Modular VTO (VTO4202F-P)

Quick Start Guide

V1.0.1

Foreword

General

This document mainly introduces product function, structure, networking, mounting process, debugging process, and web operations of modular VTO.

Models

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

Device Upgrade

Do not cut off power supply during device upgrade. Power supply can be cut off only after the device has completed upgrade and restarted.

Safety Instructions

The following categorized signal words with defined meaning might appear in the Manual.

Signal Words	Meaning
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.	July 2019

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: Providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

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 device. 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 after reading.

Operating Requirement

- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids, in order to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- Transport, use and store the device within allowed humidity and temperature range.

Power Requirement

- The product shall use electric wires (power wires) recommended by this area, which shall be used within its 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, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.

Table of Contents

1 Overview

1.1 Introduction

Modular VTO consists of camera module, indicator light module, one-button module, two-button module, five-button module, keyboard module, card swiping module, fingerprint module, audio module, and display module. Camera module and audio module are indispensable, whereas other modules can be selected as needed.

The combination of modular VTO, VTH, VTS and platform makes a voice/video communication system.

1.2 Function

- Video call: Make video calls on the modular VTO with VTH users.
- Group call: Call multiple VTH users at one VTO simultaneously.
- Be monitored: Videos captured by the VTO can be viewed in real time; support maximum 6-channel video stream.
- Emergency call: Press the key to call the Center in case of an emergency.
- Unlock: Card, fingerprint, password and remote unlock.
- Alarm: Support tamper alarm, door sensor alarm and duress password unlock alarm. Alarm information can be sent to the Management Center.
- Record search: Call records, alarm records and unlock records can be searched.

2 Structure

2.1 Camera Module

Figure 2-1 Camera module (front panel)

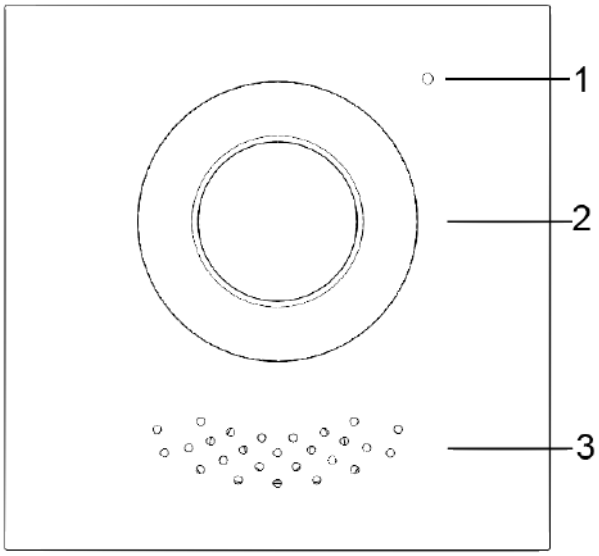


Table 2-1 Camera module (front panel) description

No.	Name	Description
1	Microphone	Audio input.
2	Camera	Monitor area in front of the door.
3	Speaker	Audio output.

Figure 2-2 Camera module (rear panel)

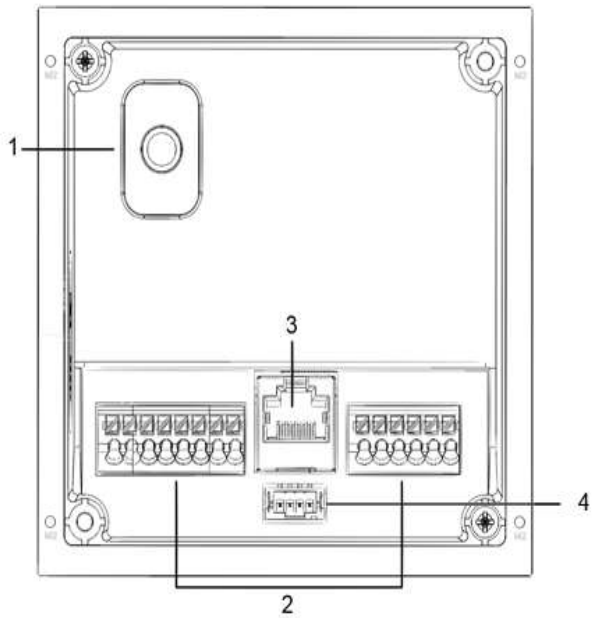
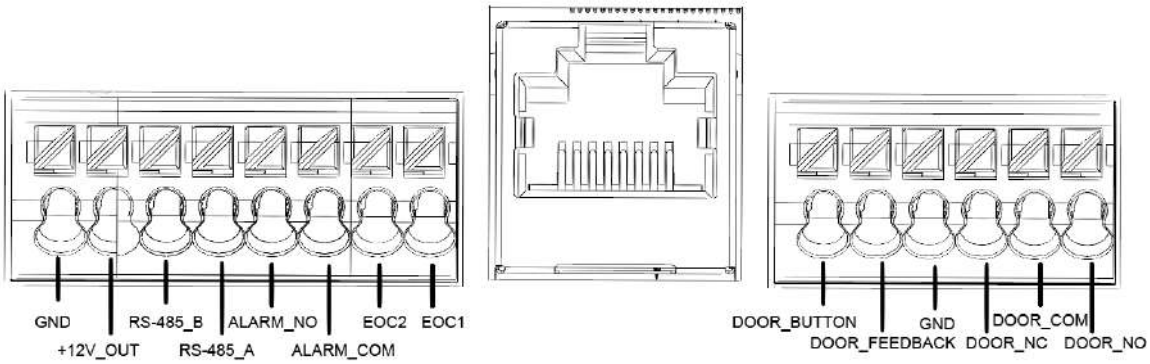


Table 2-2 Camera module (rear panel) description

No.	Name	Description
1	Tamper switch	When VTO is detached from the wall forcibly, alarm sound will be made and alarm information will be sent to management center.
2	User port	Provide power port, lock port, door sensor feedback port and exit button port to connect power supply, electric control lock, solenoid lock and exit button. See Figure 2-3.
3	Ethernet Port	Connected to network cables.
4	Cascade connection port	Connect other modules. In case of cascade connection of multiple modules, modules need cascade connection.

Figure 2-3 User ports



2.2 Indicator Light Module

Figure 2-4 Indicator light module (front panel)

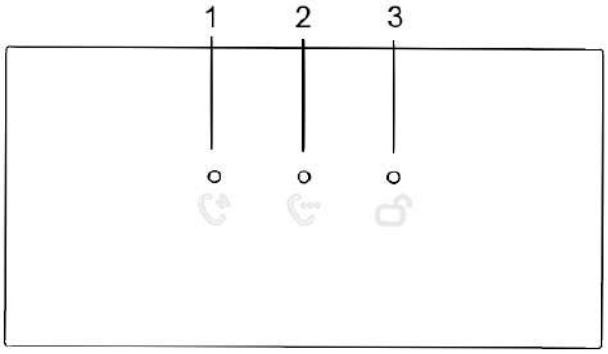


Table 2-3 Indicator light module description

No.	Name	Description
1	Call indicator	Indicate the call status.
2	Talk indicator	Indicate the talk status.
3	Unlock indicator	Indicate the unlock status.

Figure 2-5 Indicator light module (rear panel)

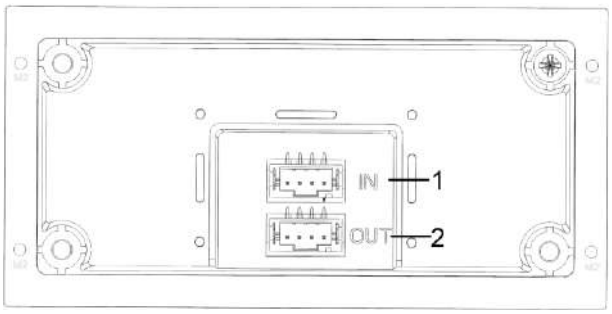


Table 2-4 Indicator light module (rear panel) description

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

2.3 Audio Module

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

Figure 2-6 Audio module

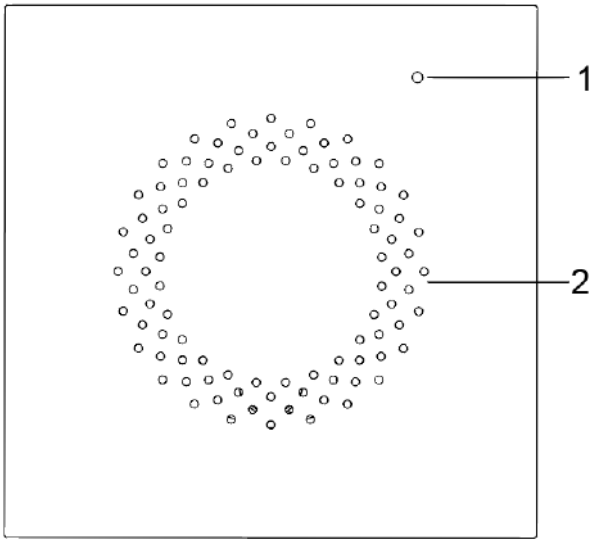


Table 2-5 Audio module description

No.	Name	Description
1	Microphone	Audio input.
2	Speaker	Audio output.

2.4 Button Module

One-button module, two-button module, and five-button module are available. Their functions are the same, although button quantity is different.

Here five-button module is taken as an example. See Figure 2-7 and Table 2-6.

Figure 2-7 Five-button module (front panel)

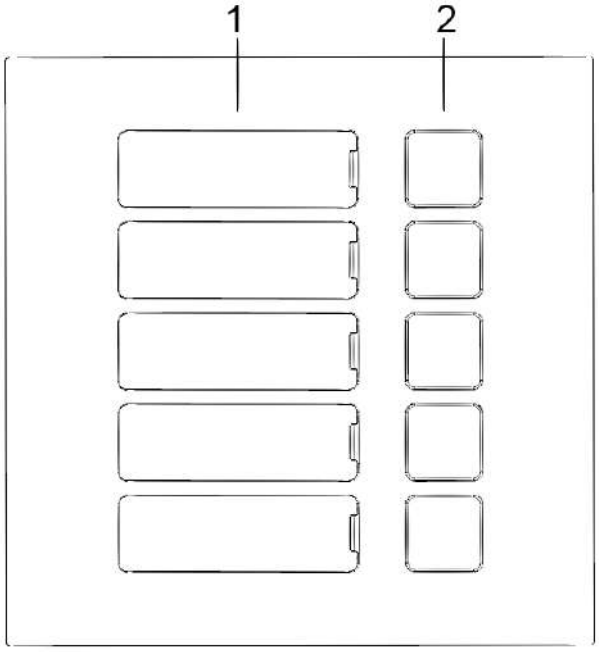


Table 2-6 Button module (front panel) description

No.	Name	Description
1	User directory	Display user information according to buttons.
2	Call button	Call the VTH and call the management center (you need to do seetings on the web first).

