Villa Door Station

User's Manual

V1.0.4

Foreword

General

This manual introduces the installation, functions and operations of the villa 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
V1.0.4	Added structure.	May 2024
V1.0.3	Added port description.	February 2024
V1.0.2	Added structure.	February 2024
V1.0.1	Added structure.	December 2023
V1.0.0	First release.	August 2023

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.

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

Important Safeguards 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.

Operation Requirements

- 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.

Installation Requirements

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Improper use of the battery might result in a fire or explosion.

- 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 power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- 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.

Table of Contents

Foreword I
Important Safeguards and Warnings III
1 Structure 1
1.1 Villa Door Station (multiple buttons) 1
1.1.1 Front Panel 1
1.1.2 Rear Panel 2
1.2 Villa Door Station (single button) 3
1.2.1 R Series 3
1.2.2 D Series 5
1.2.3 G Series 8
1.2.4 E Series 9
1.2.5 F Series 12
1.3 Button Model 23
1.3.1 Front Panel 23
1.3.2 Rear Panel 24
2 Initializing the VTO 26
2.1 Web 26
2.2 DMSS APP 26
3 Login and Resetting Password 30
3.1 Login 30
3.2 Resetting Password 30
4 Home Page 31
5 Setup Wizard 32
5.1 Setting as SIP Server 32
5.2 Not Setting as SIP Server 33
6 Local Device Configuration 34
6.1 Basic Settings 34
6.1.1 Villa Door Station 34
6.1.2 Second Confirmation Station 37
6.2 Access Control 39
6.2.1 Config 39
6.2.2 RS-485 40
6.2.3 Configuring the Password 41
6.3 Configuring Wiegand 42
6.4 Layout 43
6.4.1 Layout (Multiple Buttons) 43
6.4.2 Layout (Multiple Modules) 45

6.5 Adding the IPC 46
6.5.1 Adding the IPC One by One 46
6.5.2 Exporting the IPC Information in Batches 48
6.5.3 Importing the IPC Information in Batches 48
7 System 49
7.1 Video 49
7.2 Audio 51
7.3 Time 52
7.4 ONVIF User 54
7.5 Config 55
7.6 Maintenance 55
7.7 Updating 56
7.8 Legal Information 56
7.9 System Information 56
8 Device Setting 58
8.1 VTO No. Management 58
8.2 VTH Management 59
8.3 VTS Management 61
9 Person Management 63
10 Network Settings 67
10.1 TCP/IP 67
10.2 Port 68
10.3 SIP Server 68
10.4 Second Confirmation Station Cascading 72
10.5 Cloud Service 73
10.6 UPnP 73
10.6.1 Enabling UPnP Services 74
10.6.2 Adding UPnP Services 74
10.7 Wi-Fi 76
10.8 Basic Services 76
11 Log Management 79
11.1 Call History 79
11.2 Alarm Logs 79
11.3 Unlock Records 80
11.4 Log 80
12 Security Management 82
12.1 Security Status 82
12.2 System Service 82
12.3 Attack Defense 83
12.3.1 Firewall 83

12.3.2 Account Lockout....84
12.3.3 Anti-DoS Attack....85
12.4 CA Certificate....85
12.5 Video Encryption....86
12.6 Security Warning....86
13 Button Model Configuration....88
13.1 Cable Connection....88
13.2 VTH Configuration....89
Appendix 1 Cybersecurity Recommendations....91

1 Structure

1.1 Villa Door Station (multiple buttons)

1.1.1 Front Panel

Figure 1-1 Front panel

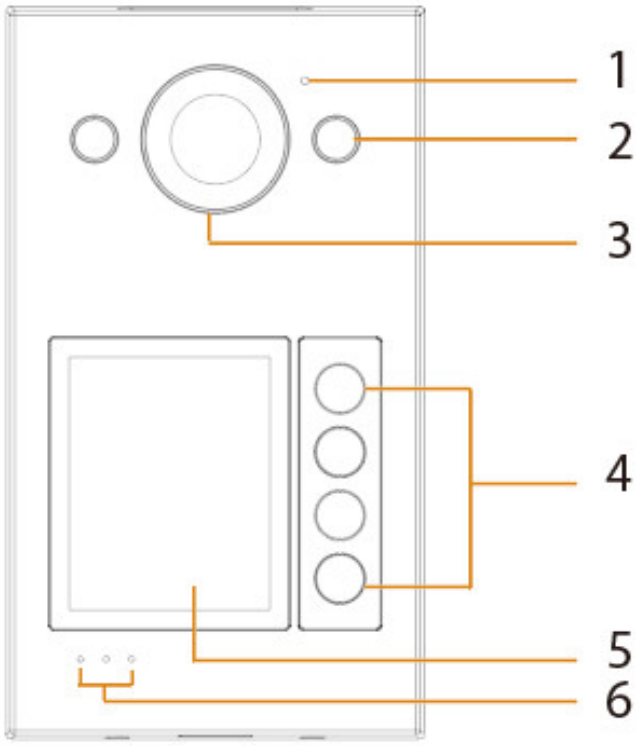


Table 1-1 Components

No.	Name	Function
1	MIC	Audio input.
2	Illuminator	Provide a constant light to focus more easily on a subject in dark surroundings.
3	Camera	Capture images or record videos for the VTO.
4	Call buttons	Call the VTH.
5	Card swiping area	Swipe the registered cards to unlock doors.
6	Indicators	From left to right: • Ring: VTO is calling the VTH. • Talking: VTO is on the talk with the VTH. • Unlocking: VTO unlocking successful.

1.1.2 Rear Panel

The multi-function port might differ depending on the actual models.

Figure 1-2 Rear panel

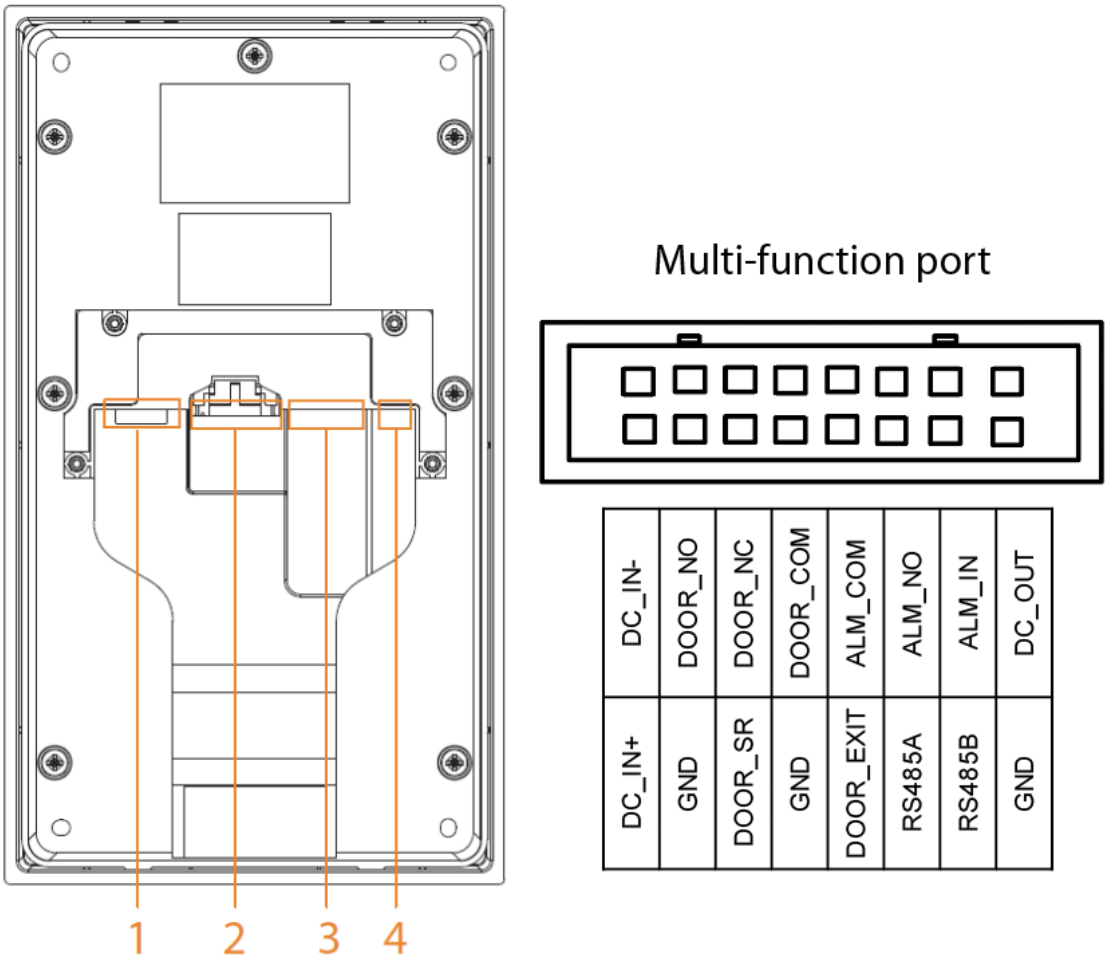


Table 1-2 Components

No.	Name	Function
1	SD card slot	Used to insert SD card so that data information such as images and videos can be stored.
2	Multi-function port	Alarm port, door detector port, 485 port, power port and other ports.
3	Network port	RJ-485 network port to connect to the network.
4	Reset button	Press and hold the button for several seconds to reset to factory settings.

1.2 Villa Door Station (single button)

1.2.1 R Series

1.2.1.1 Front Panel

Size and appearance might differ depending on the models of product.

Figure 1-3 Front panel

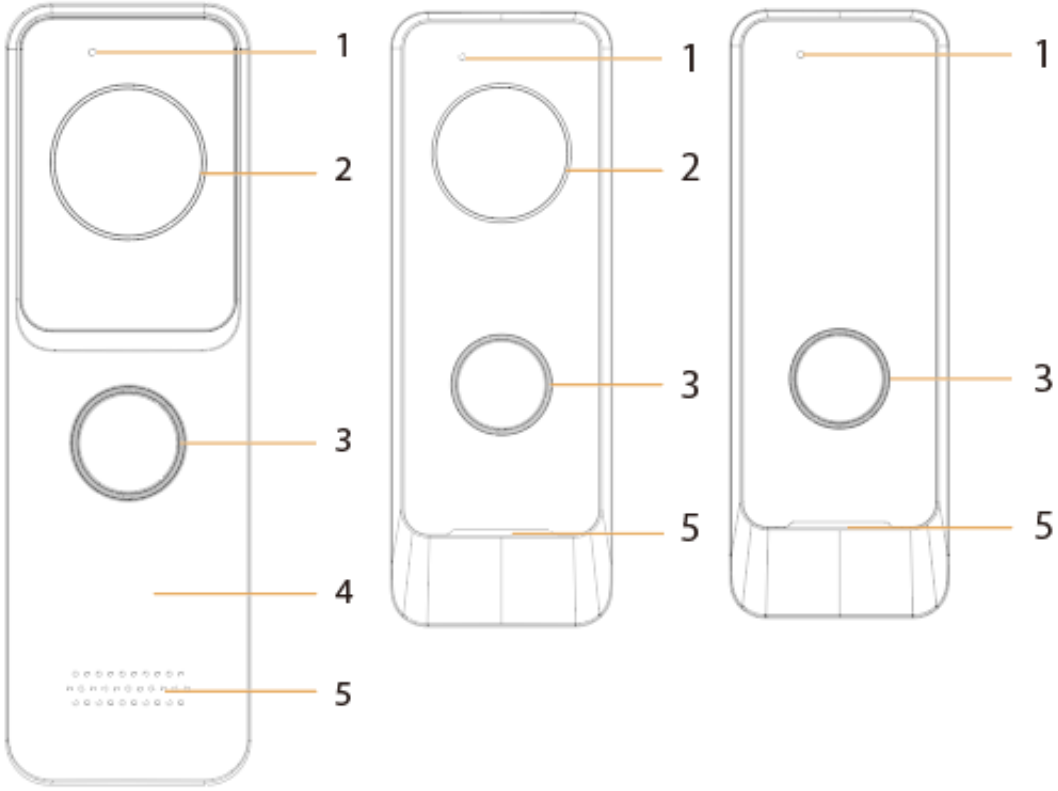


Table 1-3 Components

No.	Name	Function
1	MIC	Audio input.
2	Camera	Capture images or record videos for the VTO.
3	Call button	Call the VTH.
4	Card swiping area	Swipe the registered cards to unlock doors. The card swiping function is only available on select models.
5	Speaker	Audio output.

1.2.1.2 Rear Panel

The multi-function port might differ depending on the model. Here are two models used as examples.

Figure 1-4 Rear panel (1)

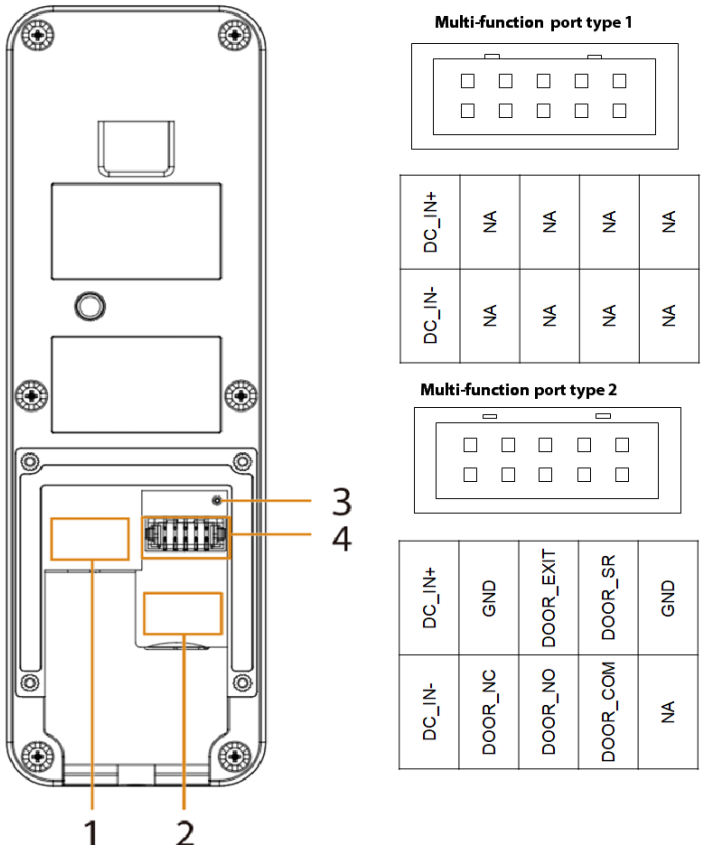


Table 1-4 Components

No.	Name	Function
1	Network port	Connects to the network.
2	SD card slot	Insert SD card so that data information such as images and videos can be stored.
3	Reset button	Press and hold the button for several seconds to reset to factory settings.
4	Multi-function port	• Type 1: The multi-function port only has a power input port to connect to power supply. • Type2: The multi-function port includes a power input port and a door detector port.

Figure 1-5 Rear panel (2)

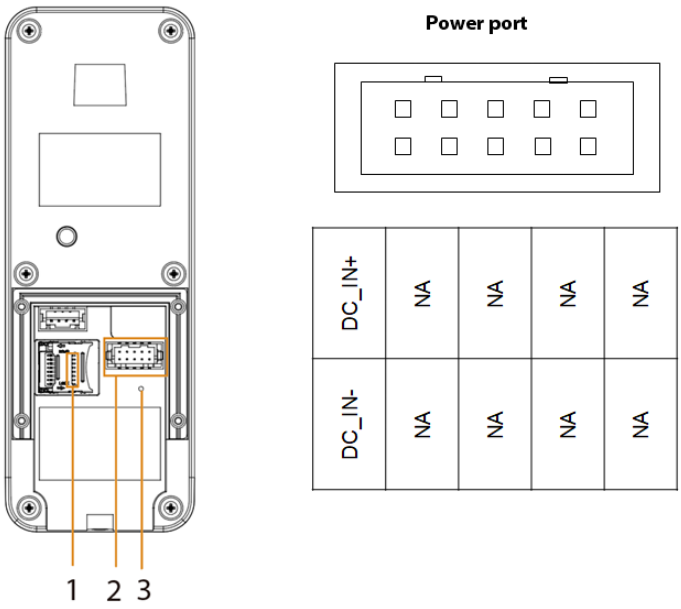


Table 1-5 Components

No.	Name	Function
1	SD card slot	Insert SD card so that data information such as images and videos can be stored.
2	Power port	Connects to the power supply.
3	Reset button	Press and hold the button for several seconds to reset to factory settings.

1.2.2 D Series

1.2.2.1 Front Panel

Figure 1-6 Front panel

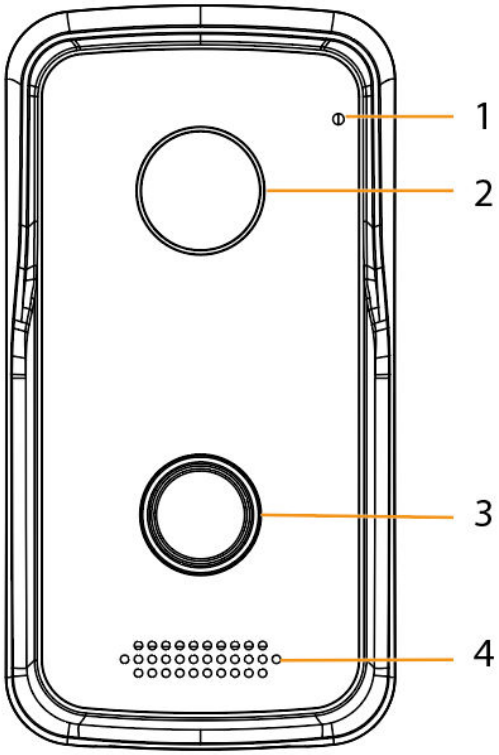


Table 1-6 Components

No.	Name	Function
1	MIC	Audio input.
2	Camera	Capture images or record videos for the VTO.
3	Call button	Call the VTH.
4	Speaker	Audio output.

1.2.2.2 Rear Panel

Figure 1-7 Rear panel

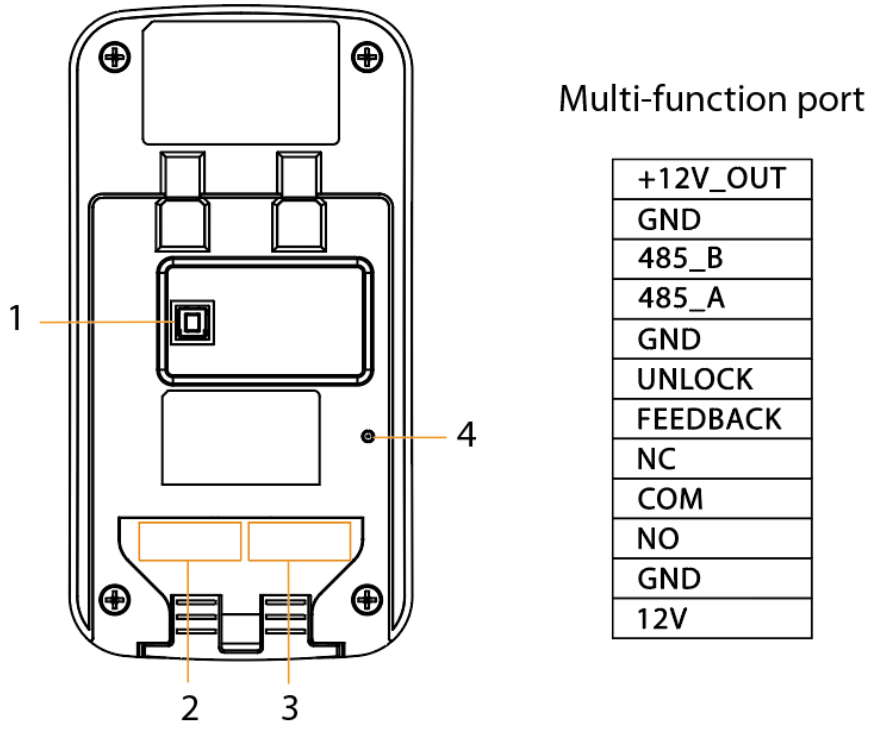


Table 1-7 Components

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	Connects to the network.
4	Reset button	Press and hold the button for several seconds to reset to factory settings.

1.2.3 G Series

1.2.3.1 Front Panel

Figure 1-8 Front panel

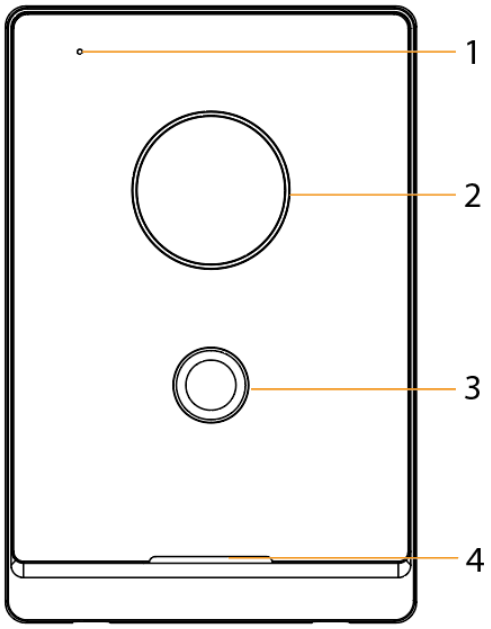


Table 1-8 Components

No.	Name	Function
1	MIC	Audio input.
2	Camera	Capture images or record videos for the VTO.
3	Call button	Call the VTH. The button displays different colors in different statuses. ● Standby: No light. ● Call not answered: Solid green. ● Call answered: Solid blue. ● Unlock when the device is in standby status: Red. ● Unlock when the call is not answered: Flashes green, yellow and then green. ● Unlock after the call is answered: Flashes blue, pink and then blue. ● Network disconnected: Green breathing light.
4	Speaker	Audio output.

1.2.3.2 Rear Panel

Figure 1-9 Rear panel

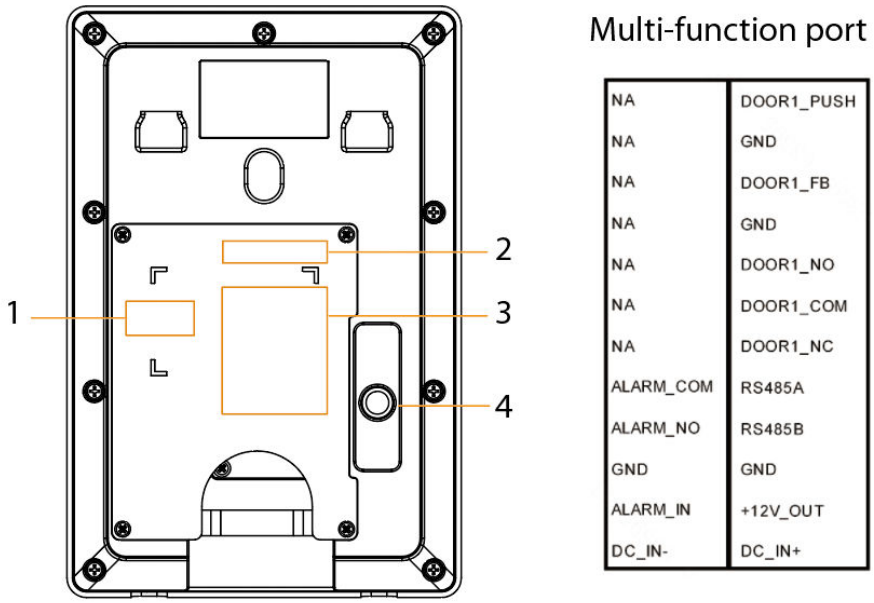


Table 1-9 Components

No.	Name	Function
1	Network port	Connects to the network.
2	Multi-function port	Alarm port, door detector port, 485 port, power port and more.
3	SD card slot	Insert SD card so that data information such as images and videos can be stored.
4	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.

1.2.4 E Series

1.2.4.1 Front Panel

Figure 1-10 Front panel

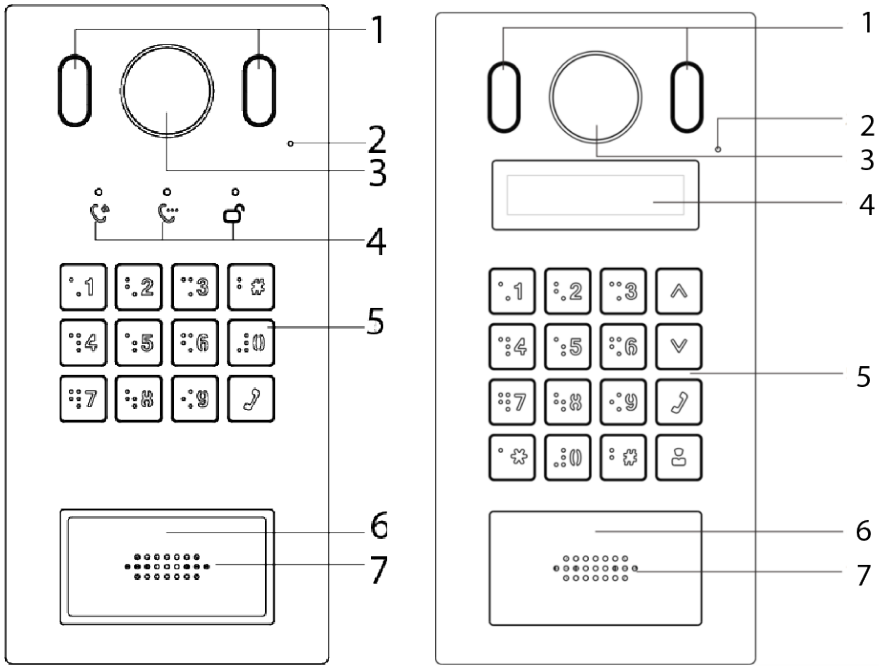


Table 1-10 Front panel description

No.	Name	Description
1	Illuminator	Provides extra light for the camera when it is dark.
2	Microphone	Audio input.
3	Camera	Capture images or record videos for the VTO.
4	Indicators	Displays status on calling, talking and unlock.
5	Keypad	—
6	Card reading area	Swipe a card here to unlock the door.
7	Speaker	Audio output.

