Villa Door Station (Version 4.3)

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the structure, mounting process, and basic configuration of the door station (hereinafter referred to as "VTO").

Safety Instructions

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

Signal Words	Meaning
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.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.0	First release	March 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 device. Please read the manual carefully before use to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

Operating Requirement

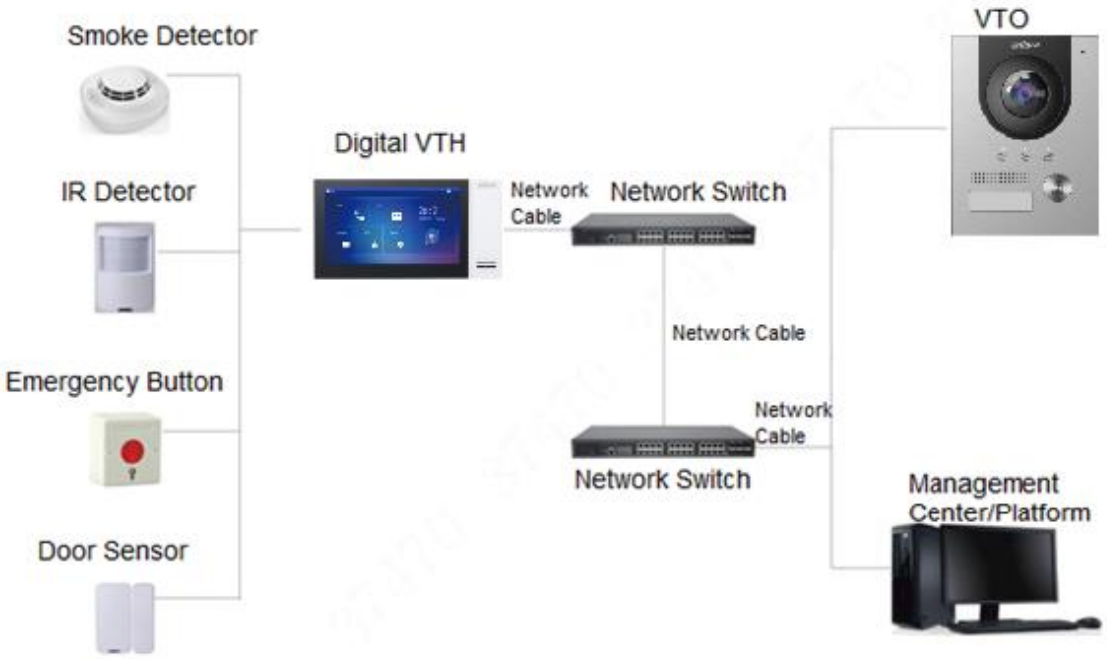
- Do not place and install the device in an area exposed to direct sunlight or near heat generating devices.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids 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) required by the region where the device will be used.
- 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 Network Diagram



2 Appearance

2.1 VTO2101E-P

2.1.1 Front Panel

Figure 2-1 VTO2101E-P

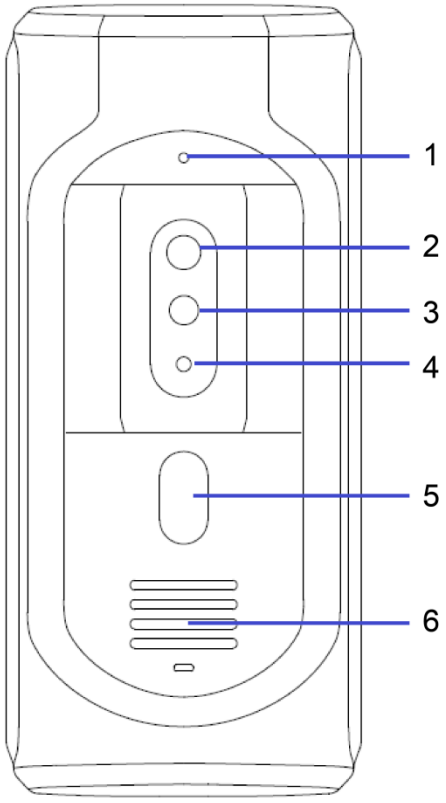


Table 2-1 Front panel description

No.	Name	Description
1	MIC	Inputs audio.
2	Camera	Monitors doorway area.
3	IR illunimation light	Provides extra IR light for the camera when it is dark.
4	Light sensor	Detects ambient lighting condition.
5	Call button	Press the button to call VTH or the management center.
6	Speaker	Outputs audio.

2.1.2 Rear Panel

Figure 2-2 VTO2101E-P

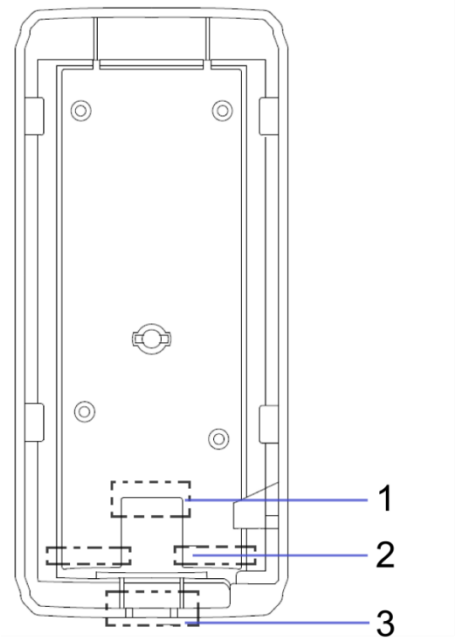


Table 2-2 Rear panel description

No.	Name	Description
1	Network port	Connected to the network with network cables.
2	RS-485 ports	See Figure 2-3 and Table 2-3.
3	Cable tray	You can thread cables through the cable tray.

Figure 2-3 Cable connection

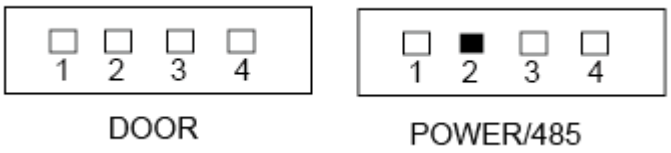


Table 2-3 Port description

DOOR		POWER/485	
No.	Name	No.	Name
1	NO	1	+12V
2	NC	2	GND
3	COM	3	RS-485A
4	ALARM IN	4	RS-485B

2.2 VTO3211D-P

2.2.1 Front Panel

Number of buttons on the front panel varies on different models. VTO3211D-P2 has two buttons; VTO3211D-P4 has four buttons. VTO3211D-P4 will be taken as an example.

Figure 2-4 VTO3211D-P

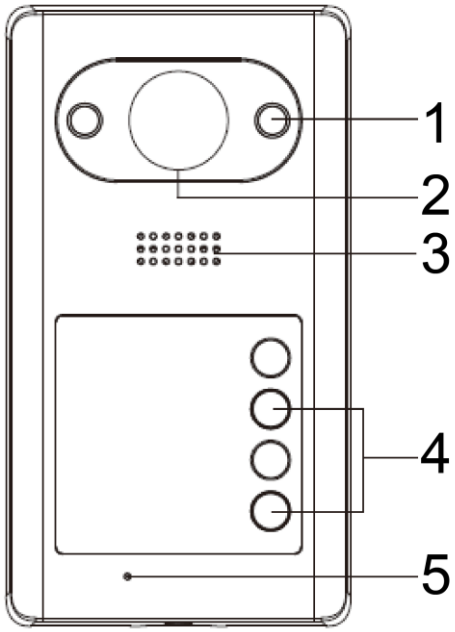


Table 2-4 Front panel description

No.	Name	Description
1	IR illumination light	Provides extra IR light for the camera when it is dark.
2	Camera	Monitors doorway area.
3	Speaker	Outputs audio.
4	Call button	Press the button to call VTH or the management center.
5	MIC	Inputs audio.

2.2.2 Rear Panel

Figure 2-5 VTO3211D-P

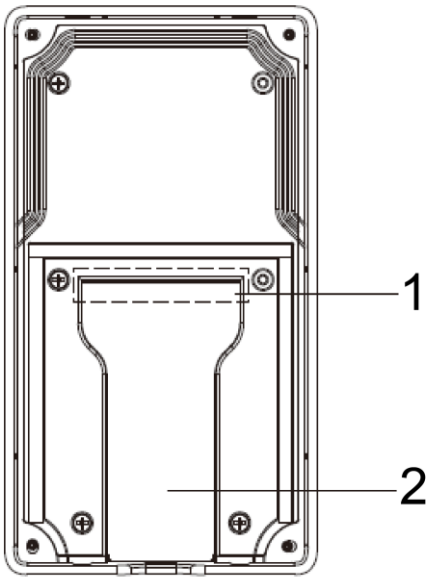


Table 2-5 Rear panel description

No.	Name	Description
1	Cable ports	See Figure 2-6 and Table 2-6.
2	Cable tray	You can thread the cable through the cable tray.

