


# i504&i506 User Manual

Version: 2.12 | Date: 2024.4.12

## Directory


**Directory** ..... **1**

**1 Safety Instruction** ..... **6**

1.1 Safety Instruction ..... 6

1.2 FCC ..... 7

**2 Product Overview** ..... **9**

2.1 Overview ..... 9

2.2 Specification Parameter ..... 10

**3 Installation Instructions** ..... **11**

3.1 Device Inventory ..... 11

3.2 Installation Procedure ..... 11

3.2.1 Wall-mounted ..... 11

**4 User Guide** ..... **14**

4.1 Button and Interface Instructions ..... 14

4.2 Setup Guide ..... 15

4.3 Language Settings ..... 15

4.4 Standby Screen Instructions ..... 15

4.5 Touchscreen Instructions ..... 16

4.5.1 Touch Method ..... 16

4.5.2 Touch Keyboard ..... 17

4.6 Menu Introduction ..... 17

4.7 Device Status ..... 18

4.8 Web Management ..... 19

4.8.1 Device IP Address ..... 19

4.8.2 Web Interface ..... 19

4.9 Line Settings ..... 20

**5 Call Features** ..... **21**

5.1 Making Calls ..... 21

5.1.1 Making Calls ..... 21

5.1.2 IP Call ..... 21

5.2 Answer Call ..... 22
5.2.1 Answer Call ..... 22
5.2.2 Auto Answer ..... 22
5.3 Reject The Call ..... 23
5.3.1 Manually Reject ..... 23
5.3.2 DND ..... 23
5.4 End The Call ..... 23
5.5 Mute ..... 23
5.5.1 Mute The Call ..... 24
5.5.2 Ringing Mute ..... 24
5.6 Call Hold/Resume ..... 24
5.7 Call Forward ..... 24
**6 Advance Function ..... 26**
6.1 Intercom ..... 26
6.1.1 Initiate Intercom. ..... 26
6.1.2 Intercom Call ..... 26
6.2 MCAST ..... 27
6.3 Hotspot ..... 28
6.3.1 Hotspot ..... 28
6.3.2 Hotspot Extension Management ..... 30
6.4 SMS ..... 30
6.4.1 SMS ..... 31
6.4.2 Voice Message ..... 31
**7 Open Door ..... 33**
7.1 Open The Door Under Standby ..... 33
7.1.1 Open The Door Under Standby ..... 33
7.1.2 Settings Of Open The Door Under Standby ..... 33
7.2 Open the door during a call ..... 34
7.2.1 Open The Door During A Call ..... 34
7.2.2 Settings Of Open The Door During A Call ..... 34
**8 Video Preview ..... 36**

8.1 Video Preview ..... 36
8.2 Monitor ..... 36
8.2.1 Manual Addition ..... 37
8.2.2 Scan Addition ..... 37
8.3 Video Linkage ..... 38
**9 Contacts ..... 39**
9.1 DoorPhone List ..... 39
9.2 Local Phonebook ..... 40
9.2.1 Add/ Edit / Delete Contact ..... 40
9.2.2 Add/ Edit / Delete Group ..... 41
9.2.3 Browse/ Add /Delete Contacts In Group ..... 42
9.3 Cloud Phonebook ..... 42
9.3.1 Configure Cloud Phonebook ..... 43
9.3.2 Downloading Cloud Phonebook ..... 43
9.4 Blocked List ..... 43
9.5 Allowed List ..... 44
9.6 Restricted Outgoning List ..... 45
**10 Call Log ..... 46**
**11 Device Settings ..... 47**
11.1 Time Plan ..... 47
11.2 Action Plan ..... 48
11.3 Maintenance ..... 49
11.3.1 Configurations ..... 49
11.3.2 Upgrade ..... 49
11.3.3 Auto Provision ..... 51
**12 Screen Setting ..... 56**
12.1 Time Settings ..... 56
12.2 Screen Setting ..... 57
12.2.1 Brightness and backlight ..... 57
12.2.2 Screen Saver ..... 58
12.2.3 UI Settings ..... 59

12.2.4 Screen Saver ..... 60
12.3 Audio Settings ..... 60
12.3.1 Ring Setting ..... 60
12.3.2 Volume Setting ..... 61
12.3.3 Alert Info Ring Setting ..... 61
12.3.4 Tone Setting ..... 62
12.3.5 Upload Ring ..... 63
12.4 Greeting Words Setting ..... 63
**13 Function Key Settings ..... 65**
13.1 Function Key ..... 65
13.2 Wireless Key(Only i506(W) Support it) ..... 67
13.2.1 Scan To Add ..... 67
13.2.2 Manual Addtion ..... 68
**14 Network Settings ..... 70**
14.1 Ethernet Connection ..... 70
14.2 Wireless Network ..... 71
14.3 Network Mode ..... 71
14.4 Network Server ..... 72
14.5 VPN ..... 72
14.6 VLAN ..... 74
**15 Security Settings ..... 76**
15.1 Alarm Input ..... 76
15.2 Short-circuit Input ..... 77
15.3 Relay Output ..... 79
**16 Security ..... 81**
16.1 Menu Password ..... 81
16.2 Web Password ..... 81
16.3 Security Password ..... 82
16.4 Web Filter ..... 82
16.5 Mutual Authentication ..... 83
16.6 Network Firewall ..... 84

**17 Trouble Shooting** ..... **87**

17.1 Get Device System Information ..... 87

17.2 Reboot Device ..... 87

17.3 Device Factory Reset ..... 87

17.4 Screenshot ..... 88

17.5 Network Packets Capture ..... 88

17.6 Get Device Log ..... 88

17.7 Common Trouble Cases ..... 89

**18 Appendix Table** ..... **91**

18.1 Appendix I - Function Icon ..... 91

18.2 Appendix II - Menu Icon ..... 91

18.3 Appendix III - Status And Notification Icon ..... 92

18.4 Appendix IV - Function Key Status Definition ..... 93

18.5 Appendix V – Keyboard Character Lookup Table ..... 94

# 1 Safety Instruction

## 1.1 Safety Instruction

Please read the following safety notices before installing or using this unit. They are crucial for the safe and reliable operation of the device.

- Please use the product-specified power adapter. If you need to use a power adapter provided by another manufacturer due to special circumstances, please confirm that the voltage and current of the provided adapter meet the specifications of this product, and it is recommended to use a product that has passed safety certification, otherwise it may cause fire or electric shock accidents. When using this product, do not damage the power cord, do not twist, stretch and strap it, and do not press it under heavy objects or sandwich between items, otherwise it may cause fire or electric shock caused by broken power cord.
- Before using the product, please confirm that the temperature and humidity of the environment in which it is located meet the working needs of the product. (Moving this product from the air-conditioner to the natural temperature, the surface or internal components of this product may produce condensate vapor, and the product needs to be dried naturally before turning on the power supply.)
- Do not attempt to open it. Non-expert handling of the device could damage it. Consult your authorized dealer for help, or else it may cause fire, electric shock and breakdown.
- Please refrain from inserting metal objects such as pins or wires into the vents or crevices. Doing so may cause electric shock accidents due to the passage of current through the metal objects. If foreign objects or similar metallic items fall inside the product, usage should be stopped promptly.
- Please do not discard or store the plastic bags used for packaging in places accessible to children to prevent them from covering their heads, leading to obstruction of the nose and mouth, which may cause suffocation.

- Do not install this phone in an ill-ventilated place. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

## 1.2 FCC

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received; including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

• Reorient or relocate the receiving antenna.

• Increase the separation between the equipment and receiver.

• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

• Consult the dealer or an experienced radio/TV technician for help.

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

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled

environment. This equipment should be installed and operated with minimum distance of 20cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

# 2 Product Overview

## 2.1 Overview

i504&i504W is an indoor station with 7-inch color touch screen and rich interfaces. i506W is an indoor station with 10.1-inch color touch screen and rich interfaces. It is mainly used in residential area, villa, office building and other places for receiving calls and communicating through the door phone and achieving remote door-opening. It provides more reliable security assurance and the easier access control for the users, creating a safe and comfortable living environment.

In order to help some interested users to better understand the details of the product, the user manual can be used as a reference guide for the use of i504&i504W&i506W. This document may not apply to the latest version of the software. If you have any questions, you can use the help prompt interface that comes with the i504&i504W&i506W device, or download and update your user manual from the official website.

## 2.2 Specification Parameter

| Spec. | i504 | i504W | i506W |
|---|---|---|---|
| Material quality | ABS | | |
| Screen | 7” 1024*600 | | 10” 1280*800 |
| Wi-Fi | / | 2.4G/5G | 2.4G/5G |
| Speaker | 2W | | |
| Interface | 8×short-circuit input<br>1×doorbell input.<br>1×short-circuit output<br>1×RS485 | | |
| Network | 10/100 Mbps adaptive | | |
| Operating temperature | -10℃~50℃ | | |
| Size (LWH) | 177.38x113.99x22.5mm | | |
| Wall-mounted | Support | | |

# 3 Installation Instructions

## 3.1 Device Inventory



Indoor Unit



Quick Installation Guide



Wall-mount Bracket



2*3 pin Cable*3



Screw Fixing Seat*4



TA4*30mm Screw*4



KM3*30mm Screw*2



TM6#*20mm Screw*4



PM4*16mm Screw*2

## 3.2 Installation Procedure

### 3.2.1 Wall-mounted

Wall-mount Bracket support：

- Chinese standard:86 Box
- American standard:Single cylinder lateral, Double cylinder
- European standard:80 bottom box

**Installation preparation：**

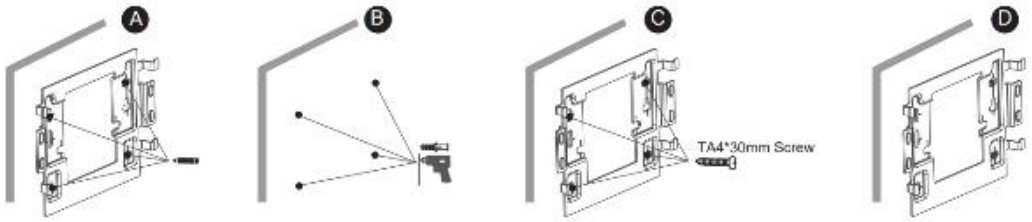
- **Step 1**：Installation of the bracket
  - **There is no junction box on the wall.**

  A. Mark the position of 4 fixing holes on the wall with a wall-mount bracket.

  B. Remove the bracket, use a power drill to drill four holes at the marked positions, and then hammer wall plugs into the holes.

C. Secure the bracket to the wall with four TA4*30mm screws.

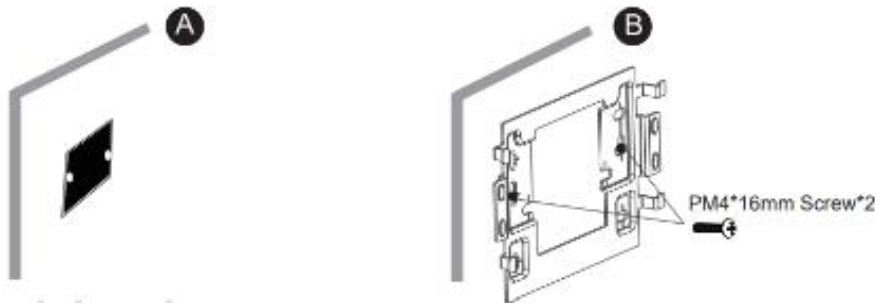
D. Installation of the wall-mount bracket is complete.