1.2.4.2 Rear Panel

Figure 1-11 Rear panel

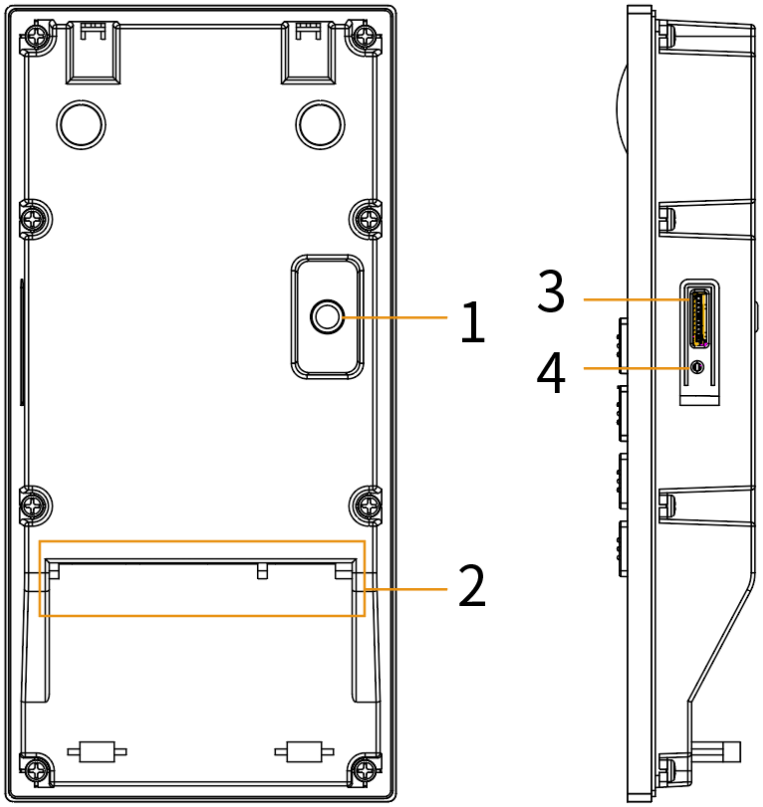
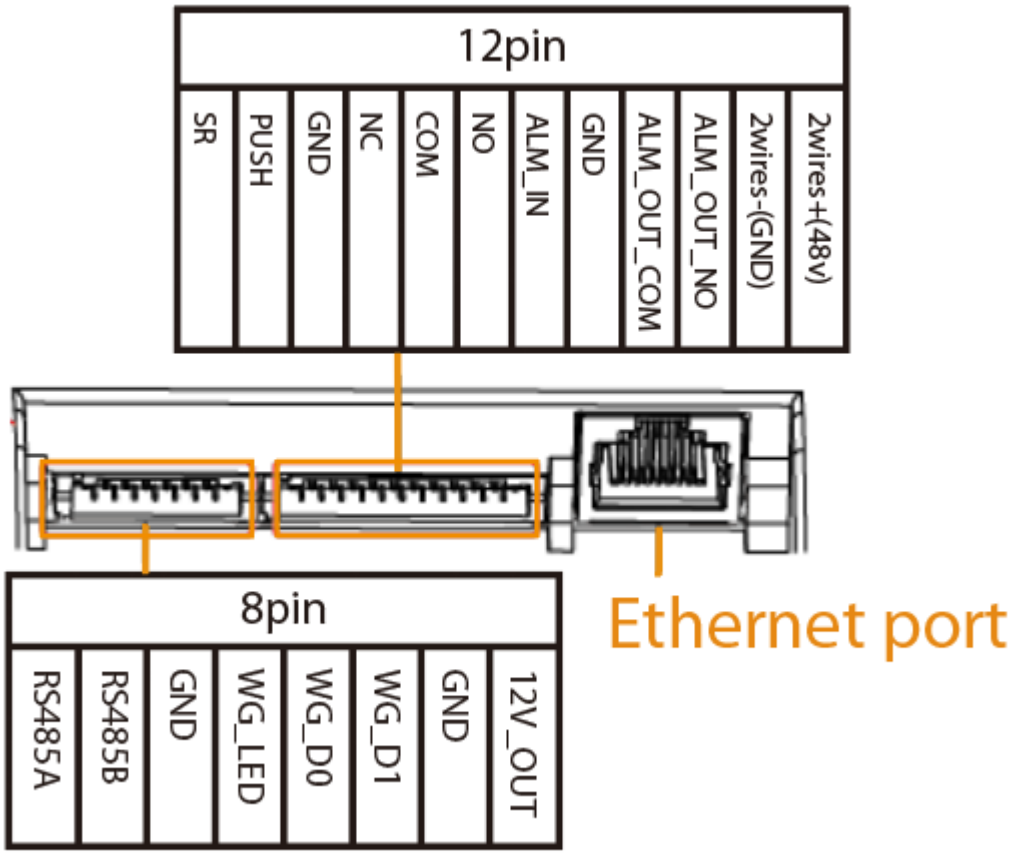


Table 1-11 Rear panel description

No.	Name	Description
1	Anti-tampering switch	When the VTO is removed from the wall forcibly, an alarm will be triggered and the alarm information will be sent to management center.
2	Multi-function port	For details, see Figure 1-12 .
3	SD card slot	Plug in the SD card.
4	Reset button	Press and hold it for 10 seconds to reset all settings.

Figure 1-12 Multi-function port



1.2.5 F Series

1.2.5.1 Front Panel

Figure 1-13 Front panel

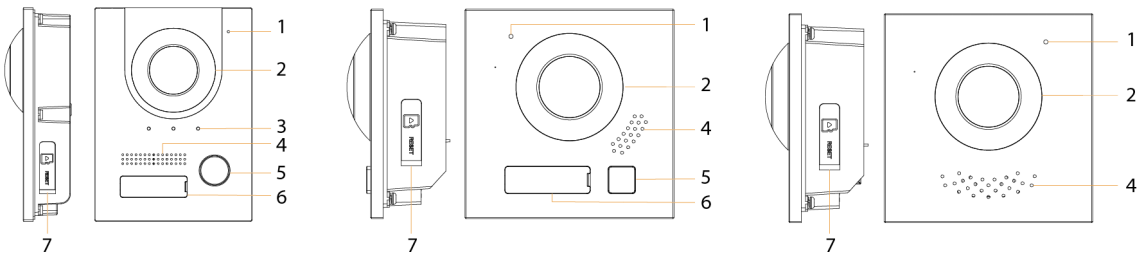


Table 1-12 Front panel description

No.	Name	Description
1	Microphone	Audio input.
2	Camera	Capture images or record videos for the VTO.

No.	Name	Description
3	Indicators	Display status on calling, talking and unlock.
4	Speaker	Audio output.
5	Call button	Call the VTH and the management center.
6	Nameplate	Displays the custom information.
7	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.

1.2.5.2 Rear Panel

Figure 1-14 Rear panel

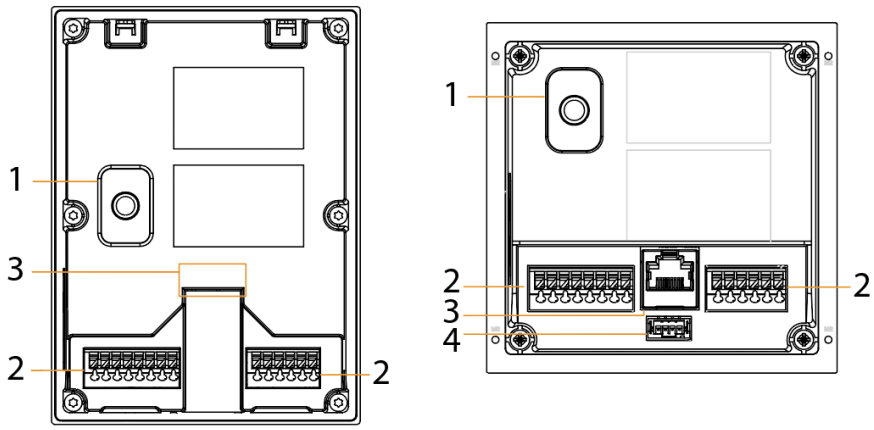


Table 1-13 Rear panel description

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 1-15 Multi-function ports

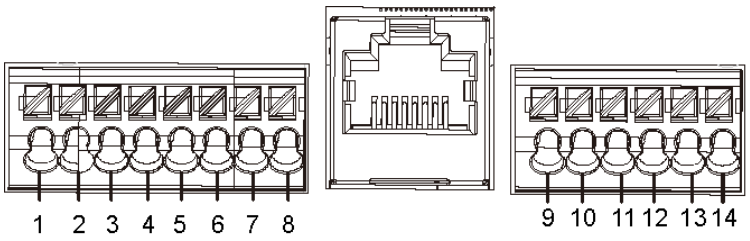


Table 1-14 Port description

No.	Description	No.	Description
1	GND	8	• 2wires-(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	• 2wires+(48V) for a digital 2-wire camera module • 12 V_IN for a full digital camera module	14	DOOR_NO

1.2.5.3 Indicator Module

Figure 1-16 Front panel

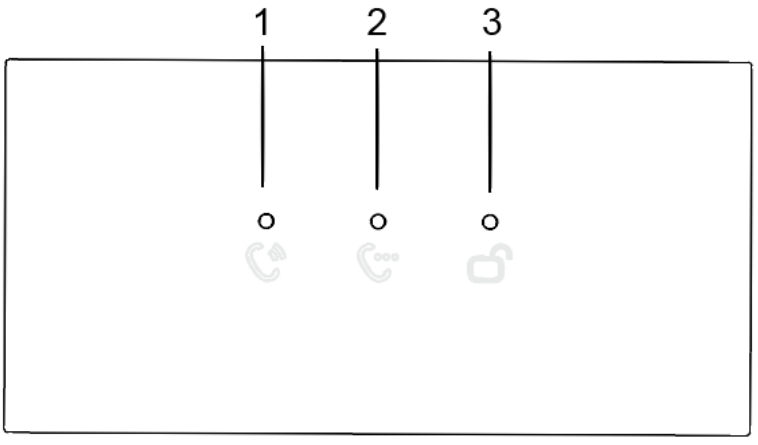


Table 1-15 Front panel description

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

Figure 1-17 Rear panel

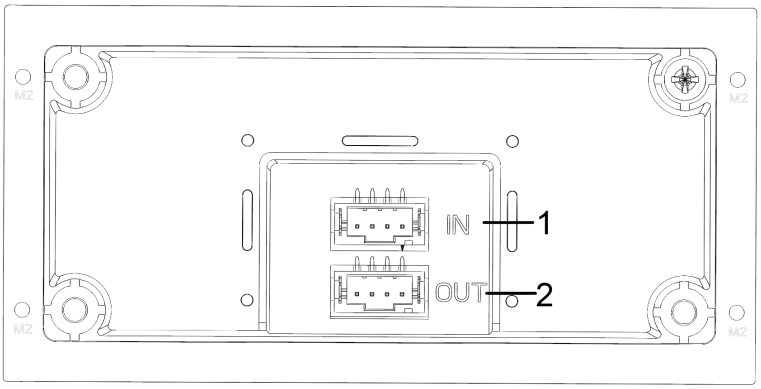


Table 1-16 Rear panel description

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

1.2.5.4 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 1-18 Front panel of the five-button module

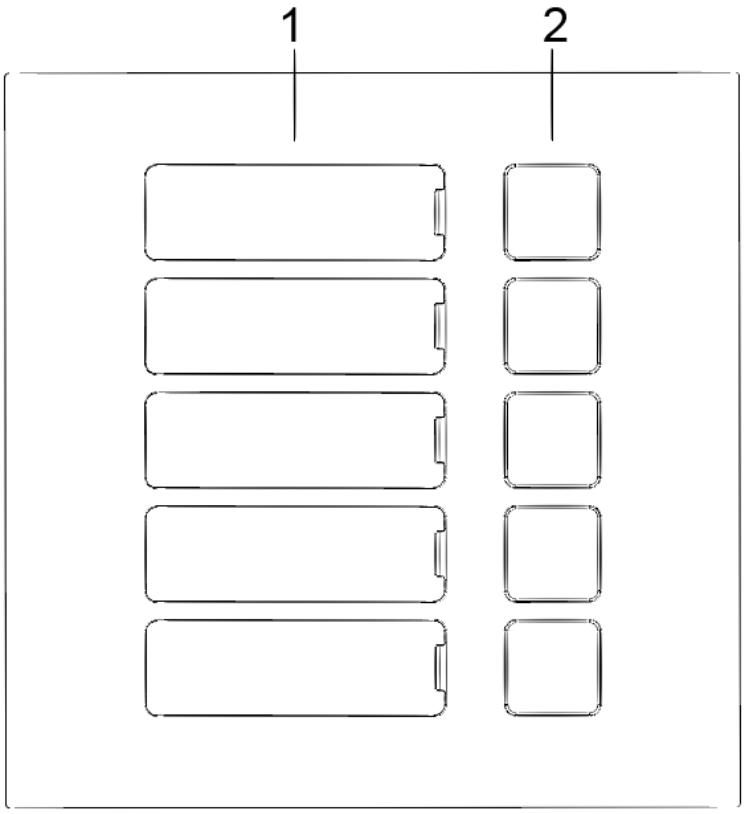


Table 1-17 Front panel description

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

Figure 1-19 Rear panel of the five-button module

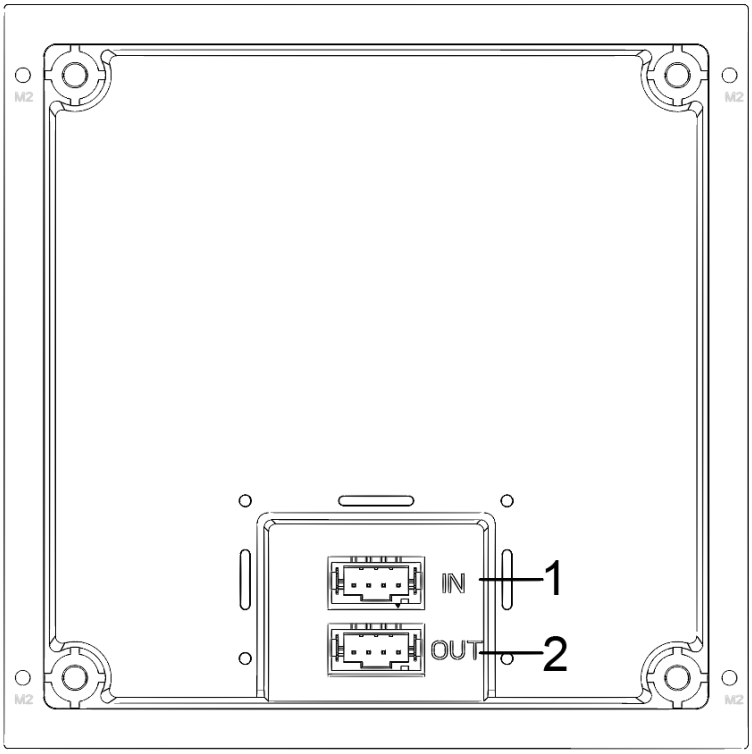


Table 1-18 Rear panel description

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

1.2.5.5 Keyboard Module (with Braille)

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

Figure 1-20 Keyboard module

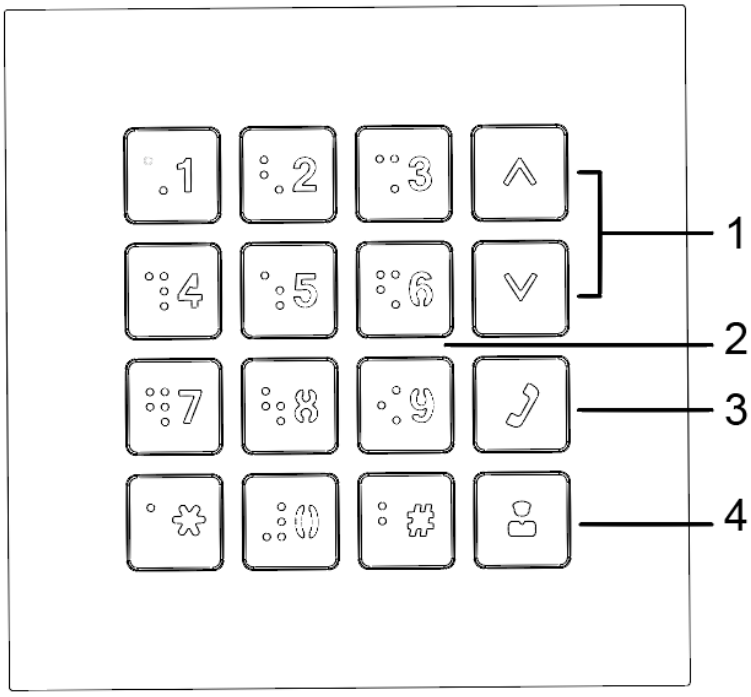


Table 1-19 Keyboard module description

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.

1.2.5.6 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.

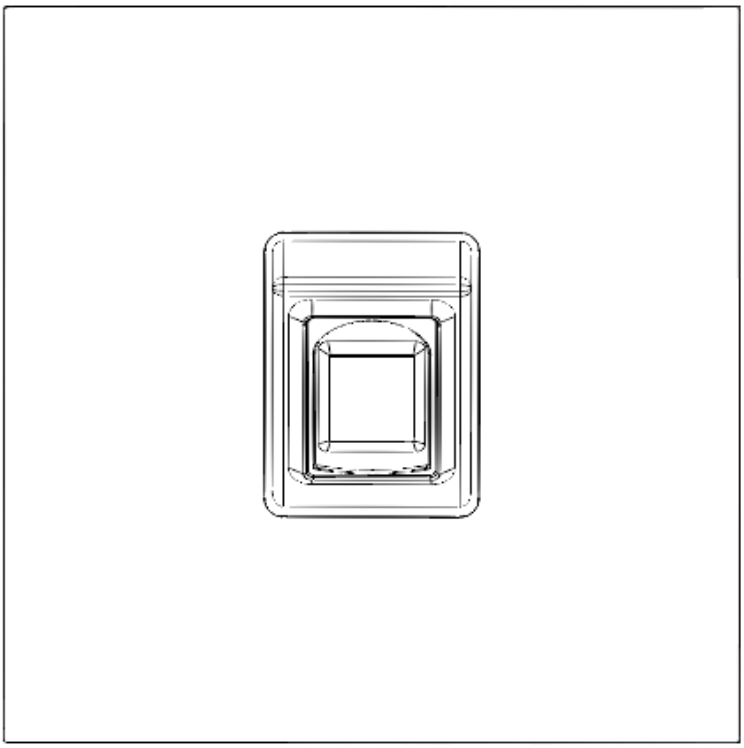
Figure 1-21 Card module

1.2.5.7 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 1-22 Fingerprint module

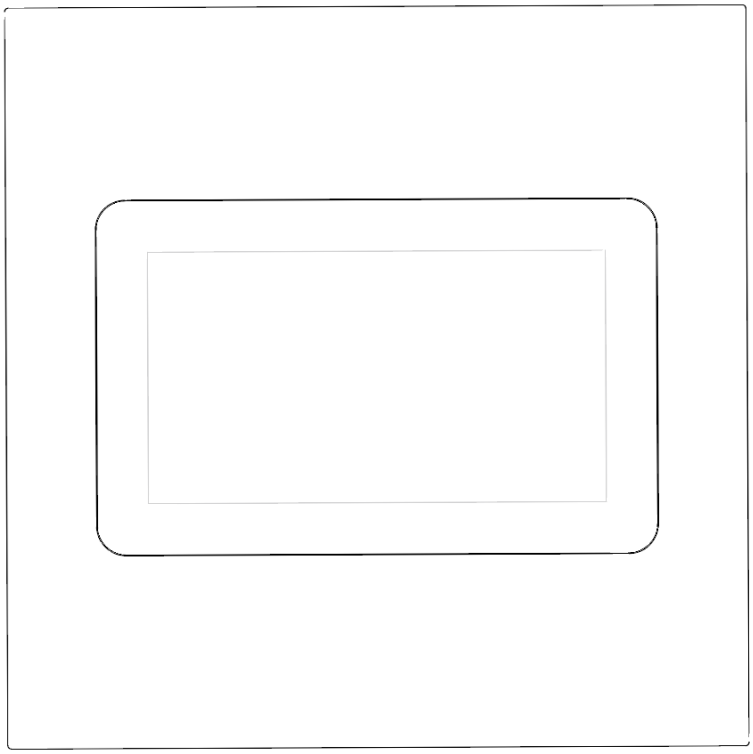


1.2.5.8 Display Module

Displays user information.

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

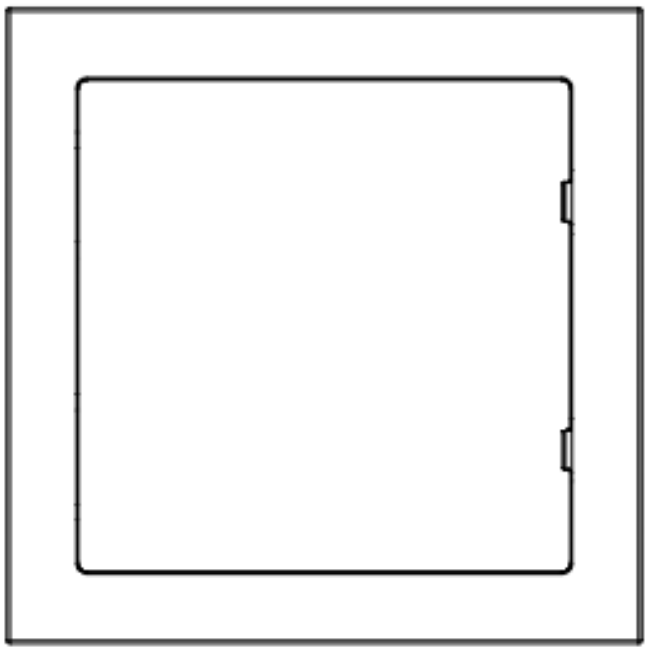
Figure 1-23 Display module



1.2.5.9 Information Module

Displays room number and guest message.

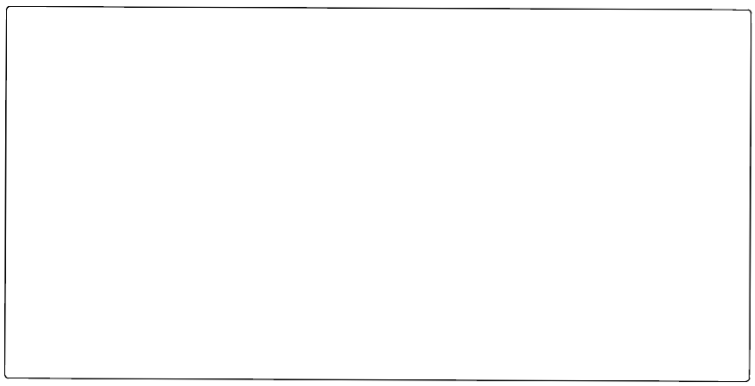
Figure 1-24 Information module



1.2.5.10 Blank Module

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

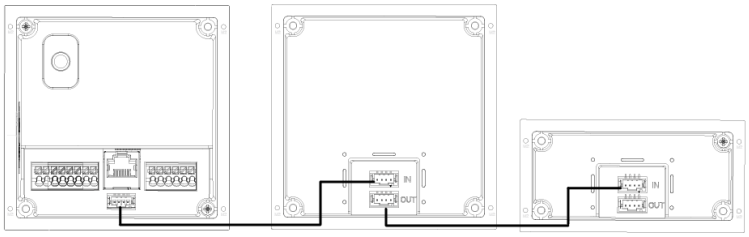
Figure 1-25 Blank module



1.2.5.11 Cascade Connection

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

Figure 1-26 Cascade connection example



1.3 Button Model

1.3.1 Front Panel

Figure 1-27 Front panel

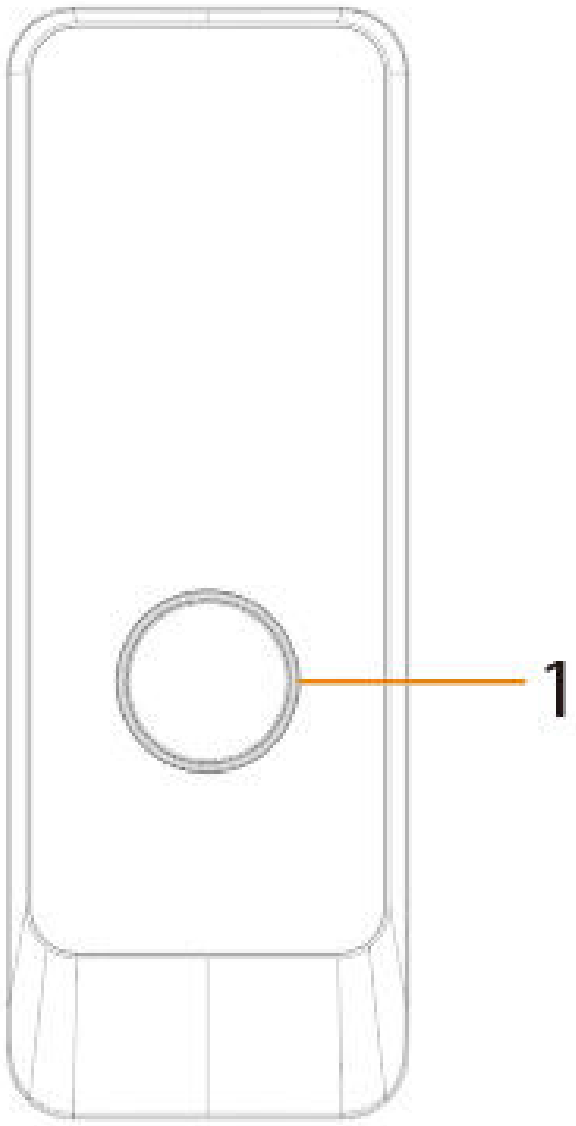


Table 1-20 Components

No.	Name	Function
1	Press button	The button model can be connected to the VTH. Press the button on the model and the VTH receives an alarm signal.

