Unit VTO (Version 4.8.1)

User Manual



V1.0.2

Foreword

This manual introduces the structure and configuration of the unit VTO. Read carefully before using the VTO, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Software Version	Revision Content	Release Time
V1.0.2	-	Updated RS-485.	August 2025
V1.0.1	V4.800.0000001.0.R	• Updated homepage. • Updated local device configuration. • Updated device setting. • Updated person management. • Updated maintenance center.	June 2025
V1.0.0	-	First release.	November 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguard and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Installation Requirements

 WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Please follow the electrical requirements to power the device.
  - Following are the requirements for selecting a power adapter.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - We recommend using the power adapter provided with the device.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Install the device on a stable surface to prevent it from falling.
- Install the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- The device must be installed at a height of 2 meters or below.

Operation Requirements

 DANGER

Battery Pack Precautions

Preventive measures (including but not limited to):

- Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.

- Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
- Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
- Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.



- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Transport, use and store the device under allowed humidity and temperature conditions.
- If the device is powered off for longer than a month, it should be placed in its original package and sealed. Make sure to keep it away from moisture, and store it under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.

Table of Contents

Foreword I
Important Safeguard and Warnings III
1 Product Overview 1
1.1 Introduction 1
1.2 Function 1
1.3 Front Panel 2
1.3.1 65 Series 3
1.3.2 75 Series 4
1.3.3 95 Series 5
1.3.4 7 Series 6
1.3.5 9 Series 7
1.4 Rear Panel 7
1.4.1 65 Series 8
1.4.2 75 Series 10
1.4.3 95 Series 12
1.4.4 7 Series 14
1.4.5 9 Series 16
2 VTO Operation 18
2.1 65 Series 18
2.1.1 Home Screen 18
2.1.2 Engineering Setting 19
2.2 75/95/7/9 Series 34
2.2.1 Home Screen 35
2.2.2 Engineering Setting 36
2.2.3 Owner Registration 50
2.2.4 Unlock 53
2.2.5 Call 55
2.2.6 Messages 56
3 Webpage Operations 57
3.1 Initialization 57
3.1.1 Initialization through the Device 57
3.1.2 Initialization through the DoLynk Care 57
3.2 Logging in to the Webpage 58
3.3 Home Page Introduction 58
3.4 Setup Wizard 59
3.4.1 Setting as SIP Server 60
3.4.2 Not Setting as SIP Server 61

3.5 Admin Center 62
3.5.1 Resetting the Password 62
3.5.2 Changing the User Message 62
3.5.3 Restoring the Factory Default Settings 63
3.5.4 Restarting the Device 63
3.5.5 Logging Out 63
3.6 Security Center 64
3.6.1 Security Status 64
3.6.2 Configuring HTTPS 65
3.6.3 Attack Defense 65
3.6.4 Installing Device Certificate 68
3.6.5 Installing the Trusted CA Certificate 71
3.6.6 Video Encryption 72
3.6.7 Security Warning 73
3.6.8 Security Authentication 74
3.7 Local Device Configuration 74
3.7.1 Basic Settings 75
3.7.2 Configuring Access Control Parameters 76
3.7.3 Configuring Light Control 82
3.7.4 Adding the IPC 83
3.7.5 Configuring Cards 85
3.7.6 Configuring Wiegand 86
3.7.7 Configuring Face Detection 88
3.7.8 Configuring QR Code 90
3.7.9 Configuring Fingerprint 90
3.8 Device Setting 91
3.8.1 Adding the VTO 91
3.8.2 Adding the VTH 93
3.8.3 Adding the VTS 94
3.8.4 Related Operations 95
3.9 Person Management 96
3.10 Network Settings 99
3.10.1 Configuring TCP/IP 99
3.10.2 Configuring Port 101
3.10.3 Configuring the SIP Server 102
3.10.4 Configuring Cloud Service 106
3.10.5 Configuring UPnP 107
3.10.6 Configuring Basic Services 108
3.10.7 Configuring Auto Registration 110
3.10.8 Configuring Registration Management 111

3.11 System 112
3.11.1 Configuring Alarm 112
3.11.2 Configuring Video Parameters 115
3.11.3 Configuring Audio Parameters 119
3.11.4 Configuring Time 120
3.11.5 Configuring Shortcut 122
3.11.6 Adding ONVIF Users 123
3.12 Personalization 123
3.12.1 Configuring Advertisements 123
3.12.2 Adding Resources 126
3.12.3 Configuring Notifications 127
3.13 Maintenance Center 127
3.13.1 One-Click Diagnosis 128
3.13.2 System Information 128
3.13.3 Data Capacity 129
3.13.4 Viewing Logs 129
3.13.5 Maintenance Management 131
3.13.6 Updating the System 132
3.13.7 Advanced Maintenance 133
Appendix 1 Security Recommendation 135

1 Product Overview

1.1 Introduction

The Digital Door Station (hereinafter referred to as "VTO") uses capacitive touch screen and anodized aluminum frame, and is equipped with 2-MP dual-lens network camera. The VTO integrates deep learning algorithm to enable the user open the door through the recognition function. There are multiple authentication methods, such as QR code recognition, fingerprint recognition and password opening. Supports emergency call, announcement, log search and other functions. The VTO is generally used in residential areas.

1.2 Function

Video and Voice Call

Makes video and voice calls to the VTH or the VTS.

Group Call

If the current VTO works as the SIP server, it can call many VTHs or VTSs at the same time.

Emergency Call

Directly calls the management center in an emergency.

Unlock

- Unlock through the face: The VTO recognizes the face using the latest deep learning algorithm and opens the door.
- Unlock through the fingerprint: The built-in fingerprint module recognizes the fingerprint.
- Unlock through the QR code: The VTO recognizes the QR code to open the door.
- Unlock through the card: Swipe the authorized card to open the door.

Being Monitored

The VTH or the management center can monitor the VTO. The VTO supports up to 6 streams for monitoring.

Auto Snapshot

Takes snapshots while you are on a call or unlocking the door, and stores them to the SD card.

Access Control

Directly controls the locks.

Alarm Management

The VTO has functions of tamper alarm and door detector detection alarm.

Alarm Linkage Setting

The VTO can adopt buzzer to ring the calls.

Linkage with the Elevator

Connects with the elevator to enable the elevator control linkage function.

IR Smart Illumination

Automatically detects the actual scenery and opens the illumination (white is normally adapted and red is used for assist face recognition).

Standalone Operation

Issues the cards, and registers the fingerprints and the faces through the device.

Sub VTO Management

The main VTO can connect with up to 19 sub VTOs in the same unit.

Announcement

Sends the announcement to the VTH.

Log Search

Supports searching for the call log, alarm log and unlock log.

1.3 Front Panel

1.3.1 65 Series

The device models on the first row in the following figure are VTO6521F (the same as VTO6531F) and VTO6521H. The device models on the second row in the following figure are VTO6531H and VTO6541H.

Figure 1-1 Front panel

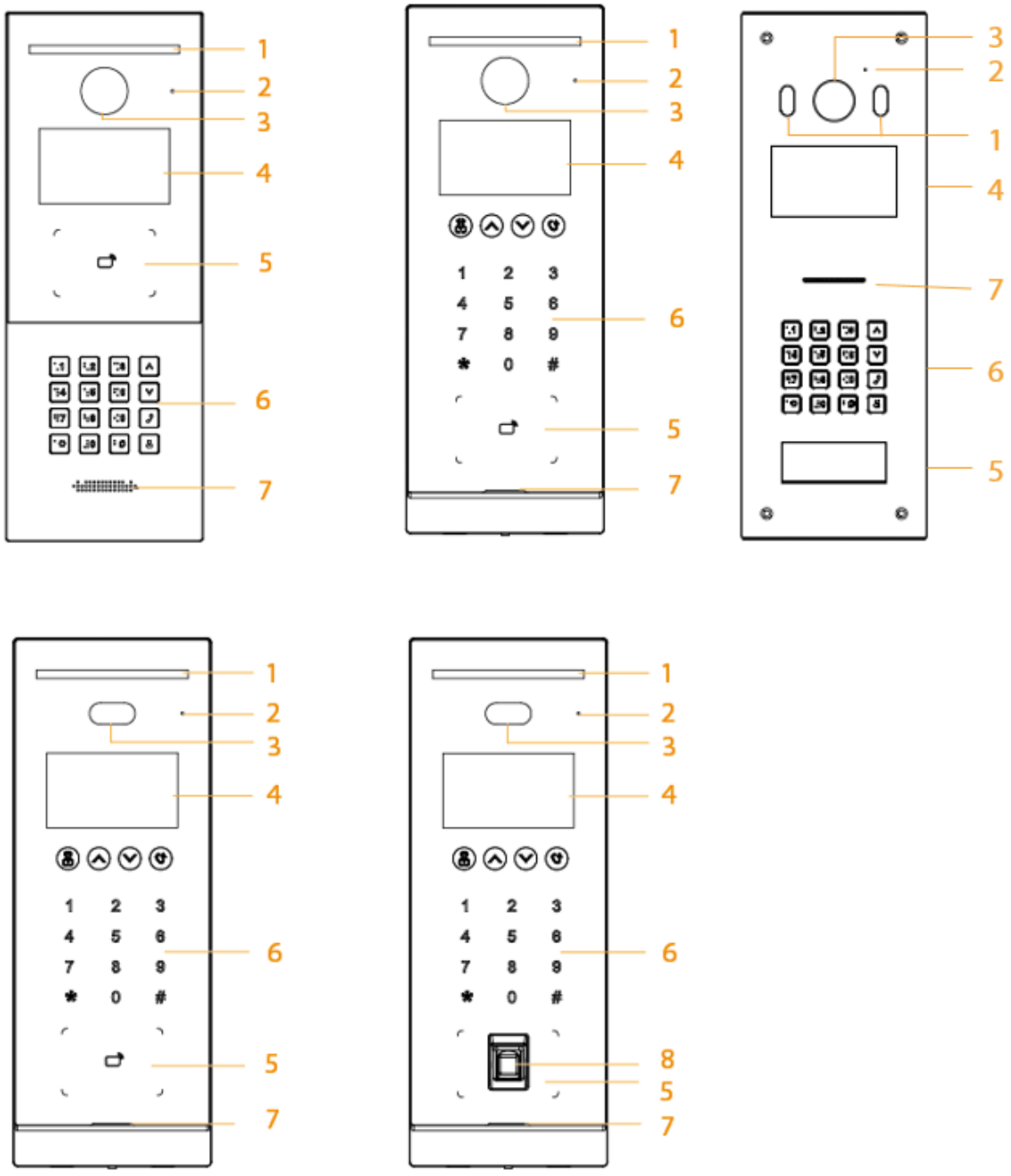


Table 1-1 Component description

No.	Description	No.	Description
1	White illuminator	5	Card swiping area
2	MIC	6	Keyboard

No.	Description	No.	Description
3	Camera	7	Loudspeaker
4	Display	8	Fingerprint sensor

1.3.2 75 Series

Figure 1-2 Front panel

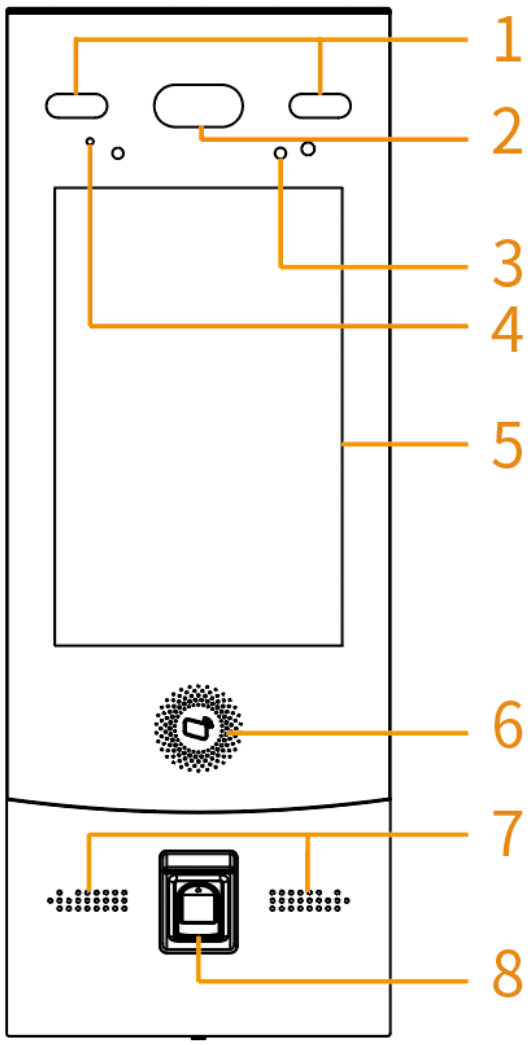


Table 1-2 Component description

No.	Description	No.	Description
1	White illuminator	5	Display
2	Camera	6	Card swiping area
3	IR illuminator	7	Loudspeaker

No.	Description	No.	Description
4	MIC	8	Fingerprint sensor Fingerprint sensor is only available for the mode of VTO7541G.

1.3.3 95 Series

Figure 1-3 Front panel

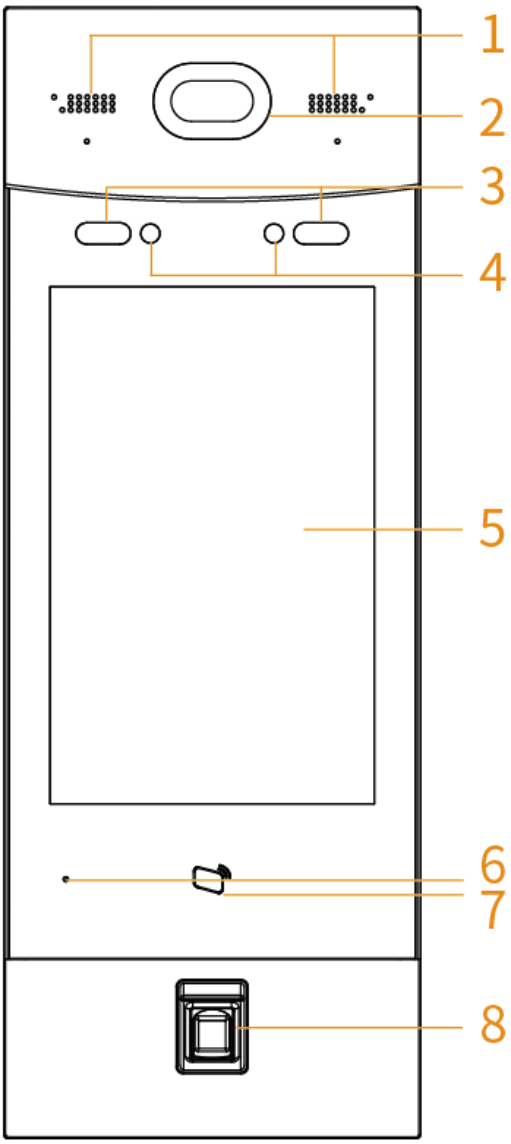


Table 1-3 Component description

No.	Description	No.	Description
1	Loudspeaker	5	Display

No.	Description	No.	Description
2	Camera	6	MIC
3	White illuminator	7	Card swiping area
4	IR illuminator	8	Fingerprint sensor

1.3.4 7 Series

Figure 1-4 Front panel

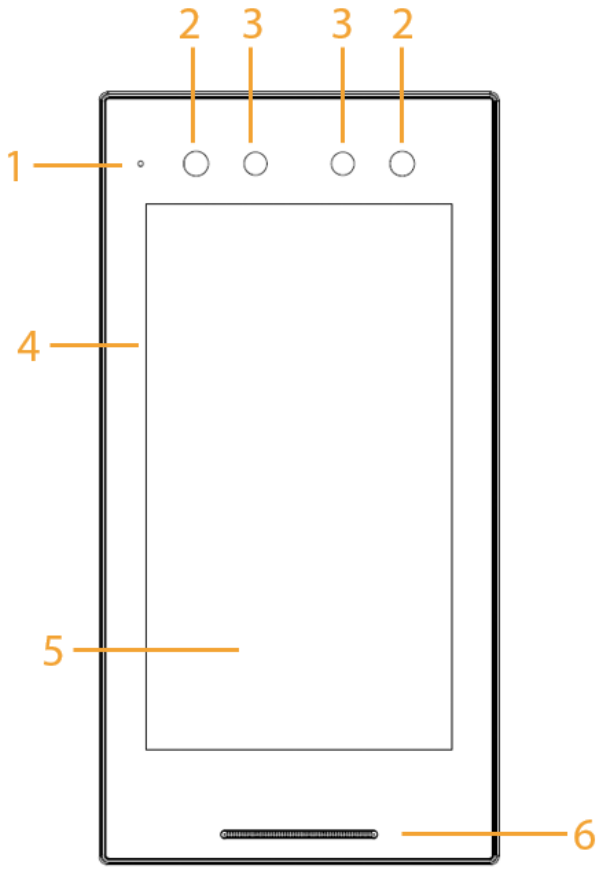


Table 1-4 Component description

No.	Description	No.	Description
1	MIC	4	Touchable display
2	IR illuminator	5	Card swiping area
3	Camera	6	Loudspeaker

1.3.5 9 Series

Figure 1-5 Front panel

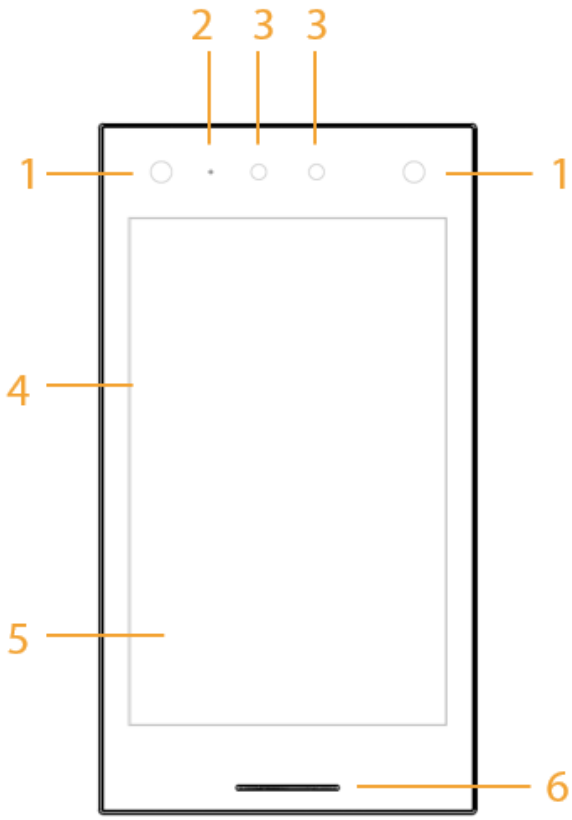


Table 1-5 Component description

No.	Description	No.	Description
1	IR illuminator	4	Display
2	MIC	5	Card swiping area
3	Camera	6	Loudspeaker

1.4 Rear Panel

1.4.1 65 Series

Figure 1-6 Rear panel

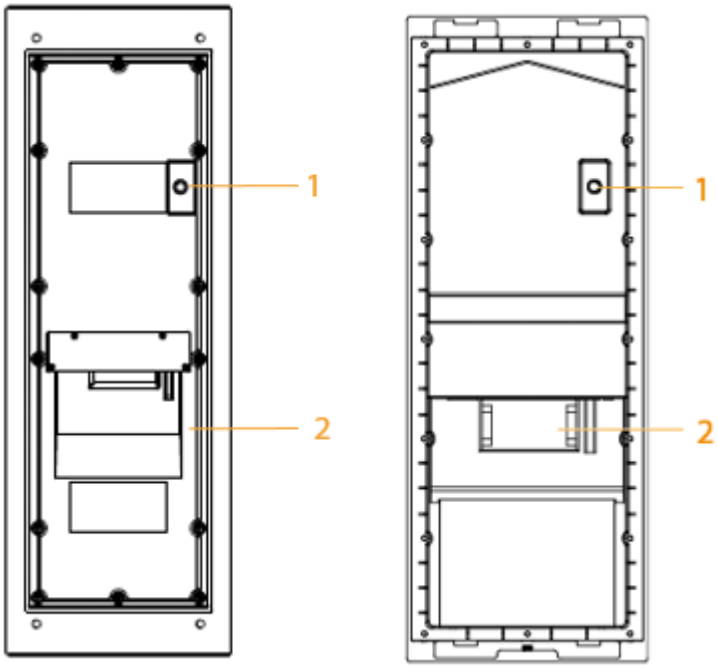
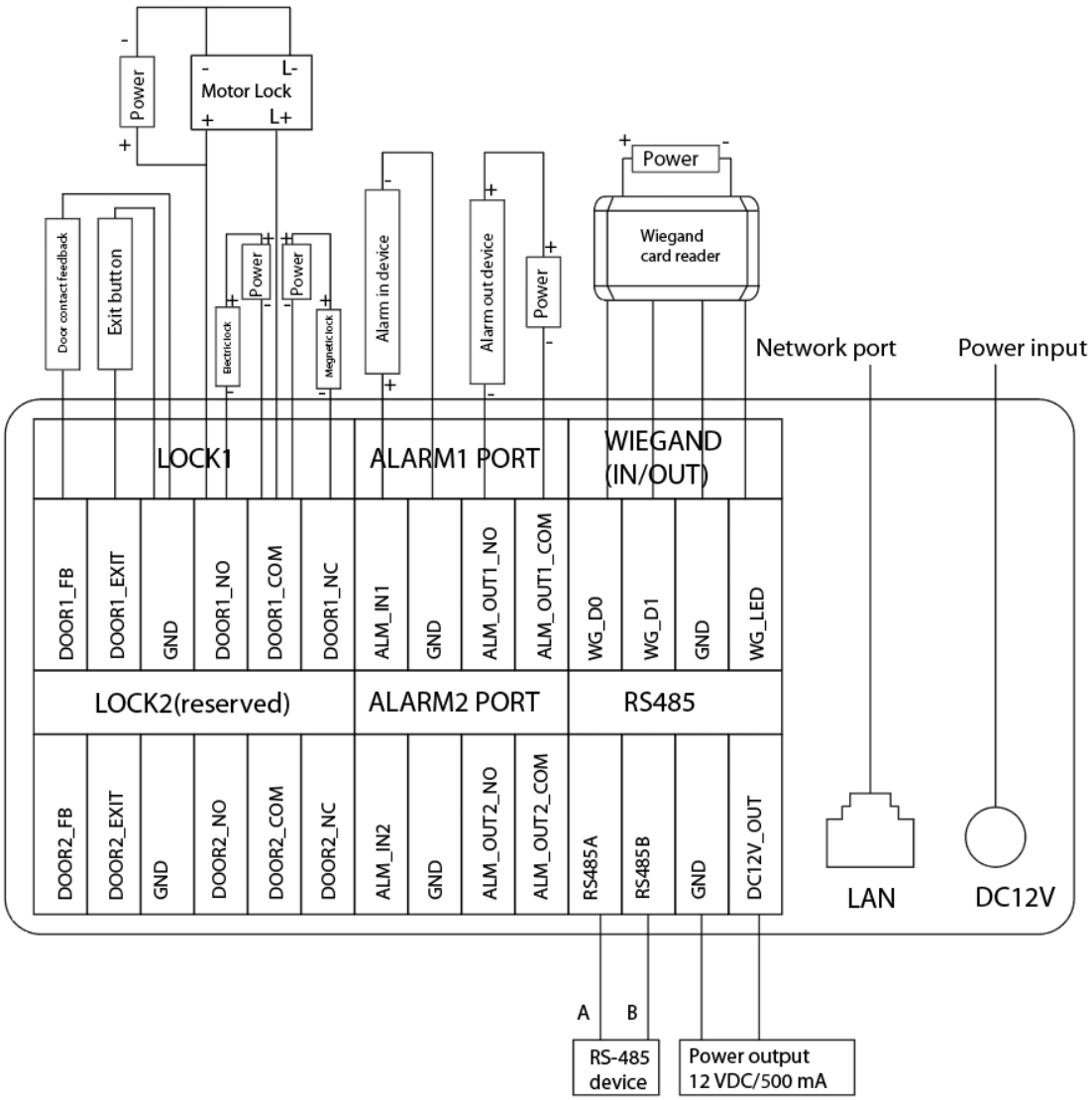


Table 1-6 Component description

No.	Description
1	Tamper button Within 10 minutes after the device is powered on, if you continuously press the tamper button for 5 times in 8 seconds, the device beeps and deletes the account information.
2	Functions ports (connected to locks, access controllers, alarm in/out devices)

For details about power port, network port and other ports, see Figure 1-7 .

Figure 1-7 Cable connection



1.4.2 75 Series

Figure 1-8 Rear panel

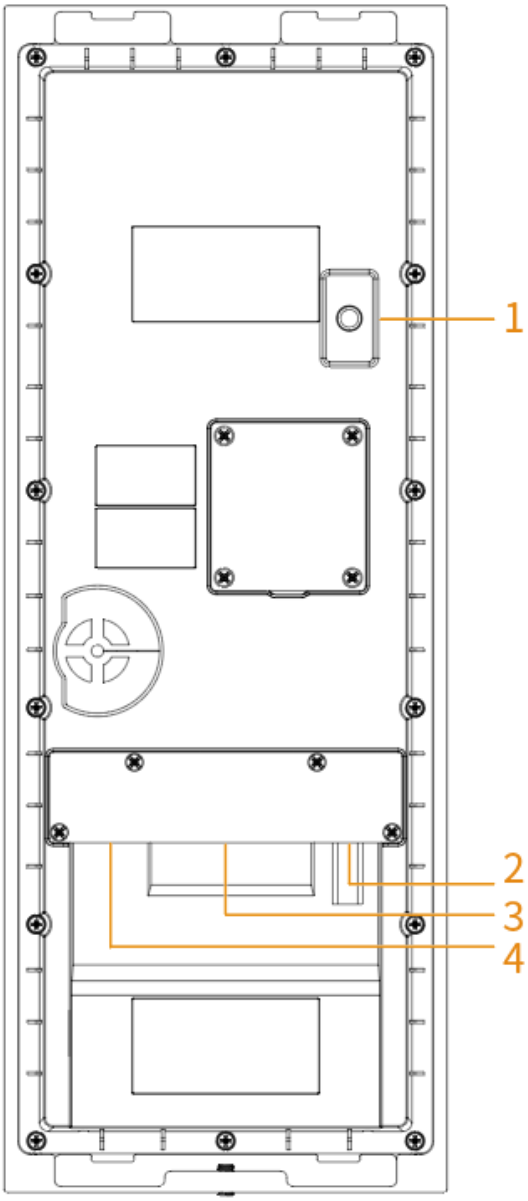
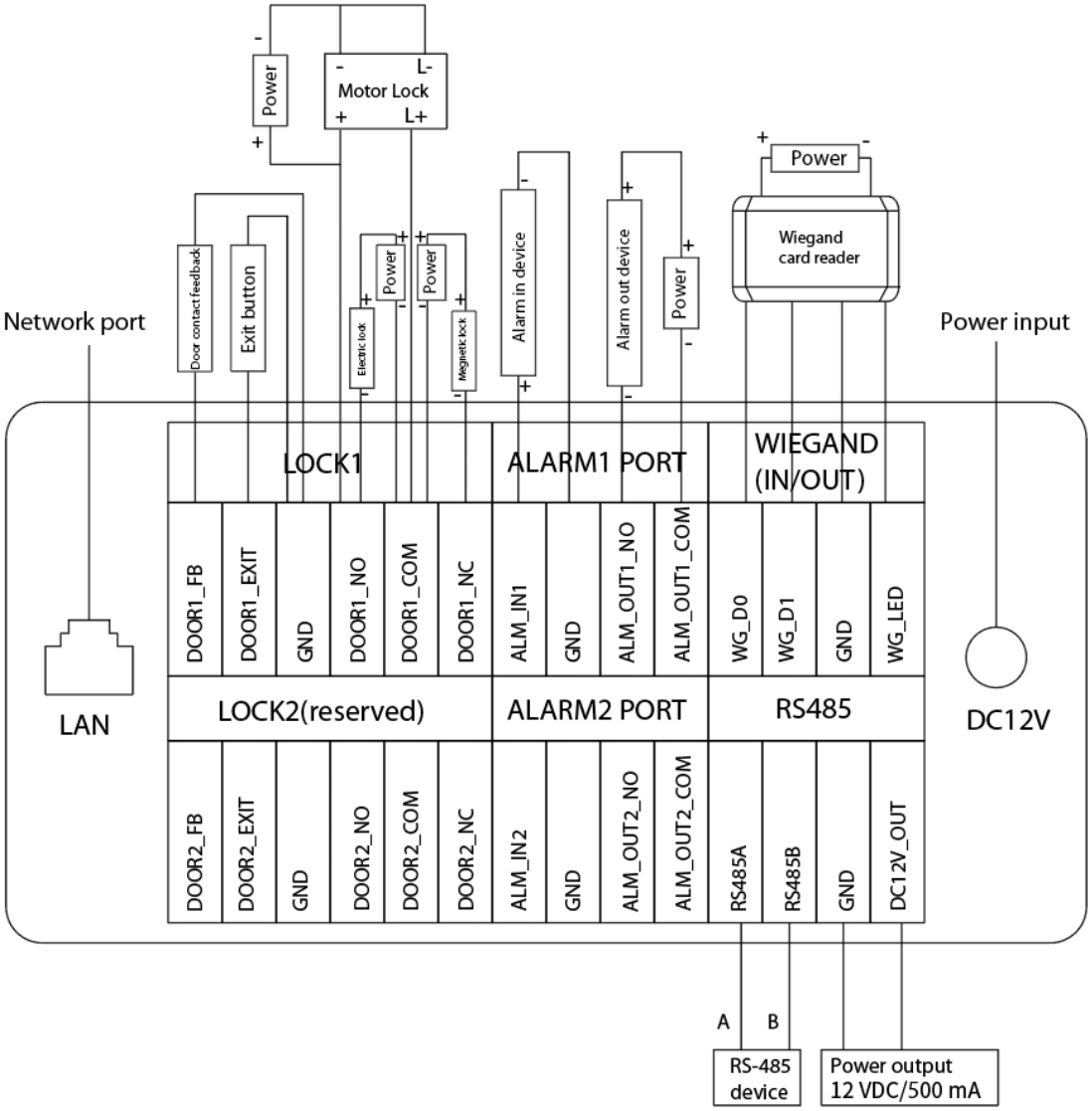


Table 1-7 Component description

No.	Description
1	Tamper button Within 10 minutes after the device is powered on, if you continuously press the tamper button for 5 times in 8 seconds, the device beeps and deletes the account information.
2	Power port
3	Function ports (such as alarm in/out port, lock port, and wiegand port)

No.	Description
4	Ethernet port

Figure 1-9 Cable connection



1.4.3 95 Series

Figure 1-10 Rear panel

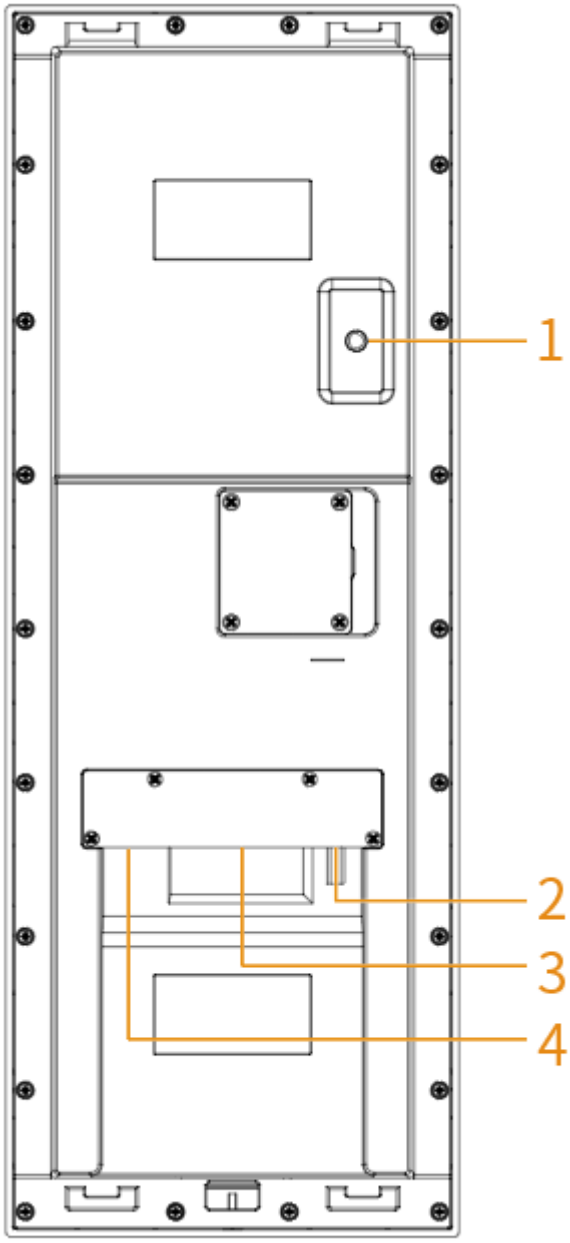
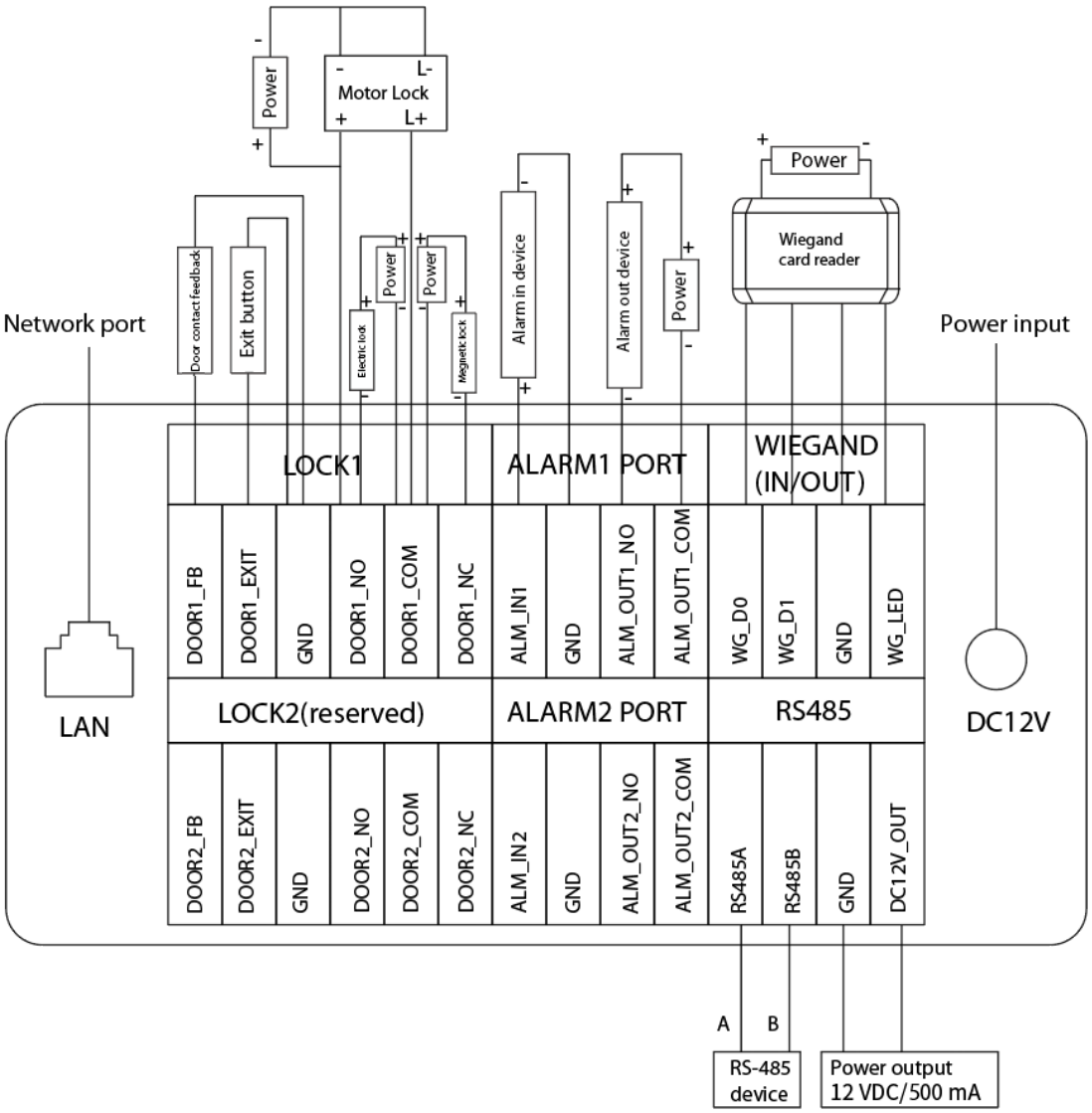


Table 1-8 Component description

No.	Description
1	Tamper button Within 10 minutes after the device is powered on, if you continuously press the tamper button for 5 times in 8 seconds, the device beeps and deletes the account information.
2	Power port

No.	Description
3	Function ports
4	Network port

Figure 1-11 Cable connection



1.4.4 7 Series

Figure 1-12 Rear panel

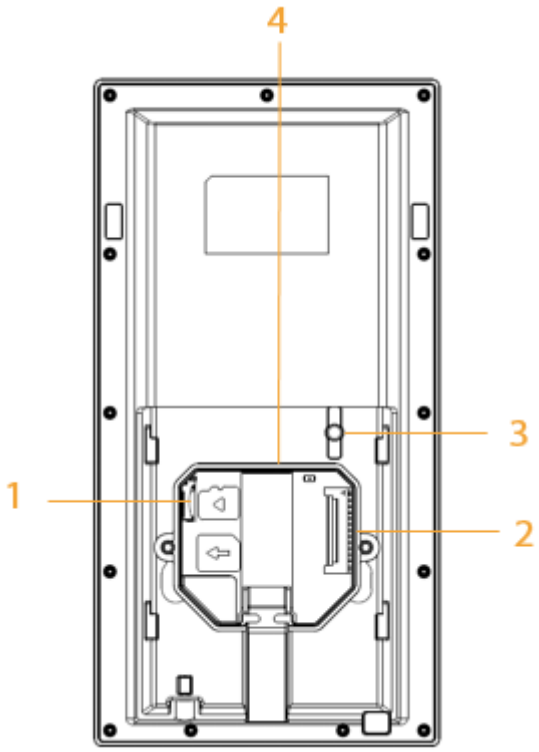
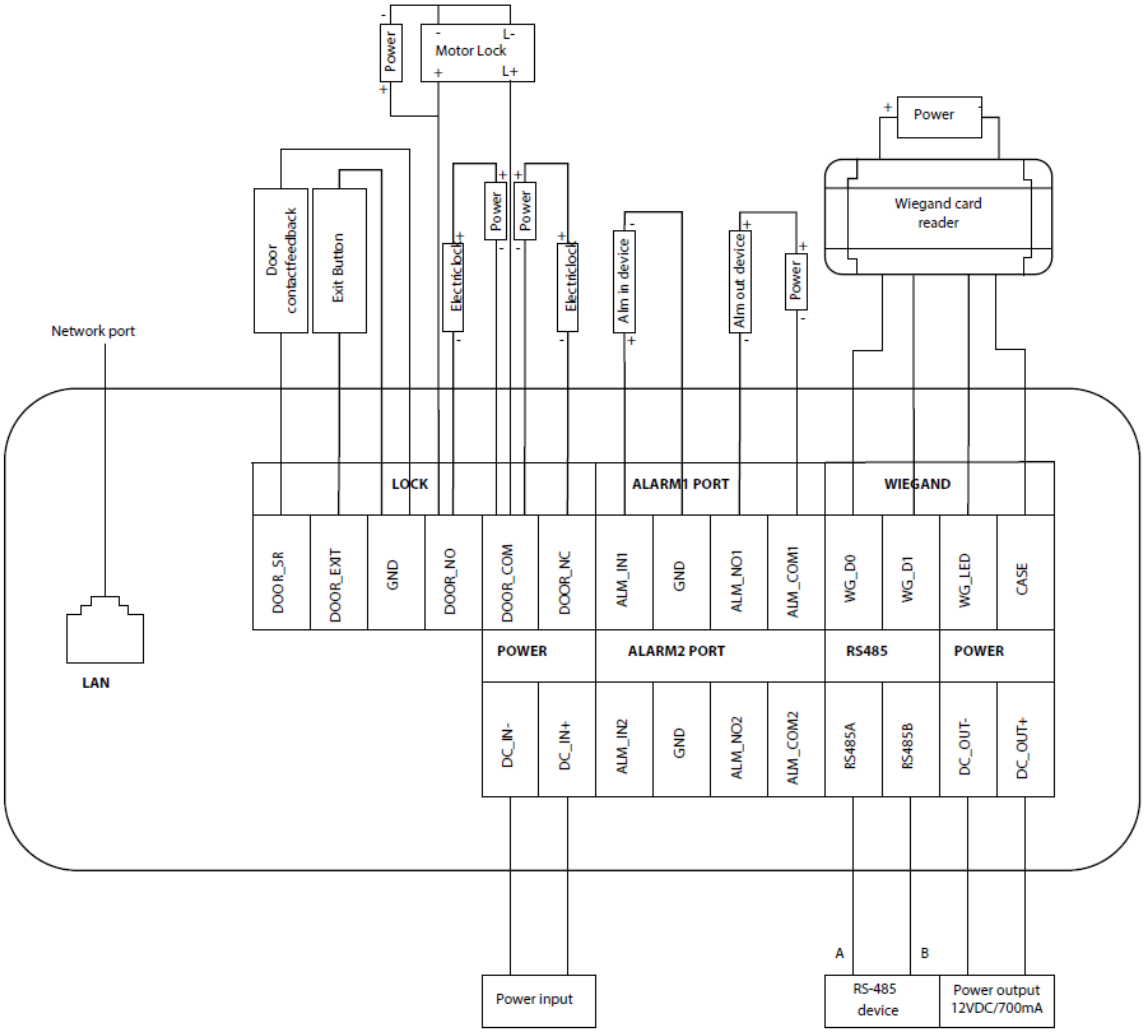


Table 1-9 Component description

No.	Description
1	SD card slot
2	Function ports, such as DC_IN/OUT, alarm in/out port, lock port, RS-485 port, and wiegand port.
3	Tamper button
4	Ethernet port

Figure 1-13 Cable connection



1.4.5 9 Series

Figure 1-14 Rear panel

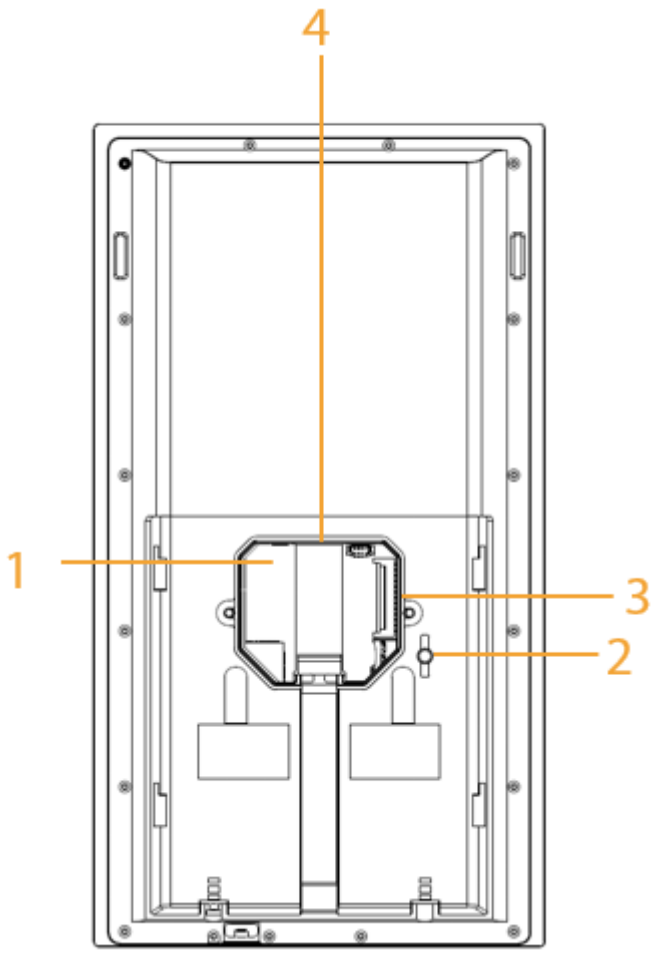
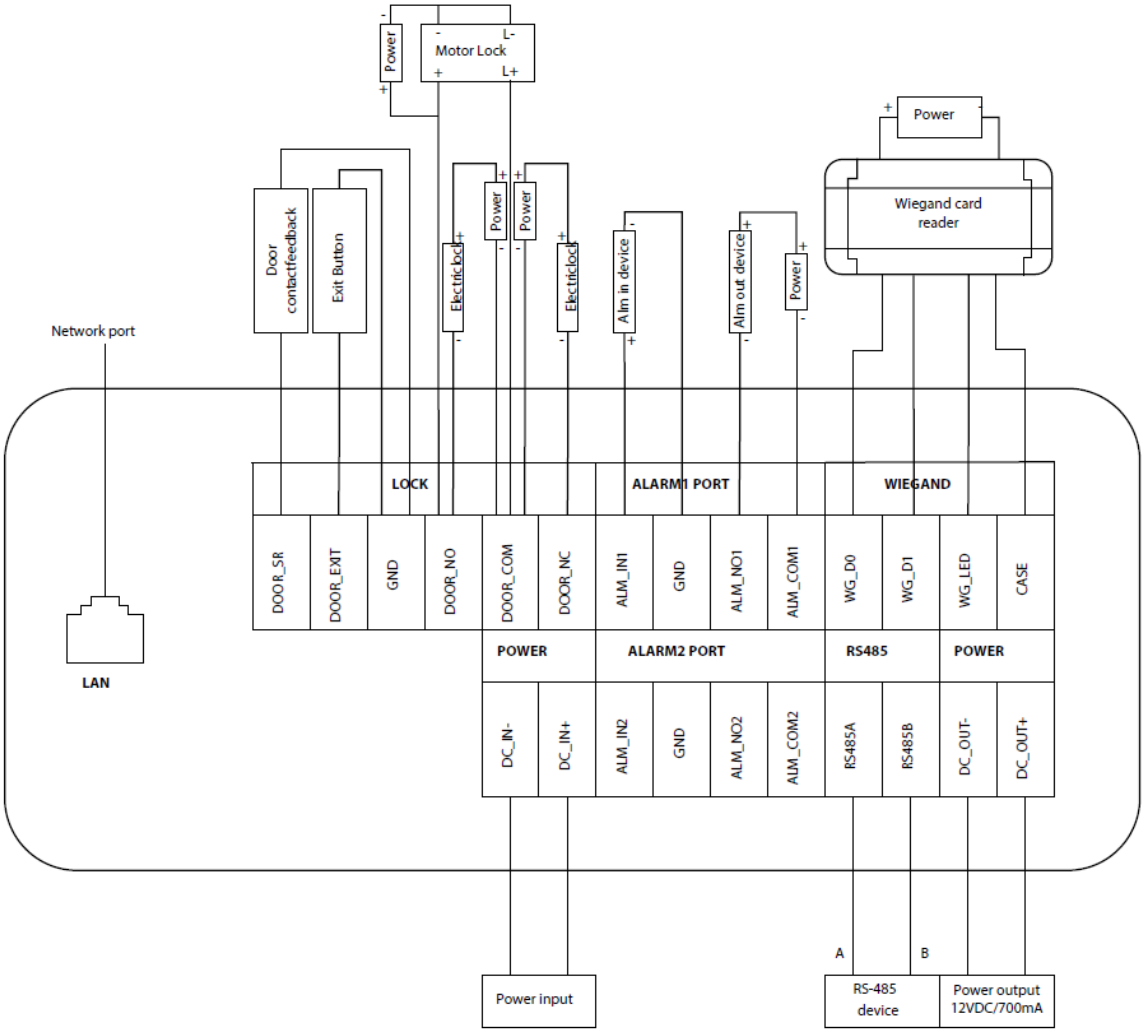


Table 1-10 Component description

No.	Description
1	Audio output port
2	Tamper button
3	Function ports
4	Ethernet port

Figure 1-15 Cable connection



2 VTO Operation

This chapter introduces the operations on the devices and uses 2 types as examples according to the displayed screen.