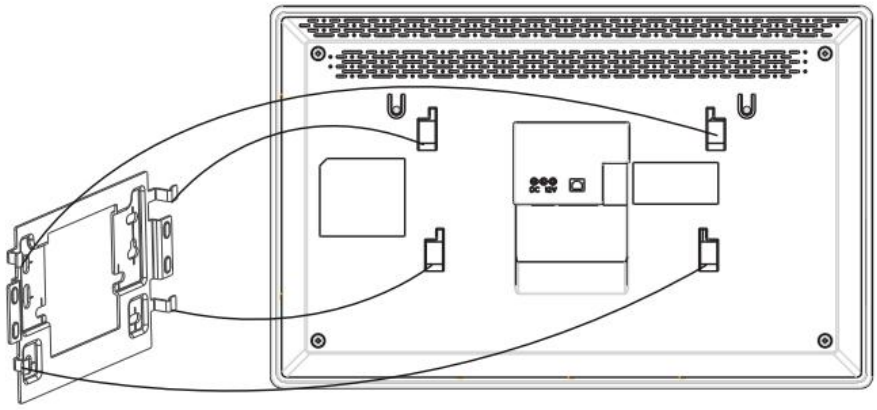

➢ **There is a junction box (86-type) on the wall.**

A. Secure the bracket to the 86 box with two PM4*16mm screws.

B. Installation of the wall-mount bracket is complete.

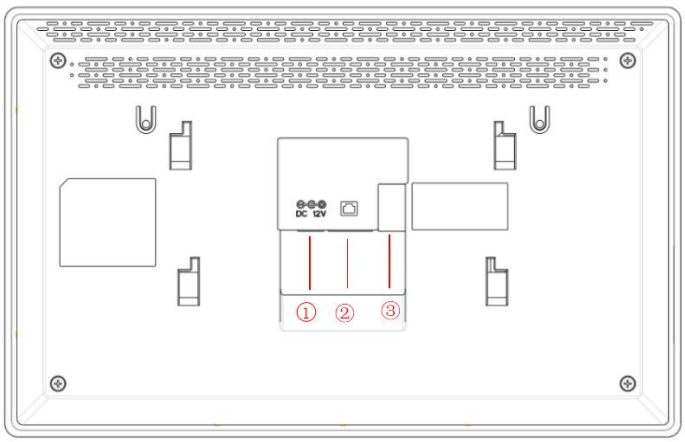


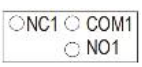
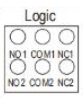

- **Step 2**： Connect peripherals. If additional input or output devices are needed, connect them to the host via the connection cable.
- **Step 3**: Power on the device for testing. If it operates normally, align the slots on the back of the host with the pins on the wall-mount bracket, then slide the host downward to complete the installation.



# 4 User Guide

## 4.1 Button and Interface Instructions




| Number | Name | Description | Interface |
|---|---|---|---|
| ① | Power interface | Power interface:12V/1A input |  |
| ② | Network interface | WAN interface,standard RJ45 interface,10/100M adaptive,support POE input,it is recommended to use CAT5 or CAT5E network cable. |  |
| ③-1 | Power interface | 2-pin, 2.0mm pitch socket, 12V/1A input. |  |
| ③-2 | 1 sets of doorbell interfaces | Can be connected to doorbell. |  |
| ③-3 | 1 sets of short-circuit output interfaces | Corresponding to the short-circuit input interface, login device web page settings, can be connected to electric locks, alarms etc. |  |
| ③-4 | 8 sets of alarm input interfaces | Input devices for connecting switches, infrared sensor, door sensor, vibration sensors etc. |  |

| | | | |
|---|---|---|---|
| ③-5 | 8 sets of alarm input interfaces | RS485 interface(Reserve) |  |

## 4.2 Setup Guide

After the device is powered on for the first time or restored to factory settings, a setup guide will appear. You can set the language, time zone, and network.After selecting the language and time zone in the setup guide interface, click **[Next]** to enter the network settings interface. Depending on the user's network environment, you can choose Ethernet or Wi-Fi, then click **[Finish]** to complete the setup guide.Clicking **[Skip]** or **[Skip All]** will keep the device's default configuration.

## 4.3 Language Settings

The user can set the phone language through the phone interface or web interface.Under factory settings, the initial language defaults to English.

**Set language under factory settings:**

Upon startup under factory settings, the device prompts a language selection dialog in the setup guide interface. Users can choose the desired language and click **[Next]** or they can click **[Skip]** to use the default language. (The default language is English.)

**Set language in the device's menu interface:**

Set language while the device is in standby mode.Click the corresponding button on the screen.**[Menu]**>>**[Settings]**>>**[Basic]**>>**[Language]**

**Set language in the web interface:**

Log in to the device's web page, then set the language from the drop-down menu in the top right corner of the page. 


## 4.4 Standby Screen Instructions

- The following image shows the default standby screen interface, which represents

the status of the user interface for most of the time.

- The icon description is described in 18.1appendix I.




| Number | Description |
|---|---|
| ① | Welcome word, number |
| ② | Time, Date |
| ③ | Status icon |
| ④ | Function Key |
| ⑤ | DND |
| ⑥ | Common Functions |

## 4.5 Touchscreen Instructions

### 4.5.1 Touch Method

- Click:

On any interface, the device can enter the settings and operations interface through a click/tap.

- Slide：

The device allows you to swipe up, down to view information that is not fully displayed on the current screen.

### 4.5.2 Touch Keyboard

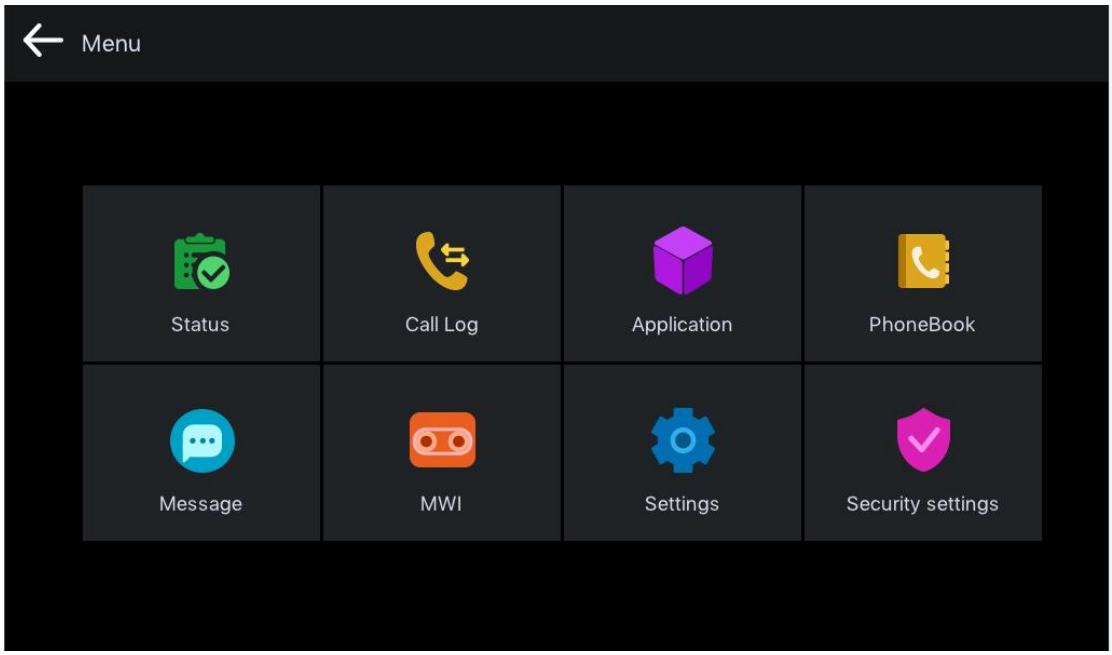
Users can input numbers or set functional parameters through the touchscreen keyboard in interfaces such as dialing and menu settings.

**It supports three types of keyboards:**

1. Numeric keypad, supporting the input of numbers and special characters.
2. Character keyboard, support to enter lowercase letters, uppercase letters and some commonly used characters.

## 4.6 Menu Introduction

On the standby screen, users can press the menu soft key to access the main menu. After entering the main menu,they can select the application icons to access the sub-menus.The main menu is displayed as follows.




| Menu | Description |
|---|---|
| Status | Display device, network, account information, etc. |

| | |
|---|---|
| Call Log | Display device call logs, including incoming, outgoing, missed, and call forwarding logs. |
| Application | Ping, QR code function. |
| PhoneBook | Access local device contacts, cloud phonebook, and access control lists to quickly search for contacts. |
| Message | View and send text messages. |
| MWI | View and listen to voicemail messages. |
| Settings | Preference settings, call settings, network settings, etc. |
| Security settings | Enable security alarm settings. |

## 4.7 Device Status

Users can view the status through the device screen or web interface.

**Viewing the status of through the device menu:**

Go to **[Menu]**>>**[Status],** which allows you to obtain the following status information:

- Common： Display device model, version, IP address, MAC address, and other relevant information.
- Network：Display device's network mode, connection mode,IP address, and other relevant information.
- Account:Provides information about registered accounts on the device, including account names/numbers and registration status.
- Device：Display device's memory size, runtime, software version, and other relevant information.

**Viewing the status through the web interface:**

Refer to the 4.8Web Management login page, go to the**[System]** >> **[Information]** page, and check the device status.

- System: Displays information such as the device model name, hardware version number, software version number, uptime, WAN port speed, memory information, system time, and other details.
- Network: Displays information such as the device's network mode, MAC address,

Ethernet IP, mask, gateway, and other details.

- Account: Displays information about the registered account names/numbers on the device, including registration status and other details.

## 4.8 Web Management

### 4.8.1 Device IP Address

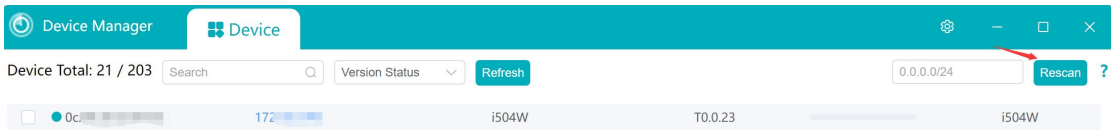
**Retrieve Device IP through Scanning Tool:**

1. Connect the computer and the device to the same local network, and install Device Manager on the PC.

(Device Manager download link:

https://www.fanvil.com/service/doc/soft/tools/tools/ipscanner/index.html);

2. Open the IP scanning tool (Device Manager), click on the scan button to obtain the IP address of the device within the local network.




**To obtain the device IP through the device menu:**

Users can access the device IP address by navigating to the device menu, selecting **[Menu]** >> **[System]** >>**[Network]**.

### 4.8.2 Web Interface

Ensure that the computer and the device are on the same local network. Open a web browser, enter the obtained device IP, log in to the device's web page, and access the login page.

Users must enter the correct username and password to log in to the web page. The default username and password are both "admin."

## 4.9 Line Settings

The device supports six SIP accounts simultaneously, Users can switch between the six SIP accounts as needed.

Users can register SIP accounts through the device menu and the web interface.

**Registering an account through the device menu:**

Users can register SIP account by navigating to **[Menu] >> [Settings] >> [Advanced] >> [Account]**. After configuring the SIP parameters, click **[Save]** to successfully register the account.

**Registering an account through the web interface:**

Users can register a SIPA account through the web page by navigating to **[Line]** >> **[SIP]** >> **[Line]**. selecting the registered line, and registering the SIP account through **[Register Settings]**. After completing the SIP parameter settings, click "Submit" to successfully register.

**SIP Parameters:**

| Parameters | Description |
|---|---|
| Line Status | On this page, the current status of the line is displayed. To obtain the latest online status, users must manually refresh the page. |
| Enable | The status of this line is 'Enabled' |
| Username | Enter the username of the service account. |
| Authentication User | Enter the authentication name of the service account. |
| Display Name | Enter the display name shown when a call request is sent. |
| Authentication Password | Enter the authentication password of the service account. |
| Server Address | Enter the SIP server address. |
| Server Port | Enter the SIP server port. |

# 5 Call Features

## 5.1 Making Calls

### 5.1.1 Making Calls

■ **Dialing method**

Users can dial a number in the following ways:

- Entering the number directly
- Selecting a phone number from phonebook contacts (Refer to 9.2Phonebook).
- Selecting a phone number from cloud phonebook contacts (Refer to 9.3 Cloud Phone Book)
- Selecting a phone number from call logs (Refer to 10 Call Log)

■ **Dial numbers**

Click **[Dialer]**  to enter the dialing screen.Input the desired number on the dialing pad.After inputting the number, users can press **[Audio]**/**[Video]** button to initiate the call.

■ **Cancel call**

When calling a number, the user can press **[End]**  to cancel the call.

### 5.1.2 IP Call

Click **[Dialer]**  to enter the dialing screen.Input the desired IP address on the dialing pad.After inputting it, users can press **[Audio]**/**[Video]** button to initiate the call.

**Note**：

Replace the "." in the IP address with "*"

## 5.2 Answer Call

### 5.2.1 Answer Call

When the device is idle and there is an incoming call, the user can answer the call by pressing **[Answer]**. To reject an incoming call, the user can press **[Reject]** button on the interface.

### 5.2.2 Auto Answer

After the device's auto-answer feature is enabled, it will automatically answer incoming calls. Auto answer can be configured to distinguish between different lines.Administrators can enable auto-answer in the web settings, or users can activate auto-answer directly from the device. When auto-answer is enabled, an icon will appear in the top right corner of the screen.

#### 5.2.2.1 Auto Answer Enabled For Line

**Auto-answer can be configured by administrators through the web settings：**

Log in to the device's web page, go to **[Line]** >> **[SIP]**, select a specific SIP account, scroll down to **[Basic Settings]** >> **[Enable Auto Answering]**, set the **[Auto Answering Delay]** , and then click **[Apply]** to activate.