1.3.2 Rear Panel

Figure 1-28 Rear panel

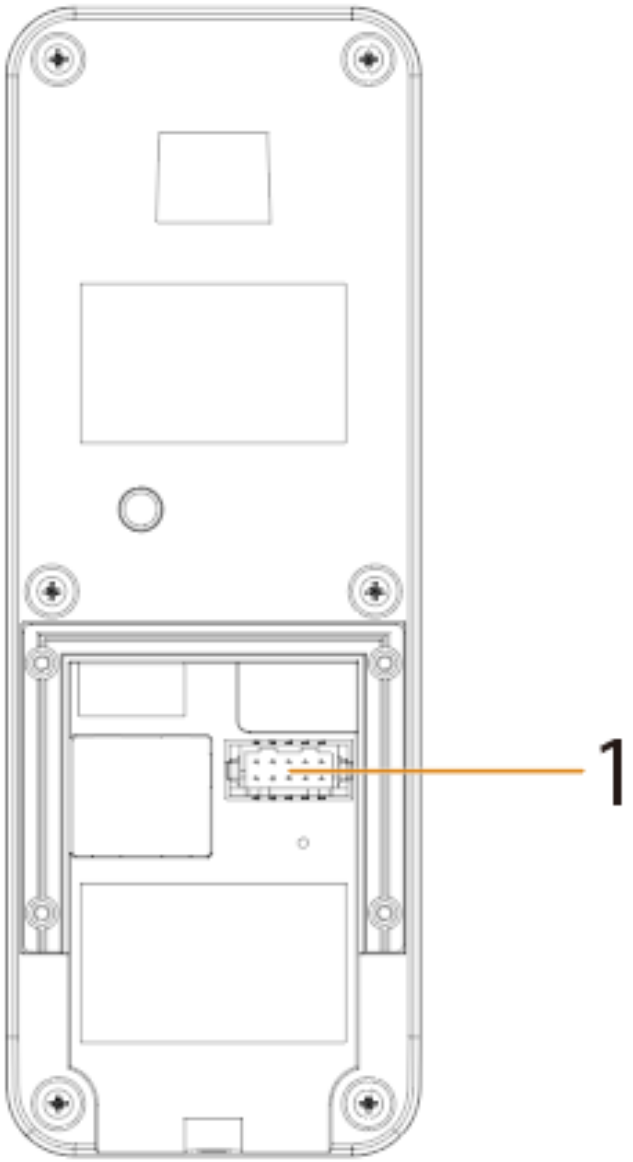
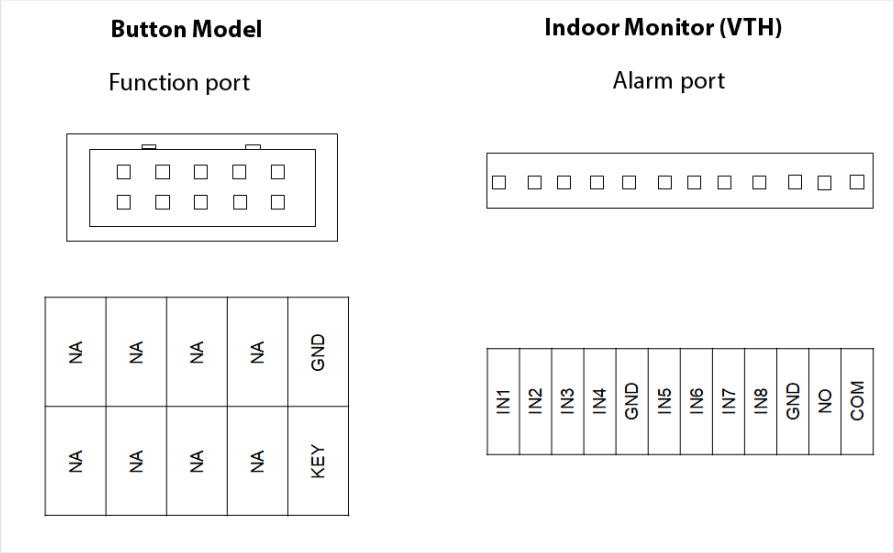


Table 1-21 Components

No.	Name	Function
1	Multi-function port	Used for alarm input.

Figure 1-29 Cable connection



Connect the KEY port of the button model to any one of the alarm input ports of the indoor monitor (VTH) with a cable thread. After that, tap **Setting** > **Alarm** > **Wired Zone** on the VTH and set the **Type** of the alarm input port you chose to connect to the KEY port as **Doorbell**.

2 Initializing the VTO

2.1 Web

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 DMSS APP

If your model only supports Wi-Fi connection to the network, you can only initialize the VTO on the DMSS app. For detailed operation of the app, refer to its user's manual.

Prerequisites

You have downloaded the DMSS in the APP Store (iOS) or Google Play (Android), and have created an account and logged in to the app.

Procedure

Step 1 Power on the VTO.

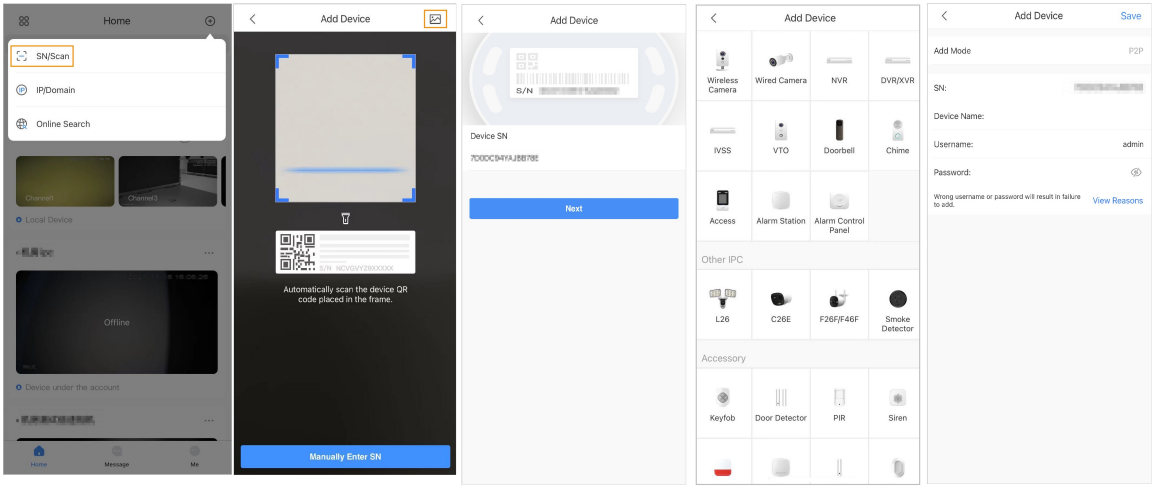
Step 2 Enable hotspot on the VTO through pressing and holding the call button on the VTO until you heard the voice prompt.

The hotspot function is to enable you connect the VTO to the network through **AP configuration** on the app.

Step 3 Add the VTO to the DMSS app.

1. On the **Home** screen, tap ⊕, and then select **SN/Scan**.
2. Add a VTO.
3. You can add through scanning the QR code at the rear panel of the VTO.
4. The SN number of the VTO appears automatically, and then tap **Next**.
5. Select device type as **VTO**, and then the device information appears.
6. Tap **View Reasons**.

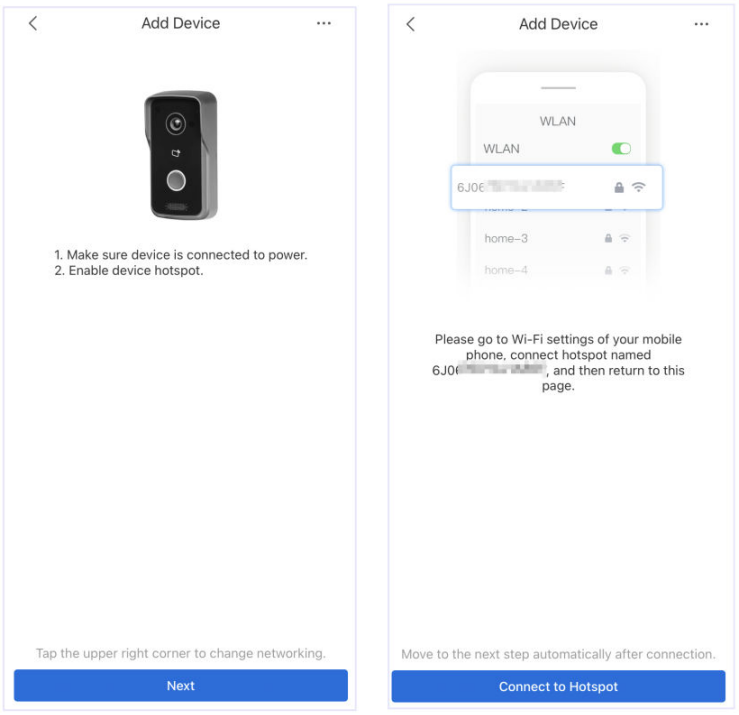
Figure 2-1 Add VTO to DMSS



7. Configure network by switch networking to **AP Configuration** , and then tap **Next**.
8. Connect your phone to the hotspot you just enabled on the VTO.

- The hotspot name is the SN number of your VTO.
- The current page will move on to the next step automatically after connection.

Figure 2-2 AP configuration

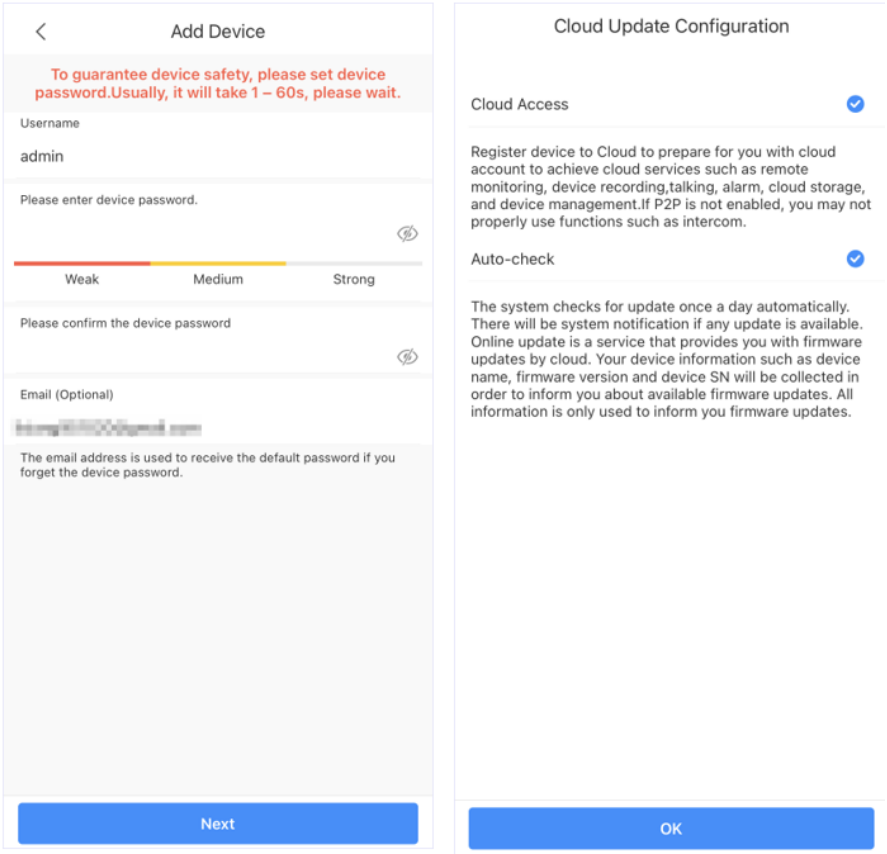


Step 4 Complete initialization based on instructions on the app.

1. Enter the password you planned for the VTO, and confirm it, and then tap **Next**.
2. Select **Cloud Access** and **Auto-check**, and then tap **OK**.

The initialization process is completed.

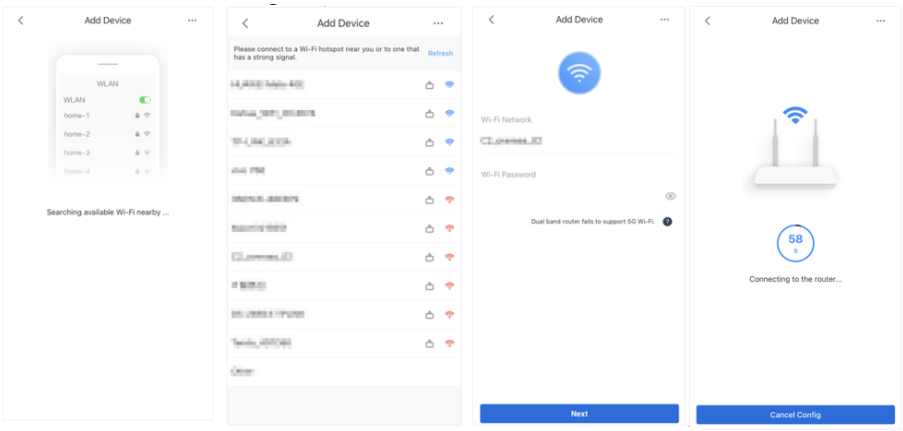
Figure 2-3 Initialization



Step 5 Connect the VTO to the network through Wi-Fi.

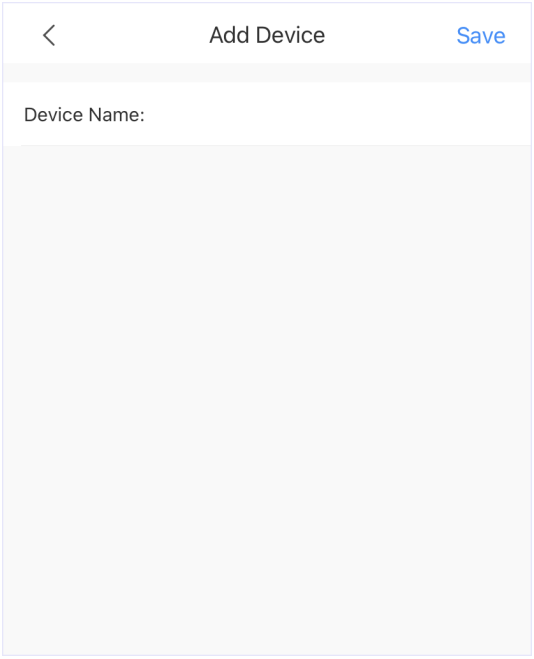
1. Select an available Wi-Fi.
2. Enter the password and tap **Next**. Wait for the VTO to connect to the router.

Figure 2-4 Wi-Fi connection



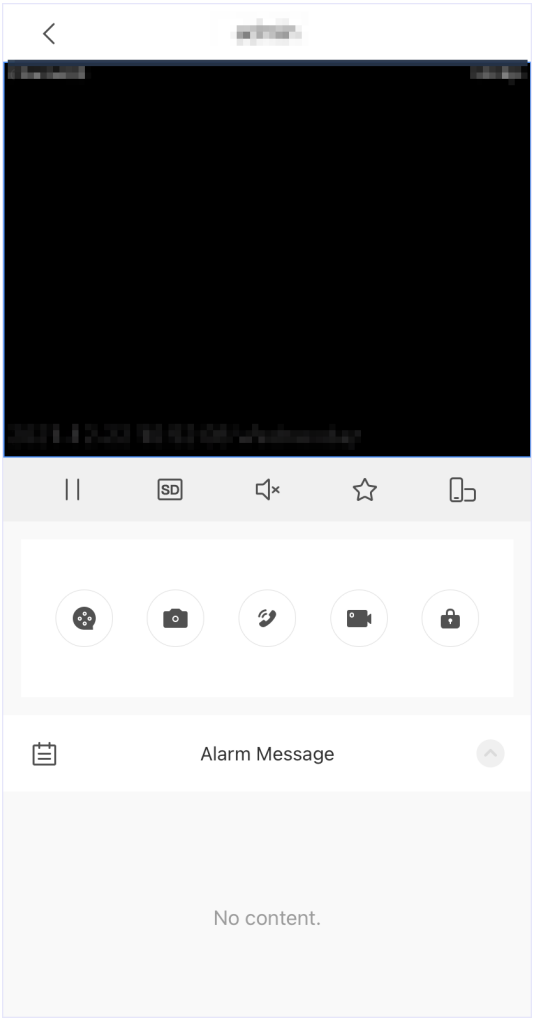
Step 6 Configure device name, and then tap **Save**.

Figure 2-5 Configure device name



Step 7 View monitoring video from the camera on the VTO.

Figure 2-6 Monitor



3 Login and Resetting Password

3.1 Login

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

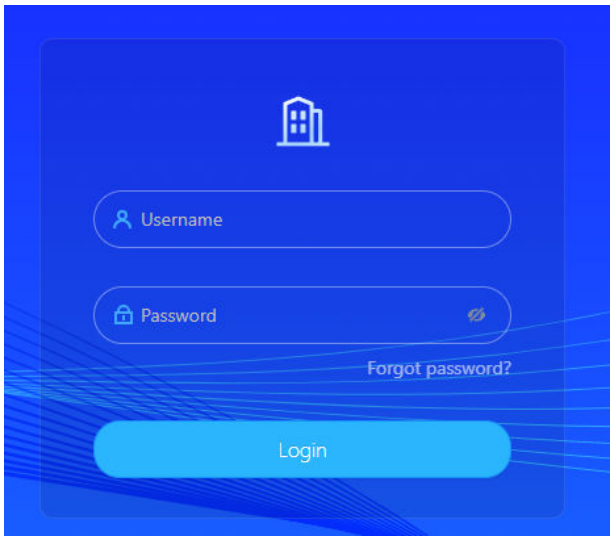
Procedure

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

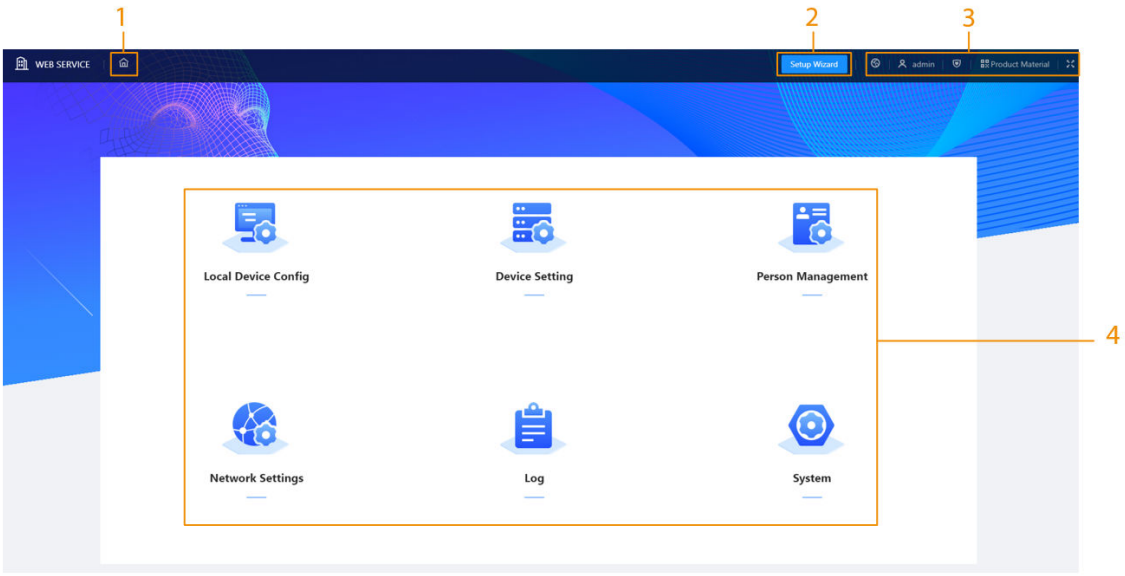


Table 4-1 Home page introduction

No.	Function	Description
1	Home button	Go 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 Material: 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

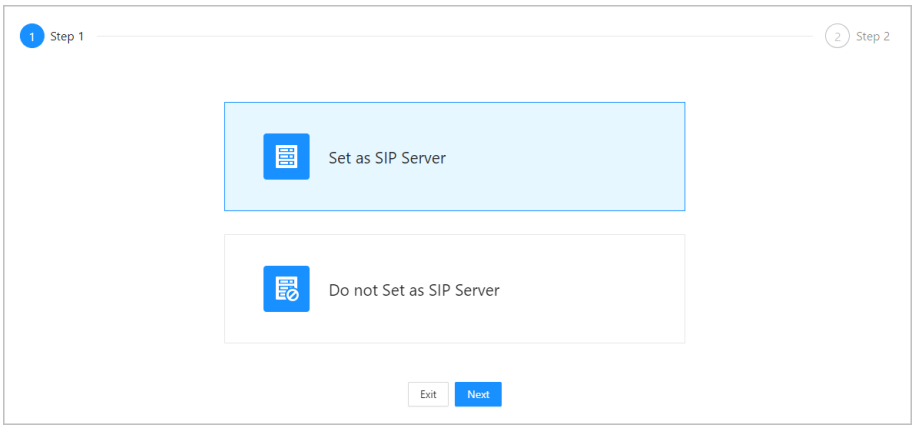
You have added VTOs on the webpage. If not, you can add them in **Set as SIP Server** page or in the **Device Setting** section.

Procedure

Step 1 Log in to the webpage of the VTO.

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

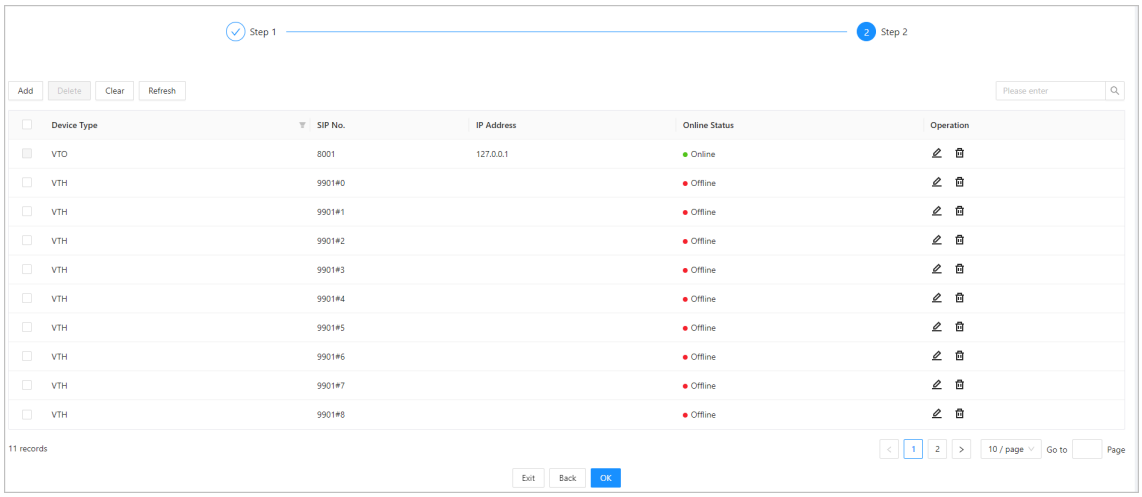
Figure 5-1 Set as SIP server



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

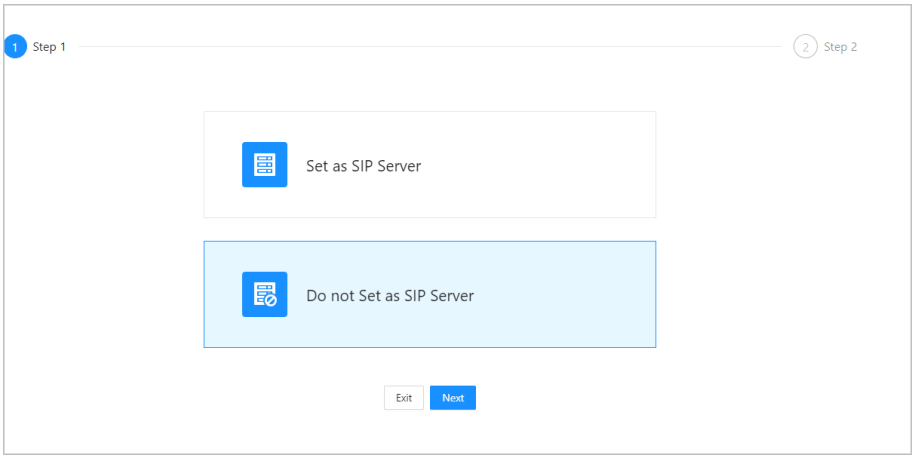
If you want to change the SIP server, you need to remove the current one from the list.

Procedure

Step 1 Log in to the webpage of the VTO.

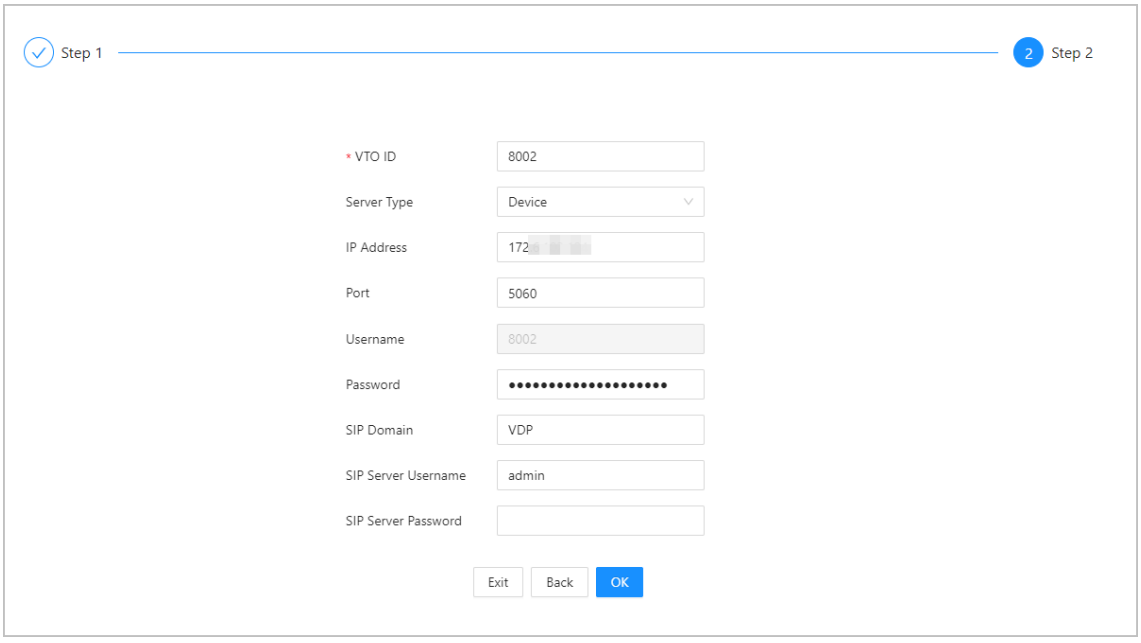
Step 2 Select **Setup Wizard** > **Do not Set as SIP Server**, and then click **Next**.

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.

6.1.1 Villa Door Station

Procedure

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

Step 2 Configure the parameters.