Figure 2-6 Cable connection

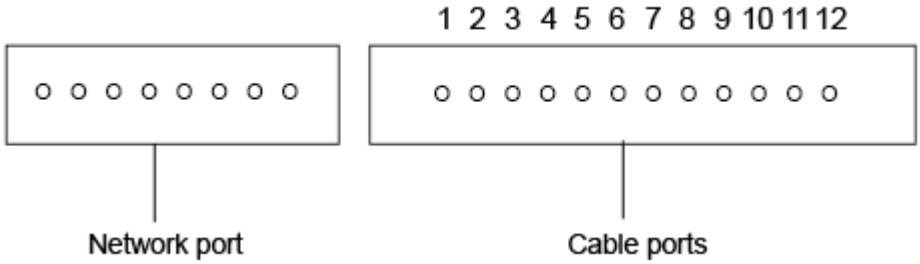


Table 2-6 Cable port description

No.	Name	No.	Name
1	ALM_COM	7	DOOR_FEED
2	ALM_NO	8	DOOR_NC
3	ALM_IN	9	DOOR_COM
4	RS485B	10	DOOR_NO
5	RS485A	11	GND
6	DOOR_OPEN	12	DC 12V

2.3 VTO2211G/VTO1201G

2.3.1 Front Panel

Figure 2-7 Front panel of VTO2211G/VTO1201G

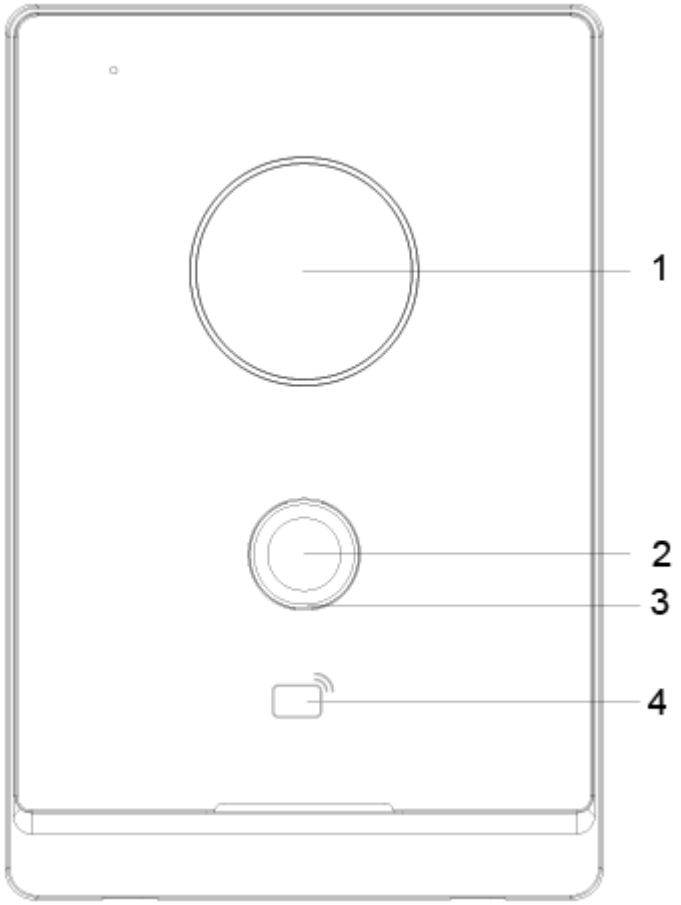


Table 2-7 Front panel description

No.	Description
1	Camera
2	Press the button to call an indoor monitor VTH or the management center.
3	Indicator light. ● Off: The device in standby mode; ● Solid green: VTO making a call; ● Solid blue: VTO during a call; ● Yellowish green: When you unlock the door through VTH while VTO is making a call. ● Bluish red: When you unlock the door through VTH while you are having a call with the VTO; ● Green breathing light: The network is disconnected.
4	Card reader (only for VTO2211G).

2.3.2 Rear Panel

Figure 2-8 Rear panel of VTO2211G/VTO1201G

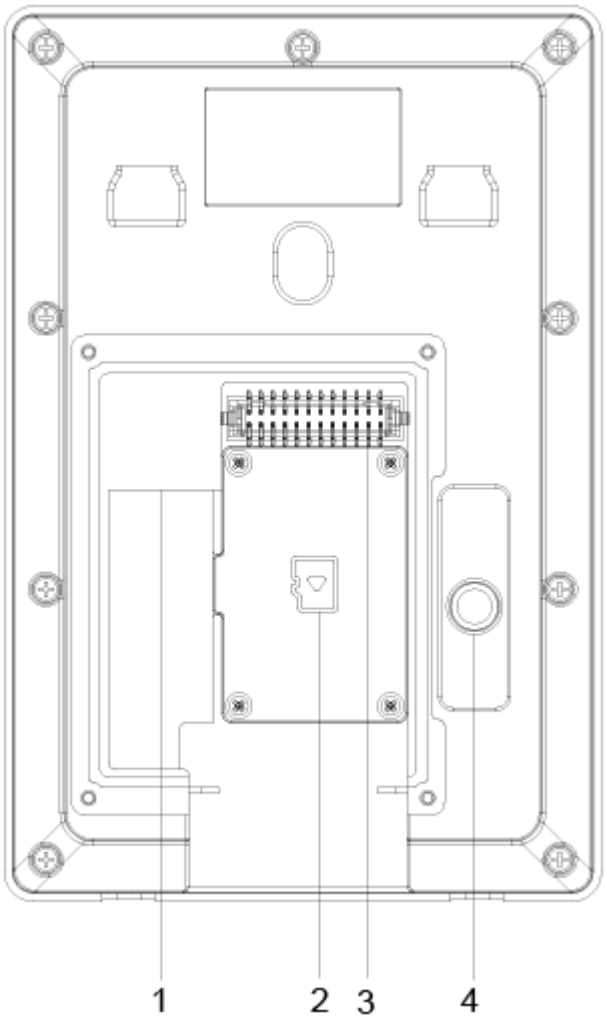


Table 2-8 Rear panel description

No.	Description	No.	Description
1	Network port	3	Ports
2	SD card cover	4	Tamper button

Figure 2-9 VTO2211G cable connection

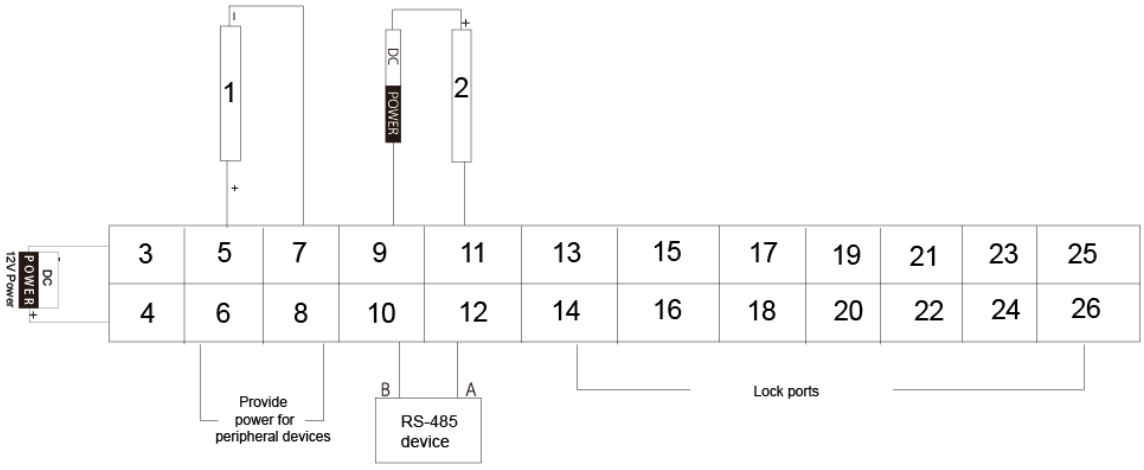


Table 2-9 Port description

No.	Name	No.	Name
1	Alarm input device	14	DOOR1_NC
2	Alarm output device	15	Not available
3	DC_IN-	16	DOOR1_COM
4	DC_IN+	17	Not available
5	ALARM_IN	18	DOOR1_NO
6	+12V_OUT	19	Not available
7	GND	20	GND
8	GND	21	Not available
9	ALARM_NO	22	DOOR1_FB
10	RS485B	23	Not available
11	ALARM_COM	24	GND
12	RS485A	25	Not available
13	Not available	26	DOOR1_PUSH