**Auto-answer can be configured through the device menu：**

Go to **[Menu]** >> **[Settings]** >> **[Call]** >> **[Account Settings]**, select the line, click the switch on the right to toggle the auto-answer option on/off, set the **[Auto Answering Delay]**, and then press the **[√]** button to save.

#### 5.2.2.2 Auto Answer Enabled For IP Call

Log in to the device web page, go to **[Lines]** >> **[Basic Settings]** >> **[SIP P2P Settings]**, enable automatic answering, set auto-answer time, then click submit.

## 5.3 Reject The Call

### 5.3.1 Manually Reject

When receiving an incoming call, you can press the **[End]**  button to reject the call. The rejected call will be displayed in the missed call list in the call log.

### 5.3.2 DND

Users can activate the "Do Not Disturb" (DND) feature on the device to reject incoming calls. This can be enabled by administrators through the web settings, or users can activate it directly from the device.

**DND can be configured by administrators through the web settings:**

Log in to the device's web page, go to **[Device settings]** >> **[Features]** >>**[DND settings]**, Select line or phone to enable the DND function. You can also schedule DND to automatically activate and deactivate at specific times. And then click **[Apply]** to activate.

**DND can be configured through the device menu：**

- Tap **[DND]**  on the right side of the device to enable the function. Then the original icon will turn red, and the screen will display a prompt "DND ON" .
- Go to **[Menu]** >> **[Settings]** >> **[Call]** >> **[DND]**, select the line/phone to enable the DND function. You can also set a schedule to automatically activate and deactivate DND at specific times. Then press the **[√]** button to save.

## 5.4 End The Call

After the user finishes the call, end the call by pressing the **[End]** button .

## 5.5 Mute

Users can enable mute mode during a call, which disables the device's microphone, preventing the local sound from being transmitted to the other party. Typically, mute

mode automatically disables upon the call's termination.

### 5.5.1 Mute The Call

- Pressing the **[mute]** button  during a call displays a blue mute icon  on the call interface.
- Unmute the call:Press the device's mute button  again on the call interface.

### 5.5.2 Ringing Mute

- Turn on mute ringing: Go to **[Menu]** >> **[Settings]** >> **[Basic]** >> **[Sound]**: Swipe left to adjust the ringtone volume, then tap [√] to save. Return to the standby interface, where the device's upper right corner displays the silent mode icon . When there's an incoming call, the device will display the incoming call interface but won't ring.
- To cancel the silent mode for incoming calls: Go to **[Menu]** >> **[Settings]** >> **[Basic]** >> **[Sound]**: Swipe right to adjust the ringtone volume, then tap [√] to save. After returning to the standby screen, the silent mode icon in the upper right corner disappears.

## 5.6 Call Hold/Resume

During a call, users can press the **[Hold]** button  to put the current call on hold. At this point, the button will change to **[Resume]** , allowing users to press the [Resume] button to resume the call.

## 5.7 Call Forward

Call forward is also known as ‘Call Divert’ which is to divert the incoming call to a specific number based on the conditions and configurations. User can configure the call forward settings of each line.

There are three types:

- **Unconditional Call Forward –** Forward any incoming call to the configured number.
- **Call Forward Busy –** When the user is busy, incoming calls will be forwarded to the configured number.
- **Call Forward on No Answer –** When user does not answer the incoming call after the configured delay time, the incoming call will be forwarded to the configured number.

**Call forward can be configured through the device menu：**

- Go to **[Menu]** >> **[Settings]** >> **[Call]** >> **[Call Settings]**, then select the line for call forwarding settings.
- After selecting the line, choose the type of call forwarding you want to set and enable it.
- Enter the number you want to forward calls to.
- Click on the **[√]** icon in the upper right corner to save the settings.

**Call forward can be configured through the web settings：**

- Go to **[Line]** >> **[SIP]** >> **[Basic Settings]**, then enable the desired call forwarding type.
- Enter the number you want to forward calls to.
- After completing the setup, click on **[Apply]** to save the settings.

# 6 Advance Function

## 6.1 Intercom

After activating the intercom mode, the device can automatically answer incoming calls in intercom mode.

### 6.1.1 Initiate Intercom.

Under standby mode, enter the **[Function Key]**  interface, then select the programmed number to make a call.

To use the intercom function, you need to set the function key as a memory key for intercom operation. This can be done either through the terminal screen settings or through the device's web page settings.

**Can be configured through the web settings：**

Enter **[Function Key]** >> **[Function Key]**, then select the key you want to set. Set the key type as a memory key, with the subtype as intercom. Enter the desired settings such as value, name, line, etc., and save the settings.

**Can be configured through the device menu：**

In standby mode, press the **[Function Key]** button , then select the key you want to edit. Set the key type as a memory key, with the subtype as intercom. Enter the desired settings such as value, name, line, etc., and save the settings.

### 6.1.2 Intercom Call

After activating the intercom mode, the device can automatically answer incoming calls in intercom mode.

Users can set intercom-related parameters through the device's web page by going to **[Device Settings]** >> **[Function Settings]** >> **[Intercom Settings]**.

**Configuration parameters:**

| Parameter | Description |
|---|---|
| Enable Intercom | When intercom is enabled, the device will accept the incoming call request with a SIP header of Alert-Info instruction to automatically answer the call after specific delay. |
| Enable Intercom Mute | Enable mute mode during the intercom call |
| Enable Intercom Tone | If the incoming call is intercom call, the phone plays the intercom tone |
| Enable Intercom Barge | Enable Intercom Barge by selecting it, the phone auto answers the intercom call during a call. If the current call is intercom call, the phone will reject the second intercom call |

## 6.2 MCAST

This feature allows user to make some kind of broadcast call to people who are in multicast group. User can configure a multicast DSS Key on the phone, which allows user to send a Real Time Transport Protocol (RTP) stream to the pre-configured multicast address without involving SIP signaling. You can also configure the phone to receive an RTP stream from pre-configured multicast listening address without involving SIP signaling.

Users can configure multicast listening address and port on the web page of **[Intercom Settings]>> [Multicast]**.

**Configuration parameters:**

| Parameters | Description |
|---|---|
| Priority | Defines the priority in the current call, with 1 being the highest priority and 10 the lowest. |
| Mcast Listening Renew Time(s) | Set the interval for re-listening to multicast after interrupting the listening. |

| | |
|---|---|
| Multicast prompt Tone | When enabled, play the prompt sound when receiving multicast. |
| Enable Prio Chan | When enabled, the same port and channel can only be connected. Channel 24 is the priority channel, higher than 1-23; channel 0 means not to use the channel. |
| Enable Page Priority | Regardless of which of the two multicast groups is called in first, the device will receive the higher priority multicast first. |
| Enable Emer Chan | When enabled, channel 25 has the highest priority. |
| Name | Set the multicast name. |
| Host:port | Set the multicast server address and port. |
| Channel | 0-25 (24: Priority Channel, 25: Emergency Channel). |

**MCAST Dynamic：**

Send multicast configuration information through SIP notify signaling. After receiving the message, the device configures it to the system for multicast monitoring or cancels multicast monitoring in the system.

## 6.3 Hotspot

### 6.3.1 Hotspot

SIP hotspot is a simple utility. Its configuration is simple, which can realize the function of group vibration and expand the quantity of sip account.

Take one device A as the SIP hotspot and the other devices (B, C) as the SIP hotspot client. When someone calls device A, devices A, B, and C will ring, and if any of them answer, the other devices will stop ringing and not be able to answer at the same time. When A B or C device is called out, it is called out with A SIP number registered with device A.

Users can set up a SIP Hotspot on the web page of **[Line]**>> **[SIP Hotspot]**.

**Configuration parameters:**

| Parameters | Description |
|---|---|
| Enable Hotspot | Enable or disable hotspot |
| Mode | Selecting 'SIP Hotspot' indicates that this device exists as a SIP Hotspot.<br>Selecting 'Client' indicates that this device exists as a client." |
| Monitor Type | The monitoring type can be broadcast or multicast. If you want to restrict broadcast packets in the network, you can choose multicast. The type of monitoring on the server side and the client side must be the same, for example, when the device on the client side is selected for multicast, the device on the SIP hotspot server side must also be set for multicast |
| Monitor Address | The multicast address used by the client and server when the monitoring type is multicast. If broadcasting is used, this address does not need to be configured, and the system will communicate by default using the broadcast address of the device's wan port IP |
| Local Port | Fill in a custom hotspot communication port. The server and client ports need to be consistent |
| Name | Fill in the name of the SIP hotspot. This configuration is used to identify different hotspots on the network to avoid connection conflicts |
| Line Settings | Sets whether to enable the SIP hotspot function on the corresponding SIP line |

**Server-side Settings:**

- Go to the device's web page: **[Line]** >> **[SIP Hotspot]** >> **[SIP Hotspot Settings]**. Enable hotspot settings as "Enabled", set the mode to "Hotspot", and assign a unique name that does not match any other hotspot server name.
- After completing the settings, click [Apply].

**Client Settings:**

As a SIP hotspot client, there is no need to set up a SIP account, which is automatically acquired and configured when the device is enabled. Just change the mode to "client"

and the other options are set in the same way as the hotspot.

The device is the hotspot server, and the default extension is 0. The device ACTS as a client, and the extension number is increased from 1 (the extension number can be viewed through the **[SIP hotspot]** page of the webpage).

Calling internal extension:

- The hotspot server and client can dial each other through the extension number before
  - Extension 1 dials extension 0.

### 6.3.2 Hotspot Extension Management

Hotspot extensions can be managed through the device's web page: **[Line]** >> **[Hotspot Extension Management]**, allowing for tasks such as upgrading, restarting, and adding to groups.

#### 6.3.2.1 Hotspot Group

You can add both the hotspot host and hotspot extensions to the same group. Set a call group number as desired; when a call is received, all devices within the group will ring, and once one device answers, the others will hang up.

#### 6.3.2.2 Manage Hotspot Extensions

If the device has enabled hotspot extension management mode, all extensions connected to the host will initially appear in the unmanaged extensions section. Users can then move these extensions to the managed extensions section, allowing them to perform tasks such as rebooting, upgrading, and adding to specified groups for the extension devices.

## 6.4 SMS

If the service of the line supports the function of the short message, when the other end sends a text message to the number, the user will receive the notification of the short message and display the button of the new SMS on the standby screen interface.

### 6.4.1 SMS

**Send messages:**

- Click on **[Menu]** >> **[Messages]** on the screen, then click  to create new message. Select the line and fill in the recipient's information.
- After editing is complete, click  to send.

**View SMS:**

- On the screen, click **[Menu]** >> **[Messages]** >> **[Inbox]**. When a new message arrives, you can also directly click "OK" on the screen to jump to the inbox.
- Click on the unread message to read it.

**Reply to messages:**

- Enter the SMS inbox interface.
- Open the message you want to reply to, click  , edit it, then click  to send.

### 6.4.2 Voice Message

If the service of the lines supports voice message feature, when the user is not available to answer the call, the caller can leave a voice message on the server to the user. User will receive voice message notification from the server and device will prompt a voice message waiting button on the standby screen.To listen to a voice message, the user must first configure the voicemail number. After the voicemail number is configured, the user can retrieve the voicemail of the default line.

**Listen to voicemail:**

- Select **[Menu]** >> **[MWI]**.
- Select the line you want to configure.
- Click  to enter the settings interface, where you can enable voice message for the line and edit the voice message retrieval number. Click  to save the

configuration.

- In the **[MWI]** interface, you can view the number of read and unread voice messages.
- Call the number of voice message , enter the PIN code when prompted, and listen to the voice messages according to the prompts.

# 7 Open Door

The indoor station can operate the door access control system to open the door while in standby mode or during a call.

## 7.1 Open The Door Under Standby

### 7.1.1 Open The Door Under Standby

In standby mode, users can click **[Open Door]** button on the desktop and then select the corresponding door access control to open the door.

### 7.1.2 Settings Of Open The Door Under Standby

The steps to set up door opening in standby mode are as follows:

- In the standby interface, click the **[Open Door]** button  to enter the door opening interface.
- Click the **[+]** button on the door opening interface to enter the settings interface.
- Enter the title, door access IP address, door access username, and door access password (matching the door access web username and password); or enter the title, open door URL, open door username, and password.
- Click the buttonin the upper right corner, then a prompt saying "Configuration completed" will appear, indicating that the configuration is finished. You can then click the back button.

**Note:**

When using with compatible directional access control devices, you only need to input the IP address, username, and password.

If using a third-party access control device, you need to input the complete URL for opening the door, along with the username and password.

