Unit VTO

User Manual

V1.0.0

Foreword

This manual introduces the structure and configuration of the 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	Revision Content	Release Time
V1.0.0	First release.	November 2025

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 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.
  - 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 Functions 1
1.3 Structures 2
1.3.1 Front Panel 2
1.3.2 Rear Panel 8
2 Initialization 18
2.1 Initialization through the Device 18
2.2 Initialization on the Webpage 18
3 VTO Operations 20
3.1 Home Screen 20
3.2 Homeowner Registration 22
3.3 Unlock 22
3.3.1 Unlocking by the Password 23
3.3.2 Unlocking by the Card 23
3.3.3 Unlocking by Identifying the Face 23
3.3.4 Unlocking by Scanning the QR Code 23
3.3.5 Unlocking by the Bluetooth 23
3.3.6 Unlocking by the Fingerprints 24
3.3.7 Unlocking through the VTH 24
3.3.8 Unlocking through the VTS 24
3.4 Call 24
3.4.1 Calling the VTH 24
3.4.2 Calling the VTS 25
3.5 Engineering Setting 26
3.5.1 Person Management 28
3.5.2 Communication 30
3.5.3 General Settings 33
3.5.4 Personalization 35
3.5.5 Device Information 36
4 Webpage Operations 38
4.1 Logging in to the Webpage 38
4.2 Resetting the Password 38
4.3 Home Page Introduction 39
4.4 Setup Wizard 40

4.4.1 Setting as SIP Server 40
4.4.2 Not Setting as SIP Server 41
4.5 Admin Center 42
4.5.1 Changing the Password 42
4.5.2 Logout 43
4.5.3 Restarting the Device 43
4.5.4 Restoring Default Factory Settings 44
4.6 Security Center 44
4.6.1 Security Status 44
4.6.2 Configuring HTTPS 45
4.6.3 Attack Defense 46
4.6.4 Installing Device Certificate 49
4.6.5 Installing the Trusted CA Certificate 52
4.6.6 Video Encryption 52
4.6.7 Security Warning 53
4.6.8 Security Authentication 54
4.7 Local Device Configuration 54
4.7.1 Basic Settings 54
4.7.2 Personalization 62
4.7.3 Configuring Access Control 74
4.7.4 Configuring Light Control 79
4.7.5 Adding the IPC 80
4.7.6 Configuring Cards 81
4.7.7 Configuring Wiegand 82
4.7.8 Configuring Face Detection 84
4.7.9 Configuring QR Code 86
4.7.10 Configuring Fingerprint 87
4.8 Device Setting 87
4.8.1 Adding the VTO 87
4.8.2 Adding the VTH 89
4.8.3 Adding the VTS 90
4.8.4 Related Operations 91
4.9 Person Management 92
4.10 Network Settings 96
4.10.1 Configuring TCP/IP 96
4.10.2 Configuring Port 98
4.10.3 Configuring the SIP Server 99
4.10.4 Configuring Cloud Service 104
4.10.5 Configuring UPnP 105
4.10.6 Configuring Wi-Fi 105

4.10.7 Configuring the Bluetooth 106
4.10.8 Configuring Basic Services 106
4.10.9 Configuring Auto Registration 108
4.10.10 Configuring Registration Management 109
4.11 System 110
4.11.1 Configuring Alarm 110
4.11.2 Configuring Video Parameters 112
4.11.3 Configuring Audio Parameters 117
4.11.4 Configuring Time 118
4.11.5 Adding ONVIF Users 120
4.12 Maintenance Center 120
4.12.1 One-Click Diagnosis 121
4.12.2 System Information 121
4.12.3 Data Capacity 122
4.12.4 Viewing Logs 123
4.12.5 Maintenance Management 124
4.12.6 Updating the System 125
4.12.7 Advanced Maintenance 126
Appendix 1 Security Recommendation 128

1 Product Overview

1.1 Introduction

The door station (hereinafter referred to as "VTO") uses capacitive touch screen and is equipped with dual-lens network camera. The VTO integrates deep learning algorithm to enable the user to unlock the door through the recognition function, such as face recognition and card opening.

1.2 Functions

Video and Voice Call

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

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: Recognized by the built-in fingerprint module. This function is available on select models.
- Unlock by the Bluetooth. This function is available on select models.
- Unlock by entering the password.
- 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 10 streams for monitoring.

Auto Snapshot

Takes snapshots while you are on a call or unlocking the door, and stores them to the SD card. This function is disabled by default.

Alarm Management

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

This function is only available on the villa door station.

Alarm Linkage Setting

The VTO can adopt buzzer to ring the calls.

IR Smart Illumination

Automatically detects the actual scenery and opens the illumination (white is normally adapted and red is used for assisting 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 Structures

The following front and rear panel figures are for reference only.

1.3.1 Front Panel

1.3.1.1 75 Series

Figure 1-1 Front panel

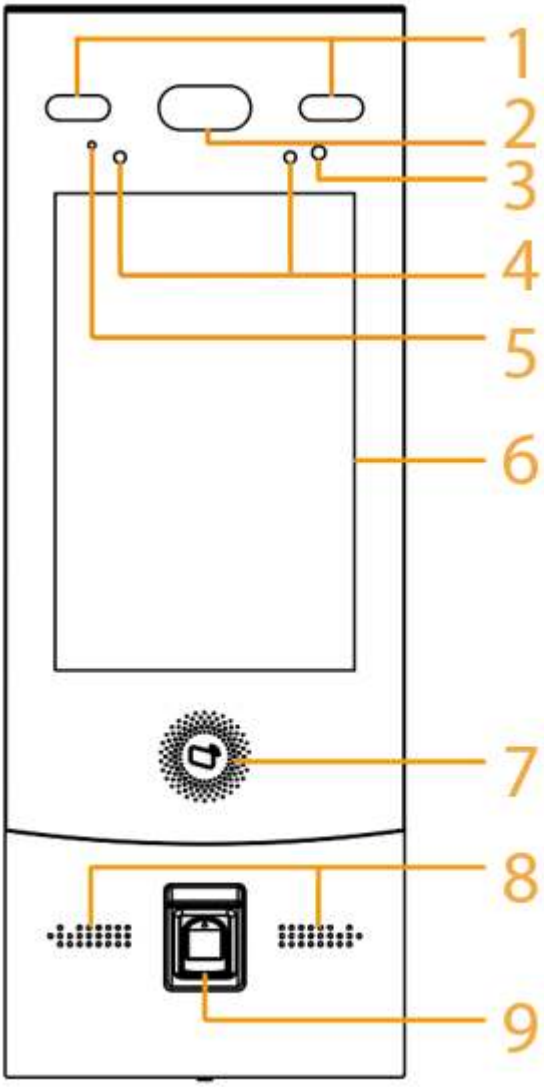


Table 1-1 Component description

No.	Description	No.	Description
1	White illuminator	6	Display
2	Camera	7	Card swiping area
3	Photosensitive sensor	8	Loudspeaker
4	IR illuminator	9	Fingerprint sensor Fingerprint sensor is only available for the mode of VTO7541G.
5	MIC	—	—

1.3.1.2 95 Series

Figure 1-2 Front panel

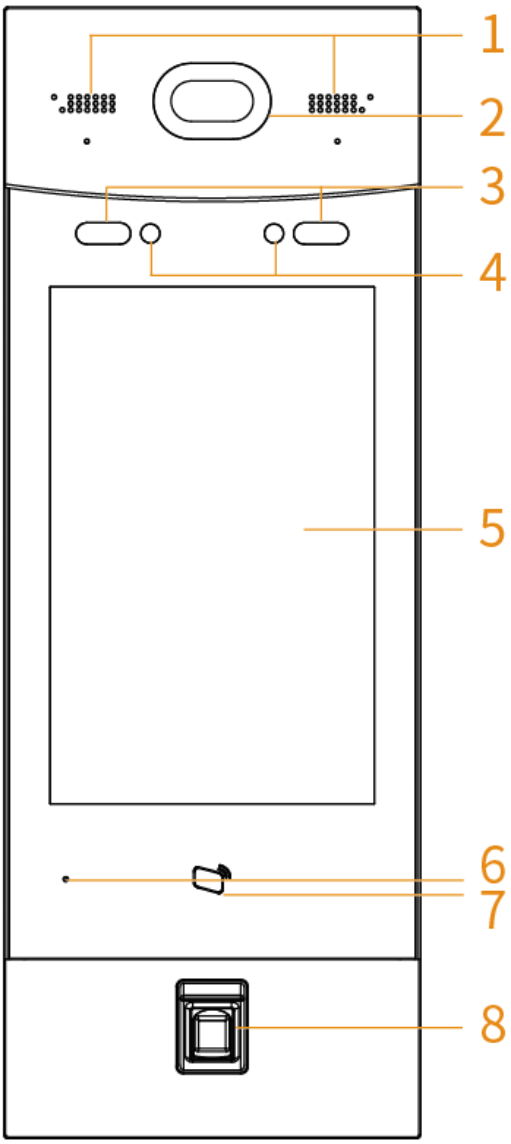


Table 1-2 Component description

No.	Description	No.	Description
1	Loudspeaker	5	Display
2	Camera	6	MIC
3	White illuminator	7	Card swiping area
4	IR illuminator	8	Fingerprint sensor

1.3.1.3 76 Series

Figure 1-3 Front panel

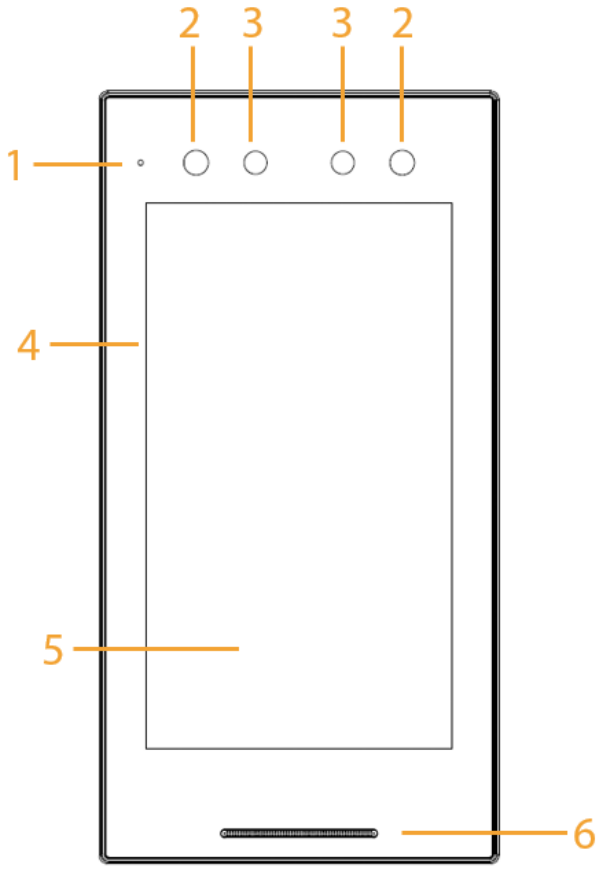


Table 1-3 Component description

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

1.3.1.4 96 Series

Figure 1-4 Front panel

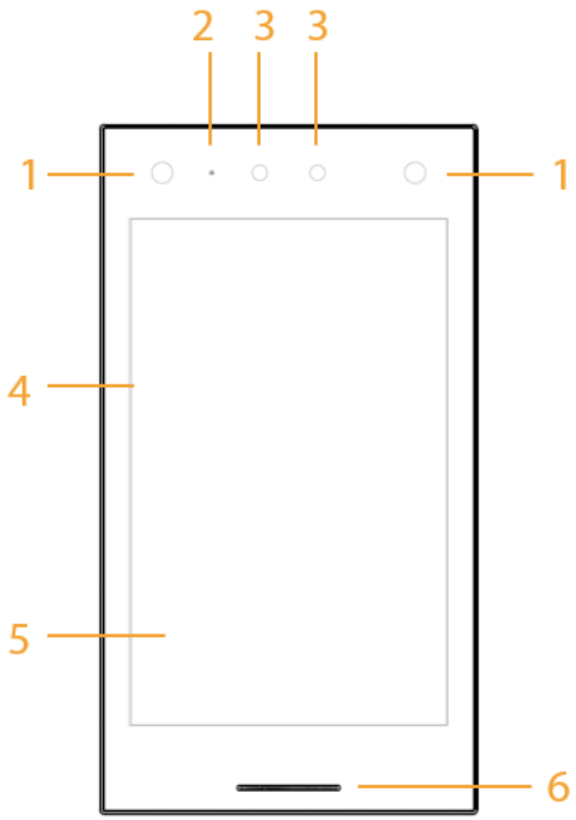


Table 1-4 Component description

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

1.3.1.5 66 Series

Figure 1-5 Front panel

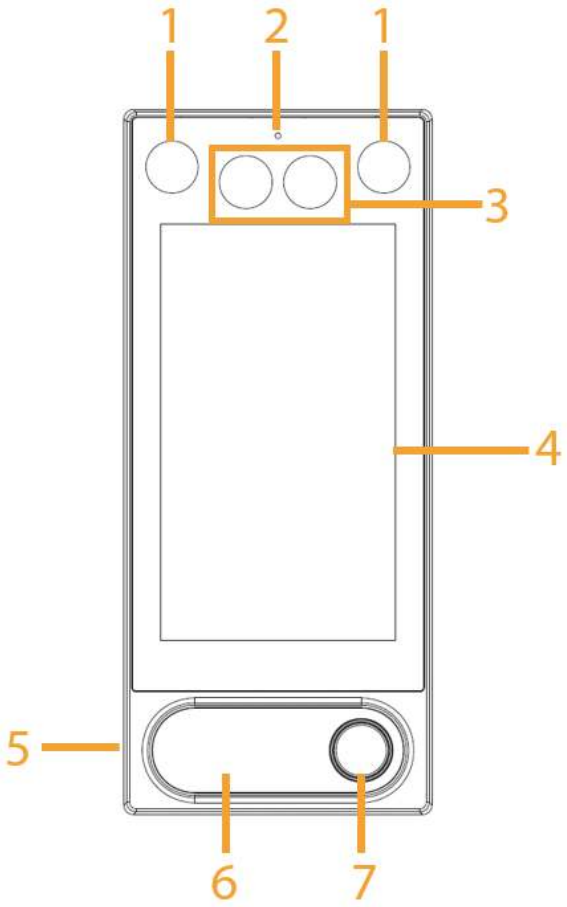


Table 1-5 Component description

No.	Description	No.	Description
1	IR illuminator	5	Loudspeaker
2	MIC	6	Card swiping area
3	Camera	7	Button Supports calling and calling by period mode.
4	Display	–	–

There is also an indicator on the outer circle of the button:

- Device starts and then performs the default status: Flashing blue and then solid blue.
- Successful verification: Quickly flashing green once.
- Failed verification: Quickly flashing red three times.
- During the intercom period: Slowly flashing blue.
- The intercom period ends: Solid blue.
- Anti-tamper function triggers: Quickly flashing red.

- When 2 locks are opened simultaneously but only one lock is successful: Flashing green once.
- SIP is broken or the network is abnormal: Slowly flashing red.

The priority of the indicator: Authentication > Anti-tampering > SIP disconnection or network anomaly > Intercom.

1.3.2 Rear Panel

1.3.2.1 75 Series

Figure 1-6 Rear panel

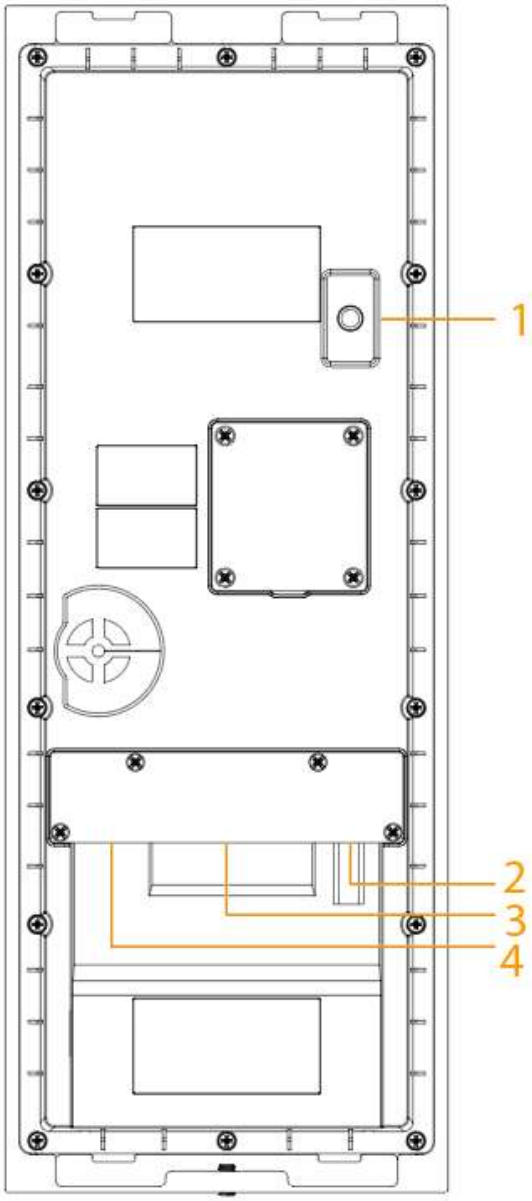
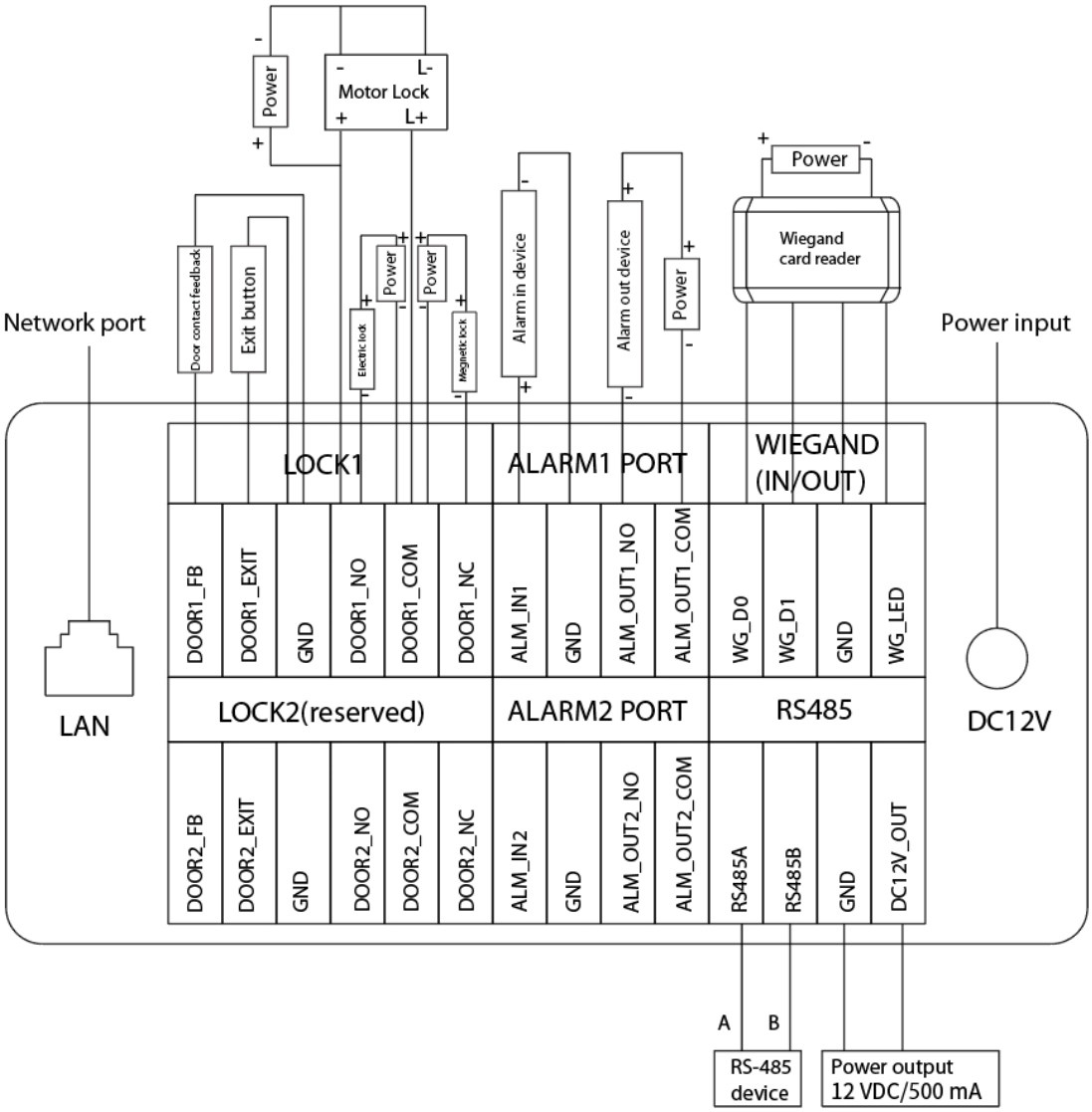


Table 1-6 Component description

No.	Description
1	Tamper button ● Triggers alarms for illegal dismantling or damage in emergency situations. ● 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 admin account information.
2	Power port
3	Function ports (such as alarm in/out port, lock port, and wiegand port)
4	Ethernet port

Figure 1-7 Cable connection



1.3.2.2 95 Series

Figure 1-8 Rear panel

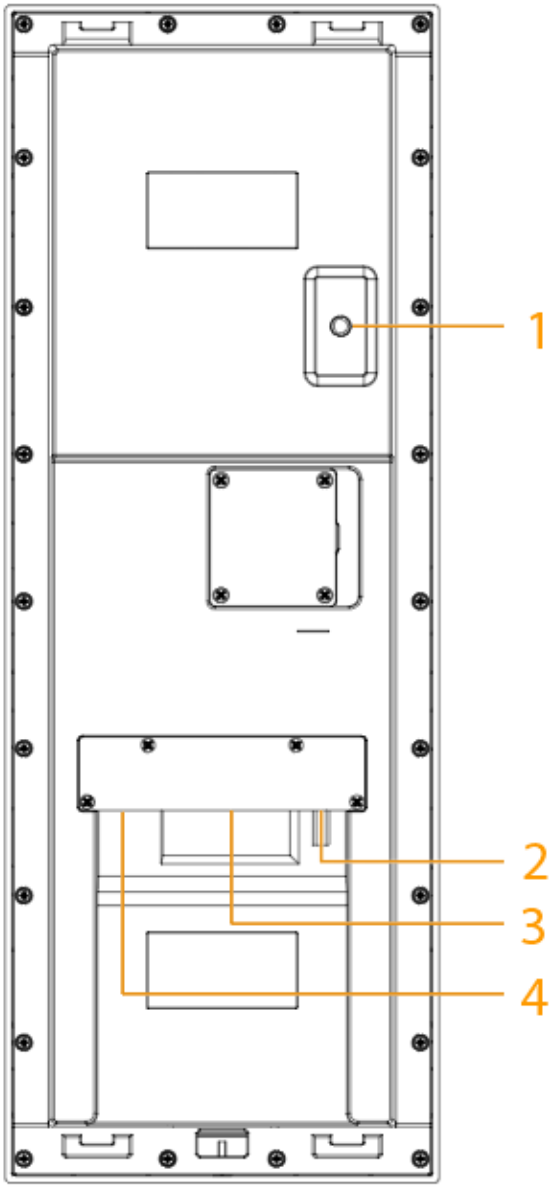
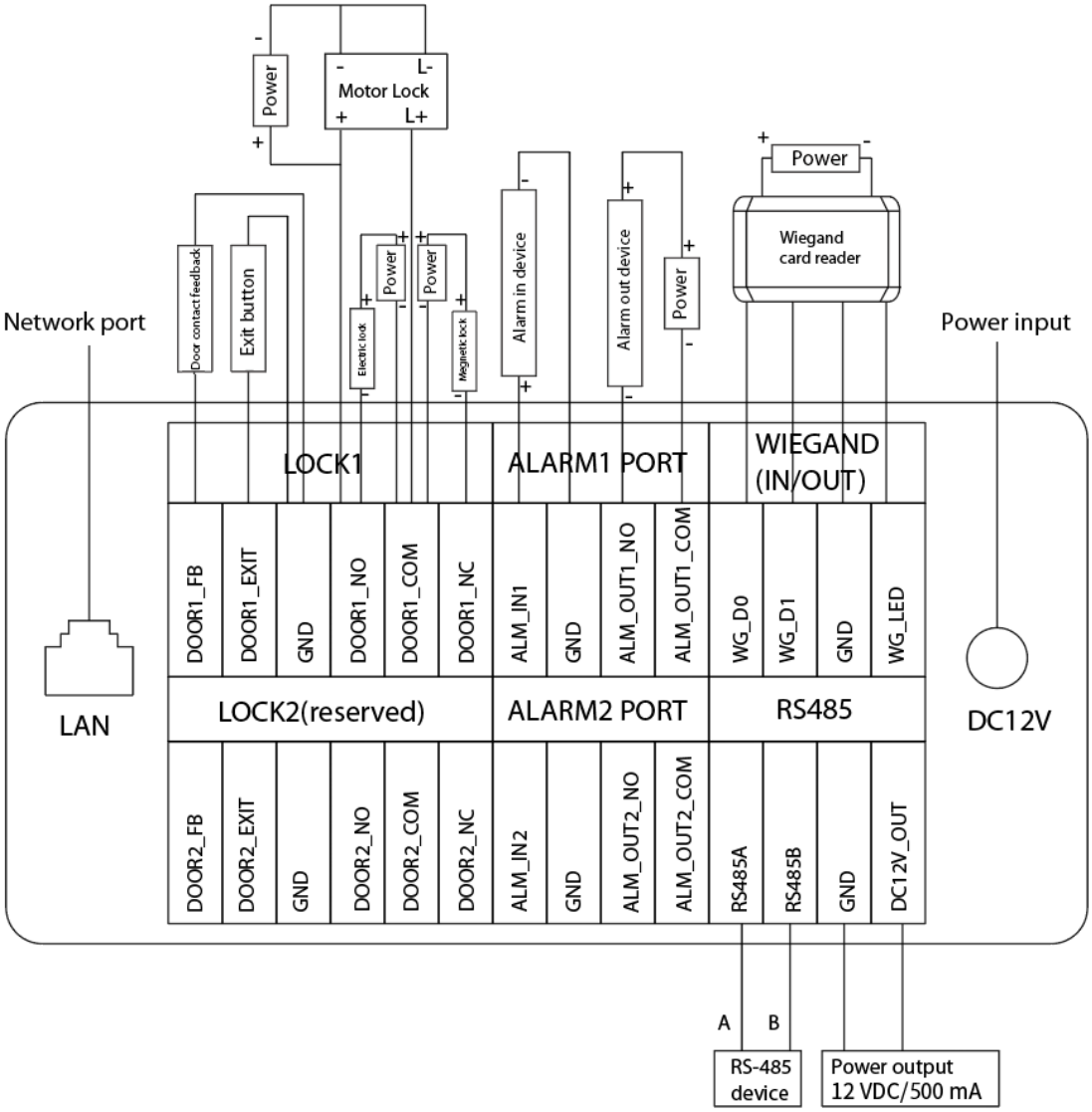


Table 1-7 Component description

No.	Description
1	Tamper button ● Triggers alarms for illegal dismantling or damage in emergency situations. ● 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 admin account information.
2	Power port

No.	Description
3	Function ports
4	Ethernet port

Figure 1-9 Cable connection



1.3.2.3 76 Series

Figure 1-10 Rear panel

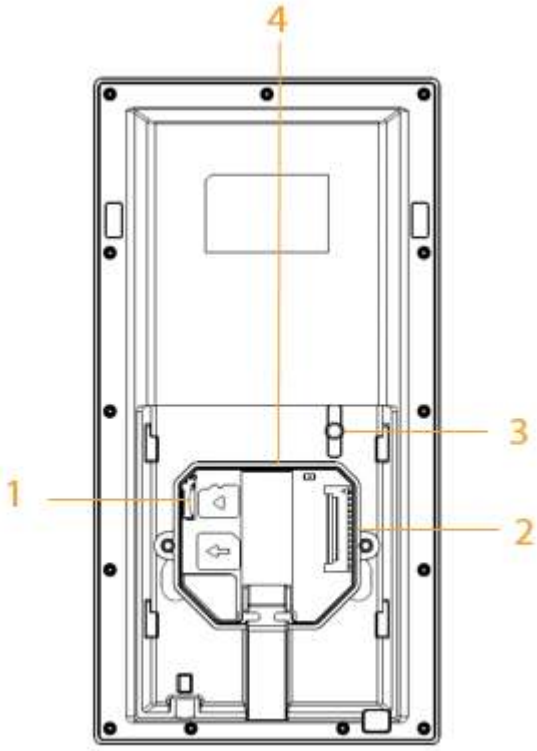
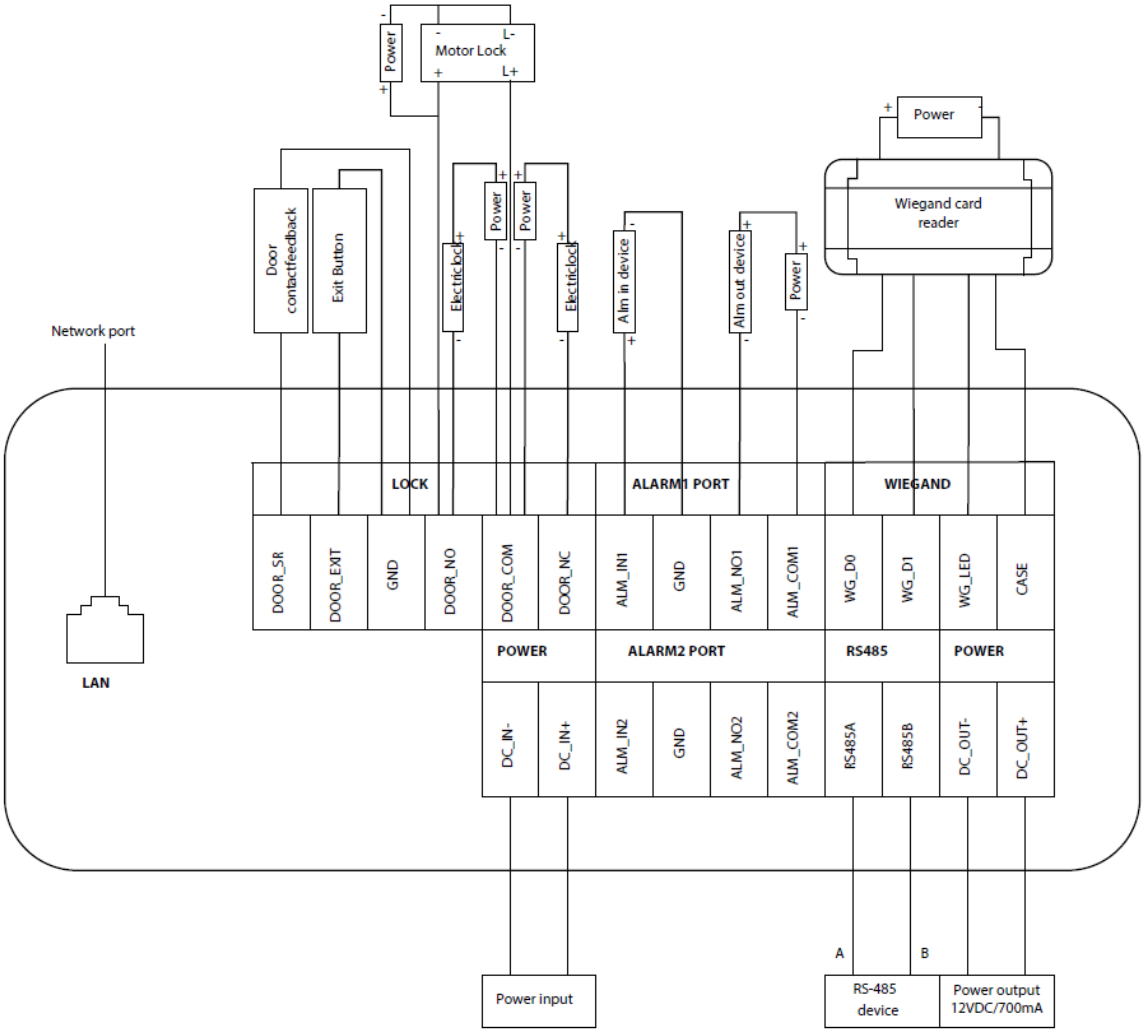


Table 1-8 Component description

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 ● Triggers alarms for illegal dismantling or damage in emergency situations. ● 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 admin account information.
4	Ethernet port