2.1 65 Series

The 65 series devices use the following screen style.

The following snapshots of the devices are for reference only, and slight differences might be found in the operation screen of the VTO, depending on your model.

2.1.1 Home Screen

Figure 2-1 Home screen (with face detection)

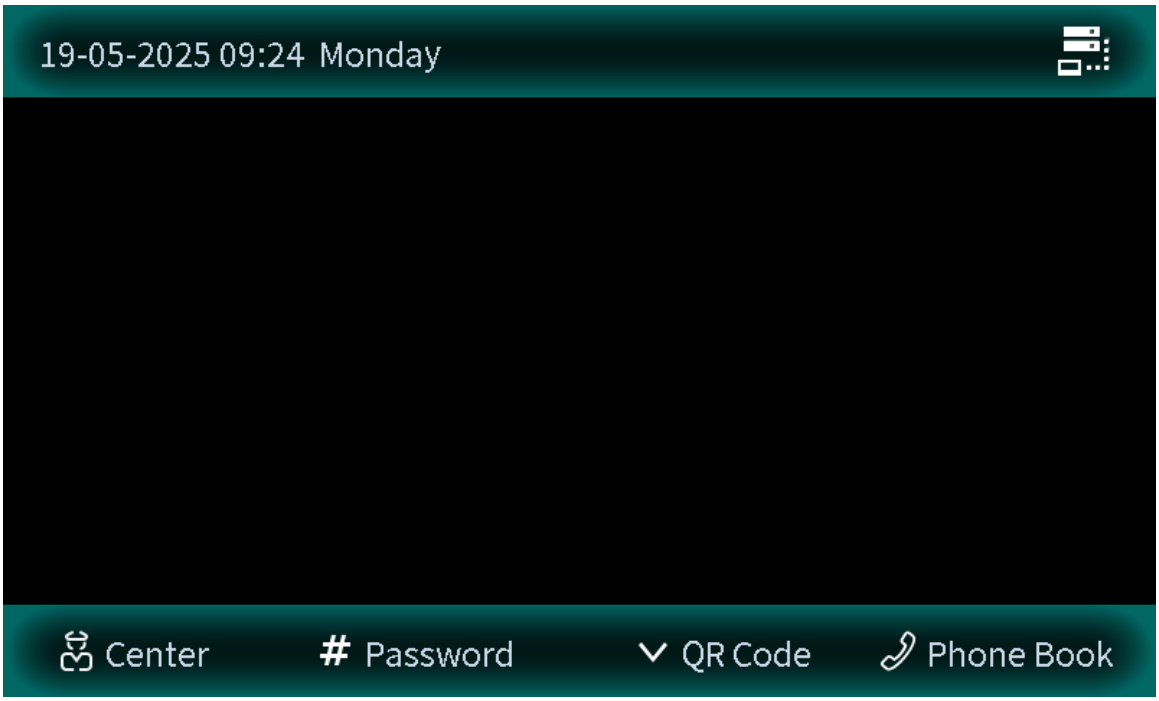


Figure 2-2 Home screen (without face detection)

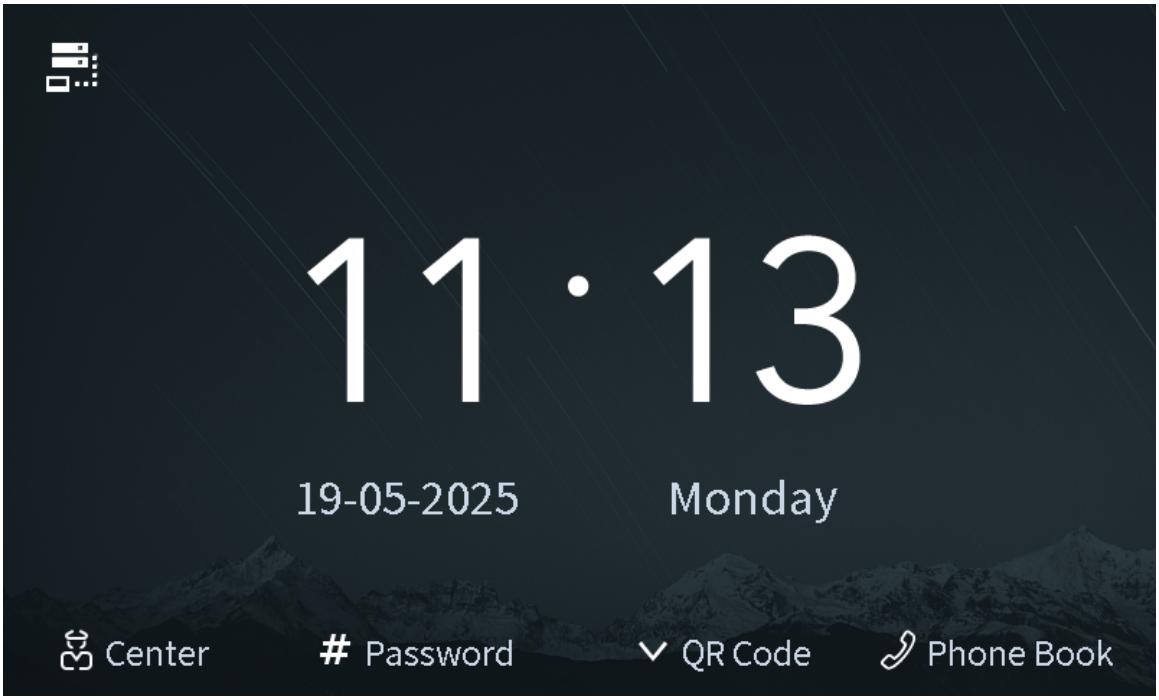
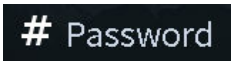


Table 2-1 Description of the home screen instructions

Instruction	Description
	Displays the status of the SIP server.
	Press it, and then call the management center.
	Press #, and then enter the password to open the door.
	Press , and then scan the QR code to open the door.
	Press to view the phonebook.

2.1.2 Engineering Setting

The engineering setting is intended for administrators to make advanced configurations to the VTO, including issuing access cards, modifying device IP address, and adding person.

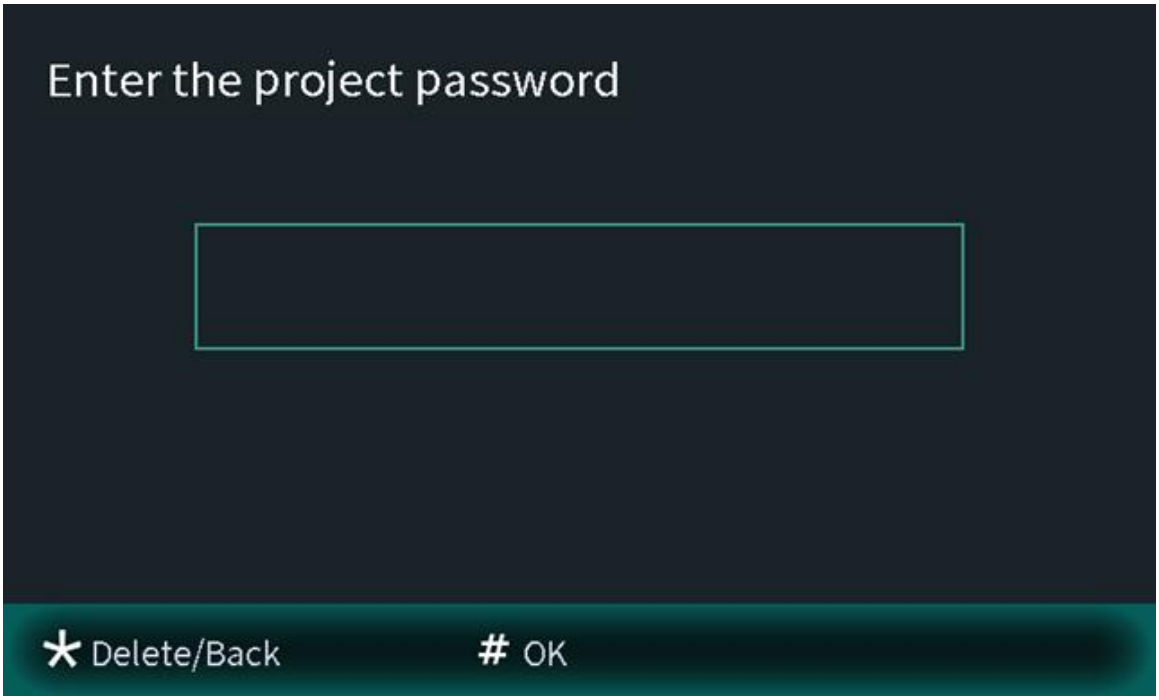
Procedure

Step 1 Press * on the VTO when the home screen is displayed.

Step 2 Enter the project password.

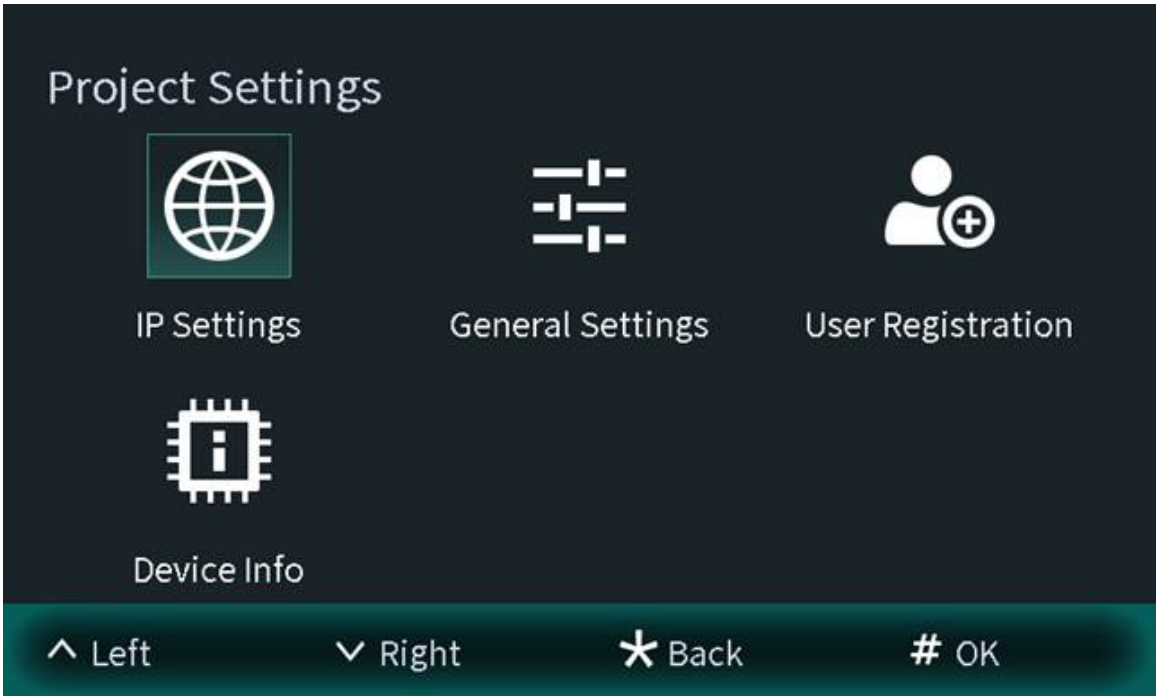
You need to set the project password by selecting **Local Setting** > **Access Control** > **Config** on the webpage of the VTO.

Figure 2-3 Enter the password



Step 3 Press # to enter the engineering setting.

Figure 2-4 Engineering setting



2.1.2.1 Configuring IP Address

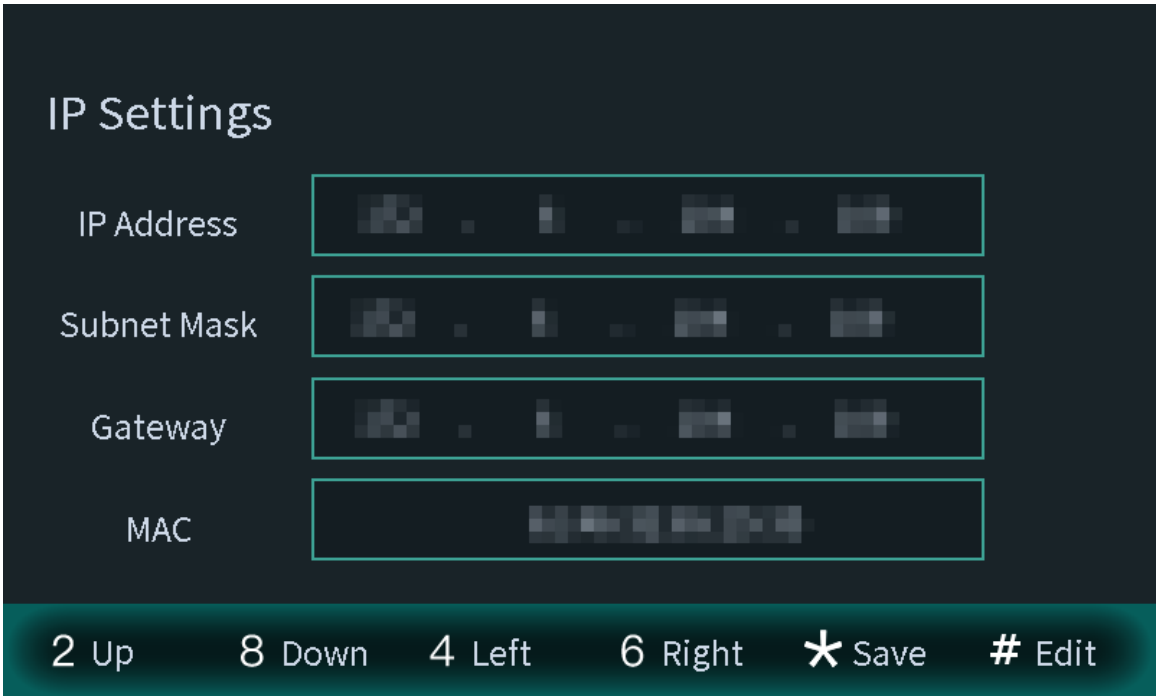
Configure the IP address of the VTO.

Procedure

Step 1 Select **IP Settings** on the **Engineering Setting** screen.

Step 2 Enter the IP address, subnet mask, and gateway.

Figure 2-5 Configure the IP



Step 3 Press * to complete the settings.

2.1.2.2 General Settings

Select **General Settings** to configure the volume, screensaver time and the screen light up time. After configuration, press * to save and go back to **General Settings** screen.

Volume

Press ⌄ to increase the device and VTO volume.

Press ⌃ to decrease the device and VTO volume.

Figure 2-6 Configuring the volume

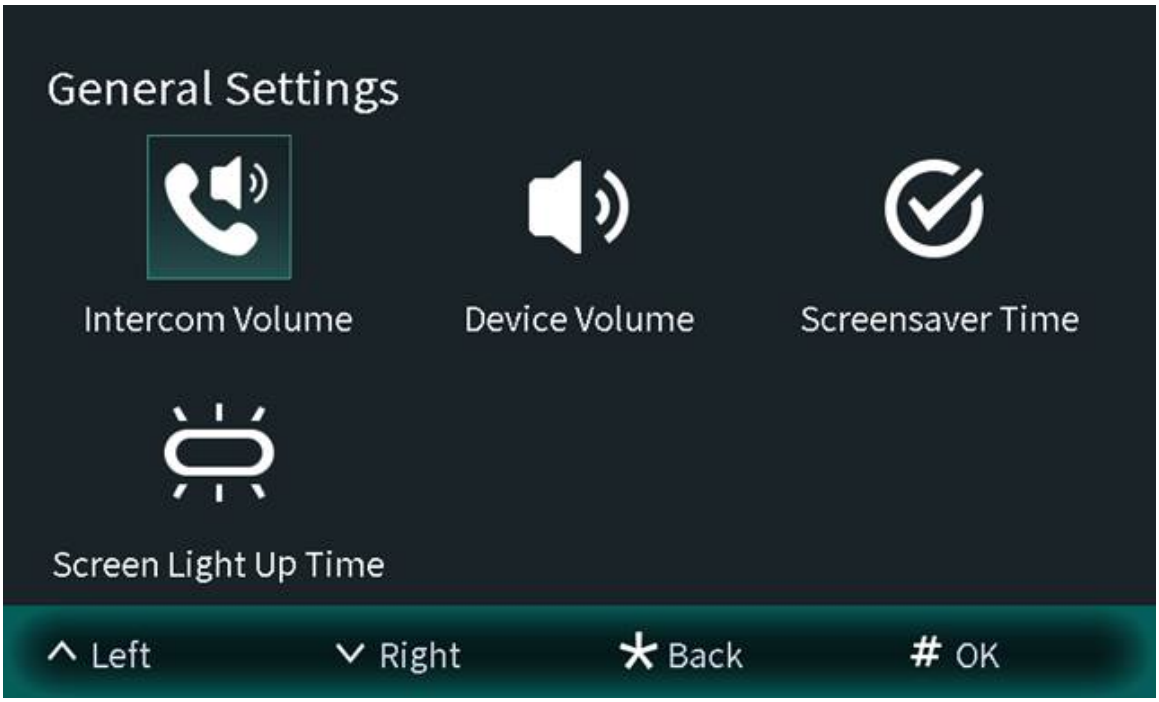


Figure 2-7 Configuring the device volume

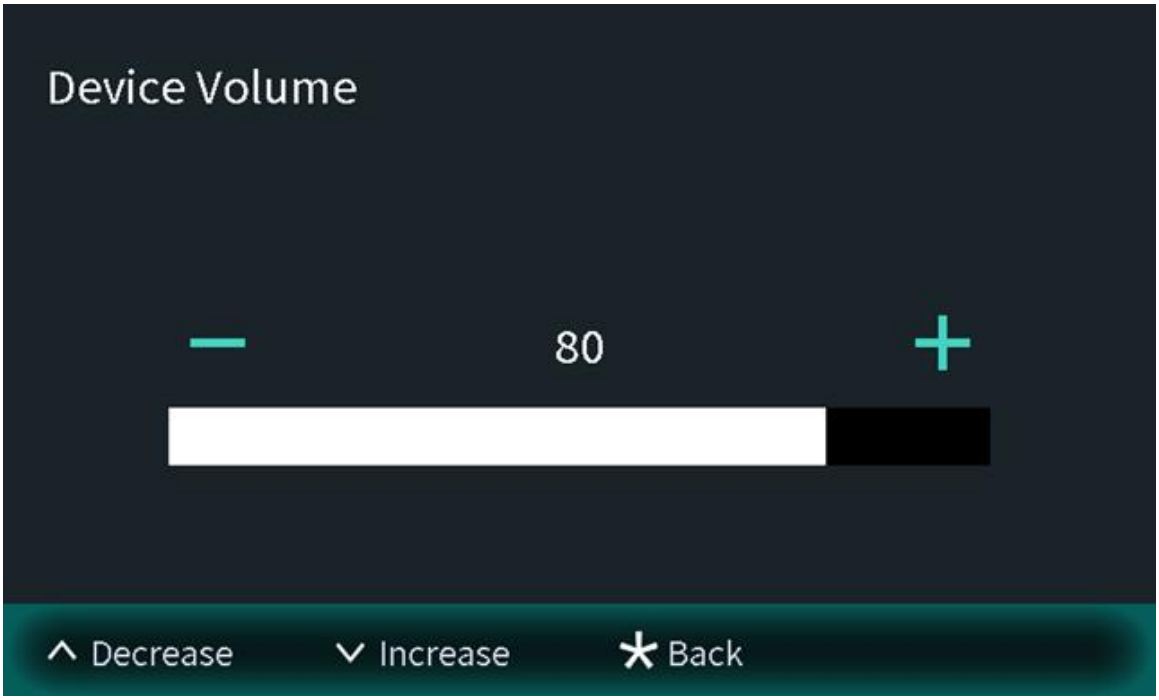
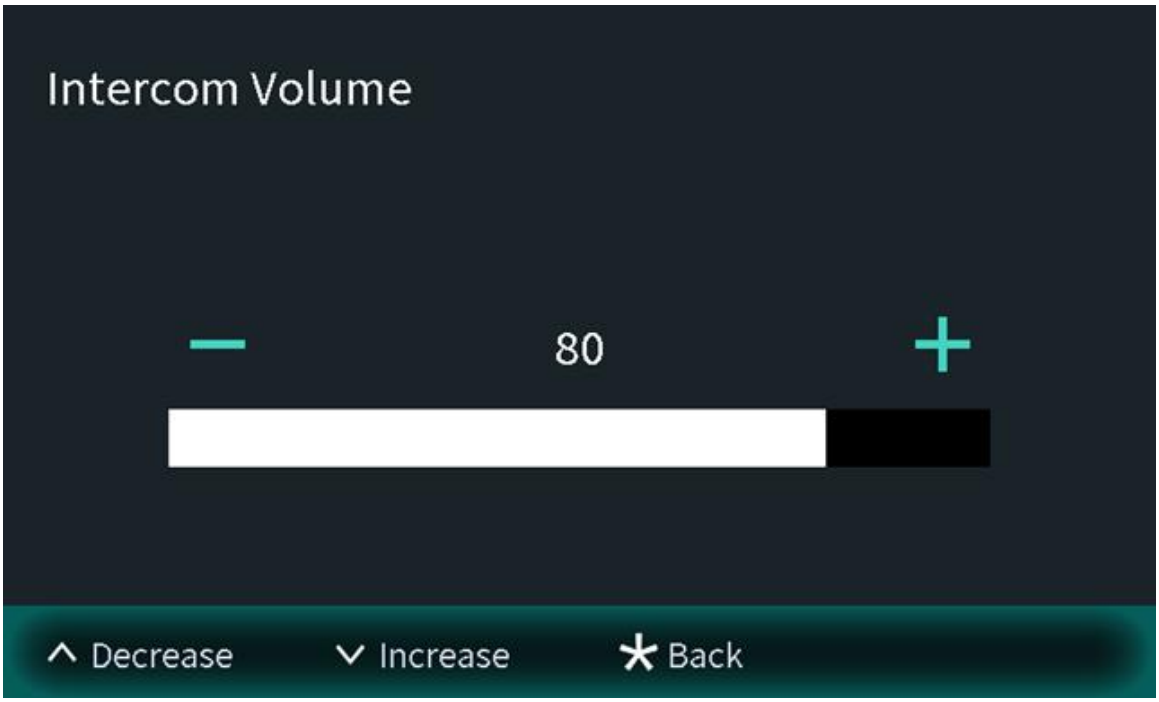


Figure 2-8 Configuring the intercom volume



Screensaver time

Press to increase the screensaver time.

Press to decrease the screensaver time.

Figure 2-9 Screensaver time

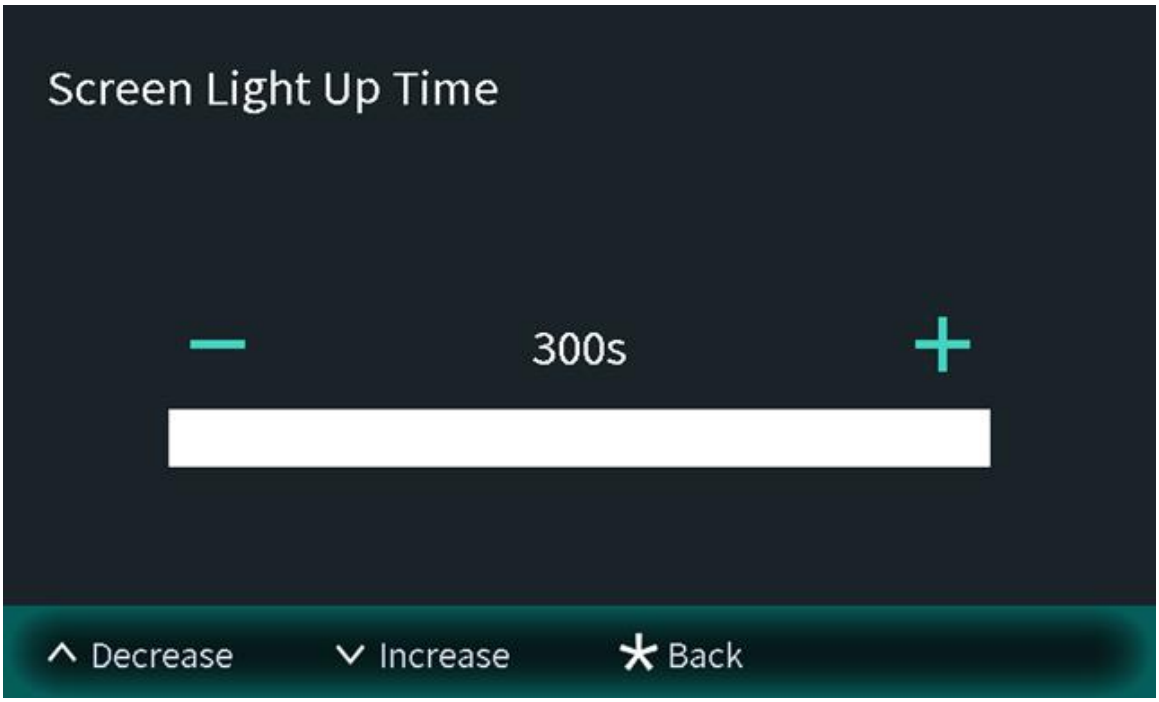


Screen Light Up Time

Press to increase the screen light up time.

Press to decrease the screen light up time.

Figure 2-10 Screen light up time



2.1.2.3 User Registration

You need to register users to unlock doors. Unlocking methods include card, face, fingerprint, QR code and password. You can add unlocking methods after configuring personnel information.

- If the current VTO or another VTO works as the SIP server, register the user on the VTO.
- If the platform works as the SIP server, the platform sends the information of face images, fingerprints and cards to the VTO.

The unlocking methods might differ depending on the actual products. Some methods are available in select models.

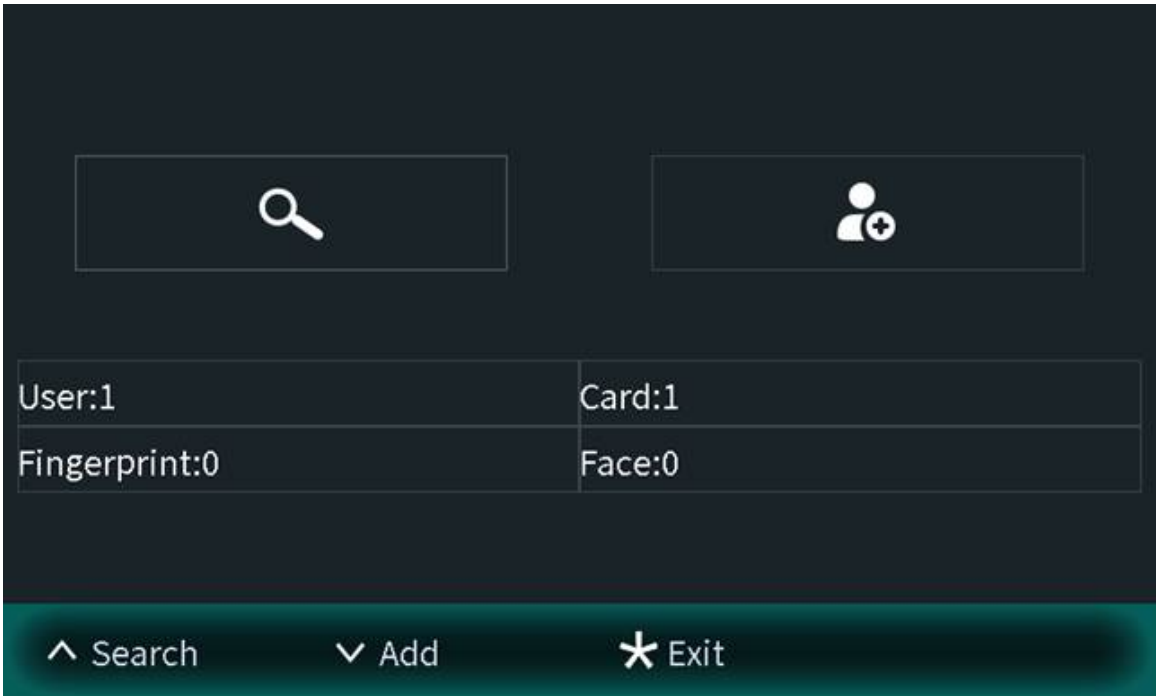
2.1.2.3.1 Adding Users

Basic information includes person ID, room number.

Procedure

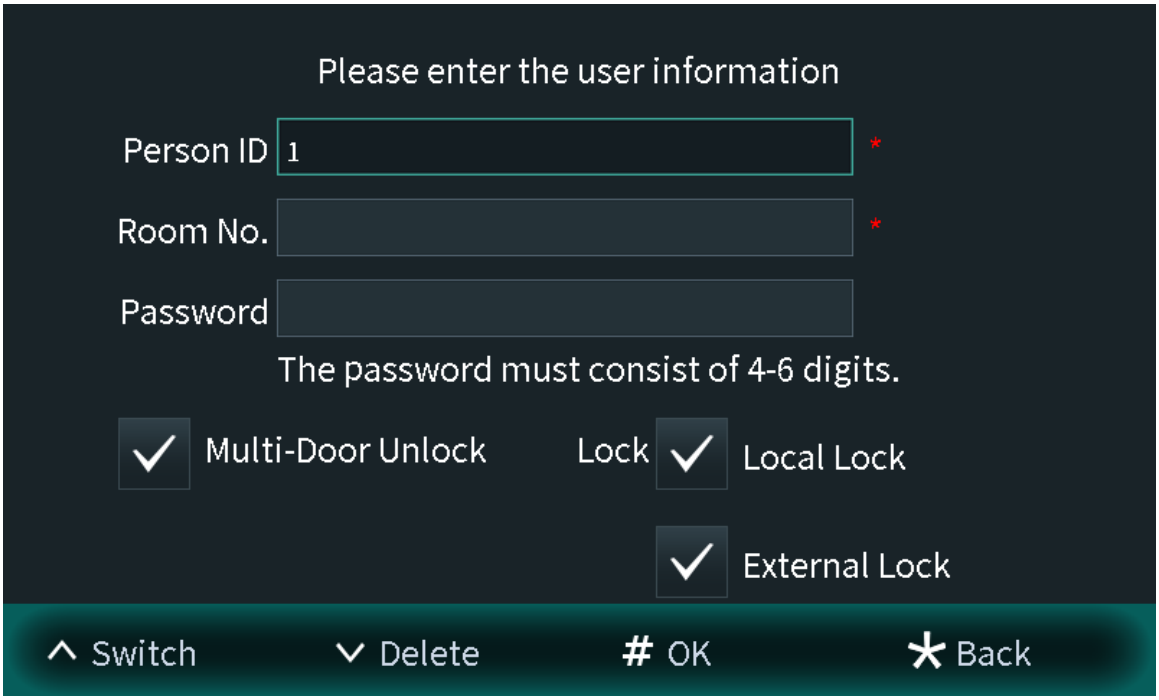
Step 1 Select **User Registration** on the **Engineering Setting** screen.

Figure 2-11 User registration



Step 2 Press to add the user.

Figure 2-12 Add the user



Step 3 Enter the person ID and room number, configure the locks and then press # to save the information.

2.1.2.3.2 Adding Faces

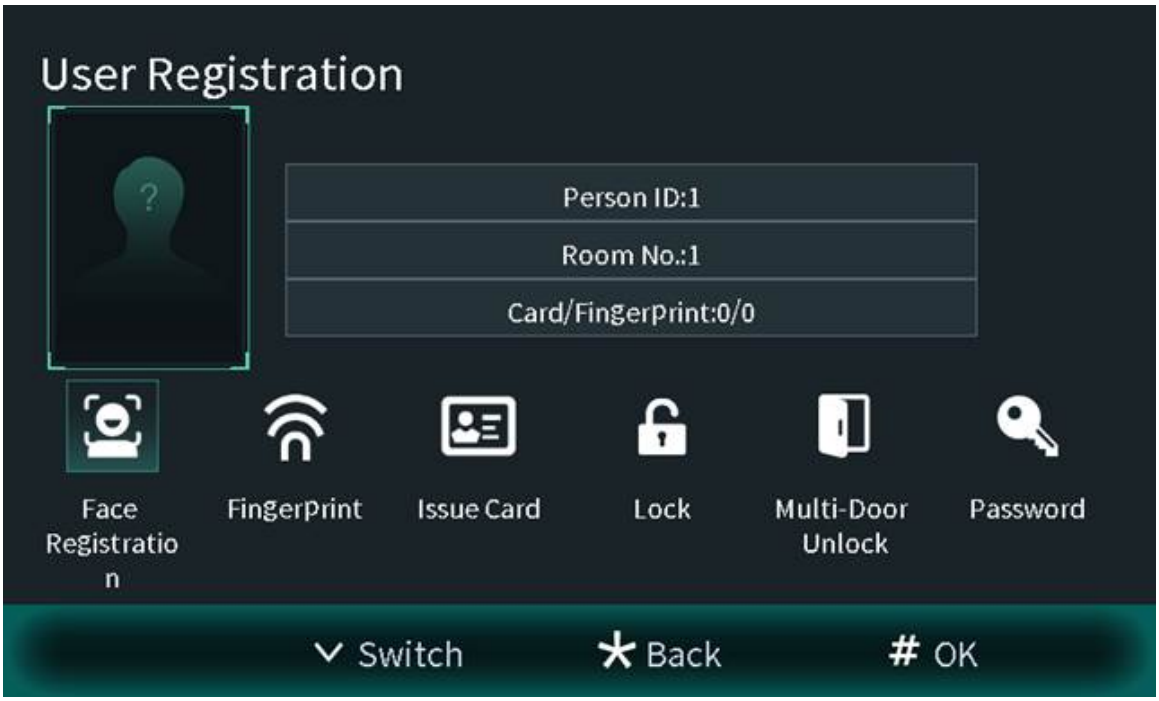
Add faces of registered users to unlock the door.

Recognition of the face is available in select models.

Procedure

Step 1 Select **Face Registration** on the **User Registration** screen.

Figure 2-13 Face registration



Step 2 Position your face in the middle of the frame, and the face image will be automatically taken.

The face image will be automatically taken. If you are not satisfied with the image, press * to cancel the photo.

Figure 2-14 Face registration



Step 3 Press**#** to save the photo.

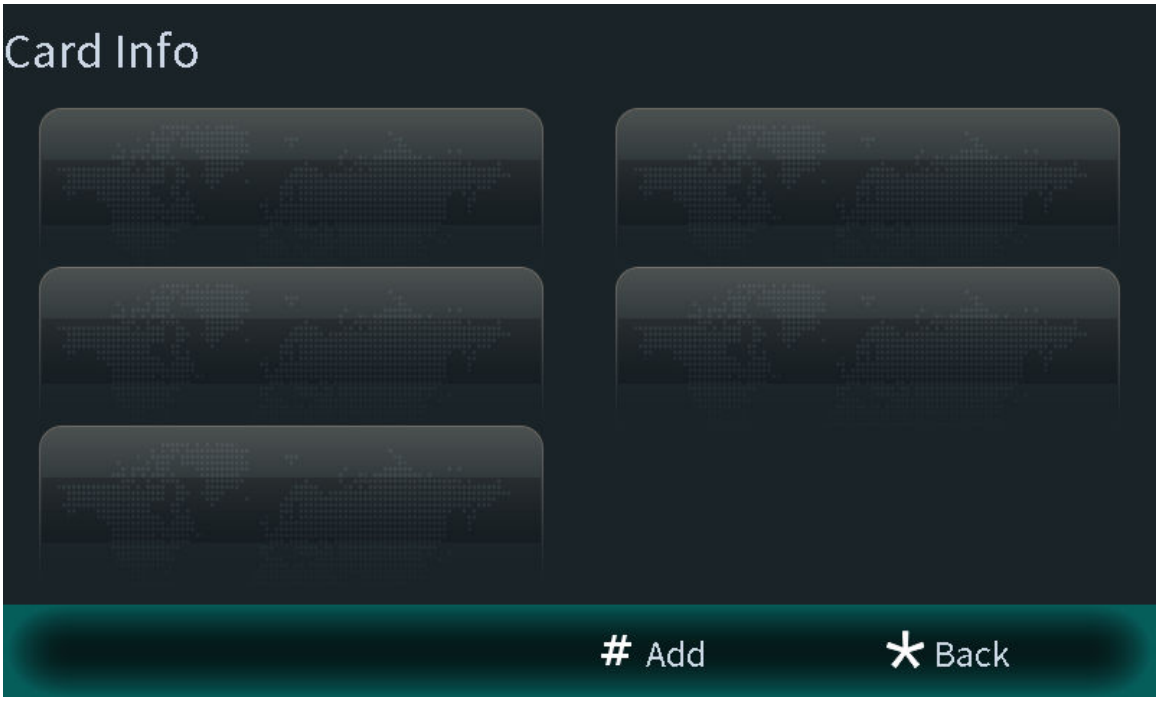
2.1.2.3.3 Issuing Cards

You can issue up to 5 cards for each user.

Procedure

Step 1 Select **Issue card** on the **User Registration** screen, and then press **#** to add the card.

Figure 2-15 Card information

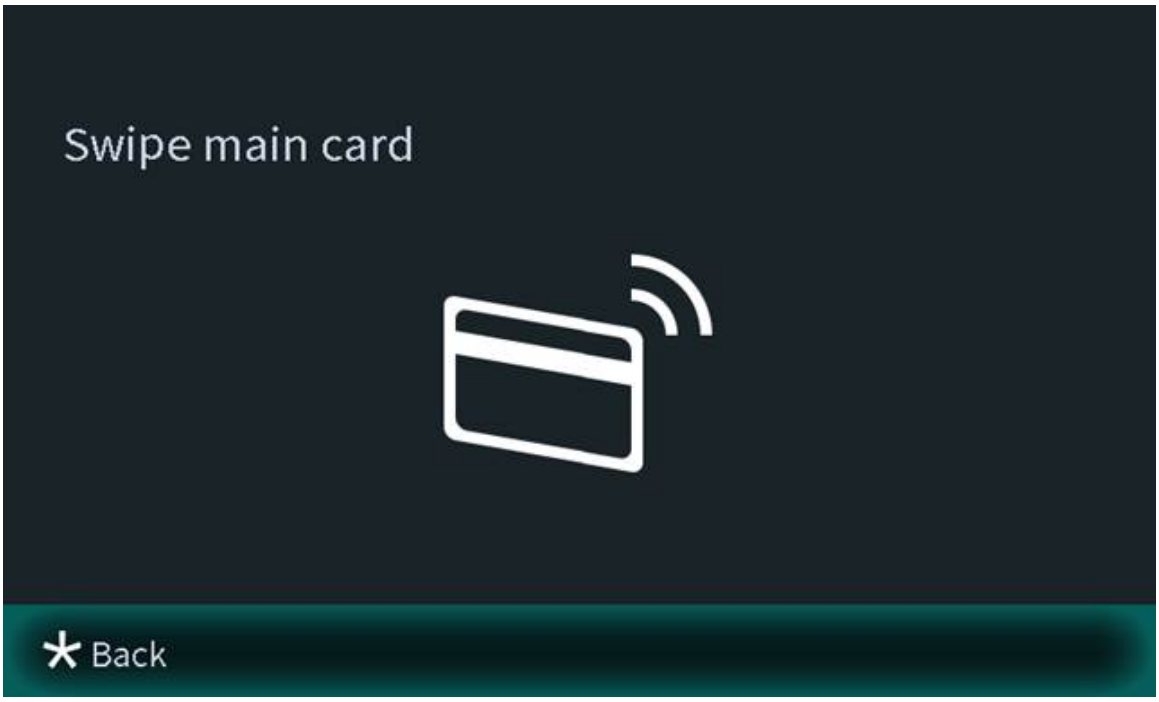


Step 2 Select **Main card** or **password** to issue cards.

1. Select **Main Card** if you want to issue cards through the main card, and then swipe your main card on the card reader to continue the card issuing process.

   If you do not have a main card, issue a card on the VTO through password. Then go to the webpage of the VTO, select **Person Management** , and then set a card as your main card or general card by clicking or .

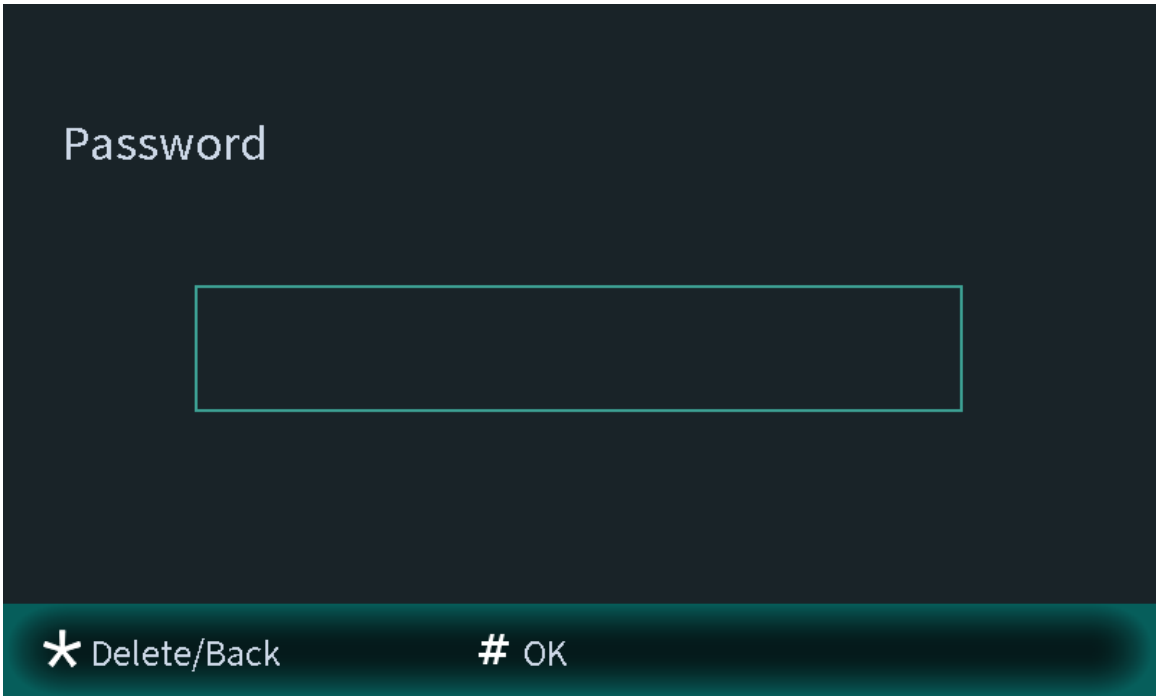
Figure 2-16 Swiping the main card



2. Select **Password** if you want to issue cards through the password. Enter the password, and then press **#**.

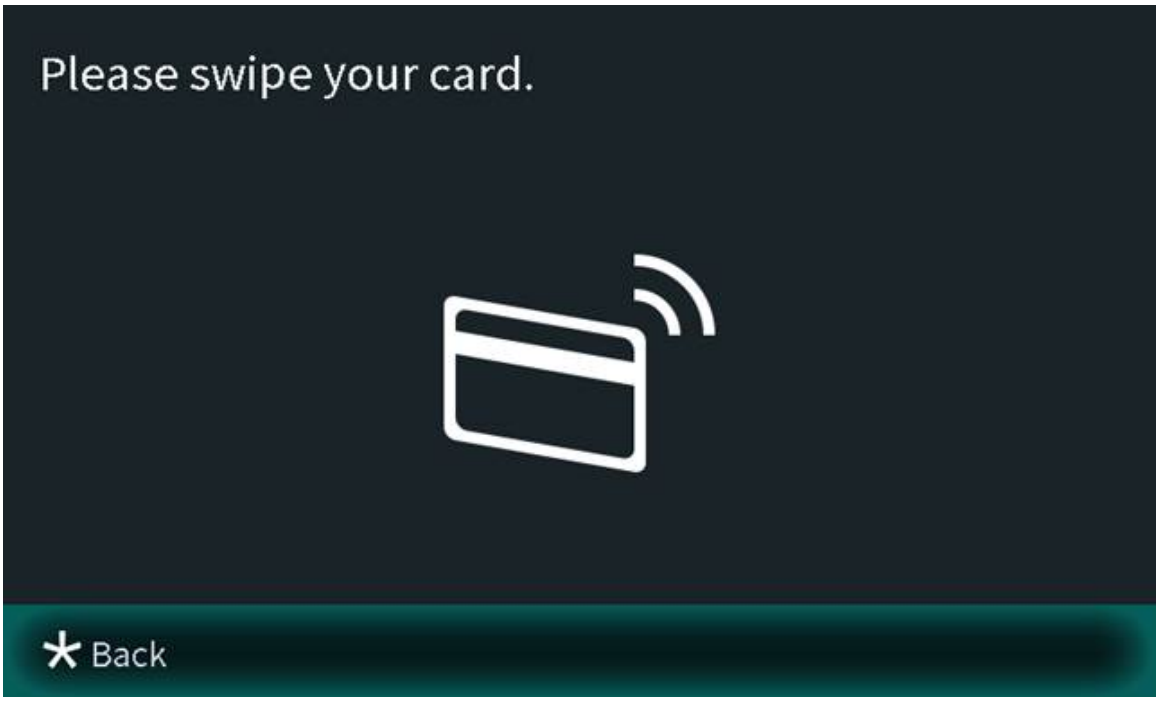
   You need to enter the password in **Issue Card Password** textbox that you planned on the webpage of the VTO through **Local Setting** > **Access Control** > **Config**.

Figure 2-17 Main card password



Step 3 Swipe cards on the card reader, and card numbers will be automatically recognized.

Figure 2-18 New card registration



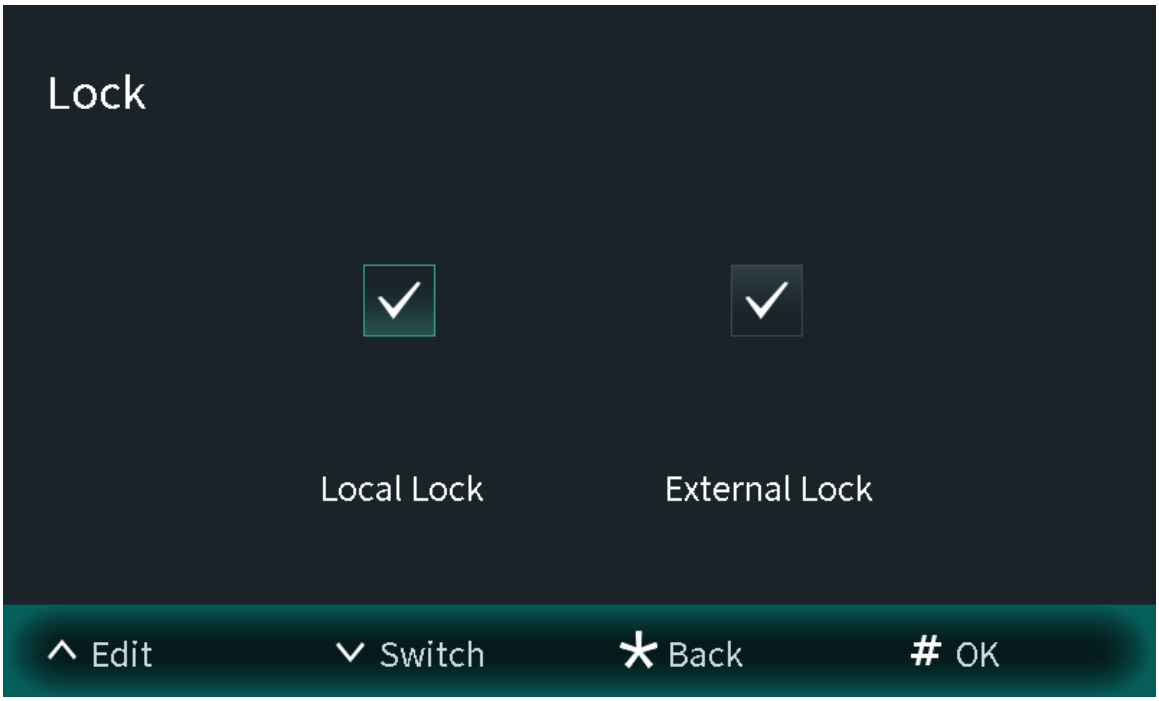
2.1.2.3.4 Configuring the Locks

Select **Lock** on the **User Registration** screen to configure the authority for opening the local lock and the external lock.