Figure 2-10 VTO1201G cable connection

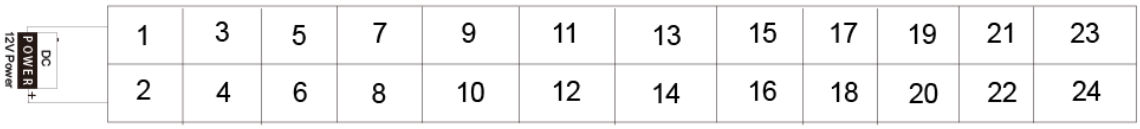


Table 2-10 Port description

No.	Name
1	DC_IN-
2	DC_IN+
3–24	Reserved function

Figure 2-11 Connecting lock cables

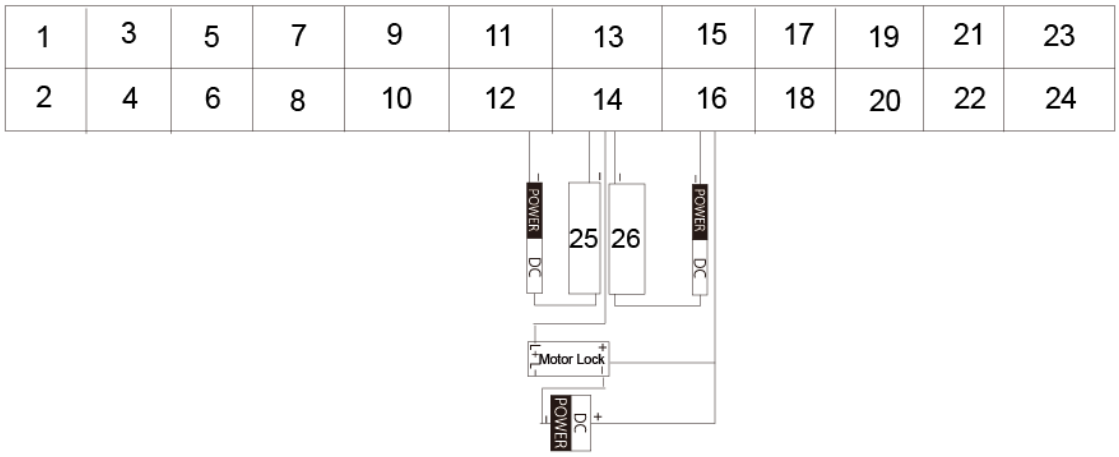


Table 2-11 Port description

No.	Name	No.	Name
1	DC_IN-	14	DOOR1_COM
2	DC_IN+	15	Not available
3	ALARM_IN	16	DOOR1_NO
4	+12V_OUT	17	Not available
5	GND	18	GND

No.	Name	No.	Name
6	GND	19	Not available
7	ALARM_NO	20	DOOR1_FB
8	RS485B	21	Not available
9	ALARM_COM	22	GND
10	RS485A	23	Not available
11	Not available	24	DOOR1_PUSH
12	DOOR1_NC	25	Magnetic lock
13	Not available	26	Electric lock

3 Installation

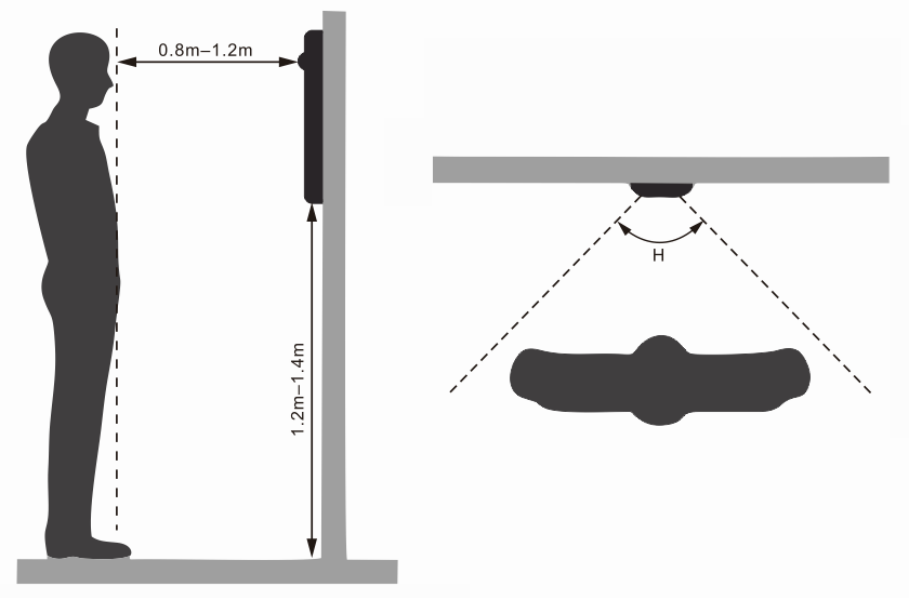
3.1 Notice

- Do not install the VTO at places with condensation, high temperature, grease or dust, chemical corrosion, direct sunlight, or zero shelter.
- The installation and adjustment must be finished by professionals, and do not disassemble the VTO.

3.2 Guidance

See Figure 3-1 the installation position. The VTO horizontal angle of view varies with different models, face the center of the VTO as much as possible.

Figure 3-1 Installation position reference



4 Configuration

This chapter introduces how to initialize, connect, and make primary configurations to VTOs and VTHs to realize basic functions, including device management, calling, and monitoring. For details, see the user manual.

4.1 Configuration Process

Before configuration, check each device and make sure there is no short circuit or open circuit.

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

Step 2 Configure VTOs. See "4.3 Configuring VTOs."

1) Initialize VTOs. See "4.3.1 Initialization."
2) Configure VTO numbers. See "4.3.2 Configuring VTO Numbers."
3) Configure VTO network parameters. See "4.3.3 Configuring Network Parameters."
4) Configure SIP Server. See "4.3.4 Configuring SIP Server."
5) Configure target room number and group call. See "4.3.5 Configuring Call No. and Group Call."
6) Add VTOs to the SIP server. See "4.3.6 Adding VTO."
7) Add room number to the SIP server. See "4.3.7 Adding Room Numbers."

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

Step 4 Verify Configuration. See "4.4 Verifying Configuration."

4.2 VDPConfig

You can download the "VDPConfig" and perform device initialization, IP address modification and system upgrading for multiple devices at the same time. For the details, see the corresponding user's manual.

4.3 Configuring VTOs

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.

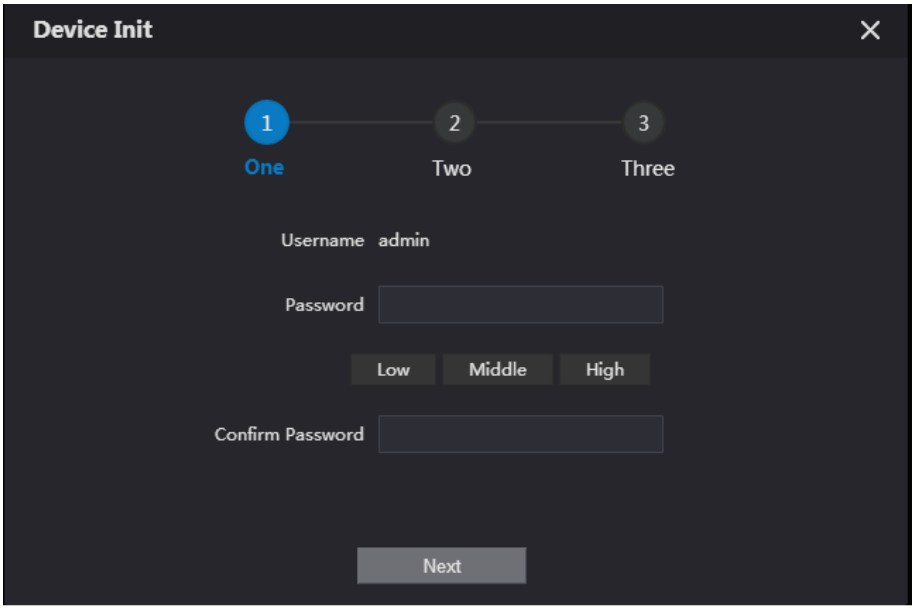
4.3.1 Initialization

The default IP address of VTO is 192.168.1.110, and make sure 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.

Figure 4-1 Device initialization



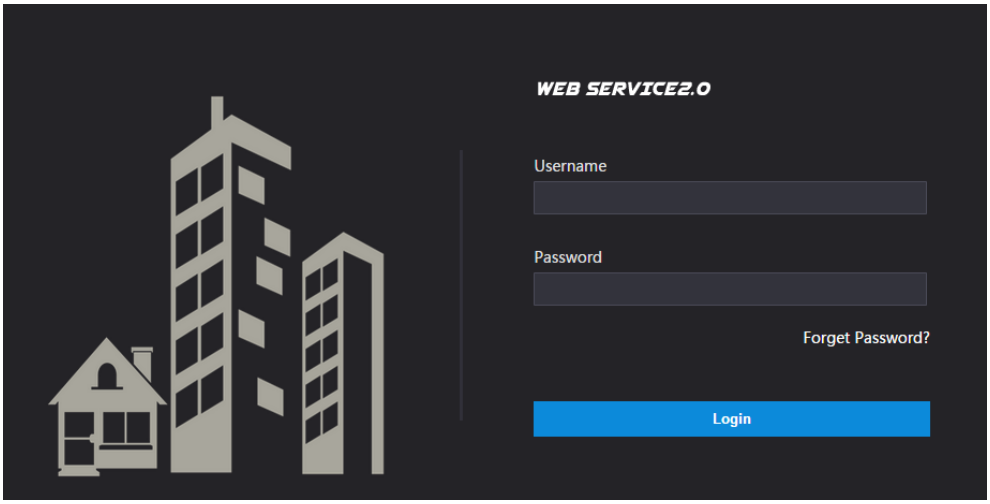
Step 3 Enter and confirm the password, and then click **Next**.
The email setting interface is displayed.

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**.