Figure 1-11 Cable connection



1.3.2.4 96 Series

Figure 1-12 Rear panel

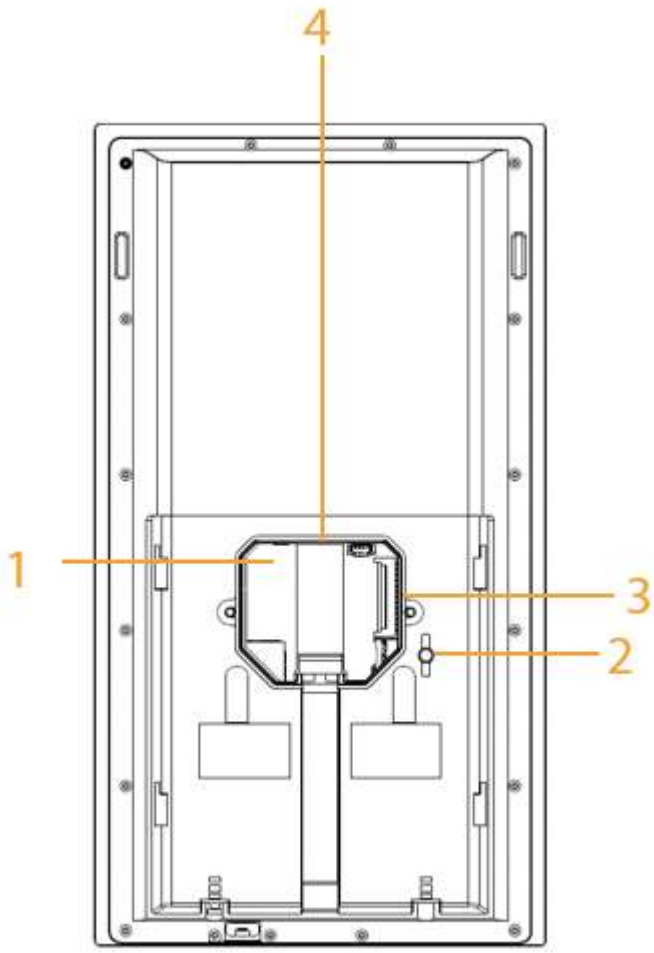
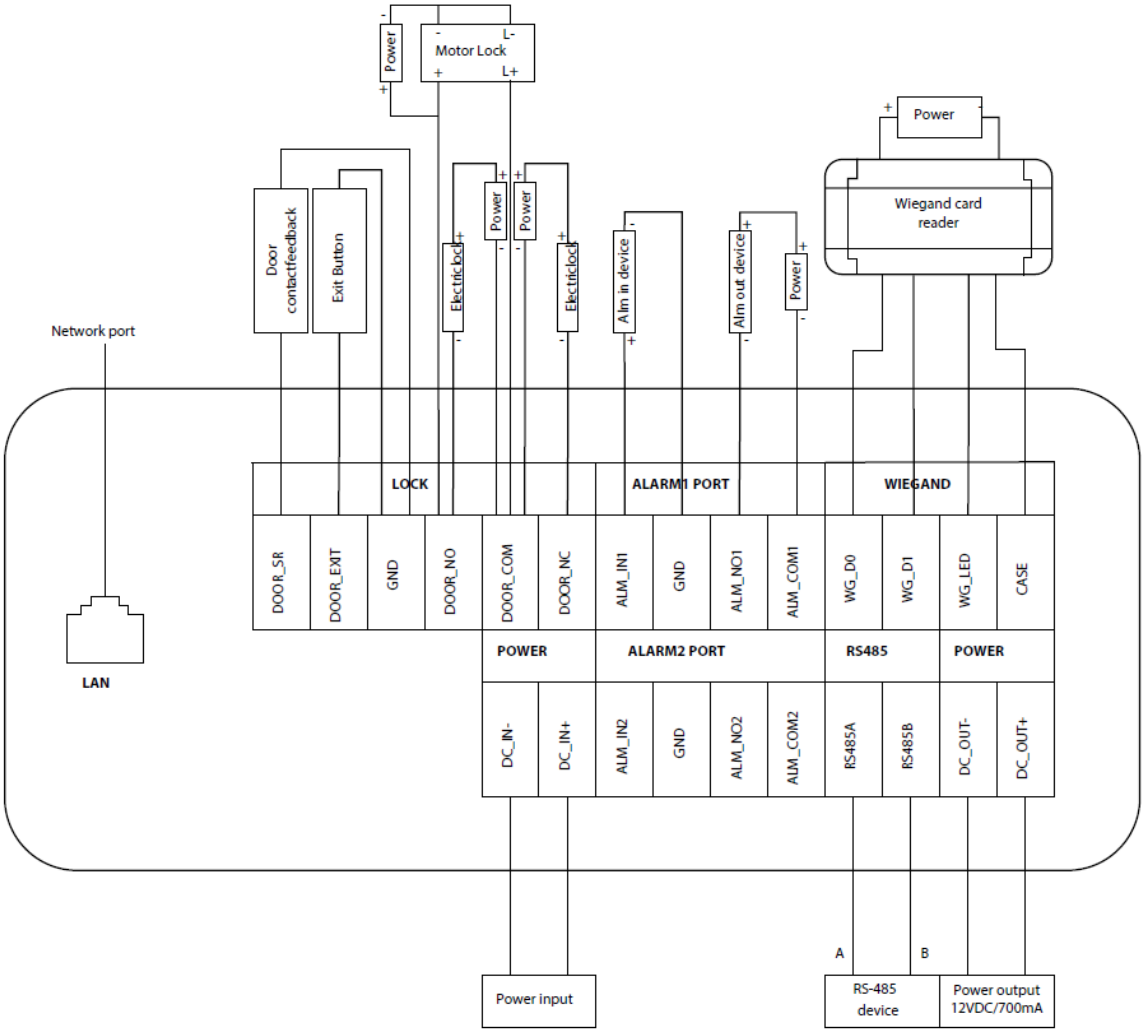


Table 1-9 Component description

No.	Description
1	Audio output port
2	Tamper button ● Triggers alarms for illegal dismantling or damage in emergency situations. ● 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 admin account information.
3	Function ports
4	Ethernet port

Figure 1-13 Cable connection



1.3.2.5 66 Series

Figure 1-14 Rear panel

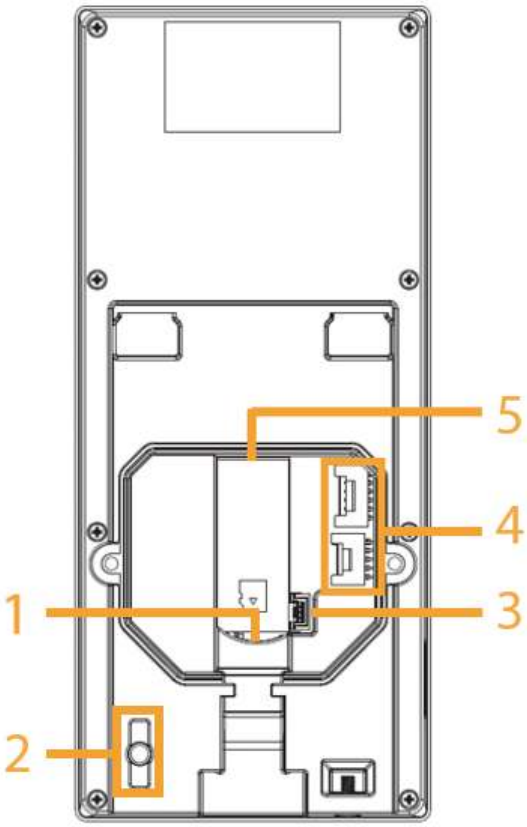
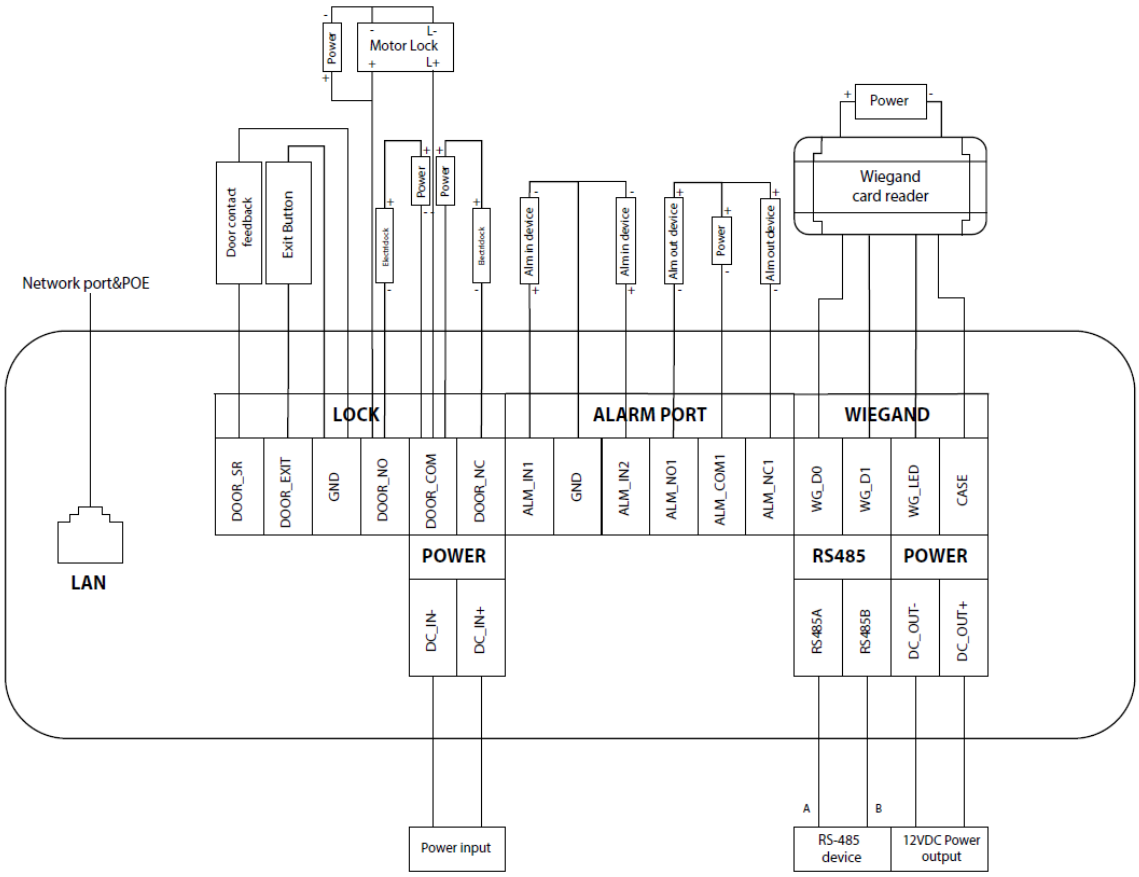


Table 1-10 Component description

No.	Description
1	SD card slot
2	Tamper button ● Triggers alarms for illegal dismantling or damage in emergency situations. ● 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 admin account information.
3	Power output port
4	Function ports
5	Ethernet port

Figure 1-15 Cable connection



- When the power input is PoE, the power output is 12 VDC/500 mA.
- When the power input is an adapter, the power output is 12 VDC/1500 mA.

2 Initialization

For the first-time use of the VTO, initialize the device first.

2.1 Initialization through the Device

Procedure

Step 1 Turn on the VTO.

Step 2 Select the language as needed, and then tap **OK**.

Step 3 Initialize the Device.

1. Configure the password, and then confirm it again.
2. Enter the Email address so that when you forget the password, you can reset it through the reserved Email address.
3. Enable the **Cloud Service** according to the actual needs, and then click **OK**.

After the function is enabled and the device connects to the network, we will collect device information, such as the IP address, MAC address, device name, and serial number.

2.2 Initialization on the Webpage

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 the first-time login, enter the default IP (192.168.1.108).

Step 3 Select the language, and then click **Next**.

Step 4 Read the software license agreement and privacy policy, select **I have read and agree to the terms of the Software License Agreement and Privacy Policy** , and then click **Next**.

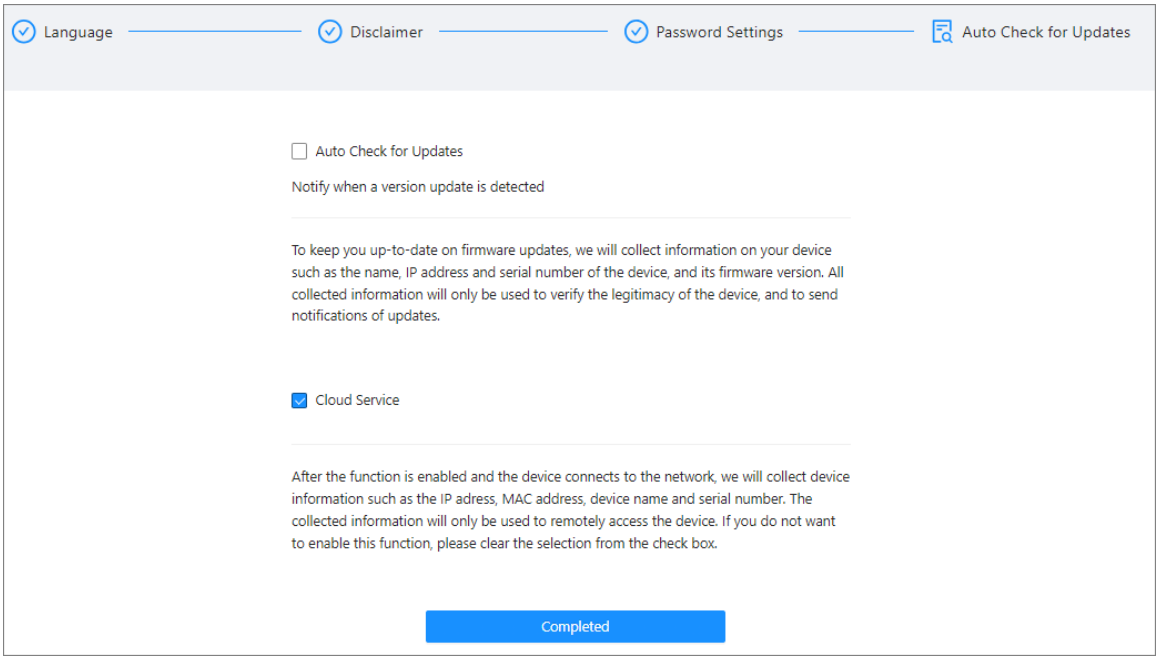
Step 5 Configure the password, and then confirm it again.

Step 6 (Optional) Select **Email Address** , enter the Email address, and then click **OK**.

When you forget the password, you can reset it through the reserved Email address.

Step 7 Select **Auto Check for Updates** and **Cloud Service** as needed.

Figure 2-1 Enable the service



Step 8 Click **Completed**.

Step 9 Click **Login** to go to the login page, and then enter the user name and the password to log in.

3 VTO Operations

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.

3.1 Home Screen

Figure 3-1 Home screen (66 series)

Figure 3-2 Home screen (75/95/76/96 series)

Table 3-1 Description of home screen

No.	Description
1	Displays the time. For details, see "4.11.4 Configuring Time".
2	Displays the device title. For details, see "3.5.4 Personalization" or "4.7.2 Personalization". Tap the title area, and then you can view the device SN.
3	Indicates that the SD card is inserted.
4	Displays the Wi-Fi function. For details, see "3.5.2.2 Wi-Fi" or "4.10.6 Configuring Wi-Fi".
5	Displays the Bluetooth function. For details, see "4.10.7 Configuring the Bluetooth" or "3.5.2.3 Bluetooth Settings".
6	Displays the network port status.
7	Displays the status of the SIP.

No.	Description
8	Tap it to configure the device language. It is temporarily effective. After the language is set and then the screen is turned off and on, it will be restored to the original setting language.
9	The zone is used for recognizing face and QR code.
10	Displays the shortcuts. For details about the shortcuts configuration, see "4.7.2.1 Configuring Personalization" and "3.5.4 Personalization". • Tap **Password**, and then enter the password to unlock the door. • Tap **Call** to make a call. • Tap **Center** to call the management center. • Tap **More** to see other shortcuts.

3.2 Homeowner Registration

Add more users through the existed homeowner.

Prerequisites

The person has been added and registered card or face.

Procedure

Step 1 Tap **Homeowner Registration** on the homepage.

If there is no **Homeowner Registration** shortcut, select **More** > **Homeowner Registration**.

Step 2 Select **Card** or **Face** to authorize the homeowner.

- Card: Swipe the card, and then goes to the **Person Management** page.
- Face: Recognize the face, and then goes to the **Person Management** page.

Step 3 Tap **Add User**, and then enter the detailed user information, including name, face, password, and fingerprint.

The room number cannot be edited, and is the same as the one of the existed homeowner.

Step 4 Tap **Person List**, and then you can view all users with the same room number as the one of the existed homeowner.

3.3 Unlock

You can unlock the door in many methods, such as entering the password, swiping the card, identifying the face, scanning the QR code, using the Bluetooth, remote unlock, and others.

3.3.1 Unlocking by the Password

Prerequisites

You have configured the password on the webpage of the VTO. For details, see"4.9 Person Management".

Procedure

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

Step 2 Enter the password to unlock the door.

The voice prompt and the device prompt **Successfully unlocked** means that the door opens and you can enter. If the device beeps, check the password.

3.3.2 Unlocking by the Card

Swipe the authorized card.

- The voice prompt and the device prompt **Successfully unlocked** means that the door opens and you can enter.
- If the device beeps, register the card. For details, see "4.9 Person Management".

3.3.3 Unlocking by Identifying the Face

When you come close to the VTO, the VTO automatically displays face detect screen and detects the face.

- That the voice prompts **Successfully unlocked** means that the door opens and you can enter.
- If the device displays **Unauthorized**, register the face first. For details, see "4.9 Person Management".

3.3.4 Unlocking by Scanning the QR Code

This function is only available on select models.

Procedure

Step 1 Get the QR code from the platform, such as DSS Pro. For details, see the user manual of the corresponding platform.

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

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

3.3.5 Unlocking by the Bluetooth

You can unlock the door by the Bluetooth via the DMSS app. This function is only available on select models.

Prepare the following things.

- The Bluetooth has been enabled. For details, see "4.10.7 Configuring the Bluetooth" or "3.5.2.3 Bluetooth Settings".
- The Device has been added to the DMSS app. For details, see the corresponding user manual.

Unlock the door via the DMSS app.

The voice prompt **Successfully unlocked** means that the door opens and you can enter.

3.3.6 Unlocking by the Fingerprints

This function is only available on select models.

Press the fingerprint.

- The voice prompt and the device prompt **Successfully unlocked** means that the door opens and you can enter.
- If the device prompts **Unregistered fingerprint**, register the fingerprint. For details, see "4.9 Person Management".

3.3.7 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 prompts **Successfully unlocked**, and then the door opens and visitors can enter.

3.3.8 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 prompts **Successfully unlocked**, and then the door opens and visitors can enter.

3.4 Call

Prerequisites

Add the VTHs and VTS on the webpage of the VTO. For details, see "4.8 Device Setting".

3.4.1 Calling the VTH

Procedure

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

Step 2 Call the VTH.

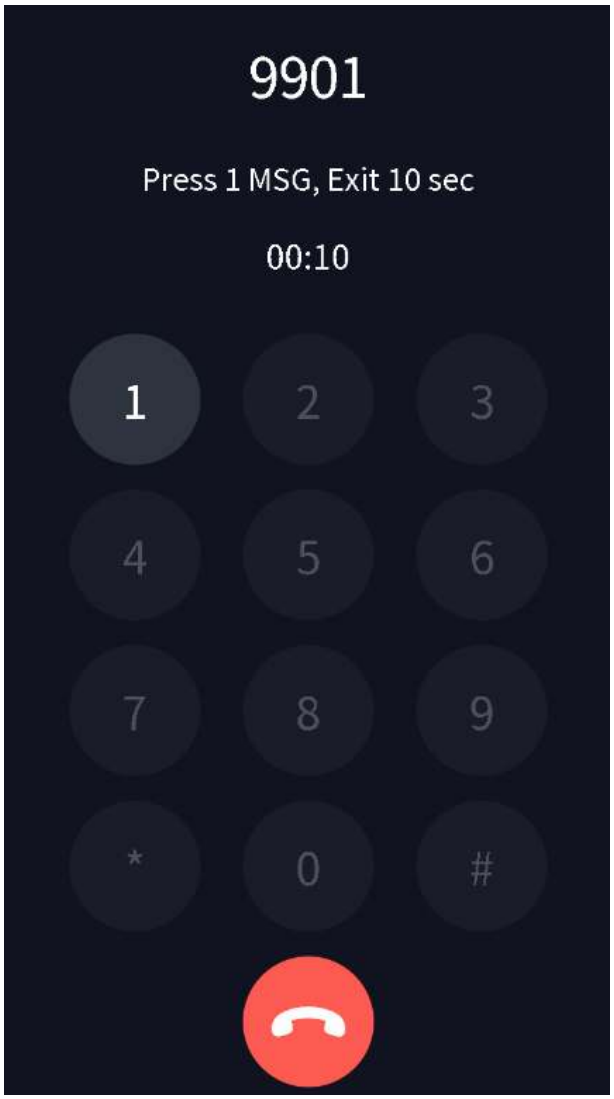
- Dial the room number of the VTH, and then tap .
- Tap **Phone Book**, and then select the VTH you want to call.

  The VTH managed in the phone book can be added on the webpage of the VTO. For details, see "4.8.2 Adding the VTH".

Related Operations

When the VTO is inserted SD card and during the calling, you can press **1** to make a leave video.

Figure 3-3 Make a leave video



3.4.2 Calling the VTS

Through the Shortcut

Tap **Center** on the homepage of the device.

Through the Call

1. Tap **Call** on the homepage of the device.
2. Tap to call the VTS.

3.5 Engineering Setting

Configure the engineering settings, including person management, communication, general settings, personalization, and device information.

Procedure

Step 1 Power on the VTO.

Step 2 Long press the home screen.

The long-press areas vary for different themes. Here use 2 themes as examples.

Figure 3-4 Theme (1)

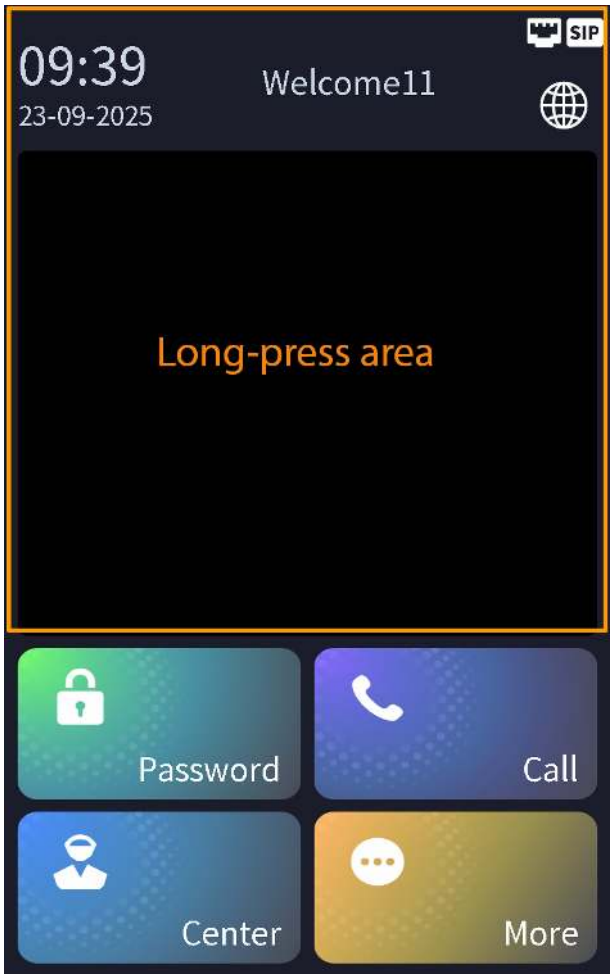
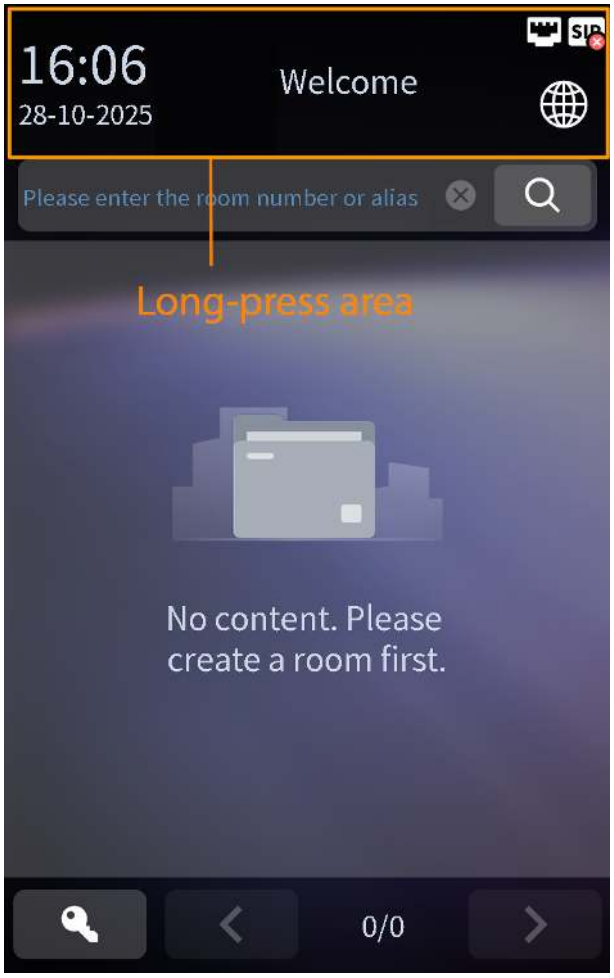
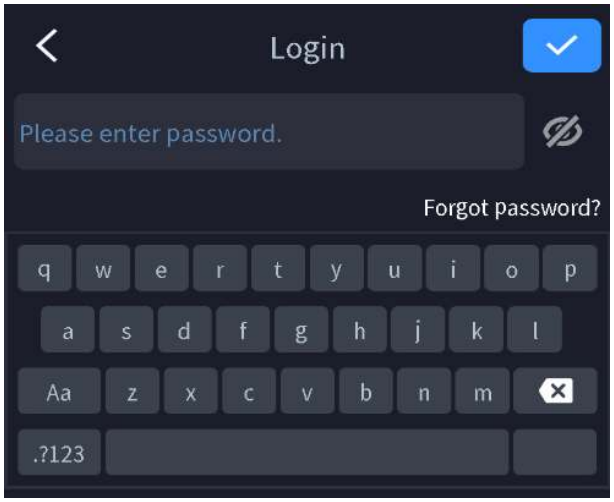


Figure 3-5 Theme (2)



Step 3 Enter the password, and then tap ✓ to go to the engineering setting.

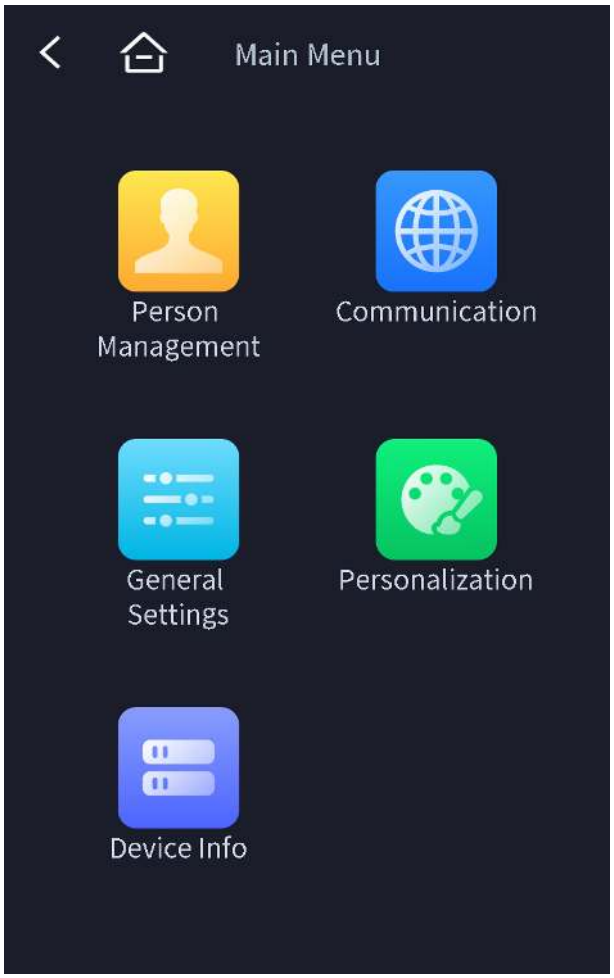
Figure 3-6 Enter the password



Results

You can configure the engineering settings on the main menu.

Figure 3-7 Main menu



3.5.1 Person Management

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

Prerequisites

Make sure the server type is configured as **Device** or **Third-party Server**. For details, see "4.10.3 Configuring the SIP Server".

Procedure

Step 1 Tap **Person Management** on the screen of the **Main Menu**.

Step 2 Tap **Add User**, and then configure the user information.

Figure 3-8 Add users

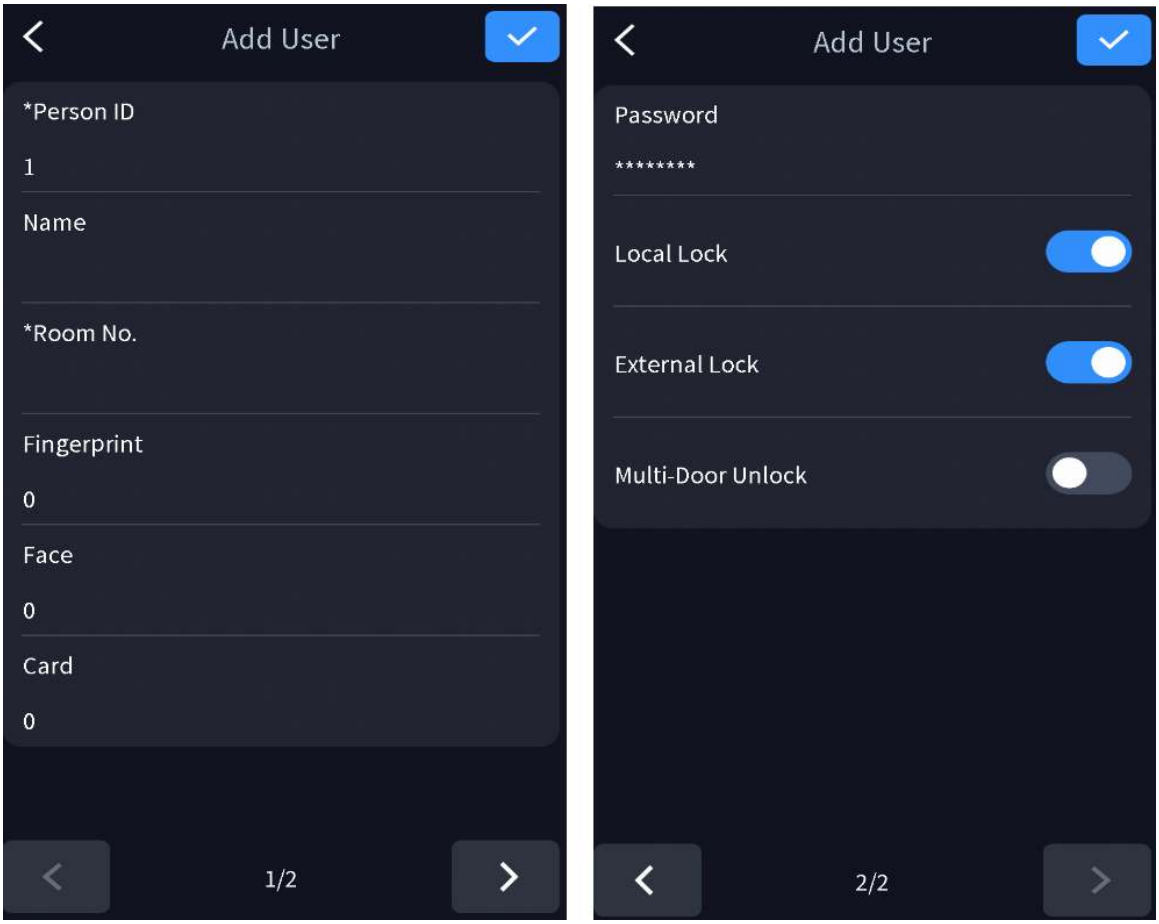


Table 3-2 User information

Parameter	Description
Person ID	Enter the person ID, room number and the user name.
Name	
Room No.	
Fingerprint	Tap **Fingerprint**, and then register the fingerprint. ● Each user can register 3 fingerprints at most. ● This function is only available on select models.
Face	Tap **Face** , capture the face, and then tap **OK**. If you are not satisfied with the picture, tap **Recapture** to capture again.
Card	Tap **Card**, and then register the card. ● Each user can register 5 cards at most. ● This function is only available on select models.

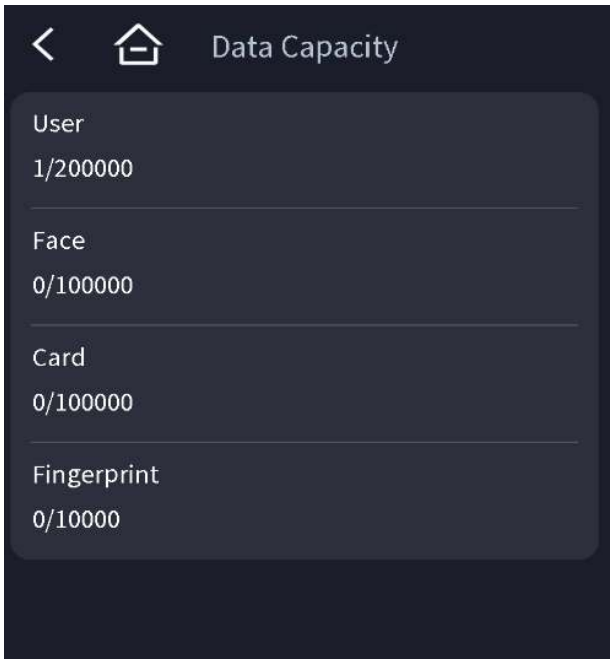
Parameter	Description
Password	Configure the user password. The password must consist of 4-6 digits.
Local Lock	After it is enabled, the user will have authority to open the local lock.
External Lock	After it is enabled, the user will have authority to open the second lock that connects to the VTO through the function port.
Multi-Door Unlock	After it is enabled, when the verification is successful, the local lock and external lock will open at the same time. The user password cannot be authenticated to perform multi-door unlock.

Step 3 Tap **Person List** to view the person list.

- Tap the person in the list, and then you can view the person information, such as person name, room number, and authorized permissions.
- Tap to search for the wanted person.

Step 4 Tap **Data Capacity** to view the capacity for person.

Figure 3-9 Data capacity



3.5.2 Communication

Tap **Communication** on the screen of the main menu to configure the communication of the Device.

3.5.2.1 IP Settings

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

Procedure

Step 1 Tap **IP Settings**, and then configure the IP address as needed.

Figure 3-10 IP settings

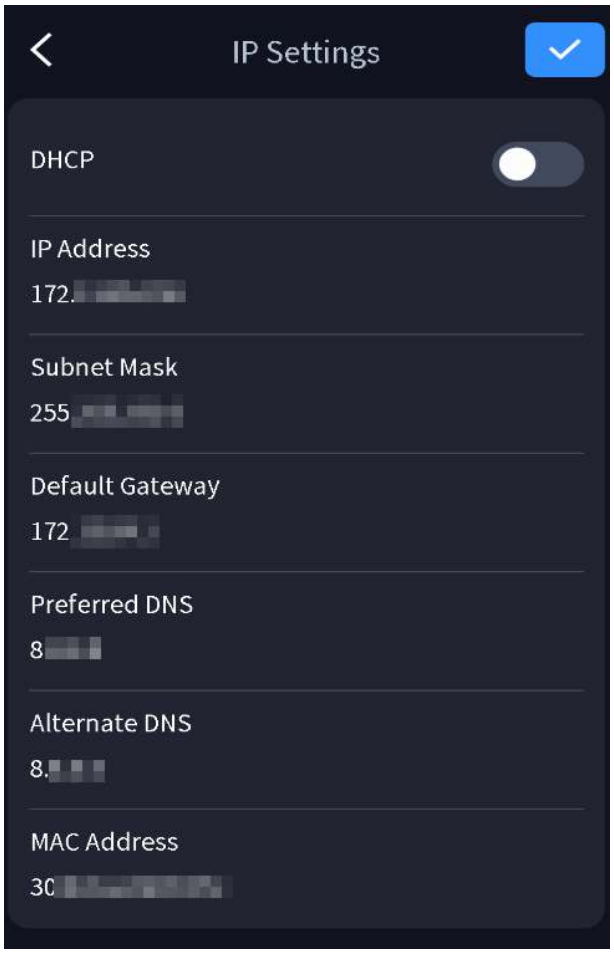


Table 3-3 Description of IP parameters

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.
IP Address	When DHCP is not enabled, tap the item to configure the IP address, subnet mask and gateway.
Subnet Mask	
Default Gateway	
Preferred DNS	Set IP address of the preferred DNS server.
Alternate DNS	Set IP address of the alternate DNS server.

Parameter	Description
MAC Address	Displays the MAC address of the Device.

Step 2 Tap .

3.5.2.2 Wi-Fi

Configure the Wi-Fi function of the Device. This function is only available on select models.

Procedure

Step 1 Tap **Wi-Fi**.

Step 2 Tap to enable the Wi-Fi function, and then you can view the available Wi-Fi list.

Figure 3-11 Wi-Fi list

Step 3 Tap the Wi-Fi to be connected, enter the password, and then tap .

Related Operations

- Tap to enter the Wi-Fi manually.
- Tap to refresh the Wi-Fi list.