- Select **Local Lock**, and the user will have authority to open the local lock.

- Select **External Lock**, and the user will have authority to open the second lock that connects to the VTO through the function port.

Figure 2-19 Lock



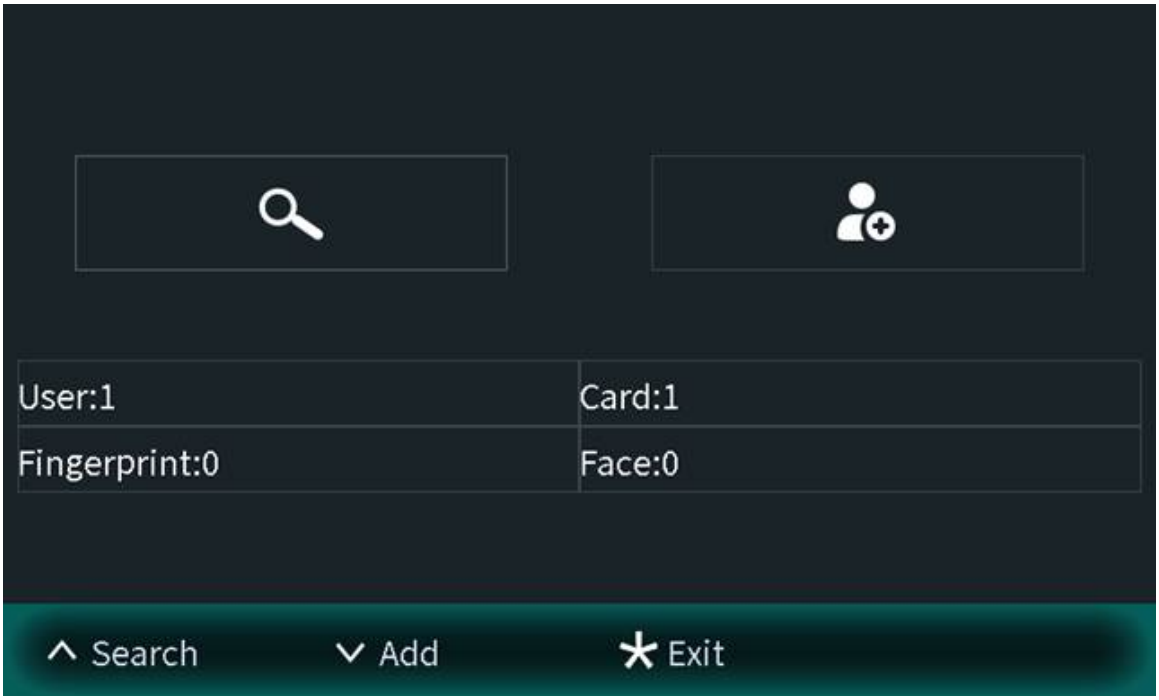
2.1.2.3.5 Searching for the User

View the user information according to the person ID or the room number. You can configure the user information.

Procedure

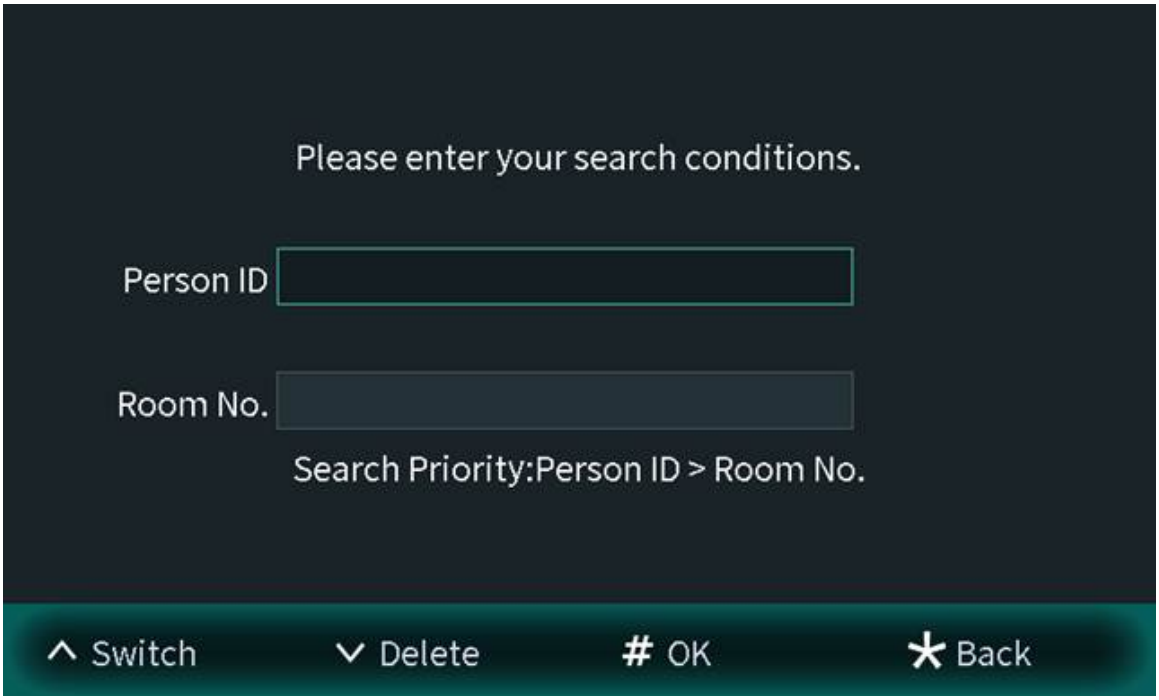
Step 1 Select **User Registration** on the **Engineering Setting** screen.

Figure 2-20 User registration



Step 2 Press ^, and then enter the person ID number or the room number.

Figure 2-21 Searching for the user



Step 3 Press # to view the user information.

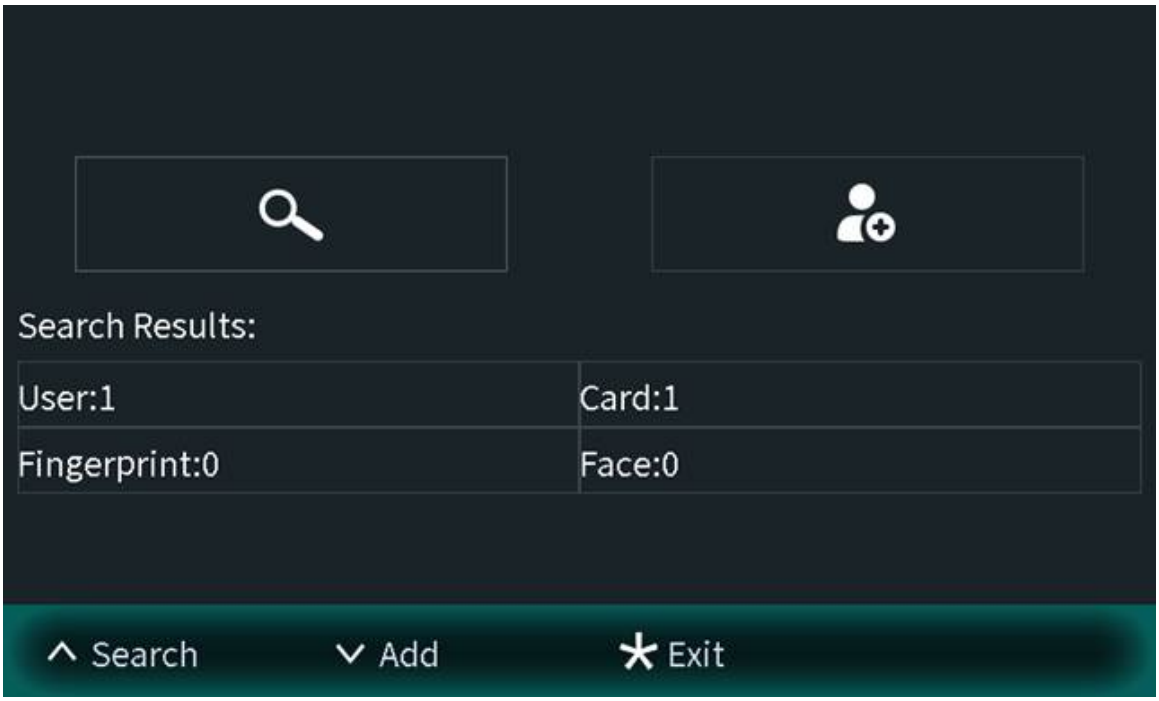
- Enter the person ID number to view the user information. You can also configure the face images, cards and locks.

Figure 2-22 User information



- Enter the room number to view the person IDs, card numbers and face image numbers of the room.

Figure 2-23 Search result



2.1.2.4 Viewing Device Information

You can view the web port number, software version, MCU version, the algorithm version and others.

Procedure

Step 1 Select **Device Info** on the **Engineering Setting** screen.

Step 2 Press ▼/▲ to switch the pages.

Figure 2-24 Device information (1)

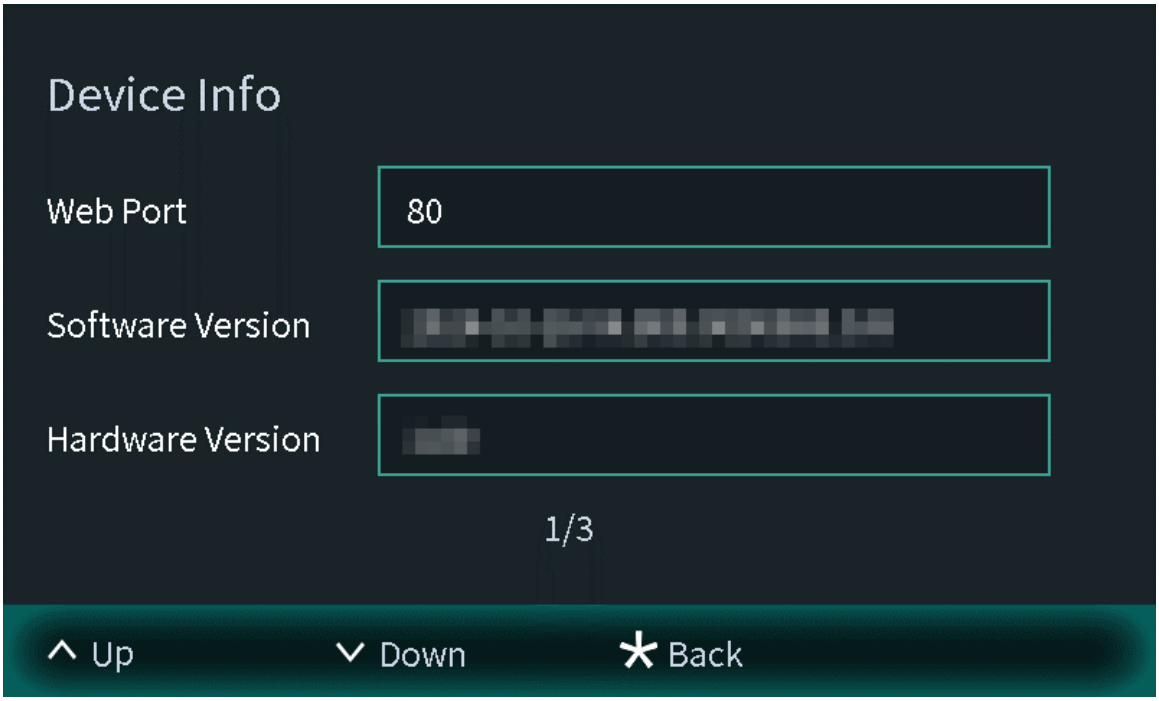


Figure 2-25 Device information (2)

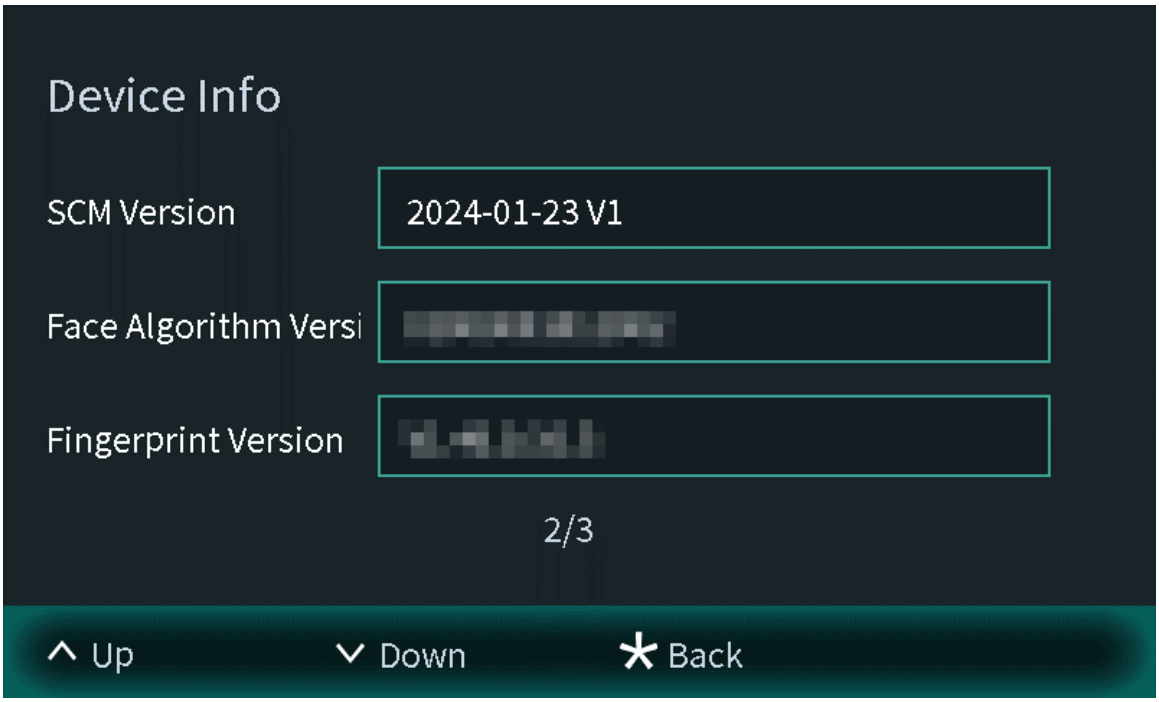
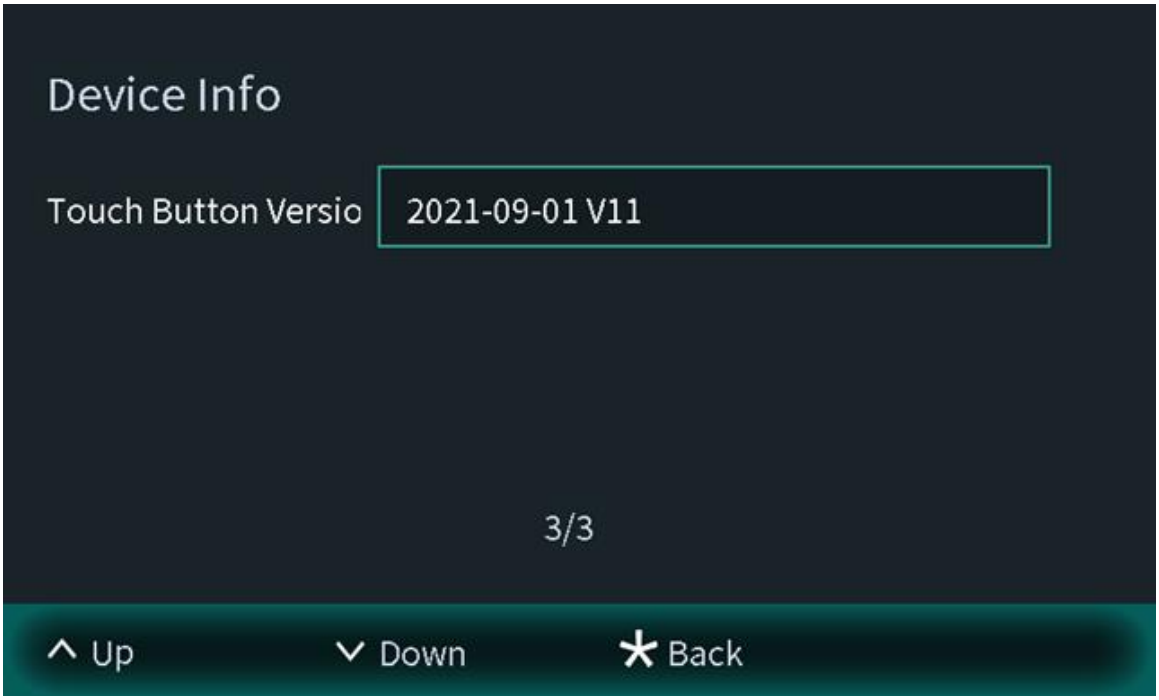


Figure 2-26 Device information (3)



2.2 75/95/7/9 Series

The 75 series and 95 series devices use the following screen style.

The following snapshots of the devices are for reference only, and slight differences might be found in the operation screen of the VTO, depending on your model.

2.2.1 Home Screen

Figure 2-27 Home screen

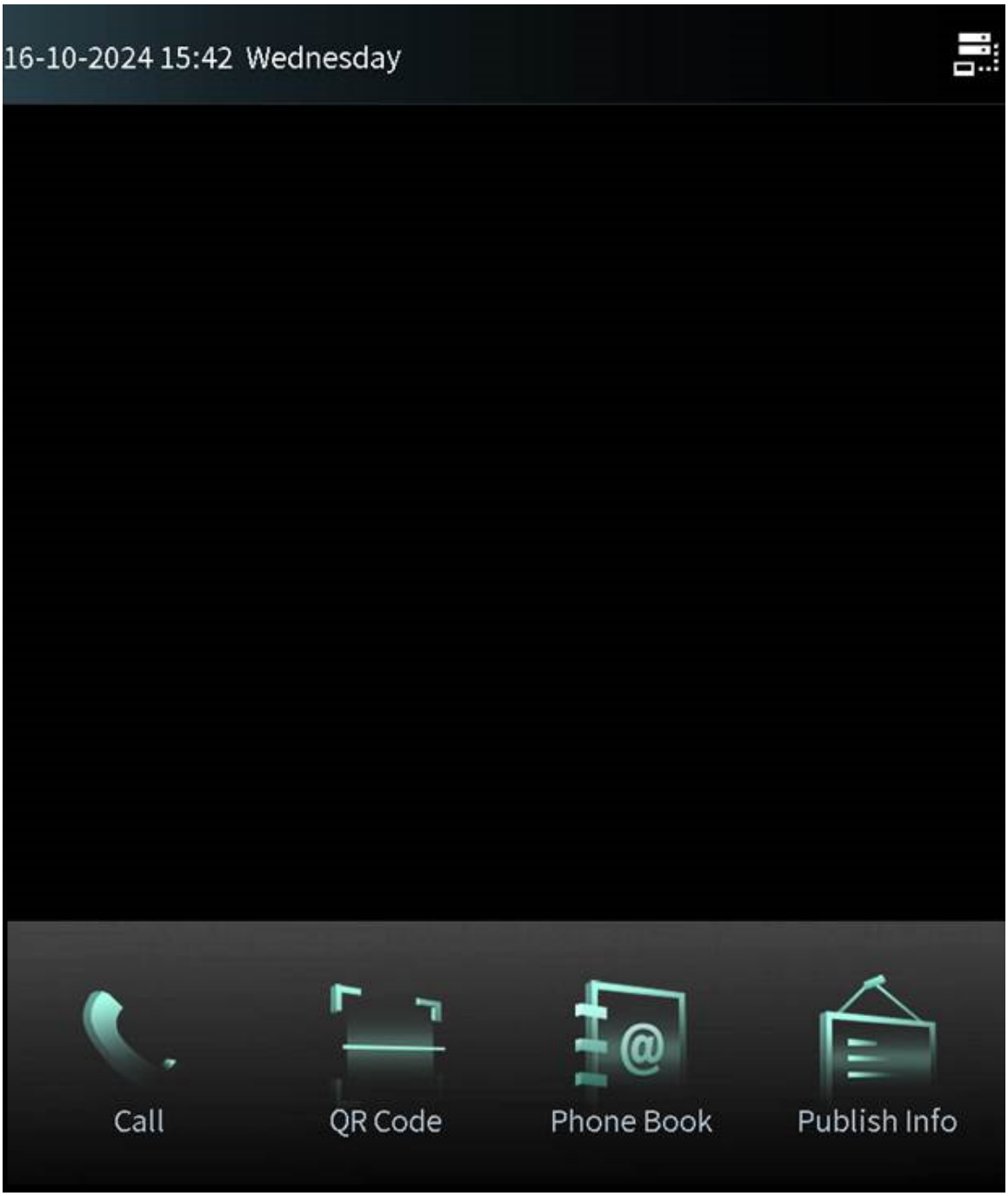


Table 2-2 Description of home screen instructions

Instruction	Description
	Displays the status of the SIP server.
	Call or enter the password to go to the screen of the engineer setting.

Instruction	Description
	Scan the QR code to open the door.
	View the phonebook.
	View the published information.

- 5 shortcuts are supported (including call, QR code, phone book, homeowner registration, and publish info), while up to 4 shortcuts can be customized to be shown in the home screen.
- Customize the shortcut on the webpage through **System** > **Shortcut Settings**.

2.2.2 Engineering Setting

Background Information

- Configure the project password through **Local Setting** > **Access Control** > **Config** on the webpage.
- Only the administrator or the engineer can operate on the engineering setting screen.

Procedure

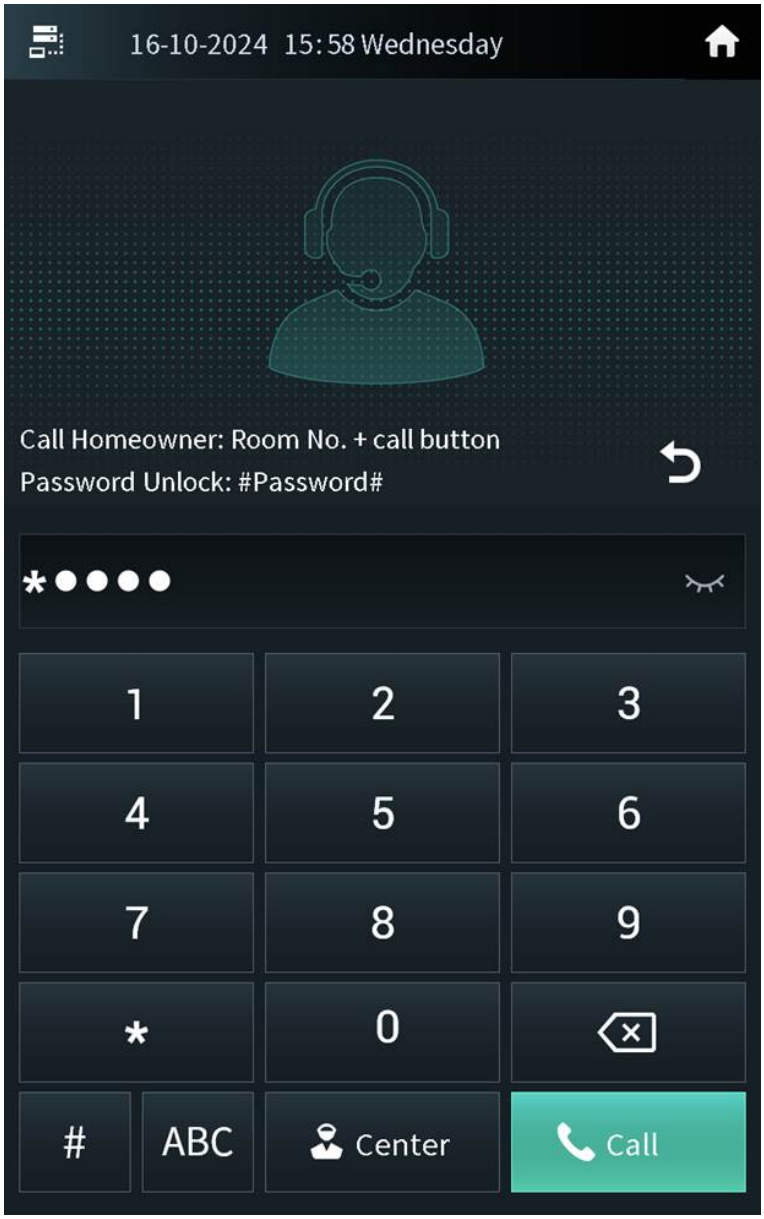
Step 1 Power on the VTO.

Step 2 Tap  on the home screen.

Step 3 Enter the password to go to the screen of the engineering setting.

- The password is *+project password+#. For example, if you configure the project password as 888888 on the webpage, enter *888888# to go to the screen of the engineering setting.
- You can also press and hold on the home screen, and then enter the admin password to go to the screen of the engineering setting.

Figure 2-28 Enter the password



2.2.2.1 Configuring the IP Address

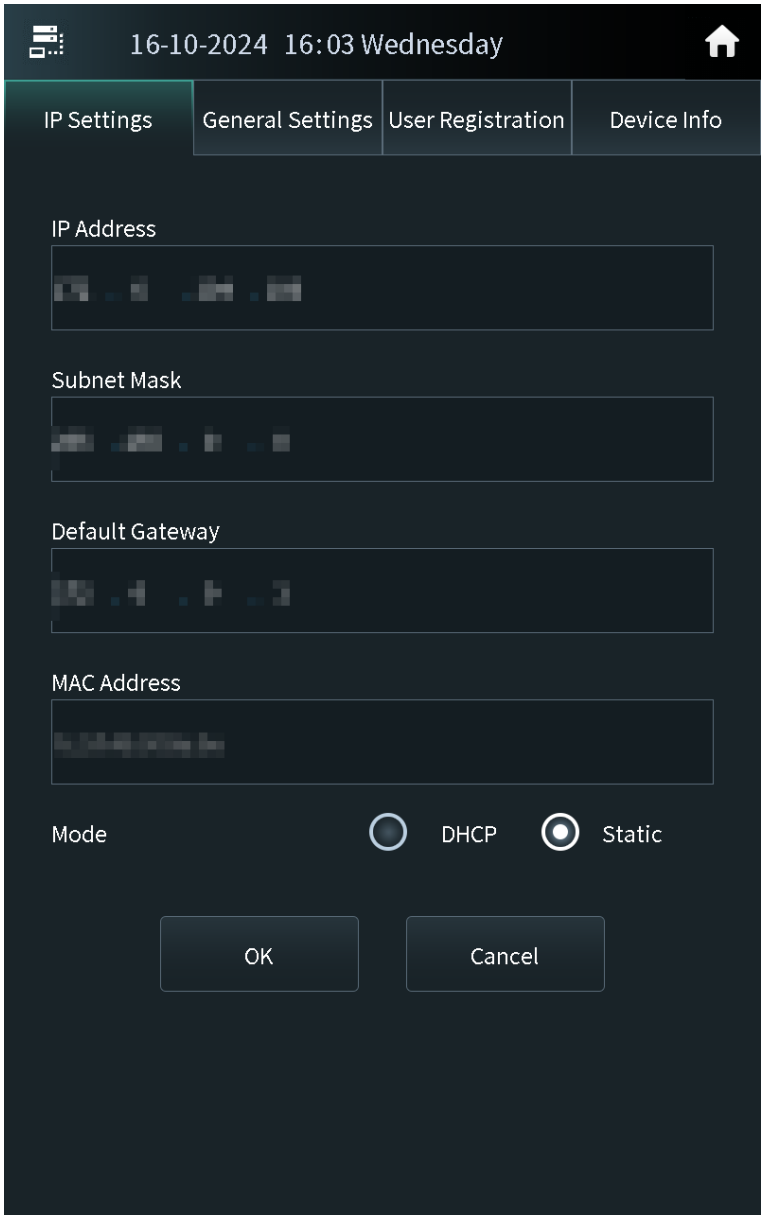
Configure the IP address of the VTO according to your actual network plan.

Procedure

Step 1 Press **IP Settings** on the screen of the engineer setting.

Step 2 Enter the IP address, subnet mask and the gateway.

Figure 2-29 IP settings



Step 3 Press **OK**.

2.2.2.2 General Settings

Configure the volume, screen light up time and other parameters.

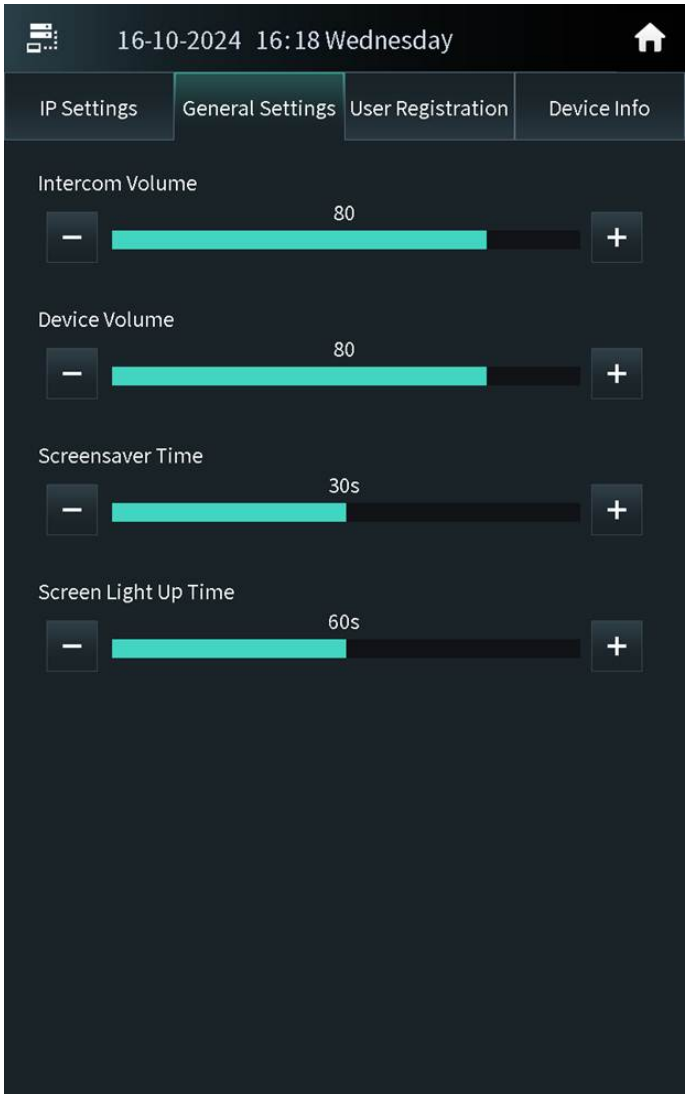
Procedure

Step 1 Press **General Settings** on the screen of the engineer setting.

Step 2 Press **+** or **–** to adjust the volume, screensaver time and the screen light up time.

- Volume: The volume of operating the VTO or calling of the VTO.
- Screensaver time: The amount of idle time that must elapse before the screensaver is activated.
- Screen Light Up Time: The screen display turns off automatically after you leave the VTO idle for the time you configure.

Figure 2-30 General settings



2.2.2.3 User Registration

If the current VTO or another VTO works as the SIP server, the administrator can register user information and add faces, fingerprints and cards. The VTO also supports configuring the main card and reporting the loss of the card.

- The faces, fingerprints and cards that are registered are only valid to the current VTO.
- If the platform works as the SIP server, the platform sends the faces, fingerprints and cards information to the VTO.

2.2.2.3.1 Adding Users

Add the user, and then register the information on the face, fingerprint and the card.

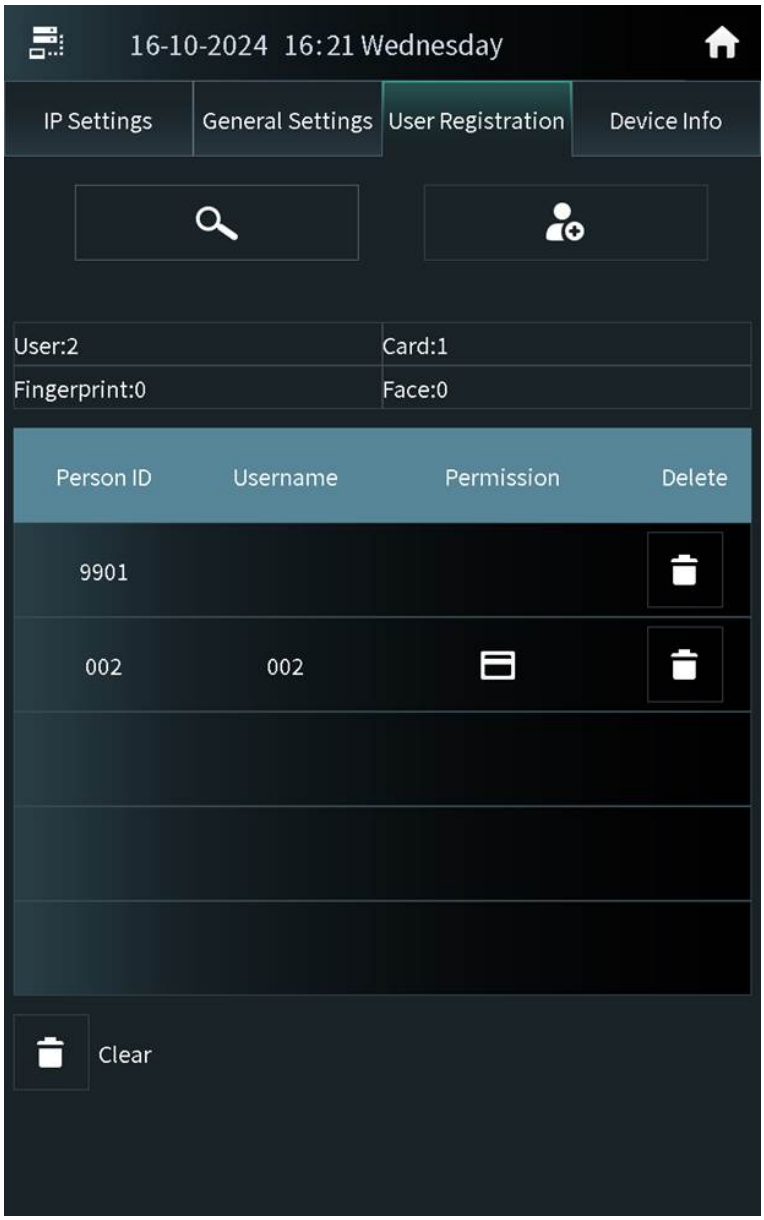
Procedure

Step 1 Tap **User Registration** on the screen of the engineer setting.

- : The user has registered the face.

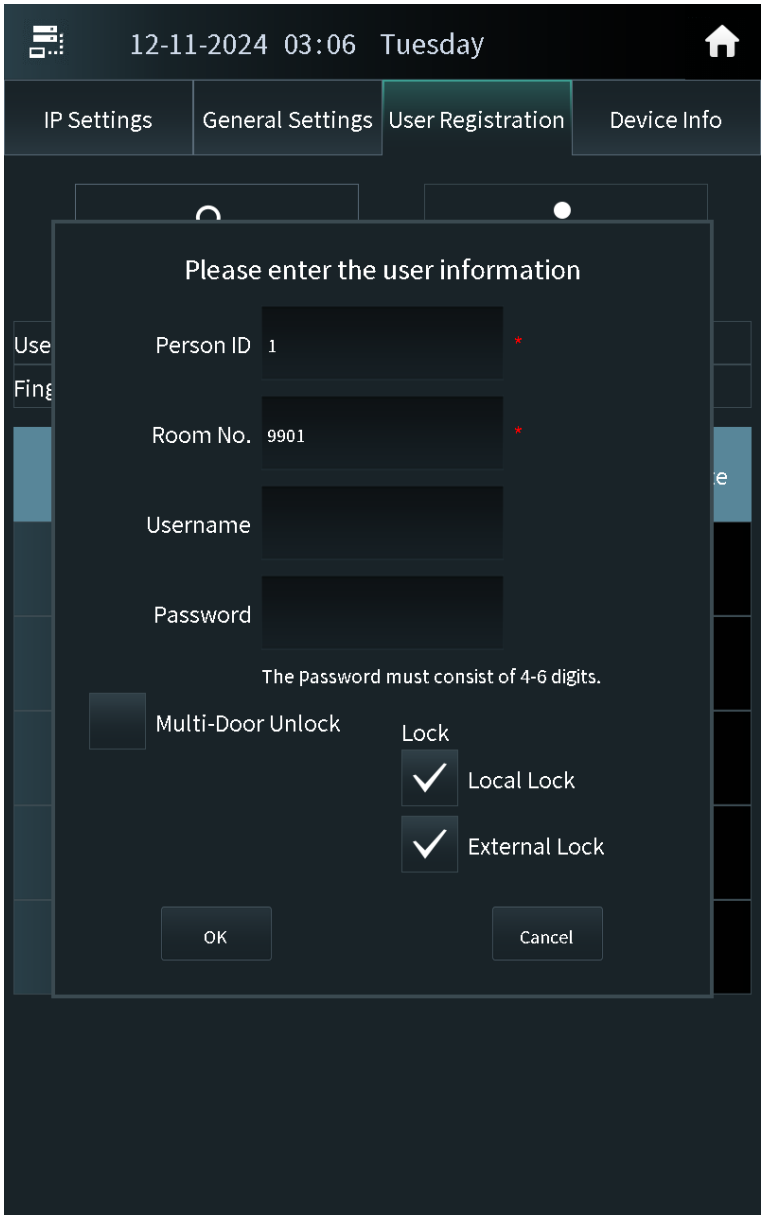
- : The user has registered the card.
- : The user has registered the fingerprint.

Figure 2-31 User registration



Step 2 Tap , enter the person ID, room number and the user name, and then configure the local lock and the external lock.

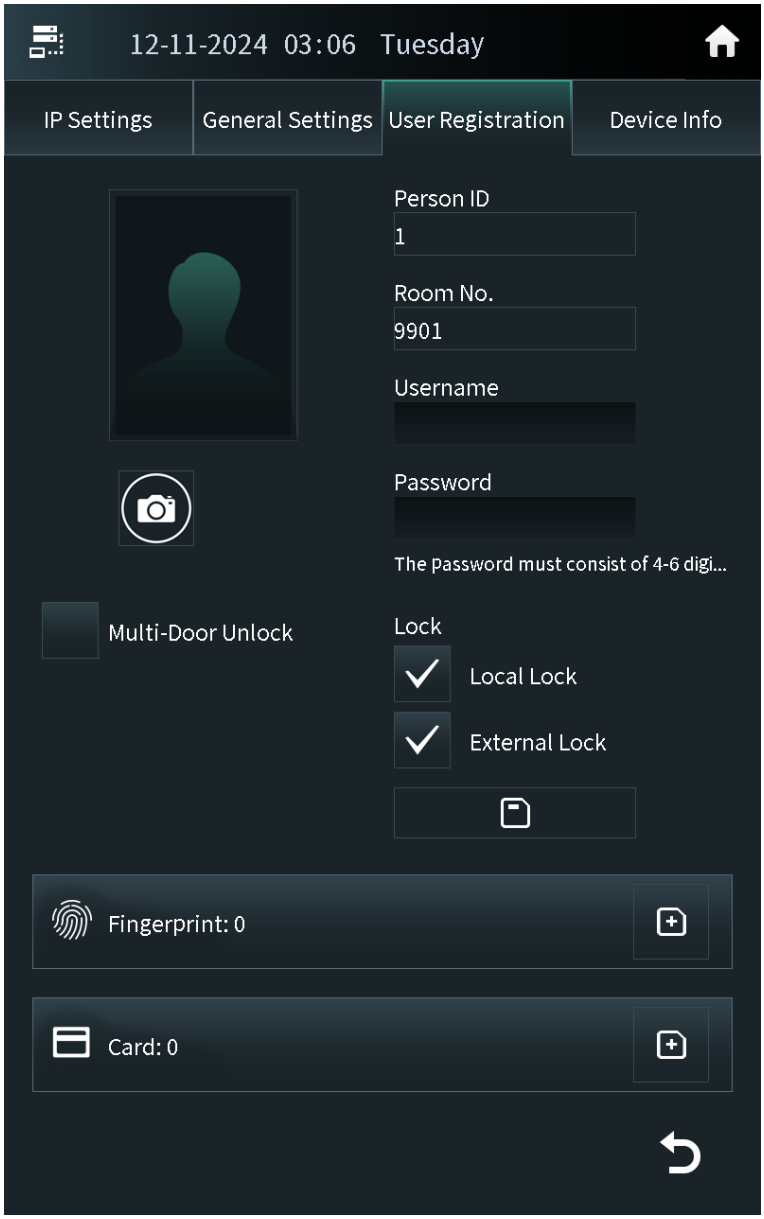
Figure 2-32 Add the user



Multi-Door Unlock: When verification is successful, the local lock and external lock will open at the same time.

Step 3 Tap **OK**.

Figure 2-33 User information



Step 4 Add the face, fingerprint and the card.

- For details about adding the face image, see "2.2.2.3.2 Adding Faces".
- For details about adding the fingerprint, see "2.2.2.3.3 Adding Fingerprints".
- For details about adding the card, see "2.2.2.3.4 Issuing Cards".

2.2.2.3.2 Adding Faces

Procedure

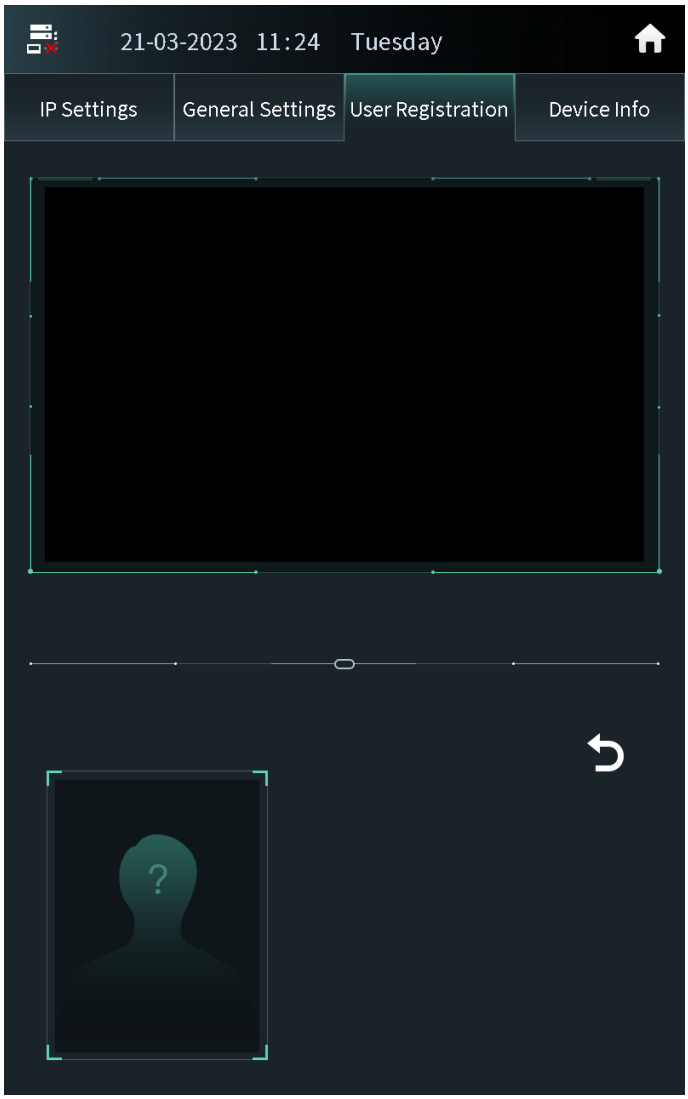
Step 1 Tap  on the screen of the user information.

If you are on the user registration screen, select the user to go to the user information screen.

Step 2 Make sure that your face is in the middle of the frame, and the face image will be automatically taken.

Tap **Cancel** to register again if you do not want the photo.

Figure 2-34 Face registration



Step 3 Tap **OK** after you confirm the face image.

2.2.2.3.3 Adding Fingerprints

Procedure

Step 1 Tap  next to the fingerprint numbers on the screen of the user information.

If you are on the user registration screen, select the user to go to the user information screen.

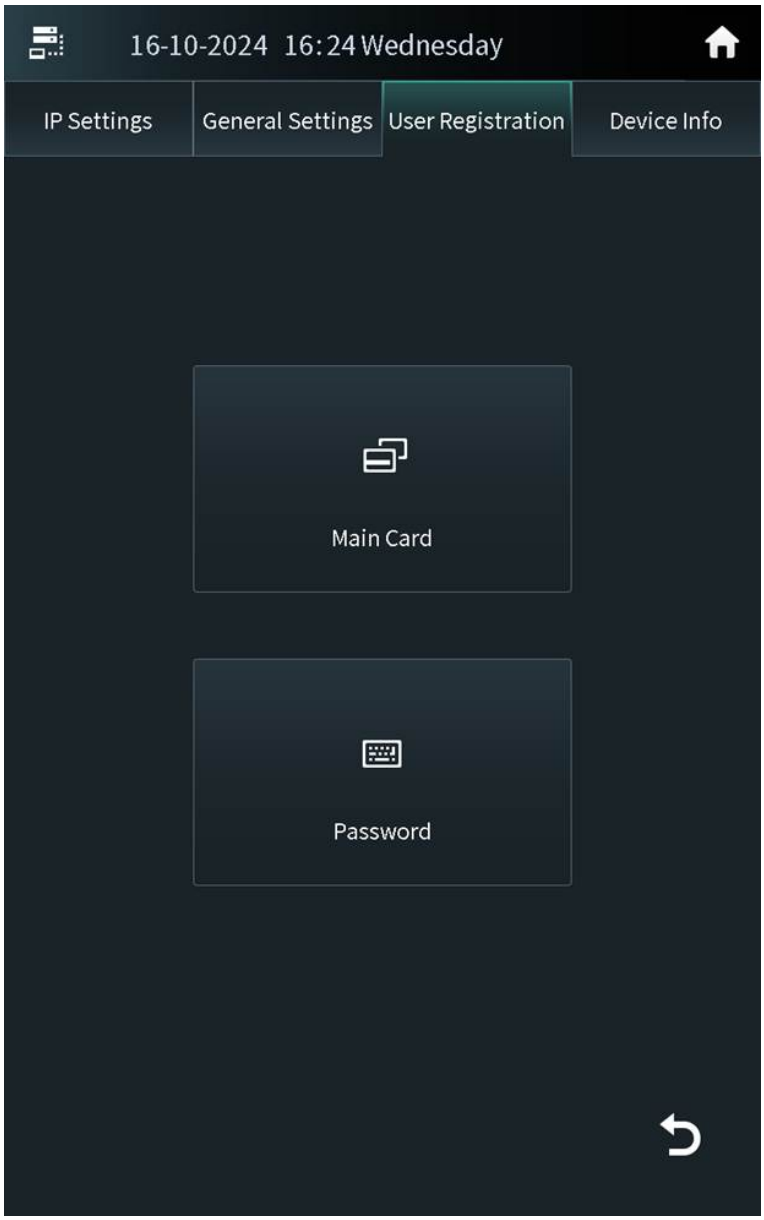
Step 2 Press the fingerprint sensor, and then move the finger after the voice or screen prompt.

2.2.2.3.4 Issuing Cards

Press  next to the card numbers on the screen of the user information.

If you are on the user registration screen, select the user to go to the user information screen.