Figure 2-8 Five-button module (rear panel)

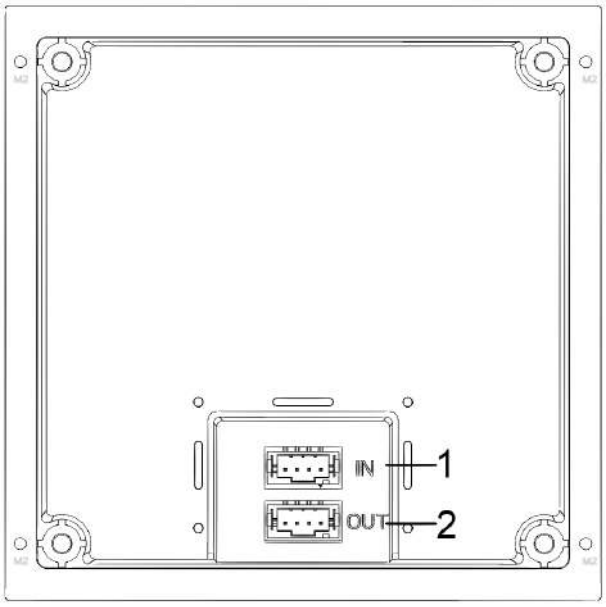


Table 2-7 Button module (rear panel) description

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

2.5 Keyboard Module (with Braille)

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

Figure 2-9 Keyboard module

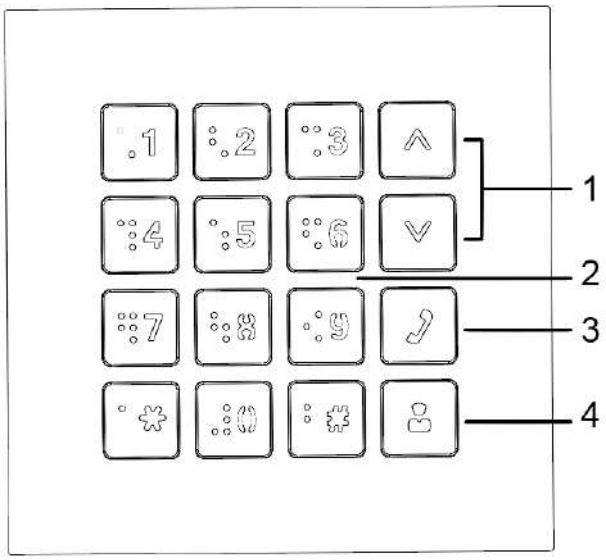


Table 2-8 Keyboard module description

No.	Name	Description
1	Selection buttons	Press the buttons to select previous or next item.
2	Numeric button	Enter the password and VTH nombers. For example, unlock password is 123456. Enter “#+ 123456 +#”.
3	Call button	Press the button to start a call to VTH.
4	Call management centre	Call management centre.

2.6 Card Swiping Module

You can swipe card near the icon shown in Figure 2-10.

Rear panel of card swiping module is the same as rear panel of button module.

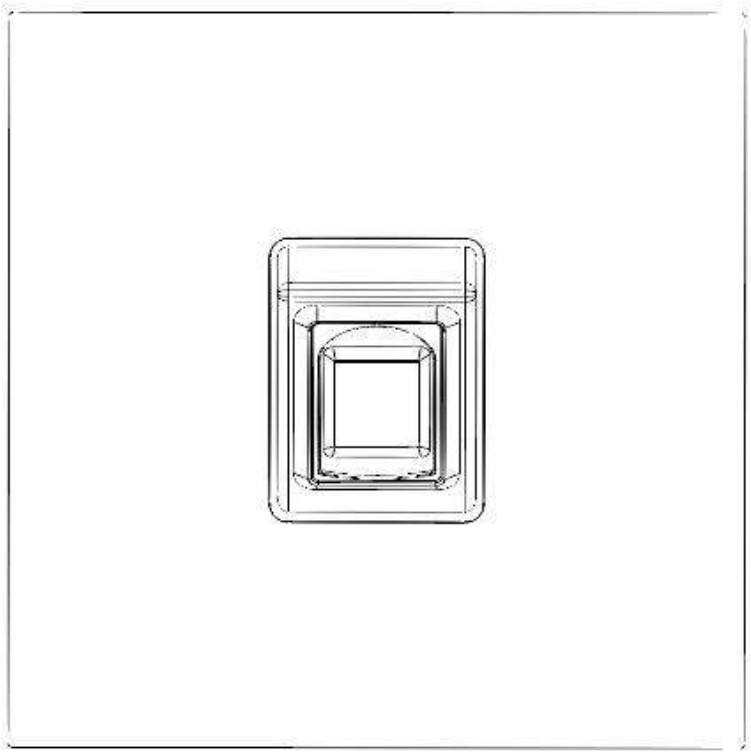
Figure 2-10 Card swiping module (mm [inch])

2.7 Fingerprint Module

The module is helpful for collecting fingerprints or unlocking with fingerprint.

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

Figure 2-11 Fingerprint module

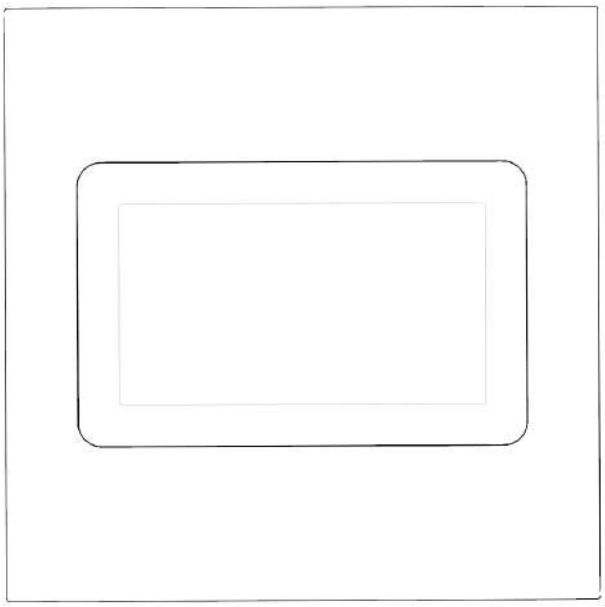


2.8 Display Module

Display module can be used for displaying 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

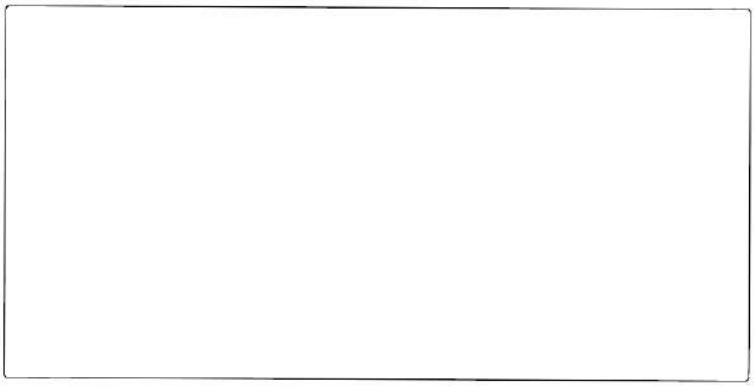


2.9 Blank Module

Blank module can be used for more attractive appearance when there is extra space.

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

Figure 2-13 Blank module



3 Installation

Modular VTO supports mounting two modules and three modules, and you can mount it horizontally or vertically. Depending on the actual conditions of the installation surface, you can install the VTO in the wall or on the wall.

This section takes 3-module mounting for example.

- Visiting cards and card cover are included in the package by default.
- When powering on after mounting, make sure that all modules have been connected; otherwise, the modules might fail to work normally.
- Before installing surface mounting box and flush mounting box, cables in the wall shall go through the bracket or mounting box.

3.1 Installing on/in the Wall

3.1.1 Installing on the Wall

Step 1 Drill holes according to hole positions of the mounting box, and put expansion pipe in place.

Step 2 Fix the mounting box onto the wall with ST4×25 screws.

Step 3 Fix the rear panel on the mounting box with M2×8 screws.

Step 4 Connect cables. See "2 Structure."

Step 5 Fix modules on the rear panel with M3×8 screws.

Step 6 Apply glue to gaps between the mounting box and the wall.

Step 7 Write room number or the username on the visiting card, and insert it into user directory.

Step 8 Apply silicone sealant to gaps between the device and the wall.

