

Modular Door Station

Quick Start Guide



Foreword

General

This document mainly introduces product function, structure, networking, mounting process, debugging process, and web operations of the modular door station (hereinafter referred to as "VTO").

Models

VTO4202F-MK, VTO4202F-MB1, VTO4202F-MB2, VTO4202F-MB5, VTO4202F-MR, VTO4202F-MS, VTO4202F-MF, VTO4202F-ML, VTO4202F-MA, VTO4202F-P, and VTO4202F-P-S2.

Device Update

Power supply can be cut off only after the device has completed update and restarted.

Safety Instructions

The following categorized signal words with defined meaning 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, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	December, 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.

- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The following description is the correct application method of the VTO. Read the manual carefully before use, in order to prevent danger and property loss. Strictly conform to the manual during application and keep it properly for future reference.

Operating Requirements

- Do not expose the device to direct sunlight or heat source.
- Do not install the device in a humid or dusty area.
- Install the device at stable places horizontally to prevent it from falling.
- Do not drip or splash liquids on the device, or put on the device anything filled with liquids.
- Install the device at well-ventilated places and do not block its vent.
- Use the device only within rated input and output range.
- Do not dismantle the device by yourself.
- Transport, use and store the device within allowed humidity and temperature range.

Power Requirements

- Use electric wires recommended in your area, and within their rated specification.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, see the label on the device.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Overview	1
1.1 Introduction	1
1.2 Features	1
2 Structure	2
2.1 Camera Module	2
2.2 Indicator Module.....	3
2.3 Audio Module.....	4
2.4 Button Module.....	5
2.5 Keyboard Module (with Braille)	6
2.6 Card Module.....	6
2.7 Fingerprint Module	7
2.8 Display Module	7
2.9 Blank Module.....	8
2.10 Cascade Connection.....	8
3 Configuration and Commissioning	9
3.1 Procedure	9
3.2 Configuring VTO	9
3.2.1 Initialization	9
3.2.2 Configuring VTO Number	10
3.2.3 Configuring Network Parameters.....	11
3.2.4 Configuring SIP Servers	11
3.2.5 Adding VTO	13
3.2.6 Adding Room Number.....	14
3.2.7 Configuring the Module.....	17
3.3 Commissioning	19
3.3.1 VTO Calling VTH.....	19
3.3.2 VTH Monitoring VTO.....	19
Appendix 1 Cybersecurity Recommendations	21

1 Overview

1.1 Introduction

You can build up the modular VTO with different modules, including the camera module, indicator module, button module, keyboard module, card module, fingerprint module, audio module, and display module. The camera and audio modules are indispensable, and the other ones can be added as needed.

1.2 Features

- Video call: Make video calls to indoor monitors (VTHs).
- Group call: Call multiple VTHs simultaneously.
- Video monitoring: Up to 6 VTHs can view the monitoring image of this VTO at the same time.
- Emergency call: Call the management center during an emergency.
- Unlock: Card, fingerprint, password and remote unlock.
- Alarm: Anti-tampering alarm, door contact alarm and duress password unlock alarm. Alarm information will be sent to the management center.
- Record search: Call records, alarm records and unlock records.

2 Structure

2.1 Camera Module

Figure 2-1 Front panel

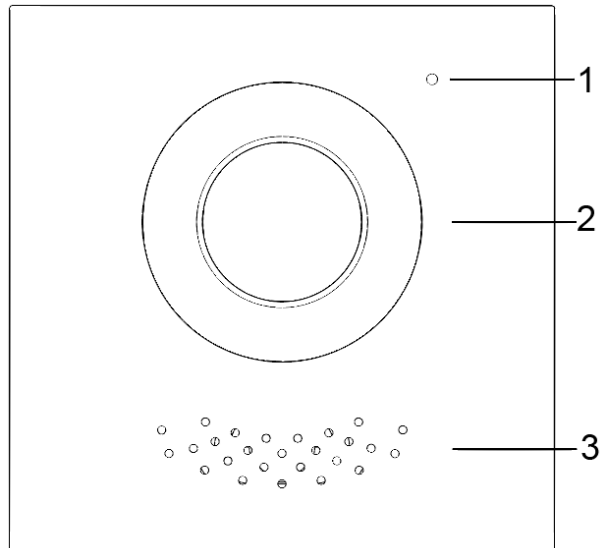


Table 2-1 Front panel description

No.	Name
1	Microphone
2	Camera
3	Speaker

Figure 2-2 Rear panel

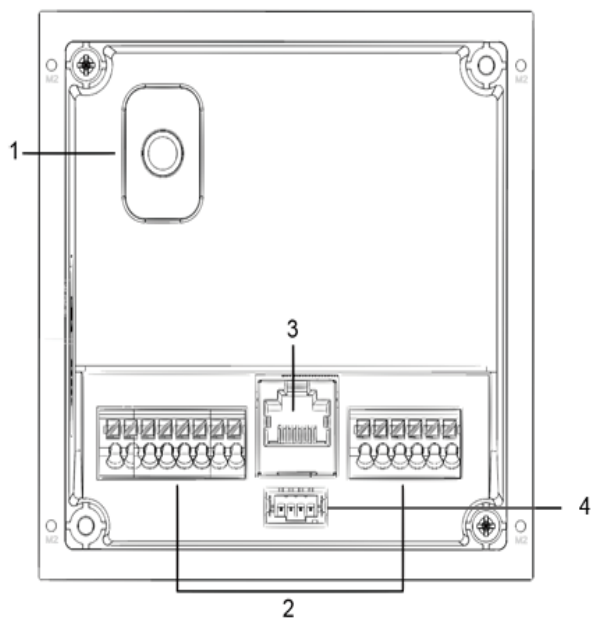


Table 2-2 Rear panel description

No.	Name	Description
1	Anti-tampering switch	When the VTO is removed from the wall forcibly, an alarm will be triggered and the alarm information will be sent to management center.
2	Ports	Connect to power supply, electric control lock, solenoid lock and exit button.
3	Ethernet port	Connect to network cables.
4	Cascade connection port	Connect to other modules.

