Modular Door Station

User Manual

V1.0.2

Foreword

General

This manual introduces the installation, functions and operations of the modular door station device (hereinafter referred to as "the VTO"). Read carefully before using the device, 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 Date
V1.0.2	Updated basic settings.	December 2025
V1.0.1	Updated RS-485.	August 2025
V1.0.0	First release.	June 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.
  - We recommend using the power adapter provided with the device.
  - When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.

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

Operation Requirements

 DANGER

Battery Pack Precautions

Preventive measures (including but not limited to):

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

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

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

Table of Contents

1 Structure

1.1 Front Panel

Figure 1-1 Front panel

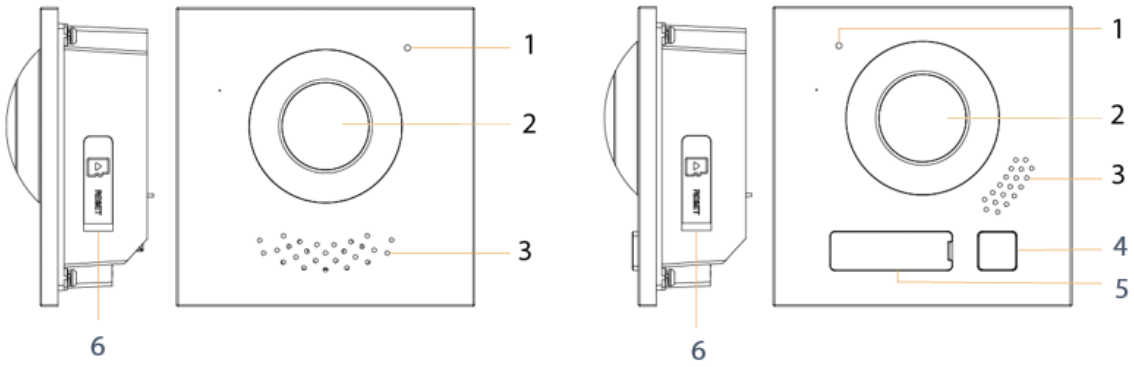


Table 1-1 Front panel description

No.	Name	Description
1	Microphone	Audio input.
2	Camera	Capture images or record videos for the VTO.
3	Speaker	Audio output.
4	Call button	Call button.
5	Nameplate	Displays the custom information.
6	Card slot and reset button	• Insert SD card so that data information such as images and videos can be stored. • Press and hold the button for several seconds to reset to factory settings.

1.2 Rear Panel

Figure 1-2 Rear panel

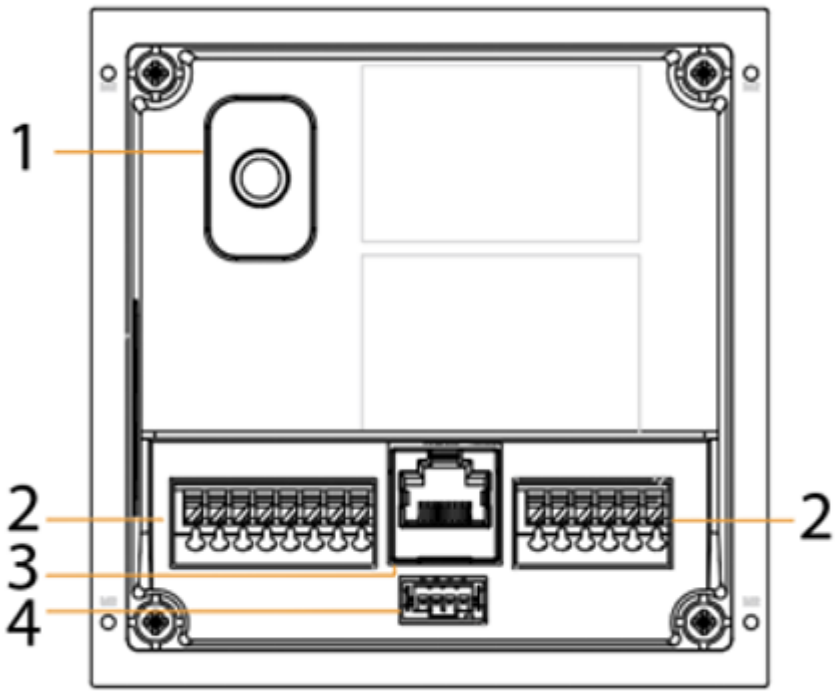


Table 1-2 Rear panel description

No.	Name	Function
1	Tamper button	• After the installed device is removed from the wall or other places, the device beeps and the alarm record will be generated. • Within 5 minutes after the device is powered on, if you press the tamper button for 5 times in 8 seconds, the device beeps and deletes the account information. The alarm record will be generated.
2	Multi-function ports	Alarm port, door detector port, 485 port, power port and more.
3	Network port	Connect to the network.
4	Cascade connection port	Connect to other modules.

Figure 1-3 Multi-function ports

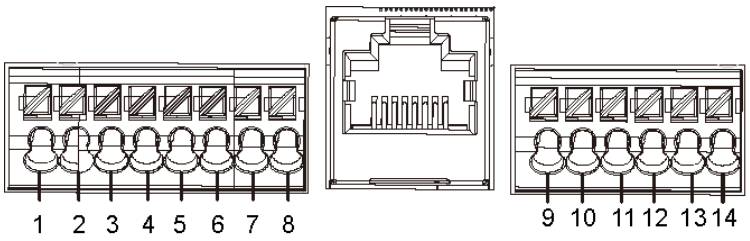


Table 1-3 Port description

No.	Description	No.	Description
1	GND	8	• 2 wires-(GND) for a digital 2-wire camera module • GND for a full digital camera module
2	+12V_OUT	9	DOOR_BUTTON
3	RS-485_B	10	DOOR_FEEDBACK
4	RS-485_A	11	GND
5	ALARM_NO	12	DOOR_NC
6	ALARM_COM	13	DOOR_COM
7	• 2 wires+(48V) for a digital 2-wire camera module • 12 V_IN for a full digital camera module	14	DOOR_NO

1.3 Indicator Module

Figure 1-4 Front panel

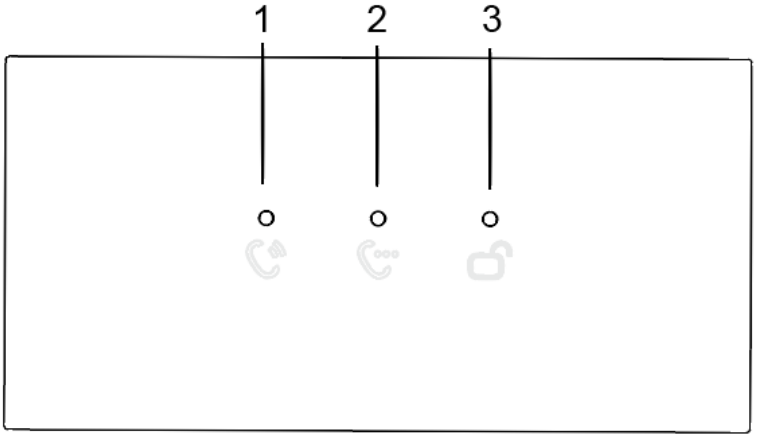


Table 1-4 Front panel description

No.	Name	Description
1	Call indicator	Activity status.
2	Talk indicator	
3	Unlock indicator	

Figure 1-5 Rear panel

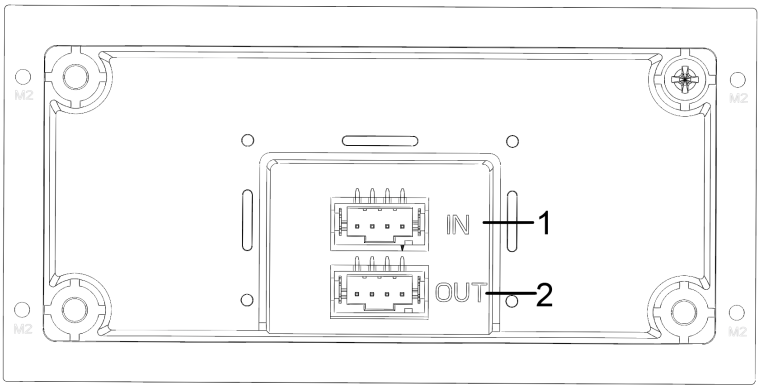


Table 1-5 Rear panel description

No.	Name	Description
1	Cascade input	Connect to other modules.
2	Cascade output	

1.4 Button Module

1-button module, 2-button module, and 5-button module

One-button module, two-button module, and five-button module are available with the same function. Here we take the five-button module as an example.

Figure 1-6 Front panel of the five-button module

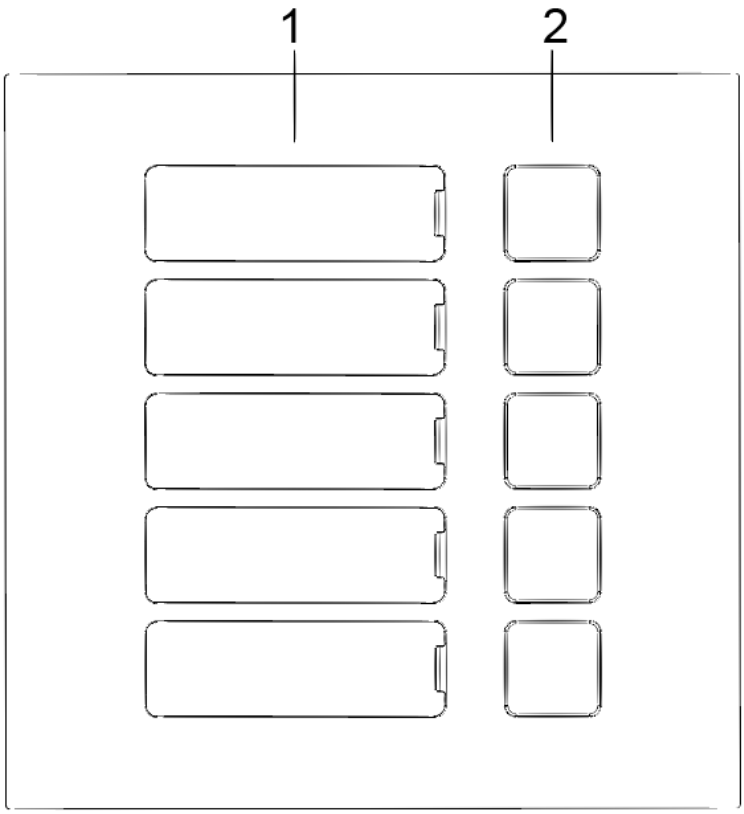


Table 1-6 Front panel description

No.	Name	Description
1	User directory	Put name cards here.
2	Call buttons	Call other VTHs or the management center.

Figure 1-7 Rear panel of the five-button module

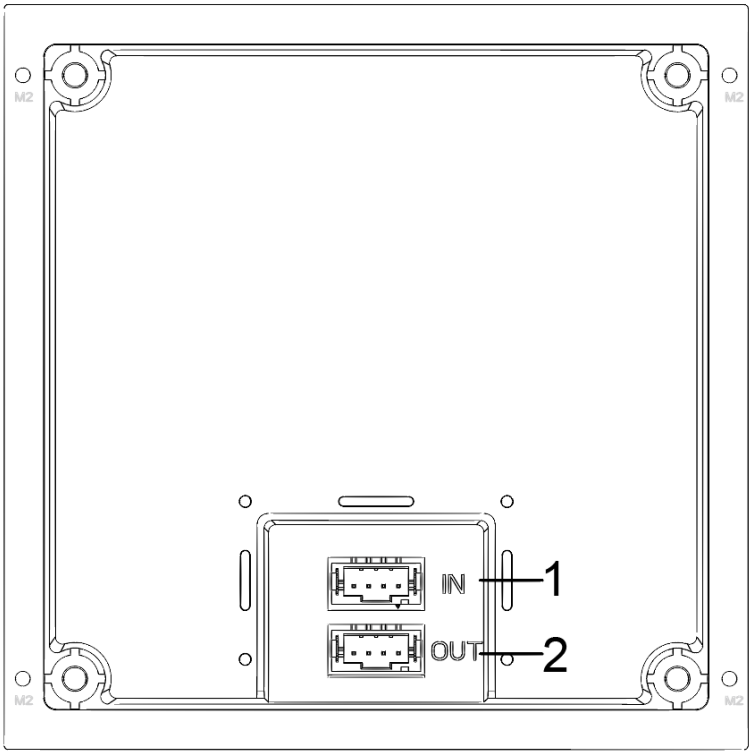


Table 1-7 Rear panel description

No.	Name	Description
1	Cascade input	Connect to other modules.
2	Cascade output	

2-button module, 4-button module, and 10-button module

Two-button module, four-button module, and ten-button module are available with the same function. Here we take the ten-button module as an example.

Figure 1-8 Front panel of the ten-button module

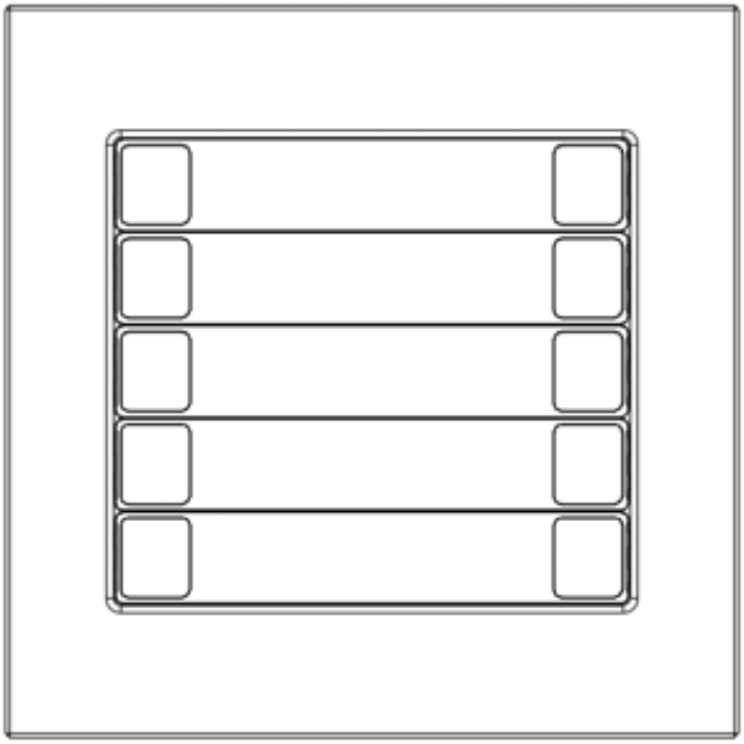


Figure 1-9 Rear panel of the ten-button module

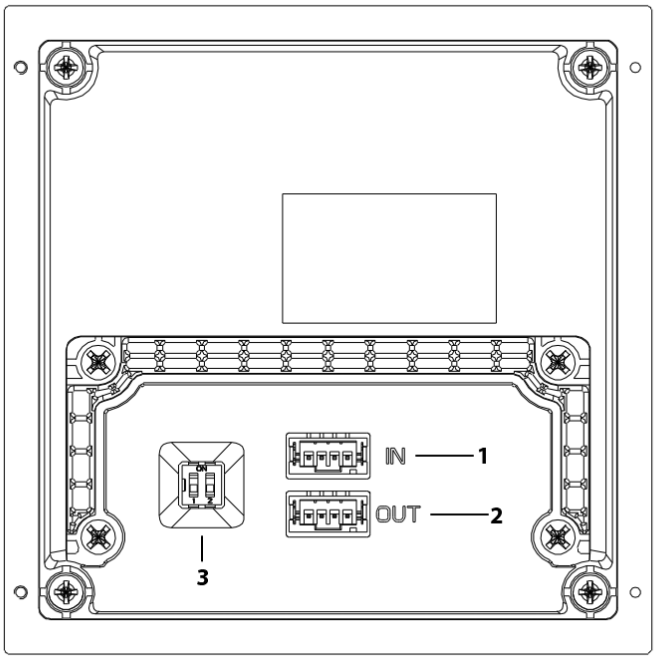


Table 1-8 Rear panel description

No.	Name	Description
1	Cascade input	Connect to other modules.
2	Cascade output	

No.	Name	Description
3	Mode switch	• Switch between single-column buttons and two-column buttons. • The first DIP switch on the left turns to **ON** indicates the single-column buttons, while to **1** indicates the two-column buttons. • It takes effect after the main VTO is restarted. • Flipping up or down the second (from left to right) DIP switch has no effect. If you want to change two-column buttons mode into single-column buttons mode, take the single-column buttons accessory from the package to replace it. For information about room number configurations on the WEB, see "6.4 Layout (Multiple Modules)".

1.5 Keyboard Module (with Braille)

The rear panel of keyboard module is the same as the button module.

Figure 1-10 Keyboard module

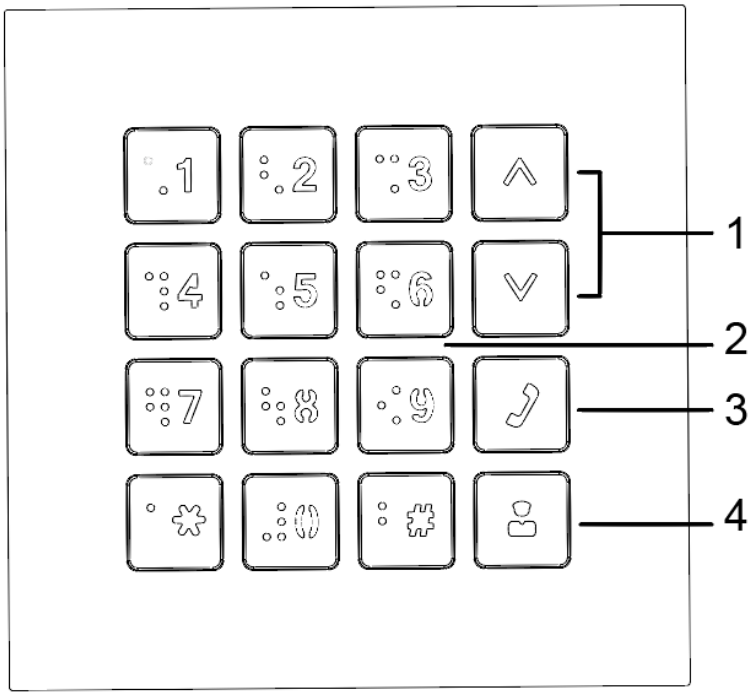


Table 1-9 Keyboard module description

No.	Name	Description
1	Selection	Tap the button to select the contact.
2	Numbers	Enter password or VTH numbers.
3	Call	Call according to the numbers.
4	Call management center	Call the management center.

1.6 Card Module

There are 2 types of the card module. Select from the ID card module and IC card module as needed.

The rear panel of card module is the same as the button module.

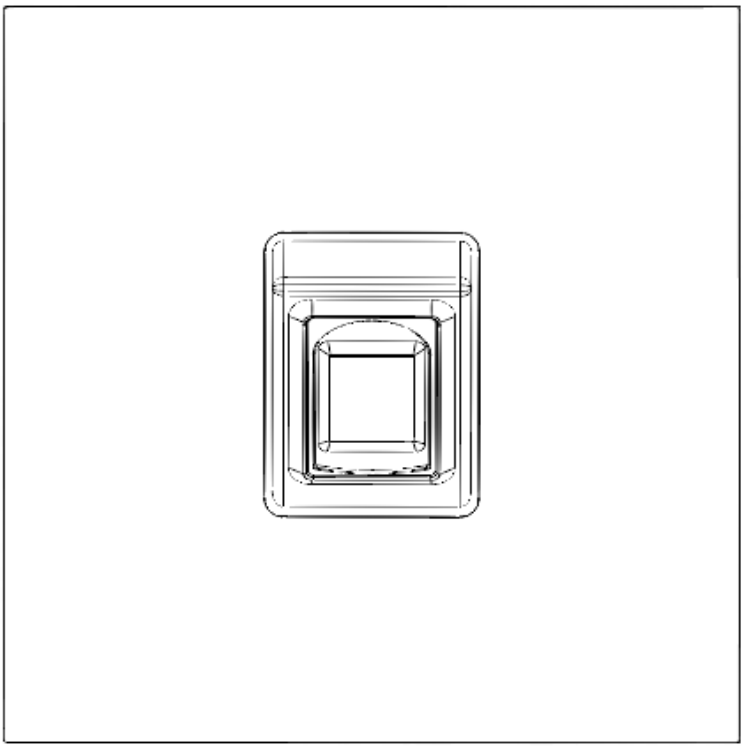
Figure 1-11 Card module

1.7 Fingerprint Module

Collects and verifies fingerprints.

- The rear panels of fingerprint module and button module have different port positions, but port functions are the same.
- When there is a fingerprint module accessed and you want to add a new fingerprint module, clear the fingerprint information on the original fingerprint module.

Figure 1-12 Fingerprint module

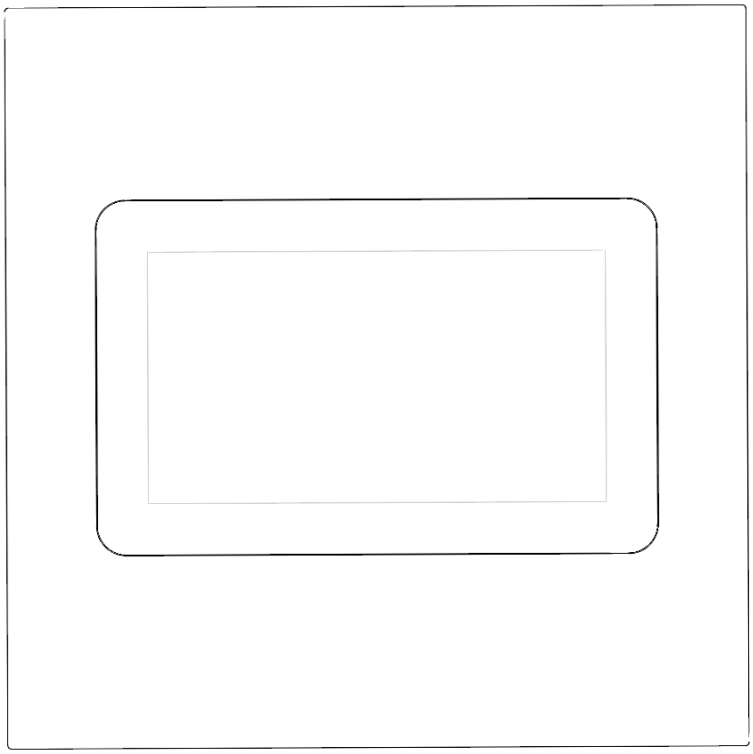


1.8 Display Module

Displays user information.

Rear panels of display module and button module have different port positions, but port functions are the same.

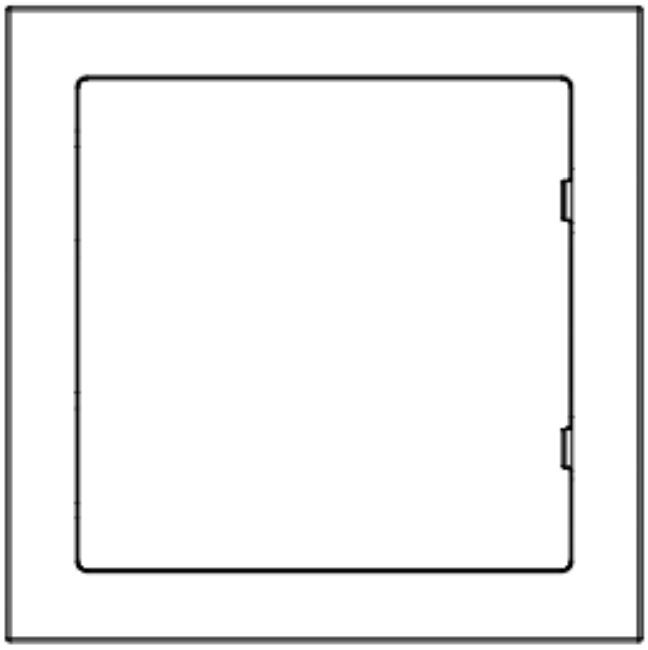
Figure 1-13 Display module



1.9 Information Module

Displays room number and guest message.