Figure 4-2 Login interface



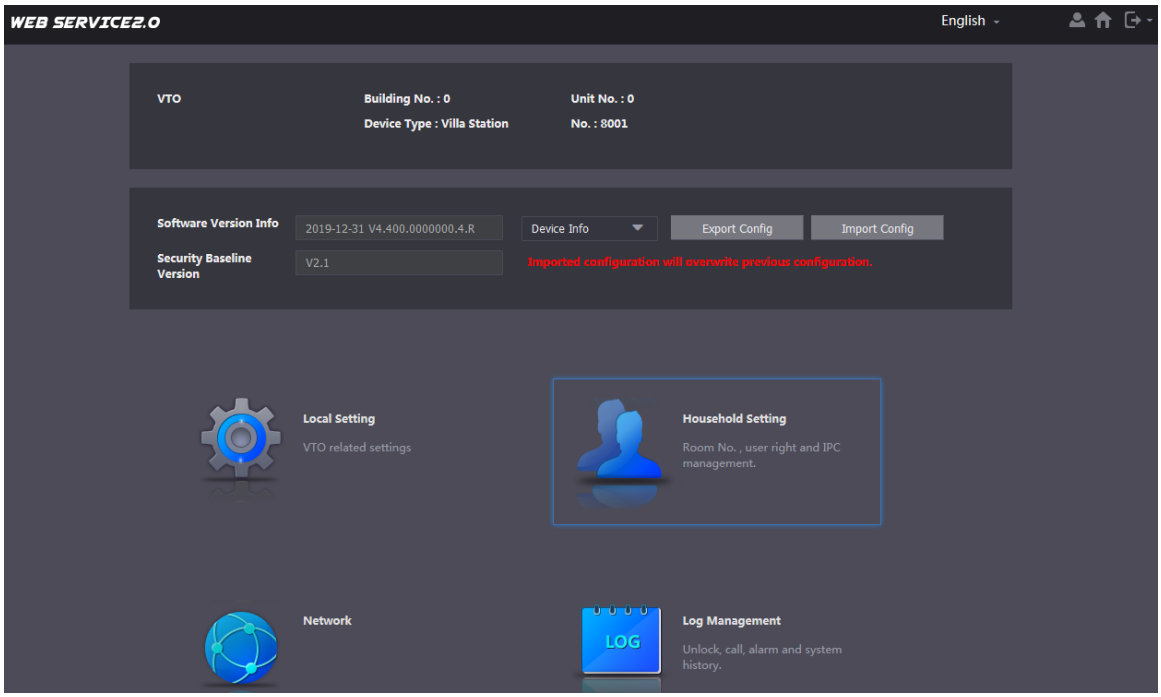
4.3.2 Configuring VTO Number

The VTO number can be used to differentiate each VTO, and it is normally configured according to apartment 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 as any room number.

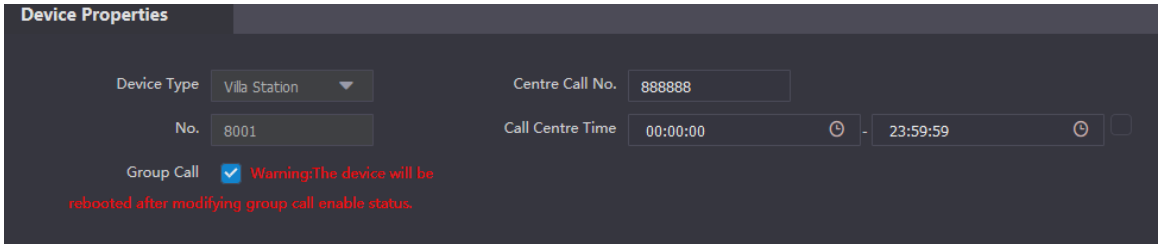
Step 1 Log in to the web interface of the VTO, and then the main interface is displayed.

Figure 4-3 Main interface



Step 2 Select Local Setting > Basic.

Figure 4-4 Device properties

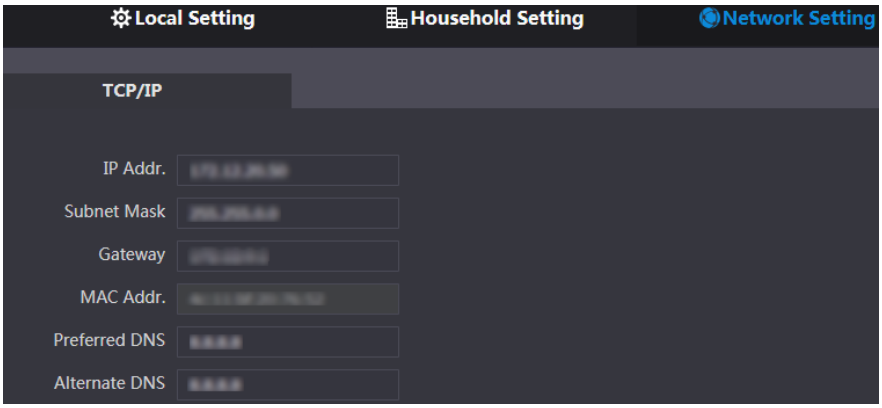


Step 3 In the **No.** input box, enter the VTO number you planned for the VTO you are operating, and then click **Confirm** to save.

4.3.3 Configuring Network Parameters

Step 1 Select Network Setting > Basic.

Figure 4-5 TCP/IP information



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

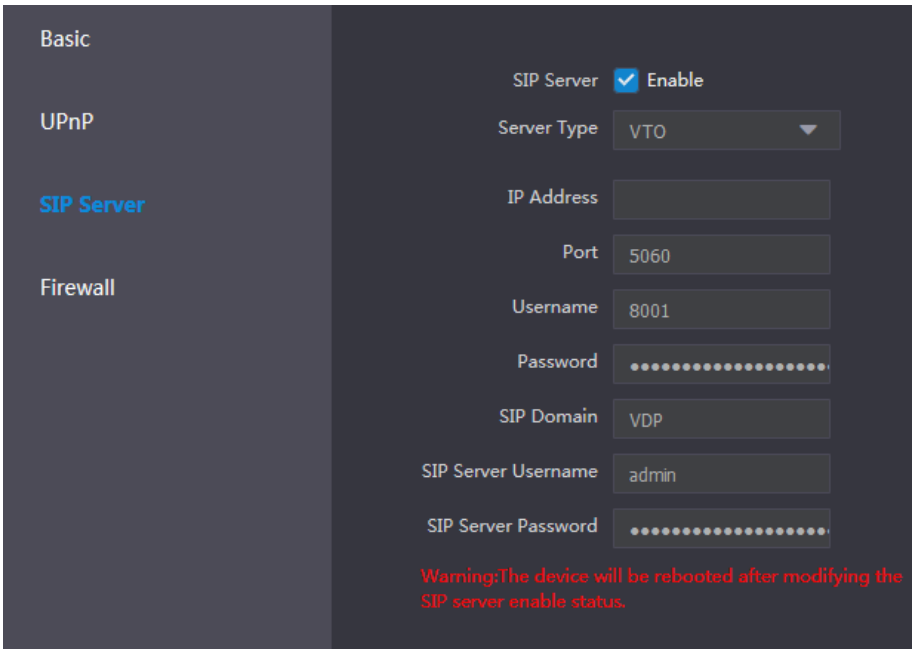
The VTO will restart, and you need to modify the IP address of your PC to the same network segment as the VTO to log in again.

4.3.4 Configuring SIP Server

The SIP server is required in the network to transmit intercom protocol, and then all the VTO and VTH connected to the same SIP server can make video calls among each other. You can use VTOs or other servers as SIP server.

Step 1 Select Network Setting > SIP Server.

Figure 4-6 SIP server



Step 2 Select the server type you need.

- If the VTO you are visiting works as SIP server
  Select the **Enable** check box at **SIP Server**, and then click **Save**.
  The VTO will restart, and after restarting, you can then add VTOs and VTH devices to the VTO you are operating. See "4.3.6 QAdding VTO and 4.3.7 Adding Room Number."

  If the VTO you are visiting does not work as SIP server, do not select the **Enable** check box at **SIP Server**, otherwise the connection will fail.
- If other VTO works as SIP server
  Select **VTO** in the **Server Type** list, and then configure the parameters. See Table 4-1.

Table 4-1 SIP server configuration

Parameter	Description
IP Addr.	The IP address of the VTO which works as SIP server.
Port	5060
Username	Keep the default value.
Password	
SIP Domain	VDP
SIP Server Username	The user name and password for the web interface of the SIP server.
SIP Server Password	

- If other servers work as SIP server
  Select **Express/DSS** in the **Server Type** list, and then see the corresponding manual for the detailed configuration.