Figure 2-3 Ports description

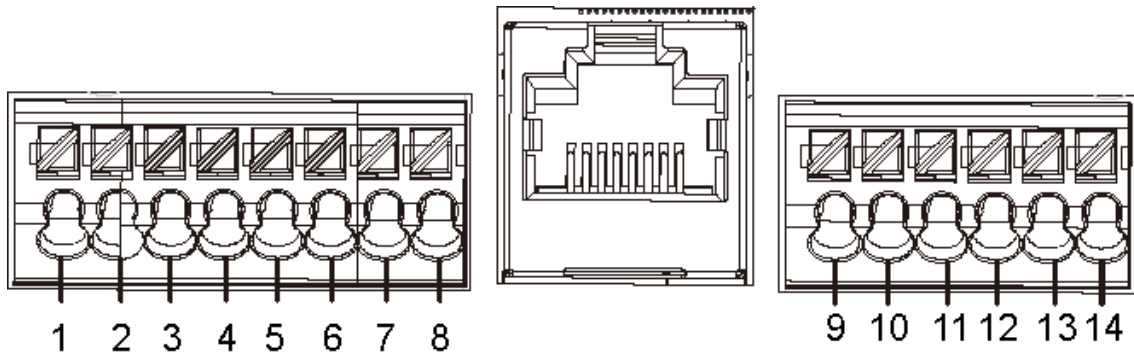


Table 2-3 Port description

No.	Description	No.	Description
1	GND	8	EOC1 (2wires -(GND) for a 2-wire 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	EOC2 (2wires +(48V) for a 2-wire camera module)	14	DOOR_NO

2.2 Indicator Module

Figure 2-4 Front panel

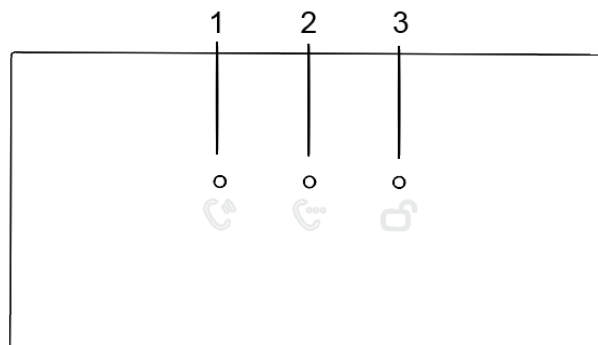


Table 2-4 Indicator module description (1)

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

Figure 2-5 Rear panel of indicator module

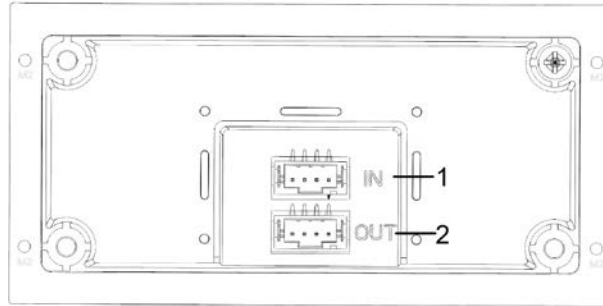


Table 2-5 Indicator module description (2)

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

2.3 Audio Module



The rear panel of audio module is the same as the camera module.

Figure 2-6 Audio module

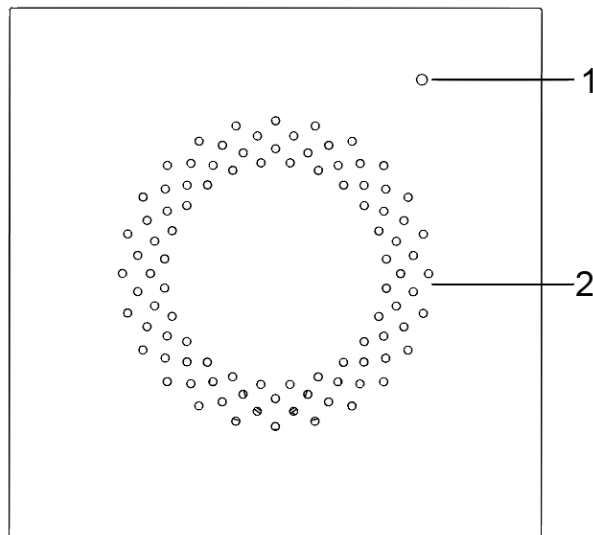


Table 2-6 Audio module description

No.	Name
1	Microphone
2	Speaker

2.4 Button Module

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

Figure 2-7 Front panel of the five-button module

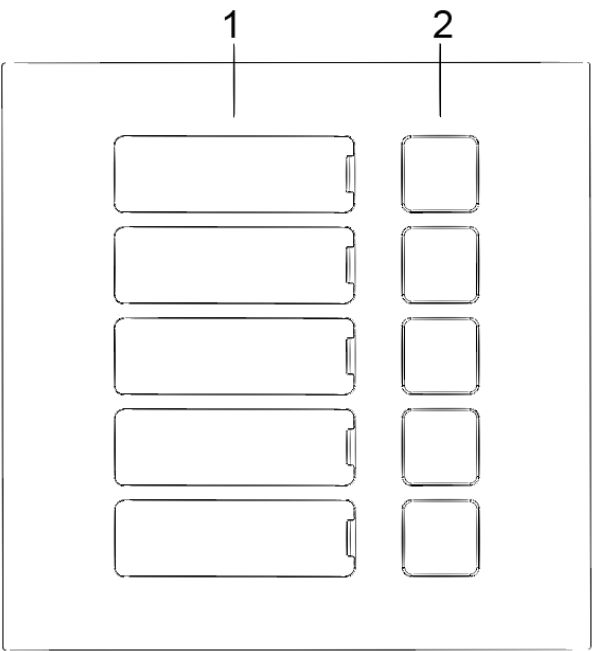


Table 2-7 Front panel description

No.	Name	Description
1	User directory	Put name cards here.
2	Call buttons	Call other VTHs or the management center.  Configure related parameters on the web interface first.