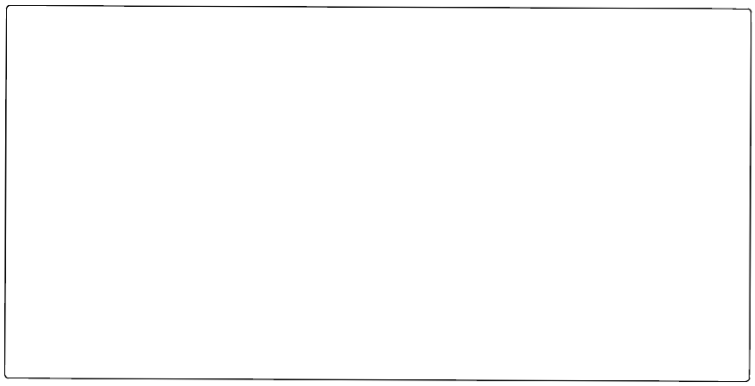
Figure 1-14 Information module



1.10 Blank Module

For a better appearance, use the blank module if there is an extra space while putting up modules together.

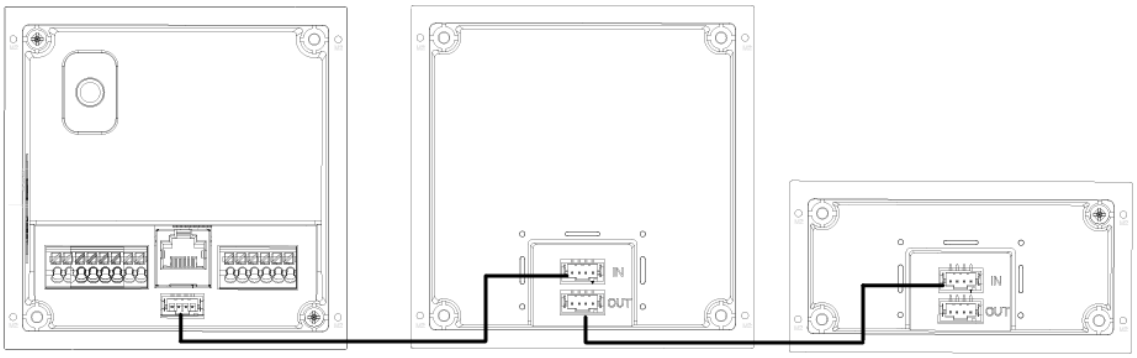
Figure 1-15 Blank module



1.11 Cascade Connection

Cascade connection is needed for all the modules to work together.

Figure 1-16 Cascade connection example



2 Initializing the VTO

2.1 Webpage

For first-time login, you need to initialize the VTO.

Procedure

Step 1 Power on the VTO.

Step 2 Go to the default IP address (192.168.1.108) of the VTO.

Make sure that the IP address of your PC is on the same network segment as the VTO.

Step 3 On the **Device Init** page, enter and confirm the password, and then click **Next**.

The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).

Step 4 Select the **Email** checkbox and enter an email address for resetting password.

Step 5 Click **Next**.

Step 6 Click **OK** to go to the login page.

Step 7 Enter the username (admin by default) and password to log in to the webpage.

2.2 DoLynk Care

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

Procedure

Step 1 On the home screen, tap ⊕.

Step 2 Tap **QR** to add a device.

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

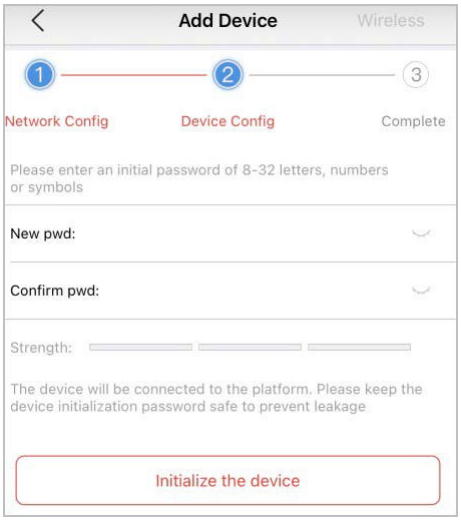
Step 4 Select a site, and then tap **OK**.

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

Step 6 Connect to wireless or wired network.

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

Figure 2-1 Initialize the device



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

3 Logging and Resetting Password

3.1 Logging

Before login, make sure that the computer is on the same network segment as the VTO.

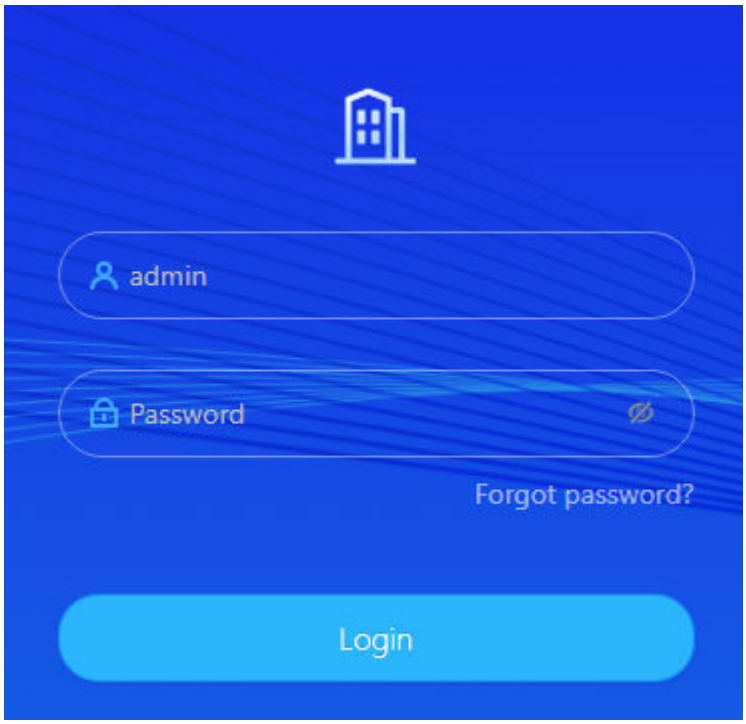
Procedure

Step 1 Go to the IP address of the VTO in the browser.

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

Step 2 Enter **admin** as the username, and enter the password you set during initialization, and then click **Login**.

Figure 3-1 Login



3.2 Resetting Password

Procedure

Step 1 On the login page, click **Forgot Password?** , and then click **Next**.

Step 2 Scan the QR code, and then you will get a string of numbers and letters.

Step 3 Send the string to the email account displayed on the page, and then the security code will be sent to the email address configured during initialization.

Step 4 Enter the security code in the input box, and then click **Next**.

- If you did not set an email address during initialization, contact your supplier or customer service for help.

- The security code will be valid only for 24 hours upon receipt.
- If you enter the wrong security code for 5 consecutive times, your account will be locked for 5 minutes.

Step 5 Enter and confirm the new password, and then click **OK**.

4 Home Page

Figure 4-1 Home page

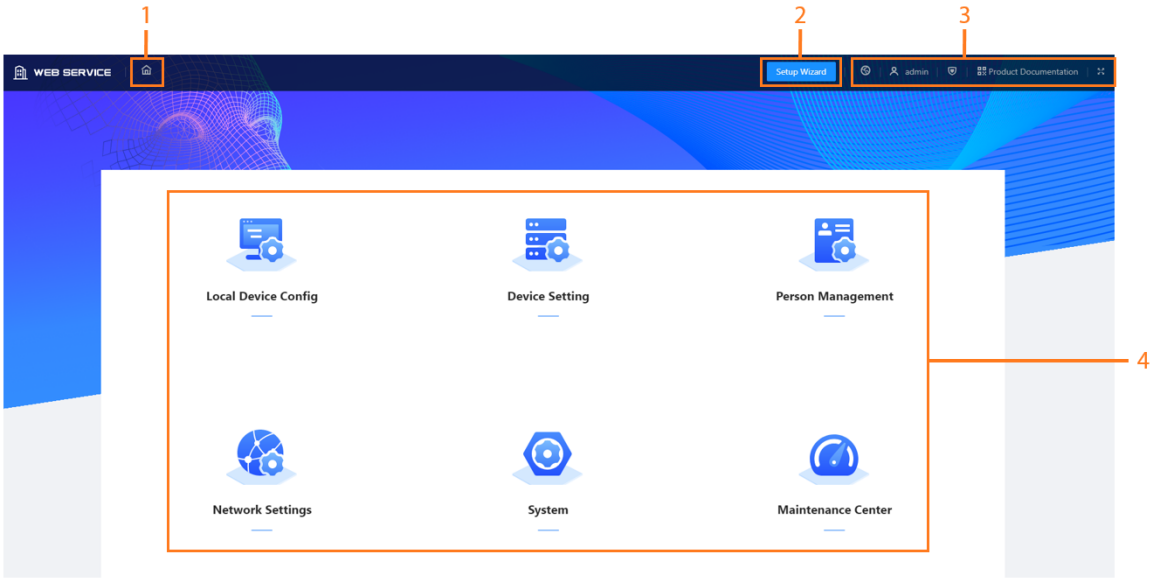


Table 4-1 Home page introduction

No.	Function	Description
1	Home button	Goes back to the home page.
2	Setup Wizard	Configure the VTO SIP server.
3	Navigation bar	• : Change language of the webpage of the VTO. • admin: Change password, log out of the current device, restart the system, and restore the device to factory settings. • : View and configure the security settings. • Product Documentation: Scan the QR code to get the product material. • : View the webpage in full screen mode.
4	VTO function	Different function areas of the VTO.

5 Setup Wizard

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

5.1 Setting as SIP Server

Set the VTO as the SIP server.

Prerequisites

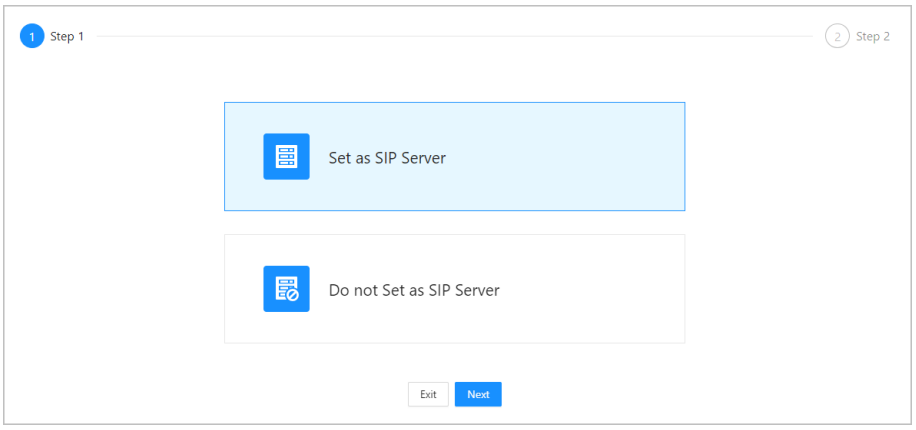
You have added VTOs on the webpage. If not, you can add them in **Set as SIP Server** page or in the **Device Setting** section.

Procedure

Step 1 Log in to the webpage of the VTO.

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

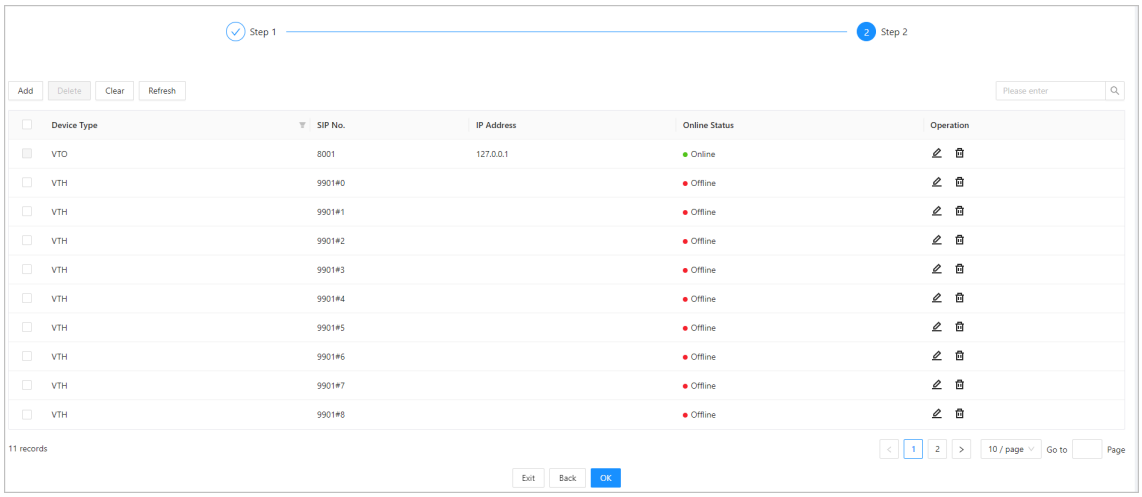
Figure 5-1 Set as SIP server



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

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

Figure 5-2 Select the SIP server



5.2 Not Setting as SIP Server

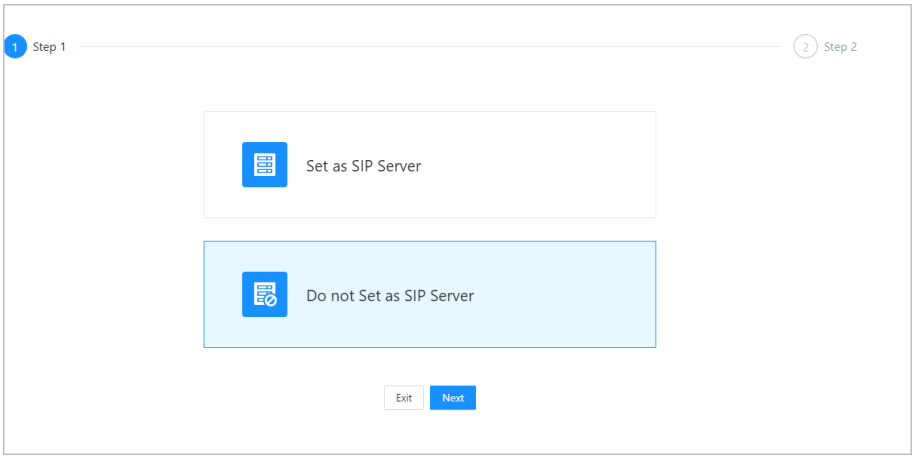
If you want to change the SIP server, you need to remove the current one from the list.

Procedure

Step 1 Log in to the webpage of the VTO.

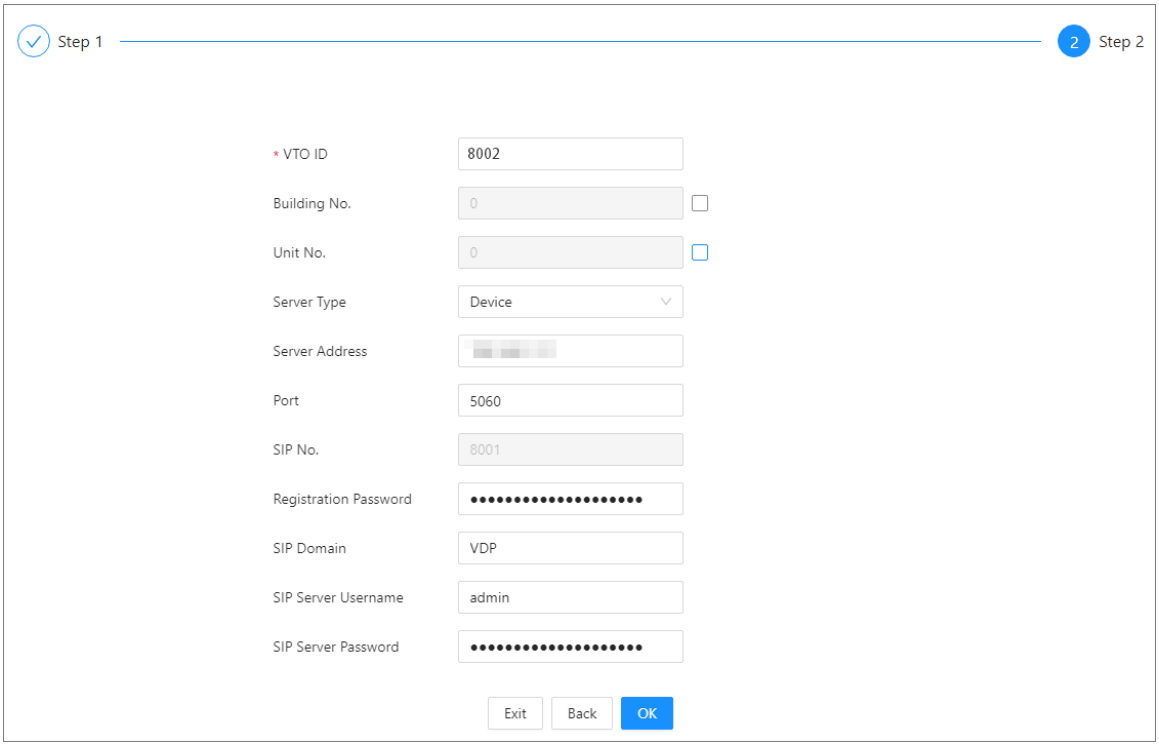
Step 2 Select **Setup Wizard** > **Do not Set as SIP Server**, and then click **Next**.

Figure 5-3 Do not set as SIP server



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

Figure 5-4 Configure information



6 Local Device Configuration

This chapter introduces the detailed configuration of the VTO.

Slight differences might be found in different models.

6.1 Basic Settings

Configure basic settings of the device.

Procedure

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

Step 2 Configure the parameters.

Figure 6-1 Basic settings (small apartment)

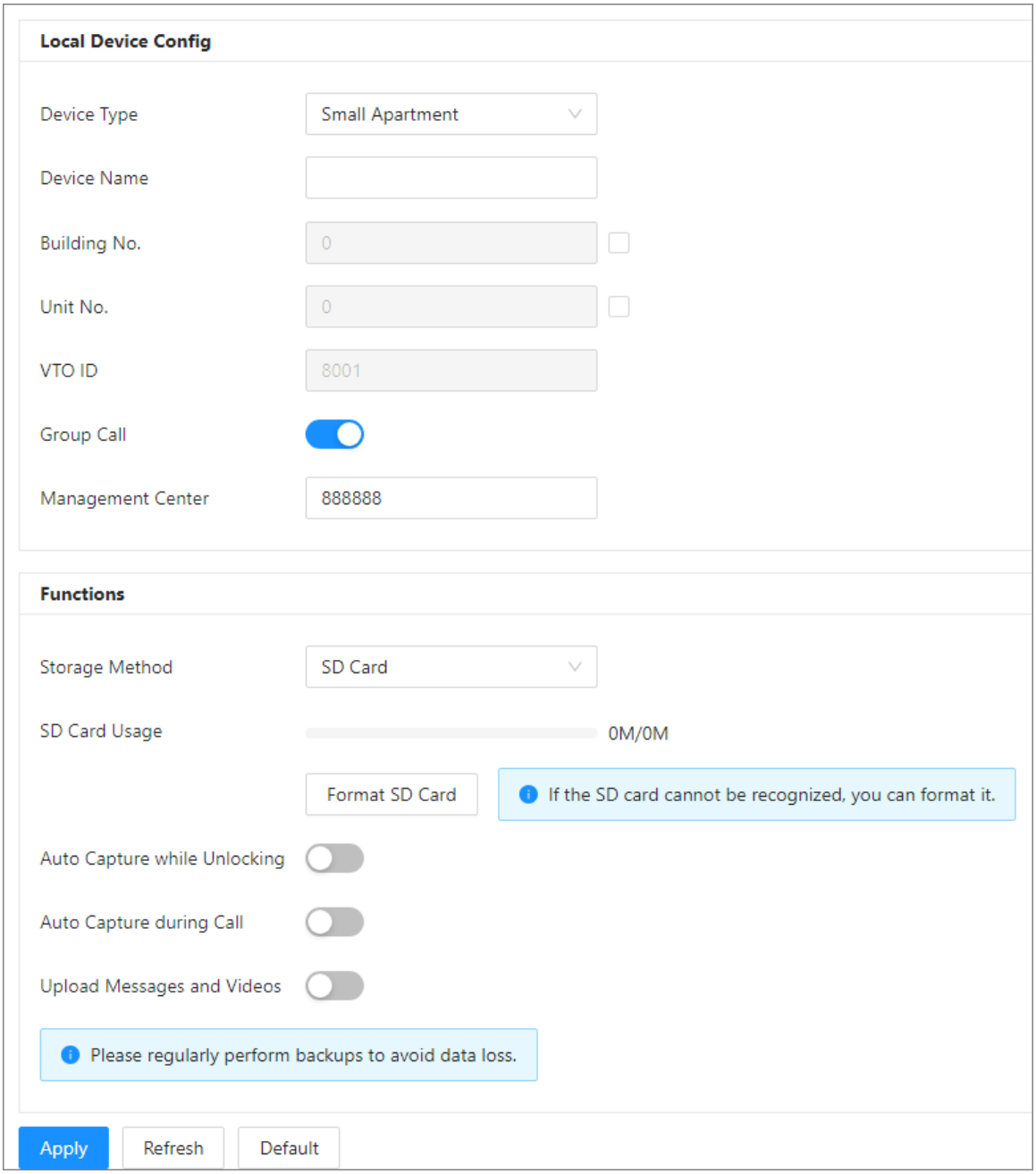


Figure 6-2 Basic settings (villa station)

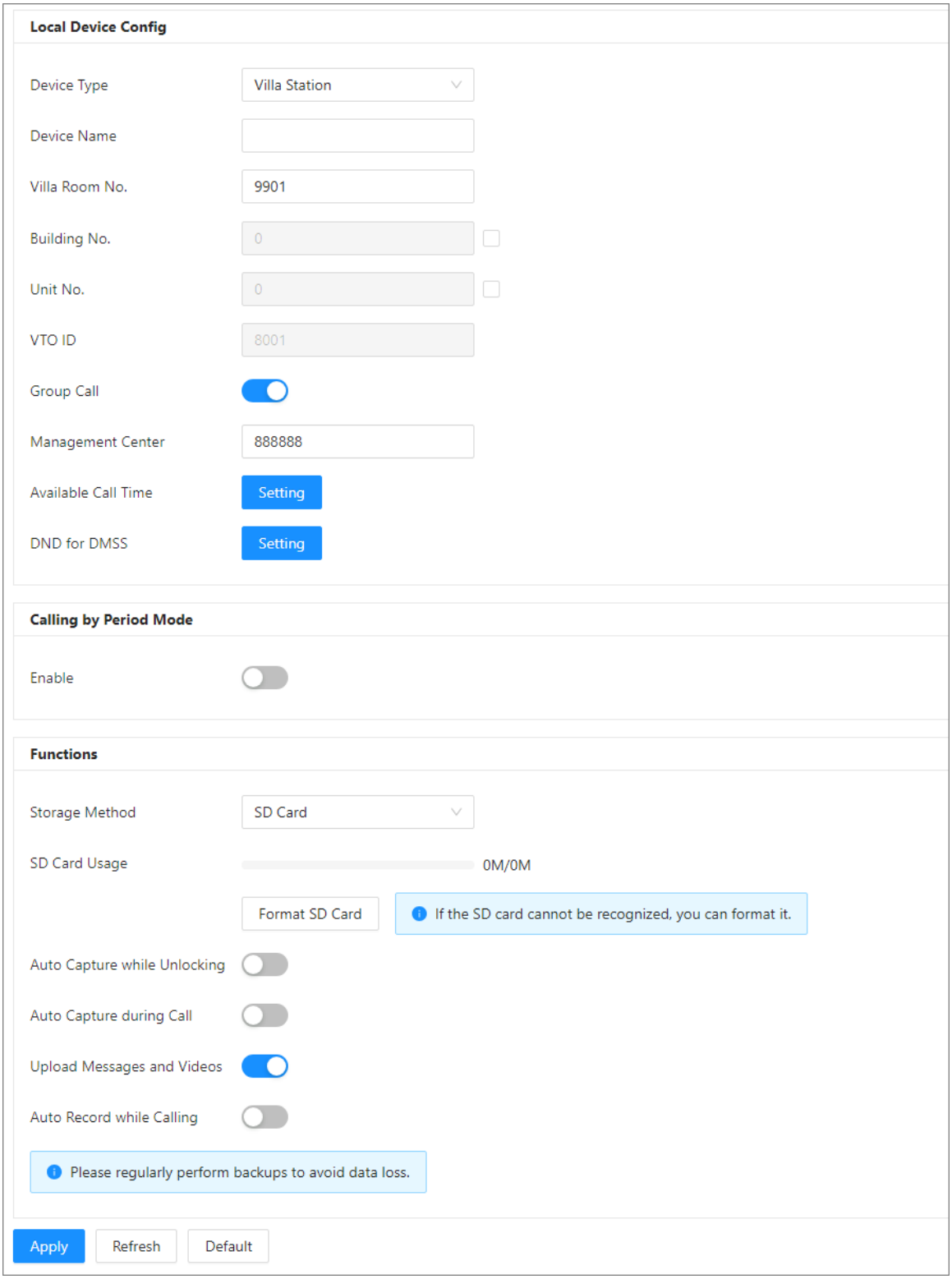


Figure 6-3 Basic settings (fence station)

