☐ to enable VPN function, and then select ◯ to enable **L2TP**.
3. In Configure **L2TP Server Address**, **Authentication Name**, and **Authentication Password**.
4. Click **Apply**.

   The Device attempts to connect. Once connected, the assigned VPN IP address will display in **Virtual Private Network (VPN) Status**.

> **NOTE**
>
> L2TP on the Device only supports basic unencrypted authentication and data transmission. If data encryption is required, use the OpenVPN.

- Configuring OpenVPN

  1. Obtain the following files from your OpenVPN service provider:
     - OpenVPN configuration File: client.ovpn
     - CA Root Certification: ca.crt
     - Client Certification: client.crt
     - Client Key: client.key
  2. On the Device's home page, select **Network** > **VPN**.
  3. Select ☐ to enable VPN function, and then select ◯ to enable **OpenVPN**.
  4. Click **Select** to select a VPN file, and then click **Upload**.

11.5 VLAN

Virtual local area network (VLAN) allows a single physical LAN to be divided into multiple logical LANs—VLANs. Each VLAN forms a separate broadcast domain, with broadcast packets confined within the VLAN. The Device supports obtaining VLAN IDs via DHCP VLAN.

Procedure

1. On the Device's home page, select **Network** > **Advanced** > **DHCP VLAN Settings**.
2. Select **Custom** from the **Option Value** drop-down list, and then set the value for **DHCP Option Vlan**.
3. Click **Apply**.

Chapter 12 System Security

12.1 Changing Web Login Password

Change the password for logging into the Device's web interface. You can change it on the Device.

Procedure

1. On the Device's home page, select **System** > **Account** > **Add New User**.
2. Enter the current password, new password, and then confirm the new password.
3. Click **Apply**.

> **NOTE**
>
> After changing the password, the user will be automatically logged out of the web interface. Please log in again with the new password.

12.2 Filtering Web Access

You can create an allowlist of IP address ranges permitted to access the web interface.

Procedure

1. On the Device's home page, select **Security** > **Web Filter**.
2. Enter the starting IP address and the ending IP address in **Start IP Address** and **End IP Address** fields.
3. Select ☐ to enable the function.
4. Click **Apply**.

Related Operations

Click **Delete** to delete the IP current address range.

> **NOTE**
>
> If your computer is on the same network as the Device, ensure its IP address falls within an allowed range. Otherwise, you cannot log in to the web interface after saving the configuration.

12.3 Mutual Authentication

Enable and manage certificates for secure, encrypted HTTPS and SIP TLS connections with mutual authentication.

Procedure

- Manage device certificates

  1. On the Device's home page, select **Security** > **Device Certificates**.
  2. Configure the parameters.
  3. Click **Apply**.

Table 12-1 Parameter description of device certificates

Parameter	Description
Device Certificates	The identity certificate that the Device presents to servers, include **Default Certificates** or **Custom Certificates**.
Import Certificates	Upload the custom device certificate. **NOTE** You can upload only one device certificate.
Certification File	Displays the uploaded custom certificate. The list is empty if no custom certificate is uploaded.

- Manage trusted certificates

  1. On the Device's home page, select **Security** > **Trust Certificates**.
  2. Configure the parameters.
  3. Click **Apply**.

Table 12-2 Parameter description of trusted certificates

Parameter	Description
Permission Certificate	Used to verify whether server certificate authentication is enabled.
Common Name Validation	Specifies whether to enable common name verification.
Certificate Mode	• **All Certificates**: Trust both custom and built-in certificates. • **Default Certificates**: Trust only the Device's built-in certificates • **Custom Certificates**: Trust only the uploaded certificates.
Import Certificates	Upload the server certificate to the trusted list.
Certificates List	Displays uploaded trusted certificates.

NOTE

- Upload the device certificate to the server's trusted certificate list, and ensure that the server's trusted certificate list contains the device's certificate. Please confirm this with the server administrator.
- On the Device's home page, select **Security** > **Trusted Certificates** >**Import Certificates**, upload the server's certificate to the Device's trusted certificate list, and then select the trusted certificate module to be used.

12.4 Network Firewall

Configure inbound and outbound firewall rules to control network access, prevent malicious traffic, and enhance system security. Each rule is assigned a unique sequence number, with up to 10 rules allowed for each rule type.