Figure 2-8 Rear panel of the five-button module

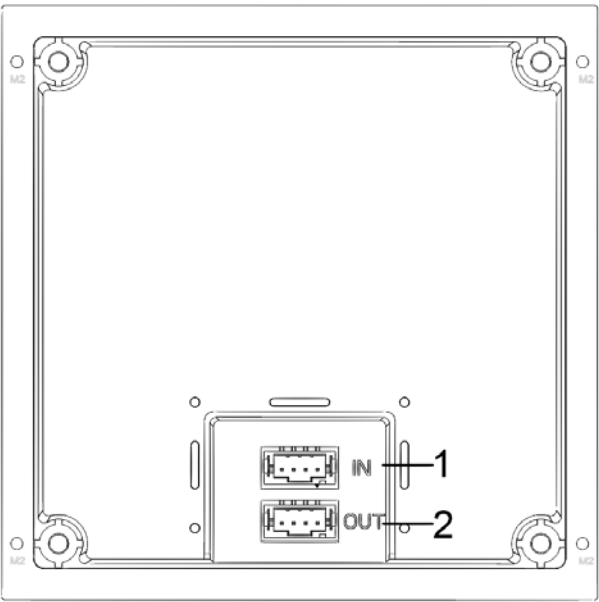


Table 2-8 Rear panel description

No.	Name
1	Cascade input
2	Cascade output

2.5 Keyboard Module (with Braille)



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

Figure 2-9 Keyboard module

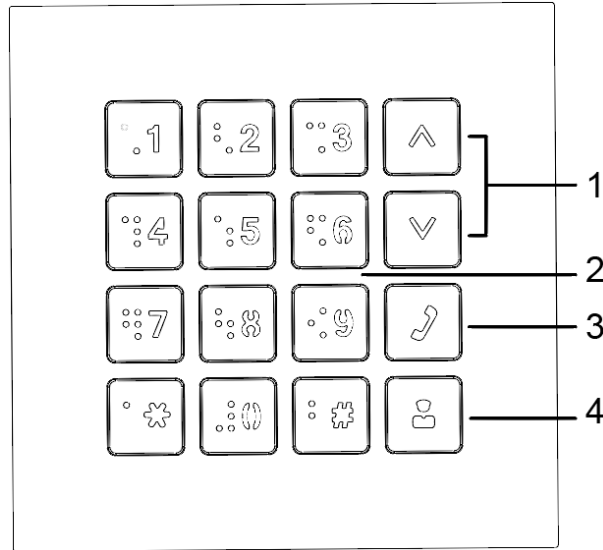


Table 2-9 Keyboard module description

No.	Name	Description
1	Selection	—
2	Numbers	Enter password or VTH numbers.
3	Call	Call VTHs.
4	Call management center	—

2.6 Card Module

Swipe your card near the icon.



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

Figure 2-10 Card module



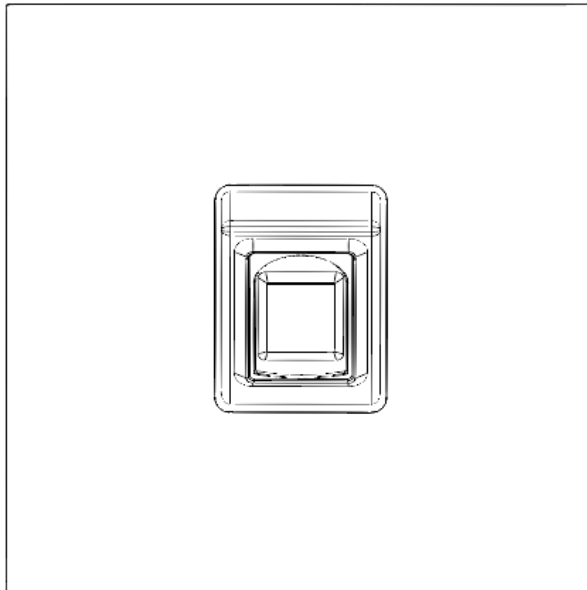
2.7 Fingerprint Module

Collects and verifies fingerprints.



The rear panels of fingerprint module and button module have different port positions, but port functions are the same.

Figure 2-11 Fingerprint module



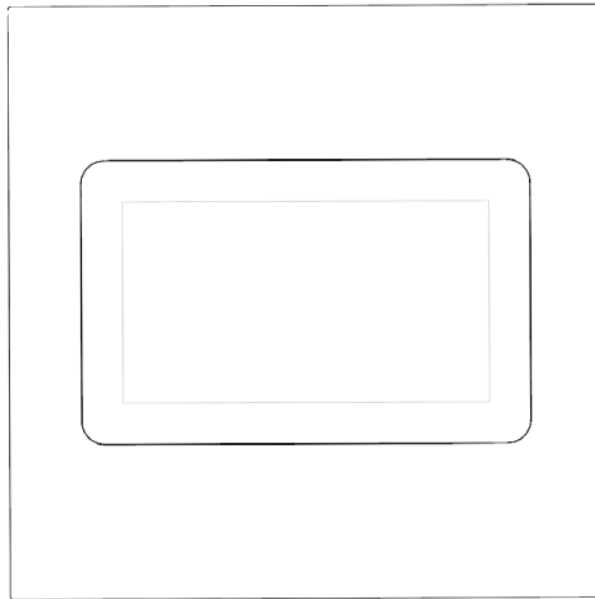
2.8 Display Module

Displays user information.



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

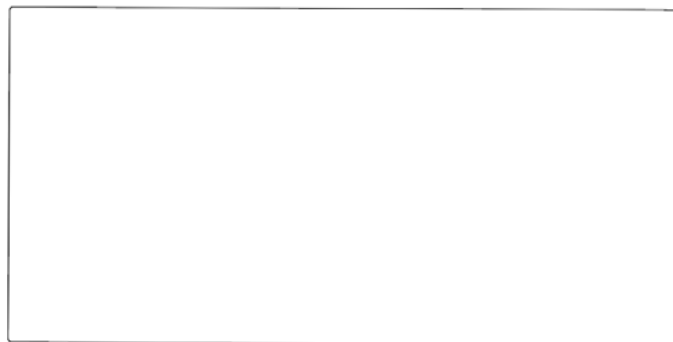
Figure 2-12 Display module



2.9 Blank Module

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

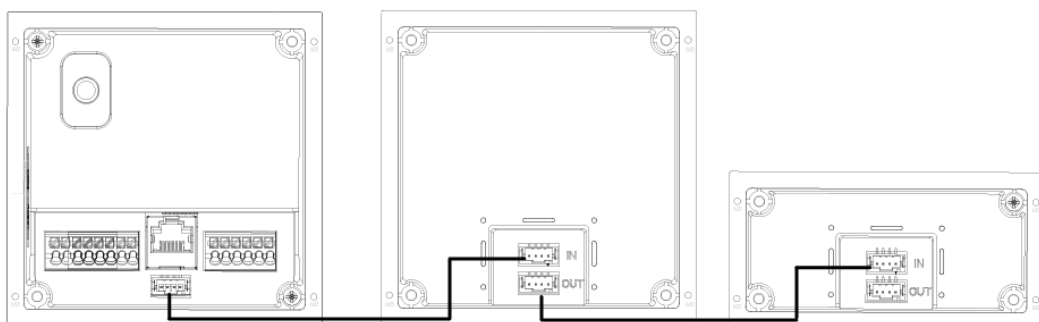
Figure 2-13 Blank module



2.10 Cascade Connection

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

Figure 2-14 Cascade connection example



3 Configuration and Commissioning

This chapter introduces basic configurations to the VTO and VTH devices.



