

Modular Door Station

User Manual



V1.0.2





Foreword

General

This manual introduces the installation, functions and operations of the modular door station device (hereinafter referred to as "the VTO"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Date
V1.0.2	Updated basic settings.	December 2025
V1.0.1	Updated RS-485.	August 2025
V1.0.0	First release.	June 2025

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user manual, use our CD-ROM, scan the QR code or visit

our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguard and Warnings

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

Installation Requirements



WARNING

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



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

Operation Requirements



DANGER

Battery Pack Precautions

Preventive measures (including but not limited to):

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

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



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

Table of Contents

Foreword.....	I
Important Safeguard and Warnings.....	III
1 Structure.....	1
1.1 Front Panel.....	1
1.2 Rear Panel.....	2
1.3 Indicator Module.....	3
1.4 Button Module.....	4
1.5 Keyboard Module (with Braille).....	8
1.6 Card Module.....	9
1.7 Fingerprint Module.....	9
1.8 Display Module.....	10
1.9 Information Module.....	11
1.10 Blank Module.....	12
1.11 Cascade Connection.....	12
2 Initializing the VTO.....	13
2.1 Webpage.....	13
2.2 DoLynk Care.....	13
3 Logging and Resetting Password.....	15
3.1 Logging	15
3.2 Resetting Password.....	15
4 Home Page.....	17
5 Setup Wizard.....	18
5.1 Setting as SIP Server.....	18
5.2 Not Setting as SIP Server.....	19
6 Local Device Configuration.....	20
6.1 Basic Settings.....	20
6.2 Access Control.....	25
6.2.1 Configuration.....	25
6.2.2 Extension Function.....	27
6.3 Light Control.....	31
6.4 Layout (Multiple Modules).....	31
6.5 Adding IPC.....	34
6.5.1 Adding IPC One by One.....	35
6.5.2 Exporting IPC Information in Batches.....	37
6.5.3 Importing IPC Information in Batches.....	37
6.6 Card Settings.....	37
7 Device Setting.....	39

7.1 VTO Management.....	39
7.2 VTH Management.....	40
7.3 VTS Management.....	43
8 Person Management.....	44
9 Network Settings.....	47
9.1 TCP/IP.....	47
9.2 Port.....	48
9.3 SIP Server.....	49
9.4 Cloud Service.....	53
9.5 UPnP.....	53
9.5.1 Enabling UPnP Services.....	54
9.5.2 Adding UPnP Services.....	54
9.6 Basic Services.....	56
9.7 Auto Registration.....	57
10 System.....	59
10.1 Alarm.....	59
10.2 Video.....	60
10.3 Audio.....	63
10.4 Time.....	64
10.5 ONVIF User.....	66
11 Maintenance Center.....	67
11.1 One-Click Diagnosis.....	67
11.2 System Information.....	67
11.2.1 Version Information.....	67
11.2.2 Legal Information.....	68
11.3 Data Capacity.....	68
11.4 Log Management.....	68
11.4.1 Call History.....	68
11.4.2 Alarm Logs.....	69
11.4.3 Unlock Records.....	69
11.4.4 Log.....	70
11.5 Maintenance Management.....	70
11.5.1 Config.....	70
11.5.2 Maintenance.....	71
11.6 Update.....	71
11.7 Advanced Maintenance.....	72
12 Security Management.....	74
12.1 Security Status.....	74
12.2 System Service.....	74
12.3 Attack Defense.....	75

12.3.1 Firewall.....	75
12.3.2 Account Lockout.....	76
12.3.3 Anti-DoS Attack.....	77
12.4 CA Certificate.....	77
12.5 Video Encryption.....	78
12.6 Security Warning.....	78
12.7 Security Authentication.....	79
Appendix 1 Security Recommendation.....	80

1 Structure

1.1 Front Panel

Figure 1-1 Front panel

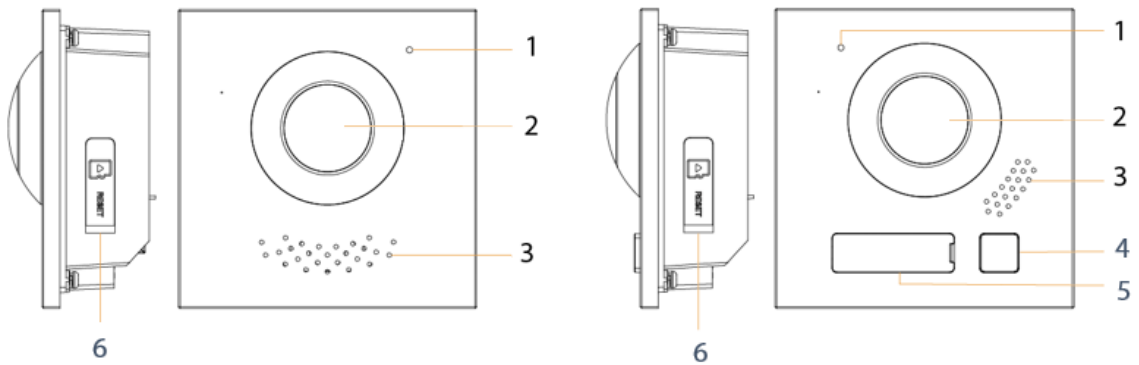


Table 1-1 Front panel description

No.	Name	Description
1	Microphone	Audio input.
2	Camera	Capture images or record videos for the VTO.
3	Speaker	Audio output.
4	Call button	Call button.
5	Nameplate	Displays the custom information.
6	Card slot and reset button	<ul style="list-style-type: none">● Insert SD card so that data information such as images and videos can be stored.● Press and hold the button for several seconds to reset to factory settings.

1.2 Rear Panel

Figure 1-2 Rear panel

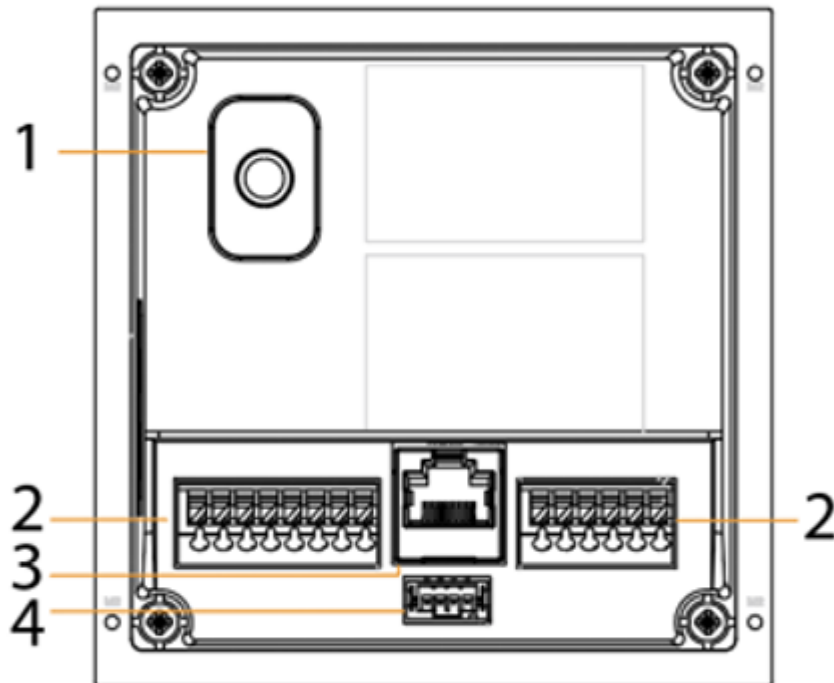


Table 1-2 Rear panel description

No.	Name	Function
1	Tamper button	<ul style="list-style-type: none">After the installed device is removed from the wall or other places, the device beeps and the alarm record will be generated.Within 5 minutes after the device is powered on, if you press the tamper button for 5 times in 8 seconds, the device beeps and deletes the account information. The alarm record will be generated.
2	Multi-function ports	Alarm port, door detector port, 485 port, power port and more.
3	Network port	Connect to the network.
4	Cascade connection port	Connect to other modules.

Figure 1-3 Multi-function ports

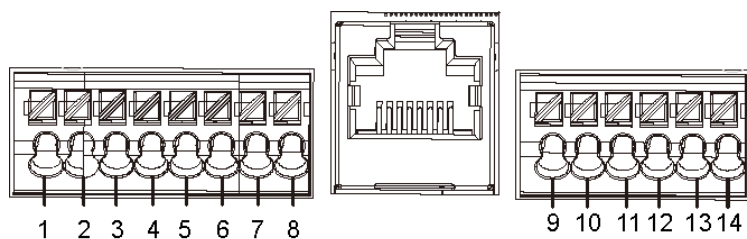


Table 1-3 Port description

No.	Description	No.	Description
1	GND	8	<ul style="list-style-type: none"> • 2 wires-(GND) for a digital 2-wire camera module • GND for a full digital camera module
2	+12V_OUT	9	DOOR_BUTTON
3	RS-485_B	10	DOOR_FEEDBACK
4	RS-485_A	11	GND
5	ALARM_NO	12	DOOR_NC
6	ALARM_COM	13	DOOR_COM
7	<ul style="list-style-type: none"> • 2 wires+(48V) for a digital 2-wire camera module • 12 V_IN for a full digital camera module 	14	DOOR_NO

