

Villa Door Station (Version 4.5)

Quick Start Guide








Foreword

General

This manual introduces the structure, mounting process, and basic configuration of the villa 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
 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 Date
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 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 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 horizontally at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device, or put on the device anything filled with liquids.
- Install the device at a well-ventilated place 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

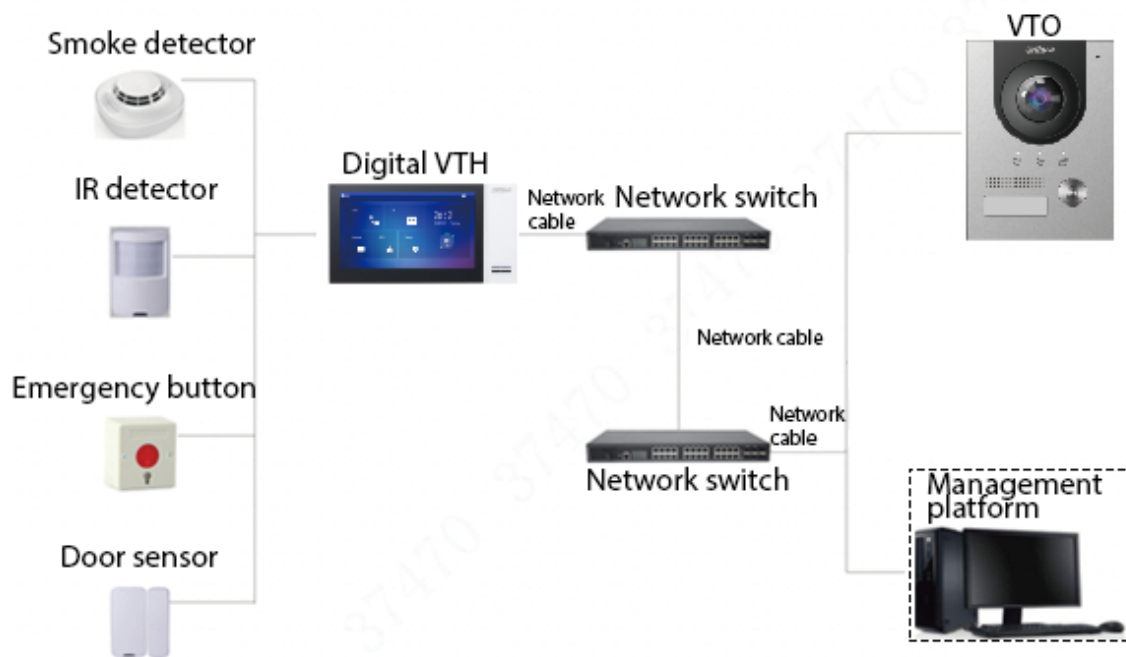
- The product must use electric wires that conform to your local requirements.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Network Diagram	1
2 Appearance	2
2.1 VTO2101E-P.....	2
2.1.1 Front Panel	2
2.1.2 Rear Panel	3
2.2 VTO2202F-P-S2/ VTO2202F-P/VTO2202F/VTO2201F-P.....	4
2.2.1 Front Panel	4
2.2.2 Rear Panel	5
2.3 VTO2111D-P-S2/VTO1101D-P	6
2.3.1 Front Panel	6
2.3.2 Rear Panel	7
2.4 VTO3211D-P-S2.....	8
2.4.1 Front Panel	8
2.4.2 Rear Panel	9
2.5 VTO3221E-P.....	10
2.5.1 Front Panel	10
2.5.2 Rear Panel	11
2.6 VTO2211G-P/VTO1201G-P.....	12
2.6.1 Front Panel	12
2.6.2 Rear Panel	13
3 Installation	15
4 Configuration	16
4.1 Procedure.....	16
4.2 Configuration Tool	16
4.3 Configuring VTO	16
4.3.1 Initialization	16
4.3.2 Configuring VTO Number	17
4.3.3 Configuring Network Parameters.....	18
4.3.4 Configuring SIP Server	19
4.3.5 Configuring Call Number and Group Call.....	20
4.3.6 Adding VTOs	20
4.3.7 Adding Room Number.....	21
4.4 Commissioning	23
4.4.1 VTO Calling VTH.....	23
4.4.2 VTH Monitoring VTO.....	23
5 EasyViewer Plus	25
Appendix 1 Cybersecurity Recommendations	26

1 Network Diagram

Figure 1-1 Network diagram



In certain applications such as villa, Management Center/Platform is usually unnecessary.

2 Appearance

2.1 VTO2101E-P

2.1.1 Front Panel

Figure 2-1 VTO2101E-P

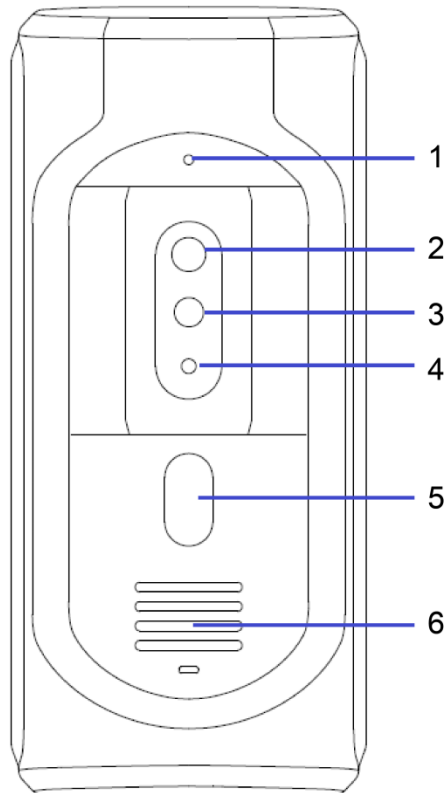


Table 2-1 Front panel description

No.	Name	Description
1	Microphone	—
2	Camera	—
3	IR illumination light	Provides extra IR light for the camera when it is dark.
4	Light sensor	Detects ambient lighting condition.
5	Call button	Call VTHs or the management center.
6	Speaker	—

2.1.2 Rear Panel

Figure 2-2 VTO2101E-P

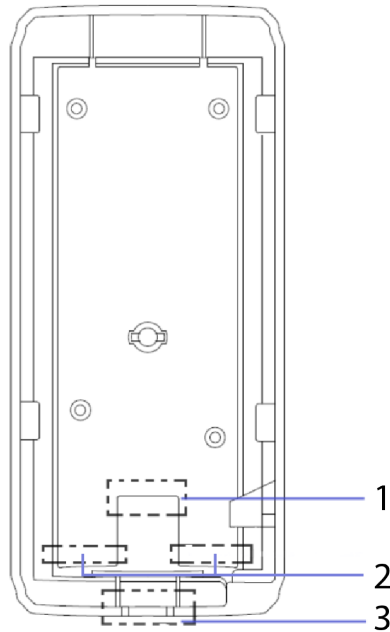


Table 2-2 Rear panel description

No.	Name	Description
1	Network port	Connects to the network cable.
2	RS-485 ports	See the figure and the table below.
3	Cable outlet	Thread the cables here.

Figure 2-3 Cable connection

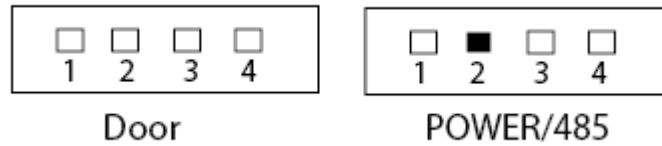


Table 2-3 Port description

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

2.2 VTO2202F-P-S2/ VTO2202F-P/VTO2202F/VTO2201F-P

2.2.1 Front Panel

Figure 2-4 Front panel

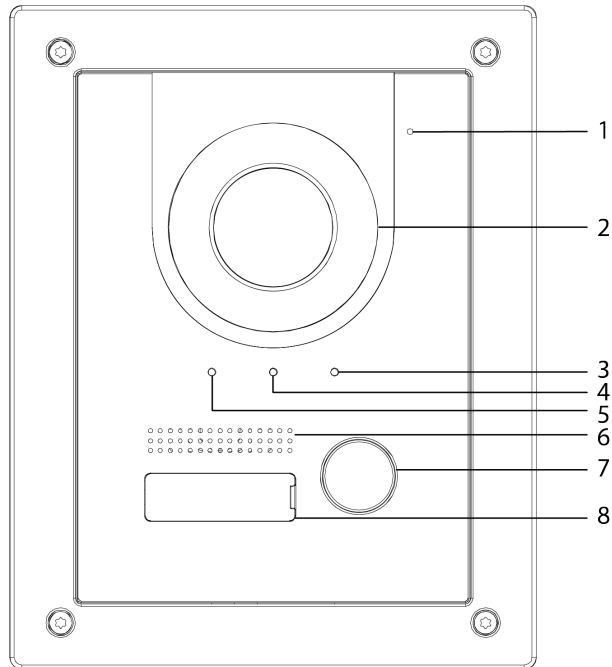


Table 2-4 Front panel description

No.	Name	Description
1	Microphone	—
2	Camera	—
3	Indicator	On: Door unlocked.
4		On: In a call.
5		On: Calling.
6	Speaker	—
7	Call button	Call other VTHs or the management center.
8	Name tag	Host name.

2.2.2 Rear Panel

Figure 2-5 Rear panel

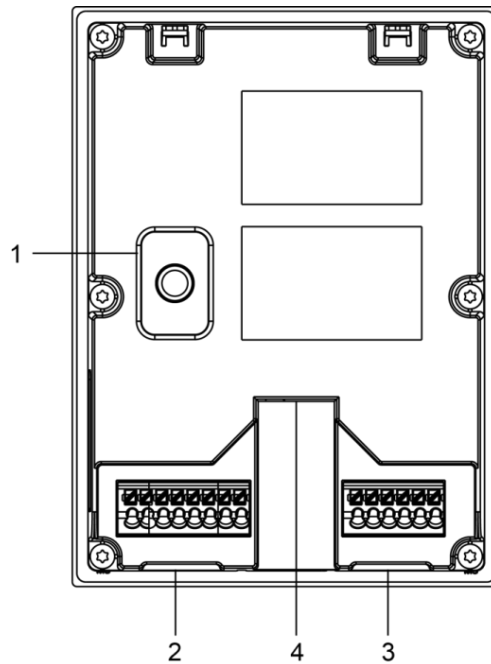



Table 2-5 Rear panel description

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	Port	From left to right: GND +12V_OUT RS485_B RS485_A ALARM_NO ALARM_COM VTO2202F-P-S2: 2-wire + (48V); VTO2202F-P and VTO2202F: EOC1 (+12V); VTO2201F: +24V. VTO2202F-P-S2: 2-wire - (GND); VTO2202F-P and VTO2202F: EOC2 (GND); VTO2201F: GND.
3		From left to right: DOOR_BUTTON DOOR_FB GND DOOR_NC DOOR_COM DOOR_NO
4	Ethernet port	Connects to the network with an Ethernet cable.  Only models with "P" support PoE.

2.3 VTO2111D-P-S2/VTO1101D-P

2.3.1 Front Panel

Figure 2-6 Front panel

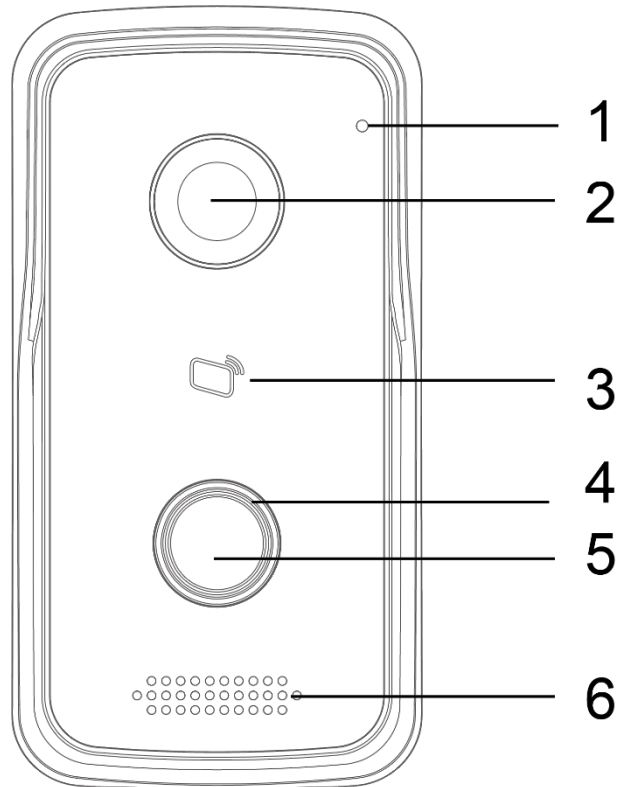


Table 2-6 Front panel description

No.	Name	Description
1	Microphone	—
2	Camera	—
3	Card reading area	Swipe to unlock or issue card.
4	Indicator	<ul style="list-style-type: none">● Solid blue: Standby mode.● Flashes blue: Calling or there is no network.
5	Call button	Call VTHs or the management center.
6	Speaker	—

2.3.2 Rear Panel

Figure 2-7 Rear panel

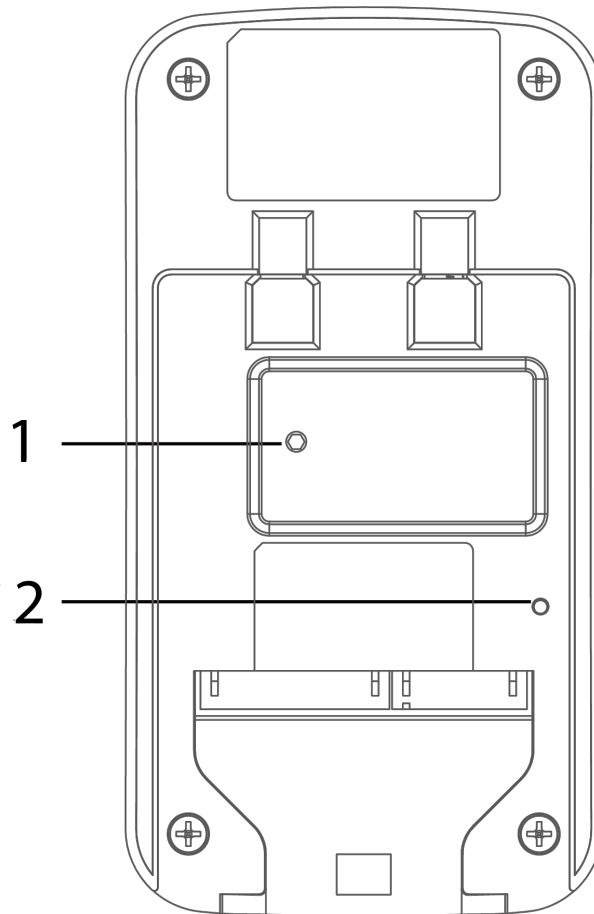


Table 2-7 Rear panel description

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	RESET	Press and hold it for 10 seconds to reset all settings.

Figure 2-8 Cable connection

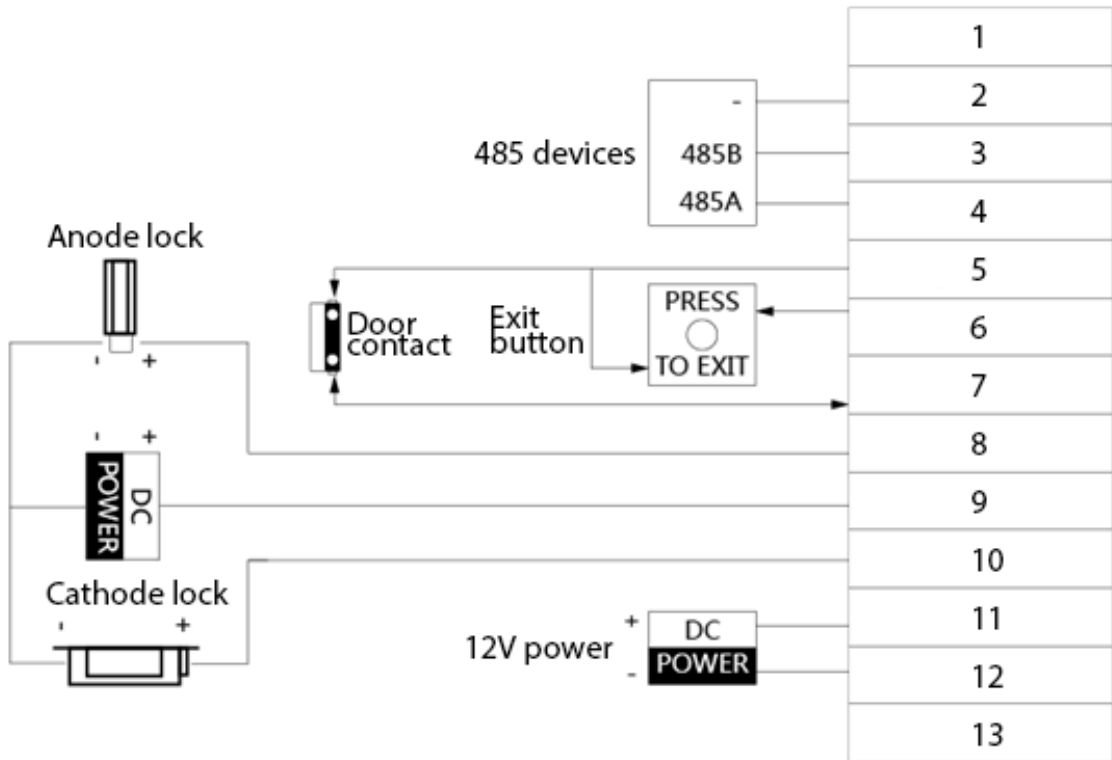


Table 2-8 Port description

No.	Description	No.	Description
1	N/A	8	NC
2	GND	9	COM
3	485_B	10	NO
4	485_A	11	GND
5	GND	12	12V
6	UNLOCK	13	NET
7	FEEDBACK	—	—

2.4 VTO3211D-P-S2

2.4.1 Front Panel

The number of buttons on the front panel varies with models. VTO3211D-P-S2 has one button, VTO3211D-P2-S2 has two buttons, and VTO3211D-P4-S2 has four buttons. Here we take VTO3211D-P4-S2 as an example.

Figure 2-9 VTO3211D-P4-S2

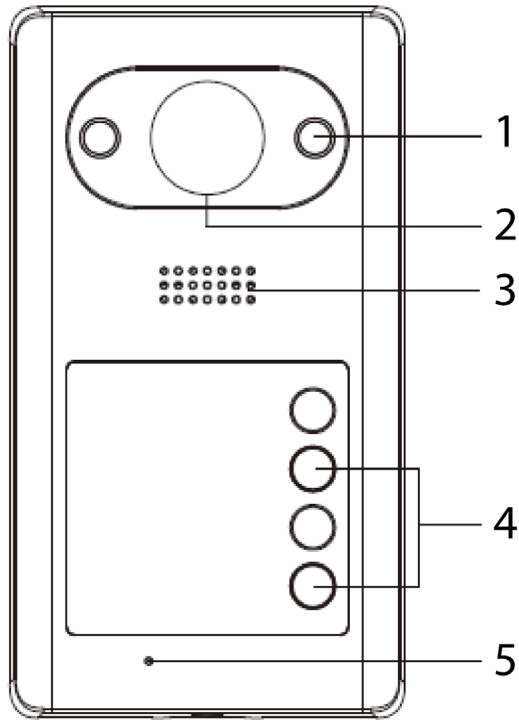


Table 2-9 Front panel description

No.	Name	Description
1	IR illuminator	Provides extra IR light for the camera when it is dark.
2	Camera	—
3	Speaker	—
4	Call button	Call VTHs or the management center.
5	Microphone	—

2.4.2 Rear Panel

Figure 2-10 VTO3211D-P4

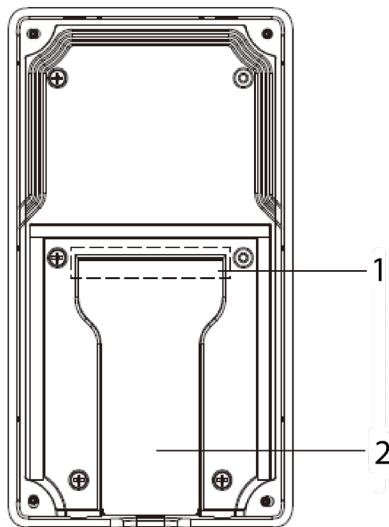


Table 2-10 Rear panel description

No.	Name	Description
1	Cable ports	See the figure and the table below.
2	Cable outlet	Thread the cables here.

Figure 2-11 Cable connection

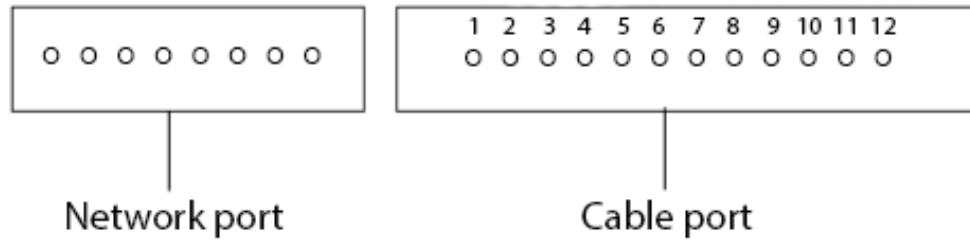


Table 2-11 Cable port description

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

2.5 VTO3221E-P

2.5.1 Front Panel

Figure 2-12 Front panel

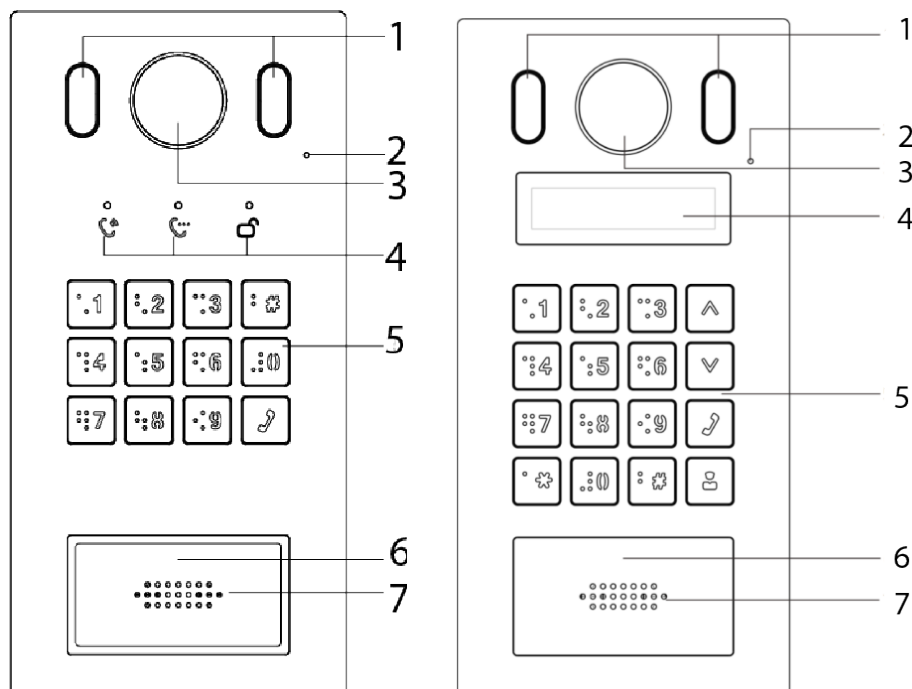


Table 2-12 Front panel description

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

2.5.2 Rear Panel

Figure 2-13 VTO3221E-P

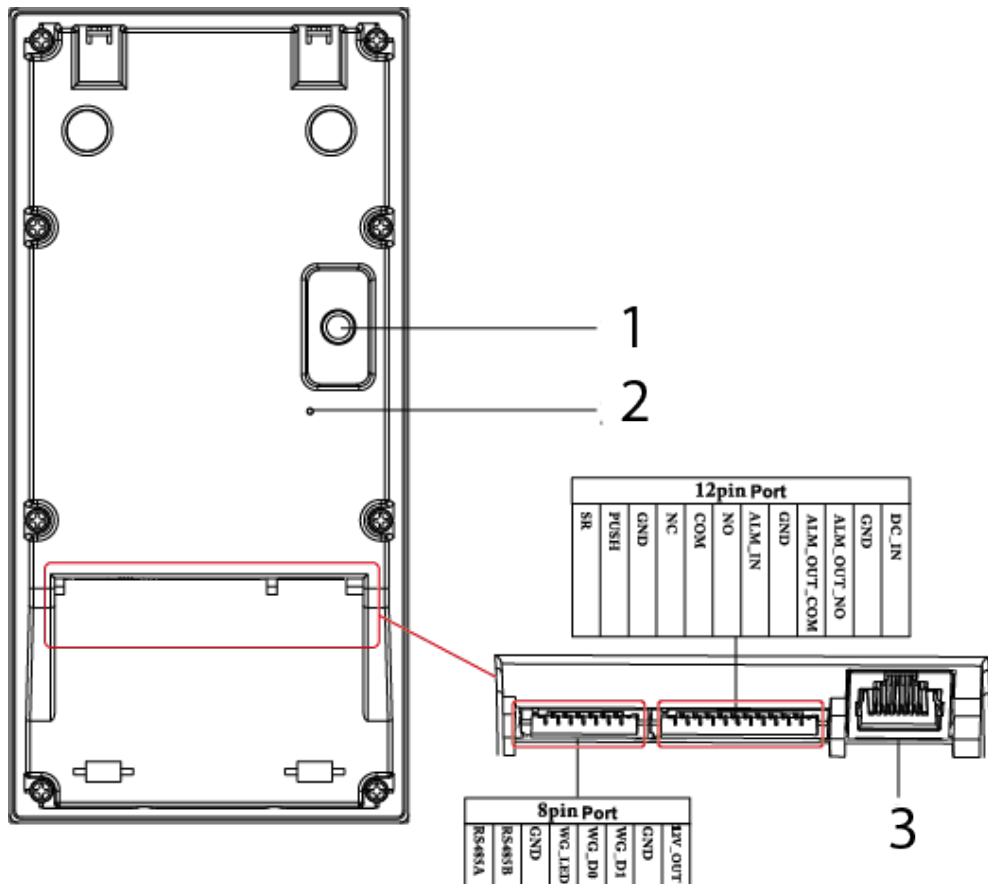


Table 2-13 Rear panel description

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	Reset button	Press and hold it for 10 s to reset all settings.
3	Ethernet port	Connects to the Ethernet cable.

2.6 VTO2211G-P/VTO1201G-P

2.6.1 Front Panel

Figure 2-14 Front panel of VTO2211G/VTO1201G

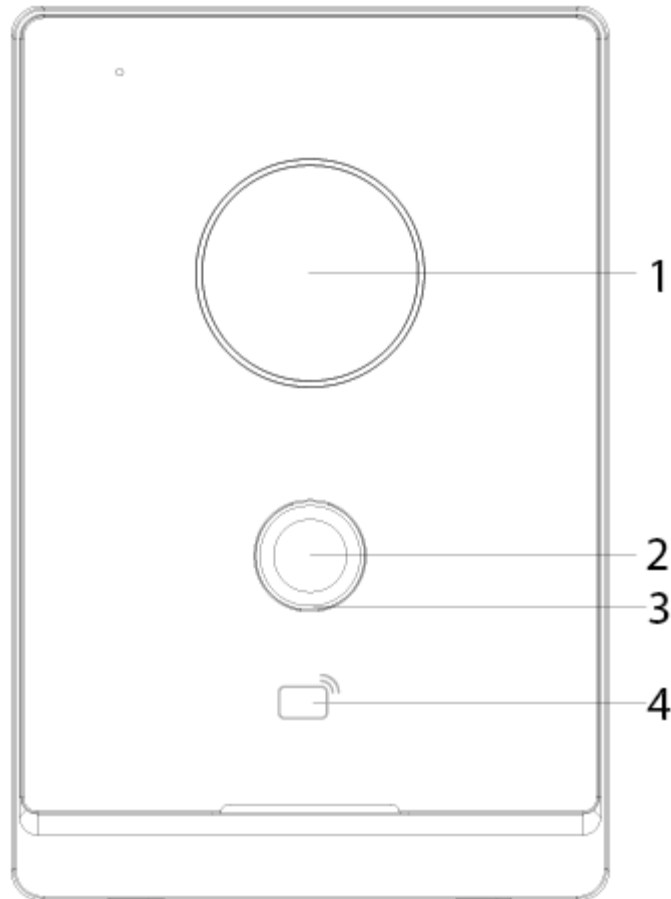


Table 2-14 Front panel description

No.	Name	Description
1	Camera	—
2	Call button	Call VTHs or the management center.
3	Indicator	<ul style="list-style-type: none">● Off: The device is in standby mode.● Solid green: Making a call.● Solid blue: In a call.● Yellow-green: Door unlocked by VTH while the VTO is making a call.● Red-blue: Door unlocked by VTH when the VTO is in a call.● Blue breathing: Network disconnected.
4	Card reading area	Swipe a card here to unlock the door (only for VTO2211G-P).

2.6.2 Rear Panel

Figure 2-15 Rear panel of VTO2211G-P/VTO1201G-P

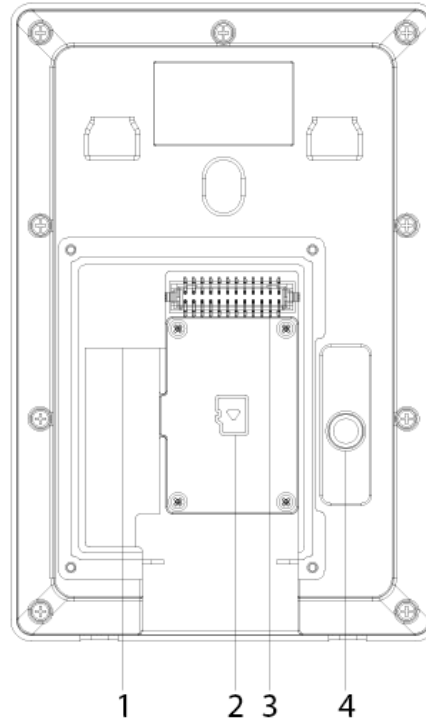
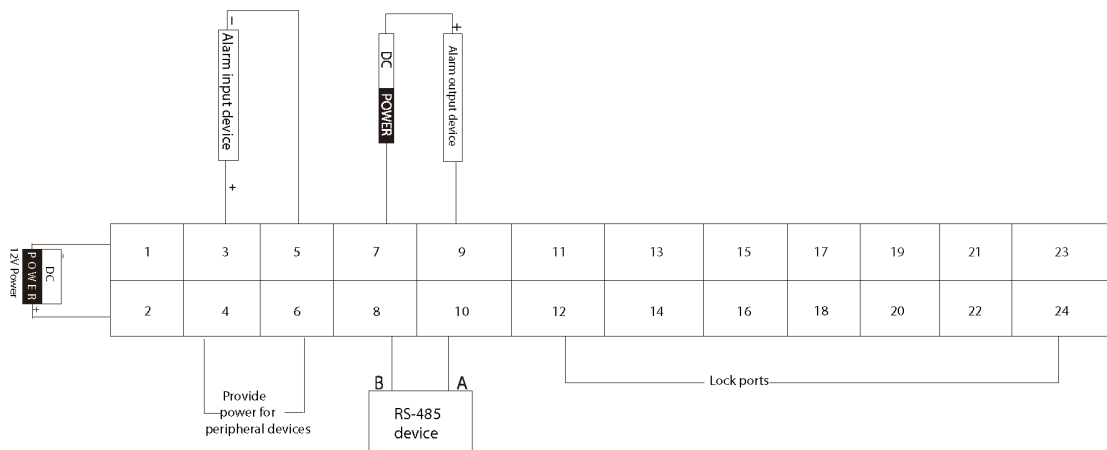


Table 2-15 Rear panel description

No.	Description	No.	Description
1	Network port	3	Ports
2	SD card cover	4	Anti-tampering switch

Figure 2-16 VTO2211G-P cable connection



Ports 12, 14, 16, 18, 20, 22 and 24 are used to connect to locks.

Table 2-16 Port description

No.	Name	No.	Name
1	DC_IN-	13	Not available
2	DC_IN+	14	DOOR1_COM

No.	Name	No.	Name
3	ALARM_IN	15	Not available
4	+12V_OUT	16	DOOR1_NO
5	GND	17	Not available
6	GND	18	GND
7	ALARM_NO	19	Not available
8	RS485B	20	DOOR1_FB
9	ALARM_COM	21	Not available
10	RS485A	22	GND
11	Not available	23	Not available
12	DOOR1_NC	24	DOOR1_PUSH

Figure 2-17 VTO1201G-P cable connection

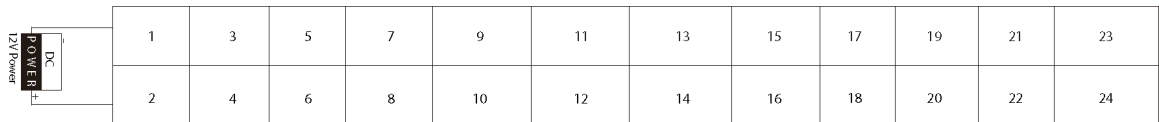
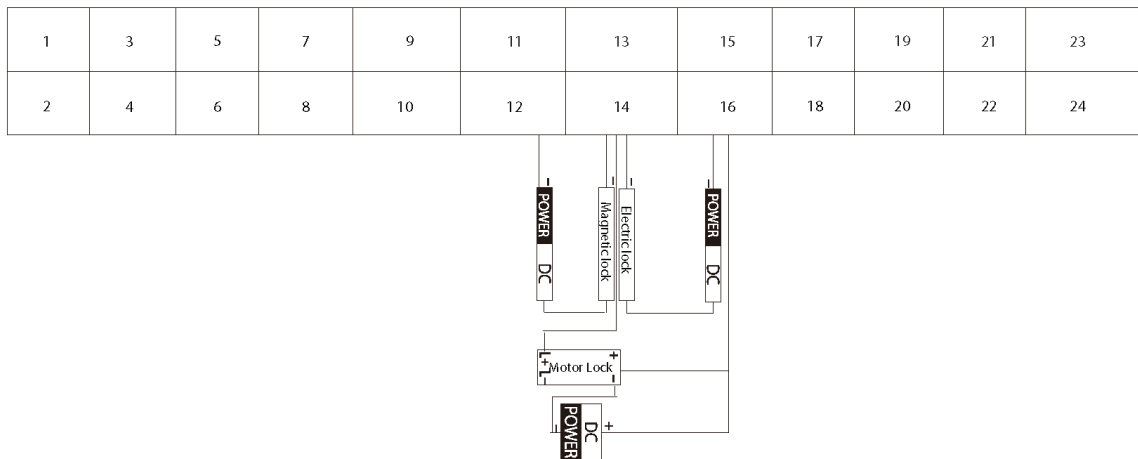


Table 2-17 Port description

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

Figure 2-18 Lock cable connection

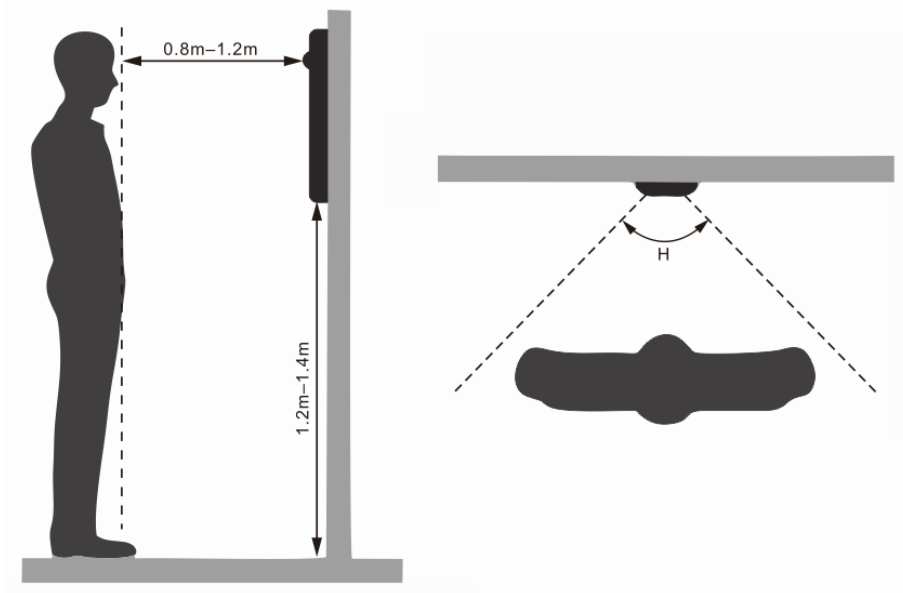


You can connect a magnetic lock or electric lock as needed. See the above figure for the port connection rules.

3 Installation

- Installation and configuration must be done by professional teams. Contact technical support if you need to repair the device.
- See the figure below for the installation position. The horizontal view angle of the device varies with models, and the human face should aim at the center of the device.

Figure 3-1 Installation position



4 Configuration

This chapter introduces basic configurations to the VTO and VTH devices. See the user's manual for details.



Interfaces might vary with software version. The actual interface shall prevail.

4.1 Procedure



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

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

Step 2 Configure the VTO. See "4.3 Configuring VTO".

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

Step 4 Check if all settings are correct. See "4.4 Commissioning".

4.2 Configuration Tool

You can download the configuration tool "VDPConfig" and use it to configure and update multiple devices. For more details, see the corresponding user's manual.

4.3 Configuring VTO

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

4.3.1 Initialization

Make sure that the PC is in the same network segment.

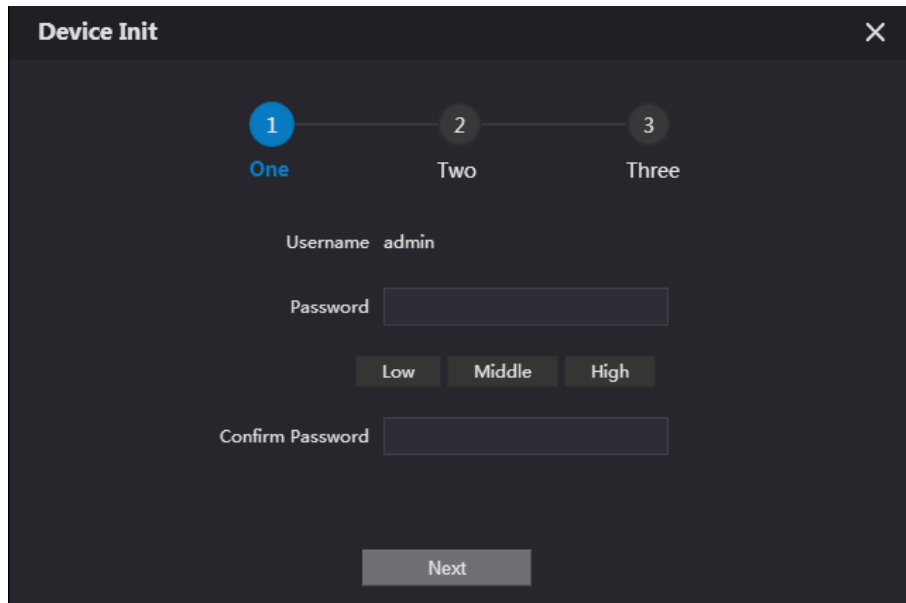
Step 1 Power on the VTO.

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 4-1 Device initialization



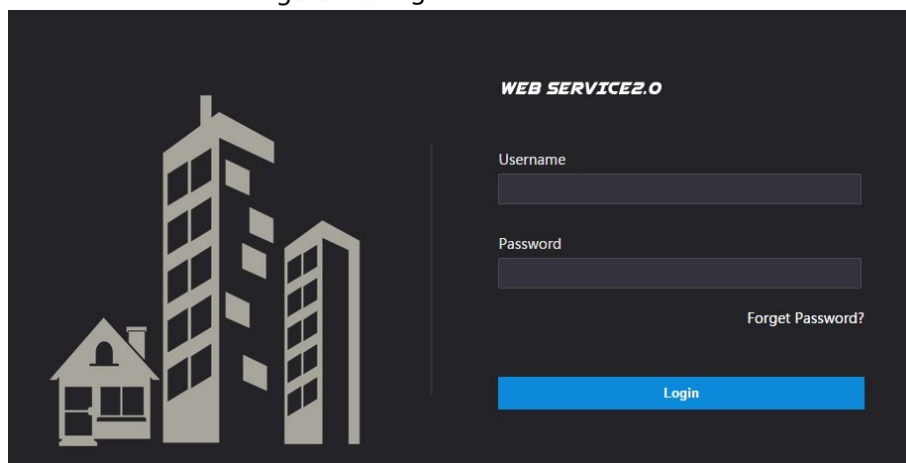
The screenshot shows a 'Device Init' window with a progress indicator at the top showing three steps: 1 (One), 2 (Two), and 3 (Three). Step 1 is currently active. Below the progress indicator, the 'Username' field is pre-filled with 'admin'. The 'Password' field is empty, with three buttons below it labeled 'Low', 'Middle', and 'High' for selecting password strength. The 'Confirm Password' field is also empty. A 'Next' button is located at the bottom center of the window.

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

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

Step 5 Click **Next**, and then click **OK** to go to the login interface.

Figure 4-2 Login interface



The screenshot shows the 'WEB SERVICE2.0' login interface. On the left side, there is a stylized illustration of a building with a house in front. On the right side, there is a login form with two input fields: 'Username' and 'Password'. Below the 'Password' field, there is a link that says 'Forget Password?'. At the bottom of the form, there is a blue button labeled 'Login'.

4.3.2 Configuring VTO Number

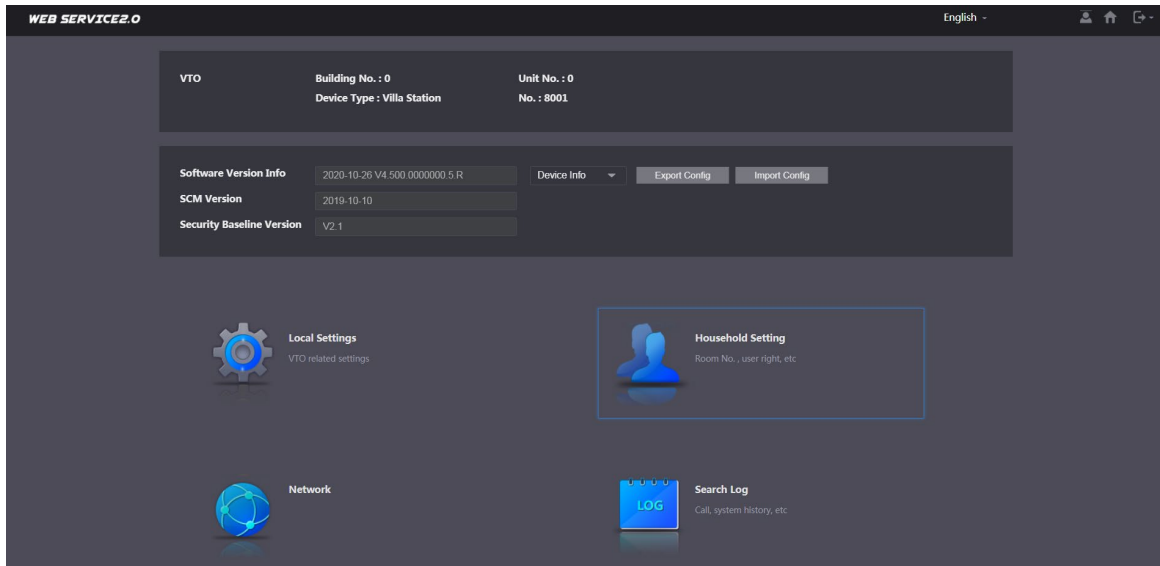
Numbers can be used to distinguish each VTO, and we recommend setting it according to unit or building number.