Interface and function might vary with the device type you configured for the VTO. The actual interface and function shall prevail.

3.1 Procedure



Before configuration, make sure that there is no short or open circuit.

Step 1 Plan IP and unit/room number (works as a phone number) for each device.

Step 2 Configure the VTO. See "3.2 Configuring VTO."

Step 3 Configure the VTH. See the VTH user's manual.

Step 4 Check if all settings are correct. See "3.3 Commissioning."

3.2 Configuring VTO

Connect the VTO to your PC with a network cable, and for first-time login, you need to create a new password for the web interface.

3.2.1 Initialization

Step 1 Power on the VTO.

Step 2 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 changing the default IP address (**Network > Basic**) to avoid conflict.

Figure 3-1 Device initialization

The 'Device Init' window has a dark background. At the top, a progress bar shows three steps: '1 One' (highlighted in blue), '2 Two', and '3 Three'. Below the progress bar, the 'Username' is set to 'admin'. There is a 'Password' input field followed by three buttons: 'Low', 'Middle', and 'High'. Below these is a 'Confirm Password' input field. At the bottom center is a 'Next' button.

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

Step 4 Select **Email**, enter an email address for resetting password, and then click **Next**.

Step 5 Click **OK**. The system goes to the login interface.

3.2.2 Configuring VTO Number

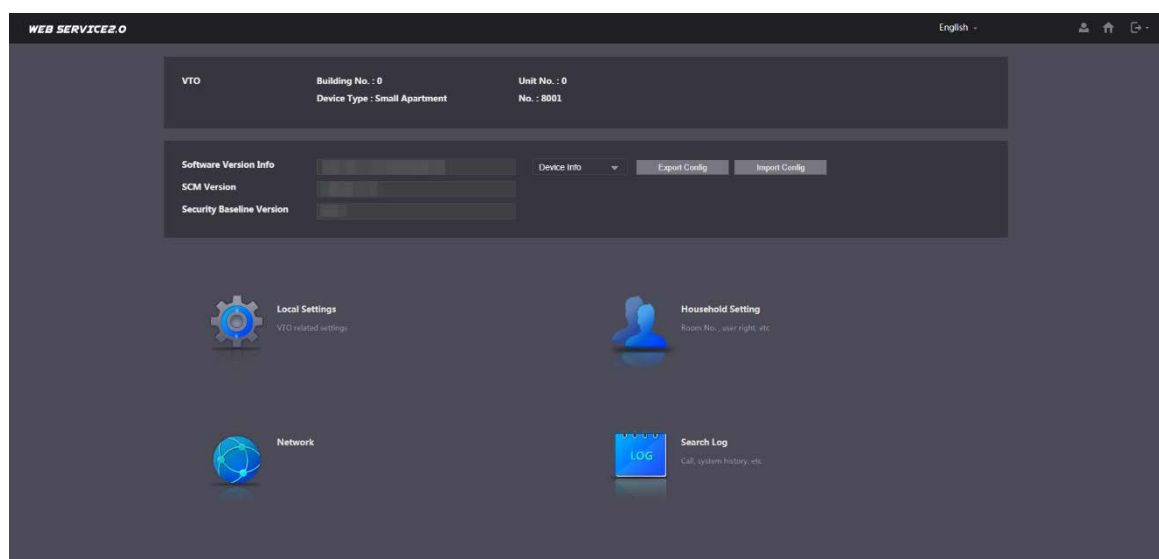
Numbers can be used to distinguish each VTO, and we recommend setting it according to unit or building number.



You can change the number of a VTO when it is not working as the SIP server. A VTO number can contain 5 numbers at most, and it cannot be the same with any room number.

Step 1 Log in to the VTO web interface.

Figure 3-2 Main interface



Step 2 Select **Local Settings > Basic**.

Figure 3-3 Device properties

Step 3 Enter the number in **No.**, and then click **Save**.

3.2.3 Configuring Network Parameters

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

Figure 3-4 TCP/IP information

Step 2 Enter the parameters and click **Save**.

The VTO will automatically restart. You need to change the IP address of your PC to the same network segment as the VTO to log in again.

3.2.4 Configuring SIP Servers

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



- If the current VTO is the SIP server, **Building No.** and **Unit No.** will not be displayed on the **Device Properties** interface.
- If you go to **Network Setting** > **SIP Server**, enable **Alternate Server** and log in to the web interface again, **Building No.** and **Unit No.** will be displayed on the **Device Properties** interface.

Step 1 Log in to the web interface.

Step 2 Select **Network** > **SIP Server**.

Figure 3-5 SIP server

Step 3 Select a SIP server.

- VTO as SIP Server: This is applicable to only one building.
 - 1) Enable **SIP Server**.
 - 2) Select **Server Type** as **VTO**.
 - 3) Configure the parameters. See Table 3-1.
 - 4) Click **Save**. The VTO will restart automatically.
- Platform (Express/DSS) as SIP server: This is applicable to multiple buildings or units. If you do not have a platform, use a VTO as the SIP server.
 - 1) Disable **SIP Server**.
 - 2) Select **Server Type** to **Express/DSS**.
 - 3) Configure the parameters.

Table 3-1 SIP server parameter description

Parameter	Description
IP Address	IP address of the SIP server.  If Alternate Server is not enabled, the VTO cannot call the VTS.
Port	● 5060 by default when VTO work as SIP server. ● 5080 by default when the platform works as SIP server.
Username/Password	Keep it default.
SIP Domain	● Must be VDP when VTO works as SIP server. ● Keep it null or default when the platform works as SIP server.
SIP Server Username/Password	Used to log in to the SIP server.
Alternate IP Addr.	IP address of the alternate server.
Alternate Username	Alternate server login username and password.
Alternate Password	
Alternate VTS IP Addr.	IP address of the alternate VTS.
Alternate Server	● After entering alternate IP address, username, password, and VTS IP address, you need to enable Alternate Server. ● After Alternate Server is enabled, you can only enter the VTS IP address, and the VTO will restart.