3.5.2.3 Bluetooth Settings

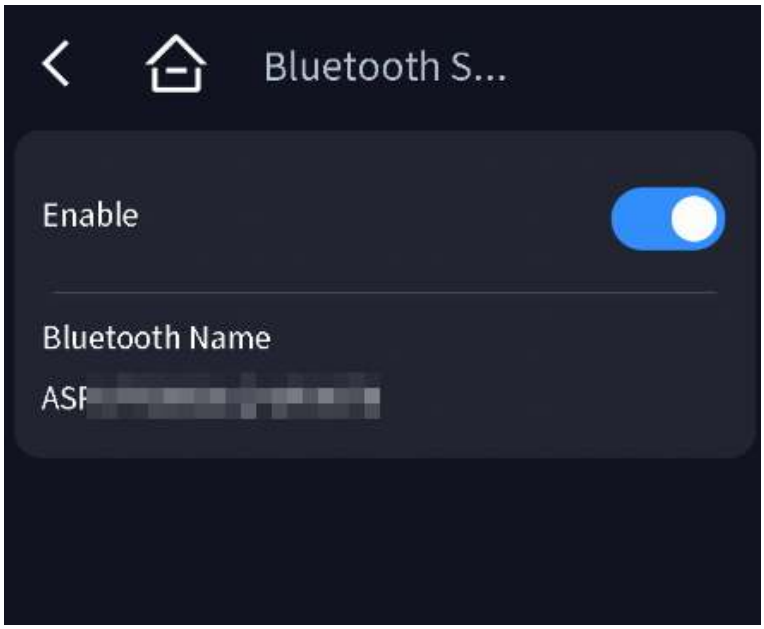
Configure the Bluetooth function of the Device. This function is only available on select models.

Procedure

Step 1 Tap **Bluetooth Settings**.

Step 2 Tap behind the **Enable** to enable the Bluetooth function.

Figure 3-12 Bluetooth



Results

You can unlock the door through the Bluetooth via the DMSS app. For details, see "3.3.5 Unlocking by the Bluetooth".

3.5.2.4 Cloud Service

Through the cloud service, you can manage the VTO through DMSS.

Procedure

Step 1 Connect the VTO to the external network through wired or wireless connection.

Step 2 Tap behind the **Cloud Service** to enable the function.

3.5.3 General Settings

Configure the volume, screen off time and other parameters.

Procedure

Step 1 Tap **General Settings** on the screen of the main menu.

Step 2 Configure the parameters.

Figure 3-13 General settings

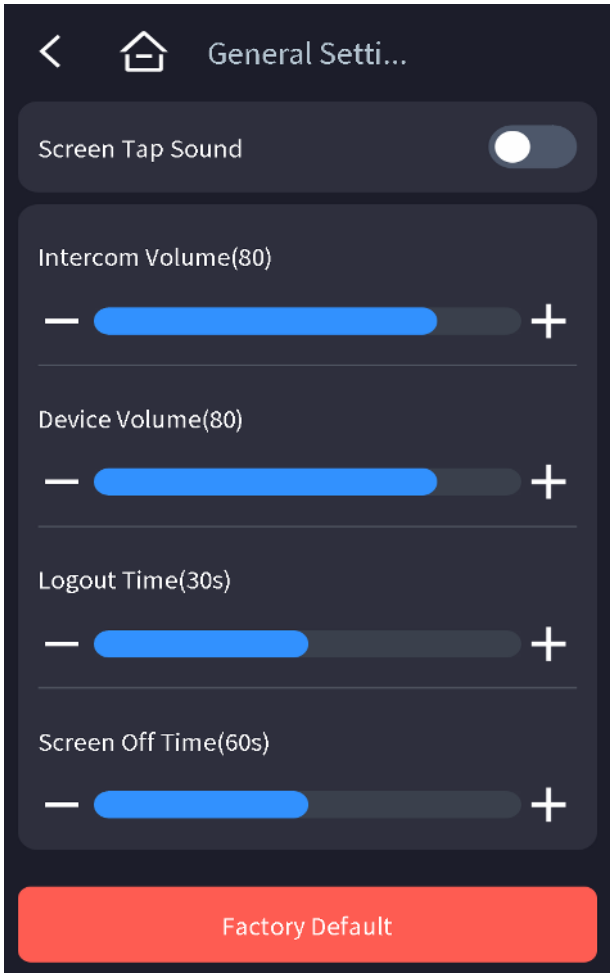


Table 3-4 Description of the general settings

Parameter	Description
Screen Tap Sound	Tap to enable the function, and then once you tap the screen, there is a tap sound.
Intercom Volume	Tap + or — to increase or decrease the volume during intercom calls.
Device Volume	Tap + or — to increase or decrease the device volume.
Logout Time	Tap + or — to increase or decrease the waiting time for automatic logout when there is no operation. The logout time must be lower than the screen time.
Screen Off Time	Tap + or — to increase or decrease the delay time for the screen to automatically turn off.

Step 3 (Optional) Tap **Factory Default** to set the device to the factory default.

All settings will be restored to default except for IP address. Please be advised.

3.5.4 Personalization

Personalize the device.

Procedure

Step 1 Tap **Personalization** on the screen of the main menu.

Step 2 Configure the personalization as needed.

The figure here is only for reference, and might differ from devices.

Figure 3-14 Personalization

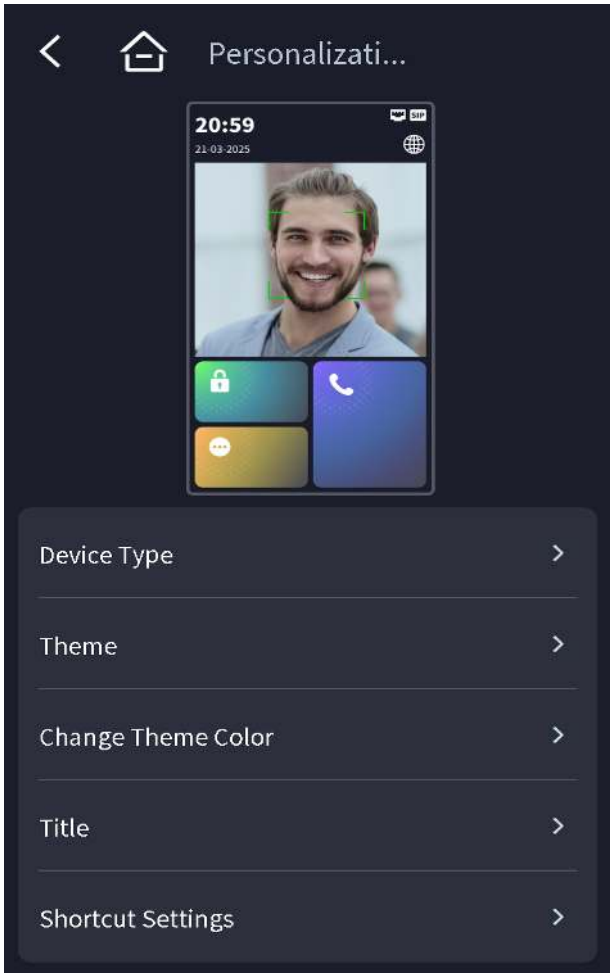


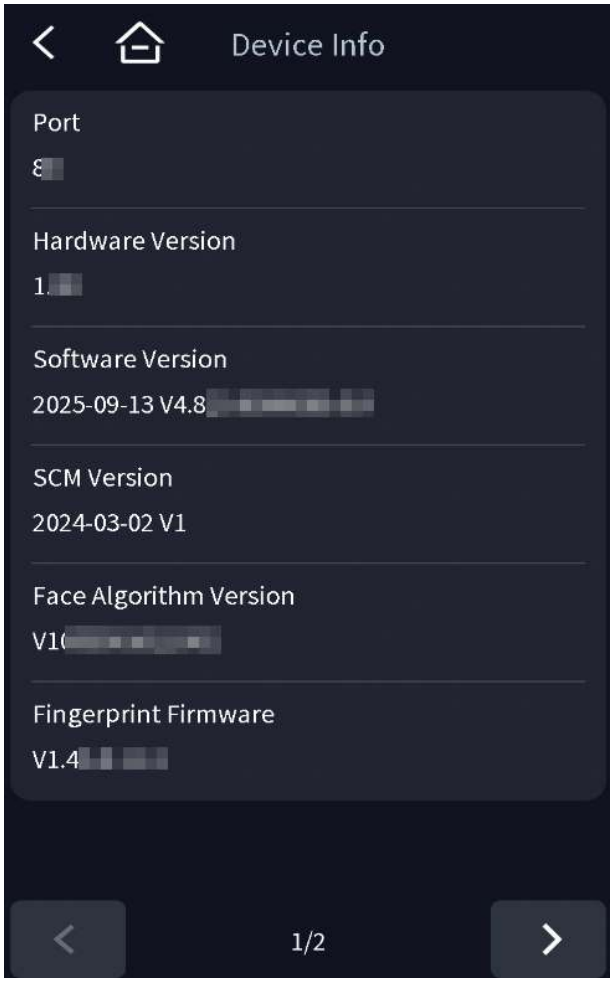
Table 3-5 Description of the personalization

Items	Description
Device Type	Select the device type from **Unit VTO** , **Fence Station**, or **Villa Station** according to the actual needs. You can also set the device type on the webpage of the device. For details, see "4.7.1 Basic Settings".
Theme	Select the device theme. After you select one theme, the feature of each theme will be displayed. You can also set the device subject on the webpage of the device. For details, see "4.7.2.1 Configuring Personalization".
Change Theme Color	Change the device theme color. You can also change the device theme on the webpage of the device. For details, see "4.7.2.1 Configuring Personalization".
Title	Change the device title. You can also change the device theme on the webpage of the device. For details, see "4.7.2.1 Configuring Personalization".
Shortcut Settings	Configure the device shortcuts. ● Password: Configure it as the shortcut, you can tap **Password** on the home screen, and then enter the password to unlock the door. ● Call: Configure it as the shortcut, and then you can tap **Call** on the home screen to make a call. ● Center: Configure it as the shortcut, you can tap **Center** on the home screen to call the management center. ● Postal Worker Unlock: Configure it as the shortcut, you can tap **Postal Worker Unlock** on the home screen to unlock the door. ● Publish Info: Configure it as the shortcut, you can tap **Publish Info** on the home screen to view the publish information. ● Homeowner Registration: Configure it as the shortcut, you can tap **Homeowner Registration** on the home screen to register homeowners. ● The number of the shortcuts depends on the theme. ● You can also configure the device shortcuts on the webpage of the device. For details, see "4.7.2.1 Configuring Personalization".

3.5.5 Device Information

Tap **Device Info** on the screen of the main menu to view the details of the device.

Figure 3-15 View the device information



4 Webpage Operations

4.1 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 user name (admin by default) and the password that you configured during the initialization.

Step 3 Click **Login**.

4.2 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**.

4.3 Home Page Introduction

Figure 4-1 Home page

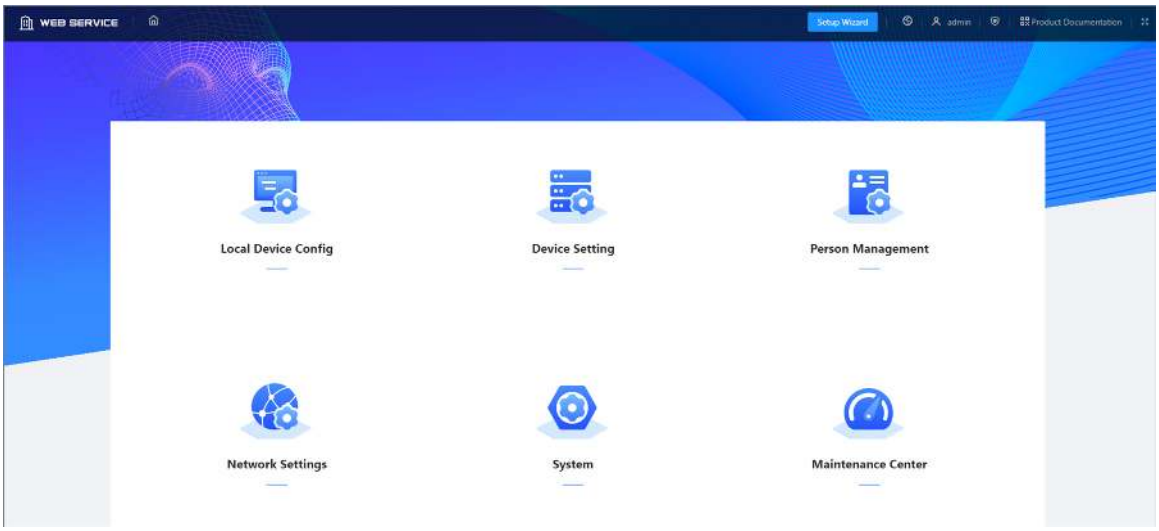


Table 4-1 Homepage introduction

Icon	Function	Description
	Home button	Click it to go back to the homepage.
Setup Wizard	Setup Wizard	Configure the VTO SIP server. For details, see "4.4 Setup Wizard".
	Language	Change language of the webpage of the VTO.
admin	Admin Center	Change password, log out of the current device, restart the system, and restore the device to factory settings. For details, see "4.5 Admin Center".
	Security Center	View and configure the security settings. For details, see "4.6 Security Center".
Product Documentation	Product Documentation	Scan the QR code to view the product documentation, such as the user manual. This function is only available on select models.
	Full screen	View the webpage in full screen mode. Click again or press the Exit key to exit the full screen mode.
	Local Device Config	Configure the basic information. For details, see "4.7 Local Device Configuration".
	Device Setting	Manage the device information. For details, see "4.8 Device Setting".

Icon	Function	Description
	Person Management	Manage the person information. For details, see "4.9 Person Management".
	Network Settings	Configure the network parameters. For details, see "4.10 Network Settings".
	System	Configure the parameters of alarm linkage, video, audio, time, and ONVIF users. For details, see "4.11 System".
	Maintenance Center	View the system information. For details, see "4.12 Maintenance Center".

4.4 Setup Wizard

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

4.4.1 Setting as SIP Server

Set the VTO as the SIP server.

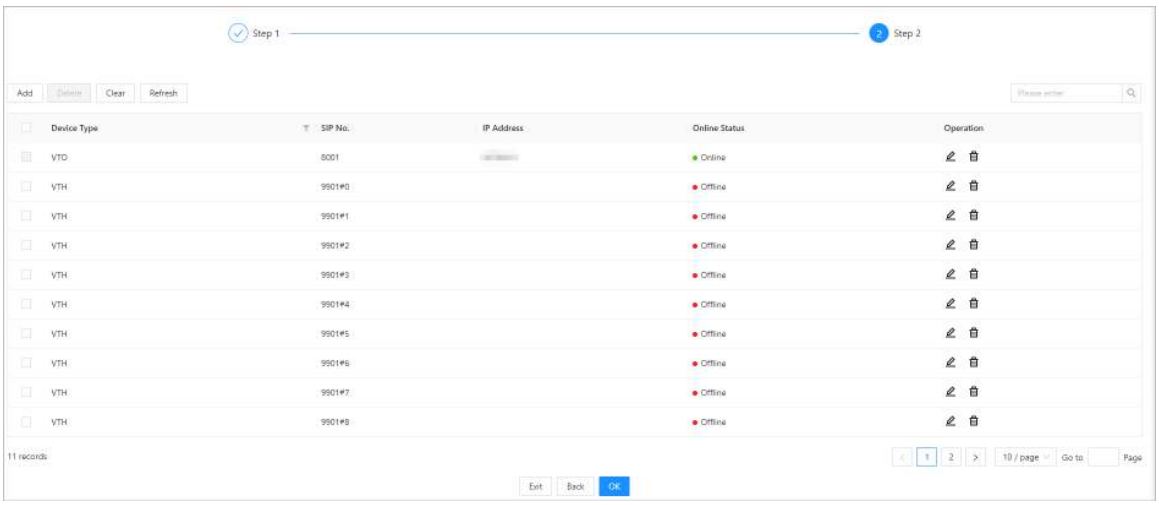
Procedure

Step 1 Log in to the webpage of the VTO.

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

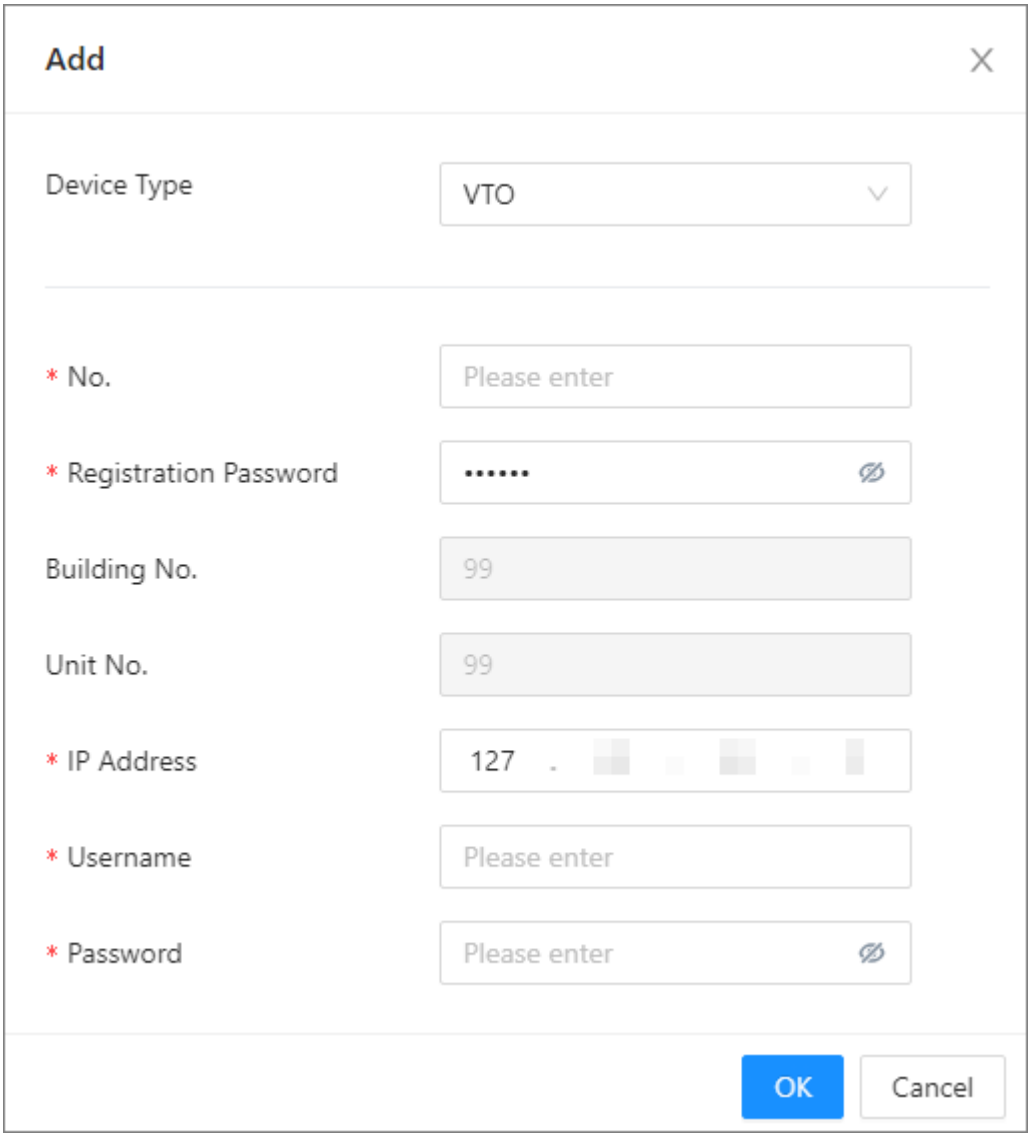
Step 3 Click **OK** to set the VTO as the SIP server.

Figure 4-2 Select the SIP server



Step 4 (Optional) Click **Add** to add VTOs, VTHS, and VTSs, and then click **OK**.

Figure 4-3 Add other devices



4.4.2 Not Setting as SIP Server

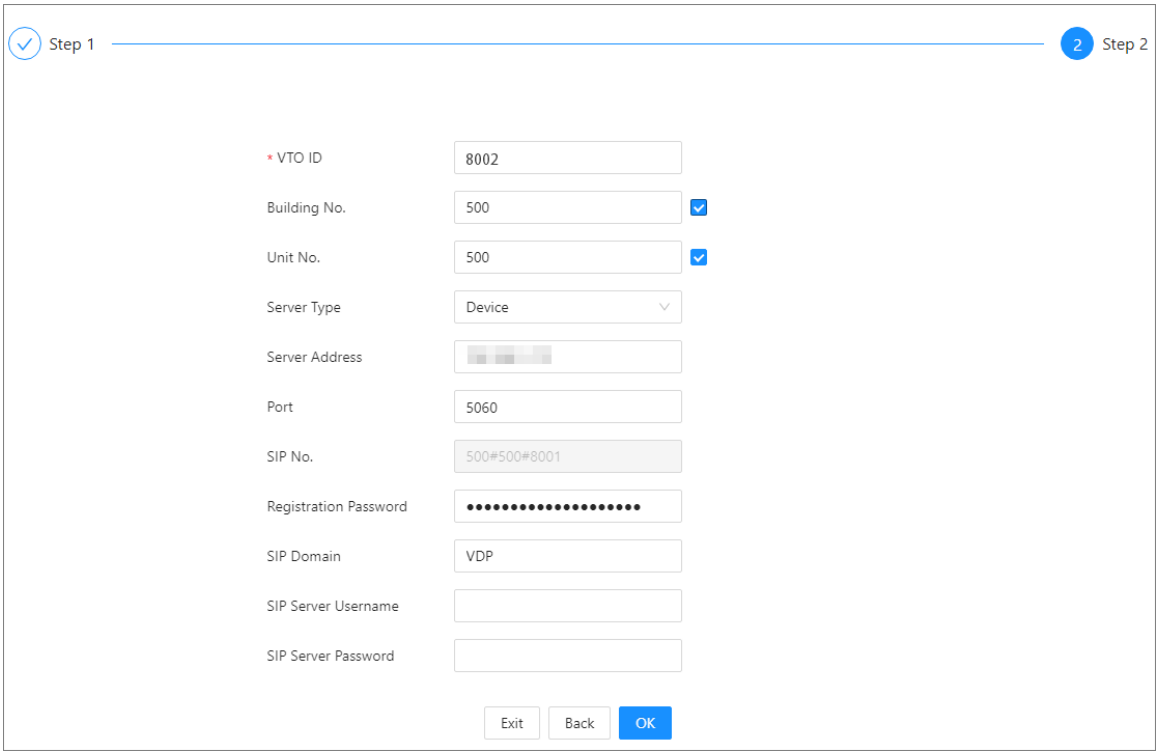
Procedure

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**.

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

Figure 4-4 Configure information



4.5 Admin Center

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

4.5.1 Changing the Password

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

Procedure

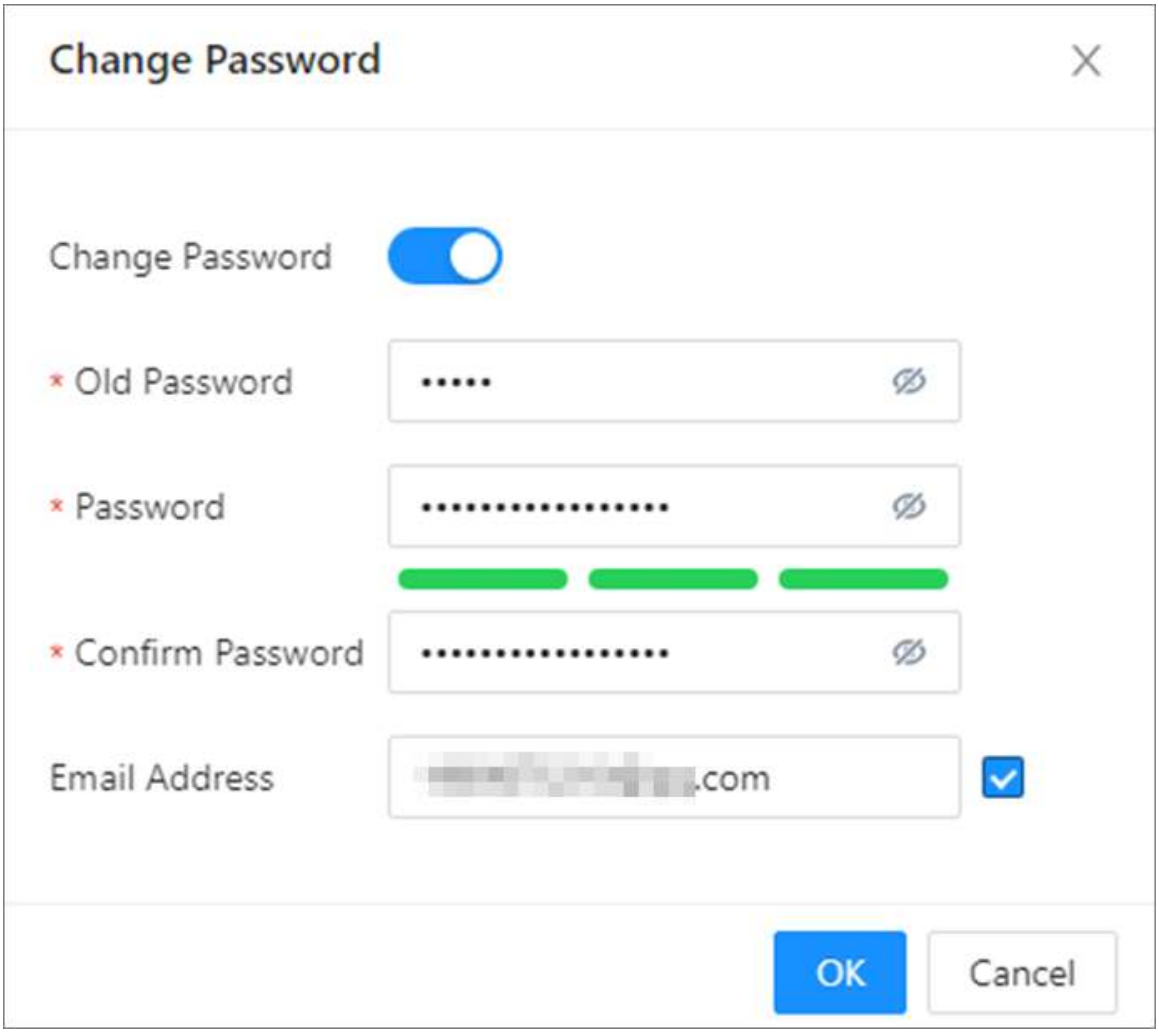
Step 1 Log in to the webpage of the VTO.

Step 2 Click admin on the homepage.

Step 3 Click **Change Password**.

Step 4 Enable the function, configure the parameters, and then click **OK**.

Figure 4-5 Change the password



4.5.2 Logout

Procedure

Step 1 Click admin on the homepage of the VTO.

Step 2 Click **Logout** , and then click **OK**.

Results

It goes to the login page of the VTO.

4.5.3 Restarting the Device

Procedure

Step 1 Click admin on the homepage of the VTO.

Step 2 Click **Restart** , and then click **OK**.

Results

The device automatically restarts, and then the webpage goes to the login page.

4.5.4 Restoring Default Factory Settings

Restore all settings to default except for IP address.

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

Procedure

Step 1 Log in to the webpage of the VTO.

Step 2 Click admin.

Step 3 Click **Factory Default**.

Step 4 Enter the login password, and then click **OK**.

Results

The device will restore to the default factory settings, and will log out the webpage automatically.

4.6 Security Center

4.6.1 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.

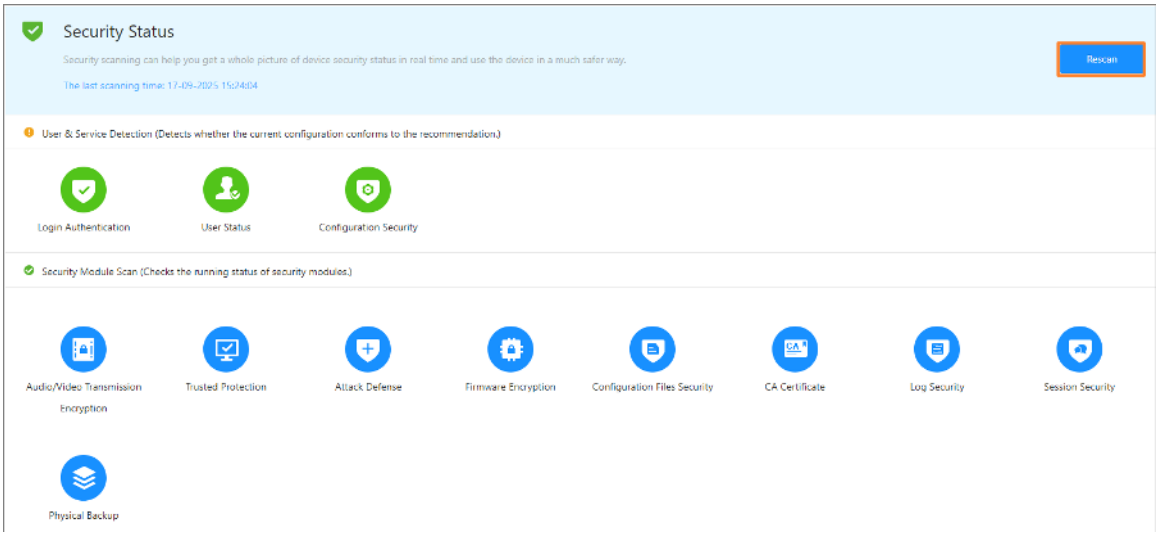
Procedure

Step 1 Select > **Security Status**.

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

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

Figure 4-6 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.

4.6.2 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**.

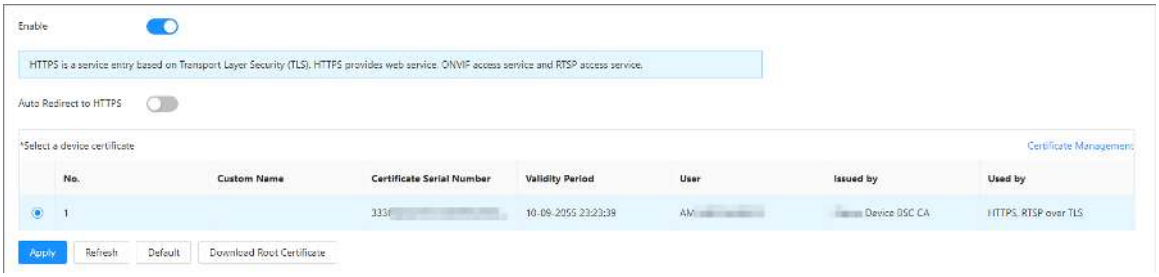
Step 2 Enable the HTTPS service.

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 4-7 HTTPS



Step 4 Click **Apply**.

Results

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

4.6.3 Attack Defense

4.6.3.1 Configuring Firewall

Configure firewall to limit access to the Device.

Procedure

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

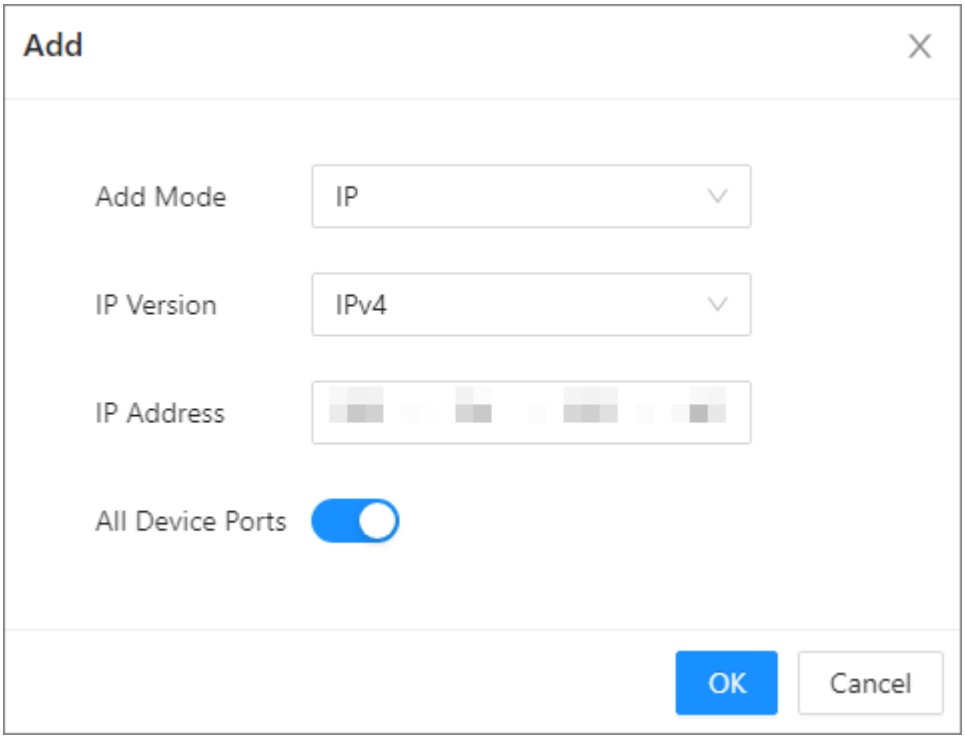
Step 2 Click to enable the firewall function.

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

- **Allowlist** : Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.
- **Blocklist** : The listed corresponding source host of IP addresses/MAC is prohibited from visiting the corresponding ports of the device by network connection.

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

Figure 4-8 Add IP information



Step 5 Click **OK**.

Related Operations

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

4.6.3.2 Configuring Account Lockout

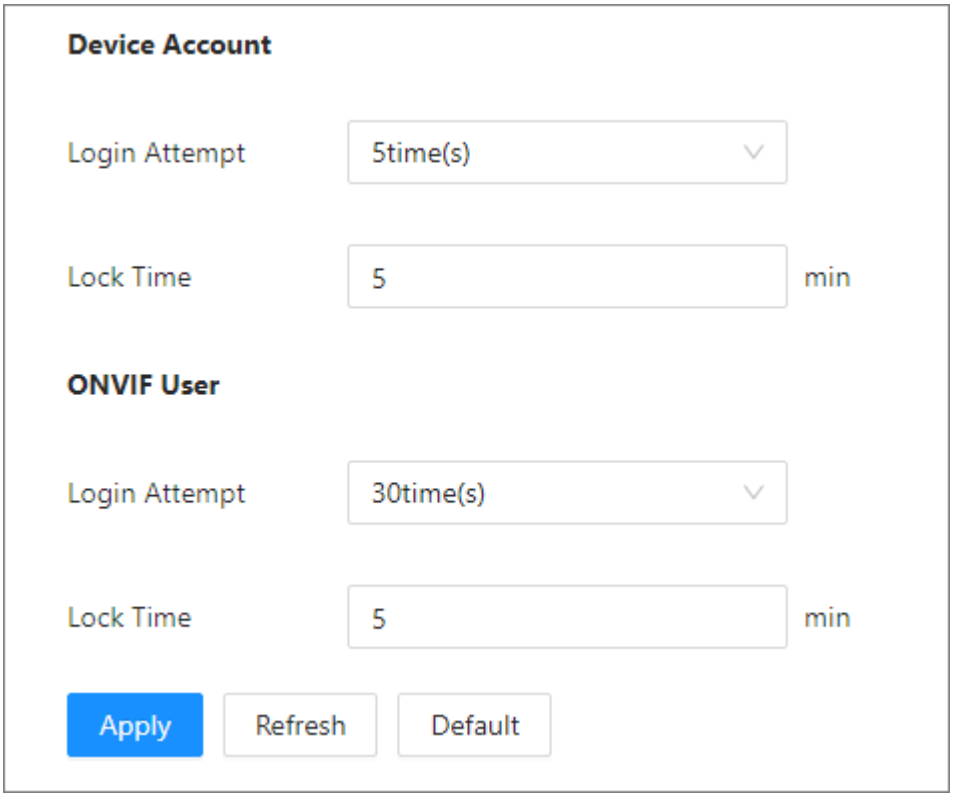
If the incorrect password is entered for a defined time, the account will be locked.

