



Video Intercom D Series Android Door Station

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE

PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction



Warning

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Please use the power adapter, which is provided by normal company. The power consumption cannot be less than the required value.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)



Caution

- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device or the detailed operating temperature), cold, dusty or damp locations.
- The device shall be kept from rain and moisture.
- The device shall be kept from explosives.
- Keep surfaces of the device clean and dry.
- Avoid contact with exposed circuits. Do not touch the exposed contacts and components when the product is powered on.



Caution

- Keep the device away from children and out of reach.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Used batteries may result in pollution to the environment. Dispose of used batteries according to the instructions provided by the battery manufacturer.

Regulatory Information

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU, the RoHS Directive 2011/65/EU



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info



Regulation (EU) 2023/1542 (Battery Regulation): This product contains a battery and it is in conformity with the Regulation (EU) 2023/1542. The battery cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), or lead (Pb). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.



Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce

potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

If a power adapter is provided in the device package, use the provided adapter only. If no power adapter is provided, ensure the power adapter or other power supply complies with Limited Power Source. Refer to the product label for the power supply output parameters.

Contents

Chapter 1 About this Manual	1
Chapter 2 Appearance	2
2.1 Door Station	2
2.2 Accessories	4
Chapter 3 Terminal and Wiring Description	10
Chapter 4 Installation	12
4.1 Install Door Station with 8-inch Screen	12
4.1.1 Surface Mounting with Gang Box	12
4.1.2 Surface Mounting with Mounting Plate	13
4.1.3 Flush Mounting	13
4.2 Install Door Station with 10.1-inch Screen	14
4.2.1 Surface Mounting with Gang Box	14
4.2.2 Surface Mounting with Mounting Plate	15
4.2.3 Flush Mounting	16
Chapter 5 Activation	18
5.1 Activate Device Locally	18
5.2 Activate Device via Web	18
5.3 Activate Device via Client Software	19
5.4 Activate Device via Web	19
Chapter 6 Local Configuration	21
6.1 Quick Configuration	21
6.2 Authentication via Admin	25
6.3 Network Parameters Settings	27
6.3.1 Edit Wired Network Parameters	27
6.3.2 Connect to Wi-Fi	28
6.3.3 Set Bluetooth	31

6.3.4 Cloud Service Settings	31
6.4 User Management	32
6.5 Preference Settings	37
6.6 Smart Settings	43
6.6.1 Enable/Disable Mask Detection via Device	43
6.6.2 Set Face Recognition Distance	45
6.6.3 Set Face 1:N Security Level via Device	47
6.6.4 Enable/Disable ECO Mode via Device	49
6.6.5 Set Face Liveness Level	51
6.6.6 Set Face Recognition Interval	53
6.6.7 Biometrics	55
6.7 System Settings	55
6.7.1 Change Language	55
6.7.2 Adjust Brightness	57
6.7.3 Set Sleep Duration via Device	58
6.7.4 Password Management	58
6.7.5 Set Door Contact via Device	58
6.7.6 Set Privacy Parameters	59
6.7.7 Device No. Settings	61
6.7.8 Sound Settings	63
6.8 Maintenance	65
6.8.1 Device Information	65
6.8.2 Reboot	67
6.8.3 Restore Door Station	67
Chapter 7 Local Operation	70
7.1 Call from the Device	70
7.1.1 Call Resident	70
7.1.2 Call Center	73

7.2 Unlock Door	73
7.2.1 Unlock by Password	73
7.2.2 Unlock by Face	78
7.2.3 Unlock by Presenting Card	78
7.2.4 Unlock by QR Code	78
Chapter 8 Quick Operation via Web Browser	80
8.1 Select Language	80
8.2 Time Settings	80
8.3 Environment Settings	80
8.4 Privacy Settings	81
8.5 Administrator Settings	81
8.6 No. and System Network	82
Chapter 9 Operation via PC Web	84
9.1 Login Web Browser	84
9.2 Forget Password	84
9.3 Overview	84
9.4 Person Management	86
9.5 Device Management	89
9.6 Maintenance and Security	91
9.6.1 Set Protocol Testing	91
9.6.2 Network Diagnosis via PC Web	91
9.6.3 Upgrade and Maintenance	92
9.6.4 Device Debugging	93
9.6.5 View Log via PC Web	95
9.6.6 Security Audit Log	95
9.6.7 Advanced Settings	96
9.6.8 Security Mode Settings	98
9.6.9 Certificate Management	99

9.7 Set Screen Display	100
9.7.1 Notice Publication	101
9.8 Configuration	102
9.8.1 System Settings	102
9.8.2 User Management	105
9.8.3 Network Settings	106
9.8.4 Set Video and Audio Parameters	114
9.8.5 Adjust Display Settings	115
9.8.6 Event Settings	117
9.8.7 Access Control Settings	117
9.8.8 Video Intercom Settings	128

Chapter 1 About this Manual

Get the manual and related software from or the official website (<http://www.hikvision.com>).

Product	
Door Station	

Chapter 2 Appearance

2.1 Door Station



Note

Refers to the specific model for the appearance of the device.

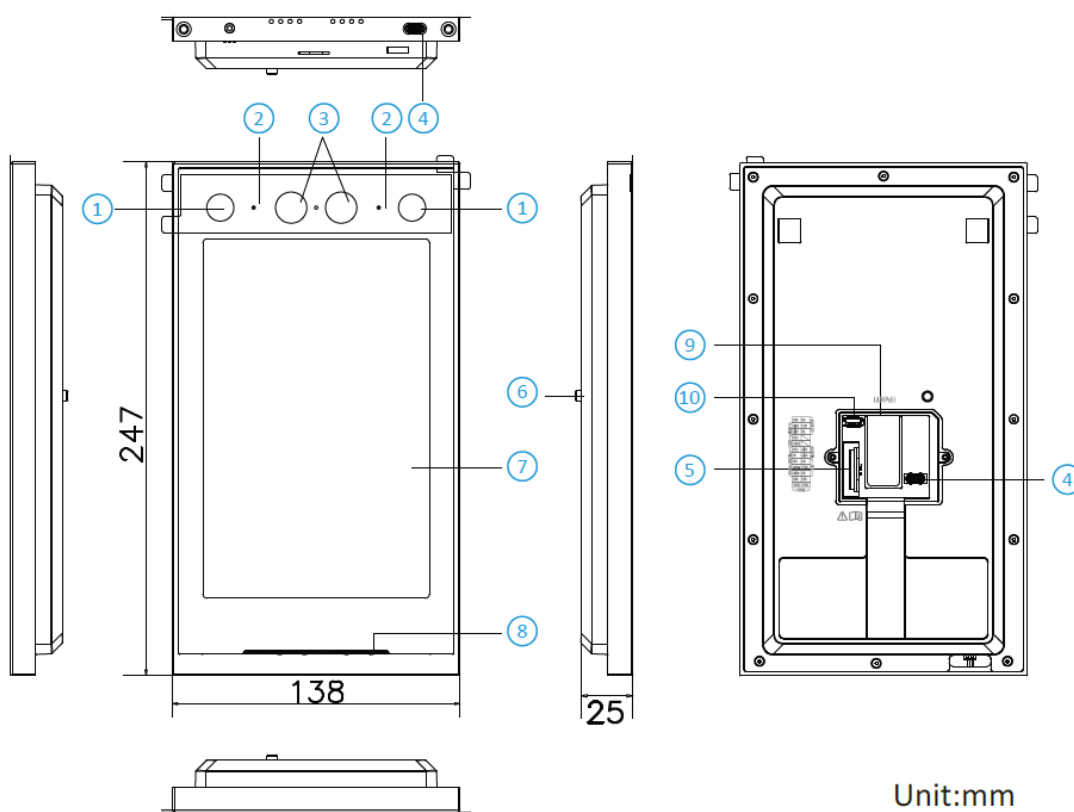


Figure 2-1 Door Station with 8-inch Screen

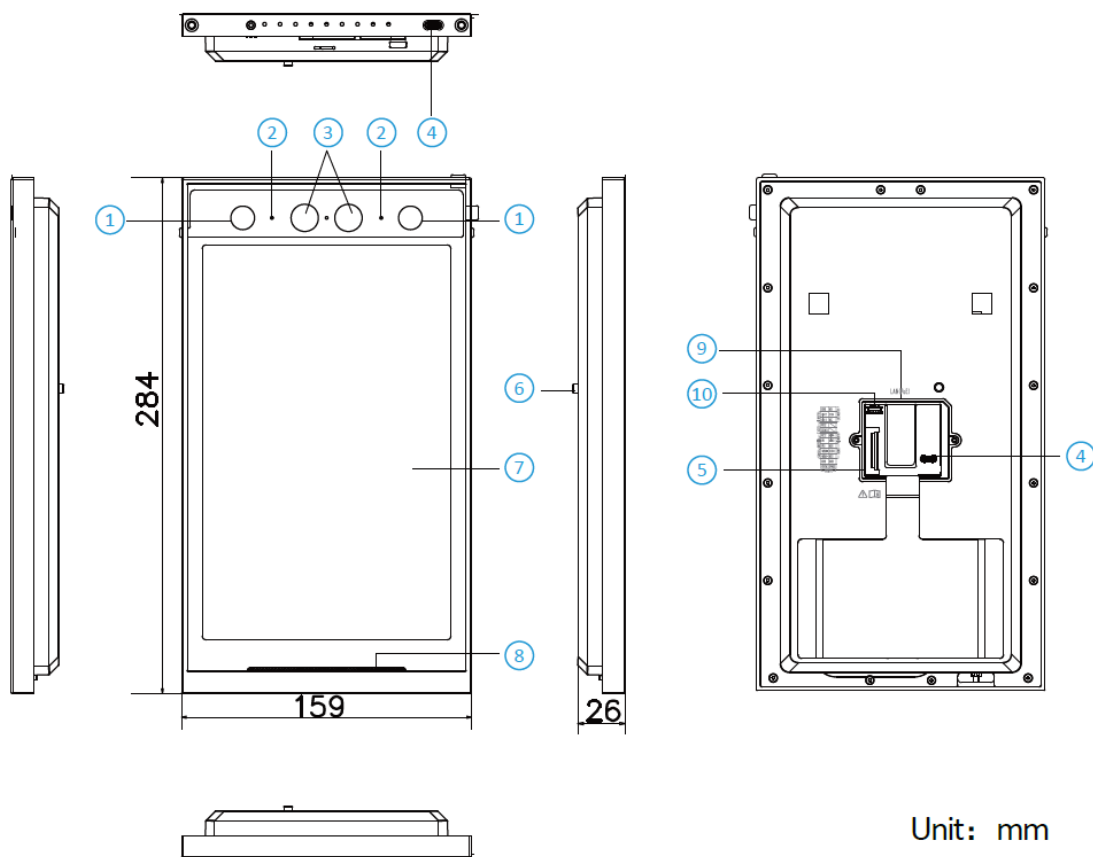


Figure 2-2 Door Station with 10.1-inch Screen

Table 2-1 Description

No.	Name
1	IR Supplement Light
2	Microphone
3	Camera
4	Type-C Interface
5	Wiring Terminal
6	TAMPER
7	Screen
8	Loudspeaker

No.	Name
9	LAN (PoE)
10	Debugging Port

2.2 Accessories



Note

Refers to the specific model for the appearance of the device.

8-inch Door Station Accessories

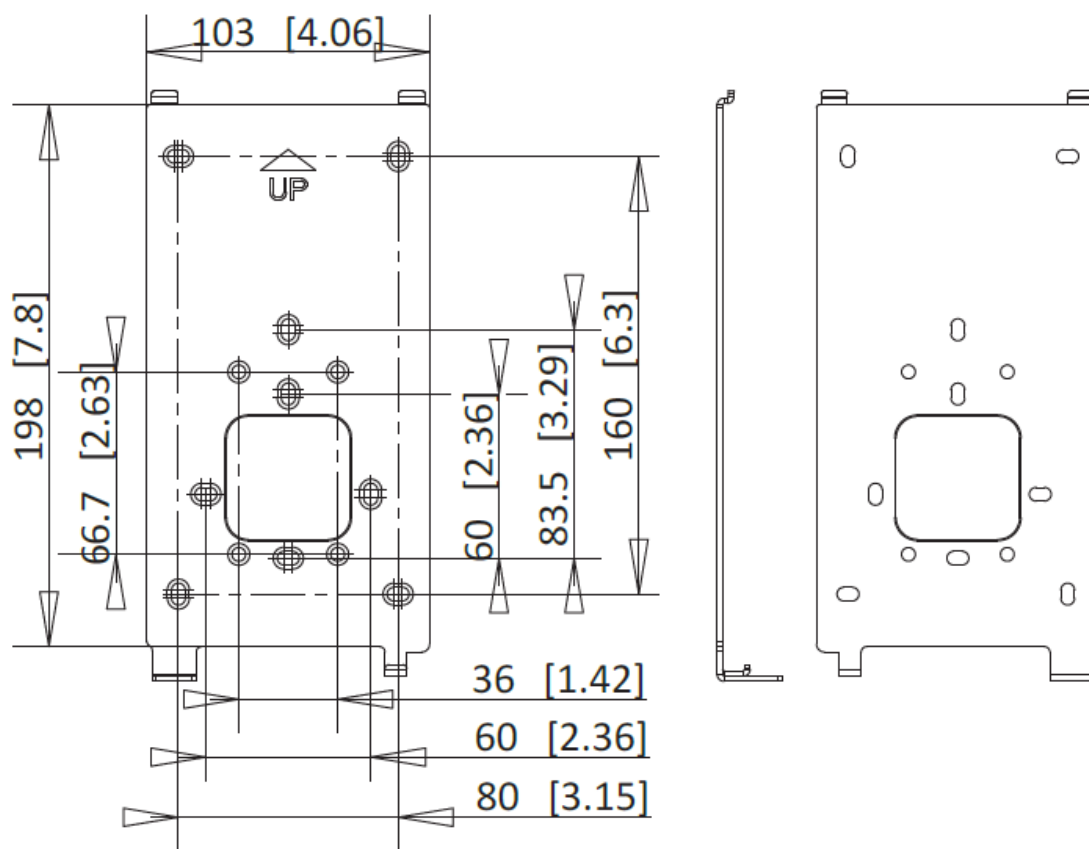


Figure 2-3 Mounting Plate

The dimension of the mounting plate is 215.87 mm (W) × 103 mm (H) × 23.5 mm (D).

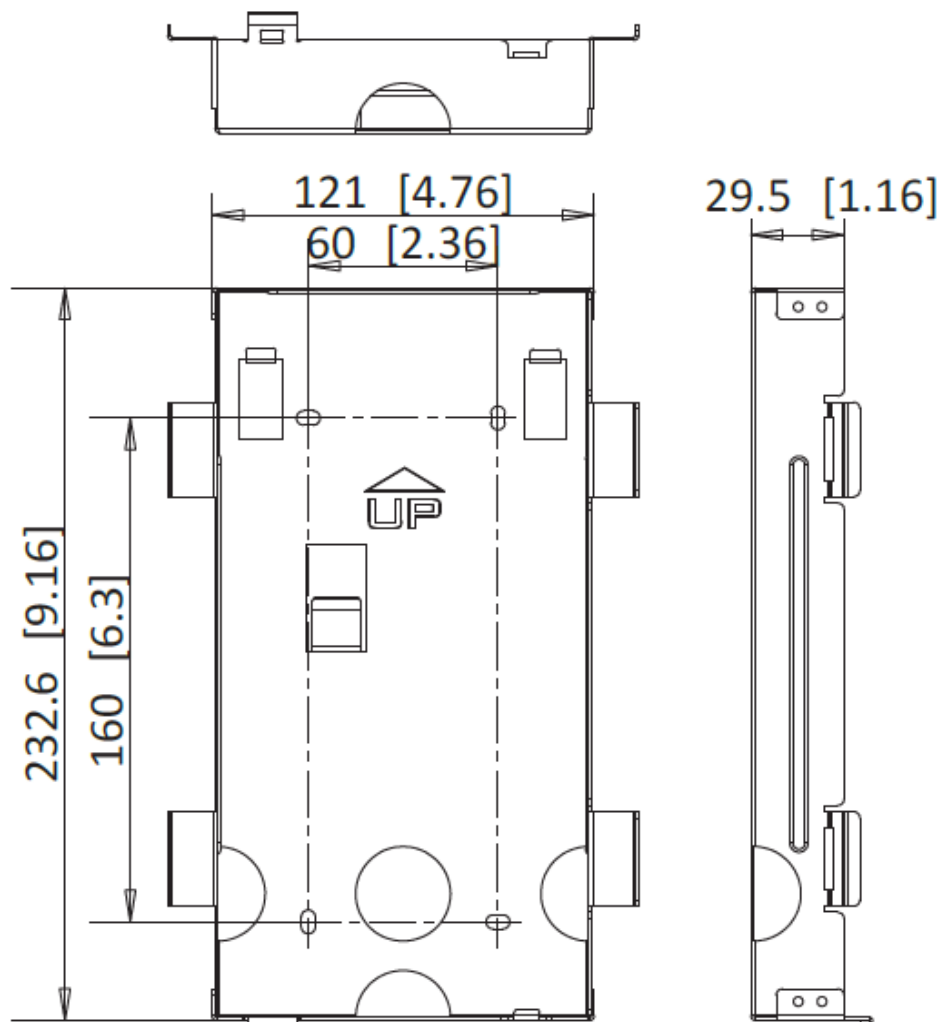


Figure 2-4 Flush Mounting Gang Box

The dimension of the gang box is 232.6 mm (H) × 119 mm (W) × 29.5 mm (D).

The installation hole should be bigger than the actual size. The suggested dimension of the installation hole is 234.6 mm (H) × 123 mm (W) × 29.5 mm (D).

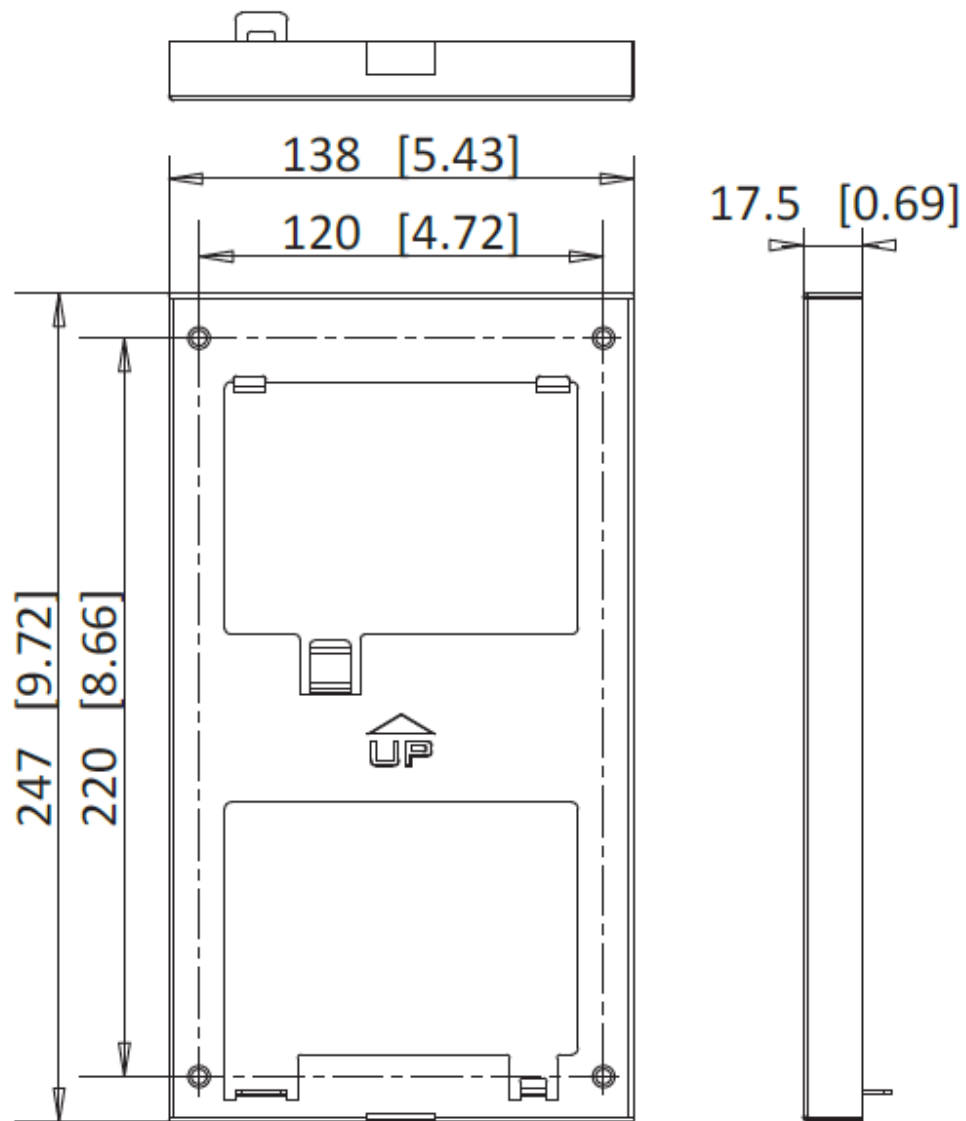


Figure 2-5 Surface Mounting Gang Box

The dimension of the gang box is 247 mm (H) × 138 mm (W) × 17.5 mm (D).
This gang box is not included in the package, you need to buy it seperately.

10.1-inch Door Station Accessories

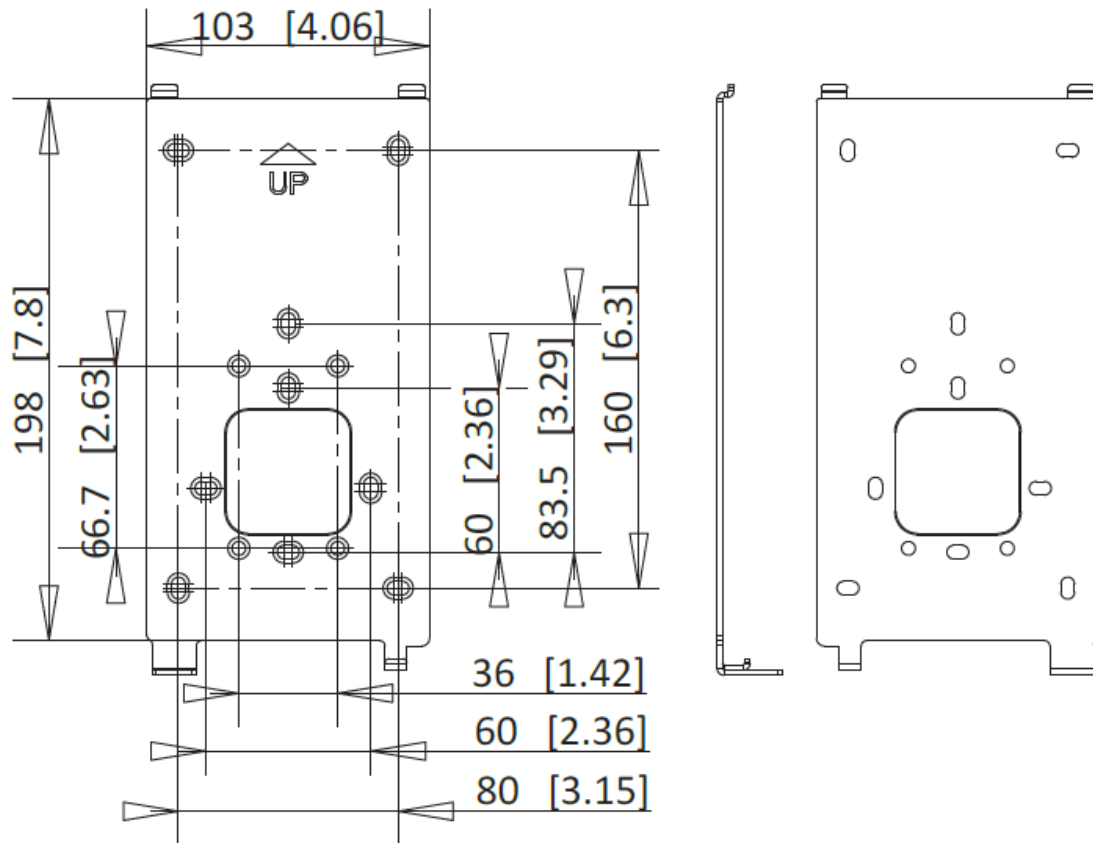


Figure 2-6 Mounting Plate

The dimension of the mounting plate is 215.87 mm (W) × 103 mm (H) × 23.5 mm (D).

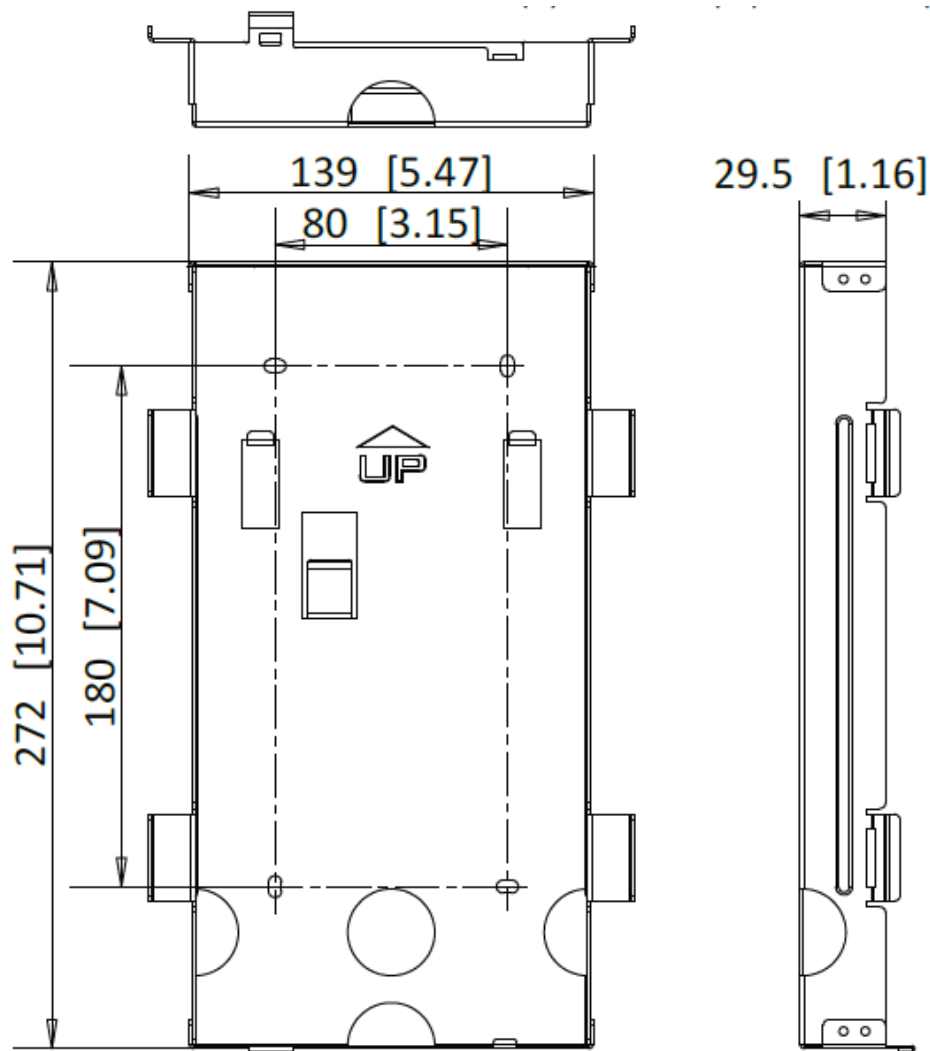


Figure 2-7 Flush Mounting Gang Box

The dimension of the gang box is 272 mm (H) × 139 mm (W) × 29.5 mm (D).

The installation hole should be bigger than the actual size. The suggested dimension of the installation hole is 274 mm (H) × 141 mm (W) × 29.5 mm (D).

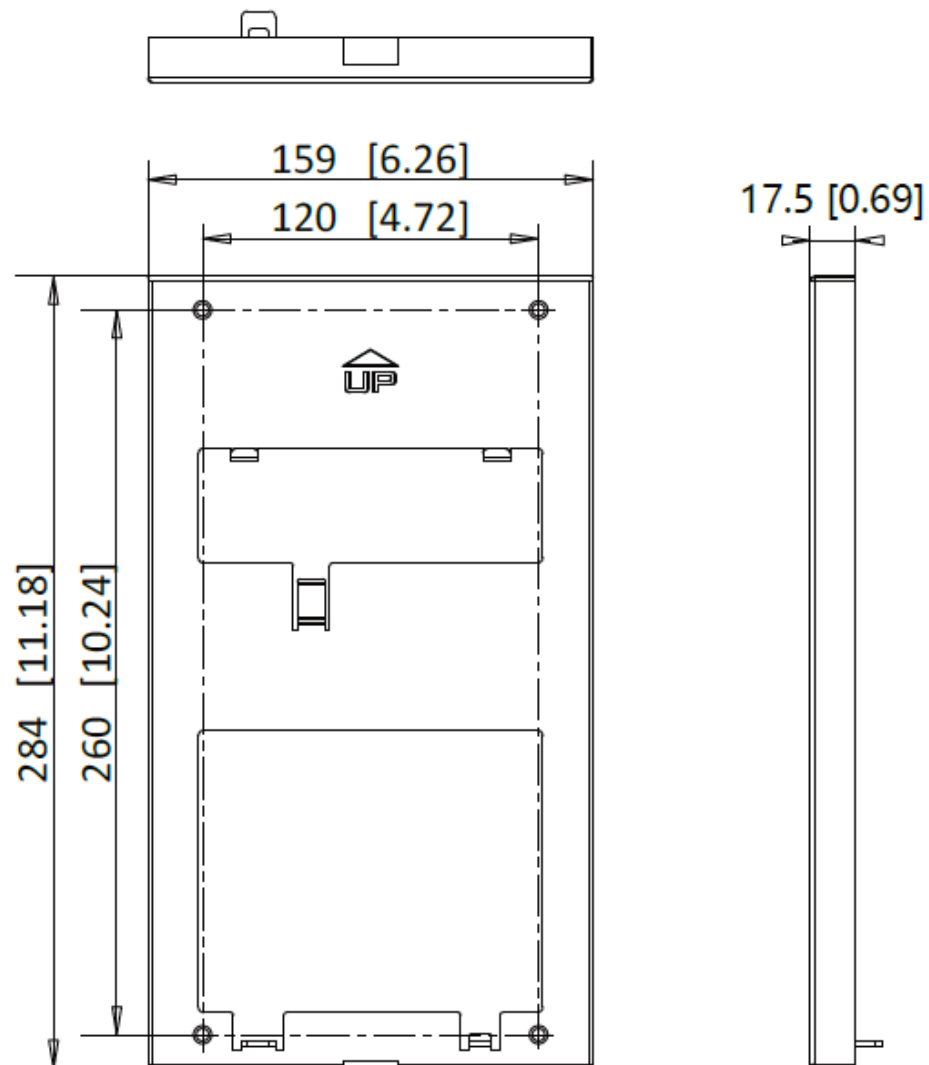


Figure 2-8 Surface Mounting Gang Box

The dimension of the gang box is 284 mm (H) × 159 mm (W) × 16.3 mm (D).
This gang box is not included in the package, you need to buy it seperately.

Chapter 3 Terminal and Wiring Description

Door station can be wired to alarm input interface, door lock, door contact and so on.