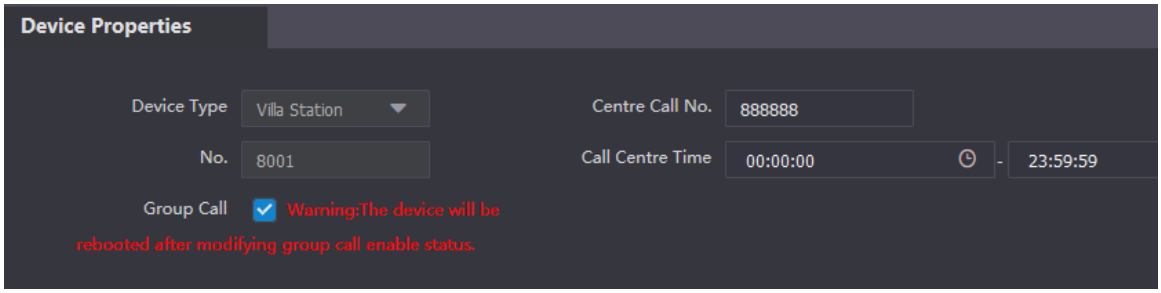
4.3.5 Configuring Call No. and Group Call

You need to configure call No. on each VTO, and then all the VTOs can call the defined room when you press the call button. On the SIP server, you can enable group call function, and when calling a master VTH, the extension VTHs will receive the call as well.

After enabling or disabling group call function the door station will restart.

Step 1 Select Local Setting > Basic.

Figure 4-7 Device properties



Step 2 In the **No.** input box, enter the room number you need to call, and then click **Confirm** to save. Repeat this operation on every villa VTO web interface.

Step 3 Log in to the web interface of the SIP server, and then select **Local Setting > Basic**.

Step 4 Select the **Group Call** check box, and then click **Confirm**.

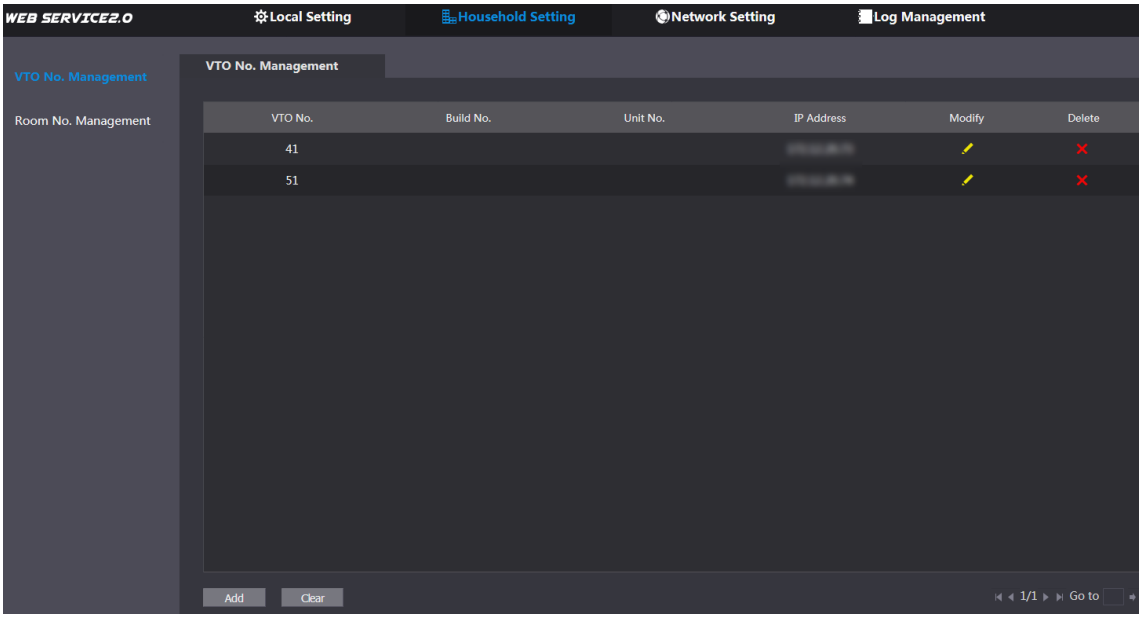
The VTO will restart, and when calling a master VTH, the extension VTH will receive the call as well.

4.3.6 Adding VTO

You can add VTOs to the SIP server, and all the VTOs connected to the same SIP server can make video calls among each other. This section applies to the condition in which a VTO works as SIP server, and if you are using other servers as SIP server, see the corresponding manual for the detailed configuration.

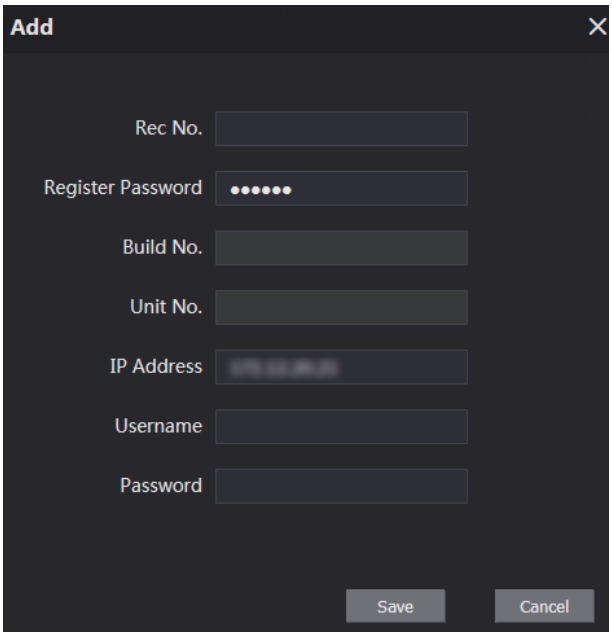
Step 1 Log in to the web interface of the SIP server, and then select **Household Setting > VTO No. Management**.

Figure 4-8 VTO No. management



Step 2 Click **Add**.

Figure 4-9 Add VTOs



Step 3 Configure the parameters, and be sure to add the SIP server itself too.

Table 4-2 Add VTOs

Parameter	Description
Rec No.	The VTO number you configured for the target VTO. See the details in "4.3.2 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**.

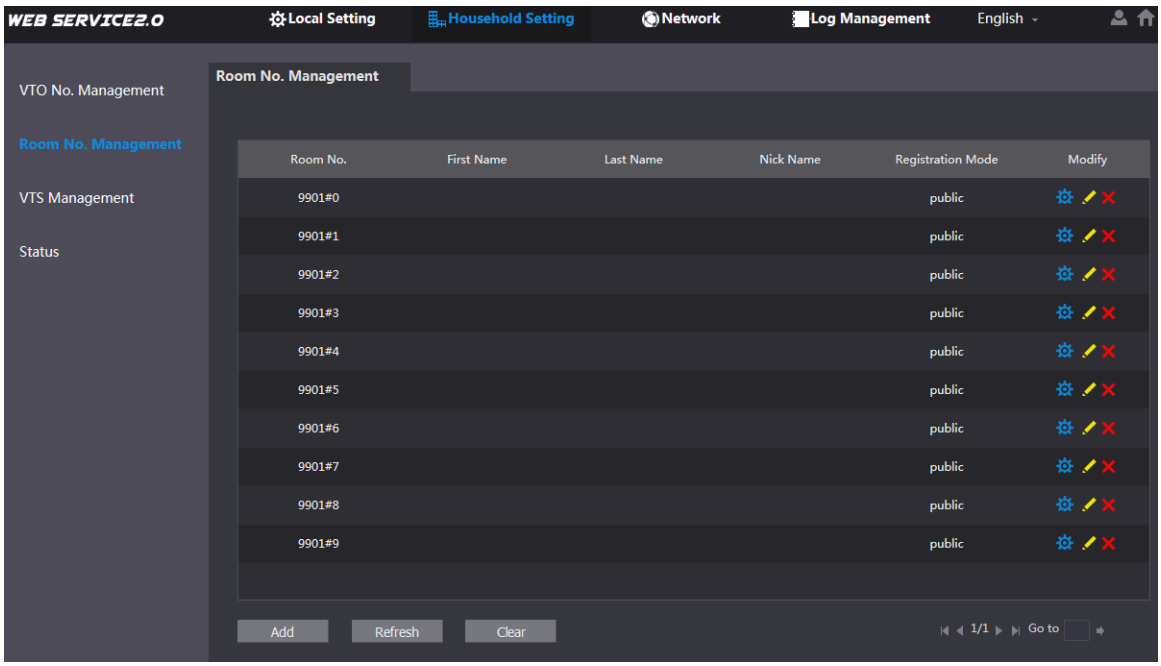
4.3.7 Adding Room Number

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

The room number can contain 6 digits of numbers or letters or their combination at most, and the room number must be unique.