Figure 3-1 Apply silicone sealant to gaps

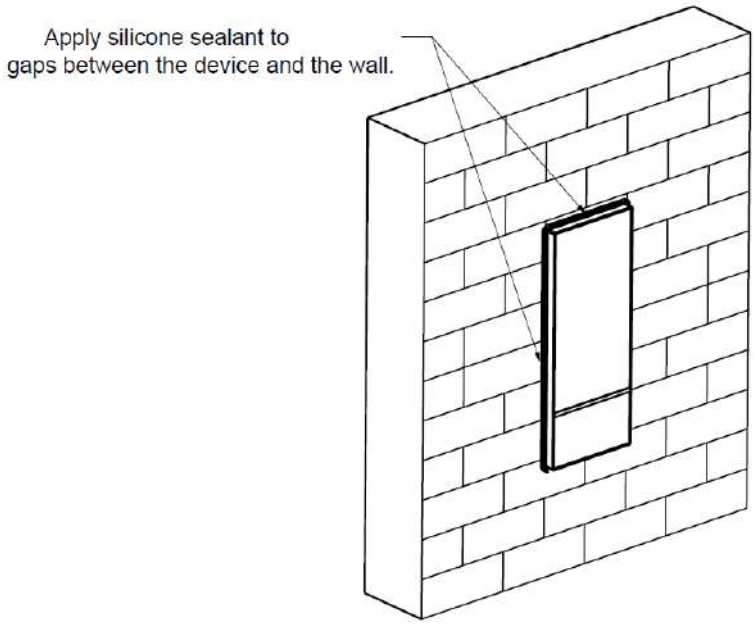
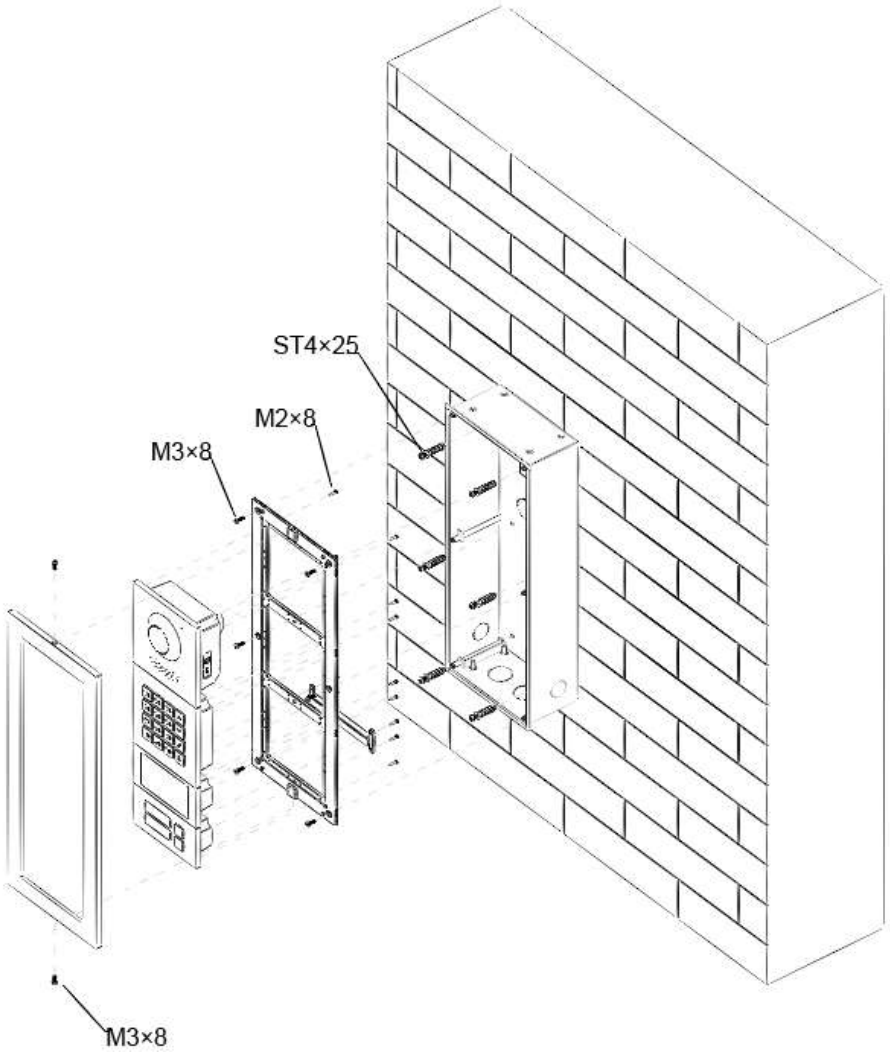


Figure 3-2 Installing on the wall



3.1.2 Installing in the Wall

Step 1 Drill a hole in the wall.

- For 2-module mounting, the rectangular hole dimension is 126mm×226mm to 128mm×228mm.
- For 3-module mounting, the rectangular hole dimension is 126mm×326mm to 268mm×329mm.

Step 2 Put the mounting box into the wall with ST4×25 screws; ensure that box edge clings to the wall.

Step 3 Fix the rear panel on the mounting box with M2×8 screws.

Step 4 Connect cables. Please refer to "2 Structure."

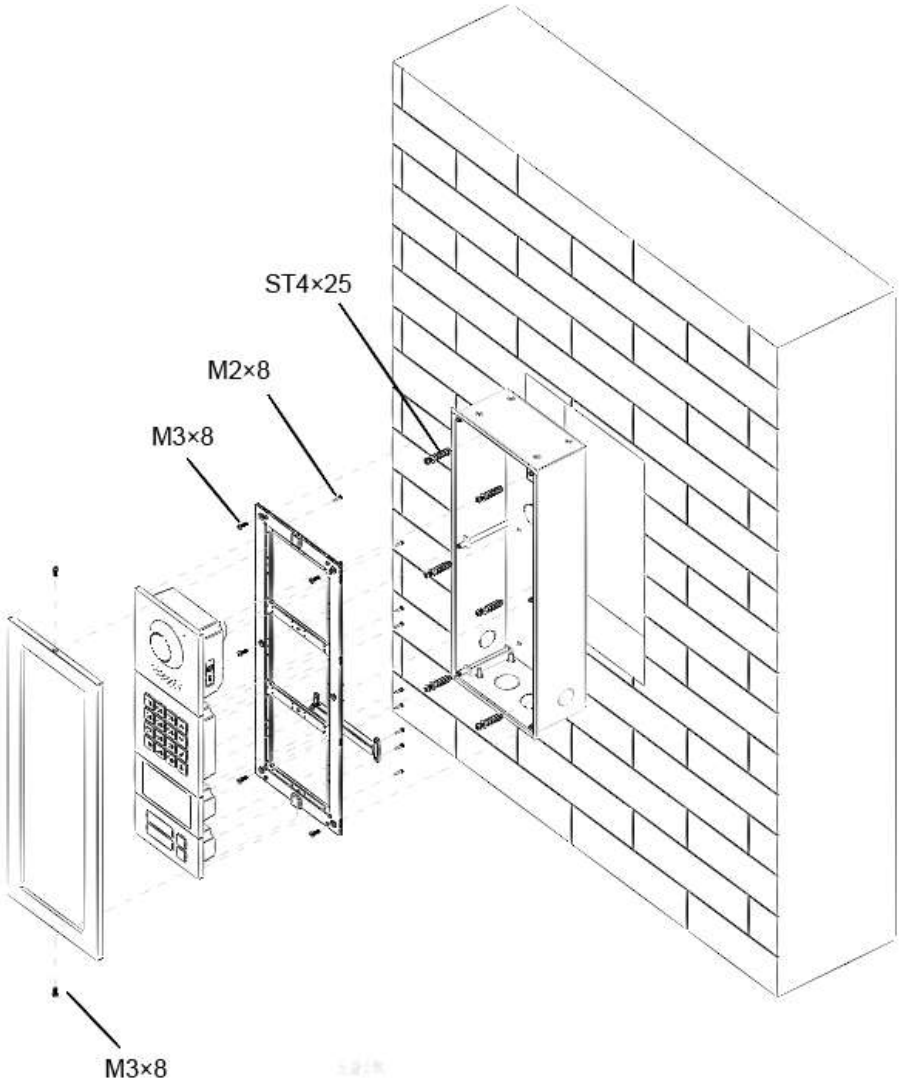
Step 5 Fix every module on the rear panel with M3×8 screws.

Step 6 Apply glue to gaps among the rear panel, mounting box and wall.

Step 7 Write room number or the username on the visiting card, and insert it into user directory.

Step 8 Apply silicone sealant to gaps between the device and the wall.

Figure 3-3 Installing in the wall



3.2 Horizontal/Vertical Mounting

3.2.1 Horizontal Mounting

Figure 3-4 Horizontal mounting (1)

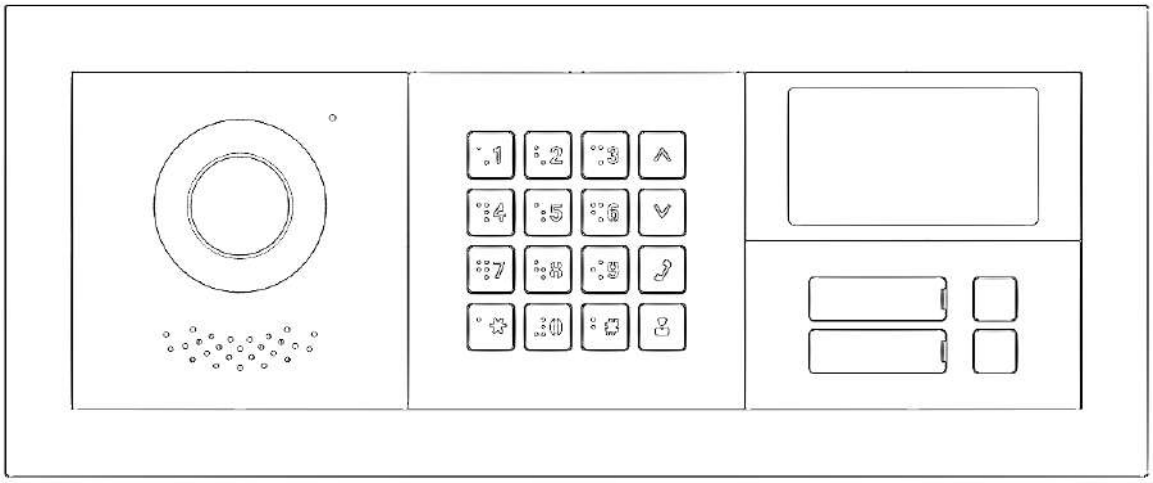
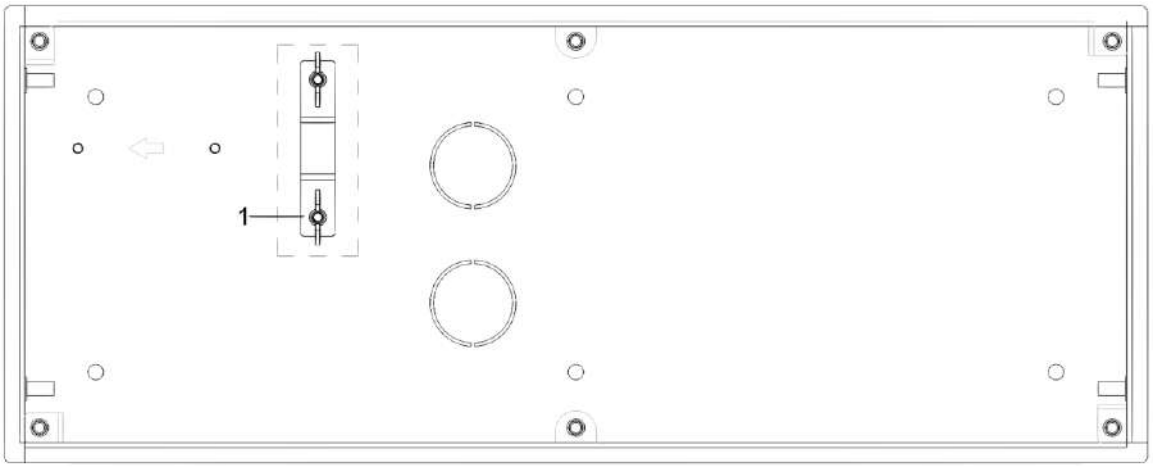