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

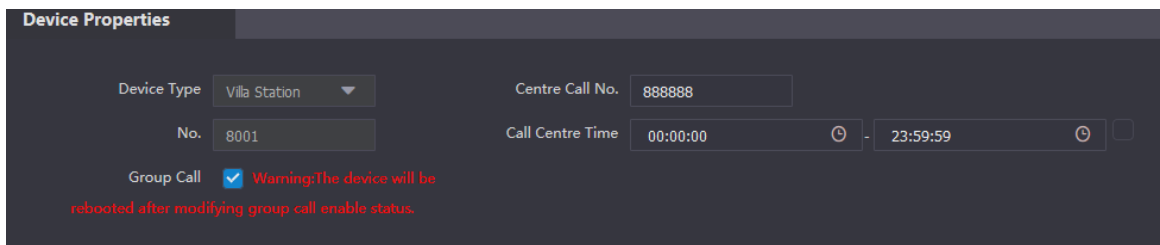
Step 1 Log in to the VTO web interface.

Figure 4-3 Main interface



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

Figure 4-4 Device properties

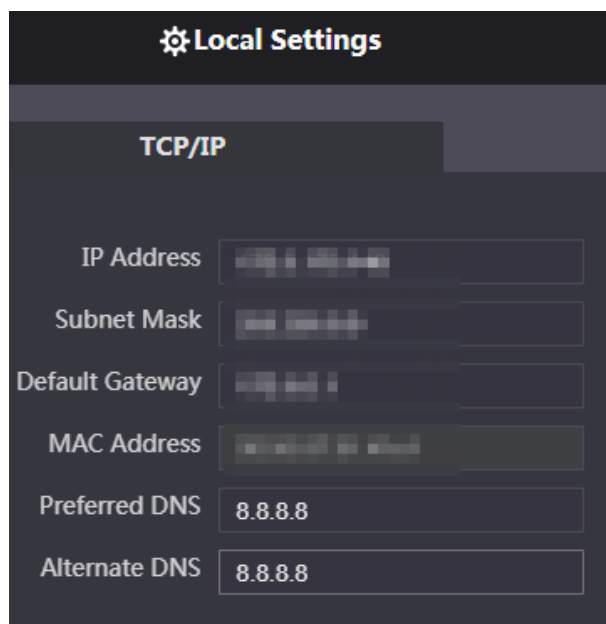


Step 3 Enter the number in **No.**, and then click **Confirm**.

4.3.3 Configuring Network Parameters

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

Figure 4-5 TCP/IP information



Step 2 Enter each parameter, and then click **Save**.

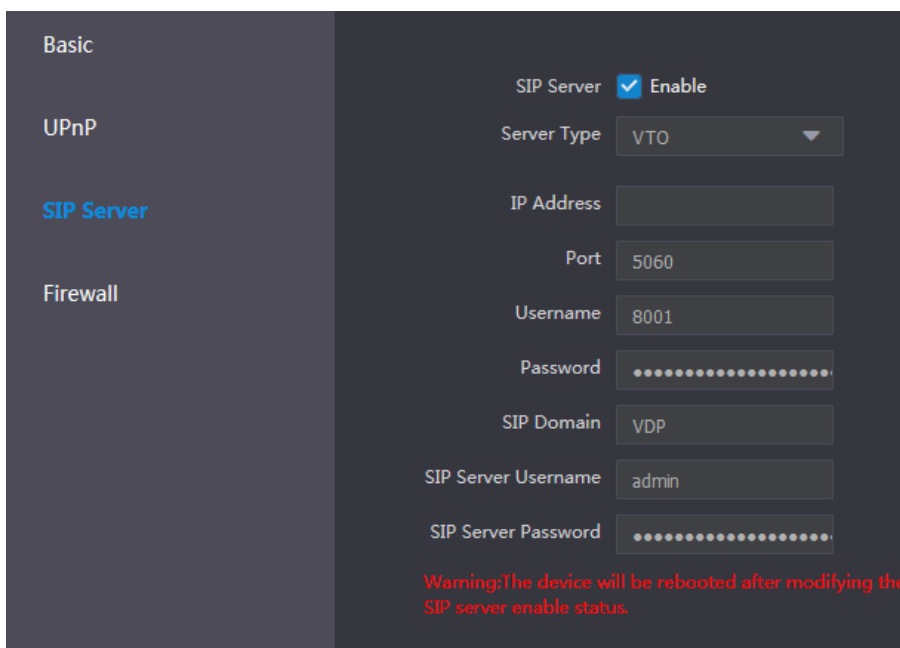
The VTO will automatically restart. You need to add the IP address of your PC to the same network segment as the VTO to log in again.

4.3.4 Configuring SIP Server

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.

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

Figure 4-6 SIP server



Step 2 Select the server type as needed.

- If the current VTO works as the SIP server, enable **SIP Server**, and then click **Save**. The VTO will automatically restart, and then you can add other VTOs and VTHs to this VTO. See "4.3.6 Adding VTOs and 4.3.7 Adding Room Number".



If the current VTO does not work as the SIP server, do not enable **SIP Server**. Otherwise the connection with this VTO will fail.

- If other VTOs work as the SIP server, set **Server Type** as VTO, and then configure the parameters.

Table 4-1 SIP server configuration

Parameter	Description
IP Addr.	The IP address of the VTO that works as the SIP server.
Port	<ul style="list-style-type: none"> • 5060 by default when VTO work as SIP server. • 5080 by default when the platform works as SIP server.
Username	Keep the default value.
Password	
SIP Domain	VDP.
SIP Server Username	SIP server web interface login username and password.
SIP Server Password	

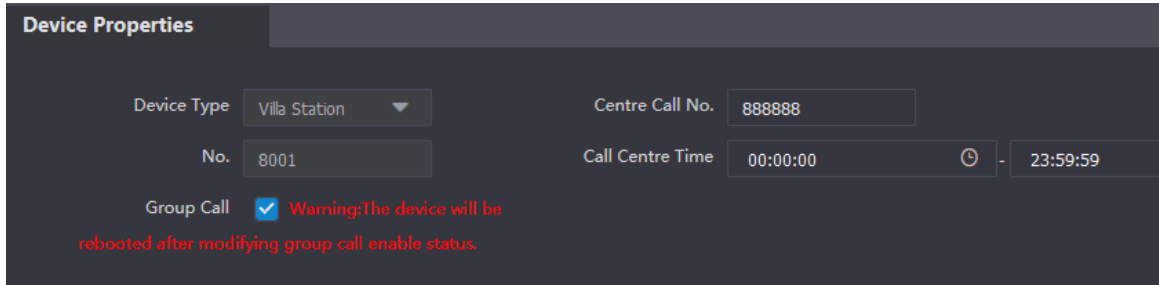
- If other servers work as the SIP server, set **Server Type** as needed, and then see the corresponding manual for details.

4.3.5 Configuring Call Number and Group Call

To dial and call a VTO, you need to configure the call number on each VTO that works as the phone number.

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

Figure 4-7 Device properties



Device Properties

Device Type: Villa Station

Centre Call No.: 888888

No.: 8001

Call Centre Time: 00:00:00 - 23:59:59

Group Call: Warning: The device will be rebooted after modifying group call enable status.

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 door station (VTO) web interface.

On the SIP server, you can enable group call function. When calling a main VTH, all extension VTH will also receive the call.



The VTO will restart after enabling or disabling the group call function.

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

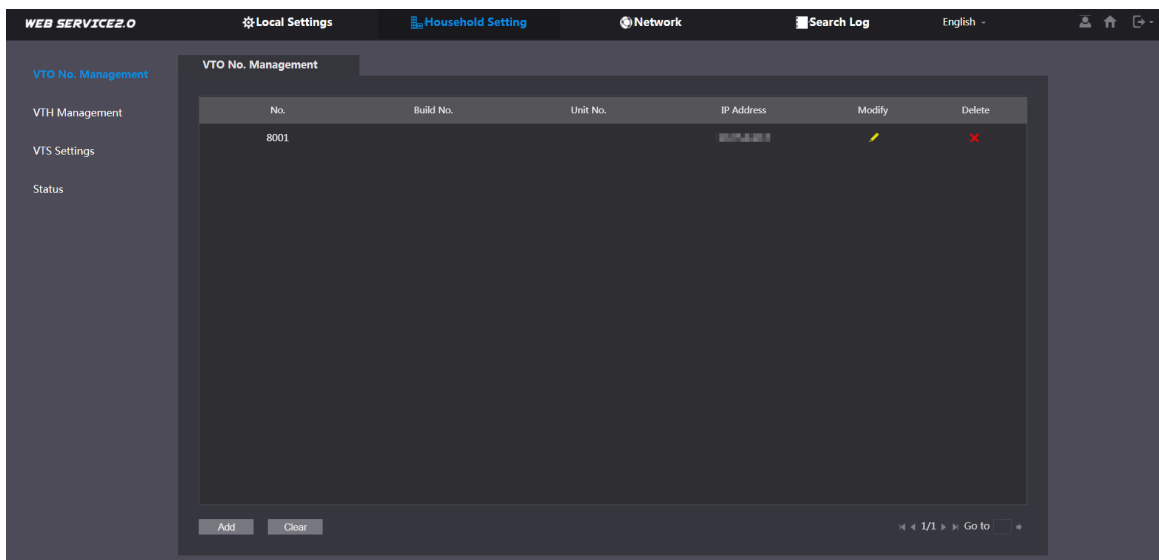
Step 4 Enable **Group Call**, click **Confirm**, and then the VTO will restart.

4.3.6 Adding VTOs

You can add VTOs to the SIP server, and all the VTOs connected to the same SIP server can make video call to each other. This section is applicable when a VTO works as the SIP server, and if you are using other servers as the 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



WEB SERVICE2.0

Local Settings Household Setting Network Search Log English

VTO No. Management

No.	Build No.	Unit No.	IP Address	Modify	Delete
8001					

Add Clear

1/1 Go to

Step 2 Click **Add**.

Figure 4-9 Add VTO

Step 3 Configure the parameters.



The SIP server must be added.

Table 4-2 Add door stations (VTO)

Parameter	Description
Rec No.	VTO number. See "4.3.2 Configuring VTO Number".
Register Password	Keep the default value.
Build No.	Available only when other servers work as the SIP server.
Unit No.	
IP Address	VTO IP address.
Username	VTO web interface login username and password.
Password	

Step 4 Click **Save**.

4.3.7 Adding Room Number

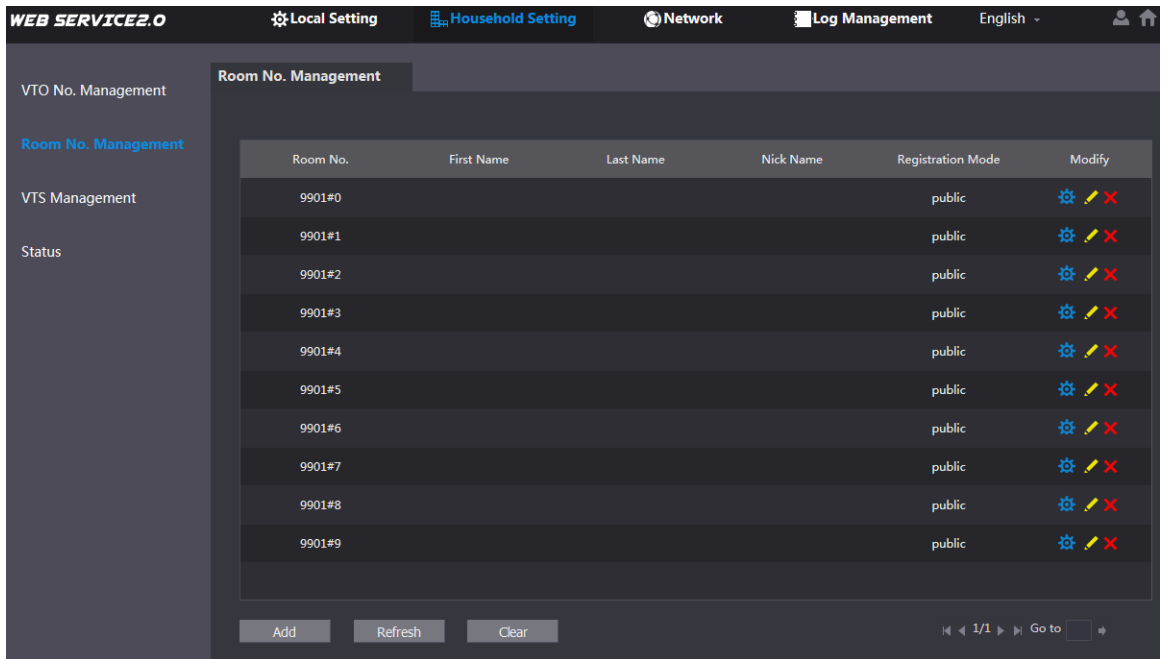
You can add room numbers to the SIP server, and then configure the room number on VTHs to connect them to the network. This section is applicable when a VTO works as the SIP server, and if you use other servers as the SIP server, see the corresponding manual for the detailed configuration.



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

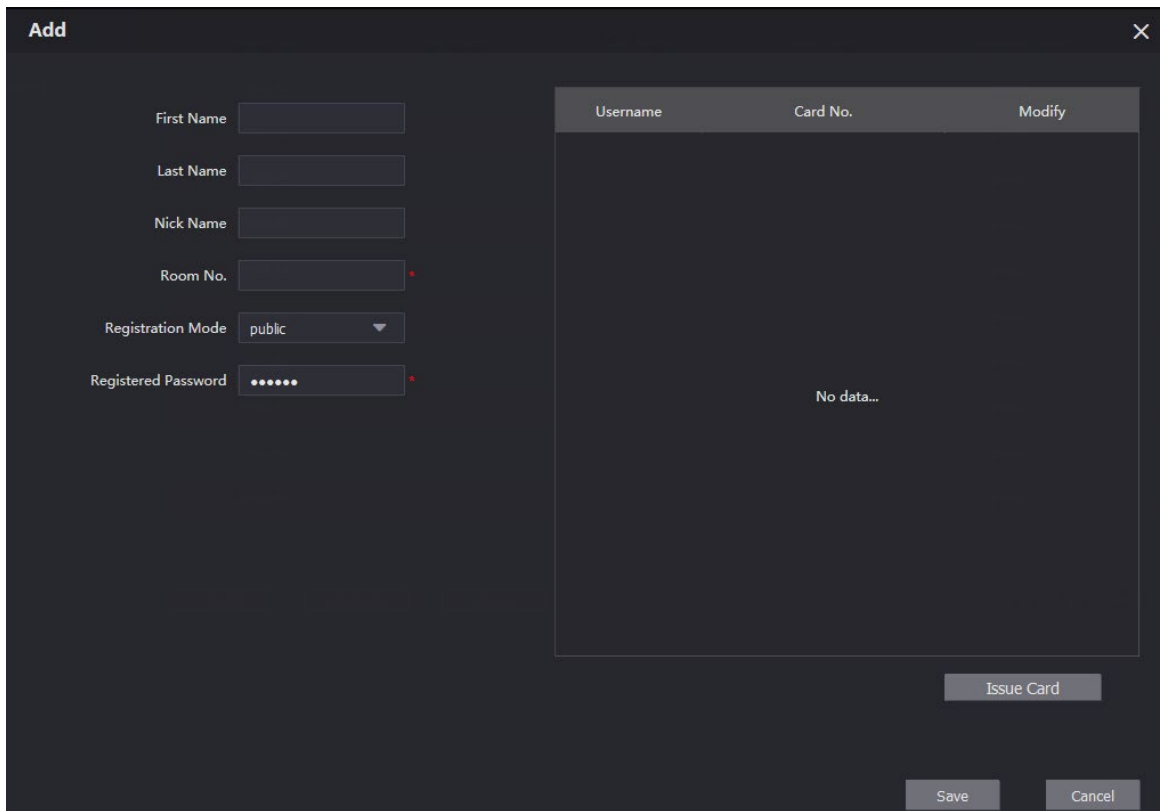
Step 1 Log in to the web interface of the SIP server, and then select **Household Setting > Room No. Management**.

Figure 4-10 Room number management



Step 2 Click **Add**.


Figure 4-11 Add a single room number





Step 3 Configure room information.

Table 4-3 Room information

Parameter	Description
First Name	Information used to differentiate each room.
Last Name	
Nick Name	
Room No.	Room number.

Parameter	Description
	 <ul style="list-style-type: none"> When there are multiple VTHs, the room number for the main VTH should end with #0, and the room numbers for extension VTHs with #1, #2... You can configure up to 9 extension VTHs for one main VTH.
Registration Mode	Select public .
Registered Password	Keep the default value.

Step 4 Click **Save**.

Click  to modify room information, and click  to delete the room.

4.4 Commissioning

4.4.1 VTO Calling VTH

Step 1 Dial a room number on the VTO.


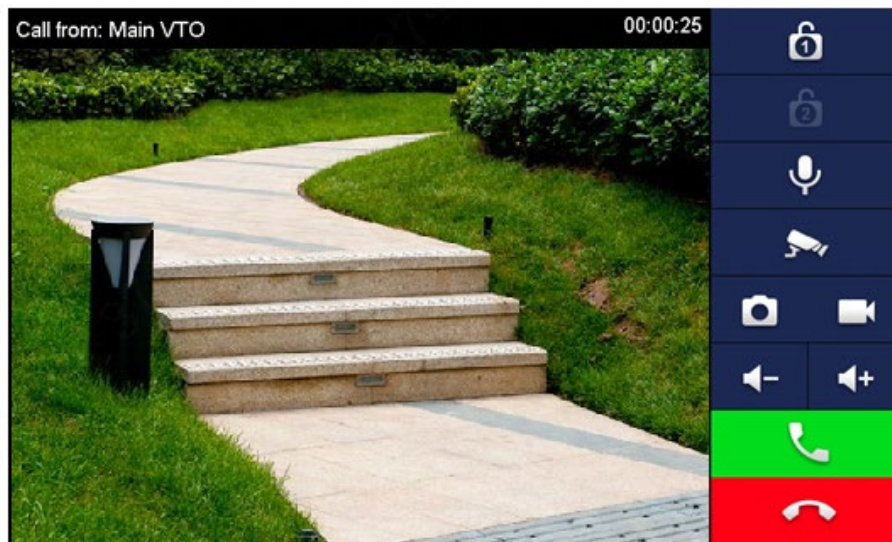
Step 2 Tap  on the VTH to answer the call.

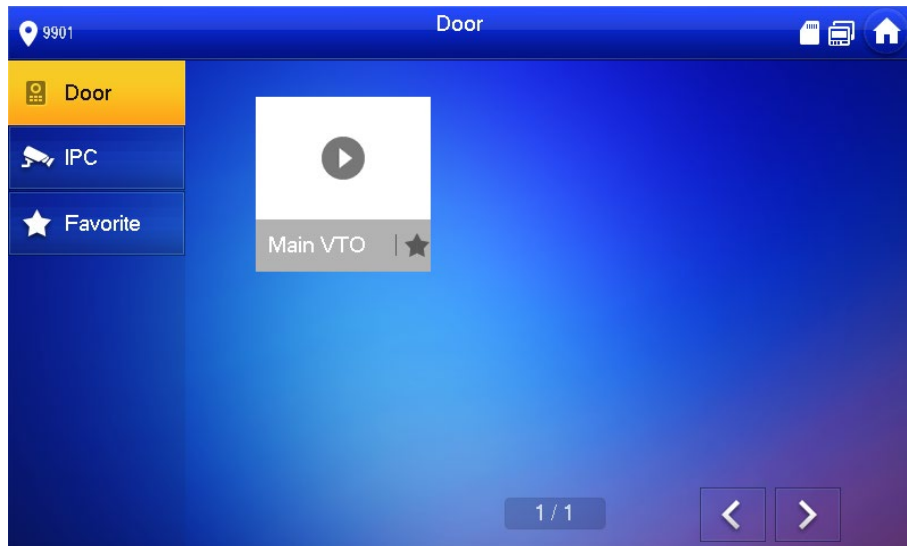
Figure 4-12 Call screen



4.4.2 VTH Monitoring VTO

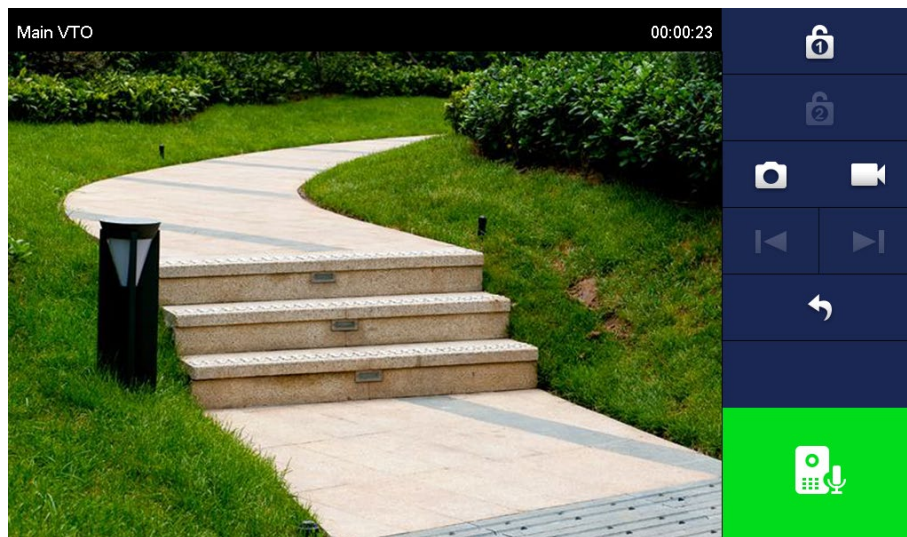
Step 1 On the main interface of the VTH, select **Monitor > Door**.

Figure 4-13 Door



Step 2 Select a VTO.

Figure 4-14 Monitoring video



5 EasyViewer Plus

The EasyViewer Plus (hereinafter referred to as the "app") allows you to manage devices, play back videos, unlock doors, and more.

Before adding the VTO to the app, you need to connect the VTO to the router through Wi-Fi, or connect the VTO to the router by using a switch, and then manually change the IP address of the VTO to the same network as the router if DHCP is not supported.

Download the app in the app store on your smartphone. On the app, select **Setting > Help and Feedback** to view instructions on each function.

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.

Villa Door Station

User's Manual





Foreword

General

This manual introduces how to configure the villa door station (hereinafter referred to as "VTO") on the web interface.

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

Revision History

Version	Revision Content	Release Date
V1.0.0	First release.	January 2021

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 jurisdictions. For detailed information, refer to 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, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and 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 occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

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

Operating Requirements

- Do not expose the device to direct sunlight or heat source.
- Do not install the device in a humid or dusty environment.
- Horizontally install the device at stable places to prevent it from falling.
- Do not drip or splash liquids onto the device, or put on the device anything filled with liquids.
- Install the device at well-ventilated places and do not block its ventilation opening.
- 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 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, 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	II
1 Initializing the VTO	1
2 Login and Resetting Password	2
2.1 Login	2
2.2 Resetting Password	2
3 Main Interface	4
4 Local Settings	5
4.1 Basic	5
4.2 Video & Audio	6
4.3 Access Control Settings	8
4.3.1 Local.....	8
4.3.2 RS-485	9
4.3.3 Password Management.....	9
4.4 System	10
4.5 Security	11
4.6 Wiegand.....	12
4.7 Onvif User.....	13
4.8 Upload File.....	13
5 Household Setting	15
5.1 VTO No. Management	15
5.2 VTH Management.....	16
5.2.1 Adding Room Number.....	16
5.2.2 Issuing Access Card	17
5.2.3 Issuing Fingerprint	18
5.3 VTS Management.....	19
5.4 IPC Setting	20
5.5 Status	21
5.6 Publish Information.....	22
5.6.1 Send Info	22
5.6.2 History Info.....	22
6 Network	24
6.1 Basic	24
6.1.1 TCP/IP	24
6.1.2 Port.....	24
6.1.3 P2P	25
6.2 UPnP.....	25
6.2.1 Enabling UPnP Services.....	25
6.2.2 Adding UPnP Services.....	25
6.3 SIP Server	26
6.4 Firewall	27
7 Log Management	29
Appendix 1 Cybersecurity Recommendations	30

1 Initializing the VTO

For first-time login or after resetting the VTO, you need to initialize it on the web interface.

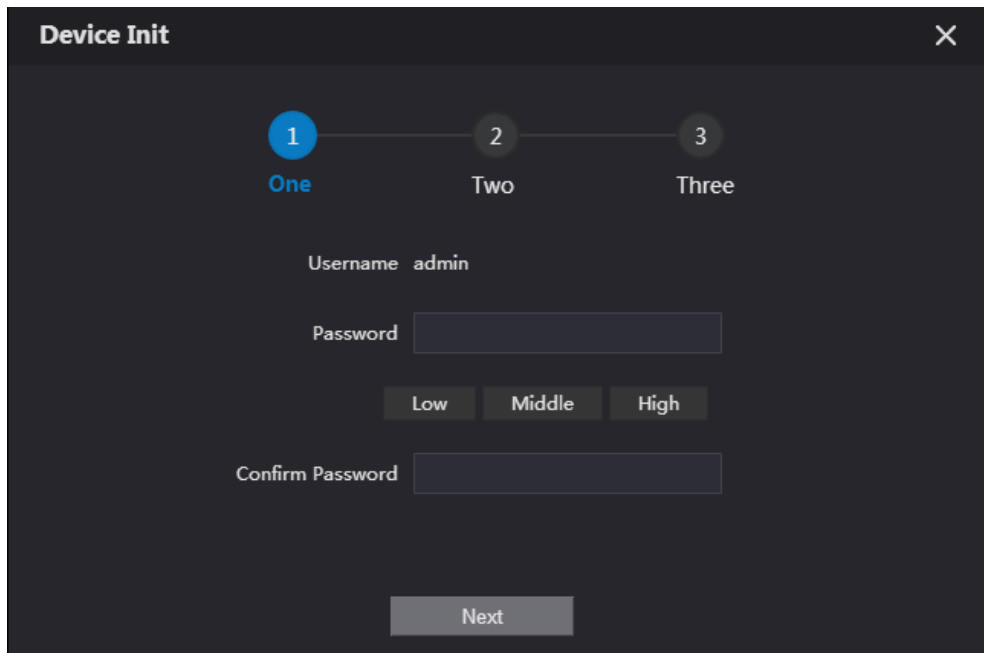
Step 1 Power on the VTO.

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



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

Figure 1-1 Device initialization



The screenshot shows a web interface titled "Device Init" with a close button (X) in the top right corner. At the top, there is a progress indicator with three steps: "1 One" (highlighted in blue), "2 Two", and "3 Three". Below this, the "Username" field is pre-filled with "admin". The "Password" field is empty, and below it are three buttons labeled "Low", "Middle", and "High". The "Confirm Password" field is also empty. At the bottom center, there is a "Next" button.

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

Step 4 Enter an email address for resetting password.

Step 5 Click **Next**, and then click **OK**.

2 Login and Resetting Password

2.1 Login

Before login, make sure that the PC is in the same network segment as the VTO.

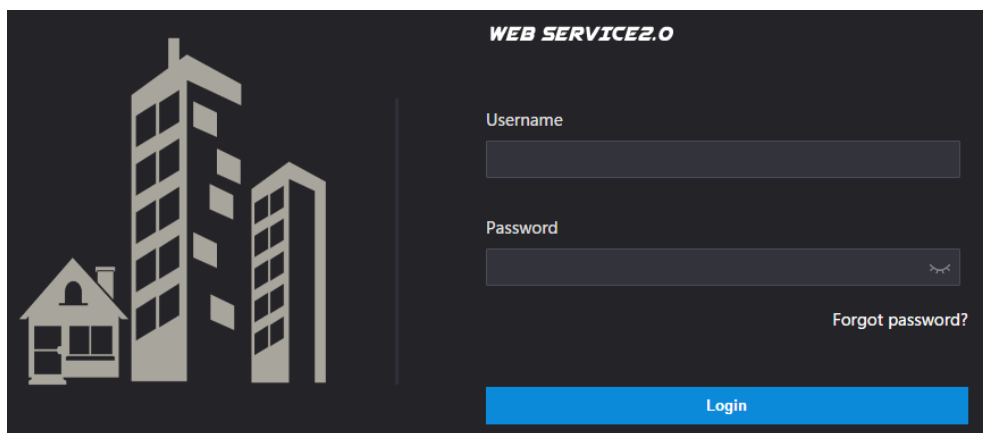
Step 1 Go to the IP address of the VTO in the browser.



For first-time login, enter the default IP (192.168.1.108). If you have multiple VTOs, we recommend changing the default IP address (**Network > Basic**) to avoid conflict.

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

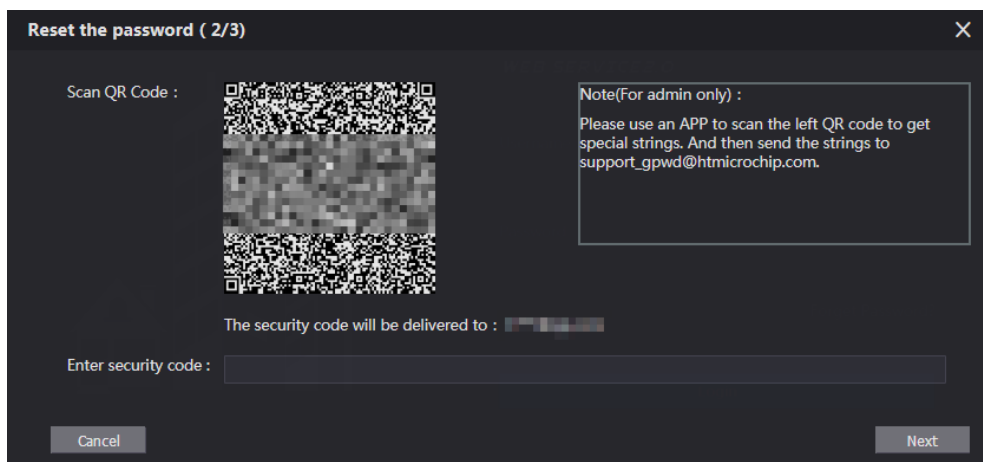
Figure 2-1 Login



2.2 Resetting Password

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

Figure 2-2 Reset the password



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

Step 3 Send the string to the email: support_gpwd@htmicrochip.com, and then the security code will be sent to the email address configured during initialization.

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



- If you did not set an email address during initialization, contact your supplier or customer service for help.
- The security code will be valid only for 24 hours upon receipt.
- If you enter the wrong security code for 5 consecutive times, your account will be locked for 5 minutes.

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

3 Main Interface

Figure 3-1 Main interface

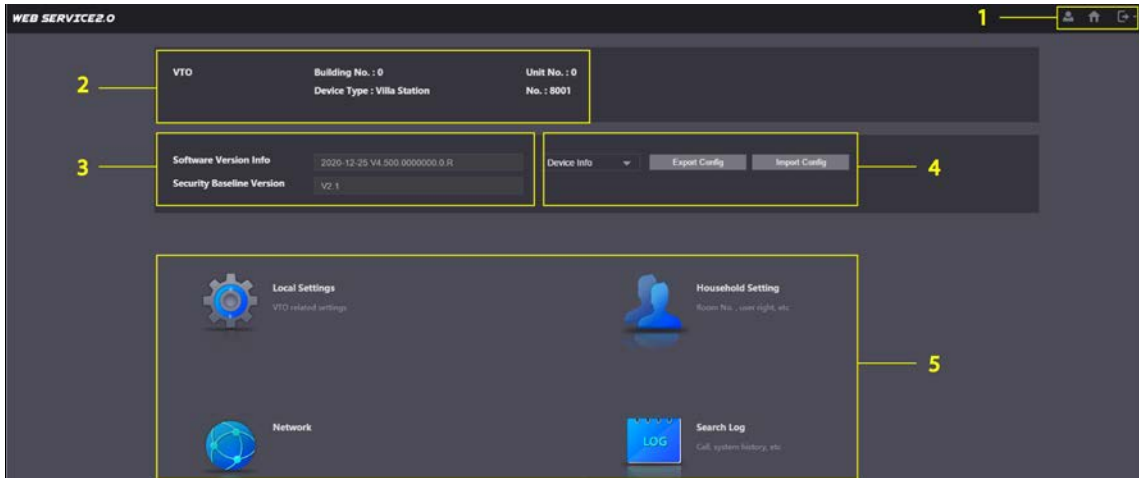


Table 3-1 Main interface introduction

No.	Function	Description
1	General function	<ul style="list-style-type: none"> : Change the password and your email address. : Go to the main interface. : Log out, restart the VTO or restore the VTO to factory settings. <p></p> <p>If you restore the VTO to factory settings, all data except external storage will be deleted. You can format the SD card to delete the data in it.</p>
2	VTO information	View the information of the VTO and the system.
3	System information	
4	Configuration manager	Export or import VTO configuration or user information.
5	Function	<p>Configure parameters for different functions.</p> <p></p> <p>Interface and function might vary with models. The actual product shall prevail.</p>

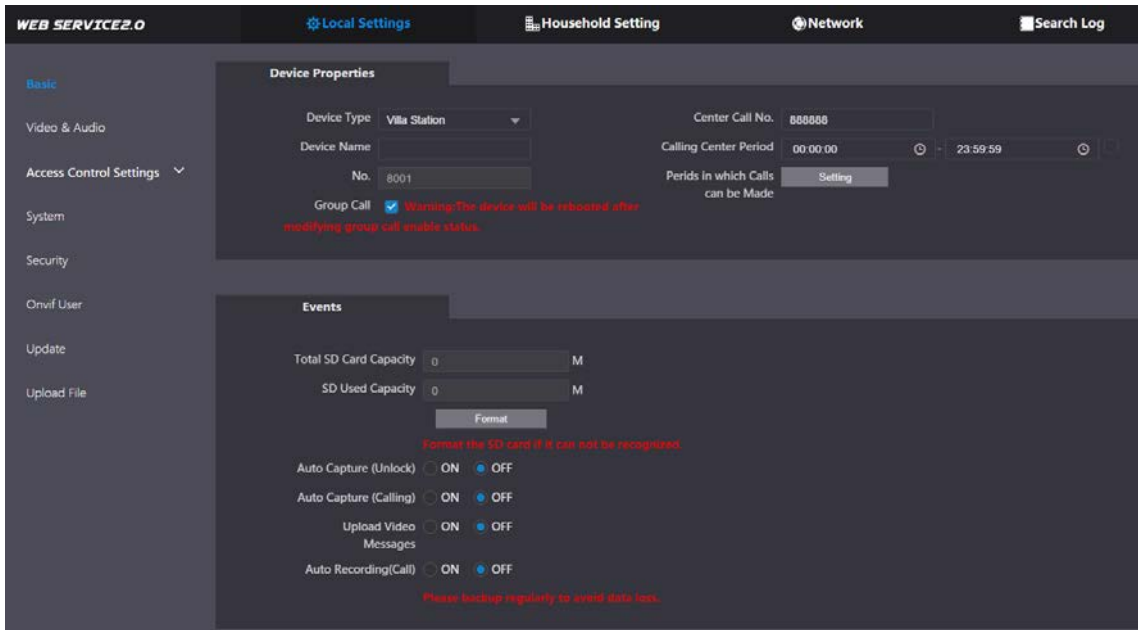
4 Local Settings

This chapter introduces the detailed configuration of the VTO.

4.1 Basic


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

Figure 4-1 Basic



Step 2 Configure the parameters.

Table 4-1 Basic parameter description

Parameter	Description
Device Type	Select Villa Station or Small Apartment as needed.
Center Call No.	The default phone number for the management center is 888888, and you can set it to any number with up to 9 digits.
Device Name	When other devices are monitoring this VTO, the device name will appear on the monitoring image.
Calling Center Period	Time period in which the management center can be called.
No.	Used to differentiate each VTO, and we recommend setting it according to unit or building number, and then you can add VTOs to the SIP server by using their numbers.  You can change the number of the VTO when it is not working as the SIP server.
Periods in which Calls can be Made	Configure the time if you only want to receive calls during a specific period.
Group Call	Enable it on the VTO that works as the SIP server, and when a main VTH receives a call, all extension VTHs will also receive the call.

Parameter	Description
Total SD Card Capacity	Displays the total and used capacity of the SD card. You can click Format to delete all the data in the SD card.
SD Used Capacity	
Format	
Auto Capture (Unlock)	When the door is unlocked, the VTO will take two snapshots and save them to the SD card.
Auto Capture (Calling)	Take a snapshot and save it in the SD card of the VTO when the VTO is calling.
Upload Video Messages	When enabled: <ul style="list-style-type: none"> ● If an SD card is inserted in both the VTH and VTO, the video message will be saved both in the SD cards of the VTH and the VTO. ● If an SD card is only inserted in the VTH or the VTO, the video message will be saved only in the SD card of the VTH or the VTO. ● If no SD card is inserted in the VTH or VTO, no video message will be saved.
Auto Recording (Call)	Take recording when the VTO is in a call, and save the recording in the SD card of the VTO.

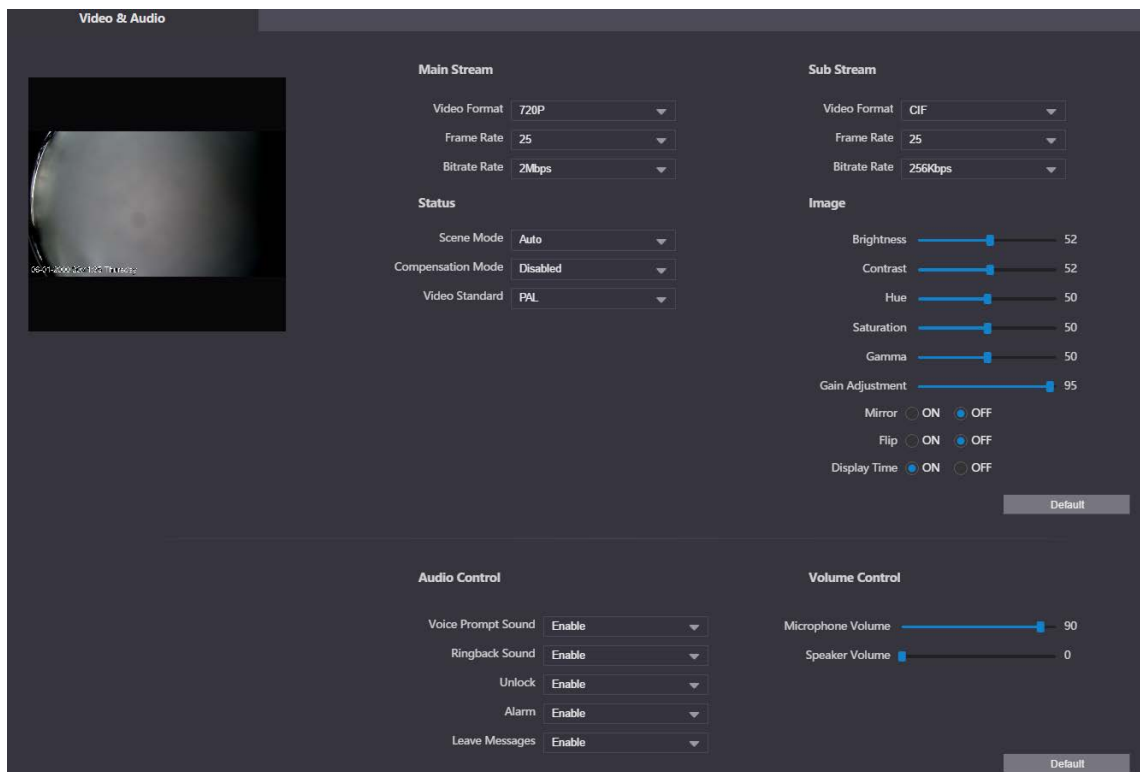
Step 3 Click **Save**.

4.2 Video & Audio

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


Step 1 Select **Local Settings > Video & Audio**.

Figure 4-2 Video and audio



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

Table 4-2 Video parameter description

Parameter		Description
Main/Sub Stream	Video Format	Select different resolution as needed: <ul style="list-style-type: none"> ● 1080P: 1920 × 1080. ● 720P: 1280 × 720. ● WVGA: 800 × 480. ● QVGA: 320 × 240. ● D1: 720 × 480. ● CIF: 352 × 288.
	Frame Rate	The larger the value, the smoother the video, but it requires more bandwidth.
	Bitrate Rate	The larger the value, the better the video quality, but it requires more bandwidth.
Status	Scene Mode	Select as needed according to the lighting condition. Auto is selected by default.
	Compensation Mode	<ul style="list-style-type: none"> ● BLC: Back light compensation. Improve the clarity of the target in the image. ● WDR: Wide dynamic range. Enhance the brightness of dark areas, and reduce the brightness of bright areas to improve the image. ● HLC: High light compensation. Reduce the brightness of the strong spots to improve the overall image.
	Video Standard	Select PAL or NTSC according to your area.  PAL is mostly used in China and Europe, and NTSC primarily in the United States and Japan.
Image	Brightness	The larger the value, the brighter the image.
	Contrast	Larger value for more contrast between bright and dark areas.
	Hue	Make the color brighter or darker. The default value is made by the light sensor, and we recommend keeping it default.
	Saturation	The larger the value, the thicker the color.
	Gamma	Changes the picture brightness and improves the picture dynamic range in a non-linear way. The larger the value, the brighter the image.
	Gain Adjustment	Amplify the video signal to increase image brightness. If the value is too large, there will be more noise in the image.
	Mirror	Display the image with left and right side reversed.
	Flip	Display the image upside down.
	Display Time	Display the current time and date on the video image.
Audio Control	—	Turn on or off each type of sound.
Volume Control	Microphone Volume	Adjust the volume as needed.
	Speaker Volume	

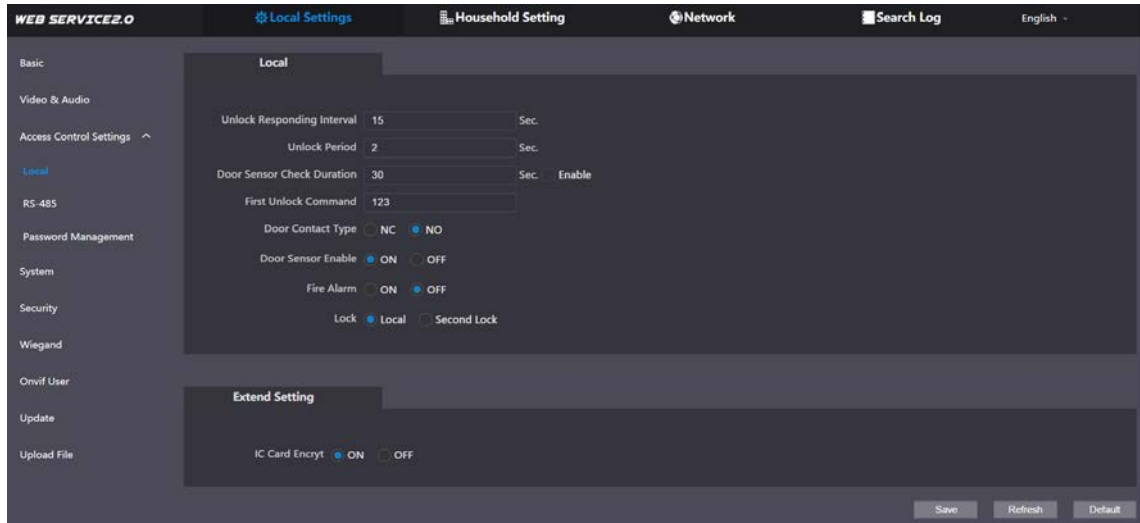
4.3 Access Control Settings

This section introduces how to configure the two locks connected to the lock port or the RS-485 port of the VTO.