1.3 Indicator Module

Figure 1-4 Front panel

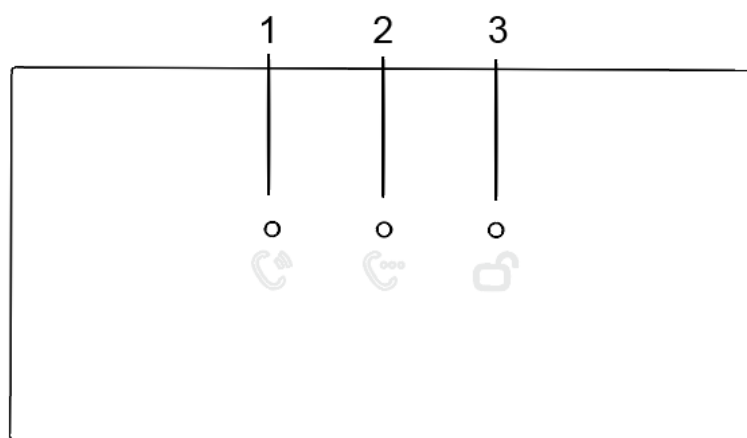


Table 1-4 Front panel description

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

Figure 1-5 Rear panel

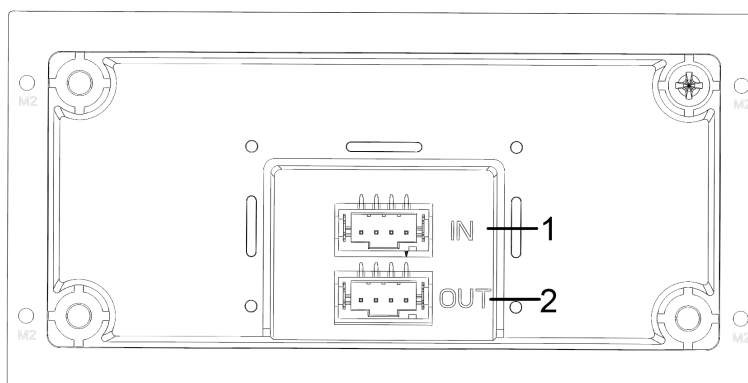


Table 1-5 Rear panel description

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

1.4 Button Module

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

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

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

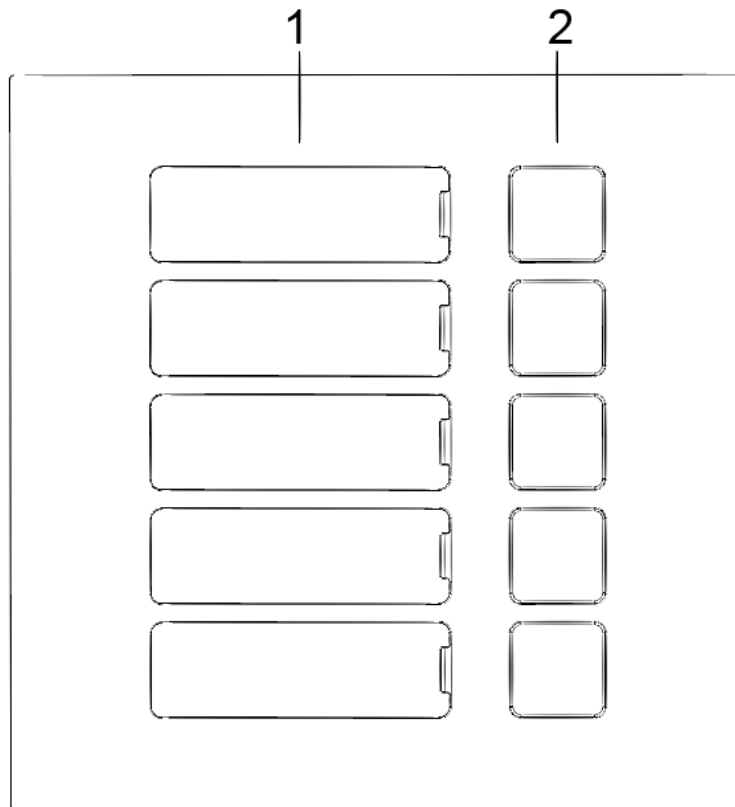


Table 1-6 Front panel description

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

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

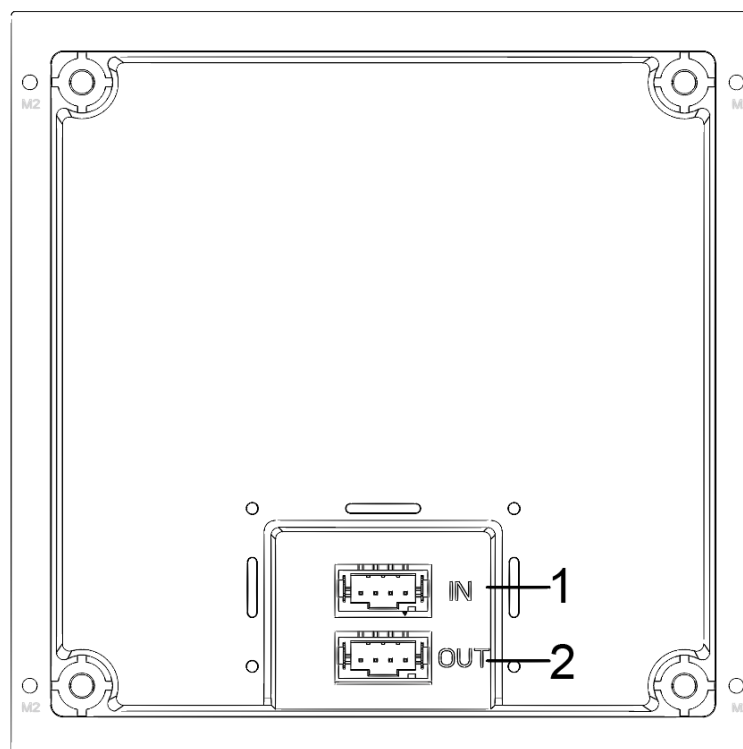


Table 1-7 Rear panel description

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

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

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

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

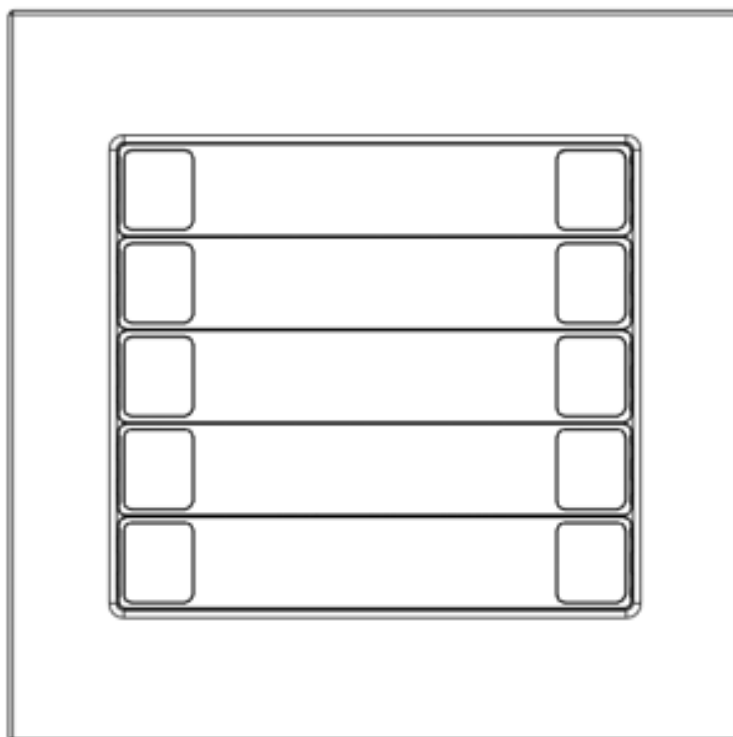


Figure 1-9 Rear panel of the ten-button module

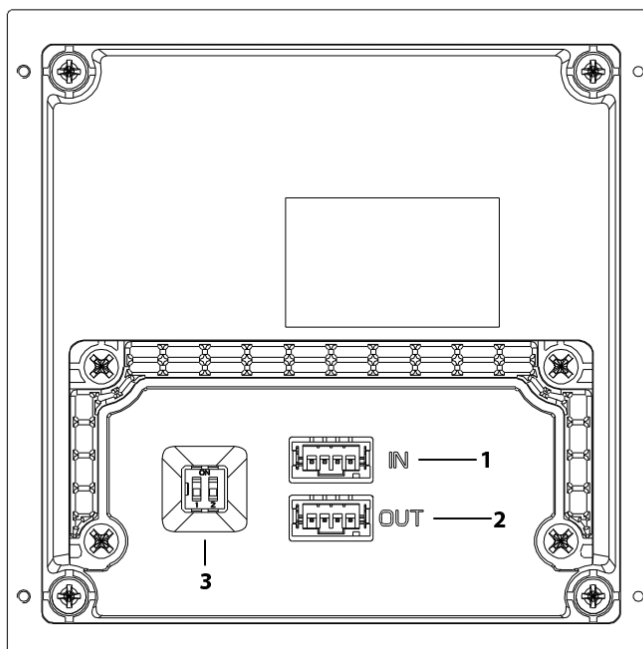



Table 1-8 Rear panel description

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

No.	Name	Description
3	Mode switch	<ul style="list-style-type: none"> Switch between single-column buttons and two-column buttons. The first DIP switch on the left turns to ON indicates the single-column buttons, while to 1 indicates the two-column buttons. It takes effect after the main VTO is restarted. Flipping up or down the second (from left to right) DIP switch has no effect. <p> If you want to change two-column buttons mode into single-column buttons mode, take the single-column buttons accessory from the package to replace it. For information about room number configurations on the WEB, see "6.4 Layout (Multiple Modules)".</p>

1.5 Keyboard Module (with Braille)



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

Figure 1-10 Keyboard module

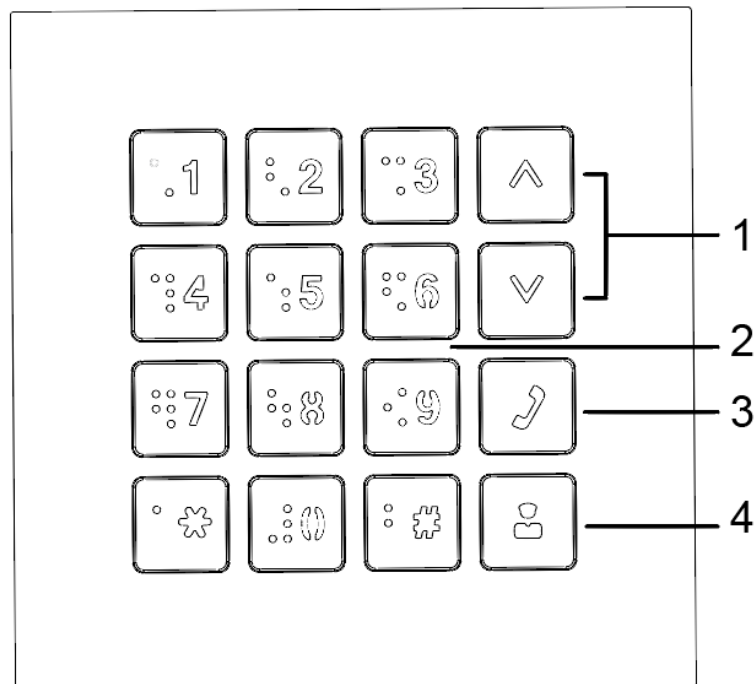


Table 1-9 Keyboard module description

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

1.6 Card Module

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



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

Figure 1-11 Card module



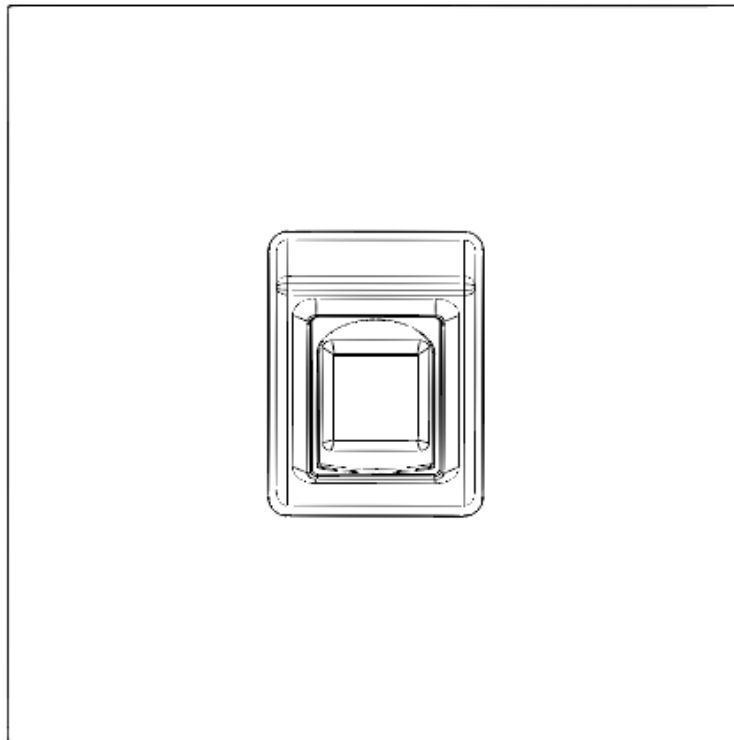
1.7 Fingerprint Module

Collects and verifies fingerprints.



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

Figure 1-12 Fingerprint module



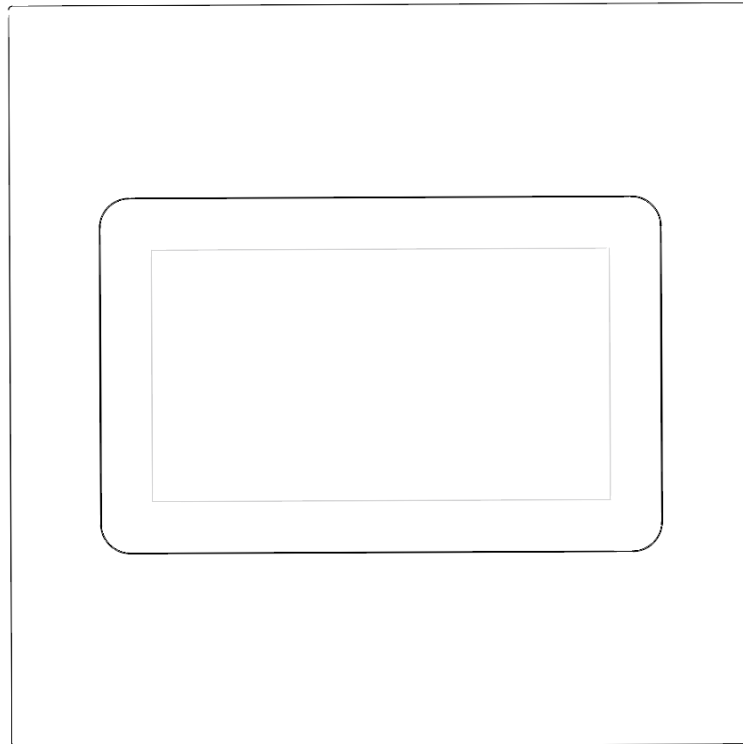
1.8 Display Module

Displays user information.



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

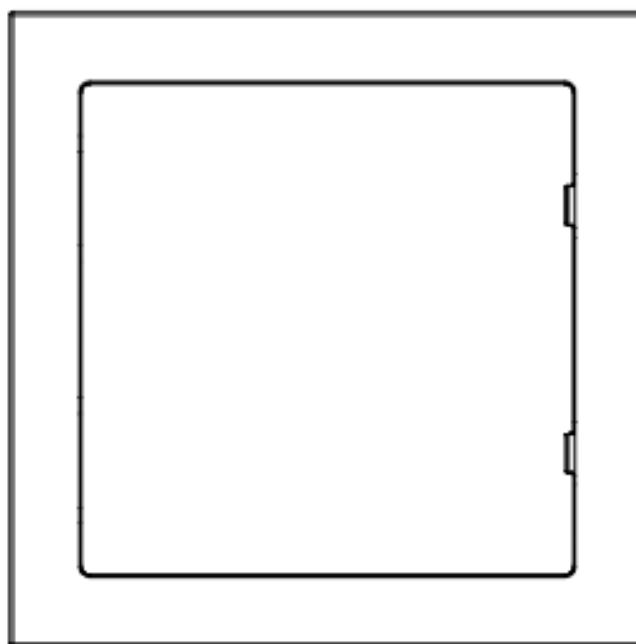
Figure 1-13 Display module



1.9 Information Module

Displays room number and guest message.