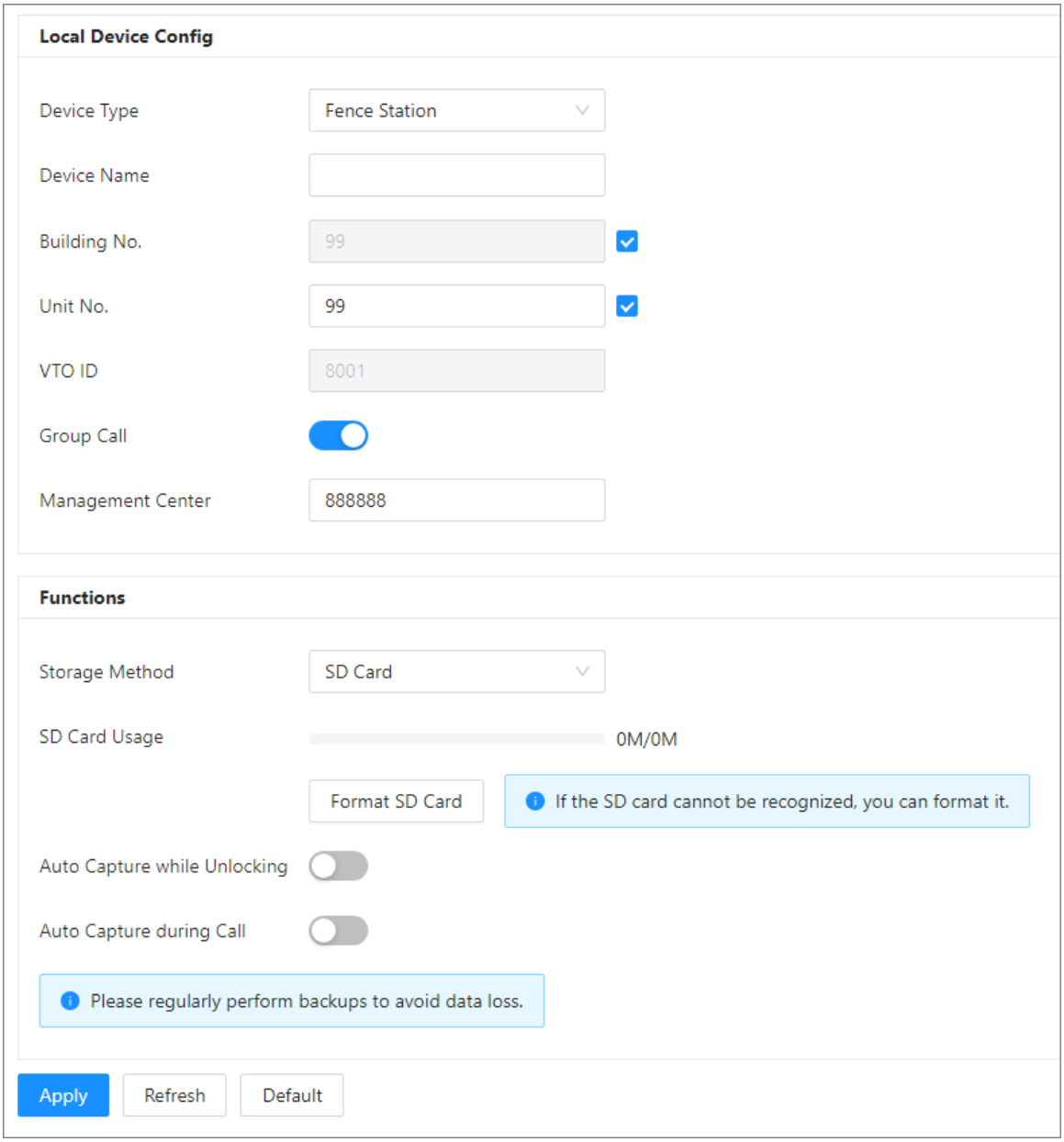


Table 6-1 Basic parameter description

Parameter	Description
Device Type	Select from **Villa Station** and **Small Apartment**. ● The small apartment is available on select models. ● If the device has been added to the DoLynk Pro, the type can not be modified.
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.

Parameter	Description
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 1 unit.
Unit No.	
VTO ID	Used to differentiate each VTO, and we recommend you set it according to unit or building number, and then you can add VTOs to the SIP server by using their numbers. The number cannot be changed when the VTO serves as the SIP server.
Group Call	Enable it on the VTO that works as the SIP server, and when a main VTH receives a call, all extension VTHs will also receive the call.
Management Center	888888 by default.
Available Call Time	The time period in which the VTO's calling to other devices is limited. Click **Setting** to set the time plan for calling.
DND for DMSS	The time period in which the calling to DMSS is not limited. Click **Setting** to set the time plan for calling.
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. • This function is only available when the mode is villa door station. • This function is available for the button  of the full keyboard module. • If the device is configured other keyboard modules, **Calling by Period Mode** of each modules can be configured in **Local Device Config** > **Layout**.
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.

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 enabled: • If an SD card is inserted in both the VTH and VTO, the video message will be saved both in the SD cards of the VTH and the VTO. • If an SD card is only inserted in the VTH or the VTO, the video message will be saved only in the SD card of the VTH or the VTO. • If no SD card is inserted in the VTH or VTO, no video message will be saved.
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**.

6.2 Access Control

6.2.1 Configuration

Procedure

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

Step 2 Configure the parameters.

Figure 6-4 Access control

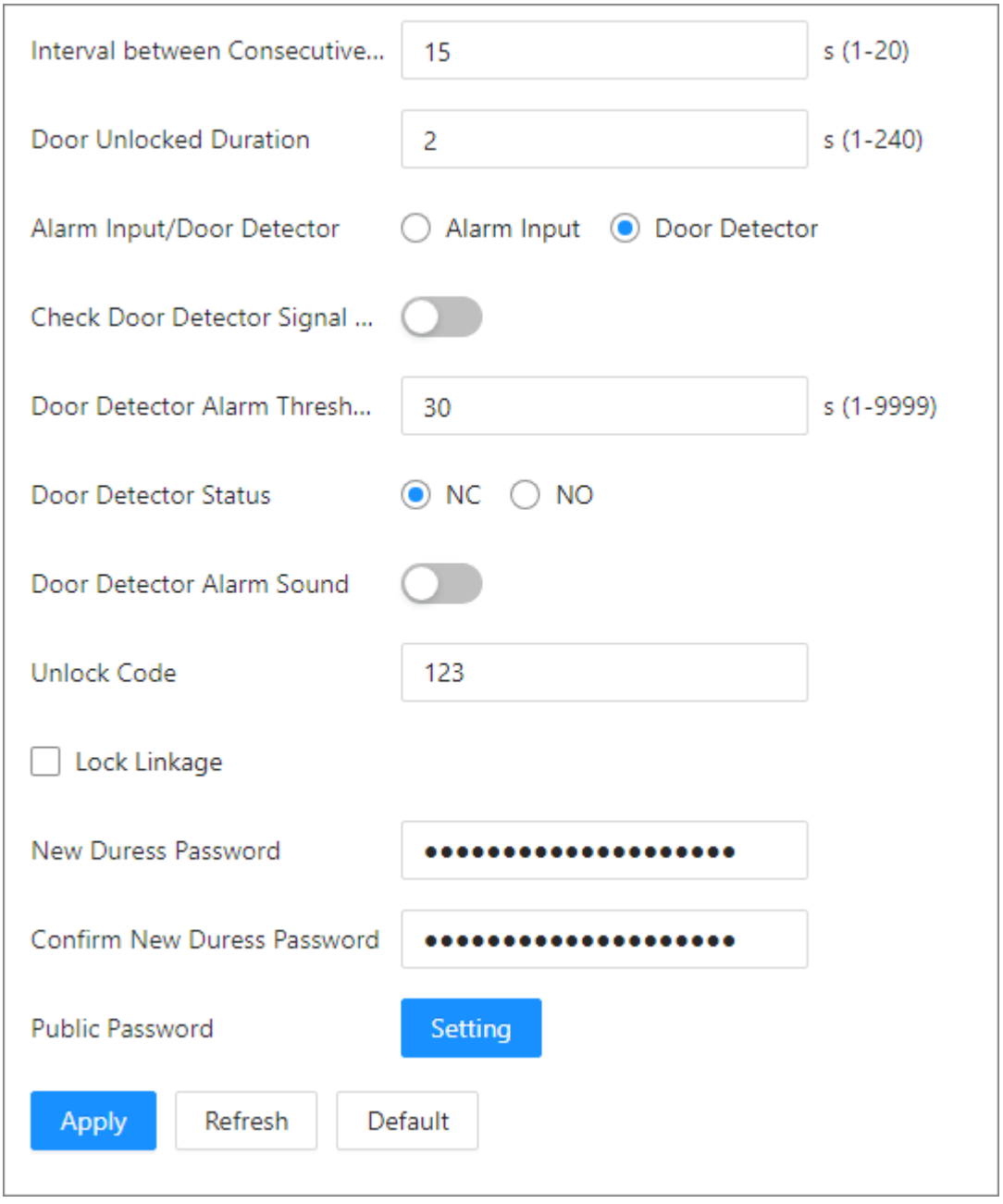


Table 6-2 Access control parameter description

Parameter	Description
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.
Alarm Input/Door Detector	Select one of them.
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.

Parameter	Description
Door Detector Status	• **NC** : Normally closed. • **NO** : Normally open.
Door Detector Alarm Sound	It is disabled by default. When it is enabled: • **Door Detector Status** is **NC**: If the door opening time exceeds the set door detection alarm threshold, the VTO will beep. And when the door detector is closed, the VTO does not beep again. • **Door Detector Status** is **NO**: If the door closing time exceeds the set door detection alarm threshold, the VTO will beep. And when the door detector is open, the VTO does not beep again.
Unlock Code	You can connect a third-party phone, such as a SIP phone, to the VTO, and use the code to open the door remotely.
Lock Linkage	Enable the **Lock Linkage**, and then select the linkage lock from the drop-down list.
New Duress Password	Enter and confirm the duress password.  When you enter the duress password. It will unlock the door normally and secretly trigger an alarm or notify management center at the same time.
Confirm New Duress Password	
Public Password	Click **Settings** to set the public password. You can add, export, and import the public password.

Step 3 Click **Apply**.

6.2.2 Extension Function

6.2.2.1 RS-485

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 6-5 RS-485

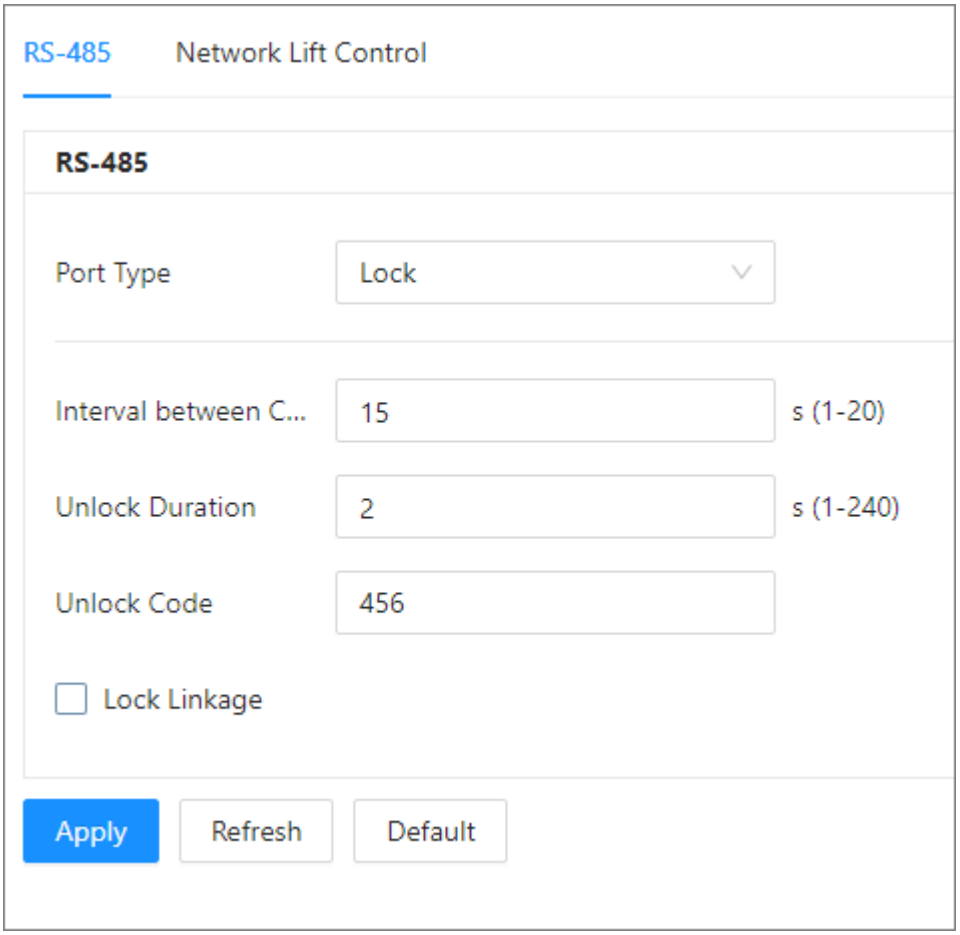


Table 6-3 RS-485 description

Parameter	Description
Port Type	Select **Lock** or **Card Reader** as the port type. It is **Lock** by default. When card reader is selected, fingerprint card reader and QR card reader are not supported.
Interval between Consecutive Unlocks	The door can only be unlocked again after the interval.
Unlock Duration	The time during which the lock stays unlocked.
Unlock Code	You can connect a third-party phone, such as a SIP phone, to the VTO, and use the command to open the door remotely. The default command is 456.
Lock Linkage	Enable the **Lock Linkage**, and then select the linkage lock from the drop-down list.

Step 3 Click **Apply**.

- When the 485 module of VTO linked with security module (DEE1010B) connects to card reader, the security module has a limit on the length of the entered password (10

digits supported). Therefore, room number (6 digits) + personal password (6 digits) can not unlock the door.

- When the 485 module of VTO linked with security module (DEE1010B) connects to QR card reader or fingerprint card reader, the door cannot be unlocked because the RS-485 of VTO does not support QR code and fingerprint transmission.
- When the 485 module of VTO linked with security module (DEE1010B) connects to card reader, cards cannot be issued through the 485 module and security module DEE1010B, because the 485 module does not support bidirectional command interaction.

6.2.2.2 Network Lift Control

The lock can be connected to network lift control.

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

Procedure

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

Step 2 Enable the network lift control.

Step 3 Configure the lift control.

Figure 6-6 Network lift control

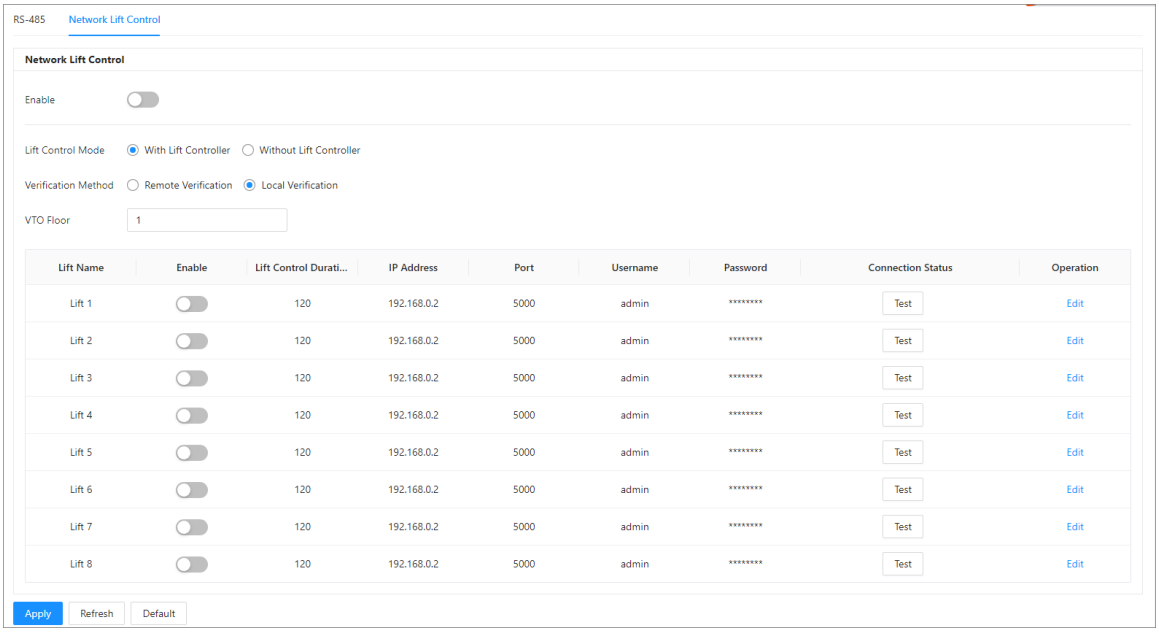


Table 6-4 Network lift control description

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.

Parameter	Description
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	Each lift controls up to 128 floors.

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

Figure 6-7 Set lift information

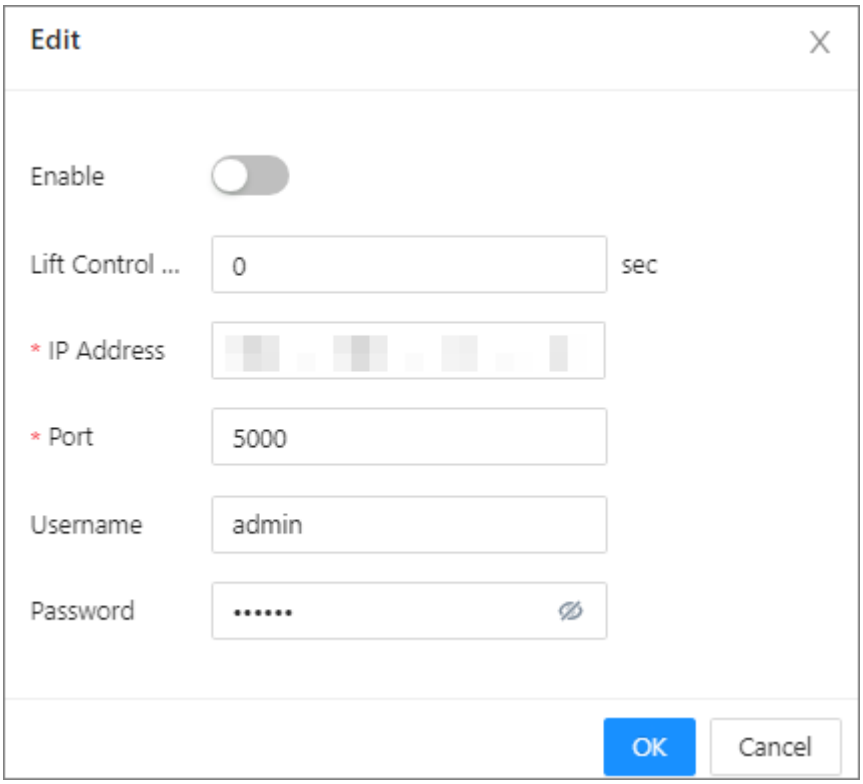


Table 6-5 Network lift control description

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

Step 5 Click **Apply**.

Related Operations

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

6.3 Light Control

Configure the illuminator as needed.

Procedure

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

Step 2 Set illuminator and device light modes 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 sets a suitable value.
- **Period** : The illuminator will be open during the defining period.

Turning off the illuminator will affect motion detection in dark environments.

Step 3 Click **Apply**.

6.4 Layout (Multiple Modules)

This function is only available for select models with multiple modules.

Procedure

Step 1 Log in to the webpage of the VTO.

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

Step 3 Click + to add modules.

Step 4 Click the button on the corresponding module to configure the related parameters.

You need to first configure the room number. Otherwise, you have no room number to select from in the module list. VTH room numbers are configured in **Device Setting**. For details, see "7.2 VTH Management".