4.3.1 Local


Step 1 Select **Local Settings > Access Control Settings**.

Figure 4-3 Local



Step 2 Configure the parameters.

Table 4-3 Local access control parameter description

Parameter	Description
Unlock Responding Interval	The door can only be unlocked again after the interval.
Unlock Period	The time during which the lock stays unlocked.
Door Sensor Check Duration	<ul style="list-style-type: none"> Enable it, and the door will not be locked until the door sensors contact each other. If the door is unlocked longer than the Door Sensor Check Duration, the door sensor alarm will be triggered, and the alarm will be sent to the management center. Disable it, and then the door will be locked after the Unlock Period.  <p>You need to install a door contact to configure this parameter.</p>
First/Second Unlock Command	You can connect a third-party phone, such as a SIP phone, to the VTO, and use the command to open the door remotely.
Door Contact Type	<ul style="list-style-type: none"> NC: Normally closed. NO: Normally open.
Door Sensor Enable	Synchronize door sensor status to indoor monitors (VTHs).
Fire Alarm	If turned on, you can connect an alarm device to the port that is originally for the door contact, but you cannot use the door contact function.
Lock	Non-remote methods, such as password or card, will unlock the lock you

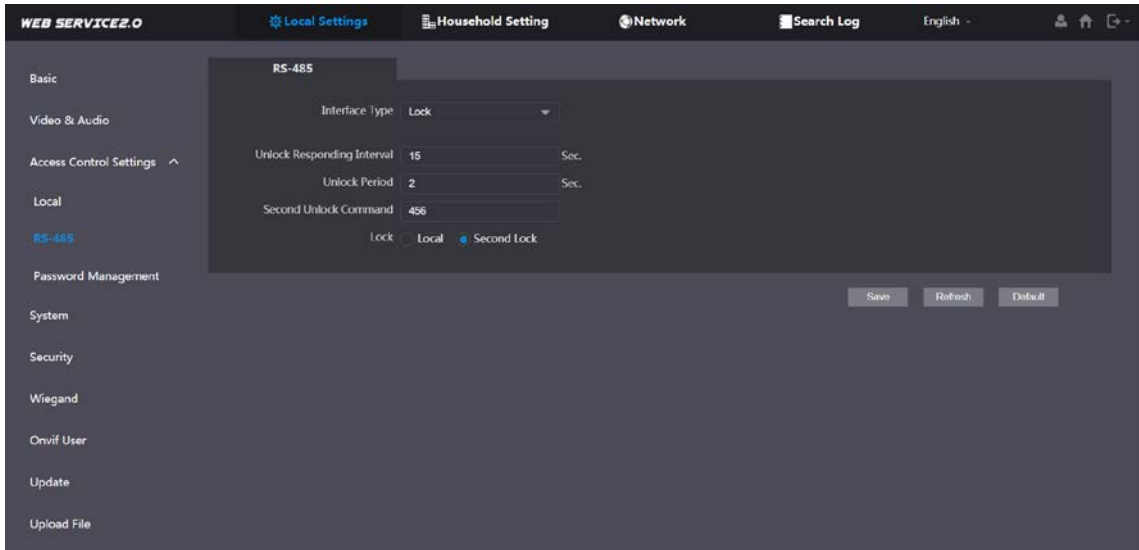
Parameter	Description
	select.
IC Card Encrypt	Access cards issued by the VTO will be encrypted and unclonable.

Step 3 Click **Save**.

4.3.2 RS-485

Select **Local Settings > Access Control Settings**, and then configure the parameters of the lock connected through the RS-485 port. See Table 4-3 for parameter description.

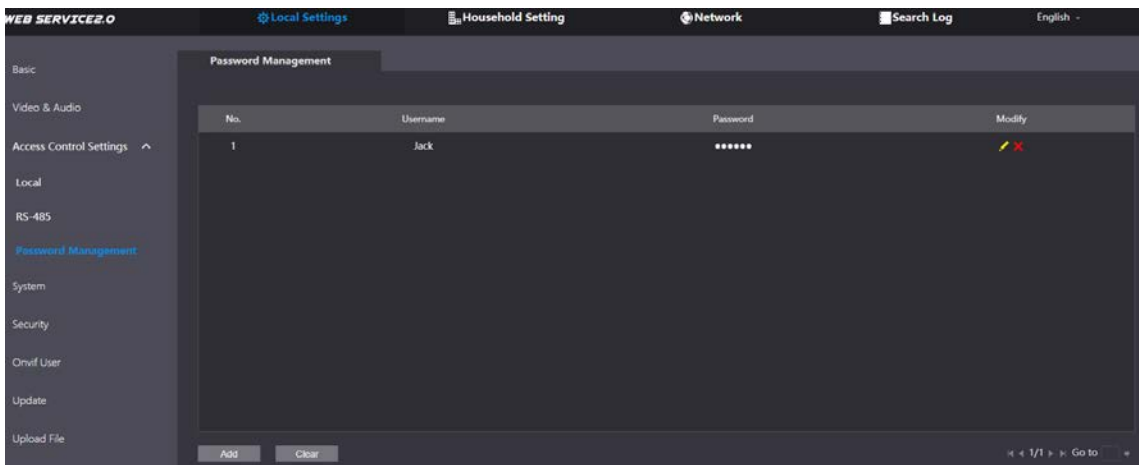
Figure 4-4 Lock connected through the RS-485 port



4.3.3 Password Management

Add a username and password used to unlock the door.

Figure 4-5 Password management

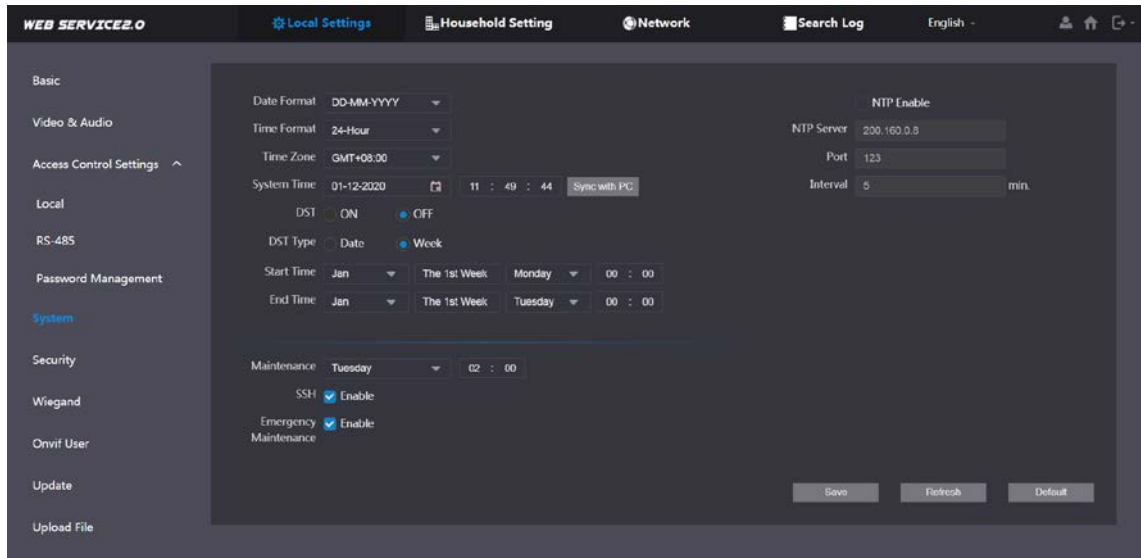


4.4 System

Configure time parameters, NTP server, and more.



Step 1 Select **Local Settings > System**.


Figure 4-6 System



Step 2 Configure the parameters.

Table 4-4 System parameter description

Parameter	Description
Date Format	Select a format as needed.
Time Format	
System Time	 Changing system time might cause problems on video searching and information publication. Turn off video recording and auto snapshot before changing it.
Time Zone	Configure the time zone as needed.
Sync with PC	Synchronize the VTO system time with your PC.
DST	Daylight saving time. If it is applicable to your area, you need to enable it, and then configure DST type, start time and end time.
DST Type	Select Date or Week as needed, and then configure the specific period.
Start Time	Configure the start time and end time of DST.
End Time	
NTP Enable	Enable NTP and enter the IP address of the NTP server, and then the VTO will synchronize time with the NTP server automatically.
NTP Server	
Port	NTP server port number.
Interval	VTO time update cycle. 30 minutes at most.
Maintenance	Define the time when the VTO will restart automatically.
SSH	 You can connect debugging devices to the VTO through SSH protocol. We recommend turning it off, and turn on security mode and outbound service information protection. See "4.5 Security". Otherwise, the VTO might be exposed

Parameter	Description
	to security risks and data leakage.
Emergency Maintenance	Enable it for fault analysis and repair.  This function will occupy 8088 and 8087 ports.

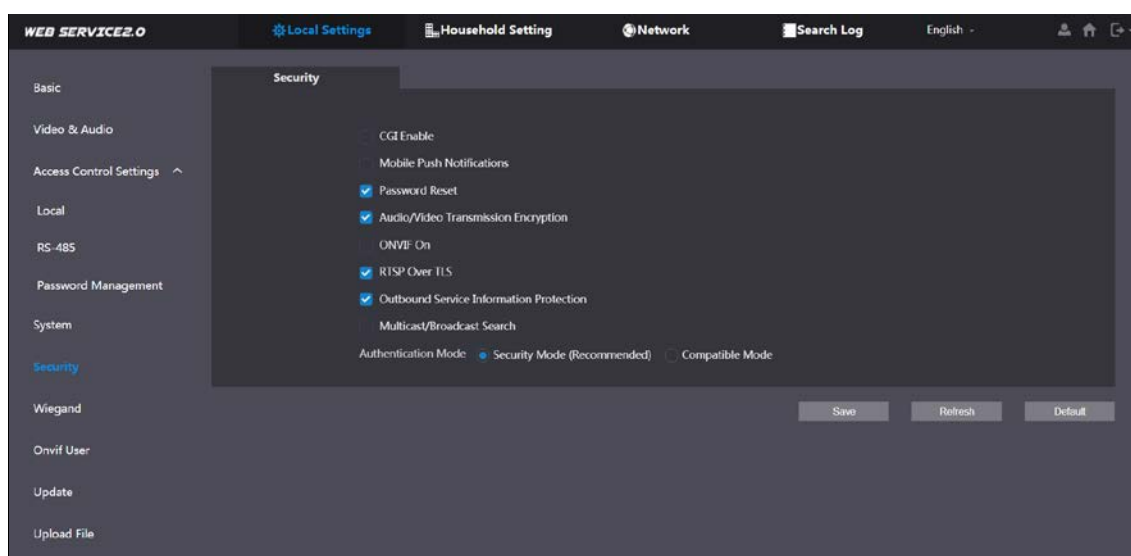
Step 3 Click **Save**.

4.5 Security

Configure functions that involve device security.




Step 1 Select **Local Settings > Security**.






Figure 4-7 Security



Step 2 Configure the parameters.

Table 4-5 Security parameter description

Parameter	Description
CGI Enable	Enable the use of CGI command.  We recommend turning it off. Otherwise, the VTO might be exposed to security risks and data leakage.
Mobile Push Notification	Send information to the app on the smartphone.  We recommend turning it off if you do not need this function. Otherwise, the VTO might be exposed to security risks and data leakage.
Password Reset	If turned off, you will not be able to reset password.
Audio/Video Transmission Encryption	Encrypt all data during voice or video call.  We recommend turning it on. Otherwise, the VTO might be exposed to

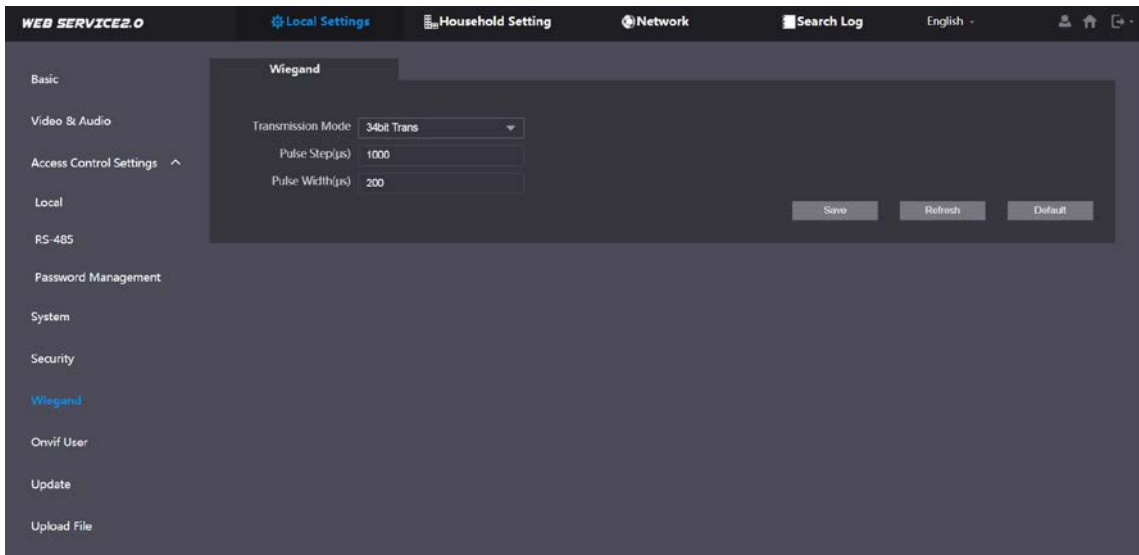
Parameter	Description
	security risks and data leakage.
ONVIF On	<p>Allow third-party to pull video stream of the VTO through the ONVIF protocol.</p> <p></p> <p>We recommend turning it off. Otherwise, the VTO might be exposed to security risks and data leakage.</p>
RTSP Over TSL	<p>Output encrypted bit stream through RTSP.</p> <p></p> <p>We recommend turning it on. Otherwise, the VTO might be exposed to security risks and data leakage.</p>
Outbound Service Information Protection	<p>Protect your passwords.</p> <p></p> <p>We recommend turning it on. Otherwise, the VTO might be exposed to security risks and data leakage.</p>
Multicast/Broadcast Search	<p>Enable it and the VTO will be found by other devices.</p> <p></p> <p>We recommend turning it off. Otherwise, the VTO might be exposed to security risks and data leakage.</p>
Authentication Mode	<ul style="list-style-type: none"> ● Security Mode (recommended): Support logging in with Digest authentication. ● Compatible Mode: Use the old login method. <p></p> <p>We recommend the security mode. Compatible mode might expose the VTO to security risks and data leakage.</p>

Step 3 Click **Save**.

4.6 Wiegand

Configure the parameters as needed when connected to other devices, such as a card reader with a Wiegand port.

Figure 4-8 Wiegand



4.7 Onvif User

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



If you delete an account, it cannot be undone.

Step 1 Select **Local Settings > Onvif User**.

Step 2 Click **Add**.

Figure 4-9 Add an ONVIF user

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

ONVIF devices can now monitor the VTO by using the account. See the user's manual of the ONVIF device for details.

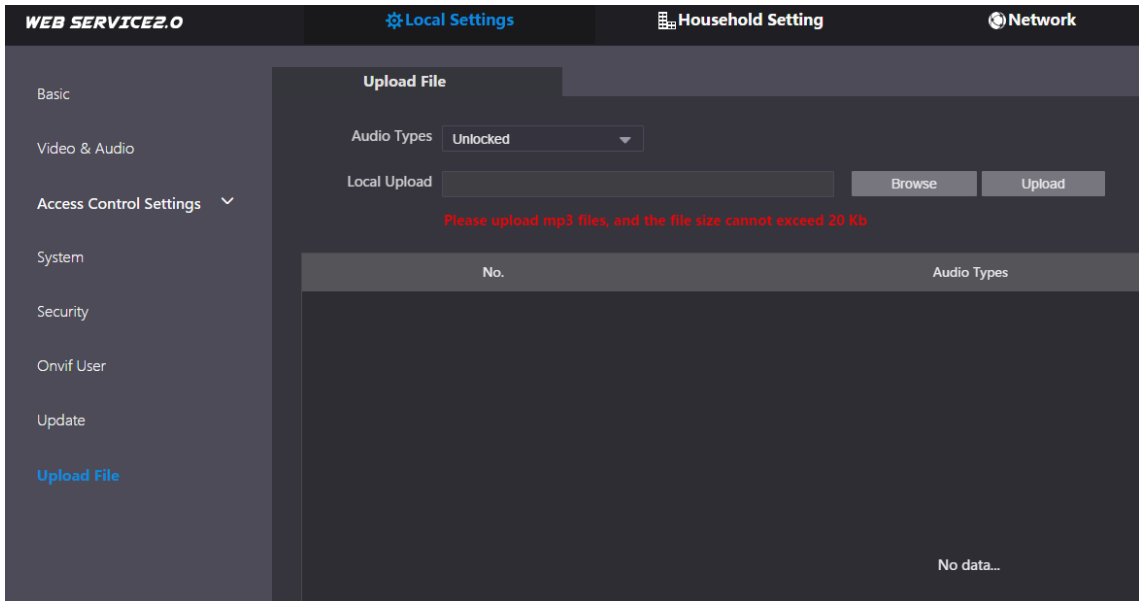
4.8 Upload File

Upload audio file to change the sound when calling, unlocking the door, and more.

Step 1 Select **Local Settings > Upload File**.

Step 2 Select an audio type, and then click **Browse** to select the audio file as needed.

Figure 4-10 Change the sound prompt



Step 3 Click **Upload**.

5 Household Setting

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



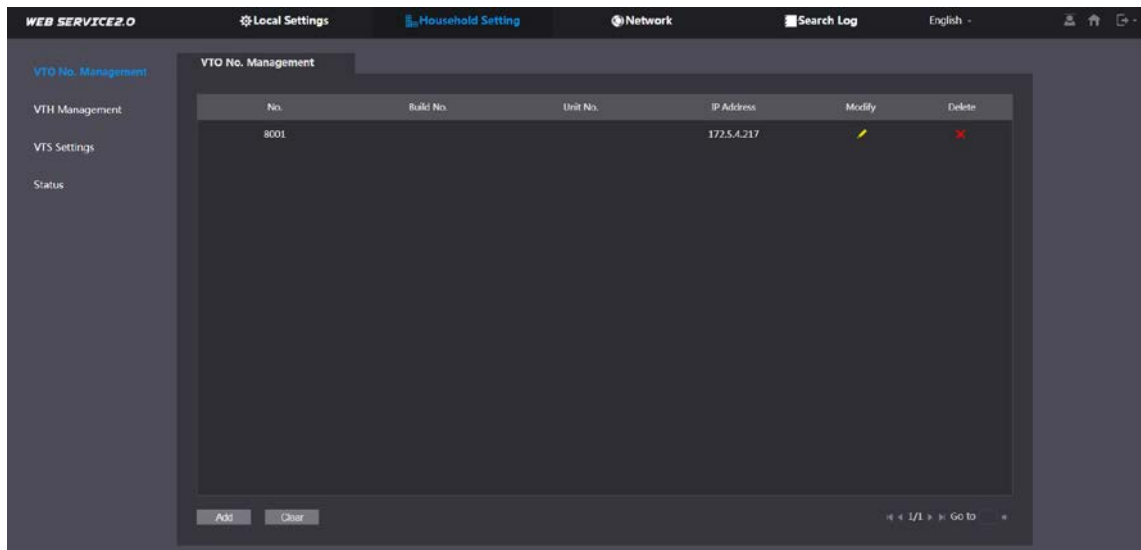
To configure SIP server parameters, see "6.3 SIP Server" for details.

5.1 VTO No. Management

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

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

Figure 5-1 VTO management



Step 2 Click **Add**.

Figure 5-2 Add VTO

The 'Add' dialog box is a dark-themed window with a close button (X) in the top right corner. It contains the following input fields:

- No. (empty text box)
- Registration Password (password field with masked characters '*****' and a show/hide icon)
- Build No. (empty text box)
- Unit No. (empty text box)
- IP Address (text box containing '127.0.0.1')
- Username (empty text box)
- Password (password field with masked characters and a show/hide icon)

At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

Step 3 Configure the parameters.





The SIP server must be added.

Table 5-1 Add VTO configuration

Parameter	Description
No.	The VTO number you configured. See Table 4-1 for details.
Registration Password	Keep it default.
Build No.	Available only when other servers work as the SIP server.
Unit No.	
IP Address	IP address of the VTO.
Username	Web interface login username and password of the VTO.
Password	

Step 4 Click **Save**.



Click  or  to modify or delete a VTO, or **Clear** to delete all added VTOs, but the one that you have logged in to cannot be modified or deleted.

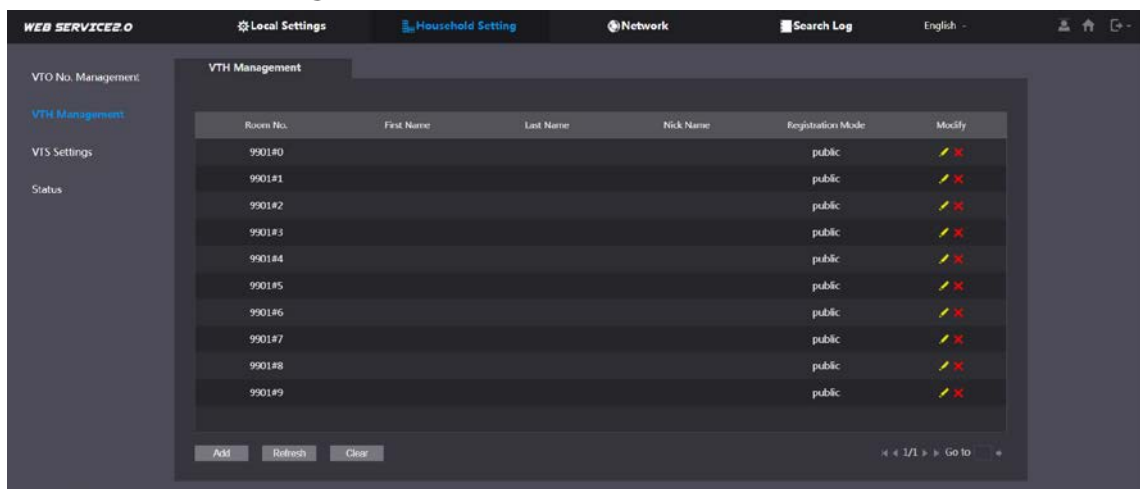
5.2 VTH Management

5.2.1 Adding Room Number

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

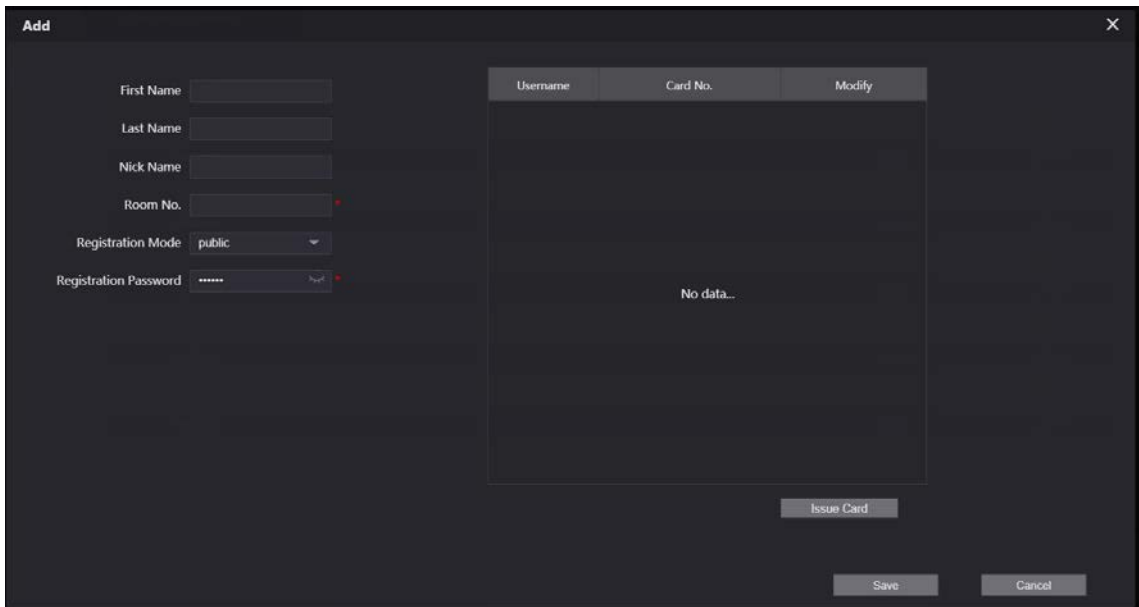
Step 1 Log in to the web interface of the SIP server, and then select **Household Setting > VTH Management**.

Figure 5-3 Room number management



Step 2 Click **Add**.

Figure 5-4 Add a room number



Step 3 Configure the parameters.

Table 5-2 Room information

Parameter	Description
First Name	Enter the information you need to differentiate each room.
Last Name	
Nick Name	
Room No.	Enter a room number, and then configure the number on a VTH to connect to connect it to the network.
Registration Type	Select public .
Registration Password	Keep it default.

Step 4 Click **Save**.



Click  or  to modify or delete a room number.

5.2.2 Issuing Access Card

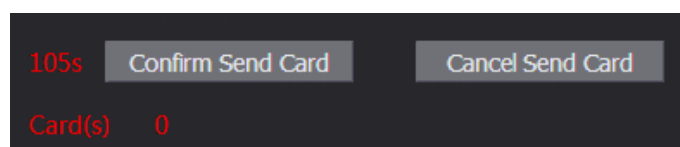
Issue an access card to unlock the door of a room.



To use this function, the VTO must have a card reader.

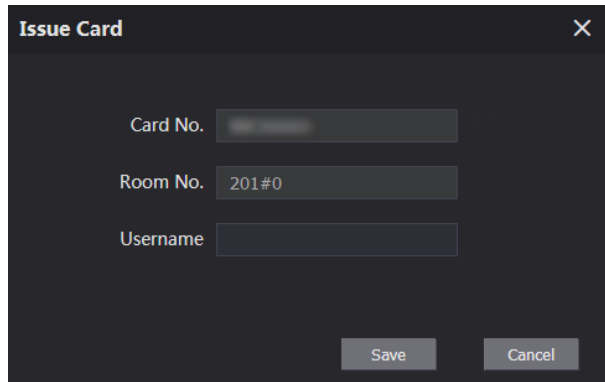
Step 1 Select **Household Setting > VTH Management**, click **Add**, and then click **Issue Card**.

Figure 5-5 Countdown notice



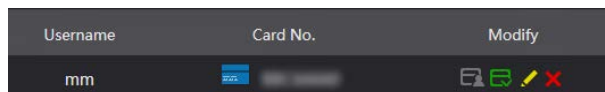
Step 2 Swipe the card on the VTO.

Figure 5-6 Issue card









Step 3 Enter the username, click **Save**, and then click **Confirm Send Card**.

Figure 5-7 Issued access card



Other Operations

- Click  to set it as the main card, and then the icon changes to . The main card can be used to issue access cards for this room on the VTO.
- Click  to set it to loss, and then the icon changes to . The lost card cannot be used to open the door.
- Click  or  to modify the username or delete the card.

5.2.3 Issuing Fingerprint

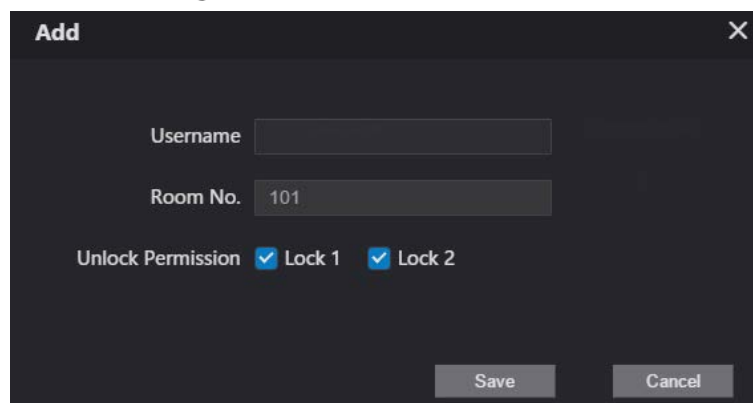
Issue fingerprints to unlock the door of a room.



To use this function, the VTO must have a fingerprint scanner.

Step 1 Select **Household Setting > VTH Management**, click **Add**, and then click **Issue Fingerprint**.

Figure 5-8 Issue fingerprint



Step 2 Enter a username, assign unlock permission as needed, and then click **Save**.

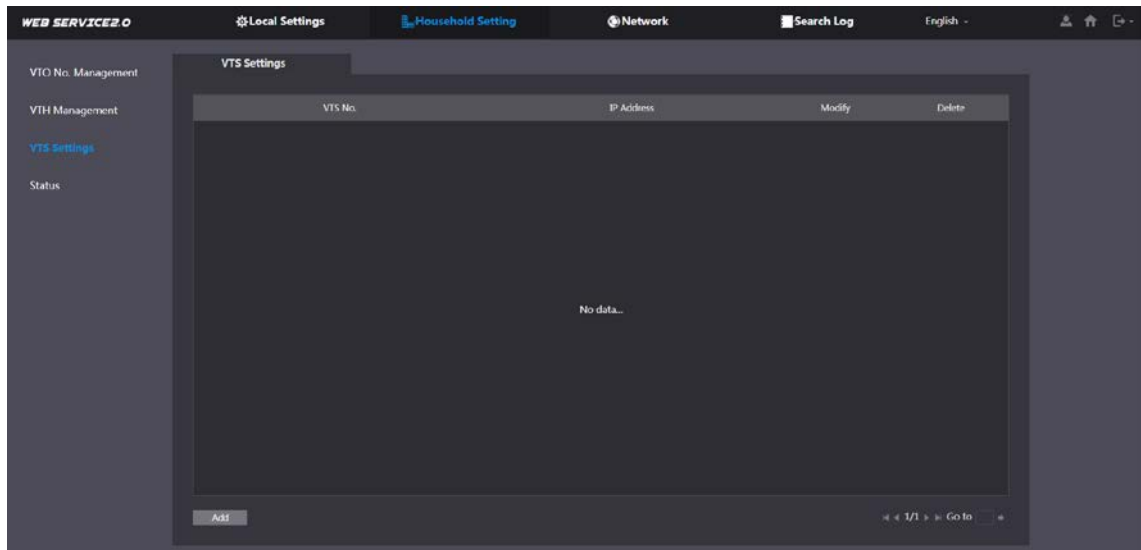
Step 3 Press your fingerprint on the scanner.

5.3 VTS Management

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

Step 1 Log in to the web interface of the VTO working as the SIP server, and then select **Household Setting > VTS Settings**.

Figure 5-9 VTS management



Step 2 Click **Add**.

Figure 5-10 Add VTS

Step 3 Configure the parameters.

Table 5-3 Add VTS configuration

Parameter	Description
VTS No.	The number of the VTS.
Registration Password	Keep it default.
IP Address	VTS IP address.

Step 4 Click **Save**.

5.4 IPC Setting

You can add IPC and NVR to the VTO working as the SIP server, and then all the connected VTHs can monitor them.



Interfaces might vary with different products. The actual interface shall prevail.

Step 1 Log in to the web interface of the VTO working as the SIP server, and then select **Household Setting > IPC Setting**.

Figure 5-11 IPC setting

IPC Name	IP Addr.	Username	Port No	Protocol	Stream	Channel	Device Type	Modify	Delete
1000	0.0.0.0	admin	554	Local	Main	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		

Step 2 Click .

Figure 5-12 Add IPC

Step 3 Configure the parameters.

Table 5-4 Add IPC configuration

Parameter	Description
IPC Name	Enter the name that identifies the IPC.
IP Address	IP address of the IPC.
Username	Web interface login username and password of the device.
Password	
Port	Keep it default.
Protocol	Select Local or Onvif .
Stream Type	<ul style="list-style-type: none"> ● Main: Better video quality but requires more bandwidth. ● Extra1: Smoother video with poorer quality, but requires less bandwidth.
Channel	The number of the channels that a device supports.
Device Type	Select the one as needed.
MediaEncrypt	Select ON if the IPC to be added is encrypted.

Step 4 Click **Save**.

Other Operations

- **Export Config**: Export the device information to your PC.
- **Import Config**: Import device information.

5.5 Status

You can view the online status and IP addresses of all the connected devices.

Log in to the web interface of the SIP server, and then select **Household Setting > Status**.

Figure 5-13 Status

Room No.	Status	IP-Port	Reg Time	Off Time
201#0	Online	192.168.1.100	2018-10-09 02:01:58	0
201#1	Online	192.168.1.101	2018-10-09 02:02:11	0
12	Online	192.168.1.102	2018-10-09 02:02:15	0
11	Online	192.168.1.103	2018-10-09 02:06:20	0

5.6 Publish Information

You can send messages from the SIP server to VTH devices, and view message history.

5.6.1 Send Info

Step 1 Log in to the web interface of the SIP server, and then select **Household Setting > Publish Information > Send Info**.

Figure 5-14 Send information

Validity Period: 2000-01-16 23:59:59

Send to: All devices

Title:

Contents:

Confirm Refresh

Step 2 Specify the **Validity Period** that the message will be valid.

Step 3 Enter the VTO number or VTH number, or select **All devices** to send the message to all the devices in the network, and then enter the title and content of your message.

Step 4 Click **Confirm**.

5.6.2 History Info

You can view the information of sent messages.

Log in to the web interface of the SIP server, select **Household Setting > Publish Information > History Info**.

Figure 5-15 History information

IssueTime	Period of validity	Title	Delete
2018-10-09 16:52:31	2018-10-09 16:54:00		X
2018-10-09 16:52:31	2018-10-09 16:53:00		X
2018-10-09 03:15:38	2018-10-09 16:52:00		X

6 Network

This chapter introduces how to configure the network parameters.

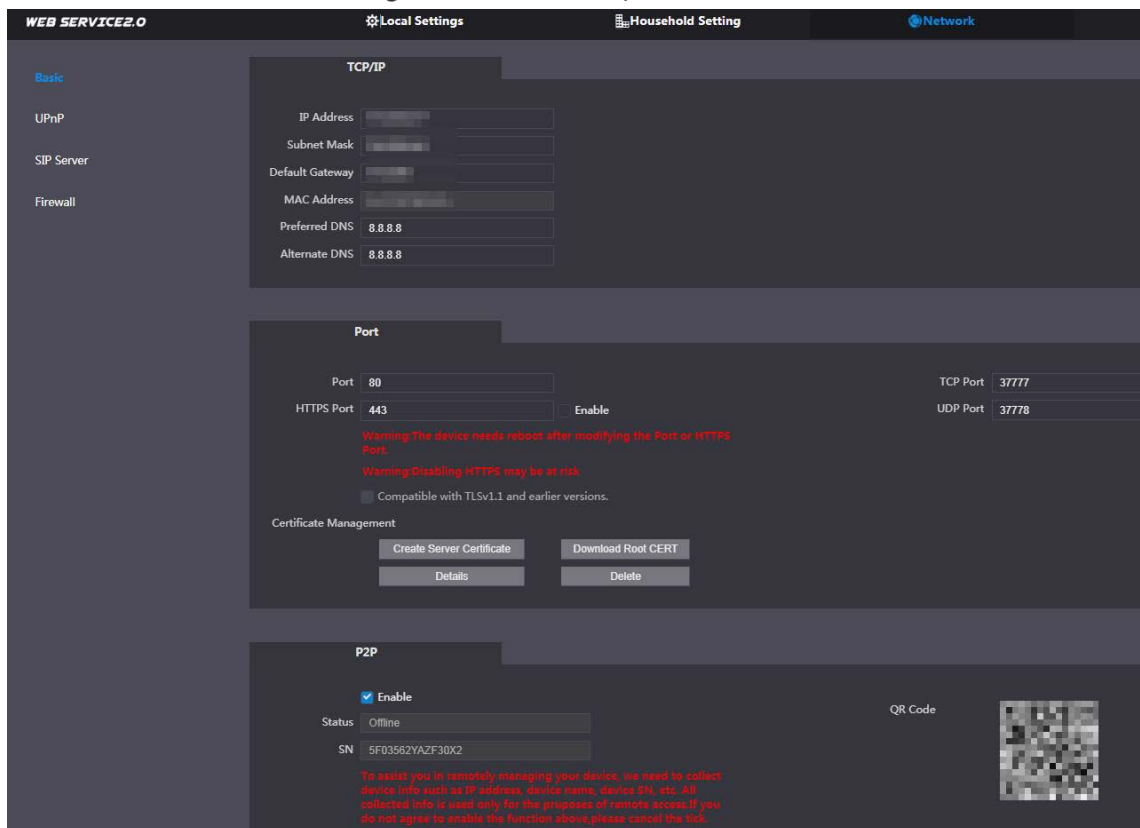
6.1 Basic

6.1.1 TCP/IP

You can modify the IP address, subnet mask, default gateway, and DNS of the VTO.

Step 1 Select **Network > Basic**.

Figure 6-1 TCP/IP and port





Step 2 Configure the parameters, 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.

6.1.2 Port

Table 6-1 Parameter description

Parameter	Description
Port	80 by default. If already used, choose any number from 1025 to 65535 as needed. You can enter <code>http://VTO IP address:Port</code> to log in to the VTO.
HTTPS Port	Enable it and click Save . You can now enter <code>https://VTO IP address:HTTPS Port</code> to

Parameter	Description
	log in to the VTO.
TCP/UDP Port	Used for accessing the VTO with devices in other networks. See "6.2 UPnP" for details.
Create Server Certificate	<p>The unique digital identification of VTO for the SSL protocol. For first time use or after changing the IP address of the VTO, you need to go through this process.</p>  <p>If you delete the certificate that has been created, it cannot be undone.</p>
Download Root CERT	<p>If you are using a PC that has never logged in to the VTO, you need to download the root certificate, double-click to install it, and then you can use the HTTPS function mentioned above.</p>  <p>If you delete the certificate that has been installed, it cannot be undone.</p>

6.1.3 P2P

Enable the **P2P** function, and then you can scan the QR code with your phone to add the VTO to the app on your smartphone. See the quick start guide for details.

6.2 UPnP

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

Preparation

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

6.2.1 Enabling UPnP Services

- Step 1 Select **Network > UPnP**.
- Step 2 Enable the services listed as needed.
- Step 3 Select **Enable**.
- Step 4 Click **Save**.

6.2.2 Adding UPnP Services


- Step 1 Select **Network > UPnP**.
- Step 2 Click **Add**.

Step 3 Configure the parameters as needed.

Figure 6-2 Add a UPnP service

The screenshot shows a dark-themed dialog box titled "Add" with a close button (X) in the top right corner. At the top, there are two radio buttons: "ON" (unselected) and "OFF" (selected). Below this are five input fields: "Service Name", "Service Type", "Internal Port", and "External Port" are text boxes, while "Protocol" is a dropdown menu currently showing "TCP". At the bottom right, there are two buttons: "Save" and "Cancel".

Table 6-2 Parameter description

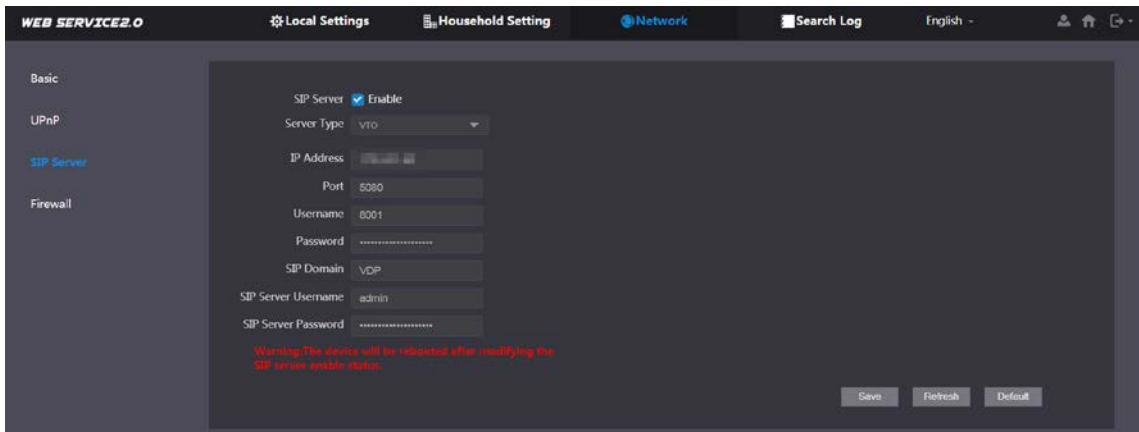
Parameter	Description
Service Name	Enter the information as needed.
Service Type	
Protocol	Select TCP or UDP as needed.
Internal Port	Use port number from 1024 through 5000.
External Port	 <ul style="list-style-type: none">Do not use port number 1–1023 to avoid conflict.If you need to configure this function for multiple devices, make sure that the ports are not the same.The port number you use must not be occupied.The internal and external port number must be the same.

6.3 SIP Server

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

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

Figure 6-3 SIP Server



Step 2 Select a server type as needed.

- The VTO you have logged in as the SIP server:
Enable **SIP Server**, and click **Save**, and then the VTO will restart. You can add VTOs and VTHs to this VTO. See the details in "5 Household Setting".



If the VTO you have logged in does not SIP server, do not enable **SIP Server**; otherwise the connection will fail.

- If another VTO works as the SIP server:
Do not enable **SIP server**. Set **Server Type** to **VTO**, configure the parameters, and then click **Save**.