Figure 2-35 Issue cards



Issuing Cards by the Main Card

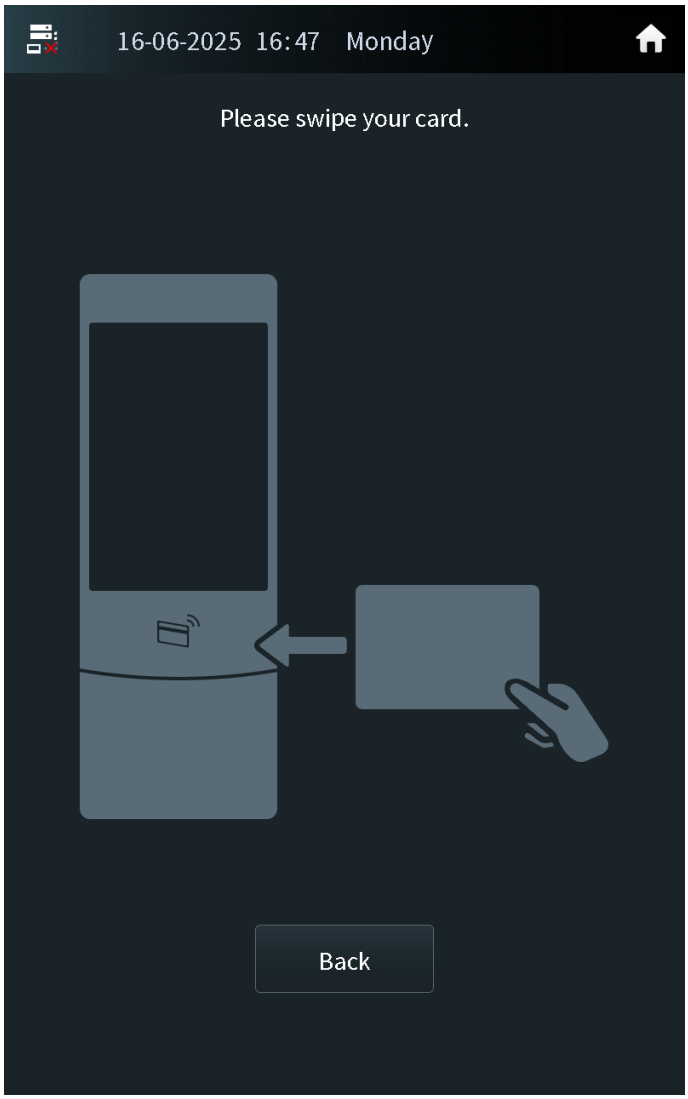
Use the authorized main card to register the new card.

Prerequisites

Make sure that there is the main card. If there is no main card, register the card by the password, and then configure the card as the main card.

1. Select **Main Card** on the issue card screen.
2. Swipe the main card.

Figure 2-36 Swipe the main card



3. Swipe the new card.

   The VTO displays **Issue Card Success** . You can swipe other cards to continuously register. Tap **Back** if you do not need to add other cards.

Issuing Cards by the Password

Use the issue card password to register the new card.

You can configure the password through **Local Device Config** > **Access Control** > **Config**.

1. Select **Password** on the issue card screen.
2. Enter the issue card password, and then tap **OK**.

Figure 2-37 Issue card password



3. Swipe the new card.

   The VTO displays **Issue Card Success** . You can swipe other cards to continuously register. Tap **Back** if you do not need to add other cards.

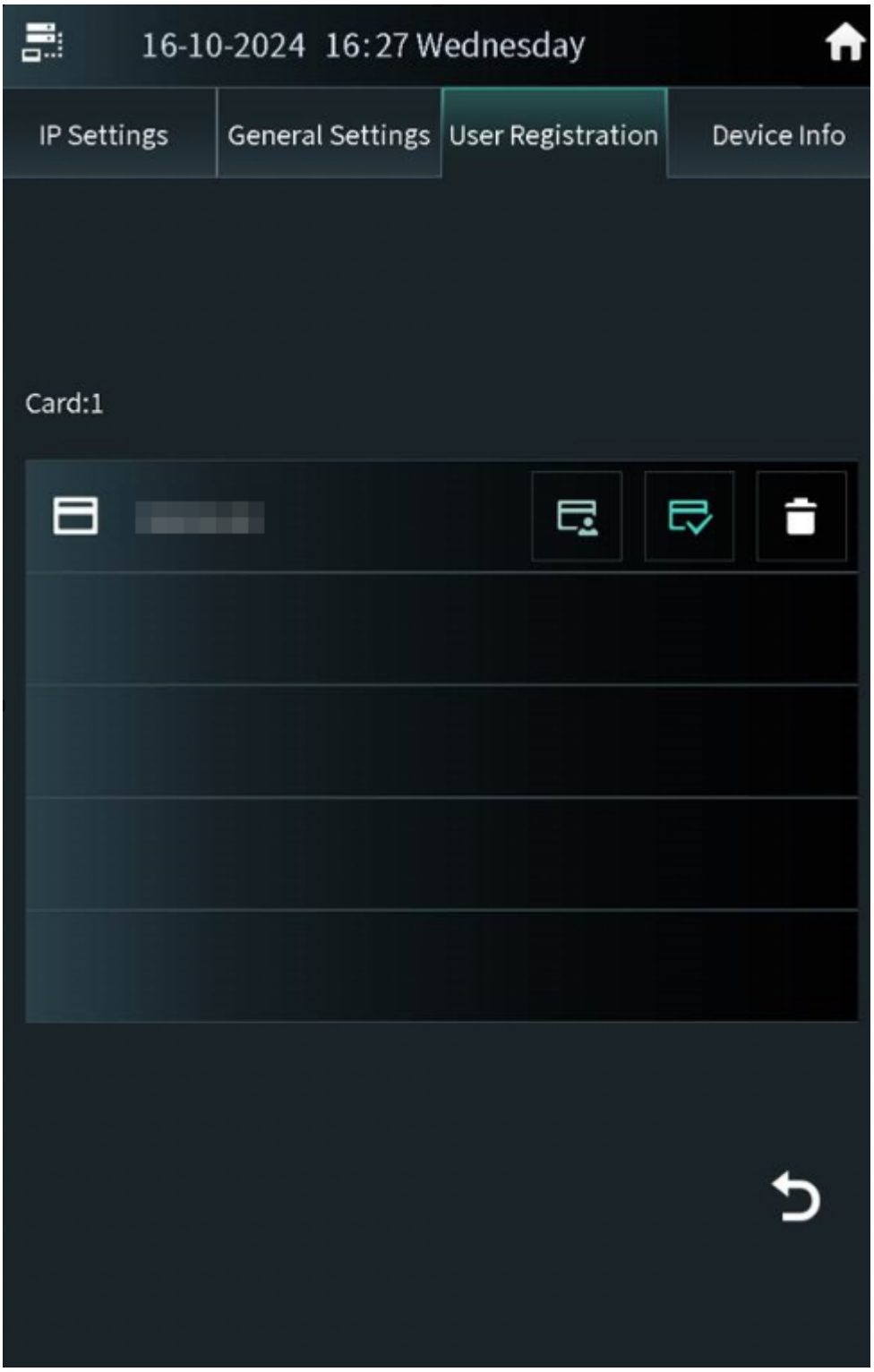
2.2.2.3.5 Card Management

Configuring the Main Card

The main card is used to register other new cards.

1. Select the user on the user registration screen.
2. Press **Card Numbers**.

Figure 2-38 Card list



3. Press , and the icon turns . The card is configured as the main card.

Press to cancel the main card.

Reporting the Loss of the Card

If you report the loss of the common card, the card cannot be used to open the door. If you report the loss of the main card, the main card cannot be used to open the door or register the new card.

1. Select the user on the user registration screen.
2. Tap **Card Numbers**.
3. Tap , and the icon turns . The card is reported the loss and cannot be used to open the door.

Tap  to cancel the report of loss. The card can be used to open the door again.

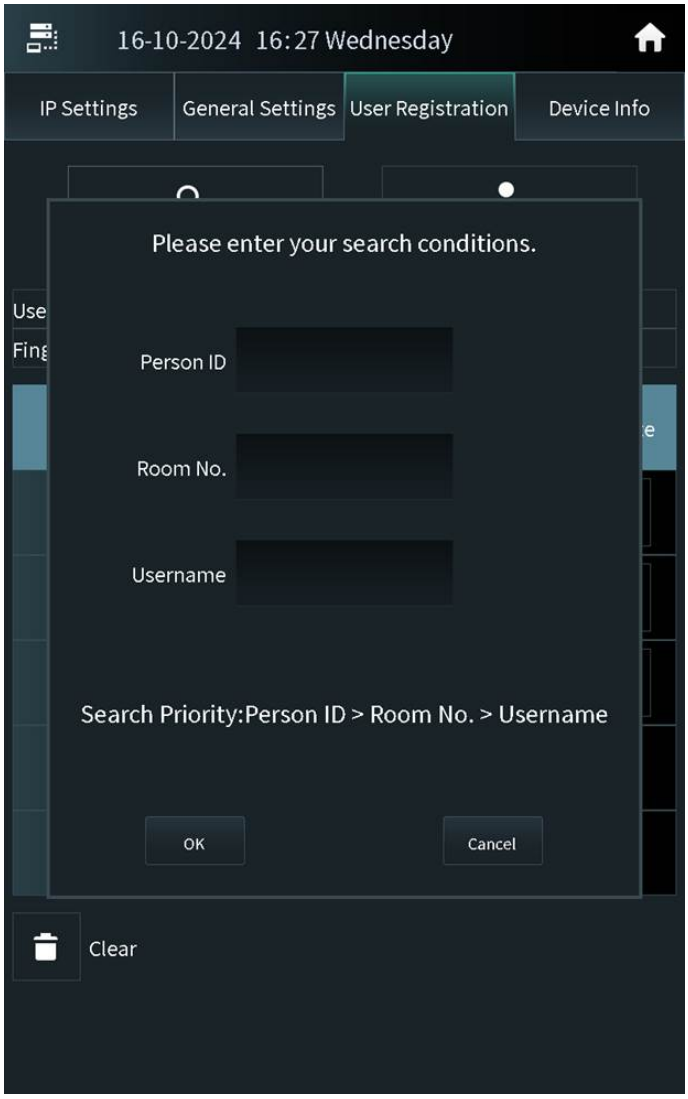
2.2.2.3.6 Searching for a User

Procedure

Step 1 Tap  on the user registration screen.

Step 2 Enter the person ID, room number or the user name, and then tap **OK**.

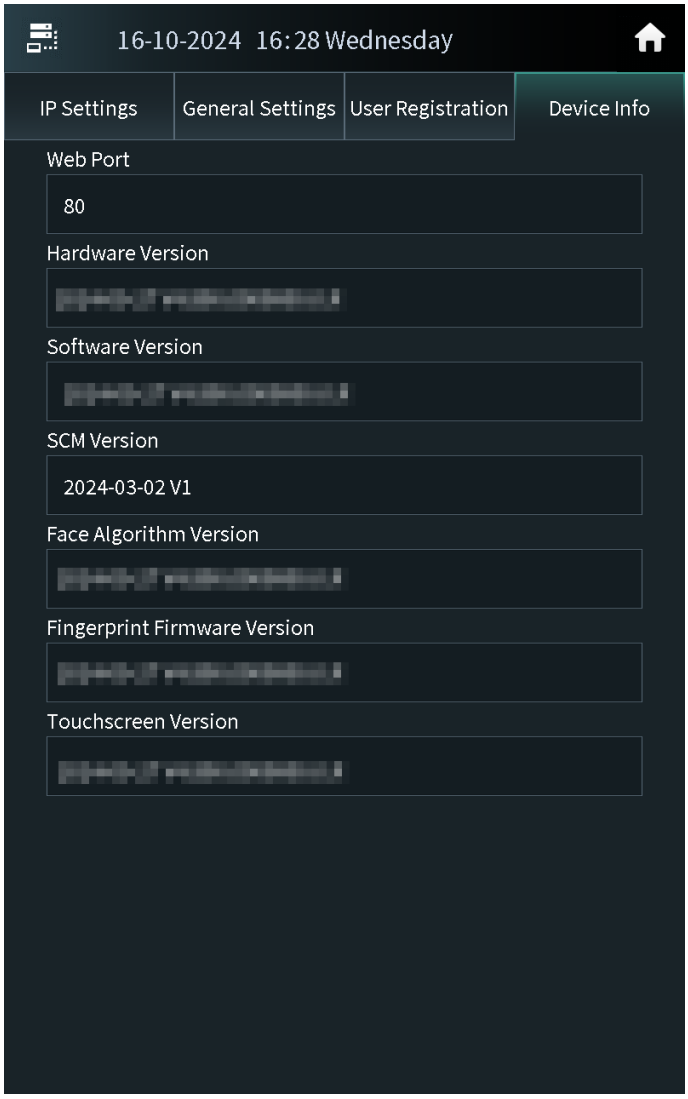
Figure 2-39 Search for the user



2.2.2.4 Viewing Device Information

Press **Device Info** on the screen of the engineer setting to view the details on the VTO.

Figure 2-40 View the device information



2.2.3 Owner Registration

The owner can only register and maintain the information, face images and fingerprints of people to the VTH.

2.2.3.1 Adding Owners

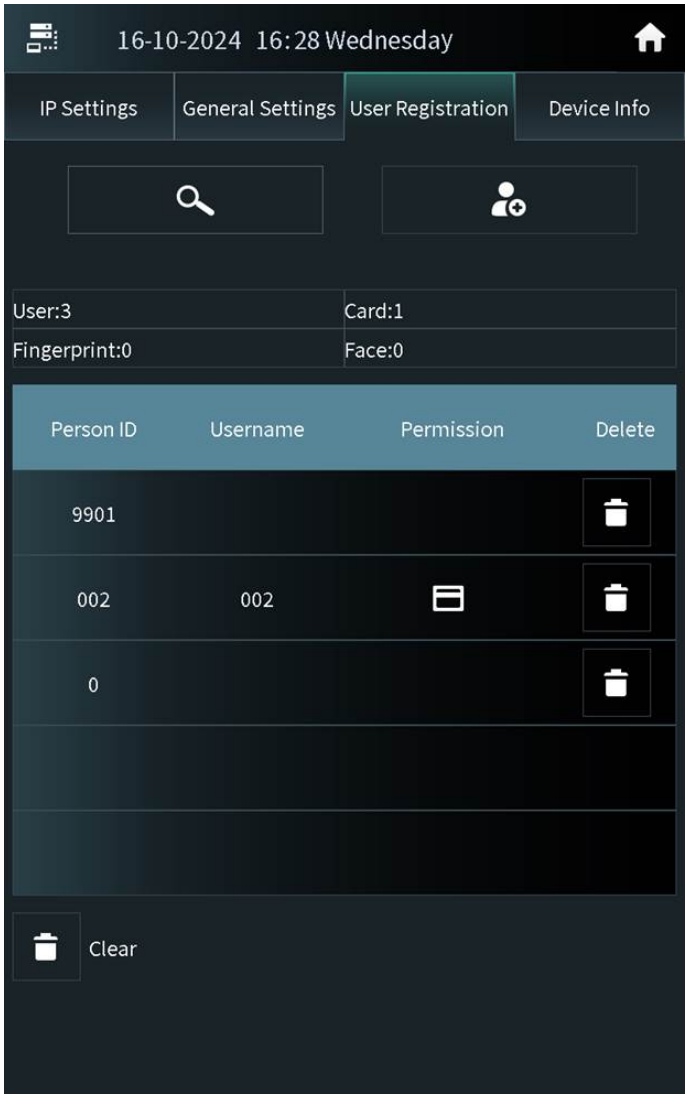
Add the owner, and then register the face and fingerprint.

Procedure

Step 1 Tap **Owner** on the home screen.

Step 2 Swipe the registered card to enter owner list.

Figure 2-41 User list

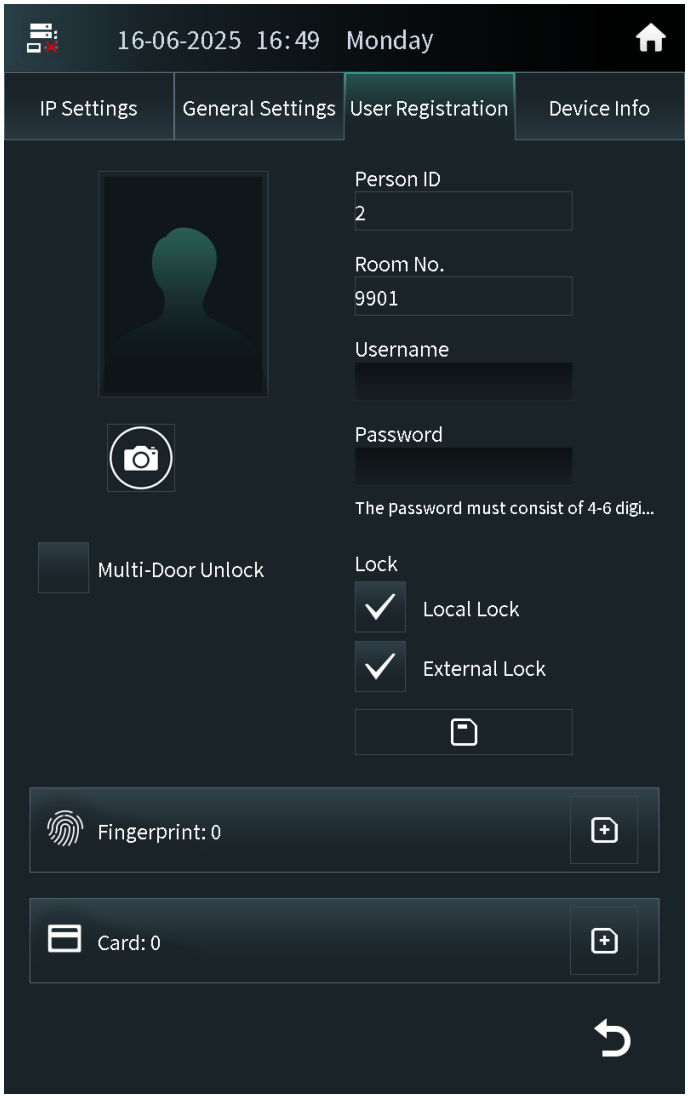


Step 3 Tap to add the user.

Step 4 Enter the person ID and the user name.

Step 5 Configure the local lock or the second lock, and then tap **OK**.

Figure 2-42 User information



Step 6 Register the face image and the fingerprint.

2.2.3.2 Adding Faces

Procedure

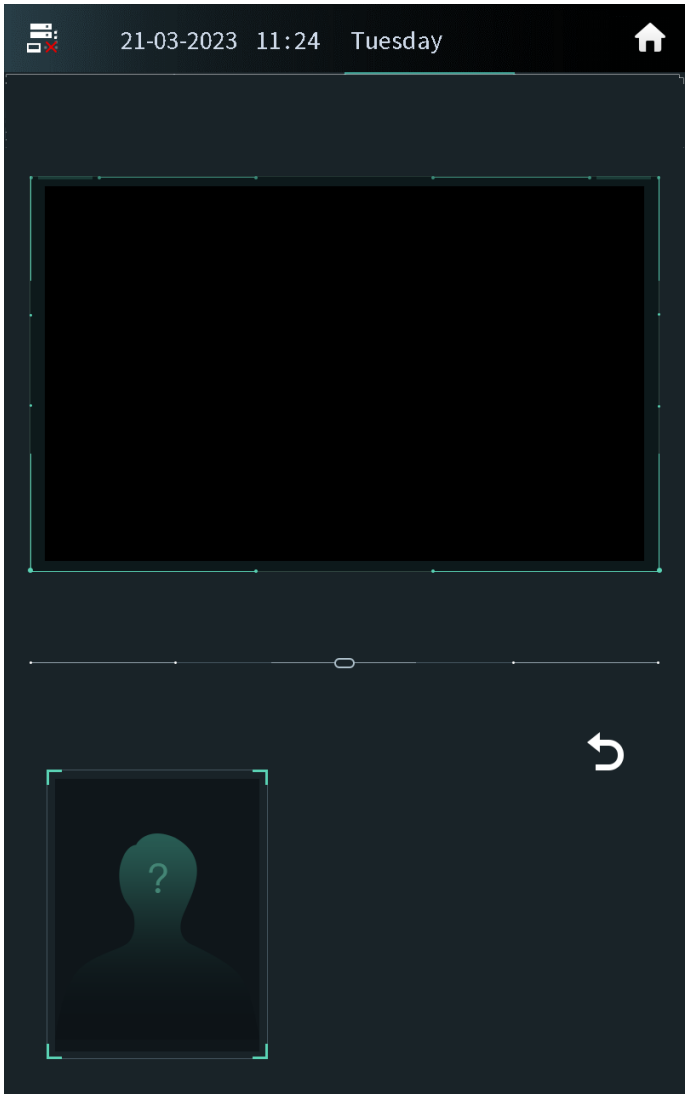
Step 1 Tap  on the screen of the user information.

If you are on the owner screen, select the user to go to the user information screen.

Step 2 Position your face in the middle of the frame.

The face image will be automatically taken. If you are not satisfied with the photo, tap **Cancel** to cancel the photo and register again.

Figure 2-43 Face registration



Step 3 Tap **OK** after you confirm the face image.

2.2.3.3 Adding Fingerprints

Procedure

Step 1 Tap  next to the fingerprint numbers on the screen of the user information.

If you are on the owner screen, select the user to go to the user information screen.

Step 2 Press the fingerprint sensor, and then move the finger after the voice or screen prompt.

2.2.4 Unlock

2.2.4.1 Unlocking by Identifying the Face

When people come close to the VTO, the VTO automatically displays face detect screen and detects the face. The voice prompt and the device prompt **Open door success** means that the door opens and you can enter. If the device displays **Unauthorized**, register the face first.

2.2.4.2 Unlocking by Scanning the QR Code

Scan the QR code to open the door. The QR code is sent by the platform. For details, see the user manual of the corresponding platform.

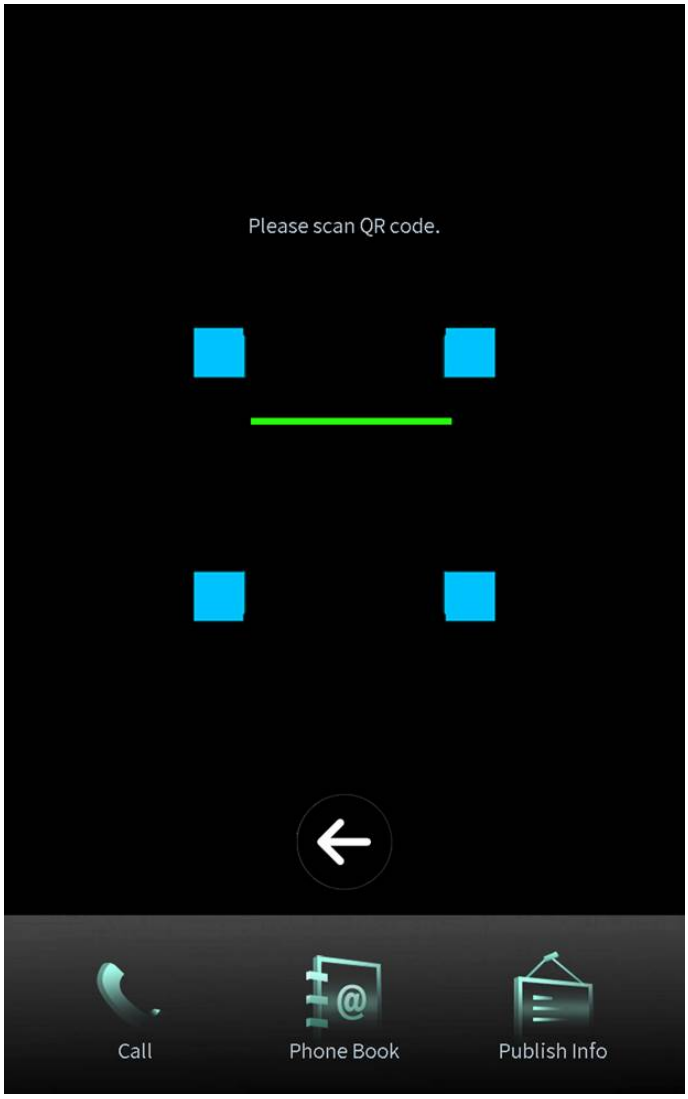
Procedure

Step 1 Press  on the home screen.

Step 2 Show the QR code, and then make sure the QR code is displayed in the viewfinder.

The voice prompt and the device prompt **Open Successfully** means that the door opens and you can enter. If the device displays **Invalid**, check the QR code.

Figure 2-44 Scan the QR code



2.2.4.3 Unlocking by the Password

Procedure

Step 1 Tap  on the home screen.

Step 2 Enter the password to open the door.

- **#+Public Password+#** : The public password here is configured through **Local Device Config** > **Access Control** > **Config** > **Public Password** on the webpage. For example, if the password is 123456, enter "#123456#" to open the door.
- **#+User Password+#** : The user password here is configured on **Person Management** of the webpage. You can set 4–6 digitals as user password. For example, if the password is 123456, enter "#123456#" to open the door.
- **#+Room number+Password+#** : The password here is configured on the VTH. If the room number has less than 6 digits, you need to enter extra 0 in front. For example, if the room number is 9901 and the password is 112233, enter "#009901112233#" to open the door.

  You need to change the default password on the VTH first if you want to use this method to open the door.

The voice prompt and the device prompt **Open Successfully** means that the door opens and you can enter. If the device displays **Password Error**, check the password.

2.2.4.4 Unlocking by the Card

Brush the authorized card. The voice prompt and the device prompt **Open door success** means that the door opens and you can enter. If the device displays **Unauthorized**, register the card.

2.2.4.5 Unlocking by the Fingerprints

Press the fingerprint. The voice prompt and the device prompt **Open door success** means that the door opens and you can enter. If the device displays **Unauthorized**, register the fingerprint.

2.2.4.6 Unlocking through the VTH

When the VTO calls the VTH or the VTH monitors the VTO, you can press the unlock button on the VTH for the visitors. The voice prompt and the device prompt **Open door success** means that the door opens and visitors can enter.

2.2.4.7 Unlocking through the VTS

When the VTO calls the VTS or the VTS monitors the VTO, you can press the unlock button on the VTS for the visitors. The voice prompt and the device prompt **Open door success** means that the door opens and visitors can enter.

2.2.5 Call

2.2.5.1 Calling the VTH

Procedure

Step 1 Tap  on the home screen.

Step 2 Enter the room number, and then tap **Call**.

Step 3 Tap  on the VTH to receive the call.

2.2.5.2 Calling the Property Management (the VTS)

Procedure

Step 1 Tap  on the home screen.

Step 2 Tap .

There is voice prompt **Calling, please wait**.

Step 3 The VTS receives the call.

2.2.6 Messages

If the VTO calls the VTH and the VTH does not answer the call, the VTO displays prompt. Press **1** to leave a message. The VTO saves the messages to the SD card of the VTH. The VTH user can view the messages in **Visitor Message**.

Select **Local Device Config** > **Basic Settings** > **Functions**, and then enable **Upload Messages and Videos**, and then the messages also can be saved to the SD card of the VTO.

3 Webpage Operations

3.1 Initialization

3.1.1 Initialization through the Device

Prerequisites

Make sure that the computer and the VTO are on the same network segment.

Procedure

Step 1 Turn on the VTO.

Step 2 Enter the IP address of the VTO in the browser.

For first-time login, enter the default IP (192.168.1.108). If you have multiple VTOs, we recommend you change the default IP address to avoid a conflict.

Step 3 Enter and confirm the new password, and then click **Next**.

Step 4 Select **Email** and enter the email address to use to reset your password.

Step 5 Click **Next** , and then click **OK** to go to the login page.

Step 6 Enter user name and the new password to log in to the webpage.

3.1.2 Initialization through the DoLynk Care

You can initialize the device on the DoLynk Care. Here uses initialization on DoLynk Care app as an example. For detailed operation of the app, refer to its user manual.

Procedure

Step 1 On the home screen, tap ⊕.

Step 2 Tap **QR**.

Step 3 Scan device QR code, or tap to manually enter device SN.

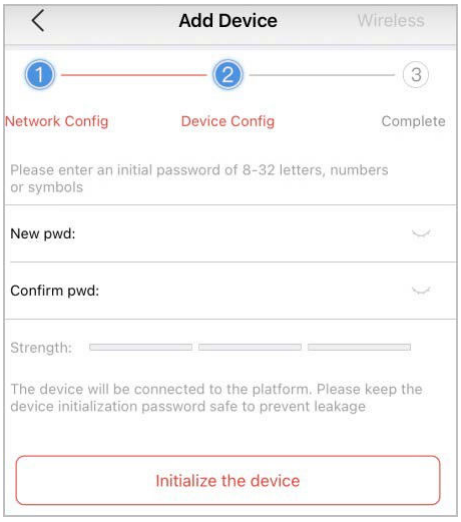
Step 4 Select a site, and then tap **OK**.

Step 5 On the **Add Device** screen, select a device type.

Step 6 Connect to wireless or wired network.

Step 7 Enter password and confirm it again, and then tap **Initialize the device** to complete initialization.

Figure 3-1 Initialize the device



Step 8 Tap **Completed**, and then you can view the device in the device list.

3.2 Logging in to the Webpage

Procedure

Step 1 Enter the IP address of the VTO in the browser bar to go to the login page, and then press the Enter key.

Step 2 Enter the username (admin by default) and the password that you configured during the initialization.

Step 3 Click **Login**.

3.3 Home Page Introduction

The system automatically goes to the home page after you log in.

Figure 3-2 Home page

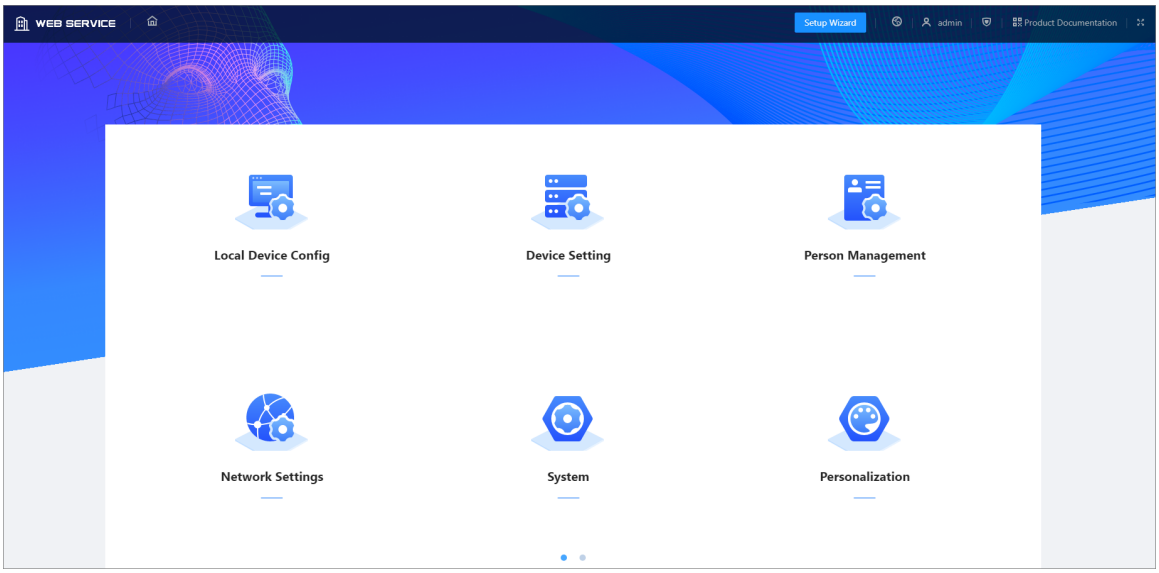
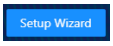
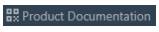


Table 3-1 Home page introduction

Icon	Function	Description
	Home button	Go back to the home page.
	Setup wizard	Configure the VTO SIP server.
	Language	Change language of the webpage of the VTO.
	Admin center	Change password, log out of the current device, restart the system, and restore the device to factory settings.
	Security center	View and configure the security settings.
	Product Documentation	Scan the QR code to view the product documentation, such as the user manual.
	Full screen	View the webpage in full screen mode. Click again or press the Exit key to exit the full screen mode.
	Page turning	Click to turn to the next page or to the previous page.
	Local device configuration	Configure the basic information, parameters of access control, card, fingerprint, face detection and Wiegand. Fingerprint is available on select models.
	Device setting	Manage the device information.
	Person management	Manage the person information.
	Network settings	Configure the network parameters such as TCP/IP, FTP, UPnP, SIP server and personnel.
	System	Configure the parameters of alarm linkage, video, audio, time, and ONVIF users.
	Personalization	Configure the display mode, advertisement resources, and announcement.
	Maintenance center	View the system information, logs. Manage the auto maintenance time. Update the device and more.

3.4 Setup Wizard

Through the setup wizard, you can finish the process of adding VTO, VTH or VTS and specific any VTO as the SIP server. You can also cancel its status of working as a SIP server.

3.4.1 Setting as SIP Server

Set the VTO as the SIP server.

Prerequisites

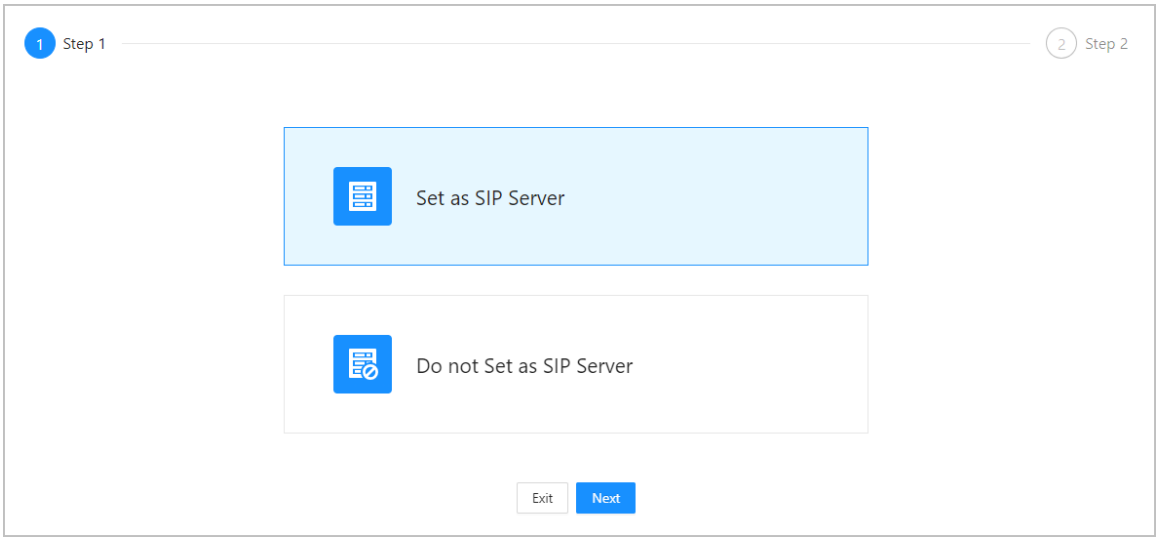
You have added VTOs on the webpage. If not, you can add them in **Set as SIP Server** page or in the **Device Setting** section.

Procedure

Step 1 Log in to the webpage of the VTO.

Step 2 Select **Setup Wizard** > **Set as SIP Server**, and then click **Next**.

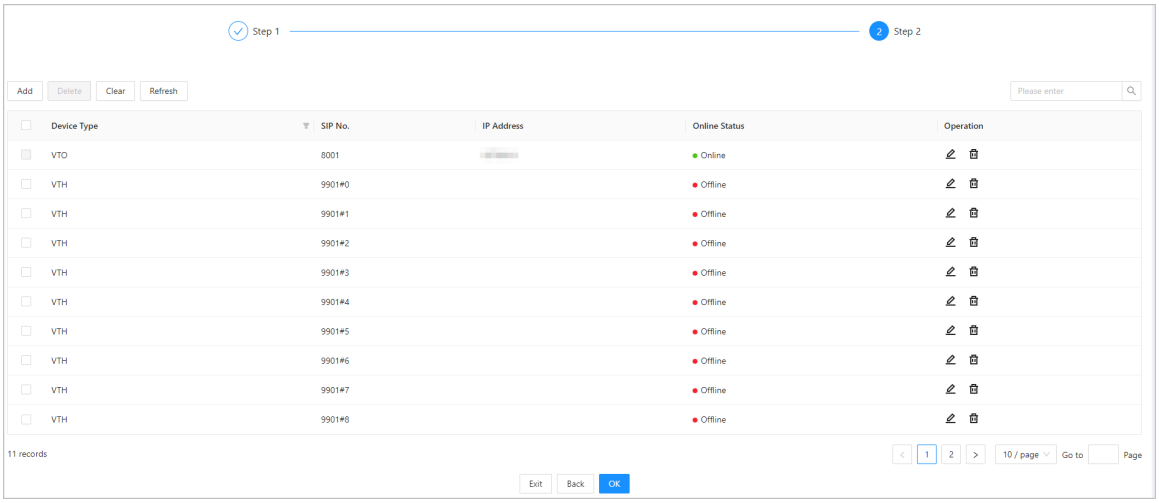
Figure 3-3 Set as SIP server



Step 3 Select the VTO to be set as the SIP server, and then click **OK**.

You can also click **Add** to add VTOs if you have not had one to work as the SIP server.

Figure 3-4 Select the SIP server



3.4.2 Not Setting as SIP Server

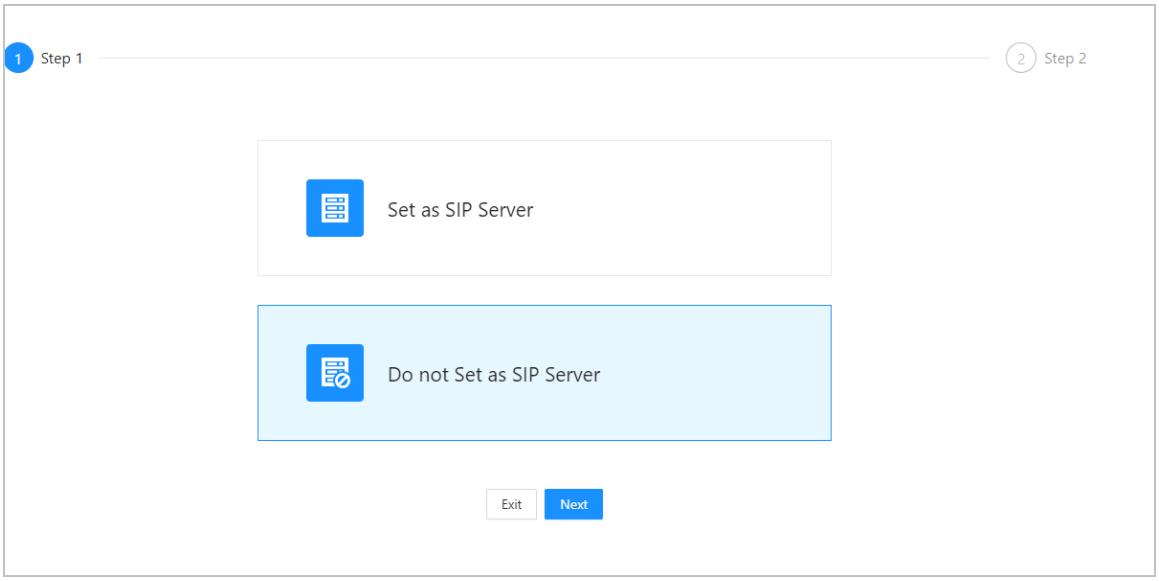
If you want to change the SIP server, you need to remove the current one from the list.

Procedure

Step 1 Log in to the webpage of the VTO.

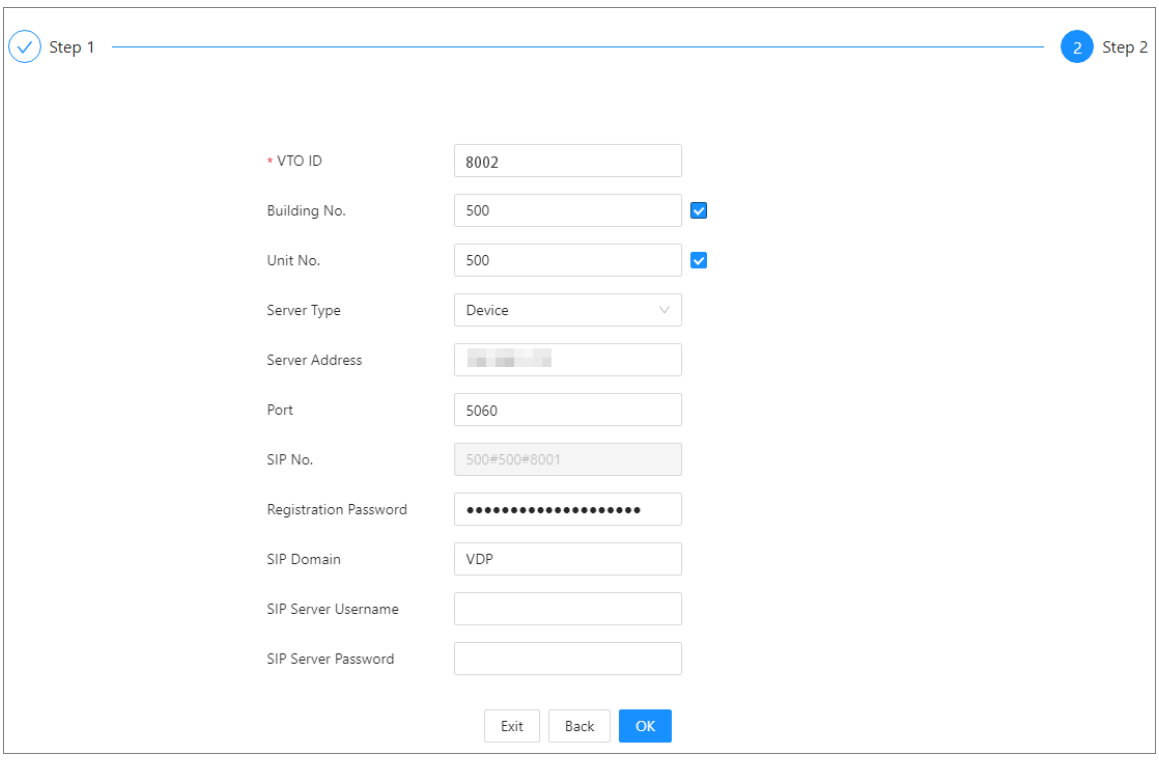
Step 2 Select **Setup Wizard** > **Do not Set as SIP Server**, and then click **Next**.

Figure 3-5 Do not set as SIP server



Step 3 Configure the information of the VTO that you do not want to set as SIP server, and then click **OK**.

Figure 3-6 Configure information



3.5 Admin Center

Change password, logout, restart the device, restore the device to factory default settings and other operations on the home page.

3.5.1 Resetting the Password

If you forget the login password of the admin account, scan the QR code to reset it.

Prerequisites

Make sure that you have enabled **Password Reset** through **Network Settings** > **Basic Services**.

If you did not configure the email address during the initialization, the system will report an error. Contact the local retailer or the technical support for help.

Procedure

Step 1 Click **Forget Password?** on the login page, and then click **Next**.

Step 2 Get the **Security Code** according to the instructions.

- You can get up to 2 security codes with the same QR code. If you need more security codes, you need to refresh the QR code and scan it again.
- The security code will be sent to your email address. You must use it in 24 hours. Otherwise, the security code will be invalid.
- The account will be locked for 5 minutes if you enter the wrong security code 5 times in a row.

Step 3 Enter the security code you received, and then click **Next**.

Step 4 Enter a new password, confirm it, and then click **OK**.

3.5.2 Changing the User Message

Change the login password and the email address of the user.

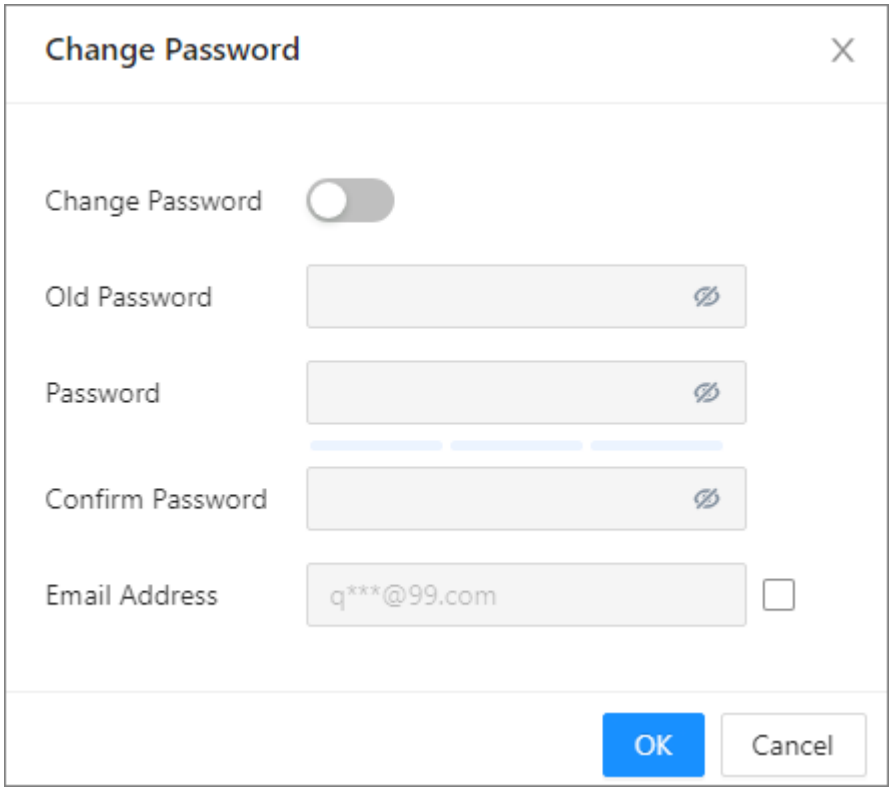
Procedure

Step 1 Click admin on the home page.

Step 2 Click **Change Password**.

Step 3 Enable the function, configure the parameters, and then click **OK**.

Figure 3-7 Changing the user message



3.5.3 Restoring the Factory Default Settings

Procedure

Step 1 Select admin > **Factory Default**.

Restoring the VTO to its default configurations will result in data loss. Please be advised.

Step 2 Enter the login password, and then click **OK**.

Step 3 Click **Factory Defaults** to resets all the configurations of the Device and delete all the data.

3.5.4 Restarting the Device

Select admin > **Restart**, and then click **OK** in the pop-up window. The device automatically restarts, and then the webpage goes to the login page.

3.5.5 Logging Out

Select admin > **Logout**. The webpage goes to the login page.

3.6 Security Center

3.6.1 Security Status

Scan the users, service, and security modules to check the security status of the VTO.

Background Information

- User and service detection: Check whether the current configuration conforms to recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio and video transmission, trusted protection, securing warning and attack defense.

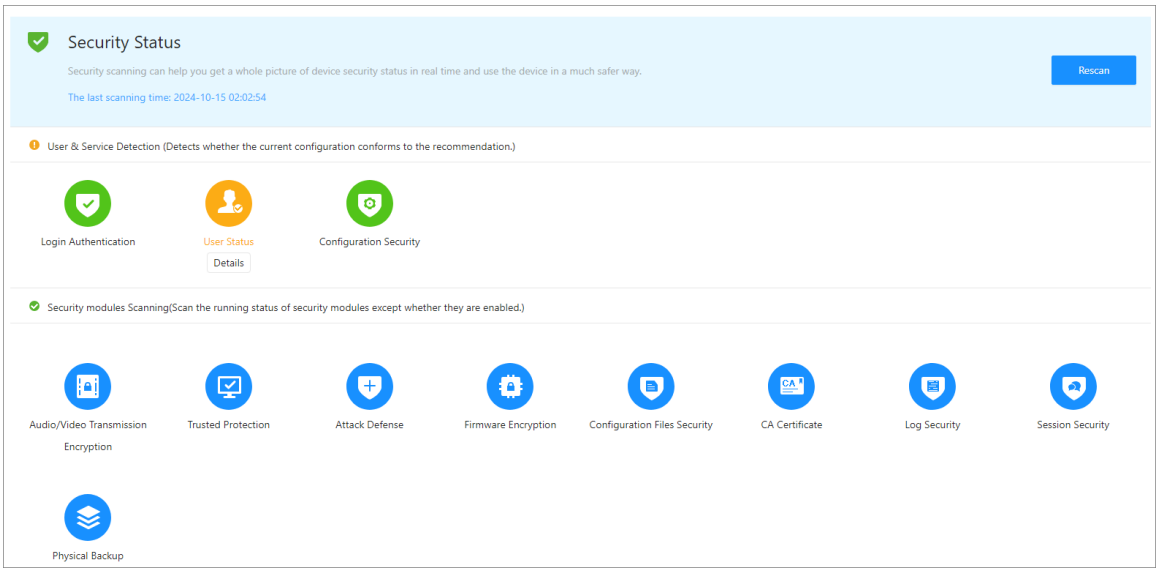
Procedure

Step 1 Select > **Security Status**.

Step 2 Click **Rescan** to perform a security scan of the Device.

Hover over the icons of the security modules to see their running status.