Step 4 Click **OK**, and the VTO will restart automatically.



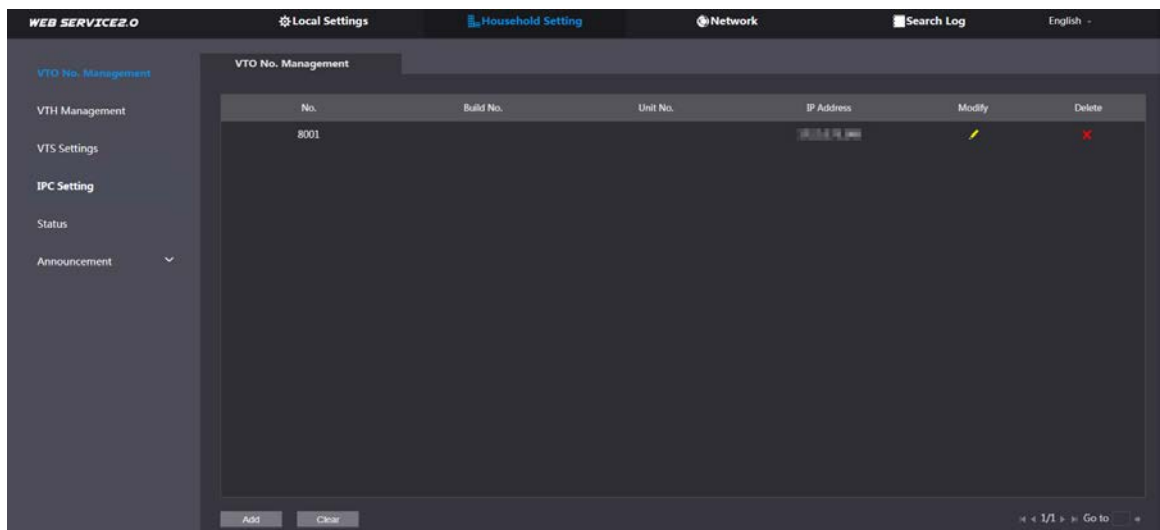
When a platform works as the SIP server, enable **Support Building** and **Support Unit** first if it is necessary to set building number and building unit number.

3.2.5 Adding VTO

You can add VTO devices to the SIP server, and all the VTO devices connected to the same SIP server can make video call between each other. This section is applicable when a VTO device works as SIP server, and if you are using other servers as SIP server, see the corresponding manual for the detailed configuration.

Step 1 Log in to the web interface of the SIP server, and then select **Household Setting > VTO No. Management**.

Figure 3-6 VTO number management



Step 2 Click **Add**.

Figure 3-7 Add VTO

Step 3 Configure the parameters.



The SIP server must be added.

Table 3-2 Add VTO

Parameter	Description
Rec No.	VTO number. See "3.2.2 Configuring VTO Number."
Register Password	Keep it default.
Build No.	Available only when other servers work as SIP server.
Unit No.	
IP Address	VTO IP address.
Username	VTO web interface login username and password.
Password	

Step 4 Click **Save**.

3.2.6 Adding Room Number

You can add the planned room number to the SIP server, and then configure the room number on VTH devices to connect them to the network. This section is applicable when the VTO works as the SIP server, and if you use other servers as SIP server, see the corresponding manual of the servers for detailed configuration.

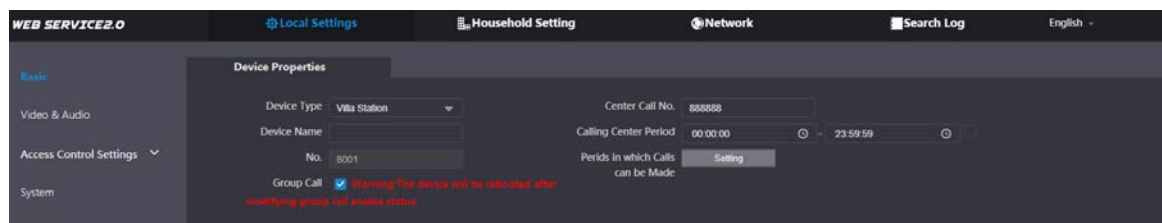


The room number can contain at most 6 digits of numbers or letters or their combination, and it cannot be the same as any VTO number.

Using the VTO in a Villa

Step 1 Log in to the web interface of the SIP server, and then select **Local Settings > Basic**.

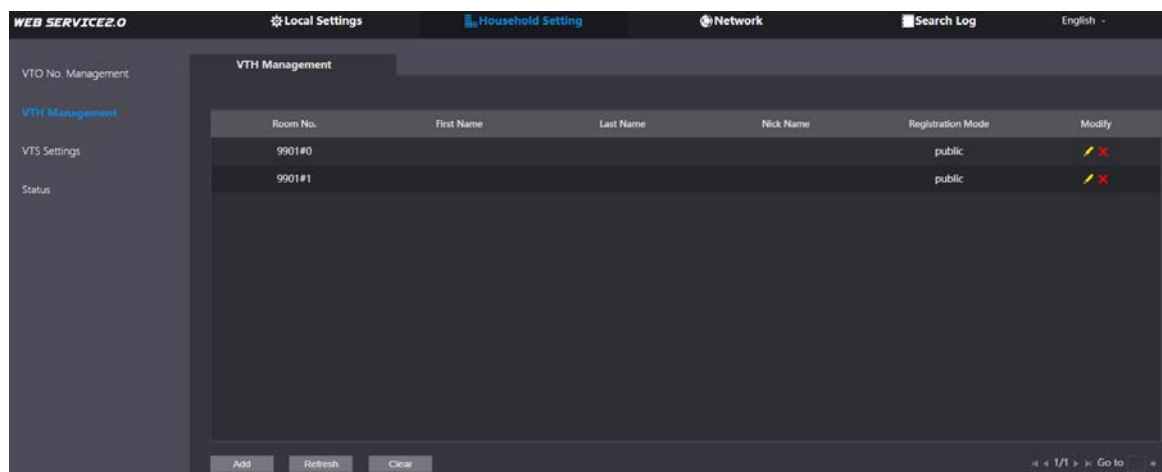
Figure 3-8 Device properties



Step 2 Set **Device Type** to **Villa Station**, and then click **Save**.

Step 3 Select **Household Setting > VTH Management**.