Table 6-3 SIP server configuration

Parameter	Description
IP Addr.	VTO IP address.
Port	<ul style="list-style-type: none"> • 5060 by default when VTO work as SIP server. • 5080 by default when the platform works as SIP server.
Username	Keep it default.
Password	
SIP Domain	VDP.
SIP Server Username	Web interface login username and password of the VTO.
SIP Server Password	

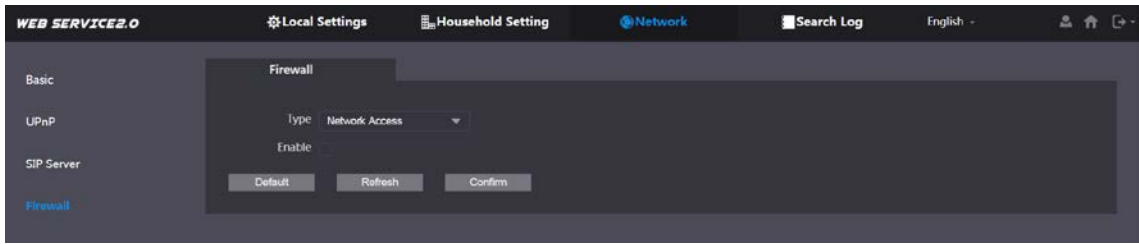
- If other servers work as the SIP server:
Select the **Server Type** as needed, and then see the corresponding manual for details.

6.4 Firewall

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

Step 1 Select **Network > Firewall**.

Figure 6-4 Firewall



Step 2 Select one or more firewall types, and then enable them.

Step 3 Configure the parameters.

Table 6-4 Firewall type description

Type	Description
Network Access	Select either Allowlist or Blocklist , and then add an IP address or segment which is allowed or denied to access the VTO.
PING Prohibited	The VTO will not response to ping to avoid ping attacks.
Anti-semijoin	Protects the VTO performance by blocking excessive SYN packets.

7 Log Management

Select **Search Log**. You can search for different logs, and export them to your PC as needed.



If storage is full, the oldest records will be overwritten. Back up the records as needed.

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, we recommend enabling 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, we recommend turning 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.

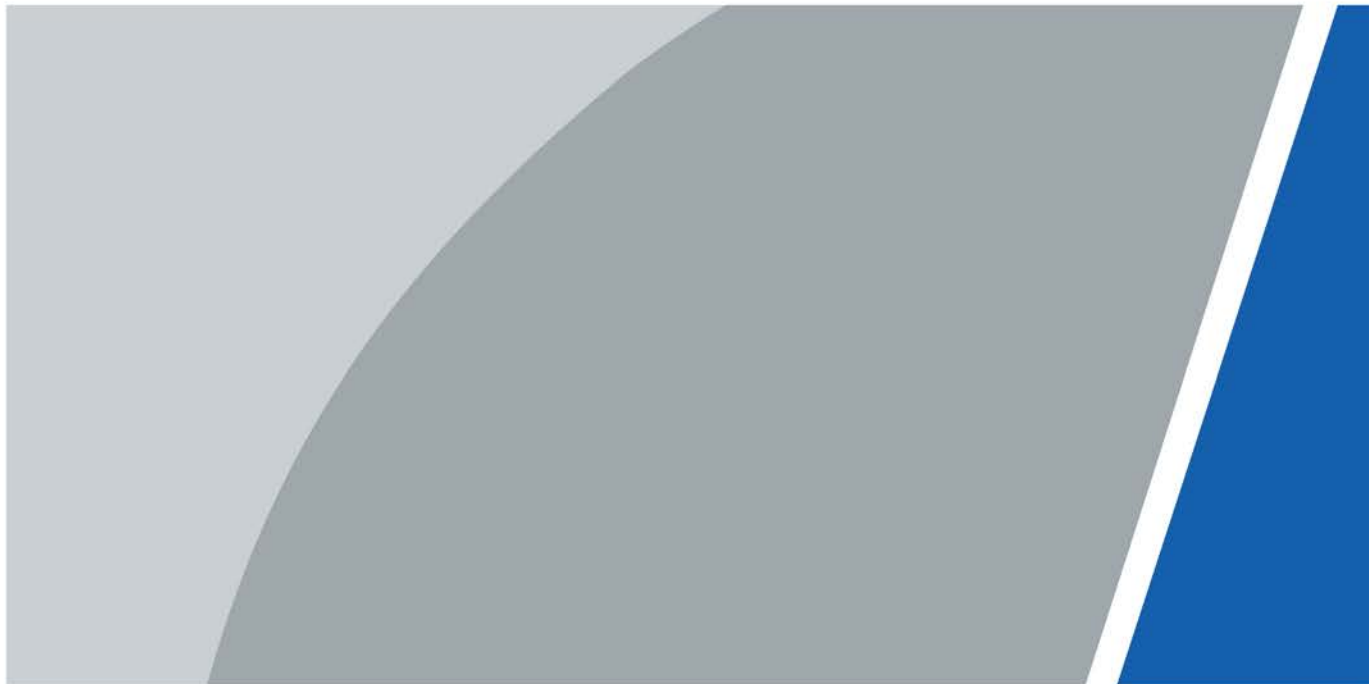
13. Construct a Safe Network Environment

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.

Digital VTH

Quick Start Guide








Foreword

General

This document mainly introduces structure, installation process and configuration of the product.

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 Date
V1.0.0	First release.	August 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 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 horizontally at stable places to prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids.
- Install the device at well-ventilated places and do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device by yourself.
- The device should be used with screened network cables.

Power Requirements

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

Device Update

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

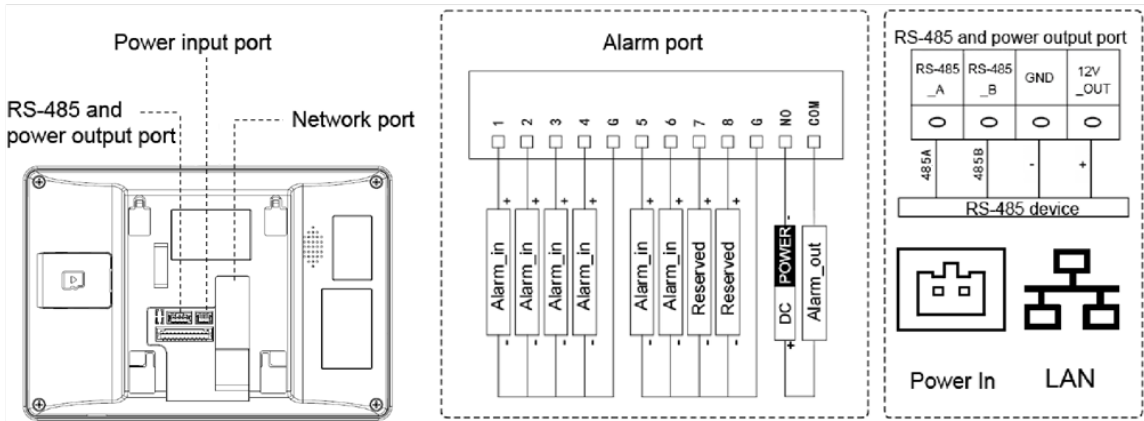
Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Rear Panel Port	1
1.1 VTH5421H	1
1.2 VTH5422H	1
2 Installation and Commissioning	2
2.1 Installation	2
2.2 Preparations	2
2.3 Commissioning	6
2.3.1 VTO Calls VTH	6
2.3.2 VTH Monitors VTO	7
Appendix 1 Cybersecurity Recommendations	9

1 Rear Panel Port

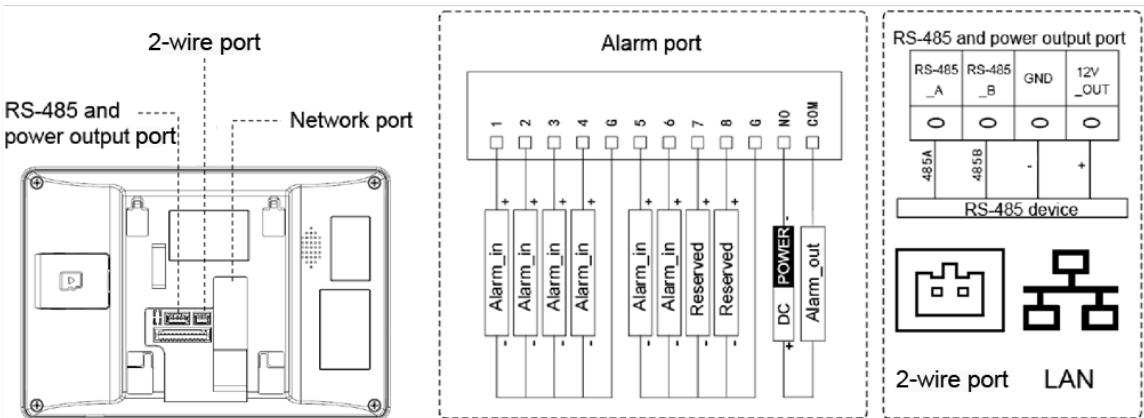
1.1 VTH5421H

Figure 1-1 Rear panel of VTH5421H



1.2 VTH5422H

Figure 1-2 Rear panel of VTH5422H



2 Installation and Commissioning

2.1 Installation



- Do not install VTH in harsh environment with condensation, high temperature, dust, corrosive substance and direct sunlight.
- In case of abnormality after powering on, unplug network cable and cut off power supply at once. Power on after troubleshooting.
- Installation and debugging should be done by professional teams. Do not dismantle or repair by yourself in case of device failure. Contact after-sales service.
- Device central point height should be 1.4 m–1.6 m above the ground (this device is only suitable for mounting at height ≤ 2 m).

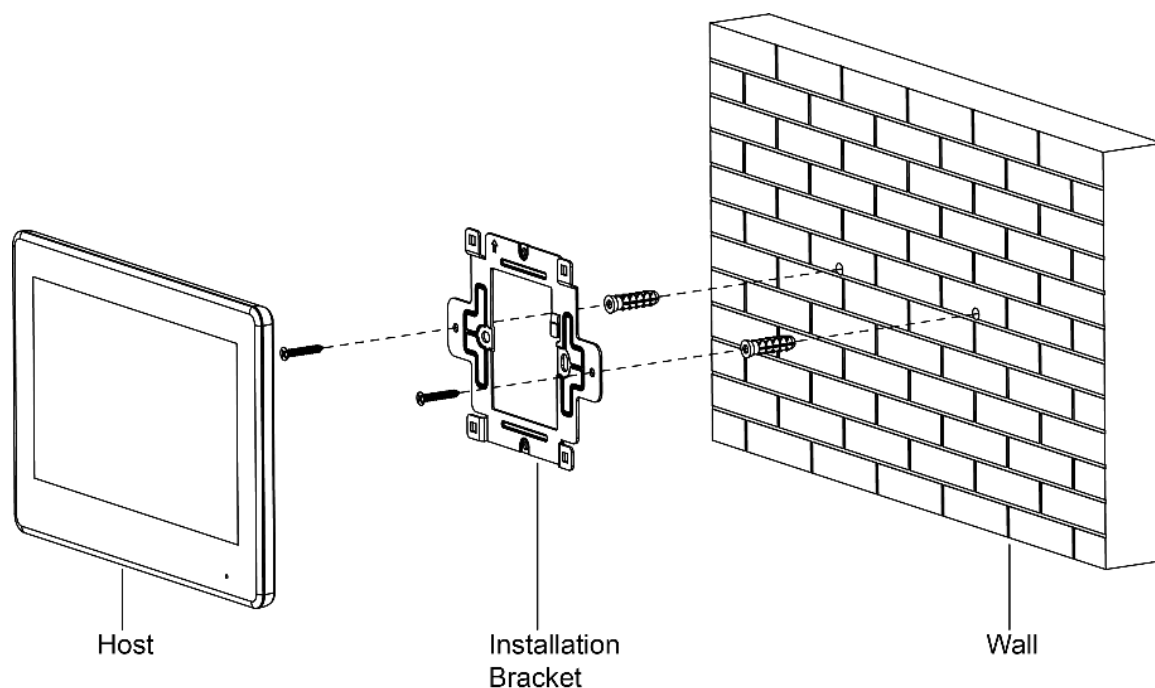
Directly install the device with a bracket onto a wall, which is suitable for all types of devices.

Step 1 Drill holes in the wall according to hole positions of the installation bracket.

Step 2 Fix the installation bracket on the wall with screws.

Step 3 Put the device into installation bracket from top down.

Figure 2-1 Surface installation



2.2 Preparations

Before commissioning, check whether the following work has been completed.

- Power on the device only after there is no short or open circuit.
- Plan IP and number (works as a phone number) for each VTO and VTH.
- Confirm the location of the SIP server.
- Scan QR code on the cover for details.
- Set VTO info and VTH info on the web interface for every VTO, and set VTH info, network info and VTO info on every VTH.

VTH Settings

For first-time use, set up password and bind Email. Password is used to enter project setting interface, while email address is used to retrieve your password when you forget it.

Step 1 Power on the device, Select region and language, and tap **OK**.

Figure 2-2 Select region and language

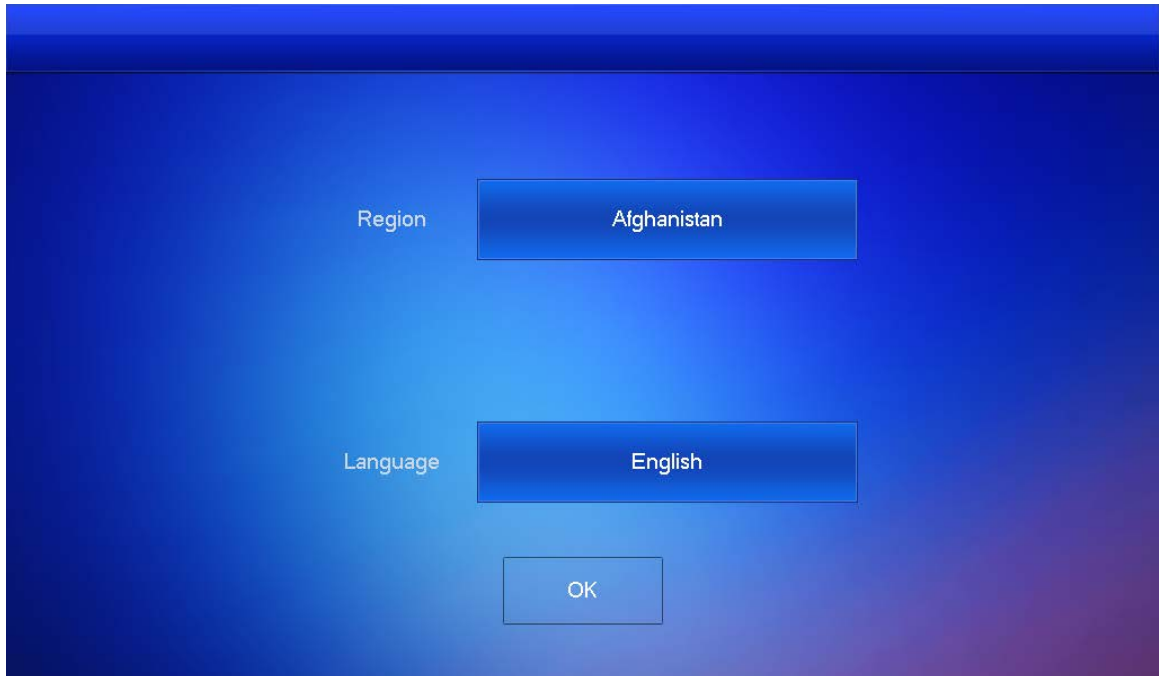
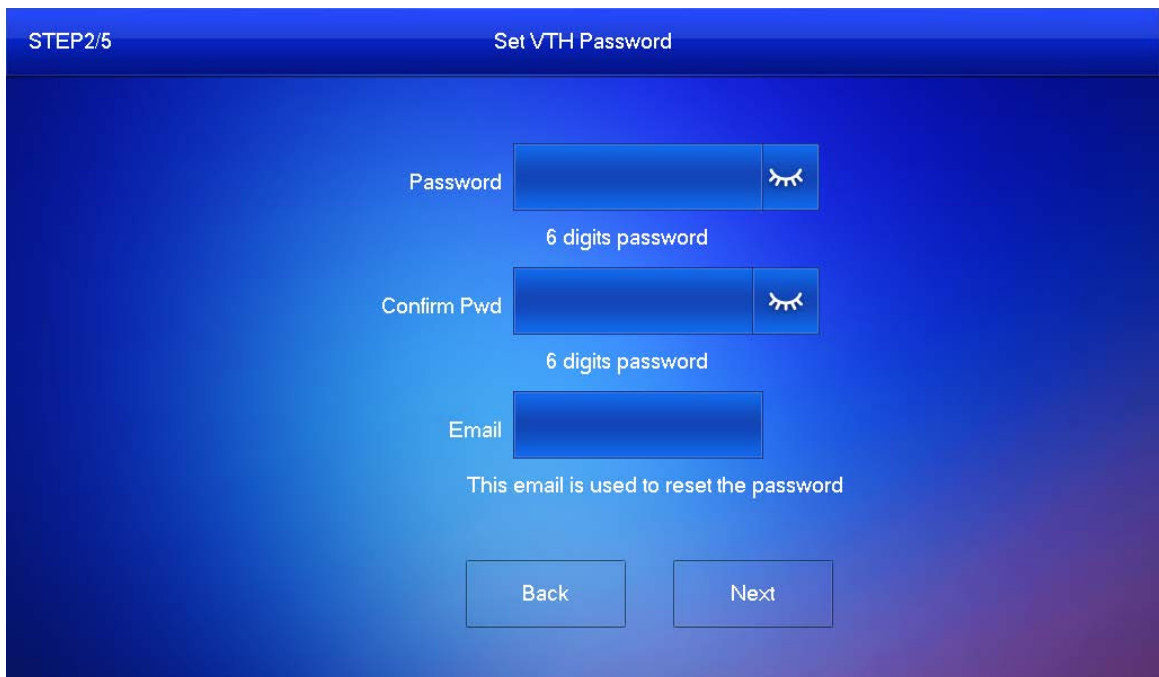


Figure 2-3 Set password for VTH



Step 2 Enter password and confirm it, enter email, and tap **Next**.

Step 3 Tap **Setting** for more than 6 seconds, enter the password set just now, and then tap **OK**.

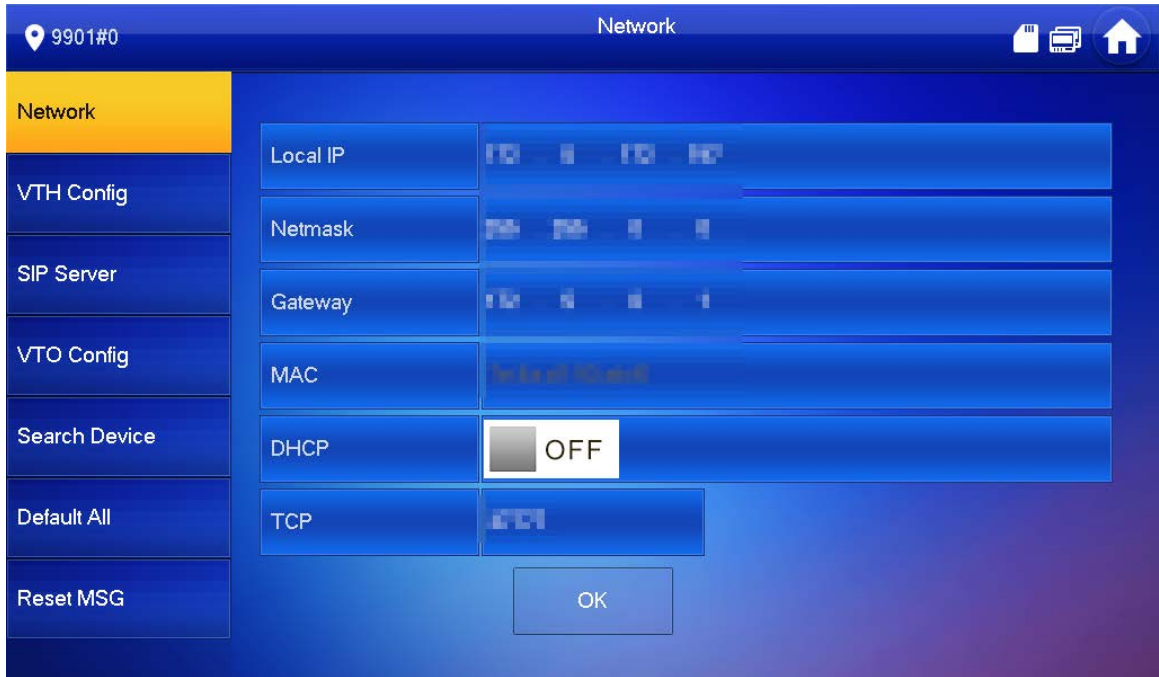
Step 4 Tap **Network**. Enter local IP, netmask, and gateway, and then tap **OK**, Or tap OFF to enable DHCP function to obtain IP info automatically.



IP addresses of VTH and VTO should be in the same network segment. Otherwise, VTH cannot

obtain VTO information after configuration.

Figure 2-4 Network



Step 5 Tap **VTH Config**.

Figure 2-5 VTH configuration



- Use as a master VTH.

Enter Room No. (such as 9901 or 101#0) and tap **OK**.



Room No. should be the same as VTH Short No., which is set when adding VTH on the web interface. Otherwise, it will fail to connect to VTO.

If there is extension VTH, room No. should end with #0. Otherwise, it will fail to connect to VTO.

- Use as an extension VTH.

1) Tap **Master** and the icon switches to **Extension**.

- 2) Enter room No. (such as 101#1) and the IP address of master VTH.
Master name and master password are the username and password of master VTH.
Default username is **admin**, and the password is the one set from previous step.



Security mode is **On** by default, and you can keep the default status.

- 3) Tap **OK** to save the settings.

Step 6 Tap **SIP Server**.

Figure 2-6 SIP server



- 1) Set parameters of **SIP Server** by reference to Table 2-1.

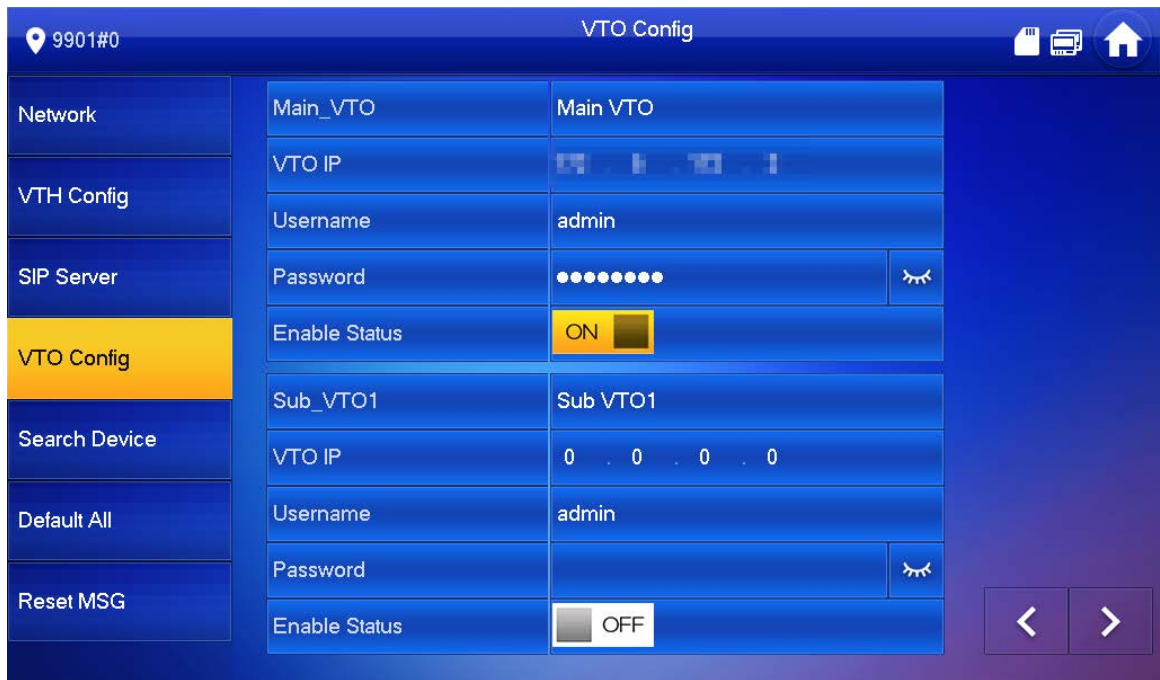
Table 2-1 SIP server

Parameter	Description
Server IP	<ul style="list-style-type: none"> When the platform works as SIP server, server IP is the IP address of the platform. When VTO works as SIP server, server IP is the IP address of the VTO.
Network Port	<ul style="list-style-type: none"> When the platform works as SIP server, network port is 5080. When VTO works as SIP server, network port is 5060.
User Name	Use default value.
Register Pwd	
Domain	Registration domain of SIP server, which can be empty. When VTO works as SIP server, registration domain of SIP server should be VDP.
Username	Username and password to log in to SIP server.
Login Pwd	


- 2) Set **Enable Status** to .
- 3) Tap **OK**.

Step 7 Tap **VTO Config**.

Figure 2-7 VTO configuration




Step 8 Add VTO.



- Add main VTO.
 - 1) Enter main VTO name, VTO IP address, username and password.
 - 2) Set **Enable Status** to .



Username and **Password** should be the same as web login username and password of VTO. Otherwise, it will fail to connect.

- Add sub VTO.
 - 1) Enter sub VTO name, sub VTO IP address, username, and password.
 - 2) Set **Enable Status** to .



Tap  /  to turn page and add more sub VTOs.

2.3 Commissioning

2.3.1 VTO Calls VTH

Dial VTH room No. (such as 101) at VTO to call VTH. VTH pops up monitoring video and operating icons. See Figure 2-8.



The following figure means that SD card has been inserted into VTH. If SD card is not inserted, recording and snapshot icons are gray.

Figure 2-8 Call VTH from VTO



2.3.2 VTH Monitors VTO

VTH is able to monitor VTO or IPC. Take VTO as an example.

Select **Monitor > Door**. See Figure 2-9. Select the VTO to enter monitoring video. See Figure 2-10.



The following figure means that SD card has been inserted into VTH. If SD card is not inserted, recording and snapshot icons are gray.

Figure 2-9 Door

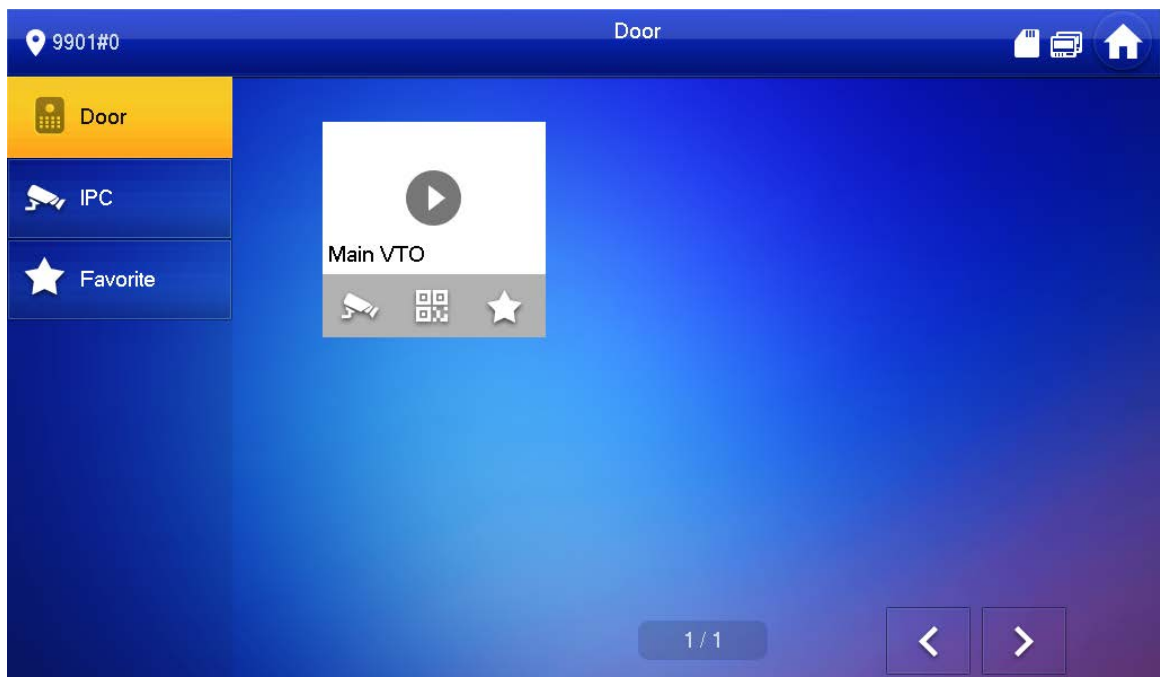
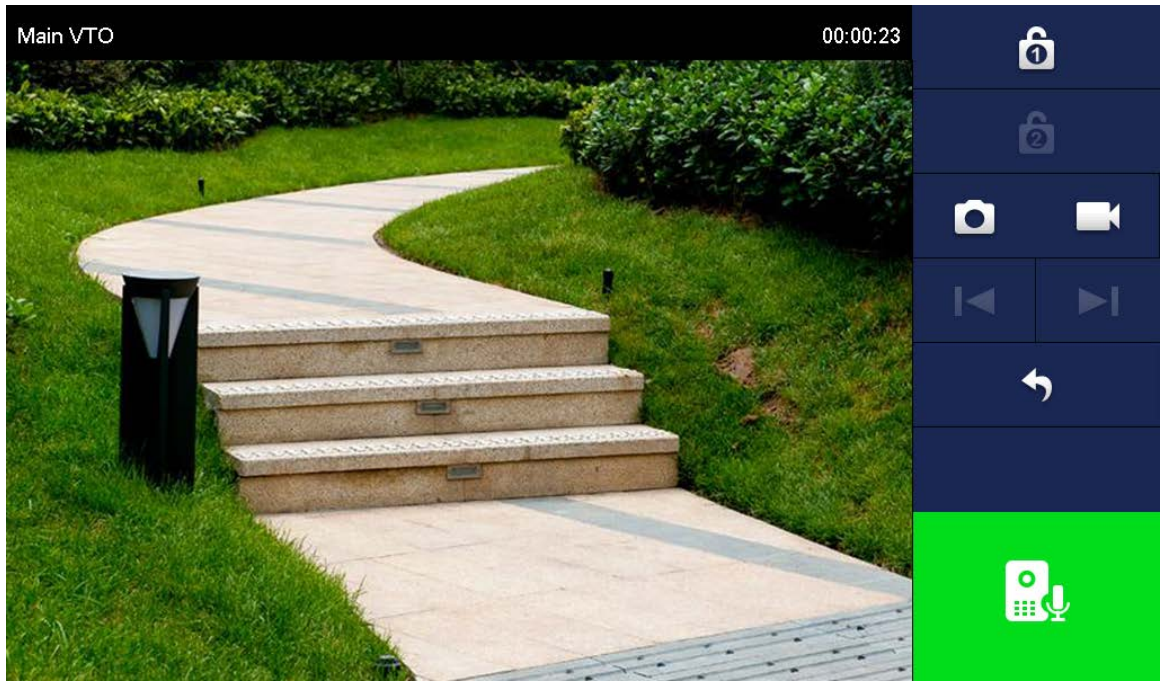


Figure 2-10 Monitoring video



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.

Digital VTH

User's Manual



Foreword

General






This document mainly introduces function, structure, networking, installation process, debugging, UI operation and technical parameter of digital VTH products.

Device Update

Do not cut off the power supply during upgrade. Power can be cut off only after the device completes upgrade and reboots.

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.	November 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 User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's 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 Guide (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, 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 expose the device to direct sunlight or heat sources.
- Do not install the device in a humid, dusty or fuliginous area.
- Install the device on a stable location horizontally to prevent it from falling.
- Prevent liquid from flowing into the device.
- Install the device at well-ventilated places and do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not disassemble the device by yourself.

Power Requirement

- Use the product with electric wires recommended in this area and within 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. See the device label for specific power supply requirements.
- Appliance coupler is a disconnecting device. Keep an angle that facilitates operation during normal use.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Product Overview	1
1.1 Introduction.....	1
1.2 Function.....	1
2 Network Diagram	3
2.1 2-wire System.....	3
2.2 Digital System.....	3
3 Preparation and Commissioning	6
3.1 Preparation.....	6
3.1.1 VTO Settings.....	6
3.1.2 VTH Settings.....	13
3.2 Commissioning.....	25
3.2.1 VTO Calling VTH.....	25
3.2.2 VTH Monitoring VTO.....	25
4 Interface Operation	27
4.1 Main Interface.....	27
4.2 Call.....	28
4.2.1 Recent Call.....	28
4.2.2 Contact.....	29
4.2.3 Call User.....	30
4.2.4 Call from User.....	32
4.2.5 Call from VTO.....	33
4.3 Info.....	34
4.3.1 Security Alarm.....	34
4.3.2 Guest Message.....	35
4.3.3 Publish Info.....	35
4.3.4 Video Pictures.....	36
4.4 Monitor.....	36
4.4.1 Monitoring VTO.....	37
4.4.2 Monitoring IPC.....	39
4.4.3 Favorite.....	41
4.5 SOS.....	42
4.6 Setting.....	42
4.6.1 Ring Settings.....	42
4.6.2 Card Information.....	45
4.6.3 Alarm Setting.....	46
4.6.4 Mode Setting.....	49
4.6.5 Forward Setting.....	50
4.6.6 General Setting.....	51
4.6.7 Product Info.....	57
4.7 Project Settings.....	58
4.7.1 Forget Password.....	58

4.7.2 Network Settings	59
4.7.3 VTH Configuration	59
4.7.4 VTO Configuration	59
4.7.5 Default	60
4.7.6 Reset MSG	60
4.8 Unlock Function	60
4.9 Arm and Disarm Function	61
4.9.1 Arm	61
4.9.2 Disarm	62
5 DSS Agile VDP	63
5.1 Downloading the App	63
5.2 Registration and Login	64
5.3 Call Functions	65
5.3.1 Forwarding Calls	66
5.3.2 Calling Operations	68
5.4 Monitoring	68
5.5 Call Records	70
5.6 Message	72
5.7 Visitor	75
5.7.1 Creating Pass	75
5.7.2 Visit Records	77
5.8 Setting	78
Appendix 1 Cybersecurity Recommendations	80

1 Product Overview

1.1 Introduction

A digital VTH is device that can perform monitoring, voice/video call, and door unlock.

1.2 Function

Wi-Fi Networking

Connect to Wi-Fi networks.

Video/Voice Call

Make video or voice call to other VTOs and VTHs.

Monitoring

Monitor fence station, VTO and IPC devices (only supported by certain models).

SOS

Make emergency call to the Call Center.

Auto Snapshot

Take snapshots when calling or monitoring, and store them in the SD card.

DND (Do Not Disturb)

Mute all message and call notifications.

Remote Unlock

Unlock doors remotely.

Arm and Disarm

Arm and disarm 6 alarm devices.

Playback

Play back videos and pictures in the SD card.

Alarm

Alarms will trigger linkage and be sent to the Call Center.

Record

View call and alarm records.

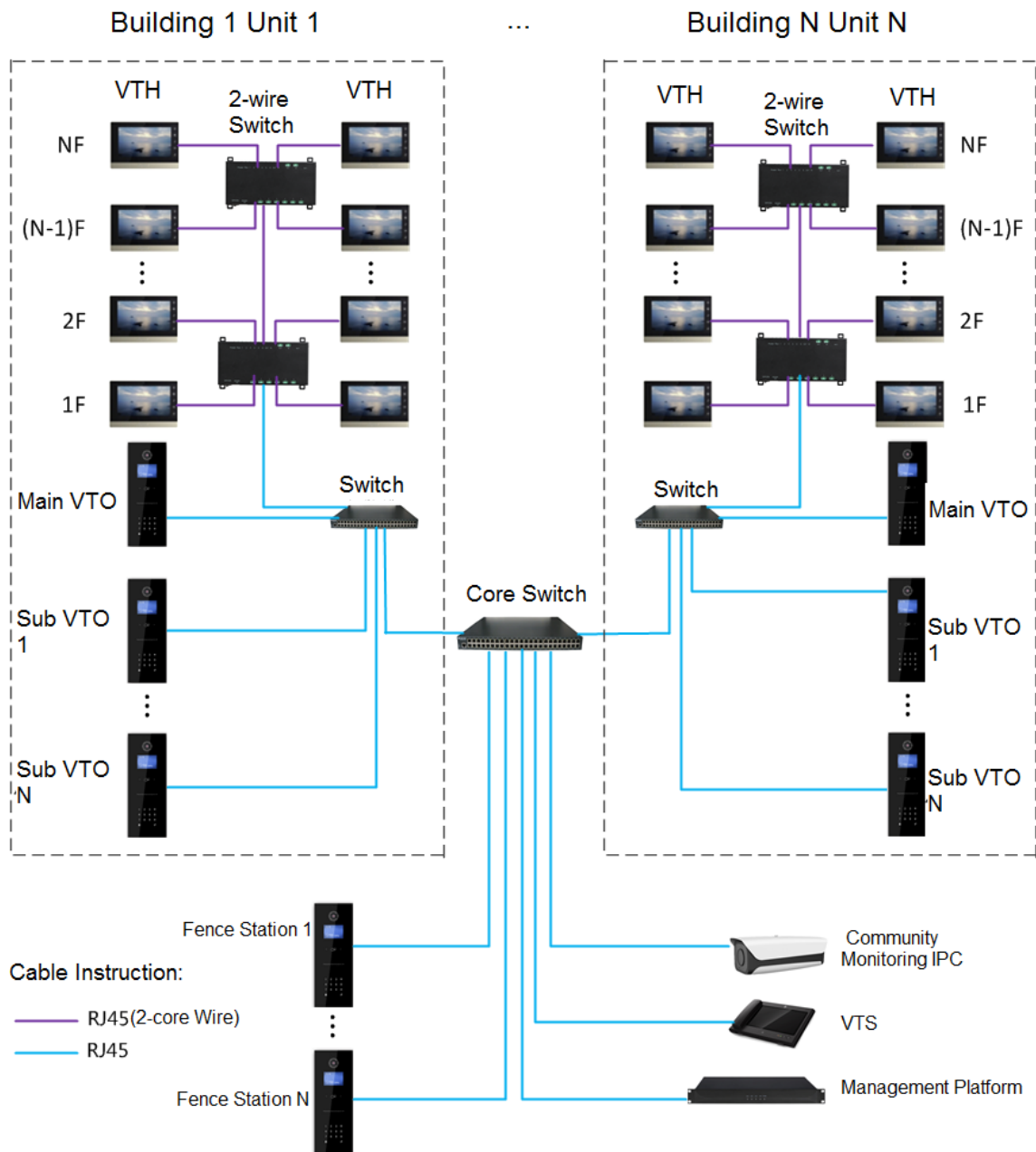
Message

View messages, including videos, pictures and announcements.

2 Network Diagram

2.1 2-wire System

Figure 2-1 Network diagram of 2-wire system

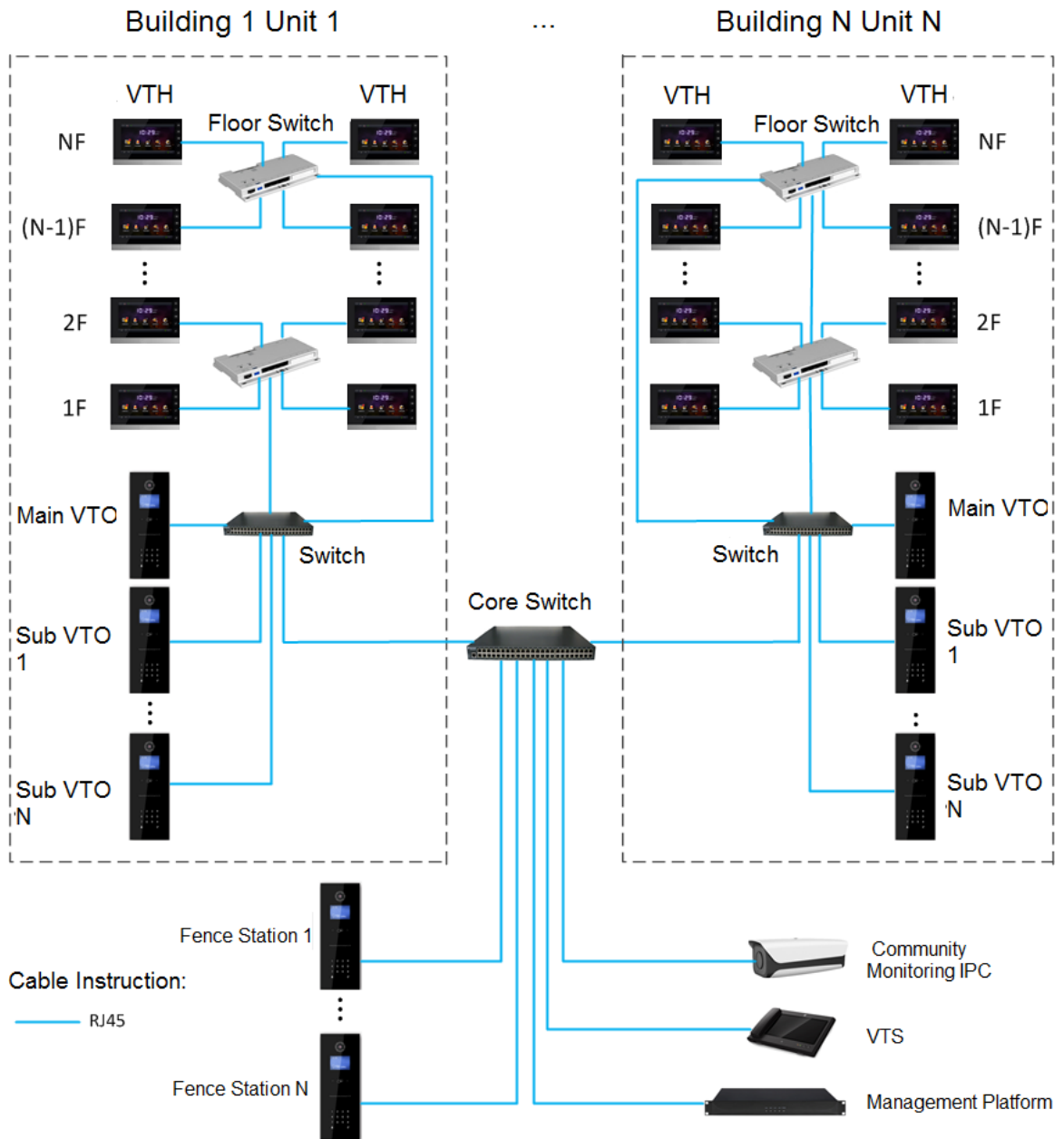


2.2 Digital System

There are two types of digital system network:

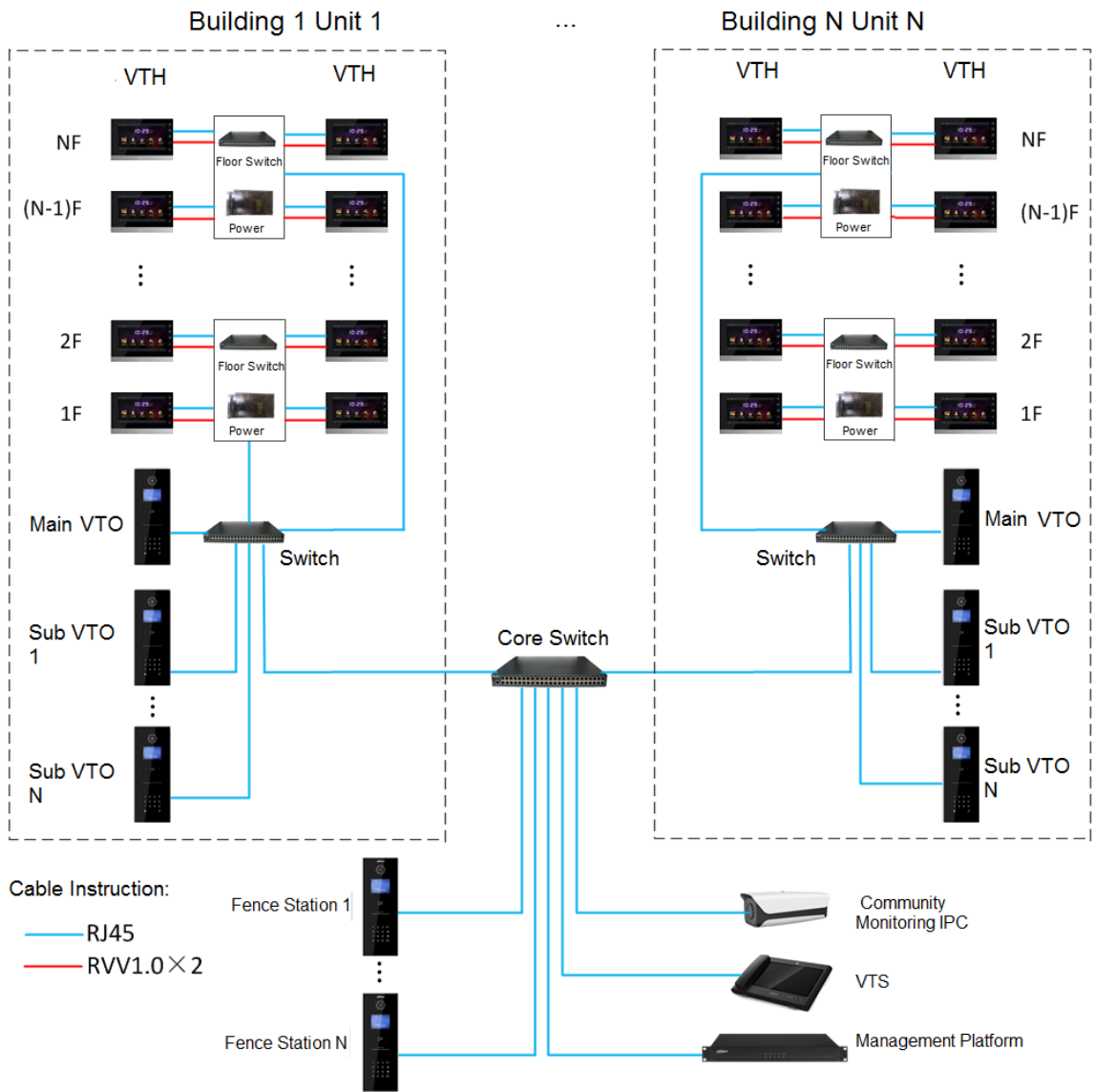
- The VTH powered through PoE from the floor switch.