Figure 6-1 Basic settings (villa station)

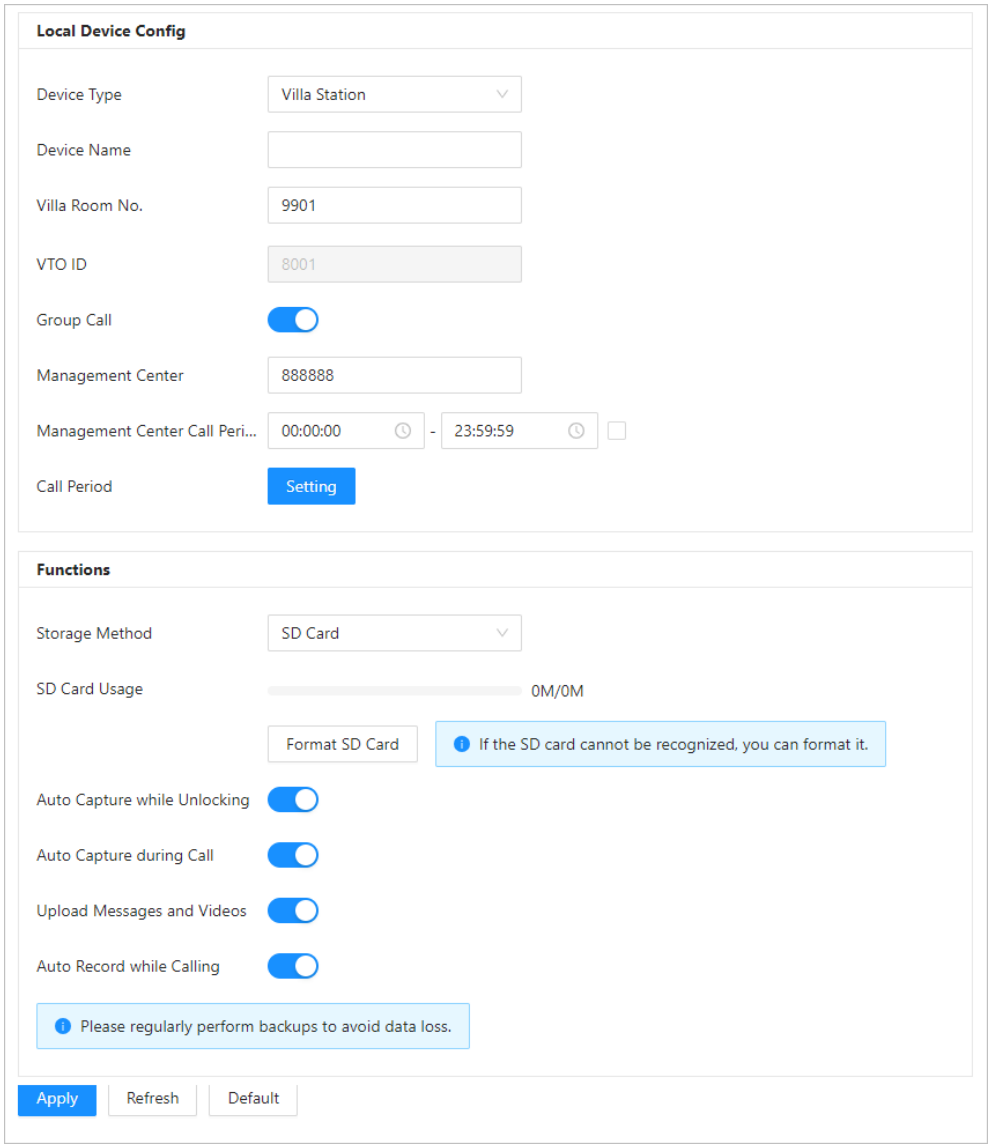


Figure 6-2 Basic settings (small apartment)

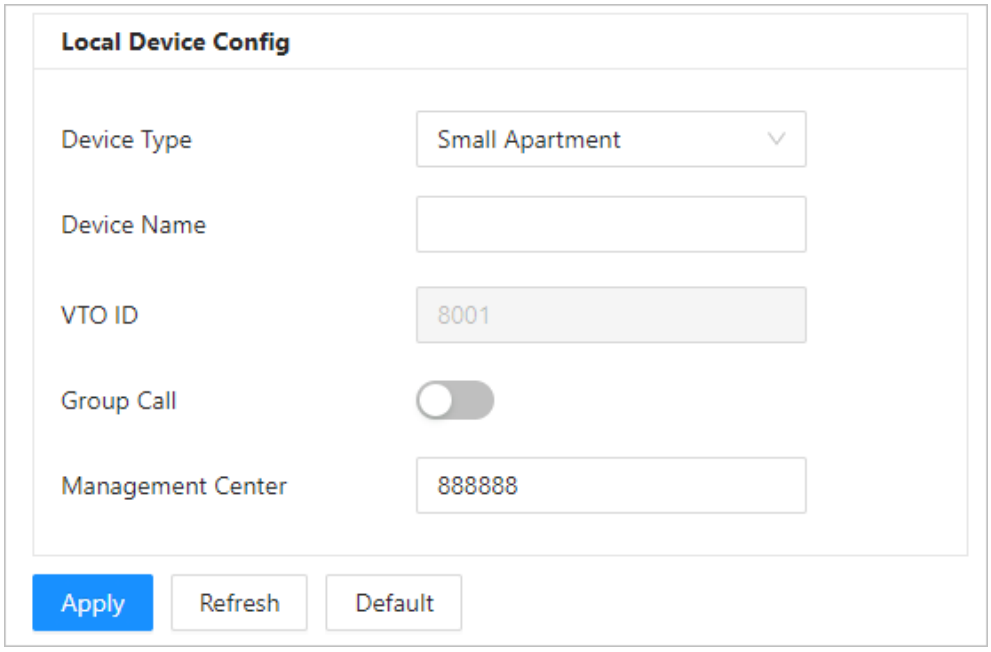


Table 6-1 Basic parameter description

Parameter	Description
Device Type	Select from **Villa Station** and **Small Apartment**. The small apartment is available on select models.
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.
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.
Management Center Call Period	Configure the time period in which the VTO can call the management center, and then enable the function.
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.
Call Period	The time period in which the VTO's calling to other devices is not limited. Click **Setting** to configure the call period in a day/week.
Storage Method	SD card by default.

Parameter	Description
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.
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.

Step 3 Click **Apply**.

6.1.2 Second Confirmation Station

The configuration of second confirmation station is available on select models.

Procedure

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

Step 2 Configure the parameters.

Figure 6-3 Basic settings (Second confirmation station)

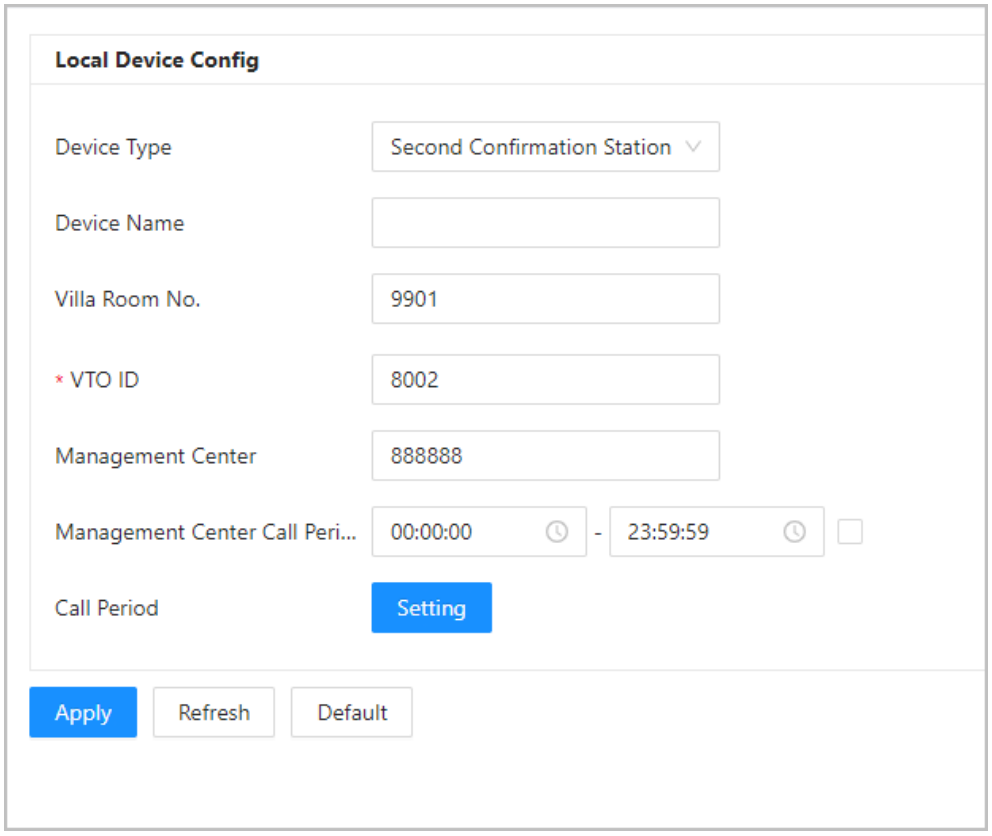


Table 6-2 Basic parameter description

Parameter	Description
Device Type	Select **Second Confirmation Station**.
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.
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.
Management Center Call Period	Configure the time if you only want to receive calls from VTH during a specific period, and then enable the function.
Call Period	Click **Setting** to configure the call period in a day/week.

Step 3 Click **Apply**.

6.2 Access Control

Different model series have varied access control functions. Here is the example for configuring the model Q series.

6.2.1 Config

Procedure

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

Step 2 Configure the parameters.

Figure 6-4 Access control

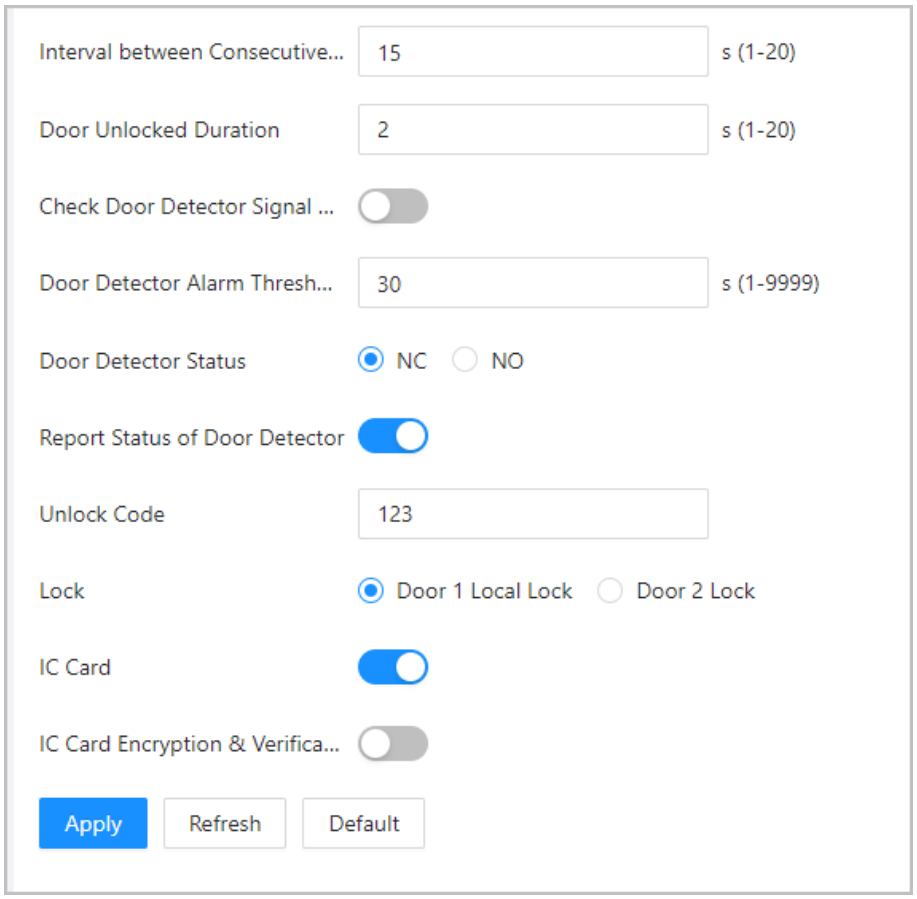


Table 6-3 Access control parameter description

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.
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.
Report Status of Door Detector	Synchronize door sensor status to indoor monitors (VTHs).
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	• **Door 1 Local Lock**: Local lock. • **Door 2 Lock**: RS-485 lock. Select the lock type to unlock the lock you select.
IC Card	Enable the function so that users can swipe cards to unlock door.
IC Card Encryption & Verification	Enable the function so that the IC card encryption and verification take effect.

Step 3 Click **Apply**.

6.2.2 RS-485

Procedure

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

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

Figure 6-5 RS-485

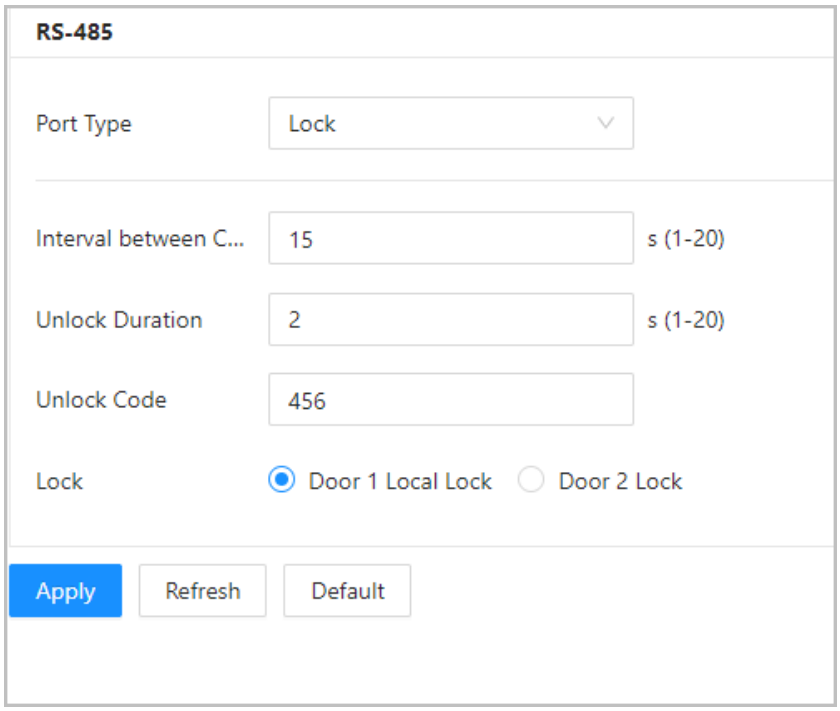


Table 6-4 RS-485 description

Parameter	Description
Port Type	**Lock** by default.

Parameter	Description
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	Select the **Lock** type to unlock the lock you select. • **Door 1 Local Lock**: Local lock. • **Door 2 Lock**: 485 lock.

Step 3 Click **Apply**.

6.2.3 Configuring the Password

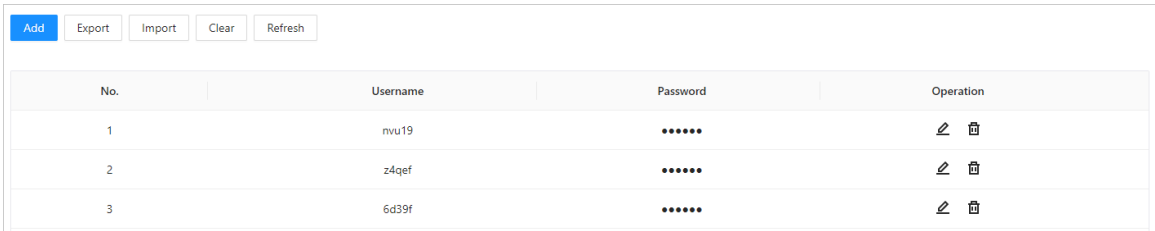
Configure the door opening password.

Procedure

Step 1 Log in to the webpage.

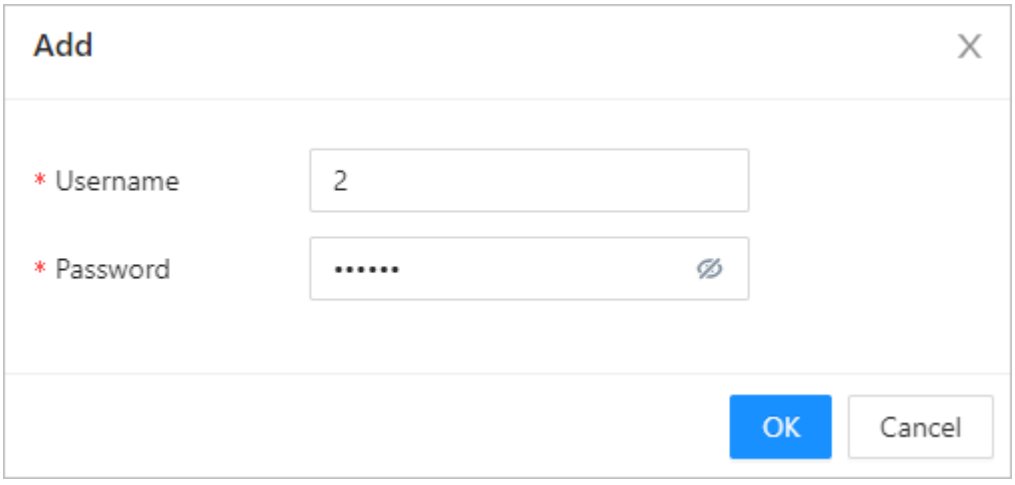
Step 2 Select **Local Device Config** > **Access Control** > **Password Settings**.

Figure 6-6 Password settings



Step 3 Click **Add**.

Figure 6-7 Add the password



Step 4 Configure the username and the password, and then click **OK**.

Related Operations

- Edit: Click to edit the password.
- Delete: Click to delete the password.
- Clear: Click **Clear** to delete all the passwords.
- Refresh: Click **Refresh** to refresh the page.
- Click **Export** or **Import** to export or import the password.

6.3 Configuring Wiegand

Supports access Wiegand devices. 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 6-8 Wiegand input

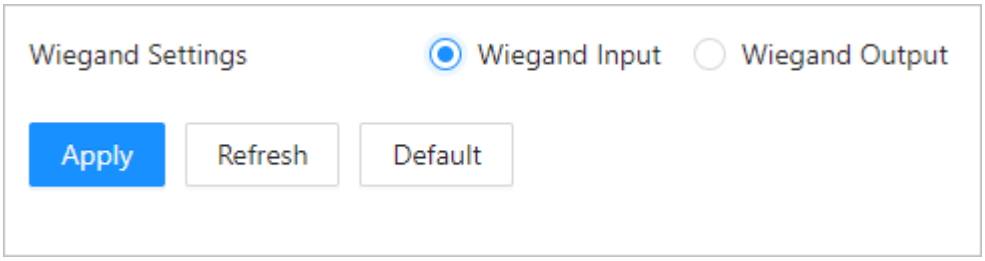


Figure 6-9 Wiegand output

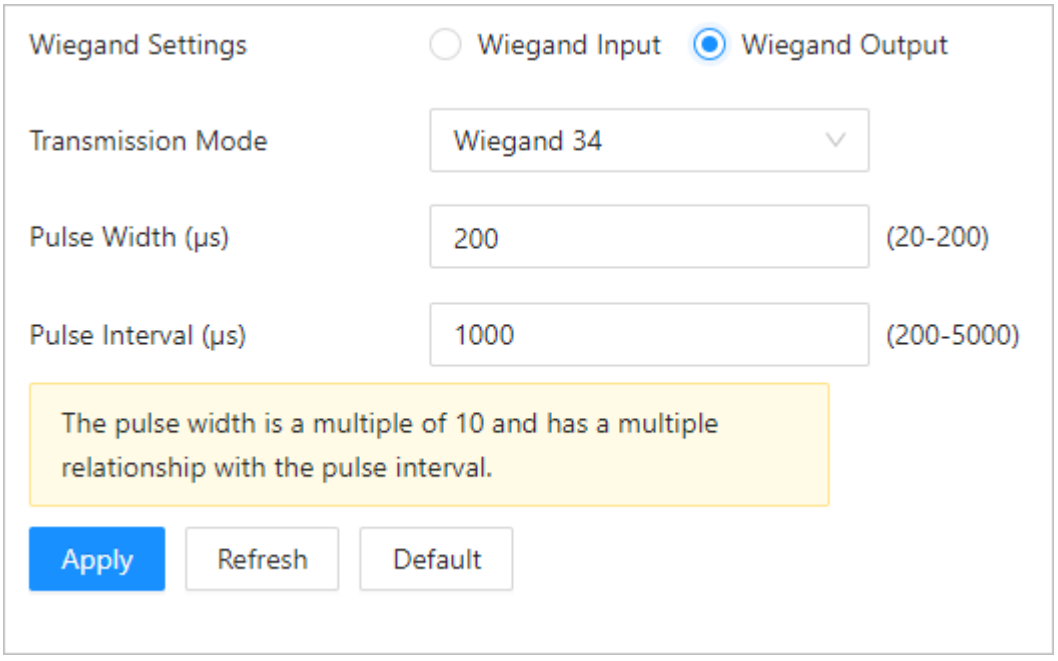


Table 6-5 Description of Wiegand parameters

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 Output	Wiegand Output Type	Select a Wiegand format to read card numbers or ID numbers. • **Wiegand26** : Reads three bytes or six digits. • **Wiegand34** : Reads four bytes or eight digits. • **Wiegand66** : Reads eight bytes or sixteen digits.
	Pulse Width	Enter the pulse width and pulse interval of Wiegand output.
	Pulse Interval	

Step 4 Click **Apply**.

6.4 Layout

6.4.1 Layout (Multiple Buttons)

This function is only available for select models with multiple buttons (1 button, 2 buttons and 4 buttons). Here is an example of configuration for the VTO that has one button installed on its device.

Procedure

Step 1 Log in to the webpage of the VTO.

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

Step 3 Click the nameplates next to where you have installed the button(s), and then select the room number(s) from the **Module** you want to bind. For example, 9901, 9902, 9903 and 9904.

- You need to first configure the room number. Otherwise, you have no room number to select from in the module list. VTH room numbers is configured in **Device Setting**. For details, see "8.2 VTH Management".
- You need to configure the room number based on your installation position of buttons. For example, if you have only installed one button next to the first nameplate, then you need to click the module of first nameplate to configure the room number on the webpage. If you have installed one button next to the fourth nameplate, then you need to click the module of fourth nameplate to configure the room number on the webpage. Keep the above configuration rule when you install 2 buttons or 4 buttons on the VTO and configure the corresponding room numbers on the webpage.

Figure 6-10 Fourth button installation

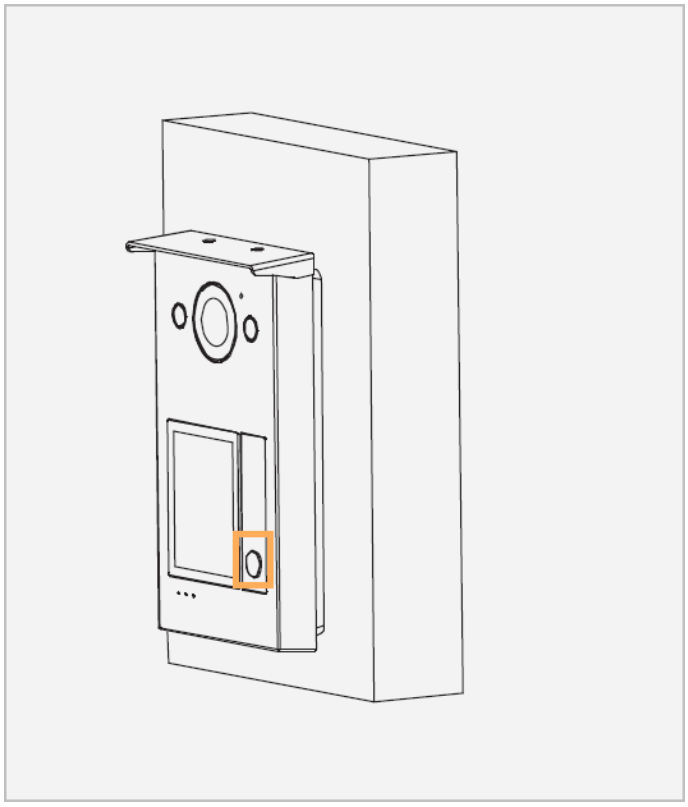
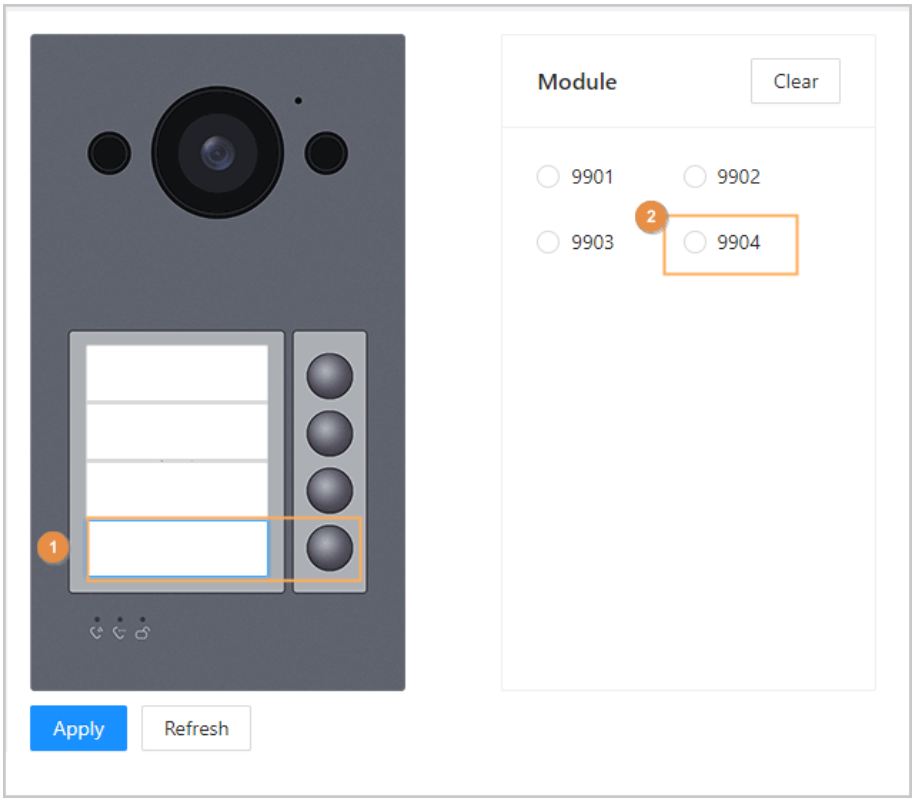
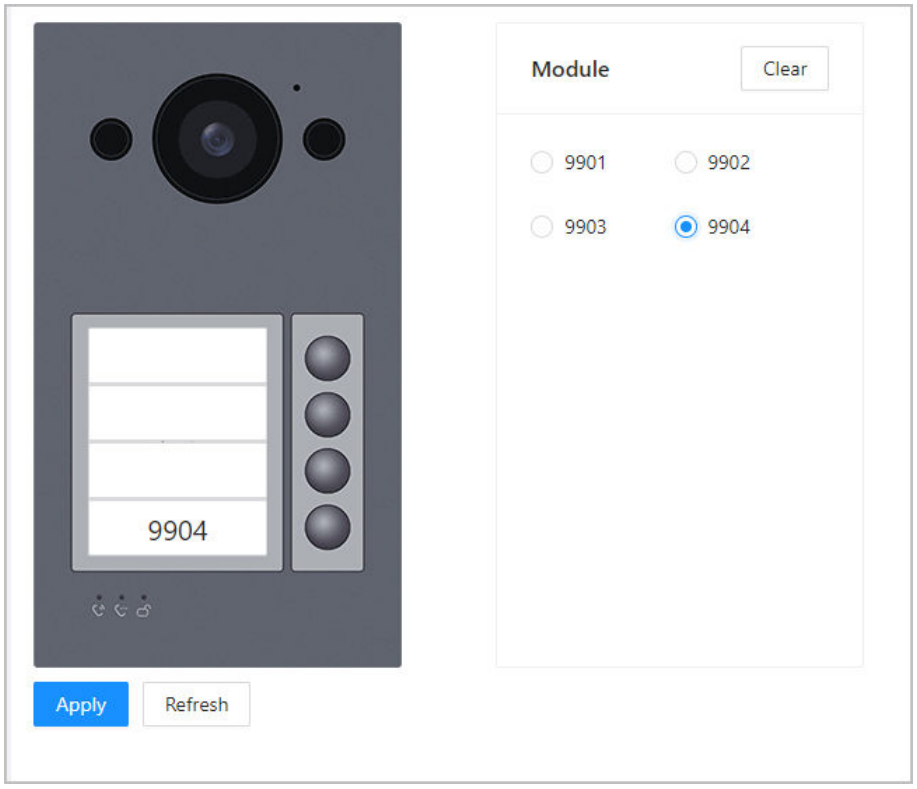


Figure 6-11 Configure the fourth nameplate (1)



Step 4 Click **Apply** to save the selected room number.

