i66&i67 User Manual

Version:2.12 | Release Date:2024/01/02

Directory

Directory I

1 Safety Instruction 1

1.1 Safety Instruction 1

1.2 FCC 1

2 Product Overview 3

2.1 Overview 3

2.2 Specification Parameter 3

3 Installation Instructions 4

3.1 Device Inventory 4

3.2 Installation Procedure 4

3.2.1 Wall-mounted 4

3.2.2 Flush mounting: 9

4 User Guide 11

4.1 Button and Interface Instructions 11

4.1.1 i66 Button and Interface Instructions 11

4.1.2 i67 Button and Interface Instructions 12

4.2 Standby Screen Instructions 13

4.2.1 i66 Standby Screen Instructions 13

4.2.2 i67 Standby Screen Instructions 14

4.3 Touchscreen Instructions（Only i67） 15

4.3.1 Touch Method 15

4.3.2 Touch Keyboard 15

4.4 Configuration Menu Introduction 15

4.5 Device Status 16

4.6 Web Management 16

4.6.1 Device IP Address 16

4.6.2 Web Interface 17

4.7 Language Settings 17

4.8 Line Settings 17

5 Calling Features 19

5.1 Making Calls 19

5.1.1 Dial Directly 19

5.1.1.1 i66 Dial Directly 19

5.1.1.2 i67 Dial Directly 19

5.1.2 IP Call 19

5.1.2.1 i66 IP Call 19
5.1.2.2 i67 IP Call 19
5.1.3 Call Through Contacts 19
5.1.3.1 i66 Call Through Contacts 19
5.1.3.2 i67 Call Through Contacts 20
5.1.4 Speed Dial 20
5.1.4.1 i66 Speed Dial 20
5.1.4.2 i67 Speed Dial 20
5.2 Answer 20
5.2.1 Auto Answer 20
5.3 End The Call 21
5.3.1 i66 End The Call 21
5.3.2 i67 End The Call 21
5.4 Call Settings 21
5.4.1 IP Call Settings 21
6 Advance Function 22
6.1 MCAST 22
6.2 Hotspot 23
7 Door Opening Operation 25
7.1 Card Management 25
7.2 Password Management 27
7.3 Face Recognition 29
7.4 Period Management 29
7.5 Relay Settings 31
7.5.1 Relay Settings 31
7.5.2 Door Sensor Settings 33
7.6 Face Settings 34
7.6.1 Face Settings 34
7.6.2 Prompts Settings 35
8 Monitoring function 36
8.1 RTSP 36
8.2 ONVIF 36
9 Contacts 37
9.1 Contact 37
9.1.1 Management Contacts 37
9.1.2 Importing & Exporting Contacts 37
9.2 Restricted Incoming Call List 38

9.3 Restricted Outgoing Call List 38
10 Open The Door Record 39
10.1 Open The Door Record 39
10.2 Passerby Record 39
10.3 Fail Record 39
11 Device Functions 40
11.1 Time Plan 40
11.2 maintenance 41
11.2.1 Configurations 41
11.2.2 Upgrade 41
11.2.3 Auto Provision 41
12 Screen Settings 45
12.1 Time/Date 45
12.2 Screen Setting 46
12.2.1 Brightness and backlight 46
12.2.2 Screen Saver 46
12.2.3 UI Settings 47
12.2.3.1 Theme 47
12.2.3.2 Boot Logo 48
12.2.3.3 Standby Logo 49
12.3 LED Settings 49
12.3.1 Fill Light 49
12.3.2 Keyboard Backlight 49
12.4 Audio Settings 49
12.4.1 Volume settings 49
12.4.2 Tone Settings 50
12.4.3 Upload Ring 52
13 Network Settings 53
13.1 Ethernet Connection 53
13.2 Network Mode 53
13.3 Network Server 54
14 Security Settings 55
14.1 Short Circuit Input 55
14.2 Relay Output 56
14.3 Tamper 57
15 Security 59

15.1 Engineering Password 59
15.2 Web Password 59
15.3 Web Filter 60
16 Trouble Shooting 61
16.1 Get device system information 61
16.2 Reboot Device 61
16.3 Device Factory Reset 61
16.4 Screenshot 62
16.5 Network Packets Capture 62
16.6 Get device log 62
16.7 Common Trouble Cases 62
17 Appendix 64
17.1 Appendix I Function Icon 64
17.2 Appendix II Menu Icon 64
17.3 Appendix III – Keyboard character query table 65

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.

- Before using the external power supply in the package, please check the home power voltage. Inaccurate power voltage may cause fire and damage.
- Please do not damage the power cord. If power cord or plug is impaired, do not use it because it may cause fire or electric shock.
- Do not drop, knock or shake the phone. Rough handling can break internal circuit boards.
- Before using the product, please confirm that the temperature and humidity of the environment meet the working requirements of the product.
- Avoid wetting the unit with any liquid.
- 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.
- Do not use harsh chemicals, cleaning solvents, or strong detergents to clean it. Wipe it with a soft cloth that has been slightly dampened in a mild soap and water solution.
- When lightning, do not touch power plug, it may cause an electric shock.
- 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

NOTE: 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 a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, 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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

2 Product Overview

2.1 Overview

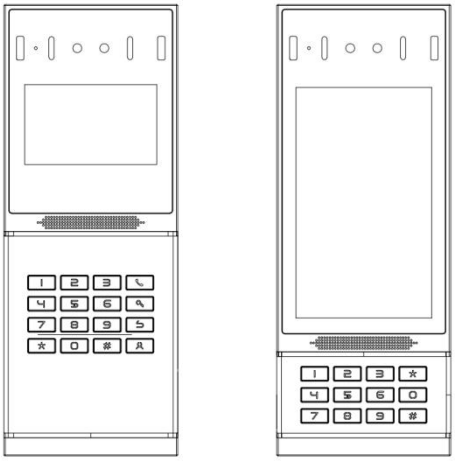
The i66 and i67 are newly designed facial recognition door phone by Fanvil. The product structure is crafted from aluminum alloy, with an explosion-proof rating of IK07. Featuring clear and thoughtful lines, the design provides users with a luxurious and elegant appearance, ensuring high-strength protection. With various door-opening methods available, it uses the standard SIP protocol, delivering high-definition voice communication quality for premium access control, security, and intercom services.

2.2 Specification Parameter

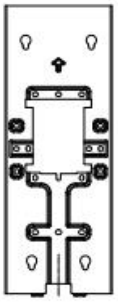
Spec.	i66	i67
Screen	4’ 800*480	7’ 600*1024
Camera	2*200M	2*200M
Short-circuit input	3	3
Relay output	2	2
Card	1,0000	1,0000
Password	1,0000	1,0000
Image	1,0000	1,0000
Tamper alarm	Support	Support
RS485	Support	Support
POE	Support	Support
Wall-mounted	Support	Support
Flush-mounted	Support	Support

3 Installation Instructions

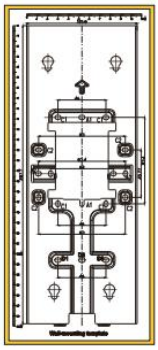
3.1 Device Inventory



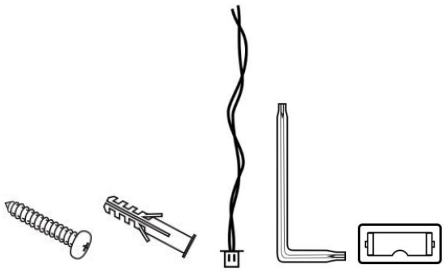
Device



Wall Bracket

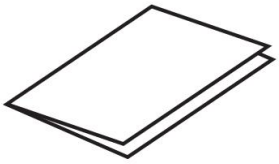


Mounting Template



Screws, Terminal Blocks, and Tools

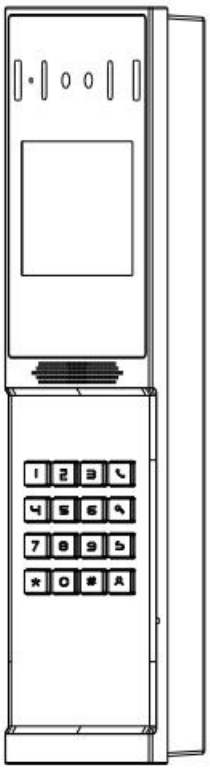
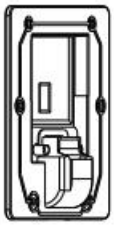
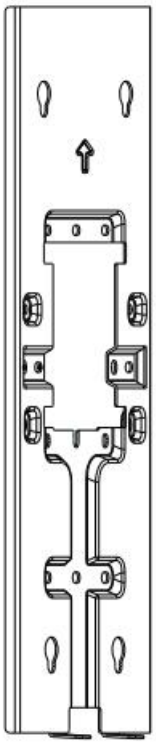
RFID Card 2pcs



Quick Installation Guide

3.2 Installation Procedure

3.2.1 Wall-mounted

Wall-mounted：

Step 1: Installation preparation

1，Check the following contents:

- KM3*30 screw x3
- TA4 x 30mm screw x5
- φ6*30mm screw anchor x5
- KM4*30 screw x3
- TM6#*20/screw x5
- KM3*6mm screw x3
- KB2.6*5 screw x1

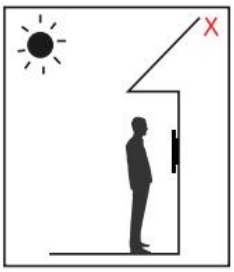
2，Tools required for installation

- The special L-shaped Torx screw tool provided with the product
- Ph2 or Ph3 Phillips screwdriver, hammer, RJ45 crimping pliers
- Wall drilling impact drill, 8mm impact drill x1

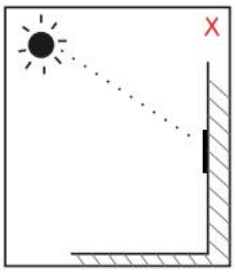
Step2：Installation Environment

- Do not install the device in the following locations: direct sunlight, high temperature, low temperature, areas with corrosive chemicals, and places with excessive dust. Install the device at an appropriate eye level, with a recommended mounting height of approximately 120-140cm.
- If installed indoors, maintain a distance of at least 2 meters from light sources and at least 3 meters from doors and windows to avoid direct sunlight.