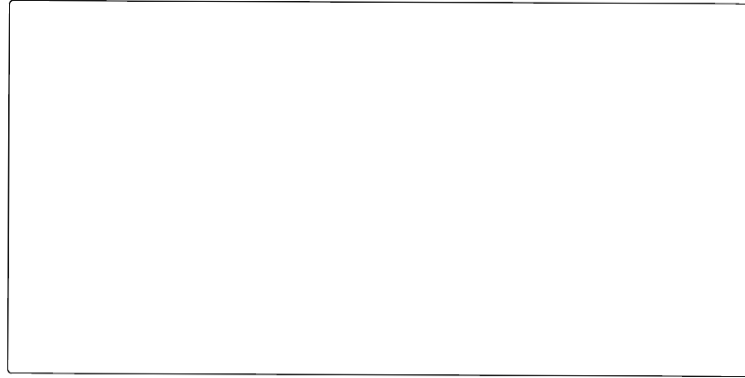
Figure 1-14 Information module



1.10 Blank Module

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

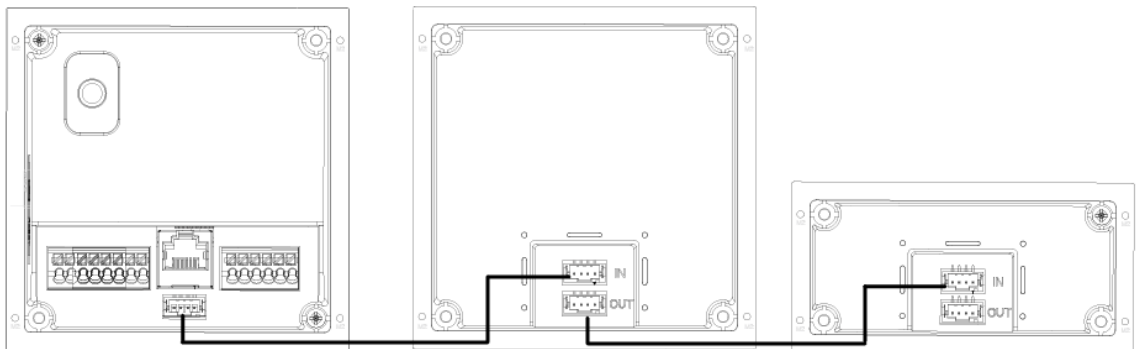
Figure 1-15 Blank module



1.11 Cascade Connection

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

Figure 1-16 Cascade connection example



2 Initializing the VTO

2.1 Webpage

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

Procedure

Step 1 Power on the VTO.

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



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

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



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

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

Step 5 Click **Next**.

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

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

2.2 DoLynk Care

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

Procedure

Step 1 On the home screen, tap .

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

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

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

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

Step 6 Connect to wireless or wired network.

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

Figure 2-1 Initialize the device

The screenshot shows a mobile application interface for adding a device. At the top, there is a header bar with a back arrow, the title 'Add Device', and the word 'Wireless'. Below the header, a progress indicator shows three steps: '1' (Network Config), '2' (Device Config), and '3' (Complete). The 'Device Config' step is currently active. The main content area contains the following elements: a text prompt 'Please enter an initial password of 8-32 letters, numbers or symbols', two password input fields labeled 'New pwd:' and 'Confirm pwd:', a password strength indicator showing three segments, and a warning message: 'The device will be connected to the platform. Please keep the device initialization password safe to prevent leakage.' At the bottom, there is a large red button labeled 'Initialize the device'.

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

3 Logging and Resetting Password

3.1 Logging

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

Procedure

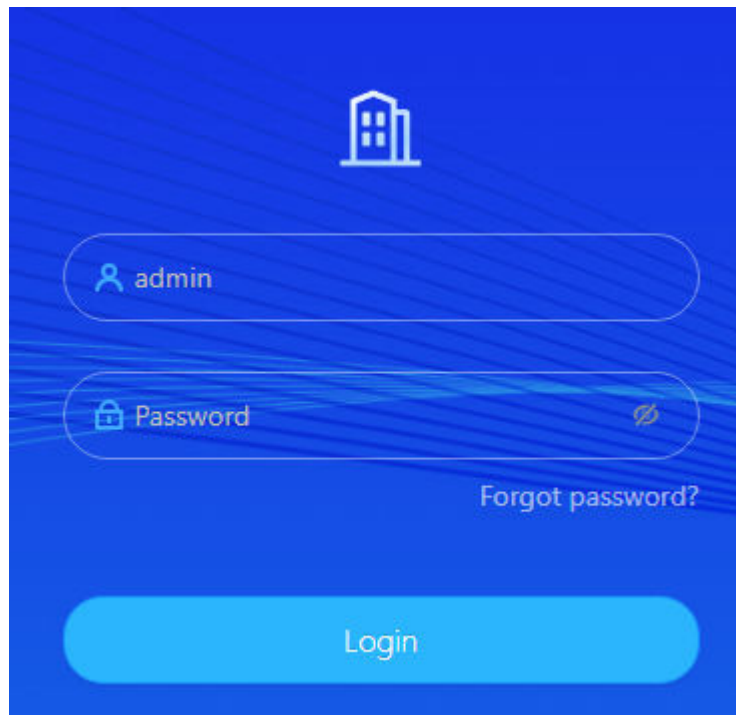
Step 1 Go to the IP address of the VTO in the browser.



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

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

Figure 3-1 Login



3.2 Resetting Password

Procedure

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

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

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

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



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

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

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

4 Home Page

Figure 4-1 Home page

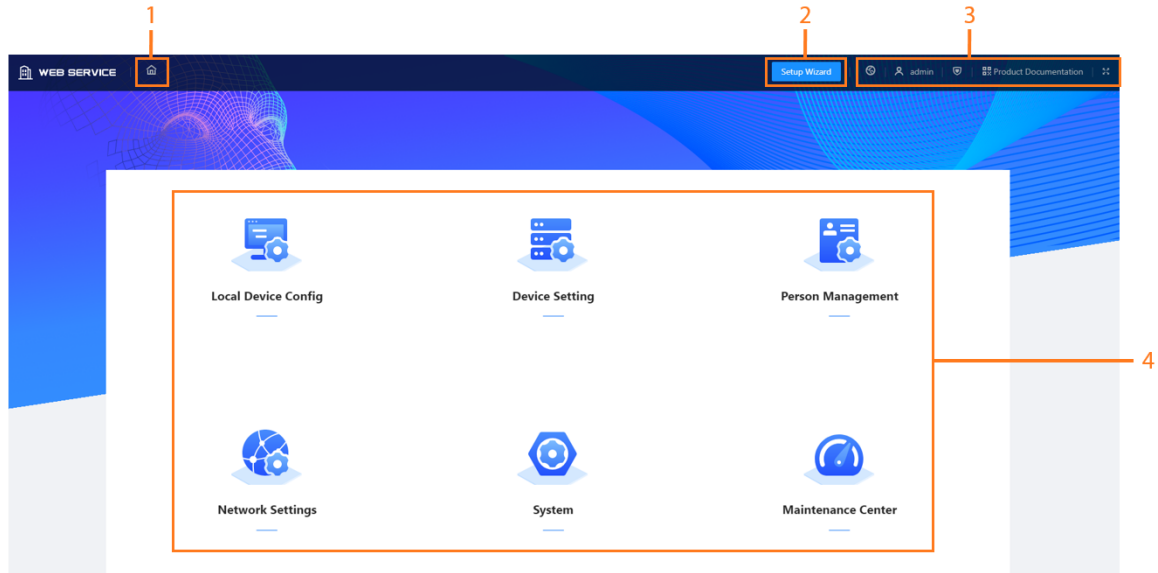







Table 4-1 Home page introduction

No.	Function	Description
1	Home button	Goes back to the home page.
2	Setup Wizard	Configure the VTO SIP server.
3	Navigation bar	<ul style="list-style-type: none"> : Change language of the webpage of the VTO. : Change password, log out of the current device, restart the system, and restore the device to factory settings. : View and configure the security settings. : 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.

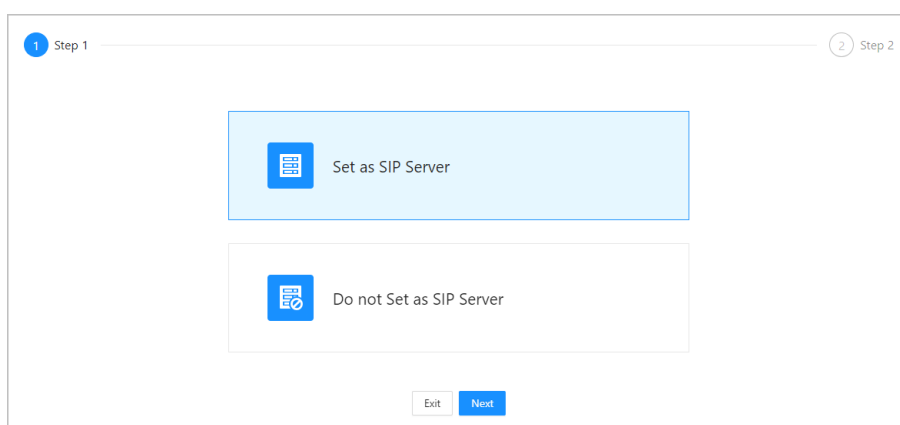
Prerequisites

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

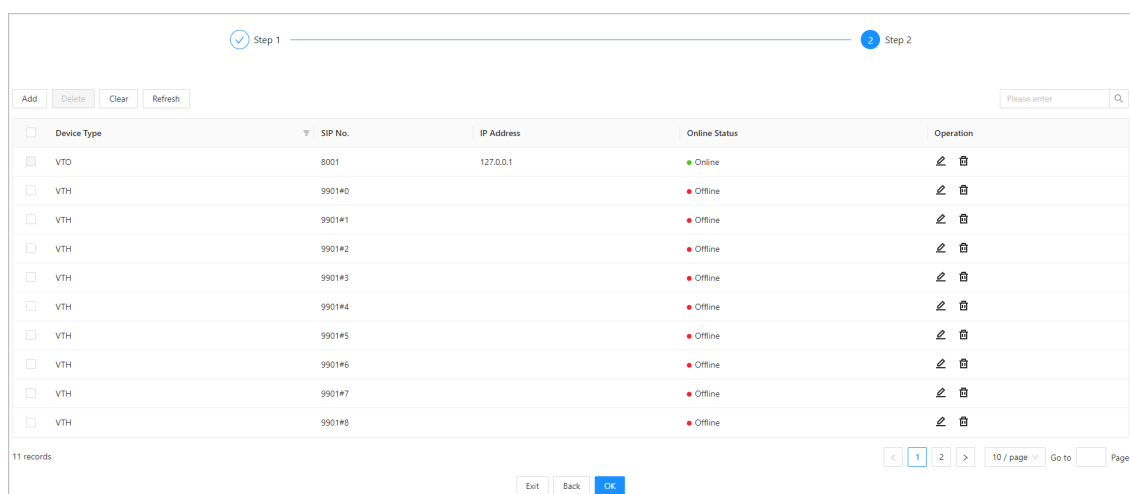
- Step 1 Log in to the webpage of the VTO.
- Step 2 Select **Setup Wizard** > **Set as SIP Server**, and then click **Next**.

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



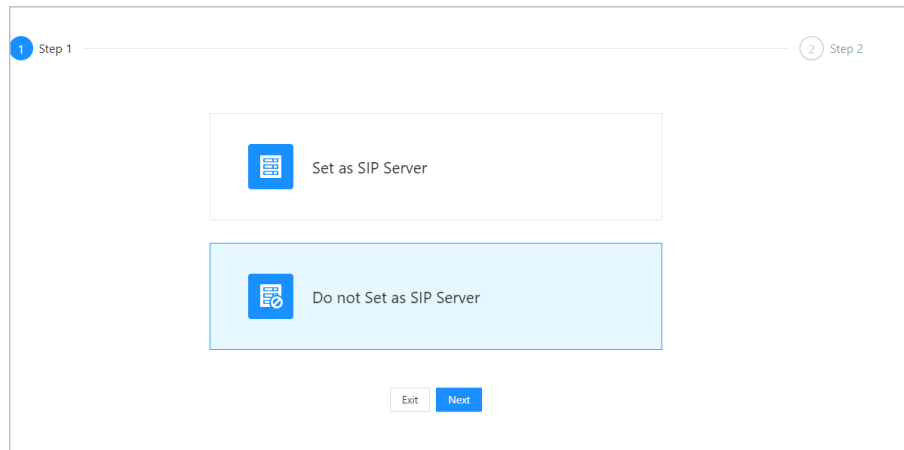
5.2 Not Setting as SIP Server

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

The screenshot shows a configuration form for Step 1 of the wizard. At the top, a progress bar indicates 'Step 1' is active and 'Step 2' is next. The form contains several fields for configuration: 'VTO ID' (8002), 'Building No.' (0), 'Unit No.' (0), 'Server Type' (Device), 'Server Address' (masked), 'Port' (5060), 'SIP No.' (8001), 'Registration Password' (masked), 'SIP Domain' (VDP), 'SIP Server Username' (admin), and 'SIP Server Password' (masked). At the bottom of the form, there are three buttons: 'Exit', 'Back', and 'OK'.

6 Local Device Configuration

This chapter introduces the detailed configuration of the VTO.



Slight differences might be found in different models.

6.1 Basic Settings

Configure basic settings of the device.