Figure 3-8 Security status



Related Operations

After you perform the scan, the results will be displayed in different colors. Yellow indicates that the security modules are abnormal, while green indicates that the security modules are normal.

- Click **Details** to view the details on the results of the scan.
- Click **Ignore** to ignore the abnormality, and it will not be scanned. The abnormality that was ignored will be highlighted in grey.
- Click **Optimize** to troubleshoot the abnormality.

3.6.2 Configuring HTTPS

Create a certificate or upload an authenticated certificate, and then you can log in to the webpage through HTTPS on your computer. HTTPS secures communication over a computer network.

Procedure

Step 1 Select > **System Service** > **HTTPS**.

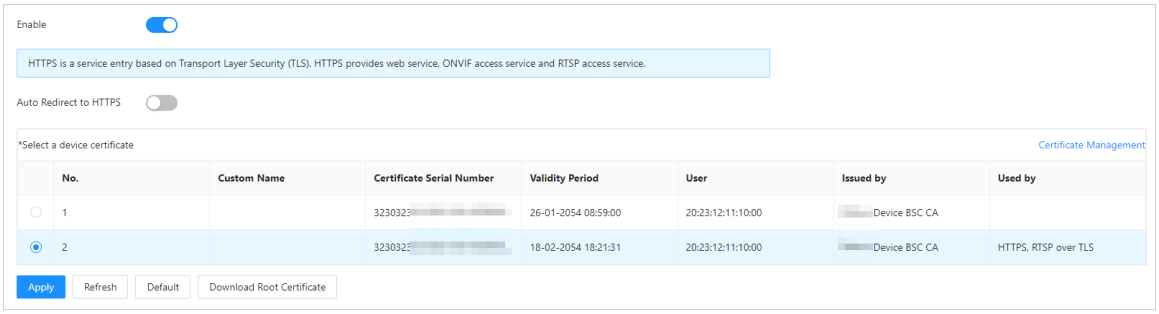
Step 2 Enable the HTTPS service.

If you turn on the compatible with TLS v1.1 and earlier versions, security risks might occur. Please be advised.

Step 3 Select the certificate.

If there are no certificates in the list, click **Certificate Management** to upload a certificate.

Figure 3-9 HTTPS



Step 4 Click **Apply**.

Enter "https://*IP address*: *httpsport*" in a web browser. If the certificate is installed, you can log in to the webpage successfully. If not, the webpage will display the certificate as wrong or untrusted.

3.6.3 Attack Defense

3.6.3.1 Configuring Firewall

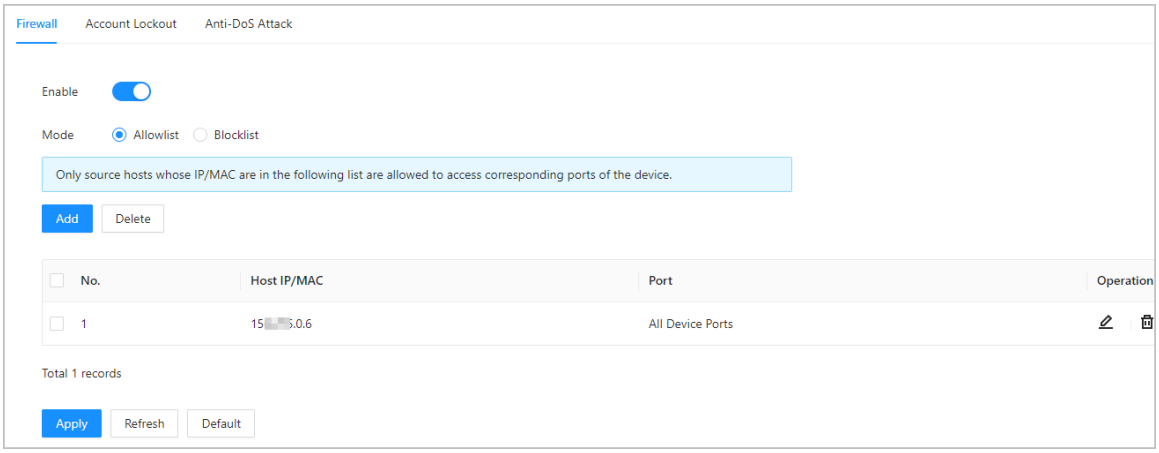
Configure firewall to limit access to the Device.

Procedure

Step 1 Select > **Attack Defense** > **Firewall**.

Step 2 Click to enable the firewall function.

Figure 3-10 Firewall

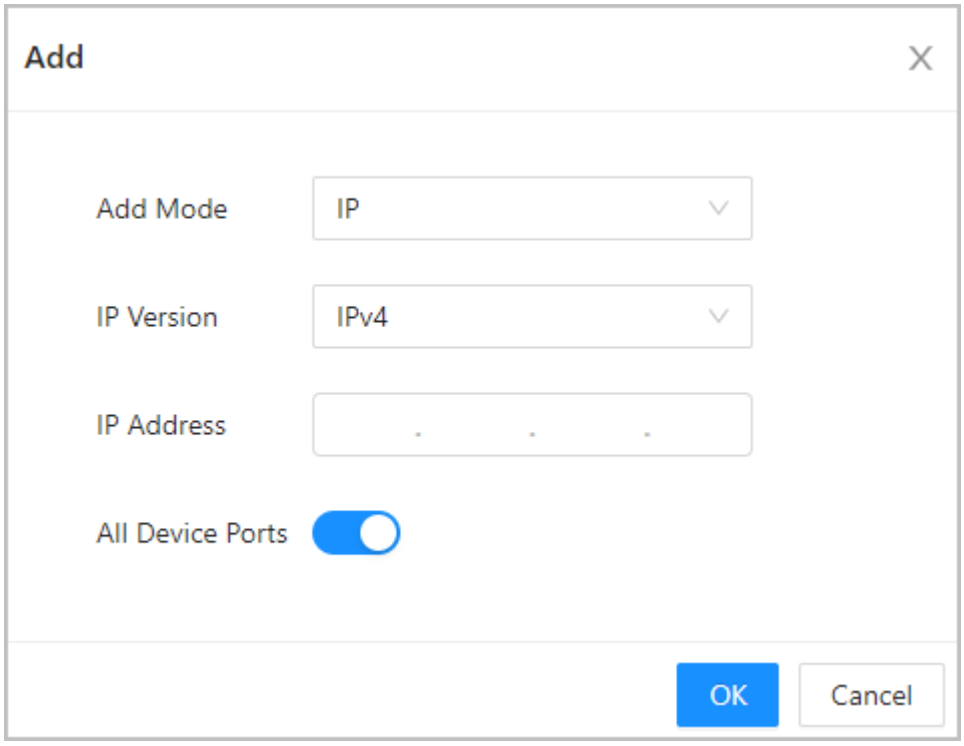


Step 3 Select the mode: **Allowlist** and **Blocklist**.

- **Allowlist** : Only IP/MAC addresses on the allowlist can access to the Device.
- **Blocklist** : The IP/MAC addresses on the blocklist cannot access to the Device.

Step 4 Click **Add** to enter the IP information.

Figure 3-11 Add IP information



Step 5 Click **OK**.

Related Operations

- Click to edit the IP information.
- Click to delete the IP address.

3.6.3.2 Configuring Account Lockout

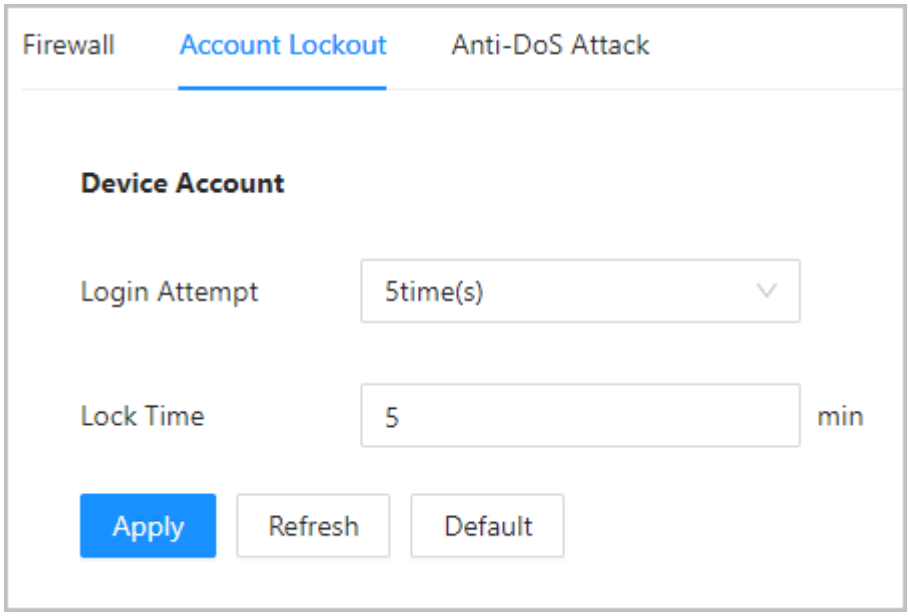
If the incorrect password is entered for a defined time, the account will be locked.

Procedure

Step 1 Select > **Attack Defense** > **Account Lockout**.

Step 2 Select the times of login attempts and set the time the administrator account and ONVIF users will be locked for.

Figure 3-12 Account lockout



- Login Attempt: The limit of login attempts. If the incorrect password is entered for a defined time, the account will be locked.
- Lock Time: The period during which you cannot log in after the account is locked.

Step 3 Click **Apply**.

3.6.3.3 Configuring Anti-DoS Attack

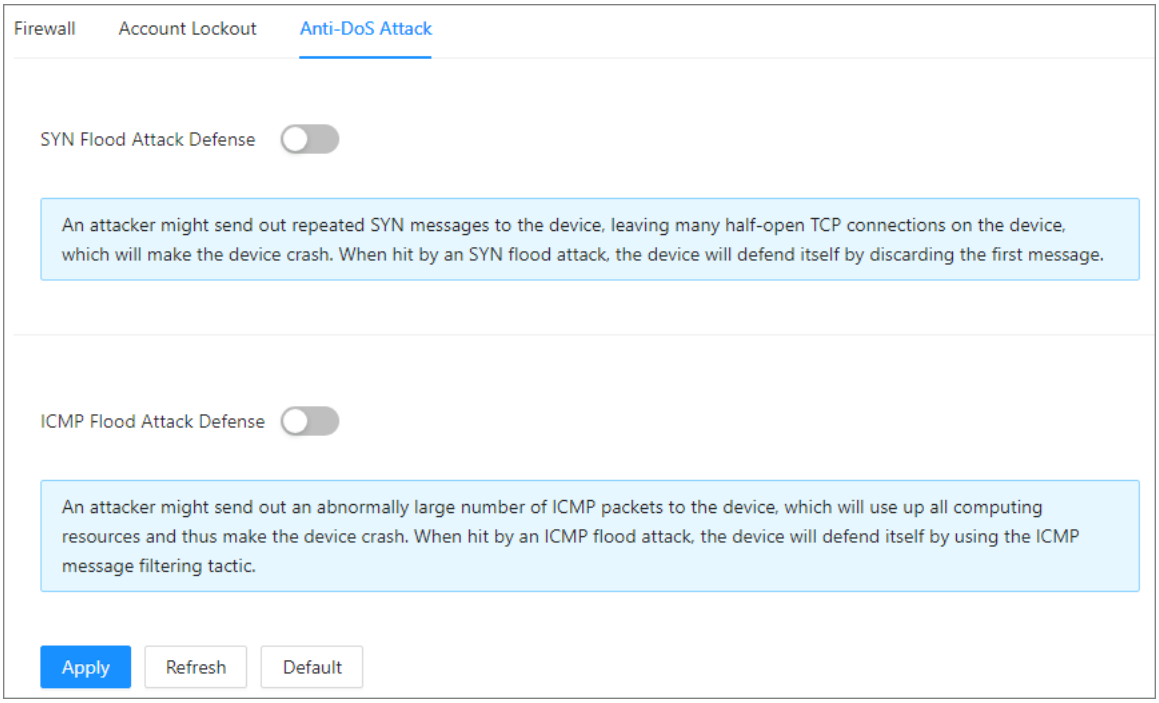
You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Device against DoS attacks.

Procedure

Step 1 Select > **Attack Defense** > **Anti-DoS Attack**.

Step 2 Enable **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to protect the Device against Dos attack.

Figure 3-13 Anti-DoS attack



Step 3 Click **Apply**.

3.6.4 Installing Device Certificate

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS on your computer.

3.6.4.1 Creating Certificate

Create a certificate for the Device.

Procedure

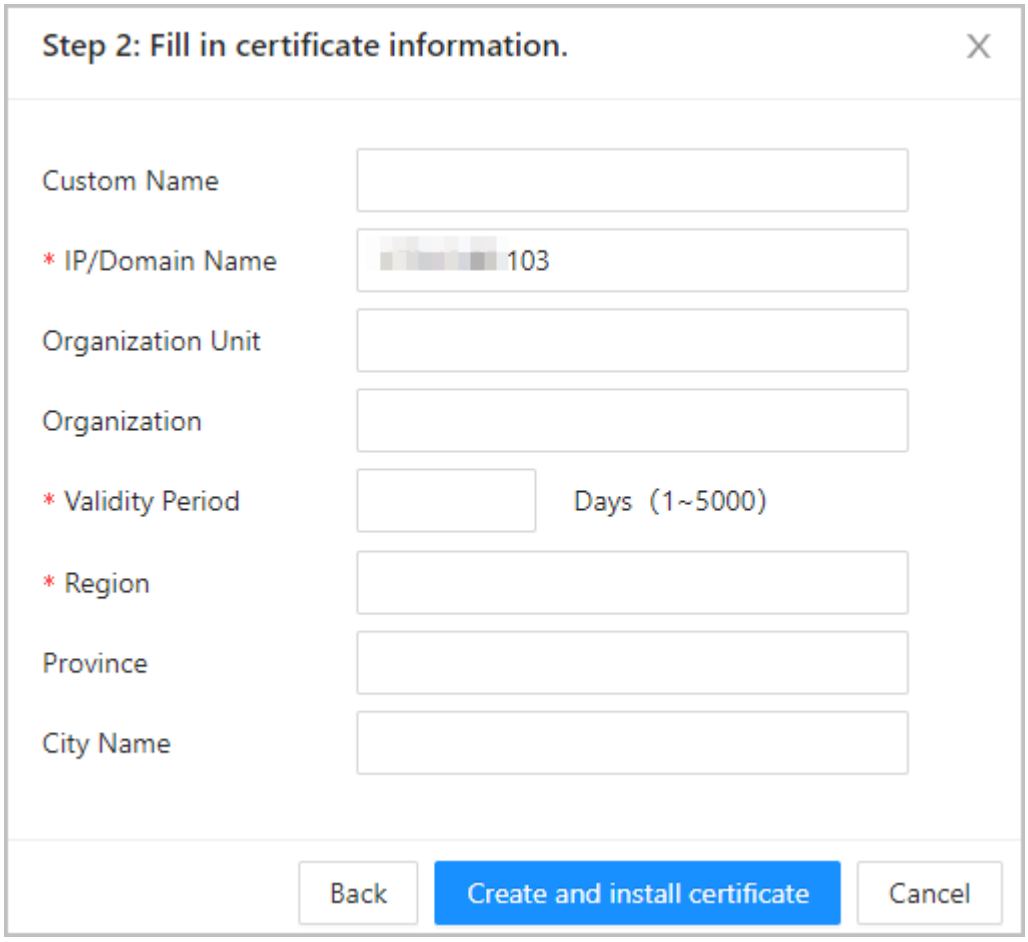
Step 1 Select > **CA Certificate** > **Device Certificate**.

Step 2 Click **Install Device Certificate**.

Step 3 Select **Create Certificate** , and then click **Next**.

Step 4 Enter the certificate information.

Figure 3-14 Certificate information



The name of region cannot exceed 2 characters. We recommend entering the abbreviation of the name of the region.

Step 5 Click **Create and install certificate**.

The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

3.6.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the Device.

Procedure

Step 1 Select > **CA Certificate** > **Device Certificate**.

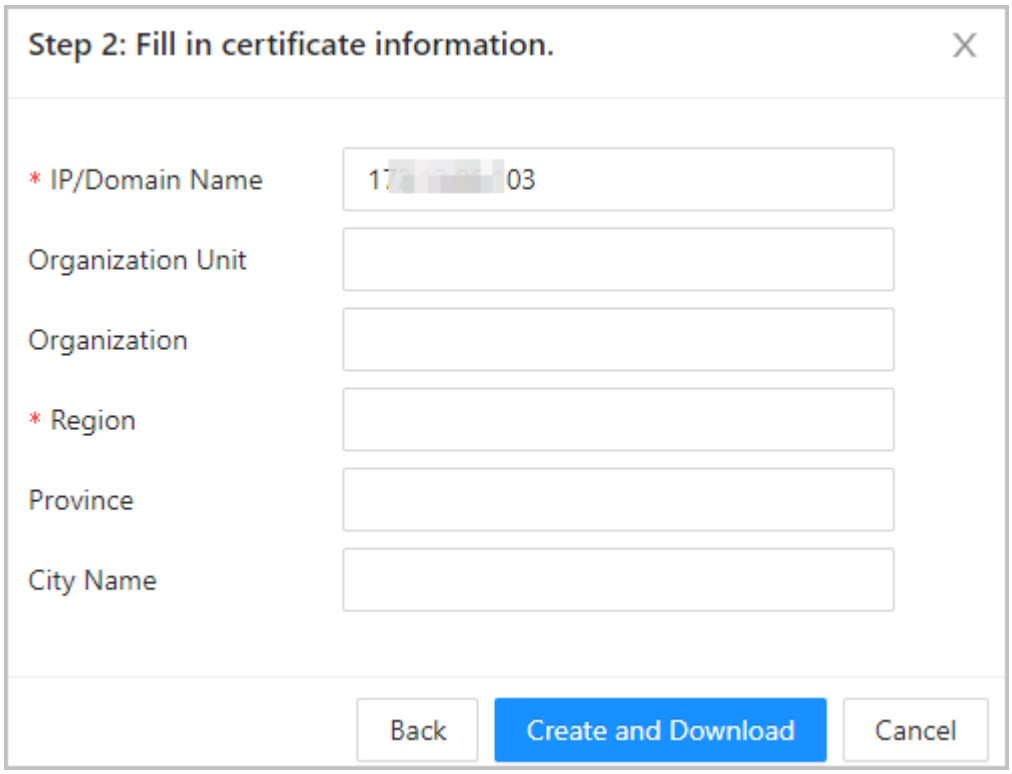
Step 2 Click **Install Device Certificate**.

Step 3 Select **Apply for CA Certificate and Import (Recommended)** , and then click **Next**.

Step 4 Enter the certificate information.

- IP/Domain name: The IP address or domain name of the Device.
- Region: The name of region must not exceed 2 characters. We recommend you enter the abbreviation of region name.

Figure 3-15 Certificate information (2)



Step 5 Click **Create and Download**.

Save the request file to your computer.

Step 6 Apply to a third-party CA authority for the certificate by using the request file.

Step 7 Import the signed CA certificate.

1. Save the CA certificate to your computer.
2. Click **Installing Device Certificate**.
3. Click **Browse** to select the CA certificate.
4. Click **Import and Install**.

   The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

   - Click **Recreate** to create the request file again.
   - Click **Import Later** to import the certificate at another time.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

3.6.4.3 Installing Existing Certificate

If you already have a certificate and private key file, import the certificate and private key file.

Procedure

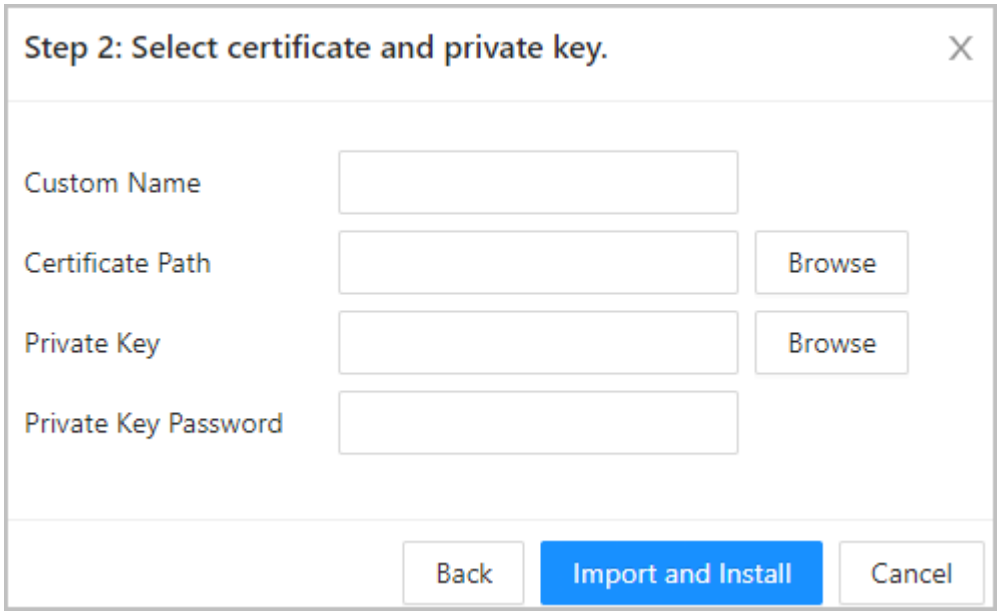
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Click **Install Device Certificate**.

Step 3 Select **Install Existing Certificate** , and then click **Next**.

Step 4 Click **Browse** to select the certificate path and private key file, and then enter a private key password.

Figure 3-16 Certificate and private key



Step 5 Click **Import and Install**.

The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.

Related Operations

- Click **Enter Edit Mode** on the **Device Certificate** page to edit the name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

3.6.5 Installing the Trusted CA Certificate

A trusted CA certificate is a digital certificate that is used for validating the identities of websites and servers. For example, when 802.1x protocol is used, the CA certificate for switches is required to authenticate its identity.

Background Information

802.1X protocol is a network authentication protocol that opens ports for network access when an organization authenticates users' identities and authorizes them access to the network.

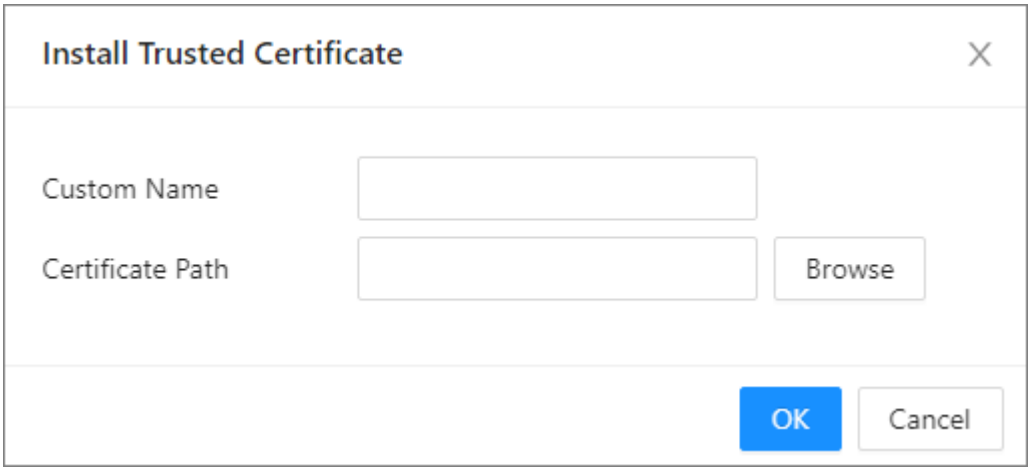
Procedure

Step 1 Select > **CA Certificate** > **Trusted CA Certificates**.

Step 2 Click **Install Trusted Certificate**.

Step 3 Click **Browse** to select the trusted certificate.

Figure 3-17 Install the trusted certificate



Step 4 Click **OK**.

The newly installed certificate is displayed on the **Trusted CA Certificates** page after the certificate is successfully installed.

Related Operations

- Click **Enter Edit Mode** on the **Trusted CA Certificates** page to edit the name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

3.6.6 Video Encryption

Procedure

Step 1 Select > **Video Encryption**.

Step 2 Configure the parameters.

Figure 3-18 Video encryption

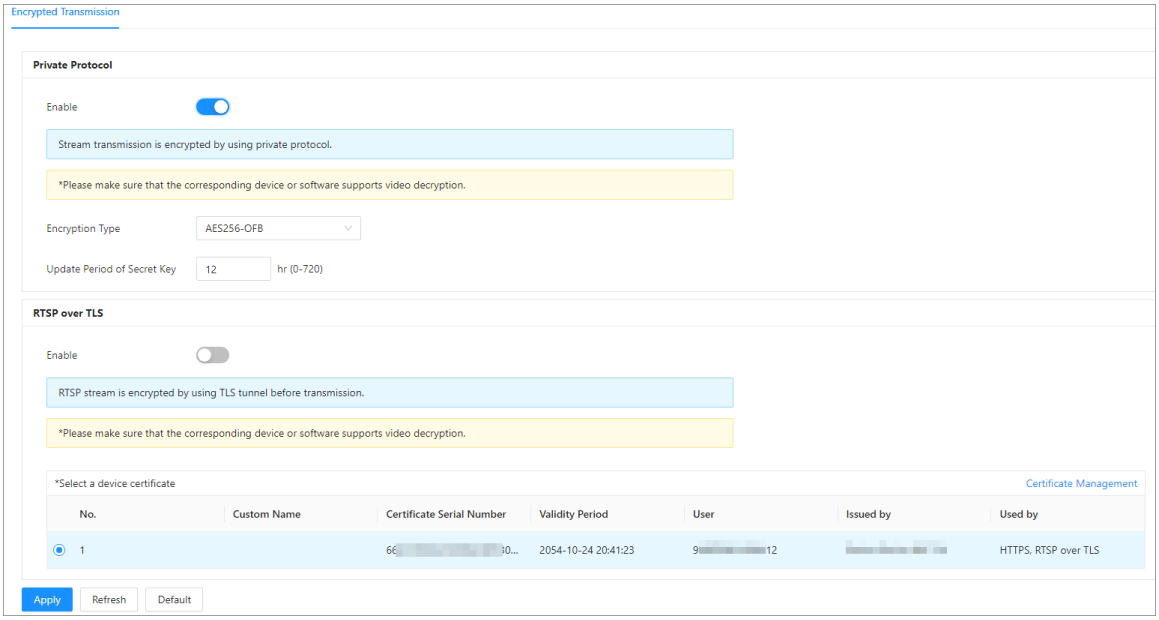


Table 3-2 Data encryption description

Parameter		Description
Private Protocol	Enable	Streams are encrypted during transmission through private protocol.
	Encryption Type	Keep it as default.
	Update Period of Secret Key	Ranges from 0 h –720 h. 0 means never updating the secret key.
RTSP over TLS	Enable	RTSP stream is encrypted during transmission through TLS tunnel.
	Certificate Management	Create or import a certificate. The installed certificates are displayed on the list.

3.6.7 Security Warning

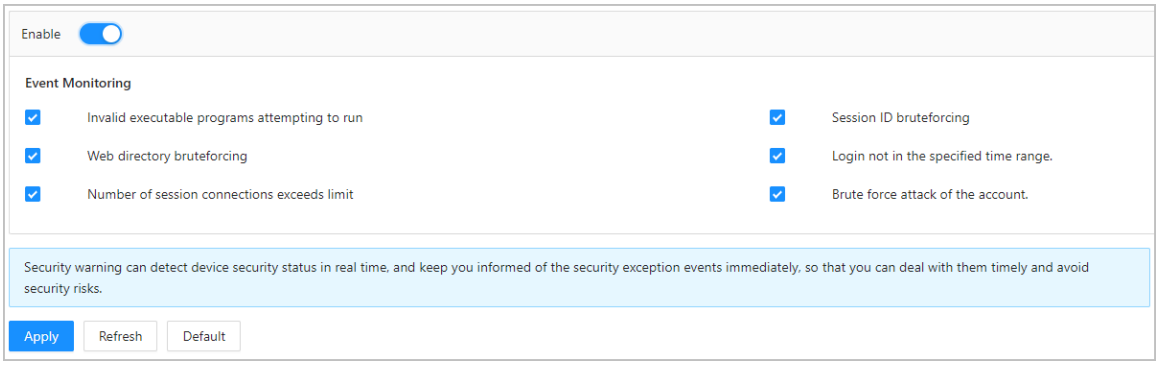
Procedure

Step 1 Select > **Security Warning**.

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 3-19 Security warning



Step 4 Click **Apply**.

3.6.8 Security Authentication

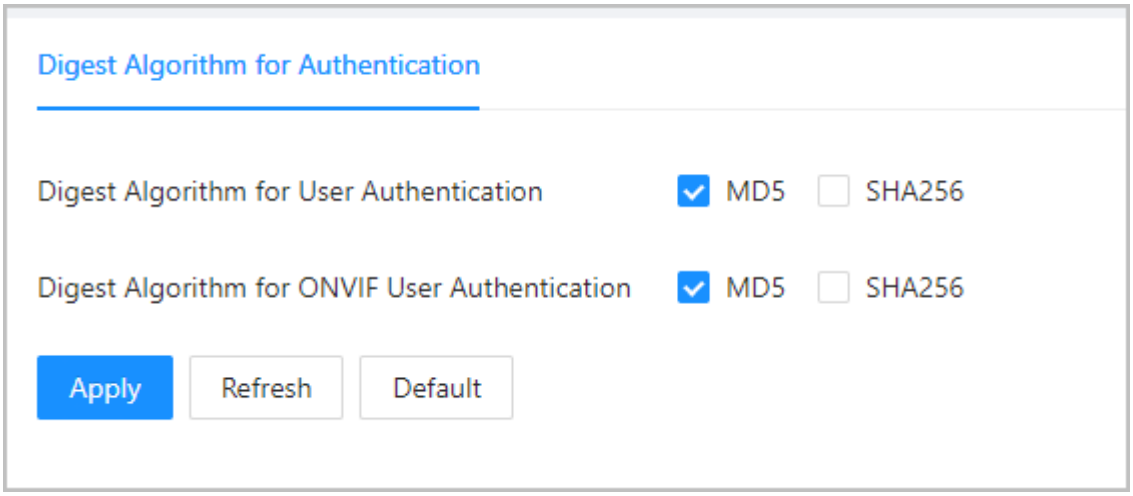
Procedure

Step 1 Select > **Security Authentication**.

Step 2 Select a message digest algorithm.

Step 3 Click **Apply**.

Figure 3-20 Security Authentication



3.7 Local Device Configuration

This chapter introduces the detailed configuration of the VTO.

Slight differences might be found in different models.

3.7.1 Basic Settings

Configure basic settings of the unit VTO or fence station.

Procedure

Step 1 Select **Local Device Config** > **Basic Settings**.

Step 2 Configure the parameters.

Figure 3-21 Basic settings

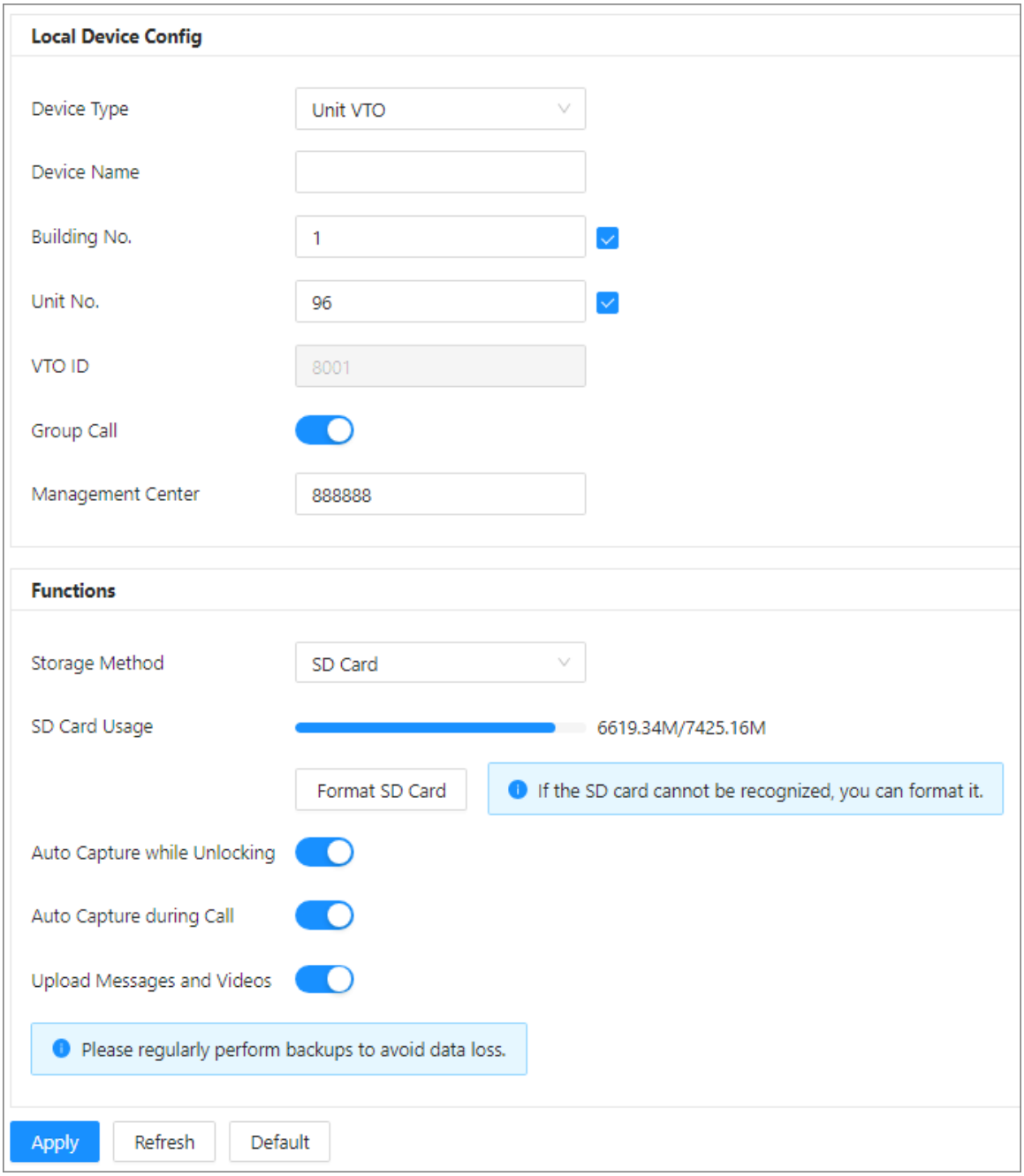


Table 3-3 Basic parameter description

Parameter	Description
Device Type	Select from **Unit VTO** and **Fence Station**.

Parameter	Description
Device Name	When other devices are monitoring this VTO, the device name will appear on the monitoring image.
Building No.	Configuring the building and unit number where the device is. If you clear the **Building No.** and **Unit No.** checkbox, it means that there is just only 1 building and unit.
Unit No.	
VTO ID	Used to differentiate each VTO, and we recommend you set it according to unit or building number, and then you can add VTOs to the SIP server by using their numbers. The number cannot be changed when the VTO serves as the SIP server.
Group Call	Enable it on the VTO that works as the SIP server, and when a main VTH receives a call, all extension VTHs will also receive the call.
Management Center	888888 by default.
Storage Method	SD card by default.
SD Card Usage	Displays the total and used capacity of the SD card. You can click **Format SD Card** to delete all the data in the SD card.
Auto Capture while Unlocking	Take a snapshot and save it in the SD card of the VTO when the VTO is unlocking. If the VTO is unlock through local unlock button, the snapshot will not be taken.
Auto Capture during Call	Take a snapshot and save it in the SD card of the VTO when the VTO is calling.
Upload Messages and Videos	When enabled: • If an SD card is inserted in both the VTH and VTO, the video message will be saved both in the SD cards of the VTH and the VTO. • If an SD card is only inserted in the VTH or the VTO, the video message will be saved only in the SD card of the VTH or the VTO. • If no SD card is inserted in the VTH or VTO, no video messages will be saved.

Step 3 Click **Apply**.

3.7.2 Configuring Access Control Parameters

3.7.2.1 Configuring Local Lock

The local lock refers to the lock that is connected to the function port of the VTO. You can configure the responding interval, unlock period, password and other parameters.

Procedure

Step 1 Select **Local Device Config** > **Access Control** > **Config**.

Step 2 Configure the parameters.

Figure 3-22 Access control

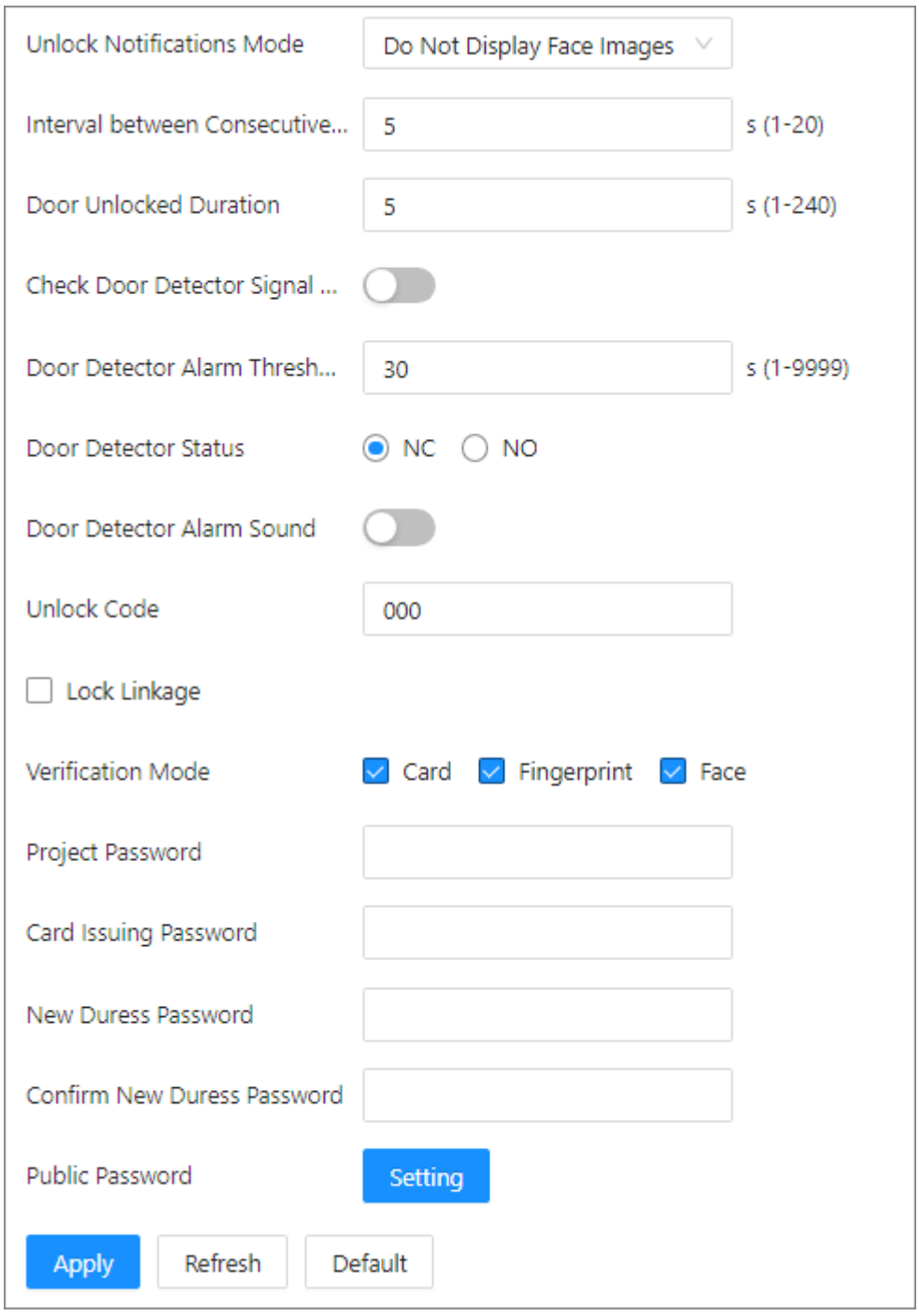


Table 3-4 Access control parameter description

Parameter	Description
Unlock Notifications Mode	Select from 3 unlock notifications modes. • **Do Not Display Face Images**. • **Only Display Face Database Images**. • **Display Snapshot and Face Database Images**.
Interval between Consecutive Unlocks	The door can only be unlocked again after the interval.
Door Unlocked Duration	The time during which the lock stays unlocked.
Check Door Detector Signal Before Locking	Enable the function based on your needs.
Door Detector Alarm Threshold	The threshold time when the door detector alarm is triggered.
Door Detector Status	• **NC** : Normally closed. • **NO** : Normally open.
Door Detector Alarm Sound	It is disabled by default. When it is enabled: • **Door Detector Status** is **NC** : If the door opening time exceeds the set door detection alarm threshold, the VTO will beep. And when the door detector is closed, the VTO does not beep again. • **Door Detector Status** is **NO** : If the door closing time exceeds the set door detection alarm threshold, the VTO will beep. And when the door detector is open, the VTO does not beep again.
Unlock Code	You can connect a third-party phone, such as a SIP phone, to the VTO, and use the code to open the door remotely.
Lock Linkage	Enable the **Lock Linkage**, and then select the linkage lock from the drop-down list.
Verification Mode	Enable the functions so that the card, fingerprint or face verification take effect. The fingerprint and face verification functions are available on select models.
Project Password	Used to go to the engineer setting screen on the VTO.
Card Issuing Password	Used to issue new cards.
New Duress Password	Configure the duress password. If you enter the password when you are forced, the alarm will be sent to the server.
Confirm New Duress Password	

Parameter	Description
Public Password	Click **Setting** to set the public password. 1. Click **Add** to add a public password. 2. Enter the user name and password., and then click **OK**. The password must consist of 4–6 digits.

Step 3 Click **Apply**.

3.7.2.2 Configuring the Extension Functions

3.7.2.2.1 RS-485

The lock can be connected through RS-485 port.

Procedure

Step 1 Select **Local Device Config** > **Access Control** > **Extension Function** > **RS-485**.

Step 2 Configure the parameters of the lock connected through the RS-485 port.

Figure 3-23 RS-485

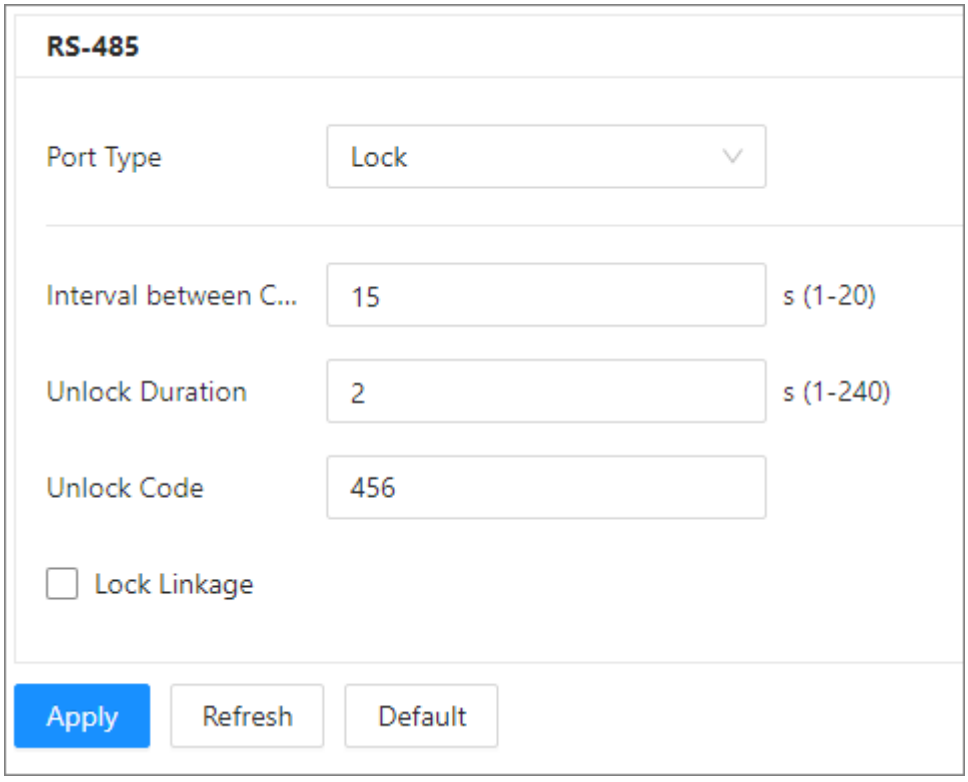


Table 3-5 RS-485 description

Parameter	Description
Port Type	Select **Lock** or **Card Reader** as the port type. It is **Lock** by default. When card reader is selected, fingerprint card reader and QR card reader are not supported.
Interval between Consecutive Unlocks	The door can only be unlocked again after the interval.
Unlock Duration	The time during which the lock stays unlocked.
Unlock Code	You can connect a third-party phone, such as a SIP phone, to the VTO, and use the code to open the door remotely.
Lock Linkage	Enable the **Lock Linkage**, and then select the linkage lock from the drop-down list.

Step 3 Click **Apply**.

- When the 485 module of VTO linked with security module (DEE1010B) connects to card reader, the security module has a limit on the length of the entered password (10 digits supported). Therefore, room number (6 digits) + personal password (6 digits) can not unlock the door.
- When the 485 module of VTO linked with security module (DEE1010B) connects to QR card reader or fingerprint card reader, the door cannot be unlocked because the RS-485 of VTO does not support QR code and fingerprint transmission.
- When the 485 module of VTO linked with security module (DEE1010B) connects to card reader, cards cannot be issued through the 485 module and security module DEE1010B, because the 485 module does not support bidirectional command interaction.

3.7.2.2.2 Network Lift Control

The lock can be connected to network lift control.

This function is available only when **Device Type** is selected as **Small Apartment**.

Procedure

Step 1 Select **Local Device Config** > **Access Control** > **Extension Function** > **Network Lift Control**.

Step 2 Enable the network lift control.

Step 3 Configure the lift control.

Figure 3-24 Network lift control

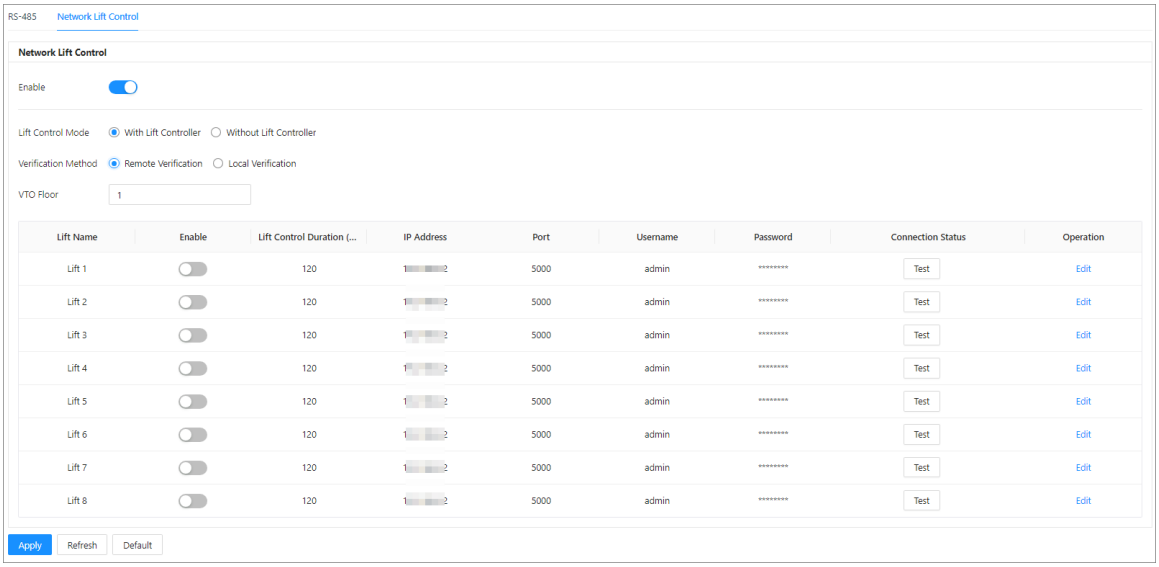


Table 3-6 Network lift control description

Parameter	Description
Lift Control Mode	• With Lift Controller: Up to 8 lifts can be added. • Without Lift Controller: Up to 6 lifts can be added.
Verification Method	It is enabled when the **Lift Control Mode** is set as **With Lift Controller**. • Remote Verification: The verification is made remotely. • Local Verification: The verification is made locally.
VTO Floor	Enter the floor in which the VTO is located.