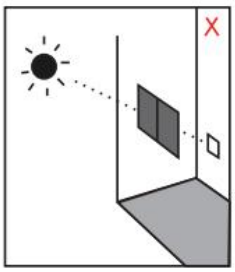
- Avoid severe vibration, collisions, and impacts, as they may cause damage to internal precision components and the outer casing.
- When the device is powered on, if any abnormal conditions are detected, the power should be immediately disconnected until the issue is resolved. After the system is abnormally disconnected, please check according to the user manual. If the cause cannot be determined, please contact the sales agent or the manufacturer's after-sales service provider. Do not attempt to repair the system on your own. When using access cards, handle them carefully to avoid damage from magnetic fields, water, bending, and other hazards. If equipped with facial recognition functionality, install it in an environment with uniform lighting to avoid situations where the camera faces strong backlight, is exposed to oblique light, or is subjected to close-range illumination.



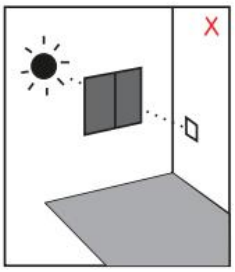
Face backlight



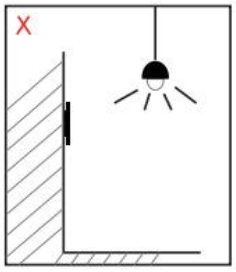
Direct sunlight



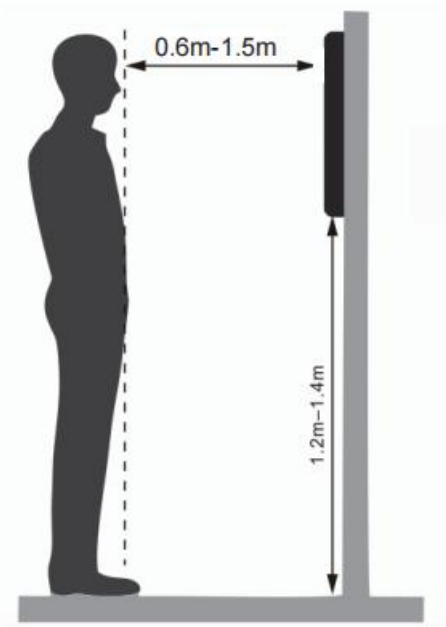
Sun shines directly through the window



Sun slanted through the window



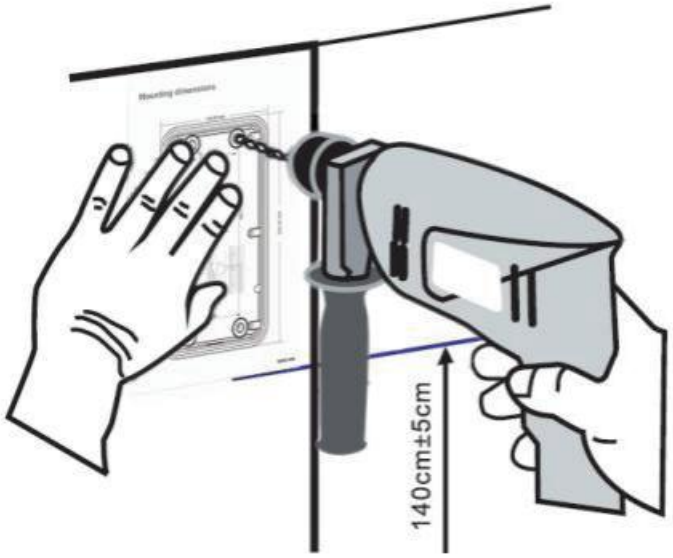
Lighting at close range



Note:

- One cannot assume that biometric recognition products are 100% applicable to all identification scenarios.

Step 3：Drilling

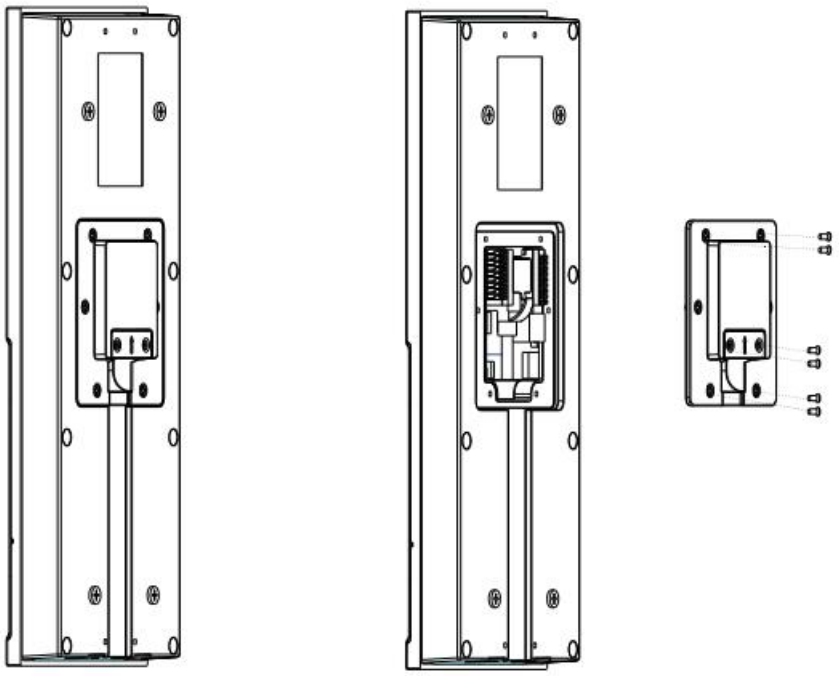


1，Paste the installation dimension drawing to the position to be installed.

2，Use an electric drill to drill the 4 holes marked on the mounting template. Remove the template when finishing drilling.

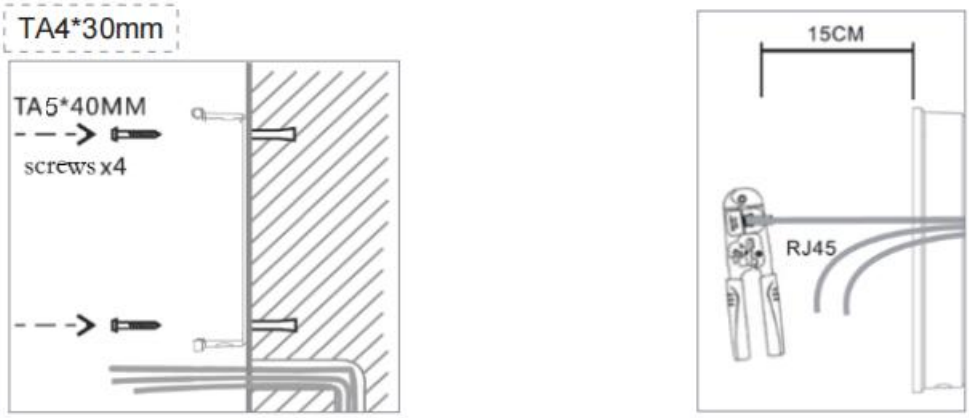
3，Push or hammer screw anchors into the drilled holes.

Step 4：Removing hanging bracket and back shell



The wall bracket is separated from the device downwards, and use a screwdriver to loosen the 6 screws of the rear case

Step 5 ： Install the wall bracket, wiring and casing

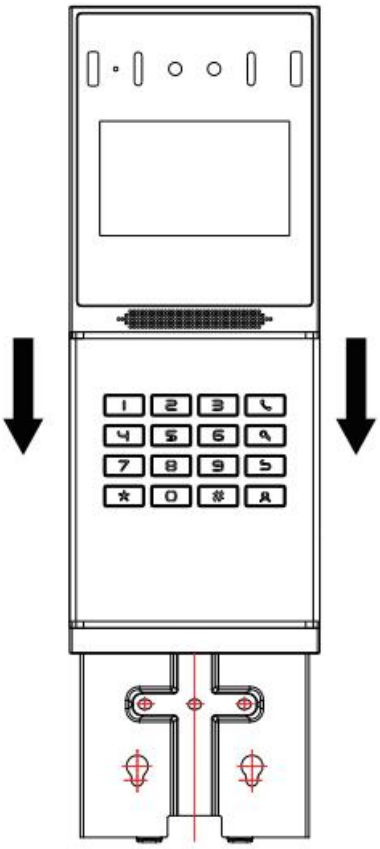


1. Align the screw holes of the wall bracket with the drilled holes on the wall, put in the φ6*30mm rubber plug, and fix it on the wall with the TA4*30mm screws provided.
2. Pass all the wires through the silicone plug in the middle of the bottom case, and reserve a length of 15~20CM for all wires。

Note：

- The outlet hole of the bottom case faces down

3. Connect the network cable with the RJ45 crystal head, and connect the power cable and the terminals of the electric lock control cable. Please refer to Section 2 for the connection sequence.
4. Connect the connected terminals to the motherboard socket, see Section 2 for the connection location.
5. Test whether there is electricity by doing the following:
   Enter the dialing interface, enter #*107, enter the password, enter the engineering mode, you can view the IP address of the device, and you can switch between static and dynamic IP modes.
   Enter the local opening password or test the indoor opening to see if the electric lock works normally.
   If it works fine, continue with the next steps.
6. Fasten the device and the wall bracket from top to bottom, and tighten the screws at the bottom



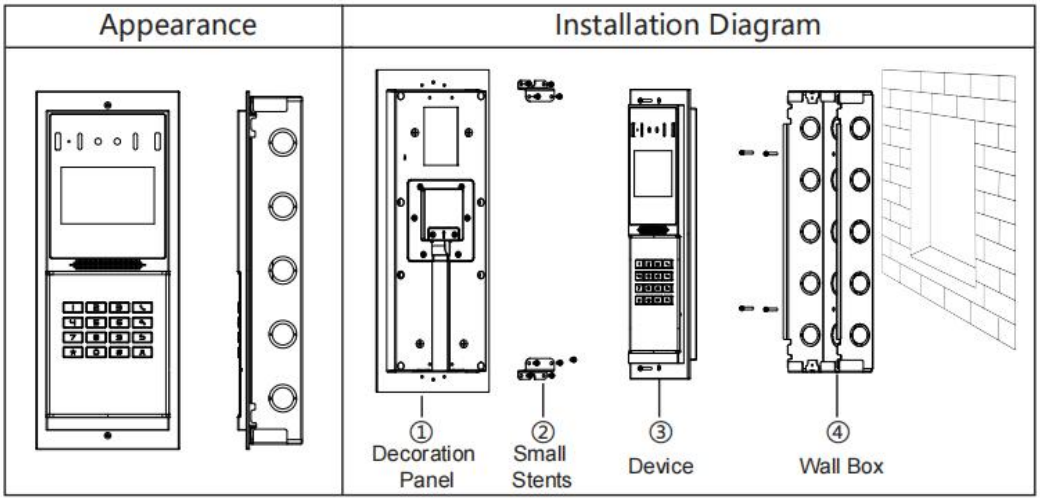
3.2.2 Flush mounting:

Step 1：Installation preparation

1，Check the following contents:

• Built-in wall box x1

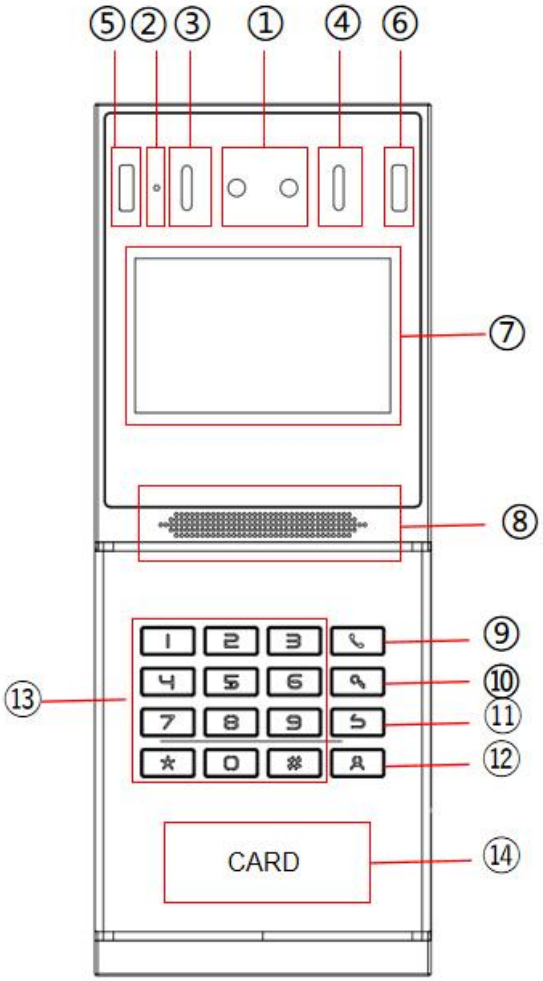
- Built-in wall decorative panel x1
- Built-in wall bracket x2
- KM3*6mm screw x3
- PM3*3mm screw x5
- PM3*4mm screw x5
- φ6*30mm screw anchor x5
- M3*70mm screwdriver x1



4 User Guide

4.1 Button and Interface Instructions

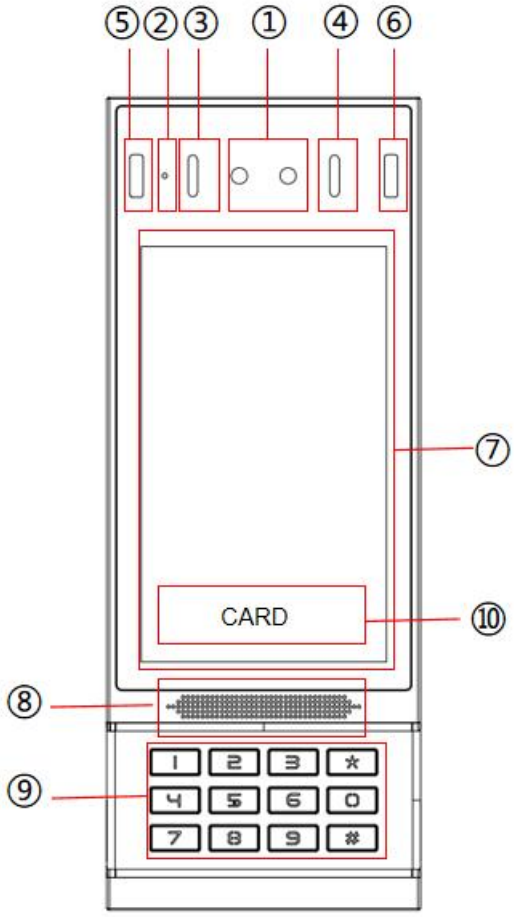
4.1.1 i66 Button and Interface Instructions



Number	Name	Description
①	IP Camera	Video signal acquisition and transmission
②	MIC	Audio acquisition
③④	Infrared lamp	Infrared Light Fill

⑤⑥	White Light Fill Light	When the lighting is insufficient and faces cannot be recognized, turn on the fill light for supplementary illumination
⑦	Screen	4-inch,Used for displaying facial recognition, calls, etc.
⑧	Speaker	Play sound
⑨	Dialing key	Dial
⑩	Unlock key	Unlock
⑪	Return key	Return
⑫	Concierge key	The user quickly calls the concierge
⑬	Numeric key	Numeric key
⑭	RFID area	Identification card

4.1.2 i67 Button and Interface Instructions



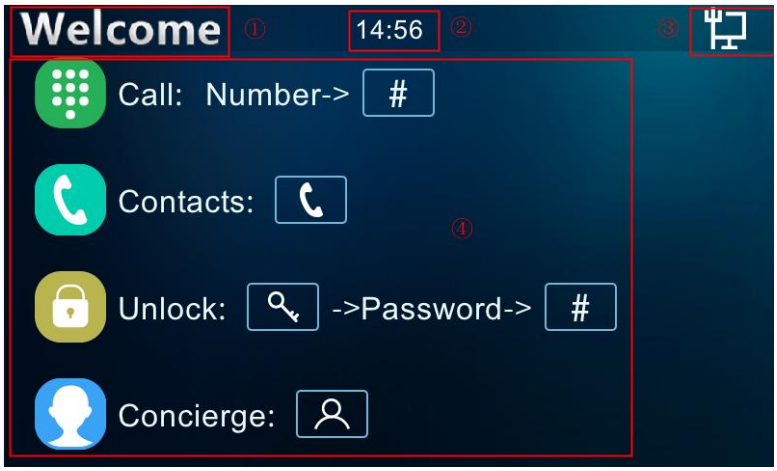
Number	Name	Description
①	IP Camera	Video signal acquisition and transmission

②	MIC	Audio acquisition
③④	Infrared lamp	Infrared Light Fill
⑤⑥	White Light Fill Light	When the lighting is insufficient and faces cannot be recognized, turn on the fill light for supplementary illumination
⑦	Screen	7-inch touch screen, Used for displaying facial recognition, calls, etc.
⑧	Speaker	Play sound
⑨	Numeric key	Numeric key
⑩	RFID area	Identification card

4.2 Standby Screen Instructions

4.2.1 i66 Standby Screen Instructions

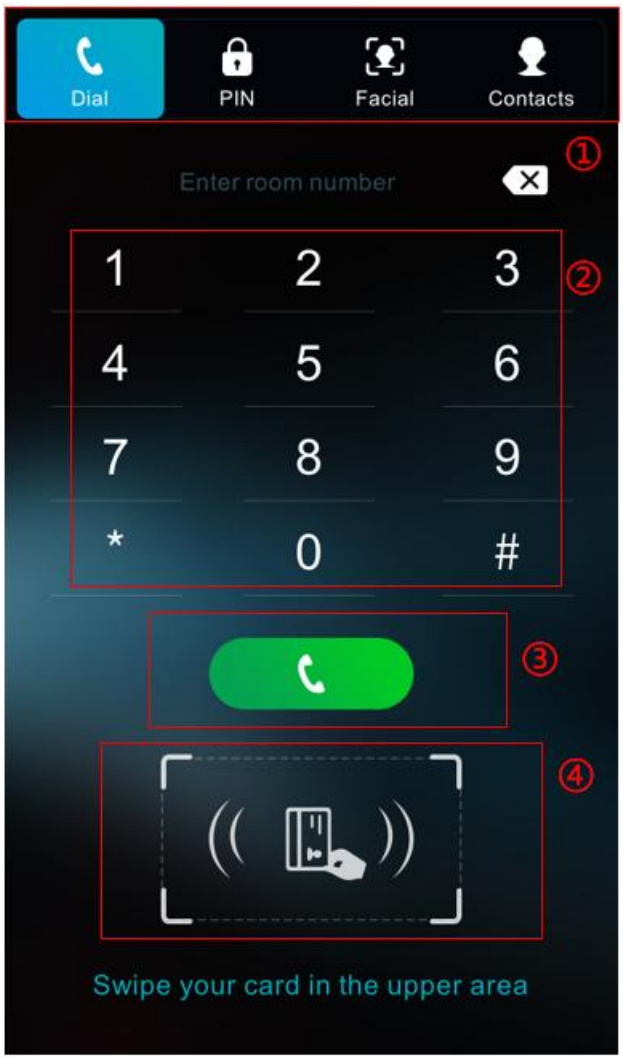
- The following image is the default standby screen interface, representing the state of the user interface for most of the time.
- The description of icons is provided in Appendix I.



Number	Description
①	Device Standby Logo
②	Display Time
③	Display Network Connection Status
④	The main screen displays operation instructions such as 'Dial,' 'Contacts,' 'Password Unlock,' 'Call Concierge,' etc.

4.2.2 i67 Standby Screen Instructions

- The following image is the default standby screen interface, representing the state of the user interface for most of the time.
- The description of icons is provided in Appendix II.



Number	Description
①	The function menu buttons allow switching between different functional interfaces. By default, they include Dial, PIN, and Contacts.
②	Number input and display area.
③	Call the entered number.
④	Card-swiping area, swipe the card in this area to open the door.

4.3 Touchscreen Instructions（Only i67）

The device can be configured and operated through the touchscreen, performing a series of configurations and operations.

4.3.1 Touch Method

- Click:

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

- Slide：

The device supports swiping up, down, left, and right.

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

4.3.2 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 keyboard, supports inputting numbers.
2. Alphabetic keyboard, supports inputting lowercase letters, uppercase letters, and common characters.
3. Character keyboard, supports inputting special characters.