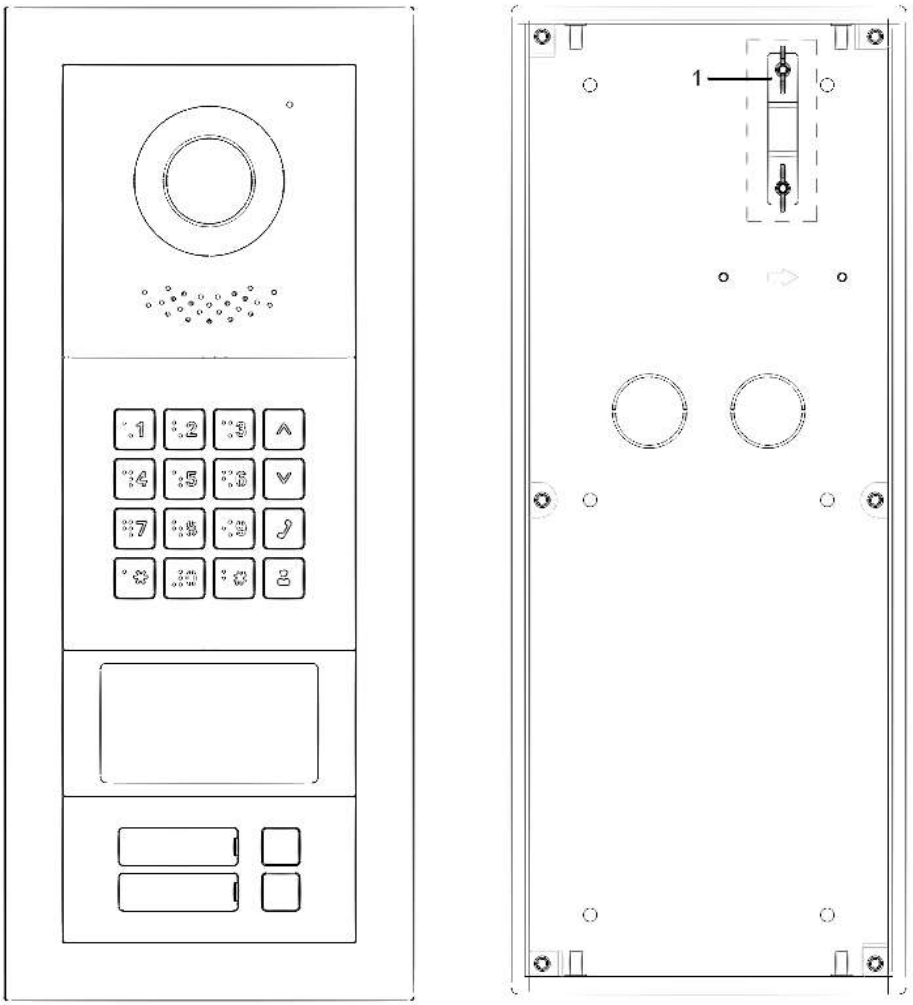
Figure 3-5 Horizontal mounting (2)



When the VTO is horizontally mounted, make sure that the tamper switch on the rear panel (marked with "1" in Figure 3-4) is retracted so that once the VTO is dismantled, tamper switch will be released, and then alarms will be triggered. The alarm will keep ringing for 15 seconds.

3.2.2 Vertical Mounting

Figure 3-6 Vertical mounting illustrations

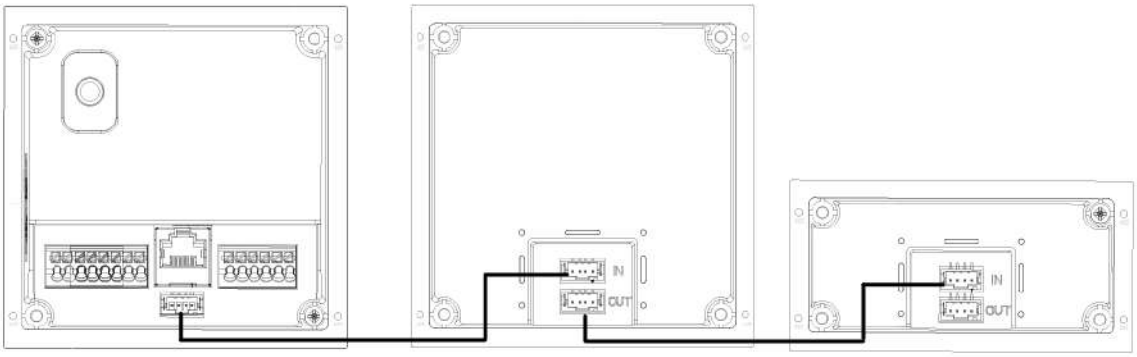


When the VTO is vertically mounted, make sure that the tamper switch on the rear panel (marked with "1" in Figure 3-5) is retracted so that once the VTO is dismantled, tamper switch will be released, and then alarms will be triggered. The alarm will keep ringing for 15 seconds.

3.3 Cascade Connection

To make modules work collaboratively, cascade connection is needed. See a cascade connection example in Figure 3-7.

Figure 3-7 Cascade connection



4 Configuration

This chapter introduces how to initialize, connect, and make primary configurations to the VTO and VTH devices to realize basic functions, including device management, calling, and monitoring. For more detailed configuration, see the user's Manual.

4.1 Configuration Process

Before configuration, check every device and make sure that there is no short circuit or open circuit in the circuits.

Step 1 Plan IP address for every device, and also plan the unit number and room number you need.

Step 2 Configure VTO. See "4.2 Configuring VTO."

1) Initialize VTO. See "4.2.1 Initialization."
2) Configure VTO number. See "4.2.2 Configuring VTO Number."
3) Configure VTO network parameters. See "4.2.3 Configuring Network Parameters."
4) Configure SIP Server. See "4.2.4 Selecting SIP Servers."
5) Add VTO devices to the SIP server. See "4.2.5 Adding VTO Devices."
6) Add room number to the SIP server. See "4.2.6 Adding Room Number."

Step 3 Configure VTH. See the VTH users' manual.

Step 4 Verify Configuration. See "4.3 Verifying Configuration."

4.2 Configuring VTO

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

4.2.1 Initialization

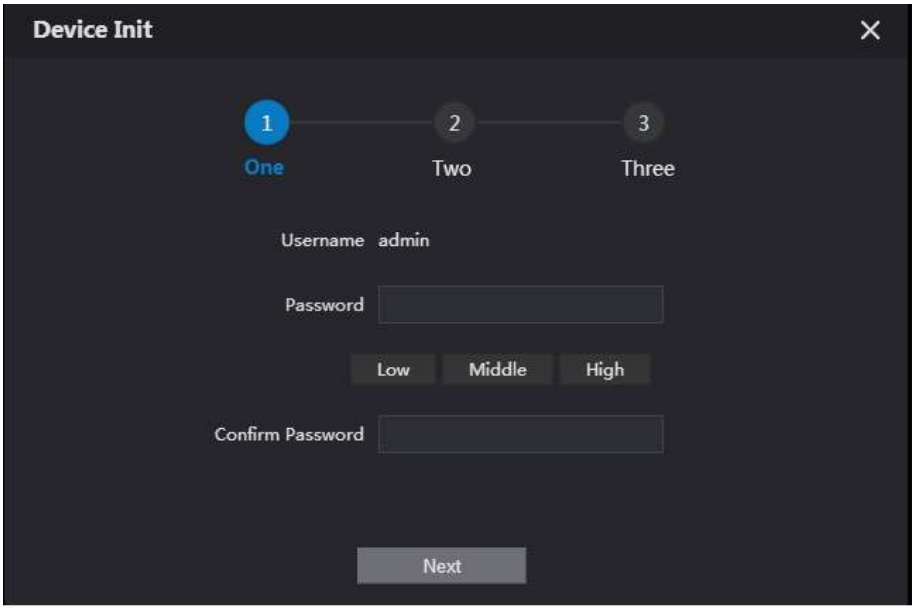
The default IP address of VTO is 192.168.1.108, and make sure that the PC is in the same network segment as the VTO.

Step 1 Connect the VTO to power source, and then boot it up.

Step 2 Open the internet browser on the PC, then enter the default IP address of the VTO in the address bar, and then press Enter.

The **Device Init** interface is displayed. See Figure 4-1.

Figure 4-1 Device initialization



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

The Email setting interface is displayed.

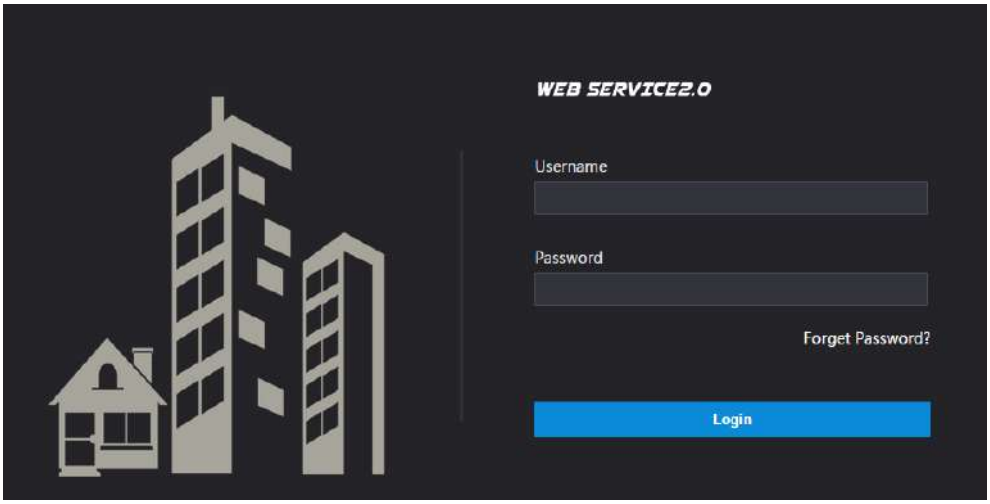
Step 4 Select the **Email** check box, and then enter your Email address. This Email address can be used to reset the password, and it is recommended to finish this setting.

Step 5 Click **Next**. The initialization succeeded.

Step 6 Click **OK**.

The **Login** interface is displayed. See Figure 4-2.