Procedure

- Step 1 Select **Local Device Config** > **Basic Settings**.
- Step 2 Configure the parameters.

Figure 6-1 Basic settings (small apartment)

Local Device Config

Device Type

Small Apartment

Device Name

Building No.

0

Unit No.

0

VTO ID

8001

Group Call

Management Center

888888

Functions

Storage Method

SD Card

SD Card Usage

0M/0M

Format SD Card

If the SD card cannot be recognized, you can format it.

Auto Capture while Unlocking

Auto Capture during Call

Upload Messages and Videos

Please regularly perform backups to avoid data loss.

Apply

Refresh

Default

Figure 6-2 Basic settings (villa station)

Local Device Config

Device Type

Villa Station

Device Name

Villa Room No.

9901

Building No.

0

Unit No.

0

VTO ID

8001

Group Call

Management Center

888888

Available Call Time

Setting

DND for DMSS

Setting

Calling by Period Mode

Enable

Functions

Storage Method

SD Card

SD Card Usage

0M/0M

Format SD Card

If the SD card cannot be recognized, you can format it.

Auto Capture while Unlocking

Auto Capture during Call

Upload Messages and Videos

Auto Record while Calling

Please regularly perform backups to avoid data loss.

Apply

Refresh

Default

Figure 6-3 Basic settings (fence station)

Local Device Config

Device Type

Fence Station

Device Name

Building No.

99

Unit No.

99

VTO ID

8001

Group Call

Management Center

888888

Functions

Storage Method

SD Card

SD Card Usage

0M/0M

Format SD Card

If the SD card cannot be recognized, you can format it.

Auto Capture while Unlocking

Auto Capture during Call


Please regularly perform backups to avoid data loss.






Apply


Refresh

Default

Table 6-1 Basic parameter description

Parameter	Description
Device Type	<p>Select from Villa Station and Small Apartment.</p> <p></p> <ul style="list-style-type: none"> The small apartment is available on select models. If the device has been added to the DoLynk Pro, the type can not be modified.
Device Name	When other devices are monitoring this VTO, the device name will appear on the monitoring image.
Villa Room No.	VTH room number. Used to call VTHs.

Parameter	Description
Building No.	Configuring the building and unit number where the device is.
Unit No.	 <p>If you clear the Building No. and Unit No. checkbox, it means that there is just only 1 building and 1 unit.</p>
VTO ID	<p>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.</p>  <p>The number cannot be changed when the VTO serves as the SIP server.</p>
Group Call	Enable it on the VTO that works as the SIP server, and when a main VTH receives a call, all extension VTHs will also receive the call.
Management Center	888888 by default.
Available Call Time	The time period in which the VTO's calling to other devices is limited. Click Setting to set the time plan for calling.
DND for DMSS	The time period in which the calling to DMSS is not limited. Click Setting to set the time plan for calling.
Calling by Period Mode	<ul style="list-style-type: none"> • If you enable the Calling by Period Mode, the specified number can be called in the specified period and the default number in other period. • Click Setting to set the time plan for calling.  <ul style="list-style-type: none"> • This function is only available when the mode is villa door station. • This function is available for the button  of the full keyboard module. • If the device is configured other keyboard modules, Calling by Period Mode of each modules can be configured in Local Device Config > Layout.
Storage Method	SD card by default.
SD Card Usage	Displays the total and used capacity of the SD card. You can click Format SD Card to delete all the data in the SD card.
Auto Capture while Unlocking	<p>Take a snapshot and save it in the SD card of the VTO when the VTO is unlocking.</p>  <p>If the VTO is unlock through local unlock button, the snapshot will not be taken.</p>

Parameter	Description
Auto Capture during Call	Take a snapshot and save it in the SD card of the VTO when the VTO is calling.
Upload Messages and Videos	<p>When enabled:</p> <ul style="list-style-type: none"> ● 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	<p>Take recording when the VTO is in a call, and save the recording in the SD card of the VTO.</p>  <ul style="list-style-type: none"> ● When the call time is less than 5 seconds, no video file will be generated. ● If there is a conflict between Auto Record while Calling and Leave Videos, Leave Videos prevails.

Step 3 Click **Apply**.

6.2 Access Control

6.2.1 Configuration

Procedure

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


Step 2 Configure the parameters.

Figure 6-4 Access control

Interval between Consecutive...	<input type="text" value="15"/>	s (1-20)
Door Unlocked Duration	<input type="text" value="2"/>	s (1-240)
Alarm Input/Door Detector	<input type="radio"/> Alarm Input <input checked="" type="radio"/> Door Detector	
Check Door Detector Signal ...	<input type="checkbox"/>	
Door Detector Alarm Thresh...	<input type="text" value="30"/>	s (1-9999)
Door Detector Status	<input checked="" type="radio"/> NC <input type="radio"/> NO	
Door Detector Alarm Sound	<input type="checkbox"/>	
Unlock Code	<input type="text" value="123"/>	
<input type="checkbox"/> Lock Linkage		
New Duress Password	<input type="password" value="....."/>	
Confirm New Duress Password	<input type="password" value="....."/>	
Public Password	<input type="button" value="Setting"/>	
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>		

Table 6-2 Access control parameter description

Parameter	Description
Interval between Consecutive Unlocks	The door can only be unlocked again after the interval.
Door Unlocked Duration	The time during which the lock stays unlocked.
Alarm Input/Door Detector	Select one of them.
Check Door Detector Signal Before Locking	Enable the function based on your needs.
Door Detector Alarm Threshold	The threshold time when the door detector alarm is triggered.

Parameter	Description
Door Detector Status	<ul style="list-style-type: none"> • NC : Normally closed. • NO : Normally open.
Door Detector Alarm Sound	<p>It is disabled by default.</p> <p>When it is enabled:</p> <ul style="list-style-type: none"> • Door Detector Status is NC: If the door opening time exceeds the set door detection alarm threshold, the VTO will beep. And when the door detector is closed, the VTO does not beep again. • Door Detector Status is NO: If the door closing time exceeds the set door detection alarm threshold, the VTO will beep. And when the door detector is open, the VTO does not beep again.
Unlock Code	You can connect a third-party phone, such as a SIP phone, to the VTO, and use the code to open the door remotely.
Lock Linkage	Enable the Lock Linkage , and then select the linkage lock from the drop-down list.
New Duress Password	Enter and confirm the duress password.
Confirm New Duress Password	 <p>When you enter the duress password. It will unlock the door normally and secretly trigger an alarm or notify management center at the same time.</p>
Public Password	Click Settings to set the public password. You can add, export, and import the public password.

Step 3 Click **Apply**.

6.2.2 Extension Function

6.2.2.1 RS-485

Procedure

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

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

Figure 6-5 RS-485

RS-485

Network Lift Control

RS-485

Port Type

Lock

Interval between C...

15

s (1-20)

Unlock Duration

2

s (1-240)

Unlock Code

456


☐ Lock Linkage

Apply

Refresh

Default

Table 6-3 RS-485 description

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

Step 3 Click **Apply**.



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

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

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

6.2.2.2 Network Lift Control

The lock can be connected to network lift control.



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

Procedure

- Step 1** Select **Local Device Config** > **Access Control** > **Extension Function** > **Network Lift Control**.
- Step 2** Enable the network lift control.
- Step 3** Configure the lift control.

Figure 6-6 Network lift control

Lift Name	Enable	Lift Control Durati...	IP Address	Port	Username	Password	Connection Status	Operation
Lift 1	<input type="checkbox"/>	120	192.168.0.2	5000	admin	*****	Test	Edit
Lift 2	<input type="checkbox"/>	120	192.168.0.2	5000	admin	*****	Test	Edit
Lift 3	<input type="checkbox"/>	120	192.168.0.2	5000	admin	*****	Test	Edit
Lift 4	<input type="checkbox"/>	120	192.168.0.2	5000	admin	*****	Test	Edit
Lift 5	<input type="checkbox"/>	120	192.168.0.2	5000	admin	*****	Test	Edit
Lift 6	<input type="checkbox"/>	120	192.168.0.2	5000	admin	*****	Test	Edit
Lift 7	<input type="checkbox"/>	120	192.168.0.2	5000	admin	*****	Test	Edit
Lift 8	<input type="checkbox"/>	120	192.168.0.2	5000	admin	*****	Test	Edit

Table 6-4 Network lift control description

Parameter	Description
Lift Control Mode	<ul style="list-style-type: none"> • With Lift Controller: Up to 8 lifts can be added. • Without Lift Controller: Up to 6 lifts can be added.

Parameter	Description
Verification Method	<p>It is enabled when the Lift Control Mode is set as With Lift Controller.</p> <ul style="list-style-type: none"> Remote Verification: The verification is made remotely. Local Verification: The verification is made locally.
VTO Floor	Each lift controls up to 128 floors.

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

Figure 6-7 Set lift information

Table 6-5 Network lift control description

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

Step 5 Click **Apply**.

Related Operations

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

6.3 Light Control

Configure the illuminator as needed.

Procedure

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

Step 2 Set illuminator and device light modes from the following modes.

- **NO** : The illuminator is open all the time.
- **NC** : The illuminator is closed all the time.
- **Self-adaptive** : The illuminator will adapt to the environment, and then sets a suitable value.
- **Period** : The illuminator will be open during the defining period.



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

Step 3 Click **Apply**.

6.4 Layout (Multiple Modules)

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

Procedure

Step 1 Log in to the webpage of the VTO.

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

Step 3 Click **+** to add modules.

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



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

Figure 6-8 Configure the layout



Figure 6-9 Configure the room number

Button Settings [X]

Button Functions ☒ Room No. ☐ Postal Worker Unlock

Room No. 103 [v]

[Clear] [OK] [Cancel]

Figure 6-10 Configure the postal worker unlock

Button Settings [X]

Button Functions ☐ Room No. ☒ Postal Worker Unlock

Enable ☒


Lock Permission ☒ Local Lock ☐ External Lock

Unlock Schedule Setting

[Clear] [OK] [Cancel]

Table 6-6 Button parameters description

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

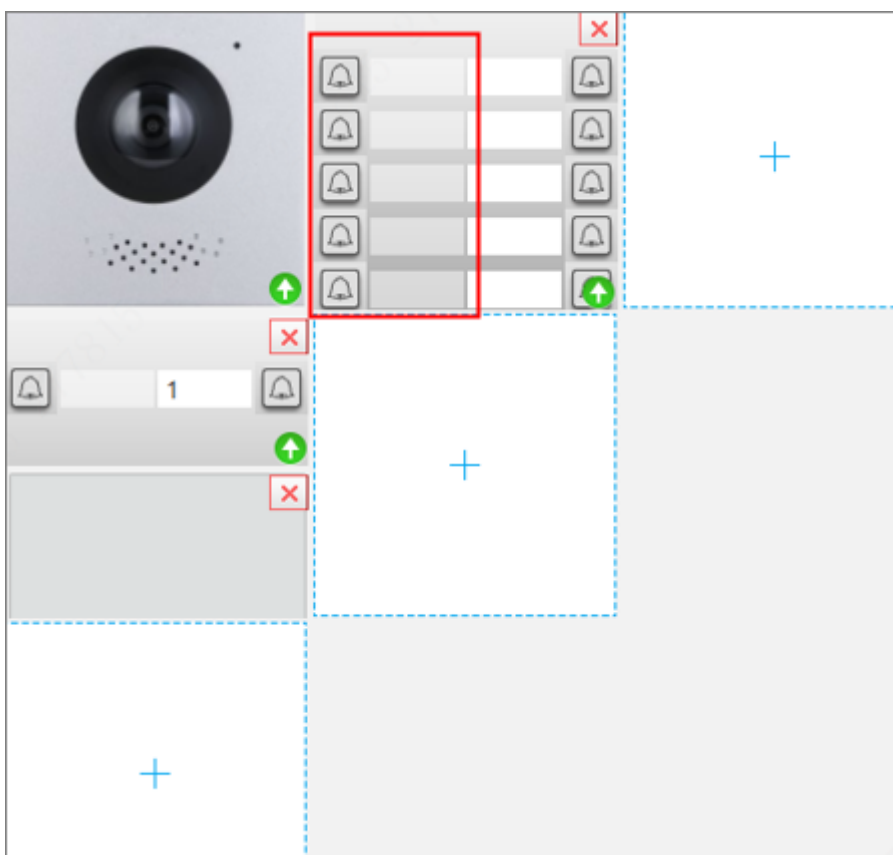
Parameter	Description
Postal Worker Unlock	<p>Configure the postal worker unlock.</p> <ol style="list-style-type: none"> 1. Click  to enable the function. 2. Set the lock permission from Local Lock and External Lock. 3. Click Setting to configure the unlock schedule. 4. Click OK.

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




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

Figure 6-11 Non-editable buttons



Related Operations

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

6.5 Adding IPC

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

You can add the IPC devices on the webpage of the VTO. The VTHs with the same online SIP server get the IPC information.



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

6.5.1 Adding IPC One by One

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



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

Procedure

- Step 1 Log in to the webpage.
- Step 2 Select **Local Device Config** > **IPC Info**.