4.4 Configuration Menu Introduction

i67 Menu:

In the dialing interface, enter '#*107' to access the engineering settings. The initial password for the engineering settings is 123456. After entering the engineering settings, click on the application icon for the corresponding submenu to access it.

i66 Menu:

In standby mode, enter '#*107' to access the engineering settings. The initial password for the engineering settings is 123456. Press the "#" key to enter the menu interface. Once in the menu interface, navigate by pressing the "2" key to move up, the "8" key to move down, and press the "Call" key to enter.

Menu Functions:

Menu	Description

System	Display network, device, and account information.
Network	Change network mode and network type.
Display	Adjust media volume, screen brightness, and time settings.
Language	Language settings.
Account	SIP account settings.
Factory Reset	Perform a factory reset on the device.
Reboot	Reboot the device.

4.5 Device Status

Users can view the status of i66/i67 through the device screen/web interface.

Viewing the status of i66/i67 through the device menu:

Entering the engineering settings menu, selecting **[System]** allows you to obtain the following status information for i66/i67:

- Network：Displays information about the device's network mode, IP address, and other network details.
- Device：Shows details such as the device's MAC address, product name, hardware version, software version, memory size, runtime, and more.
- Account：Provides information about registered accounts on the device, including account names/numbers and registration status.

Viewing the status of i66/i67 through the web interface:

Refer to the web 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, last runtime, WAN port speed, memory information, system time, SN (Serial Number), 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.

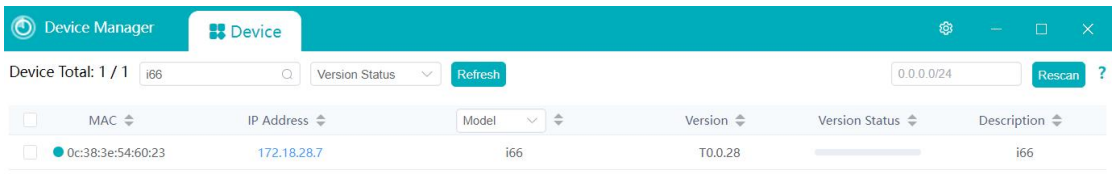
4.6 Web Management

4.6.1 Device IP Address

Retrieve Device IP through Scanning Tool:

1. Connect the computer and i66/i67 to the same local network, and install Device Manager on the PC.

2. Open the IP scanning tool (Device Manager), click on the scan button to obtain the IP address of i66/i67 devices 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 **[System]** >>**[Network]**.

4.6.2 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."

4.7 Language Settings

Users can set the language for i66/i67 through both the device interface and the web interface. Upon initial startup under factory settings, the default language is English.

Setting the language through the device menu interface:
Access the device engineering settings menu, choose **[Language],** and proceed with language settings.

To set the language through the device web interface:
Log in to the device web page, and in the language dropdown box located at the top right corner of the page, set the language.

4.8 Line Settings

The device supports two SIP accounts simultaneously, allowing registration based on application. Users can switch between the two 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 accounts through the device menu by navigating to **[Accounts]**.They can switch between SIP lines, register a SIP account, and, after completing the SIP parameter settings, click "Save" to successfully complete the registration.

Registering an account through the web interface:

Users can register a SIP account through the web page by navigating to **[Line]** >> **[SIP]** >> **[Line]**. selecting the registered line, and registering the SIP account through **[Basic 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 Calling Features

5.1 Making Calls

5.1.1 Dial Directly

5.1.1.1 i66 Dial Directly

Follow the on-screen instructions, input the desired number in standby mode, and press the **[#]** key  to make the call.

5.1.1.2 i67 Dial Directly

Enter the **[Dial]** interface, input the desired number, and click the **[Call]** button  to initiate the call.

5.1.2 IP Call

5.1.2.1 i66 IP Call

In standby mode, enter the IP address of the device you want to call. Replace the '.' in the IP address with the '*' key. After completing the input, press the **[#]** key  to initiate the call.

5.1.2.2 i67 IP Call

Enter the **[Dial]** interface, input the IP address of the device you want to call, replacing the '.' in the IP address with the '*' key. Click the **[Call]** button  to initiate the call.

5.1.3 Call Through Contacts

5.1.3.1 i66 Call Through Contacts

Reference: Speed Dial, Add Contact

In standby mode, press the **[Dial]** key  to enter the contact list. Use **[2]** or **[8]** to scroll up or down and select the desired contact to call.

After selecting, press the **[Dial]** key  to make the call. Press the **[Return]** key  to exit the contacts interface and return to the standby interface.

5.1.3.2 i67 Call Through Contacts

Reference: Manage Contacts, Add Contacts.

On the standby interface, click the **[Contacts]** icon  to enter the contact list. Choose or search for the desired contact, then click the **[Call]** button  to initiate the call.

5.1.4 Speed Dial

Users can set the quick call numbers through the web page. Navigate to **[Function Keys]**>> **[Function Keys]** on the web page.

- Type: Set the type of quick key, configure it as a memory key.
- Name: Set the name.
- Value: Enter the number to be called.
- Subtype: Set it as speed dial.
- Line: Set the calling line.
- Media: Choose between voice call or video call.

5.1.4.1 i66 Speed Dial

Press the **[Concierge]** button  for speed dial call.

5.1.4.2 i67 Speed Dial

On the dialing interface, click on the set speed dial number for calling, or click on the shortcut list to choose a quick dial number for calling.

5.2 Answer

5.2.1 Auto Answer

Users can disable the automatic answer function on the device web page (enabled by

default). Once disabled, you will hear the incoming call ringtone, and it will not automatically answer after a timeout.

- **Automatic Answer Enabled for Line:**

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

- **Automatic Answer Enabled for IP Call:**

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

5.3 End The Call

5.3.1 i66 End The Call

During a call, press the **[Return]** key  to end the call.

5.3.2 i67 End The Call

During a call, click the **[Hang Up]** button  on the call interface to end the call.

5.4 Call Settings

5.4.1 IP Call Settings

Users can configure IP call settings through the web page at **[Lines]** >> **[Basic Settings]**.

Configuration parameters:

- Enable Auto Answer: When enabled, the device will automatically answer IP calls.
- Auto Answer Delay: Set the waiting time for automatic answer in IP calls. The device will answer automatically after the specified waiting time.

6 Advance Function

6.1 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	Listened multicast server name.
Host:port	Listened multicast server's multicast IP address and port.
Channel	0-25 (24: Priority Channel, 25: Emergency Channel).

MCAST Dynamic：

Description: 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.

6.2 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. 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
Remote 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
Ring Mode	Select 'All' for both the client and hotspot to ring. Select 'Client' for only the client to ring. Select 'Hotspot' for only the hotspot to ring

Line Settings	Sets whether to enable the SIP hotspot function on the corresponding SIP line

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

7 Door Opening Operation

Unlock the door in the following ways:

1) Face recognition to open the door, through the pre-saved face data to open the door.

2) Open the door by swiping the RFID card, which supports IC card and ID card.

3) The access control helps to call owner, and the owner enters the remote opening password to open the door.

4) The other device helps to call the door phone, enters the corresponding remote authentication code, and opens the door after timeout or the password check length is reached (the authentication code shall be configured in the access list).

5) Access granted by entering a password or temporary password on the device.

6) The door can be opened through the indoor door button when the door phone is In any state.

7) Timed door opening: automatically opens the door in a predetermined time period by setting a timed task.

7.1 Card Management

Place the access card in the card reader area(

or ). Upon successful recognition, the door will unlock. The device will display a 'Door Unlocked Successfully' message and play a corresponding prompt tone. Only access cards added to the access control system will be recognized; access cards not added to the system will result in recognition failure, displaying a 'Door Unlock Failed' message on the device along with a corresponding prompt tone.

Add Card:

1. Go to the web page: **[Security Settings] >>[Card Management] >> [Add Card]**
2. Type:

Normal, namely to open the door card.

Add Card, swipe the add administrator card in the normal mode, the device will enter the card add mode, and then swipe the card, the card that has not been added to the card list will be added. Once completed, swipe the add administrator card again to switch the device's card reader back to standard mode.

Delete Card, swipe the delete card administrator card in the normal mode, the device will enter the card delete mode, and then swipe the card, the added card will be deleted.After completing the deletion, swipe the delete administrator card again to switch the device's card reader back to normal mode.

Regular residents should use the ‘Normal’ type. Property managers hold the ‘add administrator card’ and ‘delete administrator card’.

Note：

Using the add administrator card and delete administrator card requires extreme caution. Forgetting to switch the card reader mode to normal mode might lead to data corruption for users and compromise the security of access control systems.

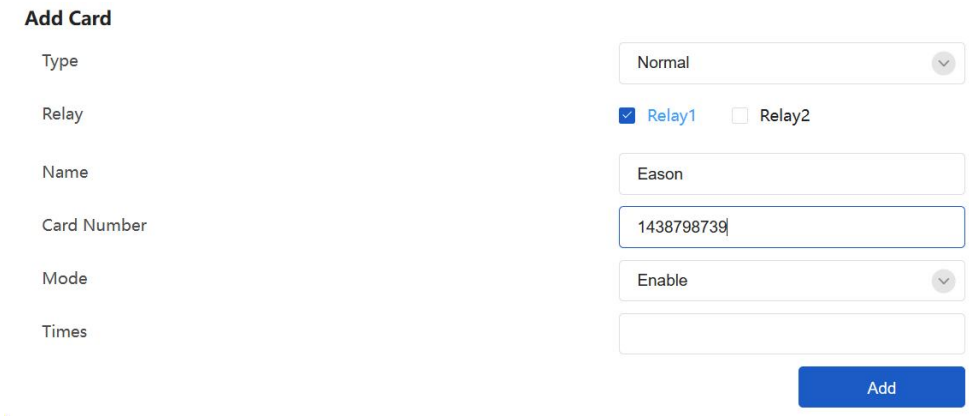
1. Mode : Disable, swiping is unsuccessful after disabling.

   Enable, swipe the card to take effect after enabling.