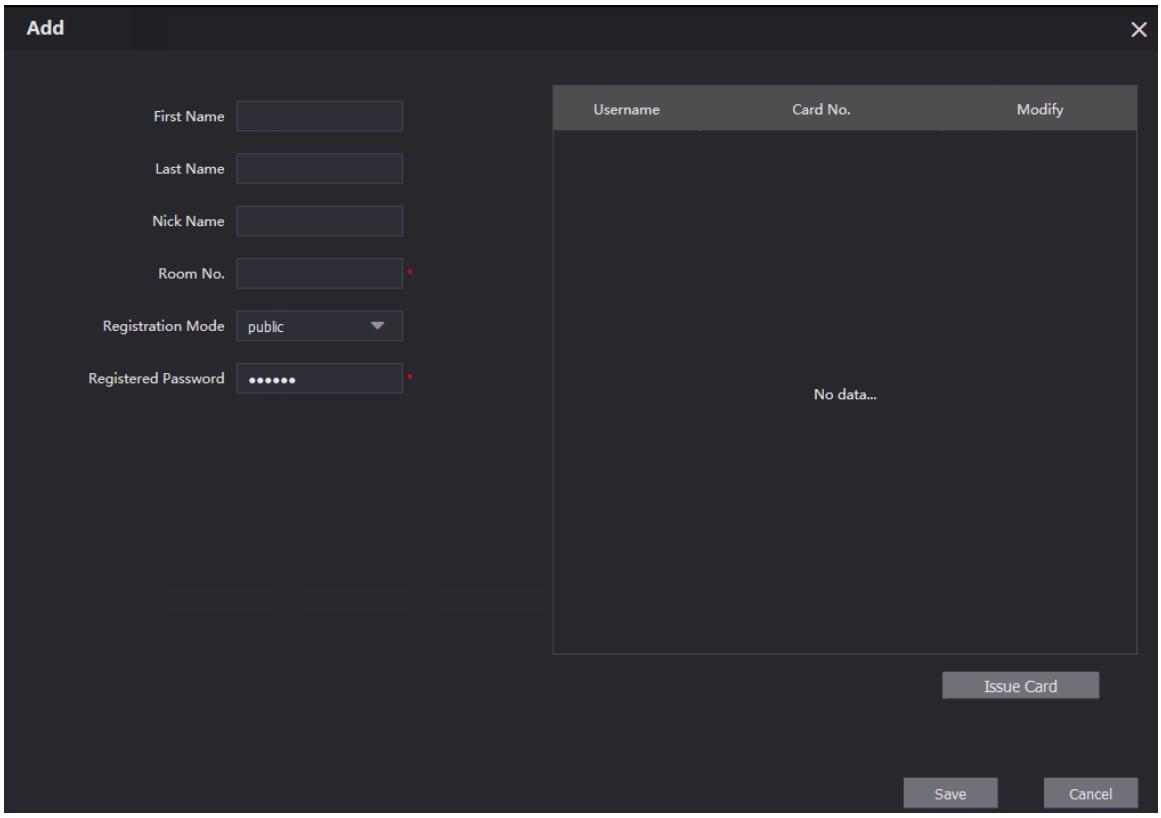
Step 1 Log in to the web interface of the SIP server, and then select **Household Setting** > **Room No. Management**.

Figure 4-10 Room No. Management



Step 2 Click **Add**.

Figure 4-11 Add single room number



Step 3 Configure room information.

Table 4-3 Room information

Parameter	Description
First Name	Enter the information you need to differentiate each room.
Last Name	
Nick Name	
Room No.	The room number you planned.

Parameter	Description
First Name	Enter the information you need to differentiate each room.
Last Name	
Nick Name	
	• If you use multiple VTHs, 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", and so on. • You can have 9 extension VTHs at most for one master VTH.
Registration Mode	Select **public**, and **local** is reserved for future use.
Registered Password	Keep the default value.

Step 4 Click **Save**.

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

4.4 Verifying Configuration

4.4.1 Calling VTH from VTO

Press the call button on the VTO to start a call with the VTH.

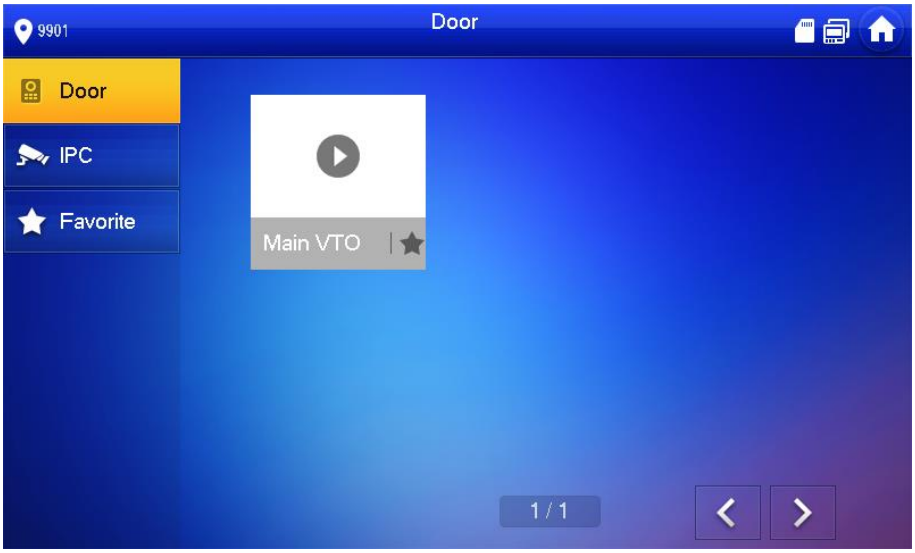
Figure 4-12 Call screen

Tap on the VTH to answer the call.

4.4.2 Watching Monitoring Videos on the VTH

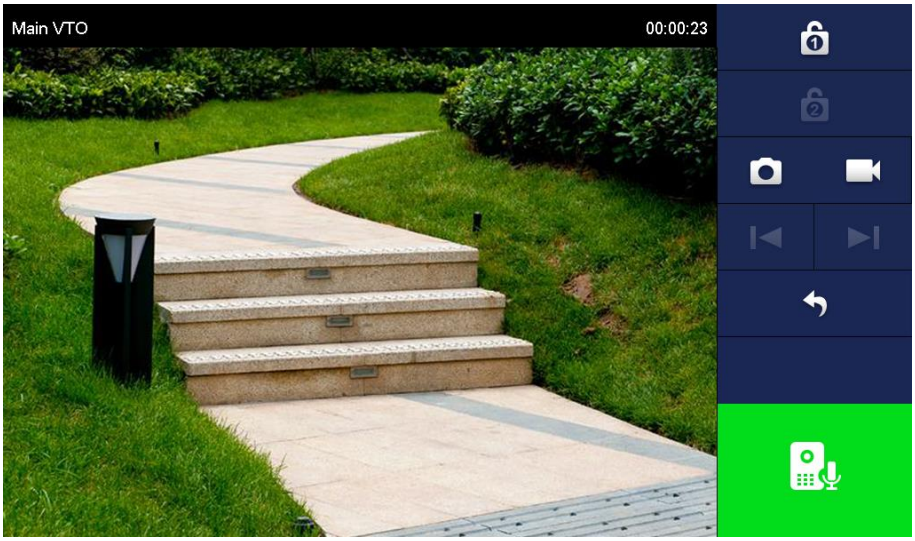
Step 1 In the main interface of the VTH, select **Monitor > Door**.

Figure 4-13 Door



Step 2 Select a VTO to watch monitoring videos.

Figure 4-14 Watching monitoring videos



5 App Installation and Adding Device

Scan the following QR code to download and install the app.

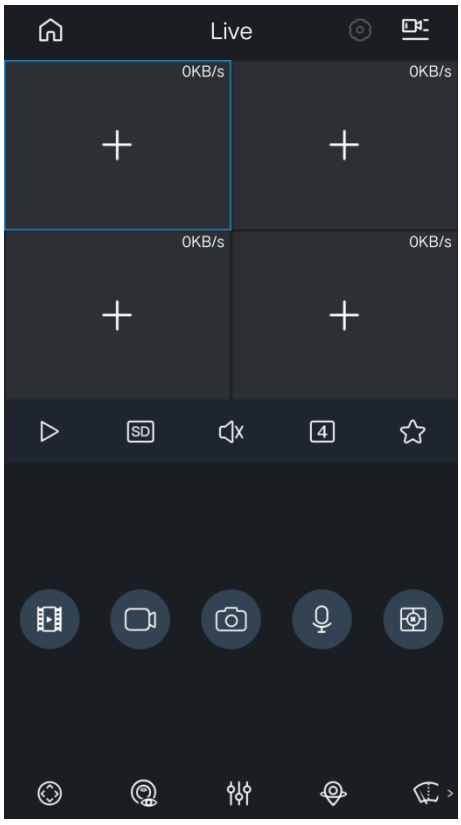
Before adding the VTO to the gDMSS Plus, you need to modify IP address of the VTO, make sure that the VTO and the router are connected to the same network, and connect the VTO to the power source.

Step 1 On your mobile phone, tap , and then follow the onscreen instructions until the region selection interface is displayed.

Step 2 Select a region.

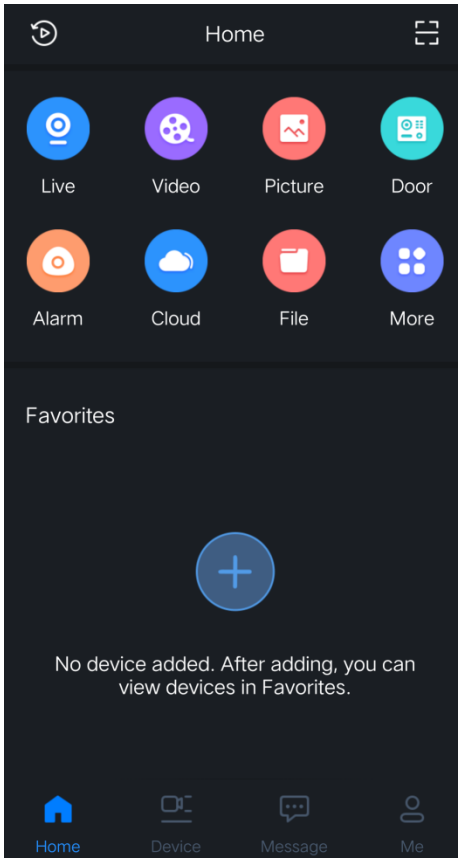
Step 3 Tap **Done** on the upper right corner of the interface.