Figure 4-2 Login



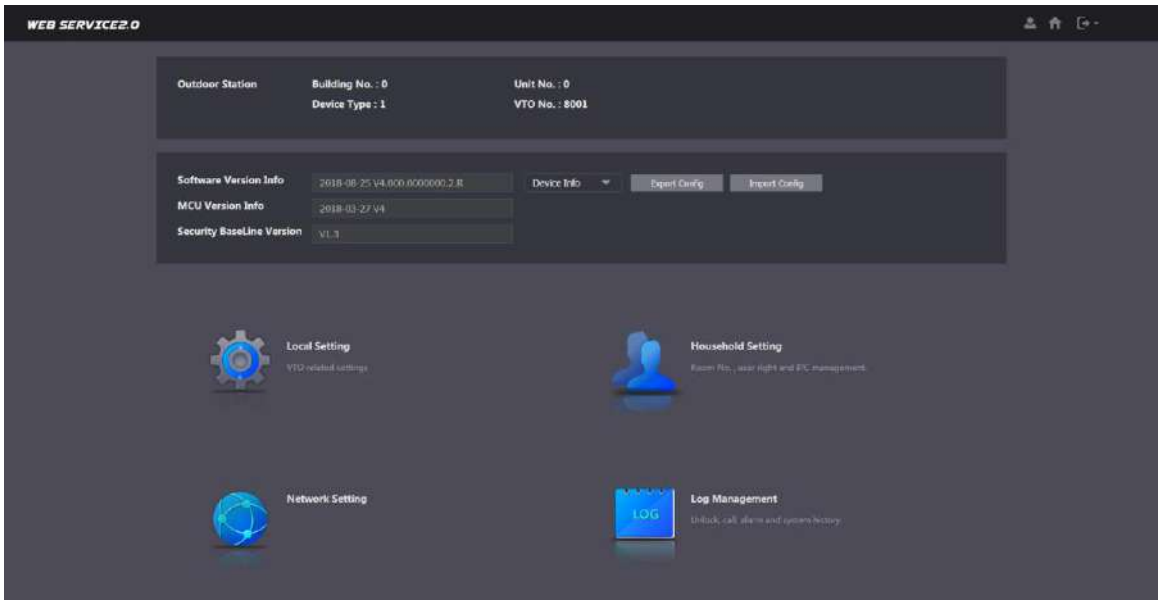
4.2.2 Configuring VTO Number

The VTO number can be used to differentiate each VTO, and it is normally configured according to unit or building number.

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

Step 1 Log in to the web interface of the VTO, and then the main interface is displayed. See Figure 4-3.

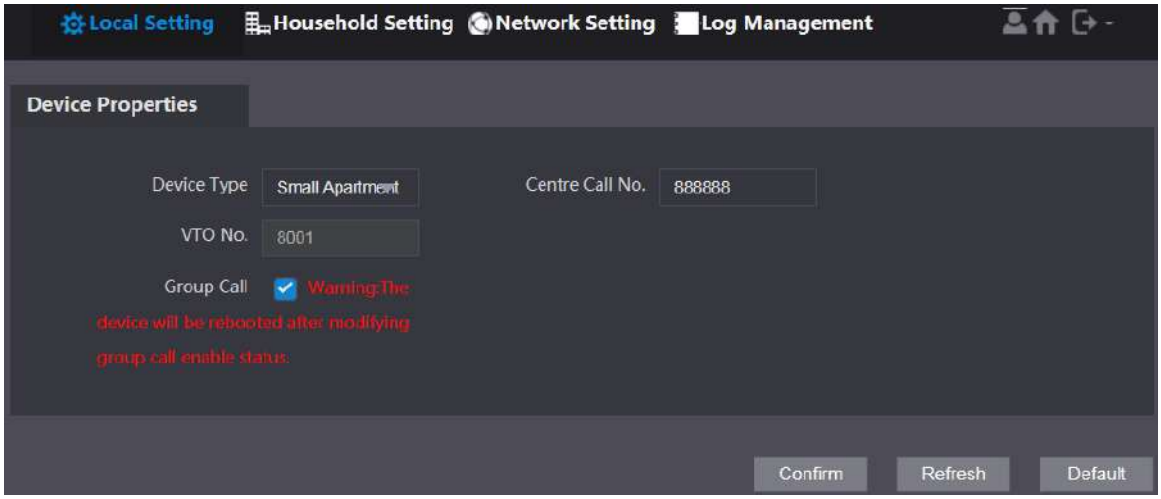
Figure 4-3 Main interface



Step 2 Select Local Setting > Basic.

The device properties are displayed. See Figure 4-4.

Figure 4-4 Device properties



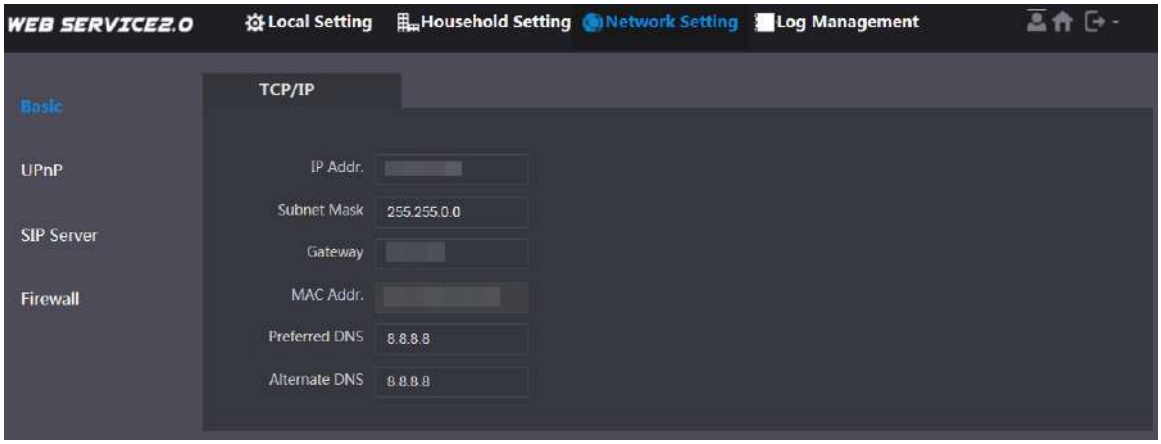
Step 3 In the **VTO No.** input box, enter the VTO number you planned for this VTO, and then click **Confirm** to save.

4.2.3 Configuring Network Parameters

Step 1 Select Network Setting > Basic.

TCP/IP interface is displayed. See Figure 4-5.

Figure 4-5 TCP/IP information



Step 2 Enter the network parameters you planed, and then click **Save**.

The VTO will restart, and you need to modify the IP address of your PC to the same network segment as that of the VTO to log in again.

4.2.4 Selecting SIP Servers

The Session Initiation Protocol (SIP) is used for signaling and controlling multimedia communication sessions in applications of voice and video calls. A SIP server is an application provides information or direction to a user agent.

- When this VTO or other VTOs work as SIP server, select **VTO** from the **Server Type** drop-down list. It applies to a scenario where there is only one building.
- When the platform (Express/DSS) works as SIP server, select **Express/DSS** from the **Server Type** drop-down list. It applies to a scenario where there are multiple buildings or multiple units.

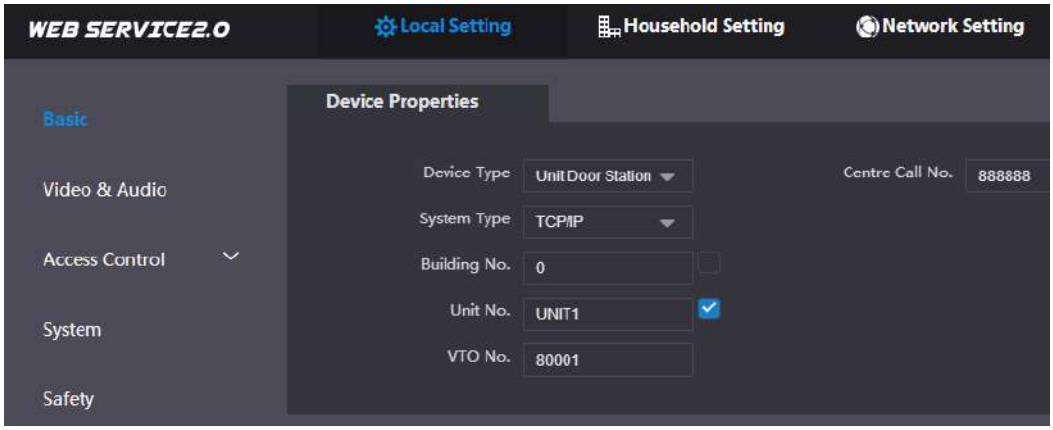
- If the VTO you are operating is the SIP server, **Building No.** and **Unit No.** will not be displayed on the **Device Properties** interface in **Local Setting > Basic**.
- If you selected the **Enable** checkbox of the **Alternate Server** in **Network Setting > SIP Server** and save the setting, you need to log in the web interface again, and **Building No.** and **Unit No.** will be displayed on the **Device Properties** interface in **Local Setting > Basic**.

Step 3 Log in to the web page.

Step 4 On the homepage, select **Local Setting > Basic**.

The **Device Properties** interface is displayed, see Figure 4-6.

Figure 4-6 Device properties



1) Select **TCP/IP** from the **System Type** drop-down list.

Default system type is analogue system and shall be changed to TCP/IP. Otherwise, it will fail to be connected to the VTH.

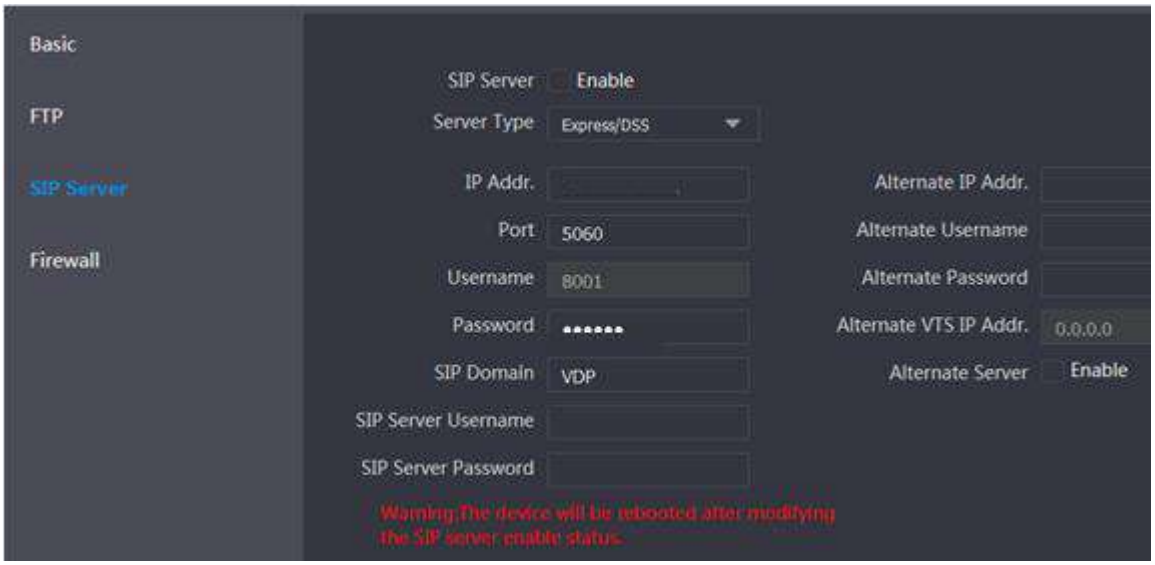
2) Click **OK** to save the settings.
3) Restart the device manually, or wait for auto reboot to make the settings effective.