Figure 6-8 Configure the layout

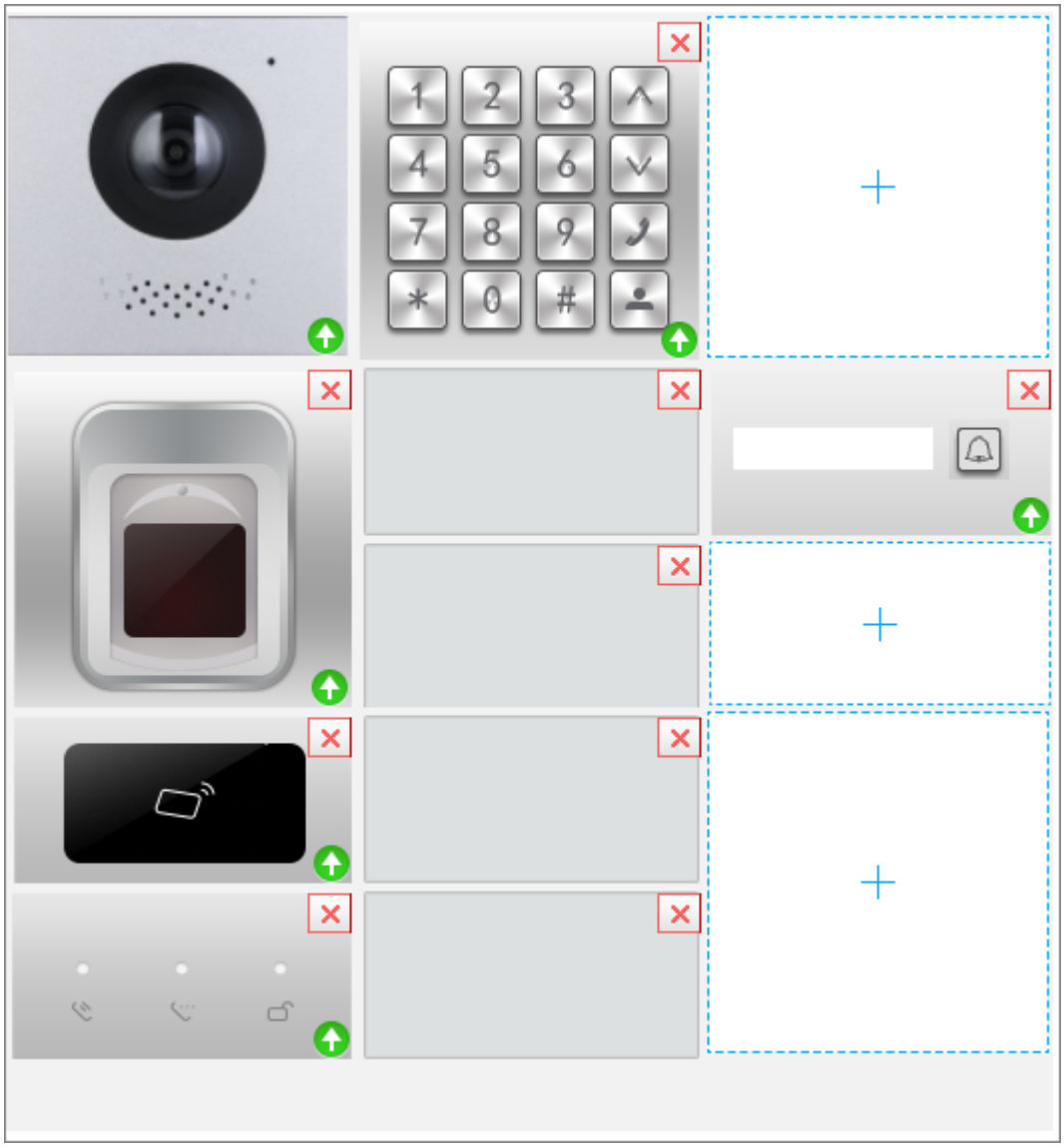


Figure 6-9 Configure the room number

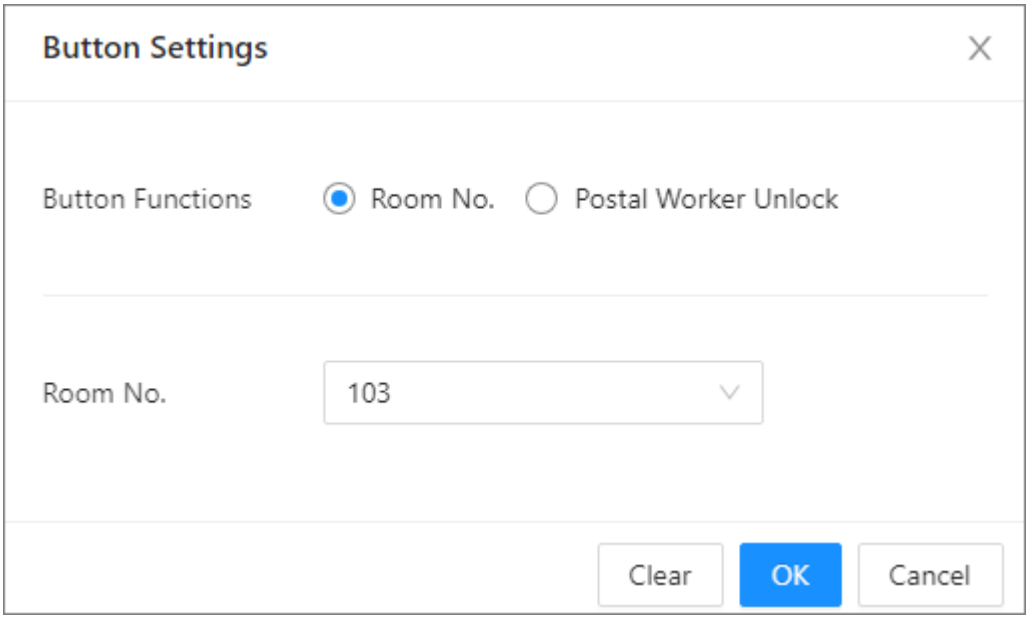


Figure 6-10 Configure the postal worker unlock

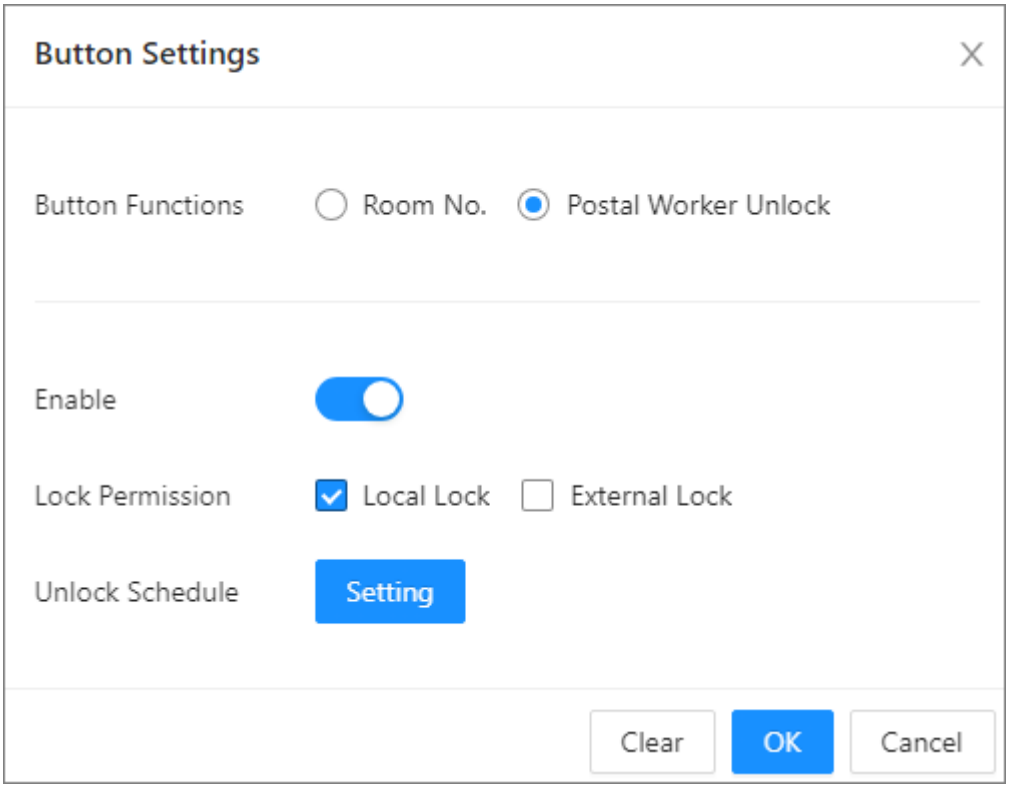


Table 6-6 Button parameters description

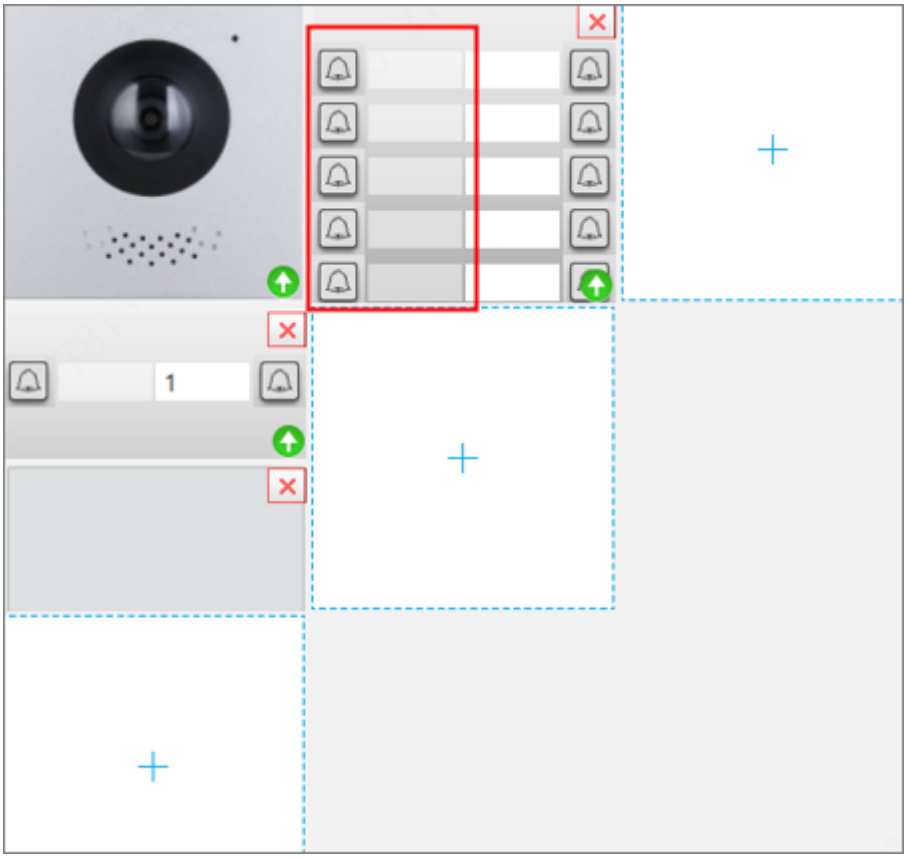
Parameter	Description
Room No.	Select the room number from the drop-down list.

Parameter	Description
Postal Worker Unlock	Configure the postal worker unlock. 1. Click to enable the function. 2. Set the lock permission from **Local Lock** and **External Lock**. 3. Click **Setting** to configure the unlock schedule. 4. Click **OK**.

Step 5 If you want to bind room numbers when you install other modules with nameplates for the VTO, repeat Step 3 to Step 4 until you have configured all of the room numbers.

When the two-button module, four-button module, and ten-button module are set to single-column button mode, the room number on the left button cannot be edited.

Figure 6-11 Non-editable buttons



Related Operations

Click to view the current version of the module or upload the update file to update the module.

6.5 Adding IPC

This function is available only when the SIP server is enabled and the device mode is set to small apartment.

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

6.5.1 Adding IPC One by One

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

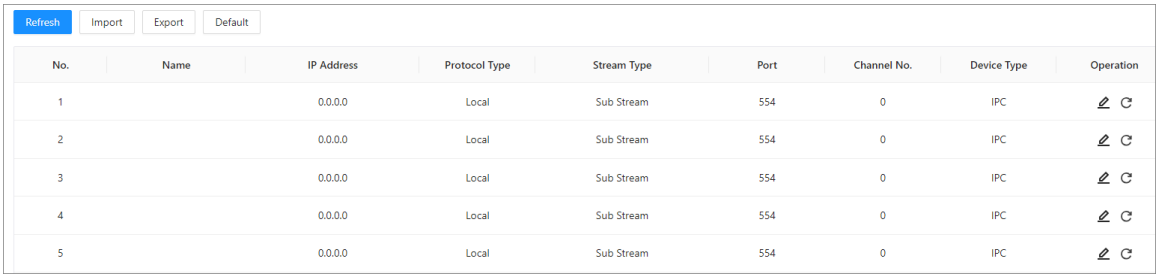
Only when the **Device Type** is set as **Small Apartment** and **Fence Station**, and the SIP function is enabled, this function can be available.

Procedure

Step 1 Log in to the webpage.

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

Figure 6-12 IPC information



Step 3 Click  to configure the parameters.

Figure 6-13 Configure the parameters

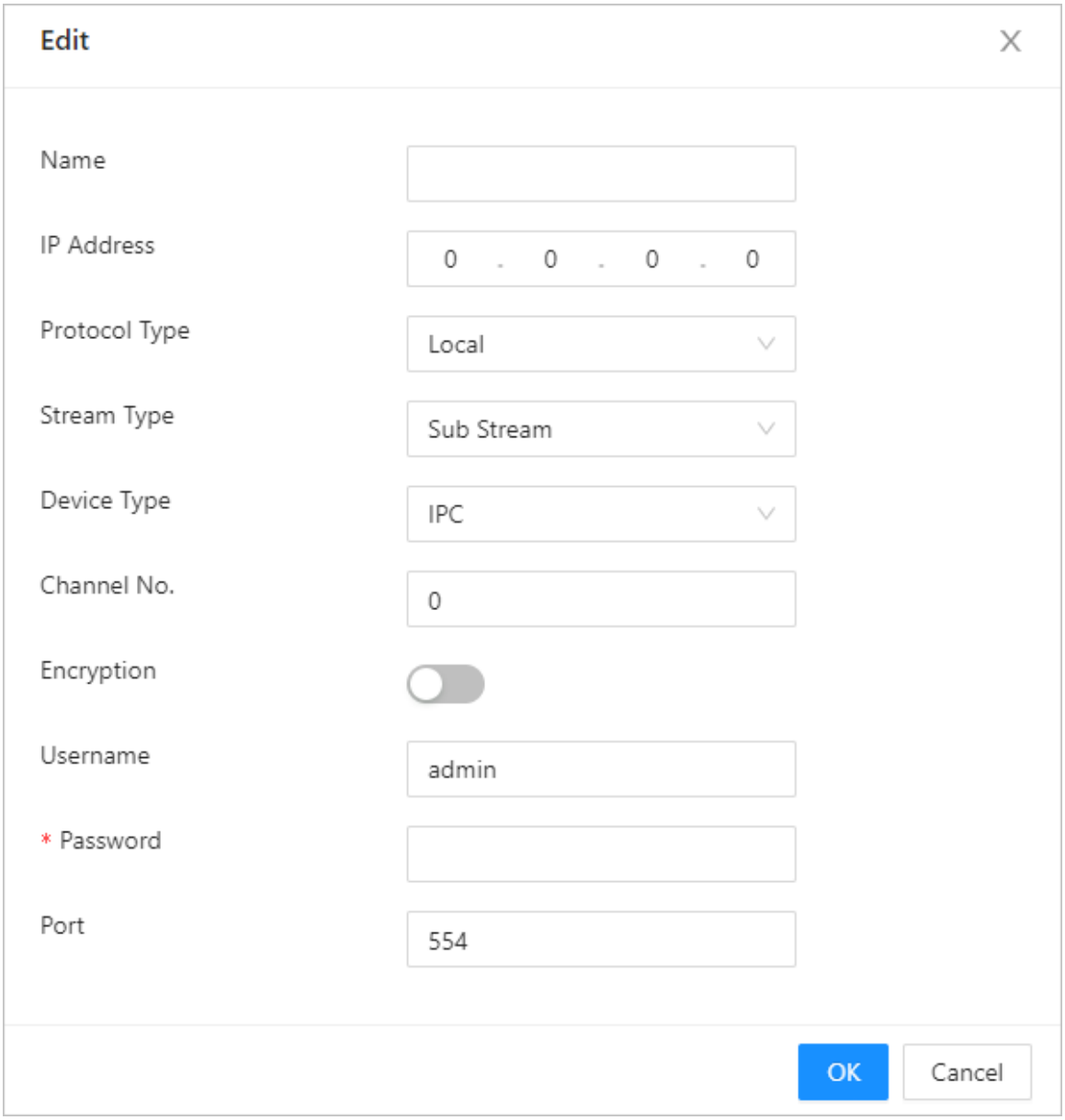


Table 6-7 Parameters description of the video monitoring device

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

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

Step 4 Click **OK**.

6.5.2 Exporting 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 login password, and then click **OK**.

The IPC configuration file is saved to the local computer.

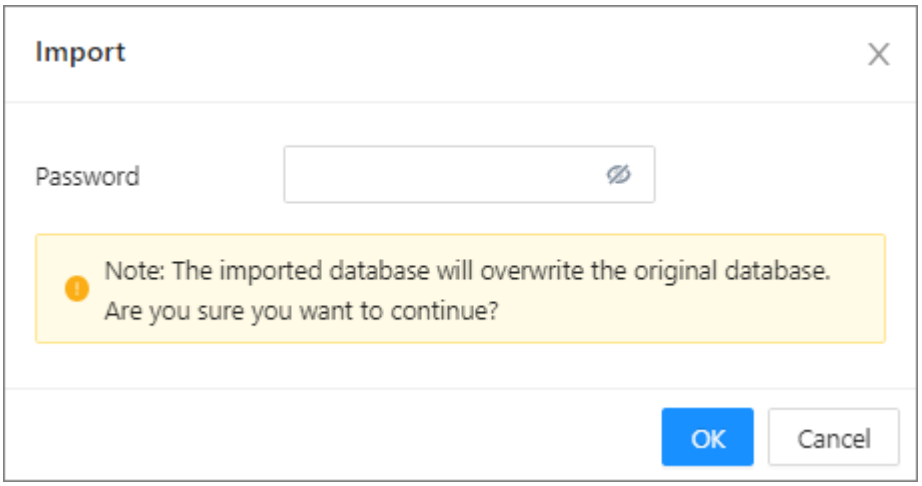
6.5.3 Importing IPC Information in Batches

Import the IPC information to the system.

Procedure

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

Figure 6-14 Import



Step 2 Select the file, and then click **Import**.

6.6 Card Settings

Procedure

Step 1 Log in to the webpage.

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

Figure 6-15 Card settings

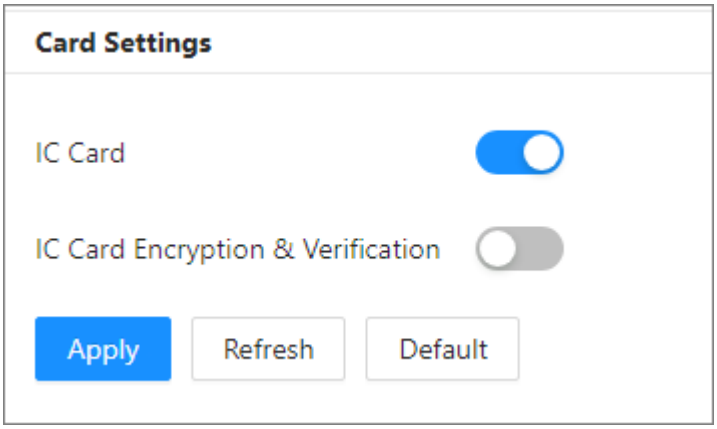


Table 6-8 Description of card parameters

Parameter	Description
IC Card	When enabled, IC card can be used to open the door.
IC Card Encryption & Verification	When enabled, the IC card is encrypted. Swipe the right card with successful encryption detection to open the door.

External card readers do not support encrypted IC cards.

Step 3 Click **Apply**.

7 Device Setting

This chapter introduces how to add, modify, and delete VTO, VTH, VTS, and IPC, and how to send messages from the SIP server to VTOs and VTHs when the VTO works as the SIP server. If you are using other servers as the SIP server, see the corresponding manual for details.

7.1 VTO Management

You can add VTOs to the SIP server, and all the VTOs connected to the same SIP server can call each other.

Procedure

Step 1 Log in to the webpage of the VTO that works as the SIP server.

Step 2 Select **Device Setting**.

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 7-1 Add VTO

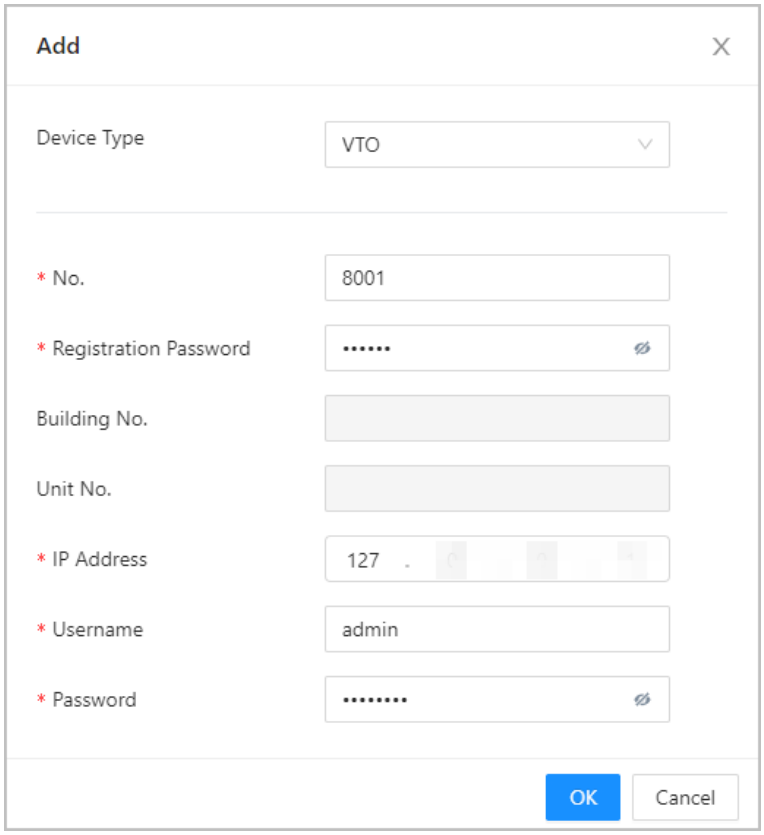


Table 7-1 Add VTO configuration

Parameter	Description
Device Type	Select **VTO**.
No.	The VTO number you configured.
Registration Password	Leave it as default.

Parameter	Description
Building No.	Available only when the platform servers or VTS work as the SIP server.
Unit No.	
IP Address	IP address of the VTO.
Username	User name and password used to log in to the webpage of the VTO.
Password	

Step 5 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.

7.2 VTH Management

You can add room numbers to the SIP server, and then configure the room number on the VTHs to connect them to the network.

Procedure

Step 1 Log in to the webpage of the SIP server.

Step 2 Select **Device Setting**.

Step 3 Click **Add**.

Step 4 Configure the parameters.

- Select the device type as **VTH**.

Figure 7-2 Add VTH one by one

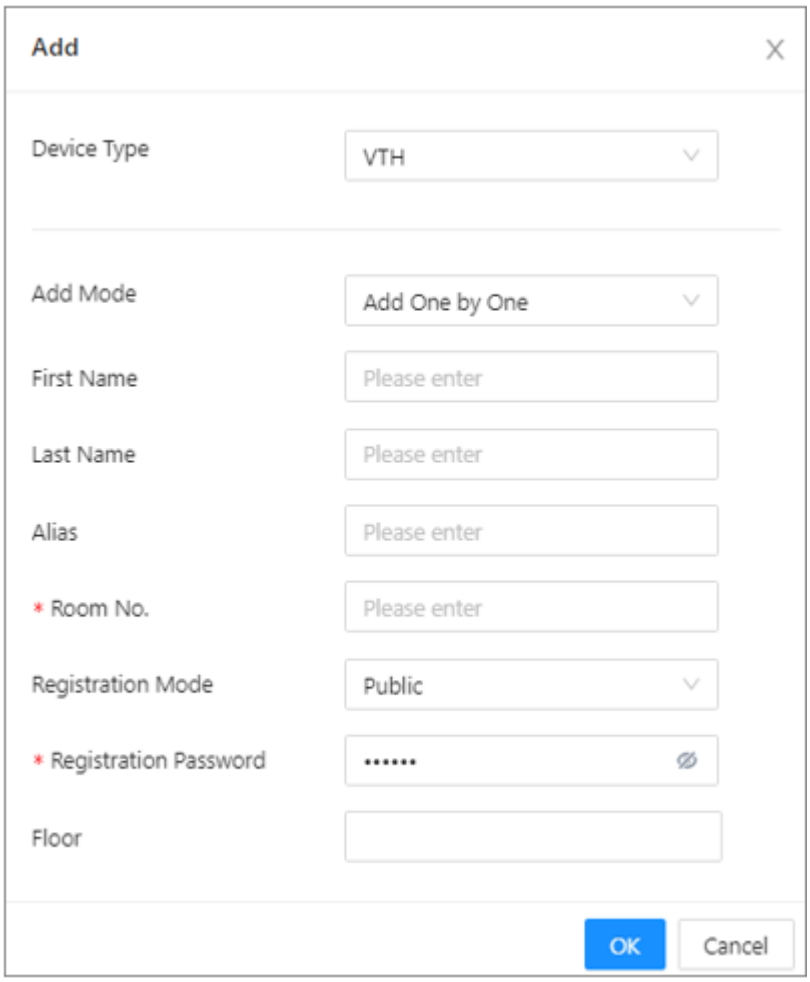


Table 7-2 Parameters description

Parameter	Description
First Name	Enter the information you need to differentiate each room.
Last Name	
Alias	
Room No.	Enter a room number, and then configure the number on a VTH to connect it to the network.
Registration Mode	Select **Public**.
Registration Password	Leave it as default.
Floor	Select the floor which can be given the permission. This parameter is available only when **Lift Control Mode** is selected as **With Lift Controller**.

- Select the add mode as **Add in Batches**.

  ◇ **Add in Batches** is not available when the device mode is set to villa.

◇ If the device has been added to the DoLynk Pro, the **Add in Batches** is not available.

Figure 7-3 Add VTH in batches

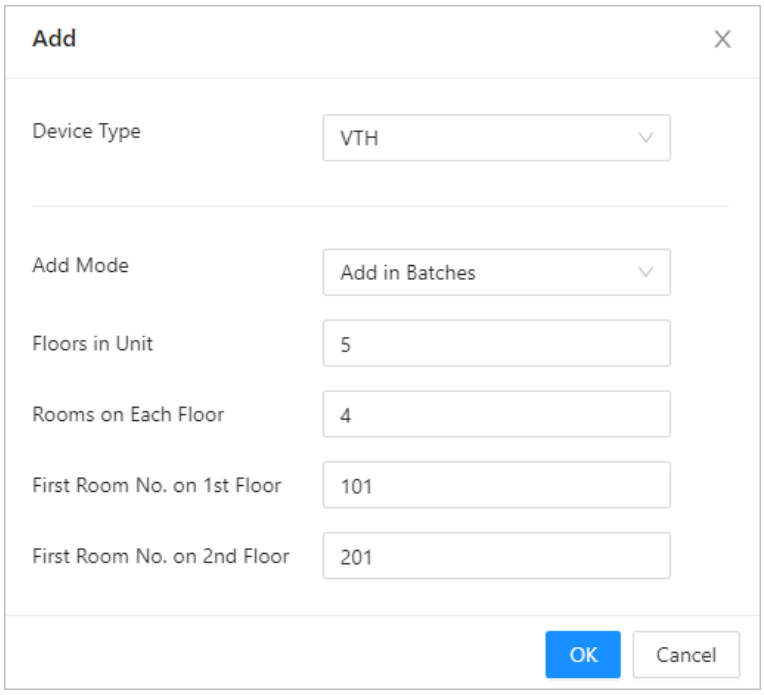


Table 7-3 Parameters description

Parameter	Description
Floors in Unit	Configure the numbers of floors and rooms.
Rooms on Each Floor	
First Room No. on 1st Floor	Configure the first room number on the first and second floor, the room number will be automatically generated.
First Room No. on 2nd Floor	

Step 5 Click **OK**.