Figure 2-2 Network diagram of digital system (1)



- The VTH is independently powered through a power supply.

Figure 2-3 Network diagram of digital system (2)



3 Preparation and Commissioning

Carry out commissioning to ensure that the device can realize basic network access, call and monitoring functions.

3.1 Preparation

Before commissioning:

- Power on the device only after there is no short or open circuit.
- Plan IP addresses and numbers (works as phone numbers) for every VTO and VTH.
- Confirm the position of the SIP server.



- The device must be used with a VTO that is the SIP server. This section takes a unit VTO as an example. See corresponding user's manuals for other VTO types.
- Log in to the web interface of every VTO and VTH and configure all relevant information.

3.1.1 VTO Settings

3.1.1.1 Initialization

For first-time use, you must initialize the device.



Make sure that the IP addresses of the PC and VTO are in the same network segment. The default IP address of VTO is 192.168.1.108.

Step 1 Power on the VTO.

Step 2 Go to the default IP address of VTO in the browser.

Figure 3-1 Device initialization

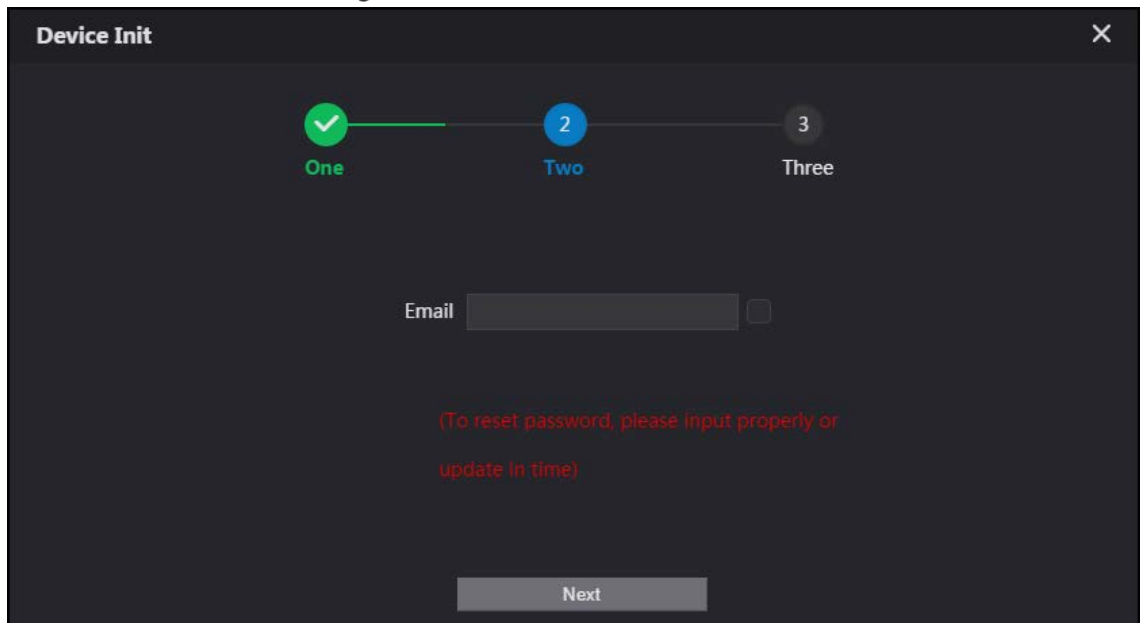
The screenshot shows a dark-themed web interface titled "Device Init" with a close button (X) in the top right corner. At the top, there is a progress indicator with three steps: "1 One", "2 Two", and "3 Three". Step 1 is highlighted in blue. Below the progress indicator, the "Username" field is pre-filled with "admin". The "Password" field is empty, and below it are three buttons labeled "Low", "Middle", and "High". The "Confirm Password" field is also empty. At the bottom center, there is a "Next" button.

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



This password is used to log in to the web interface. It must be at least 8 characters, and include a combination of at least two types among number, letter and symbol.

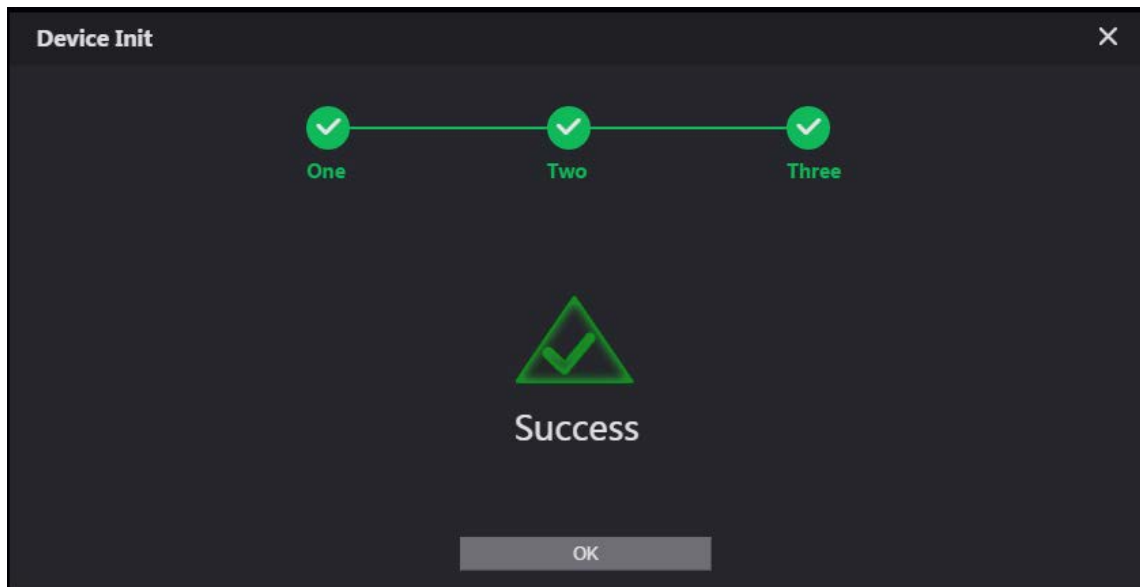
Figure 3-2 Set an email address



Step 4 Select **Email** and enter your email address for resetting password.

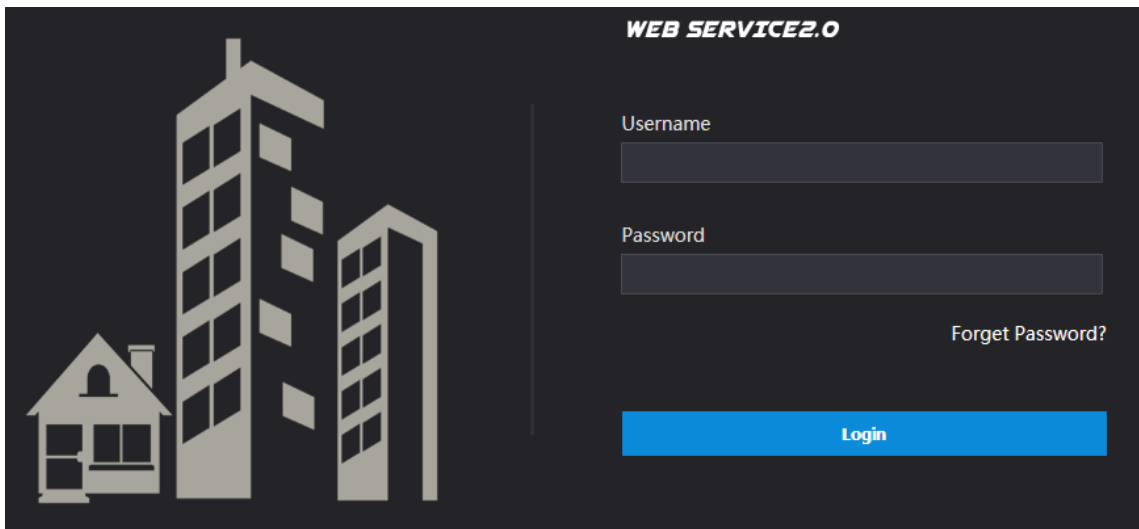
Step 5 Click **Next**.

Figure 3-3 Initialization successful



Step 6 Click **OK** and the it jumps to the login interface.

Figure 3-4 Login interface



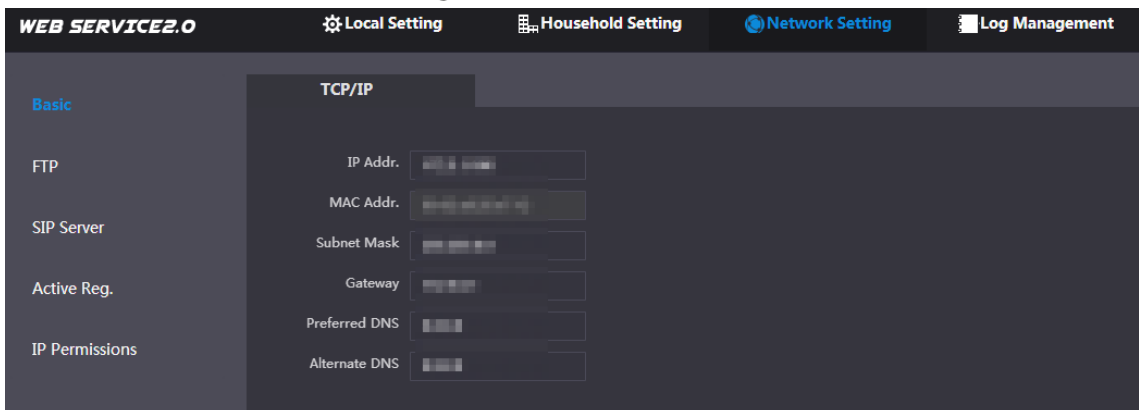
Step 7 Enter username (admin by default) and password, and then click **Login**.

3.1.1.2 Network Parameters

Change the IP address of the VTO to the one that you planned.

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

Figure 3-5 TCP/IP



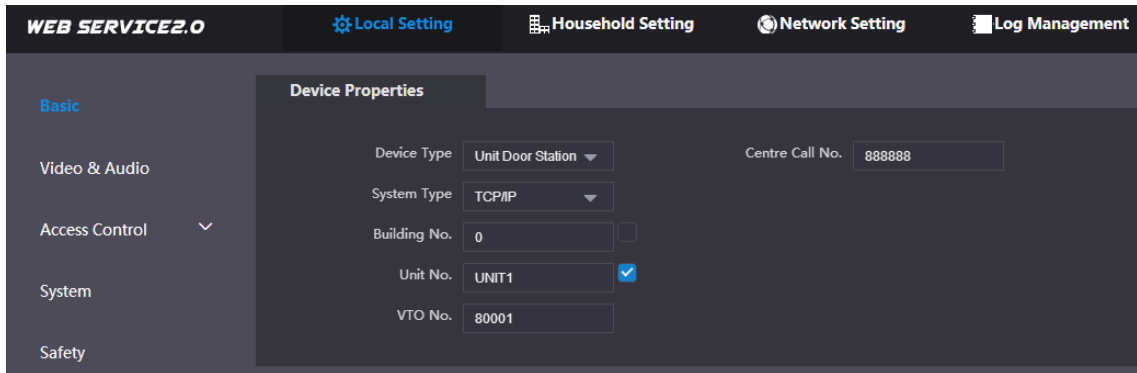
Step 2 Enter the parameters, and then click **OK**.

The VTO automatically restarts. Make sure that the PC is in the same network segment as the VTO to log in again.

3.1.1.3 System Type

Step 1 Select **Local Setting > Basic**.

Figure 3-6 Device properties



Step 2 Select **System Type** to **TCP/IP**.

Step 3 Click **OK**.

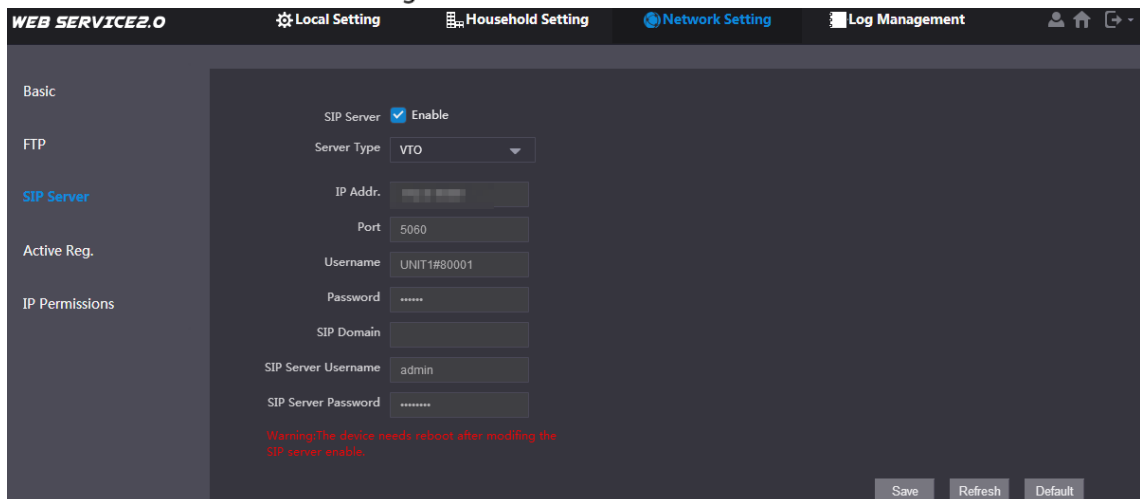
Wait for the device to automatically restart or restart it manually, and then the settings will take effect.

3.1.1.4 Server Type

You can select the type of the server that manages all VTO devices.

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

Figure 3-7 SIP server (1)



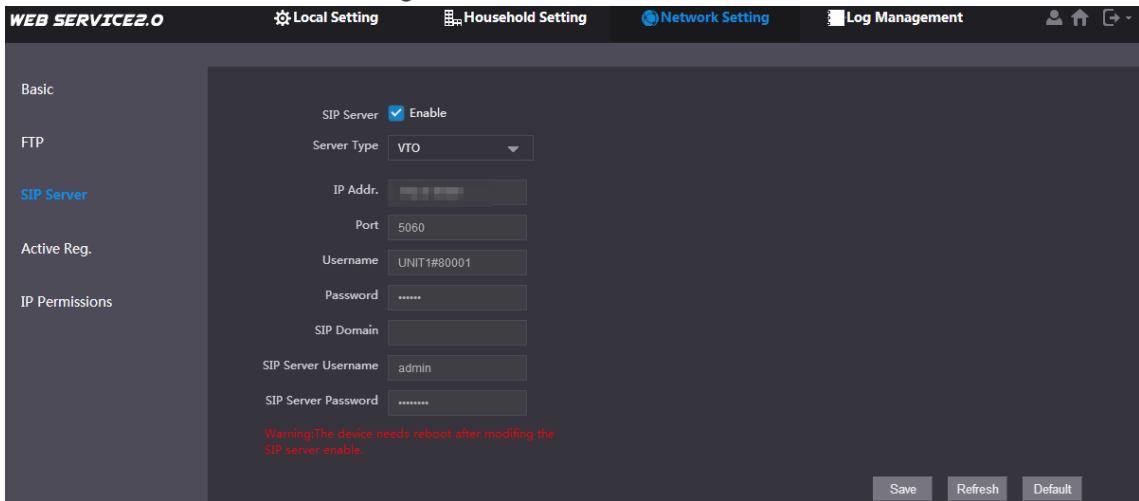
Step 2 Select a server type.

- When this VTO or another VTO works as the SIP server, select **Server Type** to **VTO**. It applies to a scenario where there is only one building.
- When a platform (such as Express/DSS) works as the SIP server, select **Server Type** to **Express/DSS**. It applies to a scenario where there are multiple buildings.

3.1.1.5 SIP Server

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

Figure 3-8 SIP server (2)



Step 2 Configure SIP server.

- The current VTO works as the SIP server.
Enable **SIP Server**, and then click **OK**. The VTO automatically restarts, and it jumps to the login interface.



If the current VTO is not the SIP server, do not enable **SIP Server**; otherwise the connection will fail.

- Another VTO works as the SIP server.
Disable **SIP Server**, configure the parameters, and then click **OK**. The VTO automatically restarts, and it jumps to the login interface.

Table 3-1 SIP server parameters when a VTO works as the SIP server

Parameter	Description
IP Address	IP address of the VTO that works as the SIP server.
Port	5060 by default.
Username	Keep it default.
Password	
SIP Domain	VDP.
Login Username	SIP server login username and password.
Login Pwd	

- The platform (Express/DSS) works as the SIP server.
- Select **Server Type** as **Express/DSS**, configure the parameters, and then click **OK**. The VTO automatically restarts, and it jumps to the login interface.

Table 3-2 SIP server parameters when the platform works as the SIP server

Parameter	Description
IP Address	IP address of the platform.
Port	5080 by default.
Username	Keep it default.
Password	
SIP Domain	Keep it default or null.
SIP Server Username	SIP server login username and password.
SIP Server Password	



- VTO settings have been completed if the platform or another VTO works as the SIP server.
- If the current VTO works as the SIP server, **Device Manager** will appear on the left. See 3.1.1.6 Adding VTO and 3.1.1.7 Adding VTH to add VTOs and VTHs.

3.1.1.6 Adding VTO

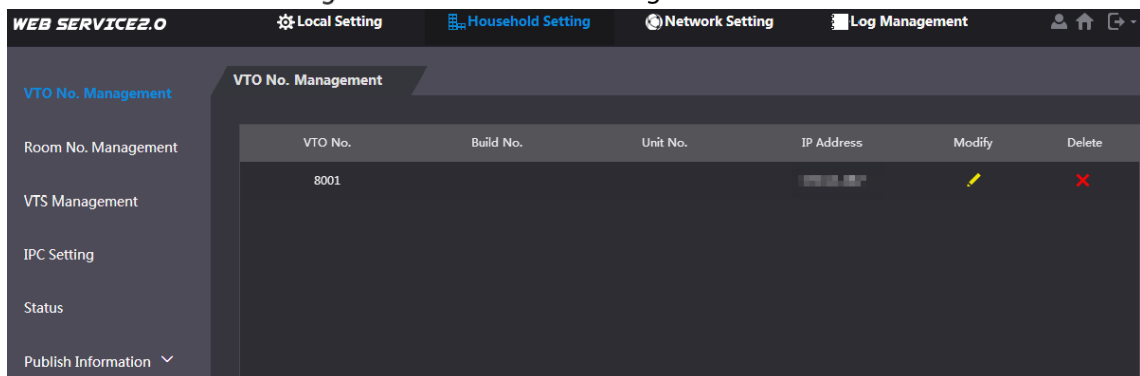


Add VTO only when the current VTO works as the SIP server.

Step 1 Log in to the web interface.

Step 2 Select **Household Setting > VTO No. Management**.

Figure 3-9 VTO number management



Step 3 Click **Add**.

Figure 3-10 Add a VTO

Step 4 Configure the parameters.

Table 3-3 Parameters of adding a VTO

Parameter	Description
Rec No.	VTO number.
Register Password	Keep it default.
IP Address	IP address of VTO.
Username	Web interface login username and password of this VTO.
Password	

Step 5 Click **OK**.

Do Step 3–Step 5 to add other VTOs.

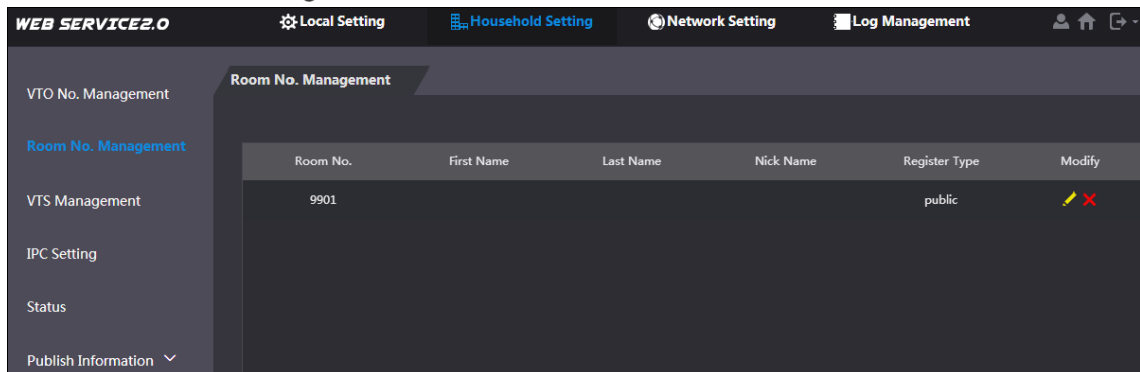
3.1.1.7 Adding VTH



- Add VTHs only when the current VTO works as the SIP server.
- Add both main and extension VTHs.

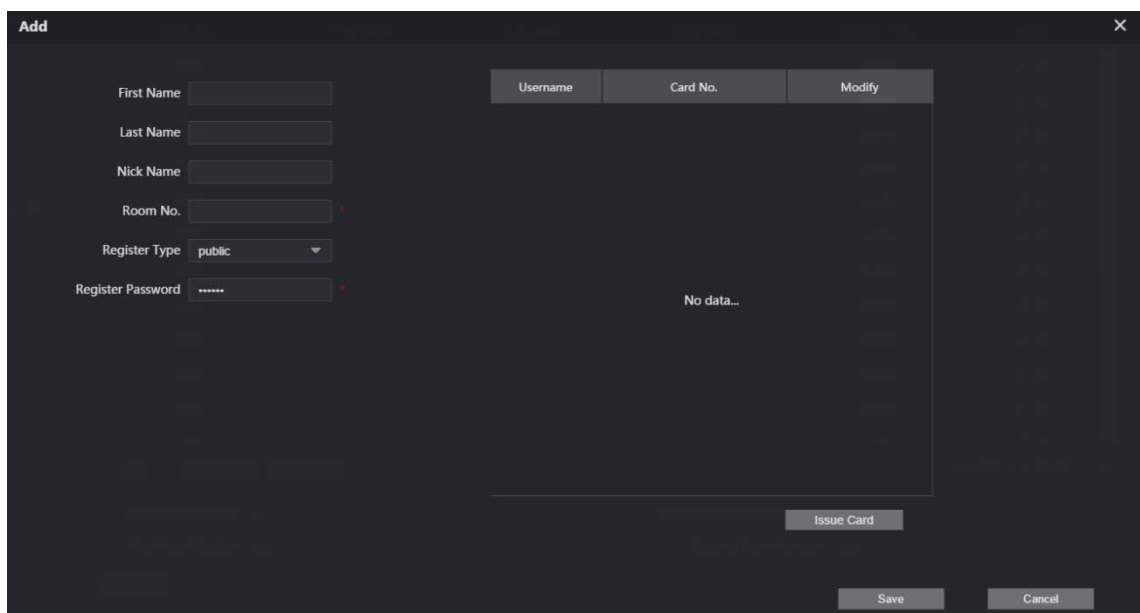
Step 1 Select **Household Setting > Room No. Management**.

Figure 3-11 Room number management




Step 2 Click **Add**.

Figure 3-12 Add a VTH



Step 3 Configure the parameters.

Table 3-4 Parameters of adding a VTH

Parameter	Description
First Name	Information to distinguish each device.
Last Name	
Nick Name	
Room No.	 <ul style="list-style-type: none"> VTH number consists of 1–6 numbers, which may include number and #. It must be consistent with room number configured at the VTH. When there are main VTH and extensions, to use group call function, the main VTH number must end with #0, and the extension VTH number must end with #1, #2 and #3. For example, if the main VTH is 101#0, extension VTHs must be 101#1, 101#2...
Register Password	Keep it default.
Register Type	

Step 4 Click **OK**.

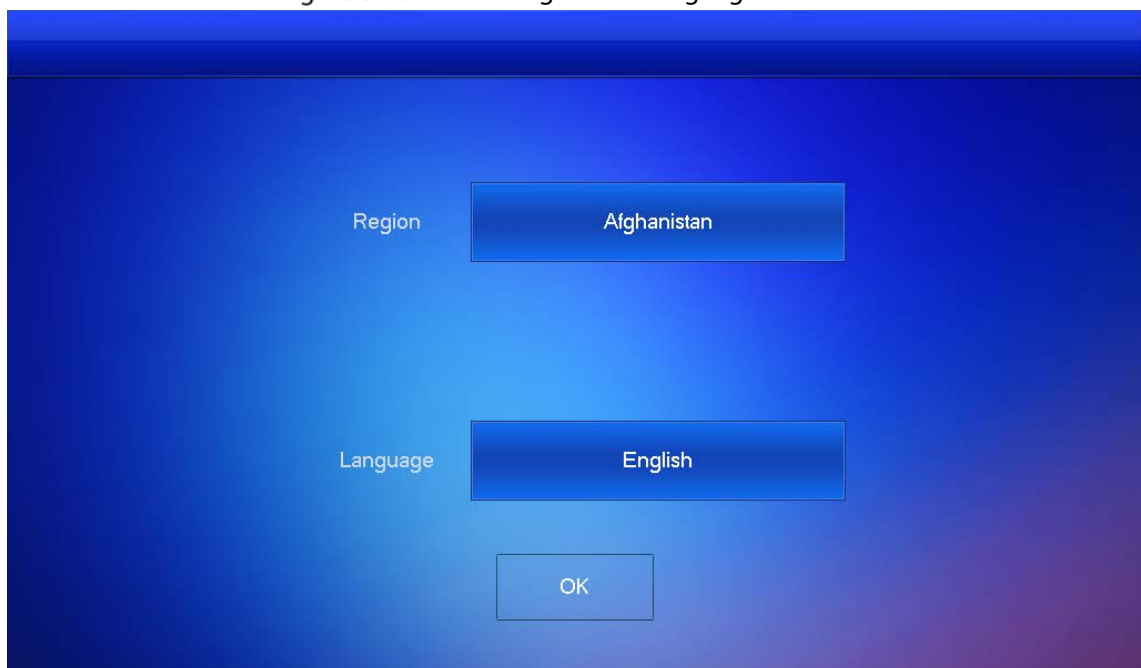
Do Step 2–Step 4 to add other VTHs.

3.1.2 VTH Settings

3.1.2.1 Initialization

Step 1 Select a region and language.

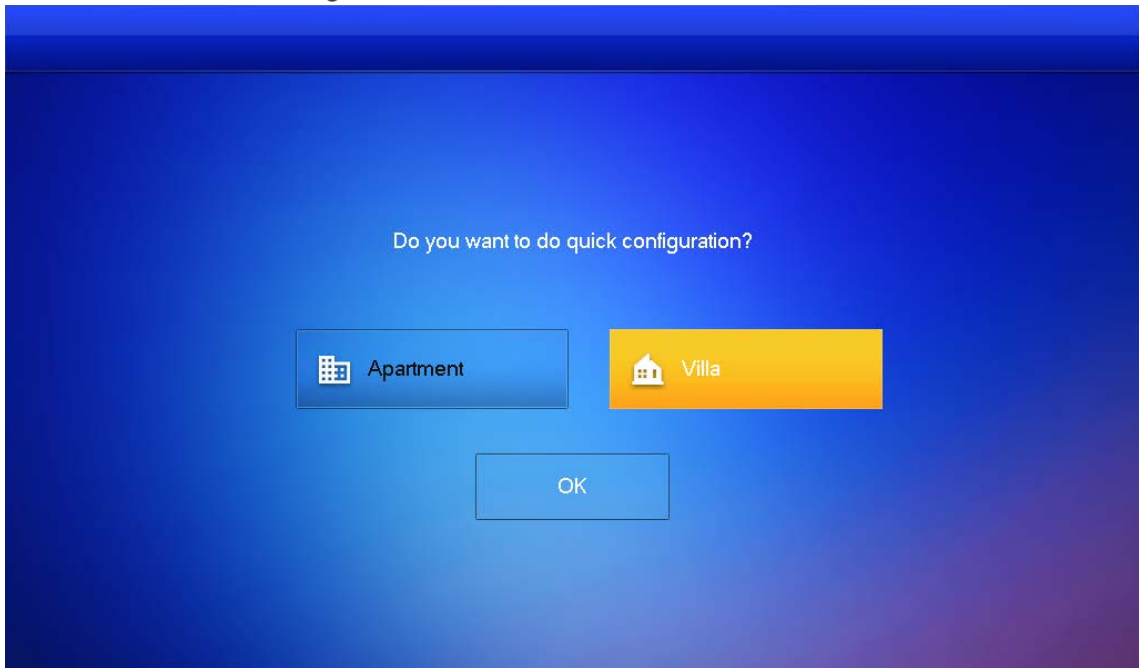
Figure 3-13 Select a region and language



Step 2 Select **Apartment** or **Villa**, and then tap **OK**.

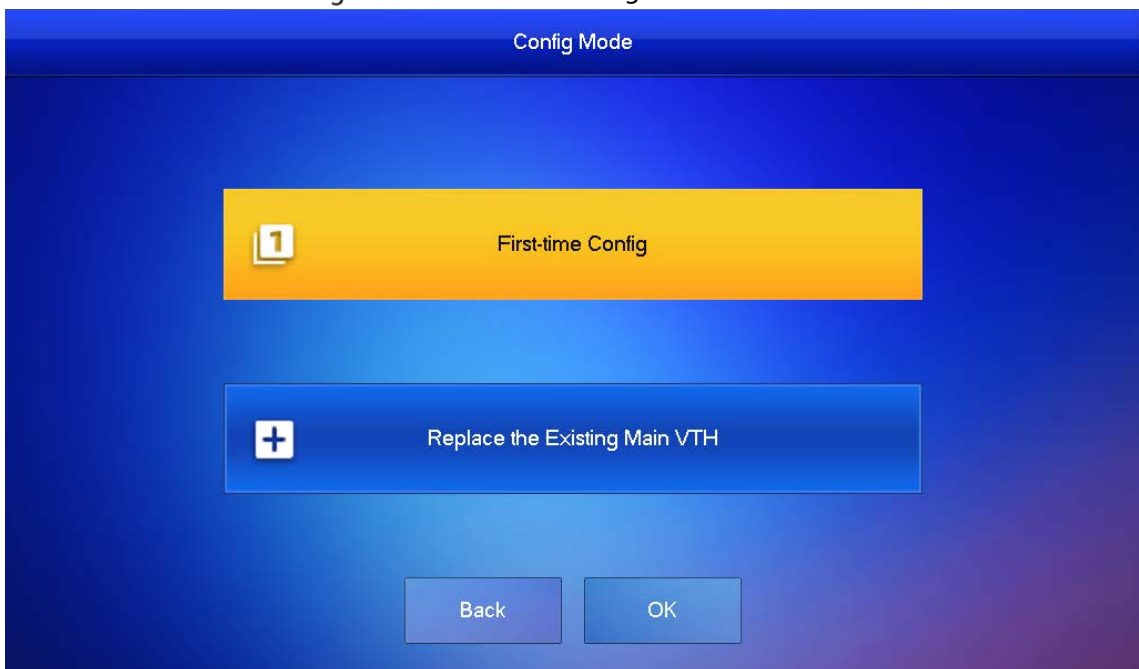
This section takes **Villa** as an example.

Figure 3-14 Select apartment or villa



Step 3 Select **First-time Config** and tap **OK**.

Figure 3-15 First-time configuration



Step 4 **DHCP** is selected by default, or select **Static IP** and configure the parameters as needed.

Figure 3-16 DHCP

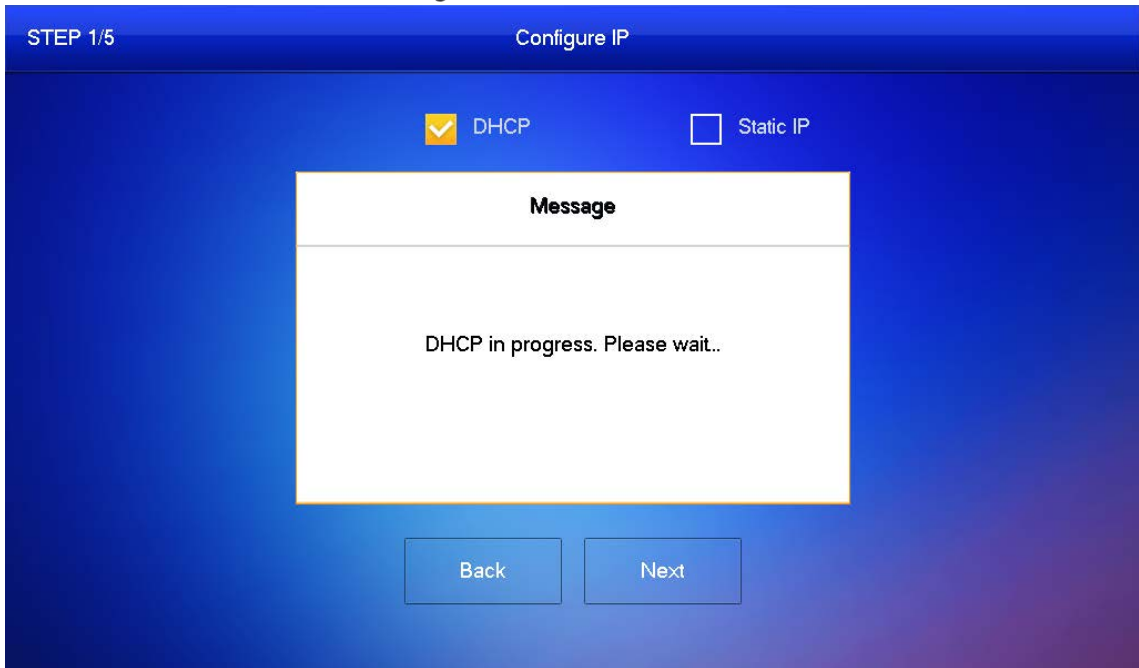
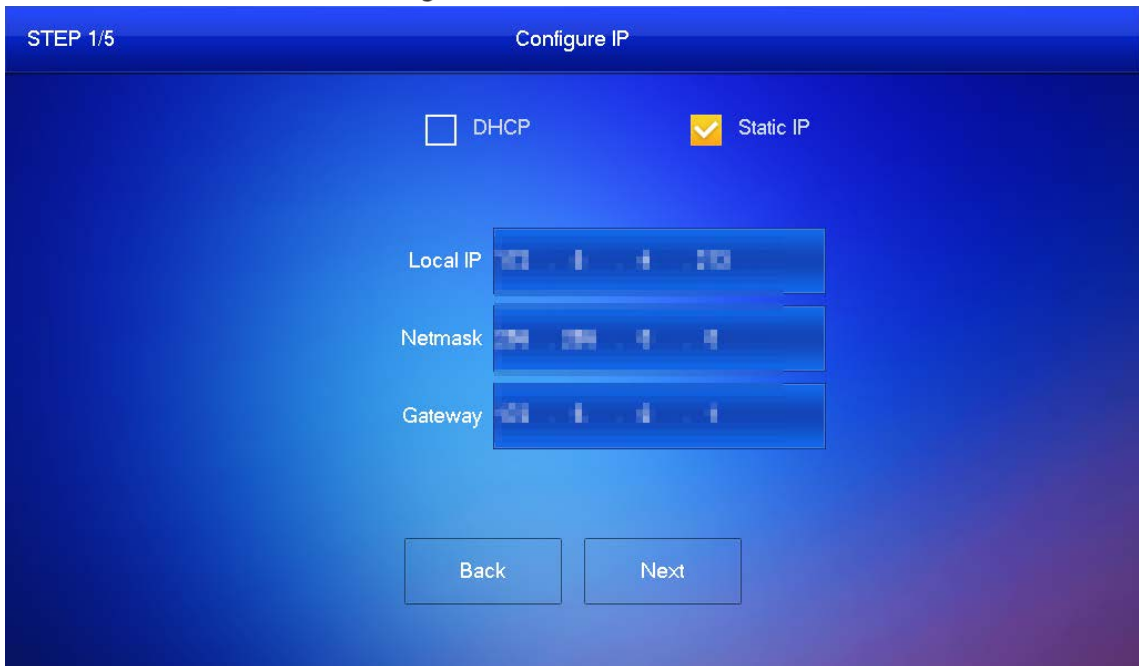


Figure 3-17 Static IP




Step 5 Set a password and an email address for the VTH, and then tap **Next**.




- The password is used to enter project setting.
- If you select **Apartment** in Step 2, initialization is completed with this step.

Figure 3-18 Set a password an email address for the VTH

STEP 2/5 Set VTH Password

Password 
6-digit password.

Confirm PWD 
6-digit password.

Email
This email is used to reset the password.

Back Next


Step 6 Set a password and an email address for the VTO.





The password is used to enter project setting.

Figure 3-19 Set a password an Email address for the VTO

STEP 3/5 Set VTO Password

Password 
8-32 characters password

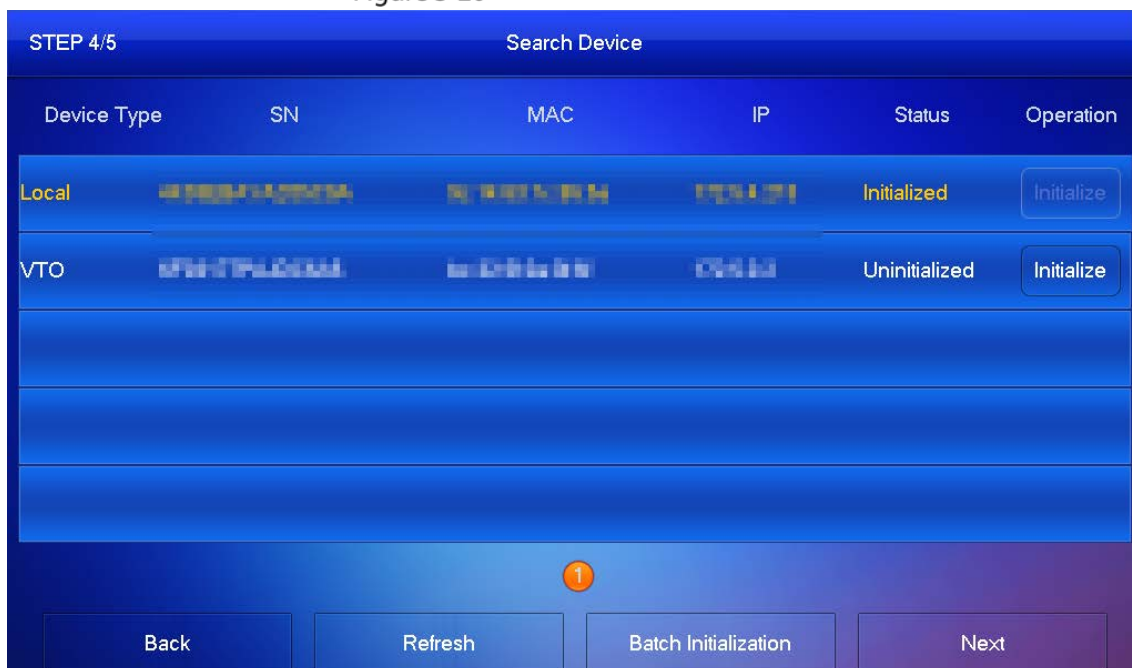
Confirm PWD 
8-32 characters password

Email 
This email is used to reset the password.

Back Next

Step 7 Click **Initialize** to initialize a single device or **Batch Initialization** to initialize all available devices, and then click **Next**.

Figure 3-20 Initialize devices



Step 8 Click **One-key Config** to go to the main interface.