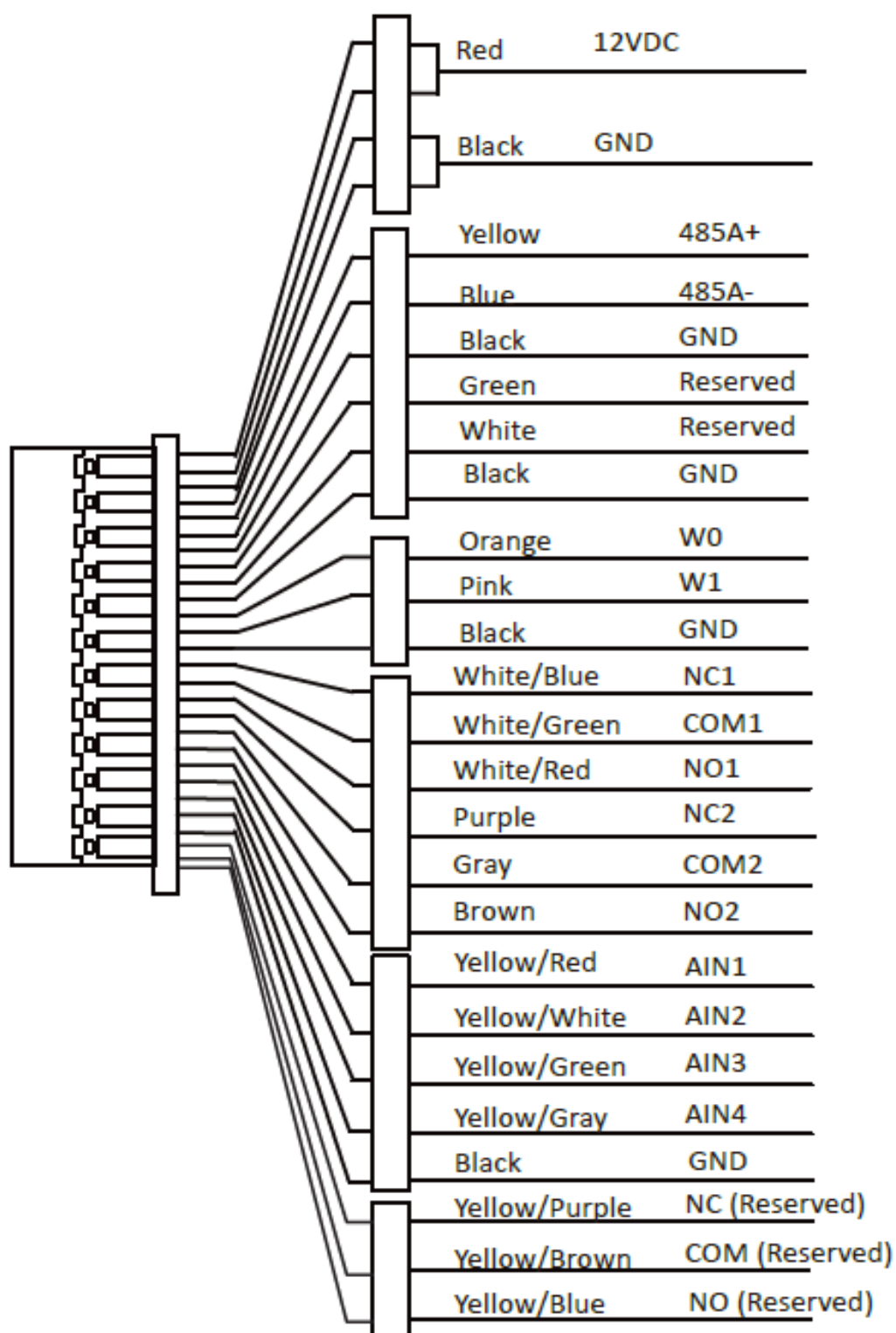


Figure 3-1 Terminal and Wiring Description

Chapter 4 Installation

4.1 Install Door Station with 8-inch Screen

Note

- The power supply the door station supports is 12 VDC. Please make sure your power supply matches your door station.
 - Complete wiring during installation. Refers to *Terminal and Wiring Description* for wiring details.
 - Make sure all the related equipment is power-off during the installation.
 - Installation Location: the lens of the device shall be 1.5 meters away from the ground.
-

4.1.1 Surface Mounting with Gang Box

Before You Start

- Accessories that you need to prepare for installation are in the package.
- Make sure the power supply meets the power requirements of the door station (12 VDC).
- Make sure all the related equipment is power-off during the installation.

Steps

1. Drill holes on the wall. Insert the expansion bolts into the screw holes. Secure the surface mounting gang box to the wall using 4 pcs of KA4×22-SUS screws.

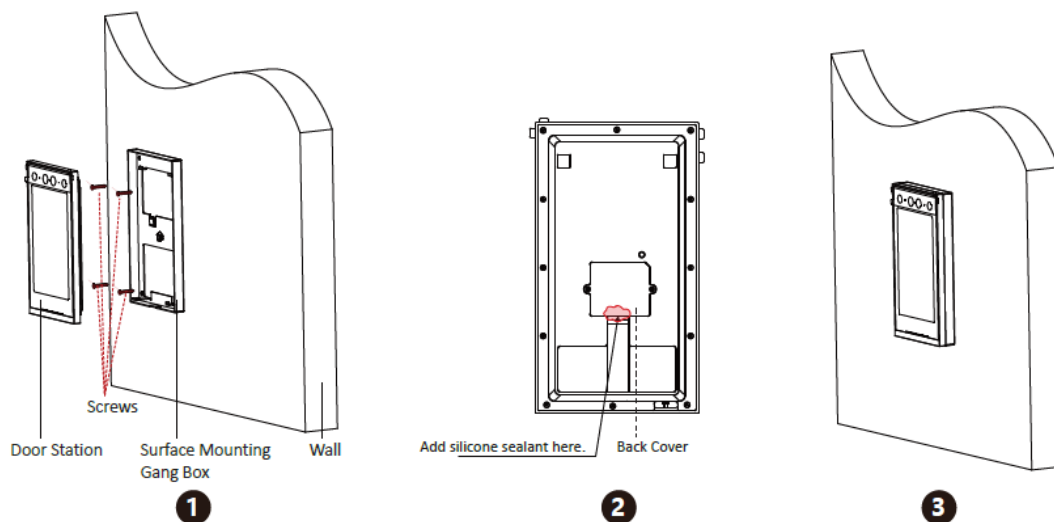


Figure 4-1 Surface Mounting with Gang Box

2. After you finish wiring, cover the back cover of the device, and secure it with 2 screws. Apply silicone sealant at the wiring outlet of the device.

3. Mount the door station on the wall and ensure it is securely installed. Apply waterproof sealant to the top and both sides of the device. The door station installation is now complete.

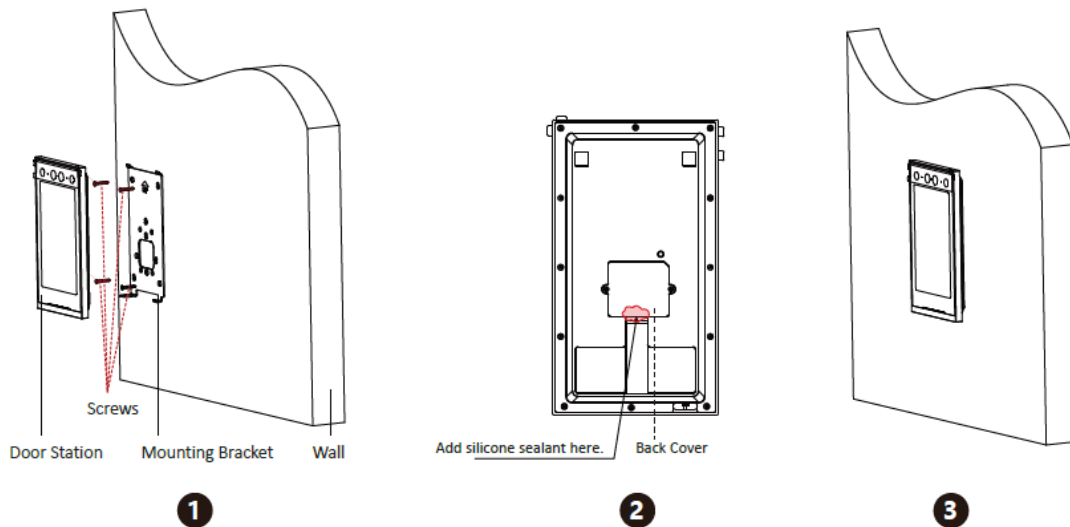
4.1.2 Surface Mounting with Mounting Plate

Before You Start

- Accessories that you need to prepare for installation are in the package.
- Make sure the power supply meets the power requirements of the door station (12 VDC).
- Make sure all the related equipment is power-off during the installation.

Steps

1. Drill holes on the wall. Insert the expansion bolts into the screw holes. Fix the mounting plate to the wall with 4 pcs of KA4×22-SUS screws.



2. After you finish wiring, cover the back cover of the device, and secure it with 2 screws. Apply silicone sealant at the wiring outlet of the device.
3. Mount the door station on the wall and ensure it is securely installed. Apply waterproof sealant to the top and both sides of the device. The door station installation is now complete.

4.1.3 Flush Mounting

Steps

1. Carve an installation hole on the wall. The suggested dimension of the installation hole is 234.6 mm (H) × 123 mm (W) × 29.5 mm (D). Pull the cable out from the wall. The suggested length of the cables left outside is 250 mm.

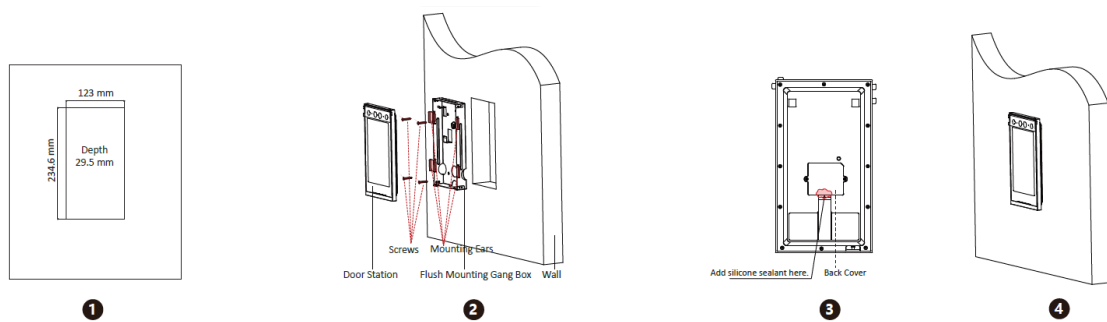


Figure 4-3 Flush Mounting

2. Install the gang box and door station to the wall.
 - 1) Insert the gang box into the installation hole. Mark the gang box screw holes' position with a marker, and take out the gang box.
 - 2) Drill 4 screw holes according to the marks on the wall, and insert the expansion sleeves into the screw holes.
 - 3) Fix the gang box with 4 pcs of KA4×22-SUS screws. Fill the gap between the gang box and the wall opening with concrete, and use tools to break off all mounting ears.
3. After you finish wiring, cover the back cover of the device, and secure it with 2 screws. Apply silicone sealant at the wiring outlet of the device.
4. Mount the door station on the wall and ensure it is securely installed. Apply waterproof sealant to the top and both sides of the device. The door station installation is now complete.

4.2 Install Door Station with 10.1-inch Screen

Note

- The power supply the door station supports is 12 VDC. Please make sure your power supply matches your door station.
- Complete wiring during installation. Refers to *Terminal and Wiring Description* for wiring details.
- Make sure all the related equipment is power-off during the installation.
- Installation Location: the lens of the device shall be 1.5 meters away from the ground.

4.2.1 Surface Mounting with Gang Box

Before You Start

- Accessories that you need to prepare for installation are in the package.
- Make sure the power supply meets the power requirements of the door station (12 VDC).
- Make sure all the related equipment is power-off during the installation.

Steps

1. Drill holes on the wall. Insert the expansion bolts into the screw holes. Secure the surface mounting gang box to the wall using 4 pcs of KA4×22-SUS screws.

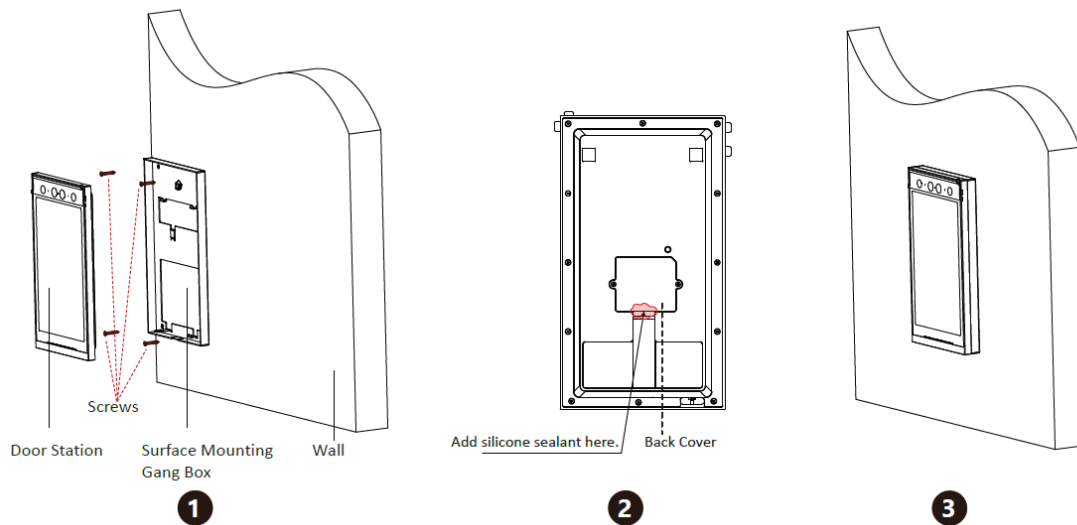


Figure 4-4 Surface Mounting with Gang Box

2. After you finish wiring, cover the back cover of the device, and secure it with 2 screws. Apply silicone sealant at the wiring outlet of the device.
3. Mount the door station on the wall and ensure it is securely installed. Apply waterproof sealant to the top and both sides of the device. The door station installation is now complete.

4.2.2 Surface Mounting with Mounting Plate

Before You Start

- Accessories that you need to prepare for installation are in the package.
- Make sure the power supply meets the power requirements of the door station (12 VDC).
- Make sure all the related equipment is power-off during the installation.

Steps

1. Drill holes on the wall. Insert the expansion bolts into the screw holes. Fix the mounting plate to the wall with 4 pcs of KA4×22-SUS screws.

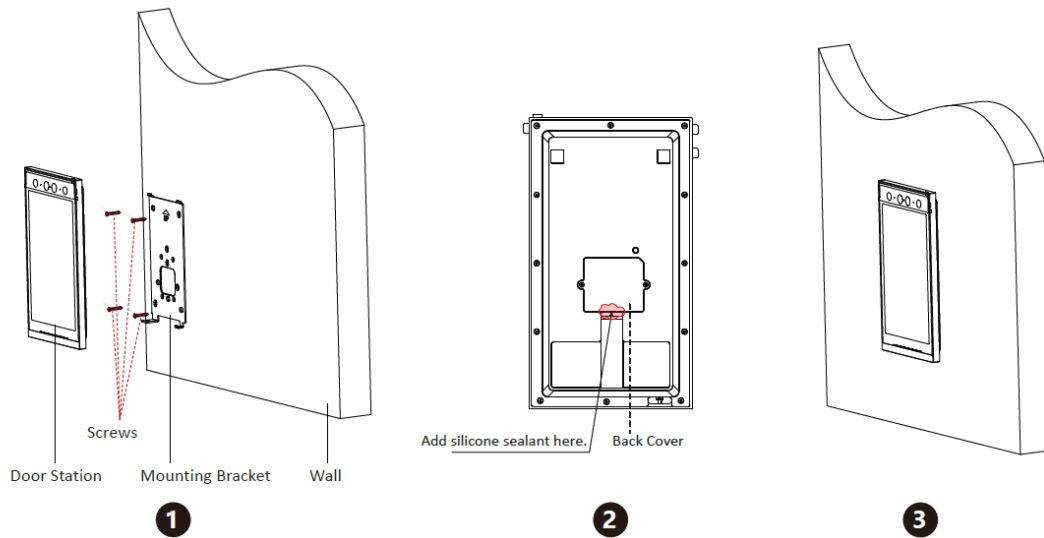


Figure 4-5 Surface Mounting with Mounting Plate

2. After you finish wiring, cover the back cover of the device, and secure it with 2 screws. Apply silicone sealant at the wiring outlet of the device.
3. Mount the door station on the wall and ensure it is securely installed. Apply waterproof sealant to the top and both sides of the device. The door station installation is now complete.

4.2.3 Flush Mounting

Steps

1. Carve an installation hole on the wall. The suggested dimension of the installation hole is 271 mm (H) × 141 mm (W) × 29.5 mm (D). Pull the cable out from the wall. The suggested length of the cables left outside is 250 mm.

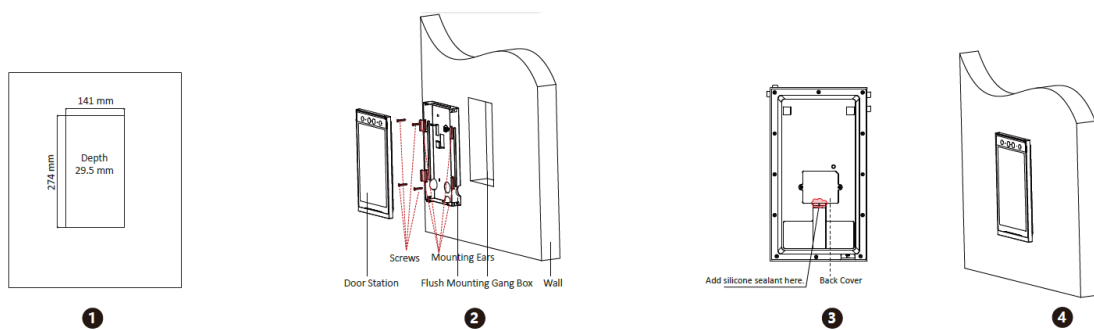


Figure 4-6 Flush Mounting

2. Install the gang box and door station to the wall.
 - 1) Insert the gang box into the installation hole. Mark the gang box screw holes' position with a marker, and take out the gang box.

- 2) Drill 4 screw holes according to the marks on the wall, and insert the expansion sleeves into the screw holes.
- 3) Fix the gang box with 4 pcs of KA4×22-SUS screws. Fill the gap between the gang box and the wall opening with concrete, and use tools to break off all mounting ears.
- 3.** After you finish wiring, cover the back cover of the device, and secure it with 2 screws. Apply silicone sealant at the wiring outlet of the device.
- 4.** Mount the door station on the wall and ensure it is securely installed. Apply waterproof sealant to the top and both sides of the device. The door station installation is now complete.

Chapter 5 Activation

5.1 Activate Device Locally

You are required to activate the device first by settings a strong password for it before you can use the device.

Steps

1. Power on the device to enter the activation page automatically.
2. Create a password and confirm it.



You can tap  to enable or disable password reveal.

3. Tap **Next** to finish activation.



We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

What to do next

After activating the device, the quick configuration page will pop-up automatically. Refers to **Quick Configuration** for details.

5.2 Activate Device via Web

Steps

1. The computer and the device should belong to the same subnet.



Default IP Address: 192.0.0.65.

2. Enter the door station IP address into the address bar of the web browser to enter the activation page.



In order to improve the network security, the set password must be from 8 to 16 digits, and be a combination of at least two or more types of numbers, lowercase letters, uppercase letters, and special characters.

3. If there are multiple door stations in your network, please edit the IP address of the door station to prevent IP address conflicts from causing abnormal access to the door station. After logging in the door station, you can click **Configuration** → **Network** → **TCP/IP** to edit the door station IP address, subnet mask, gateway and other parameters.

5.3 Activate Device via Client Software

You can only configure and operate the door station after creating a password for the device activation.

Default parameters of door station are as follows:

- Default IP Address: 192.0.0.65.
- Default Port No.: 8000.
- Default User Name: admin.

Steps

1. Run the client software, click **Maintenance and Management** → **Device Management** → **Device** to enter the page.
2. Click **Online Device**.
3. Select an inactivated device and click **Activate**.
4. Create a password, and confirm the password.

Note

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

-
5. Click **OK** to activate the device.

Note

- When the device is not activated, the basic operation and remote operation of device cannot be performed.
 - You can hold the **Ctrl** or **Shift** key to select multiple devices in the online devices, and click the **Activate** button to activate devices in batch.
-

5.4 Activate Device via Web

You are required to activate the device first by setting a strong password for it before you can use the device.

Default parameters of the door station are as follows:

- Default IP Address: 192.0.0.65.
- Default Port No.: 8000.
- Default User Name: admin.

Steps

1. Power on the device, and connect the device to the network.
2. Enter the IP address into the address bar of the web browser, and click **Enter** to enter the activation page.



Note

The computer and the device should belong to the same subnet.

3. Create and enter a password into the password field.
4. Confirm the password.
5. Click **OK** to activate the device.

Chapter 6 Local Configuration

6.1 Quick Configuration

After activating the device, the quick configuration page will pop up automatically.

Steps

1. Select the system language and tap **NEXT**.

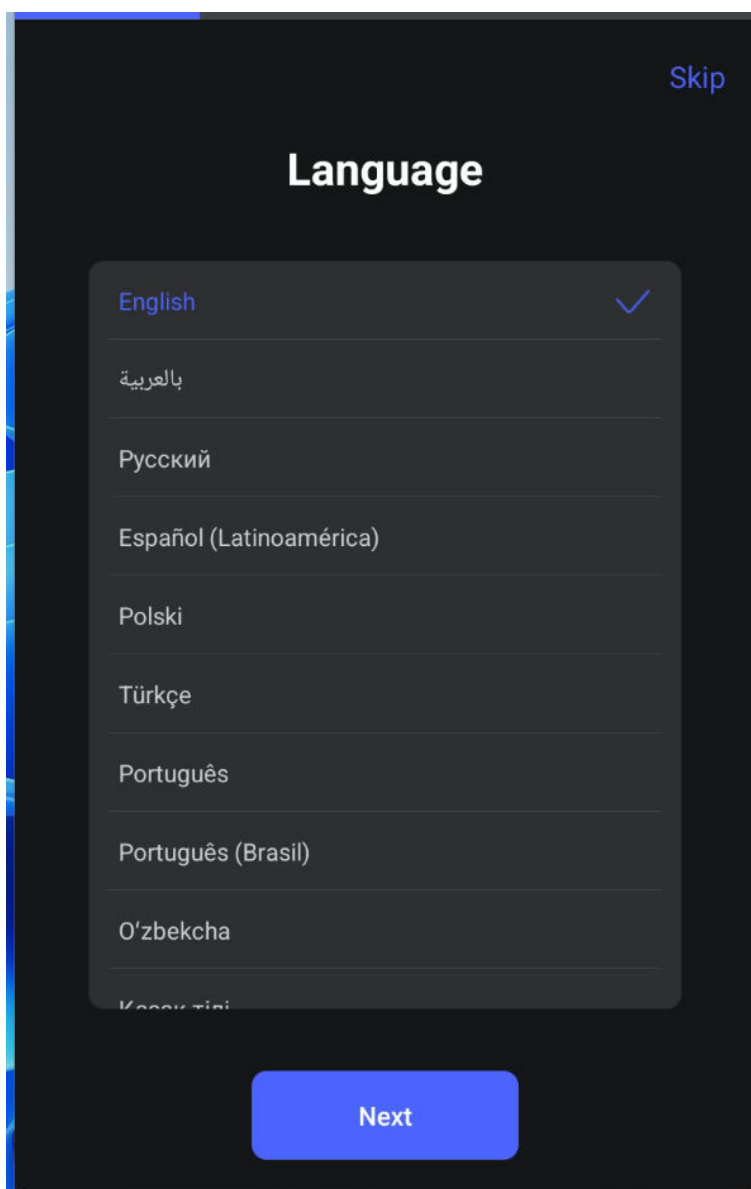


Figure 6-1 Select Language

2. Create a password and confirm the password to activate the device. Tap **NEXT**.

Password activate

New Password 

Enter 8 to 16 characters, Two or more of the following character types are allowed: digit, letter, and symbol, Password cannot include admin and its reverse order

Confirm Password

Previous Next

Figure 6-2 Create and Confirm Password

3. Set password reset method and tap **NEXT**.

- Enter the Reserved Email address, then you can reset the admin password by email.



On the security questions settings page, you can tap **Change to Reserved Email** to modify the password reset method.

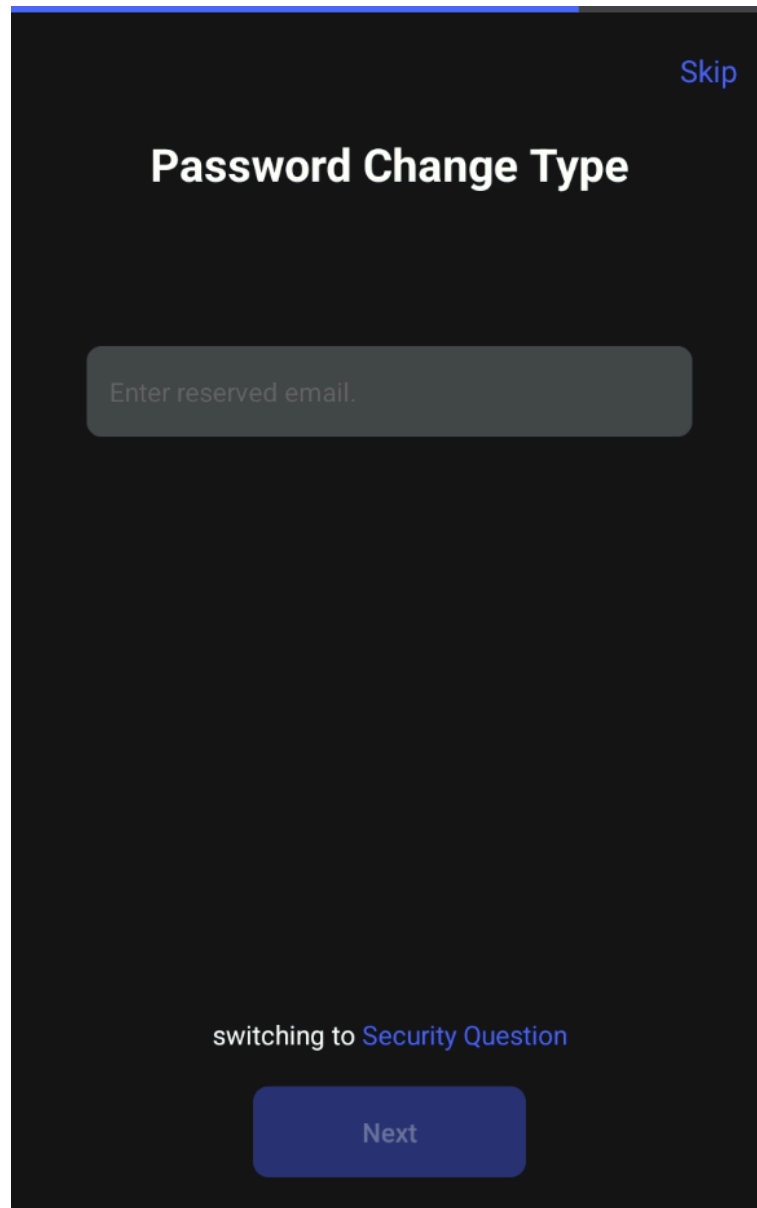


Figure 6-3 Password Reset by Setting Reserved Email Address

- Tap **Change to Security Question**. Select 3 security questions from deficiency list and enter the answers of the questions, then you can reset the password by answering security questions.

The screenshot shows a mobile application interface for changing a password. At the top right, there is a "Skip" link. The main title is "Password Change Type". Below this, there are three identical sections for setting security questions. Each section consists of a button labeled "Question 1: Select Security Question" (with a right arrow), followed by a text input field labeled "Enter the Answer". Below the third question section, there is a status message "switching to Security E-mail address" and a blue "Next" button.

Figure 6-4 Password Reset by Setting Security Questions

4. Set network parameters and tap **FINISH.**

- Set the **IP address**, **Subnet Mask** and **Gateway** manually.
- Enable **DHCP**, the device will get network parameters automatically.

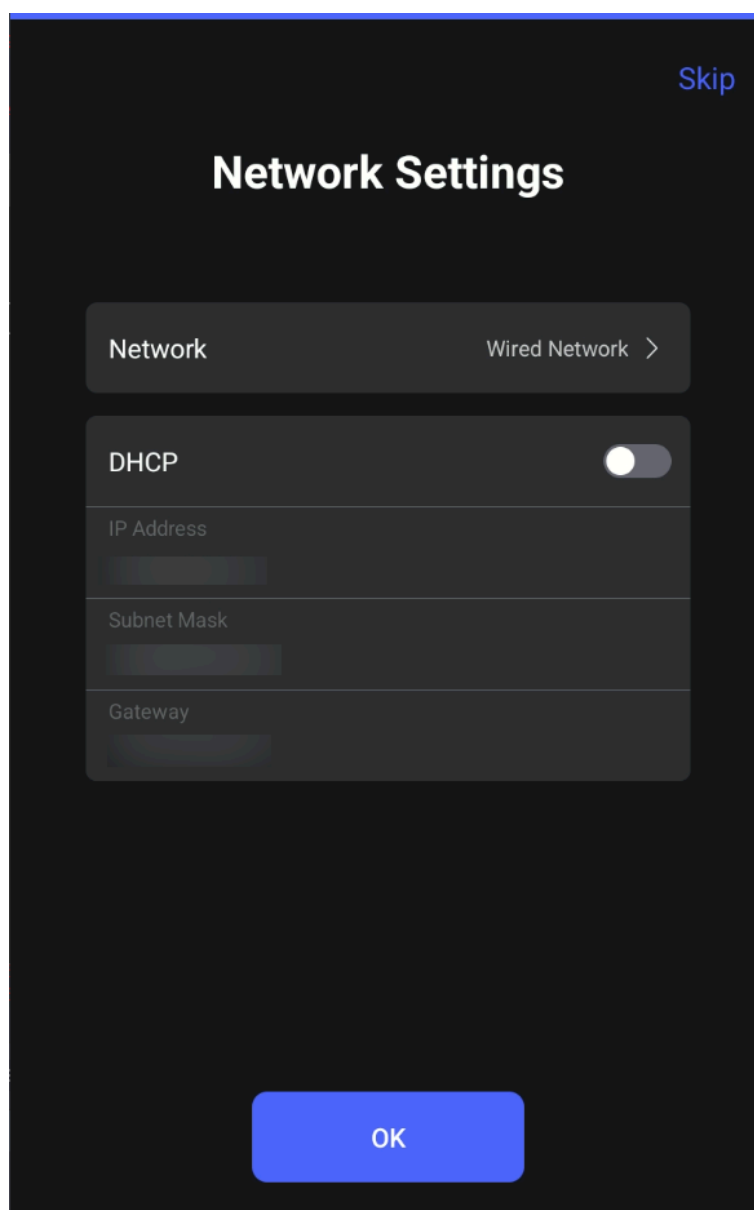


Figure 6-5 Network Parameters Settings

6.2 Authentication via Admin

You can configure the parameters of the device on the menu page. You should authenticate to enter the menu.

If you want to authenticate via face or card, you should add administrator first. Refers to [**User Management**](#) for details.

Steps

1. Hold the screen to enter the authentication page.
2. You can enter the admin password or authentication via face or card to enter the menu.



Note

Admin password is set as activation password.

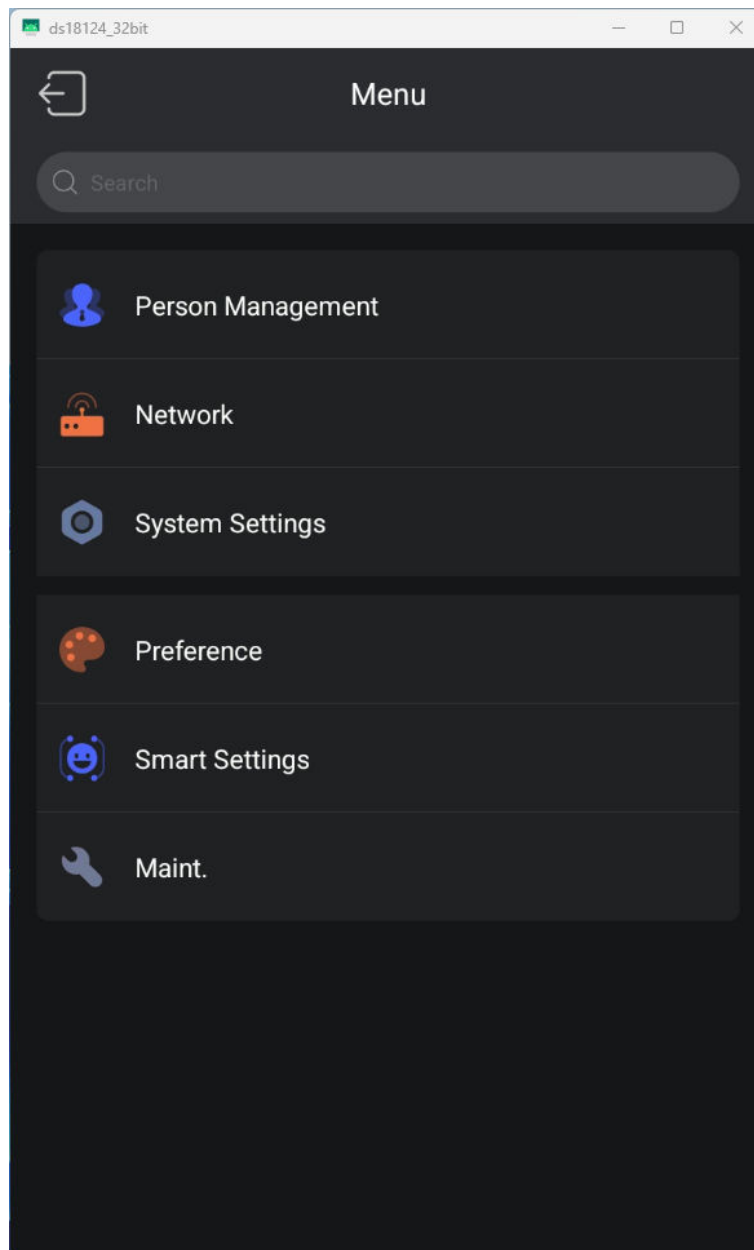


Figure 6-6 Menu Page

6.3 Network Parameters Settings

The device support wired network, wireless network and cloud service settings.



Note

Only parts of the devices support the wireless network, please refers to the actual device for detailed information.

6.3.1 Edit Wired Network Parameters

The device should be connected to the network.

Before You Start

Authenticate and enter the menu first. Refers to [**Authentication via Admin**](#) for details.