Figure 5-1 Live



Step 4 Tap on the upper left corner of the **Live** interface.

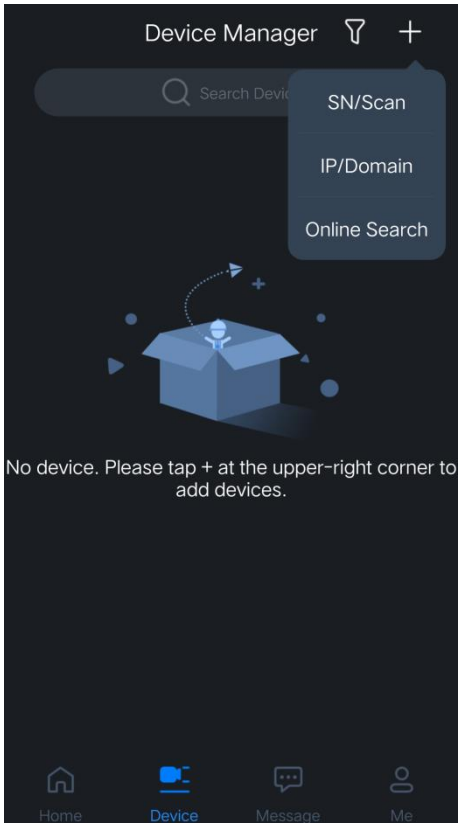
Figure 5-2 Home



Step 5 Tap  on the **Home** interface.

Step 6 Tap  on the upper-right corner of the **Device Manager** interface.

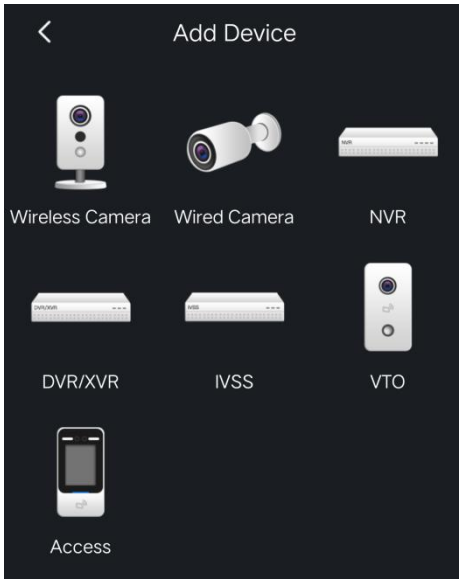
Figure 5-3 Device manager



5.1 Adding through Wired Network

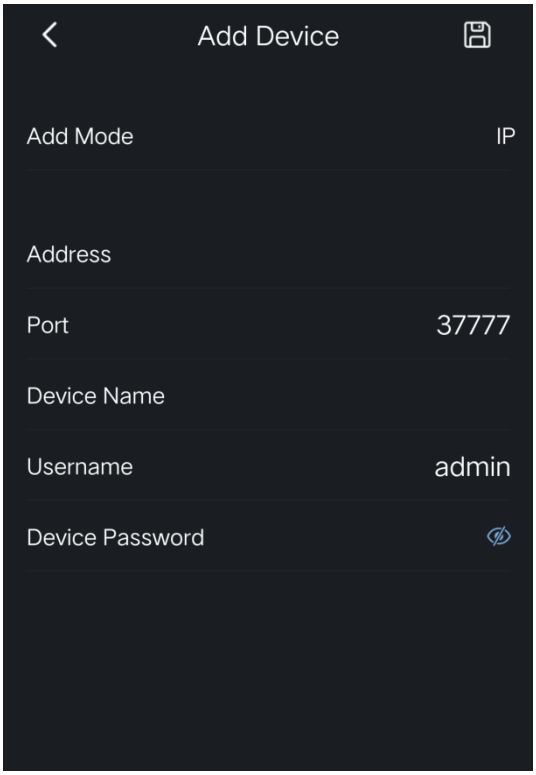
Step 1 Tap **IP/Domain** on Figure 5-3.

Figure 5-4 Add device



Step 2 Tap **VTO** on the **Add Device** interface.

Figure 5-5 Add device

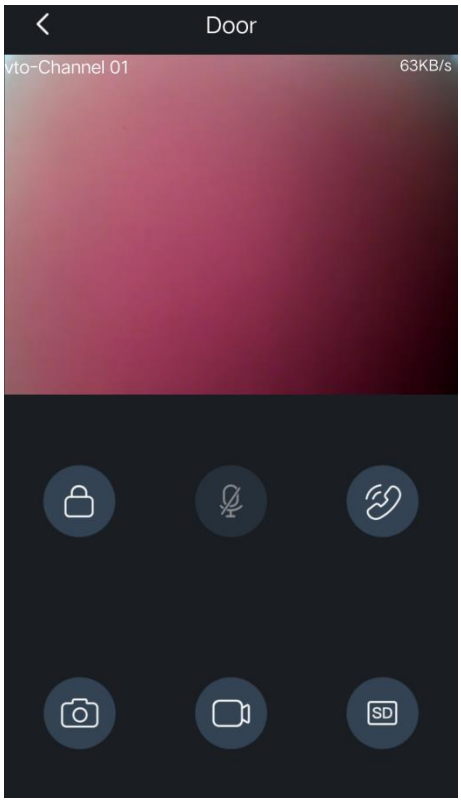


Step 3 Enter Address (IP address of the VTO), Device Name, and Device Password.

Step 4 Tap .

The VTO is added. You can watch videos captured by the VTO, call the VTO, unlock doors when there is call from the VTO, and more.

Figure 5-6 Door



5.2 Adding through Soft Access Point (AP)

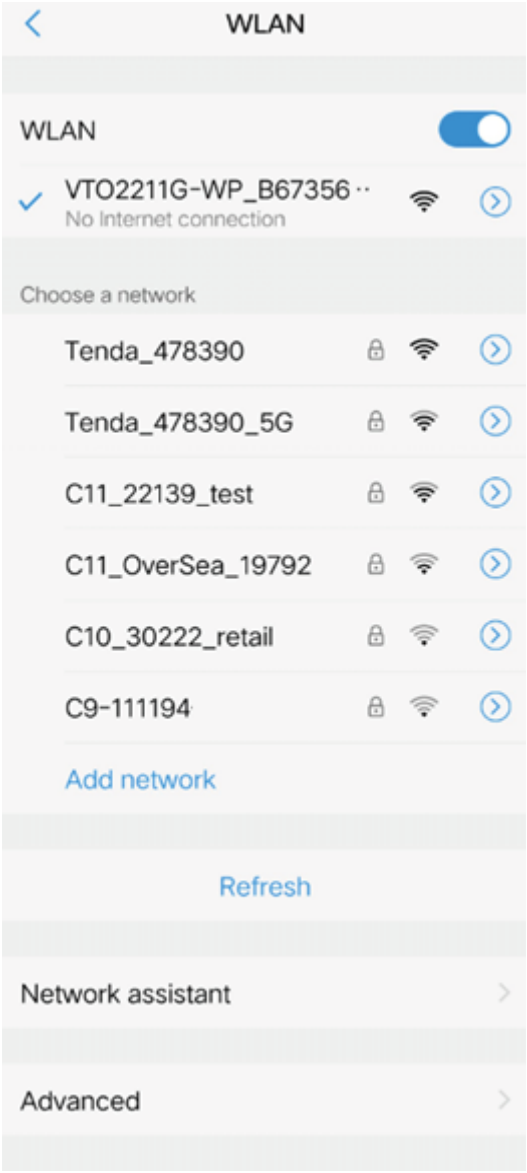
Step 1 Connect the door station to the power source.

Step 2 Go to the **WLAN** interface of your mobile phone.

Step 3 Press and hold the call button on the door station for over 5 seconds until you hear a beep.

Step 4 Connect your phone to the **VTO2211G-WP_b67356..** network.

Figure 5-7 Mobile phone WLAN



Step 5 Tap ⊞ on the upper right corner of the **Device Manager** interface (see Figure 5-3).

Step 6 Tap **SN/Scan** on Figure 5-3.