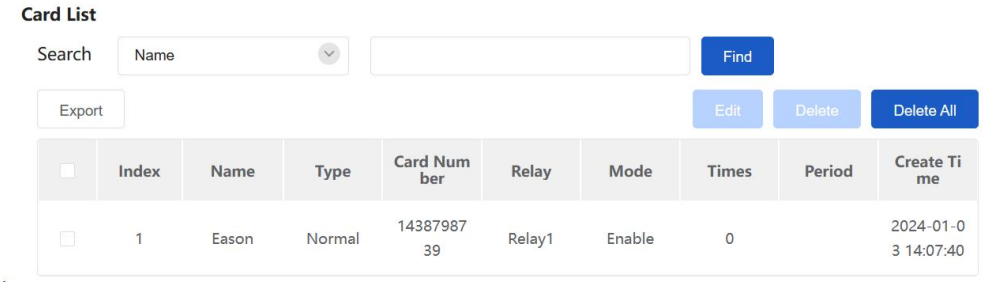
   Time period, swiping the card in the set time zone takes effect.

2. Times : Specifies the number of times a card can be swiped within a defined time frame. When no limit is configured, the card has unlimited usage. If a usage limit is set and reached, the card will be automatically 'disabled'.
3. Name : User name.
4. Card Number: RFID card number of the access card (first ten digits of the access card, for example, 0004111806). To configure and add an access card number on the web page, swipe the card once on the device, check the access log page, copy the card number, and paste it here.
5. Save Submission: The added card information will appear in the displayed list.

Add Card:



After submission:



7.2 Password Management

i66: Click the **[Unlock]** button  to access the password entry interface. Enter your personal password and press '#' to unlock the door. A popup notification will appear upon successful or unsuccessful attempts.

i67: Click on the icon 

displayed on the screen to access the password entry interface. Enter your personal password and press  to unlock the door. A popup notification will appear upon successful or unsuccessful attempts.

In the default configuration , the default door-opening password is 6789, and the default remote DTMF door-opening password is *.

Note：

It's advisable to modify the default local door-opening password to a user-defined one during the initial setup.

Add Password：

1. Go to the web page: **[Security Settings] >>[Password Management]>>[Add Password]**
2. Type:

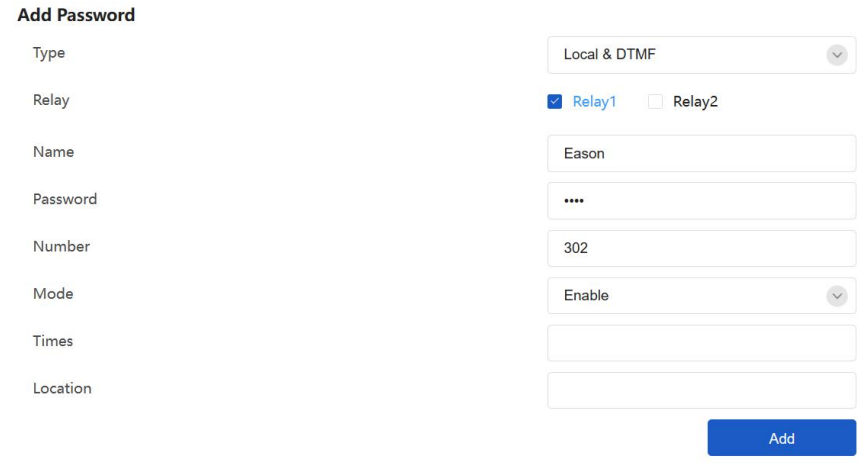
Local, that is, the local door opening password, enter the password dial interface in standby and enter the set opening password to open the door immediately.

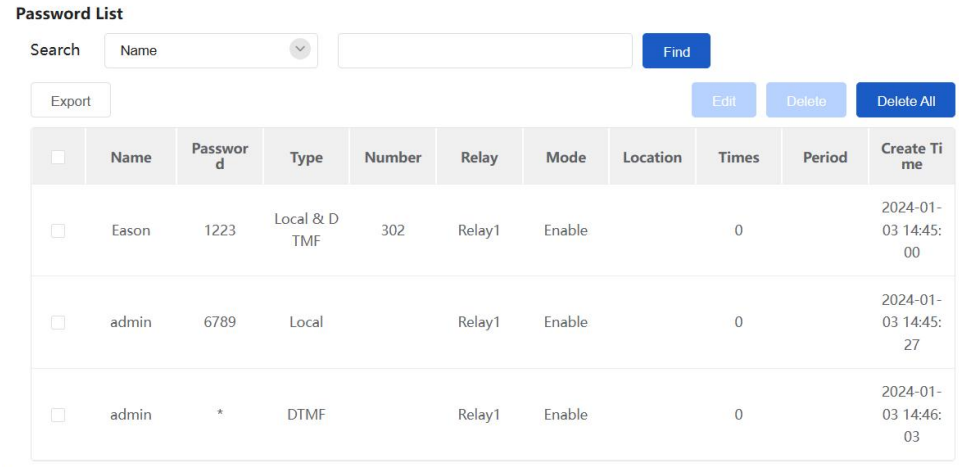
Remote, remote opening password, when the indoor unit calls the door or when the door calls the indoor unit to open the door, enter the DTMF password to open the door.

Remote and local, one password supports two door opening methods at the same time.

3. Times: The number of times the password can be used to open the door within the time period.
4. Name: User Name
5. Password: Password to open the door
6. Number: When the indoor unit calls the access control or the access control calls the indoor unit to open the door, enter the DTMF password to open the door.

Upon submission and save, the added password information will be displayed in the list. The following image illustrates the page before and after successful addition.





7.3 Face Recognition

When someone approaches the device and the face is facing the screen, the device will perform face recognition;

If the detected image has been saved in the image database, the door will be opened after recognition and the recognition will be successful;

If the detected portrait is not saved in the portrait library, the person is recognized as a stranger, and the door will not be opened and the recognition will be prompted to fail.

Adding Personnel Information：

1，Enter the web **[Facial Management] >> [Facial Management]**, click Add Upload photo

2，Upload photos

Click Add, click Upload on the Add Person page, and select a local face photo to upload; the image supports jpg format, and the image size cannot exceed 100k

Click the photo, WEB prompt "Photoing，Do not perform other operations.", LCD screen will prompt "Take the photo in five seconds.", after the completion of the photo, the portrait will be displayed in the picture area

3，Add the basic information of the person, name, relay (relay, default support 1), mode.

Mode: Disabled, disabled after the face recognition is not successful;

Enabled, face recognition takes effect after enabling;

Time period, face recognition takes effect in the set time period.

4，Submit to save, the added portrait information will be displayed in the list.

7.4 Period Management

Period Management is utilized to define specific time frames, allowing individuals to use corresponding authentication methods to open the door during the set time period.

1. Go to the web page: **[Security Settings] >> [Period]**
2. Add Schedule

Name: Set the name of the time period, e.g., 'Workdays,' 'Weekends,' etc.

Repetition Period:

No repetition: Period operates only on selected dates.

Daily: Repeats every day.

Weekly: Repeats weekly, with the option to select Monday through Sunday.

Monthly: Repeats monthly, allowing selection of specific dates (e.g., 1st, 15th, 30th).

Start Time: Defaulted to the current system time, users can choose the start date and

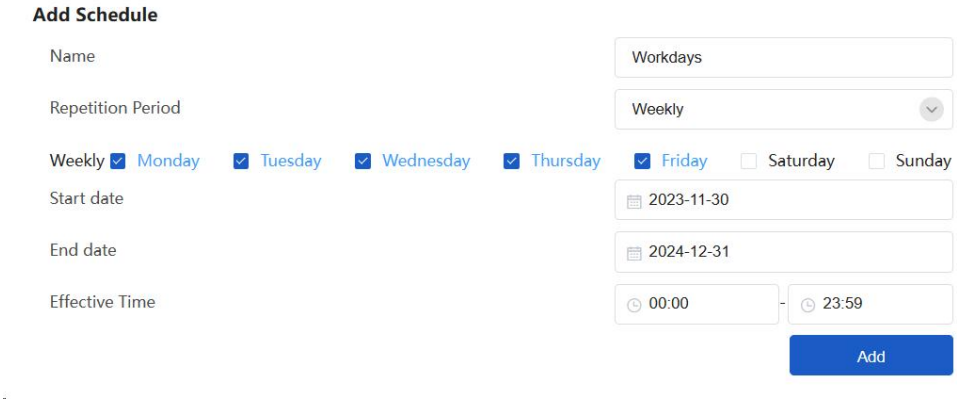
time for the period (e.g., November 30, 2023).

End Time: Users can select the end date and time for the period. The end time must be later than the start time (e.g., December 30, 2023).

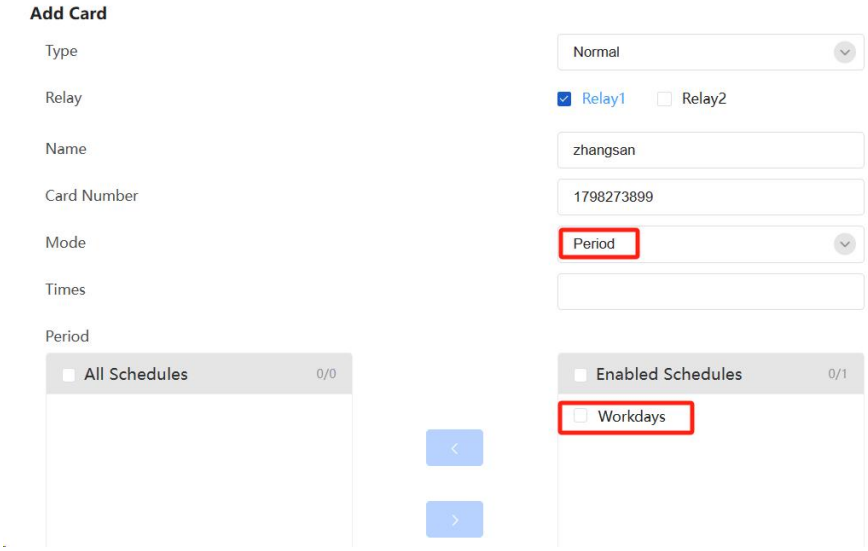
Effective Time: Time frame within each day when the period is effective, ranging from 00:00 to 23:59.

Usage Example:

1. Create a Period named 'Workdays,' set to repeat weekly from Monday to Friday, with an effective time span of 00:00 to 23:59 for those days. As shown in the picture.



2. When adding cards, passwords, or portrait, select the Enabled Schedules.



7.5 Relay Settings

7.5.1 Relay Settings

Go to the web page: **[Security Settings] >> [DoorPhone Settings],** select the operating mode of the Relay.