Steps

1. On the menu, tap **Network → Wired Network** to enter the settings page.

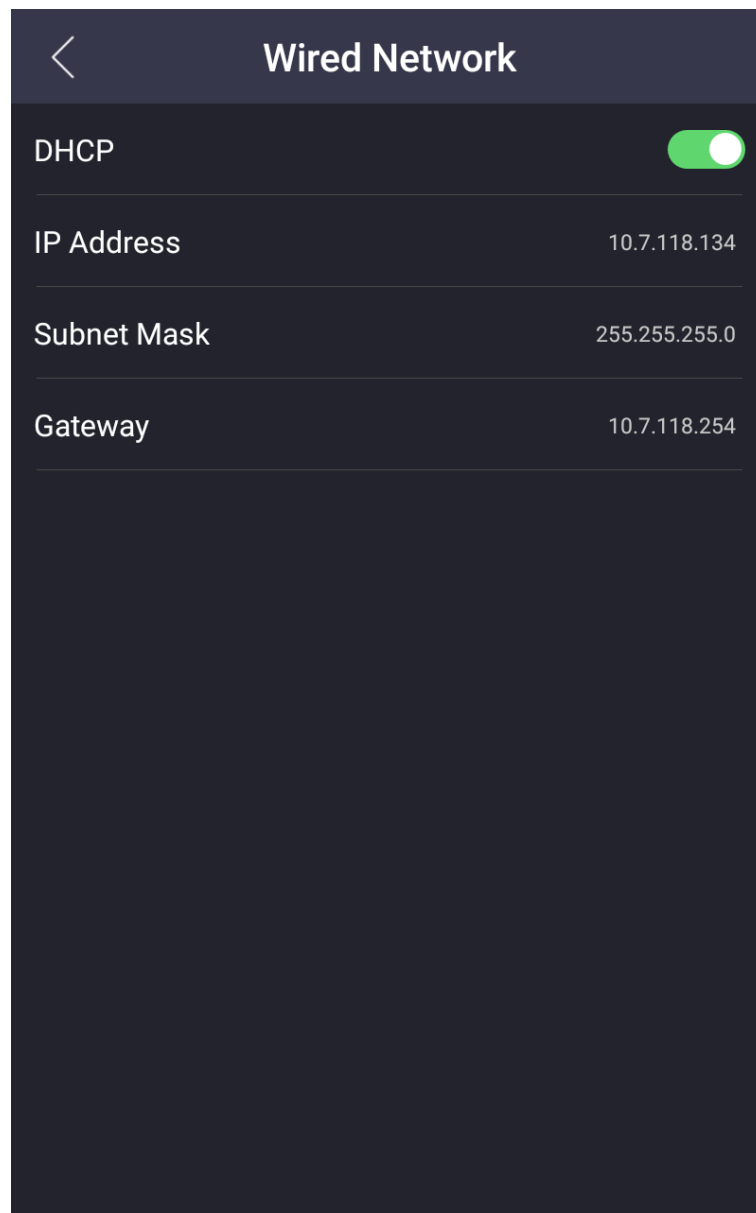


Figure 6-7 Wired Network Settings

2. Edit the wired network parameters.
 - Edit the wired network parameters manually.
 - Enable **DHCP**, and the system will get the parameters automatically.

6.3.2 Connect to Wi-Fi

Before You Start

Authenticate and enter the menu first. Refers to [**Authentication via Admin**](#) for details.

Steps

1. On the menu, tap **Network** → **Wi-Fi** to enter the settings page.

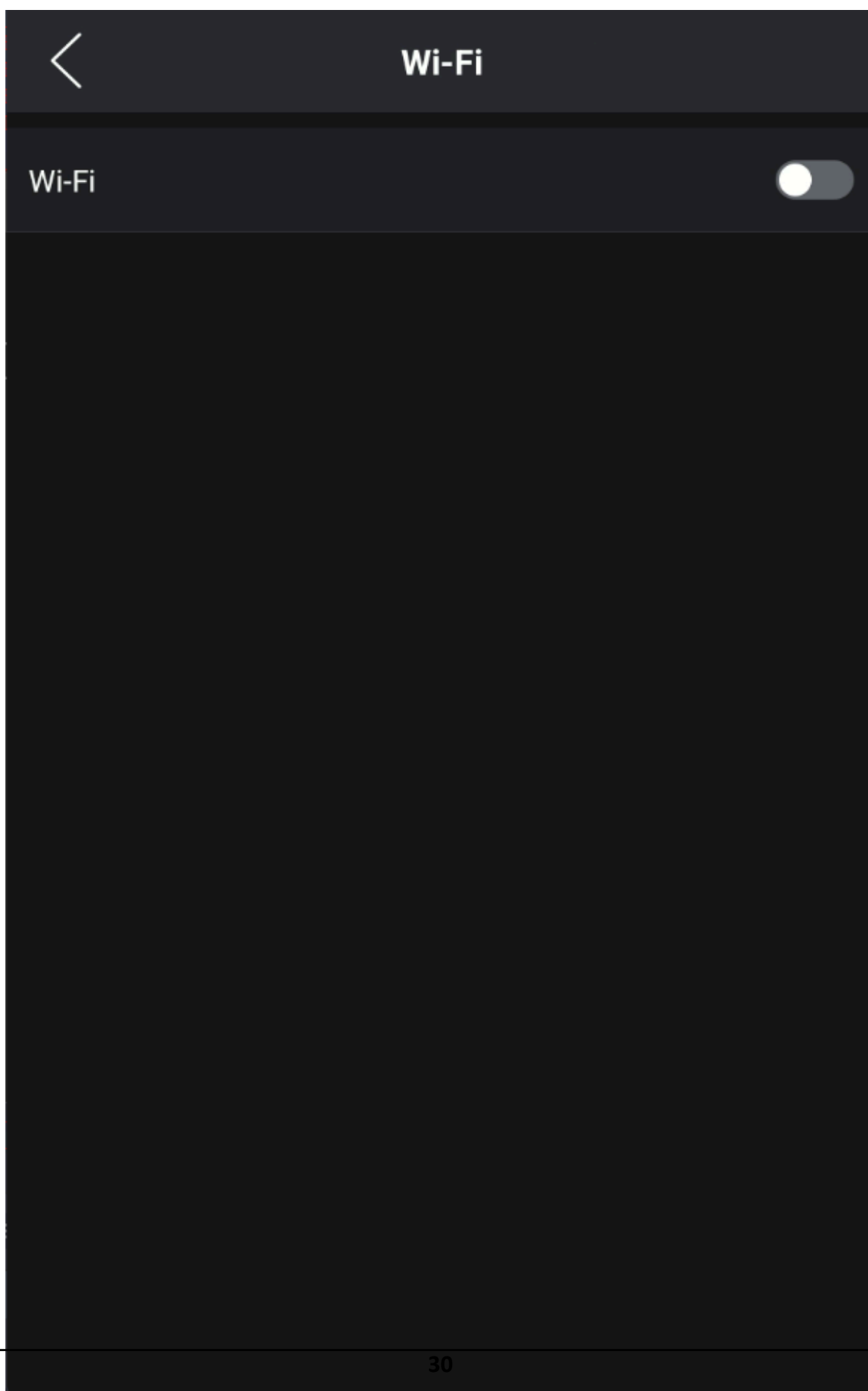


Figure 6-8 Wi-Fi Settings

2. Slide to enable the function.
3. Select a Wi-Fi and enter the password to connect.

6.3.3 Set Bluetooth

Long tap the initial page for 3 s and slide to the left/right then enter the password to enter the menu page. Tap **Network → Bluetooth** to enter the setting page.

Slide to enable bluetooth.

The device supports opening door via bluetooth. You can operate via **Hik-Connect App**.

6.3.4 Cloud Service Settings

Enable the function, you can configure the device via mobile client remotely.

Before You Start

Authenticate and enter the menu first. Refers to **Authentication via Admin** for details.

Steps

1. On the menu, tap **Network → Cloud Service** to enter the settings page.

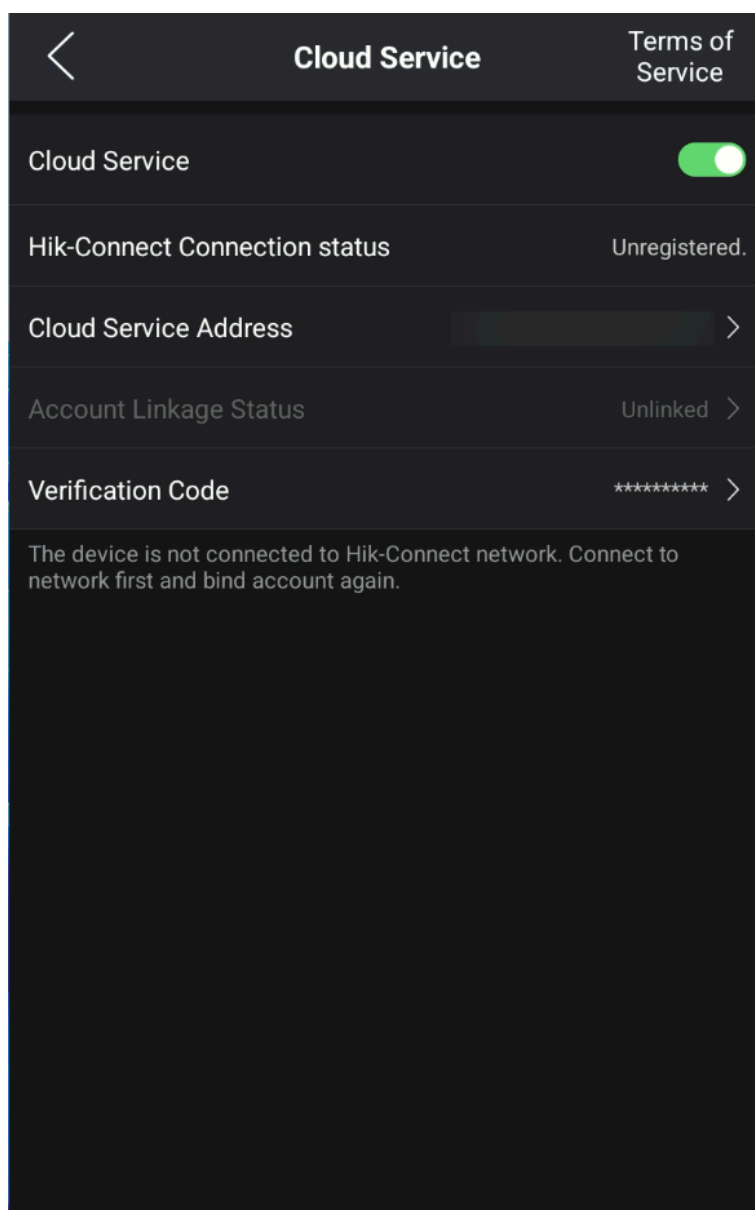


Figure 6-9 Cloud Service Settings

2. Slide to enable the function.
3. Edit the **Cloud Service Address** and create a **Verification Code**.
4. Tap **V** to save the settings.

6.4 User Management

On the user management page, you can add new users, configure the user's room information, card information, face information, and pin code.

Before You Start

Authenticate and enter the menu first. Refers to **Authentication via Admin** for details.

Steps

1. On the menu, tap **Person Management** to enter the settings page.

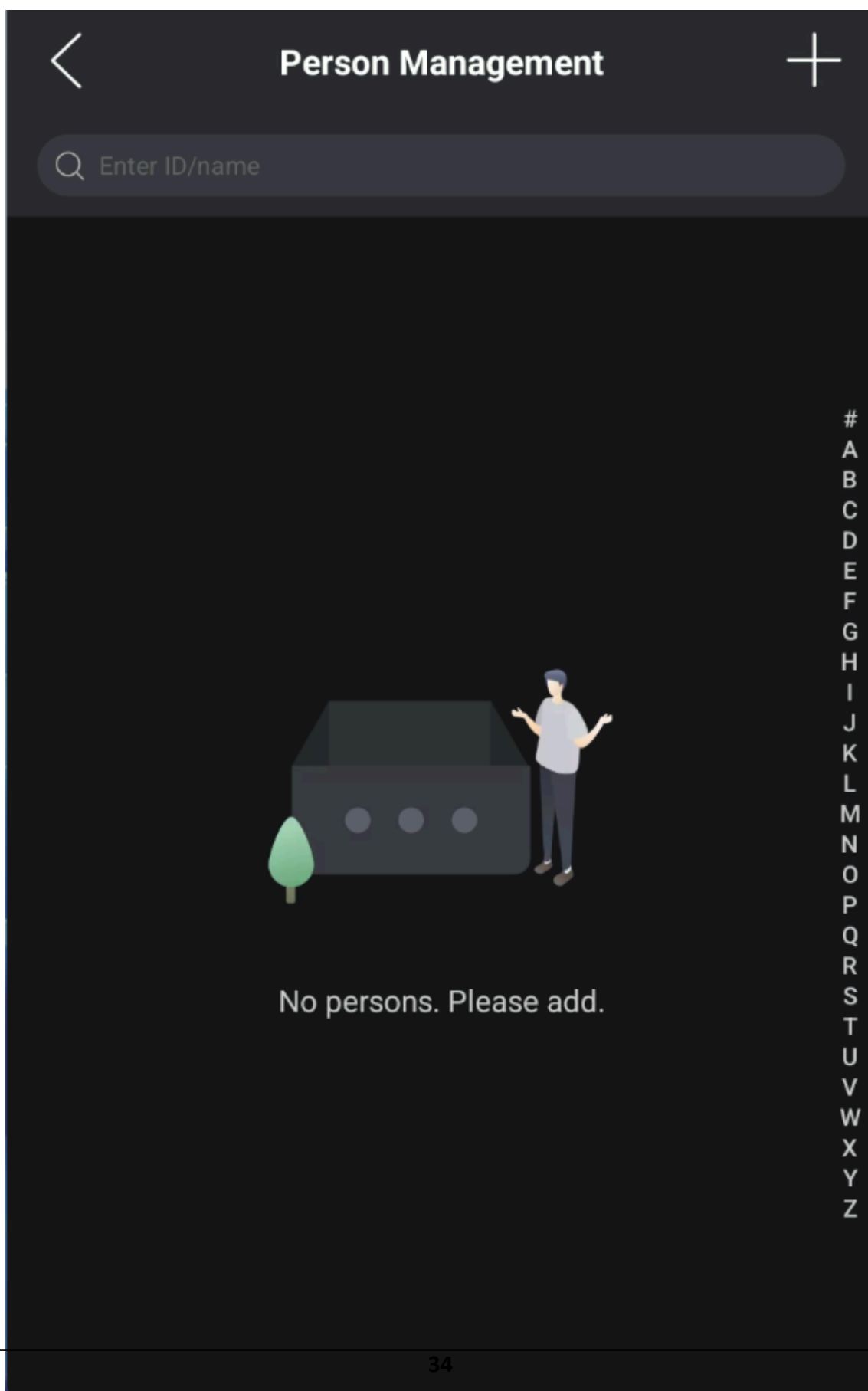


Figure 6-10 Person Management

2. Tap + to enter the add user page.

Add Person	
Employee No.	1 >
Name	Enter >
Room No.	Enter >
Person Type	Normal User
Device Administrator	☐
Face	Add >
Card	0/5 >
PIN Code	Not Configured >

Figure 6-11 Add User

3. Set Employee No., Name and Room No.

4. Add Card.

- 1) Tap **Card**, and tap **+** to enter the add card page.
- 2) Enter the card No. manually or present the card in the card presenting area to obtain the card No.
- 3) Tap **OK** to enable the settings.

5. Add Face.

- 1) Tap **Face Picture**, and point the face at the camera.
- 2) Tap  to add the face.
- 3) Tap  to enable the settings.

6. Add PIN Code.



Note

The PIN Code should have 4 to 8 numbers.

7. Set Person Type as Normal User or Device Administrator.

8. Exit the settings page.

6.5 Preference Settings

Set interface style, theme, shortcut and control center.

Before You Start

Authenticate and enter the menu first. Refers to [**Authentication via Admin**](#) for details.

Steps

- 1.** On the menu, tap **Preference** to enter the settings page.

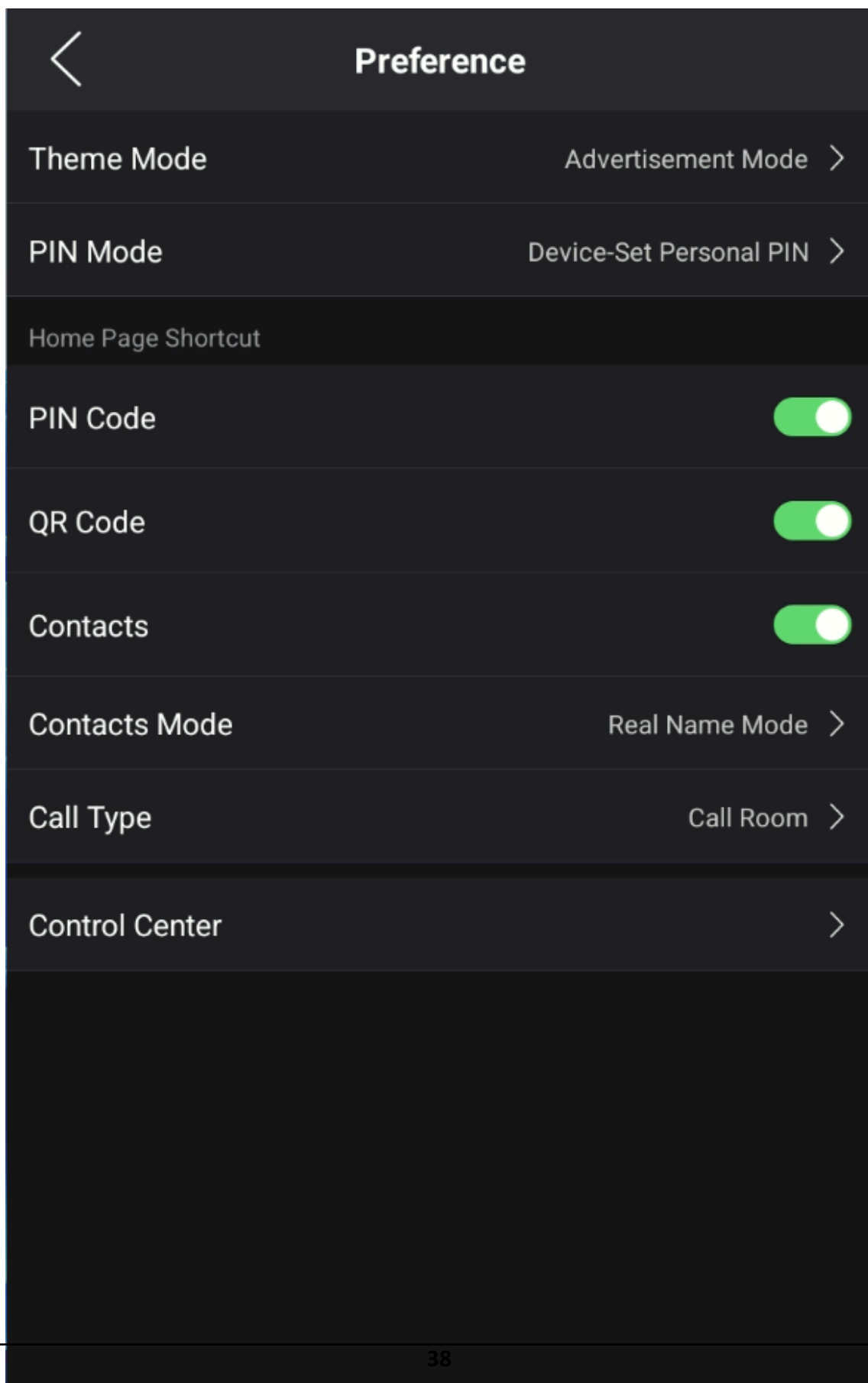


Figure 6-12 Preference

2. You can select **Theme Mode** as **Recognition Mode**, or **Advertisement Mode**.

Recognition Mode

The device authentication page will display the live view page. And the person's name, employee ID, face pictures will all be displayed after authentication.

Advertisement Mode

After selecting this mode, the advertising area and identification authentication area of the device will be displayed on separate screens. Video and advertising information playback, welcome speech display are supported.

3. Select PIN Mode as **Device-Set Personal PIN** or **Platform-Applied Personal PIN**.

Device-Set Personal PIN

It can be created or edited on the device or on the web, and cannot be set on other platforms.

Platform-Applied Personal PIN

It can be created or edited on the platform, and issued to the device before it can be used. It cannot be set on the device or on the web.

4. Choose the shortcut key that displayed on the authentication page, including the QR code function, the call function, call type, and the PIN entering function. You can slide to enable or disable **PIN Code**, **QR Code** and **Contacts** based on your actual needs.

PIN Code

Enable this function and you can enter PIN to authenticate via PIN.

QR Code

You can use the QR code scanning function on the authentication interface. The device will upload the information associated with the obtained QR code to the platform.

Contacts

Real Name Mode

Show User Name and Room No. in the local contacts.

Anonymous Mode

Show Desensitized Name and Room No. in the local contacts.

5. Select **Call Type**. You can select call type from **Call Room**, **Call Center** and **Call Specified Room No.**.

Call Room

When you tap the call button on the authentication page, you should dial a room No. to call.

Call Center

When you tap the call button on the authentication page, you can call the center directly.

Call Specified Room No.

You should set a room No. When you tap the call button on the authentication page, you can call the configured room directly without dialing.

6. Tap **Control Center** to select the control items displayed in the control center.

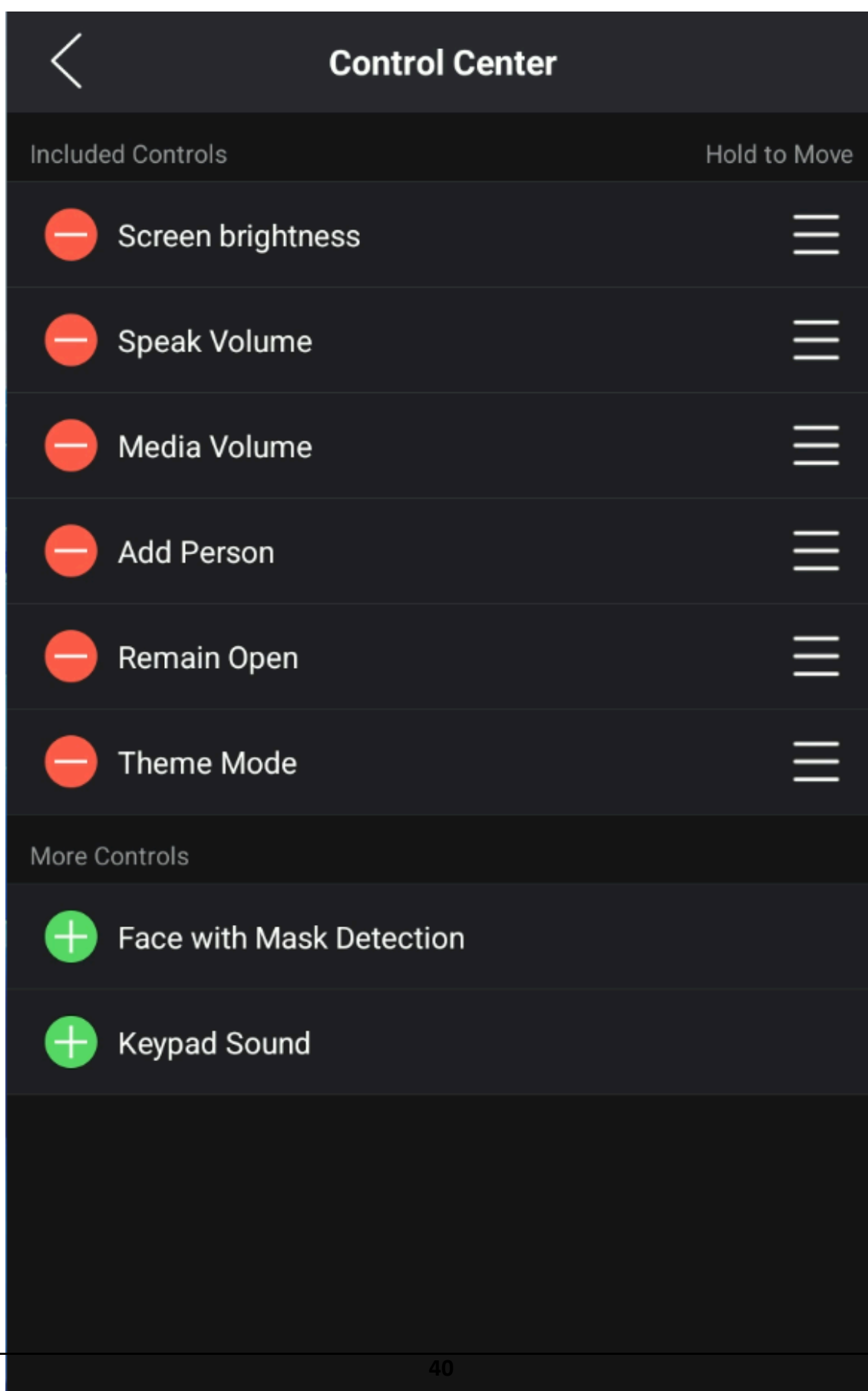


Figure 6-13 Control Center Setting Page



Note

On the authentication page, use finger to pull down to enter the control center page to view the control items.

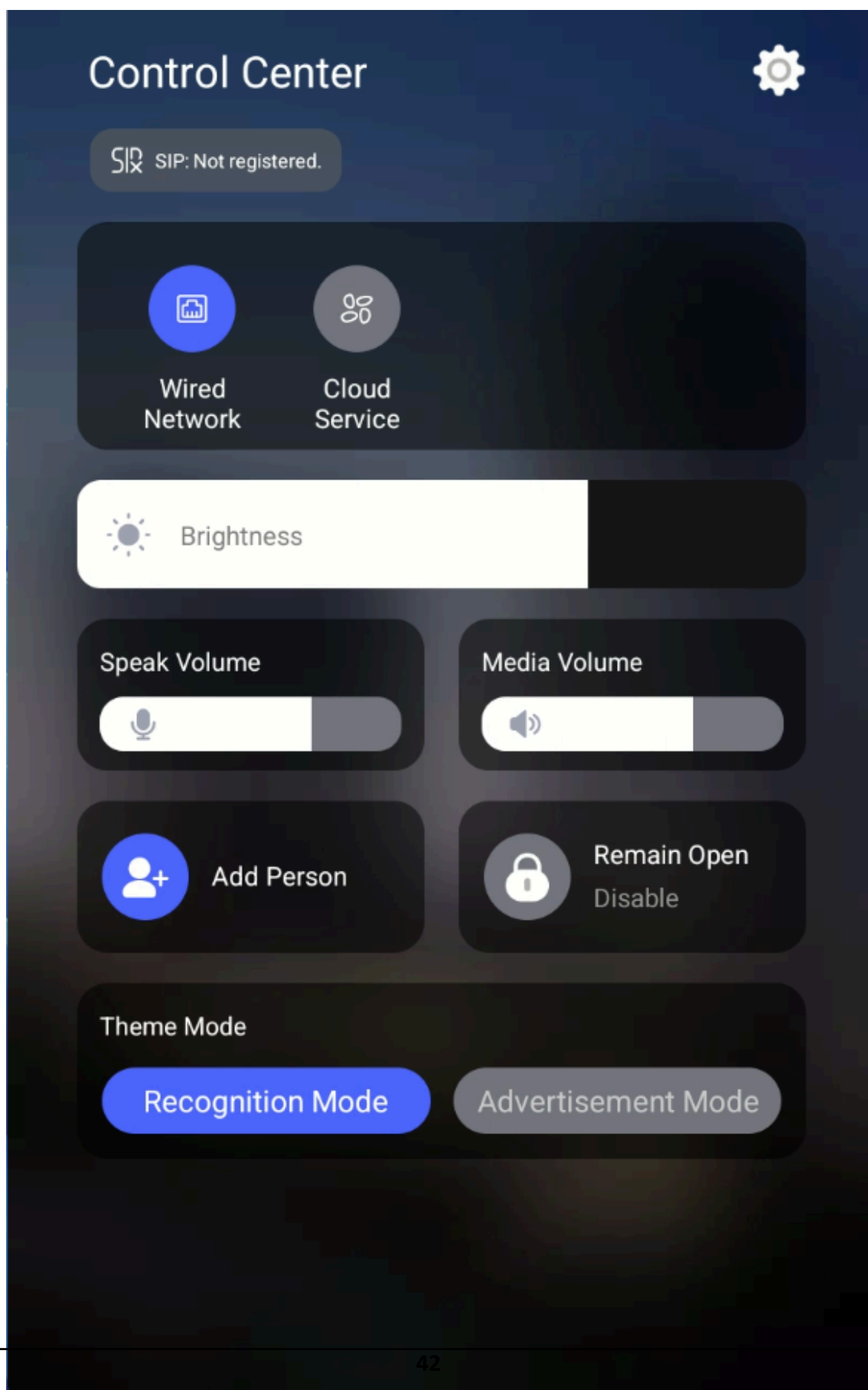


Figure 6-14 Control Center

6.6 Smart Settings

6.6.1 Enable/Disable Mask Detection via Device

After enabling the face with mask detection, the system will recognize the captured face with mask picture.

Authenticate and enter the menu first. Refers to [**Authentication via Admin**](#) for details.

On the menu, tap **Smart Settings** to enter the settings page.

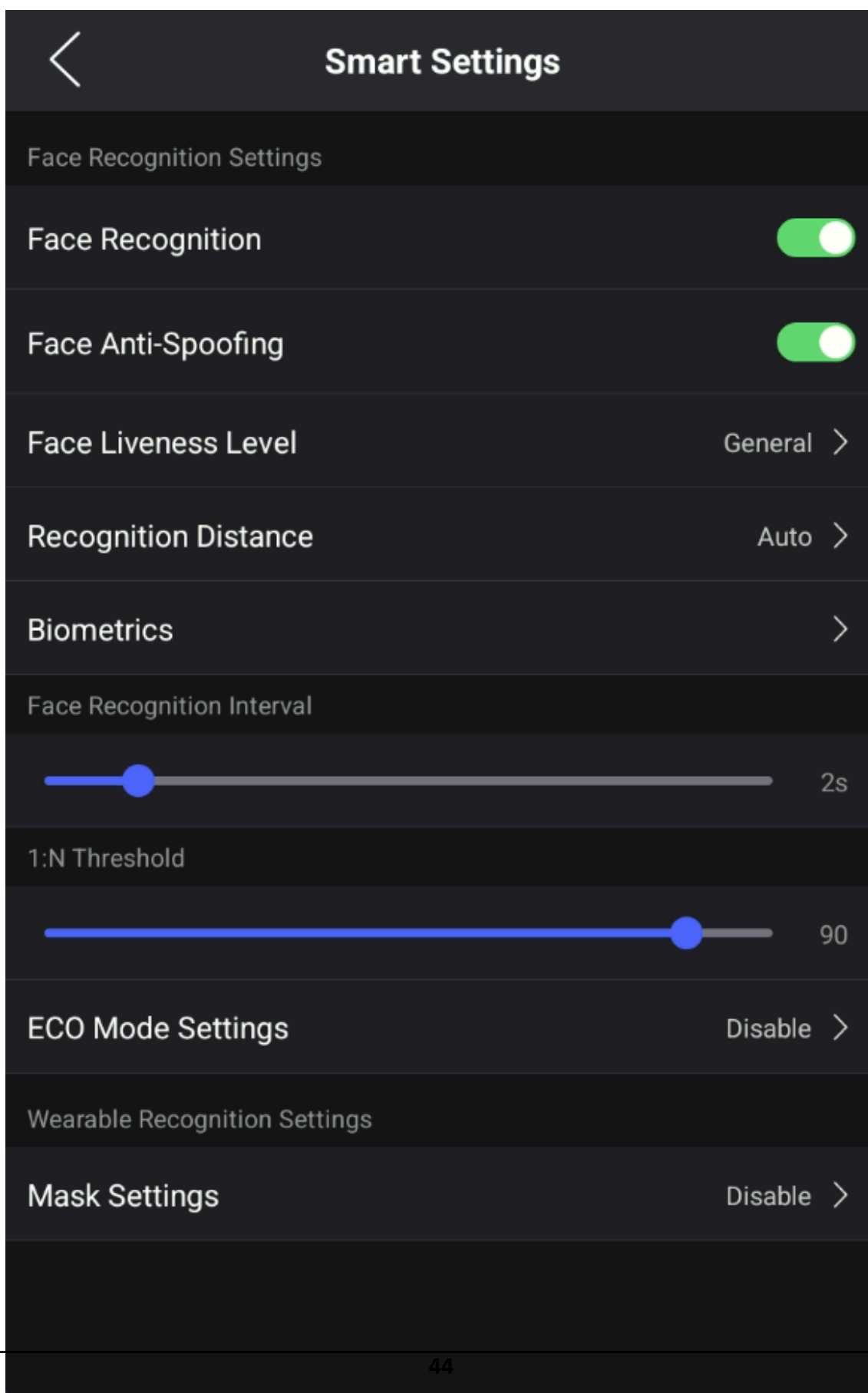


Figure 6-15 Smart Settings

Tap **Mask Settings**, If enable **Mask Settings**, you can set **Face with Mask & Face (1:1)**、**Face with Mask & Face (1:N)**、**ECO Mode (1:1) Threshold**、**ECO Mode (1:N) Threshold**, and **Prompt Method**.

Face with Mask & Face (1:1)

Set face with mask 1:1 matching threshold. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask & Face (1:N)

Set face with mask 1:N matching threshold. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

ECO Mode (1:1) Threshold

After enabling the ECO mode, you can set the face with mask function. You can set the threshold.

Set the matching threshold when authenticating via ECO mode 1:1 matching mode. The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maximum value is 100.

ECO Mode (1:N) Threshold

After enabling the ECO mode, you can set the face with mask function. You can set the threshold.

Set the matching threshold when authenticating via ECO mode 1:N matching mode. The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maximum value is 100.

Strategy

Set **None**、**Reminder of Wearing**, and **Must Wear**.