Figure 6-12 IPC information

<div>Refresh Import Export Default</div>								
No.	Name	IP Address	Protocol Type	Stream Type	Port	Channel No.	Device Type	Operation
1		0.0.0.0	Local	Sub Stream	554	0	IPC	
2		0.0.0.0	Local	Sub Stream	554	0	IPC	
3		0.0.0.0	Local	Sub Stream	554	0	IPC	
4		0.0.0.0	Local	Sub Stream	554	0	IPC	
5		0.0.0.0	Local	Sub Stream	554	0	IPC	

- Step 3 Click to configure the parameters.

Figure 6-13 Configure the parameters

Edit

X

Name

IP Address

0 . 0 . 0 . 0

Protocol Type

Local

▼

Stream Type

Sub Stream

▼

Device Type

IPC

▼

Channel No.

0

Encryption

☐

Username

admin

* Password

Port

554

OK

Cancel

Table 6-7 Parameters description of the video monitoring device

Parameter	Description
Name	Enter the name of the IPC/VNR/XVR/HCVR device.
IP Address	Enter the IP address of the IPC/VNR/XVR/HCVR device.
Protocol Type	Select from Local and ONVIF according to the device you add.
Stream Type	Select from Main Stream and Sub Stream .
Device Type	Select the type according to the actual devices.
Channel No.	<ul style="list-style-type: none"> • If you add the IPC, it is 1 by default. • If you add the NVR/XVR/HCVR, it is the channel of IPC that was configured on the VNR/XVR/HCVR device.

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

Step 4 Click **OK**.

6.5.2 Exporting IPC Information in Batches

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

Procedure

Step 1 Click **Export**.

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

The IPC configuration file is saved to the local computer.

6.5.3 Importing IPC Information in Batches

Import the IPC information to the system.

Procedure

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

Figure 6-14 Import

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

6.6 Card Settings

Procedure

Step 1 Log in to the webpage.

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

Figure 6-15 Card settings

Card Settings

IC Card

IC Card Encryption & Verification

Apply

Refresh

Default

Table 6-8 Description of card parameters

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



External card readers do not support encrypted IC cards.

Step 3 Click **Apply**.

7 Device Setting

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

7.1 VTO Management

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

Procedure

- Step 1 Log in to the webpage of the VTO that works as the SIP server.
- Step 2 Select **Device Setting**.
- Step 3 Click **Add**.
- Step 4 Configure the parameters.

Figure 7-1 Add VTO

The screenshot shows a web-based configuration window titled "Add" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Device Type:** A dropdown menu currently showing "VTO".
- * No.:** A text input field containing the value "8001".
- * Registration Password:** A password input field represented by six dots, with a small icon to its right.
- Building No.:** An empty text input field.
- Unit No.:** An empty text input field.
- * IP Address:** An IP address input field showing "127.0.0.1".
- * Username:** A text input field containing the value "admin".
- * Password:** A password input field represented by six dots, with a small icon to its right.
- Buttons:** "OK" and "Cancel" buttons are located at the bottom right of the dialog.



Table 7-1 Add VTO configuration

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

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

Step 5 Click **OK**.

Related Operations

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

7.2 VTH Management


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

Procedure

- Step 1 Log in to the webpage of the SIP server.
- Step 2 Select **Device Setting**.
- Step 3 Click **Add**.
- Step 4 Configure the parameters.
- Select the device type as **VTH**.

Figure 7-2 Add VTH one by one

Table 7-2 Parameters description

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

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



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

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





Figure 7-3 Add VTH in batches

Table 7-3 Parameters description

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

Step 5 Click **OK**.



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



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

7.3 VTS Management

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

Procedure

- Step 1 Log in to the webpage of the VTO that works as the SIP server.
- Step 2 Select **Device Setting**.
- Step 3 Click **Add**.
- Step 4 Configure the parameters.

Figure 7-4 Add VTS

Add

X

Device Type

VTS

* VTS No.

Please enter

* IP Address

* Registration Password

.....

OK

Cancel

Table 7-4 Add VTS configuration

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

- Step 5 Click **OK**.

8 Person Management



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

Procedure

Step 1 Log in to the webpage.

Step 2 Select **Person Management**.

Figure 8-1 Person management

Add		Import Person	Export Person	Delete	Clear	Refresh	Person ID/Room No./Username		Q
<input type="checkbox"/>	No.	Person ID	Room No.	Username			Verification Mode		Operation
<input type="checkbox"/>	1	10000001	1001	zrwk5ab6gcy0toux9s837pq1nijfdh			🔒 1 📄 1 🔄 1		✏️ 🗑️
<input type="checkbox"/>	2	10000002	1002	ri75m1swqbd4a9mp6jvz3ytx20kcci			🔒 1 📄 1 🔄 1		✏️ 🗑️
<input type="checkbox"/>	3	10000003	1003	eqp52mt0ubkdn9xohlgsl1czv48wrf			🔒 1 📄 1 🔄 1		✏️ 🗑️
<input type="checkbox"/>	4	10000004	1004	ule6p1rbxvtf8h5a32dic94qt07wsmo			🔒 1 📄 1 🔄 1		✏️ 🗑️
<input type="checkbox"/>	5	10000005	1005	sbuid3z1kf2cmrya85xjcp69ehngwq			🔒 1 📄 1 🔄 1		✏️ 🗑️
<input type="checkbox"/>	6	10000006	1006	jb3ldpc0sy16am8t94zrv75x2owif			🔒 1 📄 1 🔄 1		✏️ 🗑️
<input type="checkbox"/>	7	10000007	1007	spn12h38gy5wir7czlffk4bv9ug6m0o			🔒 1 📄 1 🔄 1		✏️ 🗑️
<input type="checkbox"/>	8	10000008	1008	8lhuda6174cbje0zsqypwg3itfnr2o			🔒 1 📄 1 🔄 1		✏️ 🗑️
<input type="checkbox"/>	9	10000009	1009	l8owve6zyd9rscq32tp5f7huim1gbax			🔒 1 📄 1 🔄 1		✏️ 🗑️
<input type="checkbox"/>	10	10000010	1010	g0x2umw47okad6tivcz3r5jfb8qp9e			🔒 1 📄 1 🔄 1		✏️ 🗑️
3000 records									
<div><div>< 1 2 3 4 5 ... 300 ></div><div>10 / page</div><div>Go to</div><div>Page</div></div>									

Step 3 Click **Add**.

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

Figure 8-2 Add the person

Add
×

* Person ID

* Room No.

Username

* Validity Period

Forever ▾

* Lock Permission

☒ Local Lock
☒ External Lock

Multi-Door Unlock ⓘ

☐

Verification Mode

> Password
Not Added



> Card
Not Added









> Fingerprint
Not Added

OK

Cancel

Table 8-1 Person parameters description

Parameter	Description
Person ID	Customize the number.
Room No.	Enter the corresponding room number of the VTH.
Username	Enter the user name.
Validity Period	Configure the validity period during which people have access permissions.
Lock Permission	Set the lock permission. You can enable the permission for local lock and external lock at the same time.
Multi-Door Unlock	<p>When verification is successful, the local lock and external lock will open at the same time.</p> <p></p> <p>Personal password does not support this function.</p>
Password	<ol style="list-style-type: none"> Select Password > Add. Enter the password, and then confirm it again. <p></p> <p>The password must consist of 4-6 digits.</p> <ol style="list-style-type: none"> Click OK.

Parameter	Description
Card	<ol style="list-style-type: none"> 1. Select Card > Add. 2. Enter the card number. Or you can click Issue Card, and then swipe the card on VTO. 3. Click OK. <p>You can manage the cards through the following icons.</p> <ul style="list-style-type: none"> •  /  : Configure the card as the main card or general card. •  : If you lost your card, click to report the loss. The icon becomes . •  : The card cannot be used to open the door. Click it to make the card valid. •  : Edit the card name. •  : Delete the card.
Fingerprint	<p>If a kind of modular device is added on Local Device Config > Layout, fingerprint is supported.</p> <ol style="list-style-type: none"> 1. Select Fingerprint > Add. 2. Record your fingerprint according to the prompts. 3. Click OK.
Floor	<p>Select the floor which can be given the permission.</p>  <p>This parameter is available only when Lift Control Mode is selected as Without Lift Controller.</p>

Related Operations

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

9 Network Settings

This chapter introduces how to configure the network parameters.

9.1 TCP/IP

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

Procedure


- Step 1 Log in to the webpage of the VTO.
- Step 2 Select **Network Settings** > **TCP/IP**.
- Step 3 Configure the TCP/IP parameters.

Figure 9-1 TCP/IP

The screenshot displays the TCP/IP configuration page. At the top, there is a 'DHCP' toggle switch that is currently turned off. Below this, there are several input fields: 'MAC Address', 'IP Address', 'Subnet Mask', and 'Default Gateway', each with a corresponding input box. Below these are 'Preferred DNS' and 'Alternate DNS' fields, each with a text input box containing '8.8.8.8' and '8.8.4.4' respectively. At the bottom, there is a 'Transmission Mode' section with two radio buttons: 'Multicast' (which is selected) and 'Unicast'. Below the radio buttons are three buttons: 'Apply' (in blue), 'Refresh', and 'Default'.

Table 9-1 Parameter description

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

Parameter	Description
Preferred DNS	It is 8.8.8.8 by default.
Alternate DNS	It is 8.8.4.4 by default.
Transmission Mode	<ul style="list-style-type: none"> • Multicast: Ideal for video talk. • Unicast: Ideal for group call.  <p>Unicast is not recommended when the platform is being used as an SIP server.</p>

Step 4 Click **Apply**.

9.2 Port

Procedure

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

Step 2 Configure the parameters.

Figure 9-2 Port

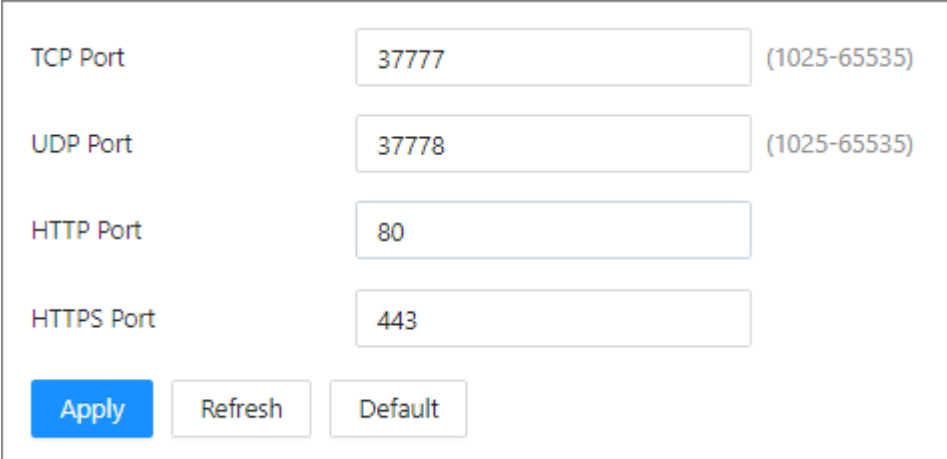


Table 9-2 Parameter description

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

Step 3 Click **Apply**.

9.3 SIP Server

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

Procedure

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

Step 2 Select a server type.

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



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

Figure 9-3 Current VTO as SIP server

Local SIP Server	<input checked="" type="checkbox"/>
Port	5060
SIP No.	8001
Registration Password	••••••••••••••••
SIP Domain	VDP
Cascade SIP Server	<input type="checkbox"/>
Backup SIP Server	<input type="checkbox"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>	

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



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

Figure 9-4 Another VTO as SIP server

Local SIP Server

Server Type

Device

Server Address

Port

5060

SIP No.

8001

Registration Password

SIP Domain

VDP

SIP Server Username

admin

SIP Server Password

Apply

Refresh

Default


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

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

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

Figure 9-5 Private SIP server

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

Parameter	Description
Server Address	IP address of the SIP server.
Port	5080 by default when the platform works as the SIP server.
SIP No.	Leave it by default.
Registration Password	
SIP Domain	
Device as Alternate Server	Enable it so that you can configure the Alternate VTS IP.
Alternate IP	<p>The alternate server will be used as the SIP server when Express or DSS stops responding. We recommend you configure the alternate IP address.</p> <p></p> <ul style="list-style-type: none"> ◇ If you enable Device as Alternate Server, the current VTO you have logged in serves as the alternate server. ◇ If you want another VTO serve as the alternate server, you need to enter the IP address of that VTO in the Alternate IP textbox. Do not enable Device as Alternate Server in this case.
Alternate Server Username/ Password	Used to log in to the alternate server.
Alternate VTS IP	IP address of the alternate VTS.

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

Figure 9-6 Third-party server

Local SIP Server

Server Type

Third-party Server

Server Address

192.168.1.111

Port

2

Custom Name

SIP No.

8001

Registration Password

.....

SIP Domain

VDP

Apply

Refresh

Default

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

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

Step 3 Click **Apply**.



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

9.4 Cloud Service

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

Figure 9-7 Cloud service


Enable ☒

After the function is enabled and the device connects to the network, we will collect device information such as the IP address, MAC address, device name and serial number. The collected information will only be used to remotely access the device. If you do not want to enable this function, please clear the selection from the check box.