Procedure

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

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

Figure 4-9 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**.

4.6.3.3 Configuring Anti-DoS Attack

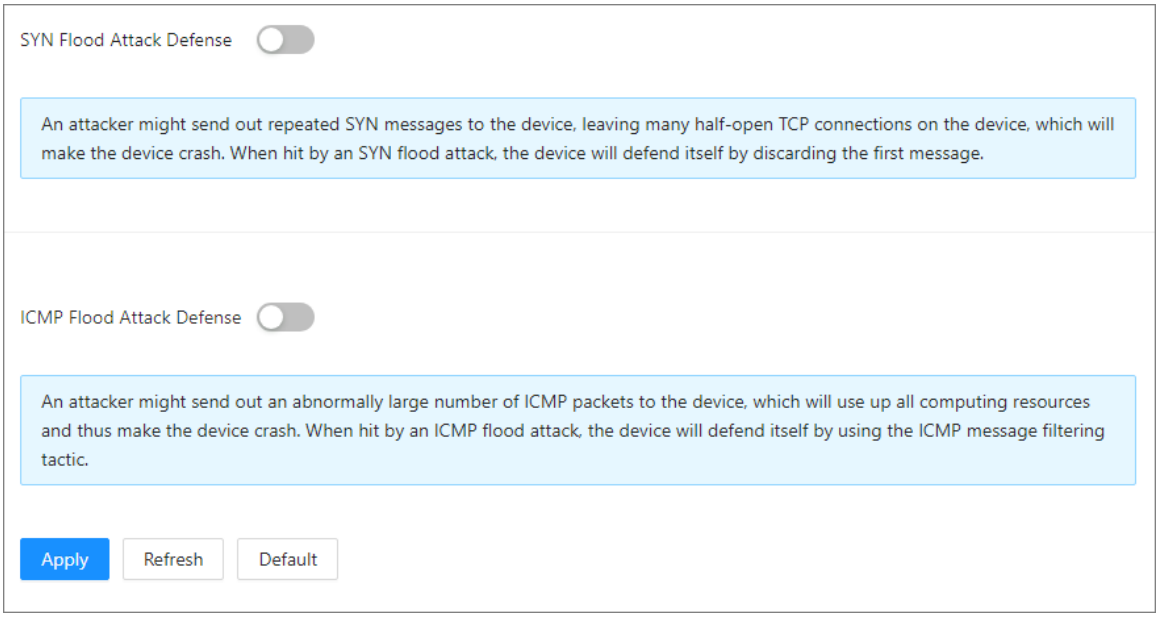
You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the VTO against DoS attacks.

Procedure

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

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

Figure 4-10 Anti-DoS attack



Step 3 Click **Apply**.

4.6.4 Installing Device Certificate

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

4.6.4.1 Creating Certificate

Create a certificate for the Device.

Procedure

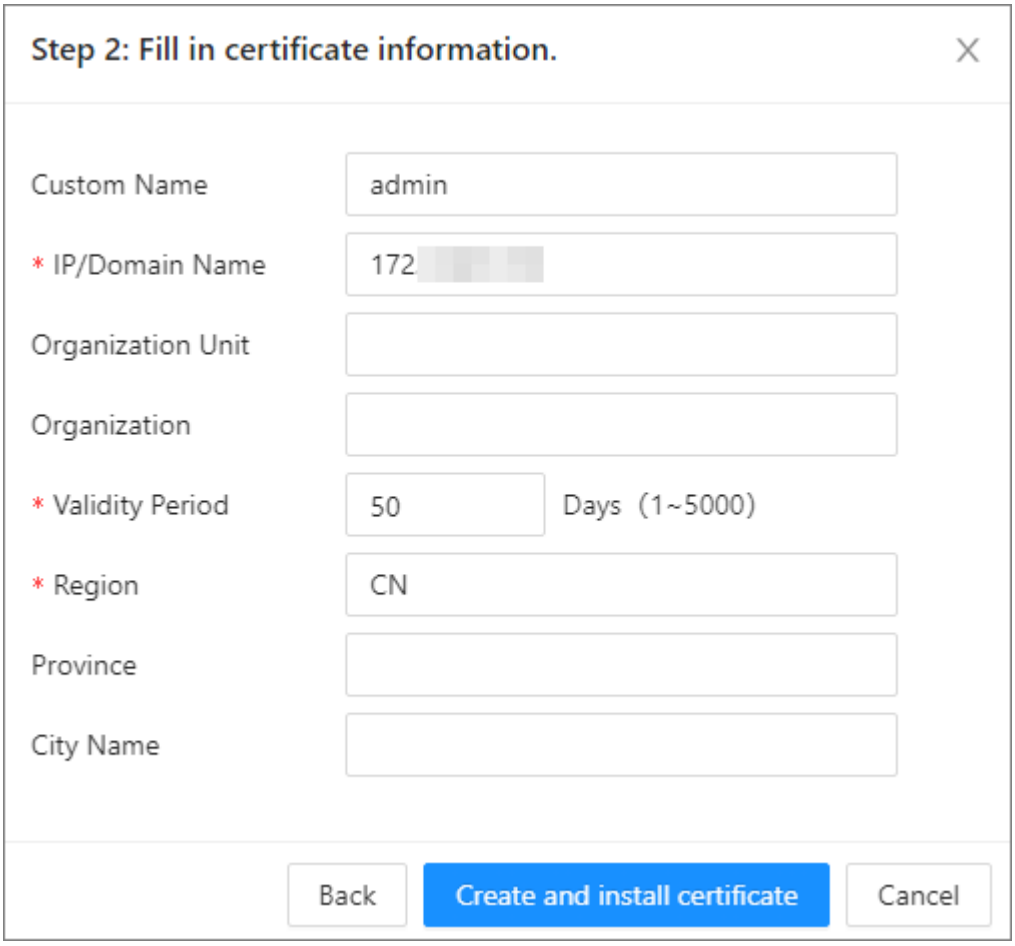
Step 1 Select > **CA Certificate** > **Device Certificate**.

Step 2 Click **Install Device Certificate**.

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

Step 4 Enter the certificate information.

Figure 4-11 Certificate information



The name of region should be 2 uppercase letters. 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.

4.6.4.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the Device.

Procedure

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

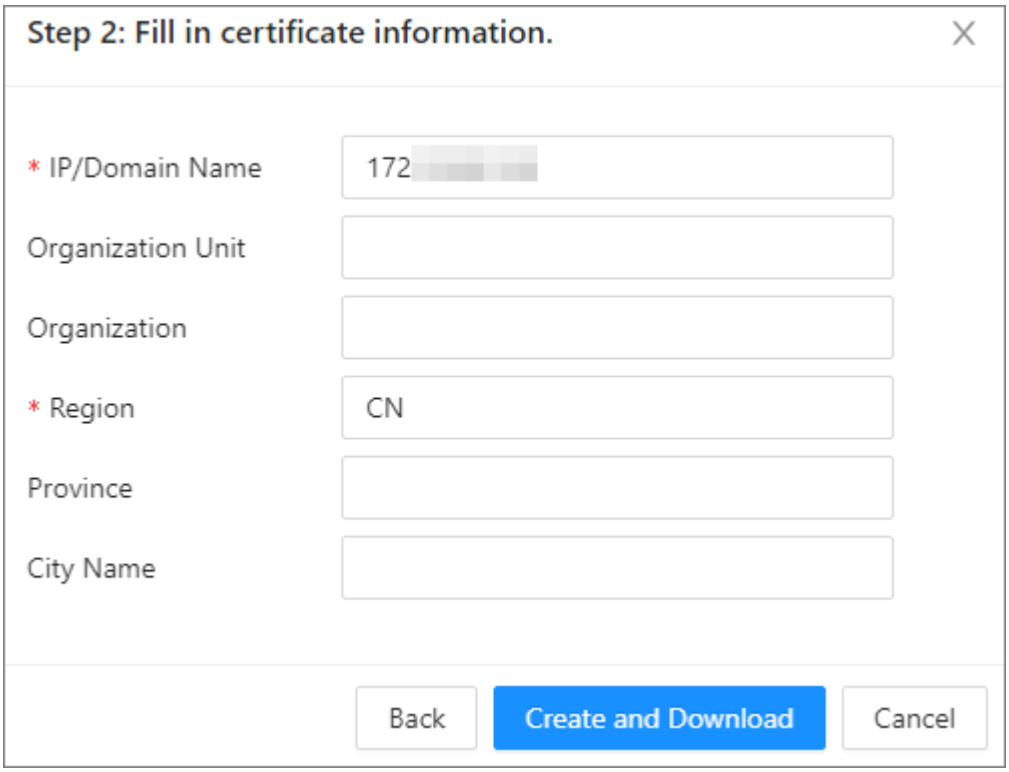
Step 2 Click **Install Device Certificate**.

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 should be 2 uppercase letters. We recommend you enter the abbreviation of region name.

Figure 4-12 Certificate information (2)



Step 5 Click **Create and Download**.

The request file will be saved to your computer.

Step 6 Import the signed CA certificate.

1. Click **Browse** to select the CA certificate.
2. Click **Import and Install**.

   The newly installed certificate is displayed on the **Device Certificate** page after the certificate is successfully installed.
3. (Optional) Click **Recreate** to create the request file again or 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.

4.6.4.3 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.

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.

4.6.5 Installing the Trusted CA Certificate

A trusted CA certificate is a digital certificate that is used for validating the identities of websites and servers.

Background Information

- For example, when 802.1x protocol is used, the CA certificate for switches is required to authenticate its identity.
- 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.

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.

4.6.6 Video Encryption

Procedure

Step 1 Select > **Video Encryption**.

Step 2 Configure the parameters.

Figure 4-13 Video encryption

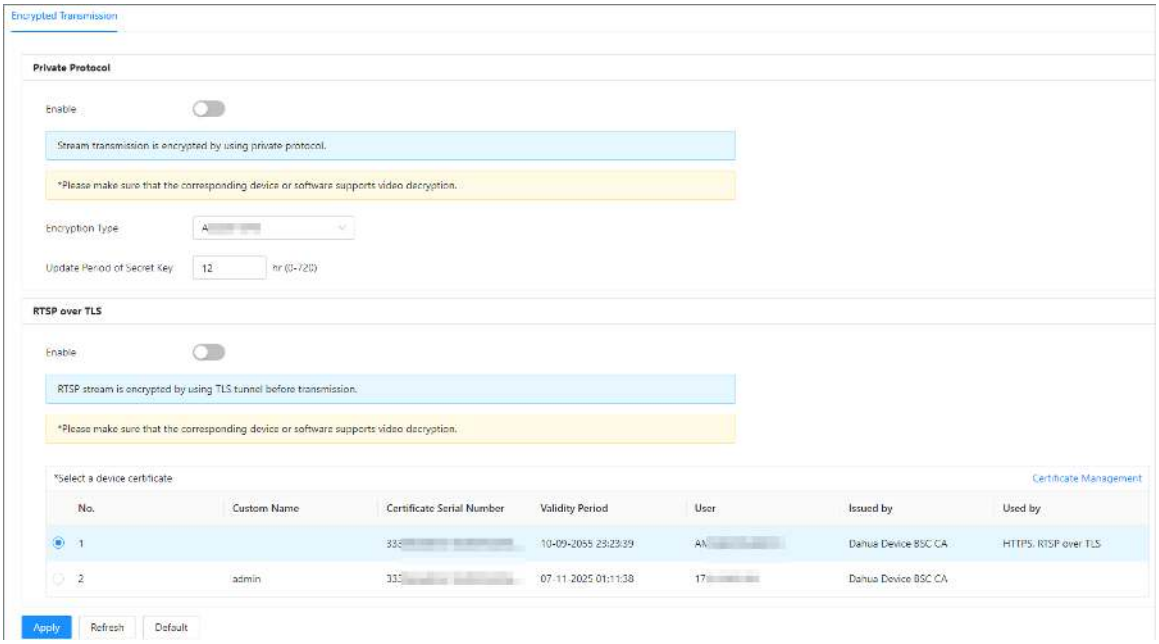


Table 4-2 Data encryption description

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.

4.6.7 Security Warning

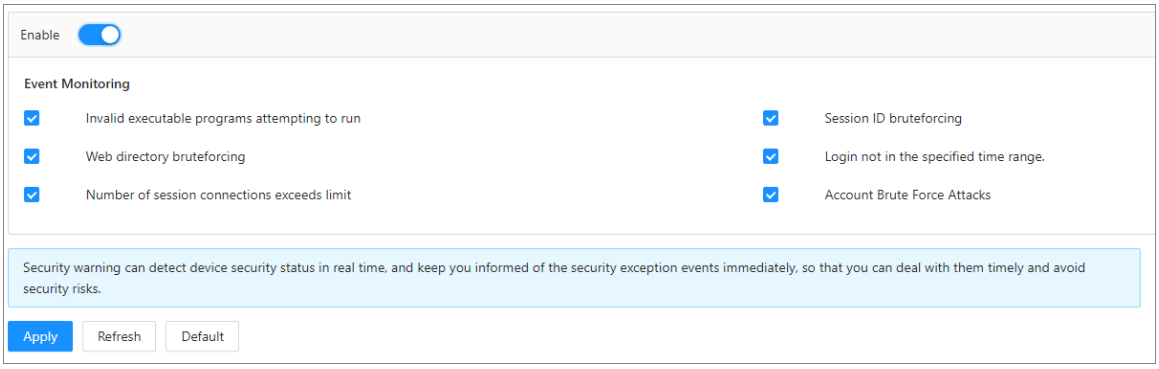
Procedure

Step 1 Select > **Security Warning**.

Step 2 Enable the security warning function.

Step 3 Select the monitoring items.

Figure 4-14 Security warning



Step 4 Click **Apply**.

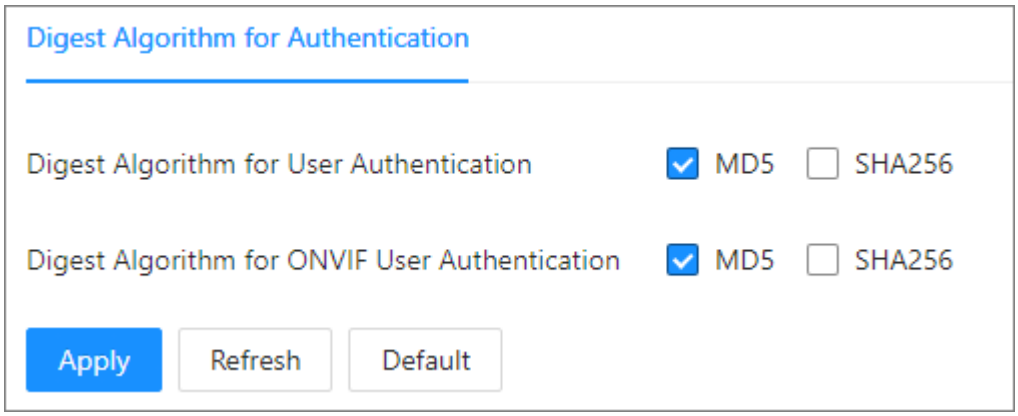
4.6.8 Security Authentication

Procedure

Step 1 Select > **Security Authentication**.

Step 2 Select a digest algorithm for user authentication and ONVIF user authentication respectively.

Figure 4-15 Security Authentication



Step 3 Click **Apply**.

4.7 Local Device Configuration

This chapter introduces the detailed configuration of the VTO.

Slight differences might be found in different models.

4.7.1 Basic Settings

The default device types vary from different devices.

4.7.1.1 Unit VTO as Device Type

Procedure

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

Step 2 Select **Unit VTO** as **Device Type**, and then configure the parameters.

Figure 4-16 Basic settings

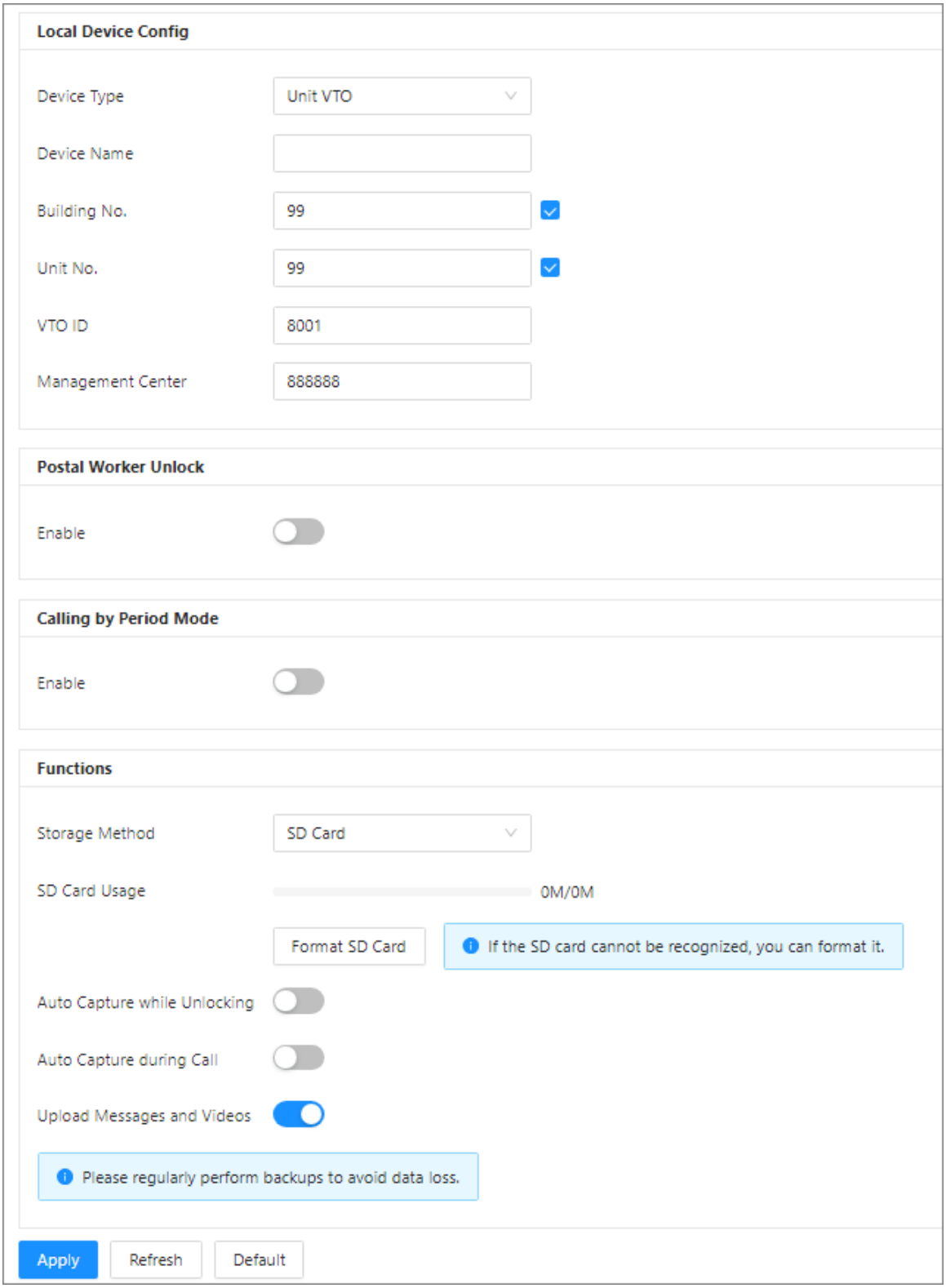


Table 4-3 Basic parameter description

Module	Parameter	Description
Local Device Config	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.**, 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.
	Management Center	888888 by default.
Postal Worker Unlock		It is disabled by default. • When it is enabled, select whether local lock or external lock can be open during the set period. • Click **Setting** to configure the unlock schedule during which the postal worker can unlock the door.
Calling by Period Mode		It is disabled by default. When it is enabled, click **Setting** to configure the time plan, during which the calling can be achieved.
Functions	Storage Method	It is 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 unlocked through the local unlock button, the snapshot will not be taken.

Module	Parameter	Description
	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 it is enabled, the leave videos will be saved in the VTH or VTO where the SD card is inserted.

Step 3 Click **Apply**.

4.7.1.2 Fence Station as Device Type

Procedure

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

Step 2 Select **Fence Station** as **Device Type**, and then configure the parameters.

Figure 4-17 Basic settings

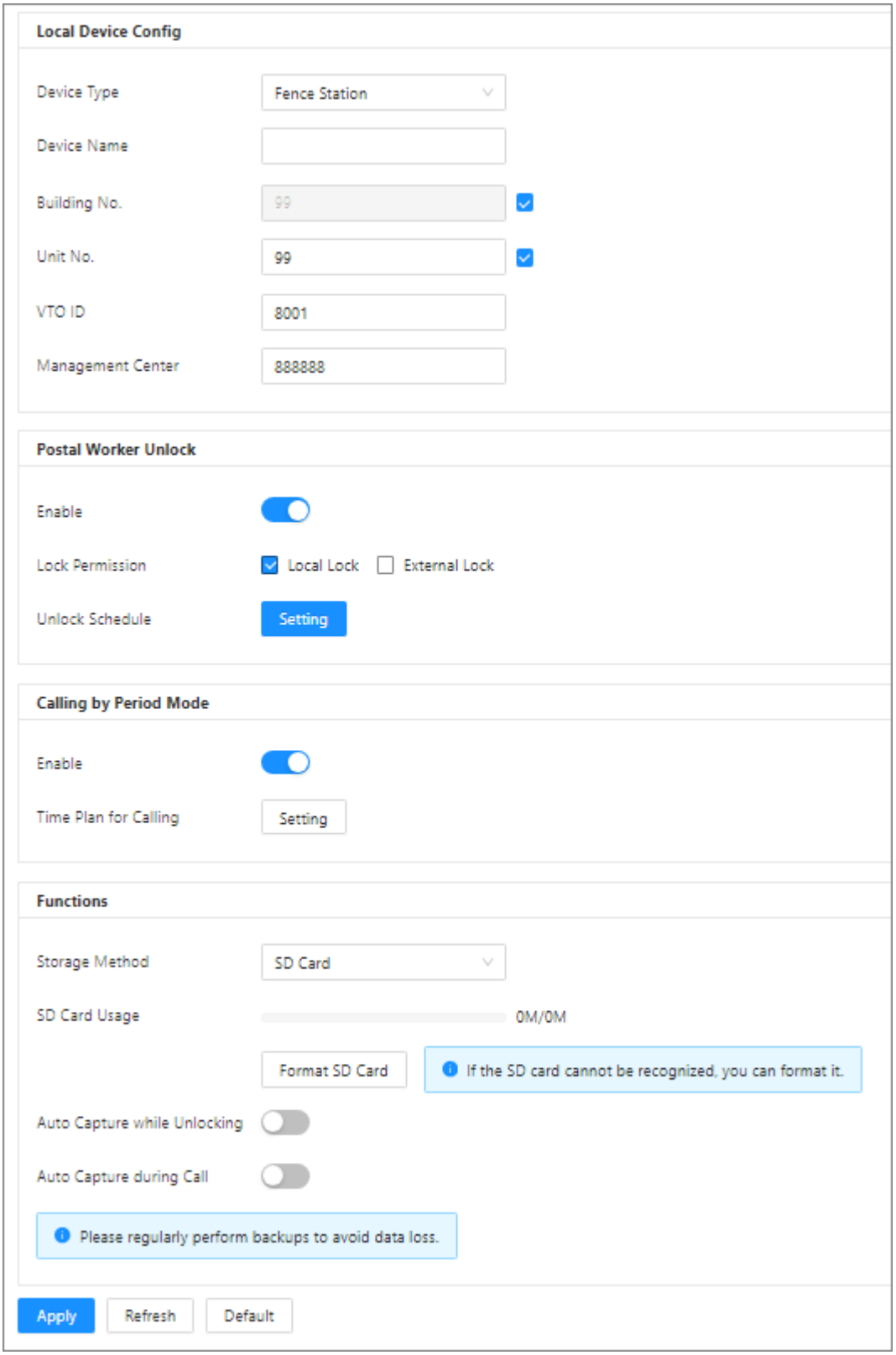


Table 4-4 Basic parameter description

Module	Parameter	Description
Local Device Config	Device Name	When other devices are monitoring this fence station, 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.**, 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.
	Management Center	888888 by default.
Postal Worker Unlock		It is disabled by default. • When it is enabled, select whether local lock or external lock can be open during the set period. • Click **Setting** to configure the unlock schedule during which the postal worker can unlock the door.
Calling by Period Mode		It is disabled by default. When it is enabled, click **Setting** to configure the time plan, during which the calling can be achieved.
Functions	Storage Method	It is 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.

Step 3 Click **Apply**.

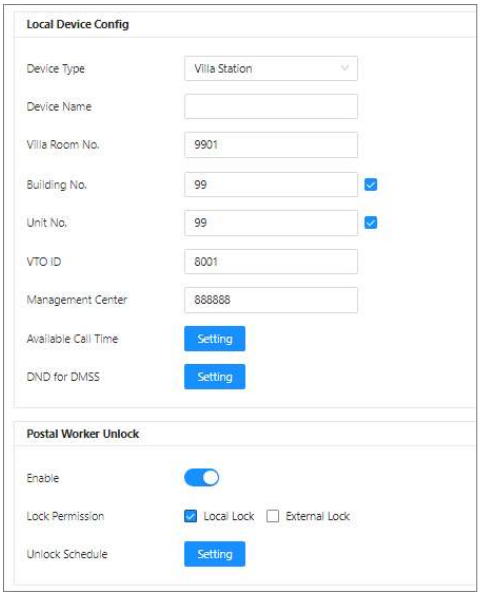
4.7.1.3 Villa Station as Device Type

Procedure

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

Step 2 Select **Villa Station** as **Device Type**, and then configure the parameters.

Figure 4-18 Basic settings



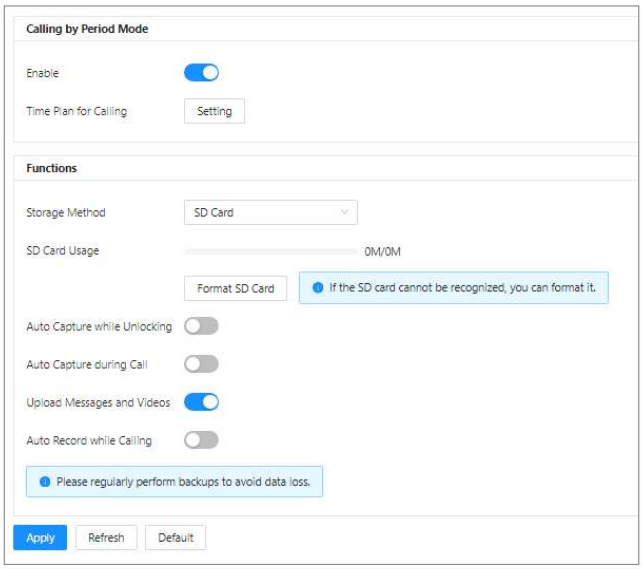


Table 4-5 Basic parameter description

Module	Parameter	Description
Local Device Config	Device Name	When other devices are monitoring this VTO, the device name will appear on the monitoring image.
	Villa Room No.	VTH room number. Used to call VTHs.
	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.
	Management Center	888888 by default.

Module	Parameter	Description
	Available Call Time	The time period during which the VTO's calling to other devices is not limited. Click **Setting** to set the time plan for calling.
	DND for DMSS	The time period during which the calling to DMSS is not limited. Click **Setting** to set the time plan for calling.
Postal Worker Unlock		It is disabled by default. ● When it is enabled, select whether local lock or external lock can be open during the set period. ● Click **Setting** to configure the unlock schedule during which the postal worker can unlock the door.
Calling by Period Mode		● If you enable the **Calling by Period Mode**, the specified number can be called in the specified period and the default number in other period. ● Click **Setting** to set the time plan for calling.
Functions	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 it is enabled, the messages and videos will be saved in the VTH or VTO where the SD card is inserted.
	Auto Record while Calling	Take recording when the VTO is in a call, and save the recording in the SD card of the VTO. ● When the call time is less than 5 seconds, no video file will be generated. ● If there is a conflict between **Auto Record while Calling** and **Leave Videos**, **Leave Videos** prevails.

Step 3 Click **Apply**.

4.7.2 Personalization

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

4.7.2.1 Configuring Personalization

The themes shown vary from different device types. Configure the theme of the device according to the actual needs.

4.7.2.1.1 Unit VTO as Device Type

When the **Unit VTO** is set as device type, there are 4 types of themes you can configure.

Procedure

Step 1 Select **Local Device Config** > **Personalization** > **Personalization**.

Step 2 Select the theme according to the actual needs.

Click each theme, the feature is shown below the theme.

Figure 4-19 Theme 1

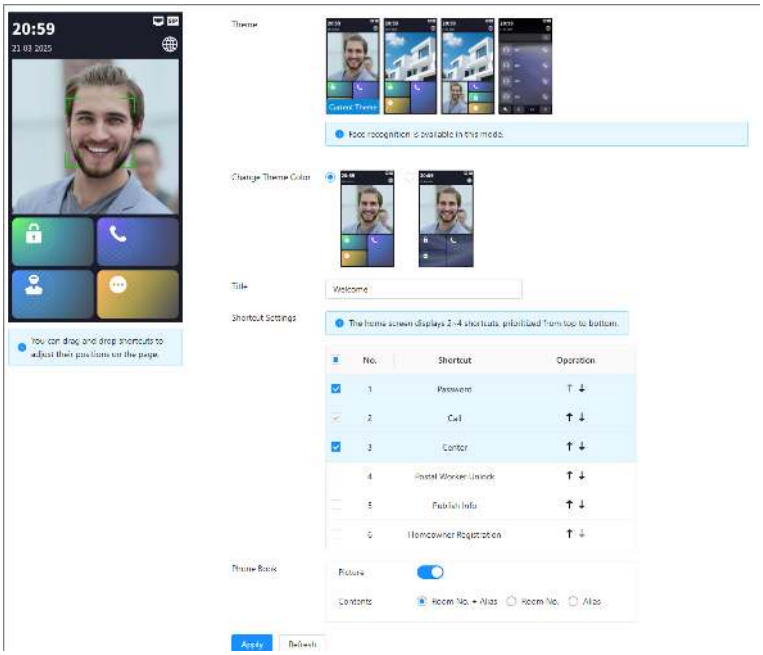


Figure 4-20 Theme 2

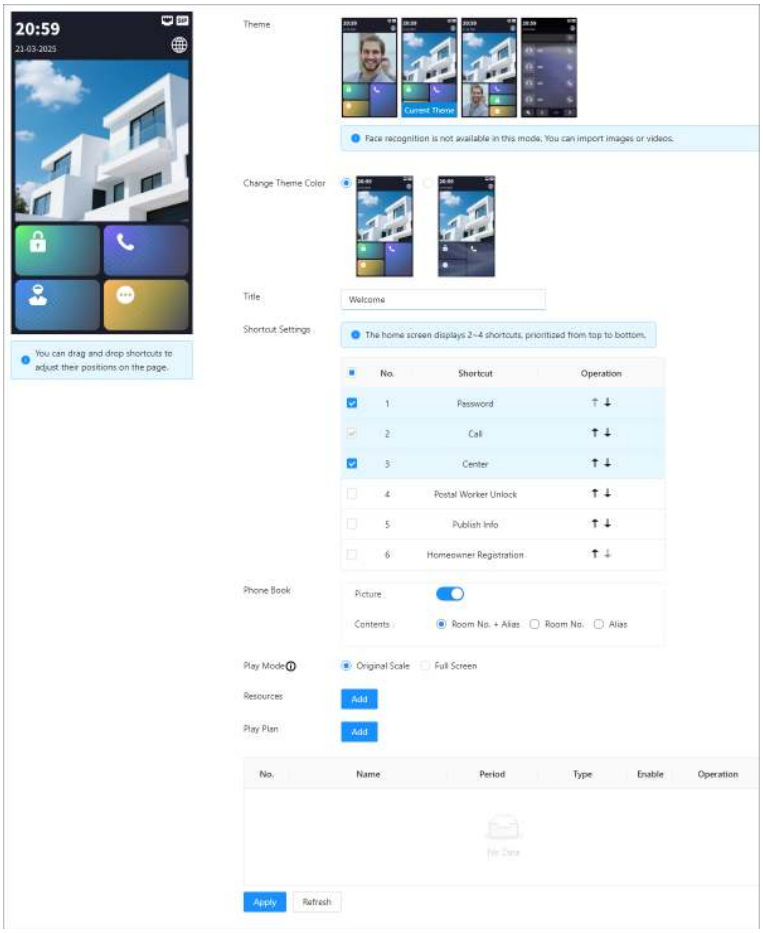


Figure 4-21 Theme 3

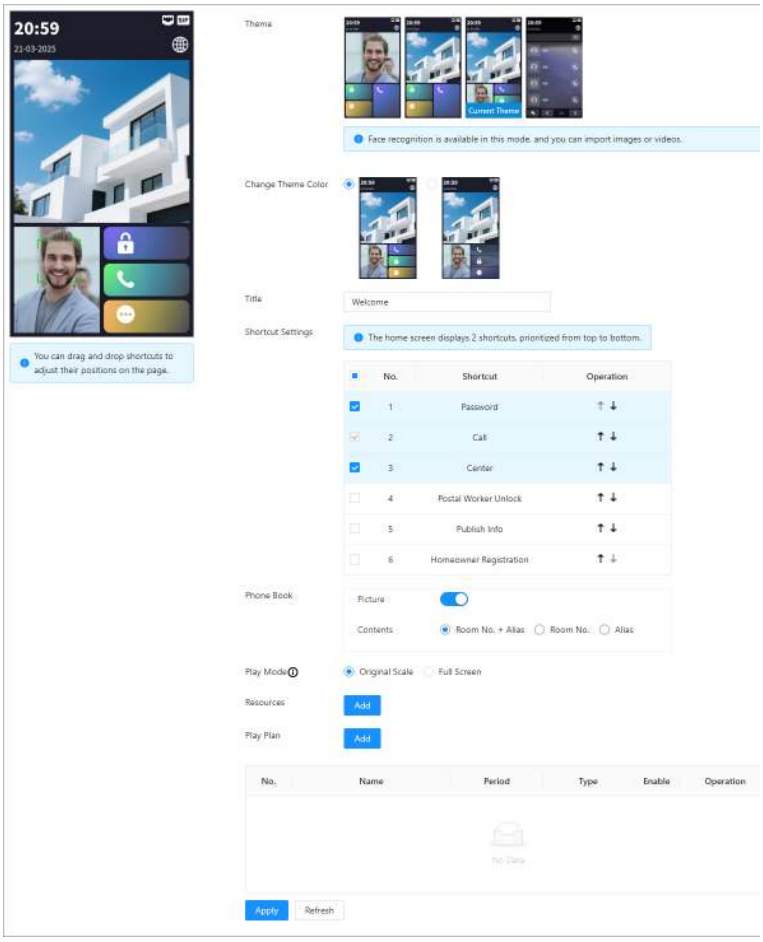


Figure 4-22 Theme 4

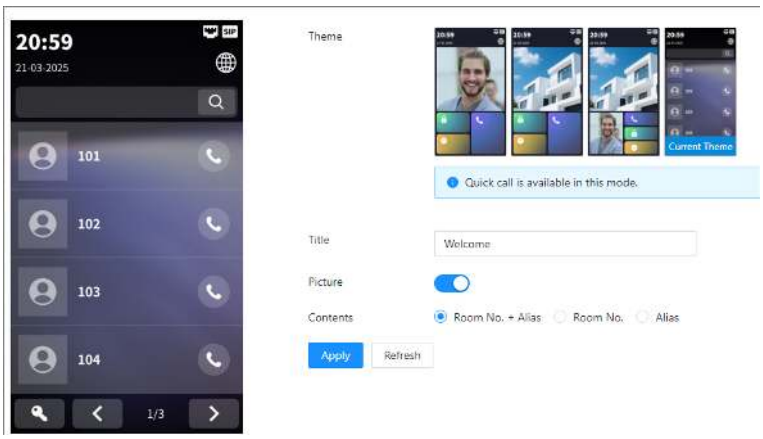
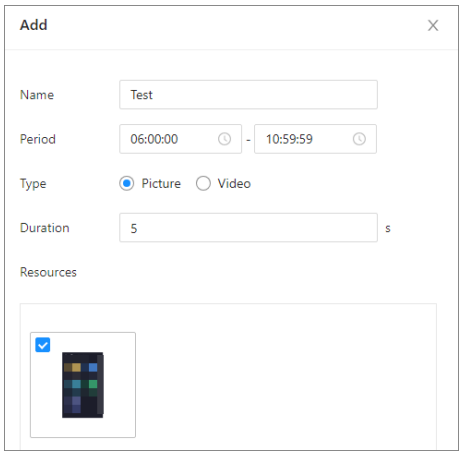


Table 4-6 Personalization

Parameter	Description
Change Theme Color	Select color theme from the 2 themes.
Title	Configure the screen title, which is shown on the home screen of the device.