None

If the person do not wear a face mask when authenticating, the device will not prompt a notification.

Reminder of Wearing

If the person do not wear a face mask when authenticating, the device prompts a notification and the door will open.

Must Wear

If the person do not wear a face mask when authenticating, the device prompts a notification and the door keeps closed.

6.6.2 Set Face Recognition Distance

Set the valid distance between the person and the device camera.

Authenticate and enter the menu first. Refers to **Authentication via Admin** for details.

On the menu, tap **Smart Settings** to enter the settings page.

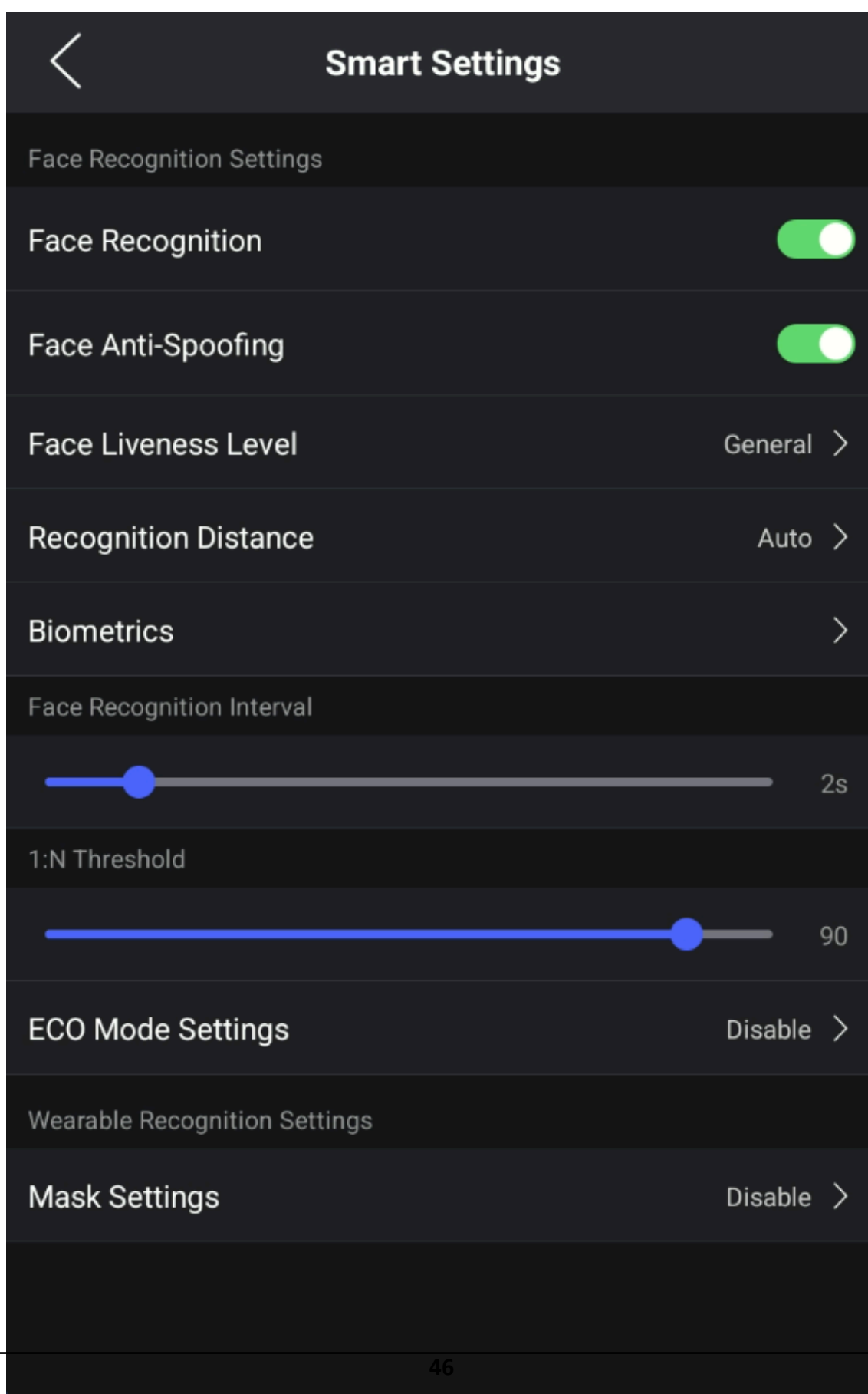


Figure 6-16 Smart Settings

Tap **Recognition Distance**. Select the valid distance between the person and the device camera when authenticating.

6.6.3 Set Face 1:N Security Level via Device

Set the matching threshold when authenticating via 1:N matching mode.

Authenticate and enter the menu first. Refers to **Authentication via Admin** for details.

On the menu, tap **Smart Settings** to enter the settings page.

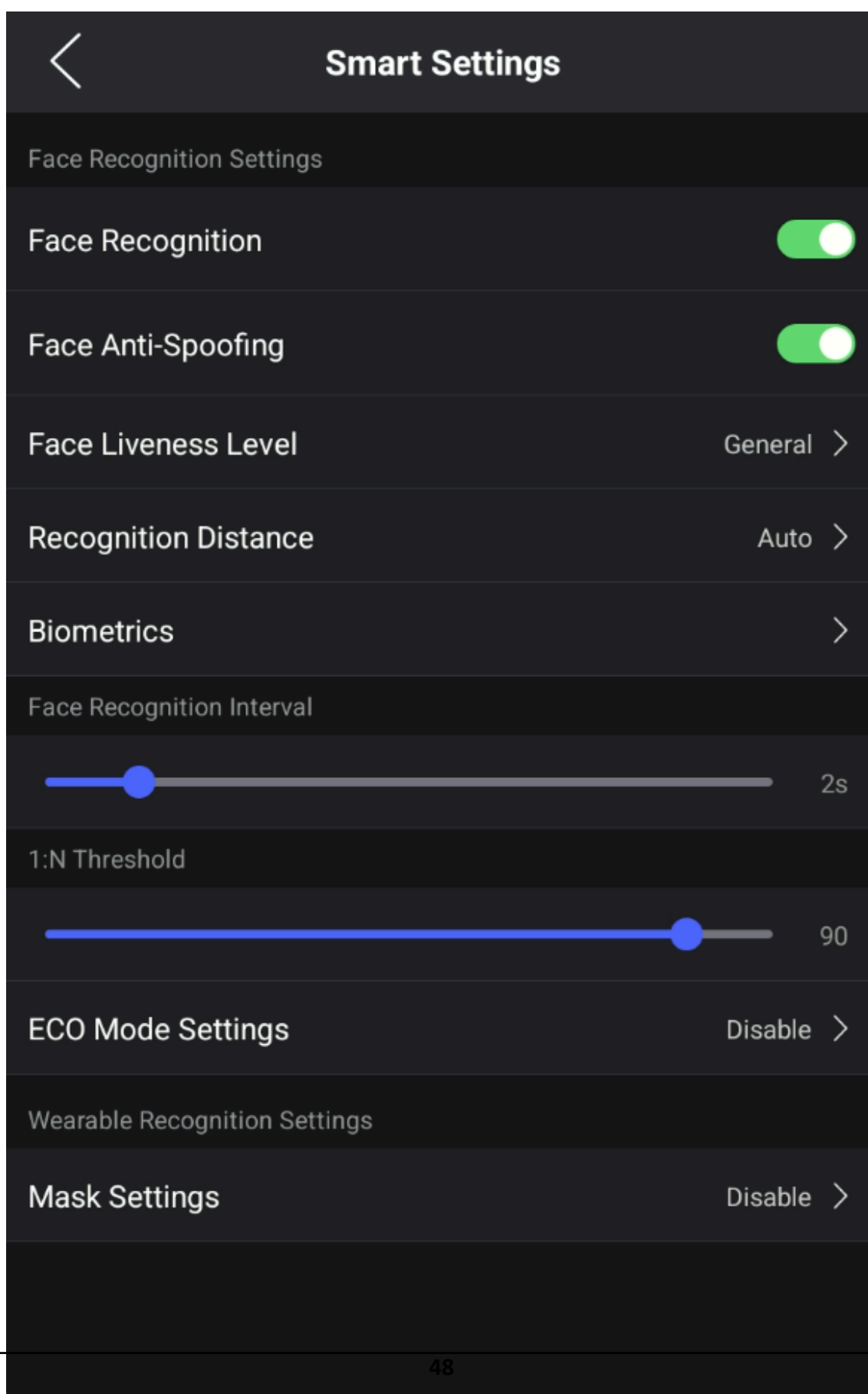


Figure 6-17 Smart Settings

Drag the bar to adjust the matching threshold when authenticating via 1:N matching mode.

(Range: 1~100)

The larger the value of the threshold, the fault acceptance rate will be lower and the false rejection rate will be higher when authenticating via face. The maximum value is 100.

6.6.4 Enable/Disable ECO Mode via Device

If the ECO mode is enabled, you can authenticate faces in the low light or dark environment with IR camera.

Authenticate and enter the menu first. Refers to [**Authentication via Admin**](#) for details.

On the menu, tap **Smart Settings** to enter the settings page.

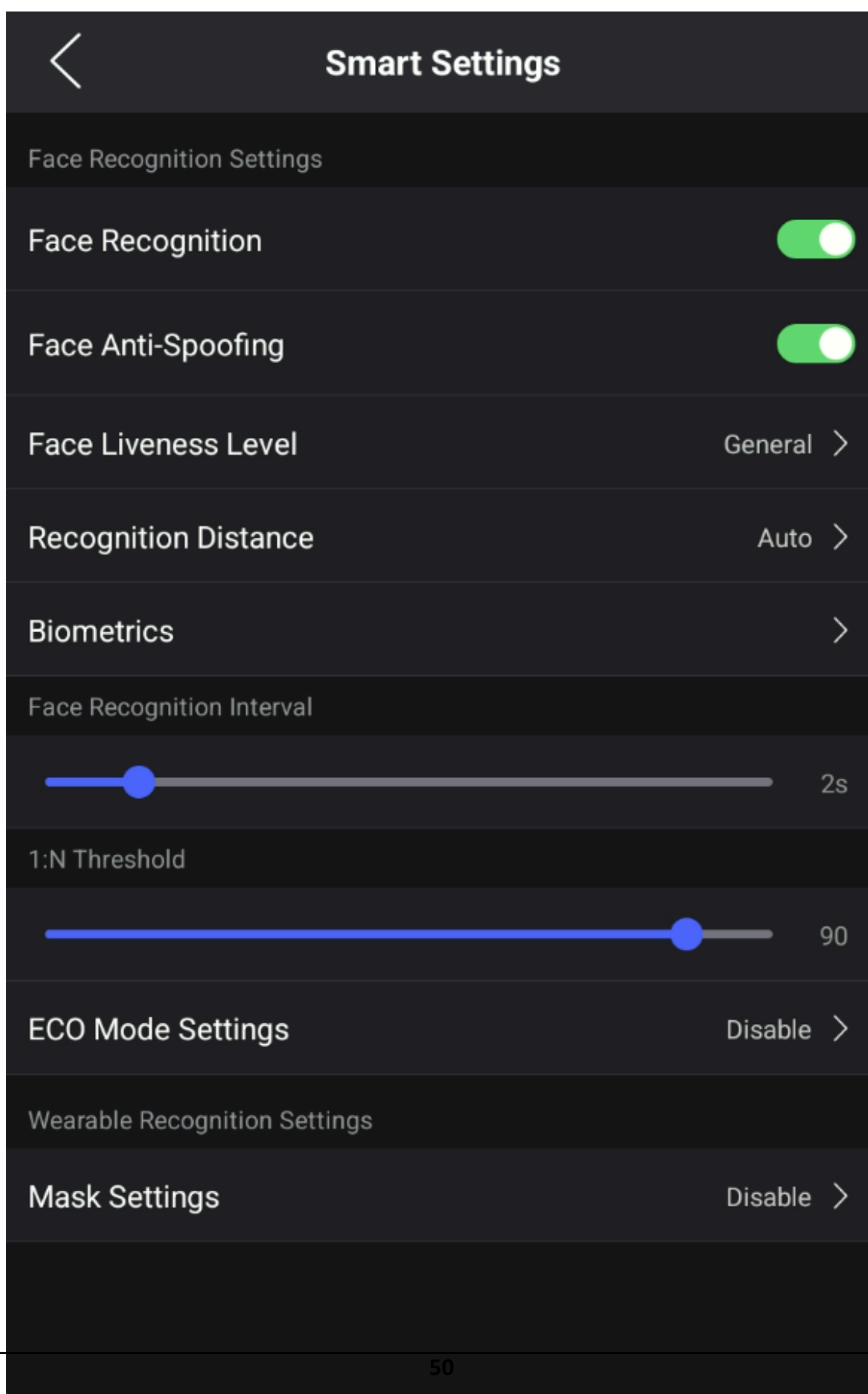


Figure 6-18 Smart Settings

Tap **ECO Mode Settings**. If the ECO mode is enabled, you can authenticate faces in the low light or dark environment with IR camera. You can set the ECO mode threshold, ECO mode (1:N), and ECO mode (1:1).

ECO Mode Threshold

When enabling the ECO mode, you can set the ECO mode's threshold. The larger the value, the easier the device entering the ECO mode. The threshold has relationship with the illumination.

ECO Mode (1:1)

Set the matching threshold when authenticating via ECO mode 1:1 matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

ECO Mode (1:N)

Set the matching threshold when authenticating via ECO mode 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

6.6.5 Set Face Liveness Level

Set the matching security level when performing face anti-spoofing authentication

Authenticate and enter the menu first. Refers to **Authentication via Admin** for details.

On the menu, tap **Smart Settings** to enter the settings page.

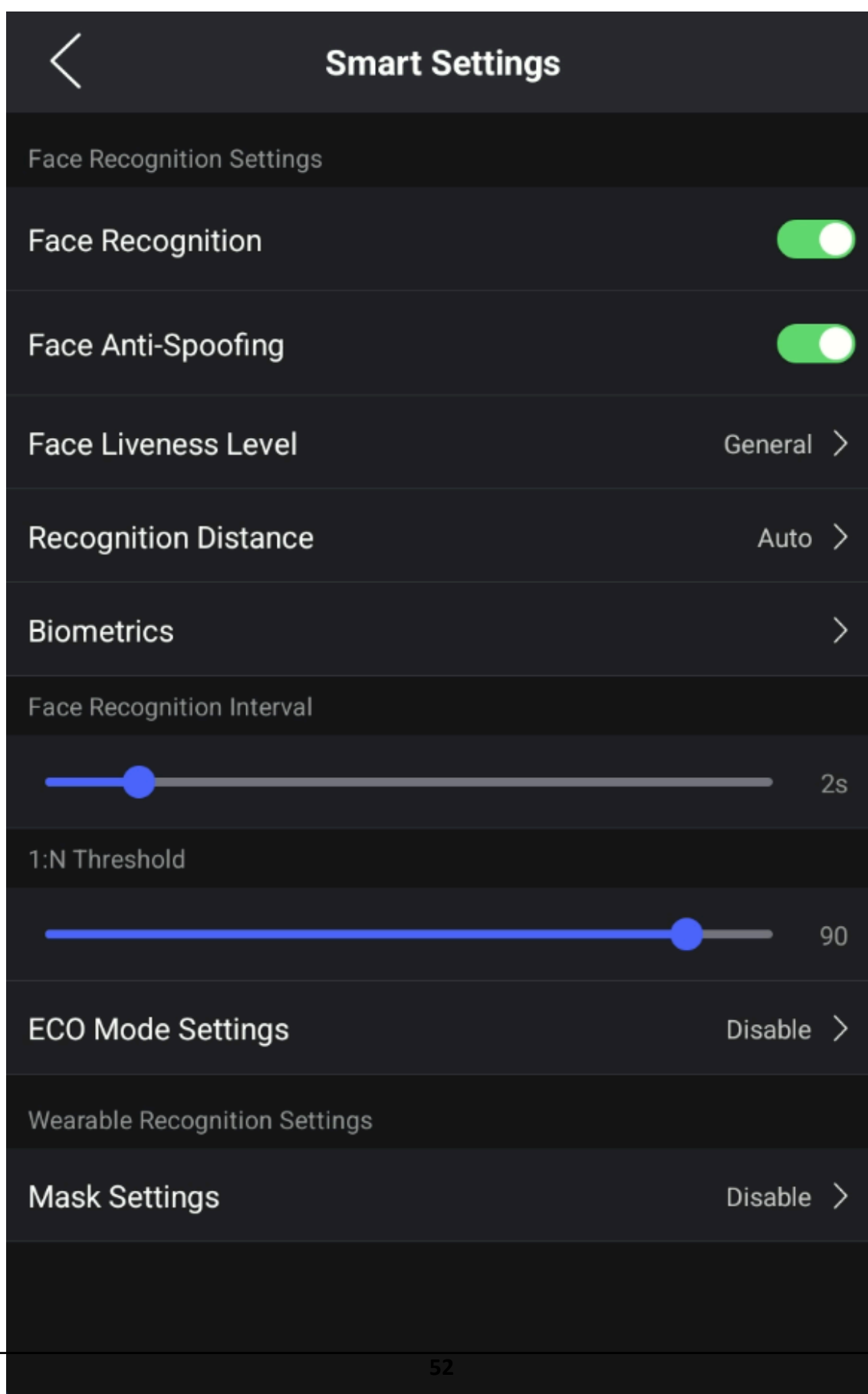


Figure 6-19 Smart Settings

After enabling face anti-spoofing function, you can set the matching security level when performing face anti-spoofing authentication. The higher the level, the more strict of the recognition.

6.6.6 Set Face Recognition Interval

You can set the time interval between 2 continuous face recognitions when authenticating.

Authenticate and enter the menu first. Refers to **Authentication via Admin** for details.

On the menu, tap **Smart Settings** to enter the settings page.

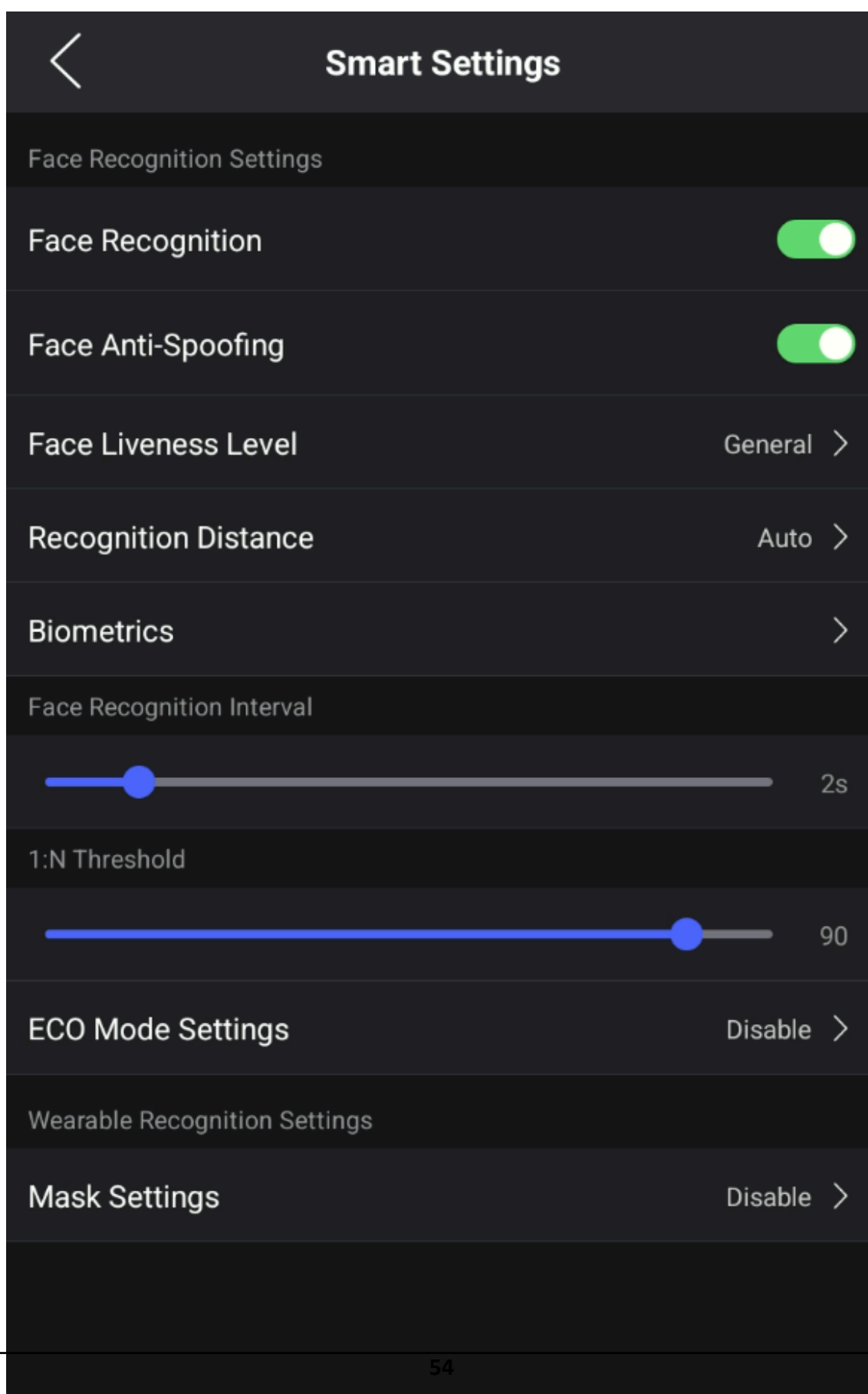


Figure 6-20 Smart Settings

Drag the bar to adjust the time interval between 2 continuous face recognitions when authenticating.



Range: 1~10s.

6.6.7 Biometrics

You can set face parameters.

Before You Start

Authenticate and enter the menu first. Refers to [Authentication via Admin](#) for details.

Steps

1. On the menu, tap **Smart Settings** → **Biometrics** and enter the admin password to enter the settings page.
2. Slide to enable or disable **Custom Anti-Spoofing Detection** and **Lock Face for Authentication** based on your actual needs. .

Face Parameter

Custom Anti-Spoofing Detection

Face Liveness Level

After enabling face anti-spoofing function, you can set the matching security level when performing live face authentication.

Anti-Spoofing Detection Threshold

The larger the value, the smaller the false accept rate and the larger the false rejection rate. The smaller the value, the larger the false accept rate and the smaller the false rejection rate.

Lock Face for Anti-Spoofing Protection

After enabling this function, the device will lock automatically when anti-spoofing detection failed.

Lock Duration

The lock duration after enabling **Lock Face for Anti-Spoofing Protection** when anti-spoofing detection failed.

6.7 System Settings

6.7.1 Change Language

Change language according to your actual needs.

Before You Start

Authenticate and enter the menu first. Refers to [***Authentication via Admin***](#) for details.

Steps

1. On the menu, tap **System Settings** to enter the settings page.

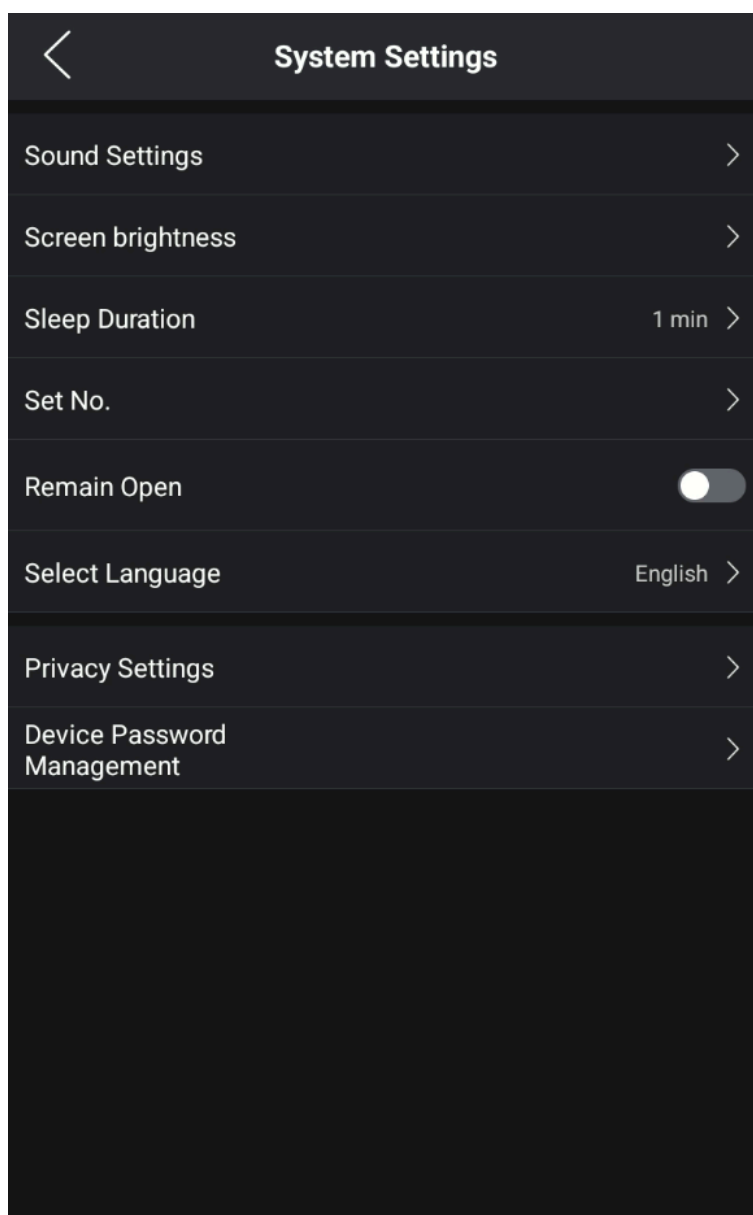


Figure 6-21 System Settings

2. Tap **Select Language** to switch the system language.

6.7.2 Adjust Brightness

Before You Start

Authenticate and enter the menu first. Refers to [***Authentication via Admin***](#) for details.

Steps

1. On the menu, tap **System Settings** to enter the settings page.

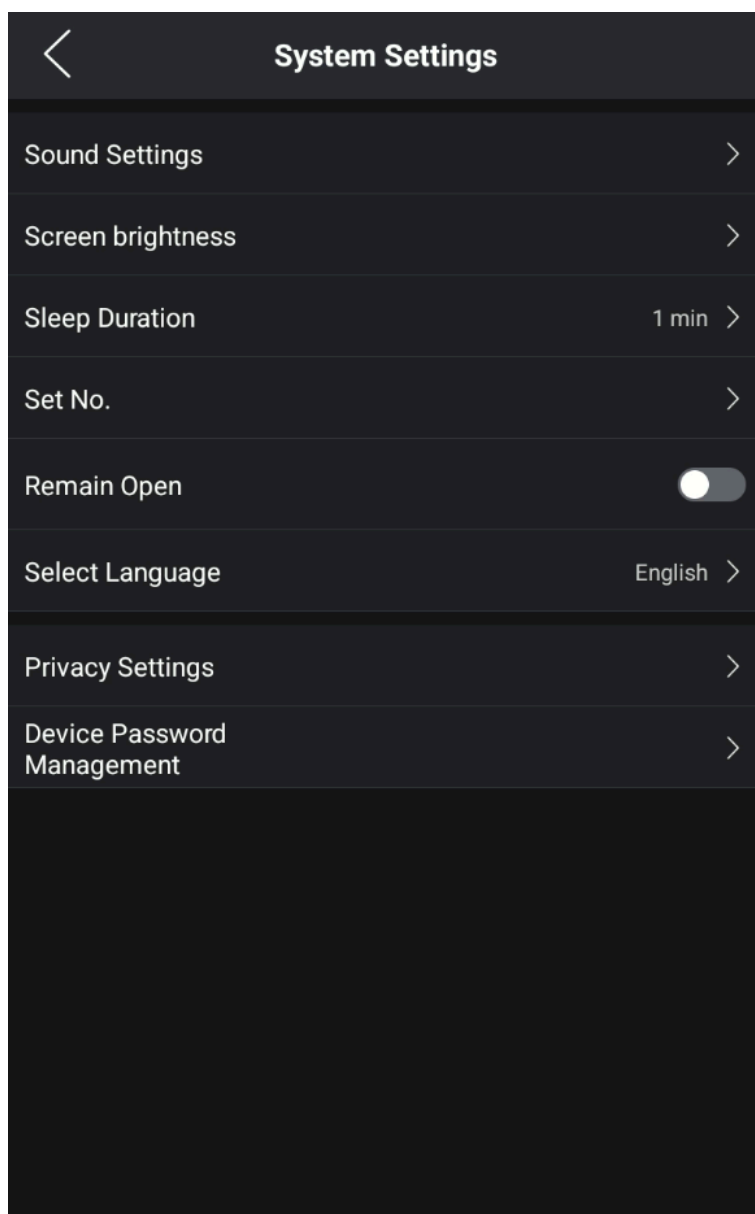


Figure 6-22 System Settings

2. Tap **Screen Brightness** to adjust the brightness of the device.

- Enable the **Auto Screen Brightness**, the device will adjust the brightness according to the environment automatically.
- Edit the number to adjust the brightness manually.

6.7.3 Set Sleep Duration via Device

Set the device sleeping waiting time.

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

On the menu, tap **System Settings → Sleep Duration** . And Set **Sleep Duration**.

When you are on the initial page and if you set the sleeping time to 30 s, the device will sleep after 30 s without any operation.

6.7.4 Password Management

You can change device password.

Steps

1. Long tap on the initial page for 3 s and slide to the left/right by following the gesture and login the device home page. Tap **System Settings** .
2. Tap **Device Password Management**. Enter the old password.
3. Enter the new password and confirm it.
4. Tap **OK**.



Note

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least two kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

-
5. You can select **Password Change Type** and set the content.

6.7.5 Set Door Contact via Device

Authenticate and enter the menu first. Refers to ***Authentication via Admin*** for details.

On the menu, tap **System Settings**. Then you can slide to enable or disable **Remain Open** based on your actual needs.

6.7.6 Set Privacy Parameters

Set picture upload and storage parameters.

Tap **System Settings** → **Privacy Settings** to enter the settings page.

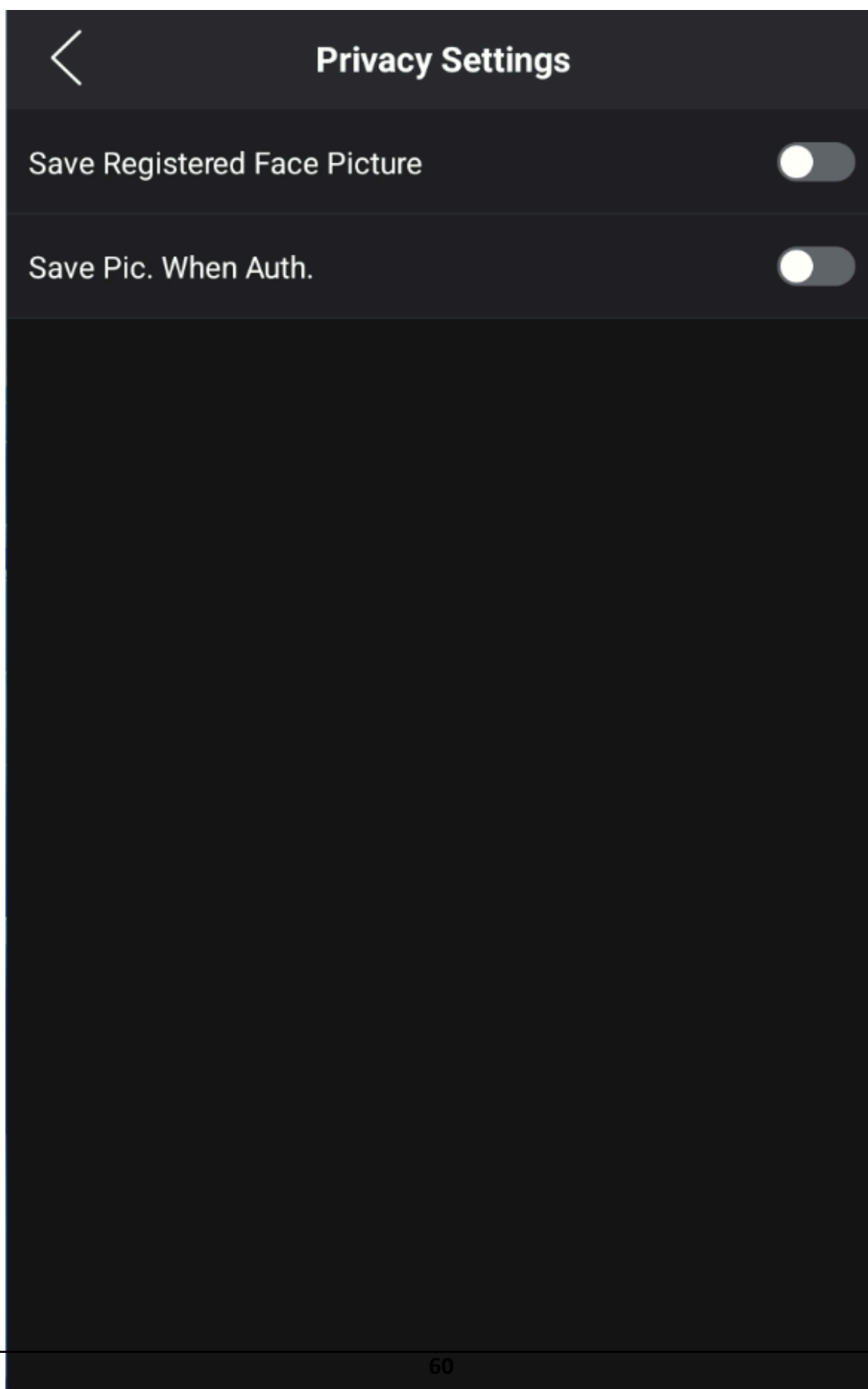


Figure 6-23 Privacy Settings

Picture Uploading and Storage

Save Registered Picture

The registered face picture will be saved to the system if you enable the function.