Step 5 Log in to the web interface again.

Step 6 Select Network Setting > SIP Server.

The **SIP Server** interface is displayed. See Figure 4-7.

Figure 4-7 SIP server (1)



Step 7 Select a SIP server.

VTO as SIP server

Step 1 Select **Enable** behind **SIP Server**.

Step 2 Select **VTO** from the **Server Type** drop-down list.

Step 3 Configure parameters (see Table 4-1 for details).

Step 4 Click **Save**.

The VTO will restart automatically.

Platform (Express/DSS) as a SIP server

Step 1 Select Network Setting > SIP Server.

The **SIP Server** interface is displayed. See Figure 4-8.

Figure 4-8 SIP server (2)

Step 2 Disable SIP Server.

Step 3 Select **Express/DSS** from the **Server Type** drop-down list.

Step 4 Set parameters according to Table 4-1.

Table 4-1 SIP server parameter description

Parameter	Description
IP Address	IP address of SIP server. When the Alternate Server checkbox is not selected, IP Addr., Username, and Password can be entered, and you cannot call the VTS through VTO.
Port	● It is 5060 by default when other VTOs work as SIP server. ● It is 5080 by default when the platform works as SIP server.
Username/Password	Use default value.
SIP Domain	● It shall be VDP when another VTO works as SIP server. ● It can be null or keep default value when the platform works as SIP server.
Login Username/ Password	Username and password to log in to SIP server.
Alternate IP Addr.	IP address of the alternate server.
Alternate Username	Username and password for logging in to the alternate server.
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

Parameter	Description
	select the **Enable** checkbox to enable the alternate server. ● After you have selected the **Alternate Server Enable** checkbox, you can only enter the VTS IP address, and the VTO will restart.

Step 5 Click **OK** to save the configuration.

The VTO will restart automatically.

When the platform works as SIP server, if it is necessary to set Building No. and Building Unit No., enable **Support Building** and **Support Unit** first.

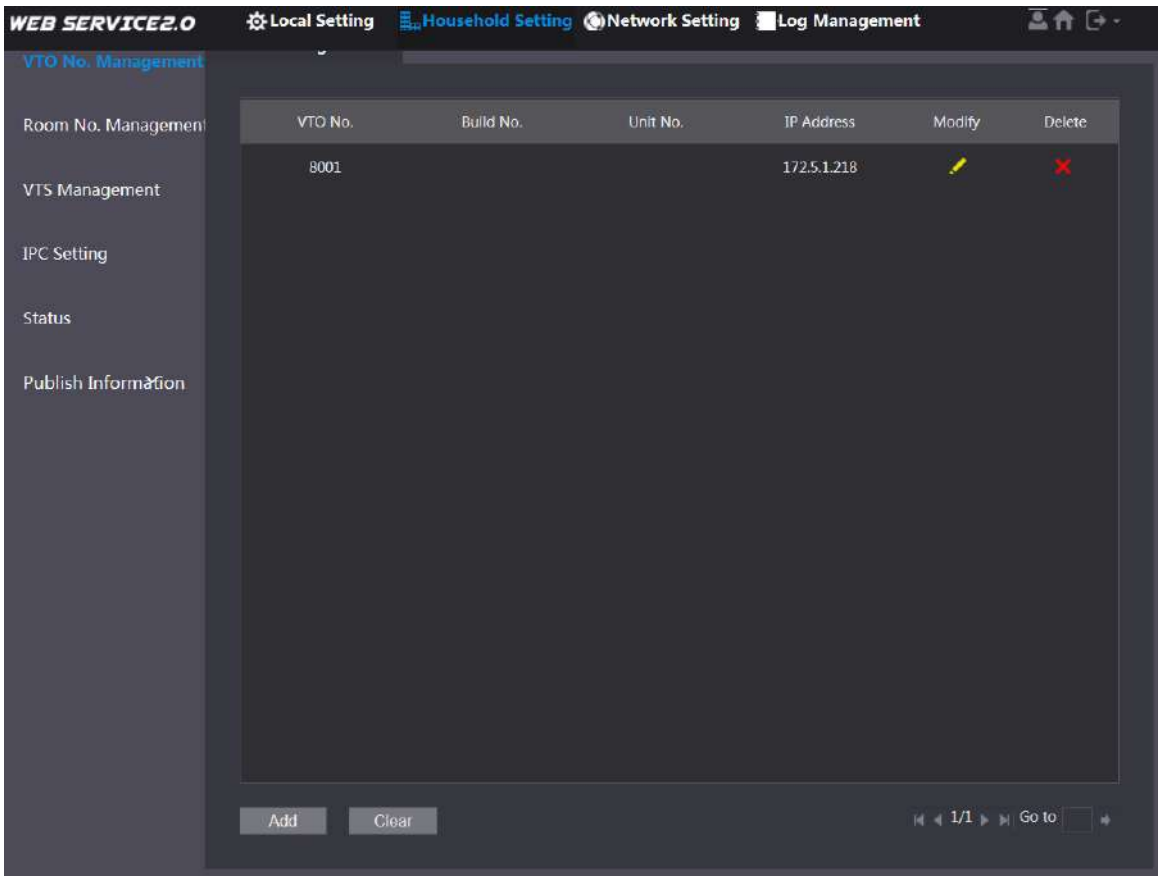
4.2.5 Adding VTO Devices

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 applies to the condition in which 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**.

The **VTO No. Management** interface is displayed. See Figure 4-9.

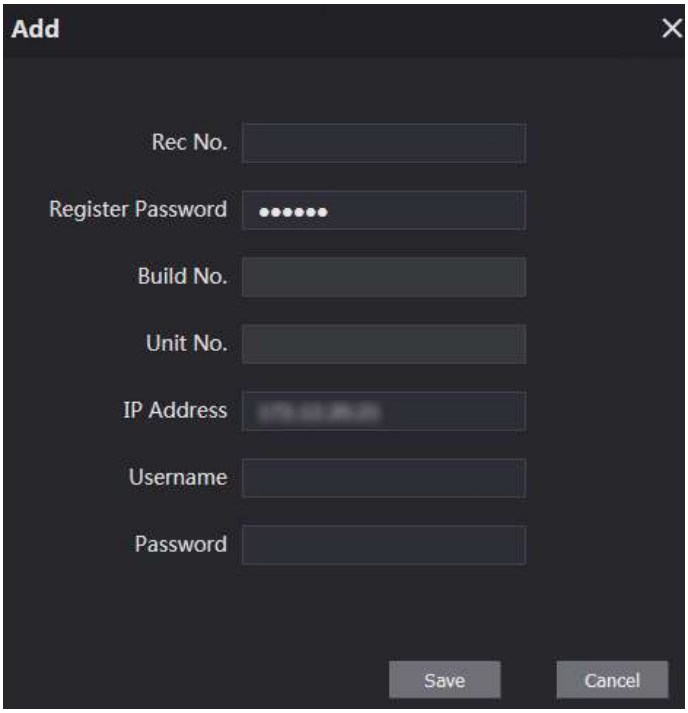
Figure 4-9 VTO No. management



Step 2 Click **Add**.

The **Add** interface is displayed. See Figure 4-10.

Figure 4-10 Add VTO



Step 3 Configure the parameters, and be sure to add the SIP server itself too. See Table 4-2.

Table 4-2 VTO configuration

Parameter	Description
Rec No.	The VTO number you configured for the target VTO. See the details in "4.2.2 Configuring VTO Number."
Register Password	Keep default value.
Build No.	Available only when other servers work as SIP server.
Unit No.	
IP Address	The IP address of the target VTO.
Username	The user name and password for the web interface of the target VTO.
Password	

Step 4 Click **Save**.

4.2.6 Adding Room Number

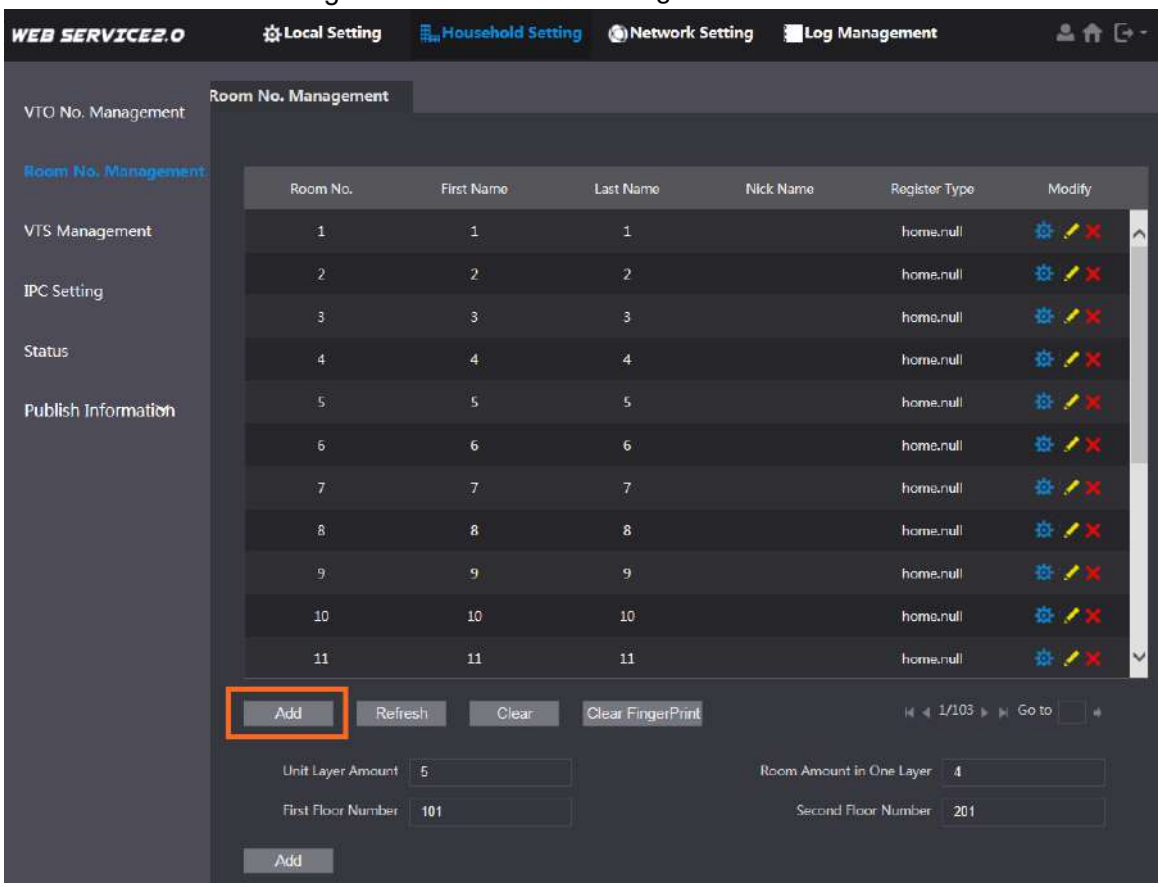
You can add the planned room number to the SIP server, and then configure the room number on VTH devices to connect them to the network. This section applies to the condition in which a VTO device works as SIP server, and if you use other servers as SIP server, see the corresponding manual for the detailed configuration.