Procedure

1. On the Device's home page, select **Security** > **Firewall**.
2. Configure the parameters.
3. Click **Add**.

Table 12-3 Parameter description of network firewall

Parameter	Description
Enable Input Rules	Select ☐ to enable **Input Rules**.
Enable Output Rules	Select ☐ to enable **Output Rules**.
Input/Output	• **Input**: The traffic to the Device. • **Output**: The traffic from the Device.
Deny/Permit	Select **Permit** to enable the rule.
Src Port Range	The source port range.
Dst Port Range	The destination port range.
Src Address	The source IP address. It can be a host address, network address, or **0.0.0.0** (all addresses).
Dst Address	The destination IP address. It can be a host address, network address, or **0.0.0.0** (all addresses).
Src Mask	The source subnet mask. When it is set to **255.255.255.255**, it indicates a specific host. When it is set to a subnet mask such as **255.255.255.0**, it indicates that a network segment is being filtered.
Dst Mask	The destination subnet mask. When it is set to **255.255.255.255**, it indicates a specific host. When it is set to a subnet mask such as **255.255.255.0**, it indicates that a network segment is being filtered.

Chapter 13 Function Keys

13.1 Setting Function Keys

The Device supports configuring multiple function keys to perform specific functions. You can configure function keys via the web interface.

Procedure

1. On the Device's home page, select **Function Key** > **Function Key**.
2. Select a type of function key, and then configure the parameters.
3. Click **Apply**.

Table 13-1 Parameter description of function keys setting

Type	Subtype	Description
Memory Key		
	Speed Dial	In standby mode, press the button to immediately dial a configured number.
	Intercom	Calls the configured number in intercom mode. If the called party is configured to receive intercom calls, the call will be answered automatically.
Key Event		
	Voice Mail	Displays detailed voicemail information for all SIP lines.
	DND	Enters the DND settings screen to enable or disable the DND function.
	Phonebook	Holds or resumes the current call.
	Redial	Redials the last outgoing number.
	Call Forward	Enters the call forwarding screen.
	Logs	Enters the call logs screen to view the history of incoming, outgoing, and missed calls.

	SMS	Enters the text message screen.
	Call Back	Dials the number of the last received incoming call.
	Intercom	Opens the dial pad to manually enter a number for an intercom call.
	Prefix	Tap to automatically add a configured number prefix to the dialed number.
	Disposition	A method of recording call information in a call center, relied on Broadsoft server.
	Escalate	During a call, sends a specific SIP message to the server to request escalation, relied on Broadsoft server.
	Trace	During a call, sends a specific SIP message to the server to request escalation, relied on Broadsoft server.
	Handfree	Enters hands-free dialing or switch to hands-free mode.
	Local Contacts	Enters the local contact list screen.
	XML Group	Enters the cloud contact list screen.
DTMF	/	During a call, press the button to send the configured DTMF tone sequence to the remote party.
URL	/	Accesses the configured remote URL, such as an XML phonebook address.
MCAST Paging	/	After configuring the multicast address and audio codec, press the button to send multicast paging.
Action URL	/	Performs basic call operations on the Device using a specific URL.
MCAST Listening	/	The Device listens to and plays the audio stream from a configured multicast IP address and port.

13.2 Setting Softkeys

You can configure softkeys via the web interface.

Procedure

1. On the Device's home page, select **Function Key** > **Softkey**.
2. Configure the parameters.
3. Click **Apply**.

Table 13-2 Parameter description of Softkeys setting

Parameters	Description
Softkey Mode	Includes **Disabled** and **More**. The default mode is **More**.
Softkey Exit Style	The position of the softkey, including left and right.
Screen	
Call Dialer	Redial/2aB/Delete/Exit/Call Back/Dial/Join/MWI/Local Contacts/Pickup/Call Log/Missed/Clear/ln/Dialed/Pause/ Next line/Prevline/Headset/Audio/Video/Remote XML/DSS Key
Conference	Hold/Split/End/Release/Mute/DSS Key/Headset
Desktop	Call Log/Menu/Local Contacts/DND/Prev Account/Next Account/Blocked List/Call Back/Call Forward/Locked/Memo/Missed/MWI/Dialed/Reboot/Redial/Remote XML/SMS/Headset/Status/DSS Key/ln
Divert Dialer	Redial/2aB/Delete/Exit/Forward/Local Contacts/Call Log/Clear/Missed/Dialed/Headset/Video/Audio/Remote XML/DSS Key
Ending	Redial/End/Headset/Release/DSS Key
Predictive Dialer	Dial/2aB/Delete/Exit/Call Back/Local Contacts/Redial/Pickup/MWI/Join/Call Log/Release/Missed/Pause/Dialed/Headset/Video/Audio/Remote XML/DSS Key/ln/Next line/Prev line
Ringing	Answer/Forward/Reject/Mute/Release/Headset/Video/Audio/DSS key
Talking	Hold/Transfer/Conference/End/Mute/Release/New Call/Local Contacts/Listen/Call Log/Next call/Prev call/Private/Headset/Video/Audio/DSS Key
Transfer Alerting	End/Transfer/Headset/Release/DSS Key
Transfer Dialer	Redial/Delete/Exit/2aB/Dial/Local Contacts/Transfer/Call Log/Clear/Missed/Dialed/Pause/Headset/Video/Audio/Remote XML/DSS Key
Trying	End/Release/Headset/DSS Key