Step 4 Click **Edit** to edit the lift information. And then click **OK**.

Figure 3-25 Set lift information

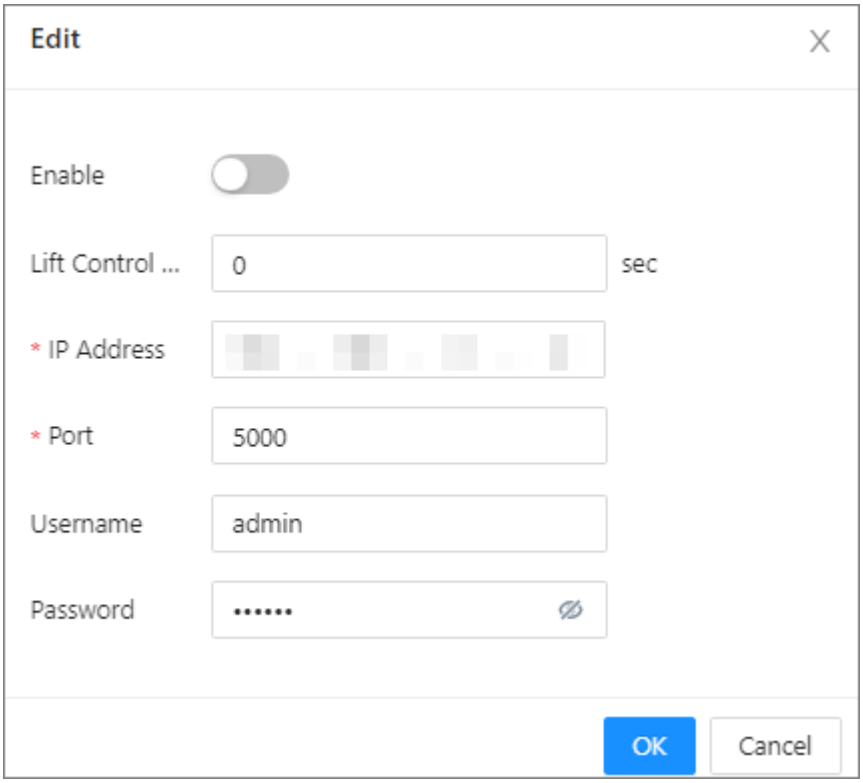


Table 3-7 Network lift control description

Parameter	Description
Lift Control Duration	Set the lift control duration from 0–999 seconds.
IP Address	Set the device IP address, port, user name and password.
Port	
Username	
Password	

Step 5 Click **Apply**.

Related Operations

Click **Test** to test the connection status of lifts.

3.7.3 Configuring Light Control

Configure the illuminator as needed.

Procedure

Step 1 Select **Local Device Config** > **Light Control**.

Step 2 Set illuminator mode from the following modes.

- **NO** : The illuminator is open all the time.
- **NC** : The illuminator is closed all the time.
- **Self-adaptive** : The illuminator will adapt to the environment, and then set a suitable value.

- **Period** : The illuminator will be open during the defining period.

Step 3 Click **Apply**.

3.7.4 Adding the IPC

If the current VTO works as the SIP server, you can add the IPC devices on the webpage of the VTO. The VTHs with the same online SIP server gets the IPC information.

- Supports adding the device with up to 32 channels.
- Supports directly adding IPC devices. You can get the IPC channel by adding NVR/XVR/HCVR.

3.7.4.1 Adding the IPC One by One

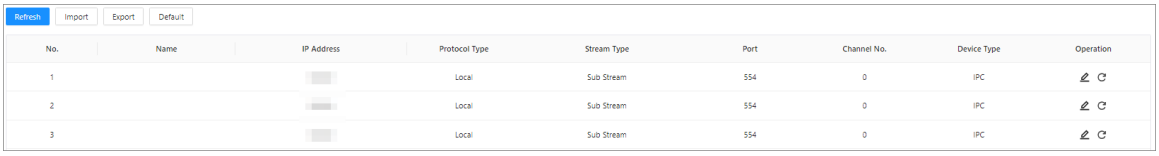
Add the information of the video monitoring device one by one.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **IPC Info**.

Figure 3-26 IPC information



Step 3 Click  to configure the parameters.

Figure 3-27 Configure the parameters

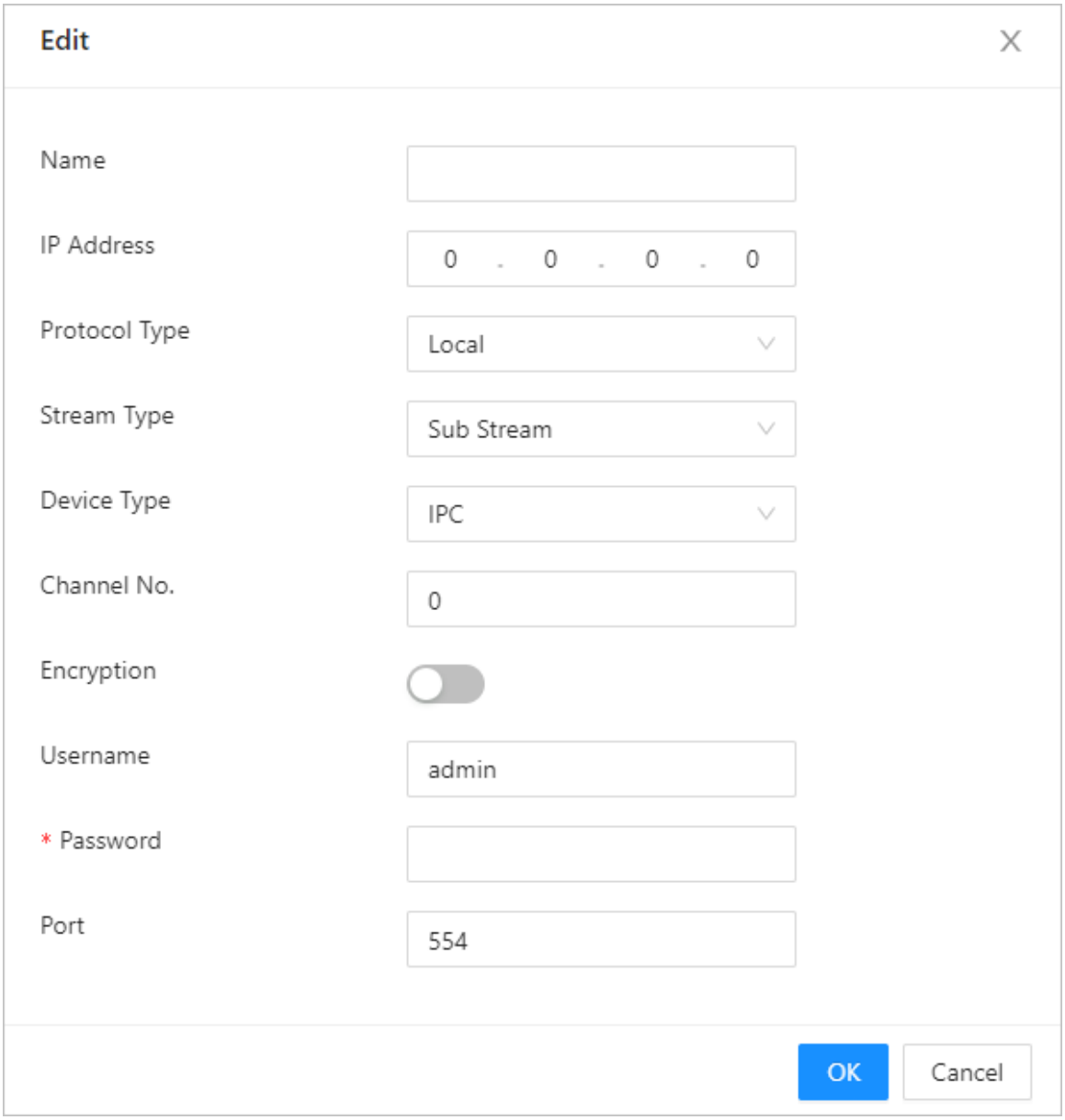


Table 3-8 Parameters description of the video monitoring device

Parameter	Description
Name	Enter the name of the IPC/VNR/XVR/HCVR device.
IP Address	Enter the IP address of the IPC/VNR/XVR/HCVR device.
Protocol Type	Select from **Local** and **ONVIF** according to the device you added.
Stream Type	Select from **Main Stream** and **Sub Stream**.
Device Type	Select the type according to the actual devices.
Channel No.	• If you add the IPC, it is 1 by default. • If you add the NVR/XVR/HCVR, it is the channel of IPC that was configured on the VNR/XVR/HCVR device.

Parameter	Description
Encryption	Keep consistent with the encryption status of the terminal device.
Username	Enter the user name and the password that used to log in to the webpage of the IPC/VNR/XVR/HCVR device.
Password	
Port	The value is 554 by default.

Step 4 Click **OK**.

3.7.4.2 Exporting the IPC Information in Batches

Export the IPC information and save the information to the local computer.

Procedure

Step 1 Click **Export**.

Step 2 Enter the password, and then click **OK**.

- The IPC configuration file is saved to the local computer.
- The password entered for exporting must be the same as the one for importing.

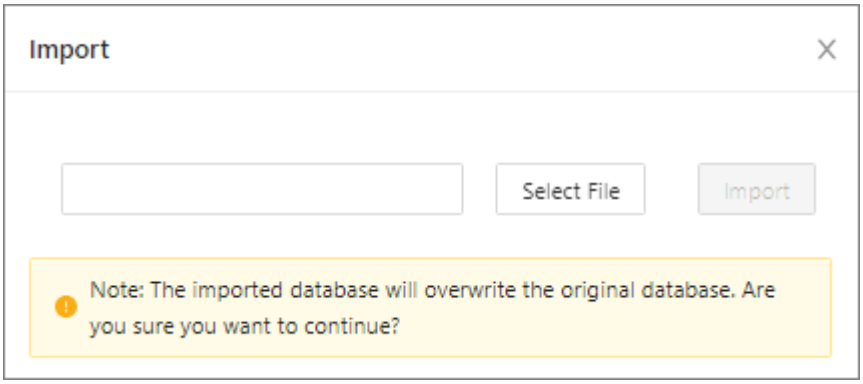
3.7.4.3 Importing the IPC Information in Batches

Import the IPC information to the system.

Procedure

Step 1 Click **Import**, and then enter the password.

Figure 3-28 Import



The password entered for exporting must be the same as the one for importing.

Step 2 Click **Select File** to add the file, and then click **Import**.

3.7.5 Configuring Cards

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Card Settings**.

Figure 3-29 Card settings

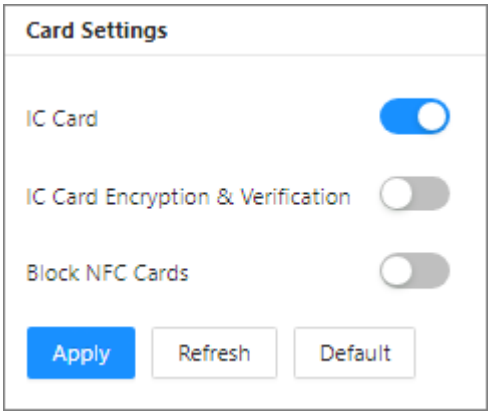


Table 3-9 Description of card parameters

Parameter	Description
IC Card	When enabled, IC card can be used to open the door.
IC Card Encryption & Verification	When enabled, the IC card is encrypted. Swipe the right card with successful encryption detection to open the door.
Block NFC Cards	Enable it so that the copied NFC cards cannot be used to open the door.

3.7.6 Configuring Wiegand

Supports access Wiegand devices such as Wiegand readers and access controllers. Configure the mode and the transmission mode according to your actual devices.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Wiegand Settings**.

Step 3 Configure the Wiegand parameters.

Figure 3-30 Wiegand input

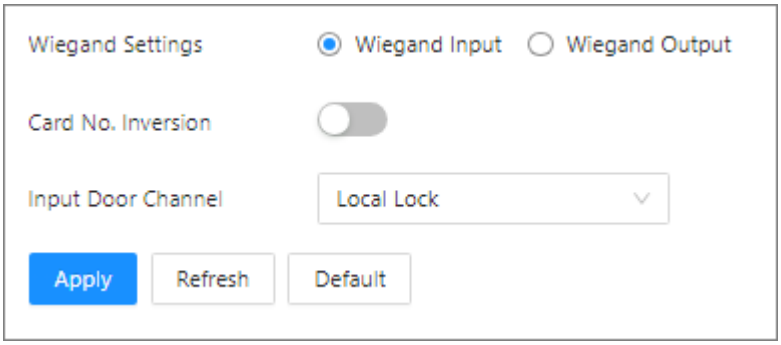


Figure 3-31 Wiegand output

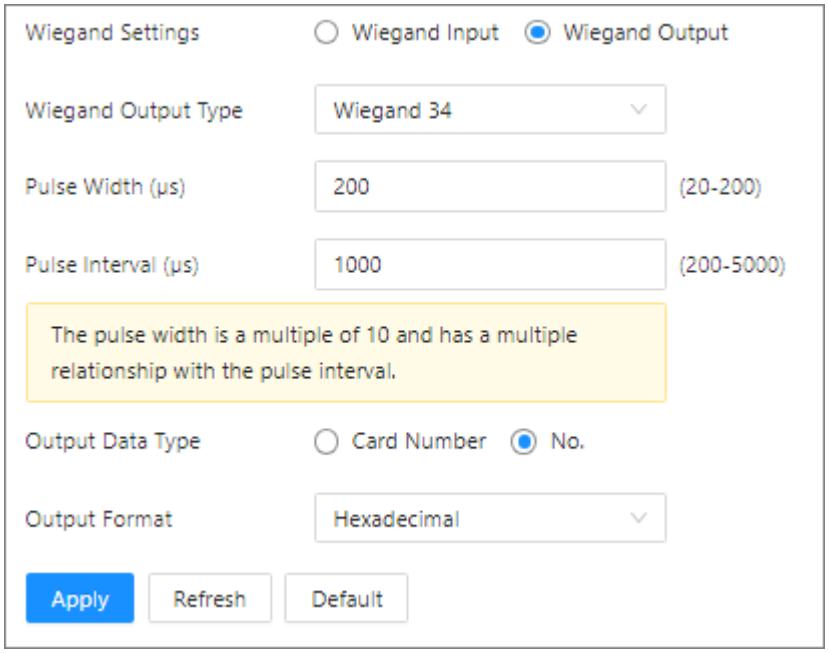


Table 3-10 Description of Wiegand parameters

Parameter		Description
Wiegand Settings		• Select **Wiegand Input** when other recognition devices are connected. • Select **Wiegand Output** when the VTO works as the recognition device. You can connect the access controller or other devices to the VTO.
Wiegand Input	Card No. Inversion	When the third party devices are connected, if the card number order recognized by the device is different from the actual card number, enable this function to correct it.
Input Door Channel		Select the channel from **Local Lock** and **External Lock**.
Wiegand Output	Wiegand Output Type	Select a Wiegand format to read card numbers or ID numbers. • **Wiegand 26** : Reads 3 bytes or 6 digits. • **Wiegand 34** : Reads 4 bytes or 8 digits. • **Wiegand 66** : Reads 8 bytes or 16 digits.
	Pulse Width	Enter the pulse width and pulse interval of Wiegand output.
	Pulse Interval	
	Output Data Type	Select the type of output data. • **Card Number** : Outputs data based on user's card number. • **No.** : Outputs data based on person ID.

Parameter		Description
	Output Format	When the output data type is configured as number, select from **Decimal** and **Hexadecimal**.

Step 4 Click **Apply**.

3.7.7 Configuring Face Detection

Configure the threshold, detection angle and other parameters.

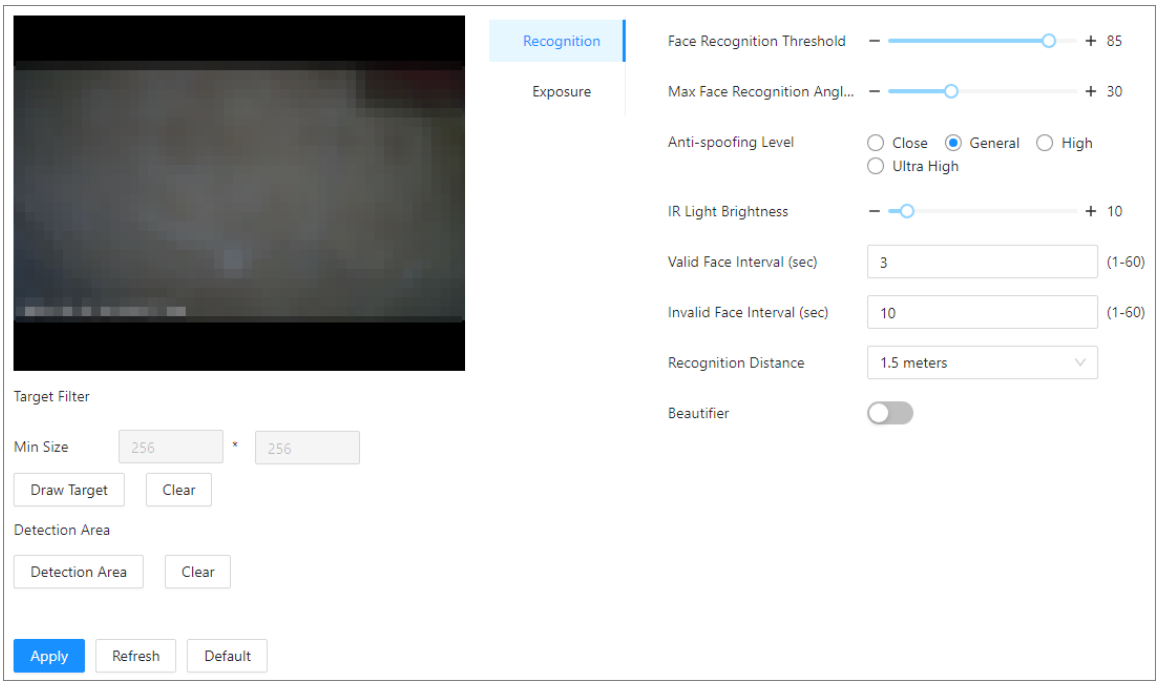
The face detection is available on select models.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Face Detection**.

Figure 3-32 Face detection parameters



Step 3 Configure the parameters.

Table 3-11 Description of face detection parameters

Name	Description
Face Recognition Threshold	Adjust the accuracy level of face recognition. Higher threshold means higher accuracy and lower false recognition rate. When the threshold is too low such as 0, the false recognition rate will be extremely high. Please be advised.

Name	Description
Max Face Recognition Angle Deviation	Set the largest angle that a face can be posed in for face detection. The larger the value, the larger the range for the face angle. If the angle a face is positioned in is not within the defined range, it might not be detected properly.
Anti-spoofing Level	This prevents people from using photos, videos, mask and other substitutes to gain unauthorized access.
IR Light Brightness	Adjust the IR light brightness of the device. Higher brightness means higher accuracy and lower false recognition rate.
Valid Face Interval (sec)	When the same face remains in front of the lens after the first successful recognition, the Device will perform recognition again for the face after a defined interval.
Invalid Face Interval (sec)	When the same face remains in front of the lens after the first failed recognition, the Device will perform recognition again for the face after a defined interval.
Recognition Distance	A certain distance between people and the device is required for recognition to be successful.
Beautifier	Beautify captured face images.

Step 4 Configure the exposure parameters.

Figure 3-33 Exposure parameters

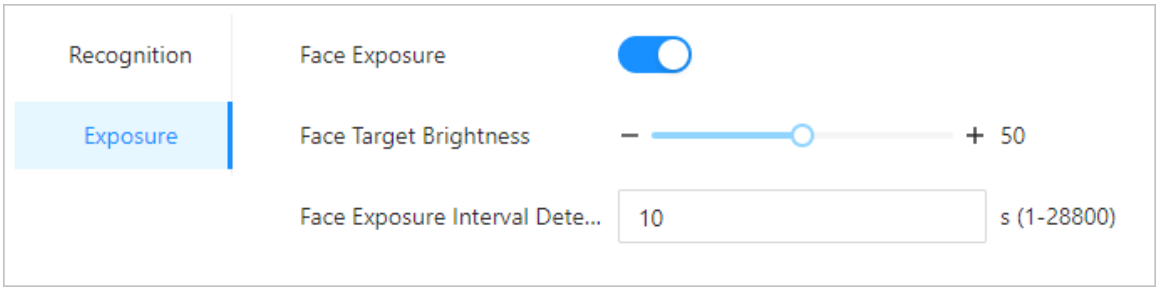


Table 3-12 Exposure parameters description

Parameter	Description
Face Exposure	After the face exposure function is enabled, the face will be exposed at the defined brightness to detect the face image clearly.
Face Target Brightness	
Face Exposure Interval Detection Time	The face will be exposed only once in a defined interval.

Related Operations

- Draw the face detection area.
  1. Click **Detection Area**.
  2. Right-click to draw the detection area, and then release the left button of the mouse to complete drawing.

     The face in the defined area will be detected.
  3. Click **Apply**.

- Draw the target size.
  1. Click **Draw Target**.
  2. Draw the recognition box to define the minimum size of detected face or enter the size.

     Only when the size of the face is larger than the defined size, the face can be detected by the Device.
  3. Click **Apply**.

3.7.8 Configuring QR Code

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **QR Code**.

Figure 3-34 QR code

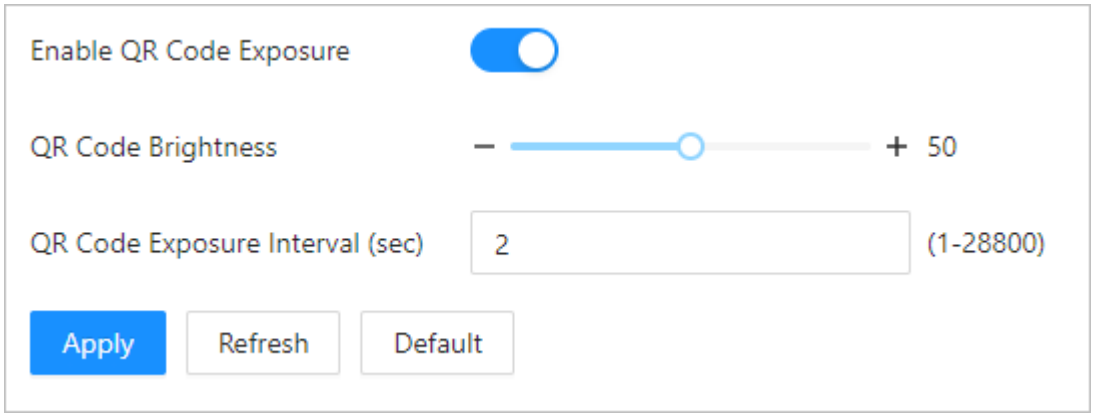


Table 3-13 QR code parameters

Parameters	Description
Enable QR Code Exposure	The QR code will be exposed at the defined brightness, and the QR code can be detected and read clearly.
QR Code Brightness	
QR Code Exposure Interval (sec)	The QR code will be exposed only once during the defined interval.

Step 3 Click **Apply**.

3.7.9 Configuring Fingerprint

Fingerprint recognition is available on select models.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Fingerprint**.

Step 3 Configure the fingerprint threshold.

The higher the value is, the more accurate the match result is.

Figure 3-35 Configure the fingerprint parameter



Step 4 Click **Apply**.

3.8 Device Setting

When the current VTO works as the SIP server, add VTH, VTS and other VTO as needed.

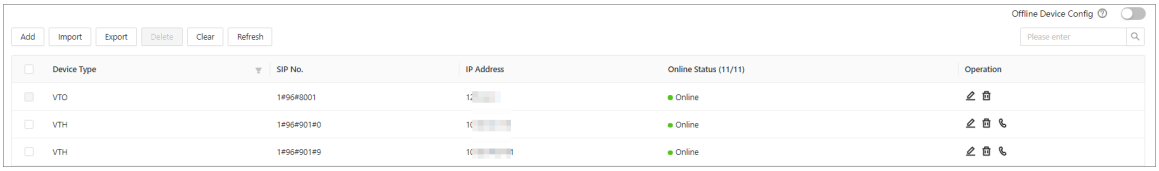
3.8.1 Adding the VTO

Procedure

Step 1 Log in to the webpage of the VTO.

Step 2 Click **Device Setting**.

Figure 3-36 Device setting



Step 3 Click **Add** , select **VTO** as the device type, and then configure the parameters.

The SIP server must be added.

Figure 3-37 Add a VTO

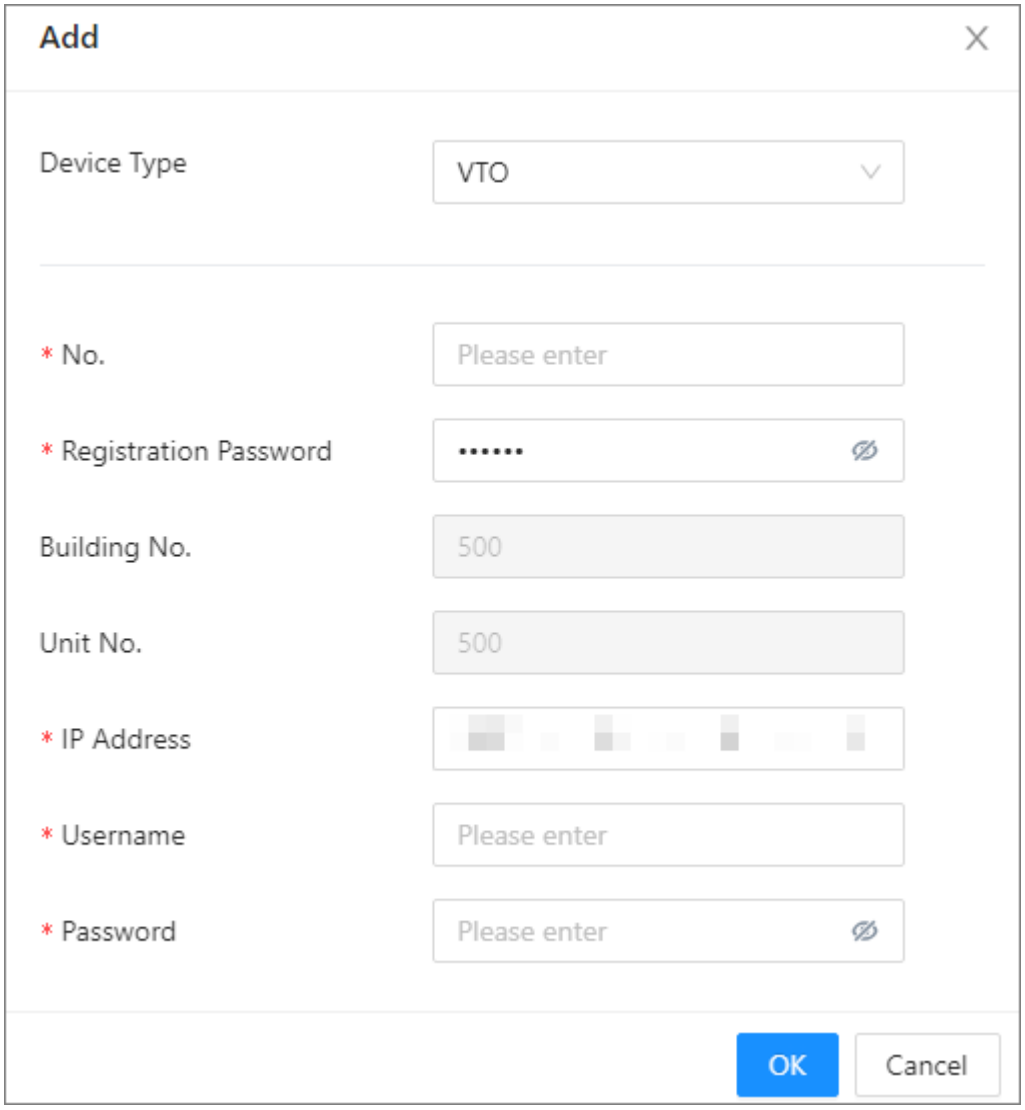


Table 3-14 VTO parameters description

Parameter	Description
No.	VTO number.
Registration Password	Default.
Building No.	Cannot be edited.
Unit No.	
IP Address	VTO IP address.
Username	The username and password of the webpage of the VTO.
Password	

Step 4 Click **OK**.

Related Operations

- Click to edit the VTO.

- Click to delete added VTOs, but the one that you have logged in to cannot be modified or deleted.
- Click or to call or hang up VTH.

  ◇ It is only available when SIP function is online.
  ◇ If the group call is enabled, the group call will be performed when call #0 or -0 VTH.

3.8.2 Adding the VTH

Procedure

Step 1 Log in to the webpage of the VTO.

Step 2 Select **Device Setting**.

Step 3 Click **Add** , select **VTH** as the device type, and then configure the parameters.

The SIP server must be added.

Figure 3-38 Add a VTH

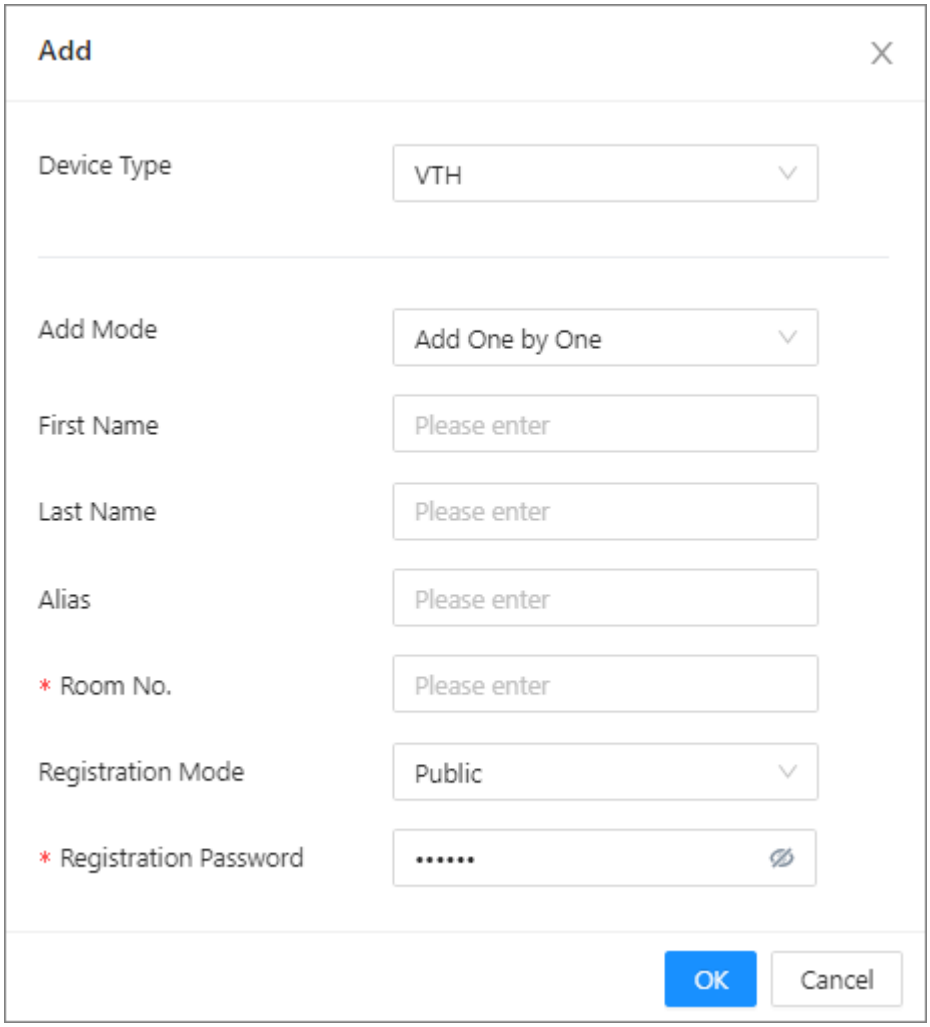


Table 3-15 VTH parameters description

Parameter	Description
Add Mode	Select from **Add One by One** and **Add in Batches**.
First Name	Information used to differentiate each room.
Last Name	
Alias	
Room No.	Room number. - The room number consists of up to 6 characters, and can contain numbers and letters. It cannot be the same as the VTO number. - When there are multiple VTHs, the room number for the main VTH should end with #0, and the room numbers for the extension VTHs end with #1, #2... - You can configure up to 5 extension VTHs for each main VTH.
Registration Mode	Select **Public** by default.
Registration Password	Default.

Step 4 Click **OK**.

3.8.3 Adding the VTS

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Device Setting**.

Step 3 Click **Add** , select **VTS** as the device type, and then configure the parameters.

The SIP server must be added.

Figure 3-39 Add a VTS

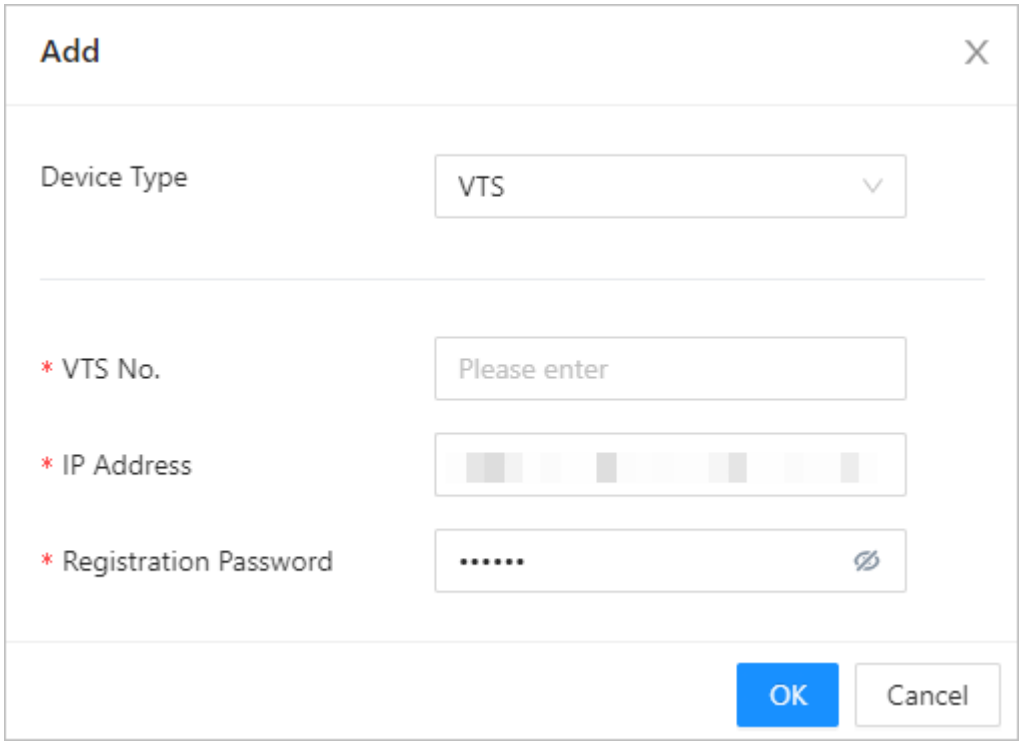


Table 3-16 VTS parameters description

Parameter	Description
VTS No.	The VTS number ranges from 888888101 through 888888999.
IP Address	The IP address of the VTS.
Registration Password	Leave the registration password as a default. If you want to register the password, make sure that it is the same with the register password of the VTS.

Step 4 Click **OK**.

3.8.4 Related Operations

Export Device Information

1. Select **Device Setting**.
2. Click **Export**.
3. Enter the login password, and then click **OK**.

   The device information is saved in your local computer.

Import Device Information

1. Select **Device Setting**.
2. Click **Import**.
3. Enter the login password, and then click **OK**.
4. Click **Browse** to select the file, and then click **OK**.

The imported data will overwrite the original data, please be advised.

Offline Device Config

When this function is enabled, the VTO sends information from the configuration file to make it easy for devices that are offline, which were added, to quickly connect to the network.

3.9 Person Management

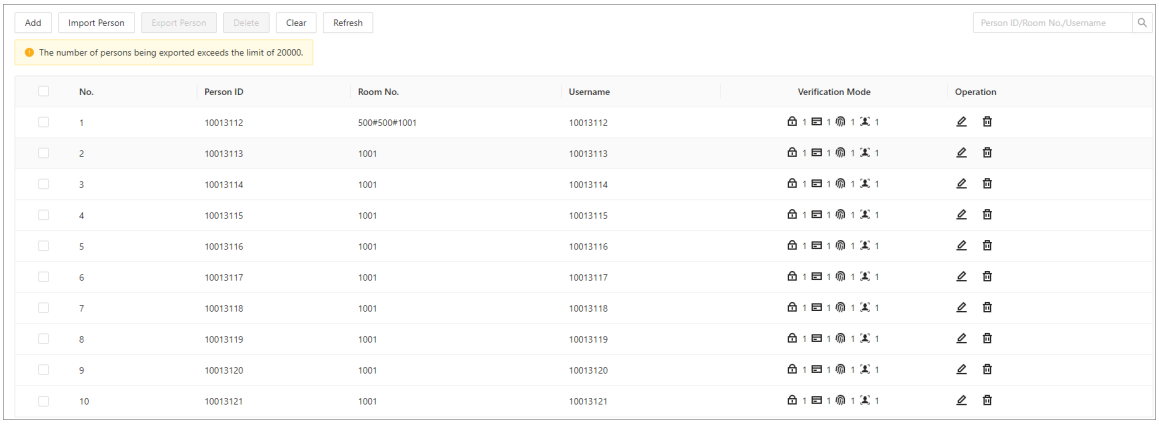
The card and fingerprint information that registered on the VTO will be uploaded to the person management in real time.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Person Management**.

Figure 3-40 Person management



Step 3 Click **Add**.

Step 4 Configure the parameters, and then click **OK**.

Figure 3-41 Add the person

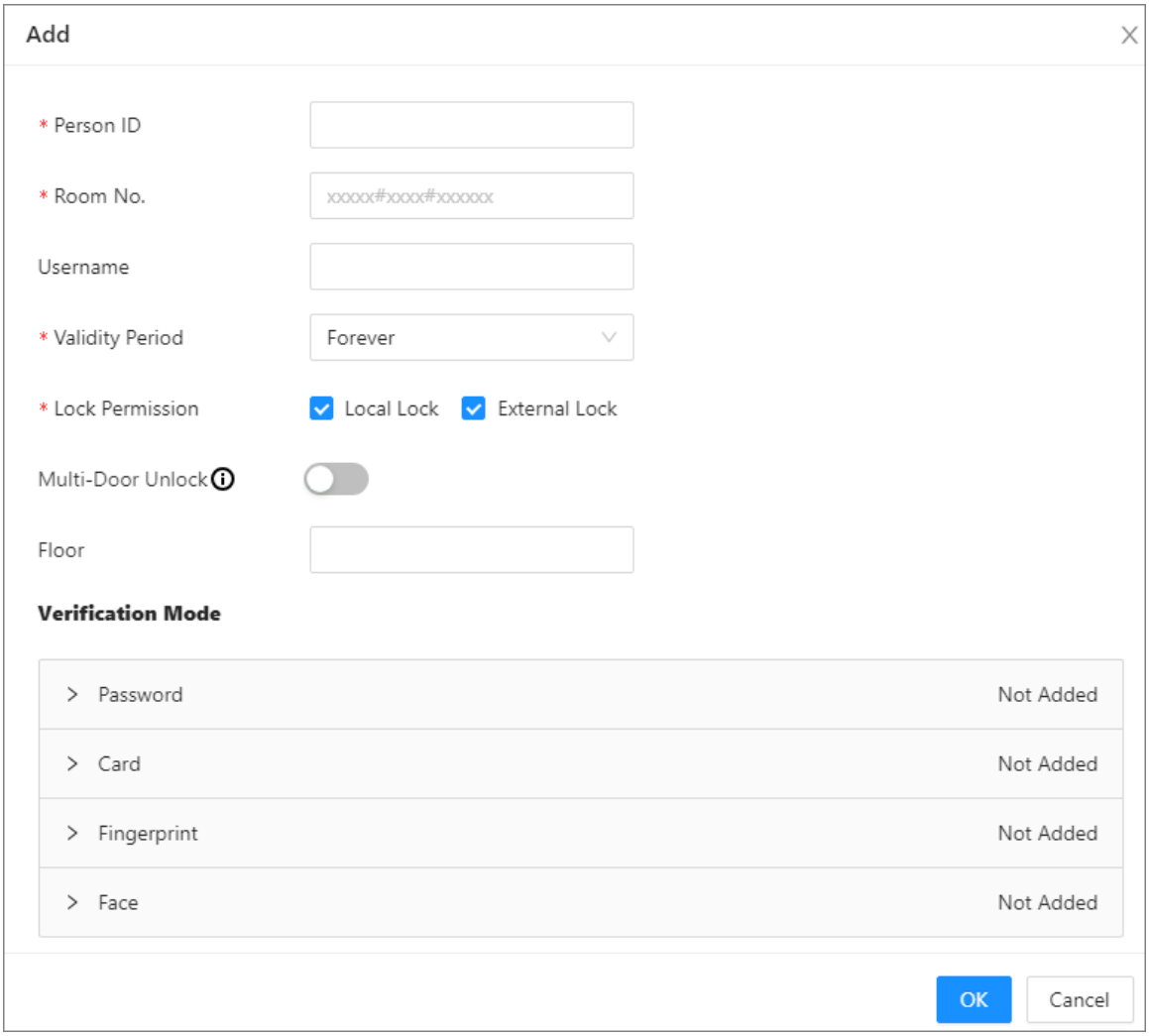


Table 3-17 Person parameters description

Parameter	Description
Person ID	Customize the number.
Room No.	Enter the corresponding room number of the VTH.
Username	Enter the user name.
Validity Period	Configure the validity period during which people have access permissions.
Lock Permission	Set the lock permission. You can enable the permission for local lock and external lock at the same time.
Multi-Door Unlock	When verification is successful, the local lock and external lock will open at the same time. The user password does not support this function.

Parameter	Description
Floor	Select the floor which can be given the permission. This parameter is available only when **Lift Control Mode** is selected as **Without Lift Controller**.
Password	1. Select **Password** > **Add**. 2. Enter the password, and then confirm it again. The password must consist of 4-6 digits. 3. Click **OK**.
Card	You can add up to 5 cards by entering the card number or adding cards on the device. 1. Select **Card** > **Add**. 2. Enter the card number. Or you can click **Issue Card**, and then swipe the card over VTO. 3. Click **OK**. You can manage the cards through the following icons. ● / : Configure the card as the main card or general card. ● : If you lost your card, click the icon to report the loss. The icon becomes . ● : The card cannot be used to open the door. Click it to make the card valid. ● : Edit the card name. ● : Delete the card.
Fingerprint	1. Select **Fingerprint** > **Add**. 2. Record your fingerprint according to the prompts. 3. Click **OK**.

Parameter	Description
Face	• **Upload** : Click **Upload** to upload the face image from the local computer. • **Local Collection** : Click **Local Collection**, and then click **Start Snapshot** to snap through the device. • The face image is only used for the device to unlock the door and does not involve other purposes. • With no face algorithm, the quality of face cannot be guaranteed, so failure or unrecognition may occur when the image is sent to VTO. • To ensure the quality of face collection, take the following requirement. ◇ The image format should be .jpg, .jpeg or .png. ◇ Do not cover your eyebrows, eyes, nose and mouth. ◇ Make sure that the face takes up more than 1/3 but no more than 2/3 of the whole image area. ◇ The horizontal rotation angle of the face, the pitch angle and the inclination angle should be within ±10°. ◇ Make sure the regular image brightness, moderate contrast, no shadow on the face, no overexposure and no underexposure. ◇ Make sure face integrity, clear outline and features, no heavy makeup, and image face area should be without editing modification processing.

3.10 Network Settings

3.10.1 Configuring TCP/IP

You need to configure IP address of Device to make sure that it can communicate with other devices.

Procedure

Step 1 Select **Network Setting** > **TCP/IP**.

Step 2 Configure the parameters.

Figure 3-42 TCP/IP

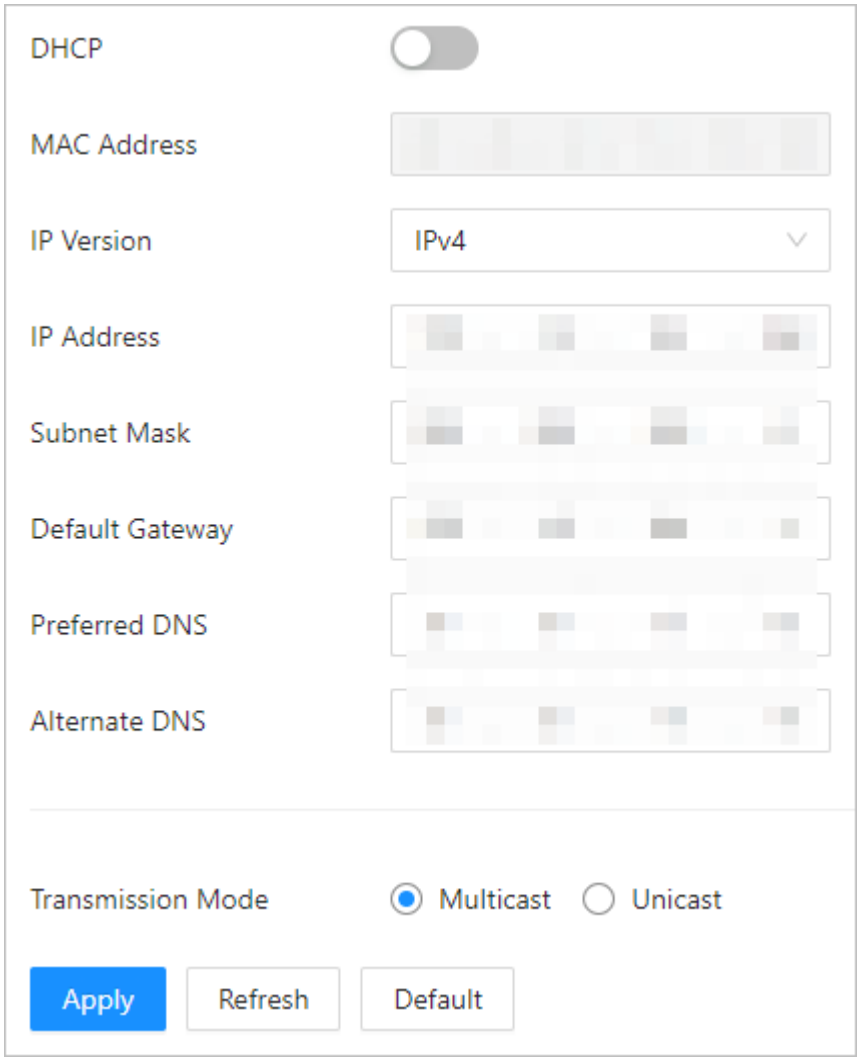


Table 3-18 Description of TCP/IP parameters

Parameter	Description
DHCP	DHCP stands for Dynamic Host Configuration Protocol. ● When not enabled, manually enter IP address, subnet mask, and gateway. ● When enabled, the Device will automatically be assigned with IP address, subnet mask, and gateway.
MAC Address	MAC address of the Device.
IP Version	IPv4 or IPv6.

Parameter	Description
IP Address	If you set the mode to **Static**, configure the IP address, subnet mask and gateway. ● IPv6 address is represented in hexadecimal. ● IPv6 version does not require setting subnet masks. ● The IP address and default gateway must be in the same network segment.
Subnet Mask	
Default Gateway	
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.
Transmission Mode	● Multicast: Ideal for video talk. ● Unicast: Ideal for group call. Unicast is not recommended when the platform is being used as an SIP server.

Step 3 Click **Apply**.