Parameter	Description
Shortcut Settings	Configure the shortcut of the home screen of the device. ● The home screen displays 2 to 4 shortcuts, prioritized from top to bottom of the list. ● You can drag and drop shortcuts on the home screen to adjust their positions. ● The shortcuts of the and are required and cannot be deleted. And the shortcuts of the cannot be moved.
Button Functions	After it is enabled, you can use one-click machine button on the VTO to make a call. If it is disabled, you will be directed to the keypad. This function is only available on select models.
Phone Book	Personalize the phone book. ● Enable **Picture**, and then the picture of the VTH will be shown in the phone book list. ● Select the displayed contents of the phone book, including Room No. + Alias, Room No., and Alias. The sequence of the VTHs in the phone book is based on the room number.
Play Mode	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.
Resources	Configure the displayed resources as needed. 1. Click **Add**. 2. Select resources type, including picture and video. ● Picture: Click **Upload**, and then select pictures from the local computer. Supports PNG, JPG, and BMP formats. The image size must not exceed 20 MB. ● Video: a. Click **Upload**. b. Click **Click here to download** to download and install the plug-in first. c. Click **Browse**, and then select videos from the local computer. Supports AVI, DAV, and MP4 formats. The video must be less than 100 MB.

Parameter	Description
Play Plan	Configure play plans of the displayed resources as needed. 1. Click **Add**. 2. Enter the plan name. 3. Select the play plan period. 4. Select resource type from **Picture** or **Video**. ● Picture: Configure the play plan duration from 1 second through 20 seconds, and then select the resources configured in the **Resources**. ● Video: Select the resources configured in the **Resources**. 5. Click **OK**. 

Step 3 Click **Apply**.

4.7.2.1.2 Fence Station as Device Type

When the **Fence Station** is set as device type, there are 3 types of themes you can configure.

Procedure

Step 1 Select **Local Device Config** > **Personalization** > **Personalization**.

Step 2 Select the theme according to the actual needs.

Click each theme, the feature is shown below the theme.

Figure 4-23 Theme 1

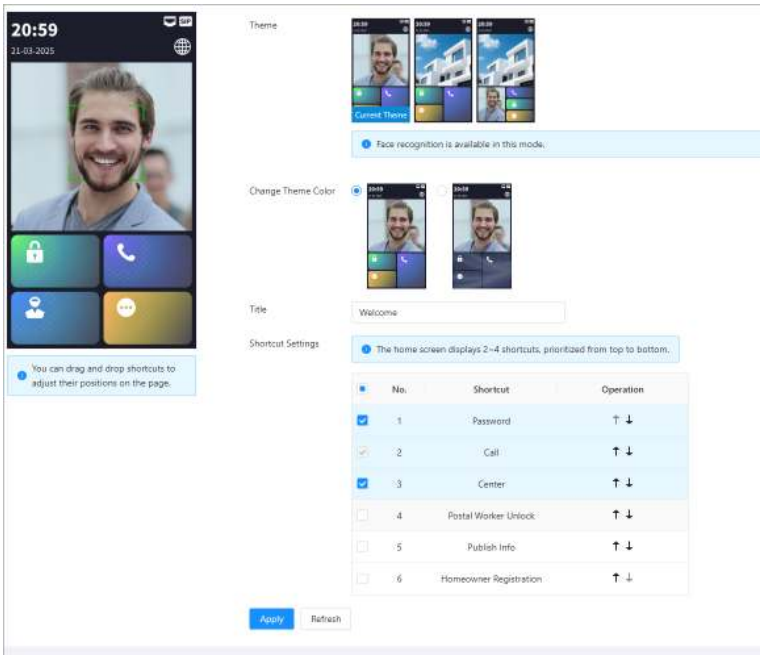


Figure 4-24 Theme 2

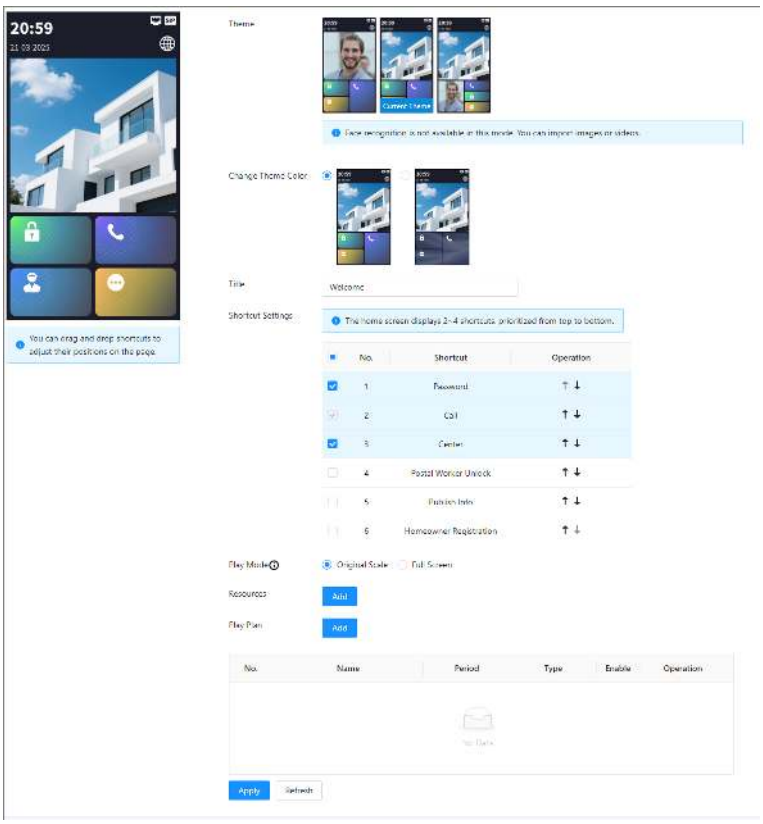


Figure 4-25 Theme 3

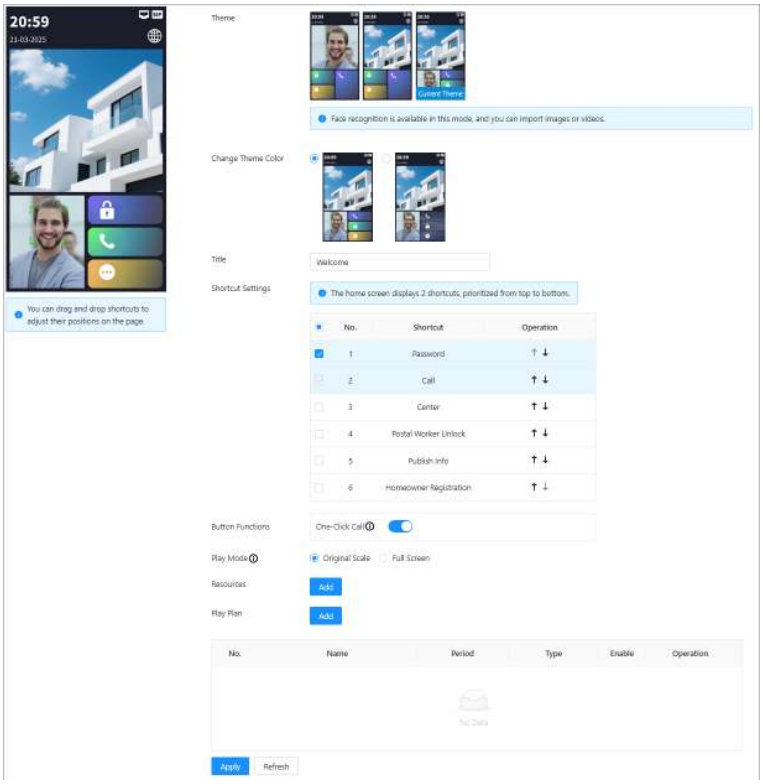
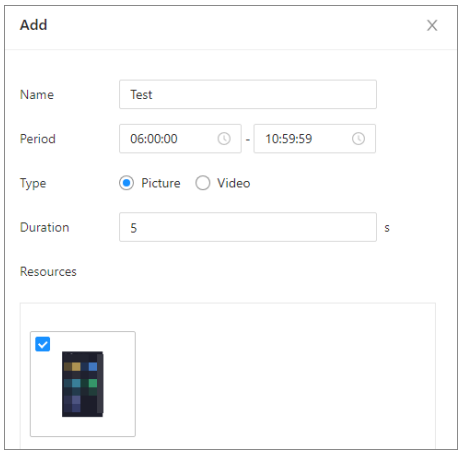


Table 4-7 Personalization

Parameter	Description
Change Theme Color	Select color theme from the 2 themes.
Title	Configure the screen title, which is shown on the home screen of the device.
Shortcut Settings	Configure the shortcut of the home screen of the device. ● The home screen displays 2 to 4 shortcuts, prioritized from top to bottom of the list. ● You can drag and drop shortcuts on the home screen to adjust their positions. ● The shortcuts of the and are required and cannot be deleted. And the shortcuts of the cannot be moved.
Button Functions	After it is enabled, you can use one-click machine button on the VTO to make a call. If it is disabled, you will be directed to the keypad. This function is only available on select models.
Play Mode	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.

Parameter	Description
Resources	Configure the displayed resources as needed. 1. Click **Add**. 2. Select resources type, including picture and video. ● Picture: Click **Upload**, and then select pictures from the local computer. Supports PNG, JPG, and BMP formats. The image size must not exceed 20 MB. ● Video: a. Click **Upload**. b. Click **Click here to download** to download and install the plug-in first. c. Click **Browse**, and then select videos from the local computer. Supports AVI, DAV, and MP4 formats. The video must be less than 100 MB.
Play Plan	Configure play plans of the displayed resources as needed. 1. Click **Add**. 2. Enter the plan name. 3. Select the play plan period. 4. Select resource type from **Picture** or **Video**. ● Picture: Configure the play plan duration from 1 second through 20 seconds, and then select the resources configured in the **Resources**. ● Video: Select the resources configured in the **Resources**. 5. Click **OK**. 

Step 3 Click **Apply**.

4.7.2.1.3 Villa Station as Device Type

When the **Villa Station** is set as device type, there are 4 types of themes you can configure.

Procedure

Step 1 Select **Local Device Config** > **Personalization** > **Personalization**.

Step 2 Select the theme according to the actual needs.

Click each theme, the feature is shown below the theme.

Figure 4-26 Theme 1

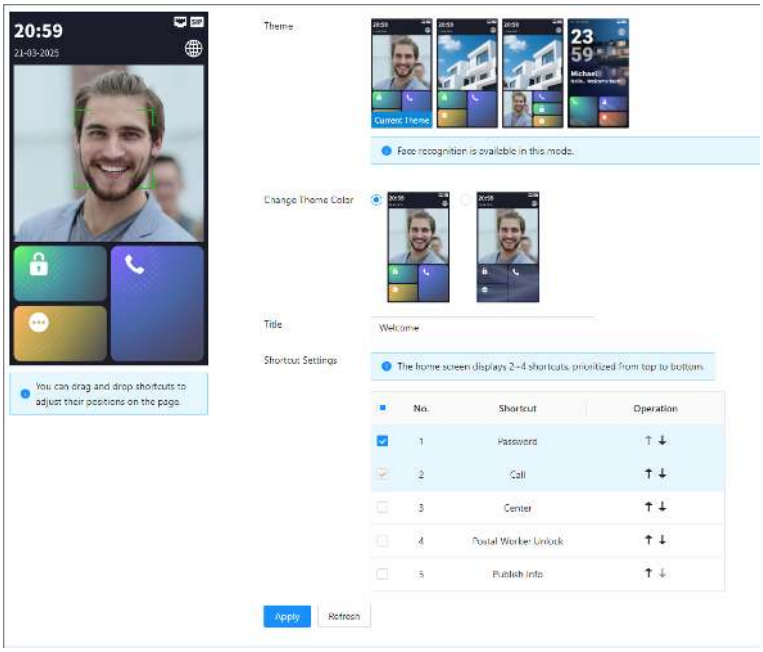


Figure 4-27 Theme 2

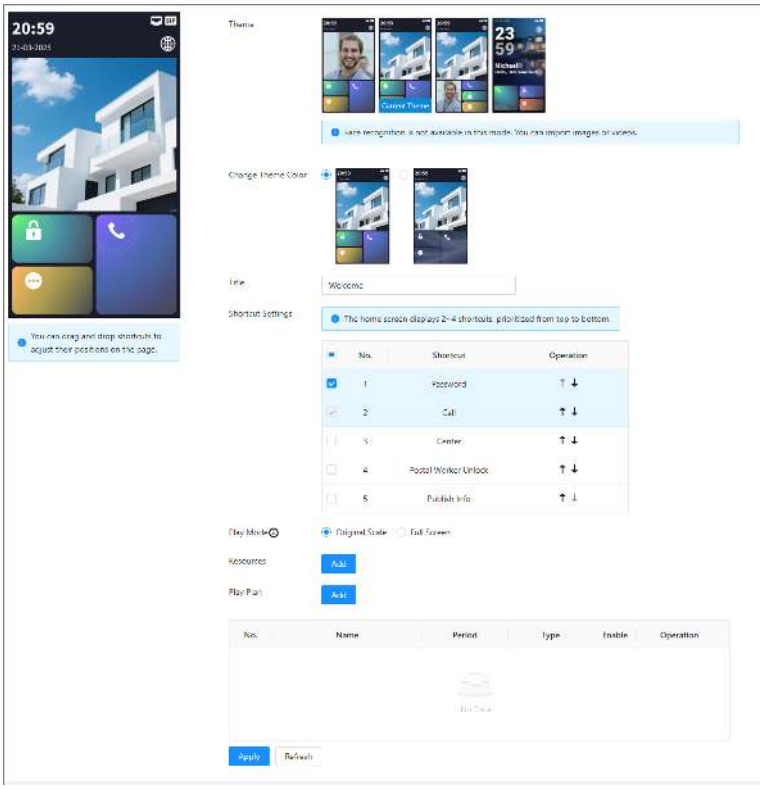


Figure 4-28 Theme 3

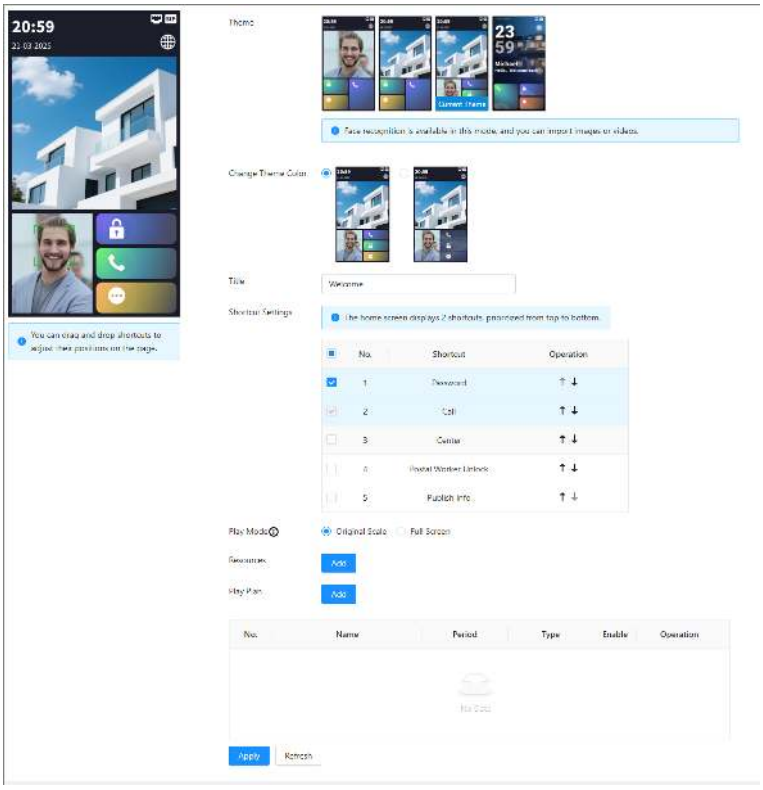


Figure 4-29 Theme 4

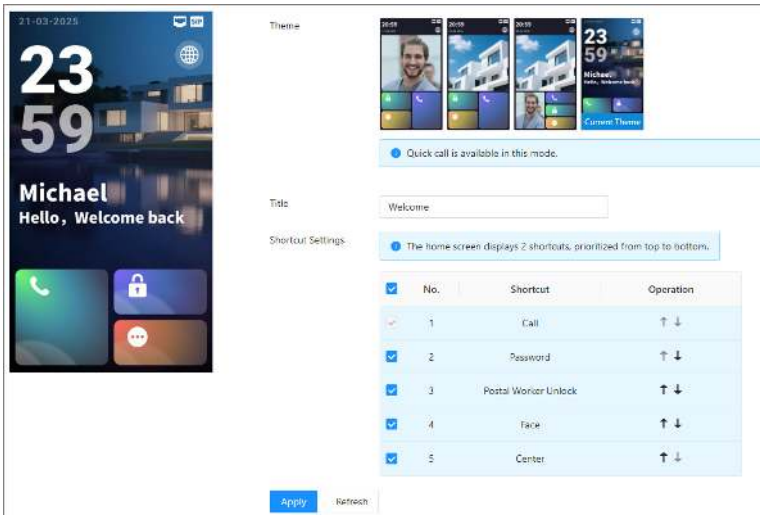
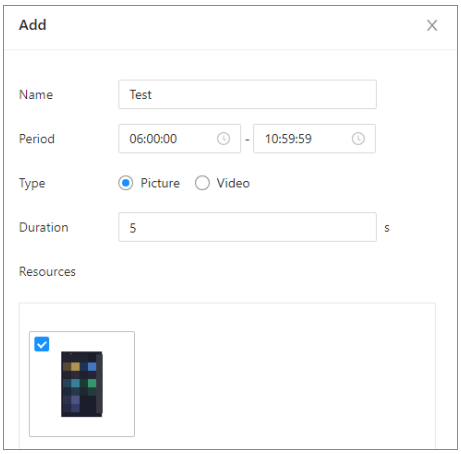


Table 4-8 Personalization

Parameter	Description
Change Theme Color	Select color theme from the 2 themes.
Title	Configure the screen title, which is shown on the home screen of the device.
Shortcut Settings	Configure the shortcut of the home screen of the device. ● The home screen displays 2 to 4 shortcuts, prioritized from top to bottom of the list. ● You can drag and drop shortcuts on the home screen to adjust their positions. ● The shortcuts of the and are required and cannot be deleted. And the shortcuts of the cannot be moved.
Button Functions	After it is enabled, you can use one-click machine button on the VTO to make a call. If it is disabled, you will be directed to the keypad. This function is only available on select models.
Play Mode	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.

Parameter	Description
Resources	Configure the displayed resources as needed. 1. Click **Add**. 2. Select resources type, including picture and video. ● Picture: Click **Upload**, and then select pictures from the local computer. Supports PNG, JPG, and BMP formats. The image size must not exceed 20 MB. ● Video: a. Click **Upload**. b. Click **Click here to download** to download and install the plug-in first. c. Click **Browse**, and then select videos from the local computer. Supports AVI, DAV, and MP4 formats. The video must be less than 100 MB.
Play Plan	Configure play plans of the displayed resources as needed. 1. Click **Add**. 2. Enter the plan name. 3. Select the play plan period. 4. Select resource type from **Picture** or **Video**. ● Picture: Configure the play plan duration from 1 second through 20 seconds, and then select the resources configured in the **Resources**. ● Video: Select the resources configured in the **Resources**. 5. Click **OK**. 

Step 3 Click **Apply**.

4.7.2.2 Configuring Notifications

Prerequisites

Set the VTO as the SIP server. For details, see "4.4.1 Setting as SIP Server".

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Local Device Config** > **Personalization** > **Publish Info**.

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

Figure 4-30 Configure the notification

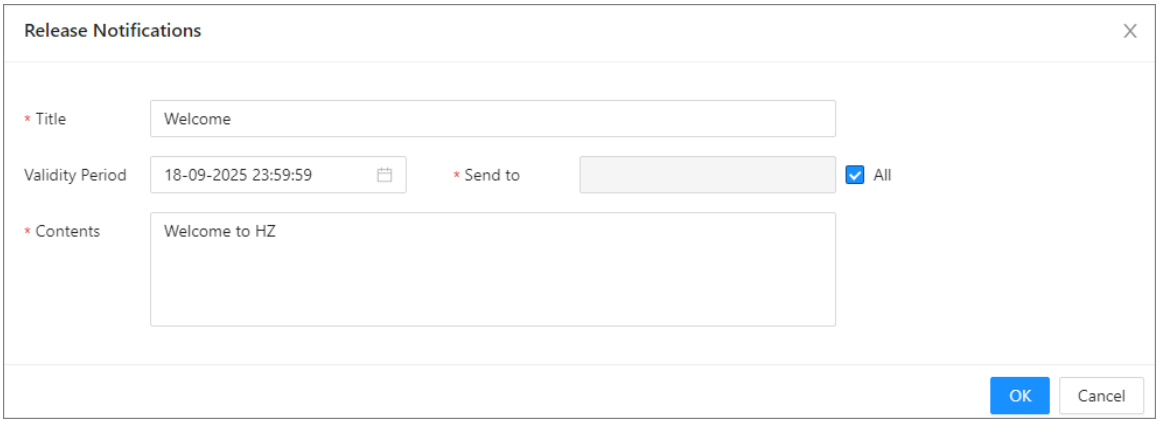


Table 4-9 Description of announcement parameters

Parameter	Description
Title	The title of the announcement.
Validity Period	Configure the validity period. All door stations that are online within the validity period can 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**.

4.7.3 Configuring Access Control

4.7.3.1 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 4-31 Access control

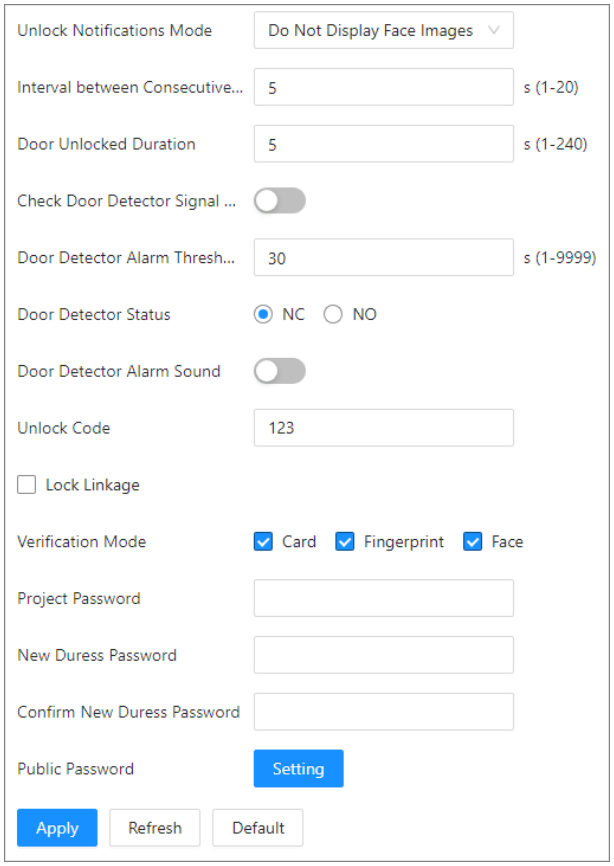


Table 4-10 Access control parameter description

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.

Parameter	Description
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.
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	
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**.

4.7.3.2 Configuring Extension Functions

4.7.3.2.1 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 4-32 RS-485

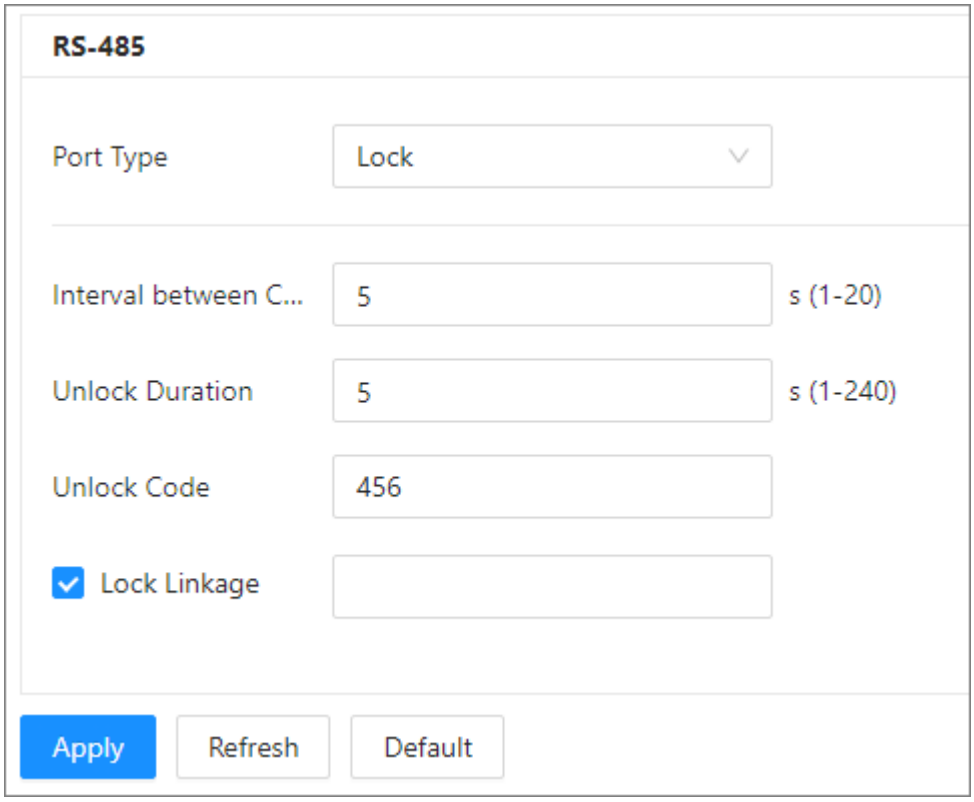


Table 4-11 RS-485 description

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	After configuring the unlock code, you can enter the unlock code on the authorized devices to accessing or controlling the VTO through the RS-485.
Lock Linkage	Enable the **Lock Linkage** , and then you can select the **Local 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) cannot 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.

4.7.3.2.2 Network Lift Control

The lock can be connected to the 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 4-33 Network lift control

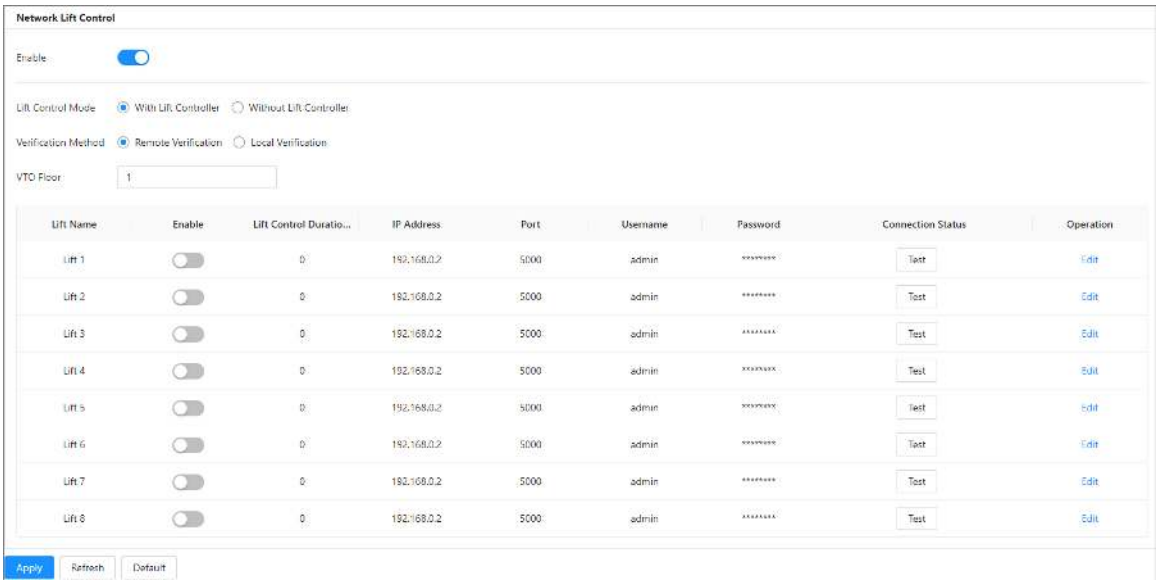


Table 4-12 Network lift control description

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 4-34 Set lift information

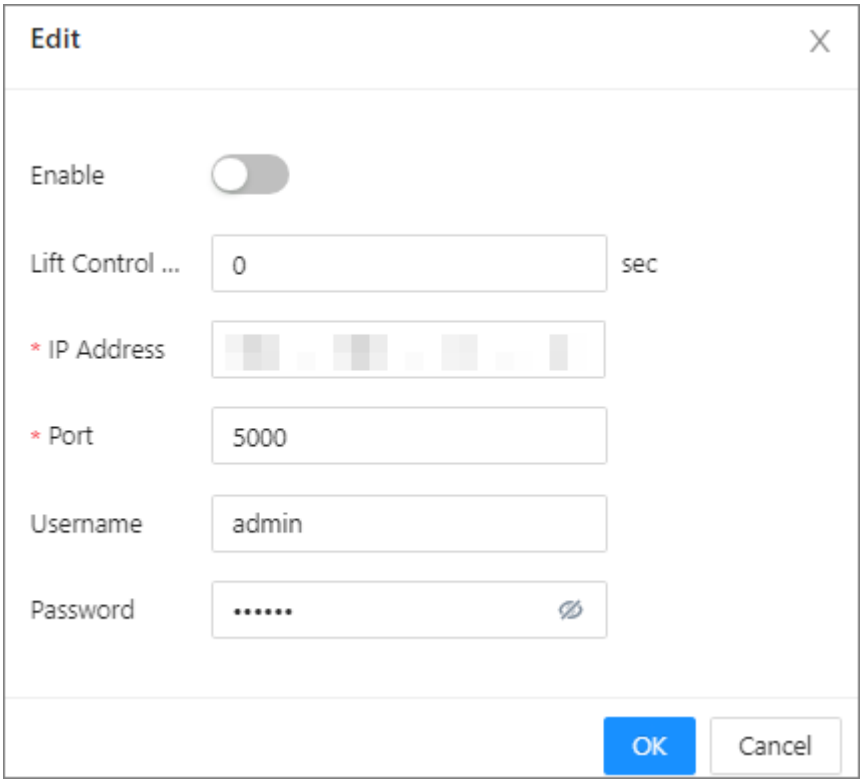


Table 4-13 Network lift control description

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

Step 5 Click **Apply**.

Related Operations

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

4.7.4 Configuring Light Control

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**.

4.7.5 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 get the IPC information.

- Supports adding the IPC devices with up to 32 channels.
- Supports directly adding IPC devices. You can also get the IPC channel by adding NVR.

4.7.5.1 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**.

Step 3 Select one of the IPC channel, and then click to configure the parameters.

Figure 4-35 Configure the parameters

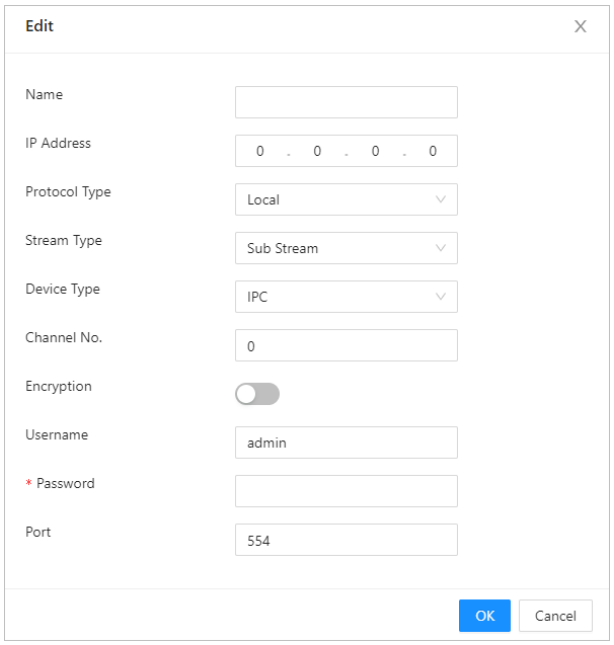


Table 4-14 Parameters description of the video monitoring device

Parameter	Description
Name	Enter the name of the IPC device.
IP Address	Enter the IP address of the IPC device.
Protocol Type	Select from **Local** and **ONVIF** according to the IPC device you added.
Stream Type	Select from **Main Stream** and **Sub Stream**.

Parameter	Description
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, it is the channel number of IPC that was configured on the VNR device.
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 device.
Password	
Port	The value is 554 by default.

Step 4 Click **OK**.

4.7.5.2 Importing the IPC Information in Batches

Import the IPC information to the system.

Procedure

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

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**.

The imported database will overwrite the original database.

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

4.7.6 Configuring Cards

Procedure

Step 1 Log in to the webpage.