Parameters	Value	Description
Relay1 Switch Mode	Monostable State , Bistability	Monostable State: Defaulting to Monostable state, where the default is to keep the door closed. When a user opens the door, the lock opens and remains open for a set duration. After the timeout, it returns to the closed state. Bistability: The Bistability option allows for long-term maintenance of either the open or closed door states. When a user swipes a card to control access, the door switches from an open state to a closed state and remains closed until the next user access control command.
Relay1 Switch On Duration	Default 5 seconds, range from 1 to 600 seconds	Effective in monostable state. Default door opening duration
Relay2 Switch Mode	Monostable State , Bistability	Same as relay 1
Relay2 Switch On Duration	Default 5 seconds, range from 1 to 600 seconds	Same as relay 1
Relay2 Follow Mode	Independent opening, synchronous,asynchronous	Independent opening: Relay 2 is independently controlled and not synchronized with Relay 1. synchronous:Relay 2 synchronizes with Relay 1, opening simultaneously when Relay 1 opens.

		Synchronous:Relay 2 opens after a delay following the opening of Relay 1.
Async Timeout	The default is 1, measured in seconds.	Effective when Relay 2 opens asynchronously.

Card Format and Wiegand Interface parameters:

Parameters	Value	Description
Card Format	8H10D , 8HR10D	Card format displayed after using the built-in card reader. 8H10D: Decimal card number, conventional card display format. 8HR10D: Card number in reverse order.
Wiegand Card Format	8H10D , 8HR10D	After a Wiegand card reader reads a card, the displayed card format. Only valid when the Wiegand out is closed.
Wiegand Mode	In, out	out: Wiegand interface operates in Wiegand output mode, used when connecting to access controller. In: Wiegand interface operates in Wiegand input mode, used when connecting to Wiegand card readers.
Wiegand Type	26bit, 34bit	Only effective in Wiegand Out mode.

Opendoor Log Server Parameter：

The device supports synchronizing door access logs to syslog server.

Parameters	Value	Description
Relay Log Export Enable	Checked or not	When checked, report Opendoor Log.
Log Server Address	IP address or domain name	Syslog Server address
Opendoor Log Server Port	514	Syslog server port, default is 514. Only supports UDP.
Opendoor Log Format	Default format replaceable	Opendoor Log Format: Relay, Status, Time, Name, Number, Format, MAC Address. Corresponding parameters will be replaced with actual values.

7.5.2 Door Sensor Settings

The door sensor is used to detect the open/close status of access control. If the access control remains open after a timeout, an alert will be triggered. Before configuring, the door sensor needs to be connected to the access control system. Users can check the status of the relay, door sensor, and control the relay via the web page **[Security Settings] >> [Relay].**

Relay Status：

Parameters	Value	Description
Door Sensor 1/2	Check to enable Door Sensor 1/2.	When the door sensor is enabled, if the door remains improperly closed after the timeout following door unlock, signaling a mismatch between the door sensor and lock status, it indicates that the physical door hasn't closed correctly, the device will sound an alarm.
Door Sensor Check Delay 1/2	The default is 5, measured in seconds.	Delay detection time for Door Sensor 1/2 matches the door opening duration. For instance, if the door remains open for 5 seconds, the door sensor delay detection is also configured for 5 seconds. If normal detection isn't confirmed after 5 seconds, and the door sensor and lock status don’t align, an alarm is triggered.
Relay Status 1/2	Open ,Close	Status of Relay 1/2
Door Sensor Status 1/2	Open ,Close	Status of Door Sensor 1/2: Indicates whether the door is properly closed as detected by the door sensor.

Relay Control：

Parameters	Value	Description
Relay	1、2、All	Select the Relay you want to control
Action	Open ,Close	Door Open/Close
Open Mode	Once, Always	Once: perform door opening action, and will be

		closed automatically after 5 seconds. Always: perform the door opening action, the door will not be closed automatically and need to closed manually when timeout.

7.6 Face Settings

7.6.1 Face Settings

Users can set facial recognition parameters by navigating to **[Facial Management] >> [Face Settings]** on the web page.

Parameters：

Parameters	Value	Description
Motion Detection	Highest, Normal, Close	For different scenarios, different biopsy models will be used to cope with "Close", "Normal" and "Highest" biopsy requirements. The highest level of motion detection is enabled by default.
Max Recognition Angle	30	Facial recognition pose angle settings, default is 30 degrees. 0 indicates the closure of pose angle detection; 10-45 degrees indicate recognition within that range.
Maximum Recognition Width	95	Maximum face width level: Used to set the distance for facial recognition. The closer the distance, the larger the face width.
Minimum Recognition Width	5	Minimum face width level: Used to set the distance for facial recognition. The closer the distance, the larger the face width.
Face Tracking	Open,Close	Whether to turn on the face tracking.
Display Results	3	Duration for displaying facial recognition results, default is 3 seconds.
Success Recognition Interval	2s	After successful recognition, the interval time of re-recognition.

Failure Identification Interval	2s	The interval time of re-identification after failed recognition.
Timeout To Turn Off White Light Filling	10s	After the timeout period, the white light fill light will be closed automatically.
Similarity Measure	70.0	The larger the face recognition similarity value is, the lower the recognition rate is; face recognition similarity will only go to the face database for comparison if it is greater than the set similarity degree.
Fill light brightness mode	Standard Performance	Standard mode is suitable for most scenarios. Performance mode has higher brightness and is suitable for darker or brighter environments.

7.6.2 Prompts Settings

Users can customize facial recognition-related prompt messages by accessing **[Facial Management] >> [Prompts Settings]** on the web page.

Parameters：

Parameters	Description
Custom Prompts	
Identify Successful Titles	Default: $name, support custom setting
Recognize Success Status Cues	Default 'Successful'.Support custom setting
Recognize The Success Message	Default 'Welcome'.Support custom setting
Identifying Failed Titles	Default 'Strange'.Support custom setting
Identify The Failure Status Prompt	Default 'Failed'.Support custom setting
Recognize The Failure Message	Default 'Please contact the administrator ！ '.Support custom setting
Successful Opening Status Prompt	Default 'Successful'.Support custom setting
Door Opening Failure Status Prompt	Default 'Failed'.Support custom setting
Failure Prompt For non-time Period	Default 'Not working hours, please contact the administrator!'.Support custom setting

8 Monitoring function

Access control systems can integrate with video surveillance systems such as NVR, VMS, etc. This section describes integration through RTSP and ONVIF protocols.

8.1 RTSP

The device enables the RTSP protocol by default, allowing users to integrate it into NVR, VMS, etc. The RTSP URL format is:
rtsp://username:password@device ip/h264/stream.live0

'stream.live0' represents the main stream, while 'stream.live1' represents the sub-stream
'username' represents the RTSP authentication username, defaulting to 'admin'.
'password' represents the RTSP authentication password, defaulting to 'admin'.

8.2 ONVIF

Users can also integrate with NVR, VMS, etc., using the ONVIF protocol. ONVIF is enabled by default.

9 Contacts

9.1 Contact

9.1.1 Management Contacts

Users can add, edit, and delete contacts through the web interface under **[Contacts] >[Contacts].**
Contacts added via the web will synchronize and appear on both the web and device interfaces for viewing.

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

After adding a contact, users can make calls by selecting the contact from the device's contact interface. For more details, refer to i67 for making calls through contacts.

9.1.2 Importing & Exporting Contacts

When there are too many contacts in the phonebook for manual management, you can use the device's web interface to import and export contacts in bulk.

Importing Contacts:
Users can navigate to the web page **[Contacts] >> [Advanced] >> [Import Contact List]** to import contacts. It supports CSV, VCF, and XML formats. Users can first export a contact template (see exporting contacts operation), edit it, and then import.

Exporting Contacts:

Users can navigate to the web page **[Contacts] >> [Advanced] >> [Export Contact List]** to export contacts. It supports CSV, VCF, and XML formats.

9.2 Restricted Incoming Call List

The device supports a restricted incoming call list, where adding a number to this list results in rejecting incoming calls from that number directly (Numbers listed in the restricted incoming call list can still make outgoing calls normally).
Users can access the web page **[Contacts] >> [Call List] >> [Restricted Incoming Calls]** to set up the restricted incoming call numbers.

9.3 Restricted Outgoing Call List

Supports setting a number that prohibits outgoing calls. If you enter this number on the dialing interface, you will not be allowed to make outgoing calls. The device will sound a tone and pop-up prompt that prohibits outgoing calls.
Users can set restricted outgoing numbers through the web page **[Contacts] >> [Call List] >> [Restricted Outgoing Calls]**.

10 Open The Door Record

10.1 Open The Door Record

The log of door opening events is displayed. Click the Export button to select Save Target As to export the door opening records in CSV format.

Parameters	Description
Relay	Relay ID
Result	Display the result of a single door opening (success or failure)
Name	Display the name of the door opening record
Type	Open the door type, including password, swipe card, etc.
Source	Open the door card number or password, etc. display
Reason	The reason for opening the door failure
Time	Open the door time

10.2 Passerby Record

Passing records are used to display the images and results of people who have been added to the portrait database and captured when face recognition is performed.
Click the Export button and select Save Target As to export the record in tar.gz format.

10.3 Fail Record

Failure record is used for people whose faces are recognized by the device but not recorded in the portrait database. When the device detects it, it will save the failure record with the captured images.
Click the Export button and select Save Target As to export the failure record in tar.gz format.

11 Device Functions

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 **[Intercom 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 restart, timing upgrade, timing sound detection, timing playback audio
Audio Path	Support local Local: select the audio file uploaded locally
Audio Settings	Select the audio file you want to play, it supports trial listening, and you can play it immediately after clicking the trial listening
Play Mode	Circle: Loop playback within the specified time frame. Once: Play once within the specified time frame.
Repetition	Do not repeat: execute once within the set time range Daily: Perform this operation in the same time frame every day Weekly: Do this in the time frame of the day of the week 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 maintenance

11.2.1 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.

- **Reset Phone**

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

11.2.2 Upgrade

Upgrade the software version of the device, and upgrade to the new version through the webpage. After the upgrade, the device will automatically restart and update to the new version.

Go to **[System] >> [Upgrade]**, select the file, choose the System Image File, and click 'Upload'.

11.2.3 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	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.
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.
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 Pay	
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.
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. 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 Mode	Provision Mode. 1. Disabled. 2. Update after reboot. 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 Settings

12.1 Time/Date

Users can set the time and date through the device web page and device menu.