Figure 3-9 Room number management



Step 4 Click **Add**.

Figure 3-10 Add a single room number

Step 5 Configure the information on the left.

Table 3-3 Room information

Parameter	Description
First Name	Information used to differentiate each room.
Last Name	
Nick Name	
Room No.	- When there are multiple VTHs, the room number for the main VTH should end with #0, and the room numbers for sub VTHs with #1, #2... - You can have up to 10 sub VTHs for one main VTH.
Registration Type	Select public .
Registration Password	Keep it default.

Step 6 Click **Save**.



- Click  or  to modify or delete a room number.
- Click **Clear** to delete all room numbers.

Using the VTO in a Small Apartment

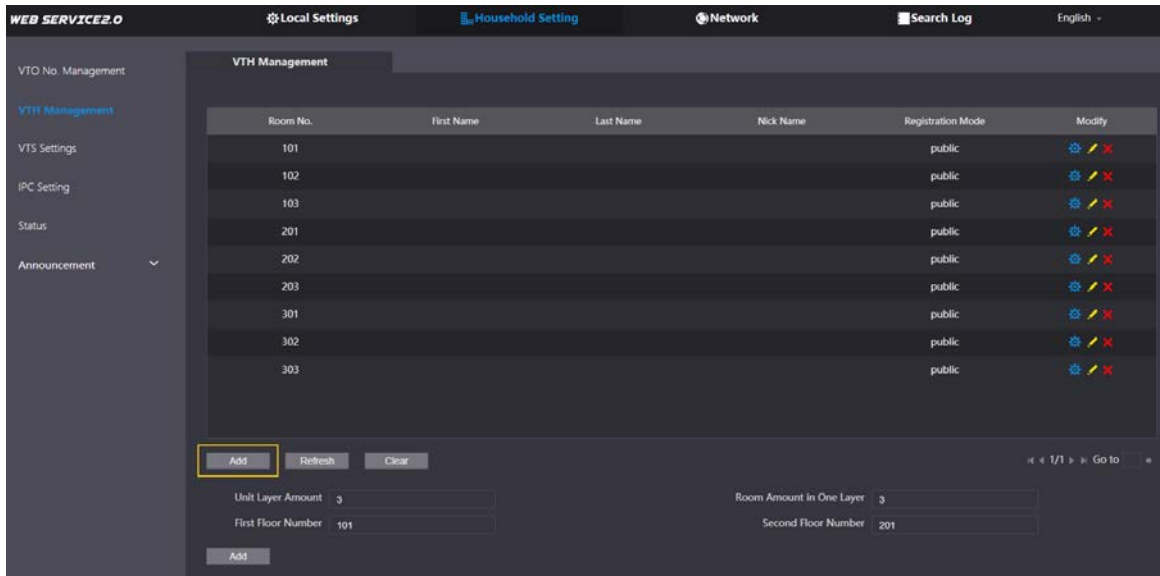
Step 1 Log in to the web interface of the SIP server, and then select **Local Settings > Basic**.

Figure 3-11 Device properties

Step 2 Set **Device Type** to **Small Apartment**, and then click **Save**.

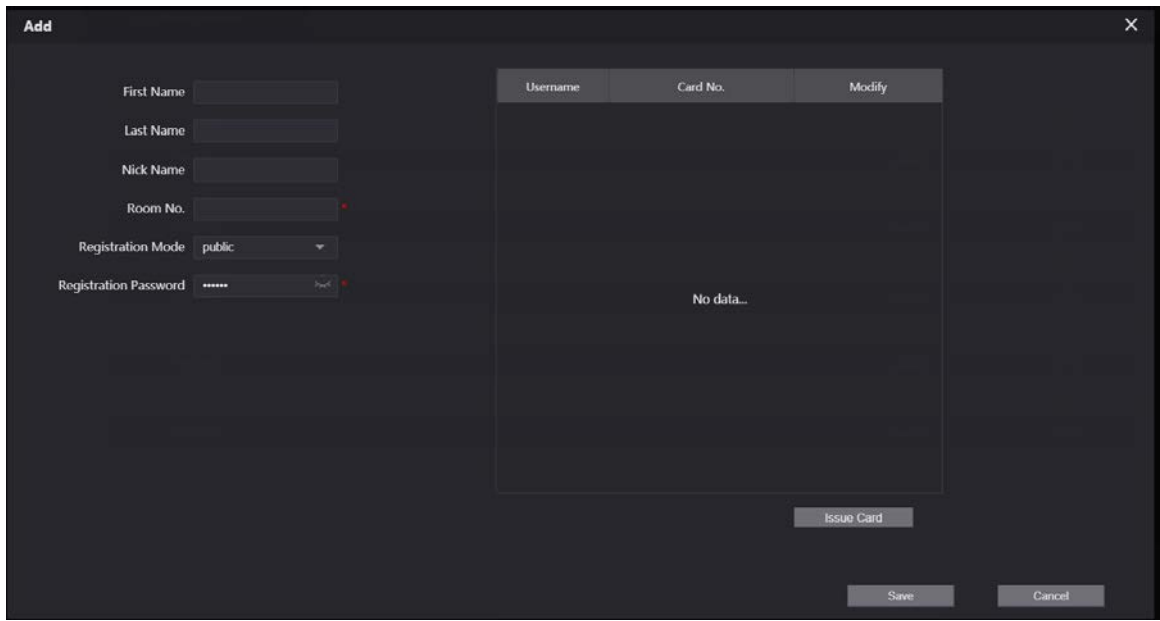
- Step 3** Select **Household Setting > VTH Management**. You can add a single room number or add them in batches.
- Add a single room number.

Figure 3-12 Add room numbers



- 1) Click **Add**.

Figure 3-13 Add a single room number



- 2) Configure the information on the left. See Table 3-3 for details.

- 3) Click **Save**.
- Add multiple room numbers.

Figure 3-14 Add room numbers in batches

- 1) Configure the information.
 - ◇ **Unit Layer Amount:** The number of floors in the apartment.
 - ◇ **Room Amount in One Layer:** The number of rooms in one floor.
 - ◇ **First Floor Number:** The first room number on the first floor.
 - ◇ **Second Floor Number:** The first room number on the second floor.
- 2) Click **Add**, and then click **Refresh** to view the latest status

 - Click  or  to modify or delete a room number.
 - Click **Clear** to delete all room numbers.

3.2.7 Configuring the Module

Camera module is added by default. All other modules need to be added in the facade layout before use.