Waiting	Hold/Transfer/Conference/End/Answer/Forward/Mute/Next call/New call/Prev. call/Reject/Release/Headset/Listen/Video/Audio/DSS Key

Chapter 14 Troubleshooting

When the Device malfunctions or operates abnormally, you can try the following methods to restore normal operation or collect relevant information and send a problem report directly to the technical support email.

14.1 Viewing System Status

You can view the Device's current state, network, and account information via the web interface.

On the Device's home page, select **System** > **Information**.

14.2 Restarting the Device

Procedure

- On the Device
  1. On the Device home screen, press the button, select **Reboot System,** and then press the **OK** button.

     The Device displays **Reboot Now?**.
  2. Click **OK**.

     You can also press and hold the button for 10 seconds to restart the Device.
- Via the web interface
  1. On the Device's home page, select **System** > **Reboot Device**.
  2. Click **Reboot**.
  3. Click **OK**.

14.3 Restoring Factory Settings

You can restore the Device to the factory settings on the Device or via the web interface.

- On the Device

  On the Device home screen, press the button, select **Reset to Default,** and then press the **OK** button.
- Via the web interface
  1. On the Device's home page, select **System** > **Configurations** > **Reset Device**.
  2. Click **Reset**.
  3. Click **OK**.

14.4 Capturing Screenshots

If the Device encounters a problem, capturing a screenshot can help technical personnel locate the relevant function and clearly identify the issue.

Procedure

1. On the Device's home page, select **System** > **Tools** > **Screenshot**.
2. Tap **Save BMP** to save the current screenshot of the Device.

14.5 Capturing Network Packets

Packet capture allows you to record network traffic to analyze call setup, registration failures, or other network-related issues.

Procedure

1. On the Device's home page, select **System** > **Tools**.
2. Click **Start** under **WLAN Packet Capture**.

   The web browser will open a download dialog, prompting you to save the packet capture file locally.
3. Click **Save** to save the offered capture file.
4. Reproduce the issue.

   For example: Make a call or register SIP account.
5. Return to the web page and click **Stop**.

   The saved file contains all network packets during that period.

14.6 Exporting Logs

The Device supports exporting system logs and Wi-Fi logs.

Procedure

- Export system logs
  1. On the Device's home page, select **System** > **Tools** > **Syslog**.
  2. Select ☐ to enable **Syslog**, and then select **Debug** from the **App Log Level** drop-down list.
  3. Select ☐ to enable **Export Log**, and then click **Apply**.
  4. Reproduce the issue, and then click **Export Log**.
- Export Wi-Fi logs
  1. On the Device's home page, select **System** > **Tools** > **WLAN Log**.

2. Select ☐ to enable **WLAN Log**, and then click **Apply**.
3. Reproduce the issue, and then click **Export Log**.

14.7 Common Issues

Table 14-1 Parameter description of common issues

Issue	Solution
The Device fails to power on	1. **Power Source**: Ensure you are using a Fanvil-approved power adapter or a standard-compliant PoE switch. Check all physical connections. 2. **POST Mode**: If the Device boots into POST mode, the system may be corrupted. Contact Fanvil support for recovery.
The Device fails to register with service provider	1. **Network Connection**: Verify the network cable is properly connected. 2. **IP Address**: Check the Device's system information. If the IP address displays **Negotiating…**, the Device has no IP. Please review your network settings. 3. **SIP Configuration**: Double-check all SIP account settings, including username, password, and server address. 4. **Service Provider**: If all else seems correct, contact your service provider or see *14.5 Capturing Network Packets* to collect data for Fanvil support analysis.

Chapter 15 Appendix

15.1 Appendix I—Status and Notification Icons

Table 15-1 Icon description of status and notification

Icon	Description
	Auto Answer
	Call Forwarding
	DND
	Enable Hotspot
	Missed Call
	Mute
	Enable VLAN
	Enable VPN
	IP Conflict
	Unread SMS
	Unread Voice Message
	Wi-Fi Connection Error
	Wi-Fi Connected
	Network Storm
	USB Drive