P2P Status ● Offline

PaaS Status ● Offline

SN A 6



Apply

Refresh

Default

9.5 UPnP

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

53

Figure 9-8 UPnP

<div>Enable <input type="checkbox"/></div> <div> Apply Refresh Default Add </div>								
Service Name	Service Type	Protocol	Internal Port	External Port	Status	Enable	Modify	
HTTP	CustomService	TCP	80	8080	Mapping Failed	<input checked="" type="checkbox"/>	Edit	Delete
TCP	CustomService	TCP	37777	37777	Mapping Failed	<input checked="" type="checkbox"/>	Edit	Delete
UDP	CustomService	UDP	37778	37778	Mapping Failed	<input checked="" type="checkbox"/>	Edit	Delete
RTSP	CustomService	TCP	554	554	Mapping Failed	<input checked="" type="checkbox"/>	Edit	Delete
PrivService	CustomService	TCP	18877	18877	Mapping Failed	<input checked="" type="checkbox"/>	Edit	Delete
SIP	CustomService	UDP	5060	5060	Mapping Failed	<input checked="" type="checkbox"/>	Edit	Delete
Rtp	CustomService	UDP	15001	15001	Mapping Failed	<input checked="" type="checkbox"/>	Edit	Delete
Rtp	CustomService	UDP	15002	15002	Mapping Failed	<input checked="" type="checkbox"/>	Edit	Delete
Rtp	CustomService	UDP	15003	15003	Mapping Failed	<input checked="" type="checkbox"/>	Edit	Delete
Rtp	CustomService	UDP	15004	15004	Mapping Failed	<input checked="" type="checkbox"/>	Edit	Delete
22 records					<div> < 1 2 3 > </div> <div> 10 / page Go to Page </div>			

Preparation

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

9.5.1 Enabling UPnP Services

Procedure

- Step 1 Select **Network Settings** > **UPnP**.
- Step 2 Select the services listed, and then click **Enable**.
- Step 3 Click **Apply**.

9.5.2 Adding UPnP Services

Procedure

- Step 1 Select **Network Settings** > **UPnP**.
- Step 2 Click **Add**.
- Step 3 Configure the parameters, and then click **OK**.



Figure 9-9 Add a UPnP service

The screenshot shows a window titled "Add" with a close button (X) in the top right corner. Inside the window, there are several configuration options:

- Enable:** A toggle switch that is currently turned off.
- * Service Name:** A text input field containing the value "VTO1".
- * Service Type:** A text input field containing the value "VTO".
- Protocol:** A dropdown menu currently set to "TCP".
- * Internal Port:** A text input field containing the value "3".
- * External Port:** A text input field containing the value "3".

At the bottom right of the window, there are two buttons: "OK" (highlighted in blue) and "Cancel".

Table 9-6 Parameter description

Parameter	Description
Service Name	Enter the name and type of the service.
Service Type	
Protocol	Select TCP or UDP .
Internal Port	<p>Internal port of the service. </p> <ul style="list-style-type: none"> • 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	<p>External port of the service. </p> <ul style="list-style-type: none"> • If you need to configure this function for multiple devices, make sure that the ports are not the same. • The port number you use must not be occupied. • The internal and external port number must be the same.

9.6 Basic Services

Configure functions that involve device security.




Procedure





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

Step 2 Enable the security functions based on your needs.

Figure 9-10 Basic services

Table 9-7 Security parameter description

Parameter	Description
SSH	<p>A secure alternative to unsecured remote protocols.</p> <p> We recommend you turn it off because there might be safety risk if this service is enabled.</p>
CGI	<p>The use of CGI command.</p> <p> We recommend you turn it off. Otherwise, the VTO might be exposed to security risks and data leakage.</p>
Mobile Push Notification	<p>Send information to the app on the phone.</p> <p> 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.</p>

Parameter	Description
Password Reset	If turned off, you will not be able to reset password.
ONVIF	Allows the communications between devices of the different brand or series.
Outbound Protection of Service Information	Protect your passwords.  We recommend you turn it on. Otherwise, the VTO might be exposed to security risks and data leakage.
Multicast/Broadcast Search	Enable it so that the VTO will be found by other devices.  We recommend you turn it off. Otherwise, the VTO might be exposed to security risks and data leakage.
Authentication Mode	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● Select an expiration period from 30 days, 60 days, 90 days, 180 days, Custom and Never. ● If you select Custom, you need to configure an expiration day between 0 and 180.
Private Protocol	Before enabling private protocol TLS, make sure that the corresponding device or software supports this function.
TLSv1.1	 We recommend you turn it off because there might be safety risk if this service is enabled.
LLDP	Improves the efficiency of information exchange among network devices.

Step 3 Click **Apply**.

9.7 Auto Registration

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

Procedure

Step 1 Log in to the webpage of VTO.

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

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

Figure 9-11 Auto registration

Enable

☐

Server Address

Port

(1-65535)

Registration ID

Apply

Refresh

Default

Table 9-8 Parameters description

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

Step 4 Click **Apply**.

10 System

10.1 Alarm

Procedure

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

Figure 10-1 Alarm

The screenshot shows a mobile application interface for configuring alarm settings. It is divided into two main sections: 'Calling Alarm' and 'Tamper Alarm'. The 'Calling Alarm' section has a single toggle switch that is currently turned off. The 'Tamper Alarm' section has three toggle switches, all of which are currently turned on: 'Tamper Sound', 'Report Event', and 'Restore Device for M...'. At the bottom of the interface, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

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

Table 10-1 Alarm parameter description

Parameter	Description
Calling Alarm	When the call is initiated, the alarm output will be linked. If the alarm out interface is connected with a buzzer, it will beep.
Tamper Sound	Configure whether the device whistles locally or not. It is enabled by default.
Report Event	Configure whether the device reports the tamper alarm to the APP, indoor unit, and back-end of the platform or not. It is enabled by default.
Restore Device for Multiple Tamper Alarms	Within 10 minutes after the device is powered on, if you continuously press the tamper button for 5 times in 8 seconds, the device beeps and deletes the account information.

Step 3 Click **Apply**.

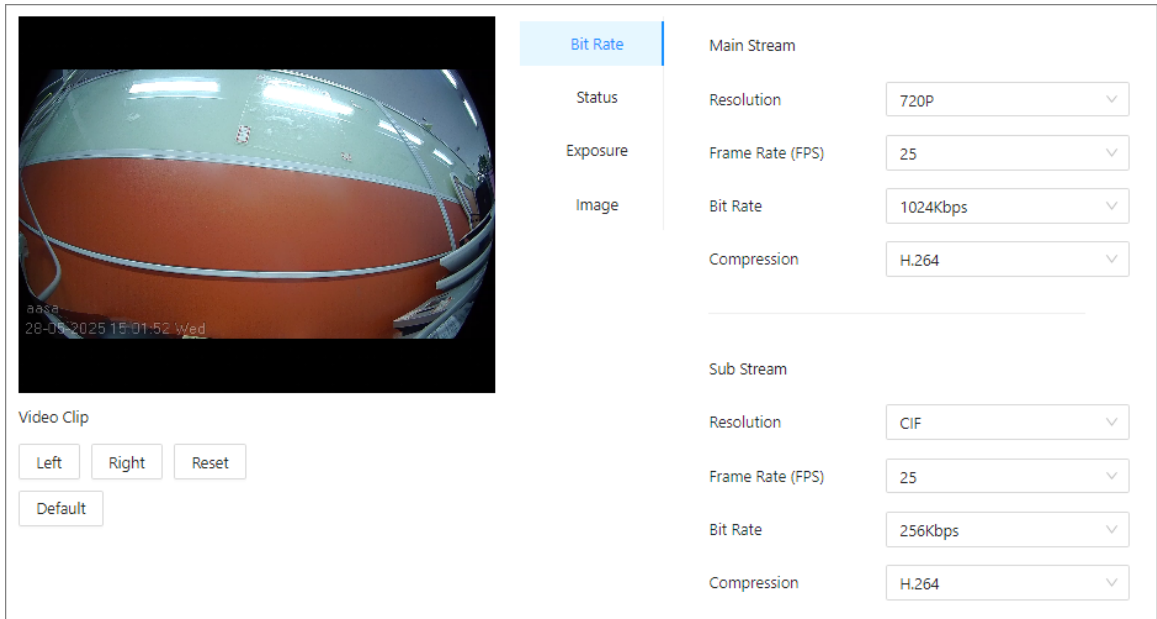
10.2 Video

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

Procedure

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

Figure 10-2 Video



The screenshot displays the video configuration interface. On the left, a video preview window shows a red and white curved surface. Below the preview are buttons for 'Left', 'Right', 'Reset', and 'Default'. On the right, a configuration panel is visible with tabs for 'Bit Rate', 'Status', 'Exposure', and 'Image'. The 'Bit Rate' tab is active, showing settings for 'Main Stream' and 'Sub Stream'. Main Stream settings include Resolution (720P), Frame Rate (FPS) (25), Bit Rate (1024Kbps), and Compression (H.264). Sub Stream settings include Resolution (CIF), Frame Rate (FPS) (25), Bit Rate (256Kbps), and Compression (H.264).

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

Table 10-2 Video parameter description

Parameter			Description
Bit Rate	Main Stream	Resolution	<ul style="list-style-type: none">● 720P : 1280 × 720.● WVGA : 800 × 480.● D1 : 704 × 576.● CIF : 352 × 288.
		Frame Rate (FPS)	<ul style="list-style-type: none">● 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). <p>The larger the value, the smoother the video, but it requires more bandwidth.</p>
		Bit Rate	The larger the value, the better the video quality, but it requires more bandwidth.
		Compression	Compared with H.264, H.265 requires smaller bandwidth.

Parameter			Description
	Sub Stream	Resolution	<ul style="list-style-type: none"> ● 1080P : 1920 × 1080. ● 720P : 1280 × 720. ● D1 : 704 × 576. ● WVGA : 800 × 480. ● CIF : 352 × 288. ● QVGA : 320 × 240.
		Frame Rate (FPS)	The range is 1 to 25. The larger the value, the smoother the video, but it requires more bandwidth.
		Bit Rate	Include 224 Kbps, 256 Kbps, 320 Kbps, 384 Kbps, 448 Kbps, 512 Kbps, 640 Kbps, 768 Kbps. The larger the value, the better the video quality, but it requires more bandwidth.
		Compression	H.264. H.265.
Status	Scene Mode		Select from Auto , Disable , Sunny and Night . Auto is selected by default.
	Compensation Mode		<ul style="list-style-type: none"> ● BLC : Back light compensation. Improve the clarity of the target in the image. ● WDR : Wide dynamic range. Enhance the brightness of dark areas, and reduce the brightness of bright areas to improve the image. ● HLC : High light compensation. Reduce the brightness of the strong spots to improve the overall image. ● Disable: Do not use any compensation mode.
	Day/Night		Select from Color , Auto and B/W .
	Video Standard		Select PAL or NTSC according to your area.
Exposure	Anti-flicker		<ul style="list-style-type: none"> ● 50Hz : The system adjusts the exposure according to ambient light automatically to ensure that stripes do not appear. ● 60Hz : The system adjusts the exposure according to ambient light automatically to ensure that stripes do not appear. ● Outdoor : If you select Outdoor, the exposure mode can be set to Gain Priority, Shutter Priority and Iris Priority. Different devices support different exposure modes.

Parameter		Description
	Exposure Mode	<ul style="list-style-type: none"> ● Auto : Exposure is automatically adjusted according to scene brightness if the overall brightness of images is in the normal exposure range. ● Manual : You can adjust the Gain and Shutter value manually. ● Shutter Priority : The camera automatically adjusts the aperture size based on the selected shutter speed to ensure proper exposure.
	Exposure Compensation	You can set the exposure compensation value. The value ranges from 0 to 100. The higher the value is, the brighter the image will be.
	3D NR	Reduce the noise of multiple-frame (at least two frames) images by using inter-frame information between two adjacent frames in a video. The higher the level is, the lower the noise will be, and the larger the trailing smear will be.
	NR Level	Noise reduction grade. The value ranges from 0 to 100. The larger the value is, the less the noise will be.
Image	Brightness	The larger the value, the brighter the image.
	Contrast	Larger value for more contrast between bright and dark areas.
	Hue	Make the color brighter or darker. The default value is made by the light sensor, and we recommend keeping it default.
	Saturation	The larger the value, the thicker the color.
	Gain Adjustment	Configure the gain.
	Mirror	Display the image with left and right side reversed.
	Flip	Display the image upside down.
	Display Time	Display the current time and date on the video image.

Step 3 (Optional) Configure the video clip.

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

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



The function is only available for the mode of F.

10.3 Audio

Procedure

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

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

Figure 10-3 Audio

Audio Control

Voice Prompt while Ringing ☒

Ringtone ☒

Unlock ☒

Alarm ☒

Voice Messages ☒

Audio Collection ☒

Volume Control

Intercom Volume + 0

Microphone Volume + 0

Device Volume + 0

Apply **Refresh** **Default**


Audio File(Please upload a WAV or MP3 file. The file size must not exceed 100K.)