## 7.2 Open the door during a call

During a call, users can click the indoor unit's door open button to open the door. After clicking, the access control unit that is currently in conversation with the indoor unit will open the door.

### 7.2.1 Open The Door During A Call

The operation steps for opening the door during a call are as follows:

- Establish a call with the access control unit.
- During the call, click the door open button  to open the door.

### 7.2.2 Settings Of Open The Door During A Call

The default door opening password during a call is the same as the default door opening password for the access control unit. If the user has not changed the access control unit's password, they can use the default configuration.

The configuration for opening the door during a call can be done in the device menu or through the device's web interface.

**Door opening can be configured through the device menu：**

- Click the **[Menu]**  on the desktop.
- Click **[Phonebook]** in the menu.
- Enter the phonebook interface, then click on **[Door Access List]**.
- Enter the access control list interface, then click the **[+]** button to add a new access control unit.
- Enter the information for the new access control unit, then click the ✓ in the upper right corner to save.
  - Name: Enter the name of the access control unit, you can customize the name

as desired.

- Number/IP: Enter the access control unit's IP address or number. Use the IP address only when the access control unit and indoor unit use IP calling.
- Line: Auto.
- Password: Enter the remote door opening password for the access control unit. This password must match the remote door opening password of the access control unit.
- Access code:Enter the remote door opening password for the access control unit. This password must match the remote door opening password of the access control unit.

**Door opening can be configured through the web settings：**

- Log in to the web page, go to **[Applications]** >> **[Access Control Settings]**, and click **[Add]**.
- Enter the access control information, then click **[Confirm]** to save.
  - Title: Enter the name of the access control unit, you can customize the name as desired.
  - Number/IP: Enter the access control unit's IP address or number. Use the IP address only when the access control unit and indoor unit use IP calling.
  - Line: Auto.
  - Password: Enter the remote door opening password for the access control unit. This password must match the remote door opening password of the access control unit.
  - Access code:Enter the remote door opening password for the access control unit. This password must match the remote door opening password of the access control unit.

**Note:**

When the indoor unit is used in conjunction with the old access control units i2 series and i3 series, the access code is the same as that of the old access control units.

# 8 Video Preview

## 8.1 Video Preview

The video preview function allows users to see the video from the access control or the IP camera linked to it before answering the call.

There are two supported methods for the video preview function:

- Preview via SIP Video
  - SIP Line: Enable preview and set preview mode through the web page under **[Line]** >> **[Advanced Settings]**.
  - IP Call: Enable it through the web page under **[Line]** >> **[Basic Settings]** >> **[SIP P2P Settings]**.

    Enable Preview: Whether to enable SIP video preview?

    Preview Mode: Preview18X: Standard SIP video preview mode; Preview2XX: Used in conjunction with directional access control devices.
- Via Video Linkage

  When the indoor unit receives a call, it matches the incoming number or IP address. If the corresponding number is bound to an RTSP video stream from a camera, the caller can see the video from the bound camera. For detailed configuration, please refer to Video Linkage.

## 8.2 Monitor

Users can click on the **[Monitor]**  button to enter the monitoring video interface, where they can see the information of the bound video screen.

The usage steps are as follows:

- Click the **[Monitor]**  button on the desktop.
- If monitoring cameras have been added, the video from the first camera will open by default.
- To switch to another camera, click  in the bottom right corner, then select the camera you want to view from the pop-up window.

- Click on the **[Back]** button in the top left corner to exit monitoring.

### 8.2.1 Manual Addition

The steps to manually add a camera are as follows:

- Click the **[Monitor]**  button on the desktop.
- Click  in the bottom right corner.
- In the pop-up window, click on the **[+]** button to open the window for manually adding a camera. Enter the parameters of the camera:
  - Title: Custom name, which will be displayed in the camera list and above the video.

    URL/IP: When adding a directional i6 series access control unit, only the IP address needs to be added. If adding other types of cameras, the complete RTSP URL needs to be added.
  - Enter the RTSP authentication username and password.
- Click ✓ in the top right corner to add.

### 8.2.2 Scan Addition

The steps to add via ONVIF scanning are as follows:

- Click the **[Monitor]**  button on the desktop.
- Click  in the bottom right corner.
- In the pop-up window, click on the search button, and the indoor unit will start scanning for IP cameras on the local network. Once the search is complete, a list of discovered IP cameras will appear. Cameras that have already been added will have ✓.
- Select the camera that hasn't been added yet, and a window will pop up for adding the camera. Enter the necessary information as follows:
  - Title: Custom name, which will be displayed in the camera list and above the video.

- User: The username required for ONVIF authentication.
- Password: The password required for ONVIF authentication.

- Click ✓ in the top right corner to add.

> **Note：**
>
> The access control or camera being scanned must have ONVIF functionality enabled. If it's not enabled, it needs to be enabled before scanning and adding.

## 8.3 Video Linkage

The indoor unit can display the video from the bound access control or IP camera during an incoming call or conversation. The video linkage function is configured via the web interface, with the following steps:

- Log in to the indoor station's web interface.Go to **[Line]** >> **[Action Plan]**.Set the following parameters:
  - Action: Video.
  - Number: The number of the access control or the IP address of the access control. When using an extension to call, enter the number; when using IP calling, enter the IP address.
  - Type: Early, "Early" indicates video linkage before answering the call; Connected, "Connected" indicates video linkage after answering the call.
  - Direction: Both, indicates video linkage for both incoming and outgoing calls; Incoming, indicates video linkage only for incoming calls; Outgoing, indicates video linkage only for outgoing calls.
  - Line: Auto, or select the corresponding local line.
  - Username: The username for RTSP authentication
  - Password: The password for RTSP authentication
  - URL: The complete address of the RTSP URL.

# 9 Contacts

## 9.1 DoorPhone List

**Device Interface Settings:**

Click on **[Menu] >> [Phonebook] >> [Door Access List]** to access the Access Control List interface. Here, you can add, delete, or modify the entry passwords for access control devices. You can also initiate video or voice calls from within the Access Control List.

**Web Interface Settings:**

Visit the web page **[Application] >> [DoorPhone Settings]** to also add, delete, or modify the entry passwords for access control devices.

**Parameters：**

| Parameters | Description |
|---|---|
| Title | Setting the Name for Added Access Control |
| Number | The access control number. Supports IP addresses and SIP numbers. |
| Line | Select the line to dial out |
| Access code | Enter the remote access code for door entry. This password must match the remote access code of the door entry system. |
| Password | Enter the remote access code for door entry. This password must match the remote access code of the door entry system. |

**Note：**

When the indoor unit is used in conjunction with the old door access i2 and i3 series, the access code should match the access code of the old door access system.

## 9.2 Local Phonebook

Users can save contact information in the phonebook and directly dial the contact's phone number from the phonebook. By default, the phonebook is empty but can be populated via the device interface or web interface. Users can manually add contacts or import them from call logs (or cloud phonebook) into the phonebook.

### 9.2.1 Add/ Edit / Delete Contact

**Adding contacts via the device interface:**

Click **[Menu] >> [Phonebook] >> [Local Contacts]** to enter the local contacts list interface where contacts can be added.

**Adding contacts via the web interface:**

Access the web page **[Phonebook] >> [Contacts]** to add contacts; users can edit contact information by clicking **[Edit].**

**Parameters：**

| Parameters | Description |
|---|---|
| Name | Contact Name |
| Phone | Contact Phone Number (required), supports IP address and SIP number |
| Phone 1 | Contact Phone Number (optional), supports IP address and SIP number |
| Phone 2 | Contact Phone Number (optional), supports IP address and SIP number |
| Line | Select the outgoing line |
| Ring | Choose a specific ringtone for incoming calls from this contact |
| Group | Select default or pre-configured group |

**Edit Contacts:**

Editing contacts via the device interface:

After adding a contact, users can edit the contact information by clicking **[Menu] >>**

**[Phonebook] >> [Local Contacts]**, and then clicking on the contact's avatar in the contact list.

Editing contacts via the web interface:

Via the web interface, go to **[Phonebook] >> [Contacts] and click [Edit]** to edit contact information.

**Delete Contacts：**

Deleting contacts via the device interface:

Users can delete contacts by navigating to **[Menu] >> [Phonebook] >> [Local Contacts]**, first clicking the delete button , selecting the contacts to be deleted or selecting all, clicking the delete button again, and then clicking confirm to delete.

Deleting contacts via the web interface:

Alternatively, via the web interface go to **[Phonebook] >> [Contacts]**, select the contacts you wish to delete from the contact list, and click the **[Delete]** button to delete them.

**Searching for contacts:** By clicking the search button , you can query existing contacts.

### 9.2.2 Add/ Edit / Delete Group

By default, the group list is empty. Users can create their own groups, edit group names, add or remove contacts from groups, and delete groups.

**Setting up groups via the device interface:**

Click **[Menu] >> [Phonebook] >> [Group]**

- Adding a group: Click the button , enter the group name, and select a ringtone.
- Deleting a group: Click the delete button , select the group to delete or select all, click the delete button again, and then click **[Confirm]** to delete.

- Editing a group: Click on a group to enter its interface, click the edit button  to make changes. The number in parentheses indicates the total number of contacts in that group.

**Setting up groups via the web interface:**

Access the web page >> **[Phonebook] >> [Advanced] >> [Group List]** to add, edit, and delete groups.

- Adding a group: Click the **[Add Contact Group]** button, enter the group name, and select a ring.
- Deleting a group: Select the group to delete or select all, then click the [Delete] button to delete.
- Editing a group: Click the [Edit] button on the group you wish to edit to make changes.

### 9.2.3 Browse/ Add /Delete Contacts In Group

Open a group and click the edit button . In the group editing interface under **[Group Members]**, browse, add, or remove contacts.

## 9.3 Cloud Phonebook

The cloud phonebook allows users to download the phonebook from a cloud server to their device. This is very convenient for office users in terms of using the phonebook, as it can be downloaded with a single click from the cloud phonebook server, making it very easy to create and maintain contact lists.

**Note：**

The cloud phonebook ensures its content is the latest version by temporarily

downloading its contacts to the device each time it is accessed. However, the download time can take a few seconds, depending on the quality of the network connection at the time of use. Therefore, to save time waiting for downloads, it is recommended that users save important contact information from the cloud phonebook to the local device.

### 9.3.1 Configure Cloud Phonebook

Open the cloud phonebook list by clicking **[Menu] >> [Phonebook] >> [Cloud Contacts].**

**Note：**

Initial configuration requires setting up in the web page under **[Phonebook] >> [Cloud Phonebook].** After setting up on the web page, it can be viewed on the device.

### 9.3.2 Downloading Cloud Phonebook

On the cloud phonebook screen interface, users can select the cloud phonebook, and the device will begin loading it. If the download fails, a warning message will be displayed.

Once the cloud phonebook has downloaded successfully, users can search for contacts and dial from the top-right corner, using the same method as with the local phonebook.

## 9.4 Blocked List

The device supports a call blocking list. If a number is added to the call blocking list, incoming calls from that number are directly rejected by the recipient, and the device on this end will display a missed call. (Numbers on the call blocking list can still be dialed out normally for outgoing calls.)

- **Device interface settings:**
- There are multiple ways to add numbers to the call blocking list, including directly through **[Menu] >> [Phonebook] >> [Blocked List].**
- From within the phonebook (both local and network), you can select any number to add to the blocking list.
- From the call log, you can select any number to configure and add.

- **Web interface settings:**
- Access the web page **[Phonebook] >> [Call List] >> [Restricted Incoming Calls]**, and click on add new.

## 9.5 Allowed List

The device supports an allowed calls list. If a number is added to this list, it can still receive calls from that number even when the device has Do Not Disturb (DND) or call forwarding activated. Calls from numbers not on the allowed calls list will be automatically rejected or forwarded as set by the device settings.

**Device interface settings:**

- There are multiple ways to add numbers to the allowed calls list. You can directly add numbers/prefixes and specify the type of allowed calls under **[Menu] >> [Phonebook] >> [Allowed List].**
- From within the phonebook (both local and network), select any number to configure and add.
- From the call log, select any number to configure and add.

**Web interface settings:**

- - Access the web page **[Phonebook] >> [Call List] >> [Allowed Incoming Calls]**, and click on add new.

## 9.6 Restricted Outgoning List

The device supports setting restrictions on dialing out certain numbers. If these numbers are entered on the dialing interface, the call will not be allowed, and the device will emit a prohibited call tone and display a pop-up notification.

Users can set up restricted outgoing numbers via the web interface by navigating to **[Phonebook] >> [Call List] >> [Restricted Outgoing Calls]**.