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

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

7.3 VTS Management

You can add a VTS to the SIP server, and then it can be used as the management center. It can also manage, call, or receive calls from all the VTOs and VTHs in the network. See the corresponding user's manual for details.

Procedure

Step 1 Log in to the webpage of the VTO that works as the SIP server.

Step 2 Select **Device Setting**.

Step 3 Click **Add**.

Step 4 Configure the parameters.

Figure 7-4 Add VTS

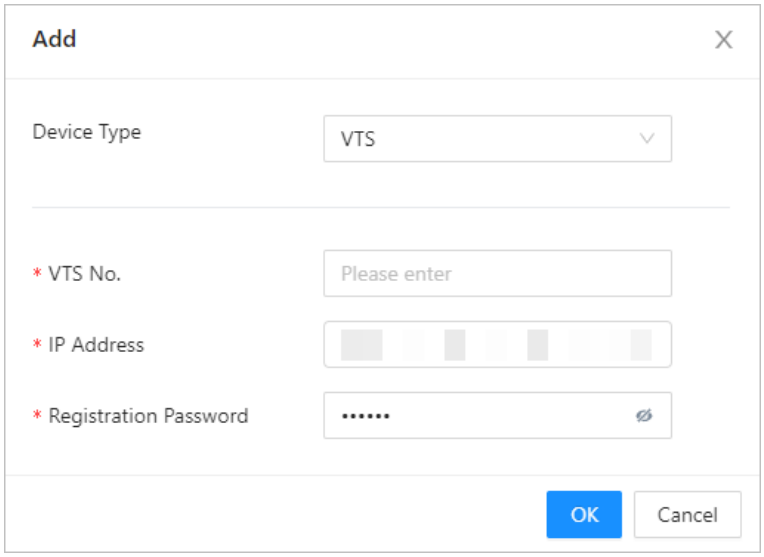


Table 7-4 Add VTS configuration

Parameter	Description
Device Type	Select **VTS**.
VTS No.	The number of the VTS.
Registration Password	Leave it as default.
IP Address	VTS IP address.

Step 5 Click **OK**.

8 Person Management

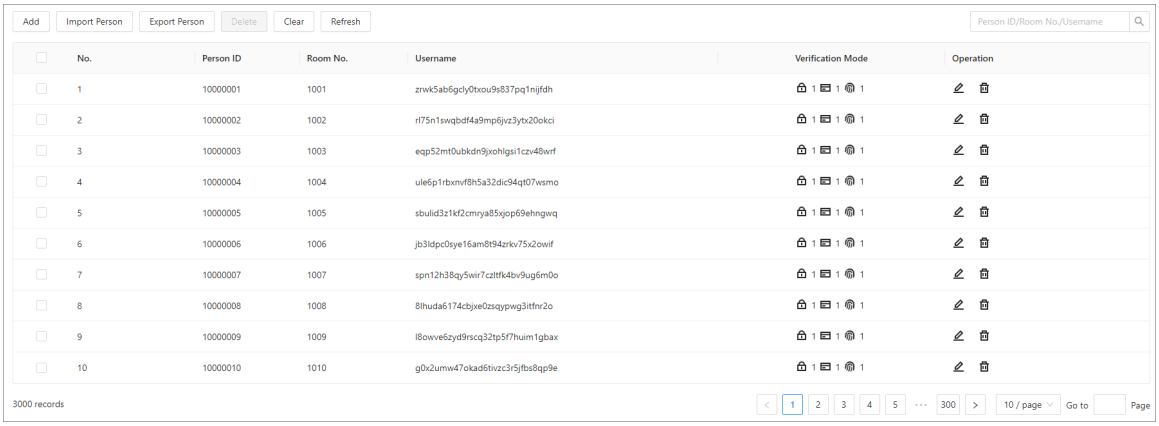
The card and fingerprint information that registered on the VTO will be uploaded to the person management in real time.

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Person Management**.

Figure 8-1 Person management



Step 3 Click **Add**.

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

Figure 8-2 Add the person

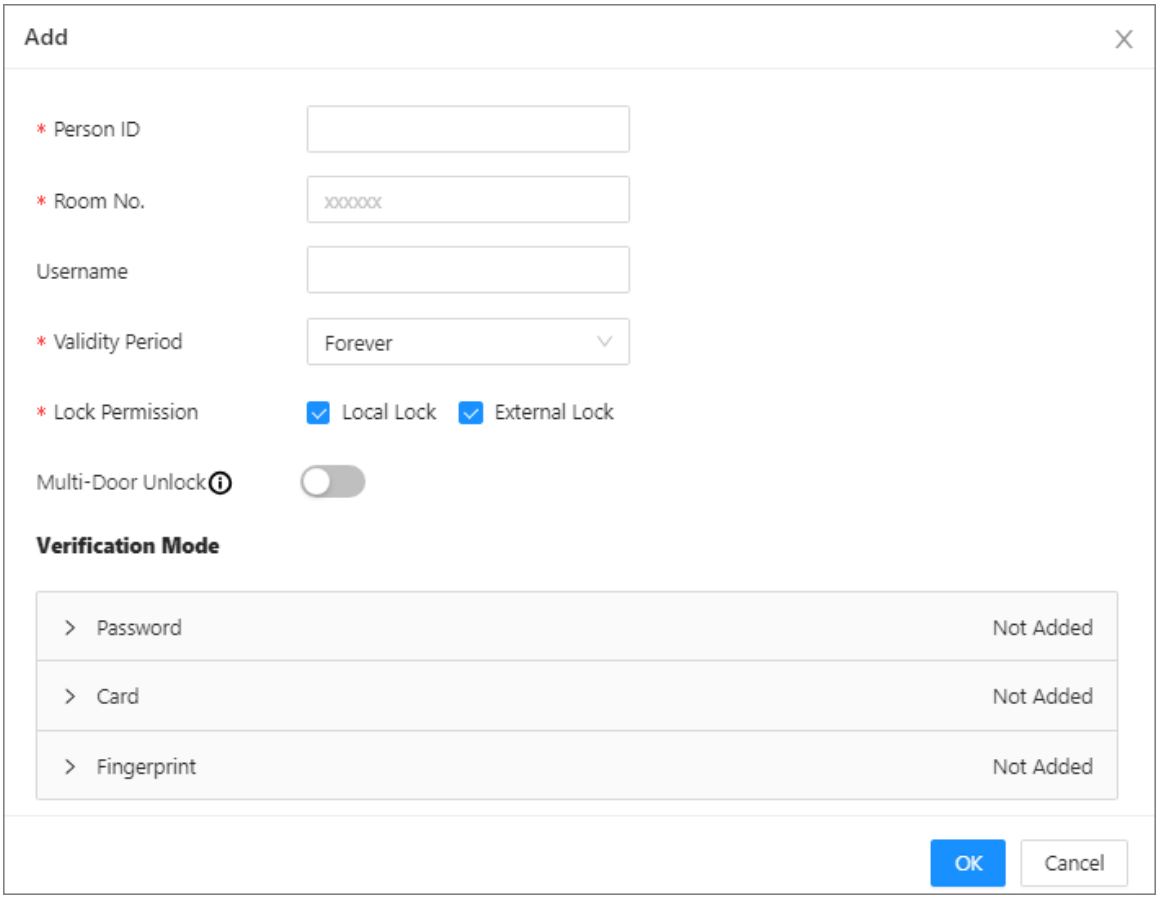


Table 8-1 Person parameters description

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

Parameter	Description
Card	1. Select **Card** > **Add**. 2. Enter the card number. Or you can click **Issue Card**, and then swipe the card on VTO. 3. Click **OK**. You can manage the cards through the following icons. ● / : Configure the card as the main card or general card. ● : If you lost your card, click 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	If a kind of modular device is added on **Local Device Config** > **Layout**, fingerprint is supported. 1. Select **Fingerprint** > **Add**. 2. Record your fingerprint according to the prompts. 3. Click **OK**.
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**.

Related Operations

- Click **Export Person**, and then enter the encryption password for the file to export the person information.
- Click **Import Person**, and then select the file to import the person information.

9 Network Settings

This chapter introduces how to configure the network parameters.

9.1 TCP/IP

You need to configure the TCP/IP information to connect the VTO to the network.

Procedure

Step 1 Log in to the webpage of the VTO.

Step 2 Select **Network Settings** > **TCP/IP**.

Step 3 Configure the TCP/IP parameters.

Figure 9-1 TCP/IP

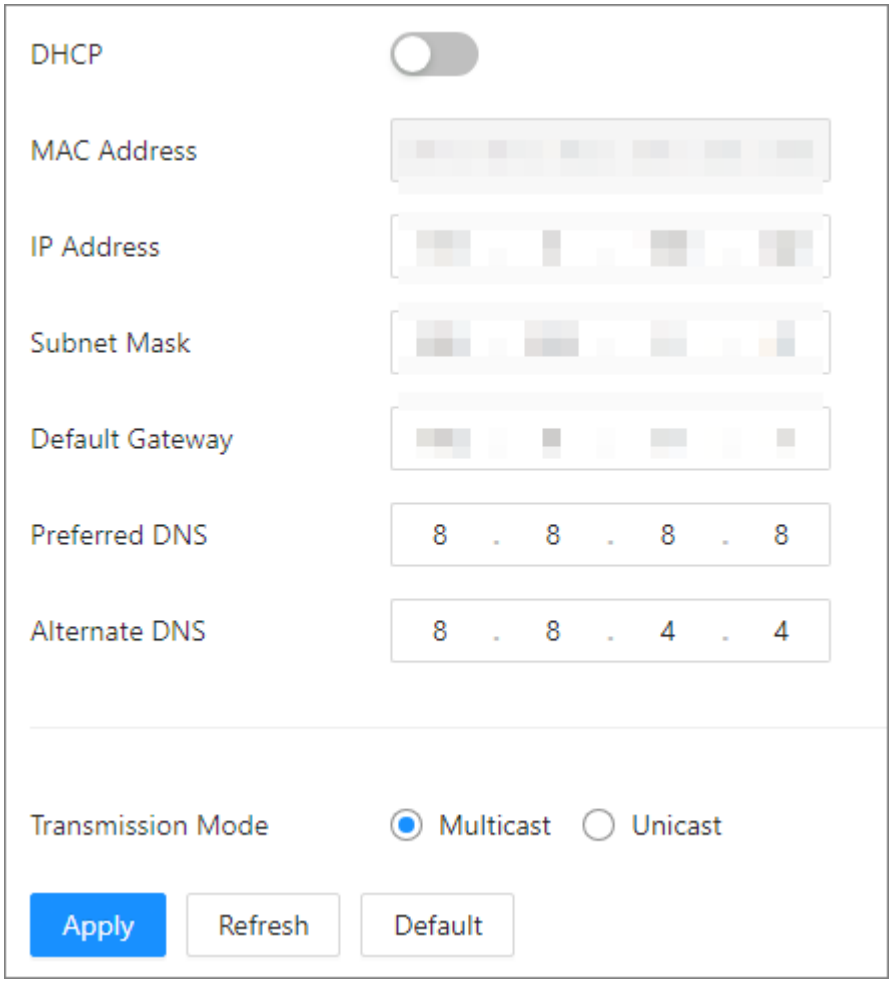


Table 9-1 Parameter description

Parameter	Description
DHCP	Automatically assigns IP addresses and other network configuration parameters.
IP Address	Your planned IP address for the VTO.

Parameter	Description
Preferred DNS	It is 8.8.8.8 by default.
Alternate DNS	It is 8.8.4.4 by default.
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 4 Click **Apply**.

9.2 Port

Procedure

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

Step 2 Configure the parameters.

Figure 9-2 Port

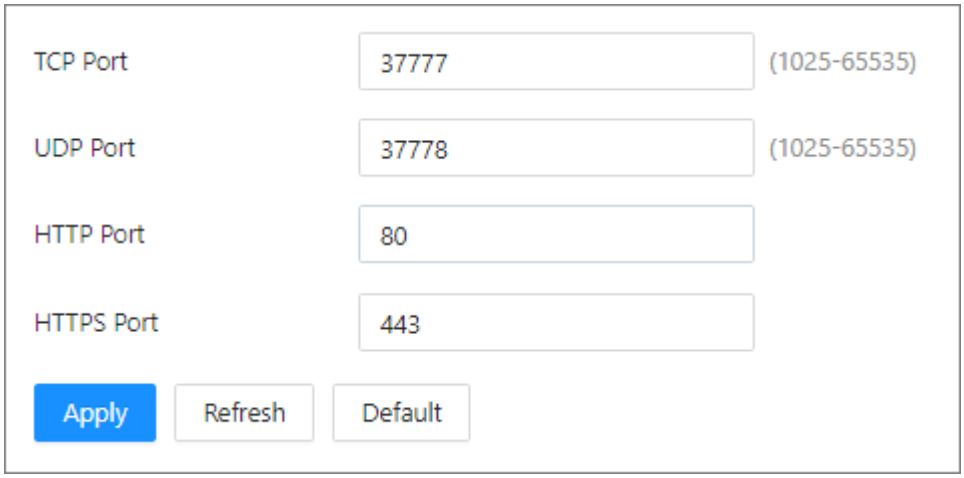


Table 9-2 Parameter description

Parameter	Description
HTTP Port	You can now enter http://VTO IP address: HTTP Port to log in to the VTO.
TCP/UDP Port	Used for accessing the VTO with devices in other networks.
HTTPS Port	You can now enter https://VTO IP address: HTTPS Port to log in to the VTO.

Step 3 Click **Apply**.

9.3 SIP Server

There must be a SIP server in the network for all connected VTOs and VTHs to call each other. You can use a VTO or other servers as the SIP server.

Procedure

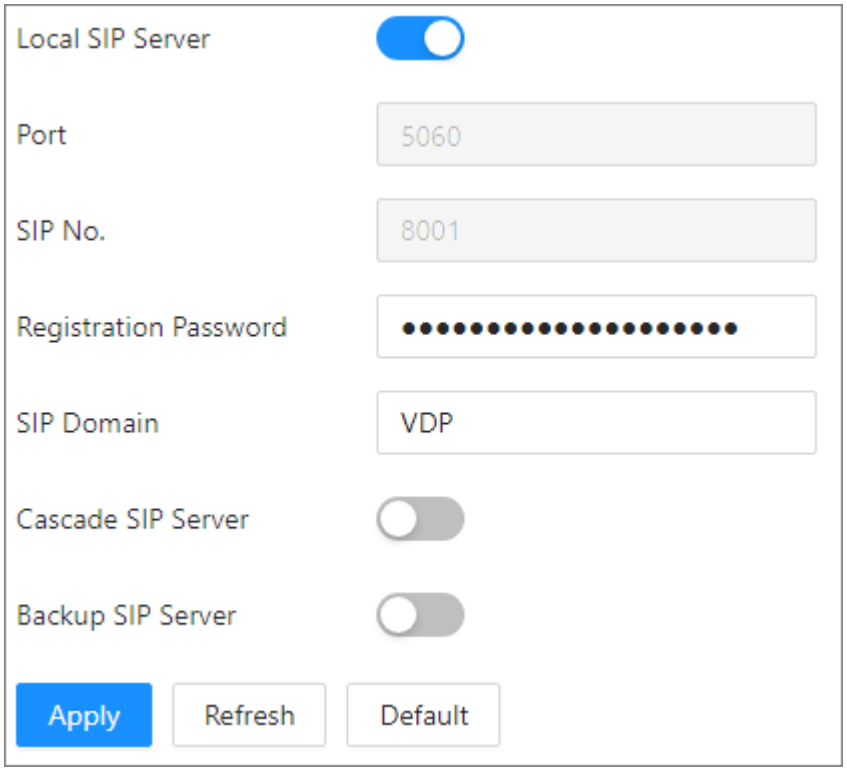
Step 1 Select **Network Settings** > **SIP Server**.

Step 2 Select a server type.

- The VTO you have logged in as the SIP server: Enable **Local SIP Server**, and then configure the parameters for the VTO.

  Some parameters would become grey after enabling the **Local SIP Server** function.

  Figure 9-3 Current VTO as SIP server



- If another VTO works as the SIP server: Select the SIP type as **Device**, and then configure the parameters for the VTO working as the SIP.

  If the VTO you have logged in does not work as the SIP server, do not enable **Local SIP Server**. Otherwise, the connection would fail.

Figure 9-4 Another VTO as SIP server

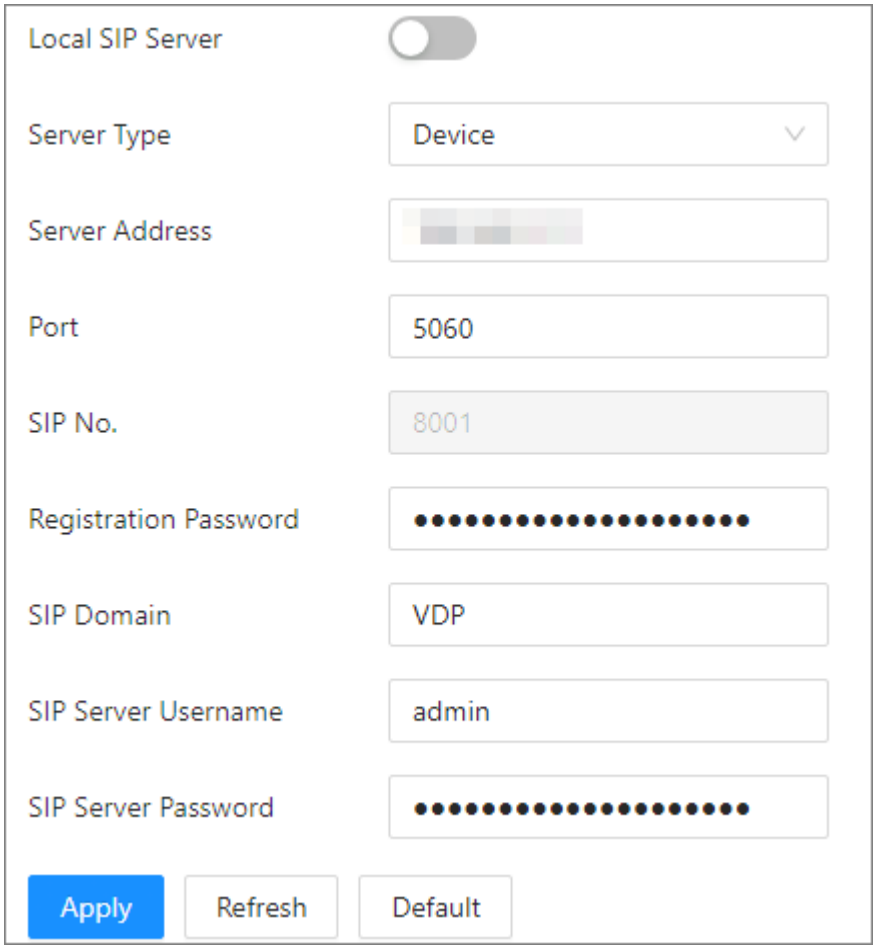


Table 9-3 SIP server configuration (VTO as the SIP server)

Parameter	Description
Server Address	Planned IP address of the VTO.
Port	5060 by default.
SIP No.	VDP by default. Leave it as default.
Registration Password	
SIP Domain	
SIP Server Username	Username and password used to log into the webpage of the SIP server.
SIP Server Password	

- The DSS platform works as the SIP server: Set **Private SIP Server** as **Server Type**, and then configure the parameters.

Figure 9-5 Private SIP server

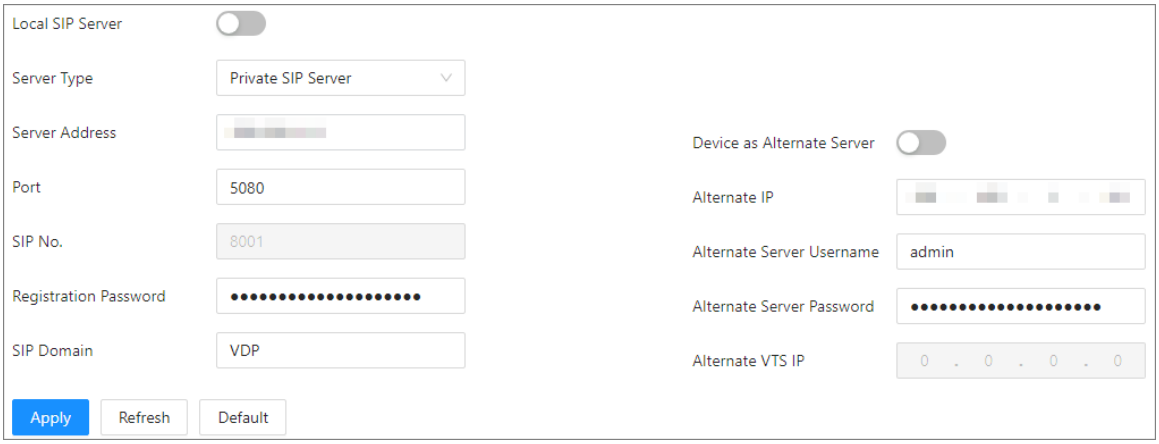


Table 9-4 SIP server description (platform as the SIP server)

Parameter	Description
Server Address	IP address of the SIP server.
Port	5080 by default when the platform works as the SIP server.
SIP No.	Leave it by default.
Registration Password	
SIP Domain	
Device as Alternate Server	Enable it so that you can configure the Alternate VTS IP.
Alternate IP	The alternate server will be used as the SIP server when Express or DSS stops responding. We recommend you configure the alternate IP address. ◇ If you enable **Device as Alternate Server**, the current VTO you have logged in serves as the alternate server. ◇ If you want another VTO serve as the alternate server, you need to enter the IP address of that VTO in the **Alternate IP** textbox. Do not enable **Device as Alternate Server** in this case.
Alternate Server Username/ Password	Used to log in to the alternate server.
Alternate VTS IP	IP address of the alternate VTS.

- The third-party server works as the SIP server: Set **Third-party Server** as **Server Type**, and then configure the parameters.