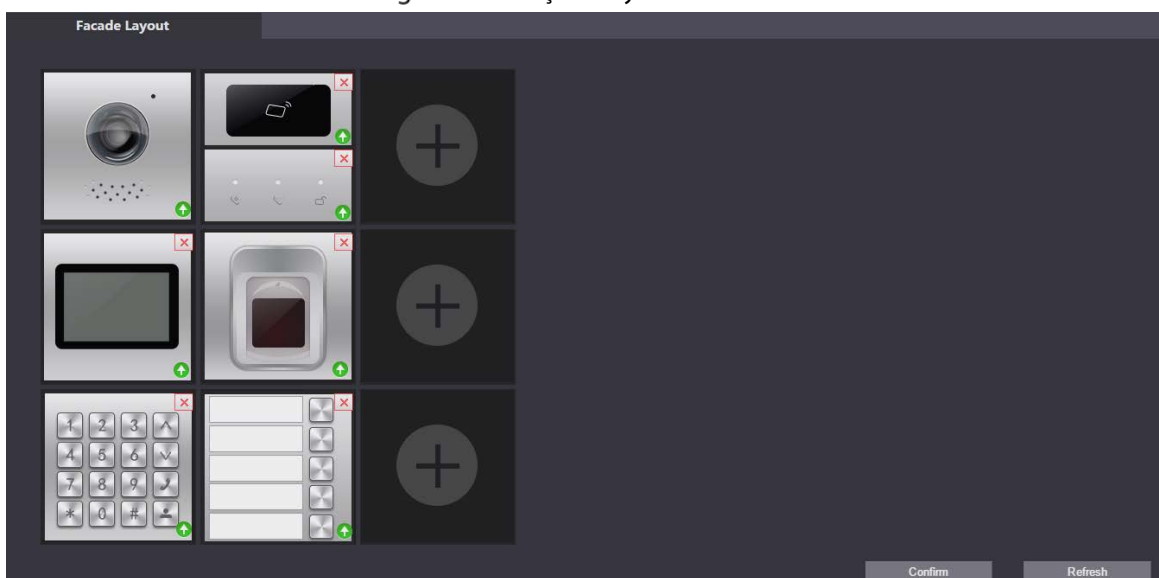


The VTO can have up to 9 functional modules. For fingerprint module, card module, and keyboard module, you can add only one of each type. For other modules, you can add as many as needed.

3.2.7.1 Adding Modules

Step 1 Select **Local Settings > Basic > Façade Layout**.

Figure 3-15 Façade layout



Step 2 Click , available modules will be displayed.



Keyboard module, card module, and fingerprint module will not be displayed if they have been added.

Step 3 Select modules according to the actual layout of the VTO.



The order must be from top to bottom and from left to right.

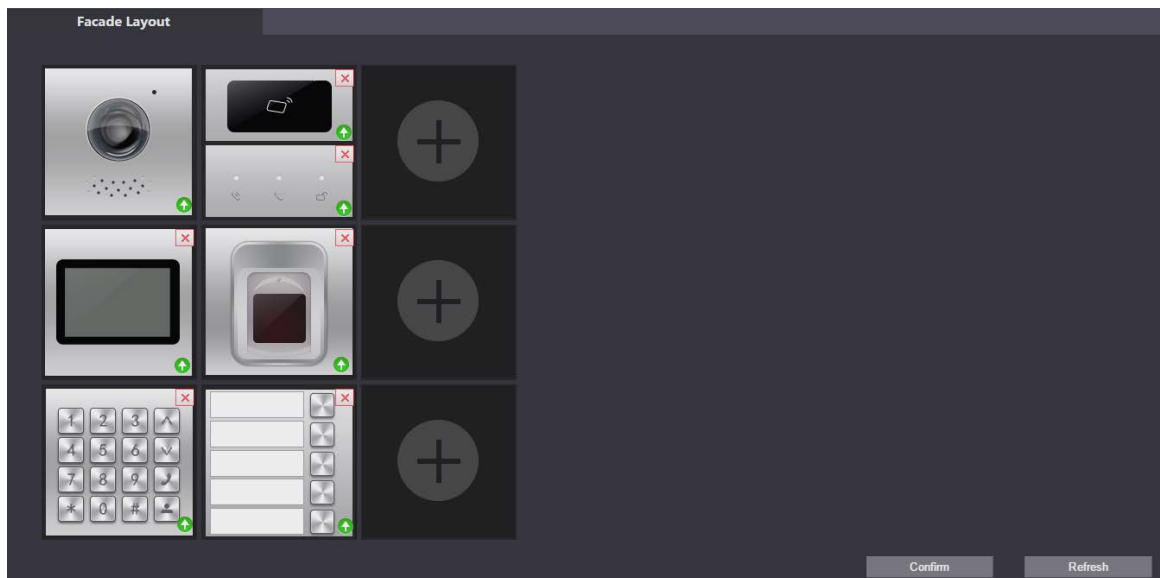
Step 4 Click **Confirm**, and then restart the browser to apply the changes.

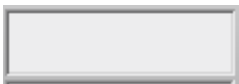
3.2.7.2 Configuring Modules

You need to configure room numbers for the button module.

Step 1 Select **Local Settings > Basic > Façade Layout**.

Figure 3-16 Configure the button module

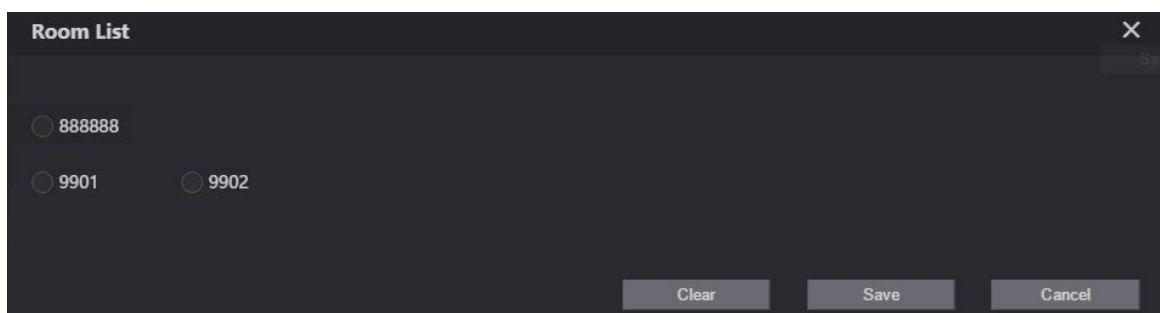


Step 2 Click .