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

Figure 4-36 Card settings

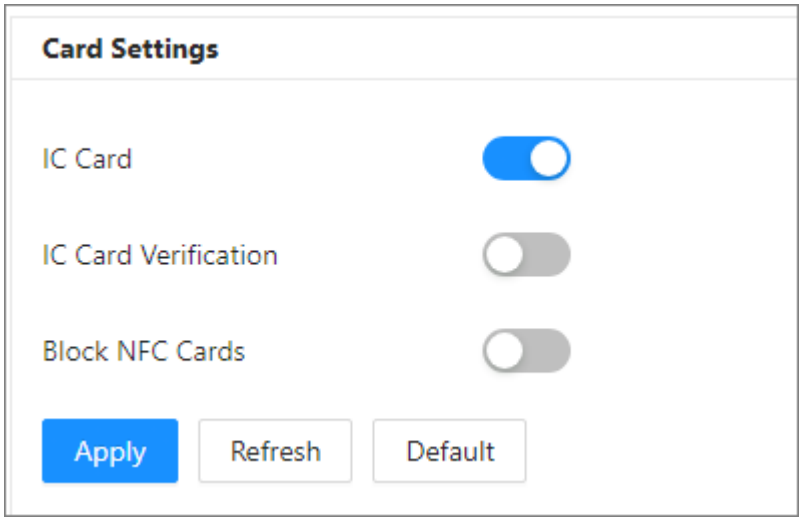


Table 4-15 Description of card parameters

Parameter	Description
IC Card	When enabled, IC card can be used to unlock the door.
IC Card Verification	When enabled, the IC card is encrypted. Swipe the right card with successful encryption detection to unlock the door.
Block NFC Cards	After it is enabled, the copied NFC cards cannot unlock the door.

4.7.7 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 4-37 Wiegand input

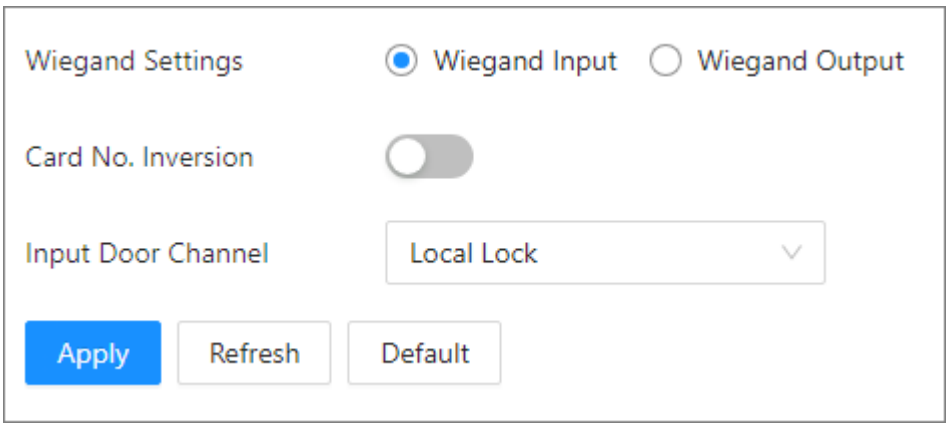


Figure 4-38 Wiegand output

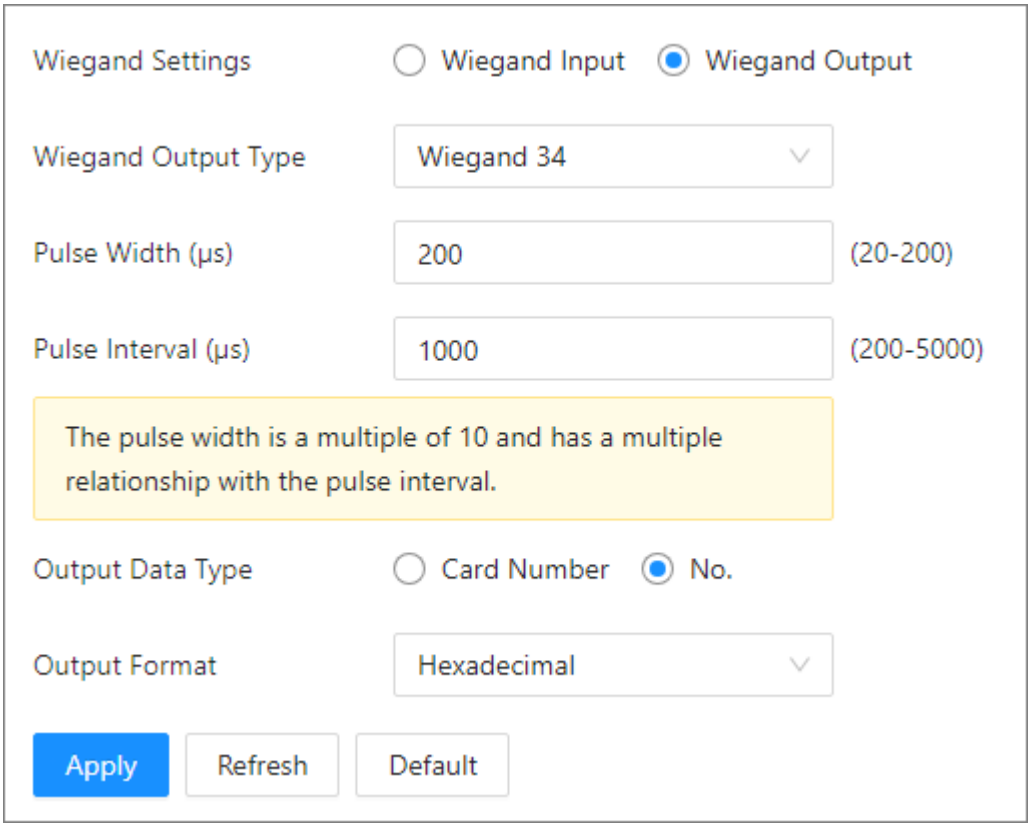


Table 4-16 Description of Wiegand parameters

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	

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

Step 4 Click **Apply**.

4.7.8 Configuring Face Detection

Configure the threshold, detection angle and other parameters.

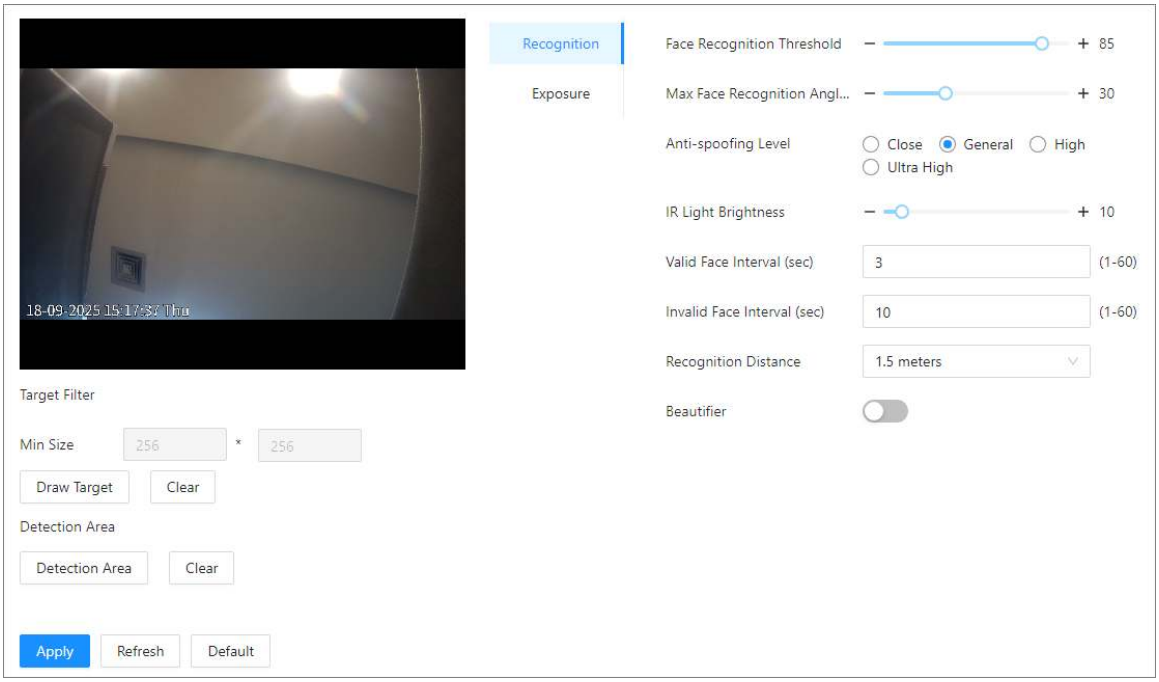
The face detection is available on select models.

Procedure

Step 1 Log in to the webpage.

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

Figure 4-39 Face detection parameters



Step 3 Configure the recognition parameters.

Table 4-17 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.
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 VTO 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 VTO 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 4-40 Exposure parameters

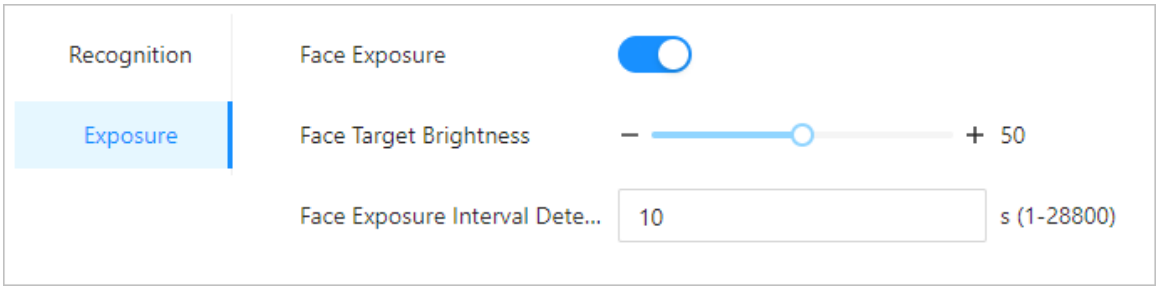


Table 4-18 Exposure parameters description

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. 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**.

4.7.9 Configuring QR Code

Procedure

Step 1 Log in to the webpage.

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

Figure 4-41 QR code

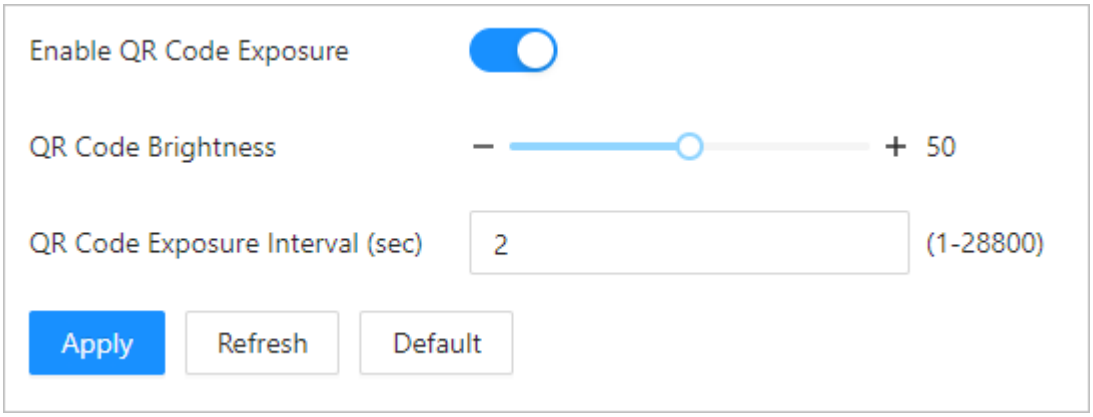


Table 4-19 QR code parameters

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**.

4.7.10 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 4-42 Configure the fingerprint parameter

Step 4 Click **Apply**.

4.8 Device Setting

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

4.8.1 Adding the VTO

Prerequisites

The SIP server must be added.

Procedure

Step 1 Log in to the webpage of the VTO.

Step 2 Click **Device Setting**.

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

Figure 4-43 Add a VTO

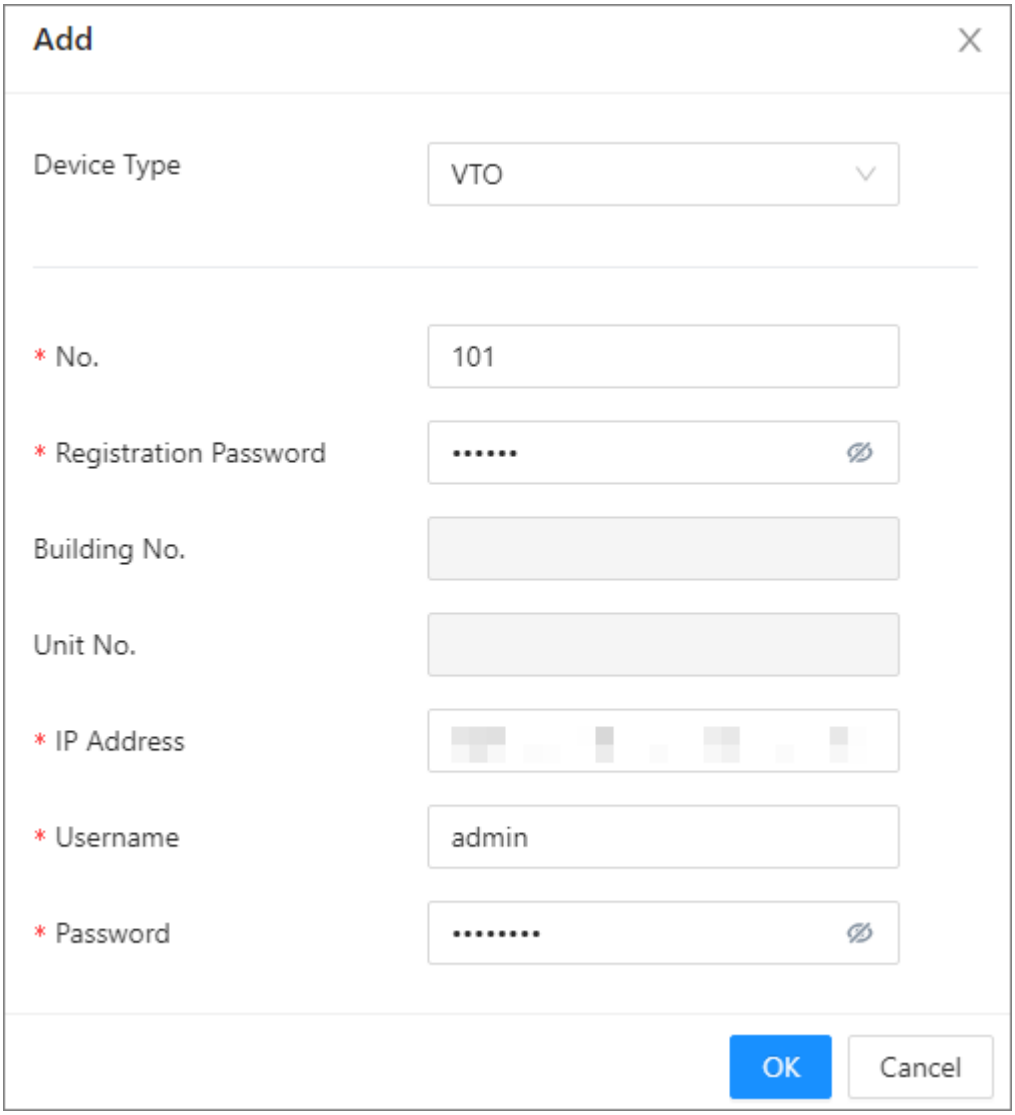


Table 4-20 VTO parameters description

Parameter	Description
No.	VTO number.
Registration Password	Keep it as default.
Building No.	Cannot be edited.
Unit No.	
IP Address	VTO IP address.
Username	The user name and password used to log in to 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.

4.8.2 Adding the VTH

Prerequisites

The SIP server must be added.

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.

Figure 4-44 Add a VTH

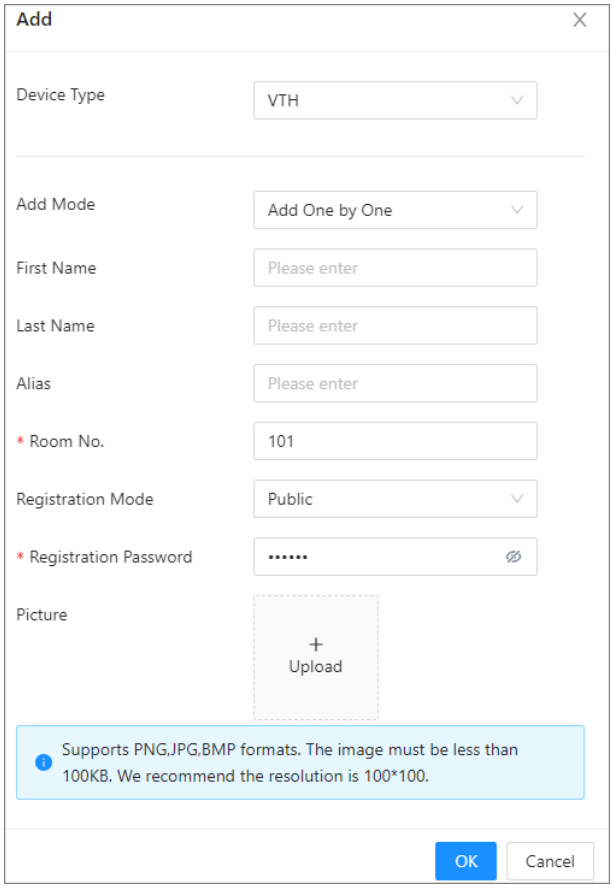


Table 4-21 VTH parameters description

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	

Parameter	Description
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.
Picture	Click **Upload** to upload the picture of the VTH. This function is available only when the **Add Mode** is **Add One by One**.

Step 4 Click **OK**.

Related Operations

- Click to edit the VTH.
- Click to delete added VTHs.
- Click to call the VTH.

4.8.3 Adding the VTS

Prerequisites

The SIP server must be added.

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.

Figure 4-45 Add a VTS

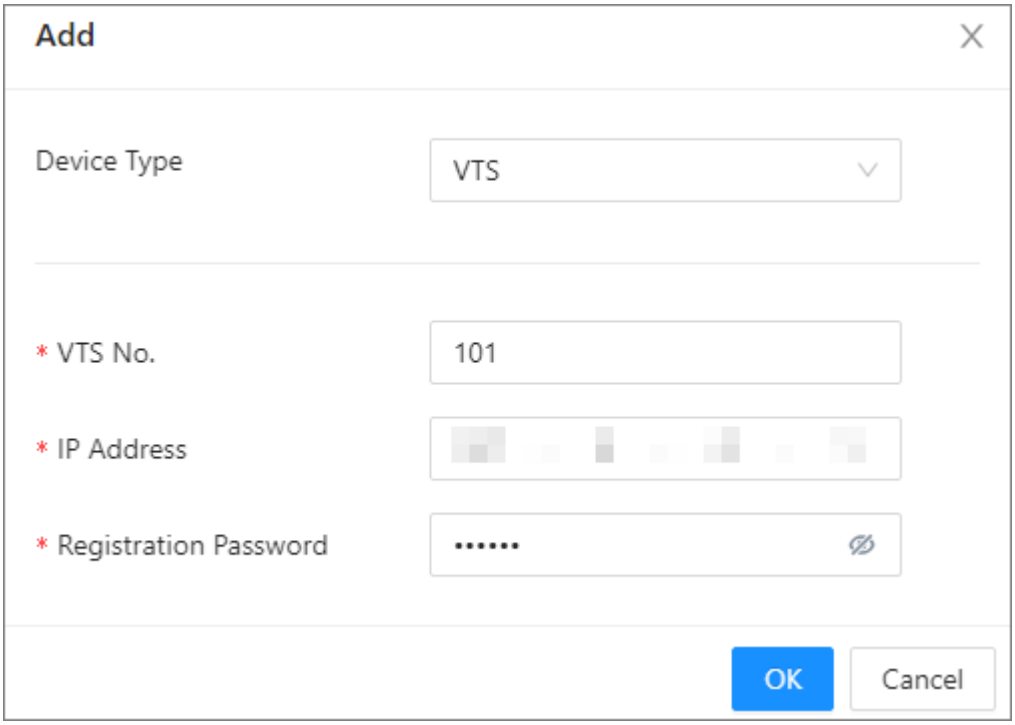


Table 4-22 VTS parameters description

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**.

4.8.4 Related Operations

Figure 4-46 Device list

Exporting Device Information

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

All device information except VTH picture is saved in your local computer.

Importing 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.

Batch Importing Images

Import images of the VTHs in batches. Prepare the images in the .zip format and name them in the room number.

1. Select **Device Setting**.
2. Click **Batch Import Images** , and then click **OK**.
3. Select the zip file to upload, and then the images will be displayed according to the VTH number.

Offline Device Configuration

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.

4.9 Person Management

The card and fingerprint information 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**.

Step 3 Click **Add**.

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

Figure 4-47 Add the person

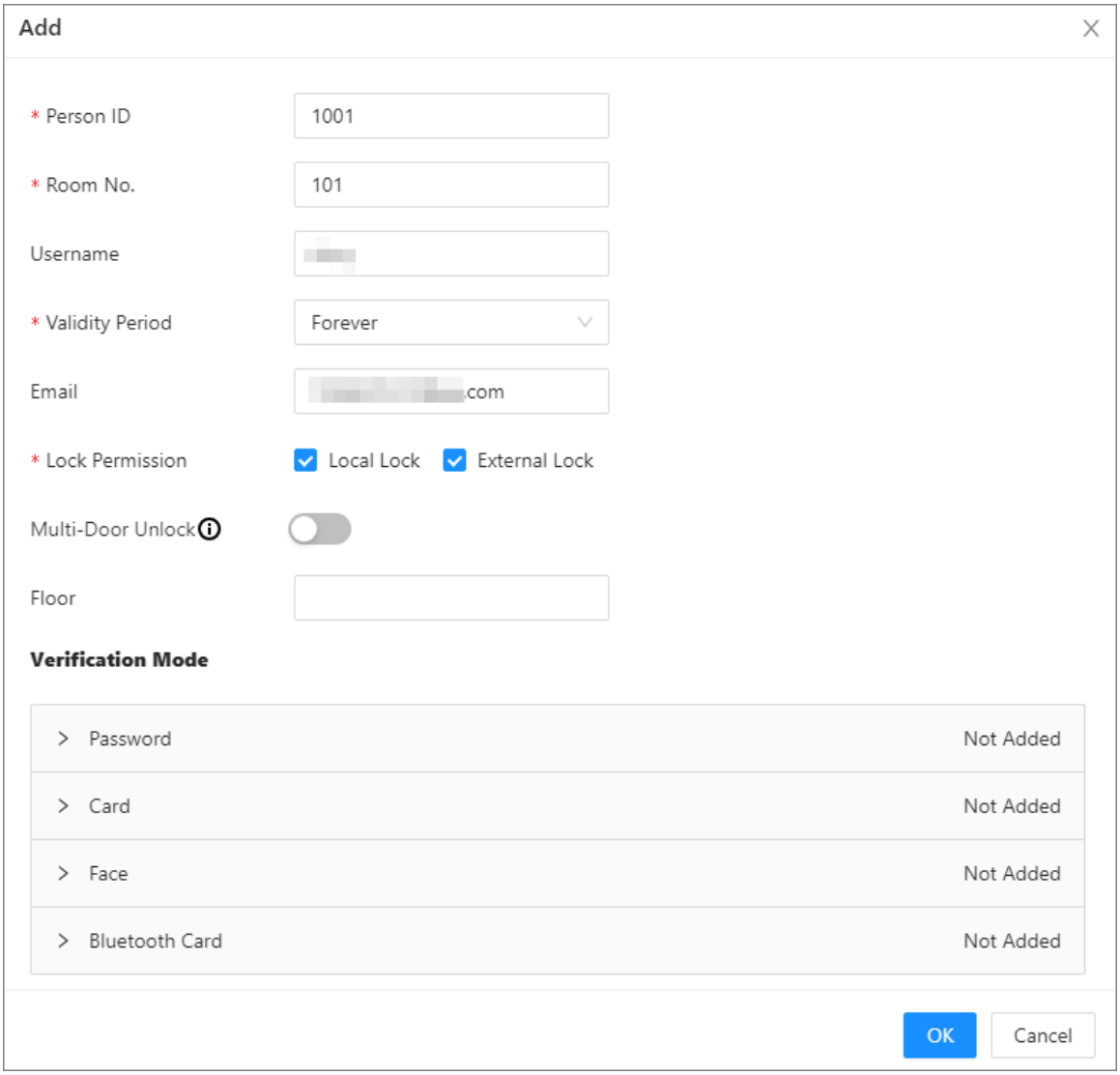


Table 4-23 Person parameters description

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.
Email	Configure the Email address so that you can request a Bluetooth card through the reserved Email.
Lock Permission	Set the lock permission. You can enable the permission for local lock and external lock at the same time.

Parameter	Description
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.
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. Click **Modify** to select the acquisition device from **Enrollment Reader** or **Device**. 3. Enter the card number. Or you can click **Issue Card**, and then swipe the card over VTO. 4. Enter the name of the card. 5. Click **OK**. You can manage the cards through the following icons. ● : 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	This function is only available on select models. 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 might 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.
Bluetooth	Click **Bluetooth** to configure the function. This function is only available on select models. • Request through Email: Suitable for the first time a Bluetooth card is requested. 1. Configure the Email that is registered to DMSS. 2. Click **Request through Email**, and then the Bluetooth cards can be requested. You can request up to 5 Bluetooth cards. • Request through Registration Code: Suitable when you have a Bluetooth card and need to add it with a registration code. 1. Copy the Bluetooth registration code from the DMSS. 2. Click **Request through Registration Code**, and then enter the code. 3. Click **OK**.

Related Operations

- Click **Export Person**, and then you can export the person file of the VTO1 to the local computer.

  On the webpage of VTO2, click **Import Person**, and then select the person file exported from the VTO1 to import the person to the VTO2 in batches.
- Select users and then click **Issue Cards to Selected Users** or click **Issue Cards to All Users**.
  - ◇ On **Requestable** tab, you can view all users who can be issued Bluetooth cards, and then click **Request through Email** to issue Bluetooth card in batches.

- Bluetooth cards can only be generated in batches through emails.
- Cloud service should be online.

◇ On **Non-Requestable** tab, you can view users without Email who cannot be issued cards.

- Click **Export Users that Lack Emails** to download the user list on the local compute, and then enter the Email.
- Click **Import** to import the user list so that you can issue card to them.

- Click **Bluetooth Cards Records**, and then you can view the Bluetooth card records. For users who issued cards unsuccessfully, you can reissue cards here.
- Click to edit the person information.
- Click to delete the person information.

4.10 Network Settings

4.10.1 Configuring TCP/IP

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 4-48 TCP/IP

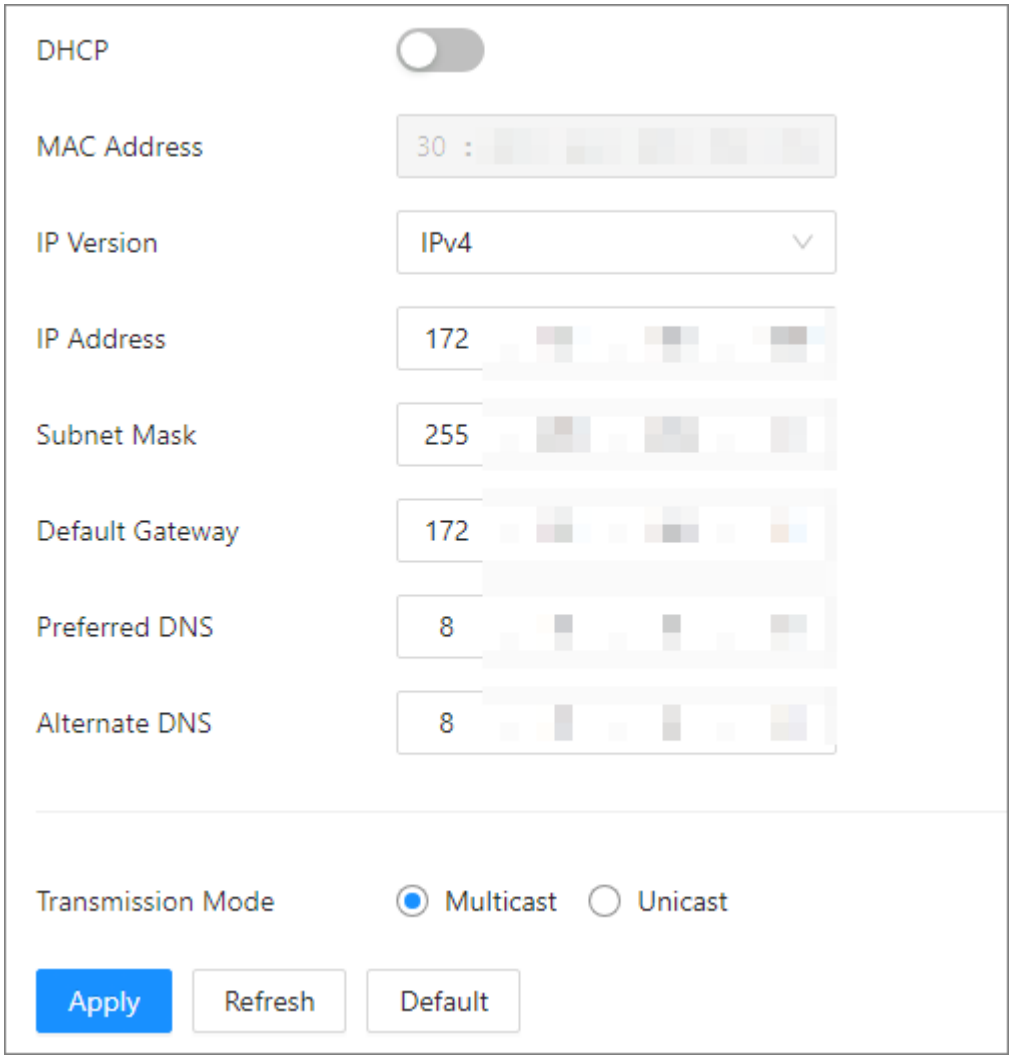


Table 4-24 Description of TCP/IP parameters

Parameter	Description
DHCP	DHCP stands for Dynamic Host Configuration Protocol. ● When it is not enabled, you can 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 the **DHCP** is not enabled, 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**.

4.10.2 Configuring Port

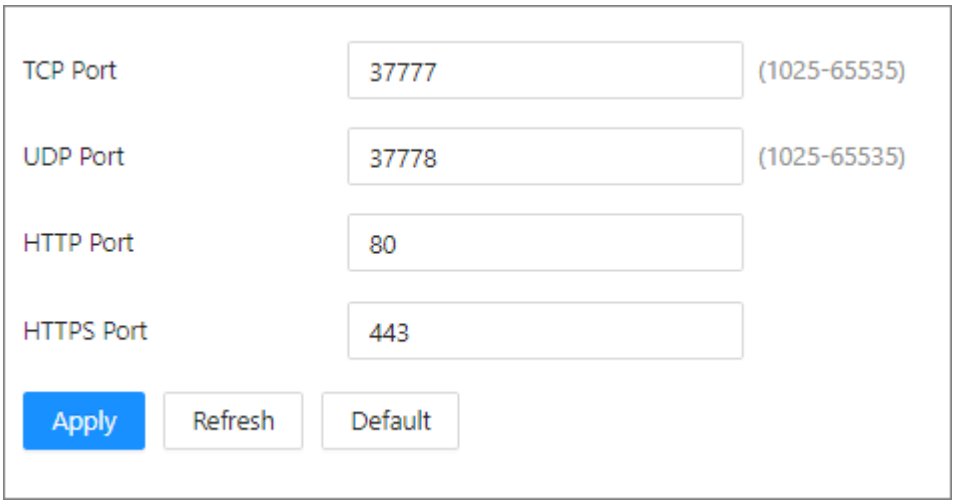
You can limit access to the Device at the same time through webpage, desktop client and mobile client.

Procedure

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

Step 2 Configure the ports.

Figure 4-49 Ports



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

Table 4-25 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**.

4.10.3 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.

4.10.3.1 VTO as the SIP Server

Procedure

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

Step 2 Set the VTO as the SIP Server.

- If the current VTO works as the SIP server, enable **Local SIP Server**, and then configure the parameters.

Figure 4-50 Current VTO as the SIP server

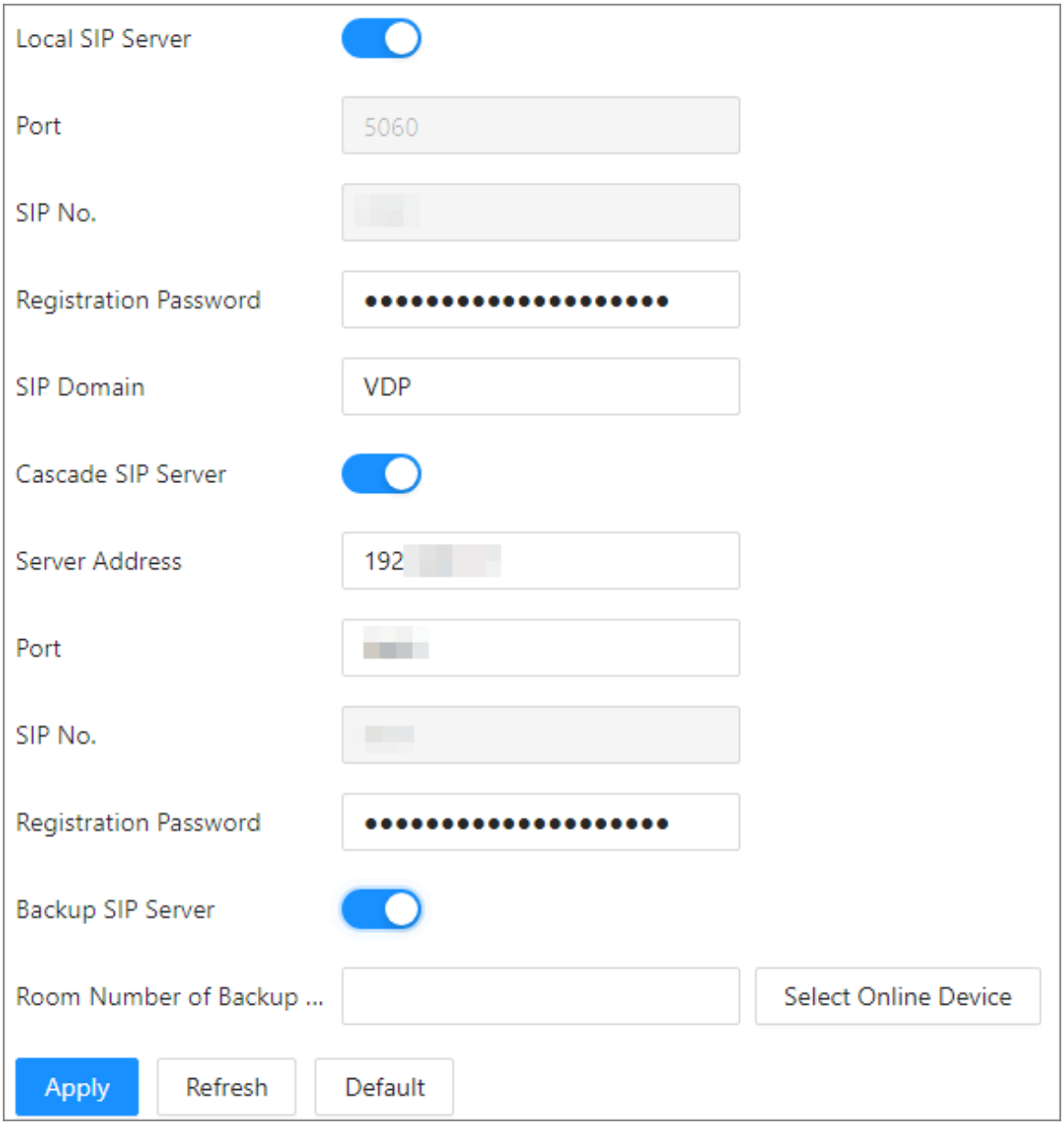


Table 4-26 SIP server configuration

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.
Cascade SIP Server	Enable the cascade SIP server, and then enter the address, port, SIP No., registration password, the user name and password of the cascade SIP server.
Server Address	
Port	
SIP No.	