Save Pic. When Auth.

If you enable this function, you can save the picture when Authenticating to the device.

Upload Pic. When Auth.

Upload the pictures captured when authenticating to the platform automatically.

6.7.7 Device No. Settings

Configure the No. of the device to make the communication easily.

Before You Start

Authenticate and enter the menu first. Refers to [**Authentication via Admin**](#) for details.

Steps

1. On the menu, tap **System Settings** → **Set No.** to enter the settings page.

< Set No.

Community No.	1 >
Building No.	1 >
Unit No.	1 >
Floor No.	1 >
No.	0 >

62

Figure 6-24 No. Settings

2. Edit **Community No.**, **Building No.**, **Unit No.**, **Floor No.** and **No.** according to the actual needs.

6.7.8 Sound Settings

Authenticate and enter the menu first. Refers to **Authentication via Admin** for details.

On the menu, tap **System Settings** → **Sound Settings** to enter the settings page.

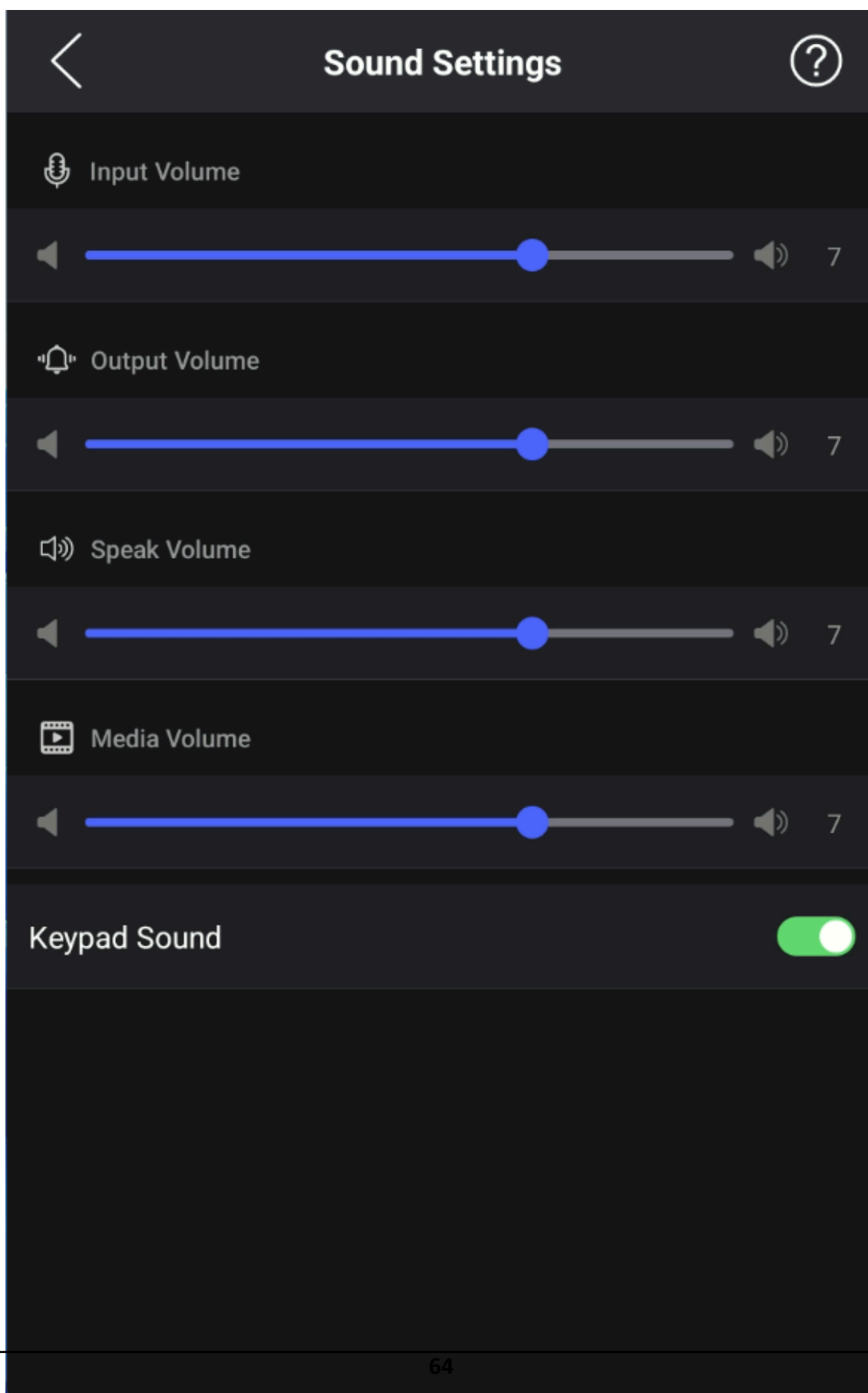


Figure 6-25 Sound Settings

You can drag the bar to adjust **Input Volume**, **Output Volume**, **Speak Volume** and **Media Volume** at this page.

Input Volume

Adjust microphone input level during intercom.

Output Volume

Adjust ringtone volume for prompts.

Speak Volume

Adjust speaker output level during intercom.

Media Volume

Adjust playback volume for media (e.g., ads).

Slide to enable or disable the **Keypad Sound** based on your actual needs.

6.8 Maintenance

6.8.1 Device Information

View the device model, system version, firmware version and open source software licenses.

Before You Start

Authenticate and enter the menu first. Refers to [**Authentication via Admin**](#) for details.

Steps

1. On the menu, tap **Maint.** to enter the page.

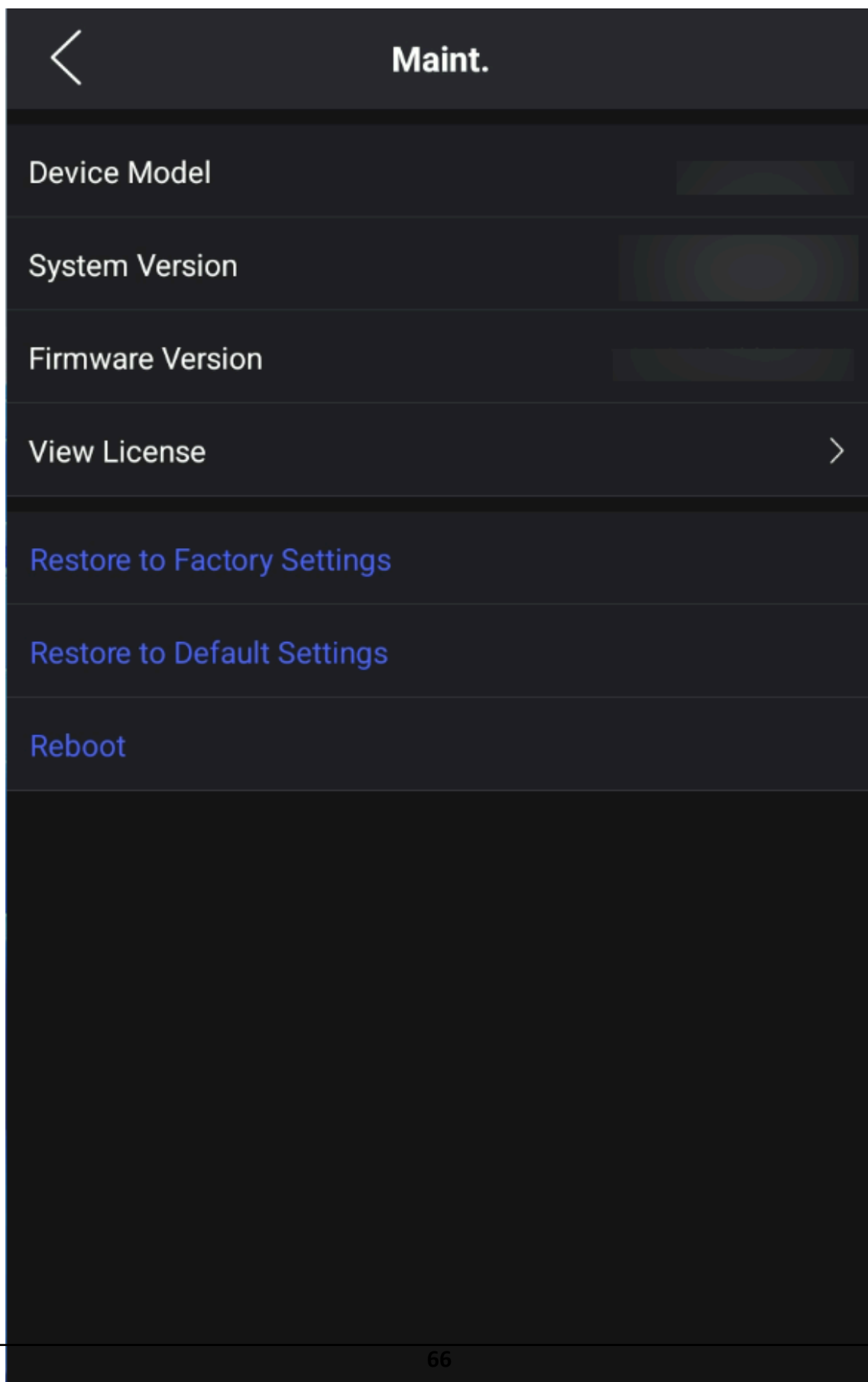


Figure 6-26 Maint.

2. You can view the device model, system version, firmware version and open source software licenses.

6.8.2 Reboot

Reboot device if needed.

Long tap on the initial page for 3 s and slide to the left/right by following the gesture. Login and tap **Maint.**

Reboot the device.

6.8.3 Restore Door Station

Before You Start

Authenticate and enter the menu first. Refers to [**Authentication via Admin**](#) for details.

Steps

1. On the menu, tap **Maint.** to enter the settings page.

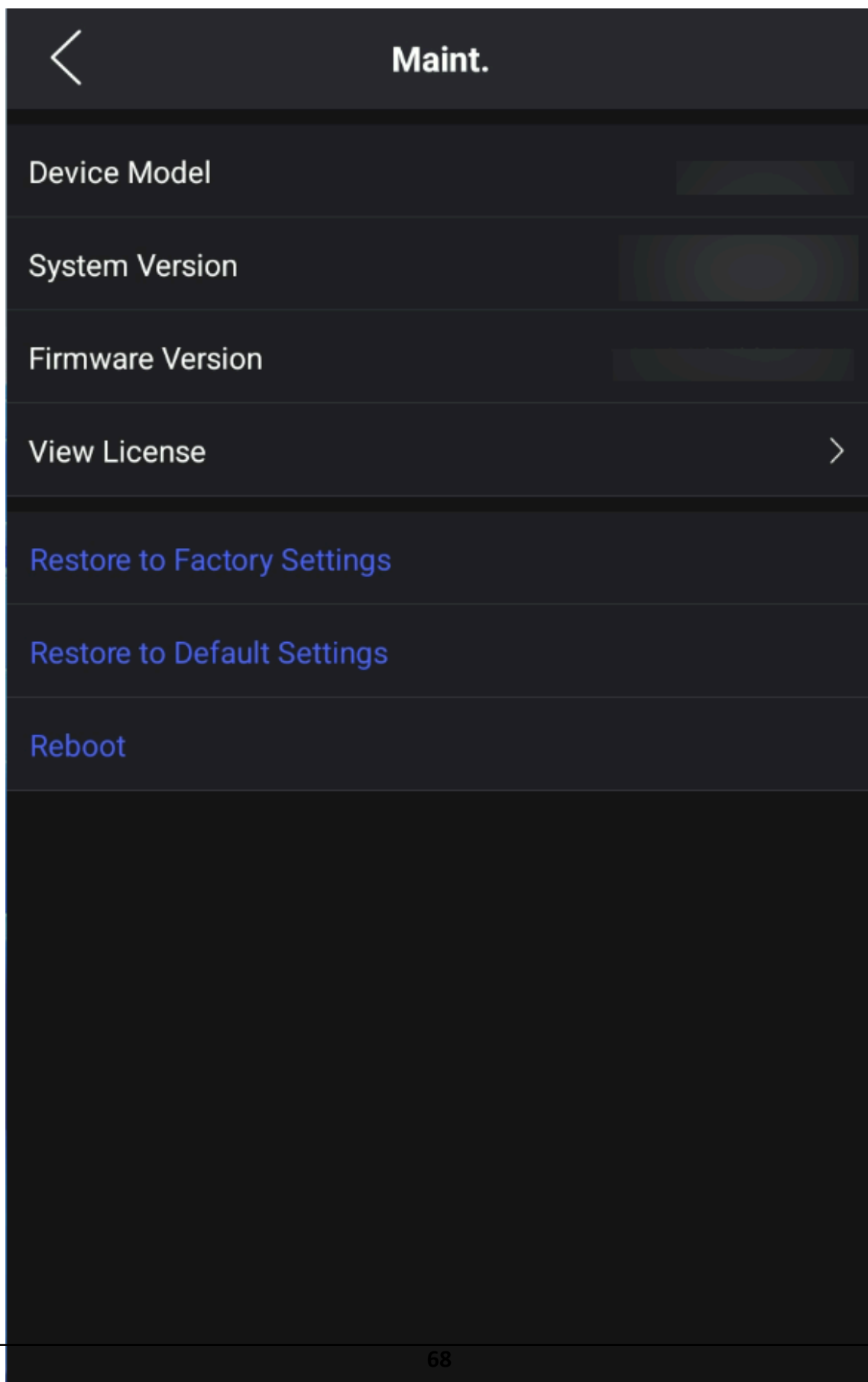


Figure 6-27 Maint.

2. Restore the device.

Restore to Default Settings

Tap **Restore to Default Settings** to reset all parameters, except IP address, subnet mask and default gateway, to the default settings.

Restore to Factory Settings

Tap **Restore to Factory Settings** to restore all parameters to default settings.

Chapter 7 Local Operation

7.1 Call from the Device

Door station supports calling users or management center.

7.1.1 Call Resident

Call Resident from Main/Sub Door Station

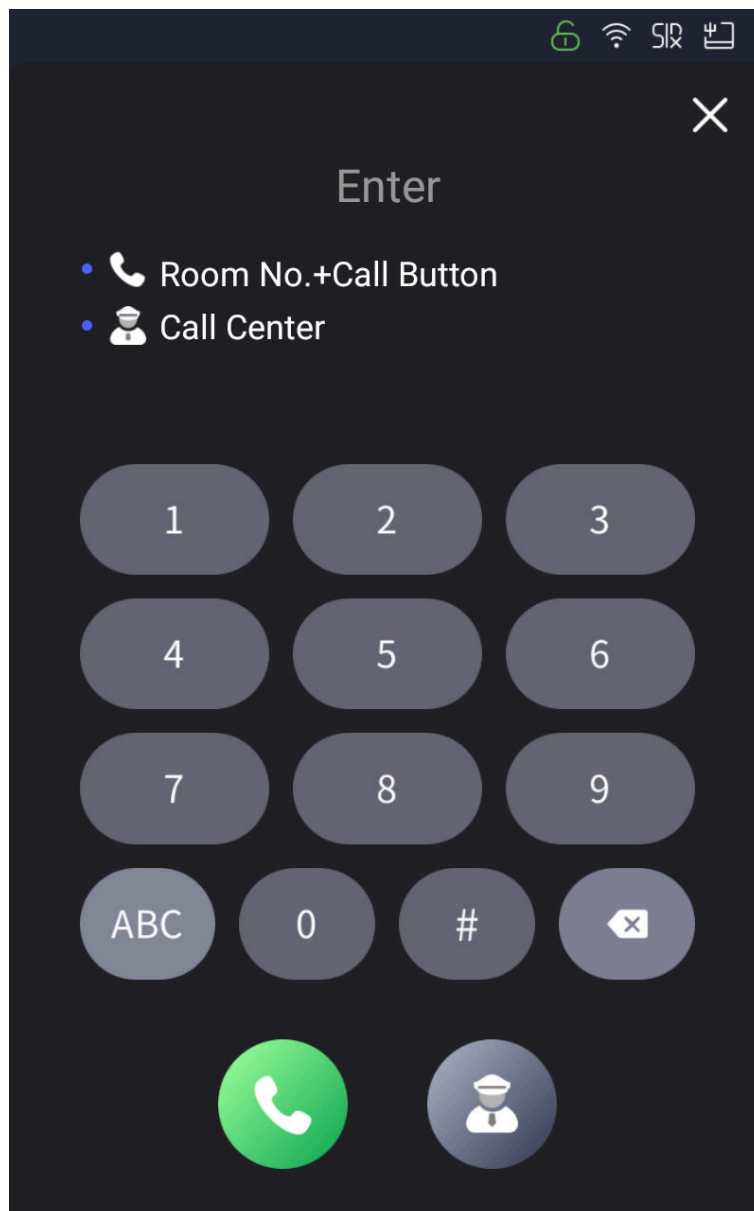


Figure 7-1 Call Resident

On the main page, tap  to enter the calling page.
Enter the **Room No.**, and tap  to call residents.

Note

- Both the main and sub door station support the elevator control function, that is, after calling the residents successfully, tap the unlock button on the indoor station, the elevator will automatically arrive at the floor where the door station is located, and the permission of the

floor where the household is located will be opened (The elevator calling will take effect only after the elevator control is configured and the corresponding configuration of the door machine is completed).

- You can enter the related No. and tap  to call residents if the function is enabled for the indoor stations. Refer to ***Device Management*** for details about related No. settings.
-

On the main page, tap contact button to enter the contact list.

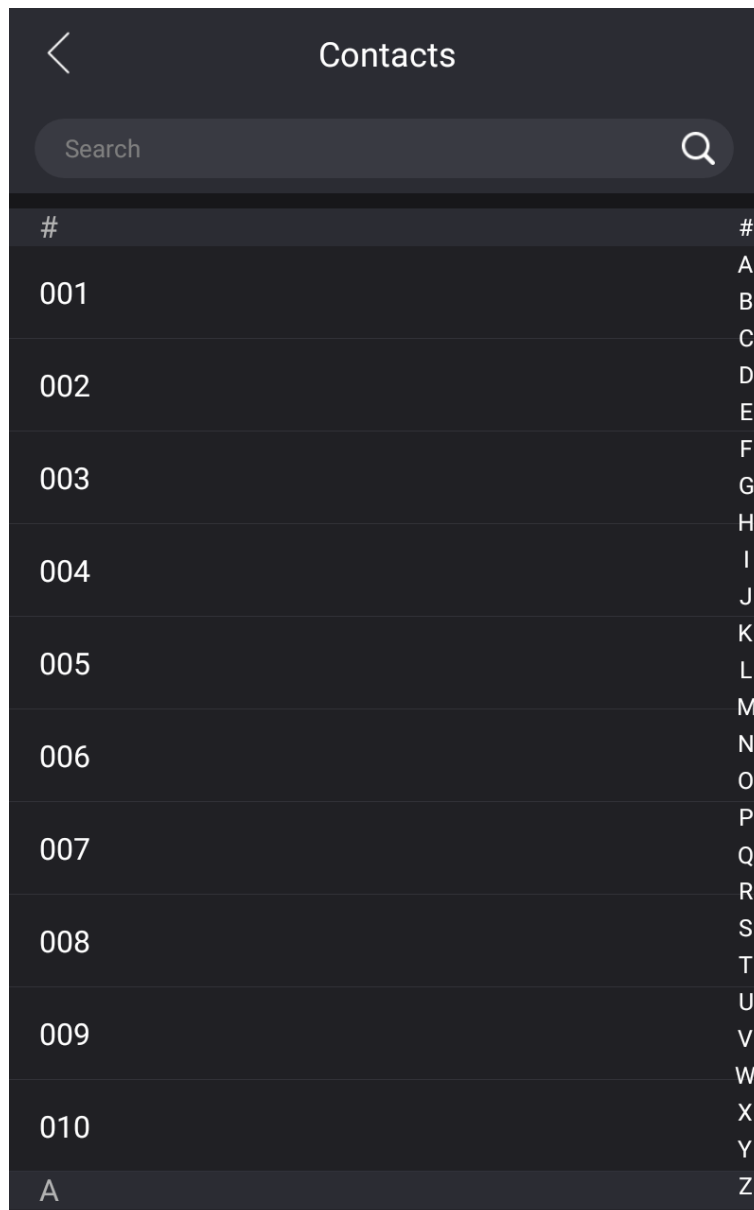


Figure 7-2 Contacts

Select a contact from the list to call. You can enter the name in the search bar or tap the letter on the right side of the screen to find a target contact.

Call Resident from Outer Door Station

On the main page of the outer door station, tap Call to enter the calling page.

Enter **Phase No. + # + Building No. + # + Unit No. + # + Room No.**, and tap Call again to call residents.

Enter **Phase No. + # + Room No.**, and tap Call again to call residents.

7.1.2 Call Center

Refers to to set the calling shortcut key.

Call Center by Calling Menu

If you set call mode as **Calling Menu**.

Tap  on the main/sub door station page to enter the calling page.

Tap  to call management center administrator. Tap cancel button to cancel during calling management center.

Call Center by Shortcut Key

If you set call mode as **Call Center**, you can tap the call button on the main page to call.

7.2 Unlock Door

You can unlock door station in following methods: Unlock by password, unlock by presenting card, unlock by face, and unlock by fingerprint.

7.2.1 Unlock by Password

Tap call button on the main page to enter the calling page.

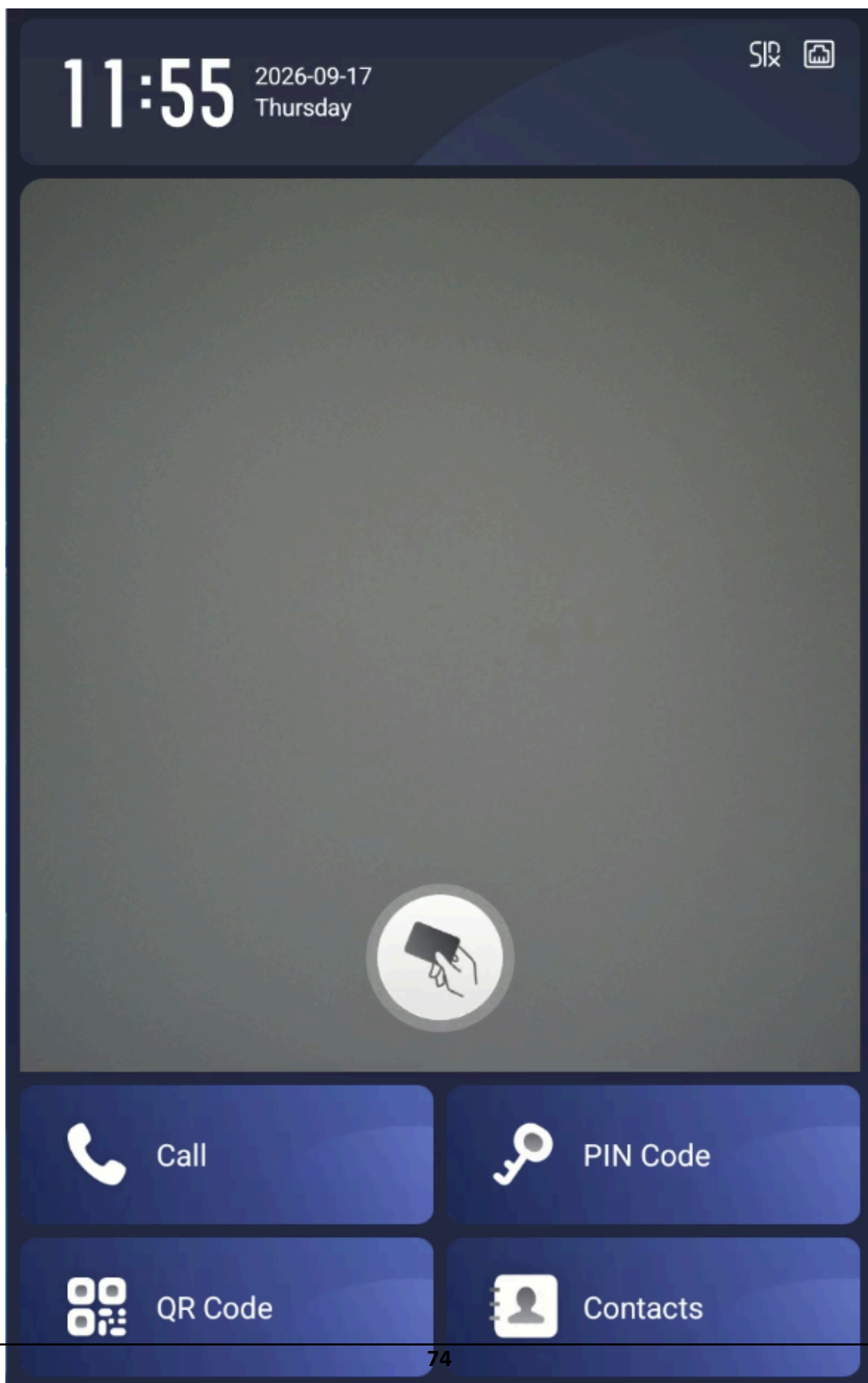


Figure 7-3 Main Page-Auth. Mode

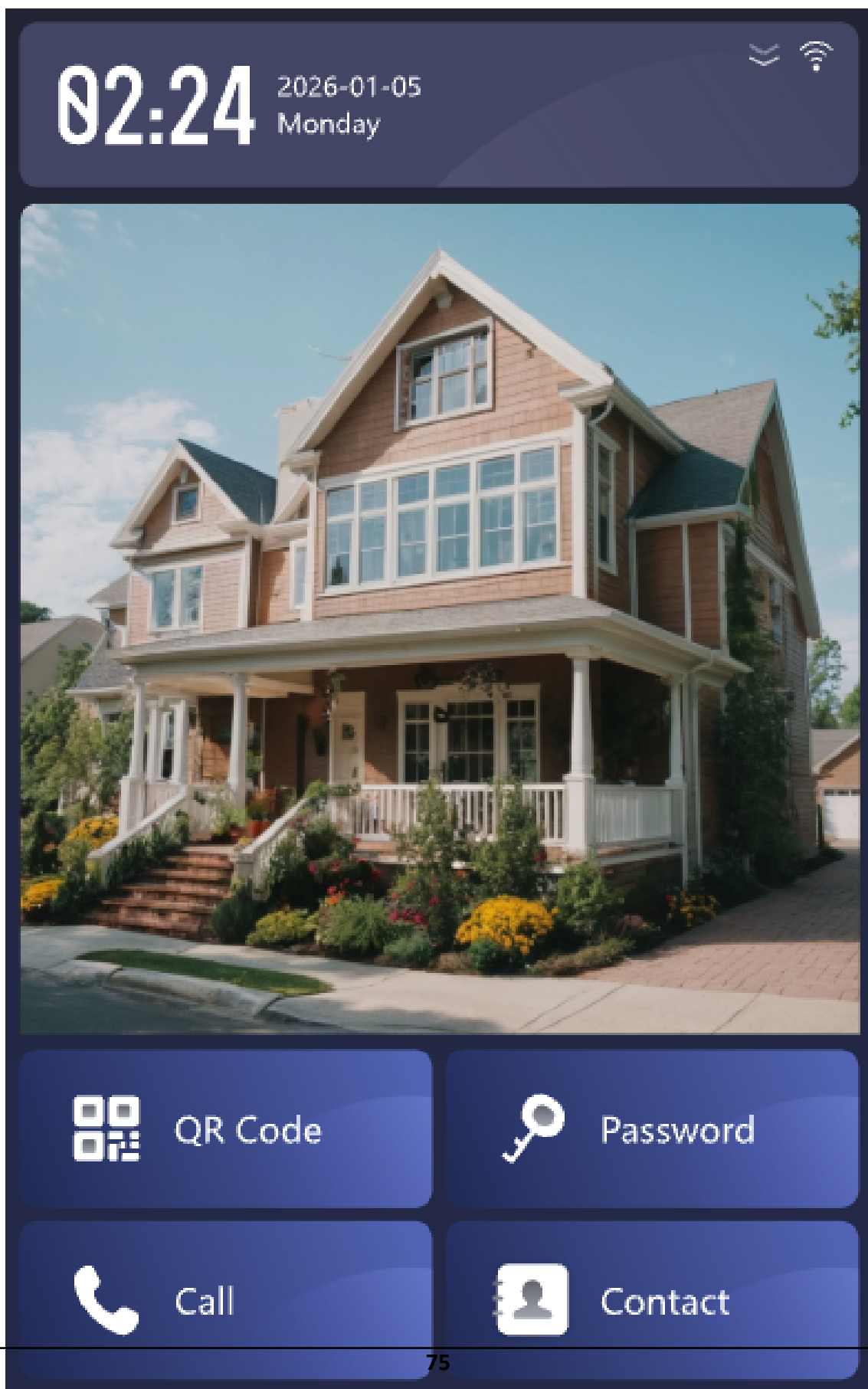


Figure 7-4 Main Page-Ad. Mode

Private/ Public Password: enter Password and tap unlock button.

Resident Password: Enter Room No.+ password and tap unlock button.

Note

User can configure unlock permission via web browser.

The door station supports two locks. You can tap to select which door(s) to open after authentication.

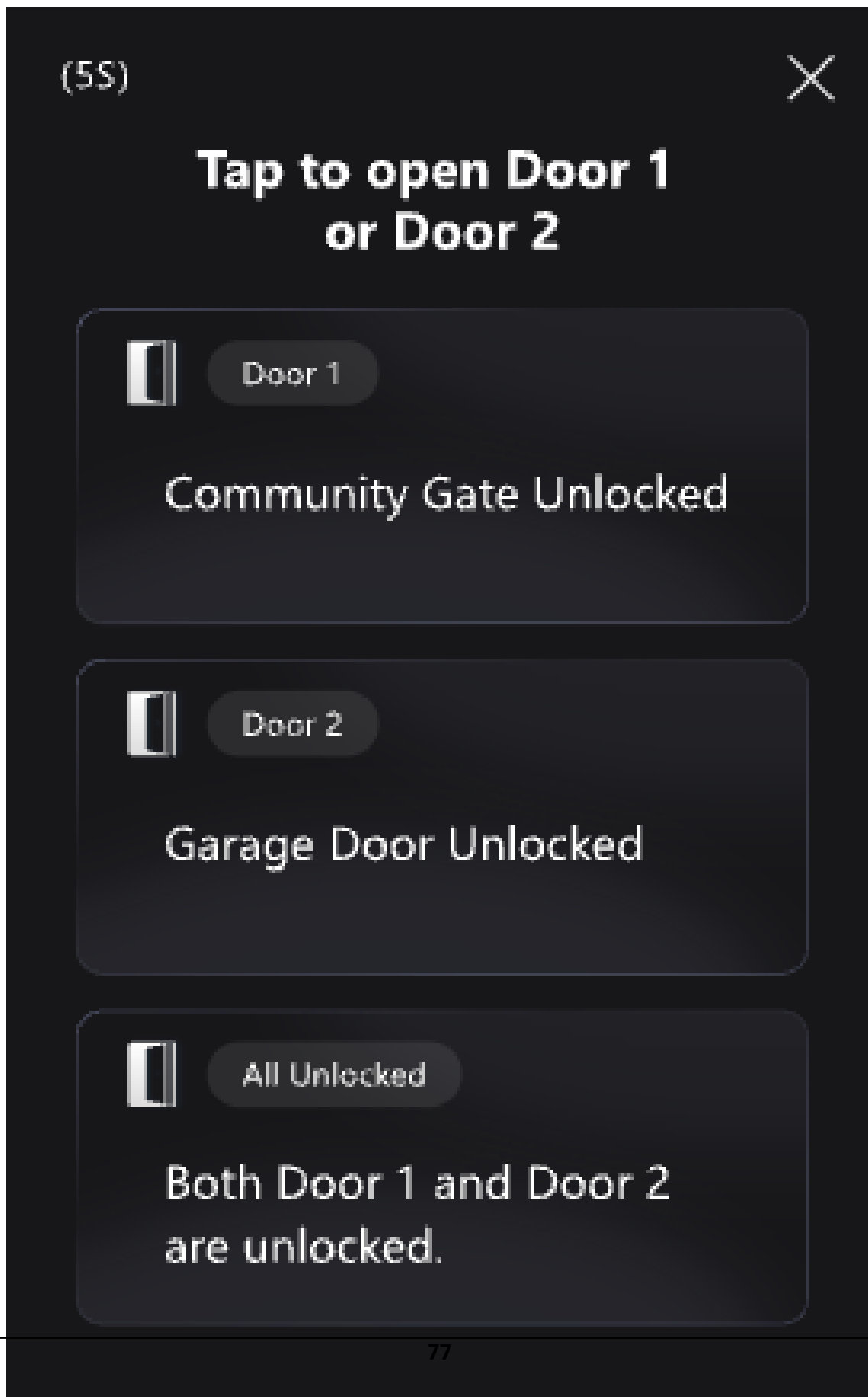


Figure 7-5 Open Two Locks

7.2.2 Unlock by Face



Make sure that you have added your face picture to the device. Refers to the *User Management* for details.

Face forward at the camera to unlock.

7.2.3 Unlock by Presenting Card



Make sure you have issued the card to the device. Refers to User Management for details.