Figure 3-21 Network configuration

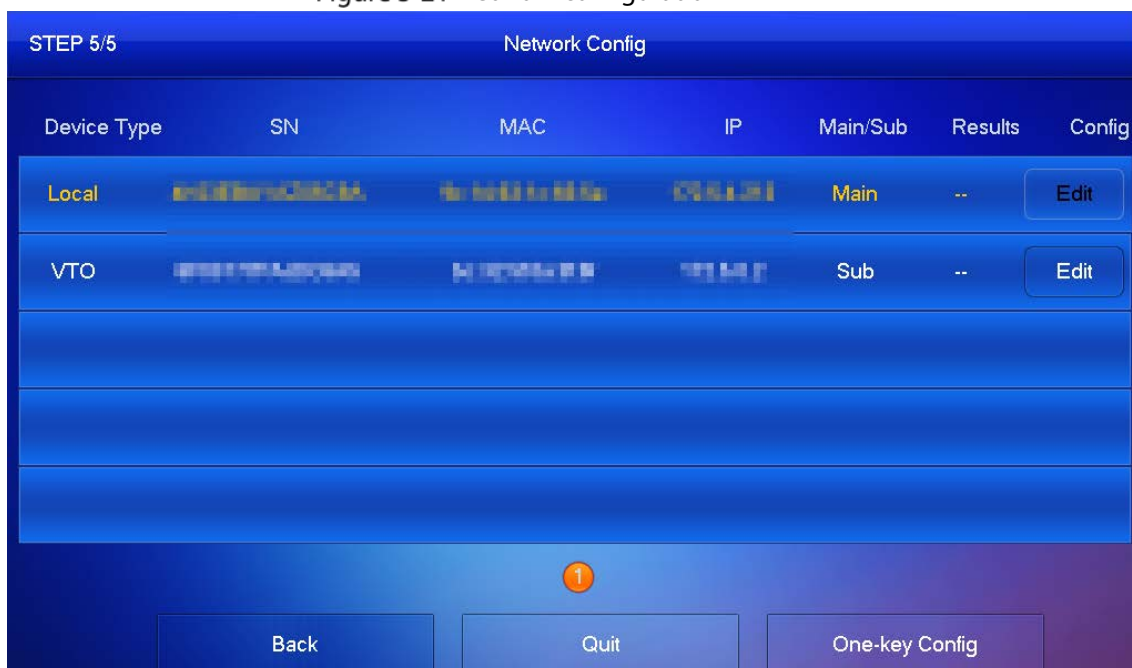
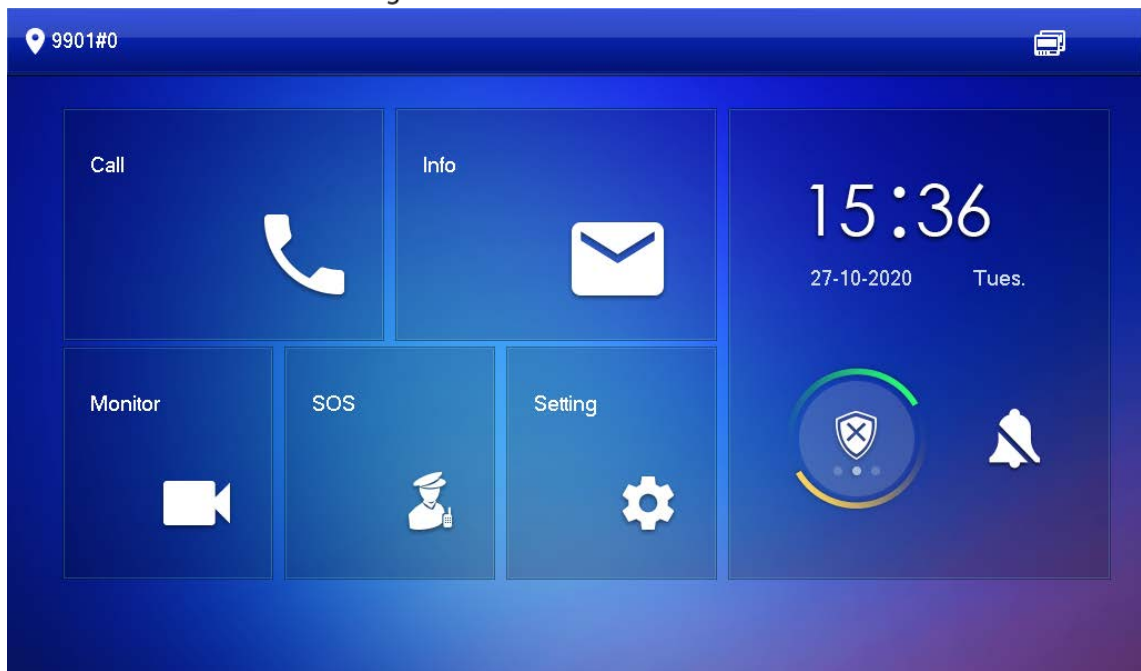


Figure 3-22 Main interface



3.1.2.2 Network Parameters



IP addresses of all VTHs and VTOs must be in the same network segment. Otherwise, the VTH will fail to obtain VTO information.

Step 1 On the main interface, tap **Setting** for more than 6 seconds.

Step 2 Enter the password and tap **OK**.

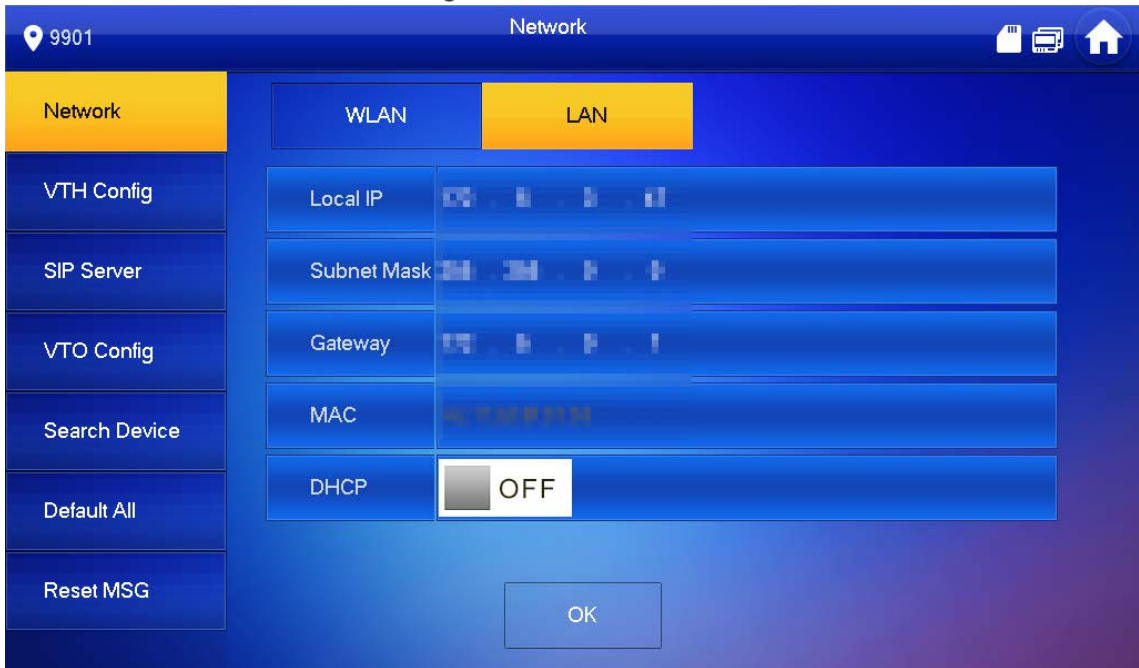
Step 3 Tap **Network**.

Step 4 Configure the parameters.

- LAN

Enter the information, and then tap **OK**; or turn on **DHCP** to obtain the information automatically.

Figure 3-23 LAN



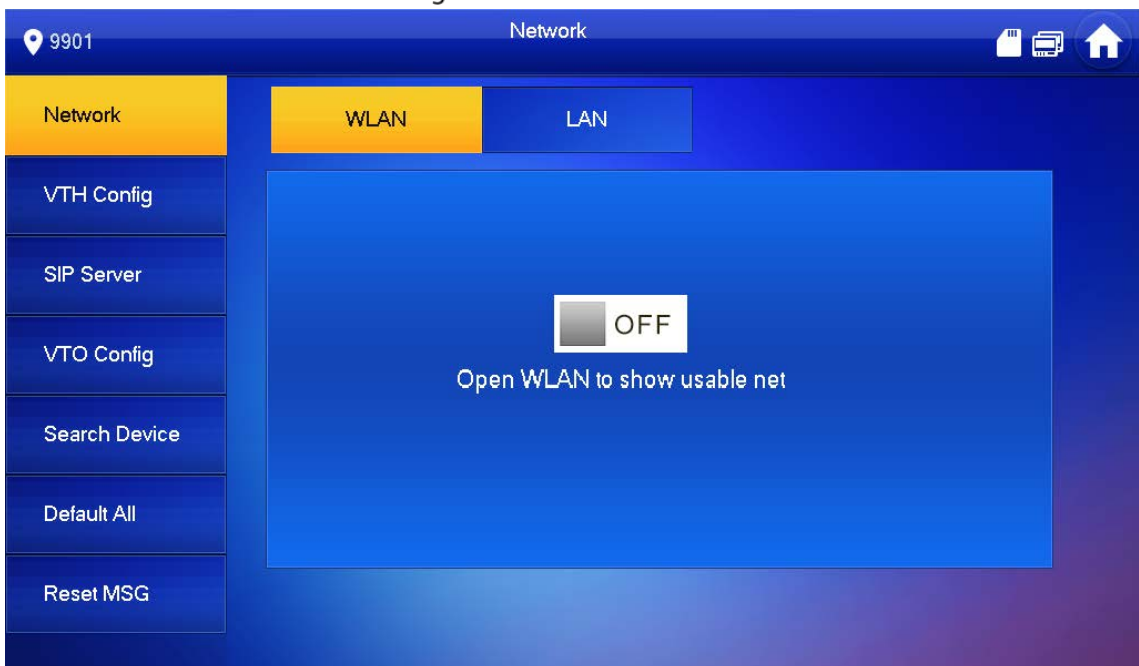
- WLAN



- Only certain models support WLAN function. The actual product shall prevail.
- Use a router with secured encryption protocols.

- 1) Turn on the WLAN function.

Figure 3-24 WLAN



- 2) Connect to a network.

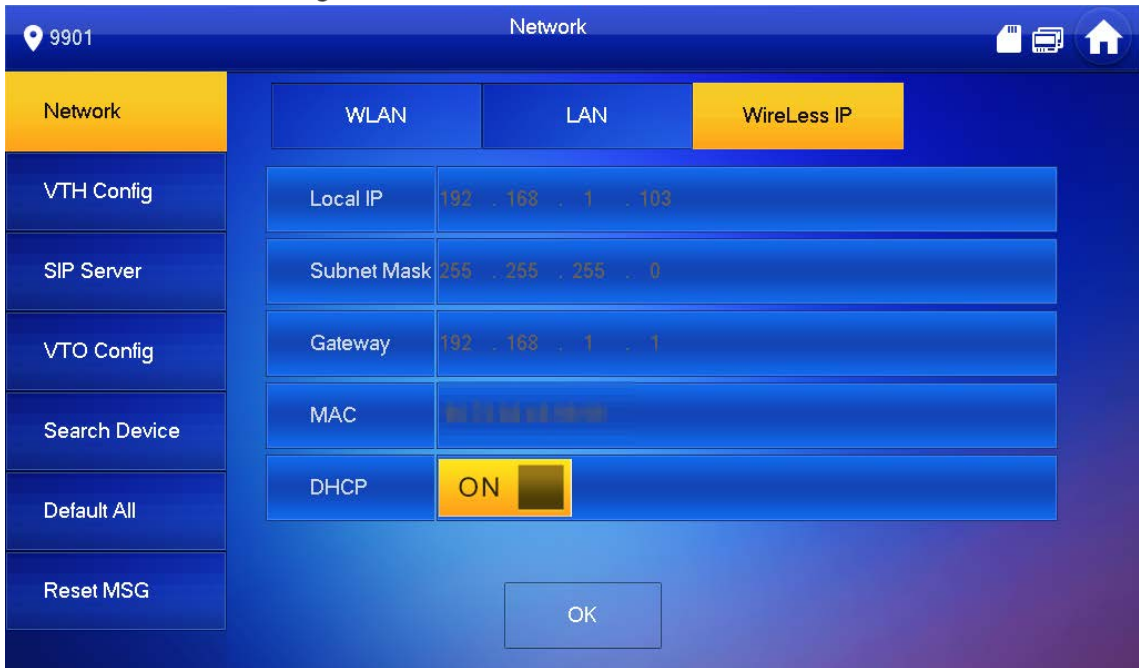
The system has 2 access ways as follows.

- ◇ Tap **Wireless IP** and enter **Local IP**, **Subnet Mask** and **Gateway**, and then tap **OK**.
- ◇ Tap **Wireless IP**, turn on **DHCP** to obtain the information automatically.



To obtain IP information with DHCP function, use a router with DHCP function.

Figure 3-25 Enable the DHCP function



3.1.2.3 VTH Config

- Step 1** On the main interface, tap **Setting** for more than 6 seconds.
- Step 2** Enter password and tap **OK**.
- Step 3** Tap **VTH Config**.

Figure 3-26 VTH configuration



- Step 4** Configure VTH information.
 - As a main VTH.
Enter the room number (such as 9901 or 101#0) and other information, and then tap **OK**.



- Room number must be the same with **VTH Short No.**, which is configured when adding VTHs on the VTO web interface. Otherwise, it will fail to connect to the VTO.
- When there are extension VTHs, room numbers must end with #0. Otherwise, it will fail to connect to the VTO.
- As an extension VTH.
 - 1) Switch **Main** to **Extension**.
 - 2) Enter the room number (such as 101#1), Main VTH IP (IP address of the main VTH) and other information, and then tap **OK**.



Main VTH Username and **Main VTH PWD** are the username and password of main VTH. Default user name is admin, and the password is the one set during initialization.

Step 5 Turn on the following functions as needed.

- **SSH:** The debugging terminal will connect to the VTH remotely through SSH protocol.
- **Security Mode:** Log in to the VTO in a secured way.
- **Password Protection:** Encrypt the password before sending out.



It is recommended to turn off SSH, and turn on security mode and password protection. Otherwise, the device might be exposed to security risks and data leakage.

Step 6 Tap **OK**.

3.1.2.4 SIP Server

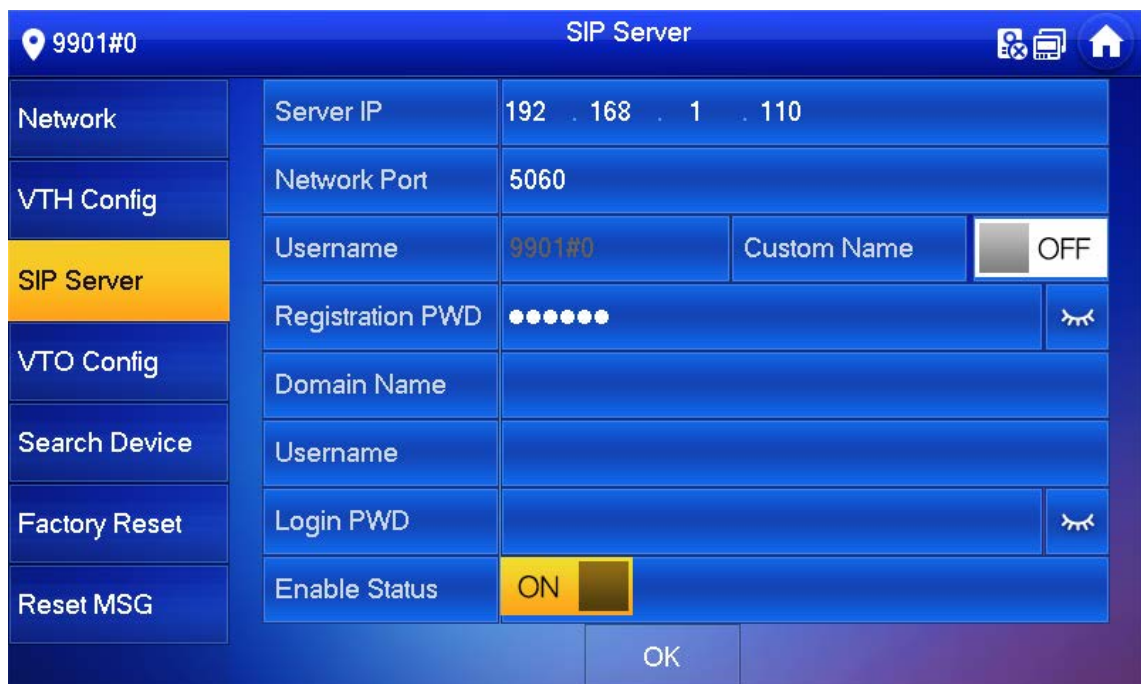
Configure SIP server information to connect to other devices.

Step 1 On the main interface, tap **Setting** for more than 6 seconds.

Step 2 Enter the password and tap **OK**.

Step 3 Tap **SIP Server**.

Figure 3-27 SIP server



Step 4 Configure the parameters.

Table 3-5 SIP server parameters

Parameter	Description
Server IP	<ul style="list-style-type: none"> When a platform works as the SIP server, it is the IP address of the platform. When a VTO works as the SIP server, it is the IP address of the VTO.
Network Port	<ul style="list-style-type: none"> 5080 when a platform works as the SIP server. 5060 when a VTO works as the SIP server.
Username	Keep it default, or turn on Custom Name , and then you can edit the username.
Registration PWD	Keep it default.
Domain Name	When a VTO works as the SIP server, it must be VDP; otherwise, it can be null.
Username	SIP server login username and password.
Login PWD	

Step 5 Turn on **Enable Status** to enable the SIP server function.

Step 6 Tap **OK**.

3.1.2.5 VTO Configuration

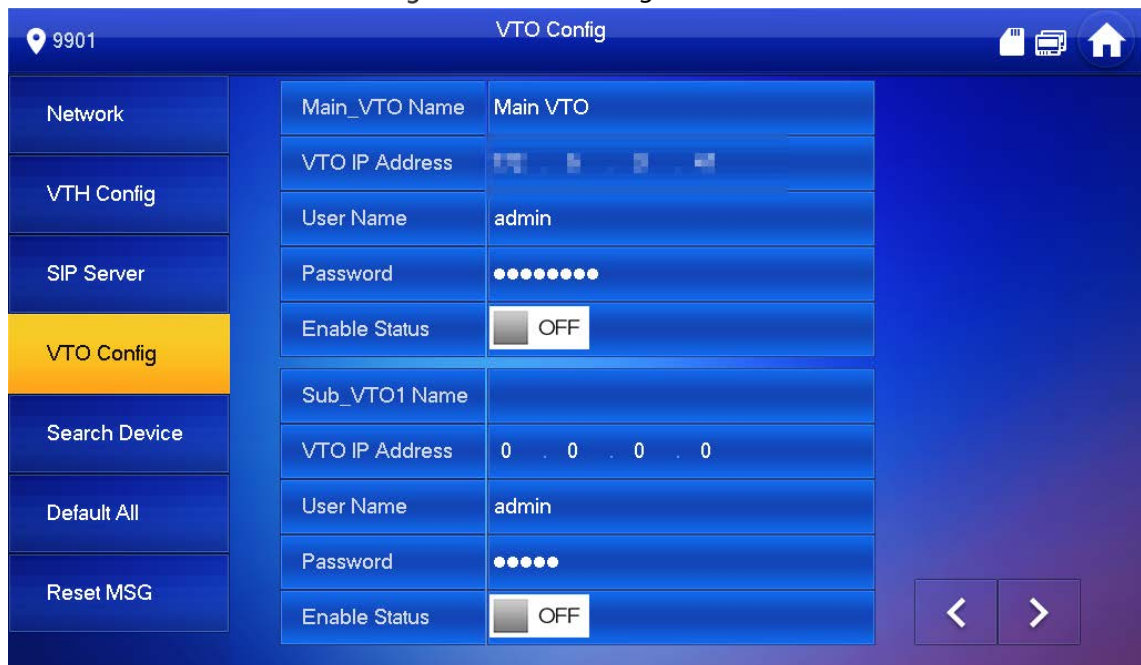
Add VTOs and fence stations to bind them with the VTH.

Step 1 On the main interface, tap **Setting** for more than 6 seconds.

Step 2 Enter the password set during initialization, and tap **OK**.

Step 3 Tap **VTO Config**.

Figure 3-28 VTO config



Step 4 Add VTO or fence station.



- Add main VTO.
 - 1) Enter the main VTO name, VTO IP address, username and password.
 - 2) Turn on **Enable Status**.



User Name and **Password** must be consistent with the web interface login username and password of the VTO.

- Add sub VTO or fence station.
 - 1) Enter the sub VTO or fence Station name, IP address, username and password.
 - 2) Turn on **Enable Status**.



Tap   to turn page and add more sub VTO or fence stations.

3.1.2.6 Searching Device

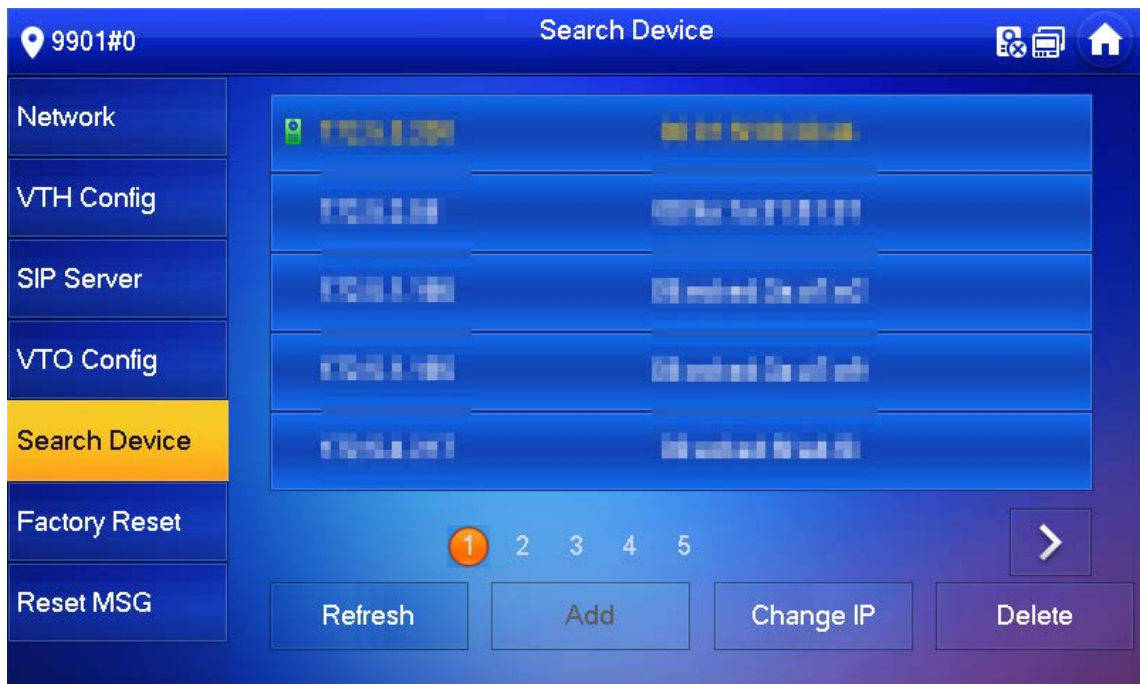
You can search for VTOs in the same network, and then add them or change their information.

Step 1 Tap **Search Device**.



If you select **Villa** in Figure 3-14, it will be **Add Device** with the similar function.

Figure 3-29 Search device



Step 2 Tap a device.



You can only add or edit villa VTOs.

- Click **Add**.

Figure 3-30 Add a VTO

Add VTO

Name: Main VTO

Channel: Vto00

Mid No.:

IP: 192.168.1.100

Port: 5000

State: Off

Searched IP: 192.168.1.100

Username: admin

Password: ●●●●●

OK

- Click **Change IP** to change the information of the VTO, including IP, netmask, and gateway.



Username and password cannot be changed here. They are the same as the ones used to log in to the web interface of the VTO, and are used to log in to the VTO.

Figure 3-31 Change the information of the VTO device

Modify VTO IP

Main VTH IF: 192.168.1.100

Netmask: 255.255.255.0

Gateway: 192.168.1.1

MAC: 08:00:27:00:00:00

Username: admin

Password: ●●●●●

OK Cancel

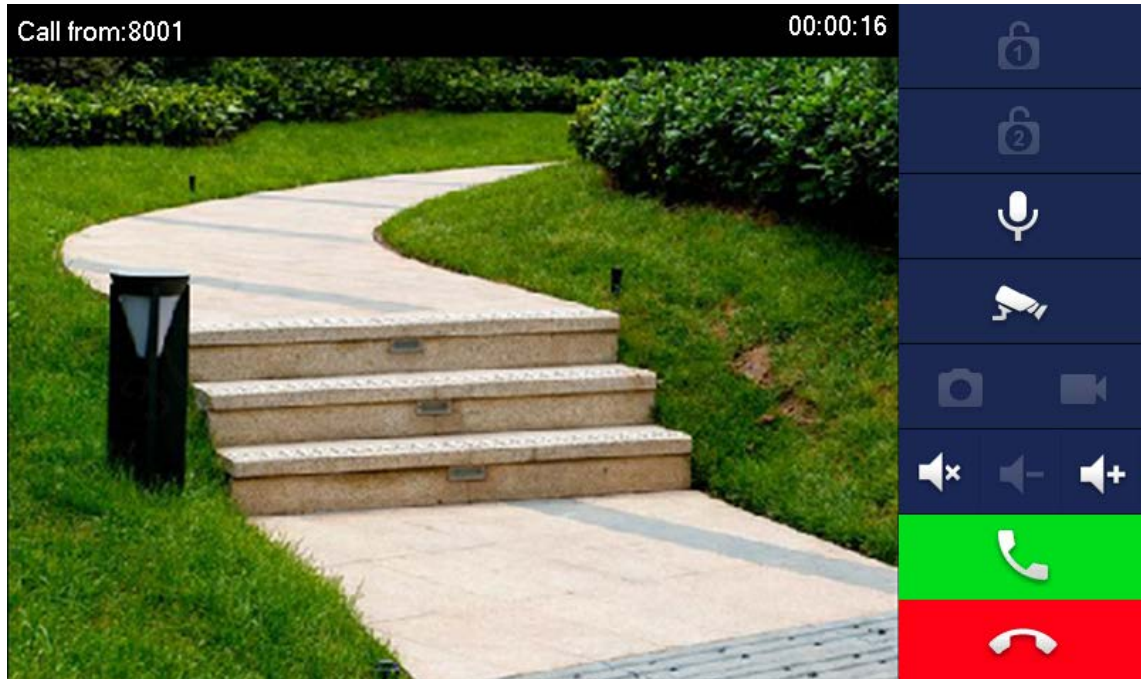
Delete

3.2 Commissioning

3.2.1 VTO Calling VTH

Dial the VTH room number (such as 101) on the VTO and the following image appears, which means all parameters are correctly configured.

Figure 3-32 Calling interface



3.2.2 VTH Monitoring VTO

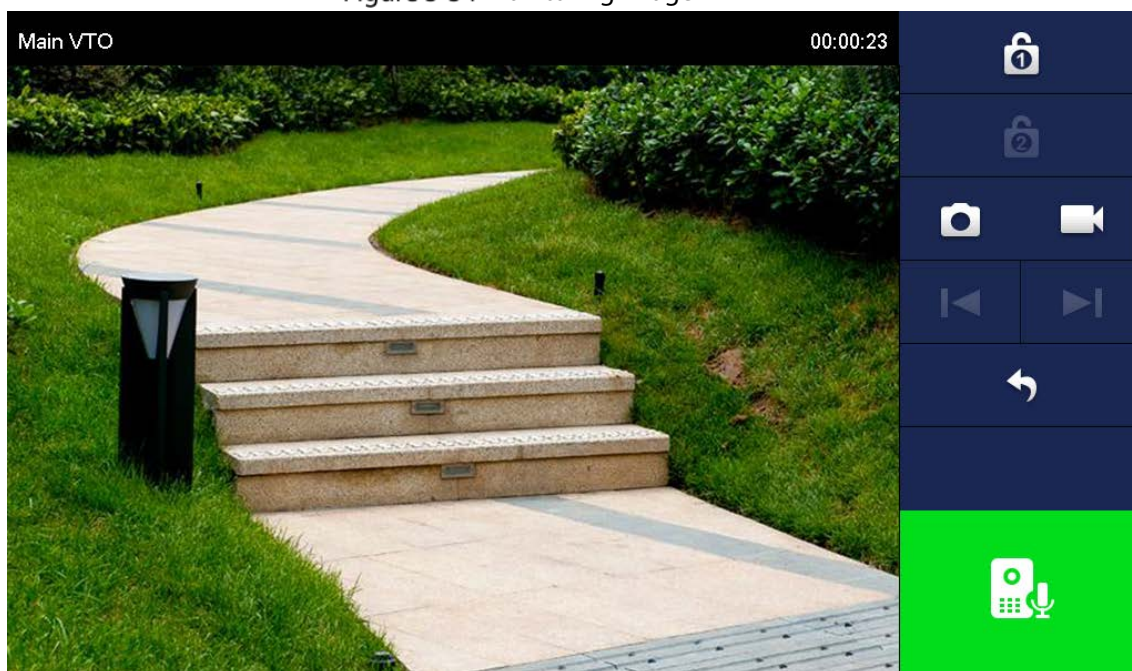
VTH can monitor VTO, fence station or IPC. This section takes monitoring VTO as an example.

On the main interface of the VTH, tap **Monitor** > **Door**, and then tap a VTO to enter monitoring image.

Figure 3-33 Door



Figure 3-34 Monitoring image



SD card is needed for recording and snapshot; otherwise, the icons will be gray.

4 Interface Operation

4.1 Main Interface

Figure 4-1 Main interface

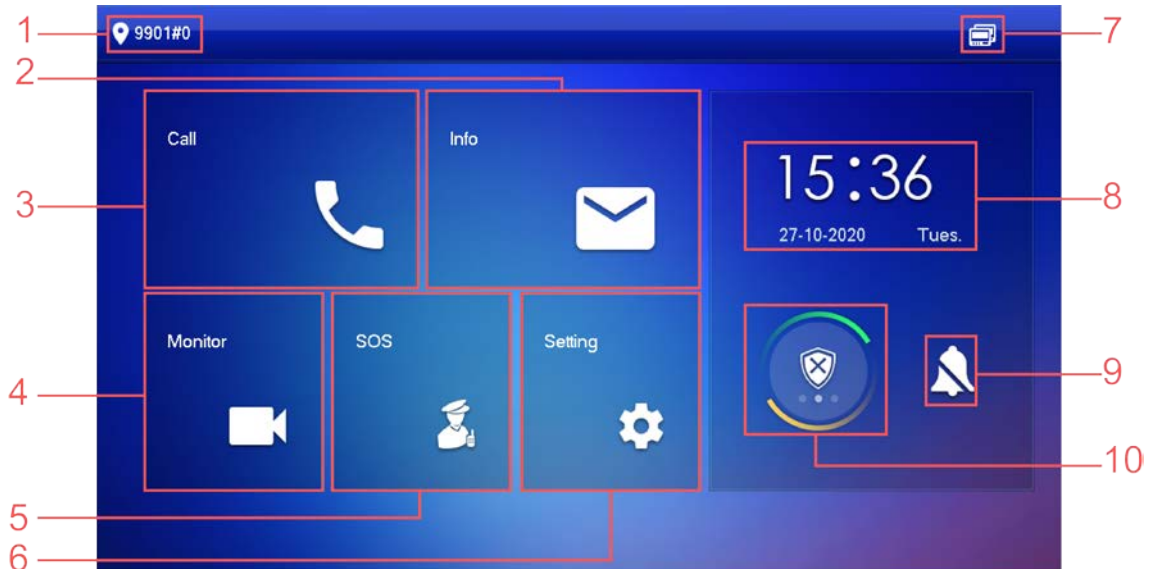








Table 4-1 Main interface description

No.	Name	Description
1	Room number	Number of the room where the VTH is located.
2	Info	<ul style="list-style-type: none"> View, delete and clear announcements or security alarm information. When the VTH does not have an SD card, and the video-audio message uploading function is enabled on the VTO, three tabs will be displayed, Guest Msg, Guest Snap and Guest Video. You can view, delete and clear the messages. When the VTH has an SD card, the Video Pic tab will be displayed. View, delete and clear the videos and pictures.
3	Call	<ul style="list-style-type: none"> Call other VTOs and VTHs. View and manage the contacts and call records.
4	Monitor	Monitor VTOs, fence stations, IPCs and NVRs.
5	SOS	Make emergency call to the Call Management Center.
6	Setting	<ul style="list-style-type: none"> Tap to enter system setting. Tap for more than 6 seconds, input the password set during initialization, and then enter project setting.
7	Status	<ul style="list-style-type: none"> : Not connected to the network. : Connected to the network through a cable. : Wirelessly connected to the network.

No.	Name	Description
		<ul style="list-style-type: none">  Failed to connect to the main VTO; when disappeared, the device has connected to the main VTO.  An SD card has been inserted into the device; when disappeared, the device does not have an SD card or support SD card.  DND function has been enabled. It is not enabled by default.
8	Time and date	—
9	Do not disturb	Enable to not receive any call or message.
10	Arm/disarm	<ul style="list-style-type: none"> Display unread alarm information. Tap to select an arm mode.

4.2 Call

Manage contact, call and view call records.

4.2.1 Recent Call

Tap **Call** > **Recent Call** to view and manage call records.



For missed call, press the call button on the device front panel to enter the recent call interface.

Figure 4-2 Recent calls



- **Call back:** Tap a call record to call back.
- **Delete:** Tap **Edit**, and then tap **Delete** to delete a record.

- **Clear:** Clear all record in the current tab (**All** or **Missed Call**).

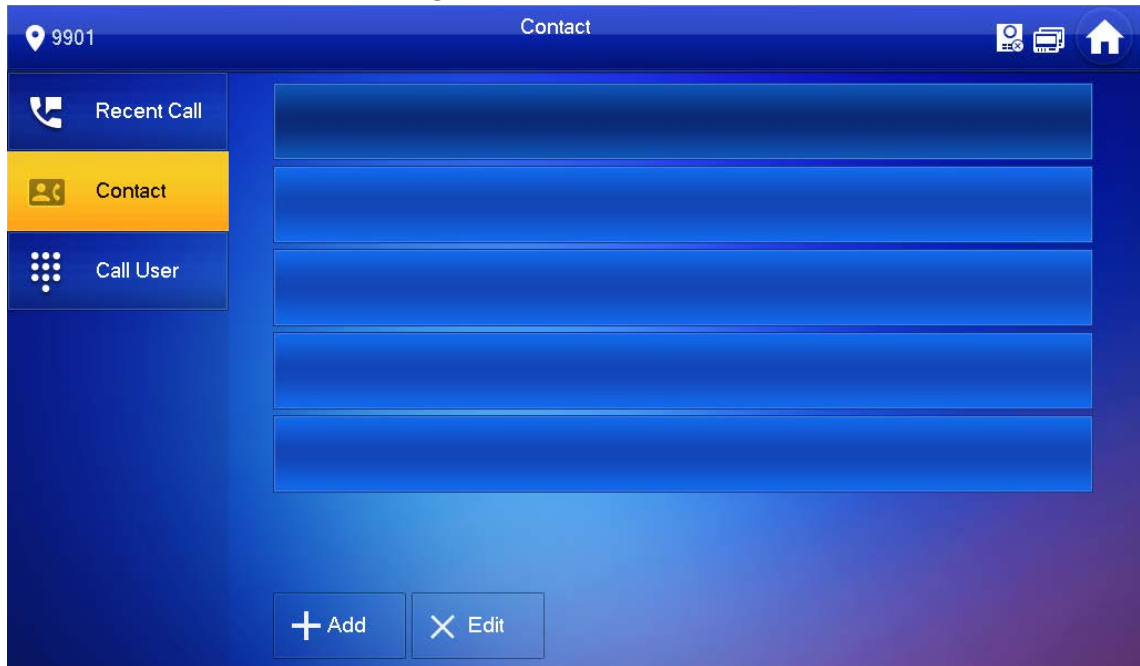


If storage is full, the oldest records will be overwritten. Back up the records as needed.

4.2.2 Contact

Tap **Call** > **Contact**, and then add or edit the users.

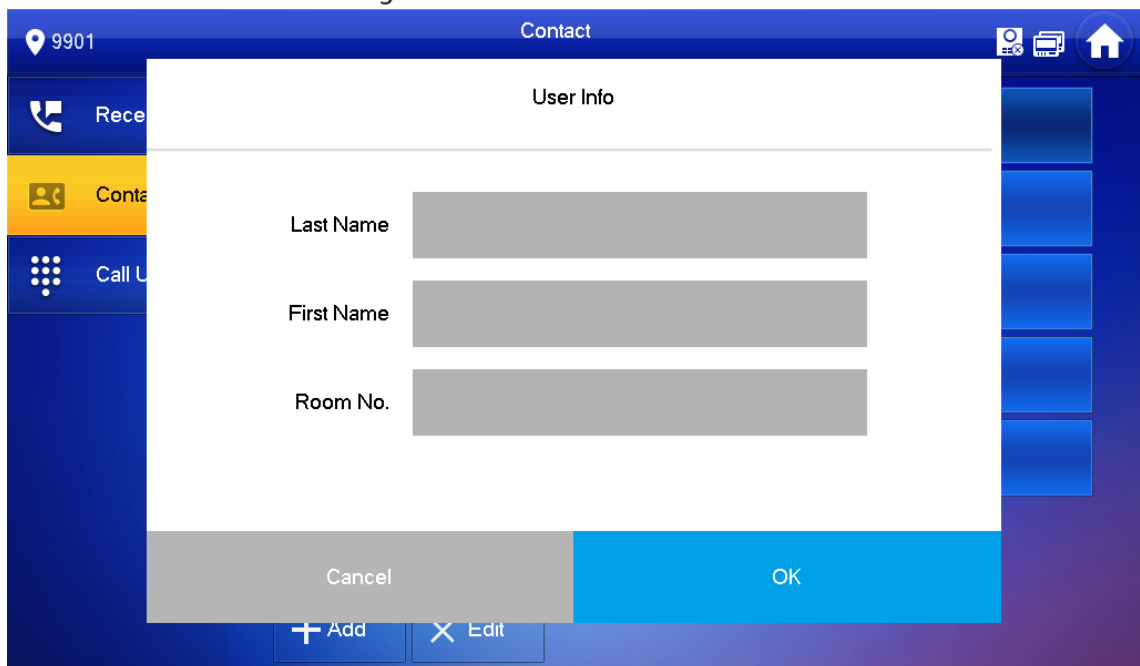
Figure 4-3 Contact



- Add a user.

Step 1 Tap **Add**.

Figure 4-4 User information



Step 2 Enter the information.

Step 3 Tap **OK**.

Related Operations

- Edit user information: Tap a user and tap **Edit**.
- Delete a user: Tap **Edit**, select a user, and then tap **Delete**.



You can select multiple contacts at the same time.

4.2.3 Call User



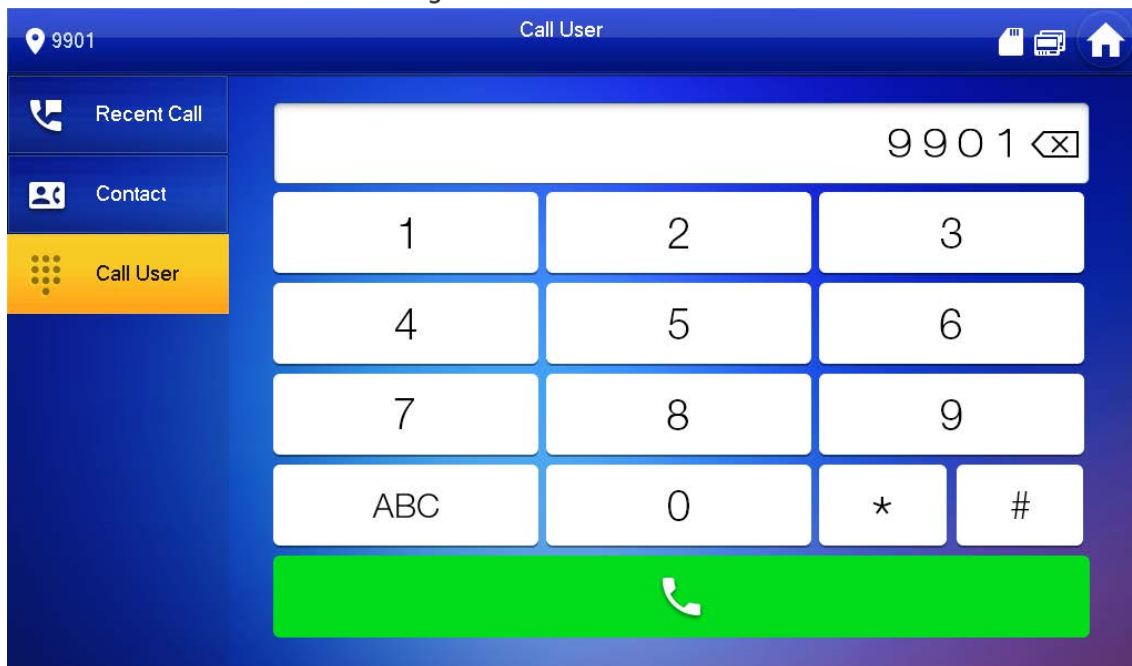
- Make sure that resident-to-resident call function has been enabled. See "4.6.6.4 QR Code" for details.
- Call function is used by VTH to call VTH.
- If both VTHs have a camera, bilateral video call can be provided.

4.2.3.1 By Room Number

On the **Call User** interface, dial and call the user.

Step 1 Select **Call > Call User**.

Figure 4-5 Call user



Step 2 Enter the room number (VTH room number).

- If VTO works as SIP server, dial room no. directly.
- If the platform works as SIP server:
 - ◇ Call a user in the same unit and the same building, dial room number directly.
 - ◇ Call a user in other buildings or units, add the building number. For example, dial 1#1#101 to call Building 1 Unit 1 Room 101.



If main VTH (101#0) calls extension (101#1), please enter room no.: #1; if the extension calls main VTH, please enter room no.: #0.

Step 3 Tap .



If the VTH has a camera, there will be videos after answering the call.