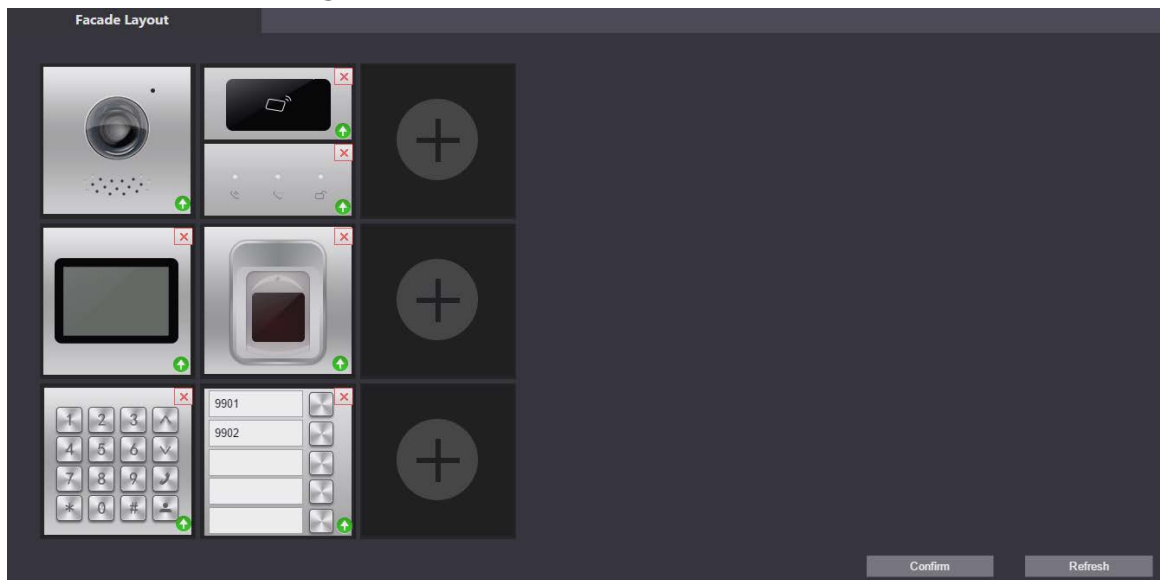
The room number displayed on the interface corresponds to the added VTH. "888888" is the number of the management center.

Figure 3-17 Room list



Step 3 Select the room number, and then click **Save**.

Figure 3-18 Room number information



Step 4 Click **Confirm**, and then restart the browser to apply the changes.

3.3 Commissioning

3.3.1 VTO Calling VTH

Step 1 Dial a room number on the VTO.

Step 2 Press .

Step 3 Tap  on the VTH to answer the call.

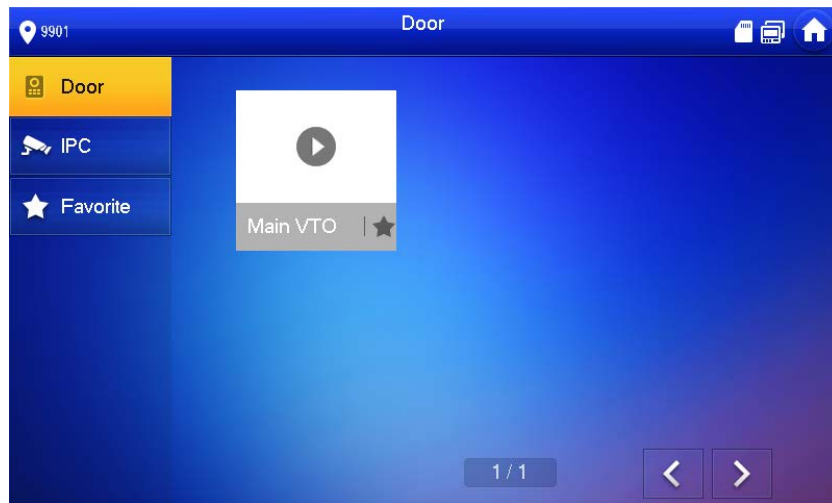
Figure 3-19 Call screen



3.3.2 VTH Monitoring VTO

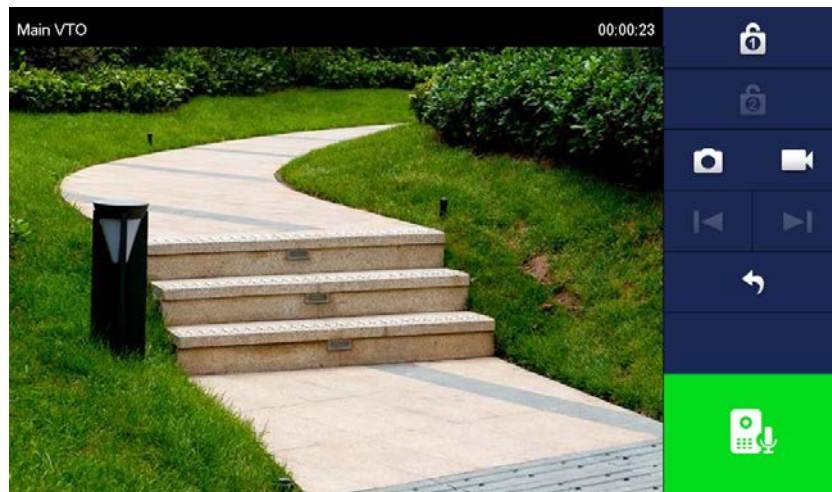
Step 1 On the VTH, select **Monitor > Door**.

Figure 3-20 Door



Step 2 Select the VTO that you want to monitor.

Figure 3-21 Monitoring video



Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

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

2. Update Firmware and Client Software in Time

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

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

1. Physical Protection

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

2. Change Passwords Regularly

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

3. Set and Update Passwords Reset Information Timely

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

4. Enable Account Lock

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

5. Change Default HTTP and Other Service Ports

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

6. Enable HTTPS

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

7. MAC Address Binding

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

8. Assign Accounts and Privileges Reasonably

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

9. Disable Unnecessary Services and Choose Secure Modes

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

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

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

10. Audio and Video Encrypted Transmission

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

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

11. Secure Auditing

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

12. Network Log

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

13. Construct a Safe Network Environment

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

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