# 10 Call Log

**Device interface for viewing call logs:**

- **Viewing:** The device can store up to 1000 call records. Users can open the call log by pressing **[Menu] >> [Call Log]** to view all incoming, outgoing, forwarded, and missed call records. In the call log screen interface, users can scroll to browse through the call logs.
- **Deleting:** Users can delete records by clicking the delete button , selecting the desired records or selecting all, then clicking the delete button again, and confirming by clicking OK.
- **Add to Phonebook:** Users can perform further actions such as adding a contact, making a call, or adding to allowed/blocked call lists by clicking the button  after viewing a call record.

**Web interface for viewing call logs:**

- **Viewing :** The system can store up to 1000 call records. Users can view the call logs by navigating to **[Call Logs] >> [Call Information]**, where they can access records of all incoming, outgoing, forwarded, and missed calls.
- **Deleting:** Users can delete call records by selecting the desired records or selecting all, then clicking the **[Delete]** button to remove them.
- **Add to Phonebook:** Users can add a contact by clicking the **[Add]** button after a call record.

# 11 Device Settings

## 11.1 Time Plan

The Time Plan feature allows users to set specific actions to occur at either a particular time or within a period. A time point triggers an action at a specific moment, while a period triggers an action during a specified duration.

Users can access this functionality through the web page under **[Device Settings] >> [Time Plan]**. They can define a Name, Type, Repetition Period, along with the effective date and time, then click 'Add'. Once configured, the device will execute the designated action at the specified times.

**Parameters：**

| Parameters | Description |
|---|---|
| Name | Enter a defined action name |
| Type | Timing reboot, timing upgrade, timing forward |
| Repetition | Do not repeat: execute once within the set time range<br>Daily: Perform this operation in the same time frame every day<br>Weekly: Do this in the time frame of the day of the week<br>Monthly: the time frame of the month to perform this operation |
| Start date | Effective date |
| End date | End date |
| Effective Time | Set the time period for execution |

**Note：**

If there's an ongoing call within the set time frame, skip and do not execute the restart or upgrade operation.

## 11.2 Action Plan

Action Plan application: a technical implementation defined and designed by Fanvil for remote control and behavior linkage between Fanvil terminal equipment and other equipment. That is, when an event occurson the Fanvil terminal, the terminal can perform an action, and this action is completed according to a Plan rule.

**Setting method:**

Users can visit the website [**Line**] >> [**Action Plan**] to configure action plan rules. After the setting is complete, the configuration is assigned to the corresponding device and updated, and the corresponding terminal will perform the corresponding action when the event occurs.

**Parameter description:**

| Parameter | Description |
|---|---|
| Action | Action when the number configuration rule is triggered. Supported types are:<br>Video: Interconnect with a third-party camera to display the video of the attached camera when an incoming call or call is made<br>Mute: The device automatically mute when the rule is triggered.<br>Answer: The device automatically answers the call when the rule is triggered. |
| Number | Auxiliary device number (support video) |
| Type | Early: trigger execution before call establishment.<br>Connected: trigger execution after call establishment |
| Direction | For call mode, incoming/outgoing call |
| Line | Set up outgoing lines. |
| Username | Bind the user name of the IP camera. |
| Password | Bind IP camera password. |
| URL | Video streaming information . |

| | |
|---|---|
| User Agent | Set user agent information |

## 11.3 Maintenance

### 11.3.1 Configurations

On this page, users with administrator privileges can view, export, or import the phone configuration, or restore the phone to factory Settings.

- **Export Configurations**

Right click to select target save as, that is, to download the device's configuration file, suffix ".txt" (note: profile export requires administrator privileges).

- **Import Configurations**

Import the configuration file of Settings.

- **Clear Configuration**

Clear configurations related to SIP, auto-deployment, shortcuts, etc.

- **Clear User Data**

Clear user data such as the phonebook, call history, blacklist/whitelist, etc.

- **Reset Device**

The device data will be cleared, including configuration and database tables.

### 11.3.2 Upgrade

#### 11.3.2.1 Web Upgrade

Upgrade Device Software Version: Upgrade to the new version via the web. Once the upgrade is complete, the device will automatically restart and update to the new version. Go to **[System] >> [Upgrade],** select a file, choose the version, and click **"Upload"** to proceed.

#### 11.3.2.2 Online Upgrade

Through online upgrading, devices can be upgraded.

Configuration for online upgrades by an administrator through a web page:

Access the web page **[System] >> [Upgrade] >> [Upgrade Server]**, configure the upgrade server, and the update cycle, etc. Place the upgrade TXT file and software on the corresponding server. When the device detects that the software version number on the server is different from its own software version number, it will prompt for an upgrade.

| Parameter | Description |
|---|---|
| **Upgrade Server** | |
| Enable Auto Upgrade | Check enable automatic upgrade, and the device can detect the txt version information and available versions in the HTTP server. |
| Upgrade Server Address1 | Fill in the available primary upgrade server (HTTP server) address. |
| Upgrade Server Address2 | Fill in the address of the available backup upgrade server (HTTP server). When the primary server is unavailable, request the backup server. |
| Upgrade Interval | The web page starts to automatically detect the upgrade and configure the interval. If the server has a new version, the device will prompt for the upgrade at the interval. |
| **Software Version information** | |
| Current Software Version | Displays the current device software version number. |
| Server software version | Displays the server software version number. |
| [**Upgrade**] button | When there is a corresponding TXT file and version on the server side, the [**Upgrade**] button changes from grayed out to available. Click [**Upgrade**] to choose whether to upgrade. |
| New version description | When the server has the corresponding TXT file and |

| | |
|---|---|
| information | version, the and version information in txt will be displayed under the new version description information. |

**Instructions:**

- After completing the configuration on the Manager web page, place the version information TXT file into the configured HTTP server. The naming format for the version information TXT file should be: vendor_model_hwv1_0.txt

- The TXT file must be in UTF-8 format, and the content format should be as follows:

```
Version=2.12.0    #Software Version Number
Firmware=http://ip:port/xxx.z     #URL of the Software Version File
BuildTime=2023.09.11 20:00
Info=TXT

Release Note：
Xxxxx
Xxxxx
Xxxxx
```

- After the update interval has elapsed, if the server has available TXT files and version files, the device UI will indicate that a new version file is available. Users can click to upgrade to the new version; the web page will show an enabled upgrade button along with the Release Note from the TXT file, allowing users to click and upgrade the version.

### 11.3.3 Auto Provision

Webpage: go to [**System**] >> [**Auto Provision**].

Devices support SIP PnP, DHCP options, Static provision, TR069. If all of the 4 methods

are enabled, the priority from high to low as below:

**PNP>DHCP>TR069> Static Provisioning**

Transferring protocol: FTP、 TFTP、 HTTP、 HTTPS

**Parameters：**

| Parameters | Description |
|---|---|
| **Basic Settings** | |
| CPE Serial Number | Display the device SN |
| Authentication Name | Configure the user name of FTP server; TFTP protocol does not need to be configured; if you use FTP protocol to download, if you do not fill in here, the default user of FTP is anonymous |
| Authentication Password | The password of provision server |
| Configuration File Encryption Key | If the device configuration file is encrypted , user should add the encryption key here |
| General Configuration File Encryption Key | If the common configuration file is encrypted, user should add the encryption key here |
| Download Fail Check Times | The default value is 1. If the download of the configuration fails, it will be re-downloaded 1 time. |
| Update Contact Interval | At preset times, the device automatically downloads the phone book and updates it. |
| Save Auto Provision Information | Configure whether to save the automatic update information. |
| Download CommonConfig enabled | Whether phone will download the common configuration file. |
| Enable Server Digest | When the feature is enable, if the configuration of server is changed, phone will download and update. |

| | |
|---|---|
| Display Provision Prompt | The Settings of the upgrade pop-up are displayed |
| Provision config priority | Normal: Automatic deployment has a high priority<br>Manual: The priority set manually is high |
| **DHCP Option Setting** | |
| Custom Option Value | Configure DHCP option, DHCP option supports DHCP custom option \| DHCP option 66 \| DHCP option 43, 3 methods to get the provision URL. The default is Option 66 |
| Custom | Custom Option value is allowed from 128 to 254. The option value must be same as server define. |
| Enable DHCP Option 120 | Use Option120 to get the SIP server address from DHCP server. |
| **DHCPv6 Option Setting** | |
| Custom Option Value | Configure DHCPv6 option, DHCPv6 option supports custom option \| option 66 \| option 43, 3 methods to get the provision URL. The default is Disable. |
| Custom | Custom option number. Must be from 128 to 254. |
| **SIP Plug And Play** | |
| Enable SIP PnP | Whether enable PnP or not. If PnP is enabled, phone will send a SIP SUBSCRIBE message with broadcast method. Any server can support the feature will respond and send a Notify with URL to phone. Phone could get the configuration file with the URL. |
| Server Address | Broadcast address. As default, it is 224.0.0.0. |
| Server Port | PnP port |
| Transport Protocol | PnP protocol, TCP or UDP. |
| Update Interval | Configuration file update interval time. As default it is 1, means phone will check the update every 1 hour. |
| **Static Provisioning Server** | |

| | |
|---|---|
| Server Address | Provisioning server address. Support both IP address and domain address. |
| Configuration File Name | The configuration file name. If it is empty, phone will request the common file and device file which is named as its MAC address.<br>The file name could be a common name, $mac.cfg, $input.cfg. The file format supports CFG/TXT/XML. |
| Protocol Type | Transferring protocol type ，supports FTP、TFTP、HTTP and HTTPS |
| Update Interval | Configuration file update interval time. As default it is 1, means phone will check the update every 1 hour. |
| Update Mode | Provision Mode.<br>1. Disabled.<br>2. Update after reboot.<br>3. Update after interval. |
| **Auto provision Now** | |
| **TR069** | |
| Enable TR069 | Enable TR069 after selection |
| ACS Server Type | There are 2 options Serve type, common and CTC. |
| ACS Server URL | ACS server address |
| ACS User | ACS server username |
| ACS Password | ACS server password |
| Enable TR069 Warning Tone | If TR069 is enabled, there will be a prompt tone when connecting. |
| TLS Version | TLS Version |
| STUN Server Address | Enable the STUN |
| STUN Enable | Enable TR069 after selection |
| Month Start | The DST start month |
| Week Start | The DST start week |
| Weekday Start | The DST start weekday |
| Day Start | The DST start day |

| | |
|---|---|
| Hour Start | The DST start hour |
| Month End | The DST end month |
| Week End | The DST end week |
| Weekday End | The DST end weekday |
| Day End | The DST end day |
| Hour End | The DST end hour |
| **Manual Time Settings** | To set the time manually, you need to disable the SNTP service first, and you need to fill in and submit each item of year, month, day, hour and minute in the figure above to make the manual settings successful. |

# 12 Screen Setting

## 12.1 Time Settings

Users can set the time and date through both the device's web interface and its menu.

**Device Interface for Setting Time/Date:**

Users can set the time and date by navigating on the device to **[Menu] >> [Settings] >> [Basic]**. After making the adjustments, press **[√]** to save the changes.

**Web Interface for Setting Time/Date:**

Users can set the device's time and date by going to the web page **[Device Settings] >> [Time/Date].**

**Parameters：**

| Parameters | Description |
|---|---|
| **Network Time Server Settings** | |
| Time Synchronized via SNTP | Enable time-sync through SNTP protocol |
| Time Synchronized via DHCP | Enable time-sync through DHCP protocol |
| Time Synchronized via DHCPv6 | Enable time-sync through DHCPv6 protocol |
| Primary Time Server | Primary Time Server |
| Secondary Time Server | Set secondary time server address, when primary server is not reachable, the device will try to connect to secondary time server to get time synchronization. |
| Time zone | Select the time zone |
| Resync Period | Time of re-synchronization with time server |
| **Date Format** | |
| 12-Hour Clock | Set the time display in 12-hour mode |
| Date Format | Select the time/date display format |

| Daylight Saving Time Settings | |
|---|---|
| Location | Choose your location, phone will set daylight saving time automatically based on the location |
| DST Set Type | Choose DST Set Type, if Manual, you need to set the start time and end time. |
| Correction Value | Daylight saving time rules are based on specific dates or relative rule dates for conversion. Display in read-only mode in automatic mode. |
| Month Start | The DST start month |
| Week Start | The DST start week |
| Weekday Start | The DST start weekday |
| Day Start | The DST start day |
| Hour Start | The DST start hour |
| Month End | The DST end month |
| Week End | The DST end week |
| Weekday End | The DST end weekday |
| Day End | The DST end day |
| Hour End | The DST end hour |
| **Manual Time Settings** | You can set your time manually |

## 12.2 Screen Setting

Users can edit screen parameters by accessing the feature menu: navigate to **[Menu] >> [Settings] >> [Basic] >> [Display]**. After editing, click **[√]** to save the changes.