Figure 4-6 Calling

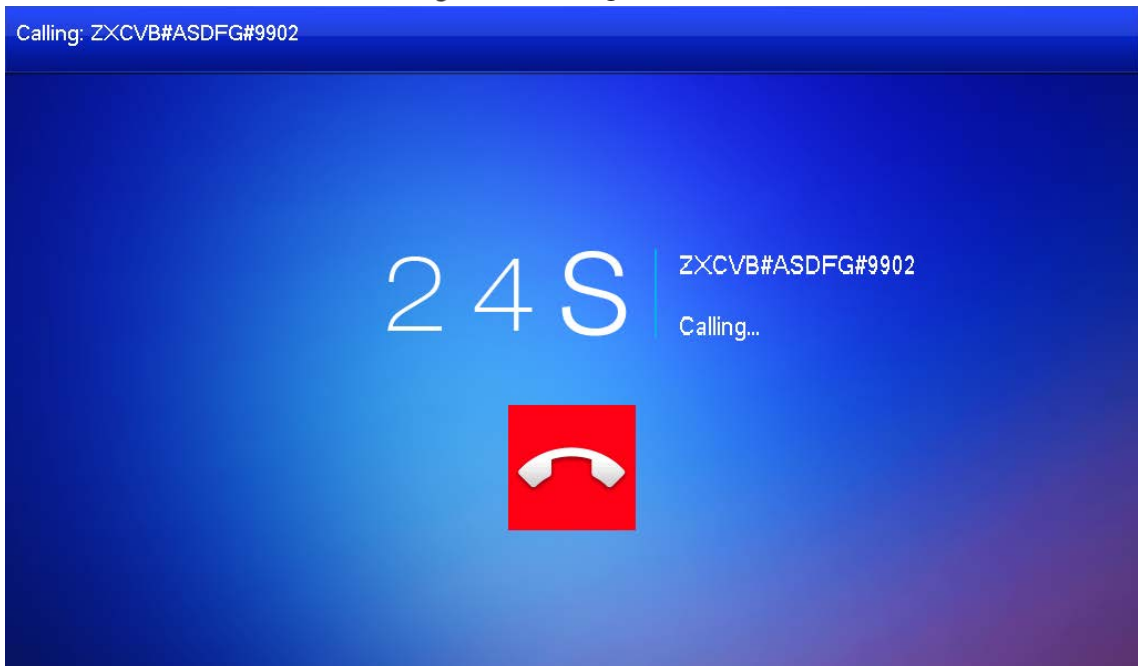
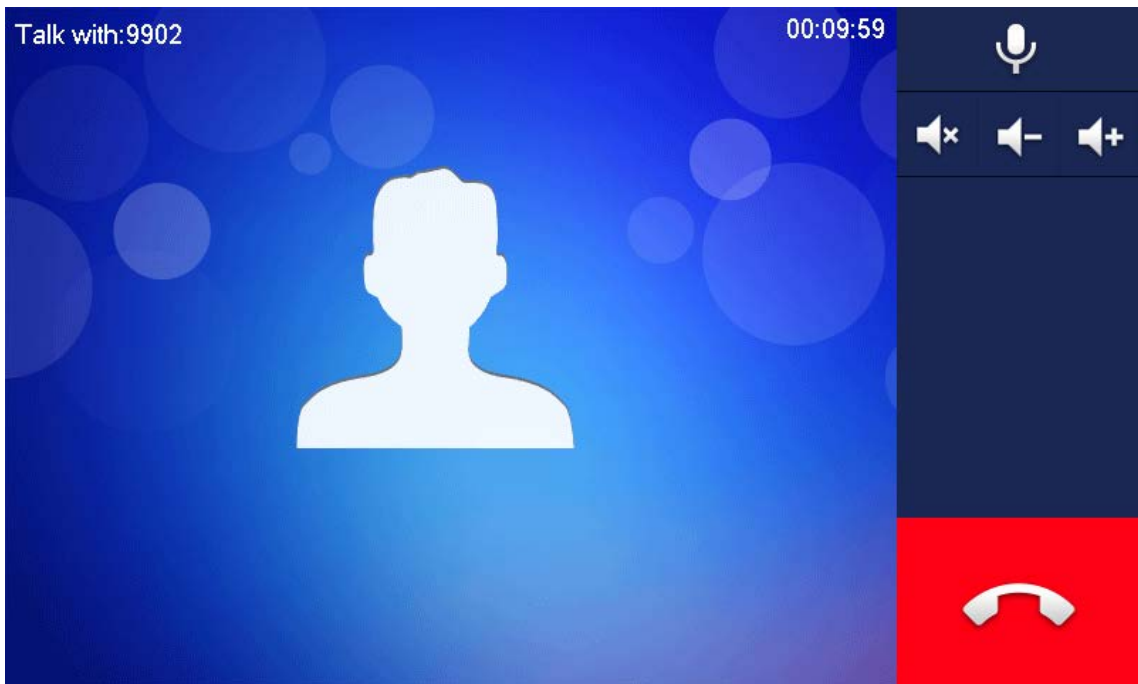


Figure 4-7 Call in progress



4.2.3.2 From Contact



Add contacts first. See 4.2.2 Contact.

Step 1 Select **Call > Contact**.

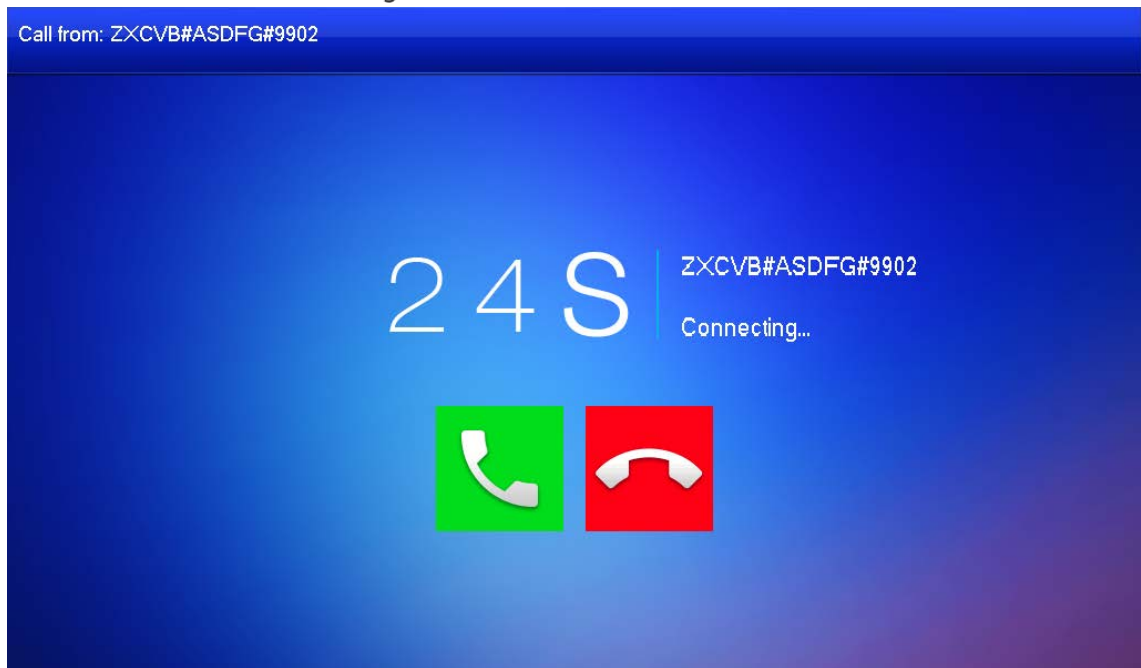
Step 2 Select the one you want to call.

Step 3 Tap  to start.

4.2.4 Call from User

When receiving calls from other VTHs, the following interface will be displayed.

Figure 4-8 Call interface (1)





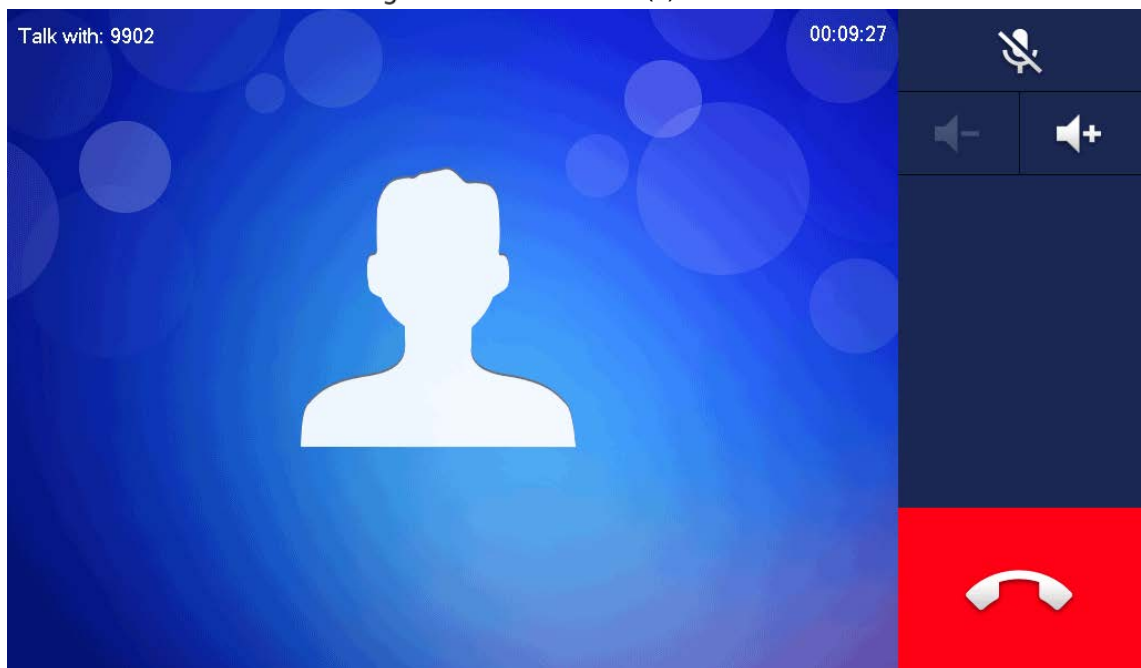
- : Answer.
- : Hang up.

Figure 4-9 Call interface (2)



4.2.5 Call from VTO

Step 1 Dial VTH room no. (such as 9901) at VTO, to call VTH.

Step 2 On the VTH interface, tap **Answer**.

Figure 4-10 Call from VTO

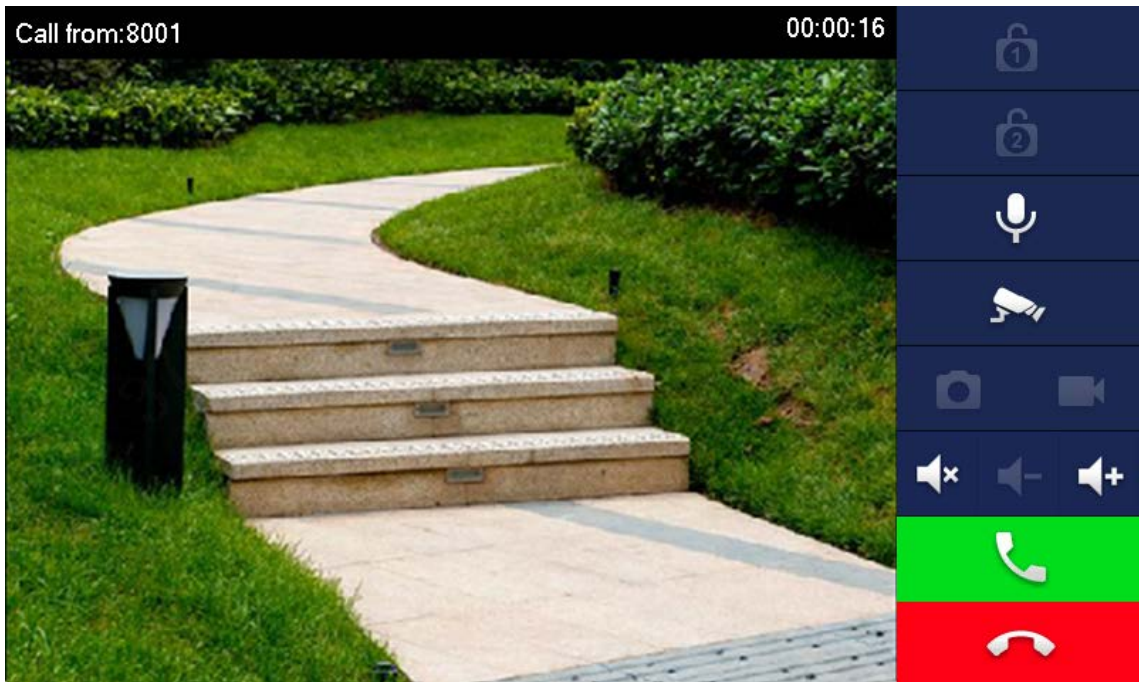






Table 4-2 Interface description

Key	Description
	Remotely unlock the door where the VTO is installed. The system provides 2-channel unlock. If the icon is gray, it means that the unlock function of this channel is not available.
	Tap to talk to the VTO.
	Select an IPC in Favorite to monitor.
	Take snapshot. This key will be gray if SD card is not inserted.
	Take recording. Complete recording when the call is completed or by tapping <ul style="list-style-type: none"> This key is gray if SD card is not installed. Videos are stored in SD card of this VTH. If SD card is full, the earlier videos will be covered.
	Mute.

Key	Description
	Reduce volume.
	Increase volume.
	Answer calls.
	Hang up.

4.3 Info

You can view and manage different kinds of information.

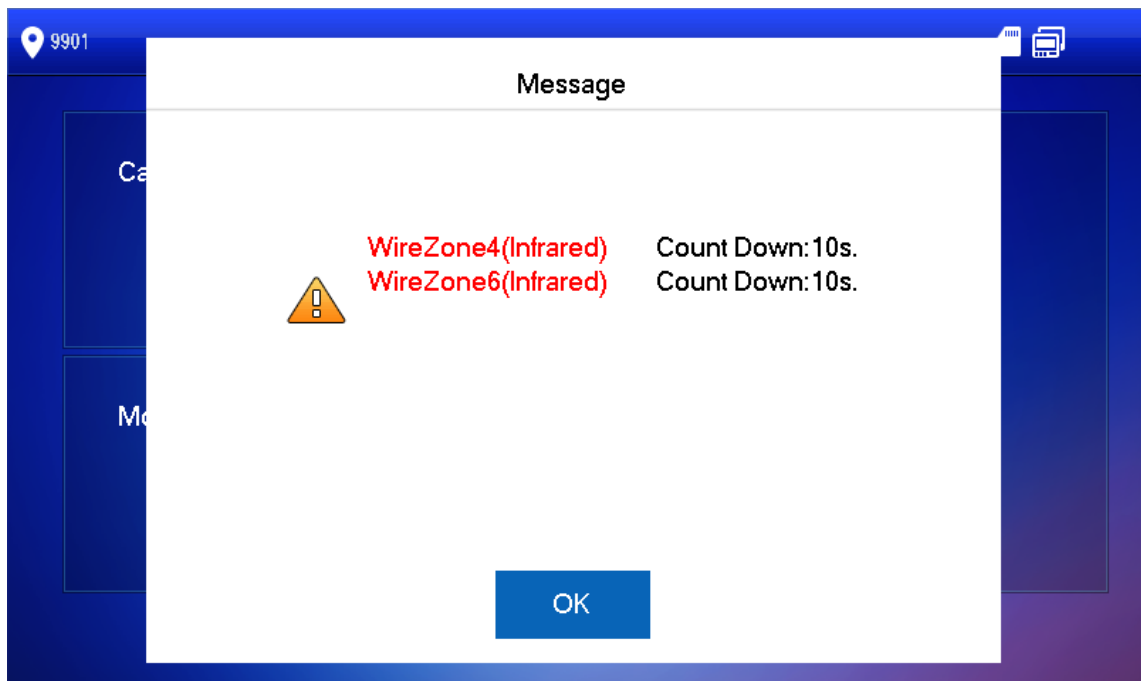


- Information in **Security Alarm** and **Publish Info** is stored in the device, and the one in **Guest Message** and **Video Pictures** is stored in the SD card, which means you need an SD card for these two functions.
- Only certain models support SD card.
- If the storage in the Device or SD card is full, the oldest records will be overwritten. Back up the records as needed.

4.3.1 Security Alarm

When an alarm is triggered, there will be 15s alarm sound, and the interface below will be displayed. The alarm information will be uploaded to the alarm record interface and management platform.

Figure 4-11 Message



Select **Info > Security Alarm**, and then you can view and manage all alarm records.

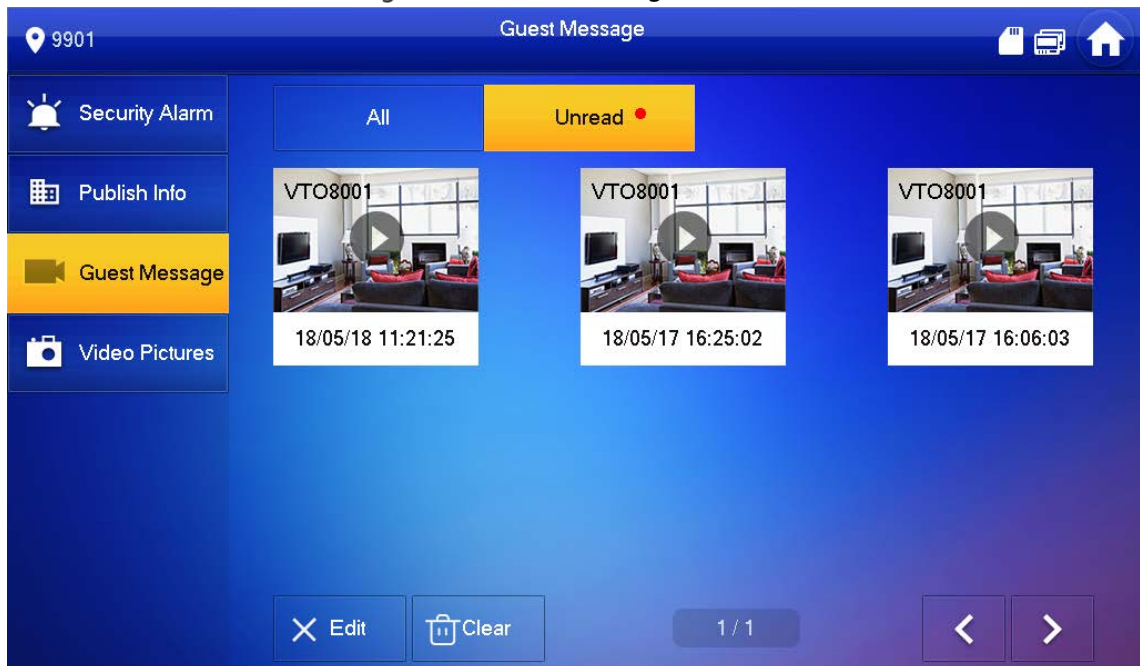
Figure 4-12 Security alarm



4.3.2 Guest Message

Select **Info > Guest Message**, and then you can view and manage all messages.

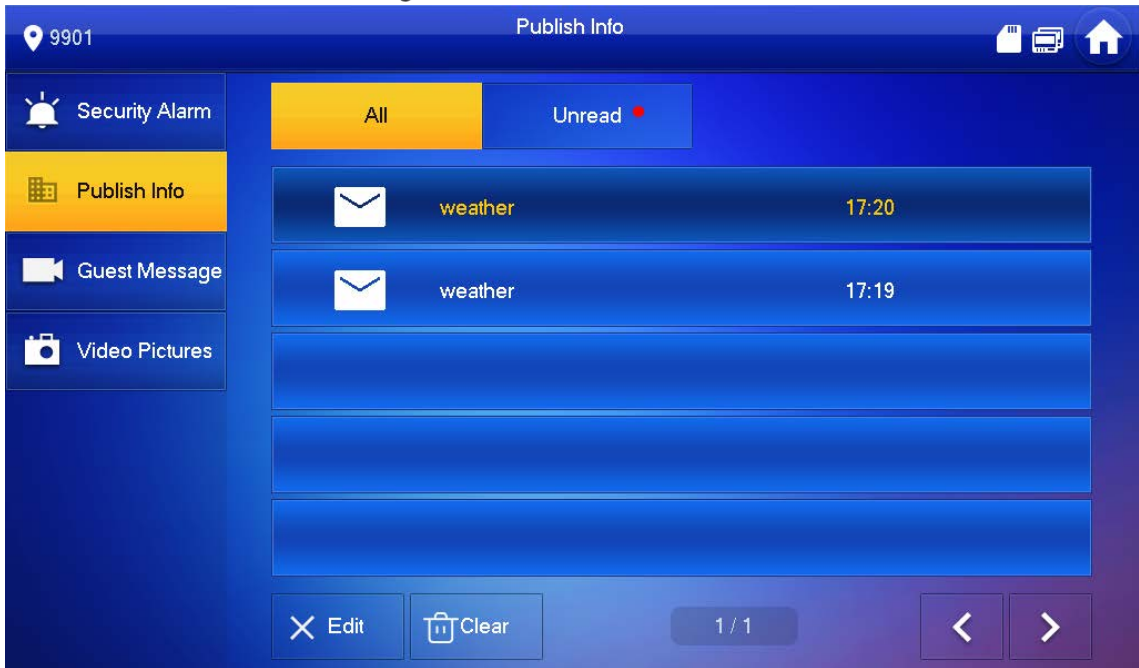
Figure 4-13 Guest message



4.3.3 Publish Info

Select **Info > Publish Info**, and then you can view and manage all messages.

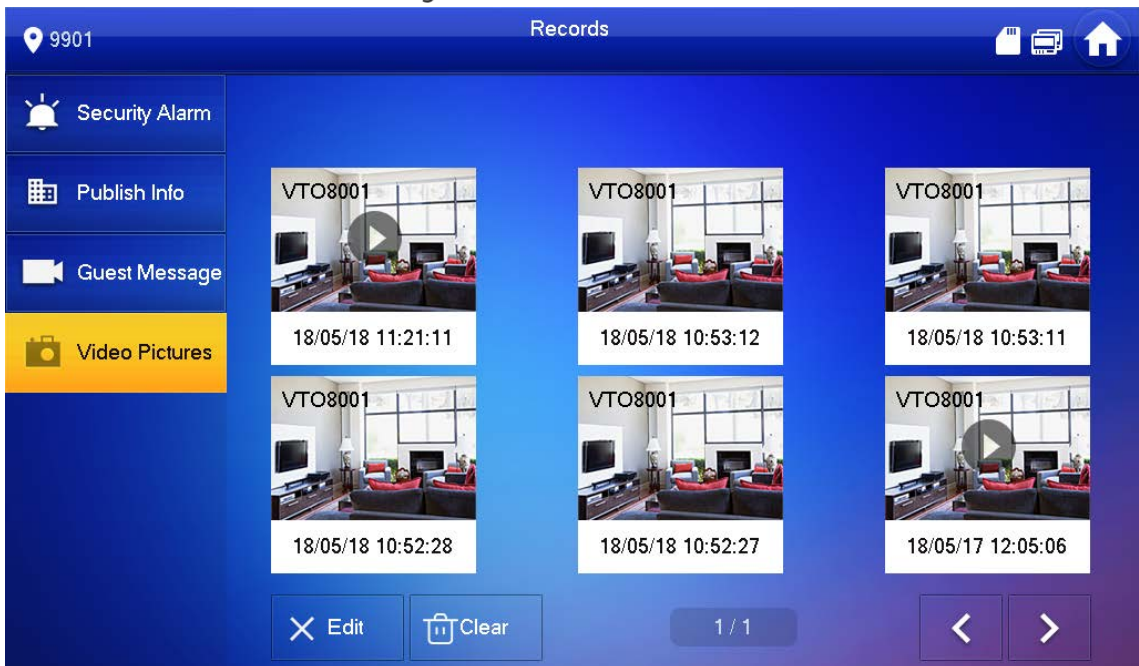
Figure 4-14 Publish info



4.3.4 Video Pictures

Select **Info > Video Pictures**, and then you can view and manage the pictures and videos.

Figure 4-15 Records



4.4 Monitor

You can monitor VTO, fence station or IPC on the VTH.

4.4.1 Monitoring VTO



When adding VTOs, make sure that the username and password of each device is consistent with the web login username and password. See 3.1.2.5 VTO Configuration for details. Otherwise, monitoring will not work properly.

When monitoring, press the call button on the device front panel of the to talk to the VTO.

Step 1 Tap **Monitor > VTO**.

Figure 4-16 Door

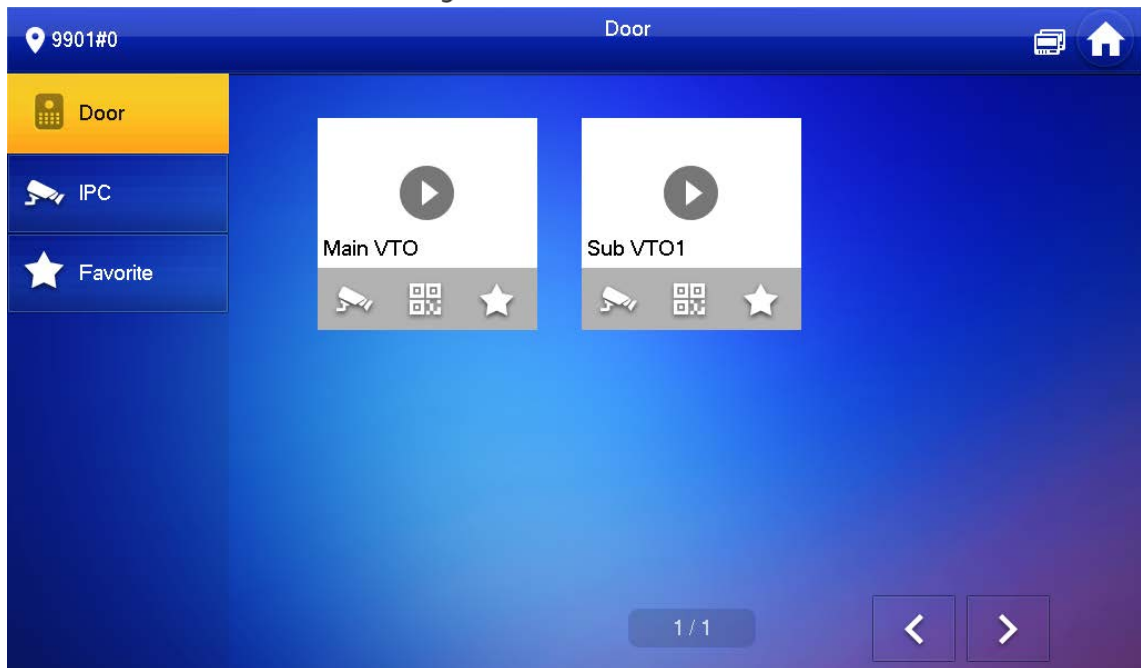


Table 4-3 Function description

Icon	Description
	Add the VTO or fence station to Favorite.
	Select an IPC, and when this VTO or fence station calls, you will see the monitoring image from this IPC. Add an IPC first. See 4.4.2.1 Adding IPC for details.
	Display the serial number of the VTO or fence station in QR code. Scan the QR code in the app to add it to the app, and then you can monitoring the VTO from your smartphone. See 5 DSS Agile VDP for details.

Step 2 Tap .

Figure 4-17 Monitoring VTO

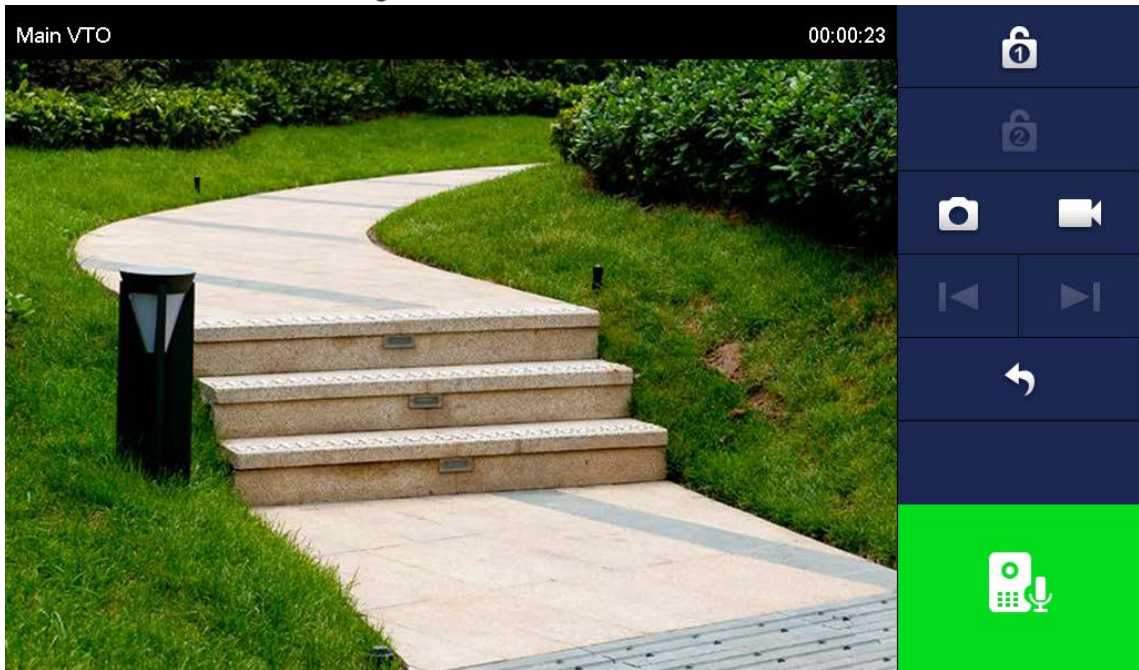














Table 4-4 Interface description

Icon	Description
	Remotely unlock the door where the VTO is located.  The system provides 2-channel unlock function. If the icon is gray, it means that unlock function of this channel is not available.
	Take snapshot.  An SD card is needed to use this function.
	Tap to start recording, and it will stop when the call is completed or by tapping  If the SD card is full, the oldest videos will be overwritten.  An SD card is needed to use this function.
	If the VTH is connected to multiple VTOs/PCs, tap  and  to switch device.
	Exit monitoring.
	Tap to speak to the other end device, and tap again to stop.

4.4.2 Monitoring IPC

4.4.2.1 Adding IPC



- IPCs added to the main VTO and Express/DSS will be synchronized to the VTH. The synchronized IPCs cannot be deleted.
- Before adding an IPC, make sure that it is powered on, and connected to the same network as the VTH.

Step 1 Select **Monitor > IPC**.


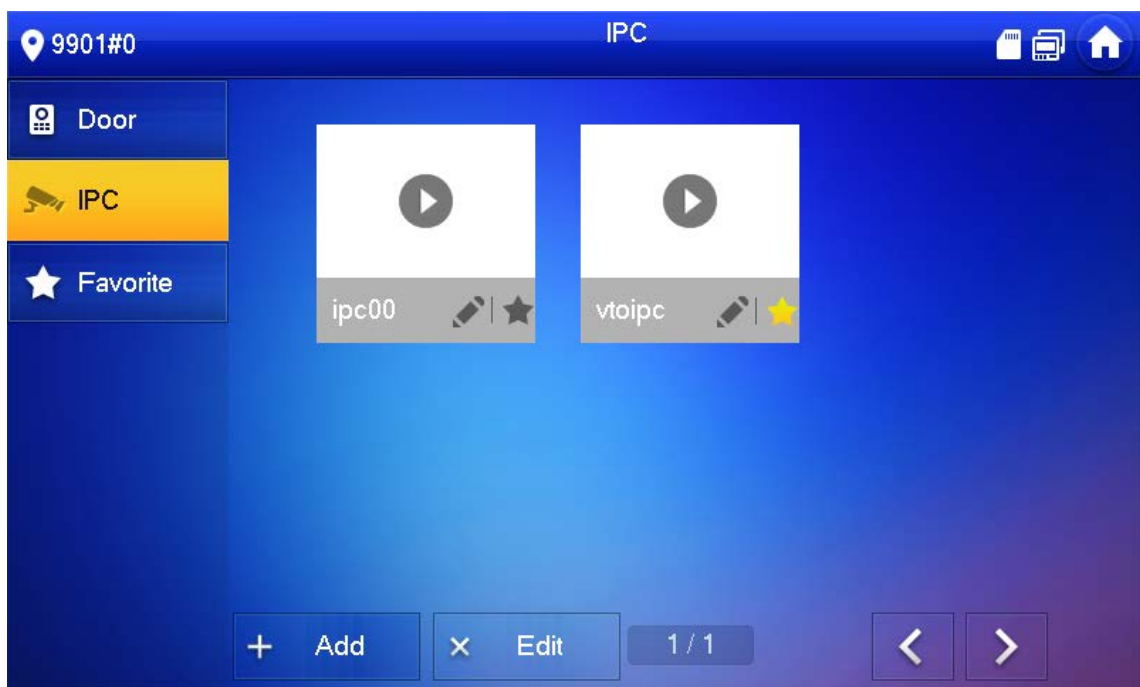
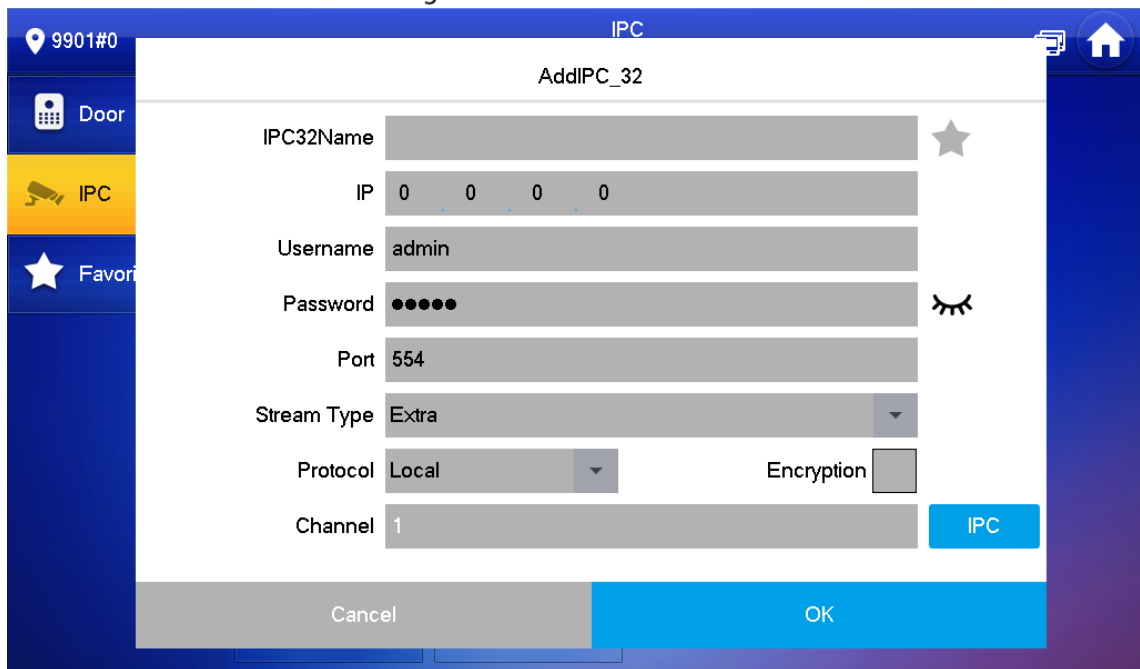
You can tap  to add the IPC to **Favorites**.

Figure 4-18 IPC



Step 2 Tap **Add**.

Figure 4-19 Add IPC



Step 3 Configure the parameters.

Table 4-5 Parameter description

Parameter	Description
IPC	Select IPC or NVR.
IPC32 Name	Name of the IPC/NVR.
IP	IP address of the IPC/NVR.
User Name	Web interface login username and password of the IPC/NVR.
Password	
Port	554 by default.
Stream Type	<ul style="list-style-type: none"> ● Main stream: High definition that needs large amount of bandwidth. Applicable to local storage. ● Extra stream: Relatively smooth image that needs small amount of bandwidth. Applicable to network with insufficient bandwidth.
Protocol	It includes local protocol and Onvif protocol. Please select according to the protocol of the connected device.
Encryption	Enable it if the IPC to be added is encrypted.
Channel	<ul style="list-style-type: none"> ● If IPC is connected, default setting is 1. ● If NVR is connected, set channel number of IPC on NVR.

Step 4 Tap **OK**.

4.4.2.2 Modifying IPC

Step 1 Select **Monitor > IPC**.

Step 2 Tap  of IPC.

Step 3 Modify IPC parameters. Please refer to Table 4-5 for details.

Step 4 Tap **OK**.

4.4.2.3 Deleting IPC

Delete IPC that has been added. However, IPC synchronized from VTO or the platform cannot be deleted.

Step 1 Select **Monitor** > **IPC**.

Step 2 Tap **Edit**.

Step 3 Select **IPC**.

Step 4 Tap **Delete** to delete the selected IPC.

4.4.2.4 Monitoring IPC

Monitor the IPC.

Step 1 Select **Monitor** > **IPC**.


Step 2 Select IPC to be monitored, and tap .

Figure 4-20 Monitoring video



Step 3 Please monitor the VTO by reference to Table 4-4.

4.4.3 Favorite

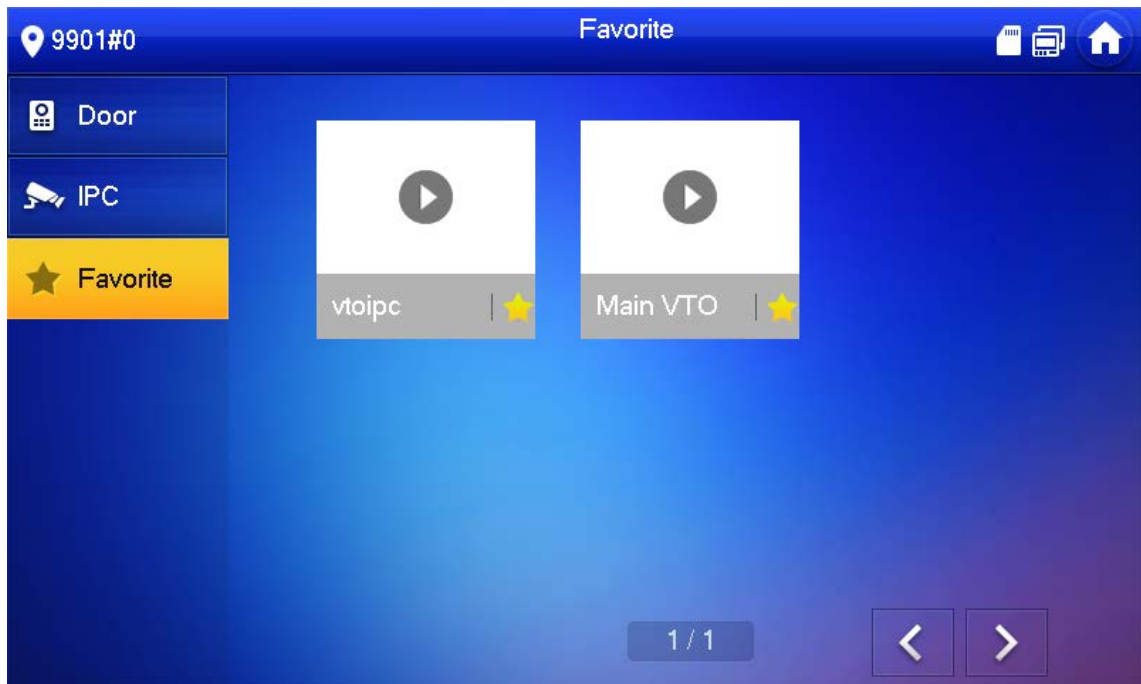
Displays VTO, fence stations or IPC that have been added to favorites.






To view favorite list, please ensure that VTO, fence station or IPC have been added to favorites. Otherwise, the list is empty.

Step 1 Select **Monitor** > **Favorite**.

Figure 4-21 Favorite



- Step 2** Select the device to be monitored, and tap  .
The system displays monitoring interface. In case of multiple devices in Favorite tab, tap  /  to switch and monitor them.

4.5 SOS



Please ensure that management center has been connected. Otherwise, it will fail to call.

In emergency, press the SOS button on the device front panel, or tap **SOS** on the main interface to call management center.

4.6 Setting

4.6.1 Ring Settings

Set VTO ring, VTH ring, alarm ring and other rings.



- There is an SD card on the VTH, and users can import ring tones to the SD card.
- Ring tones must be stored in the /Ring folder at the root directory of the SD card.
- Audio files must be .pcm files (audio files of other formats cannot be played if you change their extension names).

- Audio file size must be less than 100 KB.
- Ring tone format: .pcm.
- You can only customize 10 ring tones. Other ring tones will not be displayed at the VTH.

4.6.1.1 VTO Ring

Set a ring for the connected VTO, and support to set maximum 20 VTOs.

Step 1 Tap **Setting**.

Step 2 Tap **Ring > VTO Ring Setup**.

Tap  or  to page up and down.

Figure 4-22 VTO ring setup



Step 3 Tap text box to select rings, and tap  and  to set the volume.

4.6.1.2 VTH Ring

Set the ring for this VTH.

Step 1 Tap **Setting**.

The system pops up **Password** prompt box.

Step 2 Input login password and tap **OK**.





Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.

Step 3 Select **Ring > VTH Ring Setup**.

Figure 4-23 VTH ring setup



Step 4 Tap text box to select rings, and tap  and  to set the volume.

4.6.1.3 Alarm Ring

Set the ring when the VTH gives an alarm.

Step 1 Tap **Setting**.

Step 2 Enter login password and tap **OK**.





Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.

Step 3 Select **Ring > Alarm Ring Setup**.

Figure 4-24 Alarm ring



Step 4 Tap text box to select rings, and tap  and  to set the volume.

4.6.1.4 Other Ring Settings

Set VTO ring time, VTH ring time, MIC volume, talk volume and ring mute setting.



VTO Ring Time and **VTH Ring Time** of extension VTH are synchronized with main VTH, and cannot be set.

Step 1 Tap **Setting**.

Step 2 Enter login password and tap **OK**.







Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.

Step 3 Select **Ring** > **Other**.

Figure 4-25 Other settings



Step 4 Tap  and  to set the time or volume. Tap  OFF to enable **Ring Mute**, and the icon becomes  ON.



- VTO ring time: ring time when a VTO calls this VTH.
- VTH ring time: ring time when another VTH calls this VTH.

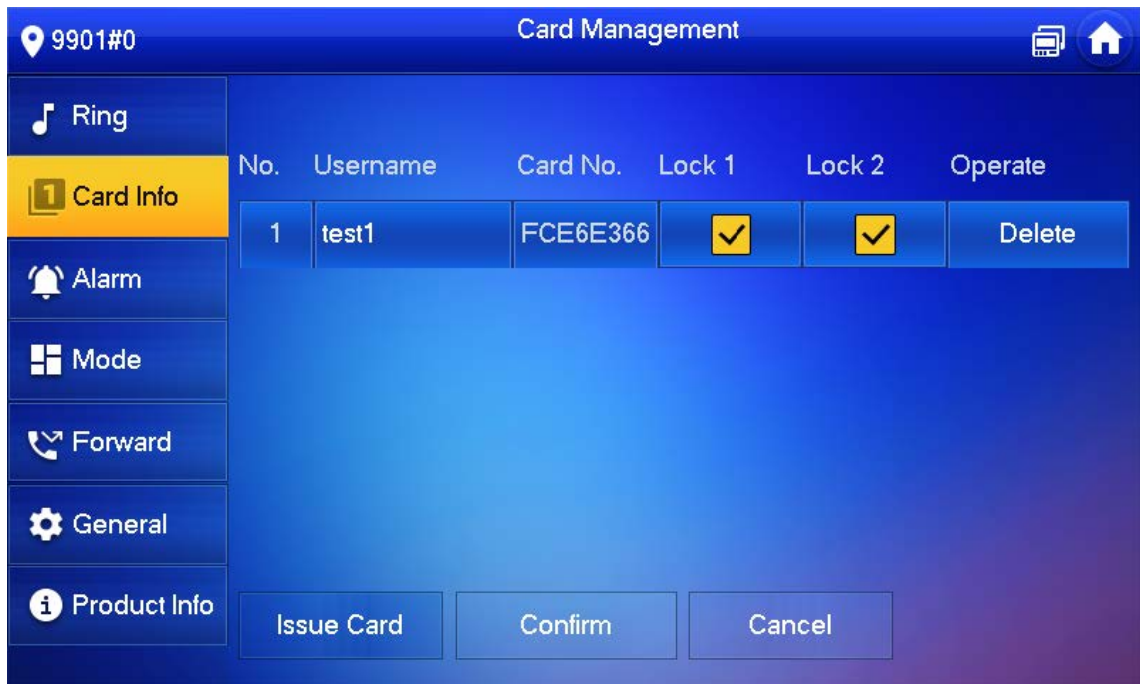
4.6.2 Card Information

Issue and manage card information.