Audio Type	Audio File	Modify
Calling	-	📁
Busy	-	📁
Successfully Unlocked	-	📁
Nobody Answered	-	📁
Call Ended	-	📁
Nonexistent Number	-	📁

Table 10-3 Audio parameter description

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

Step 3 Click **Apply**.

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



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

10.4 Time

Configure the time zone and day light saving parameters.


Procedure

Step 1 Select **System > Time**.

Step 2 Configure the time and time zone and DST.

Figure 10-4 Time

Time and Time Zone



Date :

2023-07-10 Monday

Time :

13:46:16


Time

☒ Manually Set

☐ NTP

System Time

2023-07-10 13:46:16



Sync PC

Time Format

YYYY-MM-DD

24-Hour

Time Zone

(UTC) Coordinated Universal Time

DST

Enable

☐

Type

☐ Date

☒ Week


Start Time

May

Final Week

Mon

00:00




End Time

Oct

Final Week

Mon

00:00










Apply

Refresh

Default

Table 10-4 Parameter description

Module	Parameter	Description
Time and Time Zone	Time	<ul style="list-style-type: none">Manually SetNTP

Module	Parameter	Description
	System Time	<p>The time of the VTO system.</p>  <p>Changing system time might cause problems on video searching and information publication. Turn off video recording and auto snapshot before changing it.</p>  <p>Only applicable under the Manually Set mode.</p>
	Sync PC	<p>Synchronize the VTO system time with your PC.</p>  <p>Only applicable under the Manually Set mode.</p>
	Server	<p>The address of the NTP server.</p>  <p>Only applicable under the NTP mode.</p>
	Manual Update	<p>Click the icon and the device time of the VTO will be automatically synchronized with server.</p>  <p>Only applicable under the NTP mode.</p>
	Port	<p>NTP server port number.</p>  <p>Only applicable under the NTP mode.</p>
	Interval	<p>VTO time update cycle. 30 minutes at most.</p>  <p>Only applicable under the NTP mode.</p>
	Time Format	<p>For the date format, select from one of the following:</p> <ul style="list-style-type: none"> • YYYY-MM-DD • MM-DD-YYYY • DD-MM-YYYY <p>For the time format, select from one of the following:</p> <ul style="list-style-type: none"> • 24-Hour • 12-Hour
	Time Zone	Select the time zone for the VTO system.
DST	Enable	Click to enable the DST function.
	Type	Select Date or Week as needed, and then configure the specific period.
	Start Time	Configure the start time and end time of DST.
	End Time	

Step 3 Click **Apply**.

10.5 ONVIF User

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



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

Procedure

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

Step 2 Click **Add**.

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

ONVIF devices can monitor the VTO by using the account.

Figure 10-5 ONVIF user

Add X

* Username

* Password

* Confirm Password

OK Cancel

11 Maintenance Center

11.1 One-Click Diagnosis

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

Procedure

Step 1 Log in to the webpage.

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

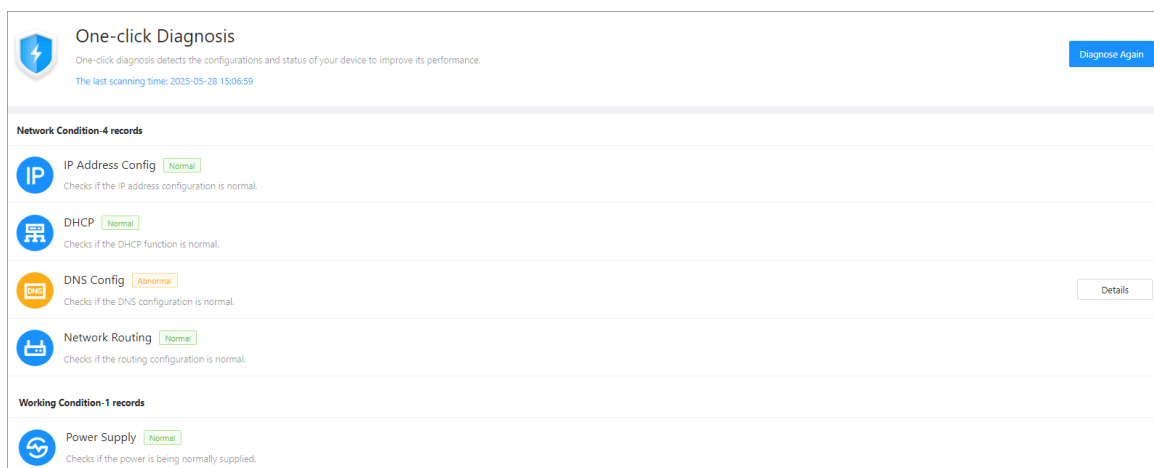
Step 3 Click **Diagnose**.

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

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

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

Figure 11-1 One-click diagnosis



11.2 System Information

11.2.1 Version Information

Procedure

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

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

Figure 11-2 System information

Device Model	
Device SN	
Hardware Version	
Software Version	
SCM Version	
Web Version	
Security Baseline Version	

11.2.2 Legal Information

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

11.3 Data Capacity

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

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

11.4 Log Management

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



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

11.4.1 Call History

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

Figure 11-3 Call history

Please keep unencrypted files well to avoid data leakage.					
Export					
No.	Call Type	Room No.	Start Time	Call Duration (min)	End Status
1	Incoming	9902	2000-03-18 00:40:45	00:30	Answered
2	Outgoing	9903	2000-03-17 08:51:39	00:00	Missed
3	Incoming	9904	2000-03-14 04:08:05	00:39	Answered
4	Incoming	9904	2000-03-14 04:05:57	00:19	Answered
5	Incoming	9905	2000-03-11 00:34:46	00:12	Answered
6	Incoming	9904	2000-03-10 08:11:20	00:12	Answered
7	Incoming	9904	2000-03-10 02:26:20	00:06	Answered
8	Incoming	9904	2000-03-10 02:25:54	00:21	Answered
9	Incoming	9904	2000-03-10 02:25:09	00:44	Answered
10	Incoming	9904	2000-03-10 00:53:06	00:06	Answered

681 records

< 1 2 3 4 5 ... 69 > 10 / page Go to Page

11.4.2 Alarm Logs

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

Figure 11-4 Alarm

Please keep unencrypted files well to avoid data leakage.				
Export				
No.	Room No.	Event	Channel	Start Time
1	8001	Tamper	1	2023-07-11 02:00:53
2	8001	Tamper	1	2023-07-07 10:07:18
3	8001	Tamper	1	2023-07-06 22:16:19
4	8001	Tamper	1	2023-07-06 22:09:52
5	8001	Tamper	1	2023-07-04 02:00:49
6	8001	Tamper	1	2023-06-29 16:29:49
7	8001	Tamper	1	2023-06-29 16:26:59
8	8001	Tamper	1	2023-06-29 15:22:09
9	8001	Tamper	1	2023-06-29 15:22:08
10	8001	Tamper	1	2023-06-27 14:07:57

12 records

< 1 2 > 10 / page Go to Page

11.4.3 Unlock Records

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

Figure 11-5 Unlock Records

Please keep unencrypted files well to avoid data leakage.

ExportTime Range29-05-2025 00:00:00 → 30-05-2025 00:00:00Search

No.	Unlock Method	VTO ID	Person ID	Room No.	Username	Card	Lock	Unlock Results	Unlock Time
1	Card Swipe Unlock	8004				FBFA192A	Local Lock	Failed	2024-10-21 11:13:42
2	Card Swipe Unlock	8004				FBFA192A	Local Lock	Failed	2024-10-21 11:13:37
3	Card Swipe Unlock	8004				FBFA192A	Local Lock	Failed	2024-10-21 11:13:36
4	Card Swipe Unlock	8004				FBFA192A	Local Lock	Failed	2024-10-21 11:13:35
5	Card Swipe Unlock	8004				FBFA192A	Local Lock	Failed	2024-10-21 11:13:33
6	Card Swipe Unlock	8004				FBFA192A	Local Lock	Failed	2024-10-21 11:13:31
7	Card Swipe Unlock	8004				FBFA192A	Local Lock	Failed	2024-10-21 11:13:30
8	Card Swipe Unlock	8004				FBFA192A	Local Lock	Failed	2024-10-21 11:13:29
9	Card Swipe Unlock	8004				FBFA192A	Local Lock	Failed	2024-10-21 11:13:27
10	Card Swipe Unlock	8004				FBFA192A	Local Lock	Failed	2024-10-21 11:13:25

1000 records12345...10010 / pageGo toPage

11.4.4 Log

Select **Maintenance Center > Log > Log**.
Select time range and type, and then you can see all the log information.

Figure 11-6 Log

Please keep unencrypted files well to avoid data leakage.

Time Range2023-07-10 00:00:00 → 2023-07-11 00:00:00TypeAllSearchReset

☐ Encrypt Log BackupExport

No.	Time	Type	Log Content
<div>No Data</div>			

11.5 Maintenance Management

11.5.1 Config

You can export and import the configuration file.
Procedure

- Step 1
- Select **Maintenance Center > Maintenance Management > Config**.
- Step 2
- Click **Export Configuration File**, or click **Browse** to select the file from local computer, and then click **Import file**.

Figure 11-7 Config

The screenshot shows a web interface titled "Config". It contains a button labeled "Export Configuration File". Below this, there is a "File" label followed by a text input field, a "Browse" button, and an "Import File" button. At the bottom, a yellow warning box contains the text: "Imported configuration will overwrite previous configuration."

11.5.2 Maintenance

Procedure

- Step 1 Select **Maintenance Center > Maintenance Management > Maintenance**.
- Step 2 Configure the auto maintenance time.

Figure 11-8 Auto maintenance

The screenshot shows a web interface titled "Maintenance". Under the "Auto Maintenance" section, there is a "Maintenance Time" label followed by a dropdown menu showing "Tue" and a time dropdown showing "02:00". Below these, there are two buttons: "Apply" and "Refresh".

- Step 3 Click **Apply**.

11.6 Update

Procedure

- Step 1 Select **Maintenance Center > Update**.
- Step 2 Select ways to check the update.
- **File Update** : Click **Browse** to add the updating file, and then click **Update**.
 - **Online Update**
 - ◇ **Auto Check for Updates** : Enable the function to check automatically whether there is a new system version.
 - ◇ **Manual Check** : Select the function to check whether there is a new system version.

Figure 11-9 Online update

Online Update

Auto Check for Updates ☐

Manual Check

System Version: 4
You are using the latest version. **Update Now**

11.7 Advanced Maintenance

Export

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

Packet Capture

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

Figure 11-10 Packet capture

Packet Capture							
NIC	Device Address	IP 1: Port 1		IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Back...
eth0	<input type="text"/>	<input type="text" value="Optional"/>	<input type="text" value="Optional"/>	<input type="text" value="Optional"/>	<input type="text" value="Optional"/>	0.00MB	►
lo	<input type="text"/>	<input type="text" value="127.0.0.1"/>	<input type="text" value="Optional"/>	<input type="text" value="Optional"/>	<input type="text" value="Optional"/>	0.00MB	►

Network Test

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

Figure 11-11 Test network

Network Test

Destination Address

11112

Test

Data Packet Size

64

Byte (64-4096)

Test Result

PING 11112 64(92) bytes of data.
72 bytes from 11112: icmp_seq = 1 ttl = 123 time = 2 ms
72 bytes from 11112: icmp_seq = 2 ttl = 123 time < 1 ms
72 bytes from 11112: icmp_seq = 3 ttl = 123 time = 1 ms
72 bytes from 11112: icmp_seq = 4 ttl = 123 time = 1 ms
72 bytes from 11112: icmp_seq = 5 ttl = 123 time = 1 ms
72 bytes from 11112: icmp_seq = 6 ttl = 123 time = 1 ms
72 bytes from 11112: icmp_seq = 7 ttl = 123 time = 1 ms
72 bytes from 11112: icmp_seq = 8 ttl = 123 time = 1 ms
72 bytes from 11112: icmp_seq = 9 ttl = 123 time = 1 ms
72 bytes from 11112: icmp_seq = 10 ttl = 123 time = 1 ms
72 bytes from 11112: icmp_seq = 11 ttl = 123 time = 2 ms