### 12.2.1 Brightness and backlight

Users can adjust brightness and backlight settings through the device menu or via a web interface. The device enters backlight mode after a set inactivity timeout.

**Device Interface Settings for Brightness and Backlight:**

- Navigate through the device menu to **[Settings] >> [Basic] >> [Display]** to set the device's brightness and backlight time.

**Web Interface Settings for Screen:**

- Access the web interface at **[Device Settings] >> [Advanced] >> [Screen Configuration]** to adjust the device's brightness and backlight time.

**Brightness and Backlight Parameters:**

- Brightness Level When in Use: Set the screen brightness level during active use.
- Brightness Level When Idle: Set the screen brightness level when the device is idle.
- Backlight Idle Wait Time: Set the timeout duration before the device enters backlight mode.

### 12.2.2 Screen Saver

Users can enable screen savers through the device menu or the web interface, which activates after a set period of inactivity.

**Device Interface Settings for Screen Saver:**

- Users can set up the screen saver through the device menu by navigating to **[Settings] >> [Basic] >> [Display].**

**Web Interface Settings for Screen Saver:**

- Access the web interface at **[Device Settings] >> [Advanced] >> [Screen Configuration]** to set up the device screen saver.

**Screen saver parameters:**

- **Screen saver:** Enable the screen saver function
- **Timeout to screen saver:** Sets the timeout period for entering the screensaver. The value can be customized

### 12.2.3 UI Settings

#### 12.2.3.1 Background

To customize the background image, access the device's web page by navigating to **[System] >> [Upgrade] >> [Background Upgrade].**

**Image Format Specifications:**

- Supported Format: BMP
- Resolution:

  i504/i504W: 1024*600

  i506W: 1280*800
- Bit Depth: 24-bit

#### 12.2.3.2 Boot Logo

To customize the startup logo displayed when the device powers on, you can update the boot logo image via the web interface. Navigate to **[System] >> [Upgrade] >> [Boot Logo Upgrade]** to upload a custom boot logo image.

**Image Format Specifications:**

- Supported Format: JPG
- Resolution:

  i504/i504W: 1024*600

  i506W: 1280*800
- Bit Depth: 24-bit

**Note：**

The boot logo image must be created strictly according to the above specifications. Please note:

- For the i506W models, rotate the image 90 degrees to the right before upgrading through the web interface.

### 12.2.4 Screen Saver

Users can enable screen savers through the device menu or the web interface, which activates after a set period of inactivity.

**Device Interface Settings for Screen Saver:**

- Users can set up the screen saver through the device menu by navigating to **[Settings] >> [Basic] >> [Display].**

**Web Interface Settings for Screen Saver:**

- Access the web interface at **[Device Settings] >> [Advanced] >> [Screen Configuration]** to set up the device screen saver.

**Custom Screensaver:**

- Users can upgrade the custom screensaver image via the web page **[System] >> [Upgrade] >> [Screensaver Upgrade].**
- Image format:
  - Supports BMP format
  - Resolution:

    i504/ i504W: 1024*600

    i506W: 1280*800
  - Bit depth: 24-bit

## 12.3 Audio Settings

### 12.3.1 Ring Setting

**Device interface for setting ringtones:**

Access the device through **[Menu] >> [Settings] >> [Basic] >> [Sound]**, edit **[Ring Type] / [ Handfree Volume ].** After making your selection, press **[√]** to save.

**Web interface for setting ringtones:**

Users can set the device's ringtone type through the web page **[Device Settings] >> [Media Settings] >> [Media Settings]**. After setting, click **[Submit]** to save.

### 12.3.2 Volume Setting

**Device interface for setting volume:**

Access the device through **[Menu] >> [Settings] >> [Basic] >> [Sound]**, edit **[Volume]** settings. After making your adjustments, press **[√]** to save.

**Web interface for setting volume:**

Users can set the device's volume through the web page **[Device Settings] >> [Media Settings] >> [Media Settings]**. After setting, click **[Submit]** to save.

**Volume parameters:**

- Hands-free ringtone: Set the volume for incoming call ringtones and door opening tones.
- Signal tone volume: Set the volume for incoming and outgoing signal tones.
- Hands-free volume: Set the volume for call audio.

### 12.3.3 Alert Info Ring Setting

**Alert Info**

Access the web page [Device Settings] >> [Media Settings] >> [Alert Info Ring Settings] to configure Alert Info rules.

**Parameters**

| **Alert Info** | |
|---|---|
| Values from Alert Info 1 to Alert Info 10 | Set the values for specific ringtone types for incoming calls. When the device receives an Invite message with an Alert Info field value that matches the set value, the device will play the corresponding ringtone type. |

| | |
|---|---|
| Line | Set whether to enable specific ringtones for incoming calls on the respective SIP line. |
| Ring type | Type1-Type7, WirelessRing |

### 12.3.4 Tone Setting

Users can set call alerts, call prompt tones, ringback tones, and reminder tones via the web page **[Device Settings] >> [Features] >> [Tone Settings]**.

| Parameters | Description |
|---|---|
| Call Hold Alert Tone | There will be an alert tone when the user presses the hold call button during a call. This feature is enabled by default on the device. |
| Call waiting alert tone | There will be an alert tone when a second incoming call is received during an ongoing call. This feature is enabled by default on the device. |
| Play Talking DTMF Tone | When the user presses the device's numeric keys during a call, DTMF prompt tones will be heard. This feature is enabled by default. |
| Automatic Answering Prompt Tone for IP Direct Dialing | Enabled: When there is an incoming SIP or IP direct dialing call, if automatic answering is enabled, there will be a prompt tone during the automatic answering.<br><br>Disabled: When there is an incoming SIP or IP direct dialing call, if automatic answering is enabled, there will be no prompt tone during the automatic answering. |
| Ring Back Tone | Closed: Disables the ringback tone for calls.<br>Default: Uses the default ringback tone.<br><br>Supports custom ringback tones, which can be set by upgrading ringtone files under **[System] >> [Upgrade] >> [Ring Upgrade]**, and then selecting the custom option for the ringback tone. |

| | |
|---|---|
| Busy Tone | Closed: Disables the call waiting tone.<br>Default: Uses the default call waiting tone.<br><br>Supports custom call waiting tones, which can be set by upgrading ringtone files under **[System] >> [Upgrade] >> [Ring Upgrade],** and then selecting the custom option for the call waiting tone. |

### 12.3.5 Upload Ring

Users can upgrade the ringtone by accessing the device webpage >> **[System] >> [Upgrade] >> [Ring Upgrade]**, selecting the ringtone file, and clicking **[Upload]**.

**Ringtone file format:**

- Supports WAV and MP3 formats
- Maximum file size : 1M

## 12.4 Greeting Words Setting

Greeting words can be set via the device or through the web interface.

**Device interface setting:**

- Access the device >> **[Menu] >> [Settings] >> [Basic] >> [Display]**, edit the Greeting words , and press **[√]** to save.

**Web interface setting:**

- Access the device web page >> **[Device Settings] >> [Advanced] >> [Greeting words ],** edit the welcome message, and press **[Submit]** to save.

**Note：**

Greeting words are only displayed on the screen if the default line selection feature is

disabled.

# 13 Function Key Settings

## 13.1 Function Key

**Function Key Setting**

Users can configure function keys through the terminal device or manage them via the web interface.

**Web Interface Configuration of Feature Keys:**

On the web page, go to **[Function keys]** to configure DSSKEY buttons. The types of buttons can include Memory keys, Function keys, DTMF, etc. Assign the configuration to the appropriate device and update.

**Terminal Device Configuration of Feature Keys:**

When the device is active, click the button at the top-right corner  of the device to expand the DSSKEY list. Select the feature key you want to configure.

**Function Key Usage:**

Function keys support the following types:

**Memory Keys**

- Speed Dial: Directly dial a preset number in standby mode.
- Intercom: Call a set number using intercom mode. If the recipient has intercom auto-answer enabled, they can automatically answer intercom calls.

**Key Event**

- MWI: Display detailed information about the voicemail box for all SIP lines.
- Do Not Disturb: Enter the Do Not Disturb settings interface to enable/disable the feature.
- Hold Call: Hold/resume the current call.
- Transfer: Enter the transfer interface, functions similarly to the Softkey-Transfer button.
- Phonebook: Access the phonebook interface.

- Redial: Redial the last dialed number.
- Call Forward: Enter the call forwarding settings interface.
- Call Log: Access the call logs interface.
- SMS: Enter the short message interface.
- Callback: Call back the last incoming call number.
- Intercom: Open the dial pad and call out using intercom mode.
- Prefix: Configure a number prefix. When dialing, pressing this key automatically adds the prefix.
- Deployment: This function depends on the Broadsoft server and is a method to record call information in call centers.
- Escalate: This function is related to the Broadsoft server and sends a corresponding SIP message to the server during a call.
- Retrace: This function is related to the Broadsoft server and sends call information during or after a call.
- Speaker: Enter handsfree dialing or switch to the hands-free channel.
- Local Contacts: Access the local contacts interface.
- XML Group: Access the cloud phonebook interface.

**DTMF:** During a call, pressing this key sends pre-configured DTMF tones sequentially to the remote party.

**URL:** Access a pre-configured remote URL, can be set for XML phonebook addresses, etc.

**MCAST Paging:** After configuring a multicast address and audio codec, pressing this key sends out a multicast.

**Action URL:** Users can perform basic call operations on the device using a specific URL.

**Multicast Listening:** Configure a multicast address; pressing this key allows listening to RTP multicast when active.

## 13.2 Wireless Key ( Only i506 (W) Support it )

When the device is in standby, pressing a configured wireless key can play a ringtone on the device or dial out via a registered line.

**Web interface configuration:**

Log in to the device's webpage, go to **[Function Keys] >> [Wireless Keys]**. A device can bind up to ten wireless keys.

Device interface configuration:

Go to **[Menu] >> [Settings] >> [Advanced] >> [Wireless Key Configuration].**

**Parameters：**

| Parameter | Description |
|---|---|
| Name | Set the wireless key name |
| Addr id | The unique identification ID of the wireless button, the addrids of each wireless button are unique (ID is displayed in hexadecimal, only numbers and letters are supported, special characters are not supported) |
| Type | Select the function type of wireless button, including: Ring, Dial number |
| Subtype | When Type is Ring, the subtype displays the ringtone selection.<br>When Type is Dial number, the subtype displays Line selection. |
| Value | When Type is Dial number, the value can be edited to speed dail number; |
| Pairing Status | Displays pairing status, including: pairing, paired, disconnected |
| Operation | Bind or disconnect the button |

### 13.2.1 Scan To Add

**To add via the web interface:**

- Log in to the device's web page at **[Function Key] >> [Wireless Keys]**.

- Click on **'Bind'** in the button list, which puts the device into pairing mode. Activate the wireless key by briefly pressing it. If the device's web page updates to **'Paired'** and displays the button's addr id, the pairing is successful. If pairing fails after one attempt, try pressing the wireless button a few more times to avoid pairing failure due to data loss.
- Once paired, you can enter a name for the new button, select its type, subtype, and optionally provide a value. Complete the setup by clicking **'Submit'.**

**To add via the device menu:**

- On the desktop, click **[Menu] >> [Settings] >> [Advanced] >> [Wireless Key].**
- Choose the wireless button to bind and select '**Scan to Bind**'.
- Activate the wireless button by briefly pressing it. After successful pairing, you can set the button's name and type. Finalize the settings by clicking the check mark (✔) at the top right to save.

### 13.2.2 Manual Addtion

**Adding through the web interface:**

- Log into the web interface and go to **[Function Key] >> [Wireless Keys]** to add a new button.
- When adding a new button, users must enter the name, addr id (a unique identifier to distinguish different buttons), type, subtype, and value (optional). After filling out this information, click on bind or submit. The device will then pair with the device that has this addr id. If the status shows as paired, it means the new button has been successfully added.

**Adding through the menu interface:**

- On the desktop, click **[Menu] >> [Settings] >> [Advanced] >> [Wireless Key]** configuration.
- Choose the wireless button to bind, a selection box will appear, select manual addition.
- When adding a new button, users must enter the name, addr id (a unique identifier to distinguish different buttons), type, subtype, and value (optional). After filling out

this information, click on bind or submit. The device will then pair with the device that has this addr id. If the status shows as paired, it means the new button has been successfully added.

# 14 Network Settings

## 14.1 Ethernet Connection

**IPv4**

- IPv4 network types offer two modes: DHCP and Static IP.