Figure 6-12 Configure the fourth nameplate (2)



Step 5 If you want to bind room numbers when you install 2 buttons or 4 buttons for the VTO, repeat Step 3 to Step 4 until you have configured all of the room numbers.

6.4.2 Layout (Multiple Modules)

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

Procedure

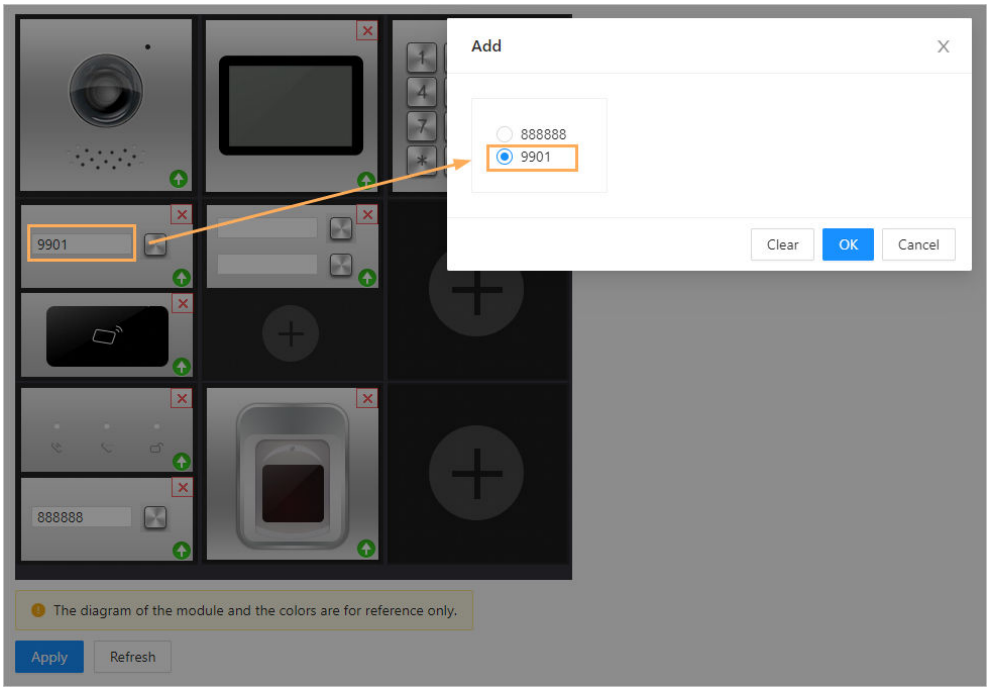
Step 1 Log in to the webpage of the VTO.

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

Step 3 Click the nameplates on the corresponding module, and then select the room number you want to bind.

You need to first configure the room number. Otherwise, you have no room number to select from in the module list. VTH room numbers is configured in **Device Setting**. For details, see "8.2 VTH Management".

Figure 6-13 Configure the nameplate



Step 4 Click **OK** to save the selected room number.

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.

Related Operations

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

6.5 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 gets the IPC information.

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

6.5.1 Adding the IPC One by One

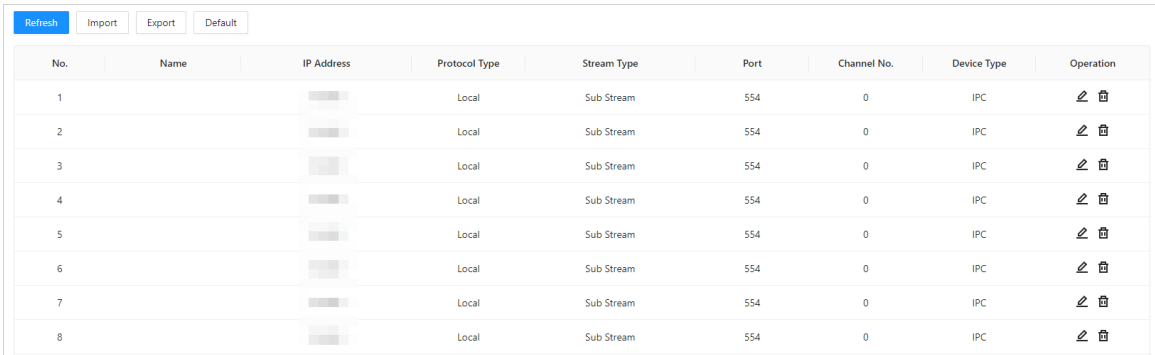
Add the information of the video monitoring device one by one.

Procedure

Step 1 Log in to the webpage.

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

Figure 6-14 IPC information



Step 3 Click to configure the parameters.

Figure 6-15 Configure the parameters

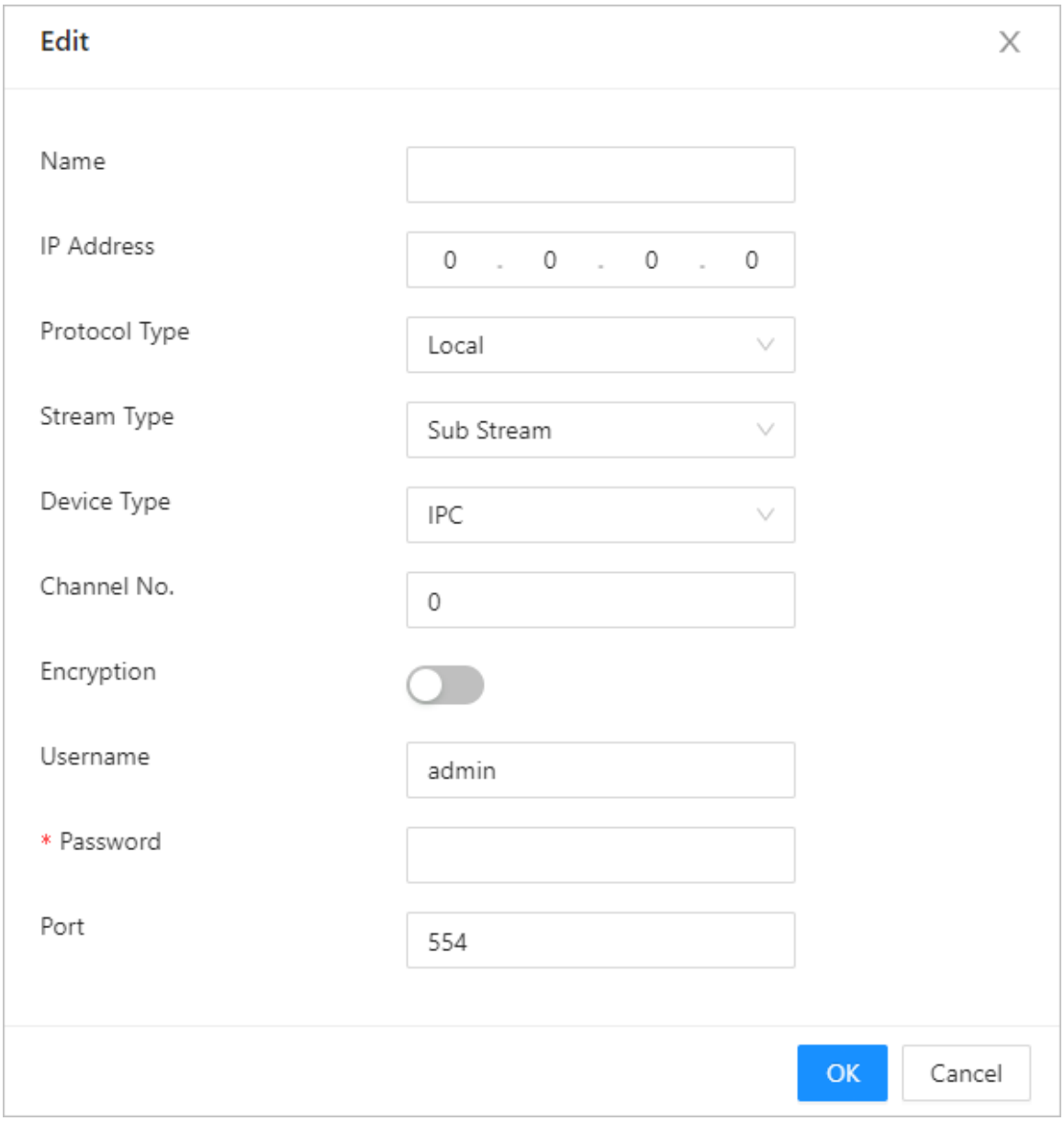


Table 6-6 Parameters description of the video monitoring device

Parameter	Description
IPC 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.
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 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 login password, and then click **OK**.

The IPC configuration file is saved to the local computer.

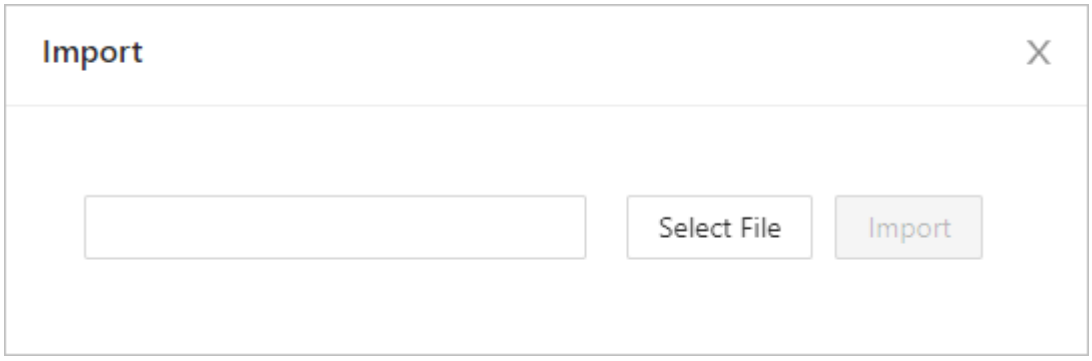
6.5.3 Importing the IPC Information in Batches

Import the IPC information to the system.

Procedure

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

Figure 6-16 Import



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

7 System

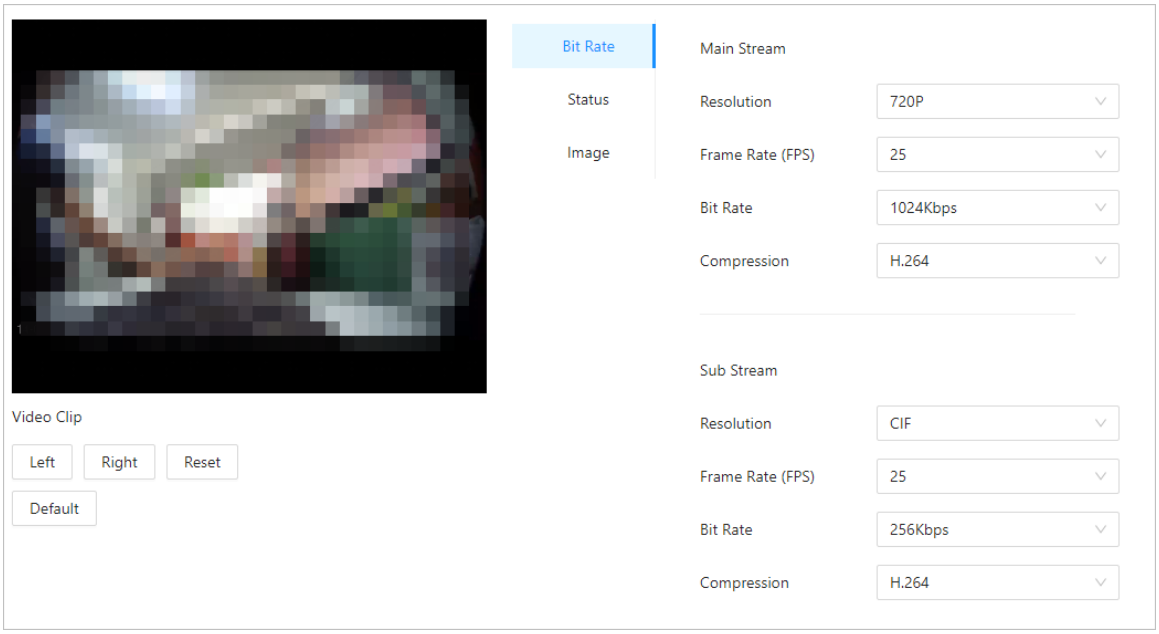
7.1 Video

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

Procedure

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

Figure 7-1 Video



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

Table 7-1 Video parameter description

Parameter		Description
Bit Rate	Resolution (Main Stream)	• **720P** : 1280 × 720. • **WVGA** : 800 × 480. • **D1** : 704 × 576. • **CIF** : 352 × 288.
	Frame Rate (FPS) (Main Stream)	• 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 (Main Stream)	Include 768 Kbps, 896 Kbps, 1024 Kbps, 1.25 Mbps, 1.5 Mbps, 1.75 Mbps, 2 Mbps and 4 Mbps and more. The larger the value, the better the video quality, but it requires more bandwidth.

Parameter		Description
	Compression (Main Stream)	H.264. H.265. Compared with H.264, H.265 requires smaller bandwidth.
	Resolution (Sub Stream)	• **1080P** : 1920 × 1080. • **WVGA** : 800 × 480. • **QVGA** : 320 × 240. • **D1** : 704 × 576. • **CIF** : 352 × 288.
	Frame Rate (FPS) (Sub Stream)	The range is 1 to 25. The larger the value, the smoother the video, but it requires more bandwidth.
	Bit Rate (Sub Stream)	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 (Sub Stream)	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.
	Illuminator Sensitivity	Configure the sensitivity value. • If the illumination intensity is lower than the configured value, the illuminator will be turned on. • If the illumination intensity is higher than the configure value, the illuminator will be turned off.
Image	Brightness	The larger the value, the brighter the image.
	Contrast	Larger value for more contrast between bright and dark areas.

Parameter		Description
	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.
	Gamma	Changes the picture brightness and improves the picture dynamic range in a non-linear way. The larger the value, the brighter the image. This function is available on select models.
	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.

Related Operations

Click **Left** or **Right** to adjust the video image.

Click **Reset** or **Default** to reset the video configurations or restore to default configurations.

7.2 Audio

Procedure

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

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

Figure 7-2 Audio

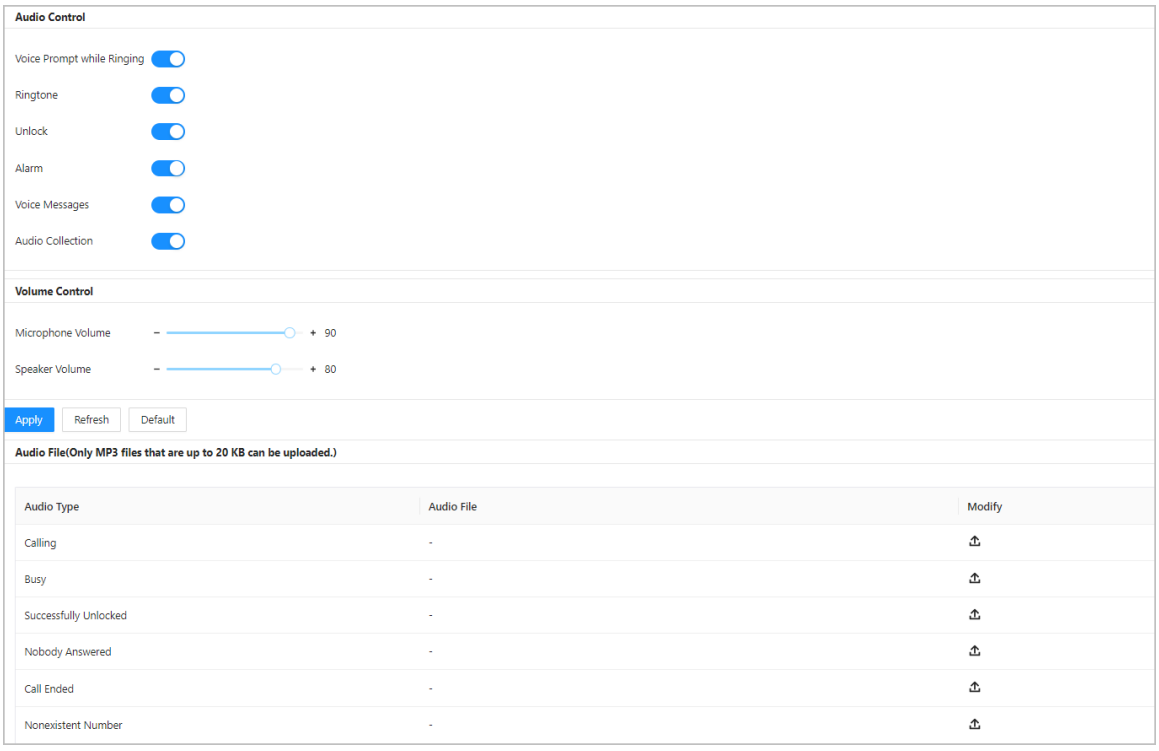


Table 7-2 Audio parameter description

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 volume.
	Speaker Volume	

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).

Only MP3 files that are up to 20 KB can be uploaded.

7.3 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 7-3 Time

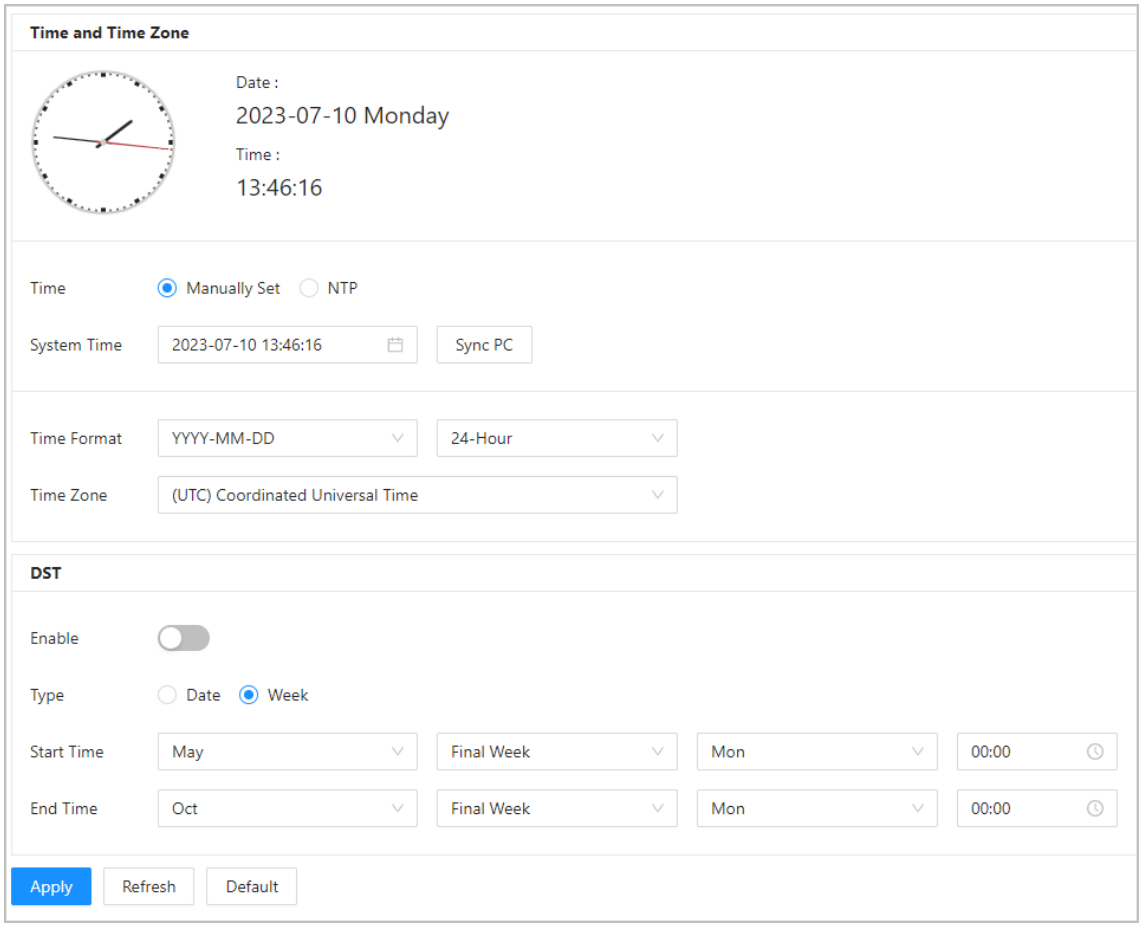


Table 7-3 Parameter description

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

Module	Parameter	Description
	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**.

7.4 ONVIF User

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

Procedure

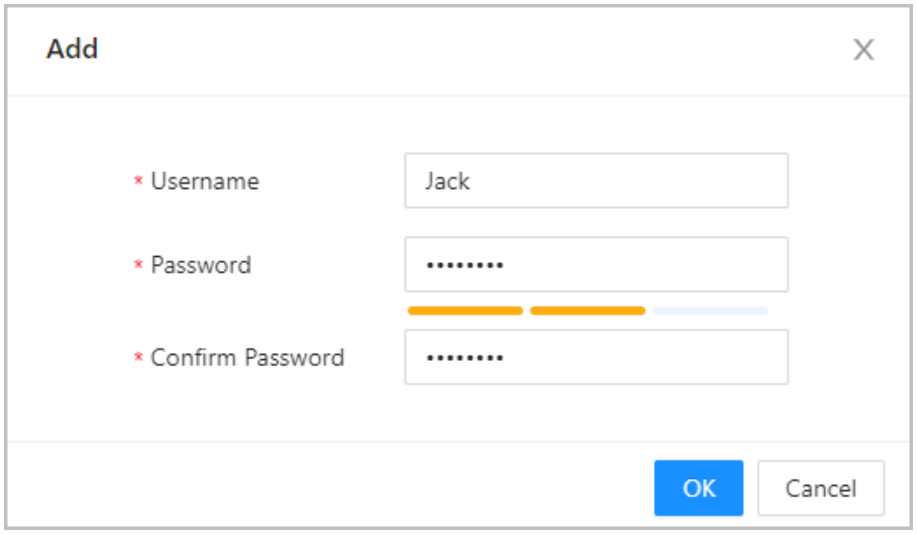
Step 1 Select **System** > **ONVIF User**.

Step 2 Click **Add**.

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

ONVIF devices can monitor the VTO by using the account.

Figure 7-4 ONVIF user



7.5 Config

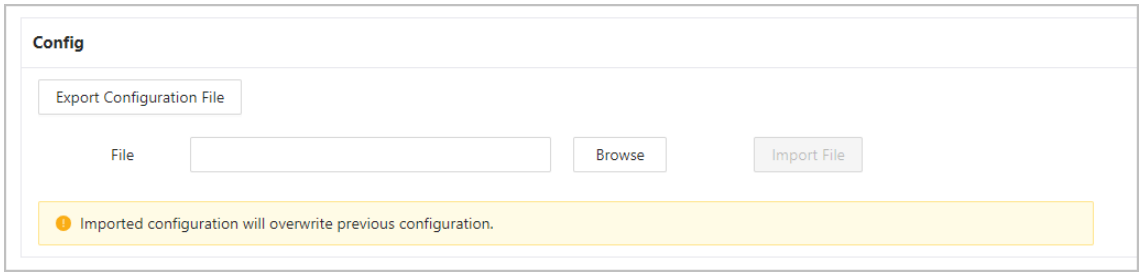
You can export and import the configuration file.

Procedure

Step 1 Select **System** > **Config**.

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

Figure 7-5 Config



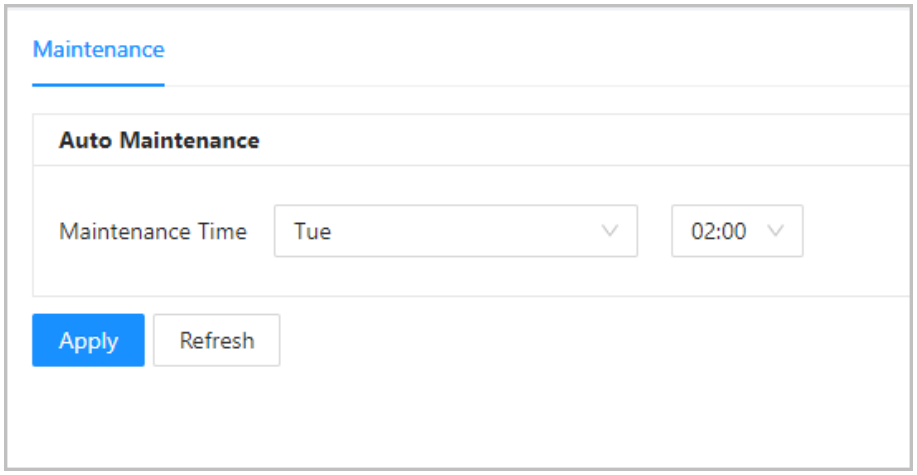
7.6 Maintenance

Procedure

Step 1 Select **System** > **Maintenance**.

Step 2 Configure the auto maintenance time.

Figure 7-6 Auto Maintenance



Step 3 Click **Apply**.