Parameter	Description
Registration 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	

- If other VTO works as the SIP server, set **Device** as **Server Type**, and then configure the parameters.

Figure 4-51 Other VTO as the SIP server

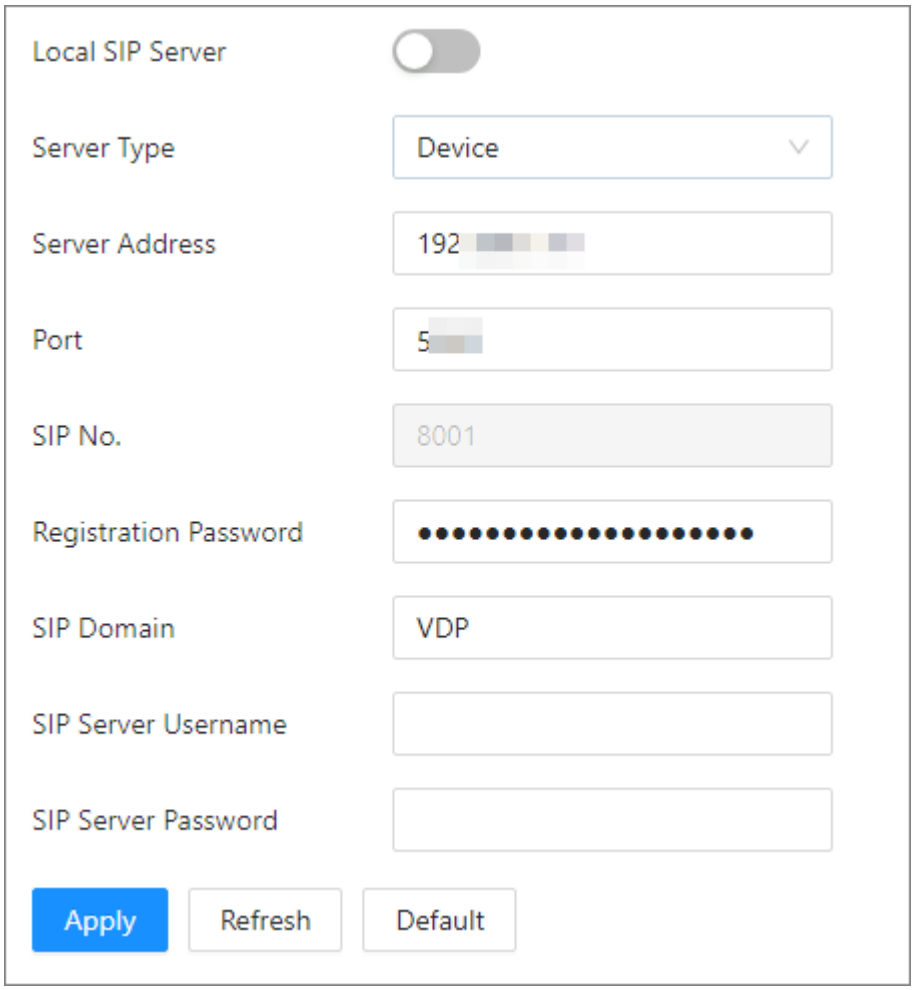


Table 4-27 SIP server configuration

Parameter	Description
Server Address	Enter the IP address of the device that servers as the SIP server.
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.
SIP Server Username	Enter the user name and the password of the device that servers as the SIP server.
SIP Server Password	

Step 3 Click **Apply**.

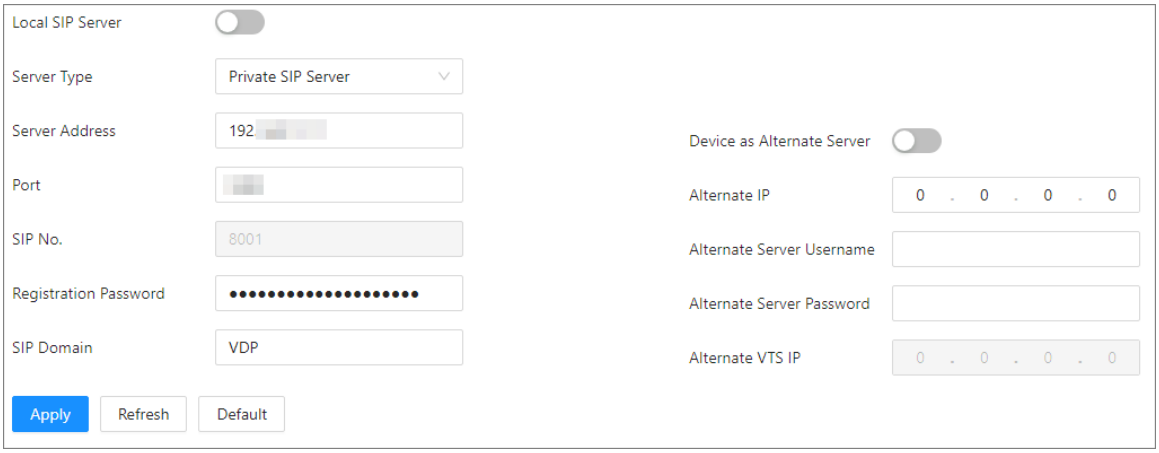
4.10.3.2 Platform as the SIP Server

Procedure

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

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

Figure 4-52 Platform as the SIP server



Step 3 Configure the parameters.

Table 4-28 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 No.	Keep default value VDP or leave it empty.
Registration Password	
SIP Domain	
Alternate IP	The alternate server will be used as the SIP server when DSS Express/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 to serve as the alternate server, you need to enter the IP address of that VTO in the **Alternate IP** . Do not enable **Alternate Server** in this case.
Alternate Server Username	Used to log in to the alternate server.
Alternate Server Password	
Alternate VTS IP	IP address of the alternate VTS.

Step 4 Click **Apply**.

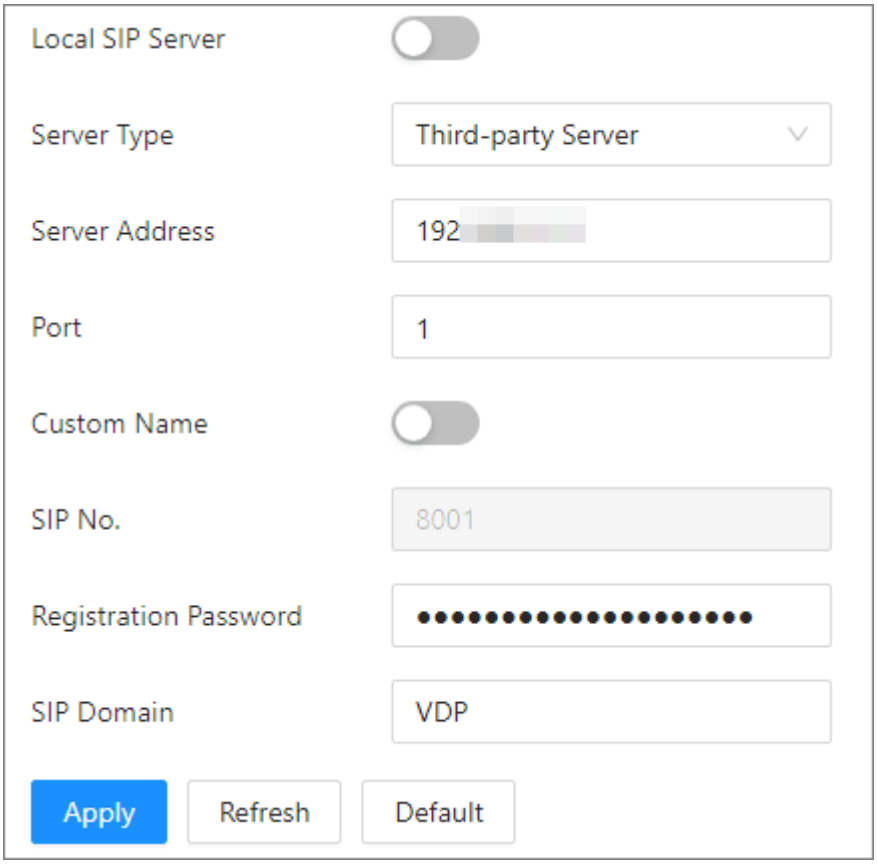
4.10.3.3 Configuring Third-Party Server

Procedure

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

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

Figure 4-53 Third-party server



Step 3 Configure the parameters.

Table 4-29 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.

4.10.4 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.

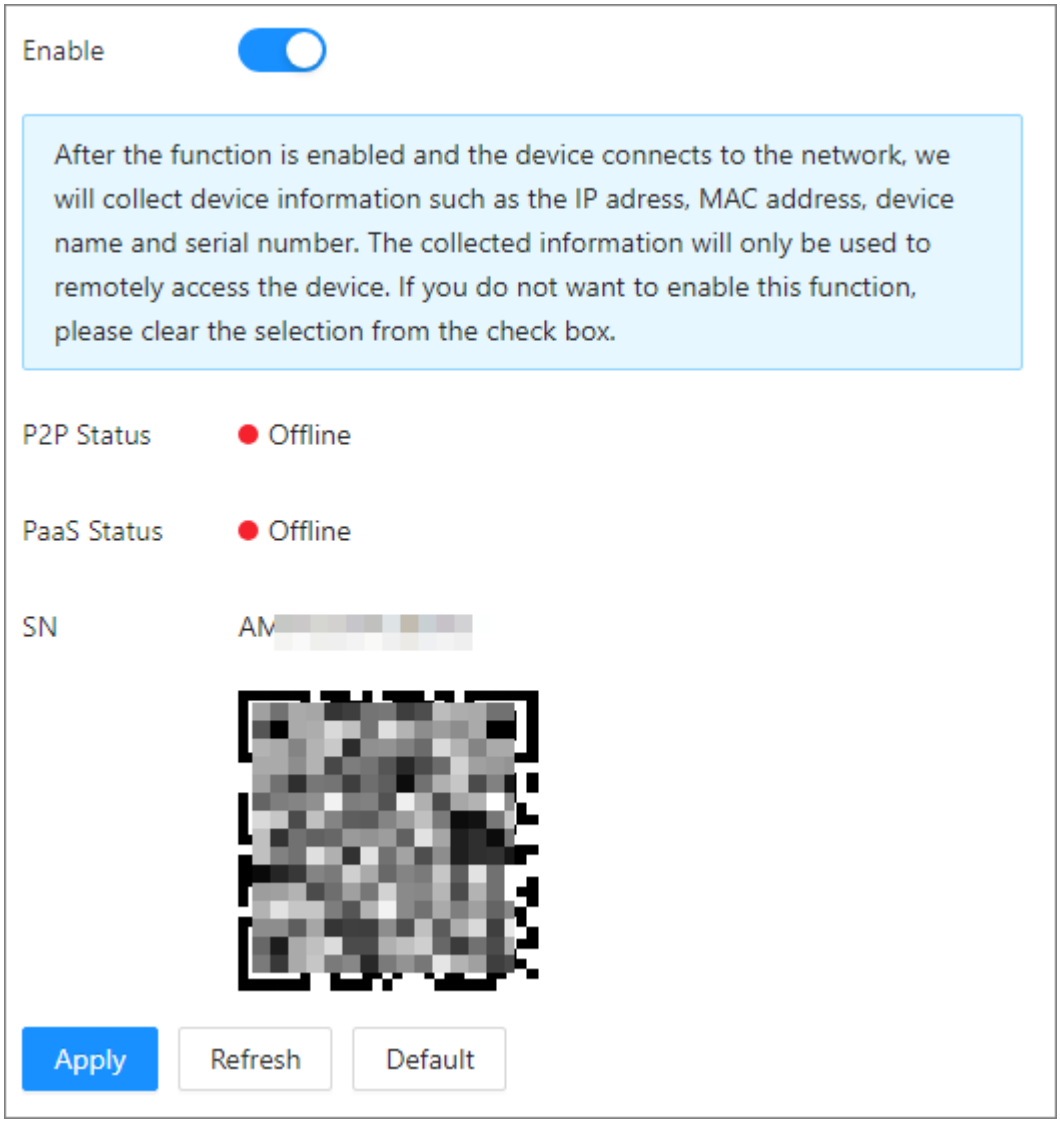
Procedure

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 4-54 Cloud service



Step 3 Click **Apply**.

Results

Scan the QR code with DMSS to add devices.

4.10.5 Configuring UPnP

Background Information

After enabling UPnP, Intranet service/port of the device will be mapped to Extranet.

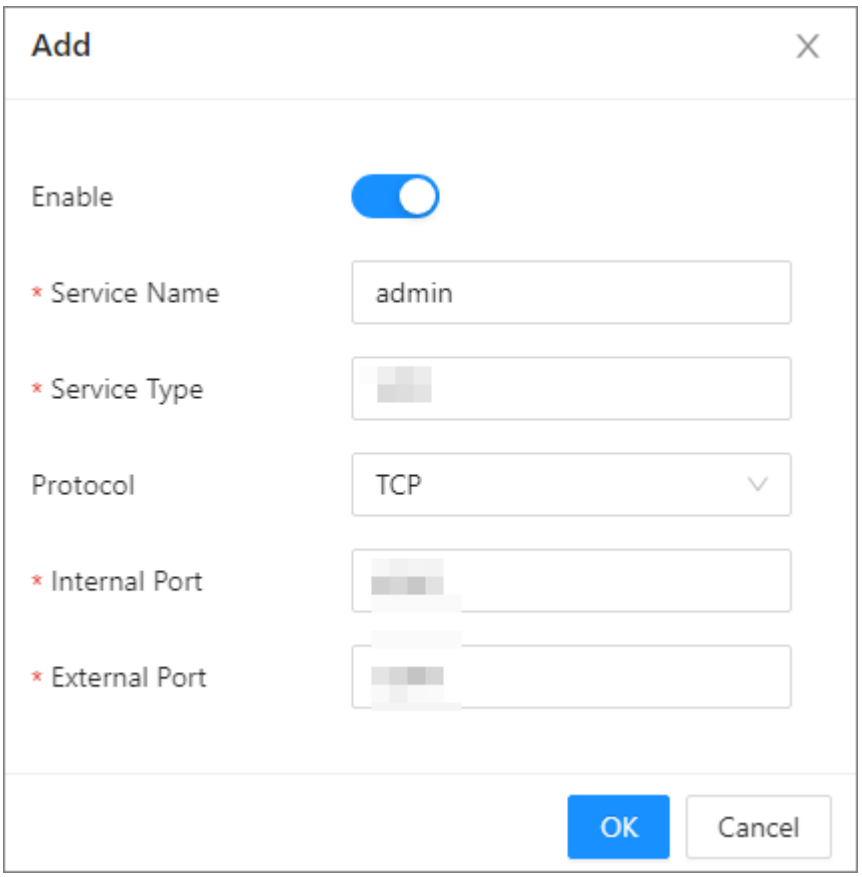
Procedure

Step 1 Select **Network Settings** > **UPnP**.

Step 2 Select to enable the function.

Step 3 Click **Add** to add new services, and then configure the parameters, and then click **OK**.

Figure 4-55 Add a new service



Step 4 Click **Apply**.

4.10.6 Configuring Wi-Fi

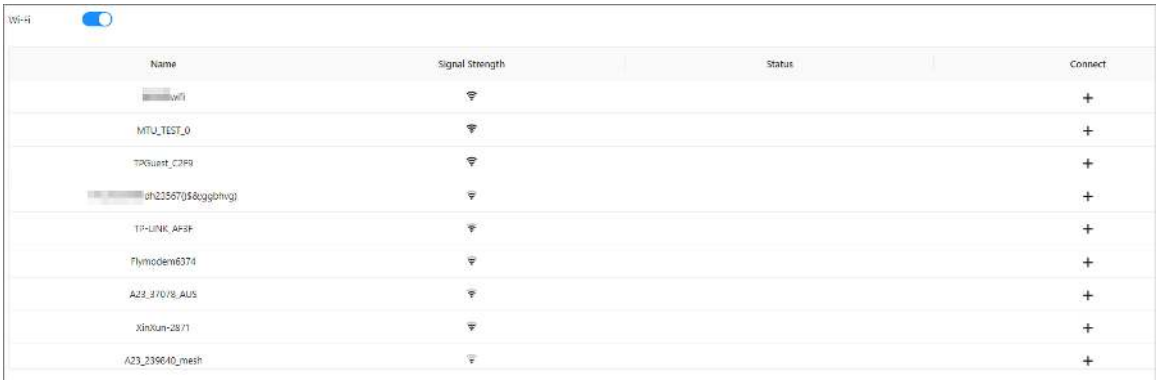
Configure the Wi-Fi function of the Device. This function is only available on select models.

Procedure

Step 1 Select **Network Settings** > **Wi-Fi**.

Step 2 Enable the function, and then you can see the available Wi-Fi list.

Figure 4-56 Wi-Fi list



Step 3 Click + behind the Wi-Fi to be connected, enter the password, and then click **Connect**.

4.10.7 Configuring the Bluetooth

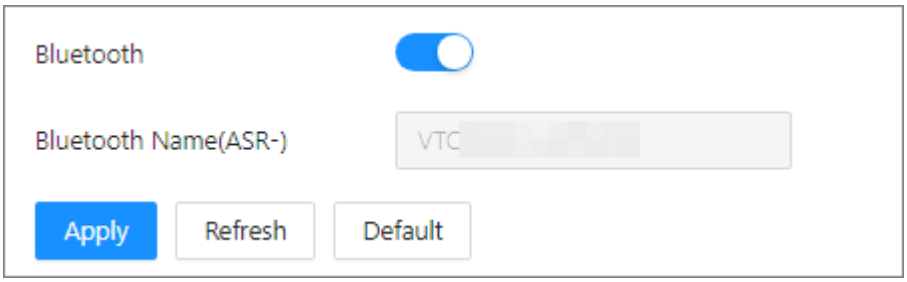
Configure the Bluetooth function of the Device. This function is only available on select models.

Procedure

Step 1 Select **Network Settings** > **Bluetooth Settings**.

Step 2 Click to enable the Bluetooth function.

Figure 4-57 Bluetooth



Results

You can unlock the door through the Bluetooth via the DMSS app. For details, see "3.3.5 Unlocking by the Bluetooth".

4.10.8 Configuring Basic Services

Procedure

Step 1 Select **Network Settings** > **Basic Services**.

Step 2 Enable the protocol as needed, and then click **Apply**.

Figure 4-58 Basic services

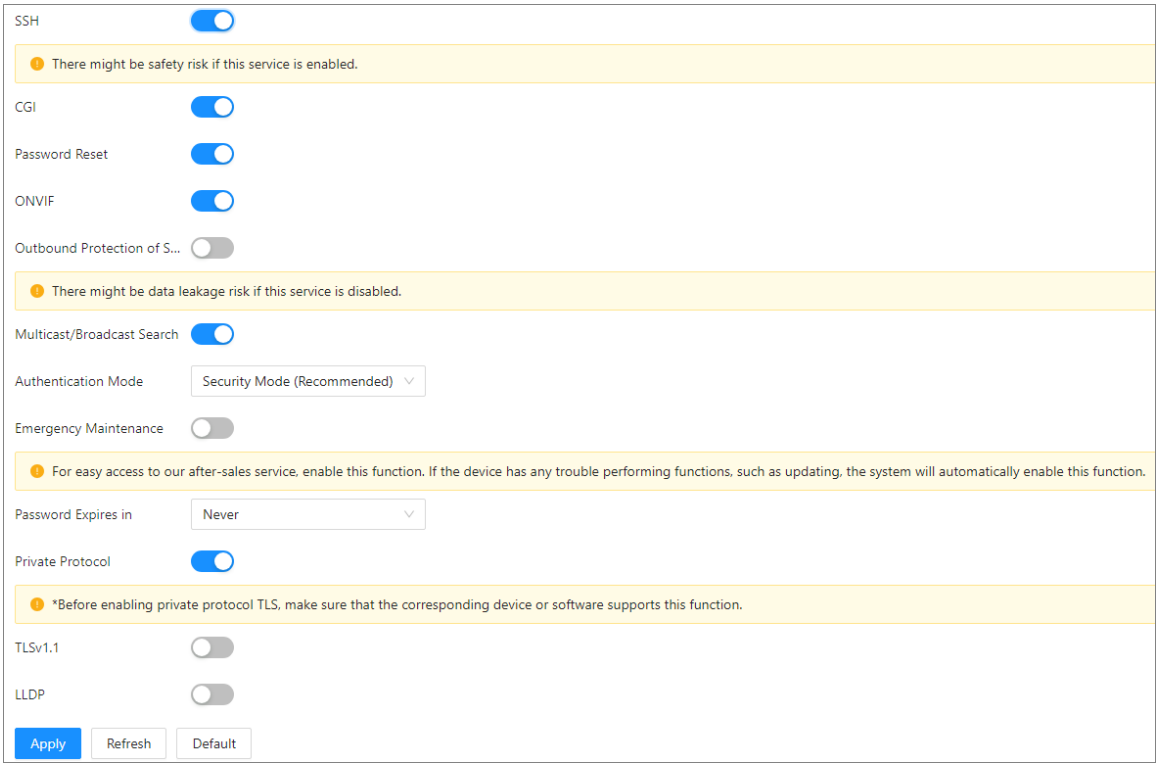


Table 4-30 Description of basic services

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.

4.10.9 Configuring Auto Registration

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

Procedure

Step 1 Select **Network Settings** > **Auto Registration**.

Step 2 Enable the function, and then enter the server address, port number and registration ID.

Figure 4-59 Auto registration

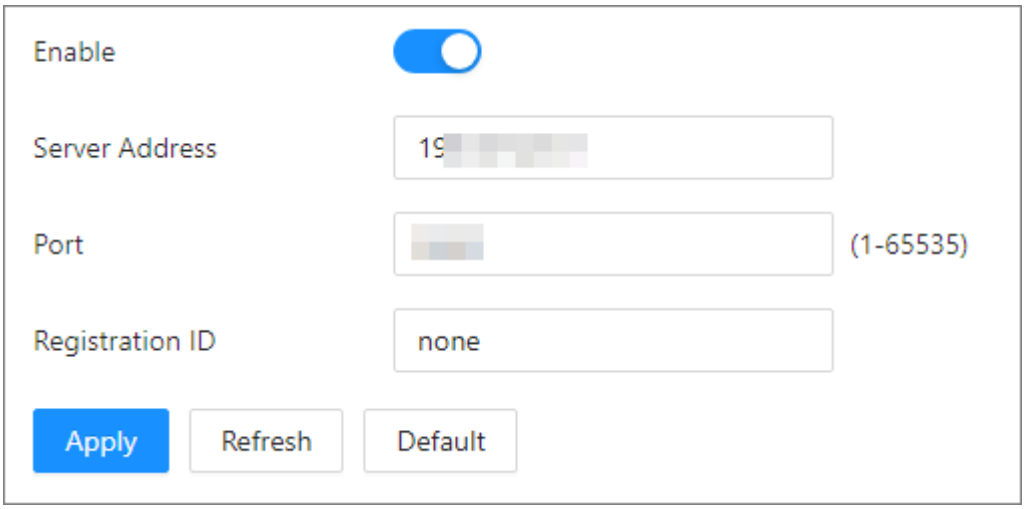


Table 4-31 Parameters description

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.

Step 3 Click **Apply**.

4.10.10 Configuring Registration Management

This function is only available when the Private SIP Server is set as server type and the **Device as Alternate Server** is enabled. For details, see "4.10.3.2 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 4-60 Configure the parameter

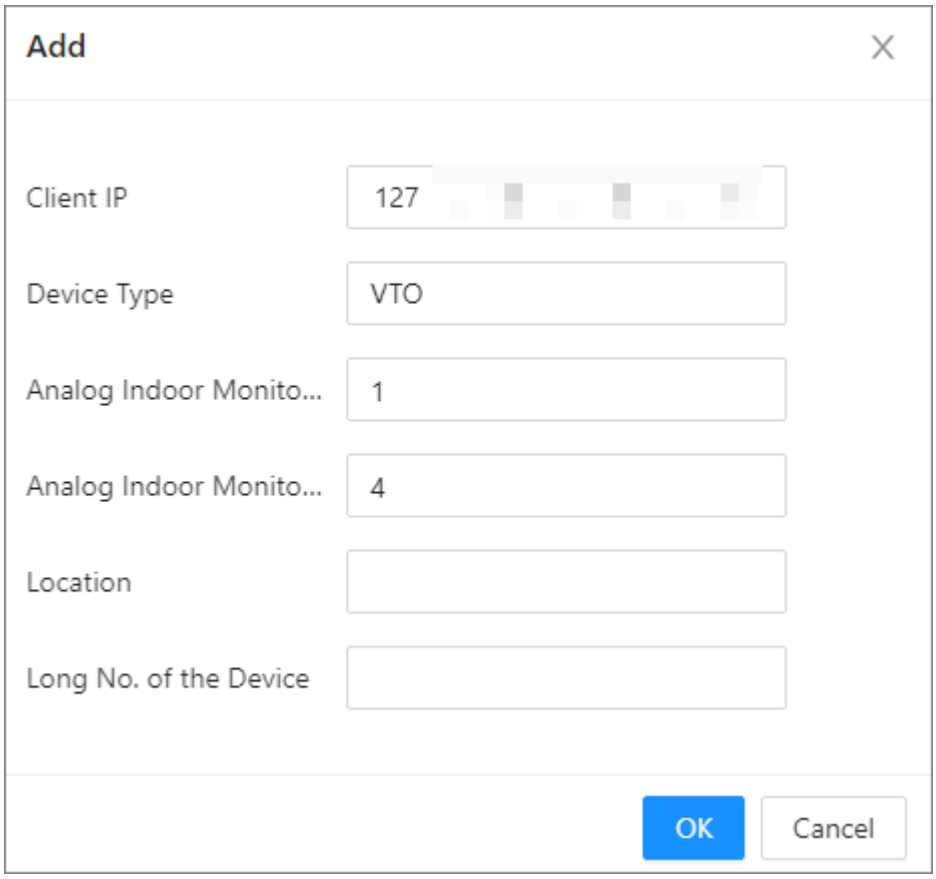


Table 4-32 Parameters description

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.

4.11 System

Configure the parameters of video, audio and time.

4.11.1 Configuring Alarm

4.11.1.1 Configuring Alarm Linkage

Procedure

Step 1 Select **System** > **Alarm** > **Alarm Linkage Setting**.

Step 2 Click ✎ to modify the parameters.

Figure 4-61 Modify the parameters

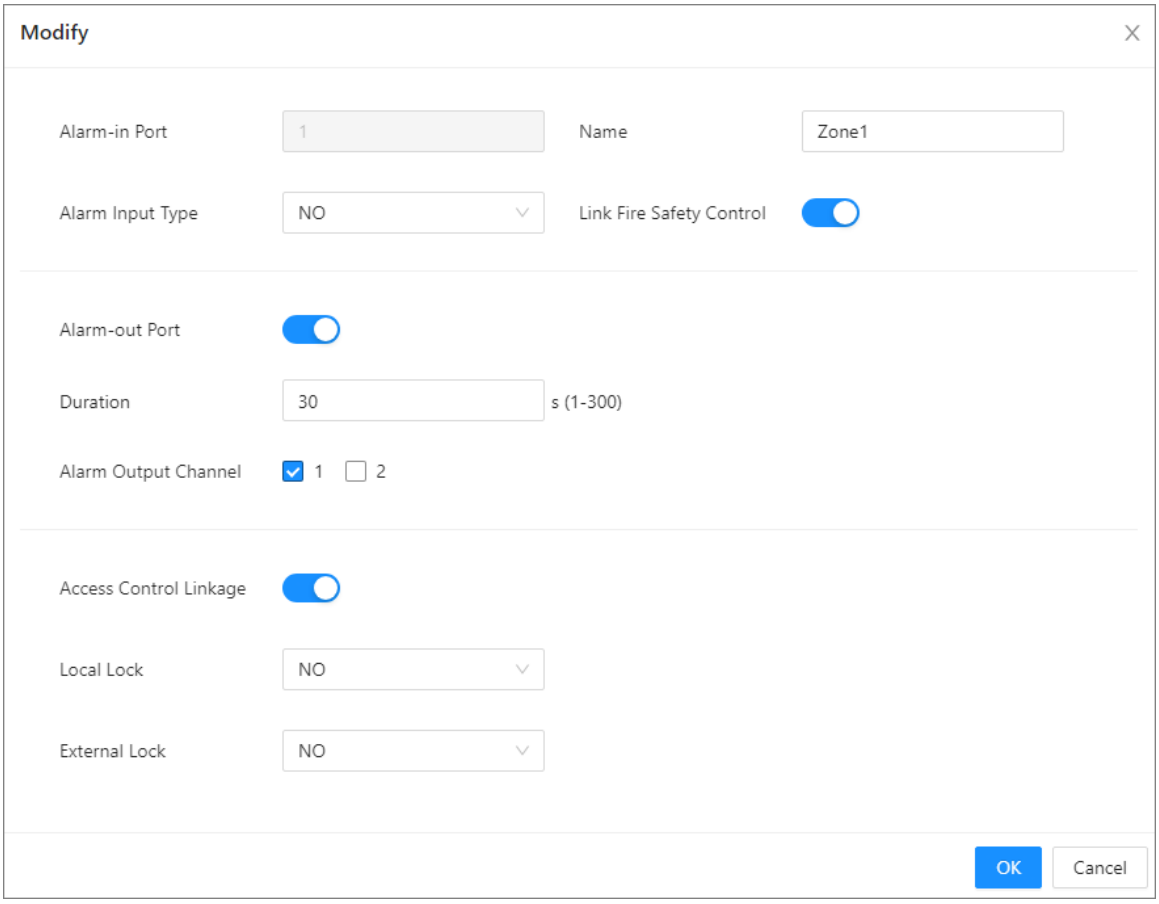


Table 4-33 Description of alarm linkage parameters

Parameter	Description
Alarm-in Port	The alarm-in port number cannot be modified.

Parameter	Description
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	
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 3 Click **OK**.

4.11.1.2 Configuring Tamper Alarm

Procedure

Step 1 Select **System** > **Alarm** > **Alarm**.

Step 2 Configure tamper alarm.

Figure 4-62 Tamper alarm

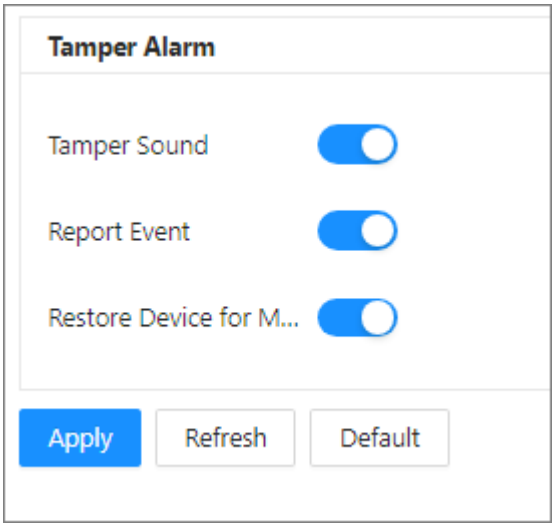


Table 4-34 Description of tamper alarm parameters

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 3 Click **Apply**.

4.11.2 Configuring Video Parameters

Procedure

Step 1 Select **System** > **Video**.

Step 2 Configure the parameters.

- Bit Rate:

Figure 4-63 Bit rate

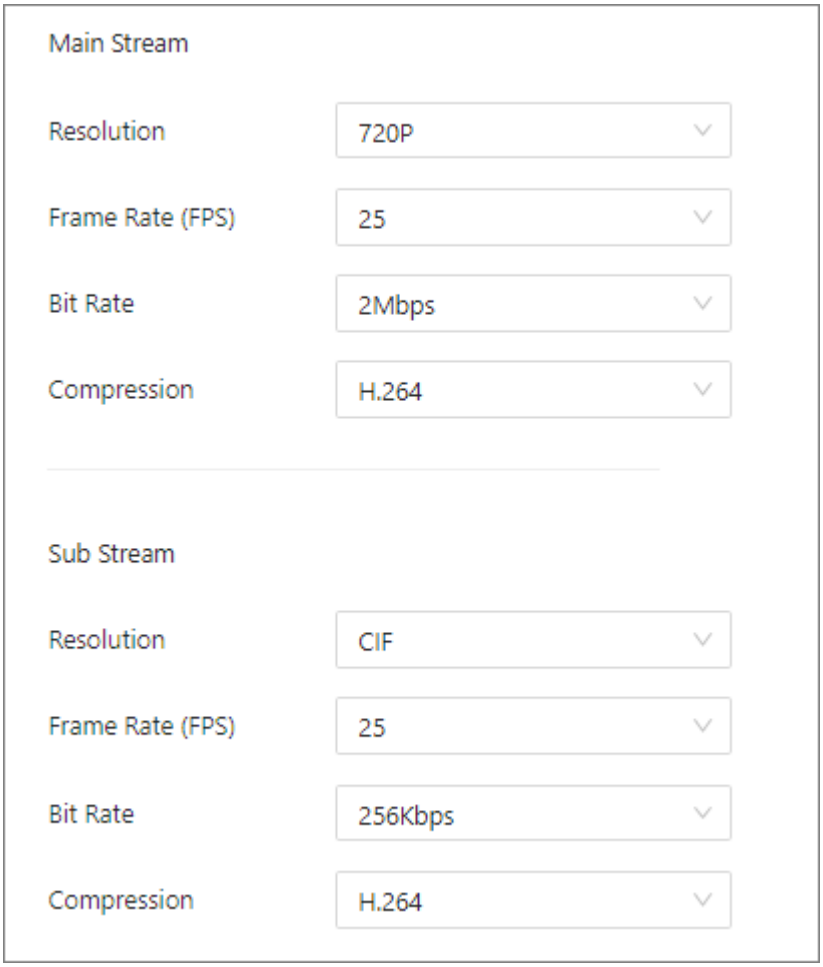


Table 4-35 Bit rate parameters description

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.
	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**.