Figure 9-6 Third-party server

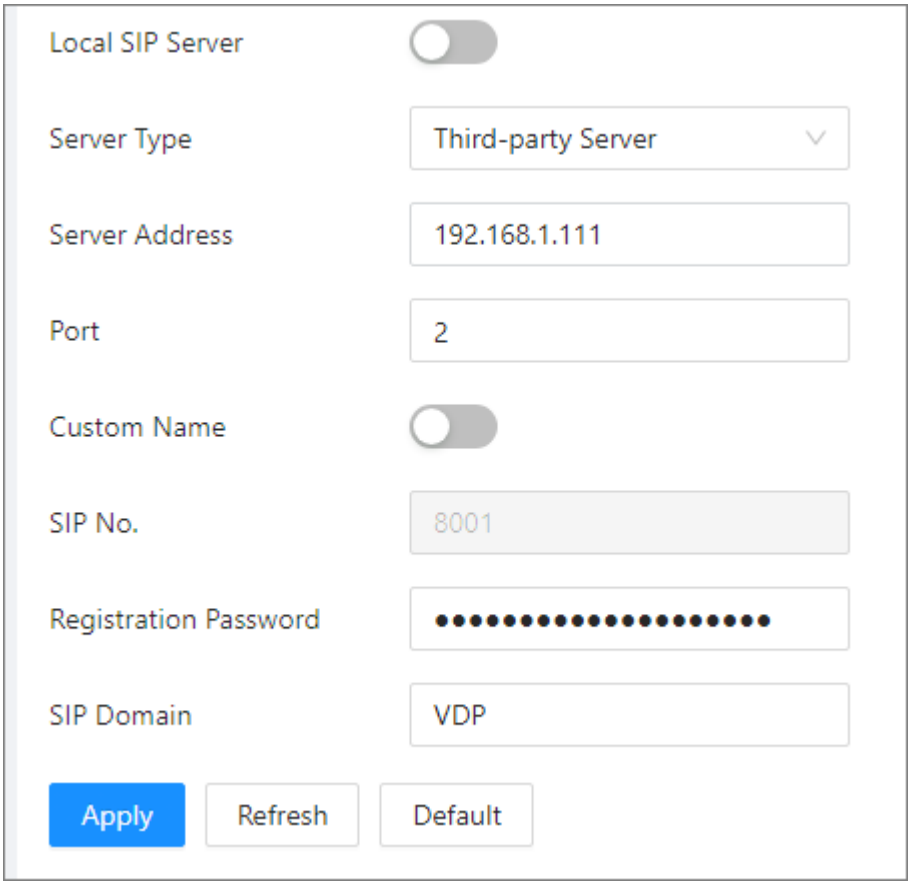


Table 9-5 SIP server description (Third-party server as the SIP server)

Parameter	Description
Server Address	IP address of the SIP server.
Port	5080 by default when the platform works as the SIP server.
SIP No.	Leave it by default.
Registration Password	
SIP Domain	

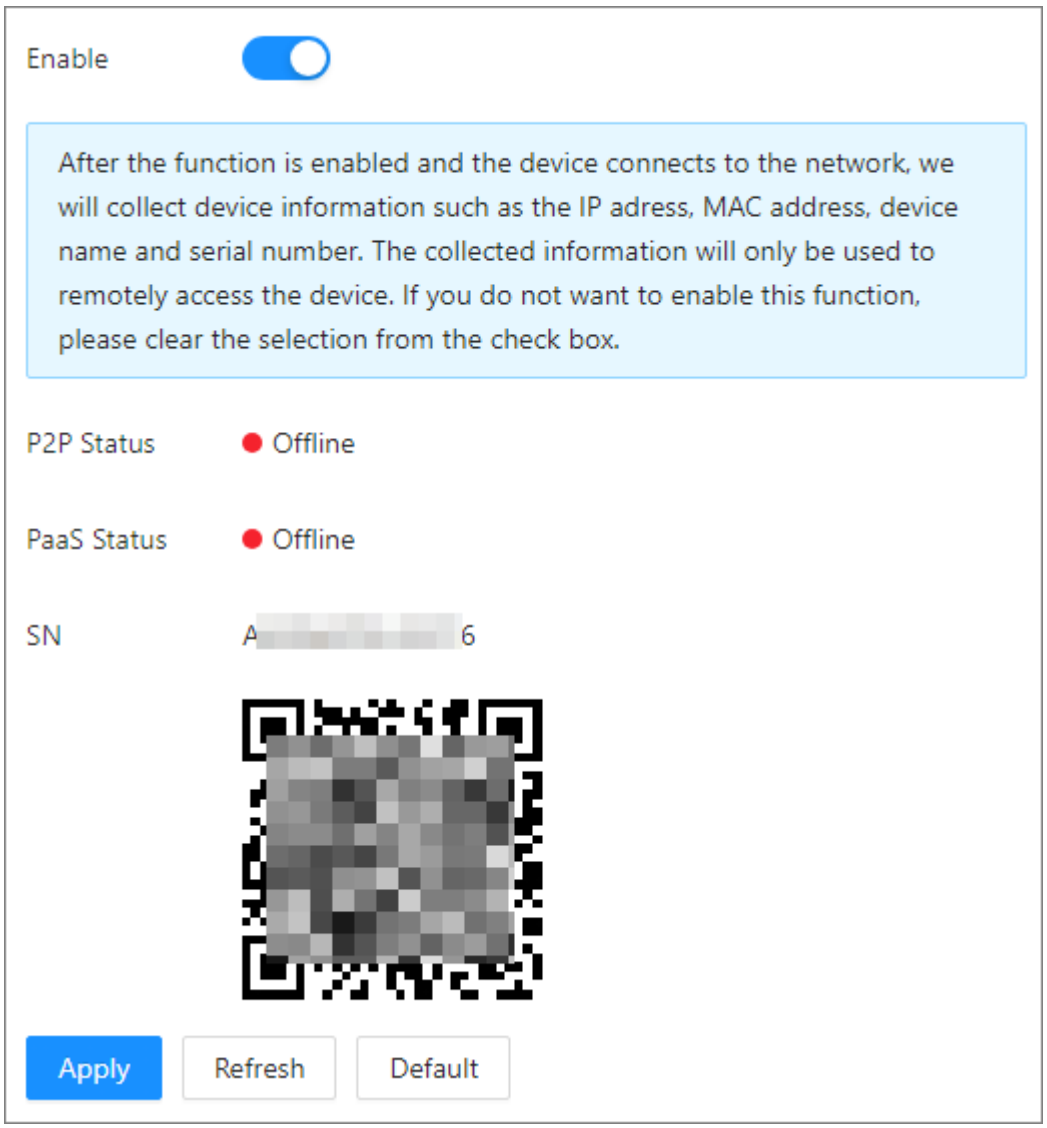
Step 3 Click **Apply**.

- 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.

9.4 Cloud Service

Enable the **Cloud Service** function, and then you can scan the QR code with your phone to add the VTO to the app on your phone.

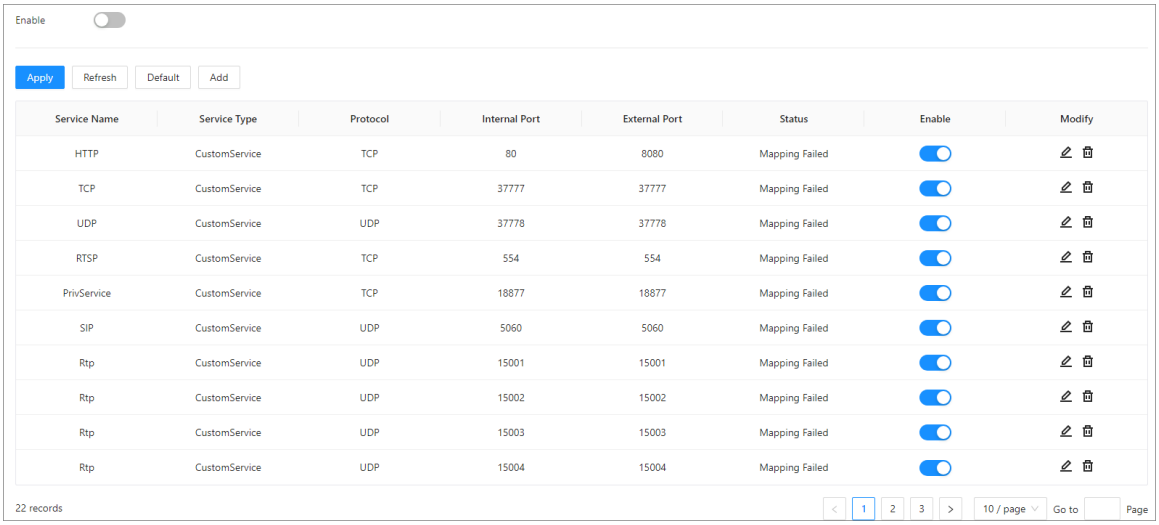
Figure 9-7 Cloud service



9.5 UPnP

When the VTO works as the SIP server, you can configure the UPnP function to allow WAN devices to log in to the VTO.

Figure 9-8 UPnP



Preparation

- Enable the UPnP function on the router, and then configure a WAN IP address for the router.
- Connect the VTO to the LAN port of the router.

9.5.1 Enabling UPnP Services

Procedure

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

Step 2 Select the services listed, and then click **Enable**.

Step 3 Click **Apply**.

9.5.2 Adding UPnP Services

Procedure

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

Step 2 Click **Add**.

Step 3 Configure the parameters, and then click **OK**.

Figure 9-9 Add a UPnP service

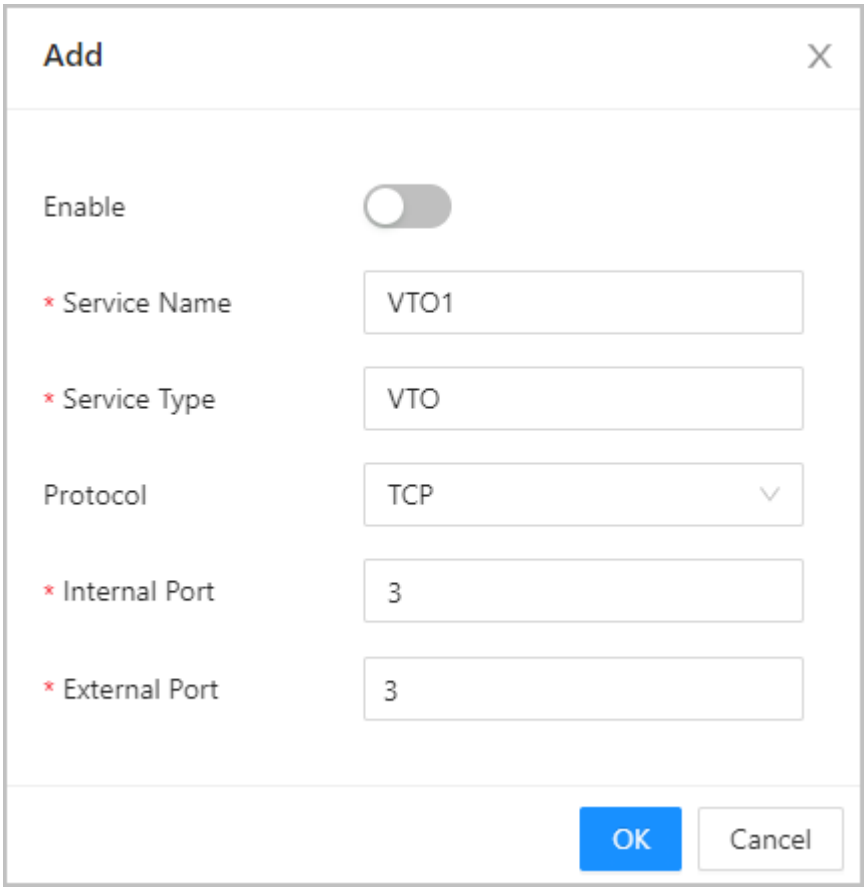


Table 9-6 Parameter description

Parameter	Description
Service Name	Enter the name and type of the service.
Service Type	
Protocol	Select **TCP** or **UDP**.
Internal Port	Internal port of the service. ● If you need to configure this function for multiple devices, make sure that the ports are not the same. ● The port number you use must not be occupied. ● The internal and external port number must be the same.
External Port	External port of the service. ● If you need to configure this function for multiple devices, make sure that the ports are not the same. ● The port number you use must not be occupied. ● The internal and external port number must be the same.

9.6 Basic Services

Configure functions that involve device security.

Procedure

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

Step 2 Enable the security functions based on your needs.

Figure 9-10 Basic services

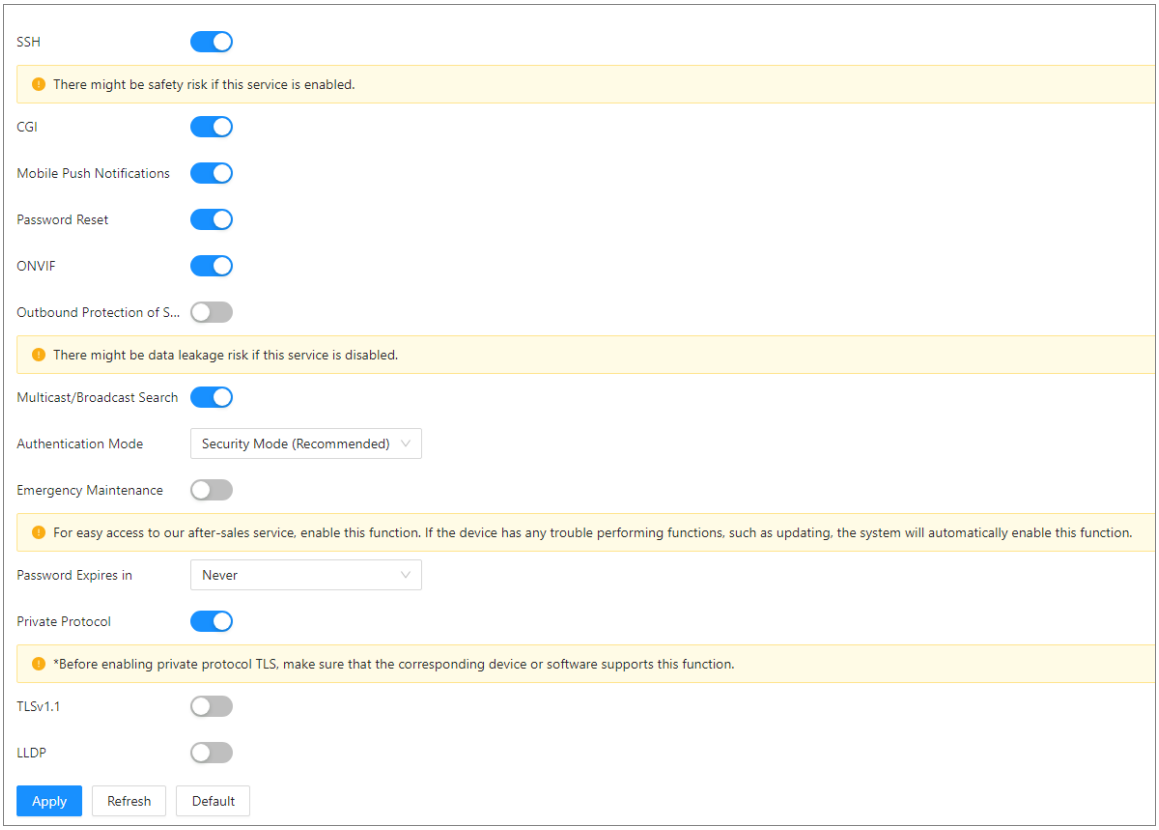


Table 9-7 Security parameter description

Parameter	Description
SSH	A secure alternative to unsecured remote protocols. We recommend you turn it off because there might be safety risk if this service is enabled.
CGI	The use of CGI command. We recommend you turn it off. Otherwise, the VTO might be exposed to security risks and data leakage.
Mobile Push Notification	Send information to the app on the phone. We recommend you turn it off if you do not need this function. Otherwise, the VTO might be exposed to security risks and data leakage.

Parameter	Description
Password Reset	If turned off, you will not be able to reset password.
ONVIF	Allows the communications between devices of the different brand or series.
Outbound Protection of Service Information	Protect your passwords. We recommend you turn it on. Otherwise, the VTO might be exposed to security risks and data leakage.
Multicast/Broadcast Search	Enable it so that the VTO will be found by other devices. We recommend you turn it off. Otherwise, the VTO might be exposed to security risks and data leakage.
Authentication Mode	• **Security Mode** (recommended): Support logging in with Digest authentication. • **Compatibility Mode** : Use the old login method. We recommend you use the security mode. Compatible mode might expose the VTO to security risks and data leakage.
Emergency Maintenance	For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.
Password Expires in	• Select an expiration period from **30** days, **60** days, **90** days, **180** days, **Custom** and **Never**. • If you select **Custom**, you need to configure an expiration day between 0 and 180.
Private Protocol	Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.
TLSv1.1	We recommend you turn it off because there might be safety risk if this service is enabled.
LLDP	Improves the efficiency of information exchange among network devices.

Step 3 Click **Apply**.

9.7 Auto Registration

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

Procedure

Step 1 Log in to the webpage of VTO.

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

Step 3 Enable the function. Enter the server address, port number and registration ID.

Figure 9-11 Auto registration

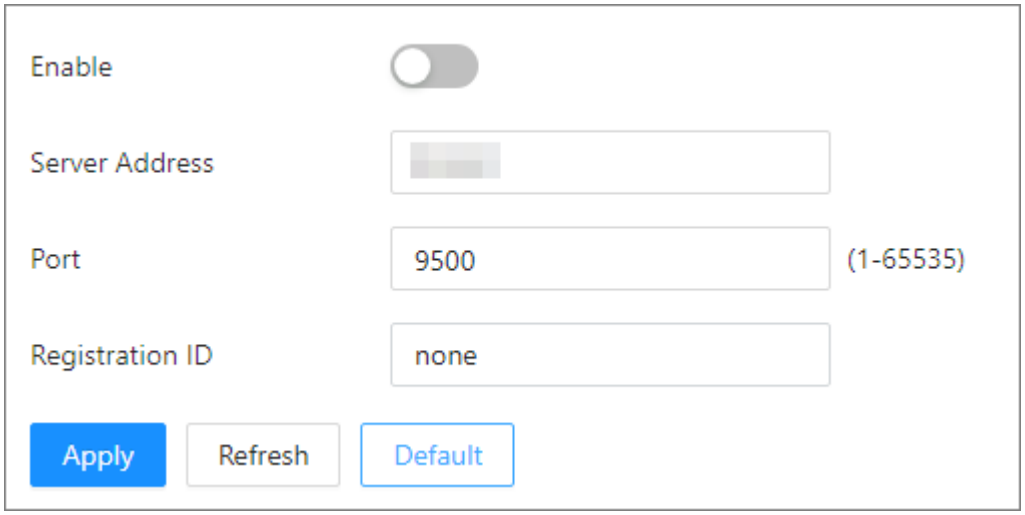


Table 9-8 Parameters description

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 4 Click **Apply**.

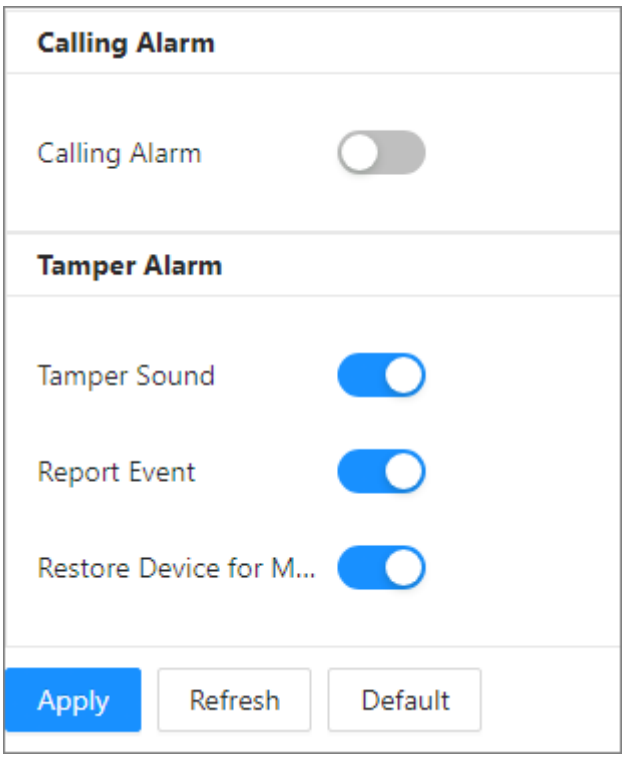
10 System

10.1 Alarm

Procedure

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

Figure 10-1 Alarm



Step 2 Configure the parameters, which will take effect upon change.

Table 10-1 Alarm parameter description

Parameter	Description
Calling Alarm	When the call is initiated, the alarm output will be linked. If the alarm out interface is connected with a buzzer, it will beep.
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**.

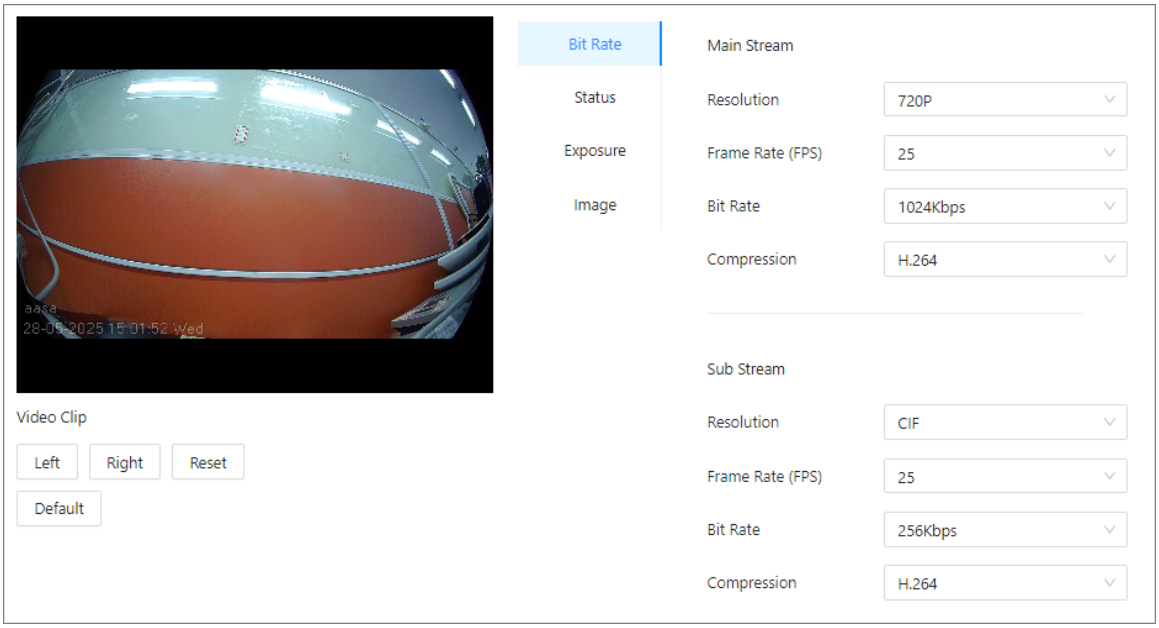
10.2 Video

Configure the video format and quality, and audio of the VTO.

Procedure

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

Figure 10-2 Video



Step 2 Configure the parameters, which will take effect upon change.

Table 10-2 Video parameter description

Parameter			Description
Bit Rate	Main Stream	Resolution	• **720P** : 1280 × 720. • **WVGA** : 800 × 480. • **D1** : 704 × 576. • **CIF** : 352 × 288.
		Frame Rate (FPS)	• If select the **Video Standard** as **PAL**: The range is 1 to 25. • If select the **Video Standard** as **NTSC**: The range is 1 to 30). The larger the value, the smoother the video, but it requires more bandwidth.
		Bit Rate	The larger the value, the better the video quality, but it requires more bandwidth.
		Compression	Compared with H.264, H.265 requires smaller bandwidth.

Parameter			Description
	Sub Stream	Resolution	• **1080P** : 1920 × 1080. • **720P** : 1280 × 720. • **D1** : 704 × 576. • **WVGA** : 800 × 480. • **CIF** : 352 × 288. • **QVGA** : 320 × 240.
		Frame Rate (FPS)	The range is 1 to 25. The larger the value, the smoother the video, but it requires more bandwidth.
		Bit Rate	Include 224 Kbps, 256 Kbps, 320 Kbps, 384 Kbps, 448 Kbps, 512 Kbps, 640 Kbps, 768 Kbps. The larger the value, the better the video quality, but it requires more bandwidth.
		Compression	H.264. H.265.
Status	Scene Mode		Select from **Auto** , **Disable**, **Sunny** and **Night**. **Auto** is selected by default.
	Compensation Mode		• **BLC** : Back light compensation. Improve the clarity of the target in the image. • **WDR** : Wide dynamic range. Enhance the brightness of dark areas, and reduce the brightness of bright areas to improve the image. • **HLC** : High light compensation. Reduce the brightness of the strong spots to improve the overall image. • **Disable**: Do not use any compensation mode.
	Day/Night		Select from **Color** , **Auto** and **B/W**.
	Video Standard		Select **PAL** or **NTSC** according to your area.
Exposure	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.

Parameter		Description
	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.
	Exposure Compensation	You can set the exposure compensation value. The value ranges from 0 to 100. The higher the value is, the brighter the image will be.
	3D NR	Reduce the noise of multiple-frame (at least two frames) images by using inter-frame information between two adjacent frames in a video. The higher the level is, the lower the noise will be, and the larger the trailing smear will be.
	NR Level	Noise reduction grade. The value ranges from 0 to 100. The larger the value is, the less the noise will be.
Image	Brightness	The larger the value, the brighter the image.
	Contrast	Larger value for more contrast between bright and dark areas.
	Hue	Make the color brighter or darker. The default value is made by the light sensor, and we recommend keeping it default.
	Saturation	The larger the value, the thicker the color.
	Gain Adjustment	Configure the gain.
	Mirror	Display the image with left and right side reversed.
	Flip	Display the image upside down.
	Display Time	Display the current time and date on the video image.

Step 3 (Optional) Configure the video clip.