Set time/date on the device interface:
Users can use the device menu **[Display]** >> **[Time/Date]** Set the device time/date.

Web interface setting time/date:
Users can use the web page **[Intercom Settings]** >> **[Time/Date]** Set the device time/date.

Parameters：

Parameters	Description
Time Synchronized via SNTP	Enable time-sync through SNTP protocol
Time Synchronized via DHCP	Enable time-sync through DHCP 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
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.
Fixed Type	Daylight saving time rules are based on specific dates or relative rule dates for conversion. Display in read-only mode in automatic mode.
Offset	The offset minutes when DST started
Month Start	The DST start month
Week Start	The DST start week

Weekday Start	The DST start weekday
Hour Start	The DST start hour
Minute Start	The DST start minute
Month End	The DST end month
Week End	The DST end week
Weekday End	The DST end weekday
Hour End	The DST end hour
Minute End	The DST end minute
Manual Time Settings	You can set your time manually

12.2 Screen Setting

12.2.1 Brightness and backlight

Users can adjust brightness and backlight settings through both the webpage and device menu. The device enters backlight mode after a period of inactivity.

Adjust brightness and backlight settings in the device interface：
Users can adjust device brightness and backlight settings through the device menu: **[Display] >> [Screen].**

Web interface screen settings:
Users can adjust device brightness and backlight settings through the web page: **[Intercom Settings] >> [Screen Settings] >> [Screen Settings].**

Brightness and backlight parameters:
Brightness level during operation: Set the brightness of the screen when the device is in use.
Brightness level during idle state: Set the brightness of the screen when the device is idle.
Backlight idle wait time: Set the timeout duration for entering backlight mode.

12.2.2 Screen Saver

When the device is idle for the preset waiting time, it will automatically display the screensaver. The screensaver can be stopped by pressing any key, touching the screen, or the device detecting someone approaching.

By default, the device will display builtin images during the screensaver. Users can customize the screensaver.

Users can enable the screensaver through both the webpage and device menu. The device enters the screensaver interface after a period of inactivity.

Device interface screensaver settings:
Users can set the device screensaver through the device menu: **[Display] >> [Screen].**

Web interface screen settings:
Users can set the device screensaver through the web page: **[Intercom Settings] >> [Screen Settings] >> [Screen Settings].**

Screensaver parameters:
Screensaver switch: Adjust the volume for incoming call ringtone and door opening prompts.
Timeout to enter screensaver: Set the volume for signals such as incoming and outgoing calls after a timeout.

Custom Screensaver:
- Users can upgrade custom screensaver images through the webpage: **[System] >> [Upgrade] >> [Screensaver].**
- Image format:
- Supports BMP and PNG formats.
- Resolution: i66: 800*480, i67: 600*1024.
- Bit Depth: 24 bits

12.2.3 UI Settings

12.2.3.1 Theme

Setting UI Theme for i67:
- The i67 device supports two themes, and users can set the device theme through the webpage: **[Intercom Settings] >> [Screen Settings] >> [Screen Settings].**
- Office: Office Theme.
- Community: Community Theme.

Setting Standby Mode:
The device supports setting the standby mode through the webpage: **[Intercom Settings] >> [Screen Settings] >> [Screen Settings],** the default standby interface.
- Password: The password interface serves as the default standby interface.
- Dialing: The dialing interface serves as the default standby interface.
- Face Recognition: The face recognition interface serves as the default standby interface.

Note:

The selected default standby interface must be within visible functionalities; otherwise, it cannot be used as a standby interface.

Setting Standby Visible Functions:

The device supports setting the visible functions for standby through the webpage: **[Intercom Settings] >> [Screen Settings] >> [Screen Settings].**

Once set as visible, the selected functions will be displayed during standby; otherwise, they will be hidden and unavailable.

- Dialing: Set the visibility of the dialing function.
- Password: Set the visibility of the password function.
- Face Recognition: Set the visibility of the face recognition function.
- Contacts: Set the visibility of the contacts function.

Display Device IP:

The device supports configuring whether the device IP address is displayed on the face recognition interface through the webpage: **[Intercom Settings] >> [Screen Settings] >> [Screen Settings].**

12.2.3.2 Boot Logo

The startup logo image displayed when the device is powered on can be customized.

Users can upgrade custom startup logo images through the webpage: **[System] >> [Upgrade] >> [Boot Logo].**

Image format:

- Supports BMP format
- Resolution:
  i66: 800*480
  i67: 600*1024
- Bit Depth: 24 bits

Note:

The startup logo image must be created strictly according to the above requirements. Please take note of the following:

- For i66, rotate the image 90 degrees to the right before upgrading through the webpage.
- For i67, rotate the image 180 degrees before upgrading through the webpage.

12.2.3.3 Standby Logo

The i66 device supports customizing the standby logo displayed in the upperleft corner of the standby interface.

Users can upgrade custom standby logo images through the webpage: **[System] >> [Upgrade] >> [Standby Logo].**
Image format:

- Supports BMP and PNG formats
- Resolution: 120*34
- Bit Depth: 32 bits

12.3 LED Settings

12.3.1 Fill Light

Users can set the fill light brightness mode through the webpage: **[Portrait Settings] >> [Face Settings]**. There are two supported modes:

- Standard Mode: It can meet the needs of most scenarios when using face recognition for door access.
- Performance Mode: This mode can be selected when using face recognition for door access in particularly dark or bright environments..

12.3.2 Keyboard Backlight

When the device detects someone approaching, the keyboard backlight automatically lights up.

12.4 Audio Settings

12.4.1 Volume settings

Users can adjust the device volume through both the web and device menu.

The device interface allows users to adjust the volume settings：
Users can set the device volume through the device menu: **[Display] >> [Media].**

Web interface volume settings:

Users can adjust the device volume through the web page: **[Intercom Settings] >> [Media Settings] >> [Media Settings].**

Volume parameters:

- Handsfree Ringtone: Adjusts the volume for incoming call ringtone and door opening prompts.
- Signal Sound Volume: Sets the volume for signals such as incoming and outgoing calls.
- Handsfree Volume: Adjusts the volume during calls when using the handsfree mode.

12.4.2 Tone Settings

Users can set the device door opening and call prompt sounds through the webpage: **[Intercom Settings] >> [Features] >> [Tone Settings]**, with options to choose from: off, default, voice, and custom.

Parameters	Descripe
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. 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. Default: Uses the default ringback tone. 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. Default: Uses the default call waiting tone. 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.

Open success prompting	Closed: No prompt tone after a successful door opening. Default: Uses the default prompt tone. Voice: Default builtin voice prompt, typically saying "Door open success." Supports custom door open success prompt tones, which can be set by upgrading ringtone files under **[System] >> [Upgrade] >> [Ring Upgrade]**, and then selecting the custom option for the door open success tone.
Open failed prompting	Closed: No prompt tone after a failed door opening. Default: Uses the default prompt tone. Voice: Default builtin voice prompt, typically saying "Door open failure." Supports custom door open failure prompt tones, which can be set by upgrading ringtone files under **[System] >> [Upgrade] >> [Ring Upgrade]**, and then selecting the custom option for the door open failure tone.
Close Door prompting	Closed: No prompt tone after closing the door. Default: Uses the default prompt tone. Voice: Default builtin voice prompt, typically saying "Door closed." Supports custom closing door prompt tones, which can be set by upgrading ringtone files under **[System] >> [Upgrade] >> [Ring Upgrade]**, and then selecting the custom option for the closing door tone.
Issuing Success Prompting	Closed: No prompt tone after a successful card addition. Default: Uses the default prompt tone. Voice: Default builtin voice prompt, typically saying "Card added successfully." Supports custom card addition success prompt tones, which can be set by upgrading ringtone files under **[System] >> [Upgrade] >> [Ringtone Upgrade],** and then selecting the custom option for the card addition success tone.
Issuing Failed Prompting	Closed: No prompt tone after a failed card addition. Default: Uses the default prompt tone. Voice: Default builtin voice prompt, typically saying "Card addition failed." Supports custom card addition failure prompt tones, which can be set by upgrading ringtone files under **[System] >> [Upgrade] >> [Ring Upgrade]**, and then selecting the custom option for the card addition failure tone.

Revoke Prompting	Closed: No prompt tone after a successful card deletion. Default: Uses the default prompt tone. Voice: Default builtin voice prompt, typically saying "Card deleted successfully." Supports custom card deletion success prompt tones, which can be set by upgrading ringtone files under **[System] >> [Upgrade] >> [Ring Upgrade]**, and then selecting the custom option for the card deletion success tone.
Revoke Failed Prompting	Closed: No prompt tone after a failed card deletion. Default: Uses the default prompt tone. Voice: Default builtin voice prompt, typically saying "Card deletion failed." Supports custom card deletion failure prompt tones, which can be set by upgrading ringtone files under **[System] >> [Upgrade] >> [Ring Upgrade]**, and then selecting the custom option for the card deletion failure tone.
Door Sensor Prompting	Closed: No prompt tone after an abnormal door magnetic detection. Default: Uses the default prompt tone. Voice: Default builtin voice prompt, typically saying "Please close the door." Supports custom door magnetic detection prompt tones, which can be set by upgrading ringtone files under **[System] >> [Upgrade] >> [Ring Upgrade]**, and then selecting the custom option for the door magnetic detection tone.
Ban Outgoing Prompting Mode	Closed: No prompt tone after the prohibition of outgoing calls. Default: Uses the default prompt tone. Custom: Supports custom prompt tones. After upgrading ringtone files under **[System] >> [Upgrade] >> [Ring Upgrade],** the custom option for the prohibition of outgoing call prompt tone becomes available for selection.

12.4.3 Upload Ring

Users can upgrade ringtone files through the webpage: **[System] >> [Upgrade] >> [Ringtone Upgrade].**

Ringtone file format:

- Supports WAV and MP3.
- Maximum size for a single file ： 6 MB

13 Network Settings

13.1 Ethernet Connection

Users can configure the Ethernet network settings through the device webpage and device menu. The device defaults to using IPv4 mode, and users can refer to the network mode to modify the network settings.

Setting up Ethernet Network via Web Interface:
Users can access the webpage **[Network] >> [Basic] >> [Network Setting]** to configure the network type. It supports setting up a static IP and DHCP.