7.7 Updating

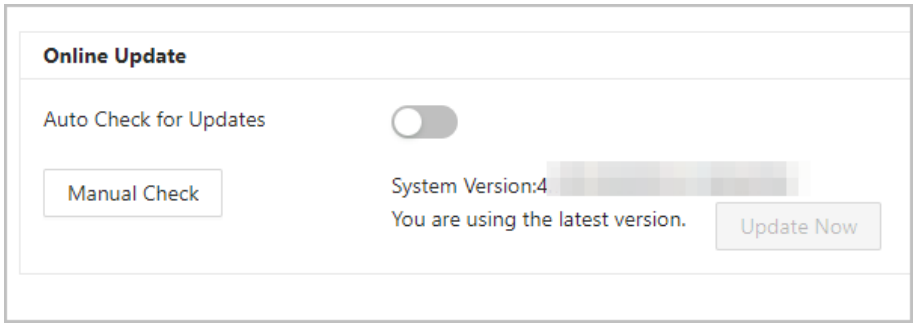
Procedure

Step 1 Select **System** > **Update**.

Step 2 Select ways to check the update.

- **Auto Check** : Select 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 7-7 Update



7.8 Legal Information

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

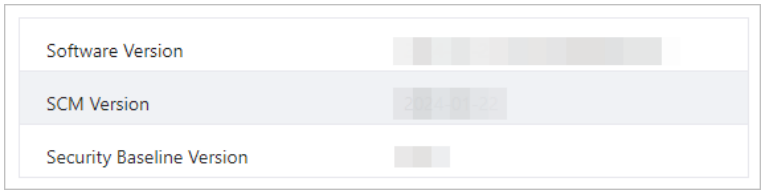
7.9 System Information

Procedure

Step 1 Select **System** > **System Info**.

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

Figure 7-8 System information



8 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.

8.1 VTO No. 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 8-1 Add VTO

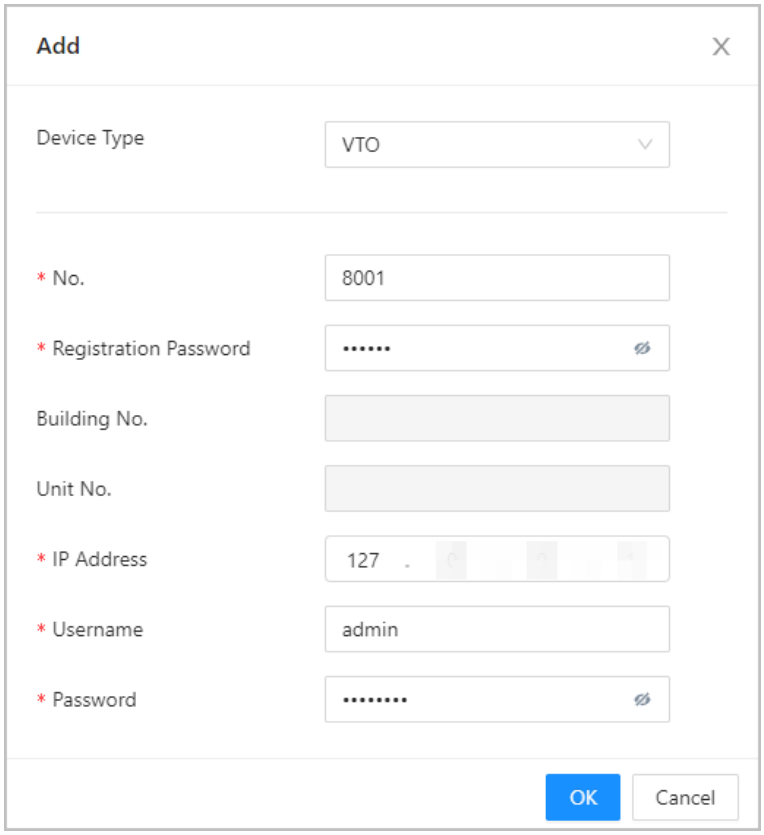


Table 8-1 Add VTO configuration

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 work as the SIP server.
Unit No.	
IP Address	IP address of the VTO.
Username	Username and password used to log in to the webpage of the VTO.
Password	

Step 5 Click **OK**.

Click to edit the VTO, or to delete added VTOs, but the one that you have logged in to cannot be modified or deleted.

8.2 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 add mode as **Add One by One**.

Figure 8-2 Add VTH one by one

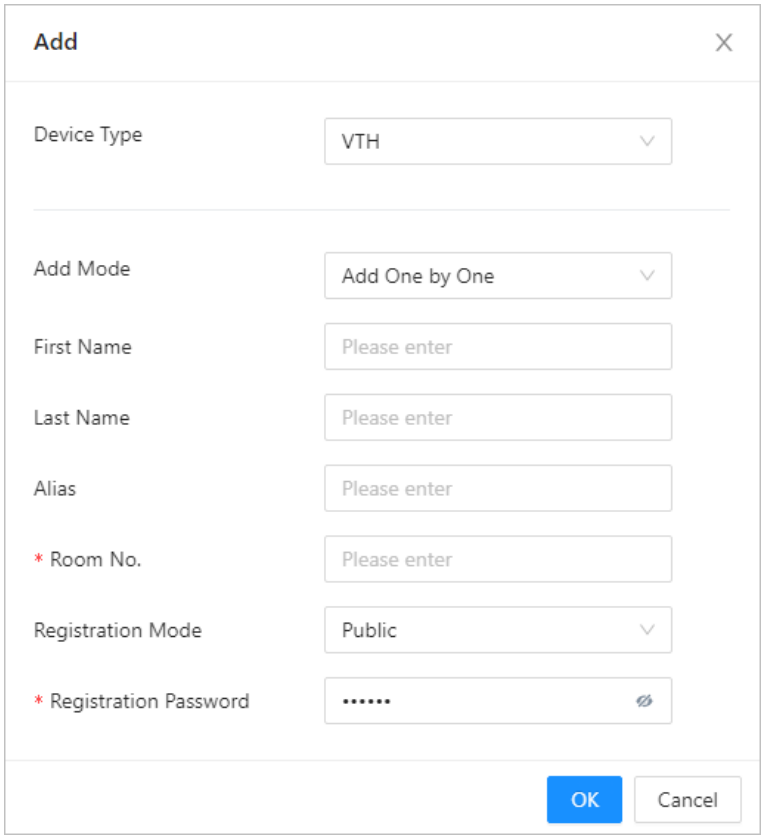


Table 8-2 Parameters description

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.

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

Figure 8-3 Add VTH in batches

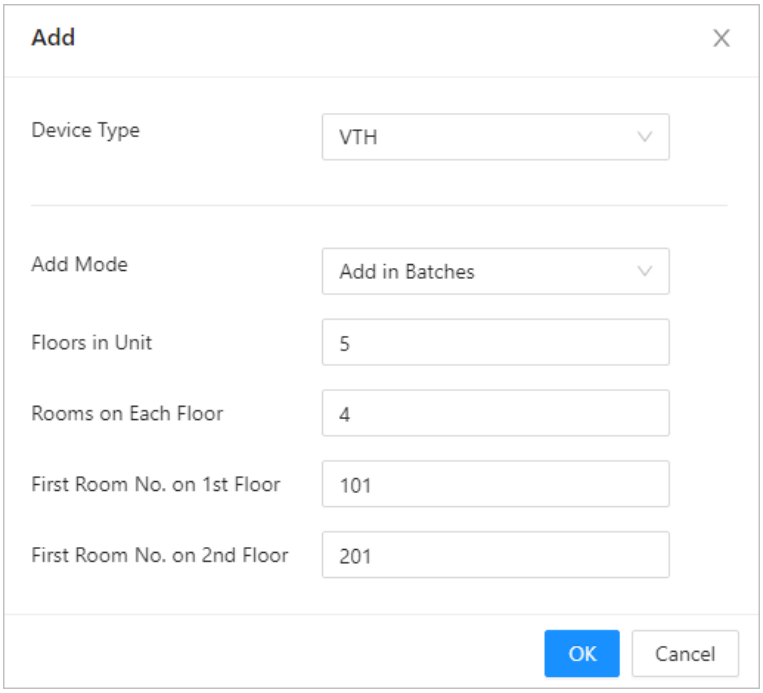


Table 8-3 Parameters description

Parameter	Description
Floors in Unit	Configure the number of floors, 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.

8.3 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 8-4 Add VTS

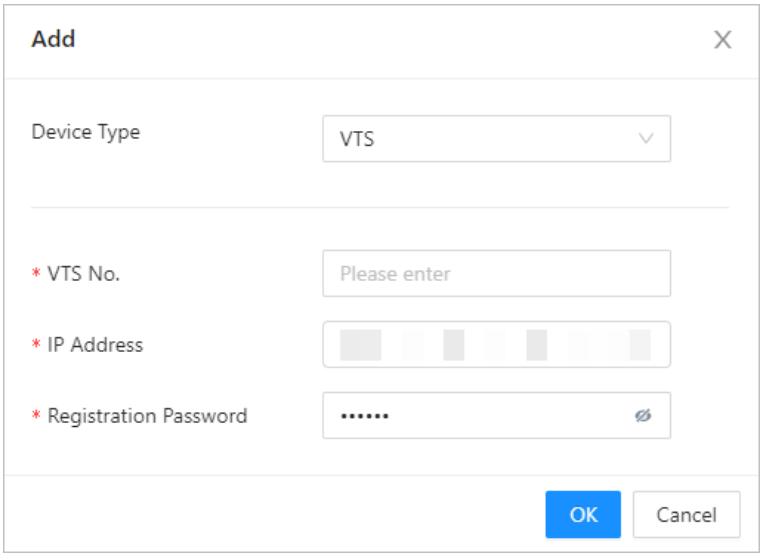


Table 8-4 Add VTS configuration

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**.

9 Person Management

Adding personnel information.

The card and fingerprint functions are available on select models or when the device is connect to the corresponding modules.

Procedure

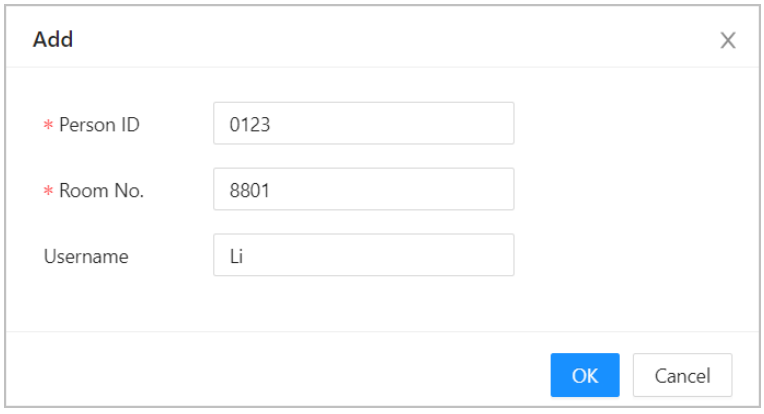
Step 1 Log in to the webpage of the VTO.

Step 2 Select **Person Management**.

Step 3 Click **Add**.

- VTO that do not have other functions or modules: Enter the room ID, room number, username, and then click **OK**.

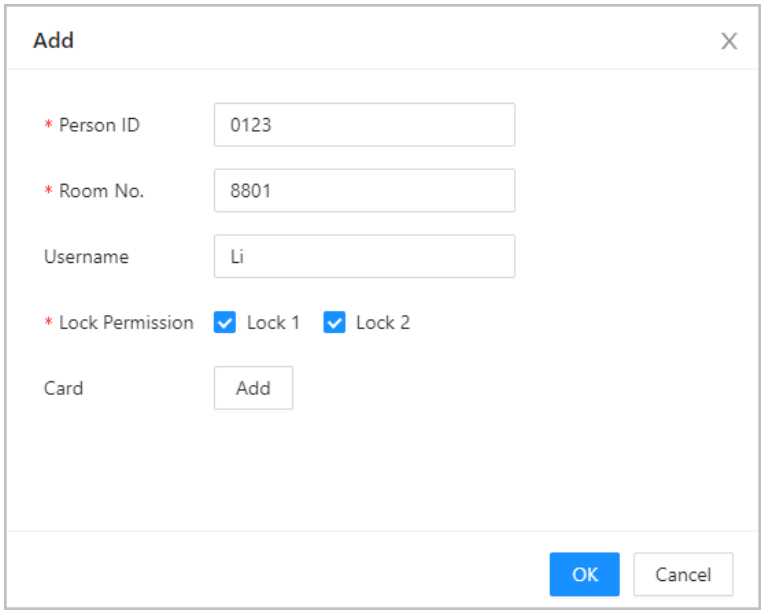
Figure 9-1 Add person



- VTO that has card issuing function or module:
  1. Enter the room ID, room number, username and select the lock permission.
     - Lock1: Local lock.
     - Lock 2: 485 lock.

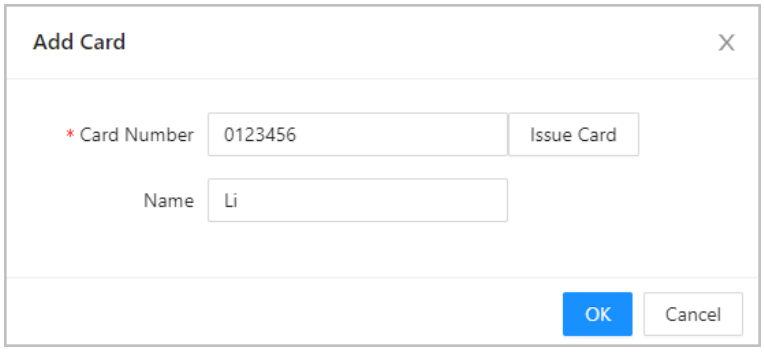
       Only models that have 485 ports support 2 types of locks.

Figure 9-2 Add a person



2. Click **Add** next to **Card**, and then enter the card number and name.

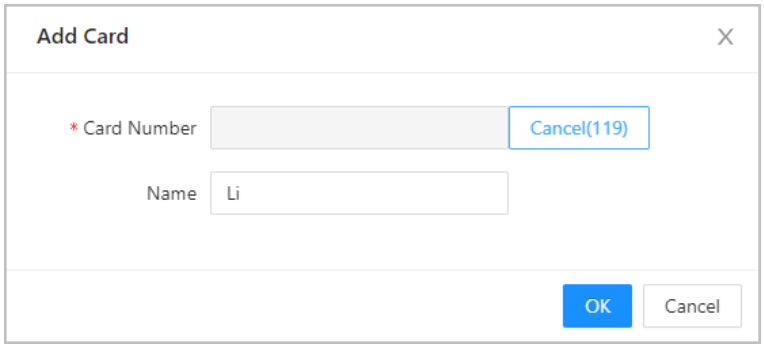
Figure 9-3 Issue card



3. Click **Issue Card**.

   The webpage displays the countdown prompt (120 seconds). Once the countdown starts, you need to swipe the card on the card reader of the VTO within this time period. After the swiping, the card number will be automatically recognized by the VTO.

Figure 9-4 Countdown



4. Click **OK** after swiping to complete the issuing process.

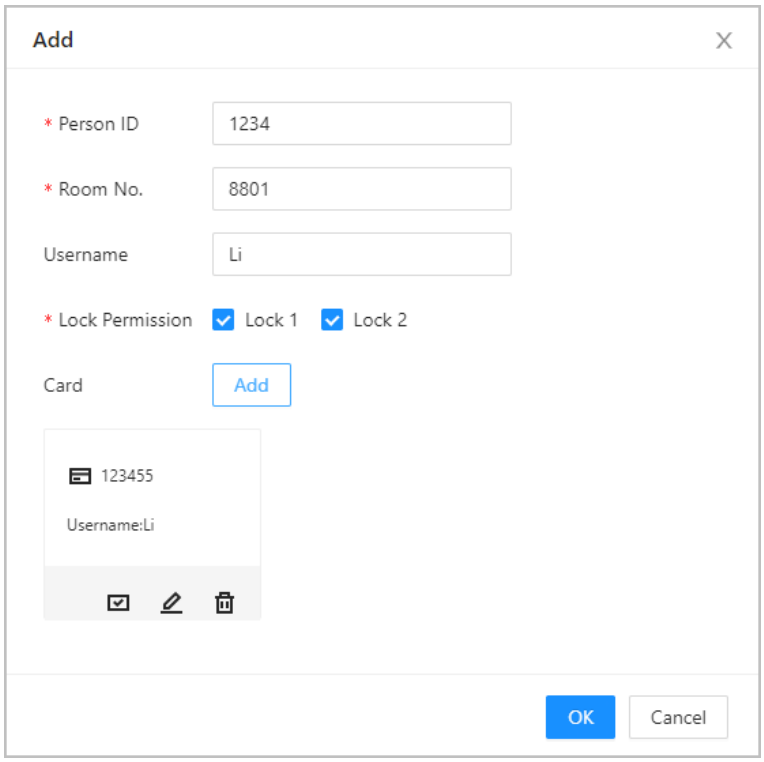
   Then the window goes back to the **Add**, with a card being added.

◇ : Report lost card. After clicking the icon, it becomes .

◇ : Edit the card information.

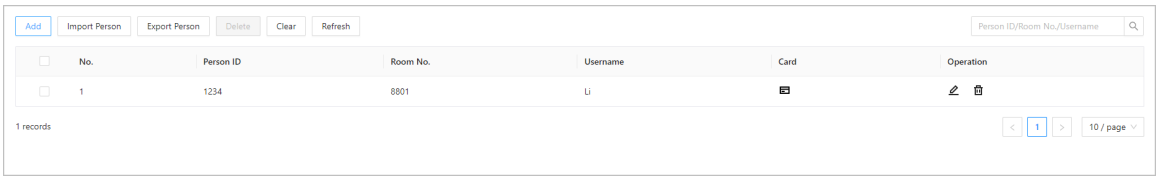
◇ : Delete the added card.

Figure 9-5 Card issued



5. Click **OK**.

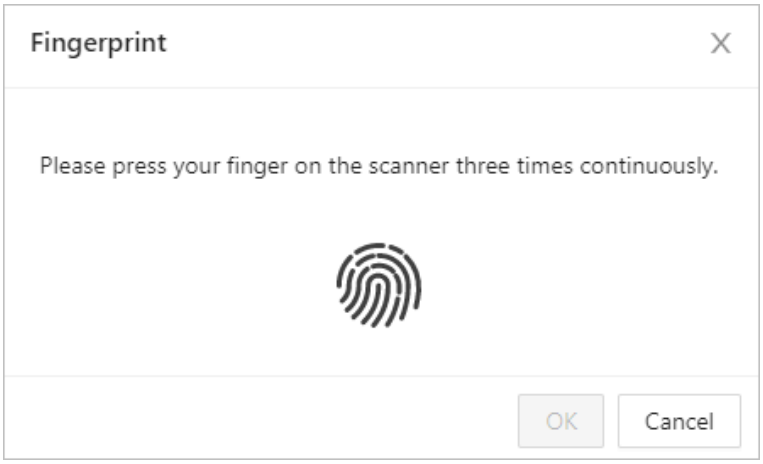
Figure 9-6 Card added successfully



- VTO that has fingerprint function or module:

1. Enter the room ID, room number, username and select the lock permission.
2. Click **Add** next to **Fingerprint**, and then press your finger according to the prompt.

Figure 9-7 Issue card



3. Click **OK**.

   Then the window goes back to the **Add**, with a fingerprint being added. You can edit the name of the fingerprint.
4. Click **OK**.

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.

10 Network Settings

This chapter introduces how to configure the network parameters.

10.1 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 10-1 TCP/IP

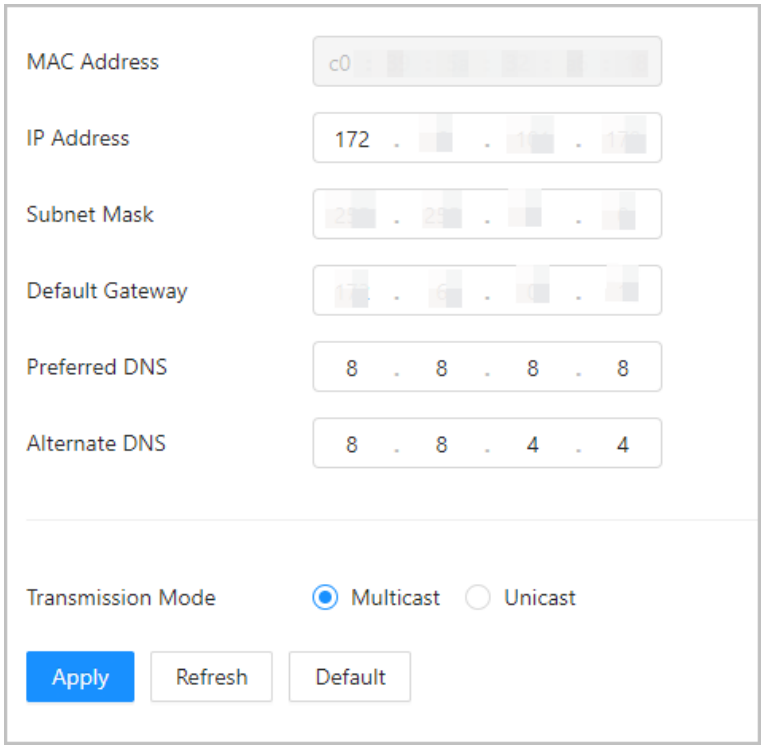


Table 10-1 Parameter description

Parameter	Description
IP Address	Your planned IP address for the VTO.
Preferred DNS	It is 8.8.8.8 by default.
Alternate DNS	It is 8.8.4.4 by default.
Transmission Mode	• Multicast. • Unicast. Unicast is preferred when the switch does not support multicast function, or when the network connection is not good.

10.2 Port

Figure 10-2 Port

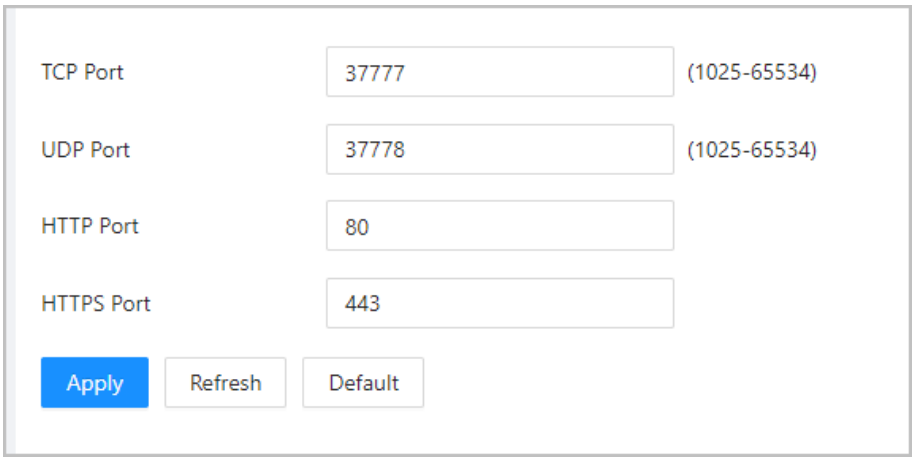


Table 10-2 Parameter description

Parameter	Description
HTTP Port	You can now enter http://VTO IP address: HTTPS 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.

10.3 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

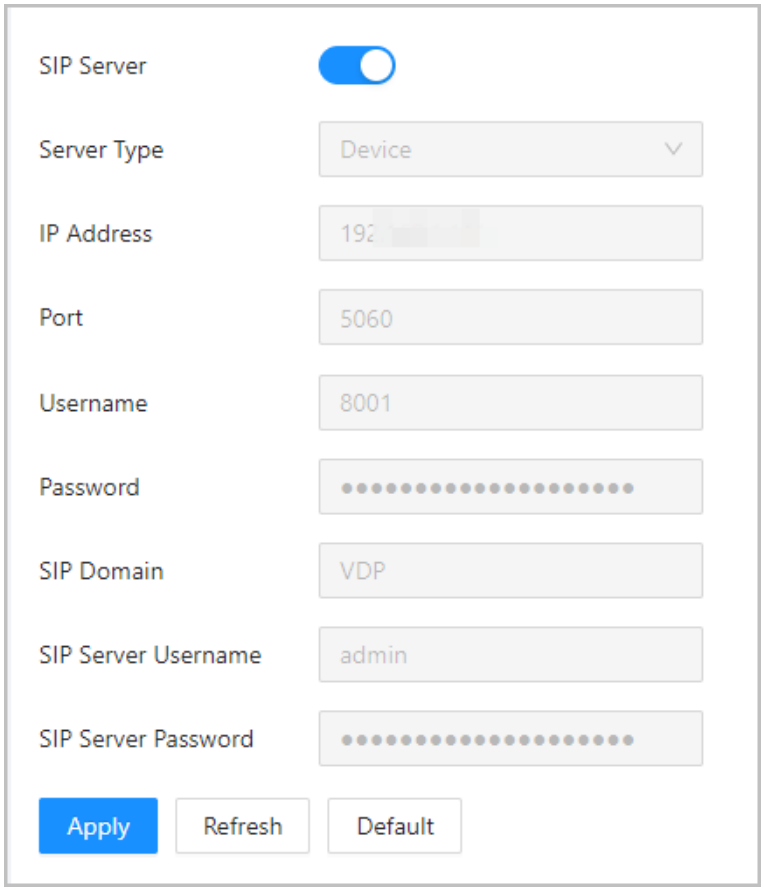
Step 1 Select **Network Settings** > **SIP Server**.

Step 2 Select a server type.

- The VTO you have logged in as the SIP server: Select the SIP type as **Device**, and configure the parameters for the VTO, and then click next to **SIP Server**.

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

Figure 10-3 Current VTO as SIP server



- If another VTO works as the SIP server: Select the SIP type as **Device**, and 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 **SIP Server**. Otherwise, the connection would fail.