Present the card on the card reading area to unlock.

7.2.4 Unlock by QR Code

Door station supports unlock by QR code. You can generate a QR code through the mobile phone client, and use the door station camera to scan the mobile phone QR code to open the door.

Steps



- Make sure that the door station IP has been added to the indoor station, and the indoor station and the door station can communicate normally.
 - Make sure that the door station is connected to the network.
 - QR code is for visitors only.
-

1. Installing Hik-Central Pro on your PC.
2. Register user accounts according to the prompts, and log in.
3. Follow the prompts to add the indoor station by scanning the QR code/barcode or manually entering the serial number.
4. Enter unlock by QR code page and generate the QR code.
5. On the main page of door station, tap down button to enter the unlock by QR code page.
6. Aim the QR code generated by the phone at the camera and scan the code to open the door.



Note

- It is recommended that when installing the door station, try to select a location that does not cause reflections, otherwise it may affect the QR code scanning. If it is acrylic door station, make sure that the membrane on the surface of the door machine has been torn off.
 - It is recommended to align the mobile phone's QR code with the door station camera horizontally when scanning the QR code.
 - QR code recognition is not supported at night.
-

Chapter 8 Quick Operation via Web Browser

8.1 Select Language

You can select a language for the device system.

Click  in the top right of the web page to enter the **Device Language Settings** page. You can select a language for the device system from the drop-down list.

By default, the system language is English.



Note

After you change the system language, the device will reboot automatically.

8.2 Time Settings

Click  in the top right of the web page to enter the wizard page. After setting device language, you can click **Next** to enter the **Time Settings** page.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address/NTP Port/Interval

You can set the server address, NTP port, and interval.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

8.3 Environment Settings

After activating the device, you should select an application mode for better device application.

Steps

1. Click  in the top right of the web page to enter the wizard page. After setting device language and time, you can click **Next** to enter the **Environment Settings** page.
2. Select **Indoor** or **Other**.

Note

- If you install the device indoors near the window or the face recognition function is not working well, select **Others**.
 - If you do not configure the application mode and tap **Next**, the system will select **Indoor** by default.
 - If you activate the device via other tools remotely, the system will select **Indoor** as the application mode by default.
-

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip environment settings.

8.4 Privacy Settings

Set the picture uploading and storage parameters.

Click  in the top right of the web page to enter the wizard page.

Save Picture When Authenticating

Save picture when authenticating automatically.

Upload Picture When Authenticating

Upload the pictures when authenticating to the platform automatically.

Save Registered Picture

The registered face picture will be saved to the system if you enable the function.

8.5 Administrator Settings

Steps

1. Click  in the top right of the web page to enter the wizard page.
2. Enter the employee ID and name of the administrator.
3. Select a credential to add.

Note

You should select at least one credential.

- 1) Click **Add Face** to upload a face picture from local storage.
-

Note

The uploaded picture should be within 200 K, in JPG、JPEG、PNG format.

- 2) Click **Add Card** to enter the Card No. and select the property of the card.
-

Note

Up to 5 cards can be supported.

8.6 No. and System Network

Steps

1. Click  in the top right of the web page to enter the wizard page. After previous settings, you can click **Next** to enter the **No. and Network System Network** settings page.
2. Set the device type.

Note

- If set the device type as **Door Station**, you can set the **Floor No.**, **Door Station No.**, **Community No.**, **Building No.**, **Unit No.**, **Floor No.**, and **Door Station No.**.
 - If set the device type as **Outer Door Station**, you can set **Outer Door Station No.**, and **Community No.**
-

Device Type

The device can be used as a door station or outer door station. Select a device type from the drop-down list.

Community No.

Set the device community No.

Building No.

Set the device building No.

Unit No.

Set the device unit No.

Floor No.

Set the device installed floor No.

Door Station No.

Set the device installed door station No.

Note

The main door station No. is 0, and the sub door station No. ranges from 1 to 16.

Outer Door Station No.

Set the device installed outer door station No.

Note

The No. ranges from 1 to 99.

3. Set the video intercom network parameters.

Registration Password

Set the registration password of the main station for communication. Set the registration password of the main station for communication.

Main Station IP

Enter the main station's IP address that used for communication.

Private Server IP

Refers to the SIP server IP. Enter the main station's IP address that used for communication. At this time the main station is used as a SIP server. Other intercom devices should registered to this server address to realize communication.

Enable Protocol 1.0

If enabled, the door station can be registered to the main station by old protocol version. If disabled, the door station can be registered to the main station by new protocol version.

4. Click **Complete** to save the settings after the configuration.

Chapter 9 Operation via PC Web

9.1 Login Web Browser

You can log into the Web browser for device configuration.

Steps

1. Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.
2. Enter the device user name and the password. Click **Login** to login to the page.

9.2 Forget Password

If you forget the password when logging in, you can change the password by email address or security questions.

On the login page, click **Forget Password**.

Select **Verification Mode**.

Security Question Verification

Answer the security questions.

E-mail Verification

1. Export the QR code and send it to ***pw_recovery@hikvision.com*** as attachment.
2. You will receive a verification code within 5 minutes in your reserved email.
3. Enter the verification code into the verification code field to verify your identification.

Click **Next**, create a new password and confirm it.

9.3 Overview

You can view the live video of the device, real-time event, linked devices, person information, network status, basic information, and device capacity.

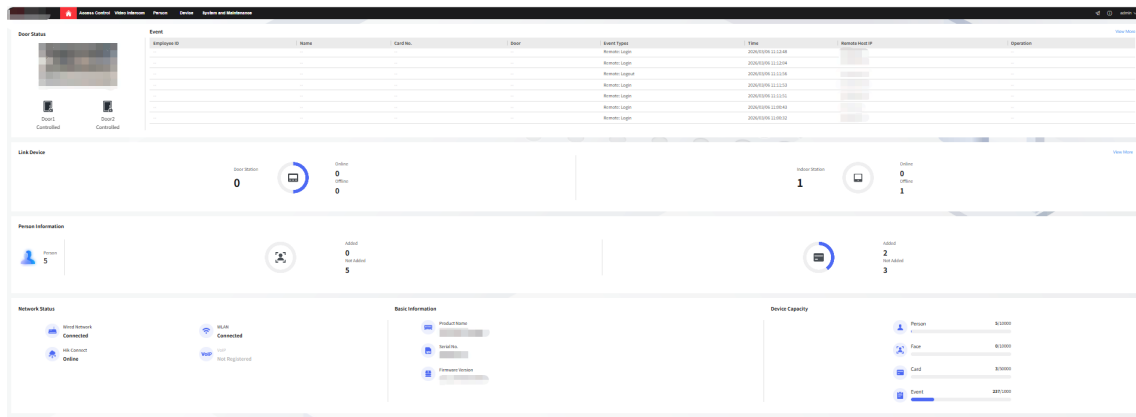


Figure 9-1 Overview Page

Function Descriptions:

Door Status

Click  to view the device live view.



Set the volume when starting live view.



Note

If you adjust the volume when starting two-way audio, you may hear a repeated sounds.



You can capture image when starting live view.



Select the streaming type when starting live view. You can select from the main stream and the sub stream.



Full screen view.



The door status is open/closed/remaining open/remaining closed.

Controlled Status

You can select open/closed/remaining open/remaining closed status according to your actual needs.

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the search conditions, including the event type, employee ID, the name, the card No., the time, the unit. Click **Search**. The results will be displayed on the right panel.

Person Information

You can view the added and not added information of person face, fingerprint and card.

Network Status

You can view the connected and registered status of wired network, VoIP and cloud service.

Basic Information

You can view the model, serial No. and firmware version.

Device Capacity

You can view the Person, Face, Card, and Event capacity.

9.4 Person Management

Click **Person** → **+Add** to enter the Add Person page. You can add the person's information, including the basic information, certificate, authentication and settings at this page.

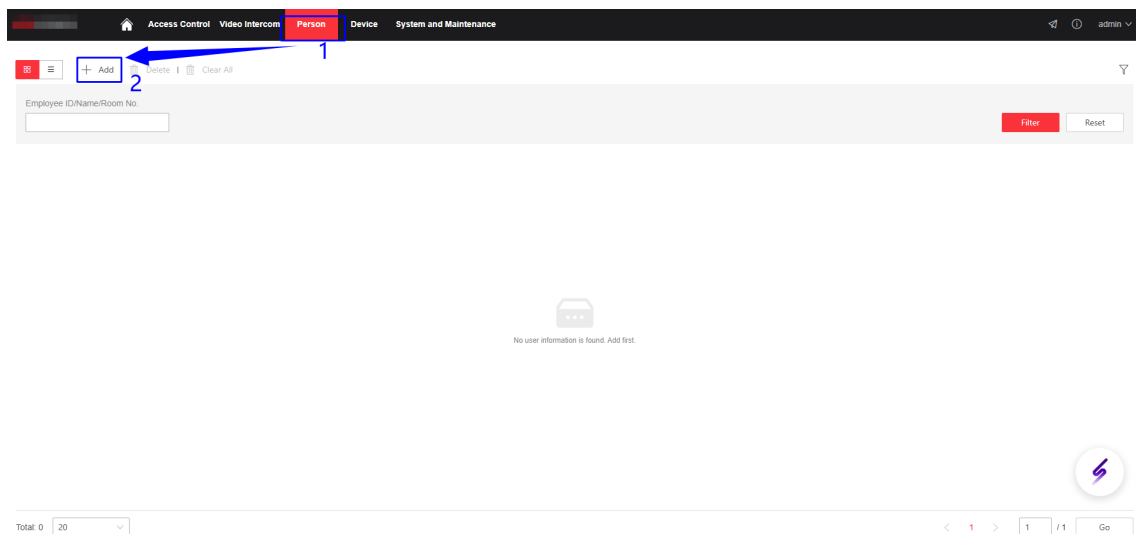
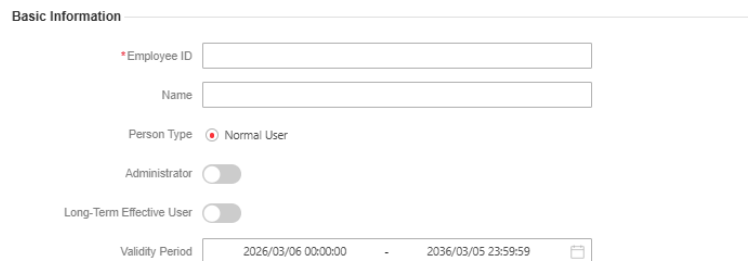


Figure 9-2 Person Page Overview

Add Basic Information

Add the person's basic information, including the employee ID, the person's name, floor No., room No., etc.



The 'Basic Information' form contains the following fields and controls:

- Employee ID:** A text input field with an asterisk indicating it is required.
- Name:** A text input field.
- Person Type:** A radio button selection with 'Normal User' selected.
- Administrator:** A toggle switch, currently turned off.
- Long-Term Effective User:** A toggle switch, currently turned off.
- Validity Period:** A date range selector showing '2026/03/06 00:00:00' to '2036/03/05 23:59:59' with a calendar icon on the right.

Figure 9-3 Basic Information

Click **Save** to save the settings.

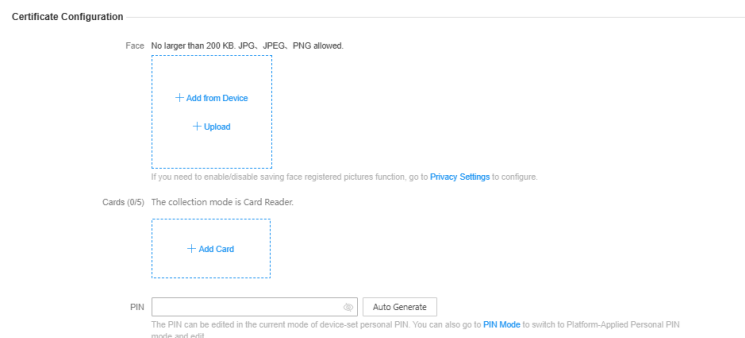
Set Validity Period

Enable **Long-Term Effective User**, or set **Start Time** and **End Time** and the person can only has the permission within the configured time period according to your actual needs.

Click **Save** to save the settings.

Authentication Settings

Set the authentication type. You can choose from face, cards, and pin configuration.



The 'Certificate Configuration' form includes the following sections:

- Face:** A dashed box containing '+ Add from Device' and '+ Upload' buttons. A note above states 'No larger than 200 KB, JPG, PNG allowed.' A note below states 'If you need to enable/disable saving face registered pictures function, go to [Privacy Settings](#) to configure.'
- Cards (0/5):** A dashed box containing '+ Add Card' button. A note above states 'The collection mode is Card Reader.'
- PIN:** A text input field with an 'Auto Generate' button. A note below states 'The PIN can be edited in the current mode of device-set personal PIN. You can also go to [PIN Mode](#) to switch to Platform-Applied Personal PIN mode and edit.'

Figure 9-4 Certificate Configuration

Click **Add** to add the person. Or you can click **Save and Continue** to add the next person.

Add Face Picture

Click + to upload a face picture from the local PC or from device.

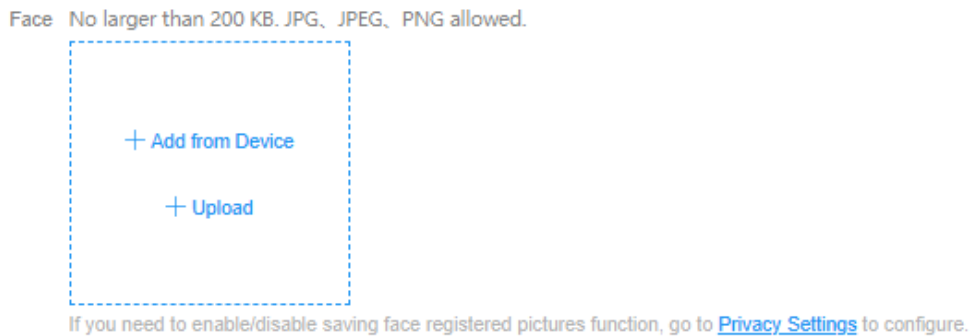


Figure 9-5 Add Face Picture

Note

The picture format should be JPG or JPEG or PNG, and the size should be less than 200 K.

Add Card

Click **+ Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.

Note

Up to 5 cards can be added.

Generate PIN

You can click **Auto Generate** to get a random pin.

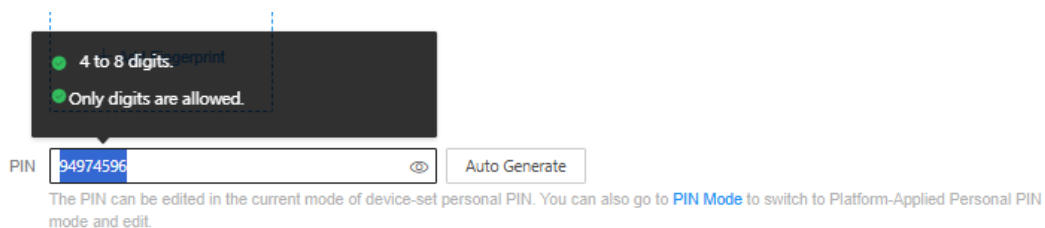


Figure 9-6 PIN

Click **Add** to add the person. Or you can click **Save and Continue** to add the next person.

No. Settings

Click **+ Add**. Then you can configure the Room No. and Floor No. for this newly-added person.

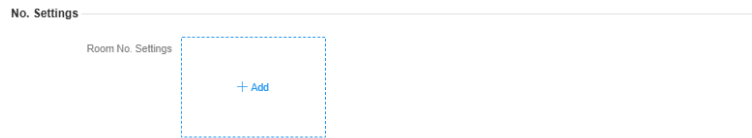


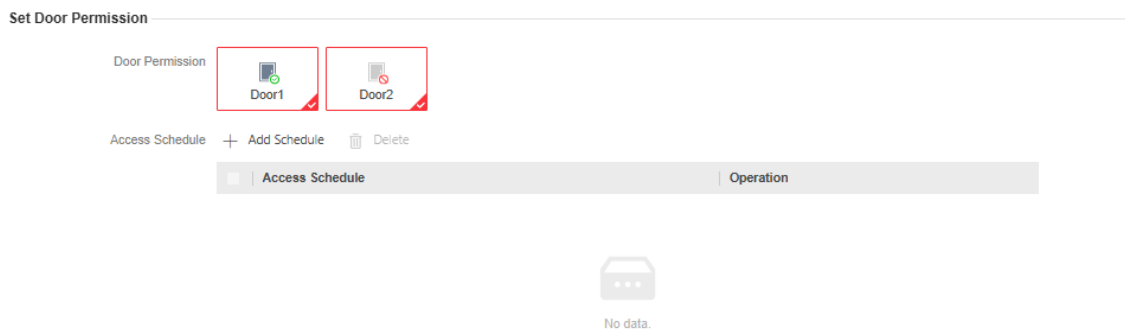
Figure 9-7 No. Settings

You can set the room No. and Floor No. for the added person here.

This helps to record visitor entrance information and can help the property management team to contact the visitor.

Set Door Permission

You can add schedule and door permission for each person.



Note

Just select an access schedule from your saved template and click **OK**.

Click **Add** to add the person. Or you can click **Save and Continue** to add the next person.

9.5 Device Management

You can manage the linked device on the page.

Click **Device** to enter the settings page.

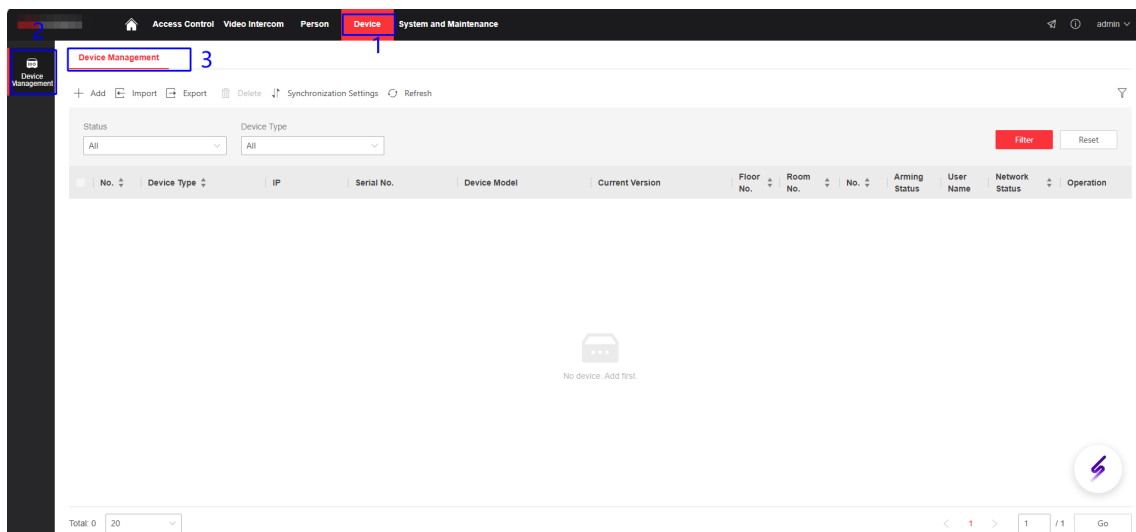


Figure 9-8 Device Management

Add Device

- Click **+Add** to add the indoor station or sub door station. Enter the parameters and click **Add** to add.
- Click **Import**. Enter the information of the device in the template to import devices in batch.

Export

Click **Export** to export the information to the PC.

Delete

Select the device and click **Delete** to remove the selected device from the list.

Synchronization Settings

Click **Synchronization Settings** and enable **Synchronize**. If enabled, the current device's settings will be synchronized to other devices.

Refresh

Click **Refresh** to get the device information.

Optional: Set Device Information.

- Click  to edit device information.
- Click  to delete device information from the list.
- Select **Status** and **Device Type** to search devices.

9.6 Maintenance and Security

9.6.1 Set Protocol Testing

Select a protocol address, and enter the protocol to test. You can debug the device according to the response header and returned value.

Go to **System and Maintenance → Maintenance → Device Debugging → Protocol Testing** .

Select a protocol address, and enter the protocol. Click **Execute**.

Debug the device according to the response header and returned value.

9.6.2 Network Diagnosis via PC Web

Enter the device IP address or domain name, you can perform PING settings. Debug the network according to the PING result.

Go to **System and Maintenance → Maintenance → Device Debugging → Network Diagnosis** .

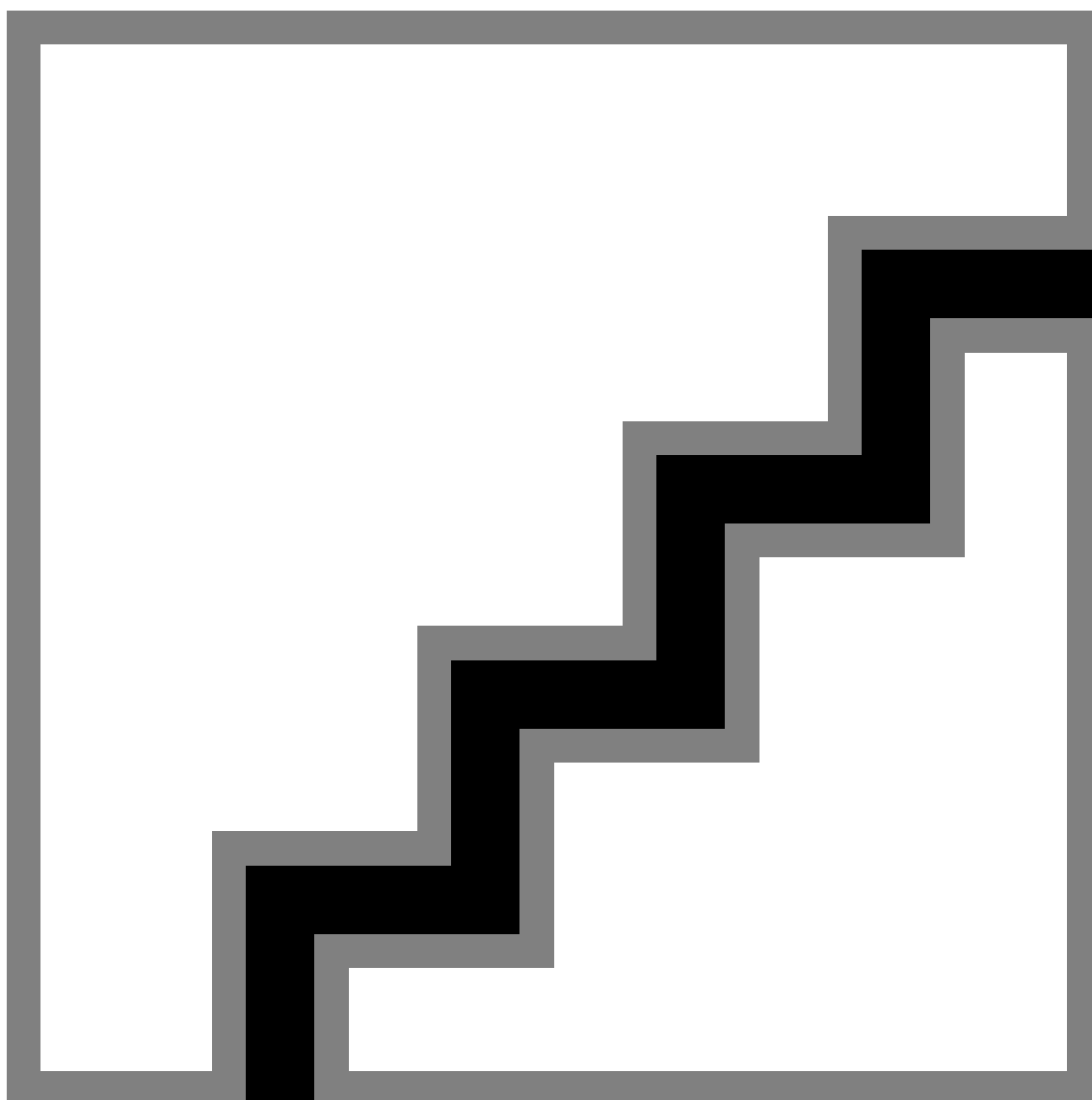


Figure 9-9 Network Diagnosis

Enter the device IP for PING operation, select the network connection mode, PING duration, and Ping data package size (default parameter is recommended.) Click **Diagnose**. The result will be displayed in **PING Result**.

9.6.3 Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device version.

Reboot Device

Click **System and Maintenance** → **Maintenance** → **Restart** .

Click **Restart** to reboot the device.

Upgrade

Click **System and Maintenance → Maintenance → Upgrade** .

Upgrades include two types: device main program upgrades and touchscreen firmware upgrades. Select an upgrade type from the drop-down list. Click  and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.

If the device has been connected to Hik-Connect and network, when there is a new installation package in Hik-Connect, you can click **Upgrade** after Online Update to upgrade the device system.



Note

Do not power off during the upgrading.

Restore Parameters

Click **System and Maintenance → Maintenance → Backup and Reset** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Restore

The device will restore to the default settings, except for the device IP address and the user information.

Import and Export Parameters

Click **System and Maintenance → Maintenance → Backup and Reset** .

Export

Click **Export** to export the device parameters.



Note

You can import the exported device parameters to another device.

Import

Click  and select the file to import. Click **Import** to start import configuration file.

9.6.4 Device Debugging

You can set device debugging parameters.

Steps

1. Click **System and Maintenance → Maintenance → Device Debugging** .

Log for Debugging Protocol Testing Network Diagnosis

SSH

Enable SSH ☐

ADB

ADB Remote Control ☐

Print Log

Print Log

Capture Network Packet

Capture Packet Duration s

Capture Network Packet

Figure 9-10 Log for Debugging

2. You can set the following parameters.

Enable SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

Note

You need to enter admin password if you want to enable SSH debugging.
The SSH protocol provides encrypted communication, ensuring data security during the debugging process and preventing the leakage of sensitive information.

ADB

Enable **ADB Remote Control** for actual needs.

Print Log

You can click **Export** to export log.

Capture Network Packet

You can set the **Capture Packet Duration**, and click **Start Capture** to capture network data.

3. Click **Save**.

9.6.5 View Log via PC Web

You can search and view the device logs.

Go to **System and Maintenance → Maintenance → Log**.

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

9.6.6 Security Audit Log

Steps

1. Click **System and Maintenance → Maintenance → Log → Security Audit Log** to enter the page.
2. Slide to enable **Log Upload Server**, **Encrypt Transmission** and **Verify Certificate**.

Log Upload Server ☒

Encrypt Transmission ☒

Verify Certificate ☒

Server Configuration

* Log Server Address

* Log Server Port

* Uploading Cycle h

Save

3. You can edit **Log Server Address**, **Log Server Port** and **Uploading Cycle**.



Note

The range of **Uploading Cycle** is 1 to 24 hour.

9.6.7 Advanced Settings

View Version Information

Click **System and Maintenance** → **Maintenance** → **Advanced Settings** → , then enter admin password to visit the page.

Advanced Configuration

Biometrics

Custom Anti-Spoofing Detection

☐

ⓘ

 Lock Face for Anti-Spoofing Protection

☒

Lock Duration

2

min

⬆

⬇

⬇

⬆

Cancel Locking Face for Anti-Spoofing Protection

Unlock

If the device is locked, click the button to unlock.

Version Information

BSP Version

V1.1.0 build20260811

DSP Version

V2.10.1 build 20260818

Engine Version

V9.2.0 build20251128

Face Algorithm Version

V9.0.212 build20251113

Save

Figure 9-11 Version Information in Advanced Configuration

Here you can view version information including BSP Version, DSP Version, Engine Version and Face Algorithm Version.

Biometrics Settings

Steps

1. Click **System and Maintenance** → **Maintenance** → **Advanced Settings** → , then enter admin password to visit the page.

Biometrics

Custom Anti-Spoofing Detection ☒

Anti-Spoofing Detection Level General

① Anti-Spoofing Detection Threshold 90

① Anti-Spoofing Detection Threshold of Face with Mask 90

① Lock Face for Anti-Spoofing Protection ☒

Lock Duration min

Cancel Locking Face for Anti-Spoofing Protection If the device is locked, click the button to unlock.

Version Information

BSP Version

DSP Version

Engine Version

Face Algorithm Version

Anti-Spoofing Detection Algorithm Version

Figure 9-12 Biometrics Settings in Advanced Configuration

2. Slide to enable **Custom Anti-spoofing Detection**, and set **Anti-Spoofing Detection Threshold** and **Anti-Spoofing Detection Threshold of Face with Mask**.

Biometrics

Custom Anti-Spoofing Detection ☒

Anti-Spoofing Detection Level General

① Anti-Spoofing Detection Threshold 90

① Anti-Spoofing Detection Threshold of Face with Mask 90

① Lock Face for Anti-Spoofing Protection ☒

Lock Duration min

Cancel Locking Face for Anti-Spoofing Protection

If the device is locked, click the button to unlock.

Figure 9-13 Biometrics Details



Note

Anti-Spoofing Detection Threshold

Range: 1 to 100. When you select a smaller value, the detection result will be less accurate and the passing efficiency will be higher.

Anti-Spoofing Detection Threshold of Face with Mask

Range: 1 to 100. When you select a smaller value, the detection result will be less accurate and the passing efficiency will be higher.

-
- Lock Face for Anti-Spoofing** is enabled by default. If enabled, the face will be locked for anti-spoofing protection after the failed attempt limit of anti-spoofing detection has been reached.
 - Set **Lock Duration**. (Range: 1 ~ 240 min)
 - Optional**: If the device is locked, you can click **Unlock** to cancel locking face for anti-spoofing protection.
 - Click **Save** to enable the settings.

9.6.8 Security Mode Settings

Set the security mode for logging in the client software.

On the Device for Management page, click **System and Maintenance** → **Safe** → **Security Service** to enter the page.

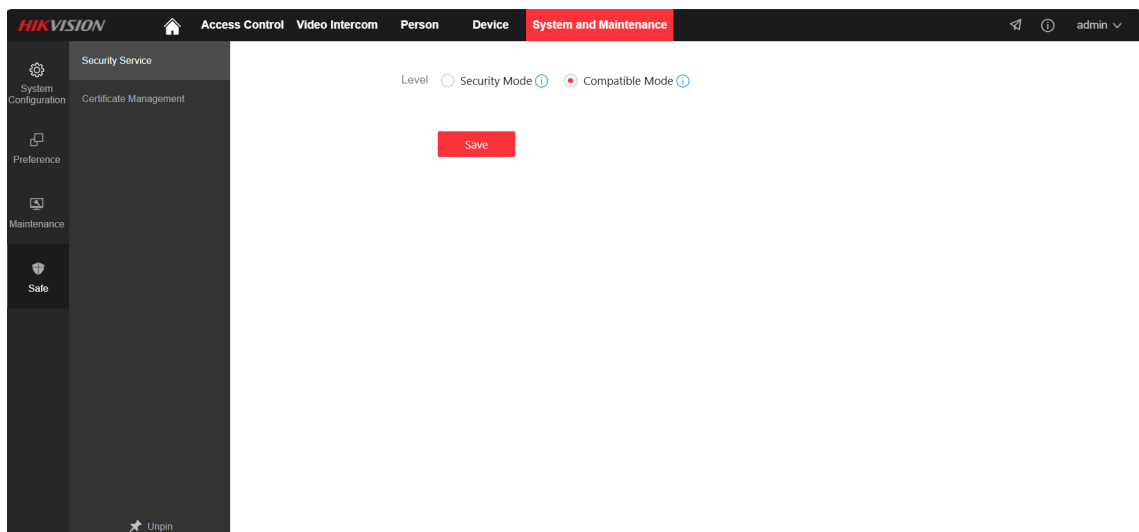


Figure 9-14 Security Service

Click to select a security mode and click **Save**.

Security Mode

High security level for user information verification when logging in the client software.

Compatible Mode

The user information verification is compatible with the old client software version when logging in.

9.6.9 Certificate Management

It helps to manage the server/client certificates and CA certificate.



Note

The function is only supported by certain device models.

Create and Import Self-signed Certificate

Steps

1. Go to **System and Maintenance** → **Safe** → **Certificate Management**.
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

The created certificate is displayed in the **Certificate Details** area.

The certificate will be saved automatically.

6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
 - 1) Select a certificate type in the **Import Key** area, and select a certificate from the local, and click **Import**.
 - 2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Import**.

Import Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. In the **Import Key** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Import**.

Import CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **System and Maintenance → Safe → Certificate Management** .
2. Create an ID in the **Import CA Certificate** area.



Note

The input certificate ID cannot be the same as the existing ones.

3. Upload a certificate file from the local.
4. Click **Import**.

9.7 Set Screen Display

You can set the contacts mode and standby image.

Steps

1. Tap **System and Maintenance → Preference → Screen Display** to enter the setting page.

Screen Display Notice Publication

Standby Image

Time to Enter Standby 30 s

Contacts Mode

☒ Name Display Mode

☒ Real Name Mode
Show User Name and Room No.

☐ Anonymous Mode
Show Room No. and Desensitized Name

Save

Figure 9-15 Screen Display

2. You can set **Time to Enter Standby**. Range: 5~30s.
3. Select **Name Display Mode** as **Real Name Mode** or **Anonymous Mode**.

Real Name Mode

Show User Name and Room No. in the local contacts.

Anonymous Mode

Show Desensitized Name and Room No. in the local contacts.

9.7.1 Notice Publication

You can set the notice publication for the device.

Click **System and Maintenance → Preference → Notice Publication** .

Theme Management + Add Program | Media Library Management

Edit Name Delete Program

No program.