Setting up Ethernet Network via Device Menu:
Users can configure the network type through the device menu **[Network],** supporting both static IP and DHCP settings.

- **Setting Static IP:**

When the network is set to a static IP, you manually configure the device's IP address.

- IP Address: Enter the desired IP address.
- Subnet Mask: Enter the subnet mask.
- Gateway: For network interconnection, fill in according to your requirements.
- Primary DNS: IP address of the main DNS server. The default is 8.8.8.8, provided by Google for free.
- Secondary DNS: IP address of the backup DNS server.

13.2 Network Mode

The device supports three network modes: IPv4, IPv6, and IPv4&IPv6. Users can configure the Ethernet network mode through both the device webpage and device menu. Each network mode allows for the configuration of network type, using either static IP or DHCP.

Setting up Ethernet Network Mode via Web Interface:
Users can access the webpage **[Network] >> [Basic] >> [Network Mode]** to configure the network mode. It supports setting IPv4, IPv6, or IPv4&IPv6.

Setting up Ethernet Network Mode via Device Menu:
Users can configure the network mode through the device menu **[Network] >> [Ethernet]**, supporting IPv4, IPv6, or IPv4&IPv6 settings.

13.3 Network Server

Users can configure the network service type through the webpage: **[Network] >> [Server Port].**

Parameters	Description
Web server type	Restart after setting takes effect. Optional web login as HTTP/HTTPS
Web login timeout	The default is 15 minutes, the timeout will automatically log out of the login page, and you need to log in again
Web auto login	No need to enter the user name and password after the timeout, it will automatically log in to the web page.
HTTP port	The default is 80, if you want system security, you can set other port Such as: 8080, web page login: HTTP://ip:8080
HTTPS port	The default is 443, same as HTTP port usage
RTP port range start	The value range is 102565535. The value of rtp port starts from the initial value set. Each time a call is made, the value of the voice and video ports is increased by 2
RTP port quantity	Number of calls

14 Security Settings

14.1 Short Circuit Input

Short Circuit Input Detection Interface: Used to connect switches, infrared detectors, door magnets, vibration sensors, and other input devices.
After a short circuit input is triggered, it can send a short message to a specified server address, or make a call to a designated number, and play a local alarm sound. This facilitates quick response by management personnel.

Users can modify the configuration parameters related to the input interface through the webpage: **[Security Settings] >> [Security Settings].**

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: ✓ parameters can be replaced with actual values. The supported parameters include: ✓ model, replace with the actual model name ✓ active_user, replace with the actual SIP username ✓ mac, replace with the MAC address of the device ✓ ip, replace with the IP address of the device ✓ trigger, replace with the triggered interface, such as input1, input2, etc. ✓ TriggerName, 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."

14.2 Relay Output

Relay Output Control Interface: Used to control electric locks, alarms, etc.

The relay output can be triggered through short messages, active URIs, call states, etc., and will reset within the set timeout period after being triggered.
Users can modify the configuration parameters related to the output interface through the webpage: **[Security Settings] >> [Security Settings]**.

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
Triggered by URI Ringtone	Triggered by URI Ringtone
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. 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.

Input Trigger	On receiving the command ALERT = [command] from a remote device or server, if correct, it triggers/resets the corresponding output port. Choose whether the relay output port can be triggered by an input port. When the input port is configured as an indoor switch, and the corresponding input port is enabled here, the door can be triggered by the input port
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: 1. Ringing 2. Talking 3. Talking (Calling) 4. Talking (Called) 5. Talking (Intercom) 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.

14.3 Tamper

After enabling the tamper alarm function, when the device is violently disassembled or moved, the device will play an alarm sound and send an alert message to the specified location.

Users can modify the tamper related configuration parameters through the webpage: **[Security Settings] >> [Security Settings] >> [Tamper Alarm Settings].**

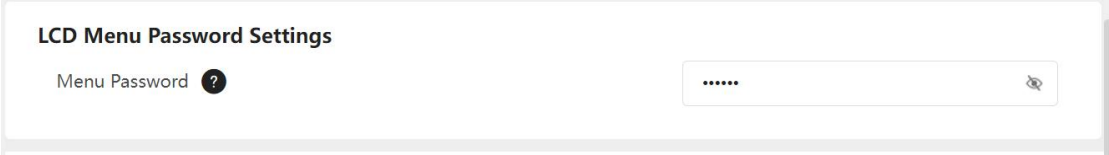
Parameters	Description
Motion Enble Tamper Alarm	Enable or disable tamper detection.
Alarm Command	If the device is tampered with, the device will continuously play the set alarm sound and send an alarm command to the server (server address same as the input port & tamper alarm server address under short circuit input settings).
Reset Command	When the server sends a reset command to the device, the device will stop playing the alarm sound.
Alarm Ringtone	When an tamper alarm occurs, the alarm sound played can be customized by the user.

Tamper Alarm Reset	
Reset Alarm Status	This button resets the tamper function to its default state.

15 Security

15.1 Engineering Password

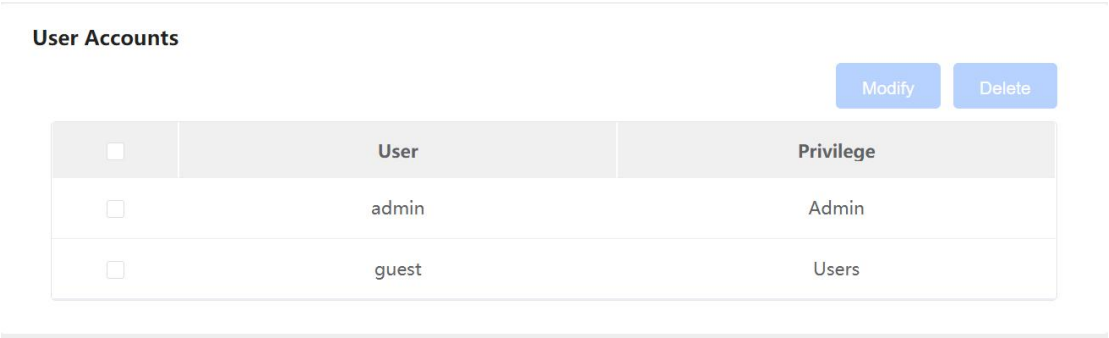
Users can customize the engineering password by entering the webpage: **[Intercom Settings] >> [Screen Settings] >> [Set Menu Password]** interface for configuration."。



After changing the password, the new password must be used to access the device menu.

15.2 Web Password

Changing the password through the user configuration interface:
Users can customize and change the web login password by entering the webpage: **[System] >> Account] >> [User Accounts],** and selecting the account for modification.



Changing the password through the login user interface avatar:
Users can customize and change the web login password. After entering the webpage, click on the 

'Change Password' option under the user avatar in the top right corner for modification.

Password Modification Parameter Settings:

- Current Password: Enter the current web login password.
- New Password: Enter the desired new login password.
- Confirm Password: Reenter the new login password for confirmation.

- After changing the password, the system will automatically log out, and you need to

enter the new password to log in again.

15.3 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 Trouble Shooting

When the device is not functioning properly, users can try the following methods to restore normal operation or collect relevant information to send a problem report to the technical support email.

16.1 Get device system information

Users can obtain information through the device webpage **[System] >> [Information] or the device [Menu] >> [System Information]** options. The following information will be provided:
Device information (model, software and hardware version), account information and Internet Information etc.

16.2 Reboot Device

Users can restart the device through the webpage or the device menu.

Restarting the device from the device interface:
Click on **[Menu] >> [Restart]** and press **[OK]**.

Restarting the device from the webpage:
Click on **[System] >> [Utilities]** >> **[Restart Device]** and press **[OK].**

Power Cycle Restart:
Simply unplug the power and restart the device.

16.3 Device Factory Reset

Users can restore the device to its default settings through the webpage or the device menu.

Reset the device from the device interface:
Click on **[Menu] >> [Restore Factory Settings]** and press **[OK]**.

Reset the device from the webpage:
Click on **[System] >> [System Configuration]** >> **[Restore Factory Settings]** >> **[Reset]** button, and press **[OK].**

16.4 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 Image] (capture the problematic screen)**, save the image, and send it to technical support for issue resolution.

16.5 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**], and click the [**Start**] option in the "Network Packets 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.

16.6 Get device log

Log information is helpful when encountering abnormal problems. In order to obtain the log information of the device, the user can log on to the device web page, open the web page **[Device Log],** click the "start" button, follow the steps of the problem until the problem appears, and then click the "end" button, "save" to the local for analysis or send the log to the technician to locate the problem.

16.7 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. 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. 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. 3. 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.。
The device's facial recognition is not successful	1. Check if the person is list in the facial recognition database. 2. Ensure that the facial photos entered are clear and free from any obstructions.

17 Appendix

17.1 Appendix I Function Icon

 Dail	i67: Click on this icon to enter the dialing interface, then proceed with the corresponding dialing operations using the screen or keyboard. i66: Press this key to enter the contact list.
 PIN	Click on this icon to enter the password interface, then use the screen or keyboard to input the access code for door entry.
 Facial	Clicking on this icon will take you to the face recognition interface. Face recognition allows for door unlocking when the face is aligned with the screen.
 Contacts	i67: Clicking on this icon will take you to the contact list interface, where you can select a contact for calling. i66: Pressing this button initiates a call to the security guard.
 Dail	Dial: In standby mode, enter the number to initiate a call.
 Shortcut List	Click this icon to enter the Speed Dial List interface.
 Call	After entering the number on the dial pad, click this icon to dial the entered number.
 Hang Up	During a call, click the icon to hang up the call.
 Open Door	After entering the door open password, click this icon to open the door.

17.2 Appendix II Menu Icon

 System	View system information.

 Network	Configure device network.
 Language	Set device language.
 Display	Set screen saver, volume, time/date.
 Account	Register a SIP account.
 Factory Reset	Perform a factory reset operation on the device.
 Reboot	Perform a restart operation on the device.

17.3 Appendix III – Keyboard character query table

 Delete	Delete entered characters, letters, or numbers.
 Keyboard	Collapse the keyboard.
 Switch	Switch to the next input field.
 Character	Switch to special character input mode.
 Alphabet	Switch to alphabet input mode.
 Number	Switch to number input mode.
	Switch to capital letter input mode.

Capital Alphabet	