The room number contains at most 6 numbers or letters or their combinations, and it cannot be the same as any VTO number.

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

The **Room No. Management** interface is displayed. See Figure 4-11.

Figure 4-11 Room No. management



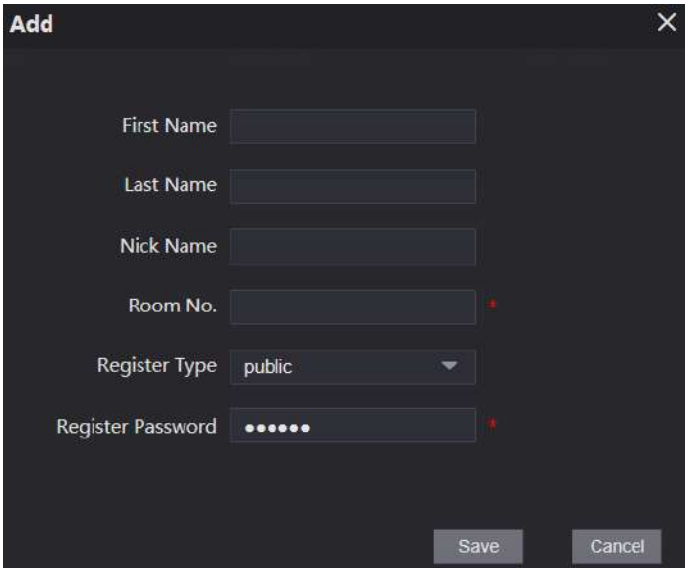
Step 2 You can add single room number or do it in batches.

- Adding single room number

1) Click **Add**. See Figure 4-11.

The **Add** interface is displayed. See Figure 4-12.

Figure 4-12 Add single room number



2) Configure room information. See Table 4-3.

Table 4-3 Room information

Parameter	Description
First Name	Enter the information you need to differentiate each room.
Last Name	

Parameter	Description
Nick Name	
Room No.	The room number you planned. ● If you use multiple VTH devices, the room number of the master VTH should be "room number#0", and the room number of the extension VTH should be "room number#1", "room number#2", …, "room number#99". ● You can have 10 extension VTH devices at most for one master VTH.
Register Type	Select **public**, and **local** is reserved for future use.
Register Password	Keep the default value.

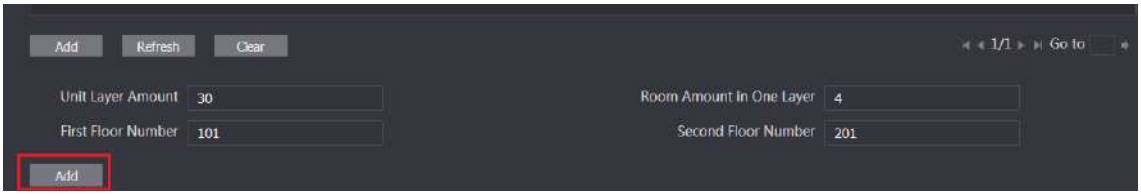
3) Click **Save**.

The added room number is displayed. Click to modify room information, and click to delete a room.

- Adding room number in batches

1) Configure the Unit Layer Amount, Room Amount in One Layer, First Floor Number, and Second Floor Number according to the actual condition.
2) Click the **Add** at the bottom. See Figure 4-13

Figure 4-13 Add in batch



All the added room numbers are displayed. Click **Refresh** to view the latest status, and click **Clear** to delete all the room numbers.

4.2.7 Configuring Module

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

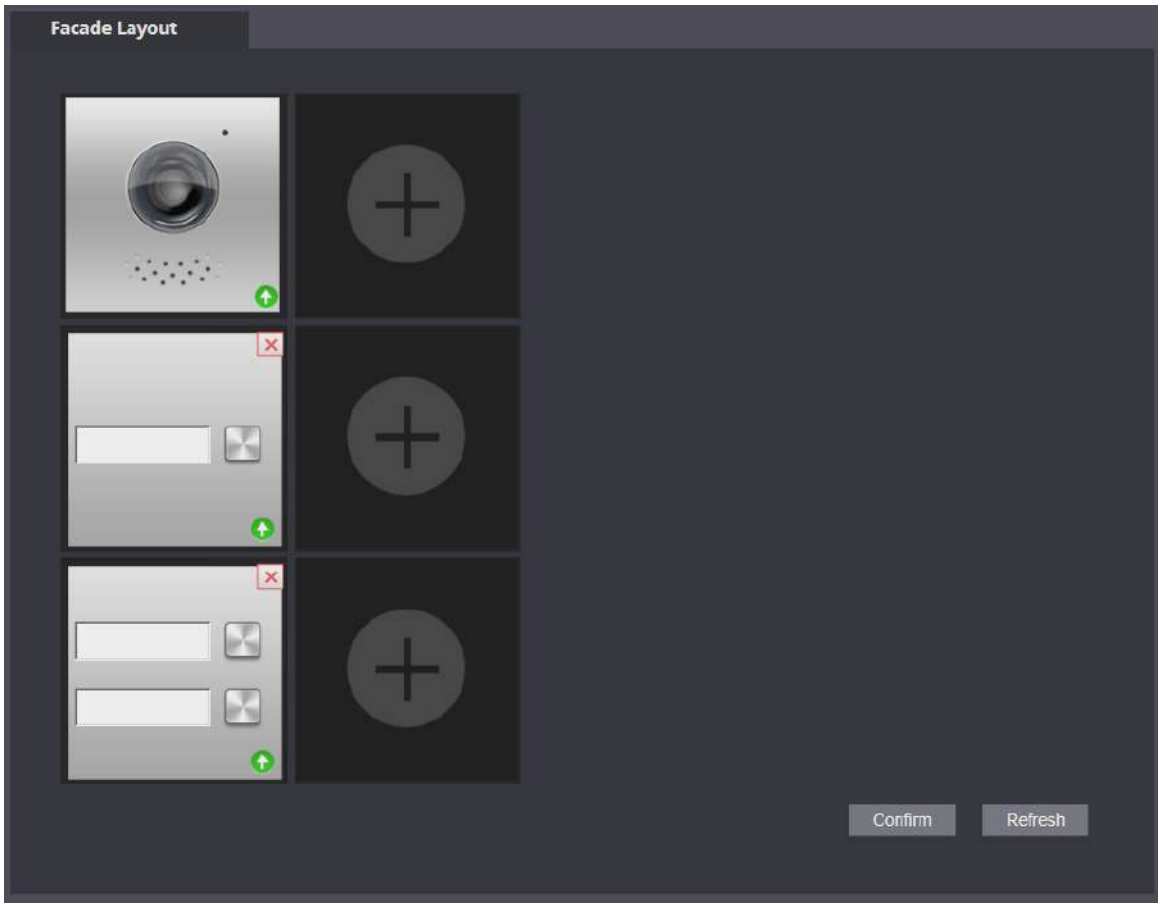
- You can add 9 modules at most to VTO4202F-MB1, VTO4202F-MB2, VTO4202F-MB5. For VTOs of other modules, you can only add one module.
- For fingerprint module, card swiping module, and keyboard module, only one module of each type can be added respectively. Other modules can be matched freely.

4.2.7.1 Adding Modules

Step 1 Select Local Setting > Basic > Façade Layout.

The **Façade Layout** interface is displayed. See Figure 4-14.

Figure 4-14 Façade layout



Step 2 Click  .

The system displays the modules available.

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

Step 3 Select modules according to actual layout of VTO.

Actual connection position of the device on web interface is from top to bottom and from left to right.

Support adding multiple modules at the same time and saving the configurations.

Step 4 Click **Confirm**, and then restart the browser to make the configurations take effective.

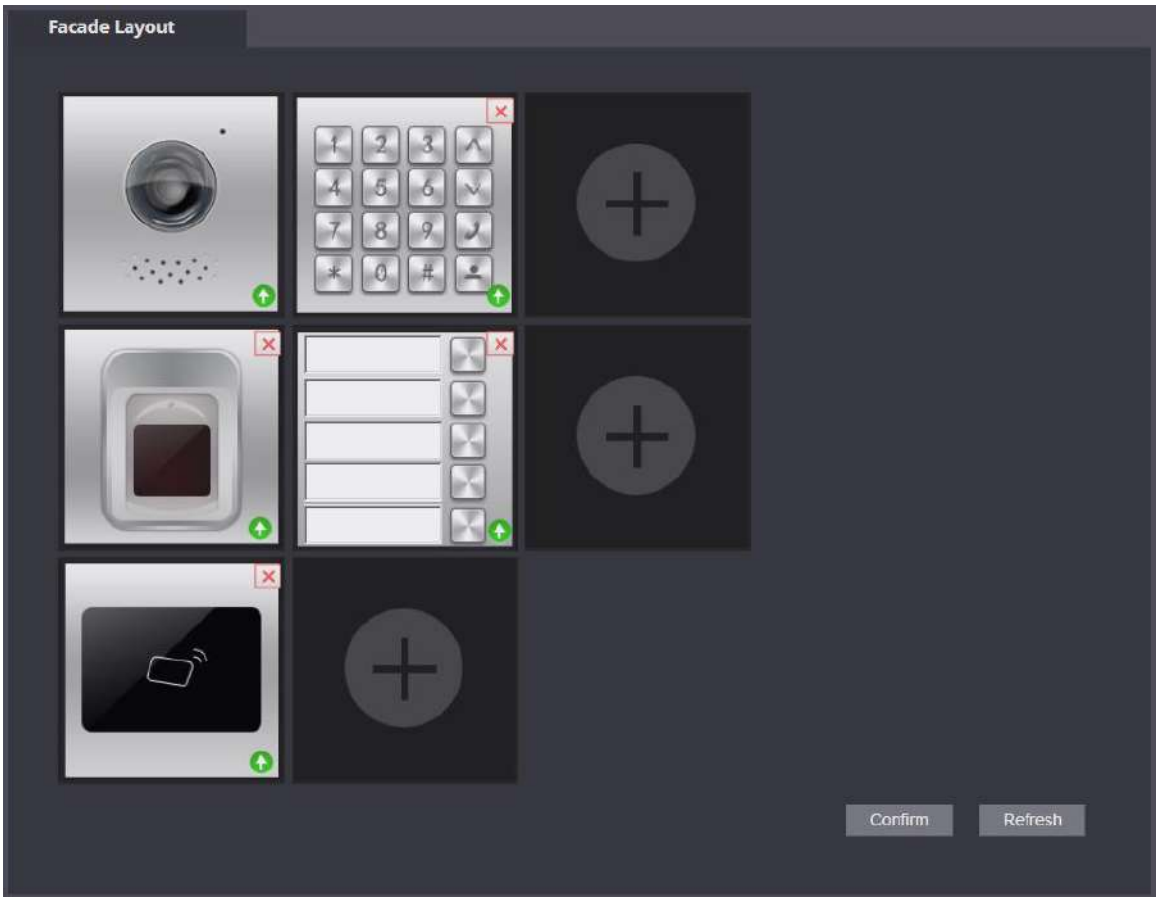
4.2.7.2 Setting Modules

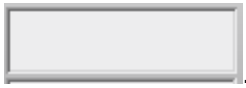
You need to set call keys for button module and camera module respectively.