3.10.2 Configuring Port

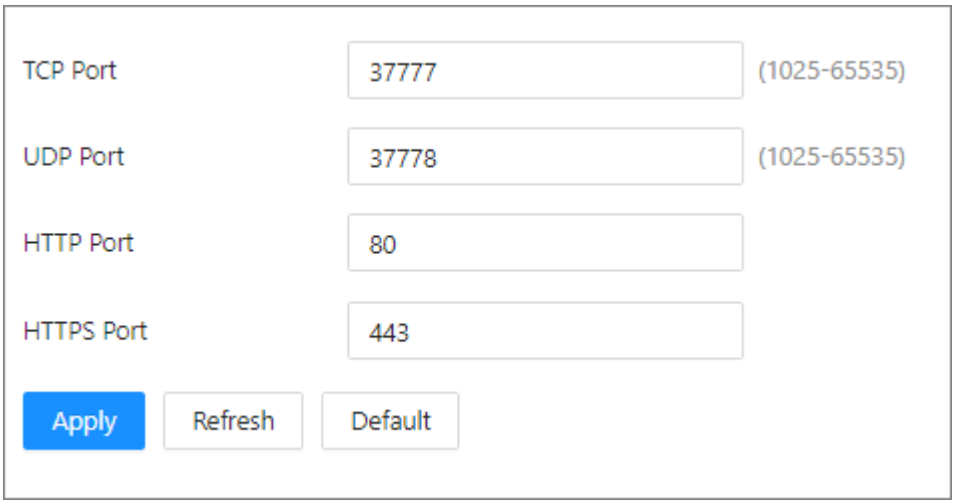
You can limit access to the Device at the same time through webpage, desktop client and mobile client.

Procedure

Step 1 Select **Network Setting** > **Port**.

Step 2 Configure the ports.

Figure 3-43 Ports



Restart the Device to make the configurations effective after you change other parameters.

Table 3-19 Description of ports

Parameter	Description
TCP Port	Default value is 37777.
UDP Port	Default value is 37778.
HTTP Port	Default value is 80. If you have changed the port number, add the port number after the IP address when access the webpage.
HTTPS Port	Default value is 443.

Step 3 Click **Apply**.

3.10.3 Configuring the SIP Server

When connected to the same SIP server, all the VTOs and VTHs can call each other. You can use a VTO or another server as the SIP server.

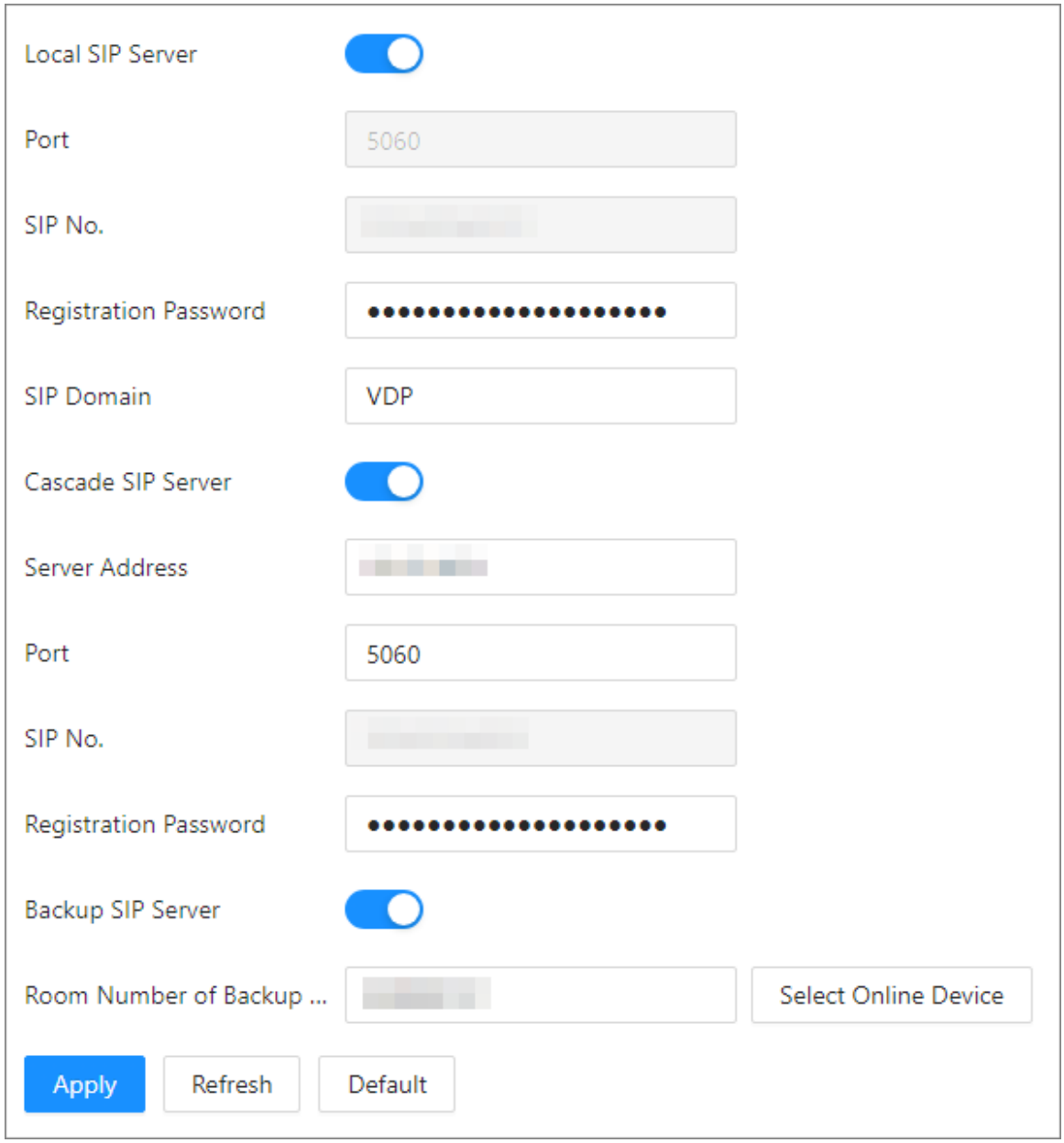
3.10.3.1 VTO as the SIP Server

Procedure

Step 1 Select **Network Settings** > **SIP Server**.

Step 2 Configure the parameters.

Figure 3-44 VTO as the SIP server



- If the current VTO works as the SIP server, enable **Local SIP Server** , and then click **Apply**.
- If another VTO is working as the SIP server, set **Device** as **Server Type**, configure the parameters, and then click **Apply**.

Table 3-20 SIP server configuration

Parameter	Description
Port	5060 by default when the VTO works as an SIP server.
SIP No.	8001 by default when the VTO works as an SIP server.
Registration Password	Leave it as default.
SIP Domain	VDP is by default.

Parameter	Description
Cascade SIP Server	Enable the cascade SIP server, and then enter the address, port, SIP No., registration password, the username and password of the cascade SIP server.
Server Address	
Port	
SIP No.	
Registration Password	
SIP Server Username	
SIP Server Password	
Backup SIP Server	Enable the backup SIP server, and then enter the room number of the server, or you can click **Select Online Device** to select an online server.
Room Number of Backup Server	

Step 3 Click **Apply**.

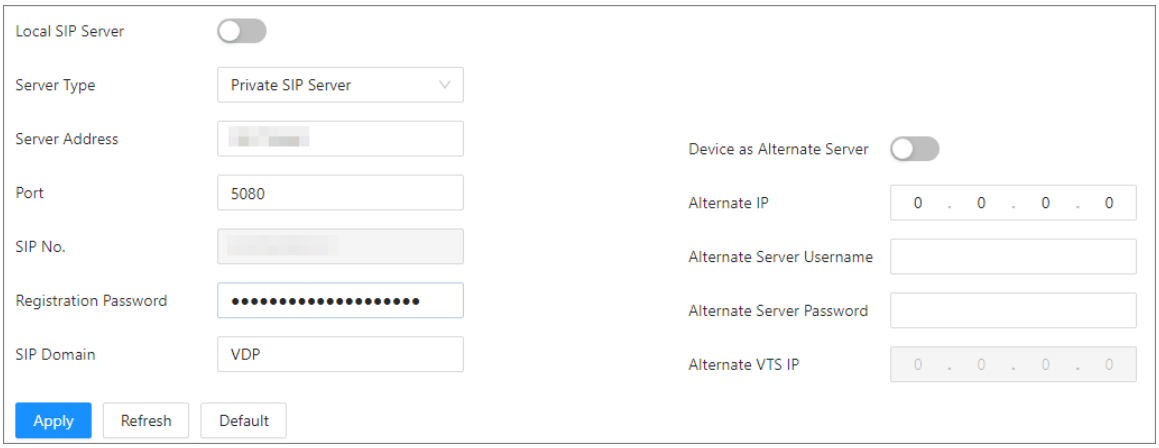
3.10.3.2 Platform as the SIP Server

Procedure

Step 1 Select **Network Settings** > **SIP Server**.

Step 2 Select **Private SIP Server** as **Server Type**.

Figure 3-45 Platform as the SIP server



Step 3 Configure the parameters.

Table 3-21 Private SIP server configuration

Parameter	Description
Server Address	The IP address of the SIP server.
Port	5080 by default when the platform works as the SIP server.
SIP Domain	Keep default value VDP or leave it empty.

Parameter	Description
Alternate IP	The alternate server will be used as the SIP server when DSSExpress/DSS pro stops responding We recommend you configure the alternate IP address. ● If you enable **Alternate Server**, the current VTO you have logged in serves as the alternate server. ● If you want another VTO serve as the alternate server, you need to enter the IP address of that VTO in the **Alternate IP Addr.** textbox. Do not enable **Alternate Server** in this case.
Alternate Username/ Password	Used to log in to the alternate server.
Alternate VTS IP	IP address of the alternate VTS.

Step 4 Click **Apply**.

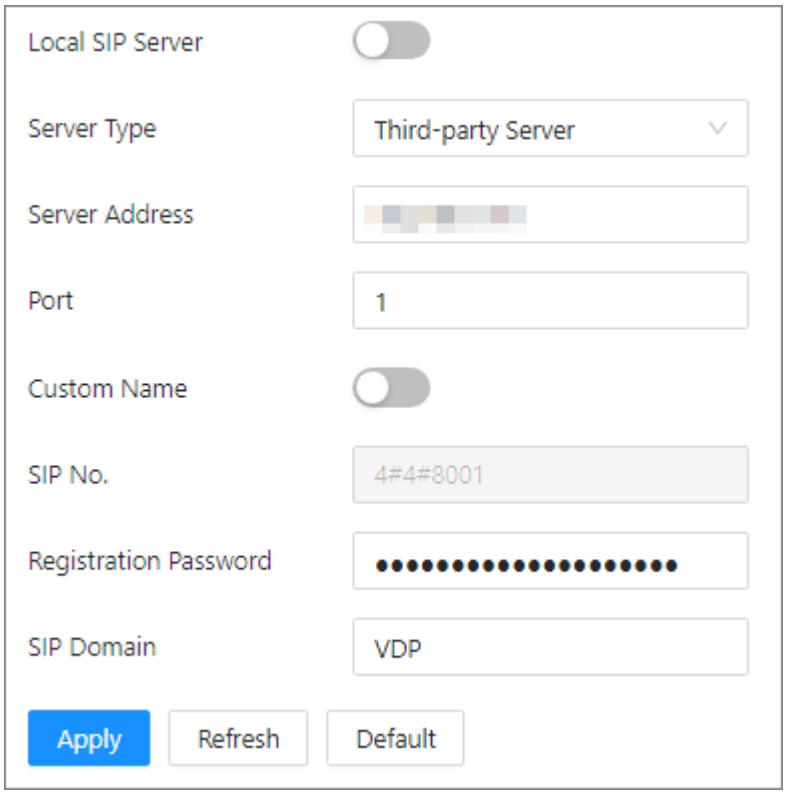
3.10.3.3 Configuring Third-Party Server

Procedure

Step 1 Select **Network Settings** > **SIP Server**.

Step 2 Set **Third-Party Server** as **Server Type**.

Figure 3-46 Third-party server



Step 3 Configure the parameters.

Table 3-22 Third-party server configuration

Parameter	Description
Server Address	The IP address of the SIP server.
Port	Enter the port of the SIP server, which is from 1 to 65535.
Custom Name	If enable the **Custom Name** , you can customize the **SIP No.**.
SIP No.	
Registration Password	Leave it as default.
SIP Domain	Keep default value VDP or leave it empty.

Step 4 Click **Apply**.

- For some third-party servers, if the intercom selects two unlocking methods of the **RFC 2833** and **SIP INFO** at the same time, the unlocking code will not available to unlock the intercom.
- When a third-party server is used to support a third-party intercom, the intercom exception or SIP offline may occur on some servers.
- If **Third-party Server-Asterisk** and **SIP Intercom** select two unlocking methods of the **RFC 2833** and **SIP INFO** at the same time, the unlocking code will not available to unlock the intercom.
- If IB intercom frequently disconnects from the 3CX server, the mapping relationship needs to be deleted.

3.10.4 Configuring Cloud Service

The cloud service provides a NAT penetration service. You can manage multiple devices through DMSS. You do not have to apply for dynamic domain name, configure port mapping or deploy server.

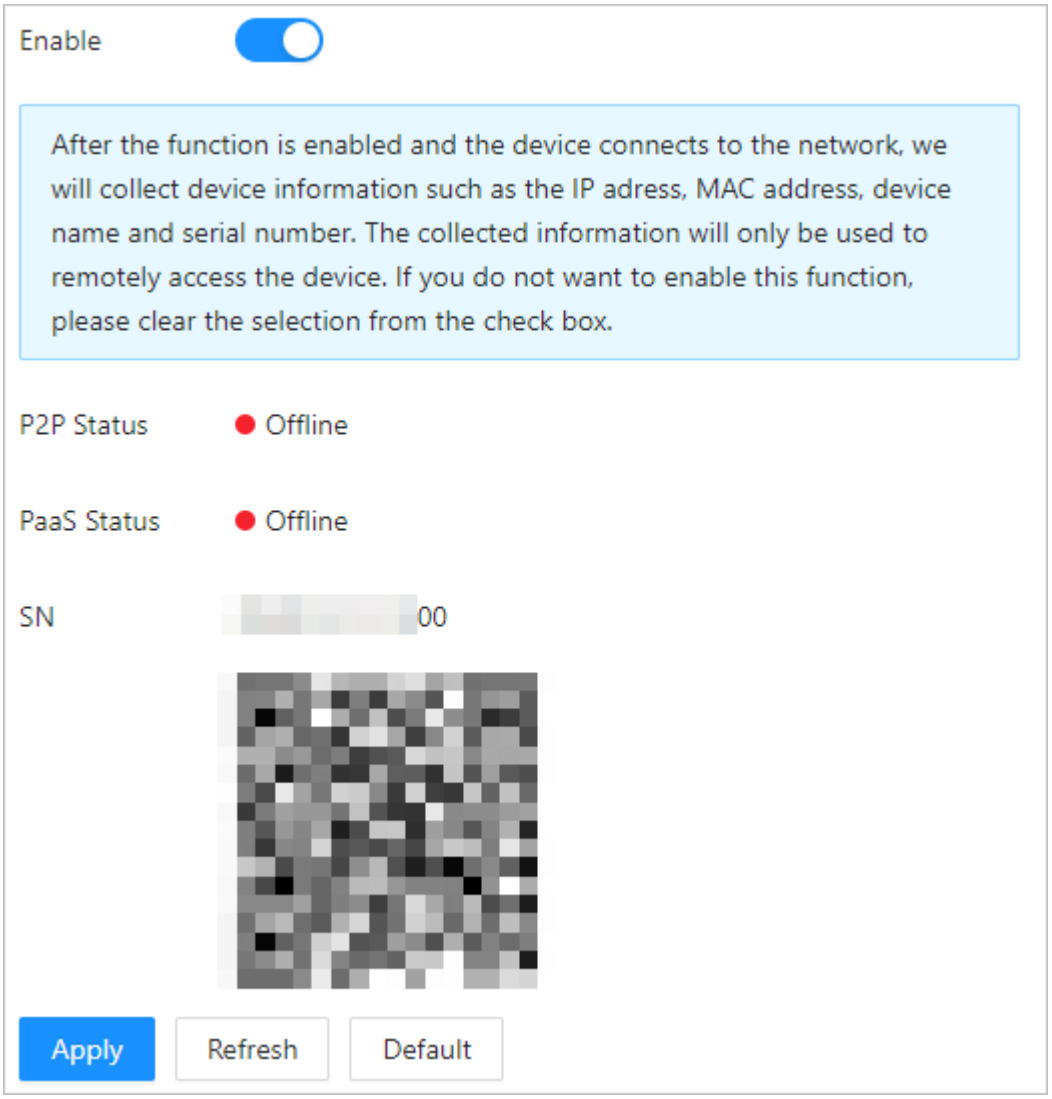
Procedure

Step 1 Select **Network Setting** > **Cloud Service**.

Step 2 Enable the cloud service function.

The cloud service goes online if the P2P and PaaS are online.

Figure 3-47 Cloud service



Step 3 Click **Apply**.

Step 4 Scan the QR code with DMSS to add devices.

3.10.5 Configuring UPnP

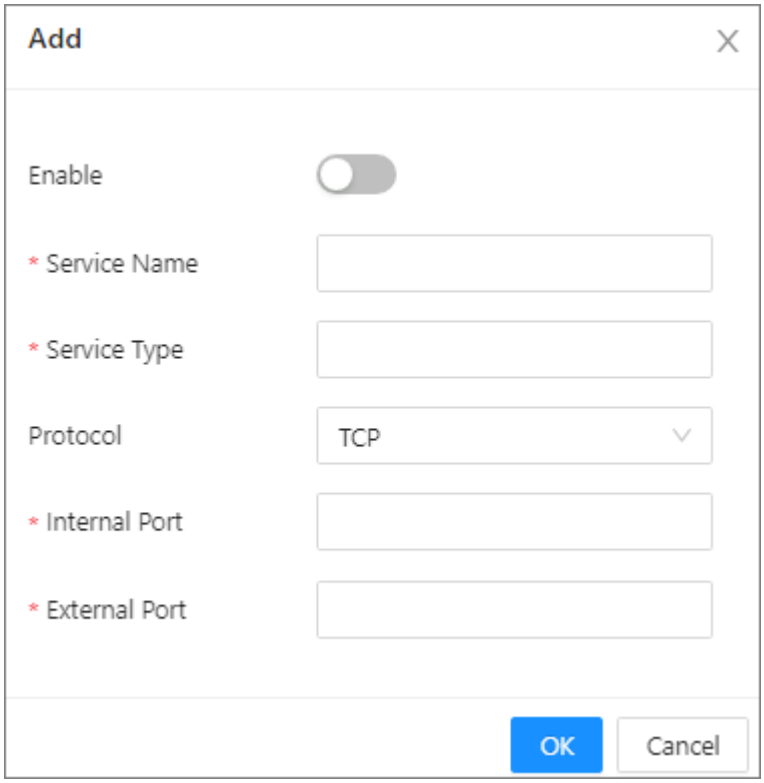
Procedure

Step 1 Log in to the webpage.

Step 2 Select **Network Settings** > **UPnP**.

Step 3 Click **Add** to add new services.

Figure 3-48 Add new service



Step 4 Click **Apply**.

3.10.6 Configuring Basic Services

Log in to the webpage of VTO, and then select **Network Settings** > **Basic Services**.

Enable the protocol as needed, and then click **Apply**.

Figure 3-49 Basic services

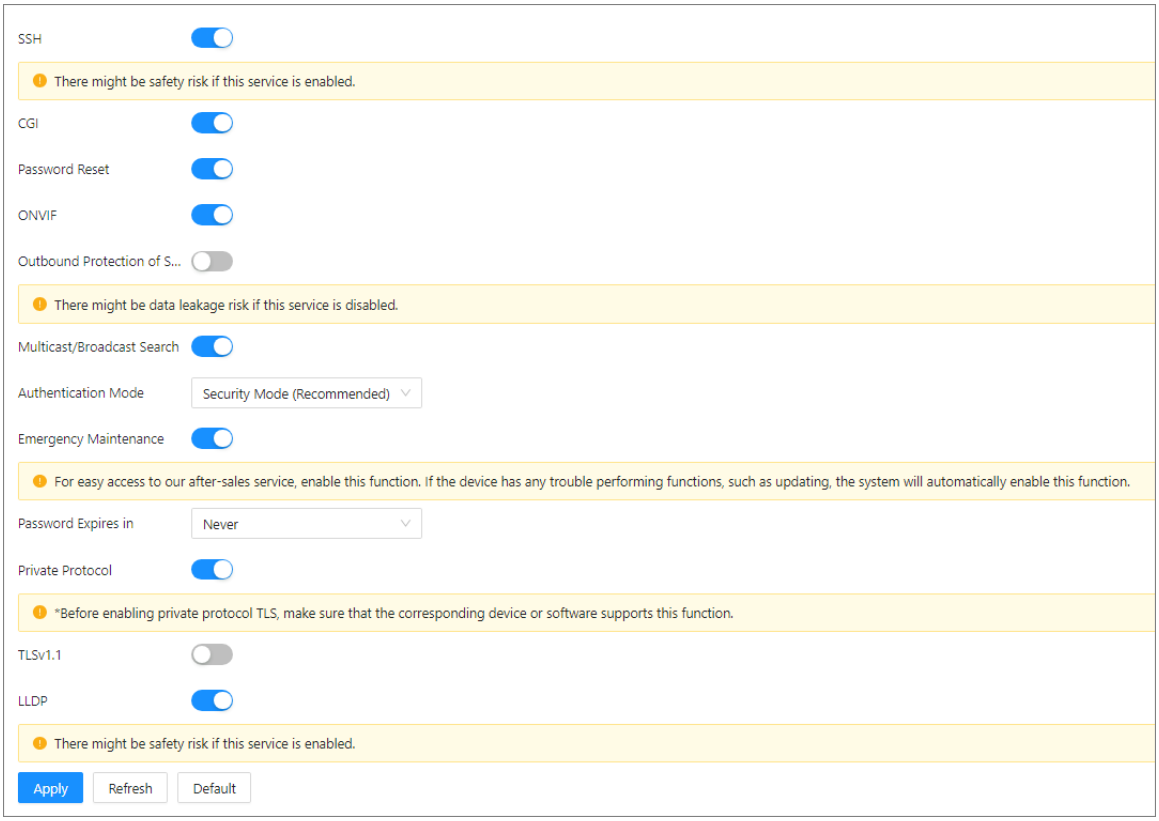


Table 3-23 Description of basic services

Service	Description
SSH	If enabled, you can log in to the VTO through SSH.
CGI	Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs similarly to console applications running on a server that dynamically generates web pages. If enabled, CGI commands can be used. The CGI is enabled by default.
Password Reset	Enabled by default. You can configure the email address. After configuration, you can click **Forget Password?** on the login page to reset the password.
ONVIF	Enable other devices to pull video stream of the device through the ONVIF protocol. Profile C and Profile S are only supported. Encoding format and image parameters are not supported.
Outbound Protection of Service Password	If enabled, the device password cannot be got through the third-party protocol tool.
Multicast/Broadcast Search	Enable this function, and then when multiple users are previewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.

Service	Description
Authentication Mode	• **Security Mode (Recommended)** : The mode does not support logging in with Digest, DES and plain text authentication. • **Compatibility Mode** : The mode supports logging in with Digest, DES and plain text authentication.
Emergency Maintenance	When the device is abnormal, enable **Emergency Maintenance** to upgrade or modify the device configuration.
Password Expires in	Set the validity period of the password.
Private Protocol	If enabled, the platform can access to the device with private protocol.
TLSv1.1	There is security risk if you enable **TLSv1.1**.
LLDP	Transmits the device basic information to the platform.

3.10.7 Configuring Auto Registration

VTO automatically registers on the server, and reports its IP address to the designated server.

Procedure

Step 1 Log in to the webpage of VTO.

Step 2 Select **Network Settings** > **Auto Registration**.

Step 3 Enable the function. Enter the server address, port number and sub-device ID.

Figure 3-50 Auto registration

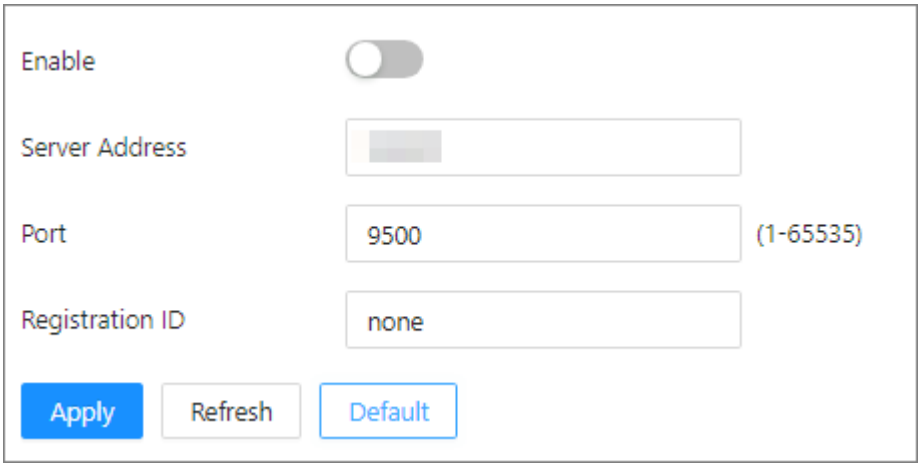


Table 3-24 Parameters description

Parameter	Description
Server Address	IP address or domain name of the server that is needed in registration.
Port	Port number that the server automatically registers.
Registration ID	The server distributes an ID for the device. Keep consistent with the ID registered on the server.

3.10.8 Configuring Registration Management

This function is only available when the Private SIP Server is set as server type and the Alternate Server is enabled. For details, see "3.10.3.2 Platform as the SIP Server".

Procedure

Step 1 Log in to the webpage of VTO.

Step 2 Select **Network Settings** > **Registration Management**.

Step 3 Click **Add** to add clients.

Figure 3-51 Configure the parameter

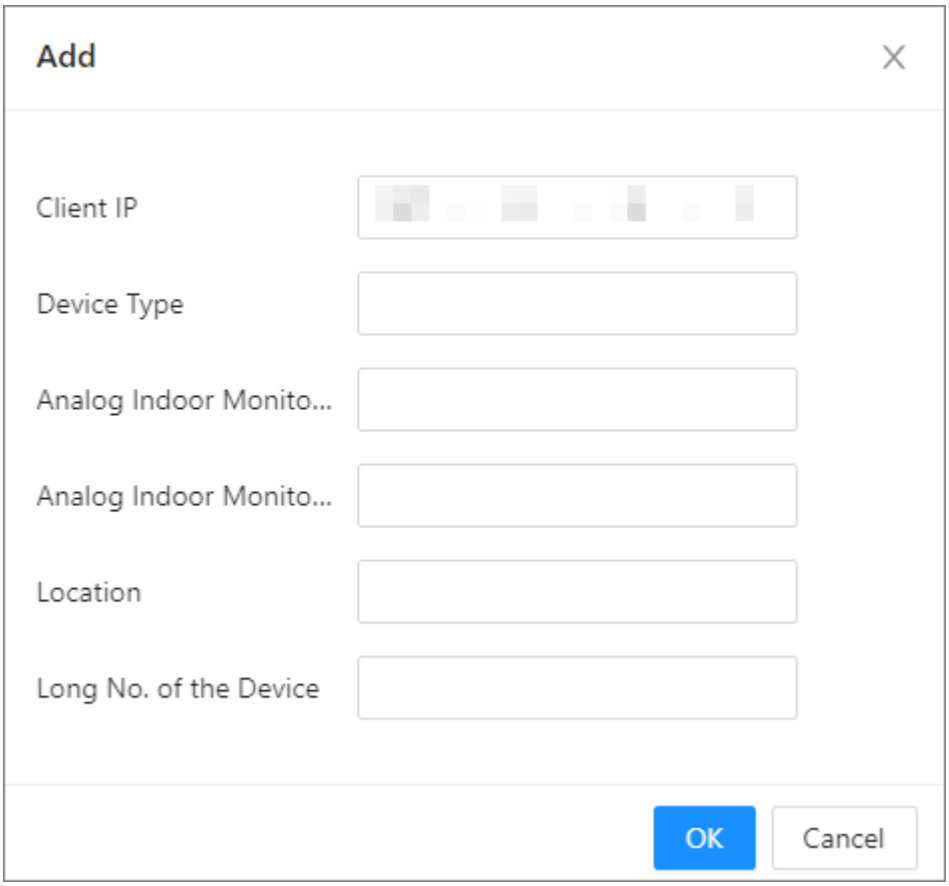


Table 3-25 Parameters description

Parameter	Description
Client IP	Enter the IP address of the device.
Device Type	Enter the type of the device.
Analog Indoor Monitor Start No.	Select the start number of the analogy indoor monitor.
Analog Indoor Monitor End No.	Select the end number of the analogy indoor monitor.
Location	Enter the room number where the device located.
Long No. of the Device	Enter the unique extended identification number of the device.

Step 4 Click **OK**.

Related Operations

- Click to edit the details.
- Click to delete.

3.11 System

Configure the parameters of video, audio and time.

3.11.1 Configuring Alarm

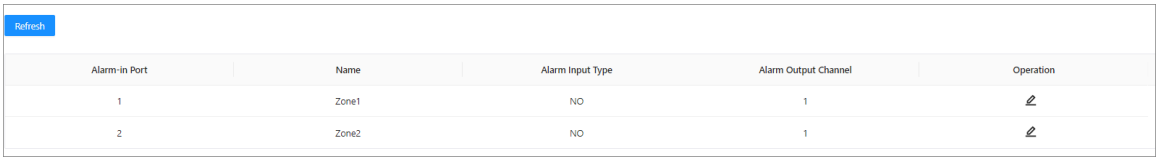
3.11.1.1 Configuring Alarm Linkage

Procedure

Step 1 Log in to the webpage.

Step 2 Select **System** > **Alarm** > **Alarm Linkage Setting**.

Figure 3-52 Alarm linkage



Step 3 Click to modify the parameters.

Figure 3-53 Modify the parameters

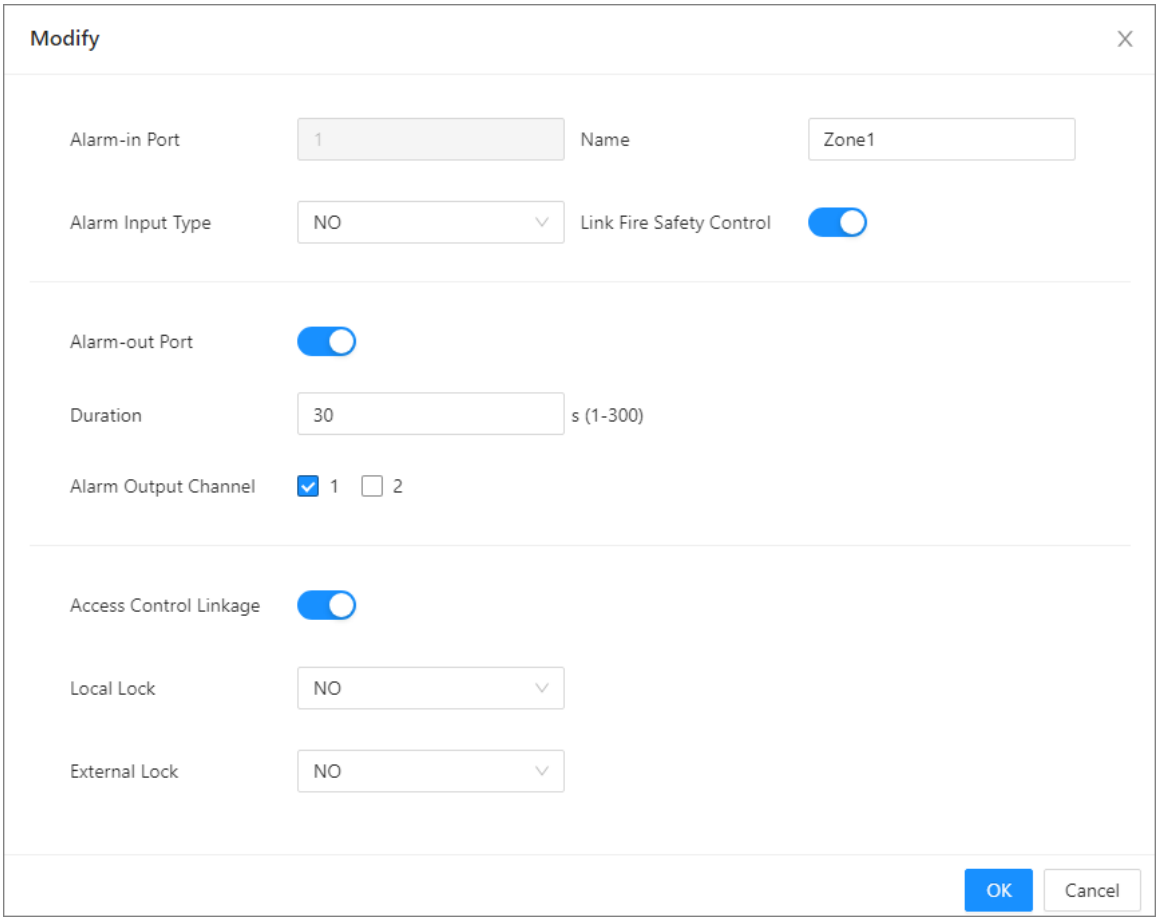


Table 3-26 Description of alarm linkage parameters

Parameter	Description
Alarm-in Port	The alarm-in port number cannot be modified.
Name	Customized.
Alarm Input Type	Select the type according to the device you purchased. • **NO** : The circuit of the alarm device is normally open, and closes when an alarm is triggered. • **NC** : The circuit of the alarm device is normally closed, and opens when an alarm is triggered.
Link Fire Safety Control	If enabled, when there is fire alarm, the device is linked to the alarm output and the access control. If enabled, the **Alarm-out Port** and **Access Control Linkage** are enabled by default.
Alarm-out Port	If alarm output is enabled, the relay can generate alarm messages. Configure the alarm duration, and then select the channel according to the actual channels.
Duration	
Alarm Output Channel	

Parameter	Description
Access Control Linkage	If you want to link access control when the fire alarm is triggered, enable this function. This function takes effect only after **Link Fire Safety Control** is enabled.
Local Lock	• NO: Normally open. The door automatically opens when fire alarm is triggered. • NC: Normally closed: The door automatically closes when fire alarm is triggered.
External Lock	

Step 4 Click **OK**.

3.11.1.2 Configuring Tamper Alarm

Procedure

Step 1 Log in to the webpage.

Step 2 Select **System** > **Alarm**.

Step 3 Configure tamper alarm.

Figure 3-54 Tamper alarm

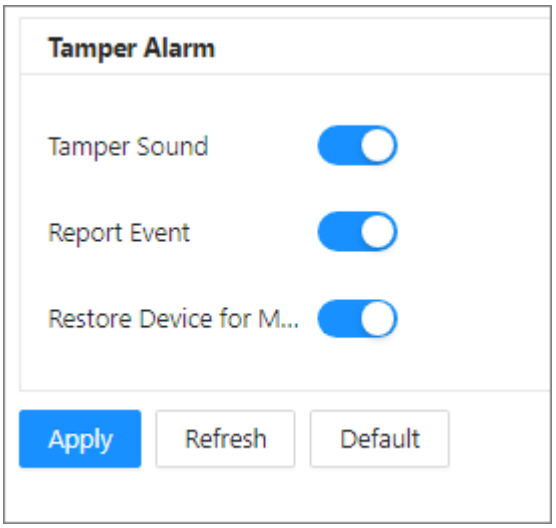


Table 3-27 Description of tamper alarm parameters

Parameter	Description
Tamper Sound	Configure whether the device whistles locally or not. It is enabled by default.
Report Event	Configure whether the device reports the tamper alarm to the app, indoor unit, and back-end of the platform or not. It is enabled by default.
Restore Device for Multiple Tamper Alarms	Within 10 minutes after the device is powered on, if you continuously press the tamper button for 5 times in 8 seconds, the device beeps and deletes the account information.

Step 4 Click **Apply**.

3.11.2 Configuring Video Parameters

Log in to the webpage of the VTO, select **System** > **Video**.

Bit Rate

Figure 3-55 Bit rate

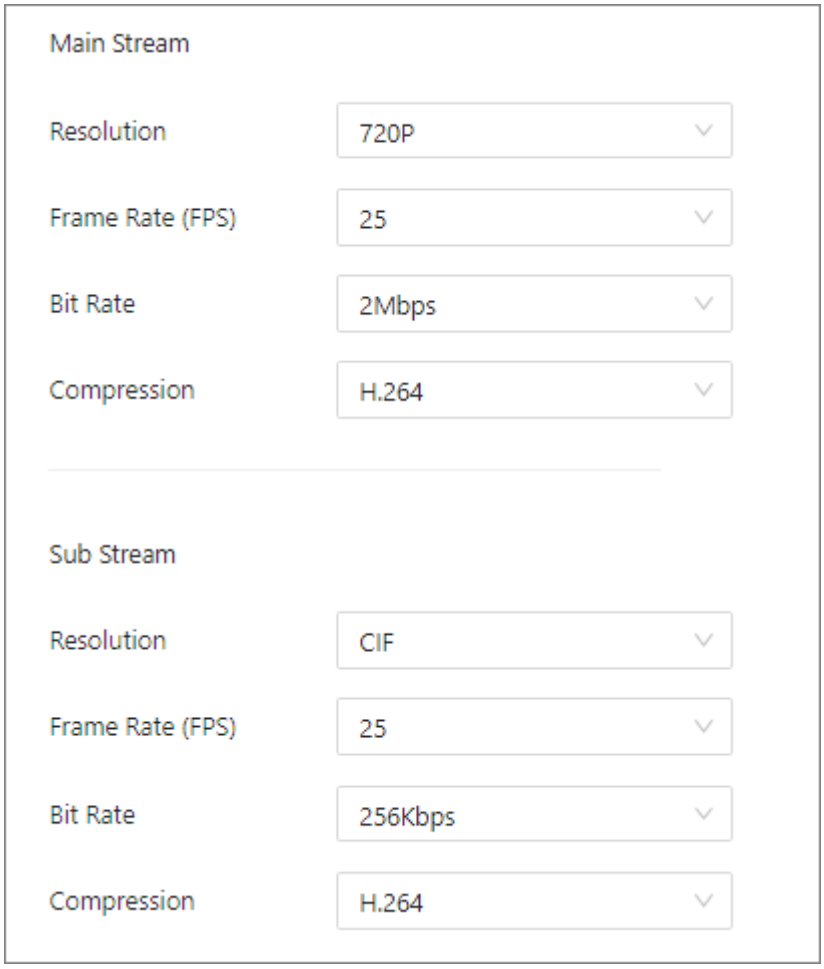


Table 3-28 Bit rate parameters description

Parameter		Description
Main Stream	Resolution	Adjust the resolution of the video. You can select from **720P** , **CIF**, **WVGA**, and **D1**.
	Frame Rate (FPS)	The number of frame in one second of video. If you select **PAL** as the video standard, you can set the frame rate up to 25. If you select **NTSC** as the video standard, you can set the frame rate up to 30.
	Bit Rate	Select according to the actual situation.

Parameter		Description
	Compression	Select from **H.264** and **H.265**. Compared with H.264, H.265 requires smaller bandwidth.
Sub Stream	Resolution	Adjust the resolution of the video. You can select from **WVGA** , **D1**, **QVGA**, **CIF**, **720P** and **1080P**.
	Frame Rate (FPS)	The number of frame in one second of video. If you select **PAL** as the video standard, you can set the frame rate up to 25. If you select **NTSC** as the video standard, you can set the frame rate up to 30.
	Bit Rate	Select according to the actual situation.
	Compression	Select from **H.264** and **H.265**.

Status

Figure 3-56 Status

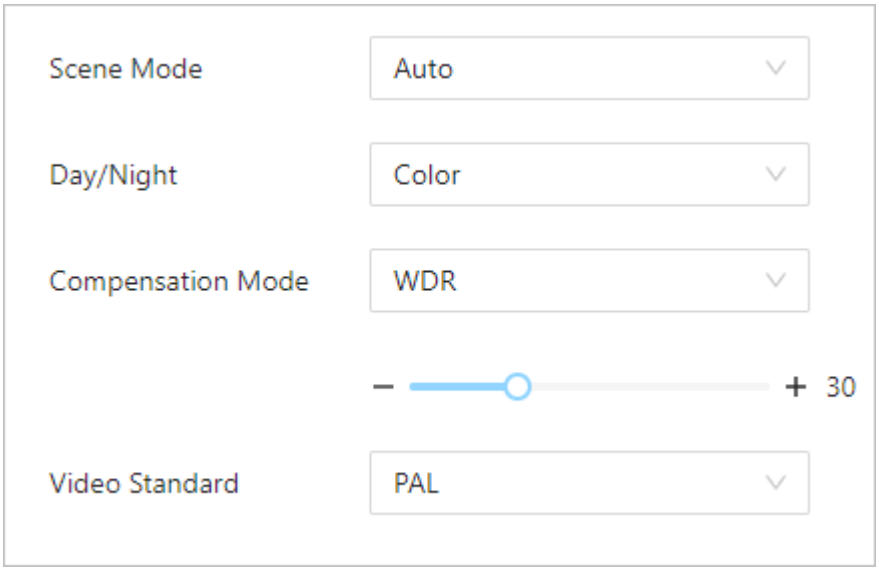


Table 3-29 Status parameters description

Parameter	Description
Scene Mode	Select from **Auto** , **Sunny**, **Night** and **Disable**
Day/Night	• **Auto** : The system switches between color and black-and-white according to actual conditions. • **Color** : The system displays the image in color. • **B/W** : The system displays black-white image.

Parameter	Description
Compensation Mode	• **Disable** : There will be no backlight. • **BLC** : The system gets a clearer image of the dark areas on the target when shooting against light. • **WDR** : The system dims bright areas and compensates for dark areas to ensure the clarity of all areas. • **HLC** : The system dims strong lights, and reduce the size of Halo zone to lower the brightness of the whole image.
Video Standard	Select from **PAL** and **NTSC**.

Exposure

Figure 3-57 Exposure

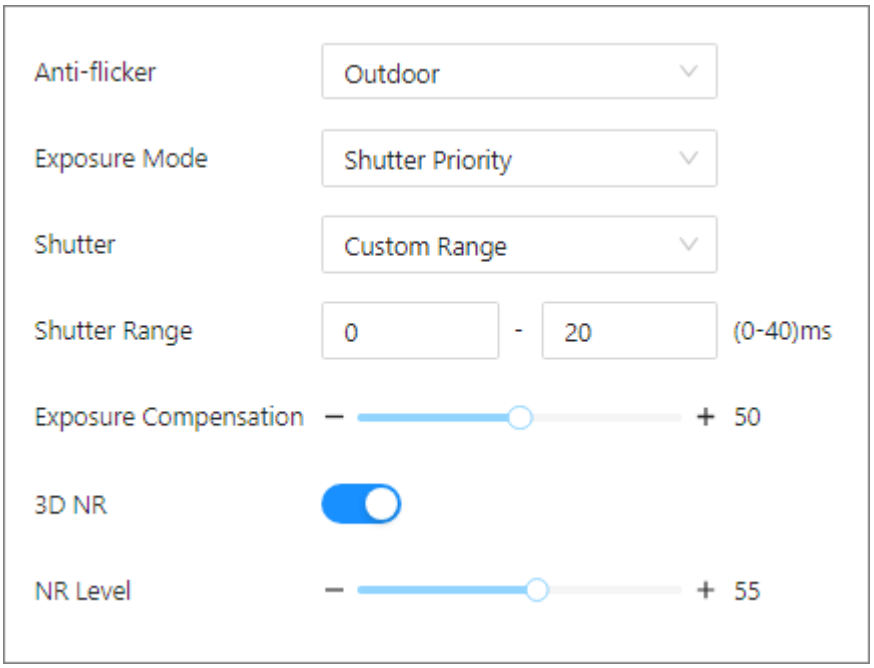


Table 3-30 Exposure parameters description

Parameter	Description
Anti-flicker	• **50Hz** : The system adjusts the exposure according to ambient light automatically to ensure that stripes do not appear. • **60Hz** : The system adjusts the exposure according to ambient light automatically to ensure that stripes do not appear. • **Outdoor** : If you select **Outdoor**, the exposure mode can be set to **Gain Priority**, **Shutter Priority** and **Iris Priority**. Different devices support different exposure modes.
Exposure Mode	• **Auto** : Exposure is automatically adjusted according to scene brightness if the overall brightness of images is in the normal exposure range. • **Manual** : You can adjust the **Gain** and **Shutter** value manually. • **Shutter Priority** : The camera automatically adjusts the aperture size based on the selected shutter speed to ensure proper exposure.

Parameter	Description
Shutter	Set the effective exposure time. The smaller the value, the shorter the exposure time.
Shutter Range	If you select **Manual** as the exposure mode, and select **Custom Range** as the shutter, you can set the shutter range in ms unit.
Exposure Compensation	You can set the exposure compensation value. The value ranges from 0 to 100. The higher the value is, the brighter the image will be.
3D NR	Reduce the noise of multiple-frame (at least two frames) images by using inter-frame information between two adjacent frames in a video. The higher the level is, the lower the noise will be, and the larger the trailing smear will be.
NR Level	Noise reduction grade. The value ranges from 0 to 100. The larger the value is, the less the noise will be.

Image

Figure 3-58 Image

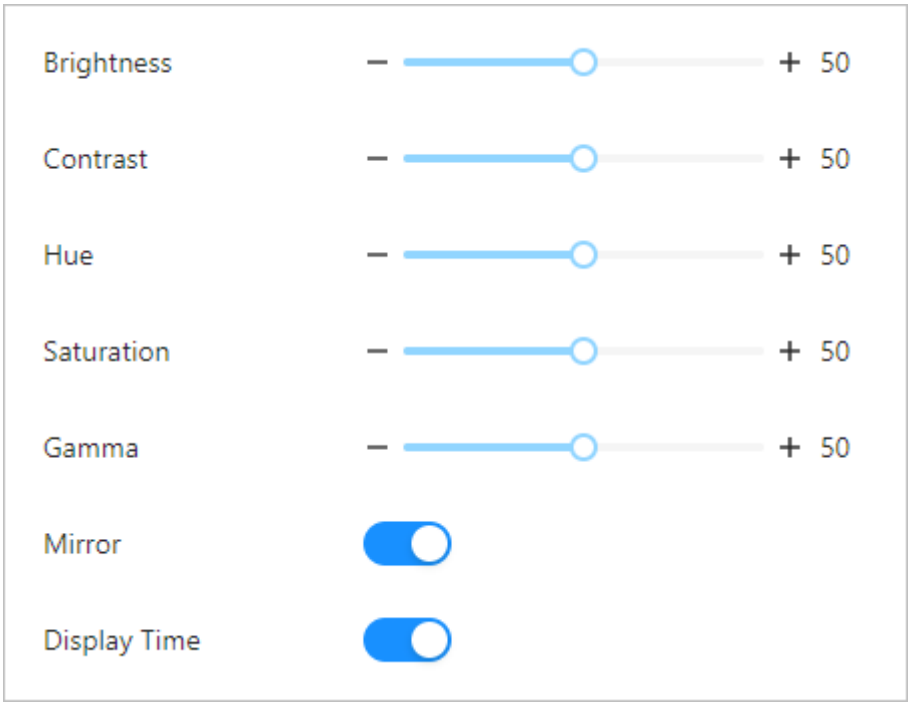


Table 3-31 Image parameters description

Parameter	Description
Brightness	Change the overall brightness of the image. The higher the value, the brighter the image.
Contrast	Change the contrast of the image. The higher the value, the greater the contrast between bright and dark areas. If the value is too big, the dark area will be too dark and the bright area will be more vulnerable to overexposure.
Hue	Makes the color deeper or lighter. The default value is made by the light sensor, and it is recommended.

Parameter	Description
Saturation	Set the intensity of colors. The higher the value, the deeper the color. Saturation value does not change image brightness.
Gamma	Change the image brightness and contrast in a non-linear way. The higher the value, the brighter the image.
Mirror	If enabled, the image flips left and right.
Display Time	If enabled, the current time displays on the video image.

3.11.3 Configuring Audio Parameters

Procedure

Step 1 Log in to the webpage.

Step 2 Select **System** > **Audio**.

Step 3 Configure the audio parameters.