- When the network type is set to DHCP, the phone receives a network IP address from a DHCP server (router).
  - Use Dynamic Domain Name Service: Enabled by default, used for domain name resolution.
  - Use Dynamic Time: Disabled by default, controls whether to use the time from the DHCP server.

- When the network is set to Static IP, the IP address must be set manually.
  - IP Address: Enter the IP address you wish to set.
  - Subnet Mask: Set the subnet mask.
  - Gateway: Used for network interconnection, fill in according to your needs.
  - Primary DNS Server: The IP address of the primary DNS server.
  - Secondary DNS Server: The IP address of the secondary DNS server.

**IPv6**

**IPv6 network types offer two modes: DHCP and Static IP.**

- When the network type is set to DHCP, the phone receives a network IP address from a DHCP server (router).
  - Use Dynamic Domain Name Service: Enabled by default, used for domain name resolution.
  - Use Dynamic Time: Disabled by default, controls whether to use the time from the DHCP server.

- When the network is set to Static IP, the IP address must be set manually.

- IP Address: Enter the IPv6 address you wish to set.
- IPv6 Prefix Length: The number of bits in the IPv6 prefix, which indicates the network portion, similar to the subnet mask in IPv4.
- Gateway: Used for network interconnection, fill in according to your needs.
- Primary DNS Server: The IP address of the primary DNS server.
- Secondary DNS Server: The IP address of the secondary DNS server.

## 14.2 Wireless Network

The device supports wireless Internet capabilities. There are two ways to connect to Wi-Fi:

- Device-side connection: Set up the wireless network connection in the device **[Menu] >> [Settings] >> [Advanced] >> [Wireless Network]**;
- Web interface connection: Set up the wireless network connection on the device webpage **[Network] >> [Wi-Fi Settings]**.

**To connect via the device interface:**

- With the device in its default standby state, press **[Menu] >> [Settings] >> [Advanced ] >> [Wireless Network]**, and click the switch to automatically search for available networks.
- Select the wireless network you want to connect to, enter the password when prompted, and click save to establish the connection.

**To connect via the web interface:**

- Log in to the device's web page, and in the **[Network] >> [Wi-Fin Settings]** interface, turn on Wi-Fi.
- After adding Wi-Fi information, click **[Add]**.
- You will then see the connected Wi-Fi in the wireless network list.

## 14.3 Network Mode

- There are three IP Mode options available: IPv4, IPv6, and IPv4 & IPv6.

- Users can set the network mode on the device by navigating to **[Menu] >> [Settings] >> [Advanced] >> [Ethernet]**.
- Users can also set the network mode via the web interface by going to **[Network] >> [Basic] >> [Network Type].**

## 14.4 Network Server

**Setting Method:**

- Log in to the device web page **[Network] >> [Service Ports] >> [Server Port Settings]** to configure the web server type, which allows configuration of web login protocol type, login ports, and other parameters.

**Configuration Details:**

- Web Server Type: Changes take effect after a restart. You can choose the web login to be either HTTP or HTTPS.
- Web Login Timeout: Default is 15 minutes. After this time, the login session will automatically expire, requiring a new login.
- Web Auto Login: After timeout, re-login to the web page does not require entering username and password; it will automatically log in.
- HTTP Port: Default is 80. For enhanced system security, you can set a port other than 80, such as 8080. Web login would be: HTTP://IP:8080
- HTTPS Port: Default is 443, used in the same way as the HTTP port.

## 14.5 VPN

**Feature Description:**

- Virtual Private Network (VPN) is a technology that allows devices to create a connection to a server and become part of the server's network. The network transmission of the indoor unit can be connected through the VPN server routing function.
- For some users, particularly corporate users, it may be necessary to establish a VPN connection before activating line registration. The device supports two VPN modes: Layer 2 Tunneling Protocol (L2TP) and OpenVPN.

- Users must enable (or disable) and configure the VPN by logging into the web page.

- **L2TP Setup Method:**
- Visit the Manager webpage **>> [Network] >> [VPN]**, enable VPN mode, select "L2TP" as the type, and then fill in the L2TP server address, L2TP authentication username, and authentication password. Click "Apply" and the phone will attempt to connect to the L2TP server.
- When establishing a VPN connection, the VPN IP address will be displayed in the VPN status area. There may be delays in establishing the connection. Users need to refresh the page to update the status timely.
- Once the VPN configuration is successful, the indoor unit will automatically attempt to connect to the VPN each time unless disabled. Sometimes, if the VPN connection is not established promptly, users can try restarting the device and check if the VPN has been successfully established after the restart.

> **Note：**
>
> The device only supports basic unencrypted authentication and data transmission. If users require data encryption, please use the OpenVPN feature instead.

**To set up an OpenVPN connection, follow these steps:**

- Obtain authentication and configuration files from your OpenVPN service provider. The files required include:
  - OpenVPN Configuration file: client.ovpn
  - CA Root Certification: ca.crt
  - Client Certification: client.crt
  - Client Key: client.key

- Upload the files listed above to the Manager's webpage under **[Network] >>[ VPN ]**, and select the OpenVPN files.

- Go to the device webpage, navigate to **[Network] >>[ VPN ]**, enable VPN mode, choose **"OpenVPN"** as the type, and submit the information to activate the OpenVPN feature.

Like the L2TP connection, the system will attempt to establish a connection upon every system restart until manually disabled by the user.

## 14.6 VLAN

VLAN (Virtual Local Area Network) technology allows a LAN to be divided into multiple logical LANs—VLANs, each VLAN being a broadcast domain where broadcast messages are confined within a single VLAN.

Support is provided for acquiring VLAN ID via LLDP, CDP, DHCP, and manual settings.

**LLDP (Link Layer Discovery Protocol)**

- Access the device web page **>> [Network] >> [Advanced] >>** Link Layer Discovery Protocol, configure LLDP settings:
  - Enable LLDP: Activate the LLDP protocol function
  - Packet Interval: Set the send interval for LLDP discovery packets
  - Enable Learning Function: Enable LLDP to autonomously learn VLAN configuration settings

**CDP (Cisco Discovery Protocol)**

- Access the device web page **>> [Network] >> [Advanced] >>** Cisco Discovery Protocol, configure CDP settings:
  - Enable CDP: Activate the CDP protocol function
  - Packet Interval: Set the send interval for CDP discovery packets

**DHCP VLAN**

- Access the device web page **>> [Network] >> [Advanced] >>** DHCP VLAN Settings, configure DHCP VLAN parameters:
  - Selection of Option Value: Enable or disable acquiring the VLAN ID through

DHCP OPTION.

- DHCP Option VLAN: Set the OPTION value, 128-254, to obtain the VLAN value via DHCP.

**Manual VLAN Setup**

- WAN VLAN Settings: Access the device web page **>> [Network] >> [Advanced] >> [WAN VLAN Settings]**, manually configure the WAN VLAN ID:
  - Enable VLAN: Activate the manual setting of the WAN VLAN function.
  - WAN VLAN ID: Set the WAN VLAN ID.。

# 15 Security Settings

## 15.1 Alarm Input

Alarm input detection interface: Used to connect devices such as infrared sensors, smoke detectors, and gas alarms.

When the alarm input is triggered, it can send a short message to a designated server address or make a call to a specified number, and play an alarm ringtone locally. This facilitates quick response by management personnel.

Users can modify related configuration parameters through the webpage at **[Security Settings] >> [Alert] >> [Input Alarm Settings],** or via the device **[Menu] >> [Security Setup] (enter security password).**

| Parameters | Description |
|---|---|
| **Basic Settings** | |
| Ringtone Duration | When the input interface triggers an alarm, if the alarm sound is enabled, specify the duration of the alarm sound. |
| Input & Tamper Server Address | Configure the remote response server address, including the remote response server address and the triggered alarm server address. When the input interface or tamper is triggered, it will send a short message to the server. The server address supports IP:PORT or SIP number. |
| Information | The alarm information to be sent:<br>✓ Parameters can be replaced with actual values. The supported parameters include:<br>✓ Model, replace with the actual model name<br>✓ Active_user, replace with the actual SIP username<br>✓ Mac, replace with the MAC address of the device<br>✓ IP, replace with the IP address of the device<br>✓ Trigger, replace with the triggered interface, such as input1, input2, etc. |

| | |
|---|---|
| | ✓ Trigger Name, replace with the triggered name. |
| **Input settings** | |
| **Parameters** | **Description** |
| Input 1 | Enable or disable Input 1 |
| Triggered by | When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger. |
| | When choosing the high level trigger (disconnect trigger), detect the input port (high level) disconnected trigger. |
| Name | Connected alarm name |
| Reset Code | Enter the reset code to stop the alarm after it has been triggered. |
| Input Duration | Set the Input change duration time, the default is 0 seconds. |
| Triggered Behavior | Enable or disable the input port from sending messages to the server. |
| Event | Triggered events: When connected to a door magnet, select door magnet; when connected to an indoor switch, select indoor switch. |
| Triggered Ringtone | Supports ringtone selection: None, no ringtone triggered. |

## 15.2 Short-circuit Input

Short-circuit input detection interface: Used for connecting devices such as switches, infrared probes, door sensors, and vibration sensors;

When the short-circuit input is triggered, it can send a text message to a specified server address, or make a call to a designated number, and play an alarm ringtone locally. This facilitates quick response by management personnel.

Users can modify the configuration parameters related to the input ports through the web interface by navigating to **[Security Settings] >> [Alert].**

| **Parameters** | **Description** |
|---|---|
| **Basic Settings** | |

| | |
|---|---|
| Ringtone Duration | When the input interface triggers an alarm, if the alarm sound is enabled, specify the duration of the alarm sound. |
| Input & Tamper Server Address | Configure the remote response server address, including the remote response server address and the triggered alarm server address. When the input interface or tamper is triggered, it will send a short message to the server. The server address supports IP:PORT or SIP number. |
| Information | The alarm information to be sent:<br>✓ Parameters can be replaced with actual values. The supported parameters include:<br>✓ Model, replace with the actual model name<br>✓ Active_user, replace with the actual SIP username<br>✓ Mac, replace with the MAC address of the device<br>✓ IP, replace with the IP address of the device<br>✓ Trigger, replace with the triggered interface, such as input1, input2, etc.<br>✓ Trigger Name, replace with the triggered name. |

**Input settings**

| **Parameters** | **Description** |
|---|---|
| Input 1 | Enable or disable Input 1 |
| Triggered by | When choosing the low level trigger (closed trigger), detect the input port (low level) closed trigger. |
| | When choosing the high level trigger (disconnect trigger), detect the input port (high level) disconnected trigger. |
| Input Duration | Set the Input change duration time, the default is 0 seconds. |
| Triggered Behavior | Enable or disable the input port from sending messages to the server. |
| Event | Triggered events: When connected to a door magnet, select door magnet; when connected to an indoor switch, select indoor switch. |
| Triggered Ringtone | Supports ringtone selection: None, no ringtone triggered. |

## 15.3 Relay Output

Relay output control interface: Used to control electric locks, alarm systems, etc.

The relay output can be triggered via SMS, active URI, call status, etc., and will reset after the configured timeout period.

Users can modify the output port settings via the web interface under **[Security Settings] >> [Alert].**

| Parameters | Description |
|---|---|
| Enable Logs | Enable or disable LOG |
| Triggered by URI Ringtone | Whether to play a prompt ringtone when the relay output port is triggered by URI. |
| Triggered By SMS Ringtone | Whether to play a prompt ringtone when the relay output port is triggered by SMS |
| Standard Status | "Whether the default state of the relay is normally closed or normally open is recommended to be kept as default. The choice between normally closed and normally open can be made by connecting to the NC/NO port of the relay. |
| Output Duration | The duration of the relay output trigger is set to 5 seconds by default. After 5 seconds, it returns to the standard state." |
| Trigger by active URI | Enable or disable URI triggering.<br>Sending commands from a remote device or server, if correct, triggers/resets the corresponding output port. |
| Trigger Message | Messages Triggered by Output Port |
| Reset Message | Messages Sent on Reset |

| | |
|---|---|
| Short Message Trigger | Enable or Disable Short Message Triggering.<br>When a command is sent to a remote device or server, if it is correct, it triggers/resets the corresponding output port. |
| Input Trigger | Choose whether the relay output port can be triggered via the input port. When the input port is configured as an indoor switch and the corresponding input is enabled here, the input port can be used to trigger the door to open. |
| Trigger By Call Status | Whether to allow call state triggering of the relay. For example, triggering the output port by a call (the output port will remain in the call state continuously responding). Supported call states include:<br>1. Ringing<br>2. Talking<br>3. Talking (Calling)<br>4. Talking (Called)<br>5. Talking (Intercom)<br>6. Talking (Multicast) |
| Triggered Hangup | Enabling the auto hangup feature by checking this option. After the relay is triggered, it will automatically hang up. |
| Hangup Delay | Default is 5 seconds. After enabling auto hangup, the relay will automatically hang up 5 seconds after opening the door. |

# 16 Security

## 16.1 Menu Password

Users can customize and change the menu password, supported through both the web interface and device menu.