Figure 10-4 Another VTO as SIP server

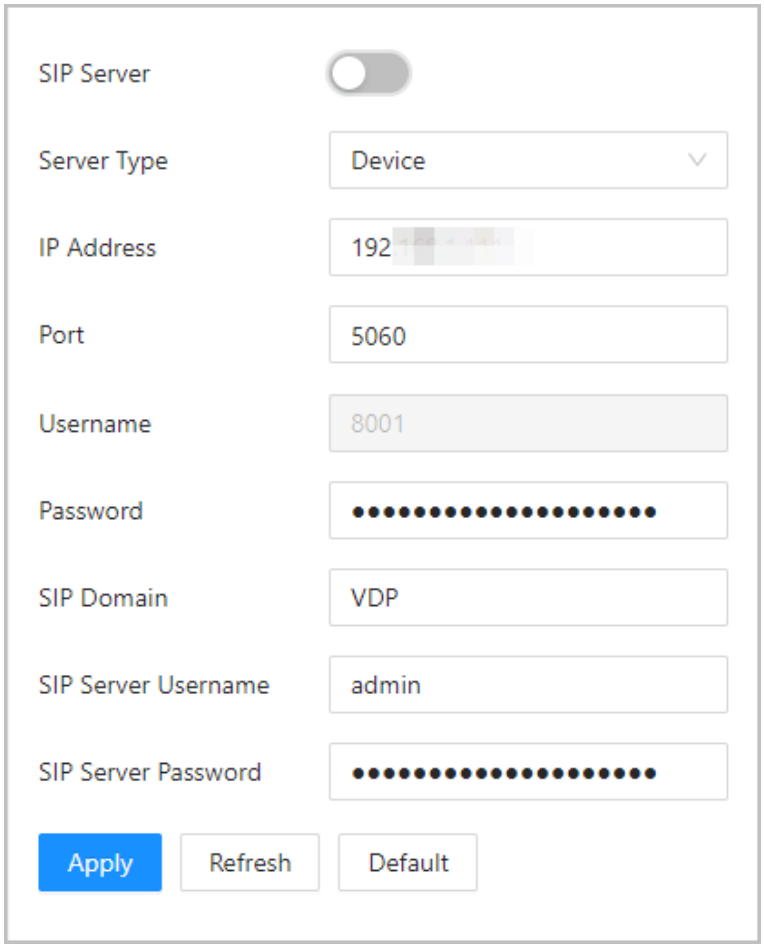


Table 10-3 SIP server configuration (VTO as the SIP server)

Parameter	Description
IP Address	Planned IP address of the VTO.
Port	5060 by default.
Username	Leave it as default.
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 **Server Type** as **Private SIP Server**, and then configure the parameters.

Figure 10-5 Private SIP server

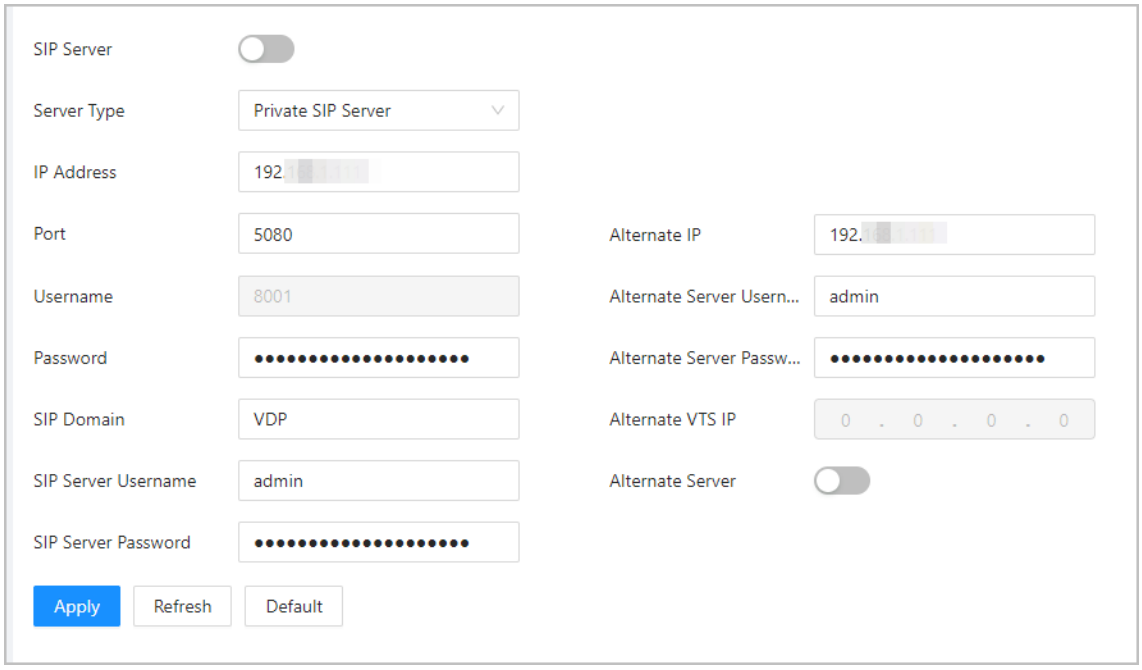


Table 10-4 SIP server description (platform as the SIP server)

Parameter	Description
IP Address	IP address of the SIP server.
Port	5080 by default when the platform works as the SIP server.
Username/Password	Leave it as default.
SIP Domain	
SIP Server Username/ Password	Used to log in to the SIP server.
Alternate IP	The alternate server will be used as the SIP server when Express/DSS stops responding. We recommend you configure the alternate IP address. ◇ If you enable **Alternate Server**, the current VTO you have logged in serves as the alternate server. ◇ If you want another VTO serve as the alternate server, you need to enter the IP address of that VTO in the **Alternate IP** textbox. Do not enable **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.
Alternate Server	Enable it so that you can configure the Alternate VTS IP.

Step 3 Click **Apply**.

10.4 Second Confirmation Station Cascading

It applied to the situation when the second confirmation station cascades to the VTH.

Prerequisites

The software version of the VTH must be V4.7 and later.

Procedure

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

Step 2 Configure the second confirmation station information in **Local Device Config** > **Basic Settings**.

The device type should be set as **Second Confirmation Station**.

Step 3 Set **Server Type** as **Device**, and then configure the parameters.

In this cascading situation, the VTH works as the SIP server.

Figure 10-6 SIP server configuration (VTH as the SIP server)

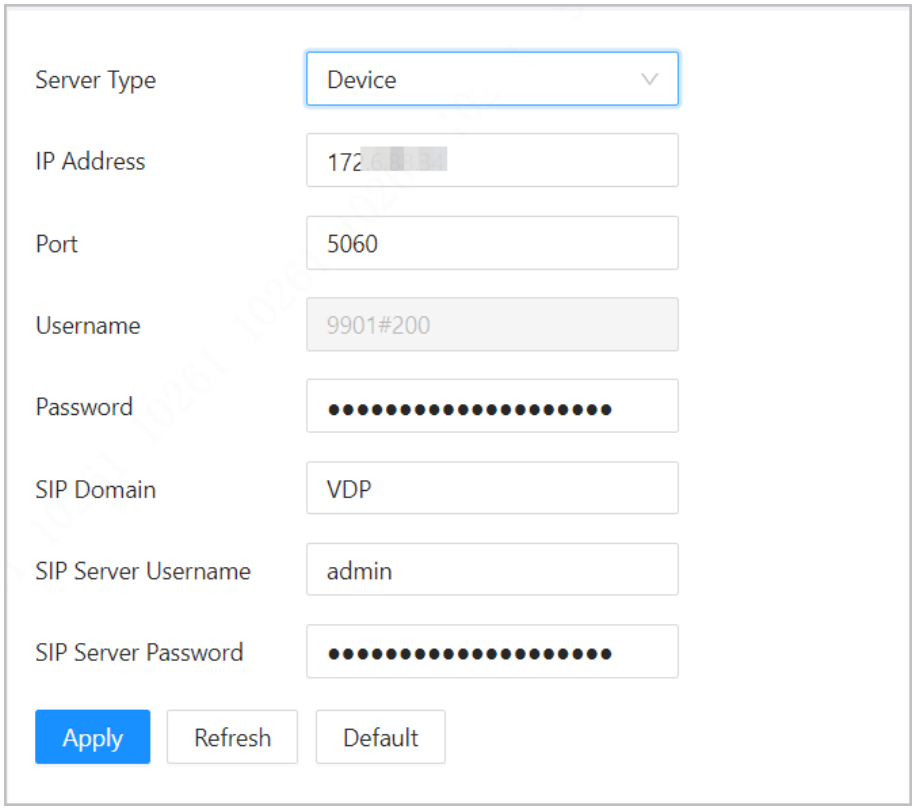


Table 10-5 SIP server configuration description (VTH as the SIP server)

Parameter	Description
IP Address	Your planned IP address of the VTH.
Port	5060 by default.
Username	Leave it as default.
Password	
SIP Domain	

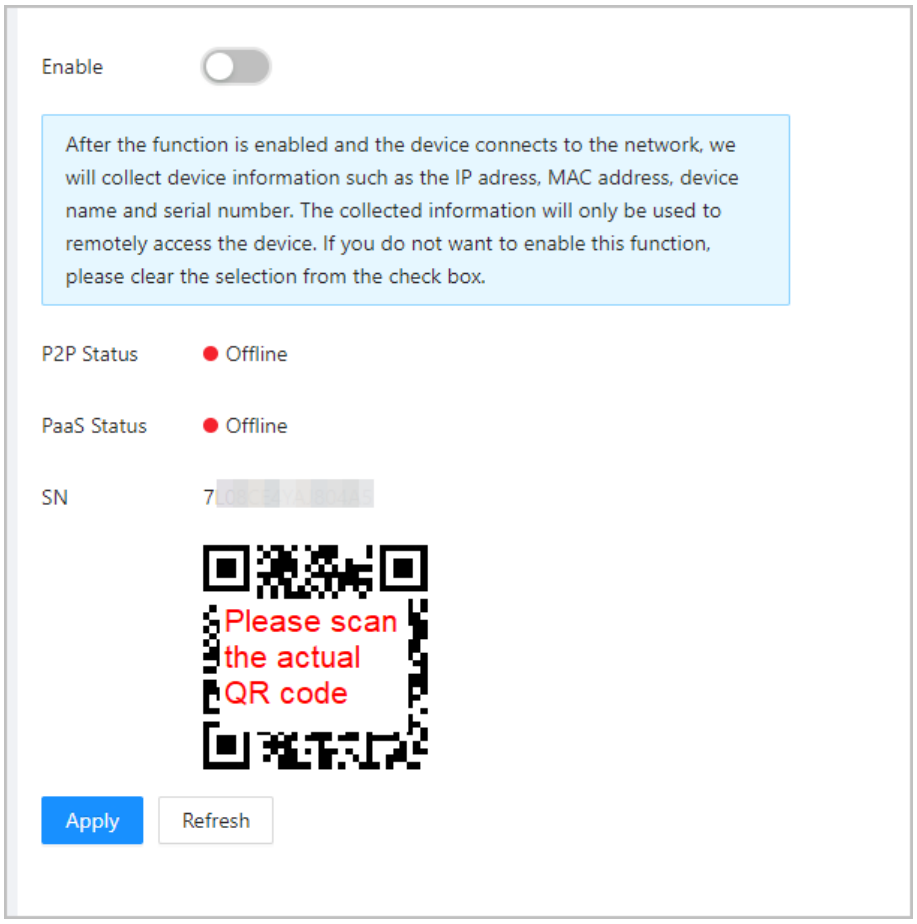
Parameter	Description
SIP Server Username	Username and password used to log into the VTH that serves as the SIP server.
SIP Server Password	

Step 4 Click **Apply**.

10.5 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.

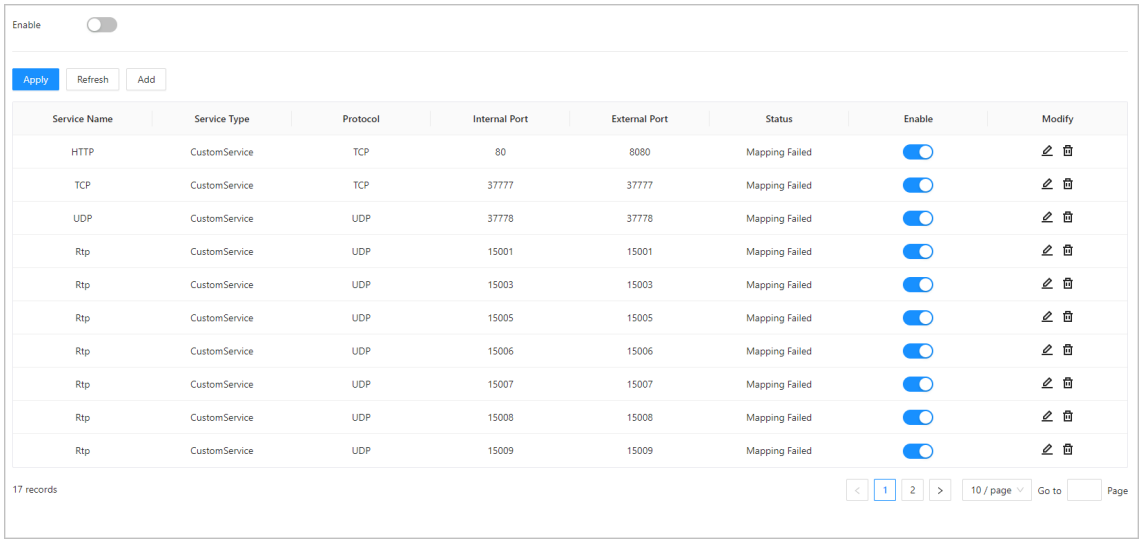
Figure 10-7 Cloud service



10.6 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 10-8 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.

10.6.1 Enabling UPnP Services

Procedure

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

Step 2 Enable the services listed.

Step 3 Select **Enable**.

Step 4 Click **Save**.

10.6.2 Adding UPnP Services

Procedure

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

Step 2 Click **Add**.

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

Figure 10-9 Add a UPnP service

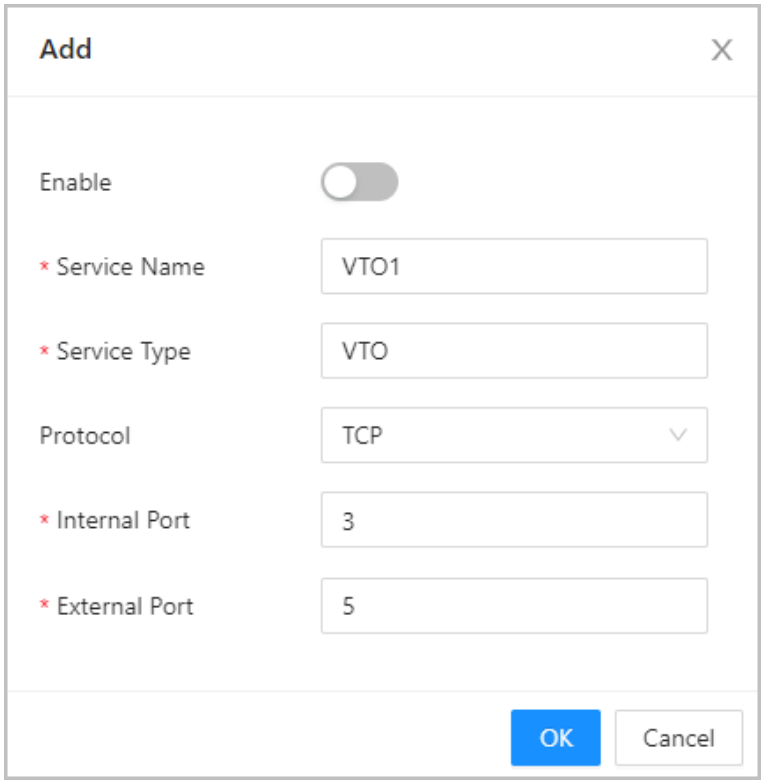


Table 10-6 Parameter description

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.

10.7 Wi-Fi

If the VTO supports Wi-Fi function, then configure the parameters here.

Procedure

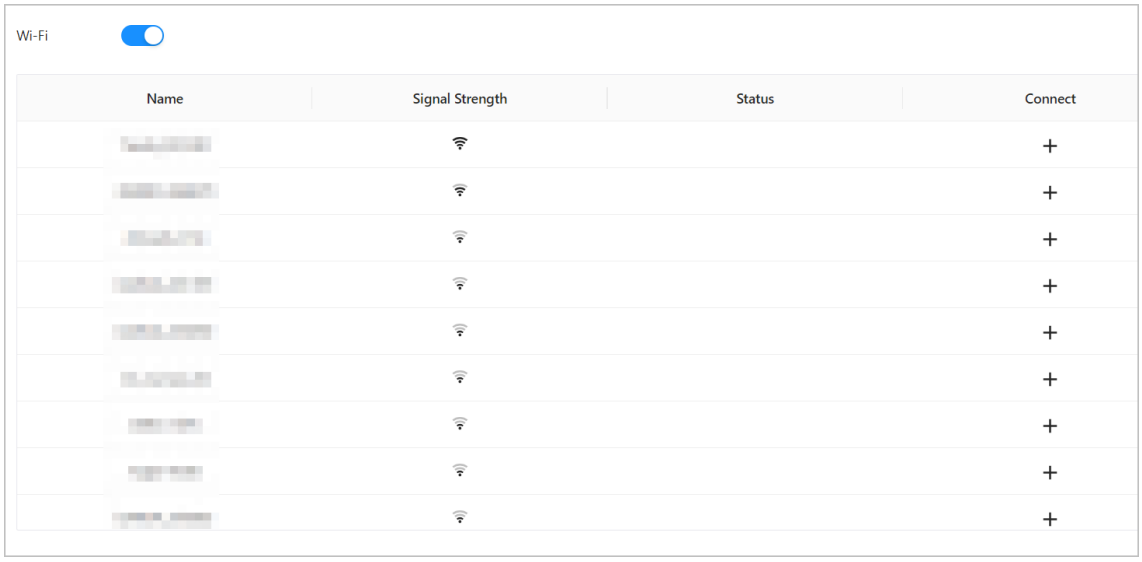
Step 1 Log in to the webpage of the VTO.

Step 2 Select **Network Settings** > **Wi-Fi**.

Step 3 Set the **Wi-Fi** status as **On**.

All the networks available are displayed.

Figure 10-10 Wi-Fi



Step 4 Click **+** of the Wi-Fi you chose, enter the password of it, and then connect to the network.

10.8 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 10-11 Basic services

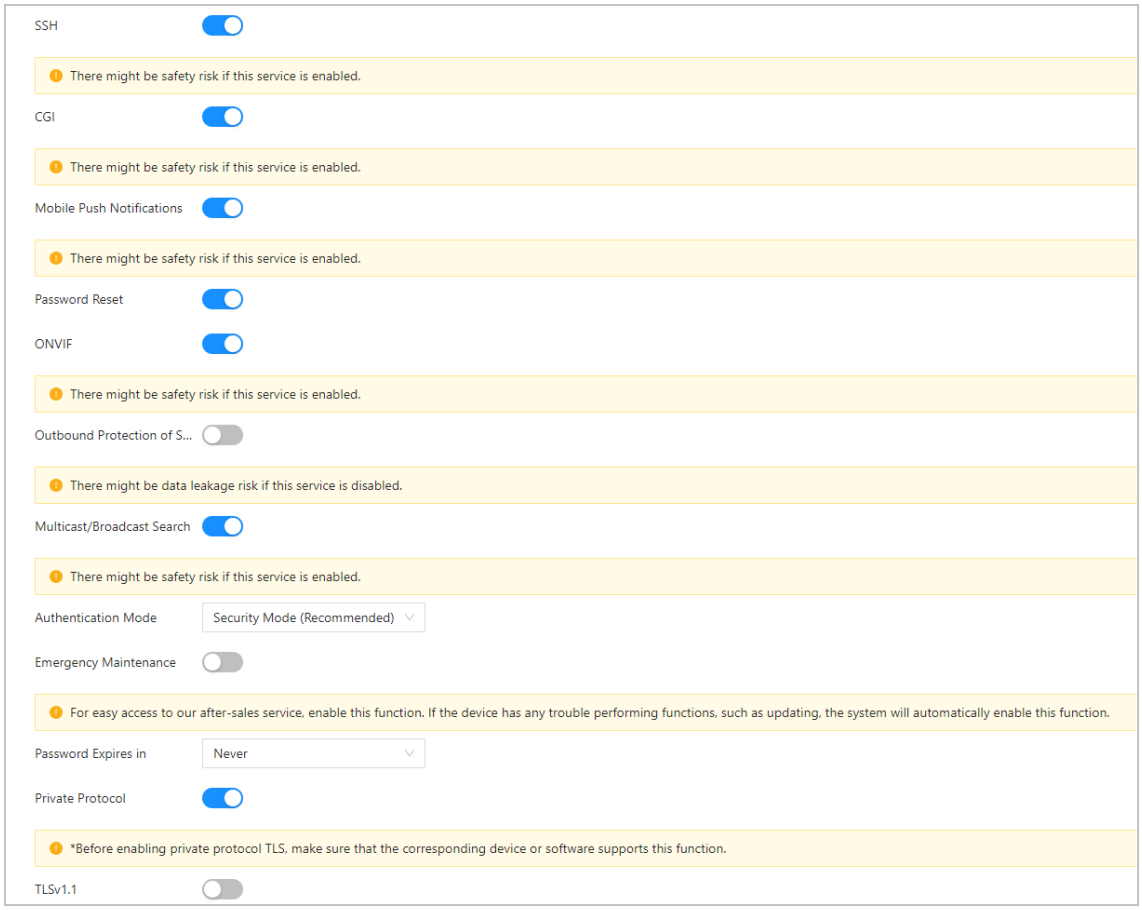


Table 10-7 Security parameter description

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.
Password Reset	If turned off, you will not be able to reset password.

Parameter	Description
ONVIF	Allow third-party to pull video stream of the VTO through the ONVIF protocol. We recommend turning it off. Otherwise, the VTO might be exposed to security risks and data leakage.
Outbound Service Information Protection	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.

Step 3 Click **Apply**.

11 Log Management

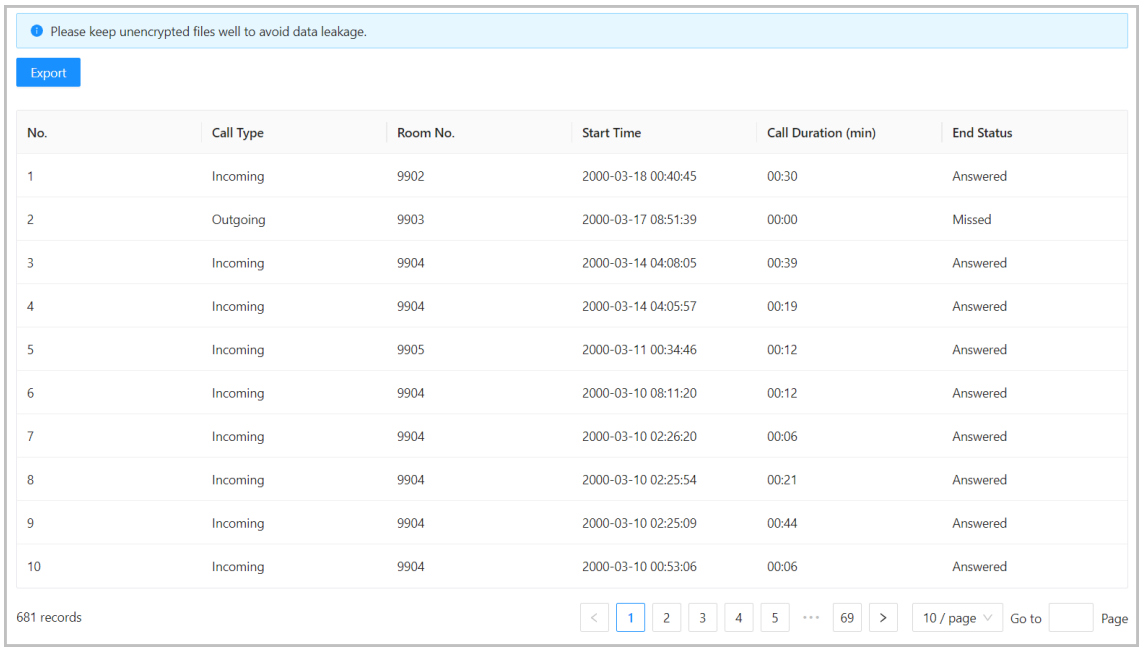
Select **Log**. You can search for different logs, and export them to your local computer.

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

11.1 Call History

Select **Log** > **Call History**.

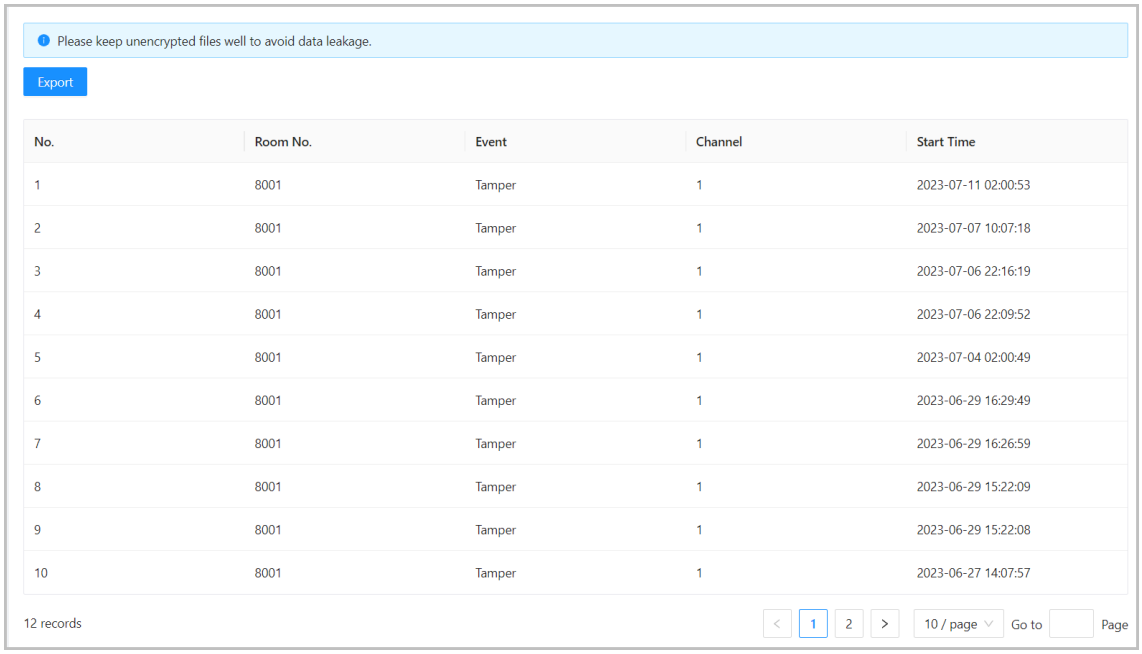
Figure 11-1 Call history



11.2 Alarm Logs

Select **Log** > **Alarm Logs**.

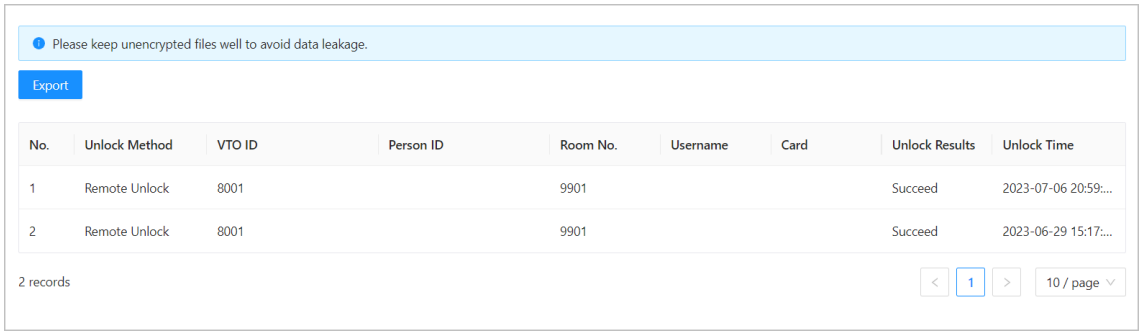
Figure 11-2 Alarm



11.3 Unlock Records

Select **Log** > **Unlock Records**.