Click **Left** or **Right** to swing the screen to the left or right.

Click **Reset** or **Default** to reset or default the device.

The function is only available for the mode of F.

10.3 Audio

Procedure

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

Step 2 Configure the parameters, which will take effect upon change.

Figure 10-3 Audio

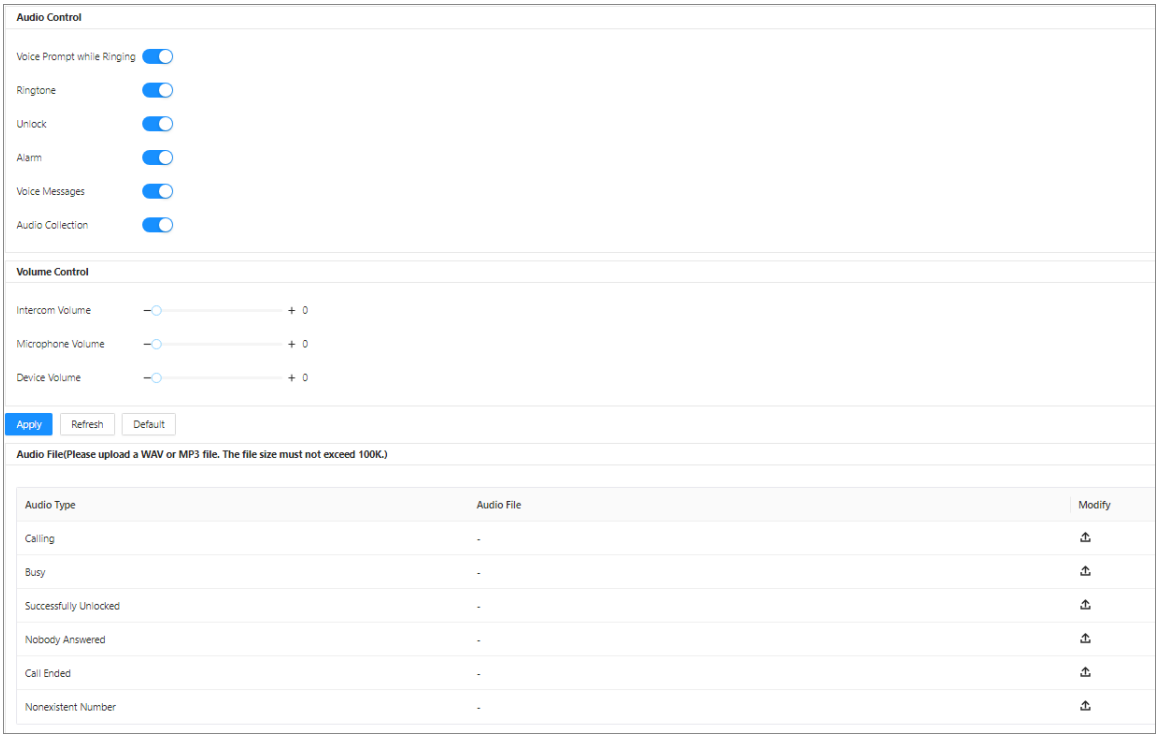


Table 10-3 Audio parameter description

Parameter		Description
Audio Control	Voice Prompt while Ringing	Turn on or off each type of sound.
	Ringtone	
	Alarm	
	Voice Messages	
	Unlock	
	Audio Collection	
Volume Control	Microphone Volume	Adjust the microphone volume of the VTO. The higher the value is, the higher the volume will be.
	Intercom Volume	Adjust the speaker volume. 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.

Step 3 Click **Apply**.

Step 4 (Optional) Upload audio file by clicking next to the corresponding audio type (including calling, busy, successfully unlocked, nobody answered, call ended and nonexistent number).

Please upload a WAV or MP3 file. The file size must not exceed 100K.

10.4 Time

Configure the time zone and day light saving parameters.

Procedure

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

Step 2 Configure the time and time zone and DST.

Figure 10-4 Time

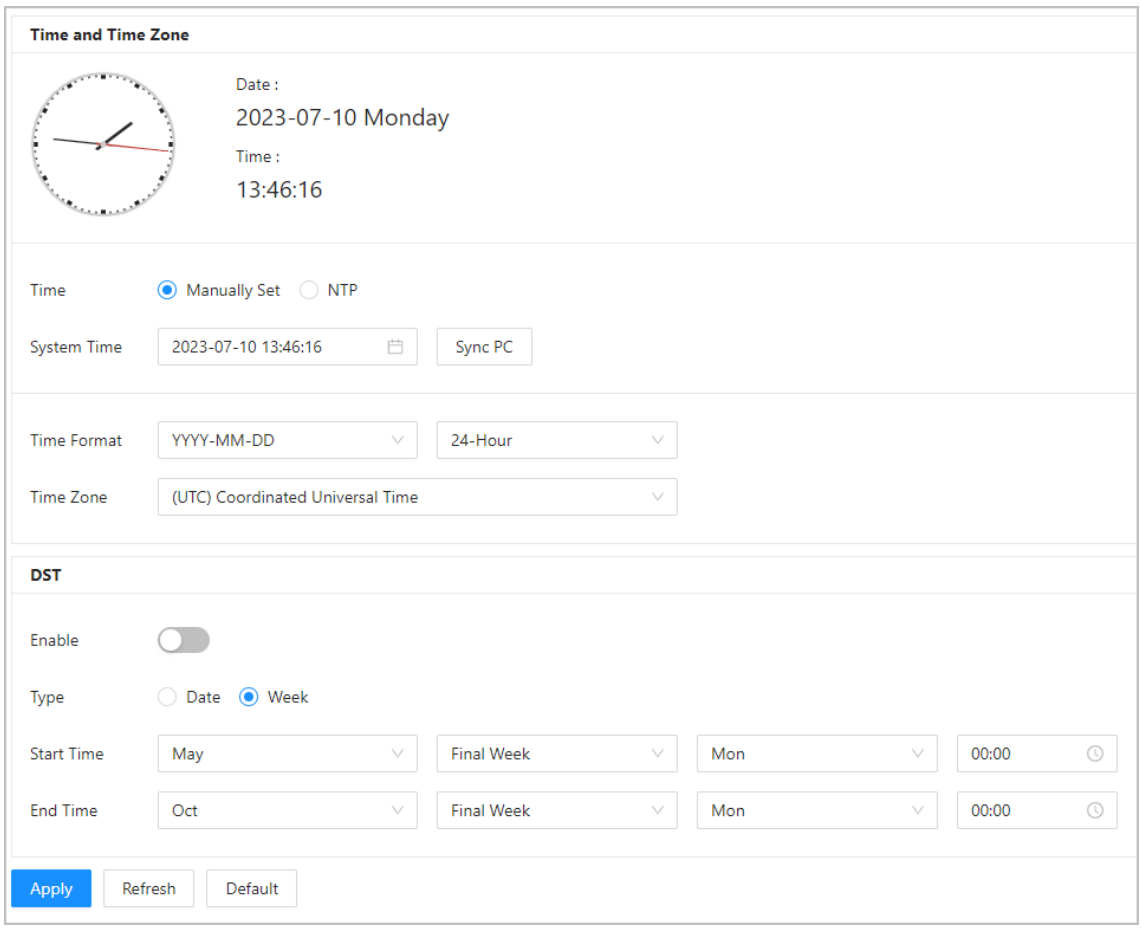


Table 10-4 Parameter description

Module	Parameter	Description
Time and Time Zone	Time	• Manually Set • NTP

Module	Parameter	Description
	System Time	The time of the VTO system. ⚠ Changing system time might cause problems on video searching and information publication. Turn off video recording and auto snapshot before changing it. 🕮 Only applicable under the **Manually Set** mode.
	Sync PC	Synchronize the VTO system time with your PC. 🕮 Only applicable under the **Manually Set** mode.
	Server	The address of the NTP server. 🕮 Only applicable under the **NTP** mode.
	Manual Update	Click the icon and the device time of the VTO will be automatically synchronized with server. 🕮 Only applicable under the **NTP** mode.
	Port	NTP server port number. 🕮 Only applicable under the **NTP** mode.
	Interval	VTO time update cycle. 30 minutes at most. 🕮 Only applicable under the **NTP** mode.
	Time Format	For the date format, select from one of the following: • YYYY-MM-DD • MM-DD-YYYY • DD-MM-YYYY For the time format, select from one of the following: • 24-Hour • 12-Hour
	Time Zone	Select the time zone for the VTO system.
DST	Enable	Click to enable the **DST** function.
	Type	Select **Date** or **Week** as needed, and then configure the specific period.
	Start Time	Configure the start time and end time of DST.
	End Time	

Step 3 Click **Apply**.

10.5 ONVIF User

Add accounts for devices to monitor the VTO through the ONVIF protocol.

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

Procedure

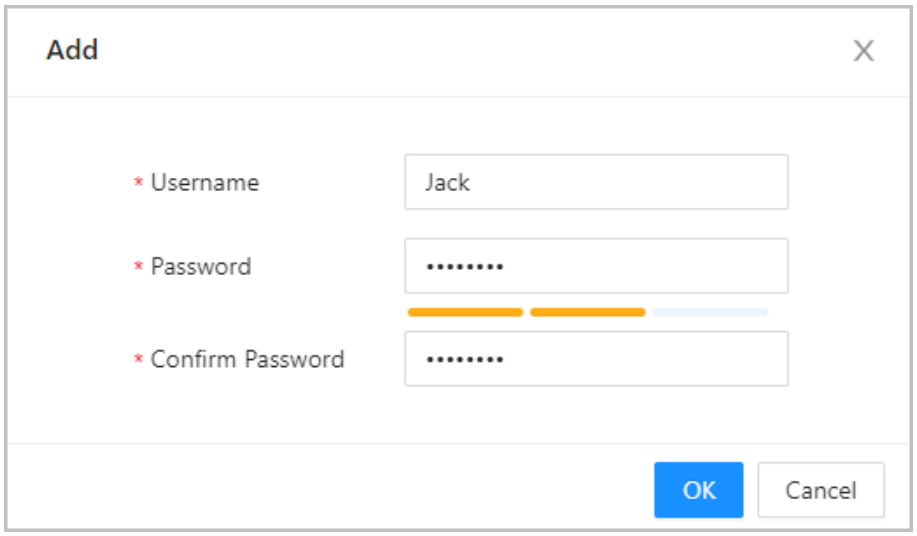
Step 1 Select **System** > **ONVIF User**.

Step 2 Click **Add**.

Step 3 Enter the information, and then click **OK**.

ONVIF devices can monitor the VTO by using the account.

Figure 10-5 ONVIF user



11 Maintenance Center

11.1 One-Click Diagnosis

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

Procedure

Step 1 Log in to the webpage.

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

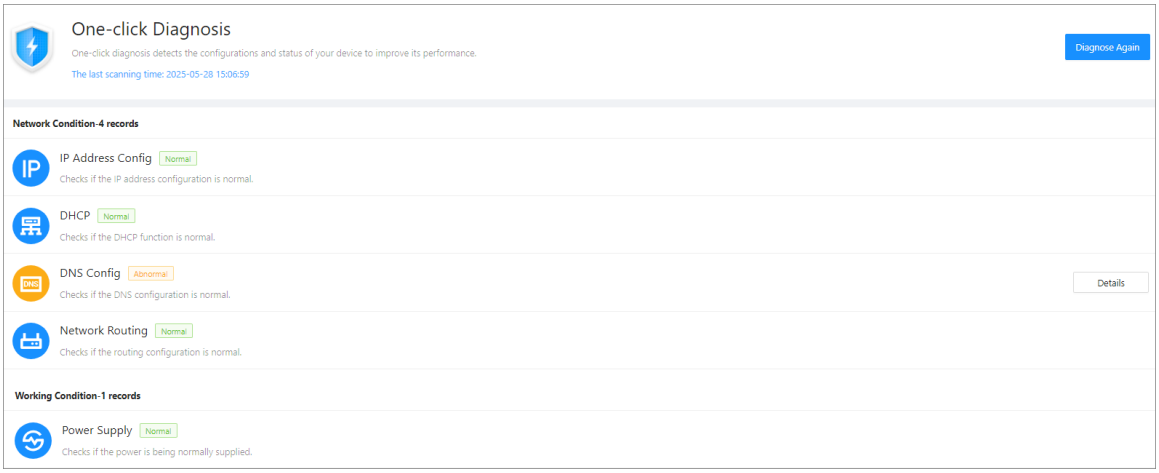
Step 3 Click **Diagnose**.

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

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

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

Figure 11-1 One-click diagnosis



11.2 System Information

11.2.1 Version Information

Procedure

Step 1 Select **Maintenance Center** > **System Info** > **Version**.

Step 2 View the software version, SCM version and security baseline version.

Figure 11-2 System information

11.2.2 Legal Information

Select **Maintenance Center** > **System Info** > **Legal Info**. You can view related legal information notices in this section.

11.3 Data Capacity

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

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

11.4 Log Management

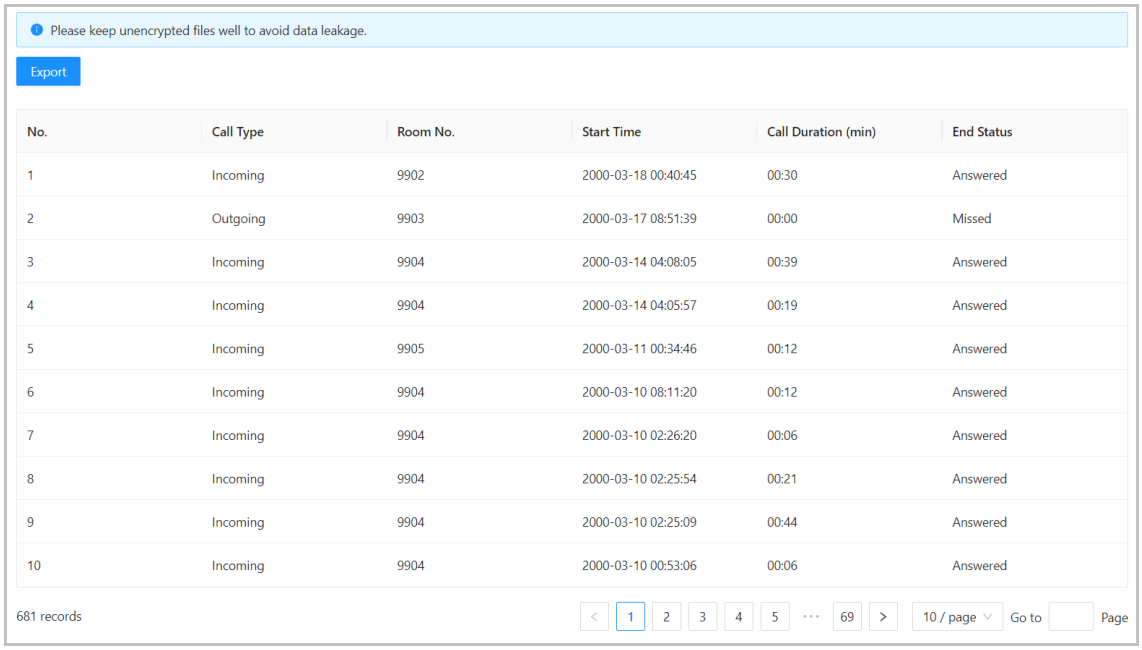
Select **Maintenance Center** > **Log**. You can search for different logs, and export them to your local computer.

If storage is full, the oldest records will be overwritten. Back up the records in time.

11.4.1 Call History

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

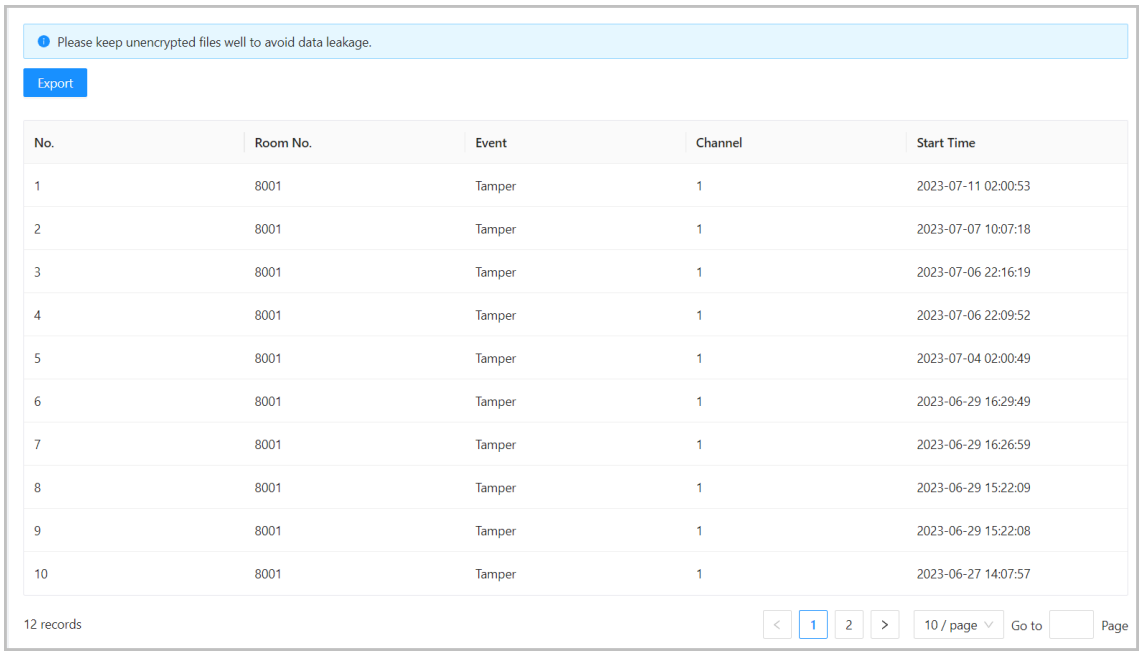
Figure 11-3 Call history



11.4.2 Alarm Logs

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

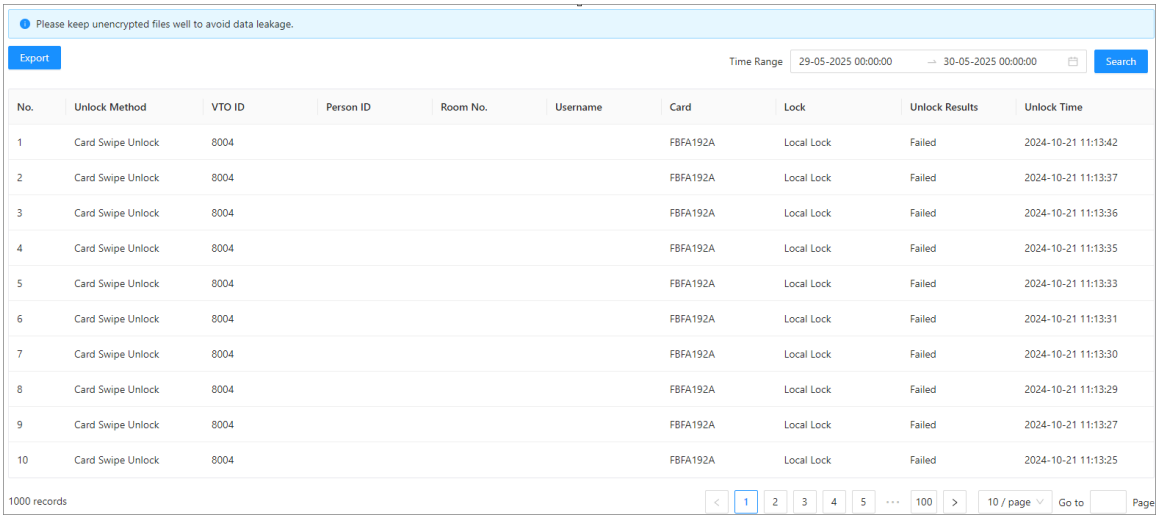
Figure 11-4 Alarm



11.4.3 Unlock Records

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

Figure 11-5 Unlock Records

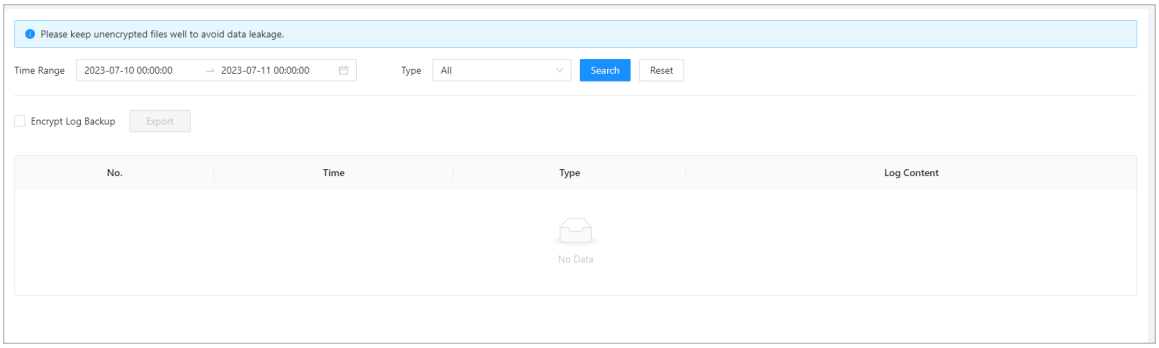


11.4.4 Log

Select **Maintenance Center** > **Log** > **Log**.

Select time range and type, and then you can see all the log information.

Figure 11-6 Log



11.5 Maintenance Management

11.5.1 Config

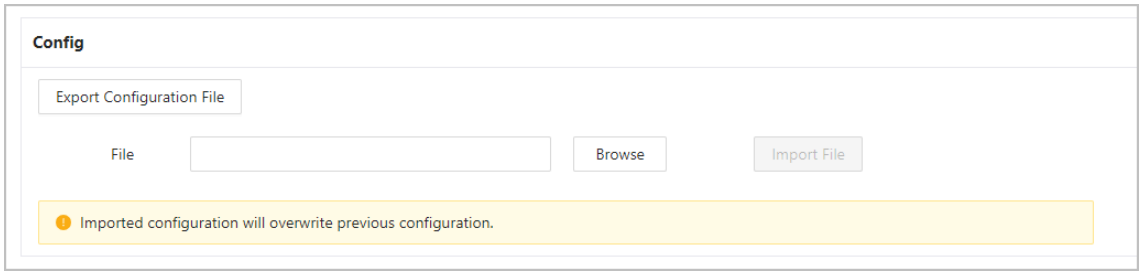
You can export and import the configuration file.

Procedure

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

Step 2 Click **Export Configuration File**, or click **Browse** to select the file from local computer, and then click **Import file**.

Figure 11-7 Config



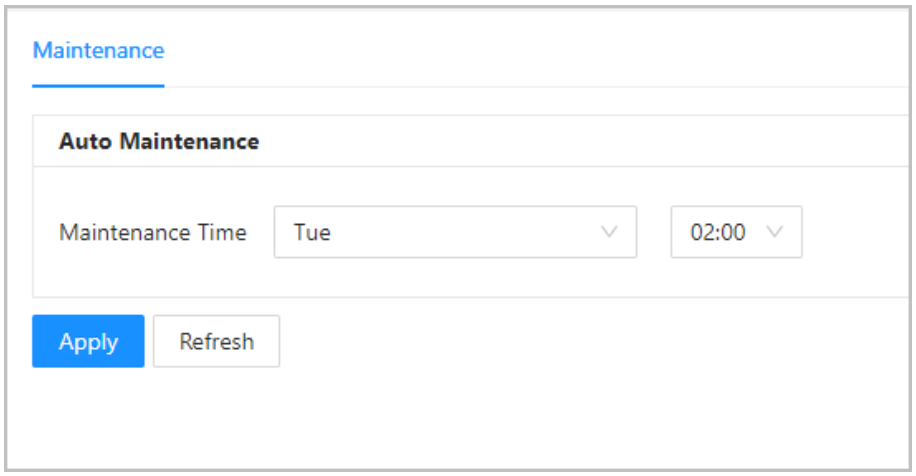
11.5.2 Maintenance

Procedure

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

Step 2 Configure the auto maintenance time.

Figure 11-8 Auto maintenance



Step 3 Click **Apply**.