Step 1 Select Local Setting > Basic > Façade Layout.

The **Façade Layout** interface is displayed. See Figure 4-15.

Figure 4-15 Set modules

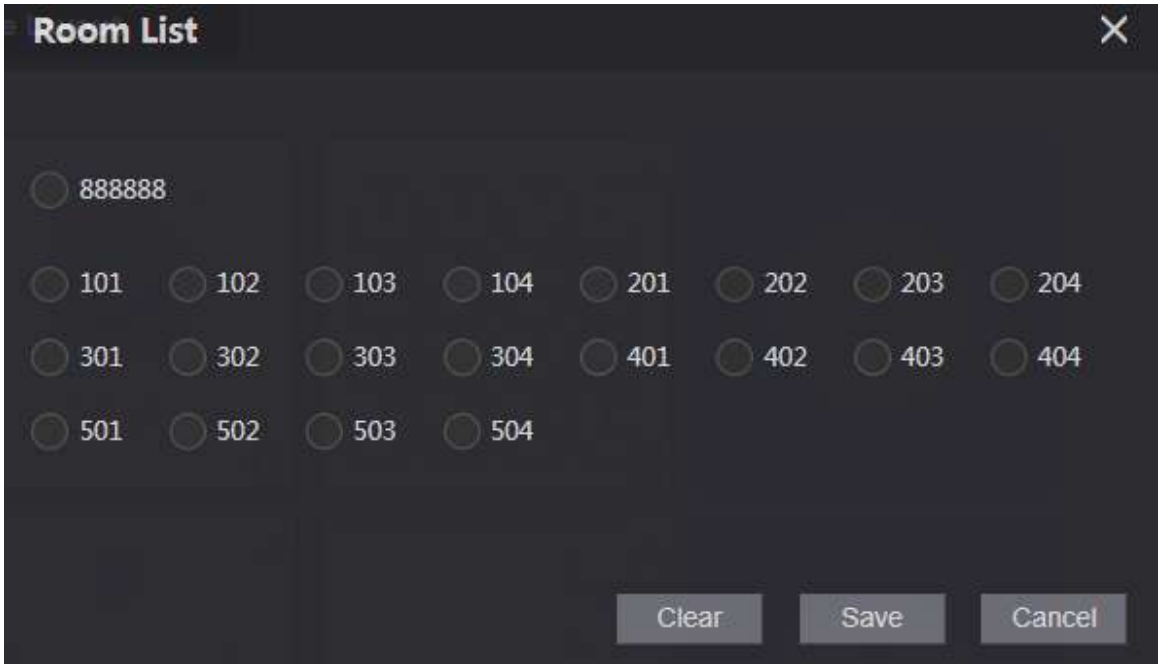


Step 2 Click  .

The **Room List** interface is displayed. See Figure 4-16.

The room no. displayed on the interface corresponds to the added VTH. "888888" is the Centre Call No.

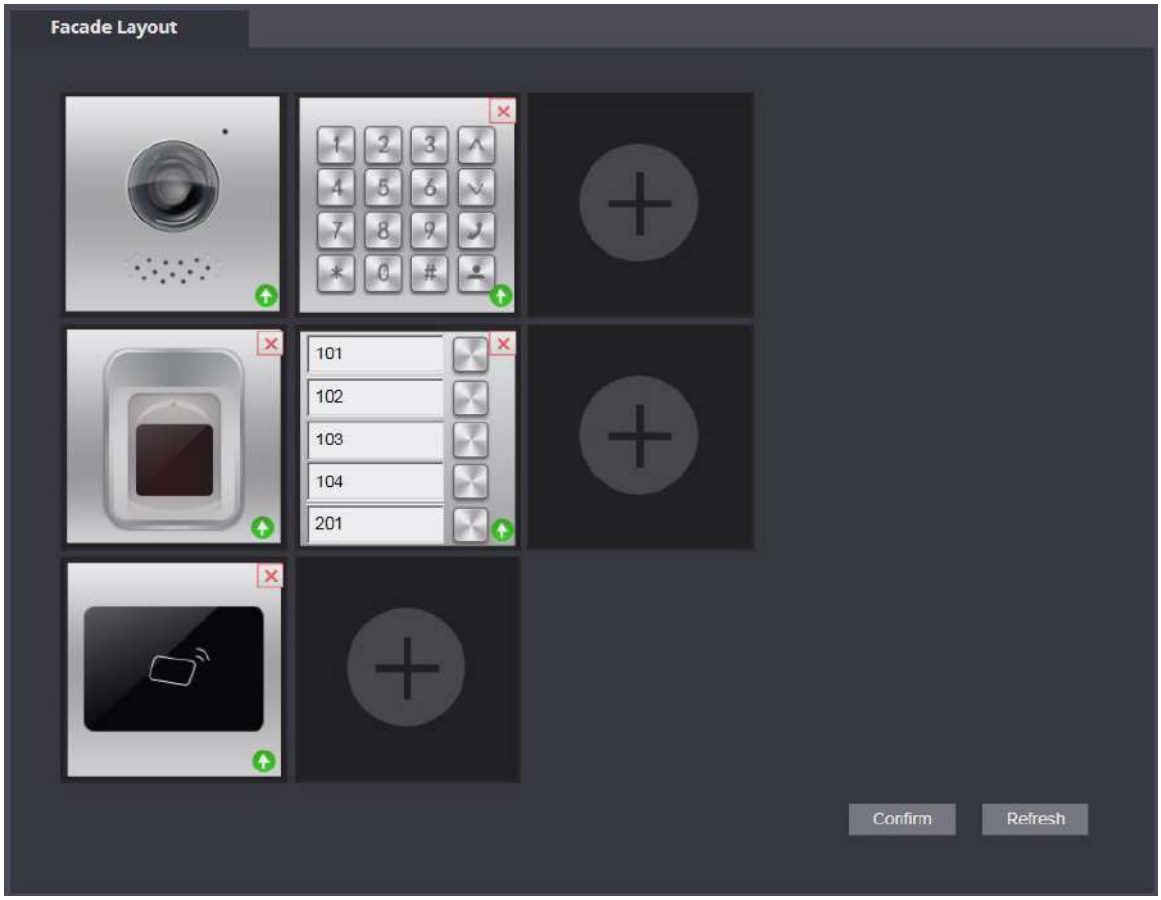
Figure 4-16 Room list



Step 3 Select room no. and click **Save**.

The interface displays room No. information. See Figure 4-17.

Figure 4-17 Room No. information



Step 4 Click **Confirm**, and then restart the browser to make the configurations take effective. save the settings.

4.3 Verifying Configuration

4.3.1 Calling VTH from VTO

Step 1 Dial room number on the VTO.

Step 2 Press .

The VTO is calling the VTH. See Figure 4-18.

Figure 4-18 Call screen

Step 3 Tap on the VTH to answer the call.

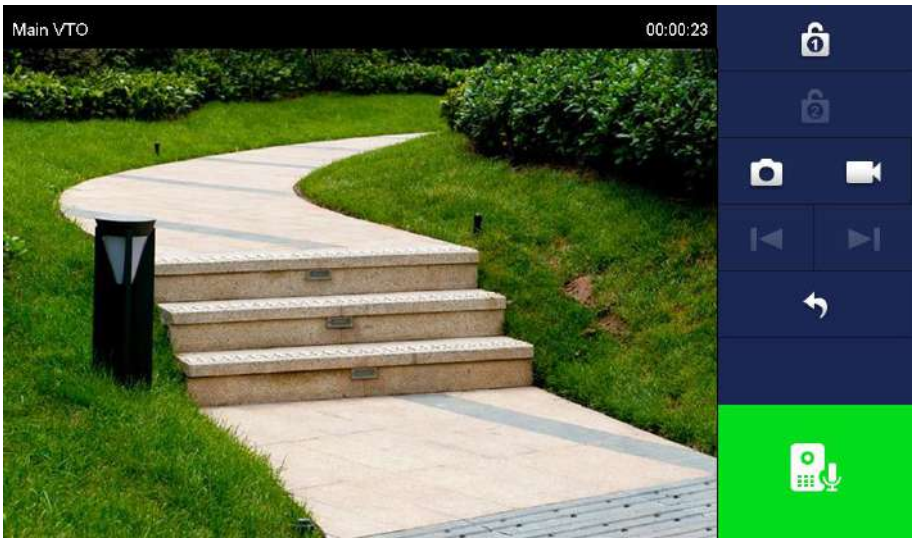
4.3.2 Doing Monitor from VTH

Step 1 On the main interface of the VTH, select **Monitor > Door**.
The **Door** interface is displayed. See Figure 4-19.

Figure 4-19 Door

Step 2 Select the VTO you need to do monitor.
The monitor screen is displayed. See Figure 4-20.

Figure 4-20 Monitor screen



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 equipment 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 equipment (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 equipment 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 equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. **MAC Address Binding**

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

9. **Assign Accounts and Privileges Reasonably**

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

10. **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.

11. **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.

12. **Secure Auditing**

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

13. **Network Log**

    Due to the limited storage capacity of the equipment, 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.

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment 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.