Figure 11-3 Unlock

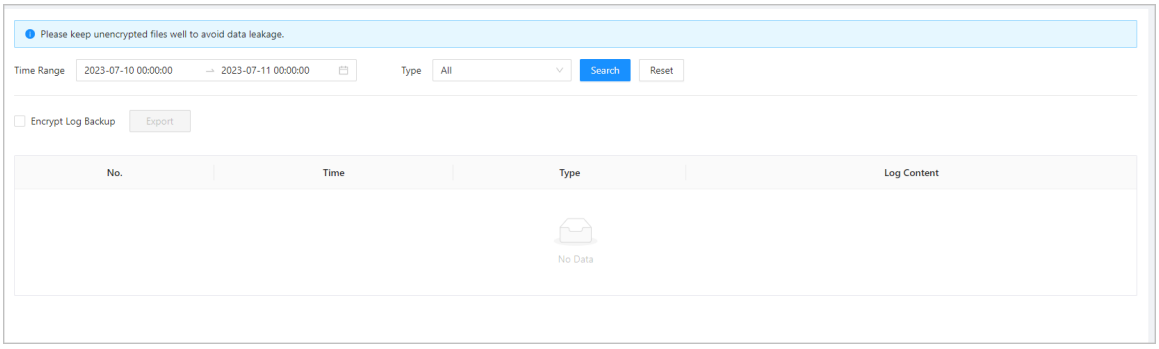


11.4 Log

Select **Log** > **Log**.

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

Figure 11-4 Log

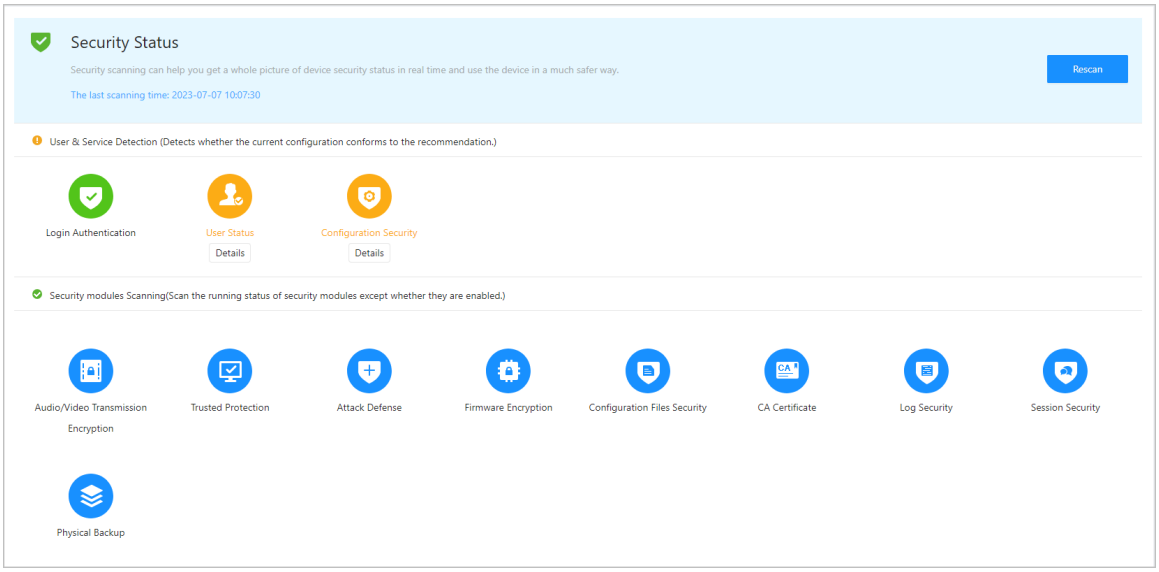


12 Security Management

12.1 Security Status

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

Figure 12-1 Security status



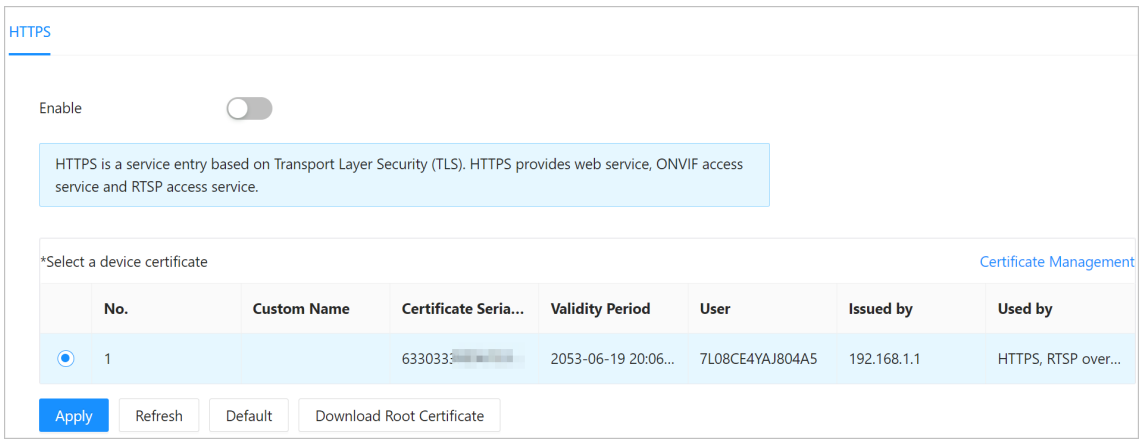
12.2 System Service

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

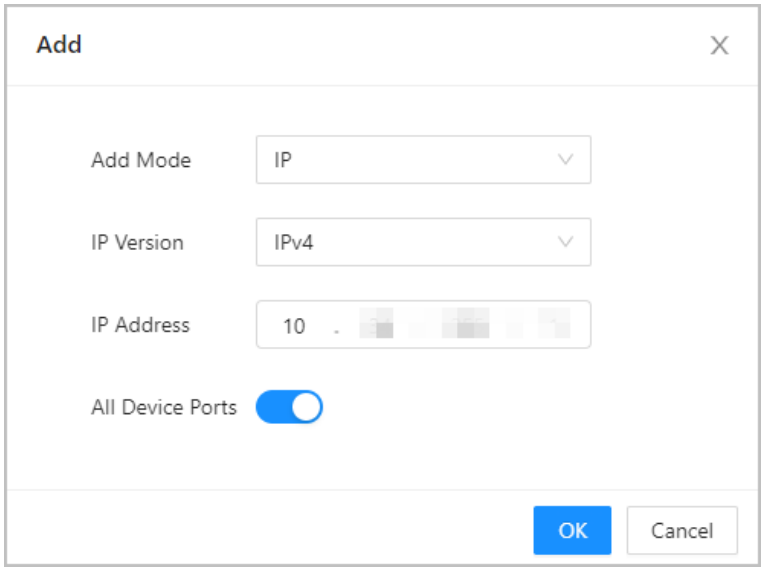
Step 1 On the home page, click , and then select **Attack Defense** > **Firewall**.

Step 2 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 3 Click **Add** to add the IP address for allowlist or blocklist.

Figure 12-3 Add

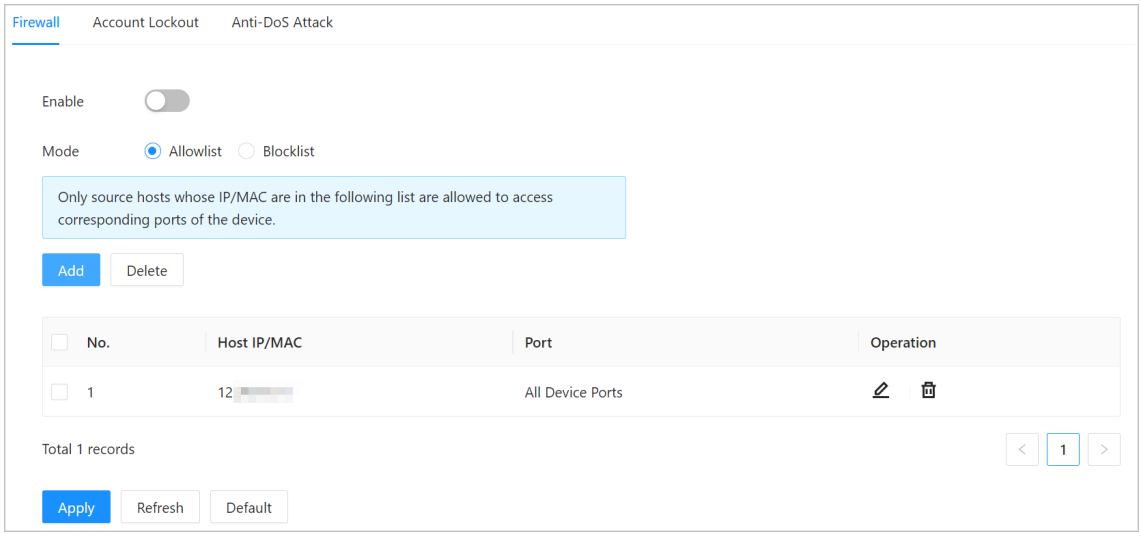


Step 4 Click **OK**.

Step 5 Click next to **Enable**.

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

Figure 12-4 Apply



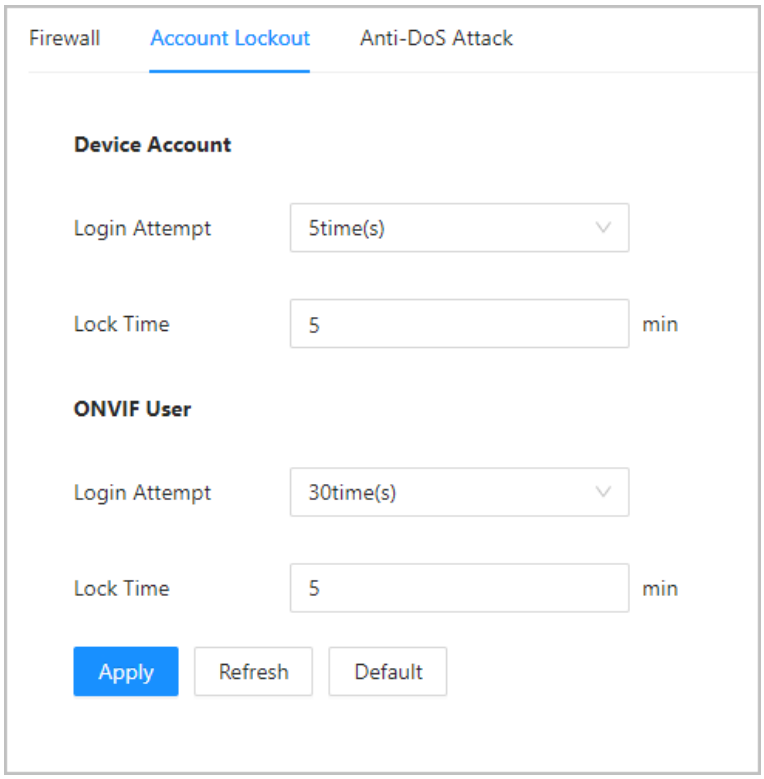
12.3.2 Account Lockout

Procedure

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

Step 2 Configure the login attempts and lock time.

Figure 12-5 Account lockout



Step 3 Click **Apply**.

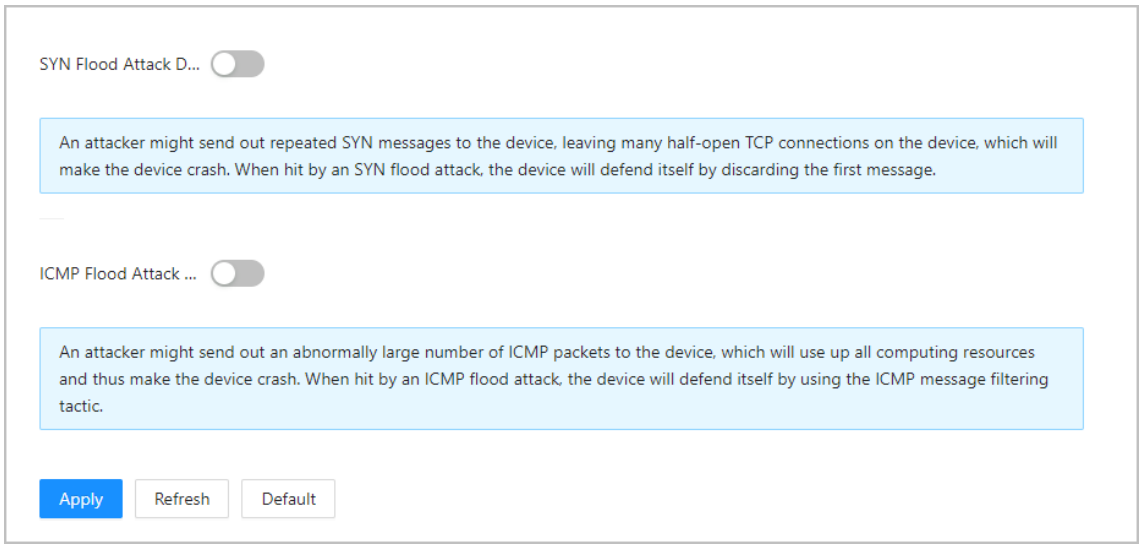
12.3.3 Anti-DoS Attack

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**.

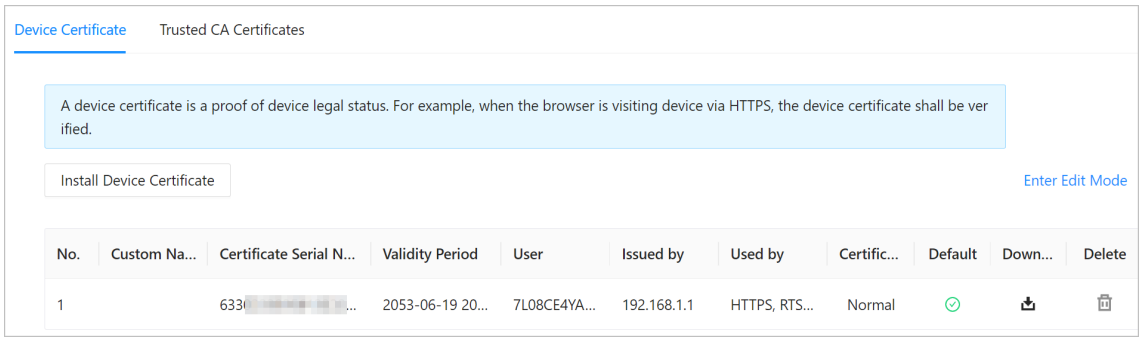
12.4 CA Certificate

Procedure

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

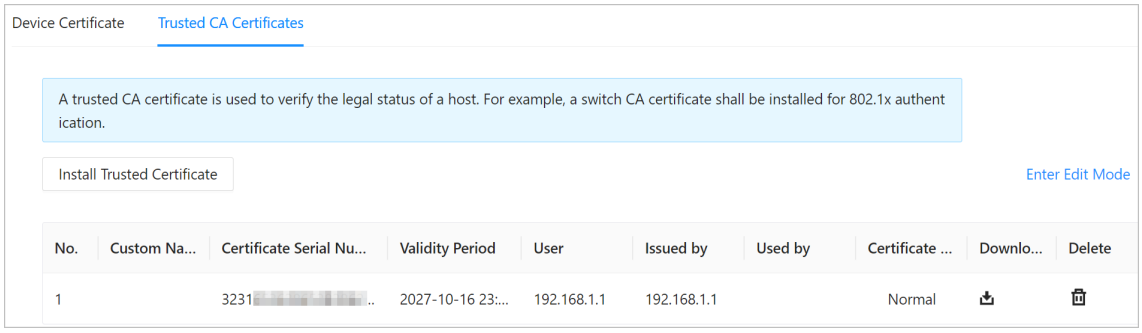
- Device Certificate

Figure 12-7 Device Certificate



- Trusted CA Certificates

Figure 12-8 Trusted CA Certificates



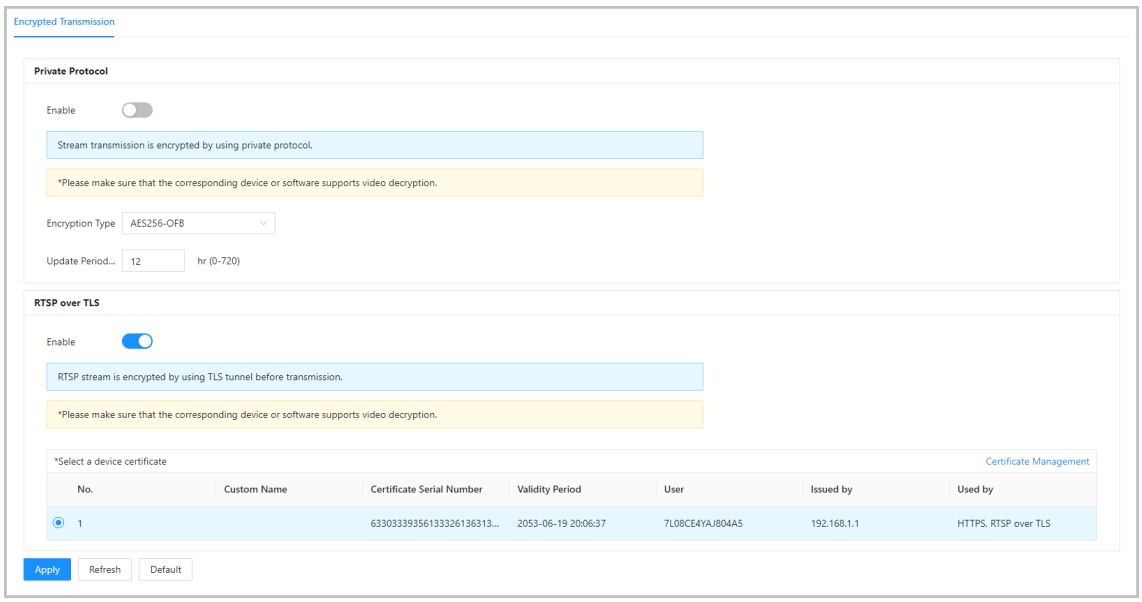
12.5 Video Encryption

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**.

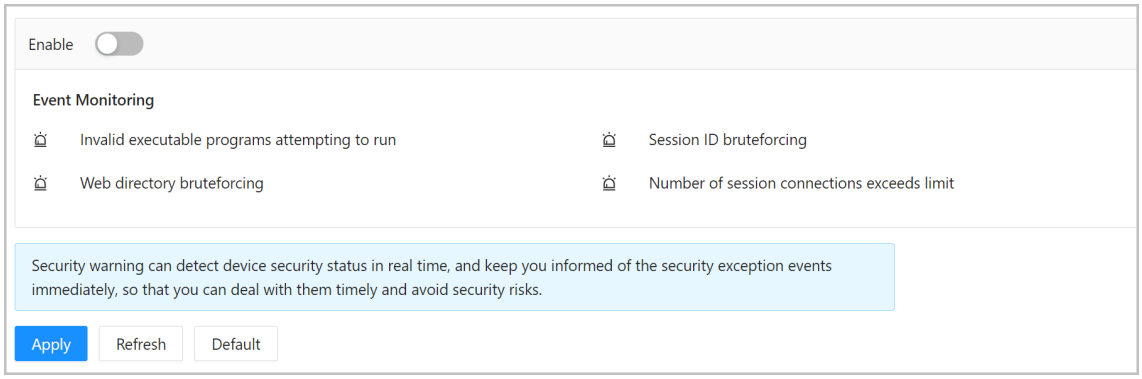
12.6 Security Warning

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



13 Button Model Configuration

The button model can be connected to the VTH to work as an alarm input button. Press the button on the front panel of the model, and then the VTH receives an alarm signal.

13.1 Cable Connection

Connect the KEY port of the button model to any one of the alarm input ports of the indoor monitor (VTH) with a cable thread.

Figure 13-1 Button model

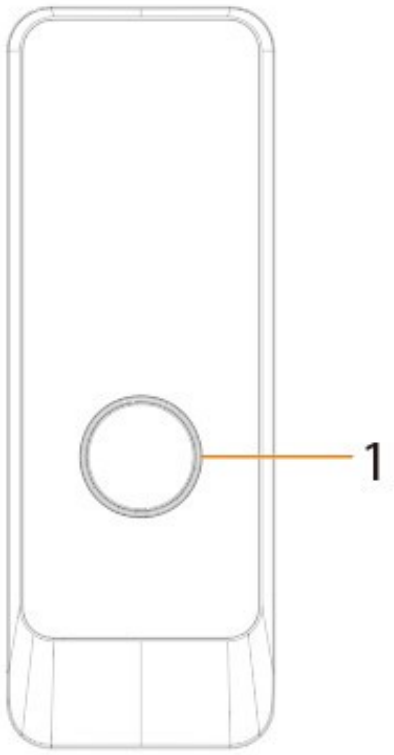
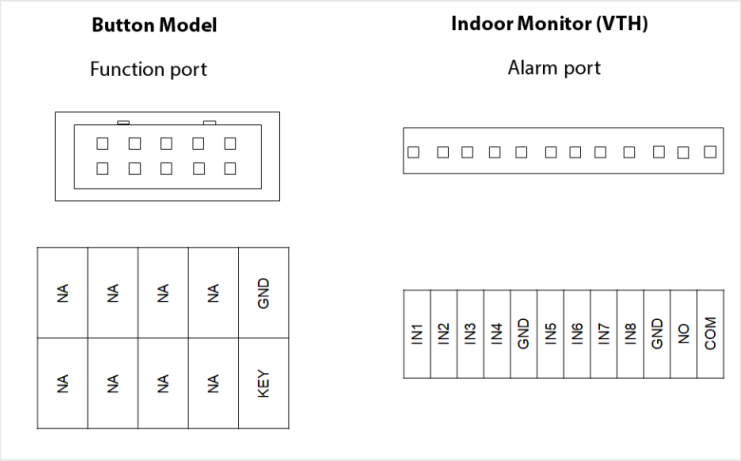


Table 13-1 Component

No.	Name	Function
1	Press button	The button model can be connected to the VTH. Press the button on the model and the VTH receives an alarm signal.

Figure 13-2 Cable connection



13.2 VTH Configuration

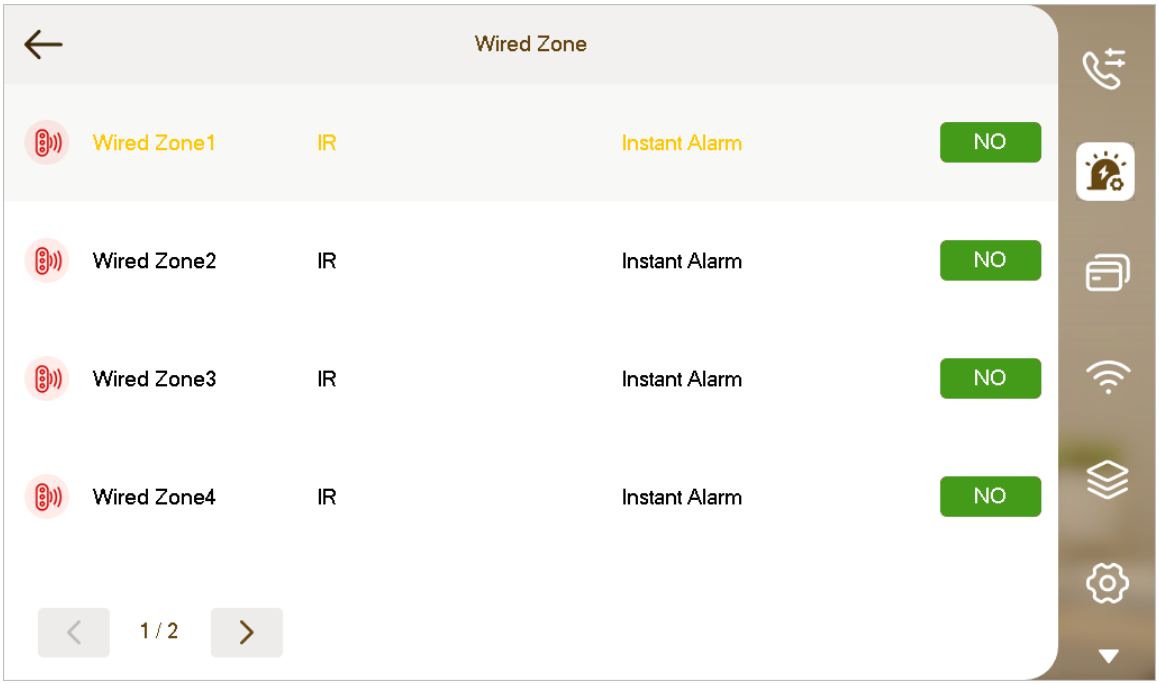
After completing cable connection, you need to set the **wired zone type** as **Doorbell** on the VTH to receive alarm signals once you press the button model.

Procedure

Step 1 Power on the VTH.

Step 2 Select **Setting** > **Alarm** > **Wired Zone** on the VTH.

Figure 13-3 Wired zone setting



Step 3 Set the **Type** as **Doorbell**, and configure the rest of the parameters.

Table 13-2 Parameter description

Parameter	Description
Area	The number cannot be modified.
NO/NC	Select NO (normally open) or NC (normally closed) according to detector type. It must be the same as detector type.
Type	Select corresponding type according to detector type.
Status	• **Instant Alarm** : After armed, if an alarm is triggered, the device produces siren at once and enters alarm status. • **Delay Alarm** : After armed, if an alarm is triggered, the device enters alarm status after a specified time, during which you can disarm and cancel the alarm. • **Bypass** : Alarm will not be triggered in the area. After disarmed, this area will restore to normal working status. • **Remove** : The area is invalid during arm/disarm. • **24 Hour** : Alarm will be triggered all the time in the area regardless of arm or disarm. A zone in **Remove** status cannot be bypassed.
Enter Delay	After entering delay, when armed area triggers an alarm, entering armed area from non-armed area within the delay time period will not lead to linkage alarm. Linkage alarm will be produced if delay time comes to an end and it is not disarmed.
Exit Delay	After arm, **Delay Alarm** area will enter arm status at the end of **Exit Delay**. If multiple areas set the exit delay, screen prompt will conform to maximum delay time.

Delay is only valid to the areas of **Delay Alarm**.

Appendix 1 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.