**Via web interface:**

Navigate to **[Device Settings] >> [Advanced] >> [LCD Menu Password Settings],** change the menu password, and click [**submit].**

**Via device menu:**

Tap on **[Menu] on the desktop >> [Settings] >> [Advanced ] >> [Password]**, enter the current menu password (default password is 123), and save after setting.

**Password change settings:**

- Current password: The password you have set, with the default password being 123.
- New password: The new menu password you wish to set.
- Confirm password: Re-enter the new menu password, which must match the new password exactly.

**Note：**

Once set, the new password takes effect immediately. To access the device menu, the new password must be used.

## 16.2 Web Password

Users can customize and change the web login password by accessing the webpage at **[System] >> [Account] >> [User Management]** and selecting the account to modify.

**Password change settings:**

Current Password: Enter the web login password.

New Password: Enter the new login password.

Confirm Password: Re-enter the new login password to confirm.

> **Note：**
>
> After changing the password, you will be automatically logged out and must re-enter the new password to log in again.

## 16.3 Security Password

Users can customize and change the security password by clicking on the desktop **[Menu] >>[Settings]>>[Advanced]>>[Password]** to modify the security password. Enter the current menu password (default password is 1234) and click save after setting.

**Password change settings:**

- Current Password: The password you have set, the default password is 1234.
- New Password: The new menu password you wish to reset.
- Confirm Password: Re-enter the new menu password, which must be exactly the same as the new password.。

> **Note：**
>
> Once the settings are complete, the new password takes effect immediately. To access the device security interface, you will need to use the new password.

## 16.4 Web Filter

Users can configure to allow only machines from a specific IP subnet to access and

manage the configuration of the device.

Navigate to the webpage **[Security] >> [Web Filter],** add or delete allowed IP subnets. Configure the starting and ending IP addresses within the specified range, then click **[Add]** to apply the changes. You can set a large subnet or add multiple subnets. When deleting, choose the starting IP of the subnet you want to remove from the dropdown menu, and then click **[Delete]** to apply the changes.

Enable Web Filtering: Configure to enable/disable web access filtering. Click the **[Submit]** button to apply the changes.

> **Note：**
>
> If accessing the device from a machine within the same subnet, do not configure the web filtering subnet to be outside of your own subnet; otherwise, you won't be able to log in to the webpage

## 16.5 Mutual Authentication

The device supports mutual authentication using HTTPS and SIP TLS.

**Certificate Management**

- Device Certificate: Access the web page **[Security] >> [Device Certificates]** to set the device certificate parameters:
  - Device Certificates: Choose the device certificate to be used for authentication, which can be either the default certificate built into the device or a custom certificate uploaded by the user.
  - Import Certificates: Upload a custom device certificate.
  - Certificate File: Displays the list of uploaded custom device certificates. Only one custom device certificate can be uploaded. If no custom certificate is uploaded, the certificate list will be empty.

- Trusted Certificates: Access the web page **[Security] >> [Trusted Certificates]** to set the trusted certificates parameters:
  - ➢ Permission Certificate: Used to decide whether to enable server certificate verification.
  - ➢ Common Name Validation: Option to enable or disable common name validation.
  - ➢ Certificate Module: Select the certificate module to be used, with the following options:
    - ✓ All Certificates: Trusts all certificate modules, including both the custom uploaded trusted certificate list and the built-in trusted list in the device.
    - ✓ Default Certificates: Trusts the built-in trusted certificate list of the device.
    - ✓ Custom Certificates: Trusts the custom uploaded trusted certificate list.
  - ➢ Import Certificates: Used to import trusted certificates from the server side.
  - ➢ Certificate List: Displays the list of custom uploaded server trusted certificates.

**Mutual Authentication Explanation**

- Upload the device certificate used to the server's trusted certificate list, ensuring that the server's trusted certificate list includes the device's certificate. Please confirm with the server administrator.
- Access the web page **[Security] >> [Trusted Certificates] >> [Import Certificates]** to upload the server's device certificate to the device's trusted certificate list and select the trusted certificate module to use.

## 16.6 Network Firewall

**Setting the Network Firewall**

- Access the device's web page >> **[Security] >> [Firewall]**, where you can set whether to enable the inbound and outbound firewall. You can also define rules for the inbound and outbound traffic through the firewall. These settings help prevent malicious network access and restrict internal users from accessing certain external network resources, thereby enhancing security.

**Feature Description**

- The firewall rule setting is a simple firewall module that supports two types of rules: inbound rules and outbound rules. Each rule is assigned a sequence number, with a maximum of 10 rules allowed for each type.
- Once the parameters are set, clicking **[Add]** will add a new item to the firewall's outbound rules.
- To delete an item, select the desired list and click **[Delete]** to remove the selected list.

**Parameters：**

| **Parameter** | **Description** |
|---|---|
| Enable Input Rules | Indicates that the input rule application is enabled. |
| Enable Output Rules | Indicates that the output rule application is enabled. |
| Input/Output | To select whether the currently added rule is an input or output rule. |
| Deny/Permit | To select whether the current rule configuration is disabled or allowed; |
| Protocol | There are four types of filtering protocols: TCP \| UDP \| ICMP \| IP. |
| Src Port Range | Filter port range |
| Src Address | Source address can be host address, network address, or all addresses 0.0.0.0; It can also be a network address similar to *.*.*.0, such as: 192.168.1.0. |
| Dst Address | The destination address can be either the specific IP address or the full address 0.0.0.0; It can also be a network address similar to *.*.*.0, such as: 192.168.1.0. |
| Src Mask | Is the source address mask. When configured as 255.255.255.255, it means that the host is specific. When set as 255.255.255.0, it means that a network segment is filtered. |
| Dst Mask | Is the destination address mask. When configured as |

| | |
|---|---|
| | 255.255.255.255, it means the specific host. When set as 255.255.255.0, it means that a network segment is filtered. |

# 17 Trouble Shooting

When the device is not in normal use, the user can try the following methods to restore normal operation of the device or collect relevant information and send a problem report to Fanvil technical support mailbox.

## 17.1 Get Device System Information

Users can obtain information through the device webpage **[System] >> [Information]** or the device **[Menu] >> [System]** options. The following information will be provided:

1. Device information (model, software and hardware version).
2. Account information.
3. Internet Information.

## 17.2 Reboot Device

Users can restart the device via the web interface or device menu.

**Device Interface Restart:**

Click on **[Menu] >> [Settings] >> [Basic] >> [Reboot] and press [OK].**

**Web Interface Restart:**

Click on **[System] >> [Reboot Device] and press [OK].**

**Power Cycle Restart:**

Simply unplug the device and plug it back in to restart.

## 17.3 Device Factory Reset

Users can restore the device to default settings through the web interface or the device menu.

**Device Interface Restore:**

Click on **[Menu] >> [Settings] >> [Advanced] (enter password:123) >> [Factory Reset]**, select **'Clean All'**, and press [√].

**Web Interface Restore:**

Click on **[System] >> [Configurations] >> [Reset Device] >> [Reset] button and press [OK]**.

## 17.4 Screenshot

If the device encounters issues, taking a screenshot can help technical support locate specific functions and understand the problem. To capture a screenshot, log in to the webpage, go to **[System] >> [Tools] >> [Screenshot], click [Save BMP] (capture the problematic screen)**, save the image, and send it to technical support for issue resolution.

## 17.5 Network Packets Capture

In order to obtain the data packet of the device, the user needs to log in to the webpage of the device, open the webpage [**System**] >> [**Tools**] >> [**LAN Packet Capture**], and click the [**Start**] option in the "Network Packets Capture".If you are using a WiFi network, click the [**Start**] option in [**WLAN Packet Capture**]. A message will pop up asking the user to save the captured file. At this time, the user can perform related operations, such as starting/deactivating the line or making a call, and clicking the [**Stop**] button on the webpage after completion. Network packets during the device are saved in a file. Users can analyze the packet or send it to the Technical Support mailbox.

## 17.6 Get Device Log

When encountering abnormal issues, log information can be helpful. The device supports exporting system logs and WiFi logs.

**Obtain system log：**

To obtain the device's log information, users can log into the device's webpage, navigate to **[System] >> [Tools] >> [Syslog]**:

- Set the system log to diagnostic mode.
- Enable log export and submit the changes.

Follow the steps where the issue occurs until it appears, then go to **[System] >> [Tools] >> [Export Log]** and click on export logs to save the logs locally for analysis or send them to technical staff for problem resolution.。

**Obtain WiFi Log:**

To obtain the device's WiFi log information, users can log into the device's webpage, navigate to **[System] >> [Tools] >> [WLAN Logs]**:

- Enable WLAN logging and submit the changes.

Follow the steps where the issue occurs until it manifests, then go to**[System] >> [Tools] >> [WLAN Logs]** and click on export logs to save the logs locally for analysis or send them to technical staff for problem resolution.。

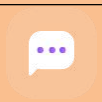
## 17.7 Common Trouble Cases

| Trouble Case | Solution |
|---|---|
| Device could not boot up | 1. The device is powered by a power adapter. Please use a compliant power adapter and check if the device is connected to power.<br>2. The device is powered by PoE. Please use a compliant PoE switch. |
| Device could not register to a service provider | 1. Please check if the device is connected to the network.<br>2. Verify if the device has an IP address. Check the system information; if the IP address is 0.0.0.0, it indicates that the |

| | |
|---|---|
| | device has not obtained an IP address. Ensure that the network configuration is correct.<br>1. If the network connection is fine, recheck your cable configuration. If all configurations are correct, contact your service provider for support, or follow the instructions in "16.5 Network Data Capture" to obtain network packets for analysis. Send them to the support email to help diagnose the issue.。 |

# 18 Appendix Table

## 18.1 Appendix I - Function Icon

| Icon | Description |
|---|---|
|  Dialer | Click this icon to enter the pre-dial interface, and then dial the number using the screen or keyboard. |
|  SMS | Have SMS writing, reading and sending functions |
|  Menu | Click this icon to enter the app list interface |
|  Monitor | Add, view, and edit monitoring devices |
|  Door Lock | Edit the door lock and open the door Settings. |
|  Function Key | Set function keys for one-touch speed dialing. |
|  Do-Not-Diturb | Enable or disable Do Not Disturb. |

## 18.2 Appendix II - Menu Icon

| 图标 | 描述 |
|---|---|
|  Status | View the status of the network, device, and account. |

| | |
|---|---|
|  Call Log | Display call logs of the device, including incoming, outgoing, missed, and forwarded calls. |
|  Application | Ping，QrCode |
|  PhoneBook | Access local contacts, cloud phonebook, and access control list on the device for quick contact search. |
|  SMS | View and send text messages. |
|  MWI | View and listen to voice messages. |
|  Settings | Personal preferences, call settings, network settings, etc. |
|  Security Settings | Enable security alarm settings. |

## 18.3 Appendix III - Status And Notification Icon

| Icon | Description |
|---|---|
|  | Auto-answering activated |
|  | Call forward activated |
|  | Do-Not-Diturb |
|  | SIP Hotspot |

| | |
|---|---|
|  | Miss Calllog |
|  | Mute Microphone |
|  | Normal Network |
|  | Network Disconnected |
|  | Enable VLAN |
|  | Enable VPN |
|  | Unread messages |
|  | Unread voice message |
|  | WIFI network anomaly |
|  | Connecting WIFI |
|  | Network storm |

## 18.4 Appendix IV - Function Key Status Definition

| Type | Icon | Status | Description |
|---|---|---|---|
| Line Key |  | Gray | Line out configured |
| |  | Green steady light | Line is available (registered) |
| |  | Green and gray alternating | Ring |
| |  | Red and gray alternating | Registering/Registration failed |
| |  | Red | Dialing/Line in use (Calling) |

| Type | Icon | Status | Description |
|---|---|---|---|
| DND |  | Red steady light | Enable DND |
| |  | White | Disable DND |
| MWI |  | Red badge with a number displayed in the top right corner | New voicemail |
| |  | White | No new voicemail |

## 18.5 Appendix V – Keyboard Character Lookup Table

| Icon | Description |
|---|---|
|  | Return |
|  | Space Key |
|  | Delete |
|  | Collapse keyboard |
|  | Move cursor left |
|  | Move cursor right |
|  | Save |
|  | Switch to uppercase letters |
|  | Switch to numeric and special character keyboard |