Figure 3-59 Audio parameters

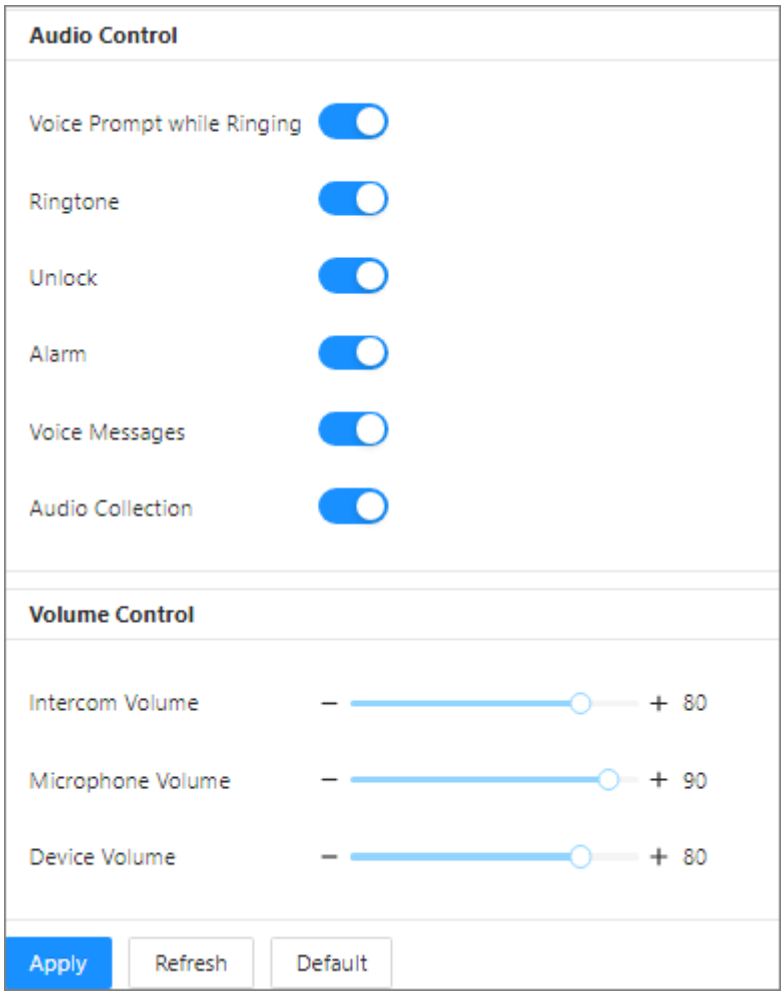


Table 3-32 Audio parameters description

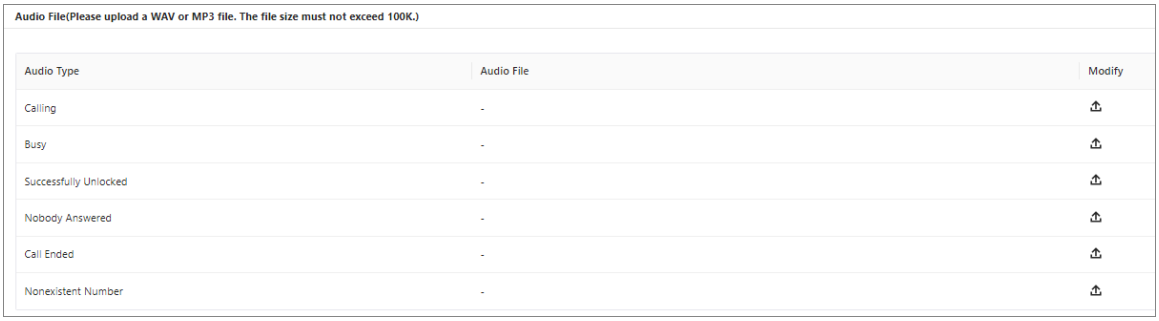
Parameter		Description
Audio Control	Voice Prompt while Ringing	If enabled, there is prompt sound when you call.
	Ringtone	If enabled, there is a ringback when you call.
	Unlock	If enabled, there is prompt sound.
	Alarm	If enabled, there is alarm sound.
	Voice Messages	If enabled, when no one answers the call from the visitor, the system plays prompt sound for messages.
	Audio Collection	If enabled, the audio will be saved.
Volume Control	Intercom Volume	Adjust the intercom volume. The higher the value is, the higher the volume will be.
	Microphone Volume	Adjust the microphone volume of the VTO. The higher the value is, the higher the volume will be.
	Device Volume	Adjust the device volume. The higher the value is, the higher the volume will be.

Related Operations

Upload the audio file.

Click , select the audio file, and then click **Open**. Upload the audio for the corresponding type.

Figure 3-60 Upload the file



3.11.4 Configuring Time

Procedure

Step 1 Log in to the webpage.

Step 2 Select **System** > **Time**.

Step 3 Configure the time parameters.

Figure 3-61 Time parameters

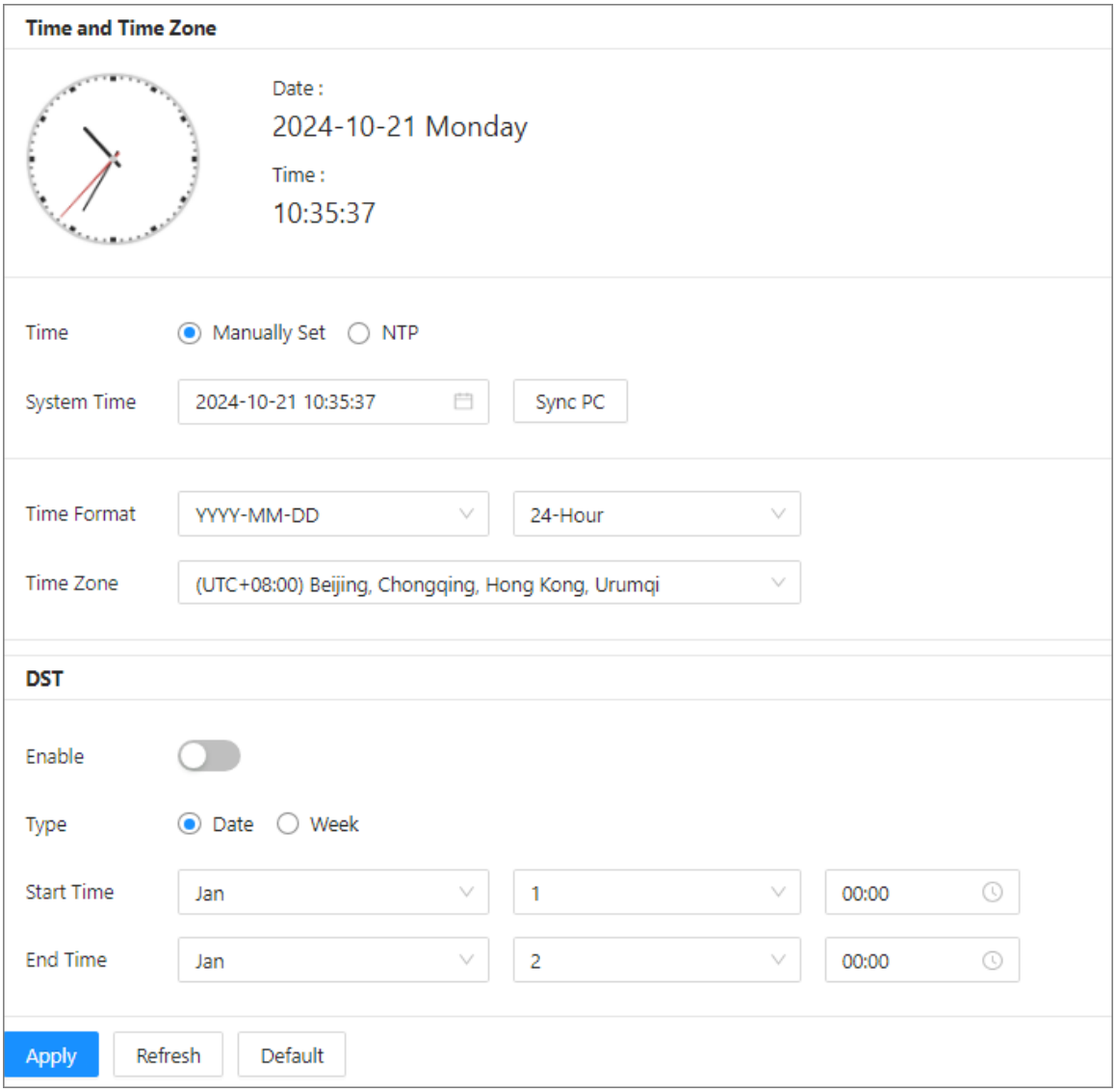


Table 3-33 Time parameters description

Parameter	Description
Time	• **Manually Set** : Configure the time manually or synchronize with your computer. • **NTP** : Configure the NTP server parameters, and the time will be synchronized.
Server	Configure the address, port number of the NTP server. The port number is 123 by default. Configure the interval that the VTO synchronize the time with the NTP server. The parameters are displayed when you select **NTP**.
Port	
Interval	
System Time	Manually configure the system time. You can also click **Sync PC** to synchronize the time of the VTO with the local computer.

Parameter	Description
Time Format	Configure the time format and the zone.
Time Zone	
DST Enable	If enabled, the system will synchronize its time with the NTP server you configure.
Type	Select from **Date** and **Week**.
Start Time	Configure the start time and end time for DST.
End Time	

Step 4 Click **Apply**.

3.11.5 Configuring Shortcut

Procedure

Step 1 Log in to the webpage.

Step 2 Select **System** > **Shortcut Settings**.

Step 3 Configure the shortcut.

Figure 3-62 Shortcut parameters

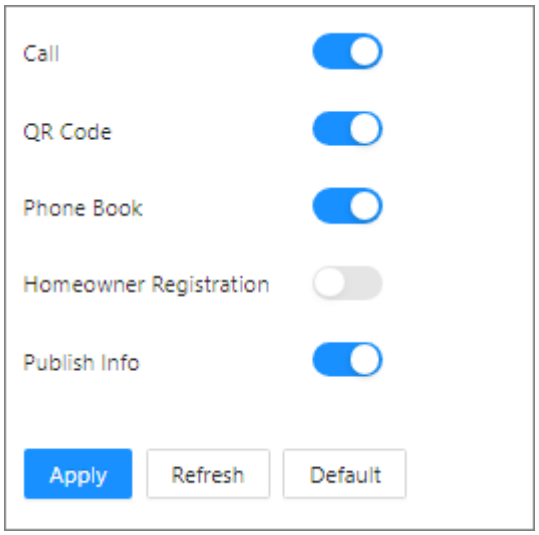


Table 3-34 Shortcut parameters description

Parameter	Description
Call	Select up to 4 items to be shown on the home screen. If the device type is fence station, there are 4 shortcut provided. The **Phone Book** is not available.
QR Code	
Phone Book	
Homeowner Registration	
Publish Info	

Step 4 Click **Apply**.

3.11.6 Adding ONVIF Users

ONVIF users are used for ONVIF protocol. The ONVIF user information will be verified before the door opens.

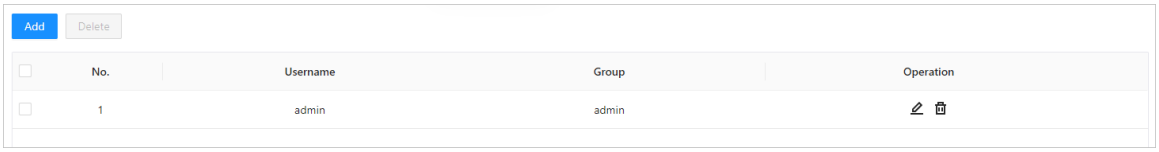
Only Profile C and Profile S are supported, while the encoding format and image parameters are not supported.

Procedure

Step 1 Log in to the webpage.

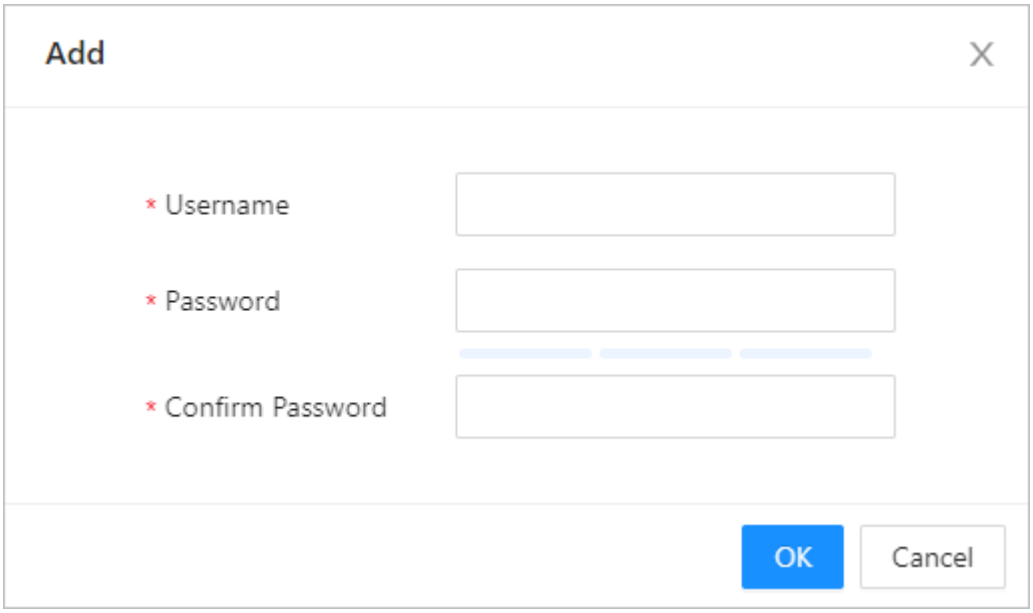
Step 2 Select **System** > **ONVIF User**.

Figure 3-63 ONVIF user



Step 3 Click **Add**, and then enter the username, password and confirm password.

Figure 3-64 Add the user



Step 4 Click **OK**.

3.12 Personalization

Configure themes and add video or image resources to the Device.

3.12.1 Configuring Advertisements

This function is only available on select models.

Procedure

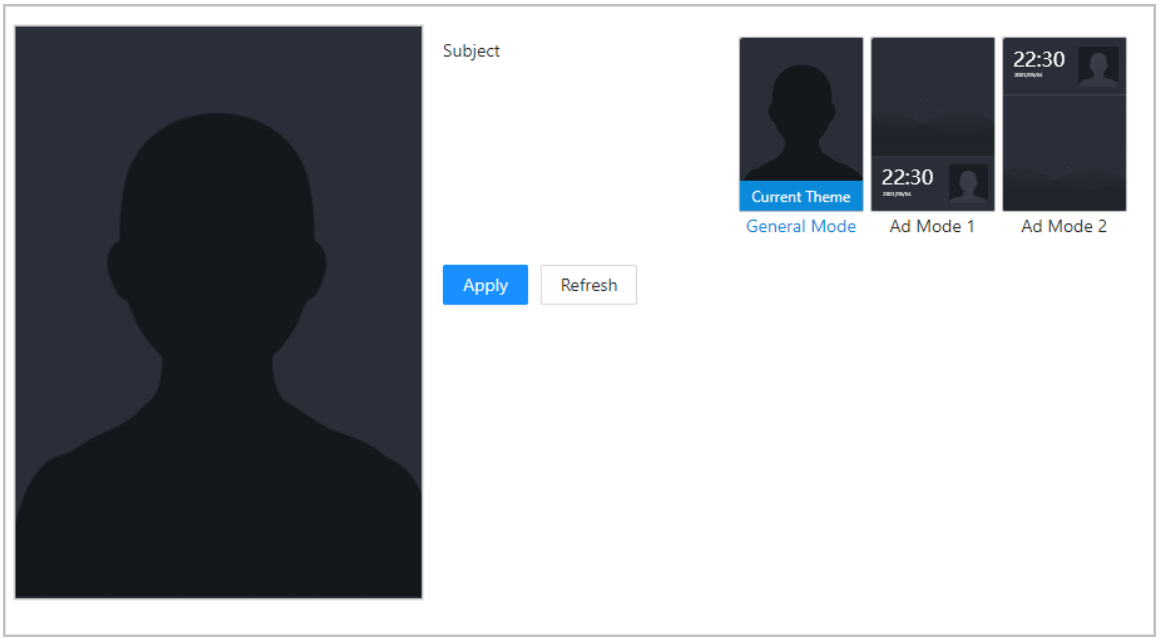
Step 1 Log in to the webpage.

Step 2 Select **Personalization** > **Personalization**.

Step 3 Select the theme.

- General Theme: Displays the face image in full screen.
- Ad Mode 1: The upper area displays the advertisements, and the lower area displays the time and the face detection box.
- Ad Mode 2: The upper area displays the time and the face detection box, and the lower area displays the advertisements.

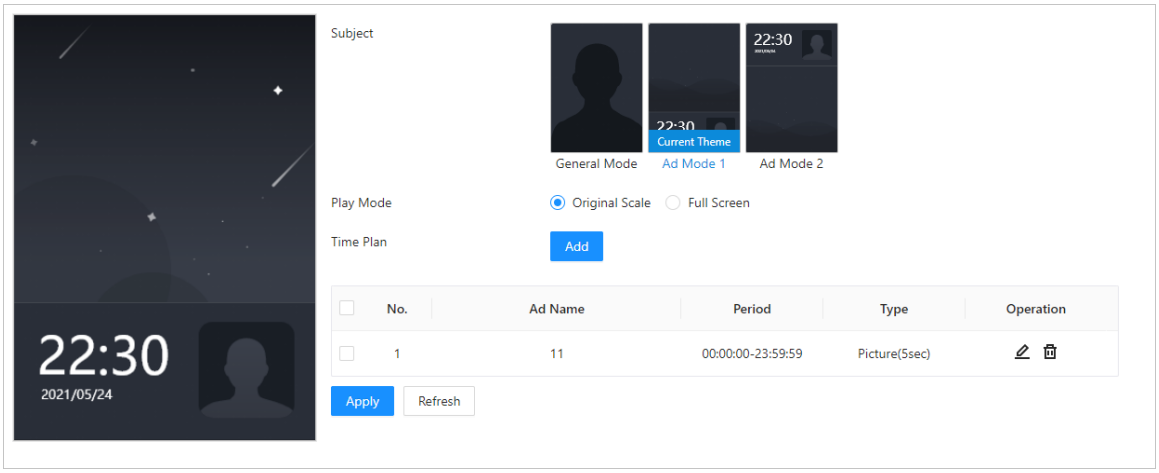
Figure 3-65 Theme



Step 4 Set play mode.

1. Select Ad mode 1 or Ad mode 2.

Figure 3-66 Play mode



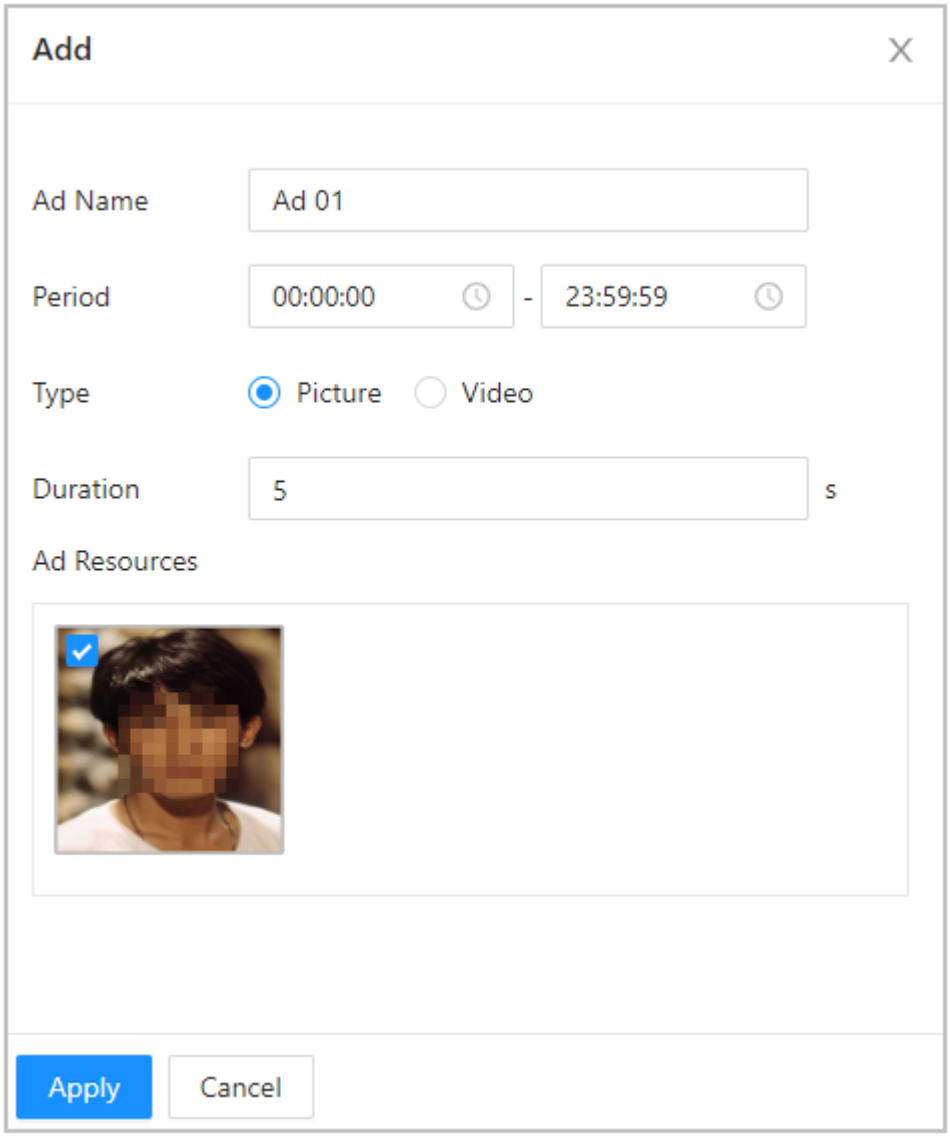
2. Select the play mode.
   - Original Scale: Plays the image and video in the original size.
   - Full Screen: Plays the image and video in full screen.

3. Click **Add** to add time plans.

   You can add up to 10 plans.
4. Enter the name of the advertisement.
5. Select the time section, file type and file.
6. Enter the duration, and then click **Apply**.

   Set the duration for a single picture when pictures are played in a loop. The duration ranges from 1 s to 20 s and it is 5 s by default.

Figure 3-67 Add time schedules



The videos and images are added in **Ad Resources**.

Step 5 Click **Apply**.

3.12.2 Adding Resources

Add images or videos to be displayed on the standby screen of the Device.

This function is only available on select models.

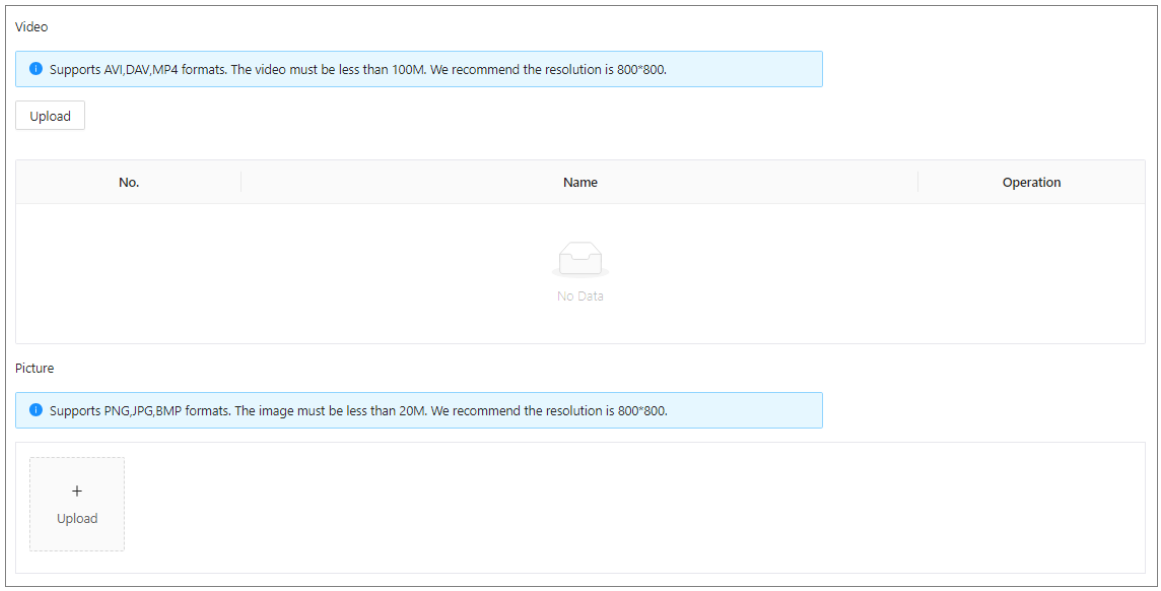
Procedure

Step 1 Log in to the webpage.

Step 2 Select **Personalization** > **Ad Resources**.

Step 3 Add videos or images.

Figure 3-68 Add videos or images



- Add videos.
  1. Click **Upload**.
  2. Click **Browse** , select the video file, and then click **Next**.

     The video is automatically uploaded to the platform after transcoding.

     - You can upload up to 5 video files.
     - Supports DAV, AVI, MP4. Video size must be less than 100 M.
     - Only supports latest version of FireFox and Chrome to upload video files.
- Add images.
  1. Click +.
  2. Select image from the local, and then upload it.

     Supports PNG, JPG, BMP. Image size must be less than 20 M.

Related Operations

Hover the mouse on the video or image, and then click to delete uploaded image or video.

Videos and images in use cannot be deleted.

3.12.3 Configuring Notifications

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Personalization** > **Publish Info**.

Step 3 Click **Release Notifications**, and then configure the parameters.

Figure 3-69 Configure the notification

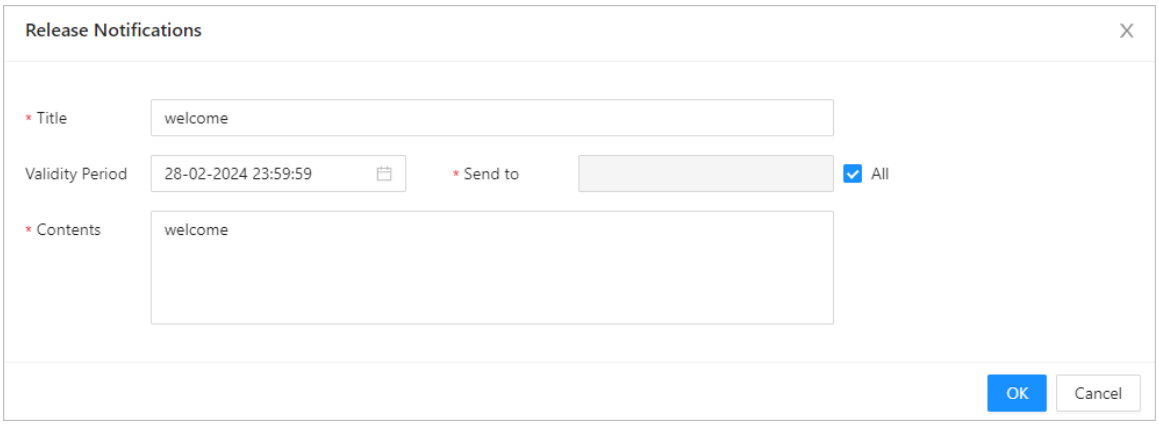


Table 3-35 Description of announcement parameters

Parameter	Description
Title	The title of the announcement.
Validity Period	Configure the validity period. You need to send the announcement within the validity period to enable the VTH receive the announcement. The history records will display all the announcements that sent by the VTO.
Send to	Configure the receiver of the announcement. • Enter the room number of the receiver to solely send the announcement. • Select **All** checkbox to send the announcement to all devices.
Contents	The content of the announcement. You can enter up to 256 characters.

Step 4 Click **OK**.

3.13 Maintenance Center

3.13.1 One-Click Diagnosis

The system automatically diagnoses the configurations and the status of the device to improve its performance.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **One-click Diagnosis**.

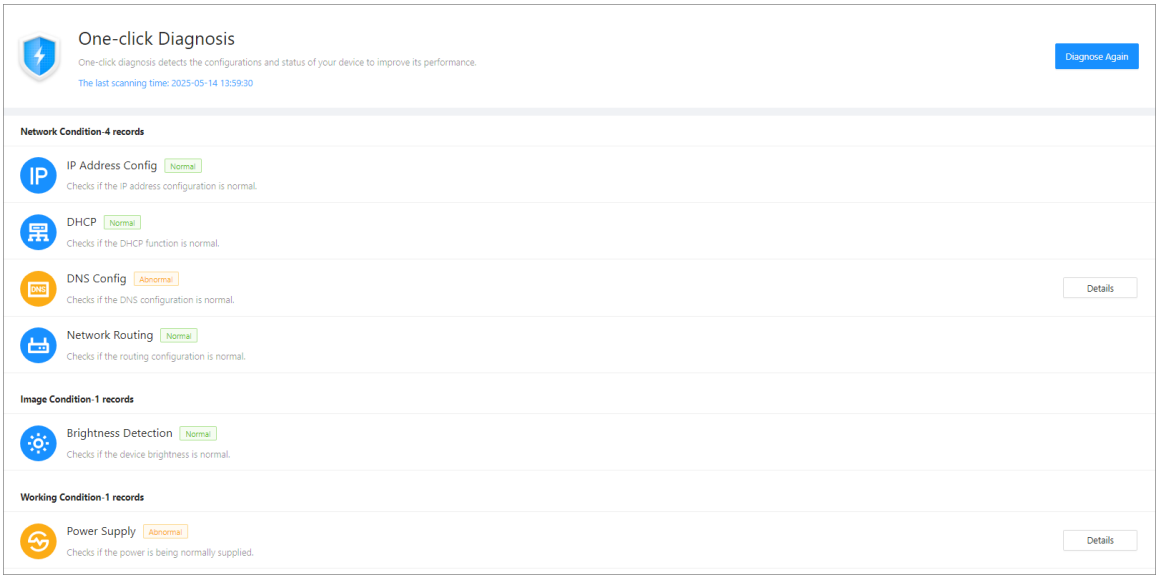
Step 3 Click **Diagnose**.

The system automatically diagnoses the configurations and the status of the device and display diagnosis results after it completes.

Step 4 (Optional) Click **Details** to view details of abnormal items.

You can ignore the abnormality or optimize it. You can also click **Diagnose Again** to perform automatic diagnosis again.

Figure 3-70 One-click diagnosis

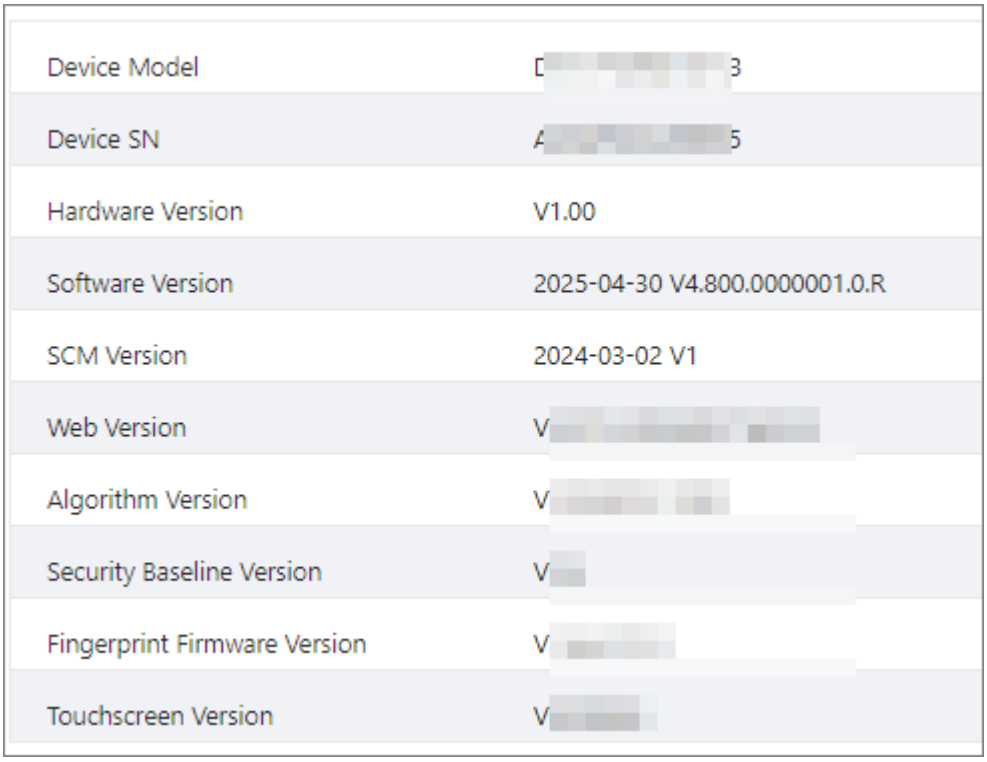


3.13.2 System Information

3.13.2.1 Viewing Version Information

On the webpage, select **Maintenance Center** > **System Info** > **Version**, and you can view version information of the Device.

Figure 3-71 Version information



3.13.2.2 Viewing Legal Information

On the home page, select **Maintenance Center** > **System Info** > **Legal Info**, and then you can view the software license agreement, privacy policy and open source software notice.

3.13.3 Data Capacity

You can see how many users, cards and face images that the VTO can store.

Log in to the webpage and select **Maintenance Center** > **Data Capacity**.

3.13.4 Viewing Logs

View logs such as system logs, alarm logs, call logs, and unlock records.

3.13.4.1 Call History

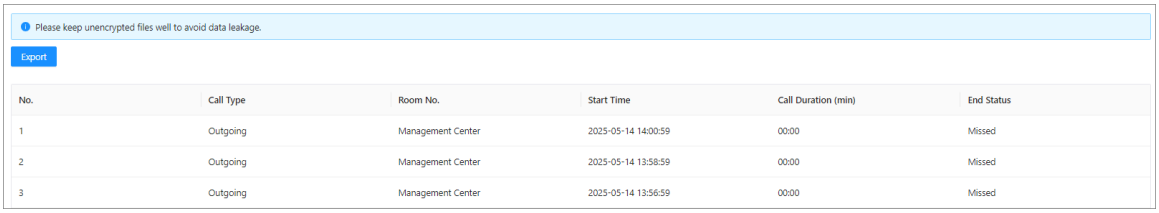
View call logs.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Log** > **Call History**.

Figure 3-72 Call history



Related Operations

Click **Export** to export the call history.

3.13.4.2 Alarm Logs

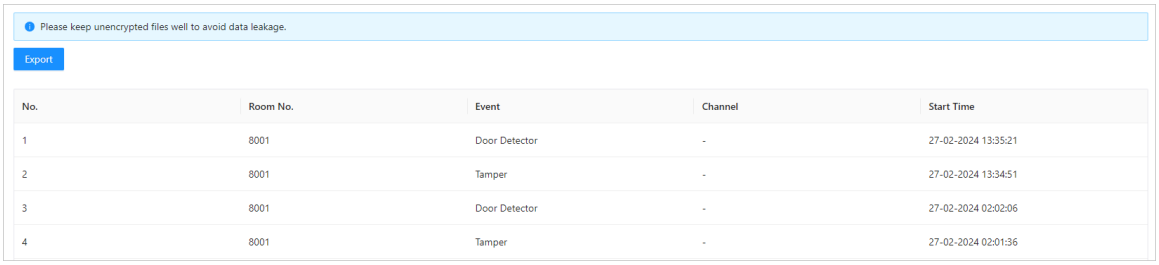
View alarm logs.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Log** > **Alarm Logs**.

Figure 3-73 Alarm logs



3.13.4.3 Unlock Records

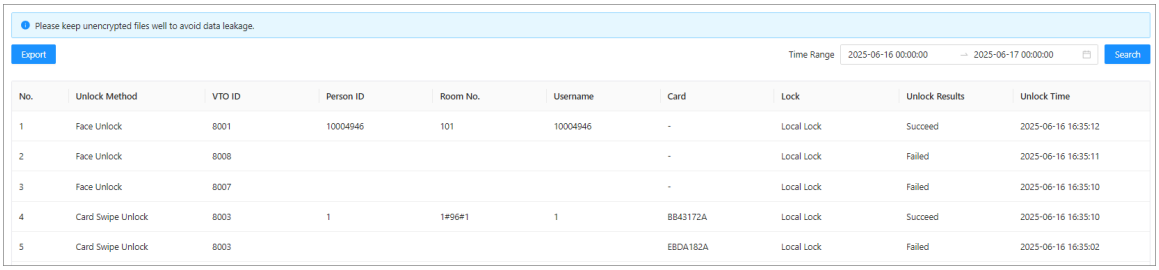
View unlock records and export them.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Log** > **Unlock Records**.

Figure 3-74 Unlock records



Related Operations

Click **Export** to download the log.

3.13.4.4 System Logs

View and search for system logs.

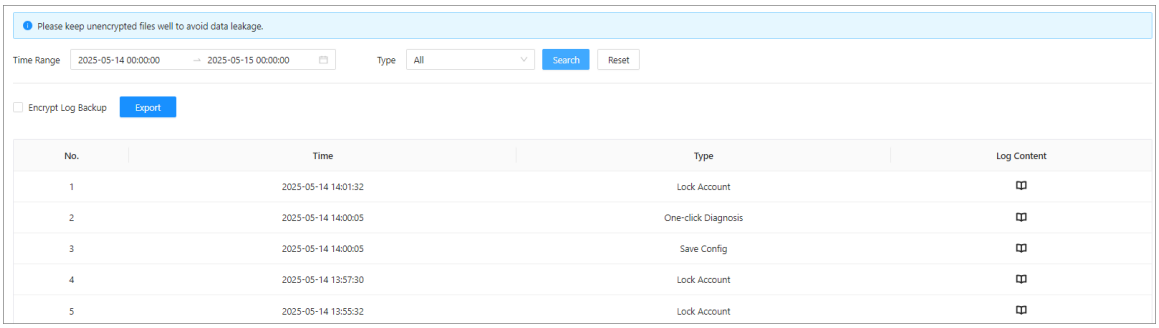
Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Log** > **Log**.

Step 3 Select the time range and the log type, and then click **Search**.

Figure 3-75



Related Operations

- Click **Export** to export the searched logs to your local computer.
- Click **Encrypt Log Backup**, and then enter a password. The exported file can be opened only after entering the password.
- Click to view details of a log.

3.13.5 Maintenance Management

When more than one Device need the same configurations, you can configure parameters for them by importing or exporting configuration files.

3.13.5.1 Exporting and Importing Configuration Files

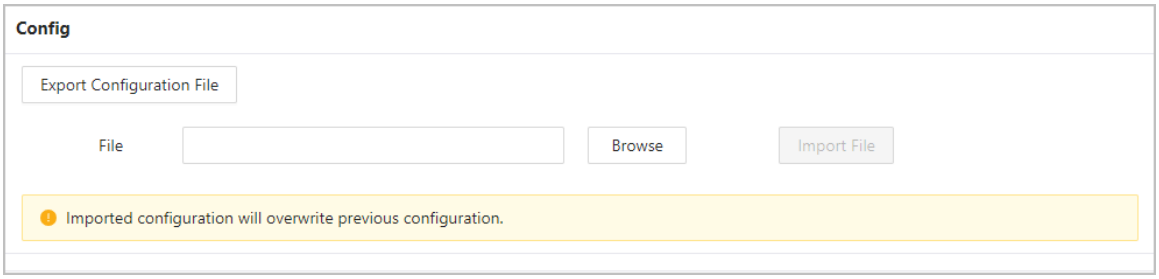
You can import and export the configuration file for the Device. When you want to apply the same configurations to multiple devices, you can import the configuration file to them.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Maintenance Management** > **Config**.

Figure 3-76 Configuration management



Step 3 Export or import configuration files.

- Export the configuration file.

Click **Export Configuration File** to download the file to the local computer.

- Import the configuration file.
  1. Click **Browse** to select the configuration file.
  2. Click **Import configuration**.

  Configuration files can only be imported to devices that have the same model.

3.13.5.2 Maintenance

Regularly restart the VTO during its idle time to improve its performance.

Procedure

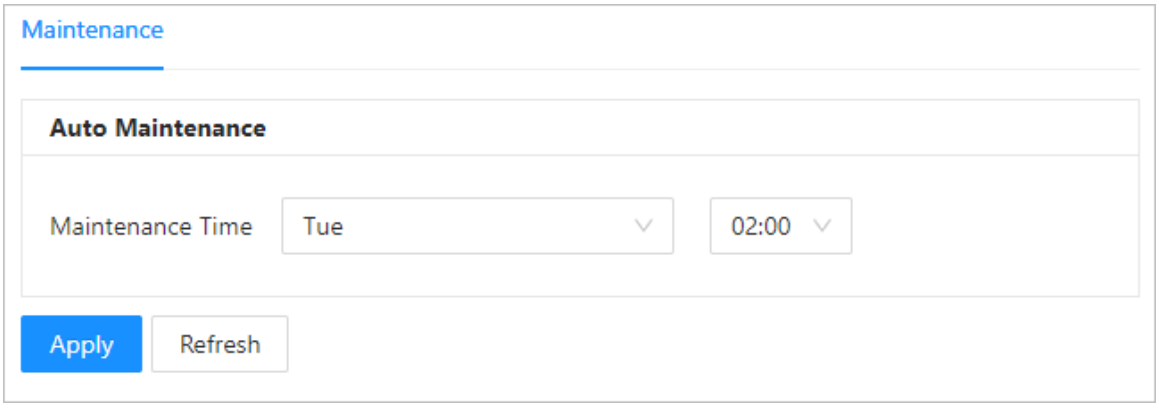
Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Maintenance Management** > **Maintenance**.

Step 3 Set the time, and then click **Apply**.

The Device will restart at the scheduled time, or you can click **Restart** to restart it immediately.

Figure 3-77 Maintenance time



3.13.6 Updating the System

- Use the correct update file. Make sure that you get the correct update file from technical support.
- Do not disconnect the power supply or network, and do not restart or shutdown the Device during the update.

File Update

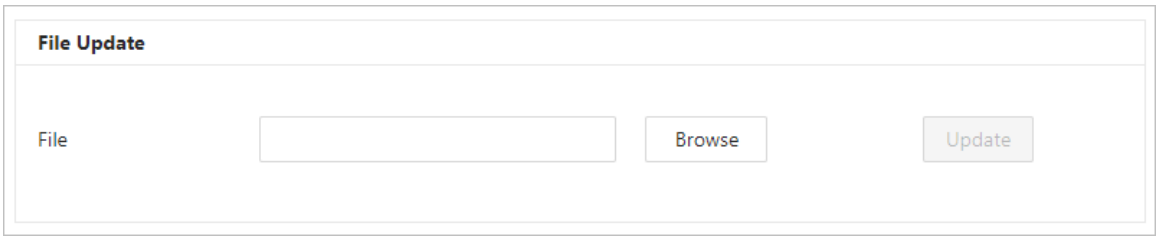
1. Log in to the webpage.
2. Select **Maintenance Center** > **Update**.
3. In the **File Update** area, click **Browse**, and then upload the update file.

   The update file should be a .bin file.

4. Click **Update**.

   The VTO will restart after the update finishes.

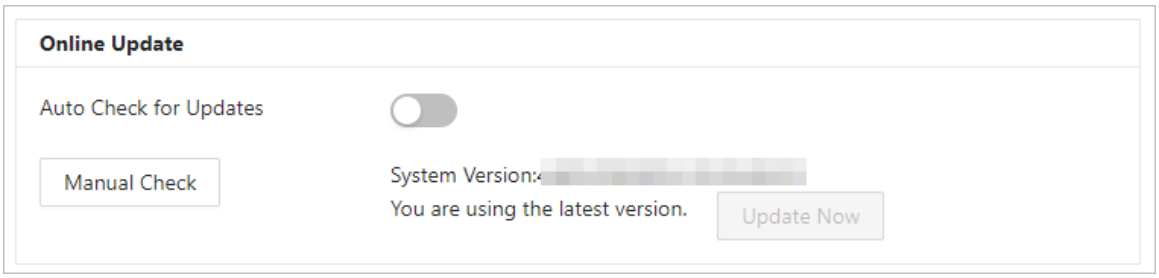
Figure 3-78 File update



Online Update

1. Log in to the webpage.
2. Select **Maintenance Center** > **Update**.
3. In the **Online Update** area, select an update method.
   - Enable **Auto Check for Updates**, and the VTO will automatically check for the latest version update.
   - Click **Manual Check**, and you can immediately check whether the latest version is available.
4. (Optional) Click **Update Now** to update the VTO immediately.

Figure 3-79 Online update



3.13.7 Advanced Maintenance

Acquire device information and capture packet to make easier for maintenance personnel to perform troubleshooting.

3.13.7.1 Exporting

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Advanced Maintenance** > **Export**.

Step 3 Click **Export** to export the serial number, firmware version, device operation logs and configuration information.

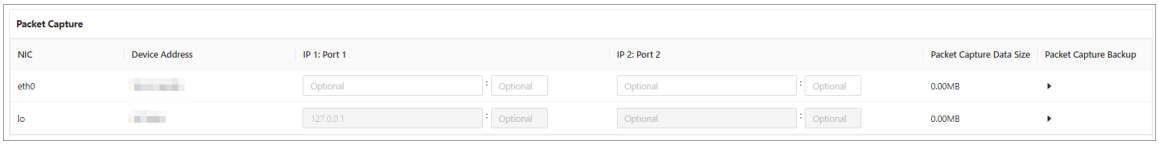
3.13.7.2 Packet Capture

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.

Figure 3-80 Packet Capture



Step 3 Enter the IP address, click ▶.

▶ changes to ⏸.

Step 4 After you acquired enough data, click ⏸.

Captured packets are automatically downloaded to your local computer.

3.13.7.3 Network Test

Procedure

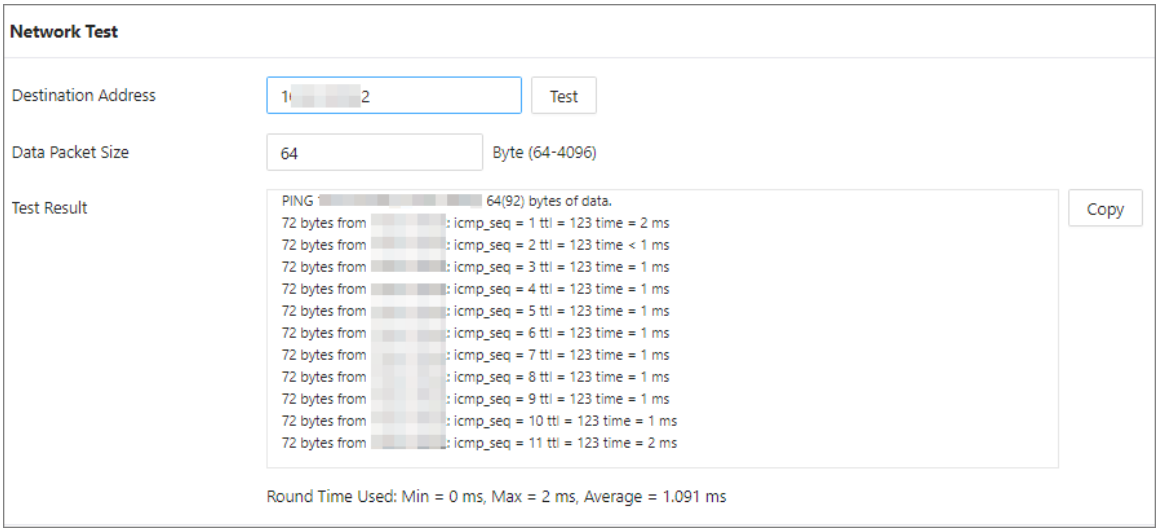
Step 1 Log in to the webpage.

Step 2 Select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.

Step 3 In the **Network Test** area, test the network as needed.

1. Enter the destination address in the box, and then click **Test**.
2. After you acquired enough data, click **Stop**, and then you can view the test result in the following box.
3. (Optional) Click **Copy** to copy the test result.

Figure 3-81 Test network



Appendix 1 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.
2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.
3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.
4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.
5. **Set and update password reset information in a timely manner**

   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

   It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.
2. **Update client software in time**

   It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).