Parameter		Description
	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 4-64 Status

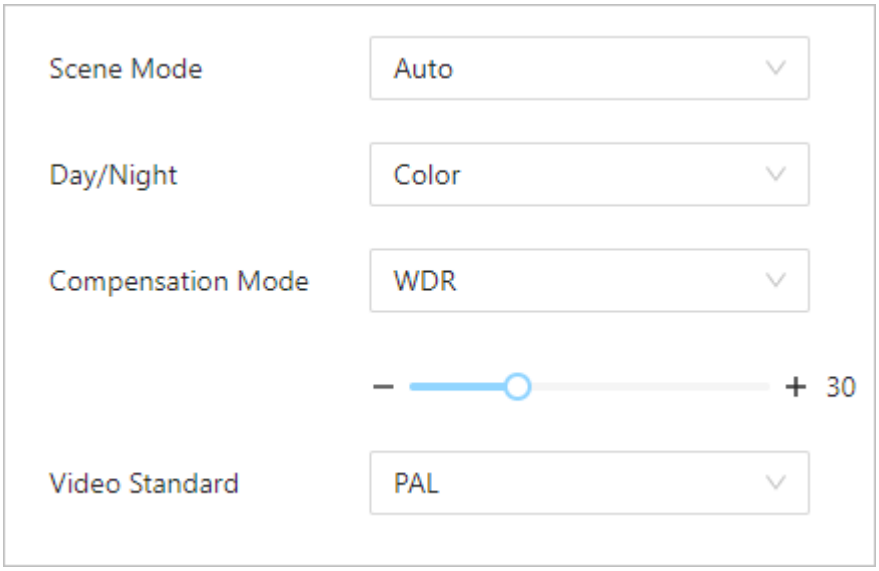


Table 4-36 Status parameters description

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.
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 4-65 Exposure

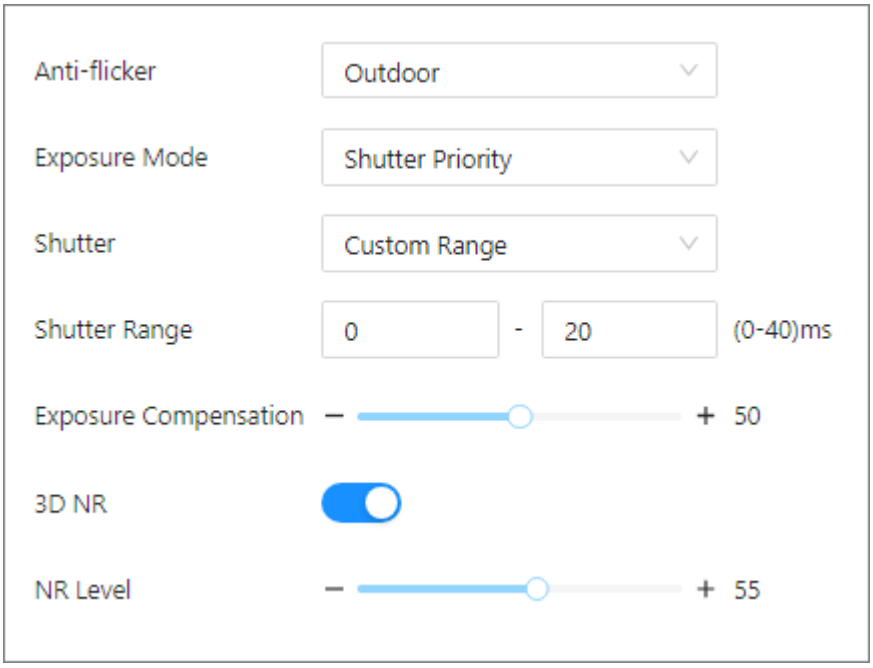


Table 4-37 Exposure parameters description

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.
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.

Parameter	Description
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 4-66 Image

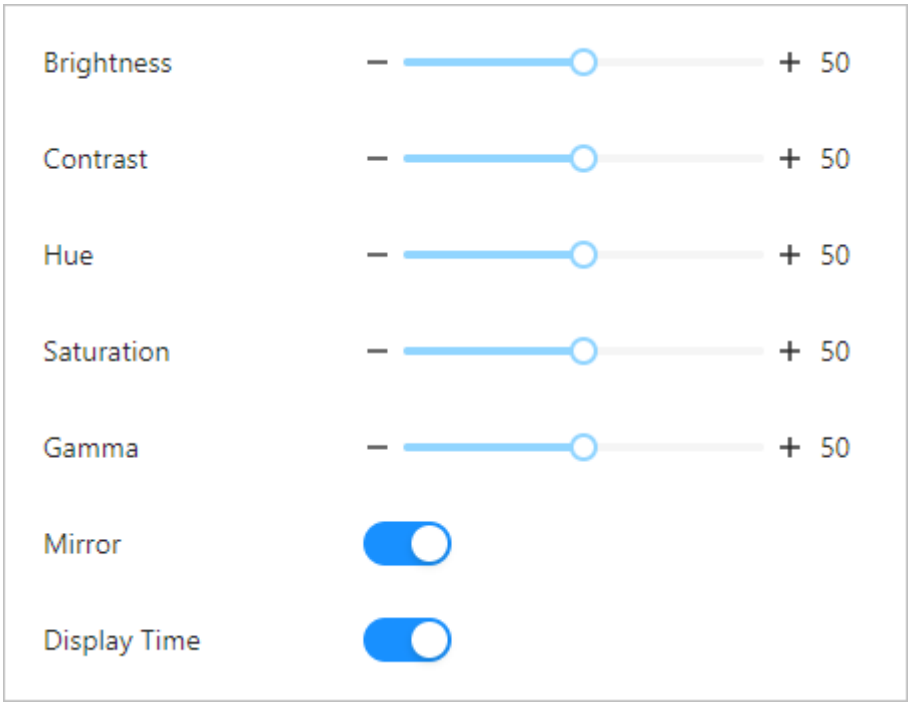


Table 4-38 Image parameters description

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.
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.

4.11.3 Configuring Audio Parameters

Procedure

Step 1 Select **System** > **Audio**.

Step 2 Configure the audio parameters.

Figure 4-67 Audio parameters

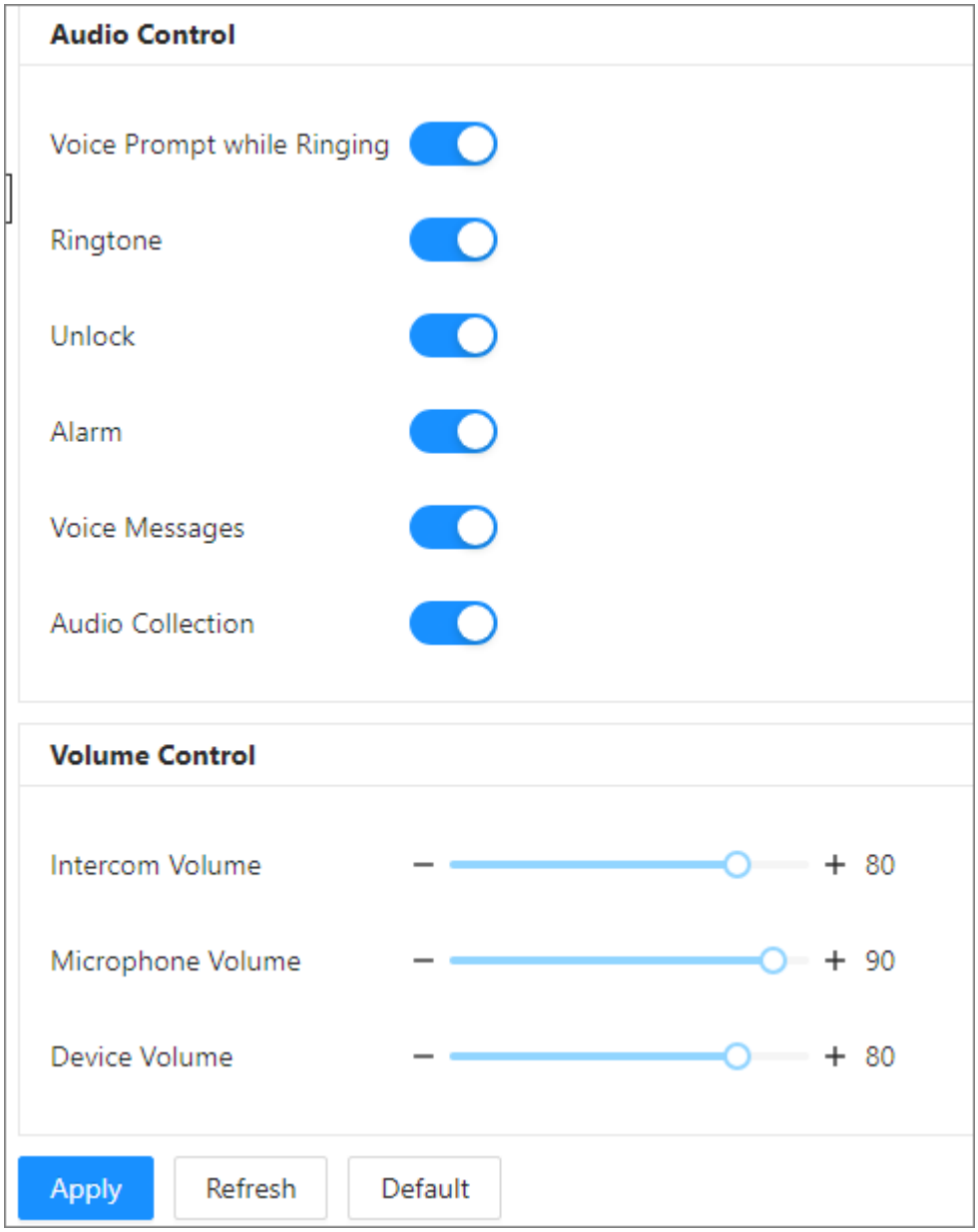


Table 4-39 Audio parameters description

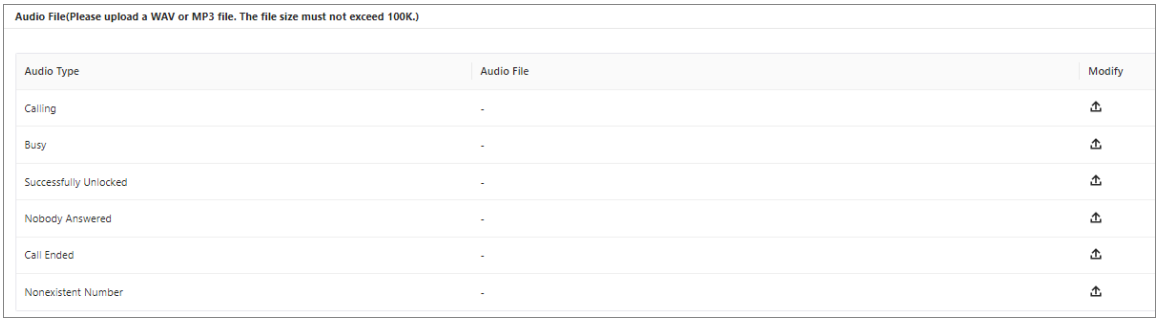
Parameter		Description
Audio Control	Voice Prompt while Ringing	If enabled, there is prompt sound when you call.
	Ringtone	If enabled, there is a ringback when you call.
	Unlock	If enabled, there is prompt sound.

Parameter		Description
	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 4-68 Upload the file



4.11.4 Configuring Time

Procedure

Step 1 Select **System** > **Time**.

Step 2 Configure the time parameters.

Figure 4-69 Time parameters

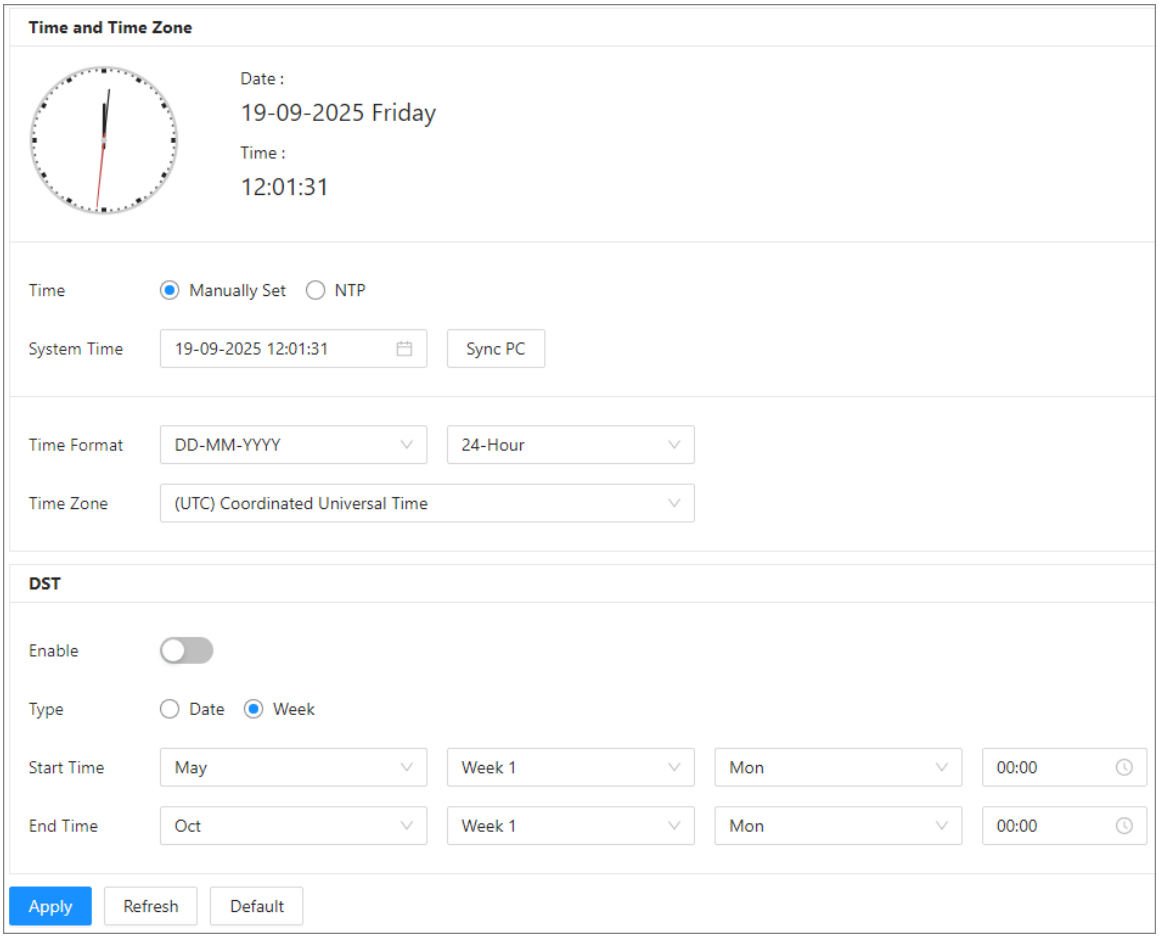


Table 4-40 Time parameters description

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.
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.

Parameter	Description
Type	Select from **Date** and **Week**.
Start Time	Configure the start time and end time for DST.
End Time	

Step 3 Click **Apply**.

4.11.5 Adding ONVIF Users

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

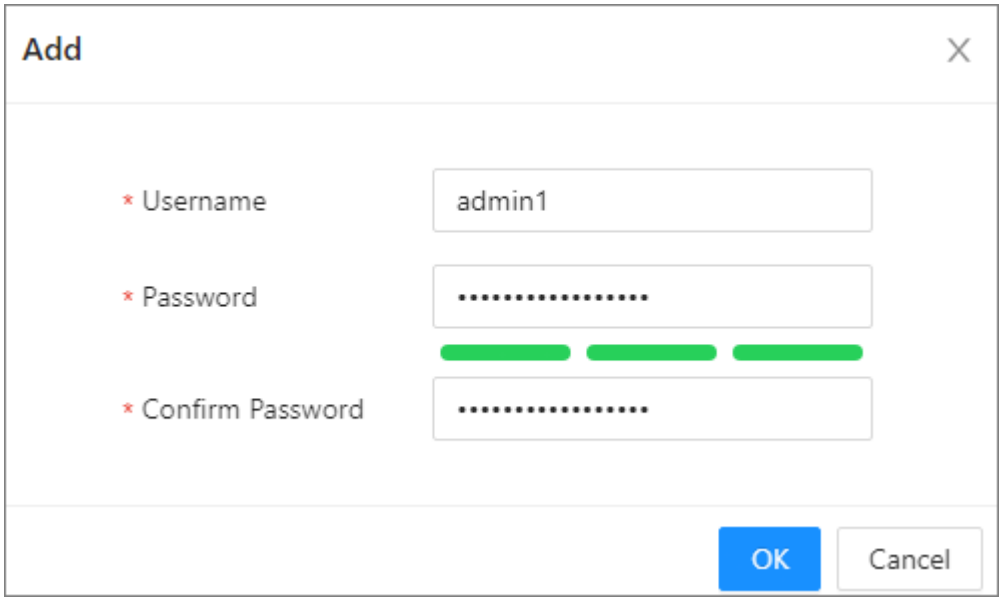
Only Profile C and Profile S are supported, while the encoding format and image parameters are not supported.

Procedure

Step 1 Select **System** > **ONVIF User**.

Step 2 Click **Add**, and then enter the user name, password and confirm password.

Figure 4-70 Add the user



Step 3 Click **OK**.

Related Operations

- Click to edit the user.
- Click to delete the user.

4.12 Maintenance Center

4.12.1 One-Click Diagnosis

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

Procedure

Step 1 Select **Maintenance Center** > **One-click Diagnosis**.

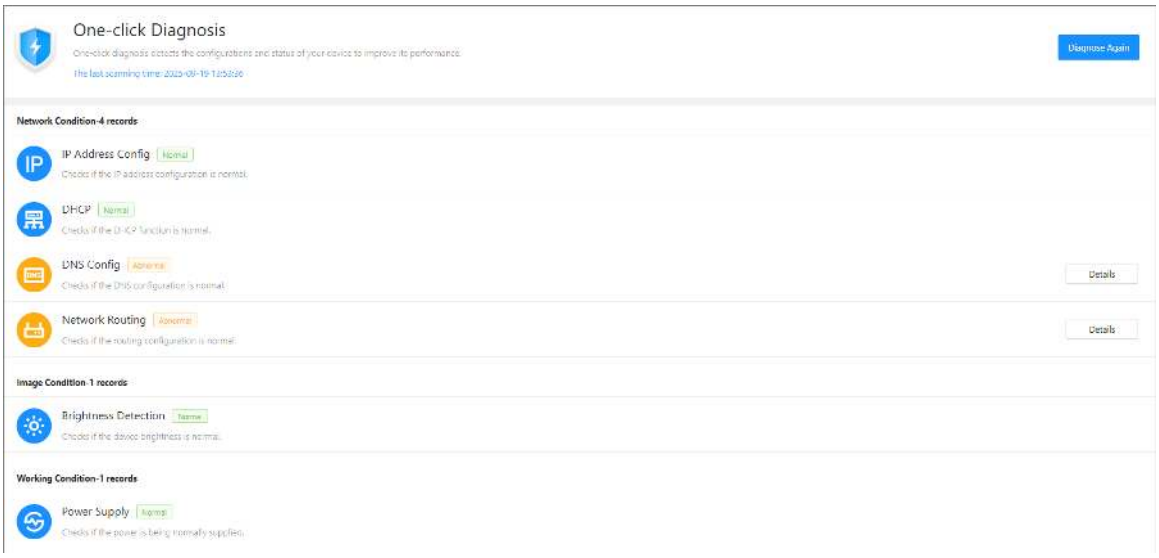
Step 2 Click **Diagnose**.

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

Step 3 (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 4-71 One-click diagnosis



4.12.2 System Information

4.12.2.1 Viewing Version Information

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

Figure 4-72 Version information

Device Model	
Device SN	AM
Hardware Version	V
Software Version	2025-09-13 V4.8
SCM Version	2024-03-02 V1
Web Version	V5.
Face Algorithm Version	V1
Security Baseline Version	V2.
Fingerprint Firmware	V1.
Touchscreen Version	V50

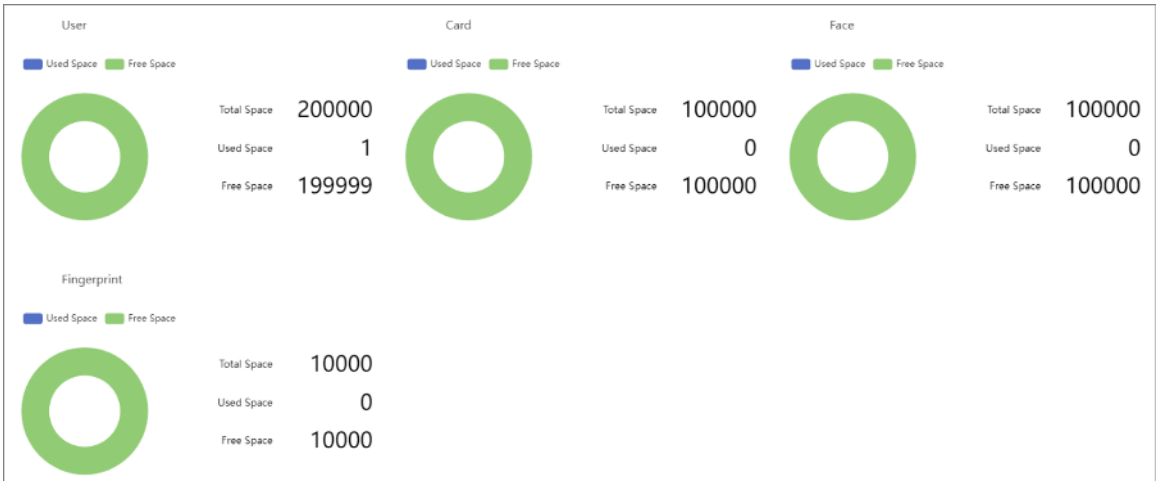
4.12.2.2 Viewing Legal Information

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

4.12.3 Data Capacity

Select **Maintenance Center** > **Data Capacity**, and then you can see the data capacity of the users, cards, face images, and fingerprint information.

Figure 4-73 Data capacity



4.12.4 Viewing Logs

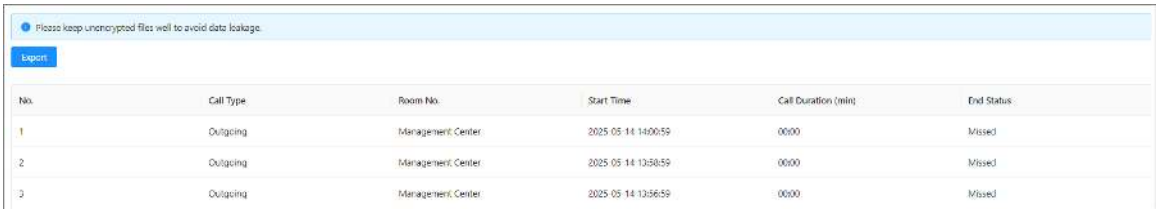
View logs such as system logs, alarm logs, call logs, and unlock records.

4.12.4.1 Call History

Procedure

Step 1 Select **Maintenance Center** > **Log** > **Call History**.

Figure 4-74 Call history



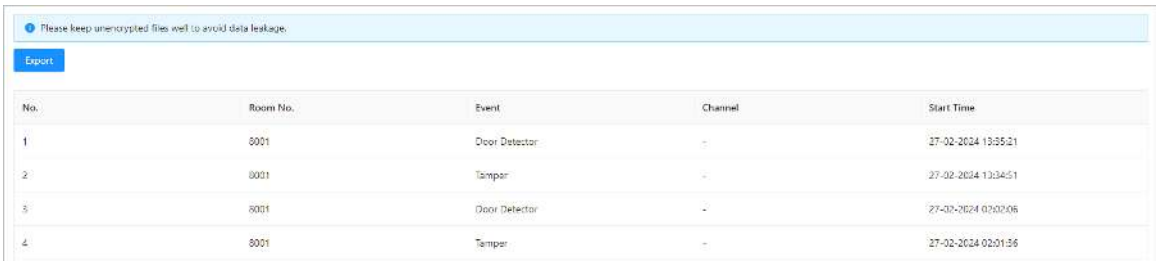
Step 2 (Optional) Click **Export** to export the call history.

4.12.4.2 Alarm Logs

Procedure

Step 1 Select **Maintenance Center** > **Log** > **Alarm Logs**.

Figure 4-75 Alarm logs



Step 2 (Optional) Click **Export** to export the logs to the local computer.

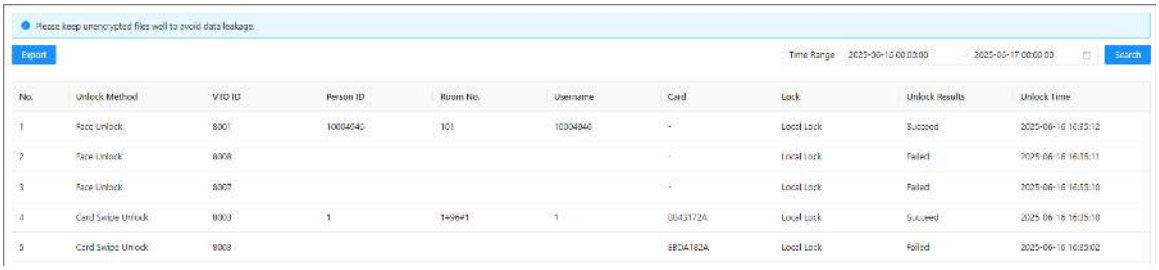
4.12.4.3 Unlock Records

Procedure

Step 1 Select **Maintenance Center** > **Log** > **Unlock Records**.

Step 2 Configure the time range, and then click **Search**.

Figure 4-76 Unlock records



Step 3 (Optional) Click **Export** to download the log.

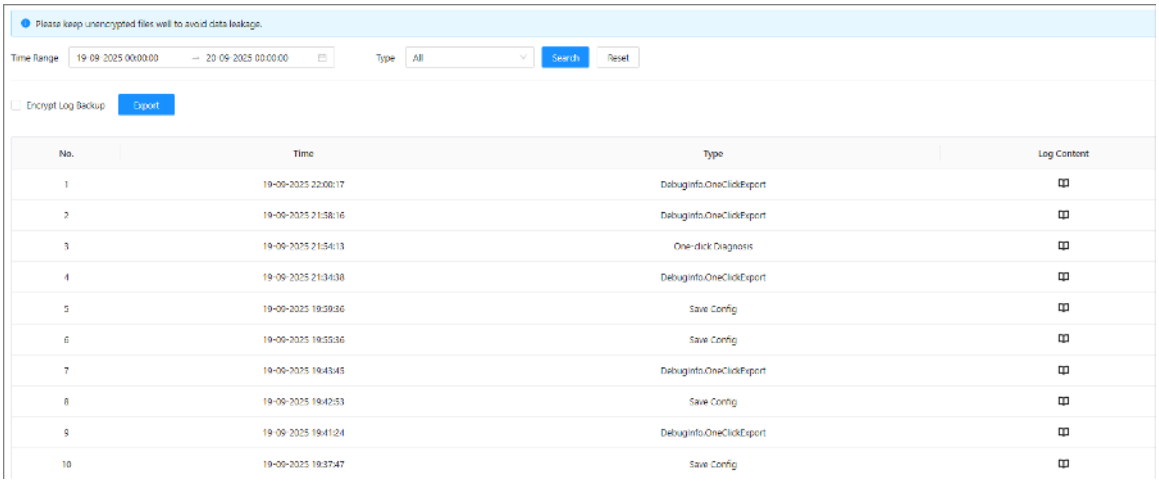
4.12.4.4 System Logs

Procedure

Step 1 Select **Maintenance Center** > **Log** > **Log**.

Step 2 Select the time range and the log type, and then click **Search**.

Figure 4-77 System logs



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.

4.12.5 Maintenance Management

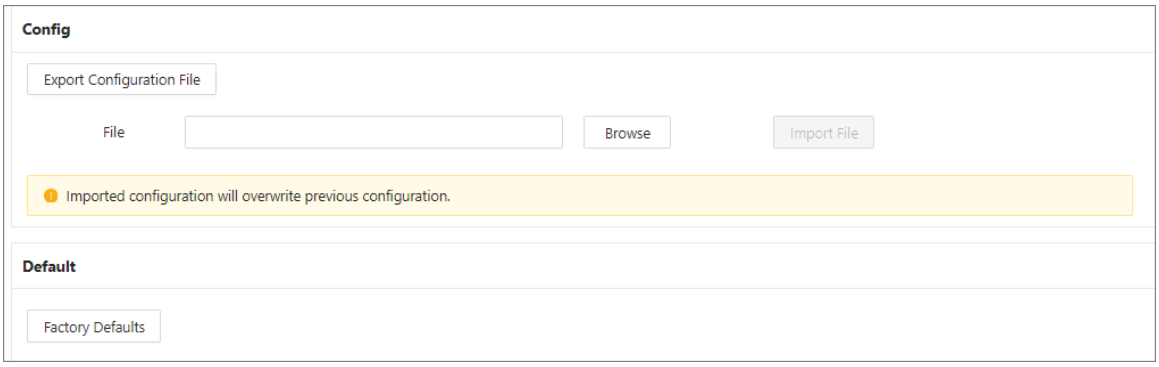
4.12.5.1 Exporting and Importing Configuration Files

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

Figure 4-78 Configuration management



Step 2 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.

Step 3 (Optional) Click **Factory Defaults** to set the device to its default settings.

4.12.5.2 Maintenance

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

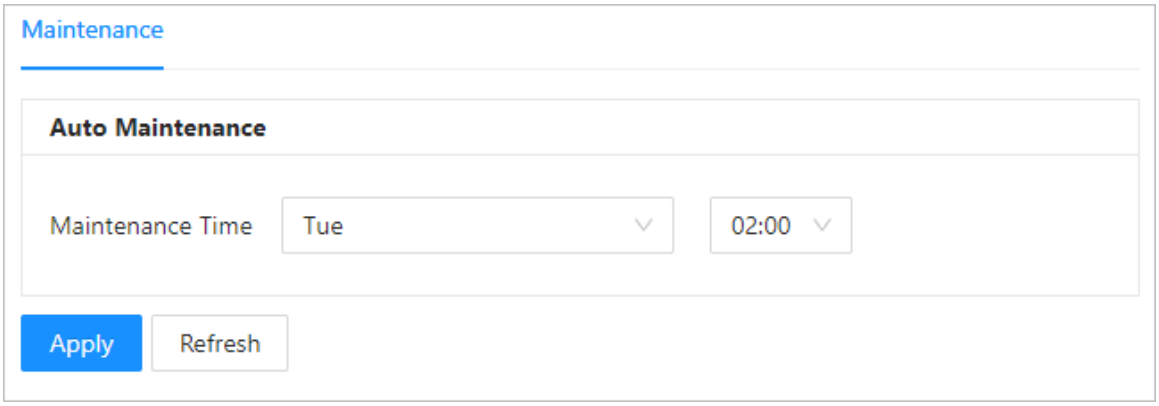
Procedure

Step 1 Select **Maintenance Center** > **Maintenance Management** > **Maintenance**.

Step 2 Set the time, and then click **Apply**.

The Device will restart at the scheduled time.

Figure 4-79 Maintenance time



4.12.6 Updating the System

- 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

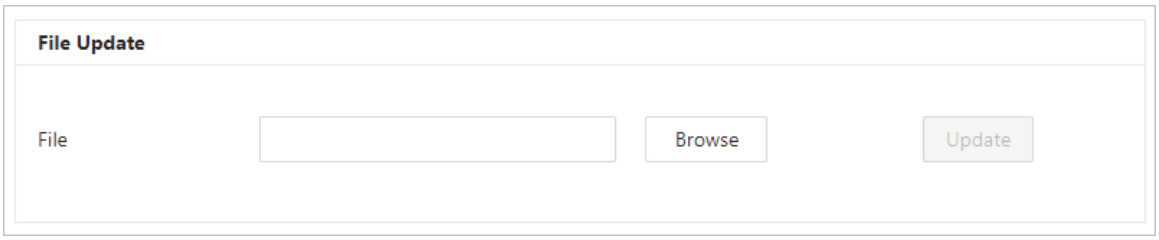
1. Select **Maintenance Center** > **Update**.
2. In the **File Update** area, click **Browse**, and then upload the update file.

   The update file should be a .bin file.

3. Click **Update**.

   The VTO will restart after the update finishes.

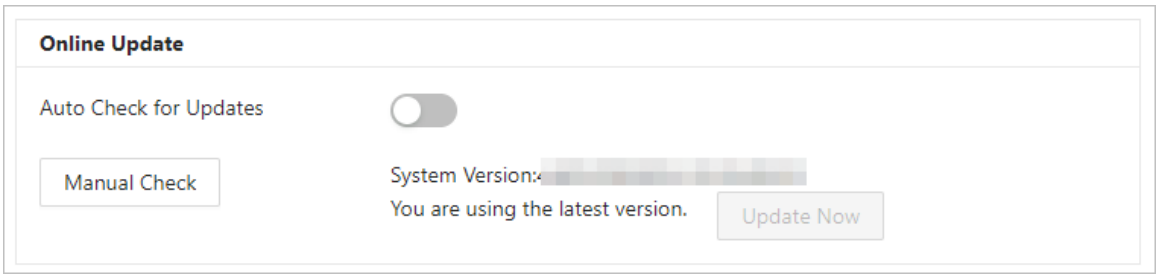
Figure 4-80 File update



Online Update

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

Figure 4-81 Online update



4.12.7 Advanced Maintenance

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

4.12.7.1 Exporting

Export the configuration information of the device.

Procedure

Step 1 Select **Maintenance Center** > **Advanced Maintenance** > **Export**.

Step 2 Click **Export** to export the serial number, firmware version, device operation logs and configuration information.

4.12.7.2 Packet Capture

Procedure

Step 1 Select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.

Figure 4-82 Packet Capture

Step 2 Enter the IP address, click ▸, and then ▸ changes to ⏸ to acquire the data.

Step 3 After you acquired enough data, click ⏸.

Captured packets are automatically downloaded to your local computer.

4.12.7.3 Network Test

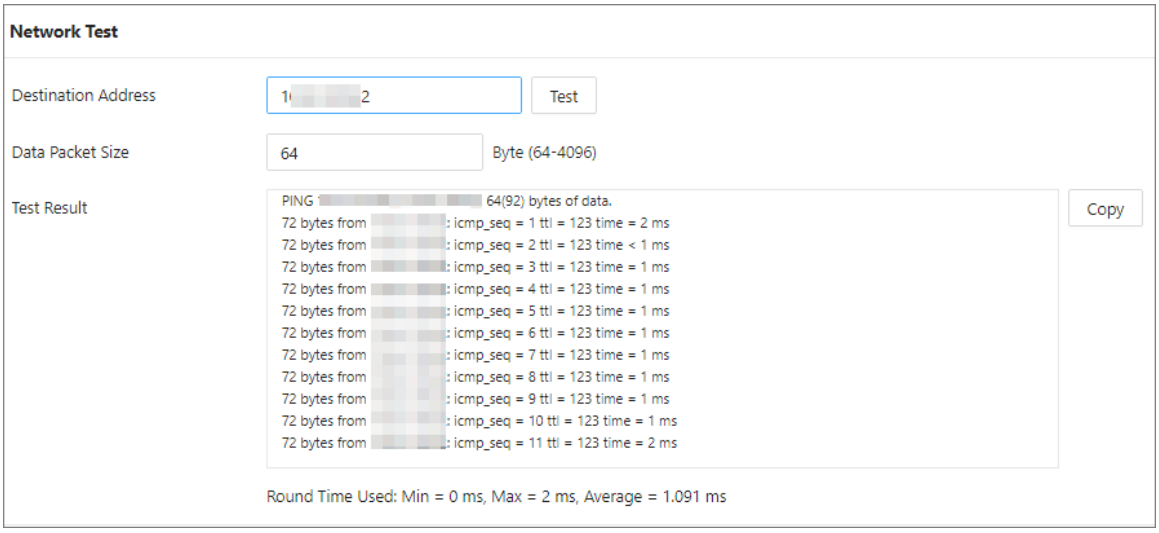
Procedure

Step 1 Select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.

Step 2 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 4-83 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).