11.6 Update

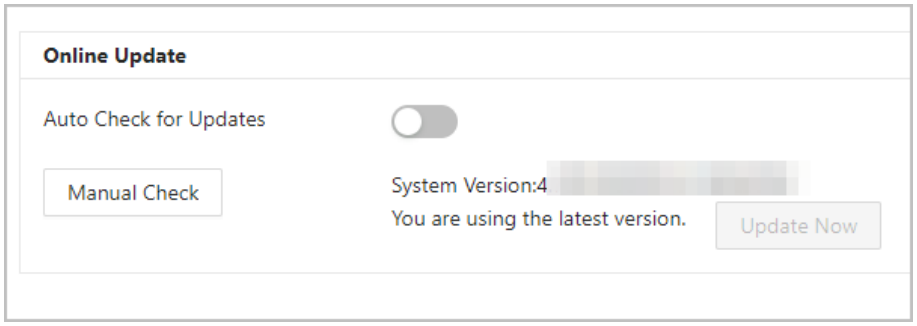
Procedure

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

Step 2 Select ways to check the update.

- **File Update** : Click **Browse** to add the updating file, and then click **Update**.
- **Online Update**
  - **Auto Check for Updates** : Enable the function to check automatically whether there is a new system version.
  - **Manual Check** : Select the function to check whether there is a new system version.

Figure 11-9 Online update



11.7 Advanced Maintenance

Export

Select **Maintenance Center** > **Advanced Maintenance** > **Export** to export the serial number, firmware version, device operation logs and configuration information.

Packet Capture

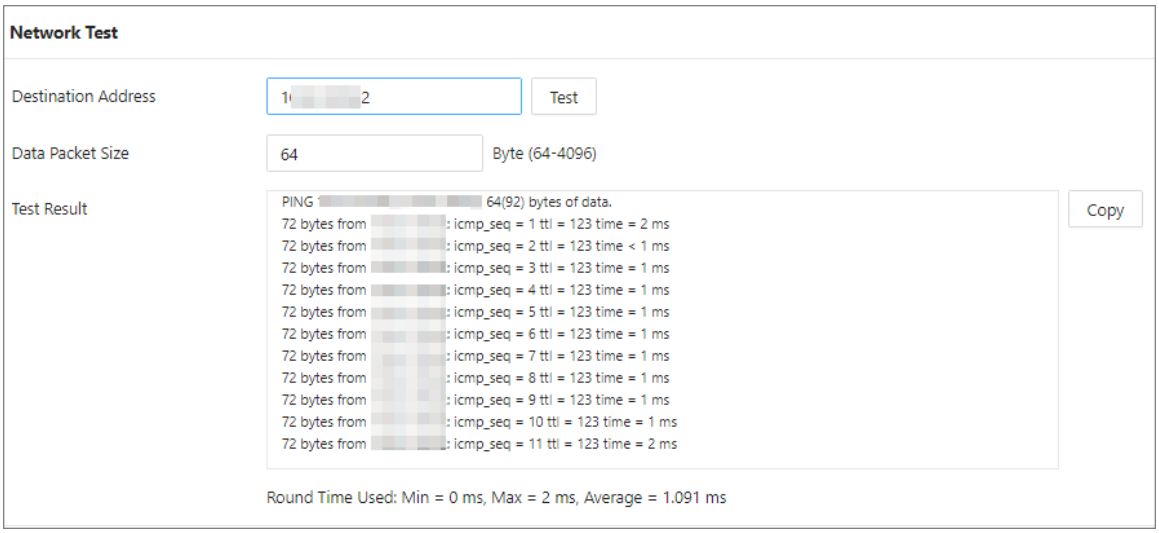
1. Select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.
2. Enter the port of the device.
3. Click ▶ to start the packet sniffer backup.

Figure 11-10 Packet capture

Network Test

1. Select **Maintenance Center** > **Advanced Maintenance** > **Packet Capture**.
2. In the **Network Test** area, test the network as needed.
   a. Enter the destination address in the box, and then click **Test**.
   b. After you acquired enough data, click **Stop**, and then you can view the test result in the following box.
   c. Click **Copy** to copy the test result.

Figure 11-11 Test network

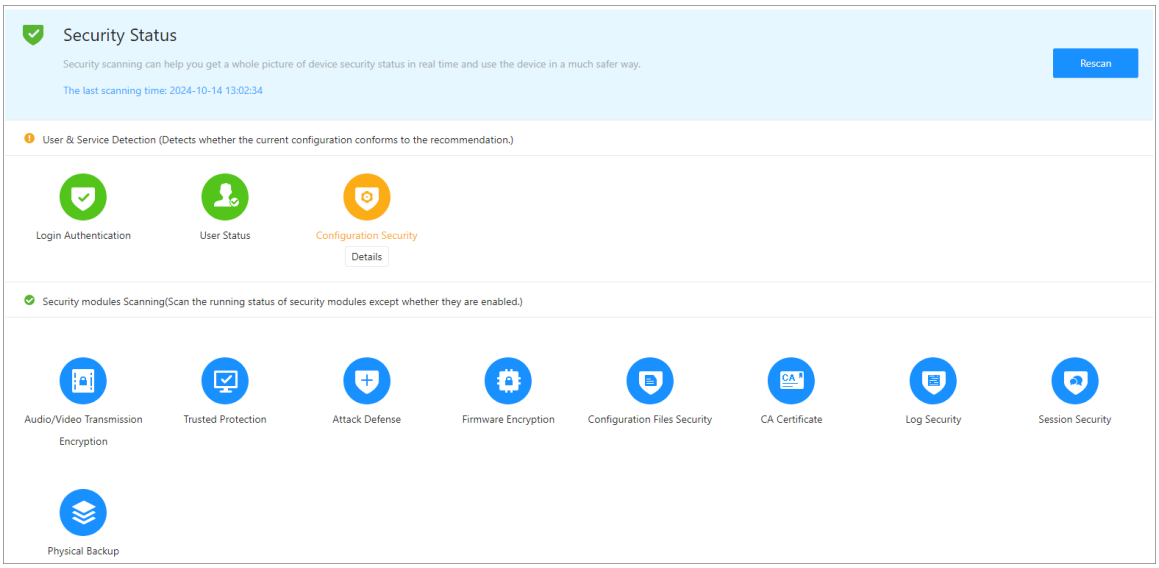


12 Security Management

12.1 Security Status

On the home page, click , and then select **Security Status**.

Figure 12-1 Security status



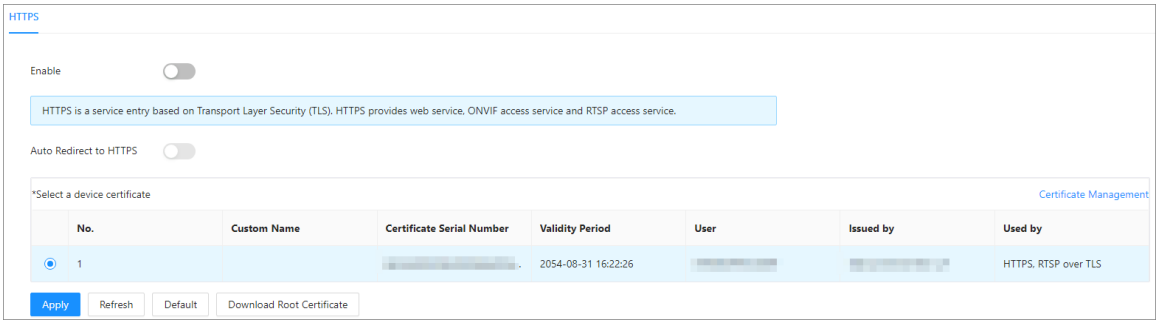
12.2 System Service

Procedure

Step 1 On the home page, click , and then select **System Service**.

Step 2 Select a device certificate, and then enable the HTTPS function.

Figure 12-2 System service



Step 3 Click **Apply**.

12.3 Attack Defense

12.3.1 Firewall

You can enable different firewall types to control network access to the VTO.

Procedure

Step 1 On the home page, click , and then select **Attack Defense** > **Firewall**.

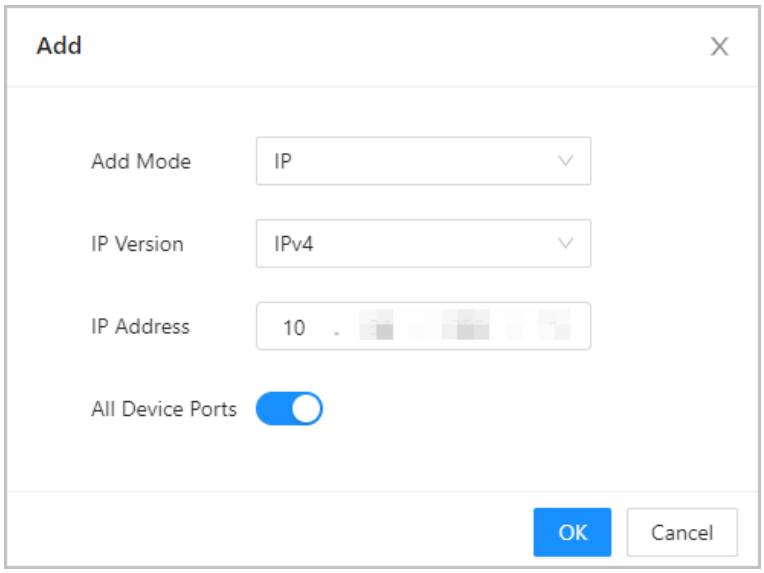
Step 2 Click next to **Enable**.

Step 3 Select the **Mode** as either **Allowlist** or **Blocklist**.

- Allowlist: Devices that have been granted an access.
- Blocklist: Devices that have been forbidden an access.

Step 4 Click **Add** to add the IP address for allowlist or blocklist.

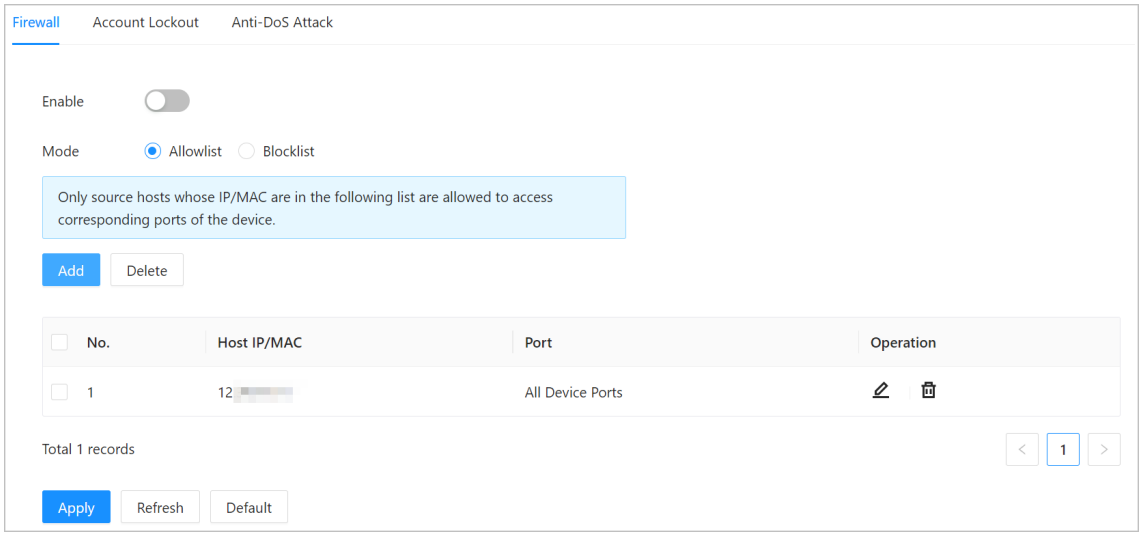
Figure 12-3 Add



Step 5 Click **OK**.

Step 6 Select an added IP address for allowlist or blocklist, and then click **Apply**.

Figure 12-4 Apply



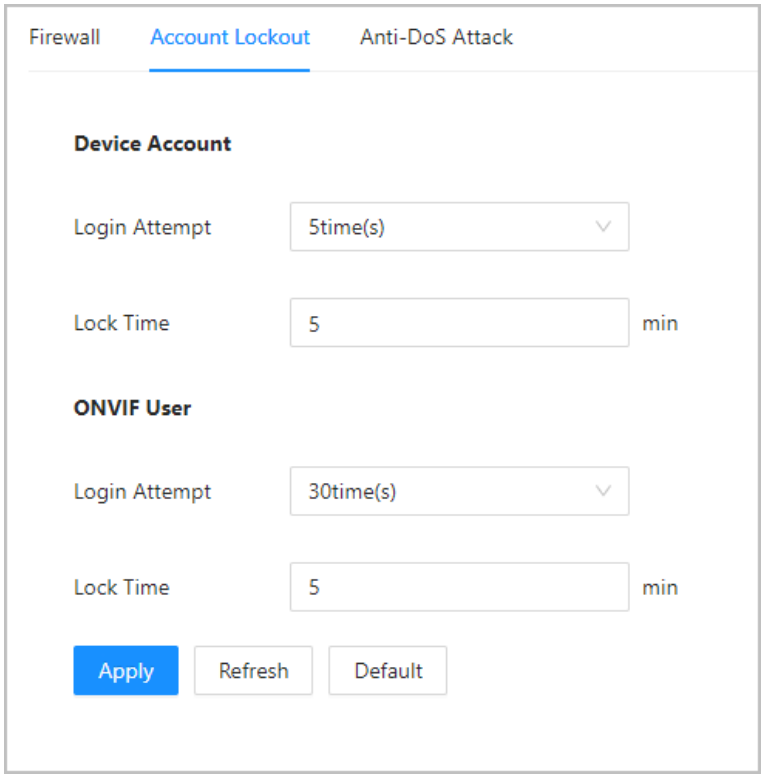
12.3.2 Account Lockout

Procedure

Step 1 On the home page, click , and then select **Attack Defense** > **Account Lockout**.

Step 2 Configure the login attempts and lock time for device account and ONVIF user.

Figure 12-5 Account lockout



Step 3 Click **Apply**.

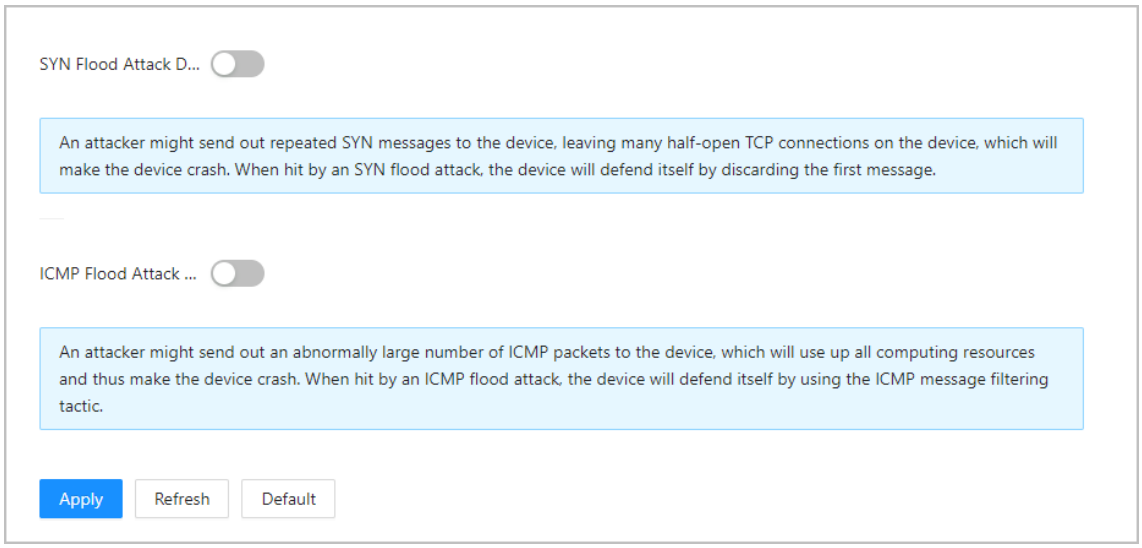
12.3.3 Anti-DoS Attack

Procedure

Step 1 On the home page, click , and then select **Attack Defense** > **Anti-DoS Attack**.

Step 2 Enable or disable the **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** function.

Figure 12-6 Anti-DoS attack



Step 3 Click **Apply**.

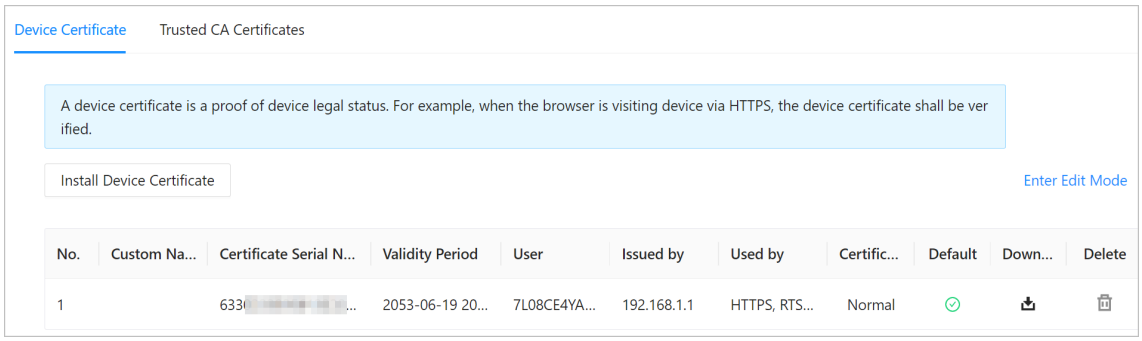
12.4 CA Certificate

Procedure

Step 1 On the home page, click , and then select **CA Certificate**.

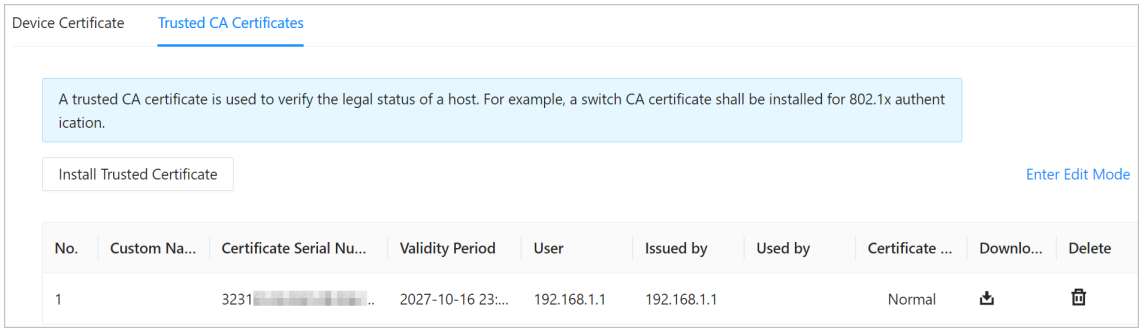
- Device Certificate

Figure 12-7 Device certificate



- Trusted CA Certificates

Figure 12-8 Trusted CA certificates



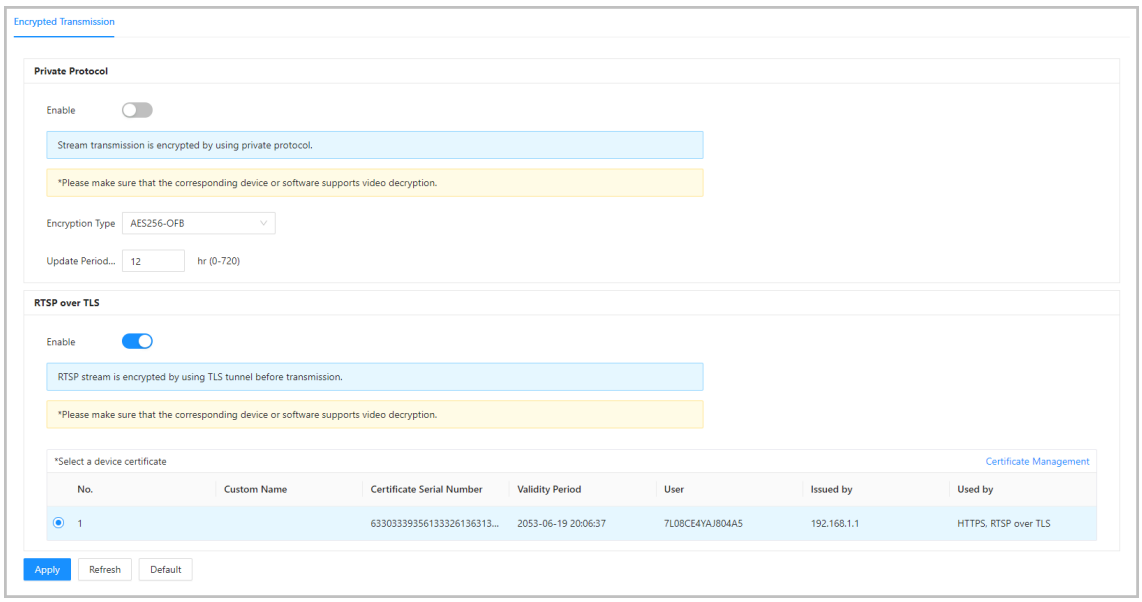
12.5 Video Encryption

Procedure

Step 1 On the home page, click , and then select **Video Encryption**.

Step 2 Configure **Private Protocol** and **RTSP over TLS** parameters.

Figure 12-9 Video encryption



Step 3 Click **Apply**.

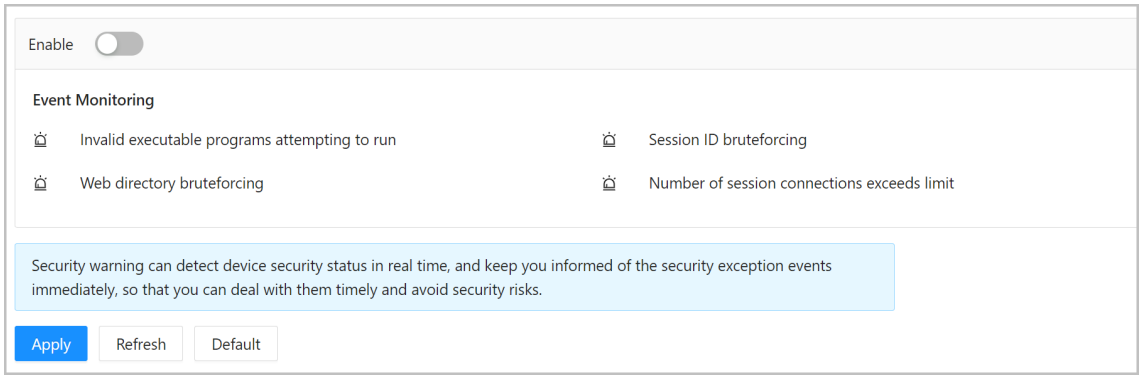
12.6 Security Warning

Procedure

Step 1 On the home page, click , and then select **Security Warning**.

Step 2 Enable event monitoring function, and then click **Apply**.

Figure 12-10 Security warning



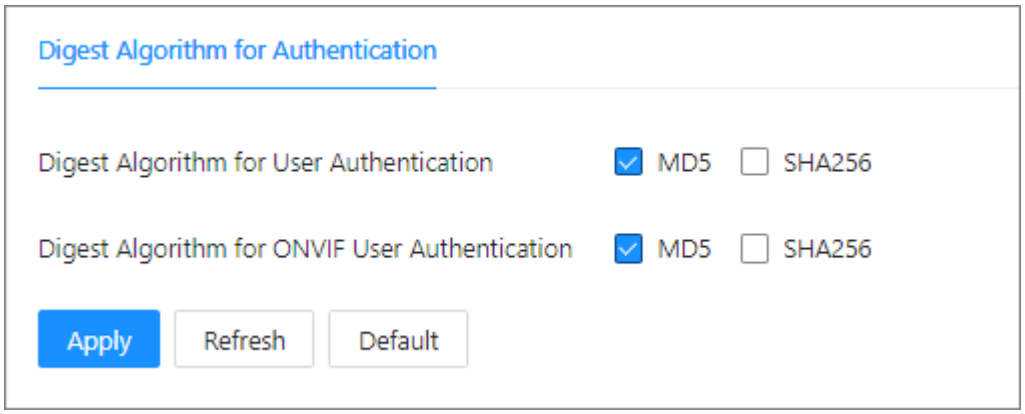
12.7 Security Authentication

Procedure

Step 1 On the home page, click , and then select **Security Authentication**.

Step 2 Configure the digest algorithm for authentication, and then click **Apply**.

Figure 12-11 Security authentication



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 Allow list**

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