Save

Figure 9-16 Notice

Theme Management

Click **Media Library Management → +** to upload the picture from the local PC.



Note

Only the format of JPG and JPEG is supported. Each picture should be smaller than 1 MB with resolution up to 1920*1280.

Add Program

Click **+** **Add Program**. You can set the program name and select program type.

Picture

If you select picture, you can click **+** to add picture.

Welcome Message

If you select welcome message, you can set the template, content, font size and color of main and sub title. You can also custom the background picture.

Slide Show Interval

Drag the block or enter the number to set the slide show interval. The picture and video will be changed according to the interval.

Schedule Management

After you have created a theme, click **+** **Add** on the schedule management panel. Select the drawn schedule, and you can edit the exact start and end time.

Select the drawn schedule and you can click **Clear** or **Clear All** to delete the schedule.

Click **Releasing Record** to view task name, releasing status, etc.

Click **View Terminal Schedule Info.** to view terminal name, schedule name, etc.

9.8 Configuration

9.8.1 System Settings

View Device Information via PC Web

View the device name, device No., language, model, serial No., version, number of channels, IO input number, IO output number, local RS-485 number, register number, number of alarm inputs, and device capacity, etc.

Click **System and Maintenance** → **System Configuration** → **System** → **System Settings** → **Basic Information** to enter the configuration page.

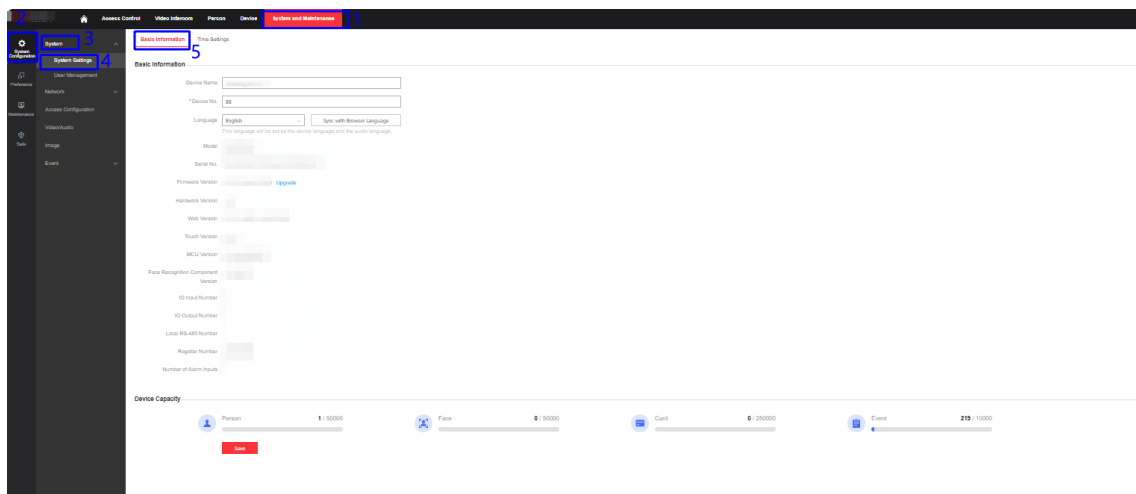


Figure 9-17 Basic Information

You can view the device name, device No., language, model, serial No., version, number of channels, IO input number, IO output number, local RS-485 number, register number, number of alarm inputs, and device capacity, etc.

Click **Upgrade** in the Firmware Version, you can go to the upgrade page to upgrade the device.

Set Time

Set the device's time zone, synchronization mode, server address, NTP port, and interval.

Click **System and Maintenance** → **System Configuration** → **System** → **System Settings** → **Time Settings**.

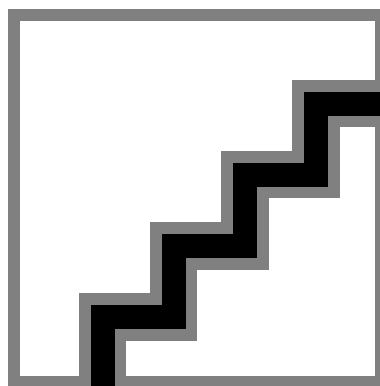


Figure 9-18 Time Settings

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address Type/Server Address/NTP Port/Interval

You can set the server address type, server address, NTP port, and interval.

Set DST

Steps

1. Click **Configuration** → **System** → **System Settings** → **Time Settings** .

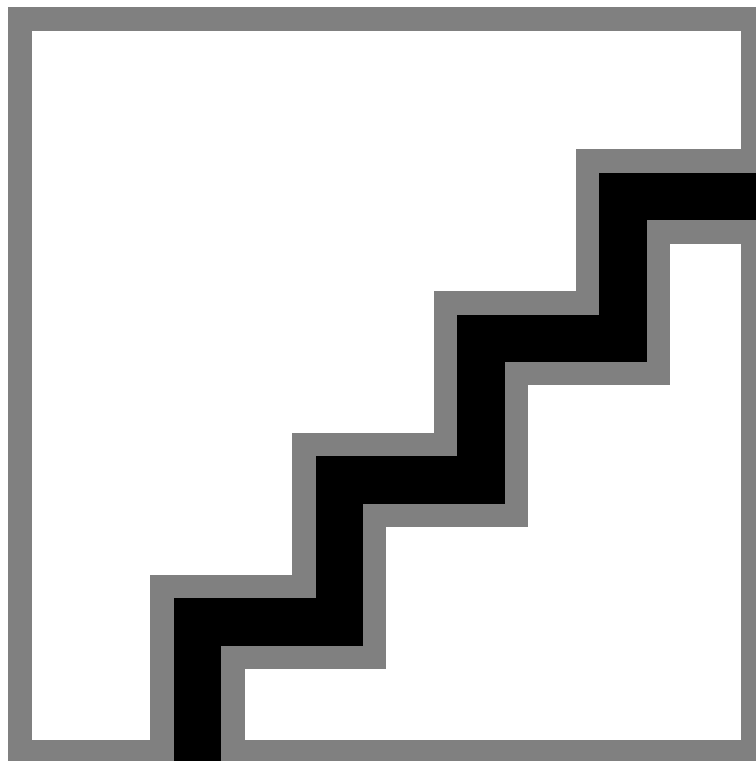


Figure 9-19 DST Page

2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

9.8.2 User Management

Change Administrator's Password

Steps

1. Click **System and Maintenance** → **System Configuration** → **System** → **User Management** → **User Management** .

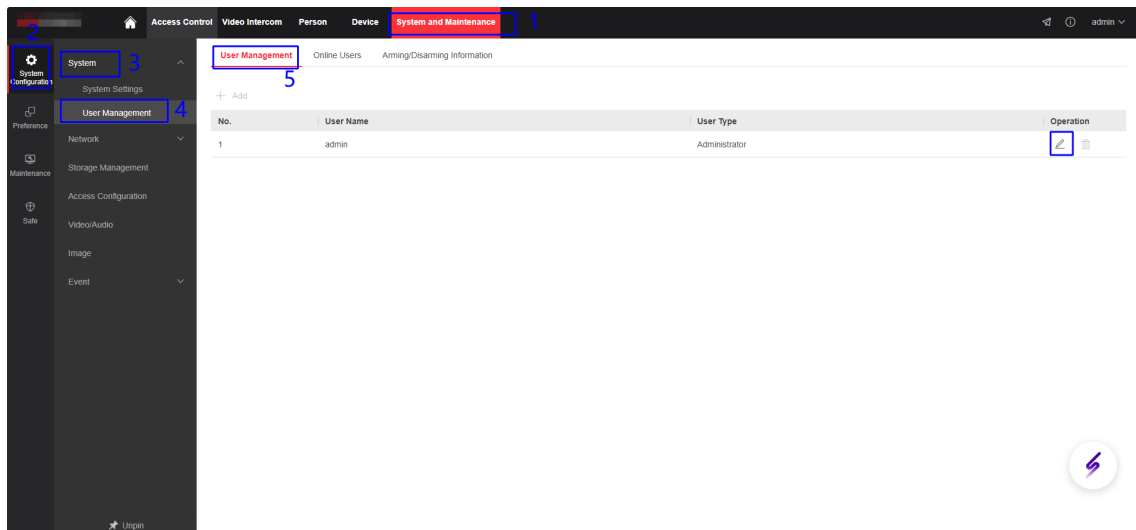


Figure 9-20 User Management

2. Click .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **Save**.

Note

- The password should be 8 to 16 characters.
- The password should contain at least 2 of the following types: digits, lowercase letters, uppercase letters and special characters.
- The username cannot be the same as the password. Password cannot be inverted write of user name.
- The password strength of the device can be automatically checked. In order to increase the security of your product, we highly recommend you change the password of your own choosing. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.

- Proper configuration of all passwords and other security settings is the responsibility of the service provider and/or end-user.
-

Online Users

The information of users logging into the device is shown.

Go to **System and Maintenance → System Configuration → System → User Management → Online Users** to view the list of online users.

View Device Arming/Disarming Information via PC Web

View device arming type and arming IP address.

Go to **System and Maintenance → System Configuration → System → User Management → Arming/Disarming Information**.

You can view the device arming/disarming information. Click **Refresh** to refresh the page.

9.8.3 Network Settings

Set Basic Network Parameters

Click **System and Maintenance → System Configuration → Network → Network Settings → TCP/IP**.

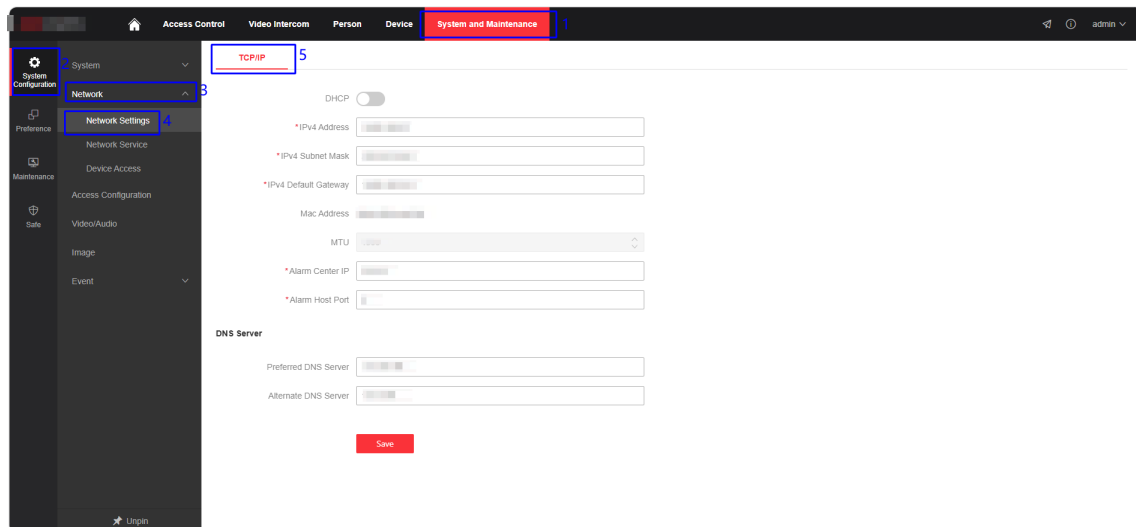


Figure 9-21 TCP/IP Settings

Set the parameters and click **Save** to save the settings.

DHCP

If disable the function, you should set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, preferred DNS server and the Alternate DNS server.

If you check the function, the system will allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway, preferred DNS server and the Alternate DNS server automatically.

Alarm Center IP and Alarm Host Port

Used to report door station alarm events to the designated alarm center or management platform.

DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Wi-Fi Settings

Some models support Wi-Fi function.

Steps

1. Click **System and Maintenance** → **System Configuration** → **Network** → **Network Settings** → **Wi-Fi** to enter the settings page.

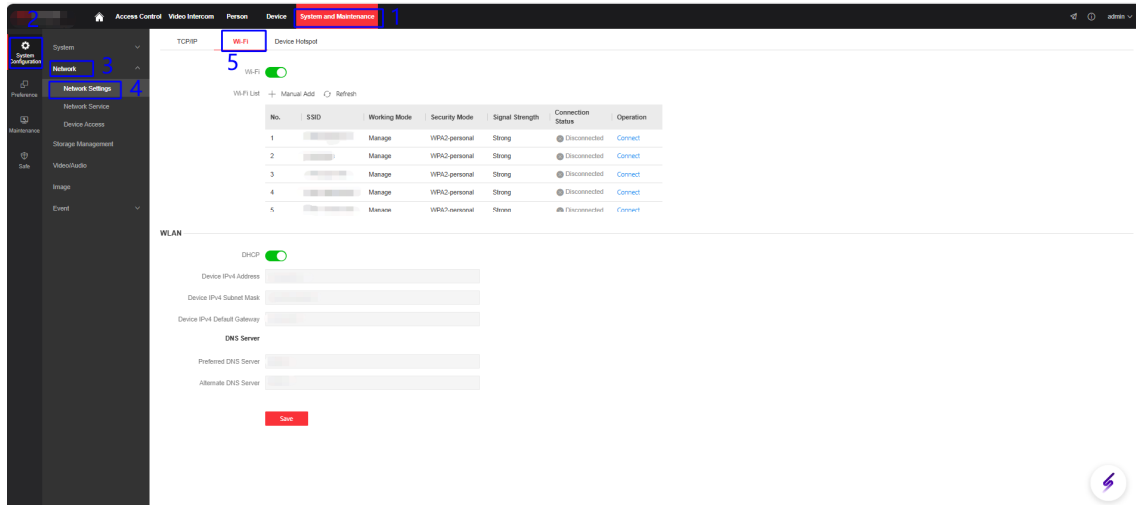


Figure 9-22 Wi-Fi

2. Enable **Wi-Fi**.
3. Click **+ Manual Add**, and set corresponding parameters and **Password** of the Wi-Fi.
 - 1) Enter the **SSID**.
 - 2) Select **Security Mode**.
 - 3) Click **Save**.
 - 4) **Optional**: Click **Refresh** to get the present information.
 - 5) Click **Connect**.
4. **Optional**: Set **WLAN**.
 - 1) Set the **WLAN** parameters.

Enable DHCP

Enable **DHCP** to **Auto DNS**, the device will allocate the IP and DNS automatically.

Disable DHCP

Manually set the IP and DNS server.

- 2) Tap **Save**.

Device Hotspot

Only some models support this function.

Steps

1. Click **Network** → **Network Settings** → **Device Hotspot** .

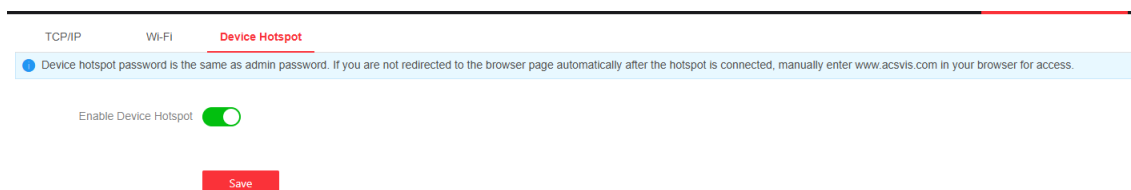


Figure 9-23 Device Hotspot

2. Slide to enable/disable device hotspot.



Note

Device hotspot password is the same as admin password. If you are not redirected to the browser page automatically after the hotspot is connected, manually enter www.acsvs.com in your browser for access.

3. Click **Save**.

Set Port Parameters

Set the HTTP, HTTPS, RTSP and Server port parameters.

Click **System Configuration** → **Network** → **Network Service** → **HTTP(S)** .

The screenshot shows a configuration interface for a Video Intercom D Series Android Door Station. At the top, there are four tabs: **HTTP(S)** (highlighted in red), RTSP, FTP, and WebSocket(s). Below the tabs, there are three main sections: HTTP, HTTPS, and Web Authentication.

HTTP Section:

- Enable: A green toggle switch is turned on.
- Enabling HTTP may cause security problems.
- HTTP Port: A dropdown menu showing 80.

HTTPS Section:

- Enable: A green toggle switch is turned on.
- HTTPS Port: A dropdown menu showing 443.

Web Authentication Section:

- Digest Algorithm: Three radio buttons are present: MD5 (unselected), SHA256 (unselected), and MD5/SHA256 (selected).
- Digest algorithm applies to both HTTP and HTTPS.

At the bottom of the Web Authentication section, there is a red **Save** button.

Figure 9-24 HTTP(S)

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter ***http://192.0.0.65:81*** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

Web Authentication

You can select **Digest Algorithm** as **MD5**, **SHA256** or **MD5/SHA256**.

Digest algorithm applies to both HTTP and HTTPS.



Note

- MD5: A widely used cryptographic hash function that produces a 128-bit hash value. It is fast but considered less secure compared to SHA256.
 - SHA256: A more secure cryptographic hash function that produces a 256-bit hash value. It offers stronger protection against collisions and brute-force attacks.
 - MD5/SHA256: A combined mode that supports both algorithms, allowing the device to accept authentication requests using either MD5 or SHA256. This ensures compatibility with older clients while still enabling stronger security when supported.
-

Click **System Configuration** → **Network** → **Network Service** → **RTSP** .

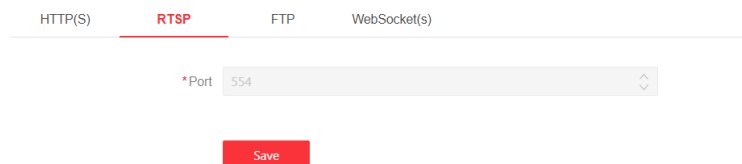


Figure 9-25 RSTP

RTSP

It refers to the port of real-time streaming protocol.

Click **System Configuration** → **Network** → **Device Access** → **SDK Server** .

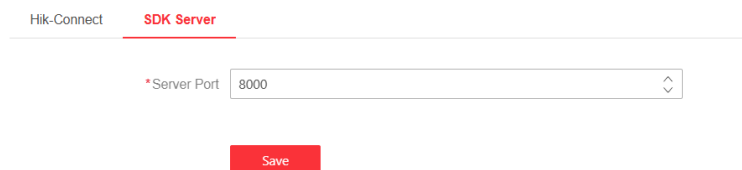


Figure 9-26 SDK Server

SDK Server

It refers to the port through which the client adds the device.

Platform Access

Platform access provides you an option to manage the devices via platform.

Steps

1. Click **System Configuration** → **Network** → **Device Access** → **Hik-Connect** to enter the settings page.



Note

Hik-Connect is an application for mobile devices. With the App, you can view live image of the device, receive alarm notification and so on.

2. Check **Enable** to enable the function.
3. **Optional:** Check the checkbox of **Custom**, and you can set the server address by yourself.
4. Enter the server IP address, and verification code.

Note

6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

5. Enter the verification code.
6. You can also click **More Configure** to adjust **Network Connection Priority**.

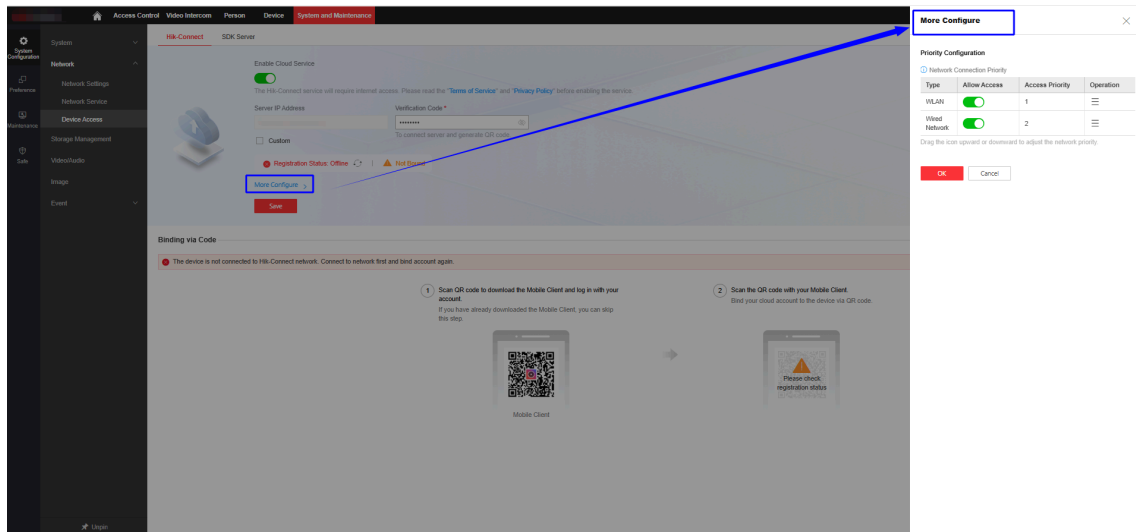


Figure 9-27 More Configure

7. Bind an account.
Binding via Code: Take your phone, open the app, then scan the QR code at the back of your device to bind the account.
8. Click **Save** to enable the settings.

Set WebSocket(s) via PC Web

View WebSocket and WebSockets port.

Go to **System and Maintenance** → **System Configuration** → **Network** → **Network Service** → **WebSocket(s)**.

View WebSocket and WebSockets port.

FTP Settings

You can configure FTP (File Transfer Protocol) parameters.

Steps

1. Click **Network** → **Network Service** → **FTP** to enter the settings page.

HTTP(S)	RTSP	FTP	WebSocket(s)
---------	------	------------	--------------

Enable FTP ☒

Server Type Server IP Address ▼

*Server IP Address

*Port

Anonymous ☐

*User Name

*Password

*Password Confirm

Directory Structure Save in the child directory ▼

Parent Directory Building No. & Unit No. ▼

Child Directory Time ▼

*Delimiter

Named Item Option1 Option2 Option3 Option4 Option5 Option6

Named Item Option1 ▼

Named Element Time ▼

Save

Figure 9-28 FTP Settings

2. Enable **FTP**.
3. Select **Server Type**.
4. Enter **Server IP Address** and **Port**.
5. Configure the FTP Settings, and the user name and password are required for the server login.



Note

If you enable **Anonymous**, you will not need to set user name and password.

6. Set the **Directory Structure**, **Parent Directory** and **Child Directory**.
7. Set naming rules.
8. Click **Save** to enable the settings.

9.8.4 Set Video and Audio Parameters

Set the image quality and resolution.

Set Video Parameters

Click **System and Maintenance** → **System Configuration** → **Video/Audio** → **Video** .

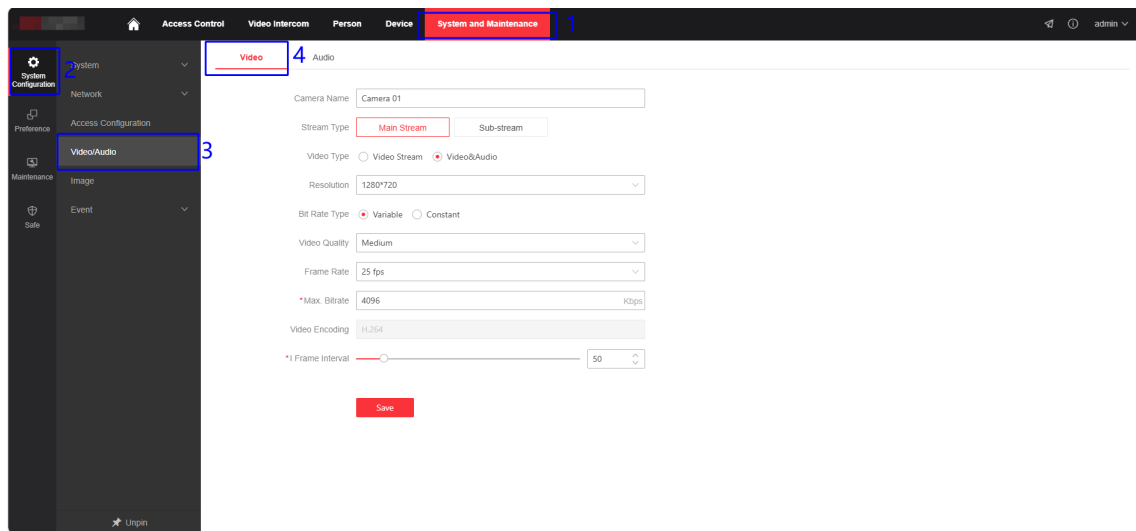


Figure 9-29 Video Settings Page

Set the stream type, the video type, the resolution, the Bit Rate type, the video quality, the frame rate, the Max. bitrate, the video encoding, and I Frame Interval.

You can also slide to **Enable Custom Payload** and set **Custom Video Stream Payload Value**.

Note

After enabling Custom Payload, you can adjust the Payload value of the video stream. For example, H.264 corresponds to 96.

Click **Save** to save the settings.

Note

The functions vary according to different models. Refers to the actual device for details.

Set Audio Parameters

Click **System and Maintenance** → **System Configuration** → **Video/Audio** → **Audio** .

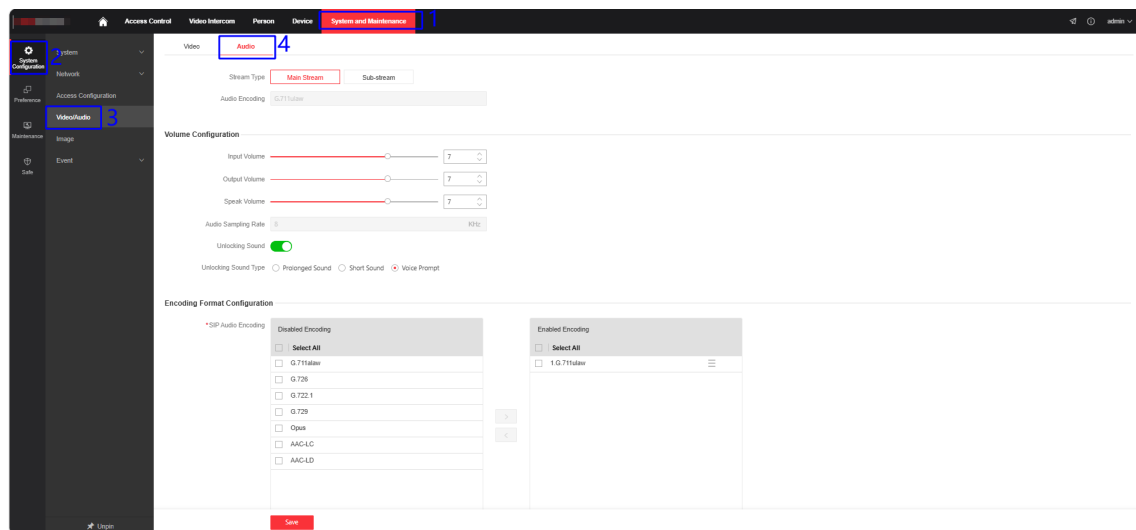


Figure 9-30 Audio Settings Page

Set the stream type, audio encoding, input volume, output volume, speak volume and audio sampling rate.

Slide to enable **Unlocking Sound** according to your actual need.

Check then click < or > to enable or disable **SIP Audio Encoding**.



Note

You can drag icon ≡ to adjust the order of the encoding.

Click **Save** to save the settings.

9.8.5 Adjust Display Settings

You can adjust display settings and OSD configuration.

Steps

1. To adjust display settings. Click **System and Maintenance** → **System Configuration** → **Image** → **Display Settings**.
2. Configure the parameters to adjust the image.

Video Adjustment

Set the video frame rate when performing live view remotely. After changing the video standard, you should reboot the device to take effect.

PAL

25 frames per second. Suitable for mainland China, Hong Kong (China), the Middle East countries, Europe countries, etc.

NTSC

30 frames per second. Suitable for the USA, Canada, Japan, Taiwan (China), Korea, the Philippines, etc.

Image Adjustment

Drag the block or enter the value to adjust the live video's brightness, contrast, saturation, and sharpness.

Backlight

- You can enable or disable the BLC function.
If enabled, you can choose BLC as **Center**, **UP**, **Down**, **Left** or **Right**.
- You can enable or disable the WDR function.
When there are both very bright and very dark areas simultaneously in the view, WDR balances the brightness level of the whole image and provide clear images with details.

Image Fusion

You can choose **Image Fusion** as **Auto** or **Disable**.

After selecting **Auto**, the device will enter automatically enter the image fusion mode. You need to set the Sensitivity. The larger the value, the higher the sensitivity, and the easier it is for the device to enter the image fusion mode.

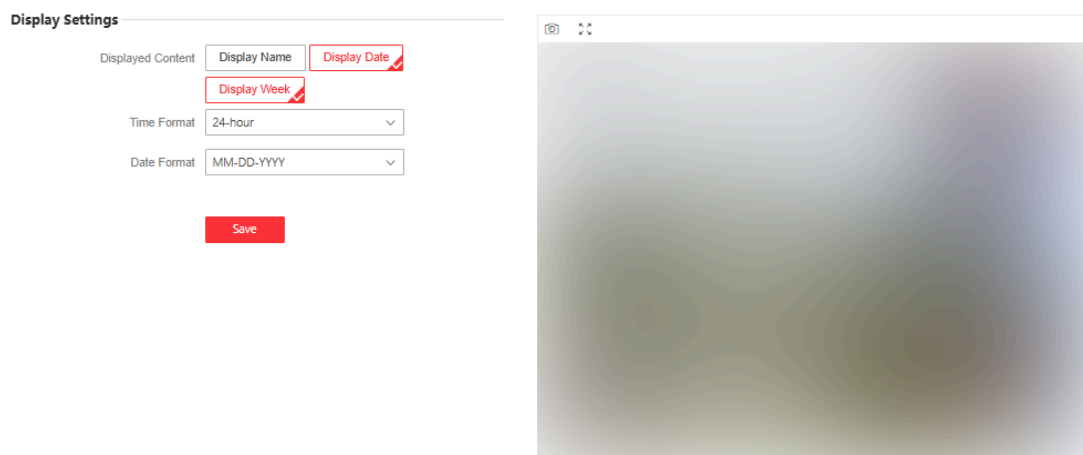
If select **Disable**, the device will not enter the image fusion mode automatically.

- Click **Restore Default Settings** to restore the parameters to the default settings.

OSD Configuration

Steps

- To adjust display settings. Click **System and Maintenance** → **System Configuration** → **Image** → **OSD Configuration**.
- At **Displayed Content**, you can click to choose what to display.



- You can also choose **Time Format** and **Date Format** according to your actual needs.

9.8.6 Event Settings

Set Motion Detection

After enable the function of motion detection, people or stuff enter the configured area will trigger alarm.

Steps

1. Click **System and Maintenance** → **System Configuration** → **Event** → **Event Detection** → **Motion** .

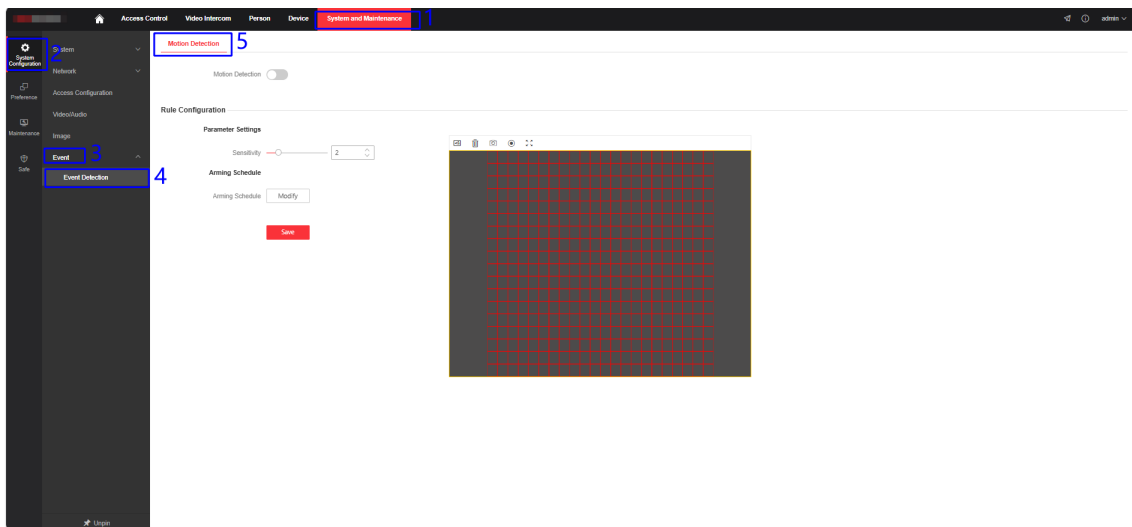


Figure 9-31 Motion Detection

2. Enable **Motion Detection**.
3. Drag the process bar to adjust the **Sensitivity** parameter.
4. Click **Save**.



Note

The arming schedule is defaulted as all-day.

9.8.7 Access Control Settings

Search Event

Click **Access Control** → **Event Search** to enter the page.