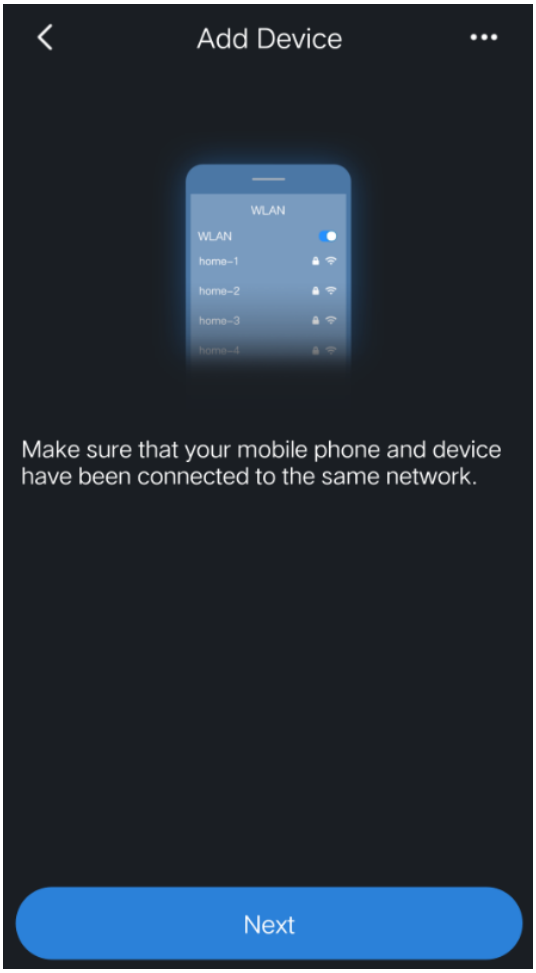
Figure 5-8 Scan the QR code

Step 7 Scan the QR code at the rear cover of the door station.

The QR code can also be found in **Network** > **Basic** > **P2P** on the web interface,

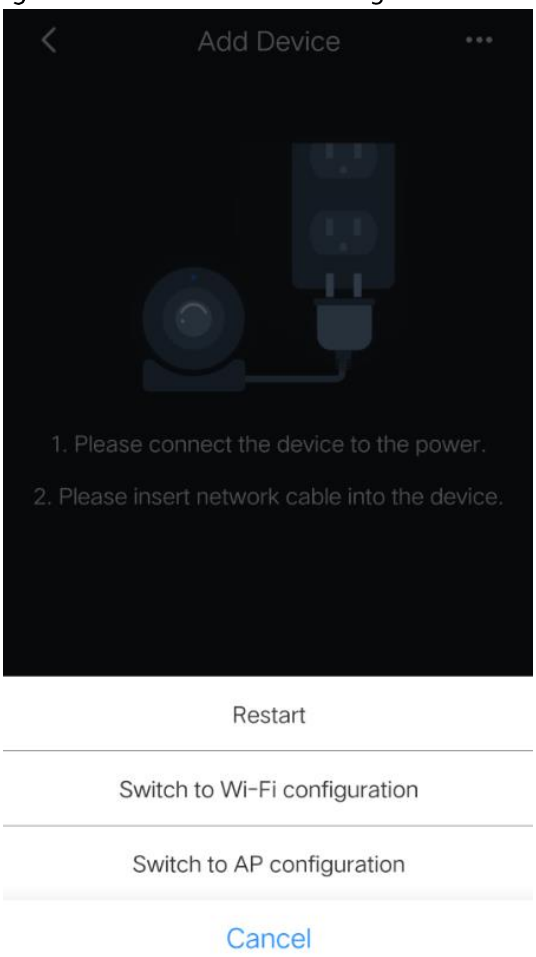
Step 8 Tap **Next**.

Figure 5-9 Add device



Step 9 Tap ••• on the upper-right corner.

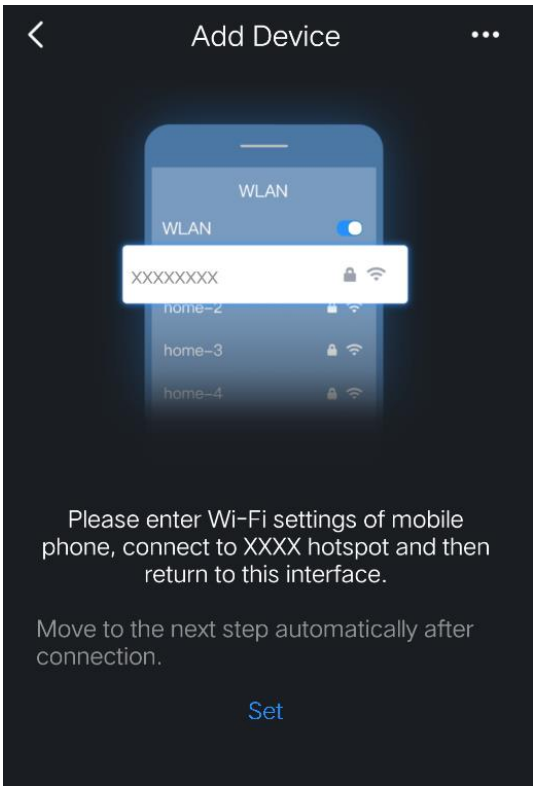
Figure 5-10 Select network configuration mode



Step 10 Select **Switch to AP Configuration**.

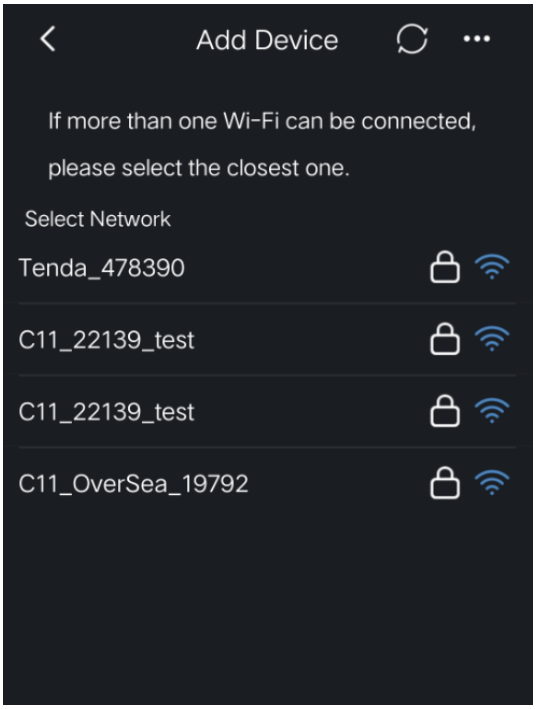
Step 11 Tap **Next**.

Figure 5-11 Set phone network



Step 12 Tap **Set**.

Figure 5-12 Select a Wi-Fi



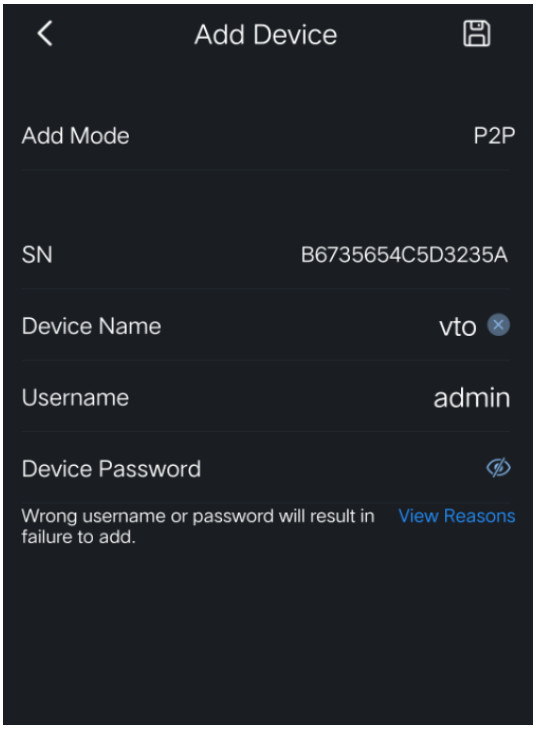
Step 13 Tap a Wi-Fi name.

Figure 5-13 Enter Wi-Fi password

Step 14 Enter the Wi-Fi password.

Step 15 Tap **Next**.

Figure 5-14 Add device



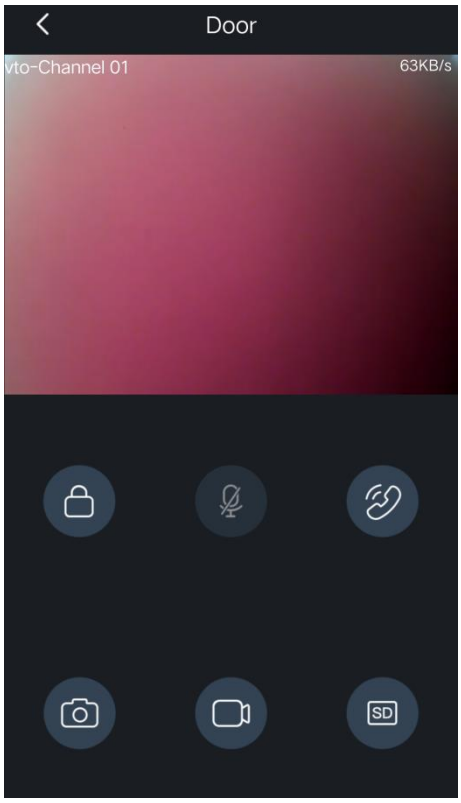
Step 16 Enter device name and device password (door station web login password).

Step 17 Tap .

The VTO is added. You can watch videos captured by the VTO, call the VTO, unlock doors when there is call from the VTO, and more.

After adding door stations to the App, you need to subscribe messages, and then push notifications can be sent to your phone.

Figure 5-15 Door



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.