Copy

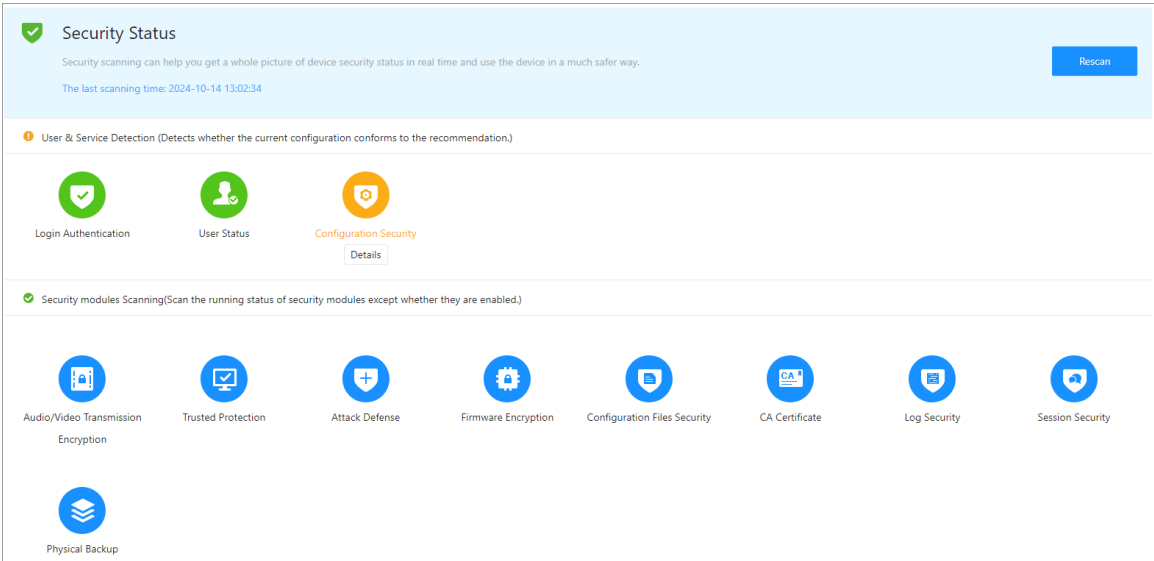
Round Time Used: Min = 0 ms, Max = 2 ms, Average = 1.091 ms

12 Security Management

12.1 Security Status

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

Figure 12-1 Security status

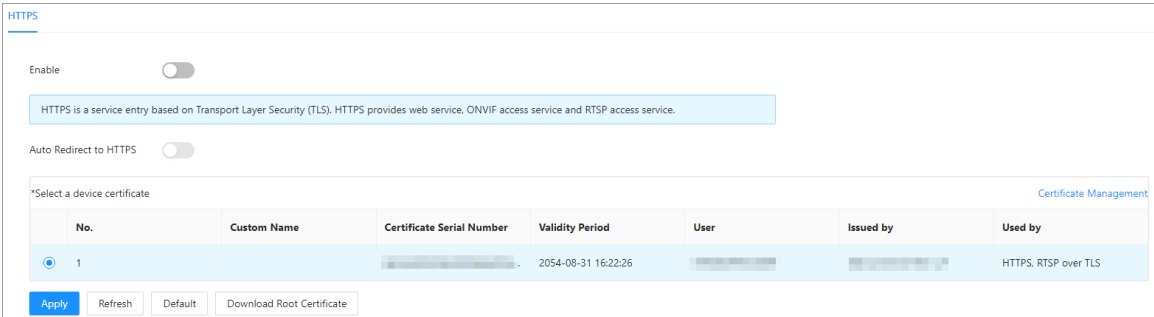


12.2 System Service

Procedure

- Step 1** On the home page, click , and then select **System Service**.
- Step 2** Select a device certificate, and then enable the HTTPS function.

Figure 12-2 System service




- Step 3** Click **Apply**.

12.3 Attack Defense

12.3.1 Firewall

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

Procedure

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

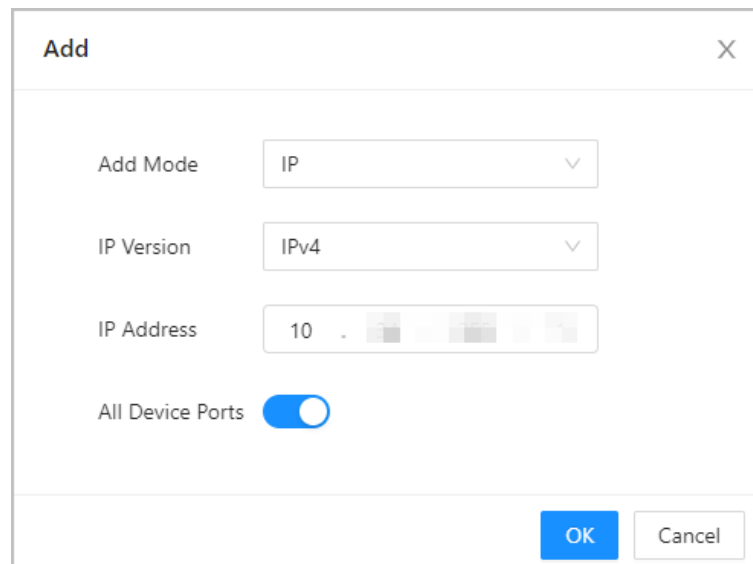
Step 2 Click ☐ next to **Enable**.

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

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

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

Figure 12-3 Add



The 'Add' dialog box is used to configure firewall rules. It contains the following fields and controls:

- Add Mode:** A dropdown menu currently set to 'IP'.
- IP Version:** A dropdown menu currently set to 'IPv4'.
- IP Address:** A field with a text input showing '10' followed by a series of boxes for the remaining octets of the IP address.
- All Device Ports:** A toggle switch that is currently turned on (blue).
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Step 5 Click **OK**.

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

Figure 12-4 Apply

The screenshot shows the 'Firewall' configuration page. At the top, there are tabs for 'Firewall', 'Account Lockout', and 'Anti-DoS Attack'. The 'Firewall' tab is active. Below the tabs, there is an 'Enable' toggle switch which is currently turned off. Under the 'Mode' section, the 'Allowlist' radio button is selected, and the 'Blocklist' radio button is unselected. A light blue box contains the text: 'Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.' Below this box are 'Add' and 'Delete' buttons. A table with the following columns is shown: 'No.', 'Host IP/MAC', 'Port', and 'Operation'. The table contains one record with 'No.' 1, 'Host IP/MAC' 12, and 'Port' All Device Ports. Below the table, it says 'Total 1 records'. At the bottom, there are 'Apply', 'Refresh', and 'Default' buttons. A pagination control shows '1' of 1 records.

12.3.2 Account Lockout

Procedure


- Step 1** On the home page, click , and then select **Attack Defense** > **Account Lockout**.
- Step 2** Configure the login attempts and lock time for device account and ONVIF user.

Figure 12-5 Account lockout

The screenshot shows the 'Account Lockout' configuration page. At the top, there are tabs for 'Firewall', 'Account Lockout', and 'Anti-DoS Attack'. The 'Account Lockout' tab is active. Below the tabs, there are two sections: 'Device Account' and 'ONVIF User'. Each section has 'Login Attempt' and 'Lock Time' settings. For 'Device Account', 'Login Attempt' is set to '5time(s)' and 'Lock Time' is set to '5 min'. For 'ONVIF User', 'Login Attempt' is set to '30time(s)' and 'Lock Time' is set to '5 min'. At the bottom, there are 'Apply', 'Refresh', and 'Default' buttons.

- Step 3** Click **Apply**.

12.3.3 Anti-DoS Attack

Procedure


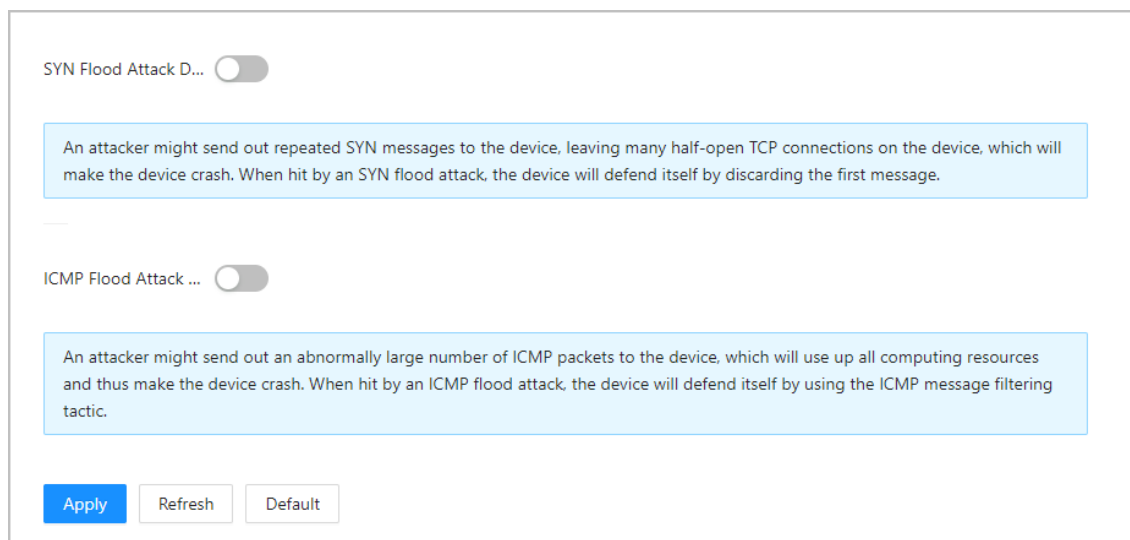
- Step 1** On the home page, click , and then select **Attack Defense > Anti-DoS Attack**.
- Step 2** Enable or disable the **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** function.

Figure 12-6 Anti-DoS attack



SYN Flood Attack D... ☐

An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.

ICMP Flood Attack ... ☐

An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

[Apply](#) [Refresh](#) [Default](#)

- Step 3** Click **Apply**.

12.4 CA Certificate

Procedure


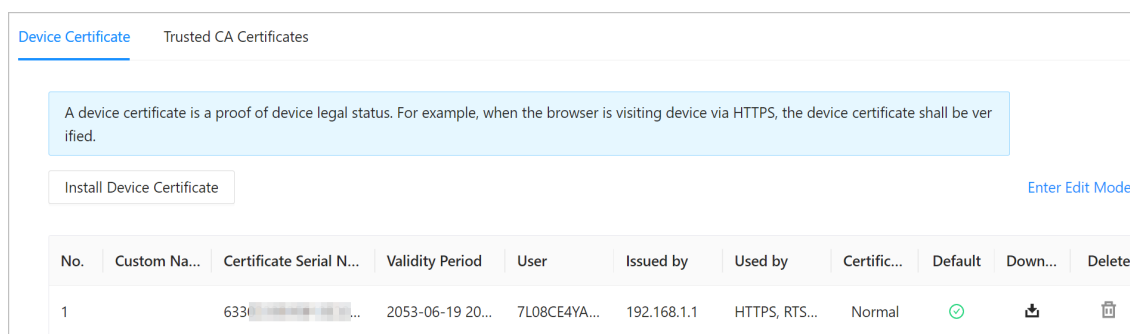
- Step 1** On the home page, click , and then select **CA Certificate**.
- Device Certificate



Figure 12-7 Device certificate



[Device Certificate](#) [Trusted CA Certificates](#)

A device certificate is a proof of device legal status. For example, when the browser is visiting device via HTTPS, the device certificate shall be verified.

[Install Device Certificate](#) [Enter Edit Mode](#)

No.	Custom Na...	Certificate Serial N...	Validity Period	User	Issued by	Used by	Certific...	Default	Down...	Delete
1		6330...	2053-06-19 20...	7L08CE4YA...	192.168.1.1	HTTPS, RTS...	Normal	<input checked="" type="checkbox"/>		

- Trusted CA Certificates

Figure 12-8 Trusted CA certificates

Device Certificate [Trusted CA Certificates](#)

A trusted CA certificate is used to verify the legal status of a host. For example, a switch CA certificate shall be installed for 802.1x authentication.

[Install Trusted Certificate](#) [Enter Edit Mode](#)

No.	Custom Na...	Certificate Serial Nu...	Validity Period	User	Issued by	Used by	Certificate ...	Downlo...	Delete
1		3231...	2027-10-16 23:...	192.168.1.1	192.168.1.1		Normal		

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

[Encrypted Transmission](#)

Private Protocol

Enable ☐

Stream transmission is encrypted by using private protocol.

*Please make sure that the corresponding device or software supports video decryption.

Encryption Type: AES256-OFB

Update Period: 12 hr (0-720)

RTSP over TLS

Enable ☒

RTSP stream is encrypted by using TLS tunnel before transmission.

*Please make sure that the corresponding device or software supports video decryption.

*Select a device certificate [Certificate Management](#)

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1		63303339356133326136313...	2053-06-19 20:06:37	7L08CE4YA0804A5	192.168.1.1	HTTPS, RTSP over TLS

[Apply](#) [Refresh](#) [Default](#)

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


Enable ☐

Event Monitoring

 Invalid executable programs attempting to run

 Session ID bruteforcing

 Web directory bruteforcing

 Number of session connections exceeds limit

Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

Apply

Refresh

Default

12.7 Security Authentication

Procedure

- Step 1

On the home page, click , and then select **Security Authentication**.
- Step 2

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

Figure 12-11 Security authentication

Digest Algorithm for Authentication

Digest Algorithm for User Authentication

☒ MD5

☐ SHA256

Digest Algorithm for ONVIF User Authentication

☒ MD5

☐ SHA256

Apply

Refresh

Default

Appendix 1 Security Recommendation

Account Management

1. Use complex passwords

Please refer to the following suggestions to set passwords:

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

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account logout function

The account logout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

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

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. Turn off non-essential services and use safe mode

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

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

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

4. Change HTTP and other default service ports

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

Network Configuration

1. **Enable Allow list**

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

2. **MAC address binding**

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

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

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

Security Auditing

1. **Check online users**

It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

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

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

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

2. **Update client software in time**

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

Physical Protection

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

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