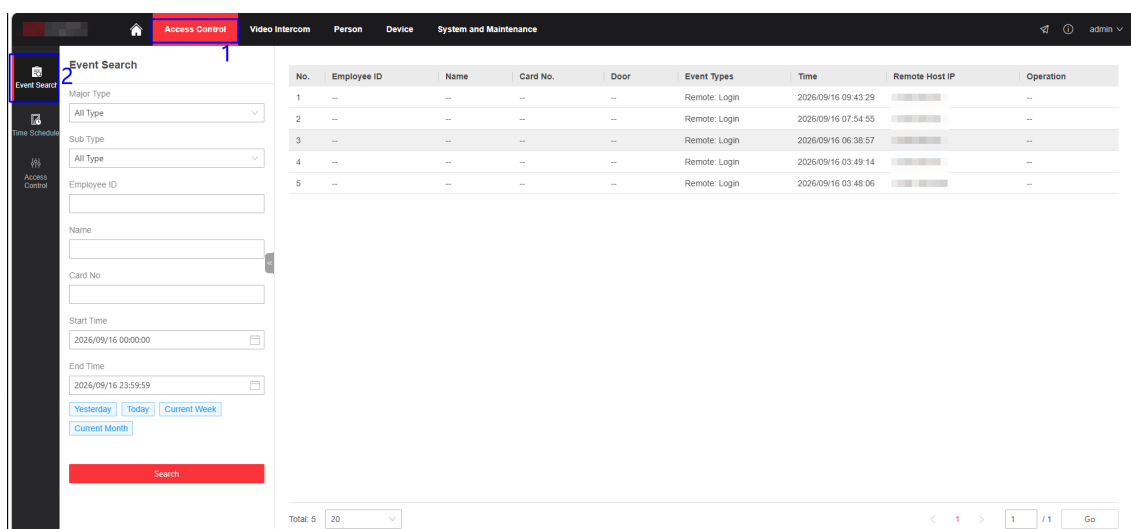


Figure 9-32 Search Event

Enter the search conditions, including the event type, the employee ID, the name, the card No., the start time, and the end time, and click **Search**.

The results will be displayed on the right panel.

Set Access Schedule

You can name and add new access template on this page.

Steps

1. Click **Access Control** → **Time Schedule** → **Access Schedule** to enter this page.

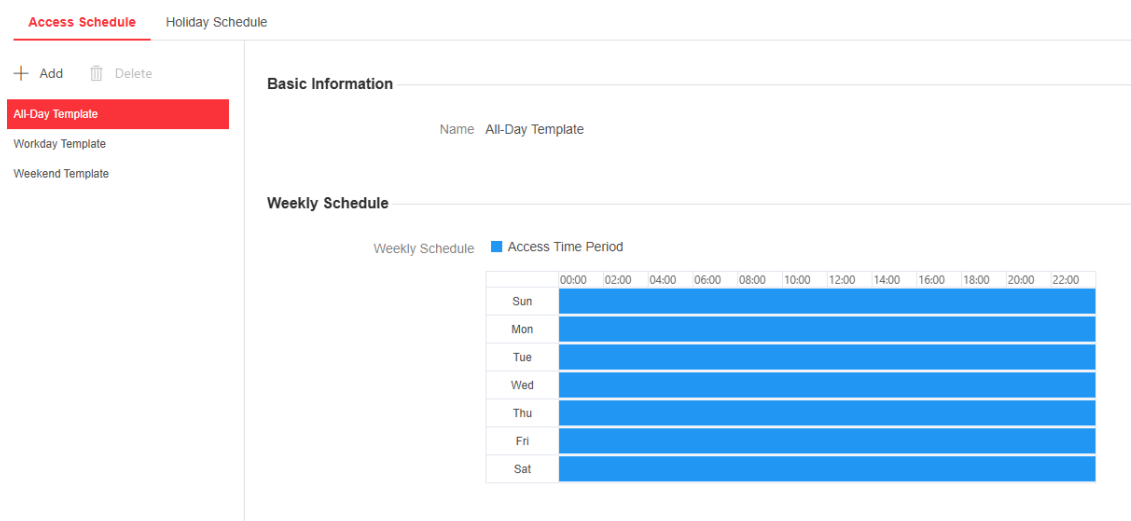


Figure 9-33 Access Schedule

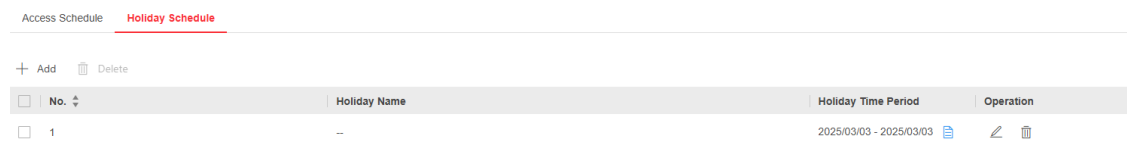
2. Click **+Add**. Then you can edit the name of the schedule.
3. Drag cursor on corresponding timestamp to map valid access period.
4. You can also click **Quick Operation** to apply existing template.
5. **Optional:** Click **Eraser** to adjust chosen time period. You can also click a certain time period then adjust it manually.
6. Click **Save** to save your settings.

Holiday Schedule Template

Set official holidays or specified dates as holidays. The access level of set holidays is higher than the other basic access level.

Steps

1. Click **Access control** → **Time Schedule** → **Holiday Schedule** → **+Add** .



Access Schedule		Holiday Schedule	
+ Add	🗑 Delete		
No.	Holiday Name	Holiday Time Period	Operation
1	-	2025/03/03 - 2025/03/03	📅 ✎ 🗑

Figure 9-34 Holiday Schedule Template

2. Enter holiday name in the right column.
3. Set Start Date and End Date.
4. Drag cursor on corresponding timestamp to map valid holiday period.
5. **Optional:** Click **Eraser** to adjust chosen time period. You can also click a certain time period then adjust it manually.
6. Click **Save**.

Access Control

Set Door Parameters

Click **Access Control** → **Access Control** → **Door Parameters** .

Door No.

*Door Name

Open Duration s

Relay Reverse ☐ Open ☒ Disable

Save

Figure 9-35 Door Parameters Settings Page

Click **Save** to save the settings after the configuration.

Door No.

Select the device corresponded door No.

Door Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked. (Range: 1~255s)

Relay Reverse

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Set Authentication Parameters

Set authentication related parameters, such as enable authentication function, select authentication mode, etc.

Set Password on PC Web

You can configure personal PIN and public PIN on this page.

Steps

1. Click **Access Control** → **Access Control** → **Authentication Settings** .
2. If you want to set **Personal PIN**, select from **Platform-Applied Personal PIN** and **Device-Set Personal PIN**.
3. If you want to configure **Public Password**, click **+ Add** to add public password.
 - 1) Select **Password Type**.
 - 2) Enter the password and confirm the password.
 - 3) **Optional**: Add remarks for the password.
 - 4) Select Electric Lock.

4. Click **Save** to save the settings.

Set Face Recognition Interval

You can set the interval between 2 continuous recognition of a same person during the authentication.

Steps

1. Click **Access Control** → **Access Control** → **Authentication Settings** .



Note

The functions vary according to different models. Refers to the actual device for details.

2. Slide to enable **Enable Face Authentication**.

3. Set **Recognition Interval**. You can set the interval between 2 continuous recognition of a same person during the authentication. Range: 1 ~ 10 s.

4. Click **Save**.

Smart Settings

Enable/Disable Face with Mask Detection via PC Web

After enabling the face with mask detection, the system will recognize the captured face with mask picture or not.

Click **Access Control** → **Access Control** → **Smart** to enter the settings page.

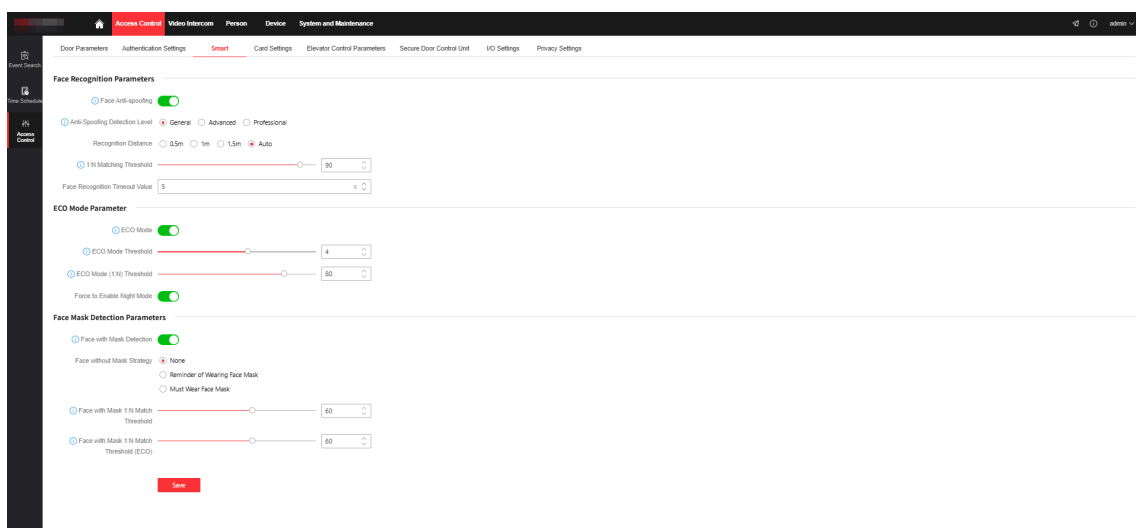


Figure 9-36 Smart Overview

After enabling the face with mask detection, you can set **Face without Mask Strategy**, **Face with Mask 1:N Match Threshold (ECO)**, and **Face with Mask 1:N Match Threshold (ECO)**.

Face without Mask Strategy

You can select **None**, **Reminder of Wearing Face Mask** and **Must Wear Face Mask** at the bottom of this page.

Reminder of Wearing Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will open.

Must Wear Face Mask

If the person do not wear the face mask when authenticating, the device will pop up a prompt and the door will keep closed.

Face with Mask&Face (1:N)

Set the matching threshold when authenticating with face mask via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate. The maximum value is 100.

Face with Mask 1:N Match Threshold (ECO)

Set the matching value when authenticating with face mask via ECO mode 1:N matching mode. The larger the threshold, the lower the recognition error rate and the higher the rejection rate when authenticating faces. The maximum value is 100.

ECO Mode

To configure **ECO Mode Parameters**, you need to enable **ECO Mode** first.

After the ECO mode is enabled, the device will use the IR camera to authenticate faces in the low light or dark environment. After the ECO mode is disabled, the effect of face comparison will be lower in the low light or dark environment.

Force to Enable Night Mode

If enabled, the device automatically switches to night mode under specific conditions to optimize image quality in low-light environments.

ECO Mode Threshold

You can drag the bar or input a certain value in the right box to adjust the threshold. If you select a smaller value, it is harder for the device to enter the eco mode.

ECO Mode (1:N) Threshold

You can drag the bar or input a certain value in the right box to adjust the threshold. It's suggested to keep the device default value. Adjusting the value will affect the false acceptance rate and false rejection rate of face recognition.

Click **Save**.

Set Face Parameters

Tap **Access Control** → **Access Control** → **Smart** to enter the configuration page.



Note

The functions vary according to different models. Refers to the actual device for details.

Click **Save** to save the settings after the configuration.

Face Anti-spoofing

You can configure the parameters below at the top of this page, in **Face Recognition Parameters** section.

Enable or disable the live face detection function. If enabling the function, the device can recognize whether the person is a live one or not.



Note

Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.

Anti-Spoofing Detection Level

After enabling the face anti-spoofing function, you can set the matching security level when performing live face authentication.

Detection accuracy rankings: General < Advanced < Professional. When you select a mode with a higher detection accuracy, the passing efficiency will be lower.

Recognition Distance

Select the distance between the authenticating user and the device camera.

1:N Matching Threshold

Set the matching threshold when authenticating via 1:N matching mode. The larger the value, the smaller the false accept rate and the larger the false rejection rate.

Face Recognition Timeout Value

Set the timeout value when face recognizing. If the face recognition time is longer than the configured value, the system will pop up a prompt.

Card Settings

Choose card types to enable. Different models may support different card types.

Go to **Access Control** → **Access Control** → **Card Settings** .

Slide to enable card types and click **Save** to save the settings.

Card Type

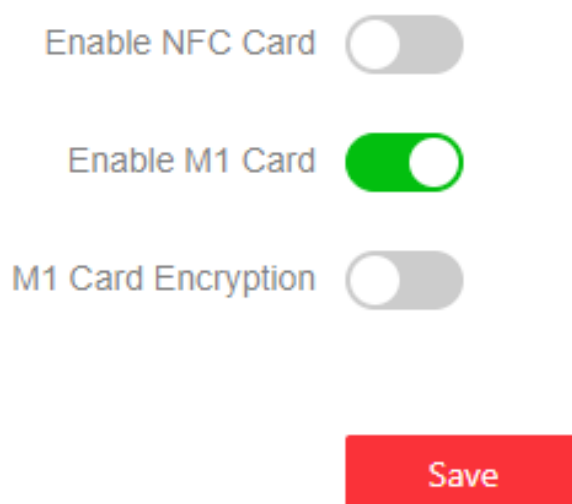


Figure 9-37 Card Type

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.



Note

The function of Enable M1 Card is enabled by default.

M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Enable NFC Card

If enabled, the device will actively detect and process communication requests from NFC cards.



Note

Different models may support different card types. The image above shows the most complete one. Please refer to your actual device.

Some models only support M1 card.

Privacy Settings

You should set the privacy parameters, including the picture uploading and storage.

Click **Access Control** → **Privacy Settings** to enter this page.

Event Storage Settings

Event Storage Type ☐ Delete Old Events Periodically
☐ Delete Old Events by Specified Time
☒ Overwrite

Picture Uploading and Storage

Save Picture When Auth. ☒
If enabled, the captured picture when authentication will be saved to the device automatically.

Upload Picture When Auth. ☒
If enabled, the captured picture when authentication will be uploaded to the platform automatically.

Save Registered Picture ☒
If enabled, the captured face picture when registered will be saved to the device.

Clear All Pictures in Device

Clear Registered Face Pictures

Clear Captured Pictures

Figure 9-38 Privacy Settings

Upload Pic. When Auth. (Upload Captured Picture When Authenticating)

Upload the pictures captured when authenticating to the platform automatically.

Save Pic. When Auth. (Save Captured Picture When Authenticating)

If you enable this function, you can save the picture when Authenticating to the device.

Save Registered Pic. (Save Registered Picture)

The registered face picture will be saved to the system if you enable the function.

Platform-Applied Personal PIN

You can create the person PIN on the platform. You should apply the PIN to the device. You cannot create or edit the PIN on the device or PC Web.

Device-Set Personal PIN

You can create or edit the PIN on the device or PC Web. You cannot set the PIN on the platform. Tap **Save** to complete the settings.

Event Storage Settings

Select a method to delete the event. You can select from **Delete Old Events Periodically**, **Delete Old Events by Specified Time**, or **Overwriting**.

Delete Old Events Periodically

Drag the block or enter number to set the period for event deleting. All events will be deleted according to the configured time duration.

Delete Old Events by Specified Time

Set a time and all events will be deleted on the configured time.

Overwriting

The earliest 10% events will be deleted when the system detects the stored events have taken the full space.

Clear All Pictures in Device



All pictures cannot be restored once they are deleted.

Clear Registered Face Pictures

All registered pictures in the device will be deleted.

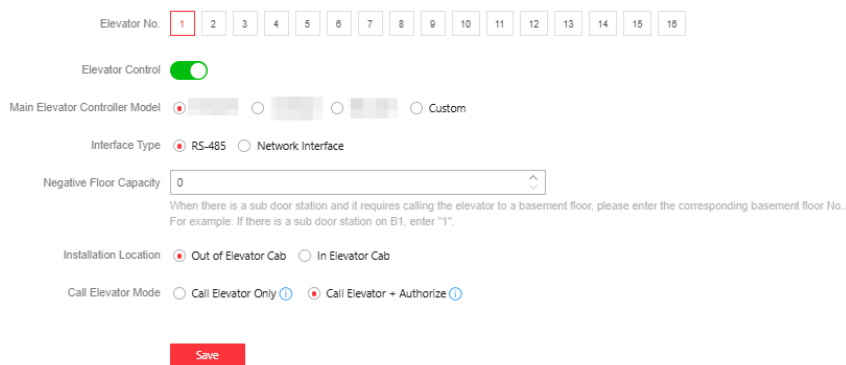
Clear Captured Pictures

All captured pictures in the device will be deleted.

Elevator Control via PC Web

Steps

1. Click **Access Control** → **Access Control** → **Elevator Control Parameters** .



Elevator No. ☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16

Elevator Control ☒

Main Elevator Controller Model ☒ ☐ ☐ ☐ Custom

Interface Type ☒ RS-485 ☐ Network Interface

Negative Floor Capacity

When there is a sub door station and it requires calling the elevator to a basement floor, please enter the corresponding basement floor No..
For example: If there is a sub door station on B1, enter "1".

Installation Location ☒ Out of Elevator Cab ☐ In Elevator Cab

Call Elevator Mode ☐ Call Elevator Only ☒ Call Elevator + Authorize

Figure 9-39 Elevator Control

2. Select an elevator No., the parameters settings below will affect the selected elevator.
3. Enable **Elevator Control**.
4. Set the elevator parameters.

Main Elevator Controller Model

View the elevator model.

Interface Type

Select a communication type from the drop-down list for elevator communication.

If you select **Network Interface**, enter the elevator controller's IP address, port No., user name, and password for communication.

Negative Floor Capacity

Set the negative floor number.

Installation Location

Select the device installation position. By default, it is **Out of Elevator Cab**.

Call Elevator Mode

Call Elevator Only

After person passes authentication on device, the device will call elevator to its floor.

Call Elevator+Authorize

After person passes authentication on device, the device will call elevator to its floor and authorize the permission of the floor linked to person room. The person can get to the target floor by pressing corresponding floor No.



Note

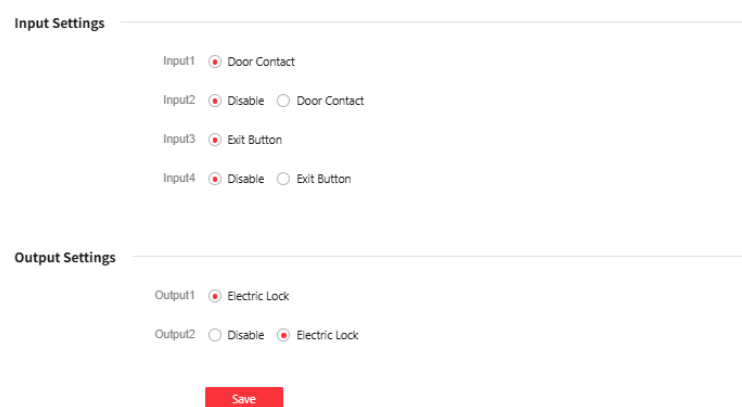
- Up to 4 elevator controllers can be connected to 1 device.
 - Up to 10 negative floors can be added.
 - Make sure the interface types of elevator controllers, which are connected to the same device, are consistent.
-

Set I/O Parameters

You can set I/O Parameters on PC Web.

Steps

1. Click **Access Control** → **Access Control** → **I/O Settings** .



Input Settings

Input1 ☒ Door Contact

Input2 ☒ Disable ☐ Door Contact

Input3 ☒ Exit Button

Input4 ☒ Disable ☐ Exit Button

Output Settings

Output1 ☒ Electric Lock

Output2 ☐ Disable ☒ Electric Lock

Save

Figure 9-40 I/O Settings

2. Select Input 2 as **Disable** or **Door Contact**. Set Input 4 as **Disable** or **Exit Button**.



Note

Because the device only has one lock. The Input 1 is **Door Contact** by default.
Input 2 and 4 is set as **Disable** by default.

3. Select Output 2 as **Disable** or **Electric Lock**.



Note

The Output 2 is **Disable** by default.

Set Secure Door Control Unit Parameters via PC Web

You can set secure door control unit parameters.

Steps

1. Click **Access Control** → **Access Control** → **Secure Door Control Unit** .
2. You can slide to enable **Auto Binding**.



Note

If the function is enabled, the connected secure door control unit will be automatically bound to the door station and cannot be used for other door stations.

9.8.8 Video Intercom Settings

No. and System Network Settings

Device No. Settings

Steps

1. Click **Video Intercom** → **Call Parameters** → **No. and System Network Settings** to enter the page.

The screenshot displays the 'No. and System Network Settings' page for the Video Intercom D Series Android Door Station. The page is organized into two main sections: 'No. Settings' and 'Video Intercom Network'.

No. Settings

- Device Type: Villa Door Station (dropdown menu)
- *Floor No.: 10 (dropdown menu)
- *Door Station No.: 0 (dropdown menu)
- More ^ (link)
- *Community No.: 1 (dropdown menu)
- *Building No.: 1 (dropdown menu)
- *Unit No.: 1 (dropdown menu)

Video Intercom Network

- *Registration Password: [input field]
- *Main Station IP: [input field]
- *Private Server IP: [input field]
- Enable Protocol 1.0: [toggle switch]
- Save (button)

2. Select the device type from the drop-down list.
3. If select the device type as **Villa Door Station**, you need to set the corresponding information including **Building No.**, **Floor No.**, **Door Station No.**, **Community No.** and **Unit No.**
4. If select the device type as **Doorphone**. You only need to set **Building No.**, **Community No.** and **Unit No.**.
5. Click **Save** to enable the device number configuration.

Linked Network Settings

Steps

1. Click **Video Intercom** → **Call Parameters** → **No. and System Network Settings** to enter the settings page.

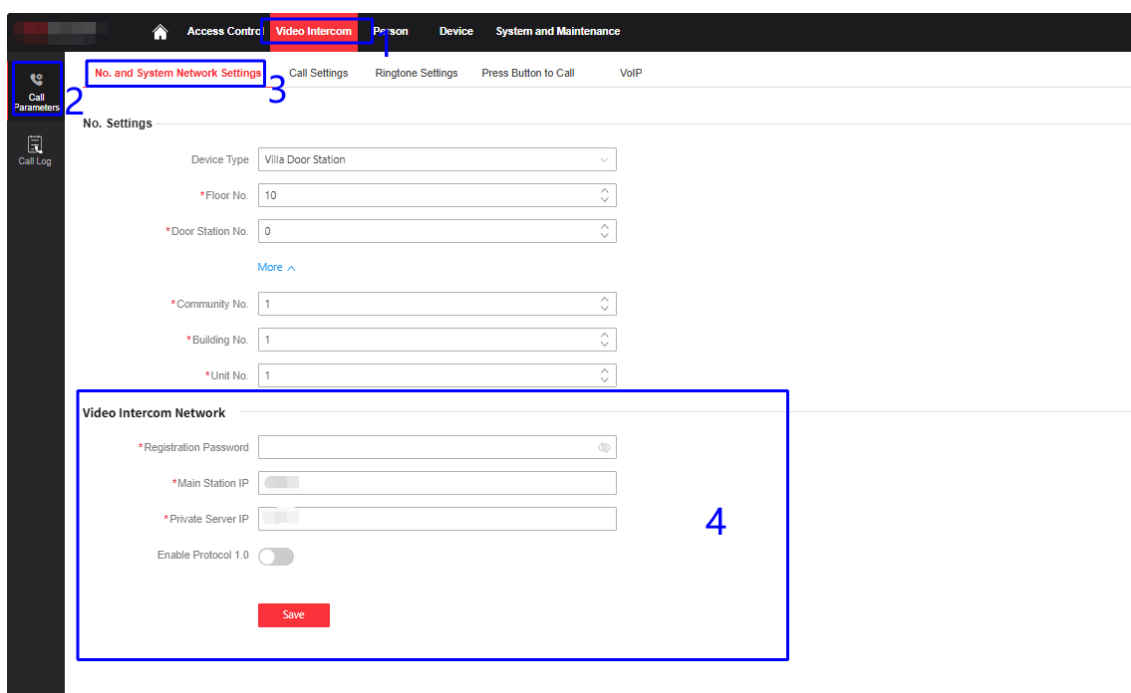


Figure 9-42 Video Intercom Network Settings

2. Set **Registration Password**.
3. Set **Main Station IP** and **Private Server IP**.
4. Enable Protocol 1.0.
5. Click **Save** to enable the settings.

Time Duration Settings

Set the Max. call duration.

Go to **Video Intercom** → **Call Parameters** → **Call Settings** .

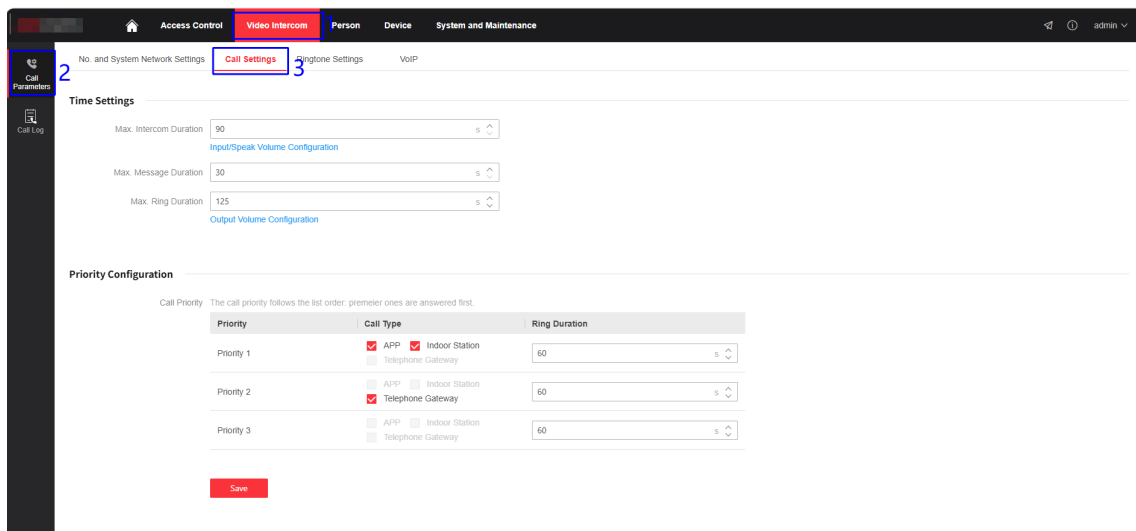


Figure 9-43 Time Settings

Set the **Max. Communication Time**, **Max. Message Duration** and **Max Ring Duration**.



Note

- The Max. communication time range is 90 s to 1800 s.
- The Max. message duration range is 30 s to 60 s.
- The Max. ring duration range is 65 s to 255 s.

Click **Save**.

Call Priority

Steps

1. Click **Video Intercom** → **Call Parameters** → **Call Settings** to enter the settings page.

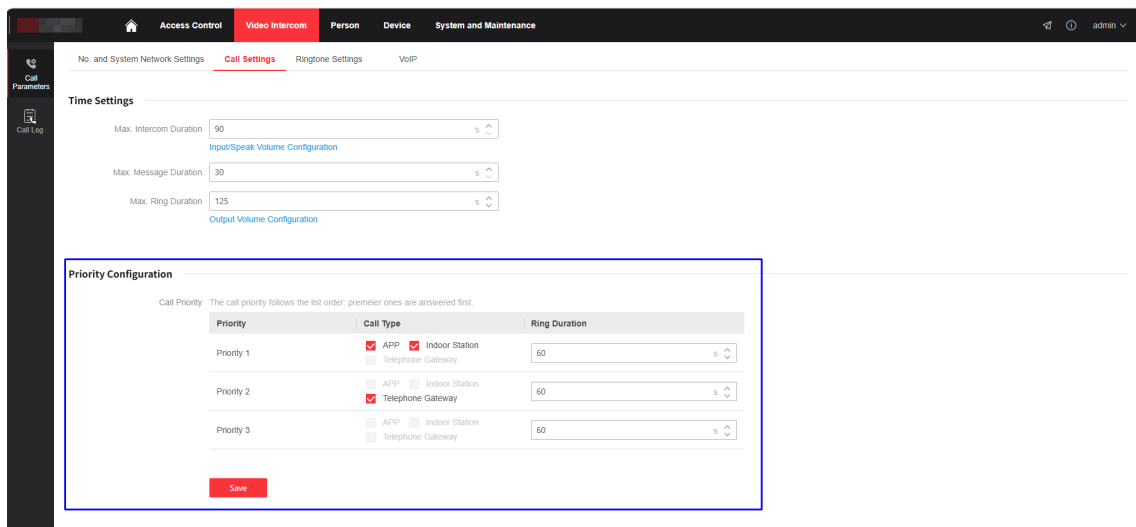


Figure 9-44 Priority Configuration

2. Check the **Call Type** and set the **Ring Duration** of each 3 priorities.
3. Click **Save** to enable the settings.



Note

The higher the level, the earlier the device to be called. After the call time is over, the next level of call is triggered.

Ringtone Settings

Steps

1. Click **Video Intercom** → **Call Parameters** → **Ringtone Settings** to enter the settings page.
2. Slide to enable **Ringtone**. Click  to import new ringtone.



Note

The supported audio file type for importing is .wav. The file should be less than 800 KB.

VoIP Account Settings

You can realize voice call by network.

Steps

1. Go to **Video Intercom** → **Call Parameters** → **VoIP** → **Basic Configuration**.

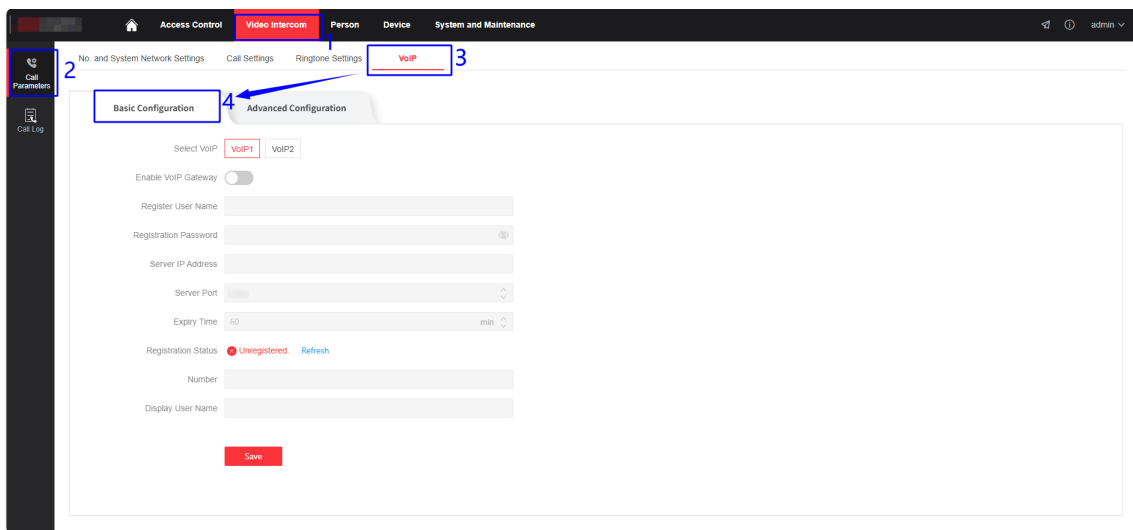


Figure 9-45 Basic Configuration-VoIP

2. Slide to **Enable VoIP Gateway**.
3. Set **Register User Name**、**Registration Password**、**Server IP Address**、**Server Port**、**Expiry Time**、**Register Status**、**Number**、**Display User Name**. and **Center No**.
4. Click **Save**.

SIP No. and P2P No. Settings

Steps

1. Click **Video Intercom** → **Call Parameters** → **VoIP** → **Advanced Configuration** to enter the settings page.

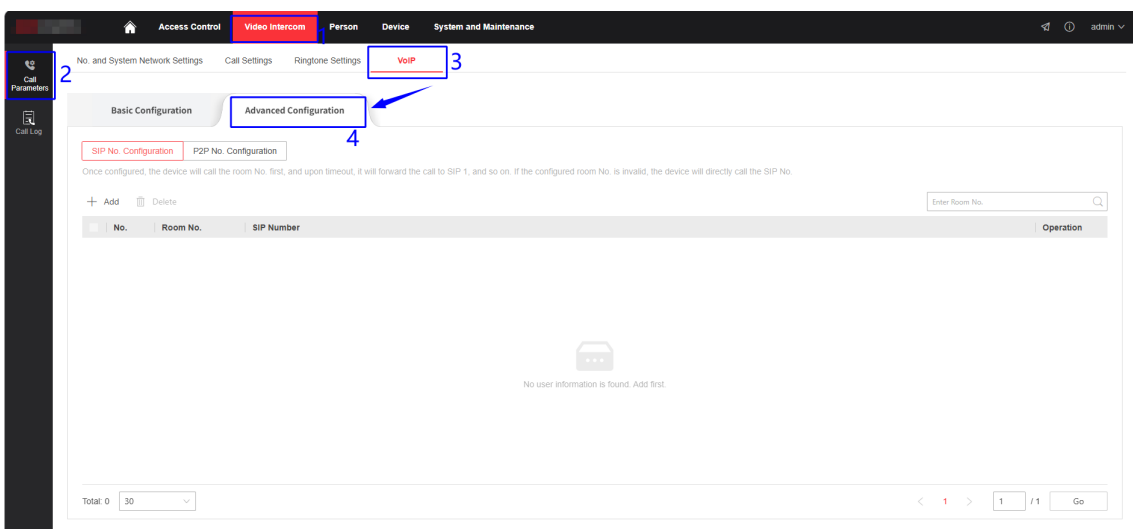
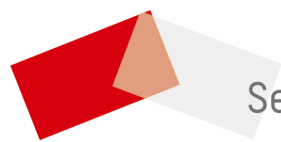


Figure 9-46 Advanced Configuration-VoIP

2. If you want to configure SIP No. Click + **Add** to add the SIP No. to the device.
 - 1) Select an item, and click **Configure** to edit the parameters.
 - 2) **Optional:** Select SIP numbers in the list, and click **Delete** to delete the selected informations.
 - 3) **Optional:** Click **Clear** to clear the informations in the list.
3. If you want to configure P2P No. Slide to enable P2P first.
 - 1) Fill in the room No., IP Address and port. Click **Save**.
 - 2) **Optional:** Select P2P numbers in the list, and click **Delete** to delete the selected informations.
 - 3) **Optional:** Click **Clear** to clear the informations in the list.



See Far, Go Further