This function is only available under **Villa**.

Figure 4-26 Card management



Step 1 Click **Issue Card**.

Step 2 Swipe the card on the corresponding VTO.

Step 3 The card information will be added to the VTH. Assign unlock permission by selecting **Lock 1** and **Lock 2** as needed.

Step 4 Click **Confirm**.



Click **Delete** to delete the card information.

4.6.3 Alarm Setting

Set wire zone, wireless zone and alarm output.



Zones can be set under disarm mode.

4.6.3.1 Wire Zone

Set zone type, NO/NC, alarm status and delay. It supports to set 8 zones at most.

Step 1 Tap Setting.

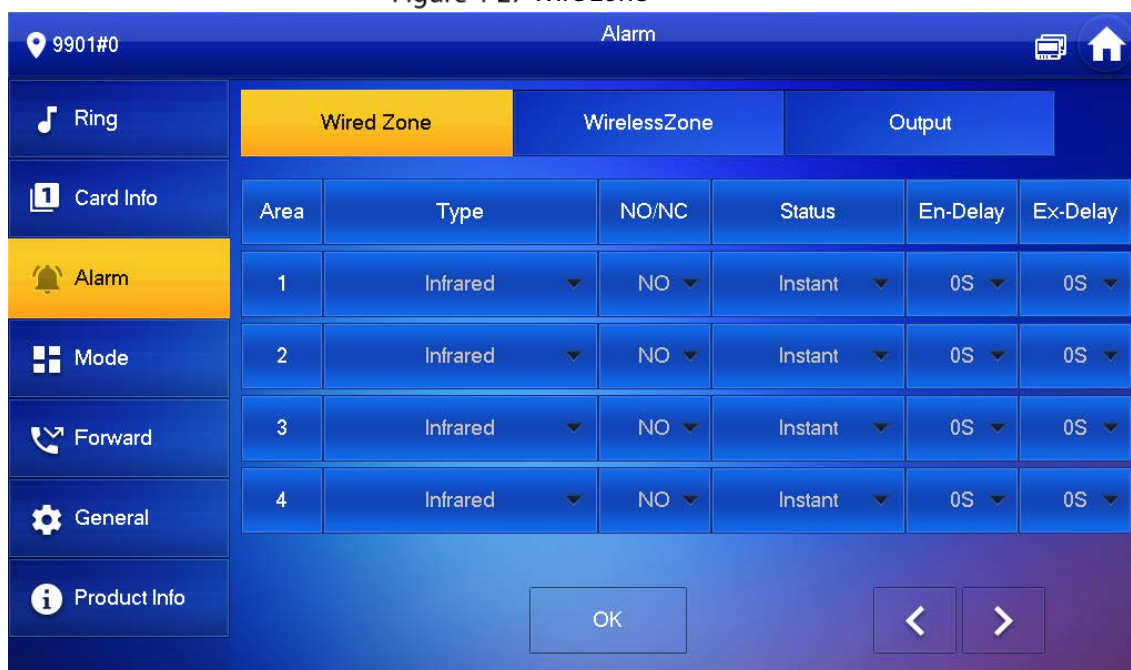
Step 2 Enter login password and tap OK.



Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.

Step 3 Select **Alarm > Wire Zone**.

Figure 4-27 Wire zone



Step 4 Tap corresponding positions to set area type, NO/NC, alarm status, enter delay and exit delay.

Table 4-6 Parameter description

Parameter	Description
Area	The number cannot be modified.
NO/NC	Select NO (normally open) or NC (normally closed) according to detector type. It shall be the same as detector type.
Type	Select corresponding type according to detector type, including IR, gas, smoke, urgency btn, door, burglar alarm, perimeter and doorbell.
Status	<ul style="list-style-type: none"> ● Instant Alarm: After armed, if an alarm is triggered, the device produces siren at once and enters alarm status. ● Delay Alarm: After armed, if an alarm is triggered, the device enters alarm status after a specified time, during which you can disarm and cancel the alarm. ● Bypass: Alarm will not be triggered in the area. After disarmed, this area will restore to normal working status. ● Remove: The area is invalid during arm/disarm. ● 24 Hour: Alarm will be triggered all the time in the area regardless of arm or disarm. <p> A zone in Remove status cannot be bypassed.</p>
Enter Delay	<p>After entering delay, when armed area triggers an alarm, entering armed area from non-armed area within the delay time period will not lead to linkage alarm. Linkage alarm will be produced if delay time comes to an end and it is not disarmed.</p> <p> Delay is only valid to the areas of Delay Alarm.</p>
Exit Delay	<p>After arm, Delay Alarm area will enter arm status at the end of Exit Delay.</p> <p> If multiple areas set the exit delay, interface prompt will conform to maximum delay time.</p>

Step 5 Tap **OK** to complete setting.

4.6.3.2 Wireless Zone



Only devices with wireless function have this function.

Add, delete and set wireless zones.

Step 1 Tap **Setting**.

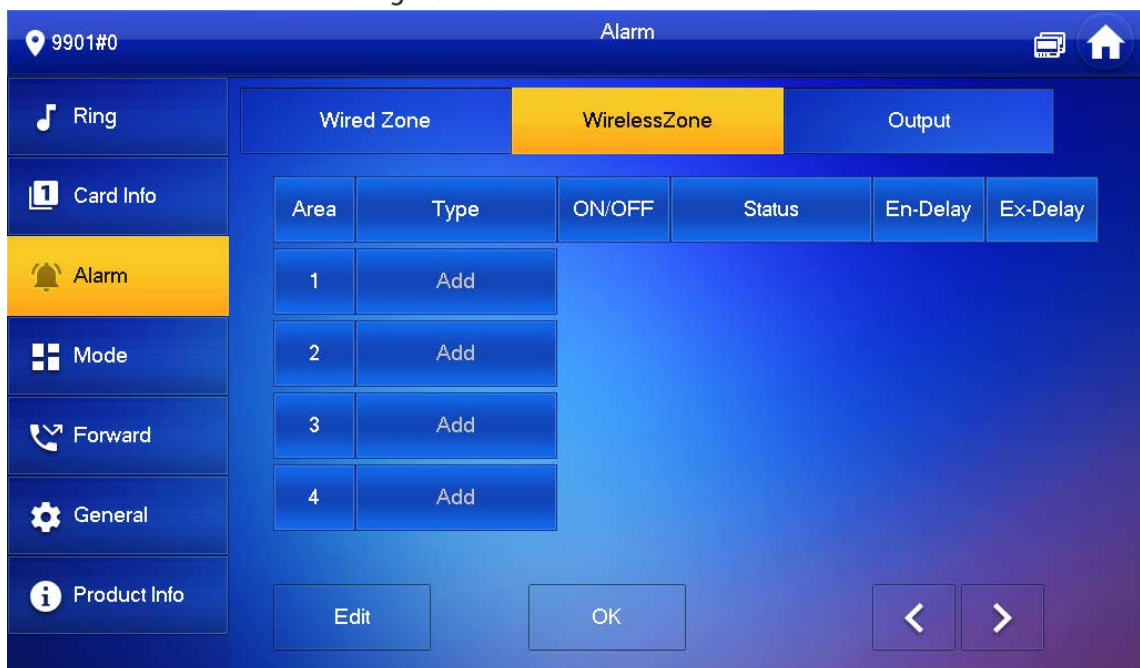
Step 2 Enter login password and tap **OK**.



Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.

Step 3 Select **Alarm > Wireless Zone**.

Figure 4-28 Wireless zone



Step 4 Tap **Add**.

Step 5 Tap wireless code button of wireless device. See wireless device user's manual for details. After successful coding, display area info.

Step 6 Tap corresponding positions to set alarm status, enter delay and exit delay. See Table 4-6 for details.



Tap **Edit** to select a zone and **Delete** to delete the selected area.

4.6.3.3 Alarm Output

After enabling alarm output, when other devices call this VTH, the alarm output device will output alarm info.

Step 1 Tap **Setting**.

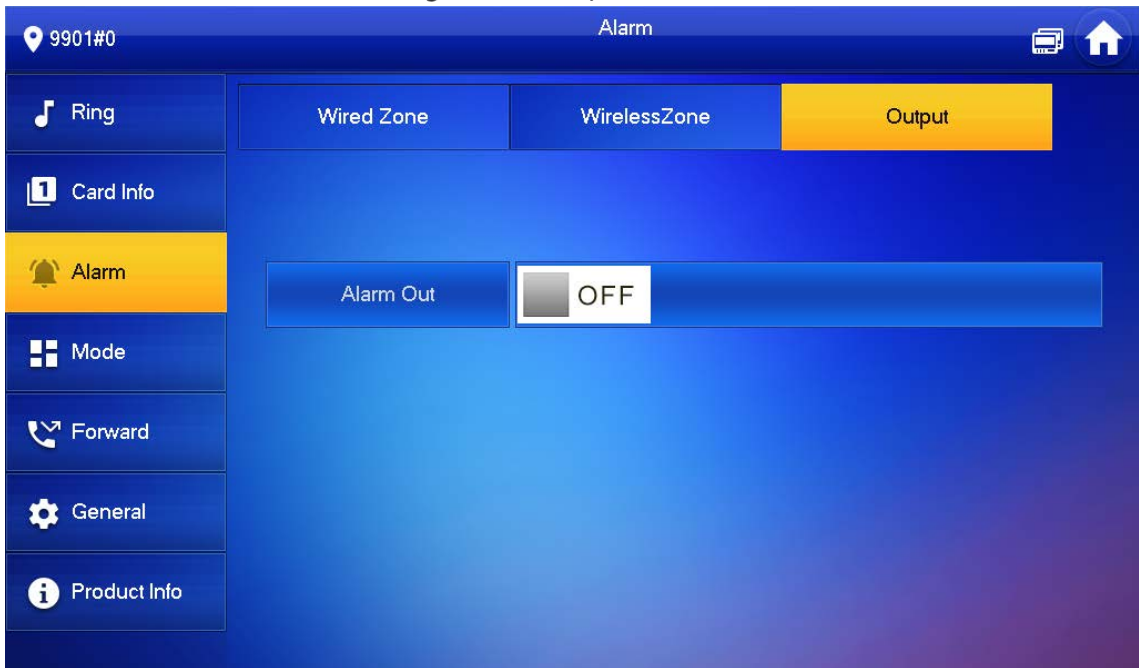
Step 2 Enter login password and tap **OK**.



Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.

Step 3 Select **Alarm > Output**.

Figure 4-29 Output



Step 4 Tap OFF to enable alarm output function, and the icon becomes ON.

4.6.4 Mode Setting

Set area on/off status under different modes.



Area mode can be set only in disarm status.

Step 1 Tap **Setting**.

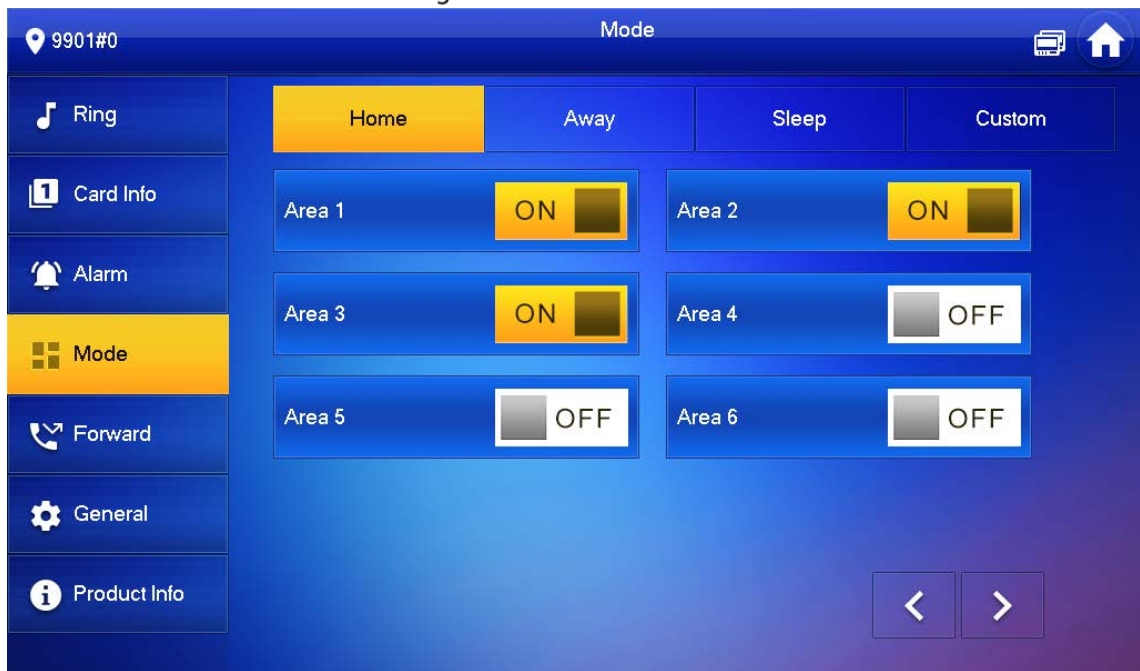
Step 2 Enter login password and tap **OK**.



Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.

Step 3 Tap **Mode**.

Figure 4-30 Mode



Step 4 Select arm mode in every tab.

Step 5 Tap OFF in every area to add it into arm mode.



Multiple areas can be added into one arm mode simultaneously, whereas one area can be added into different modes.

4.6.5 Forward Setting

Forward incoming calls.



Parameters at this interface are set on main VTH only, and extension VTH synchronizes with main VTH.

Step 1 Tap **Setting**.

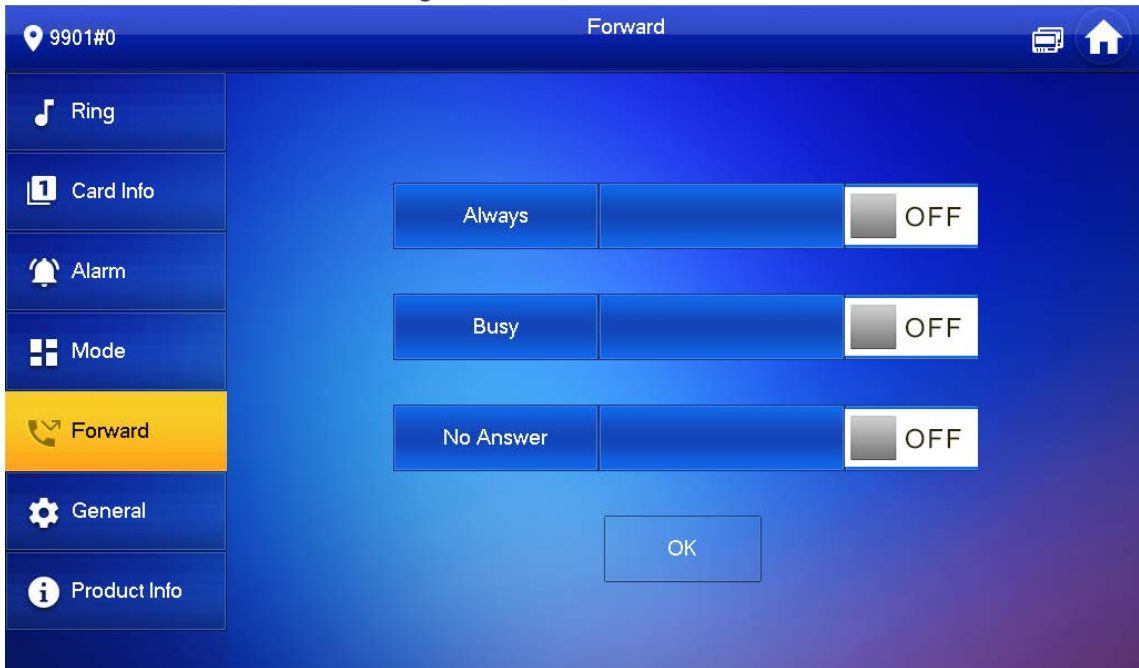
Step 2 Enter login password and tap **OK**.



Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.


Step 3 Tap **Forward**.

Figure 4-31 Forward



Step 4 Input VTH no. in the corresponding forward mode, tap OFF to enable the forward function.

Table 4-7 Parameter description

Parameter	Description
Always	All incoming calls will be forwarded to preset number immediately.
Busy	When the user is busy, incoming call from the third party will be forwarded to preset number. If No Answer is not set, when the user refuses to answer, the incoming call will be deemed as busy forwarding.
No Answer	If no one answers after VTH ring time, the incoming call will be forwarded to preset number.  Set VTH ring time at Setting > Ring > Other interface.



- To forward to a user of another building or unit, the forward number is Building + Unit + VTH room number. For example, input 1#1#101 for 101 of Unit 1, Building 1.
- To forward to a user of the same unit, the forward number is VTH room number.

Step 5 Tap **OK** to save settings.

4.6.6 General Setting

Set VTH time, display, password and others.

4.6.6.1 Time Setting

Set VTH system time, time zone and DST.



Parameters at this interface are set on main VTH only, and extension VTH synchronizes with main VTH.

Step 1 Tap **Setting**.

Step 2 Enter login password and tap **OK**.



Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.

Step 3 Select **General > Time**.

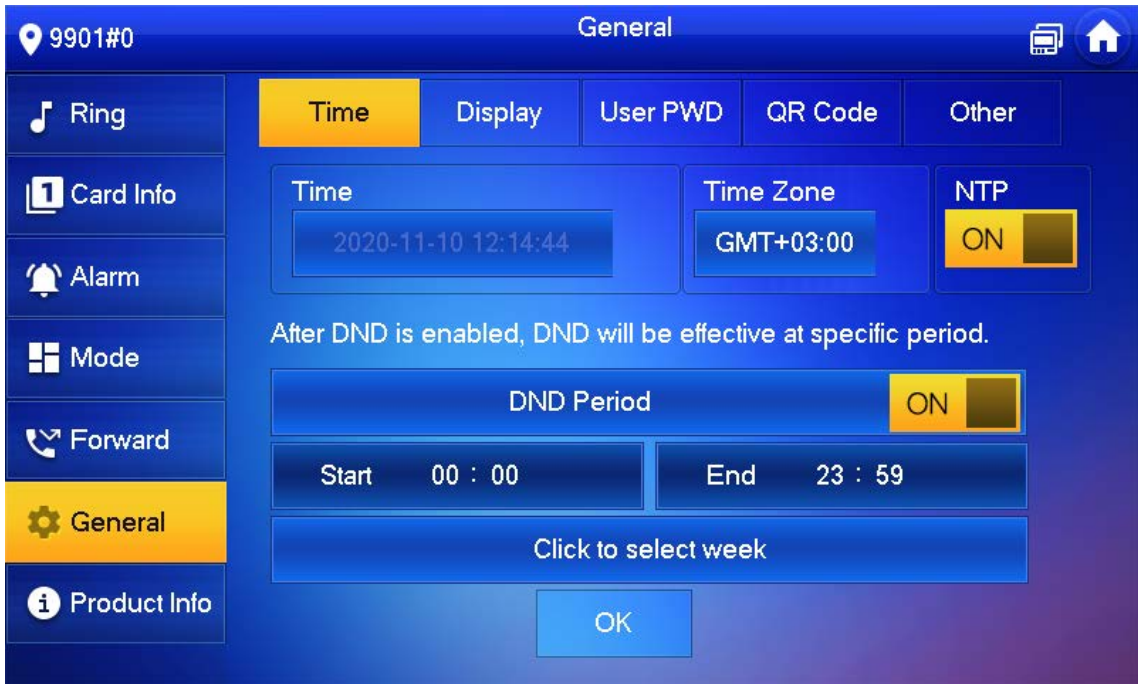
Figure 4-32 Set time and time zone



Step 4 Set time parameter.

- Turn on **NTP**, the VTH will synchronize time with the NTP server automatically; turn it off to set time or time zone manually.

Figure 4-33 Set DND period



- Turn on DND period, set start and end time or click **Click to select week** to select the day(s), and you will not receive any call or message during this period.

4.6.6.2 Display Setting

Set VTH screen brightness, screensaver time and clean.

Step 1 Tap **Setting**.

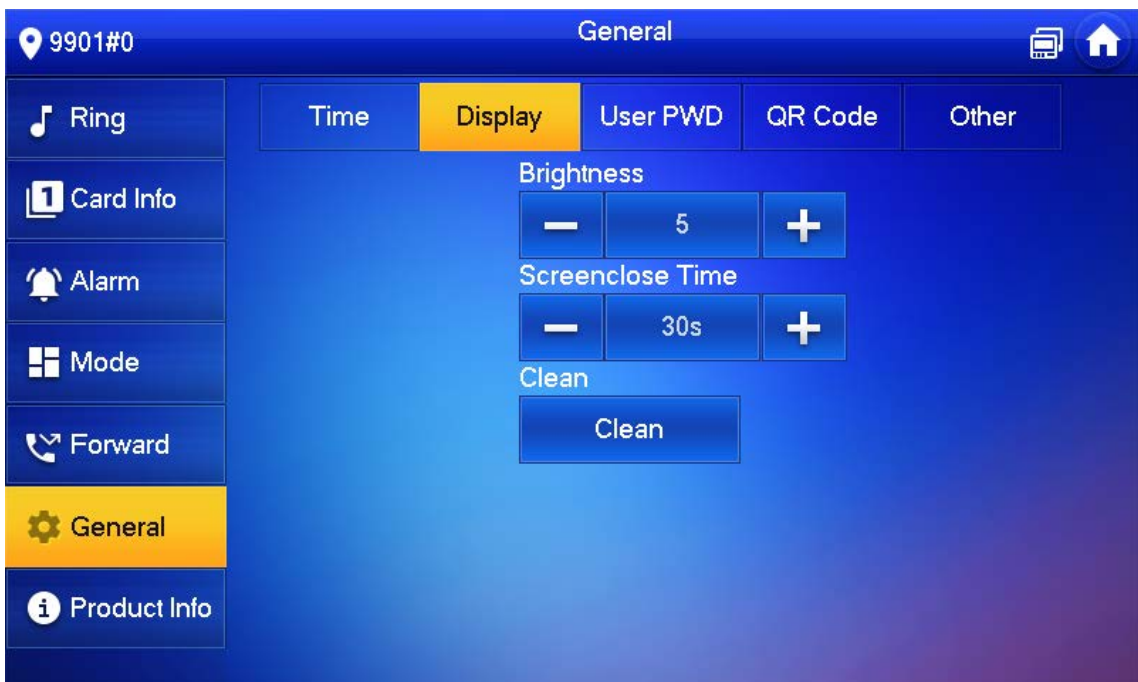
Step 2 Input login password and tap **OK**.





Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.

Step 3 Select **General > Display**.

Figure 4-34 Display



Step 4 Set parameters.

- Tap  and ; set Brightness and Screensaver Time.
- Tap Clean and the screen will be locked for 30 seconds. During the period, clean the screen. It restores after 10 seconds.

4.6.6.3 Password Setting

Set login password, arm/disarm password, unlock password and anti-hijacking password of VTH setting interface. Login password, arm/disarm password and unlock password are 123456 by default, whereas anti-hijacking password is the reversed login password.



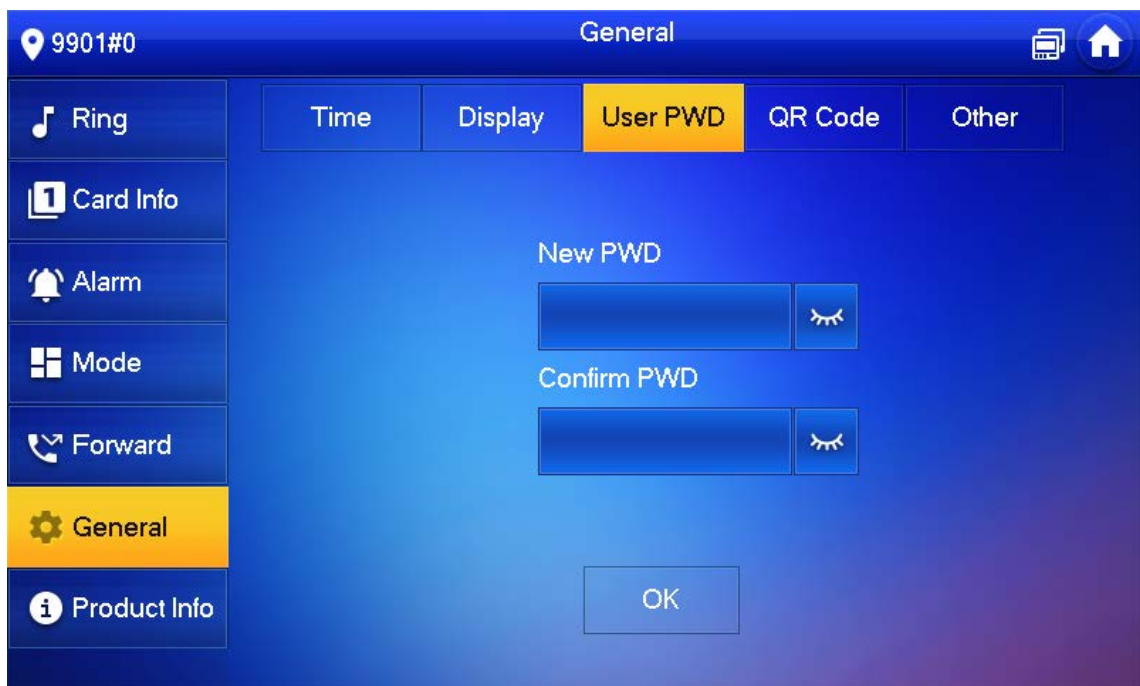
Parameters at this interface are set on main VTH only, and extension VTH synchronizes with main VTH.

Step 1 Tap **Setting**.

Step 2 Input login password and tap OK.

Step 3 Select **General > User Password**.

Figure 4-35 User password



Step 4 Enter **New Password** and **Confirm Password**.

Step 5 Tap **OK** to complete password modification.

4.6.6.4 QR Code

Download the app on your smartphone by scanning the QR code, register the VTH on the app, and then you can unlock the door, or talk to the VTH, and more directly on your smartphone.

Step 1 Tap **Setting**.

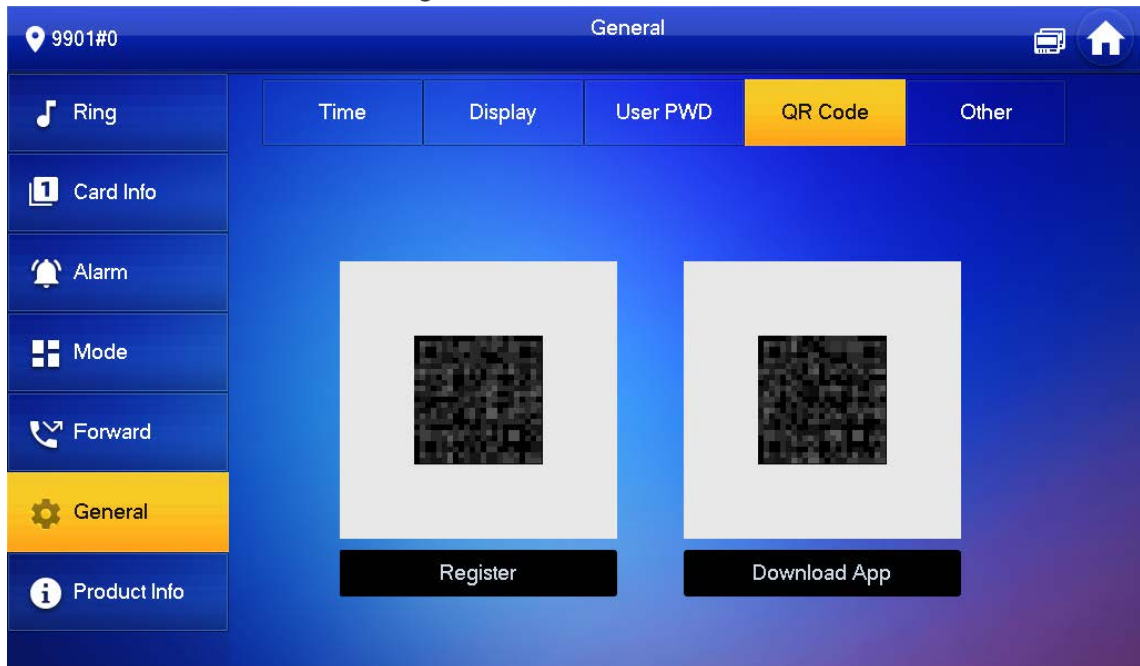
Step 2 Input login password and tap **OK**.



Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.

Step 3 Select **General > QR Code**.

Figure 4-36 QR Code



Step 4 Scan the QR code on the right to download the DSS Agile VDP on your smartphone.

Step 5 Scan the QR code on the left to register the VTH to the app.



For detailed operations of the app, see "5 DSS Agile VDP".

4.6.6.5 Other Settings

Set monitor time, record time, VTO message time, VTO talk time, resident-to-resident call enable, resident-to-resident call time, auto capture and touch ring.



Extension VTH can set Auto Capture and Touch Ring, but other parameters synchronize with main VTH and cannot be set.

Step 1 Tap **Setting**.

Step 2 Input login password and tap **OK**.



Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.




Step 3 Select **General > Other**.





Figure 4-37 Other



Step 4 Set parameters.

Table 4-8 Parameter description

Parameter	Description	Operation
Monitor Time	Maximum time to monitor VTO, IPC and fence station.	Tap  and  to set the time.
Record Time	Maximum recording time of videos during call, talk, monitoring and speaking. The system stops recording at the end of recording time.	
VTO Message Time	<ul style="list-style-type: none"> When VTO Message Time(s) is not 0: <ul style="list-style-type: none"> ◇ If the VTH has an SD card and does not answer the VTO, it will enter message status according to prompt, and save the message in the SD card. ◇ If VTH does not have SD card, and the leave message upload function is not enabled on the VTO, the call will be hung up automatically if the VTH does not answer the VTO. When VTO Message Time(s) is 0: <ul style="list-style-type: none"> In any situation, the call will be hung up automatically if the VTH does not answer the VTO. <p></p> <p>If VTO sets to forward the call to management center, if VTH doesn't answer when VTO calls, and there is no message prompt, the call will be forwarded to management center.</p>	
Resident-to-resident Call Time	Maximum talk time between VTH and VTH.	
VTO Talk Time	Maximum talk time when VTO calls VTH.	

Parameter	Description	Operation
Resident-to-resident Call Enable	<p>After resident-to-resident call is enabled, VTH can call another VTH.</p>  <p>The called party enables internal call, to realize this function.</p>	<p>Tap  OFF to enable the function. The icon becomes  ON.</p>
Auto Capture	<p>After enabled, 3 pictures will be captured automatically when the VTO calls the VTH. Tap Info > Record and Picture to view them.</p>  <ul style="list-style-type: none"> An SD card is needed for this function. After enabling auto capture, Answer and Delete Snapshots will be displayed, which when turned on, snapshots will be deleted if the VTH answers the call. 	
Touch Ring	<p>After enabling touch ring, there will be a ring when touching the screen.</p>	

4.6.7 Product Info

Reboot the system and format SD card.



If SD card isn't inserted into the device, SD format function is invalid.

Step 1 Tap **Setting**.

Step 2 Input login password and tap **OK**.



Default login password is 123456. Please refer to 4.6.6.3 Password Setting for details.

Step 3 Tap **Product Info**.

Figure 4-38 Product information



- **Restart:** Restart the device.
- **Language:** Change the language of the device.
- **Format SD Card:** Clear all data in the SD card.



Be careful with this operation.

- **Eject SD card:** Eject the SD card first to safely remove it.

4.7 Project Settings

4.7.1 Forget Password

If you forget initialization password when entering project settings interface, reset password through Forget Password at the interface or in VDPconfig tool.

4.7.1.1 Reset the Password at the Interface

Step 1 Tap **Setting** for over 6 seconds.

Step 2 Tap **Forget Password**.

Figure 4-39 QR code



- Step 3** Scan the QR code with any code-scanning APP, bind your email box, send it by email to support_gpwd@htmicrochip.com, and thus obtain security code.
- Step 4** Tap **Next**.
- Step 5** Enter **Password**, **Confirm Password** and obtained **Security Code**.
- Step 6** Tap **OK** to complete resetting the password.

4.7.1.2 Reset the Password in VDPconfig

Use VDPconfig tool to export XML file (ExportFile.xml), send it by email to support_gpwd@htmicrochip.com, and obtain XML file (result.xml). Then, import the file and reset a new password.



Please refer to VDPconfig Help Document for details.

4.7.2 Network Settings

See "3.1.2.2 Network Parameters".

4.7.3 VTH Configuration

See "3.1.2.3 VTH Config".

4.7.4 VTO Configuration

See "3.1.2.5 VTO Configuration".

4.7.5 Default

All parameters of the device will be restored to default values.



IP address and data in the SD card will not be restored. See Figure 4-38 to format the SD card.

Step 1 Tap **Setting** for over 6 seconds.

Step 2 Enter the password set during initialization, and tap OK.

Step 3 Tap **Default**.

Step 4 Tap **OK**.

The device restarts and proceeds to initialization.

4.7.6 Reset MSG

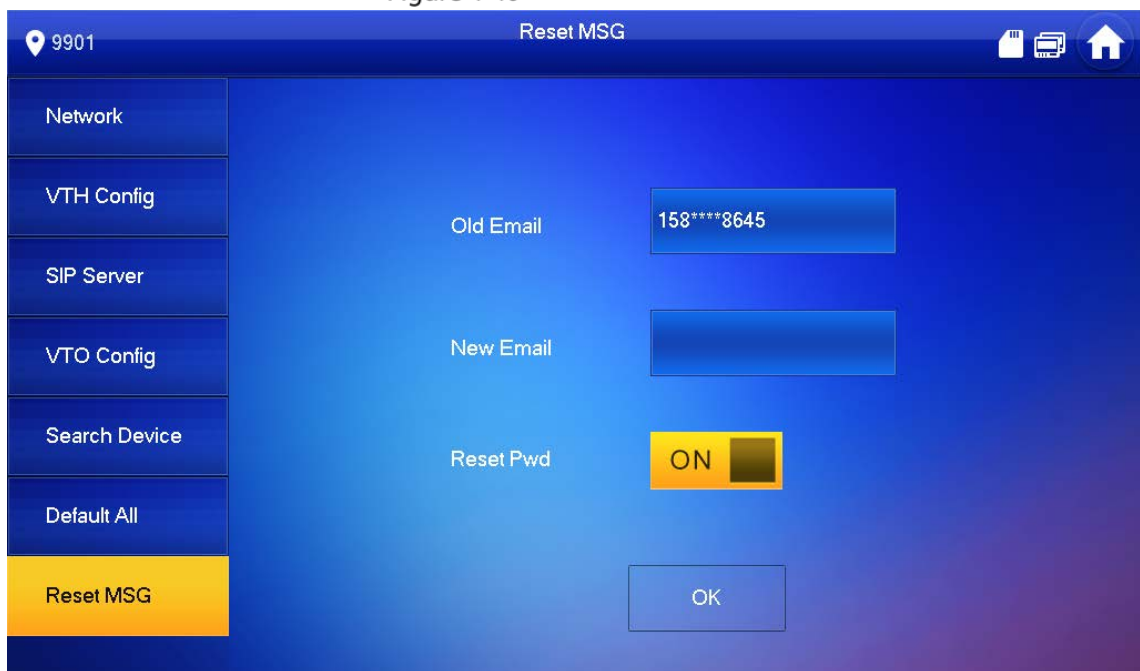
Modify the bonded Email.

Step 1 Tap **Setting** for over 6 seconds.

Step 2 Enter the password set during initialization, and tap **OK**.

Step 3 Tap **Reset MSG**.

Figure 4-40 Reset MSG



Step 4 Enter a new email address, turn on **Reset Pwd**, and then tap **OK**.



- The email will obtain security code during password resetting. See 4.7.1 Forget Password for details.
- If **Reset Pwd** is turn off, you cannot reset the password.

4.8 Unlock Function

When the VTH is being called, during monitoring, talking and speaking, tap unlock button, and the VTO will be unlocked remotely.

4.9 Arm and Disarm Function

4.9.1 Arm

In case of triggering alarm after arm, produce linkage alarm and upload alarm info.

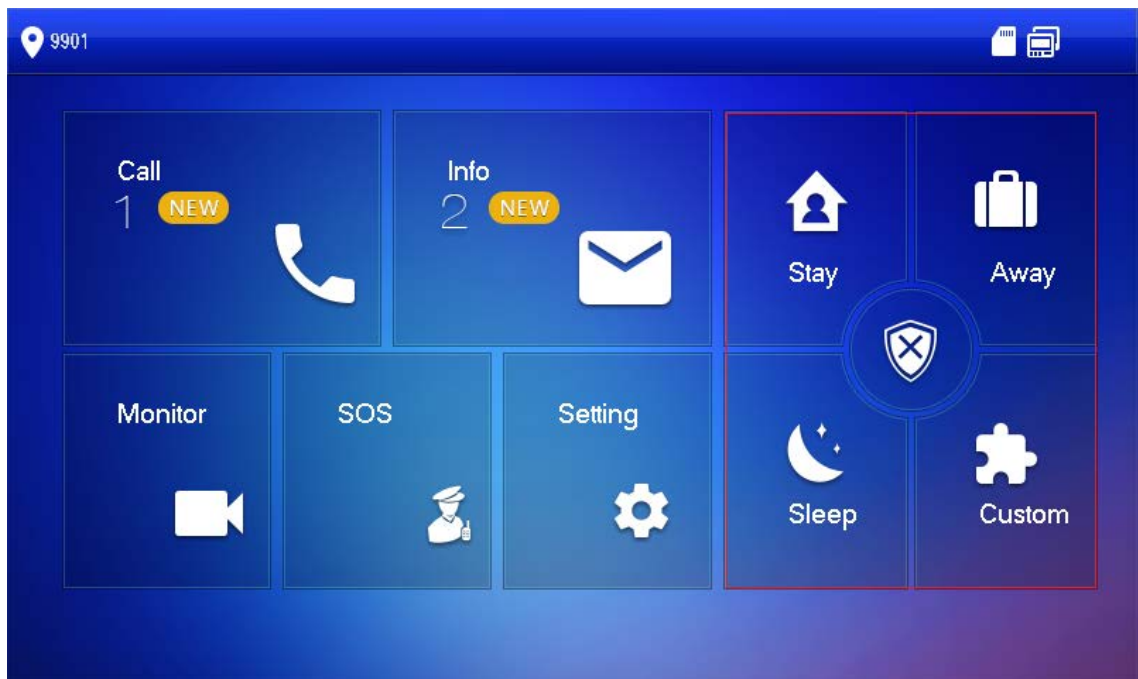


- Please ensure that the area has been added into arm mode. Otherwise, there will be no alarm triggering after arm.
- Please ensure that it is in disarmed status. Otherwise, arm will fail.



Step 1 Tap  at the main interface.

Figure 4-41 Arm mode



Step 2 Select arm mode.

Step 3 Enter arm and disarm password; tap **OK**.

The device beeps continuously, which represents successful arm. The key displays corresponding arm mode.



- Default password of arm and disarm is 123456. Please refer to 4.6.6.3 Password Setting for details.
- If delay alarm is set in the area, the device will beep continuously at the end of exit delay time.

4.9.2 Disarm



Please ensure that it is in armed status. Otherwise, disarm will fail.

Step 1 Tap disarm symbol at the lower right corner of the main interface.

Step 2 Enter arm and disarm password, and then tap **OK**.



- Default password of arm and disarm is 123456. Please refer to 4.6.6.3 Password Setting for details.
- If you are forced to enter disarm password in case of emergencies, enter anti-hijacking password, which is the reversed arm password. The system will disarm, and at the same time, upload alarm info to management center/platform.

5 DSS Agile VDP

You can download DSS Agile VDP (hereinafter referred to as the "app") and link your VTH to the app to unlock the door, talk to connected VTO devices, call the management center, and view call records and messages.



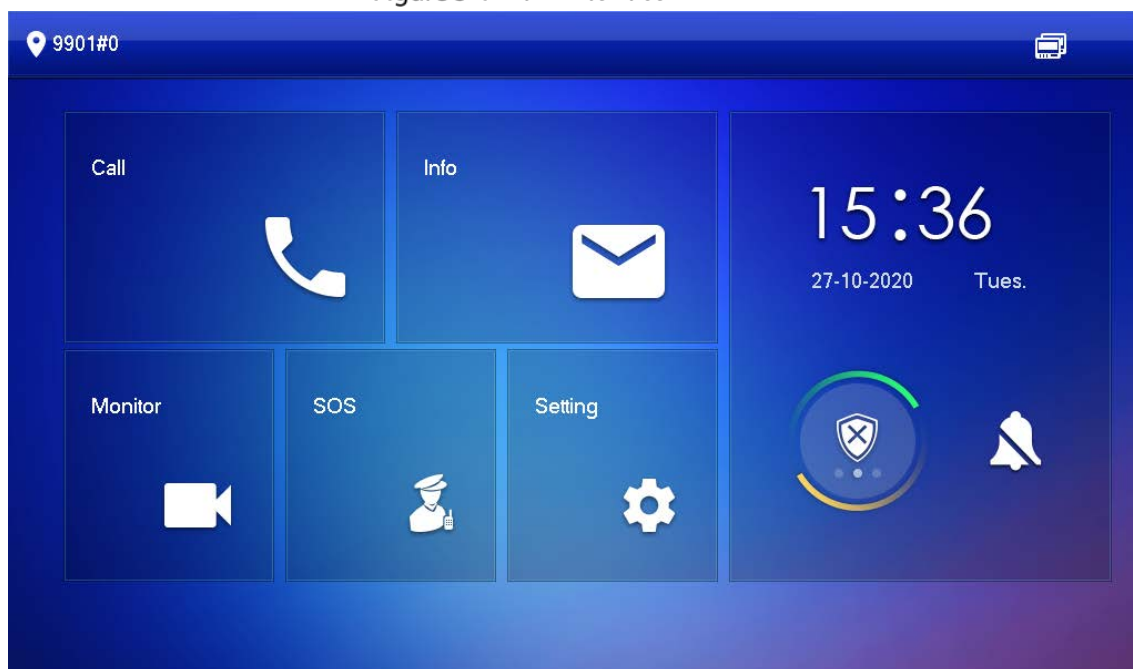
Interfaces and operations might vary between iOS and Android OS. This section takes Android OS as an example.

5.1 Downloading the App

Before you start, make sure the VTO, VTH, and DSS server are properly connected.

Step 1 On the VTH main interface, tap **Setting**.

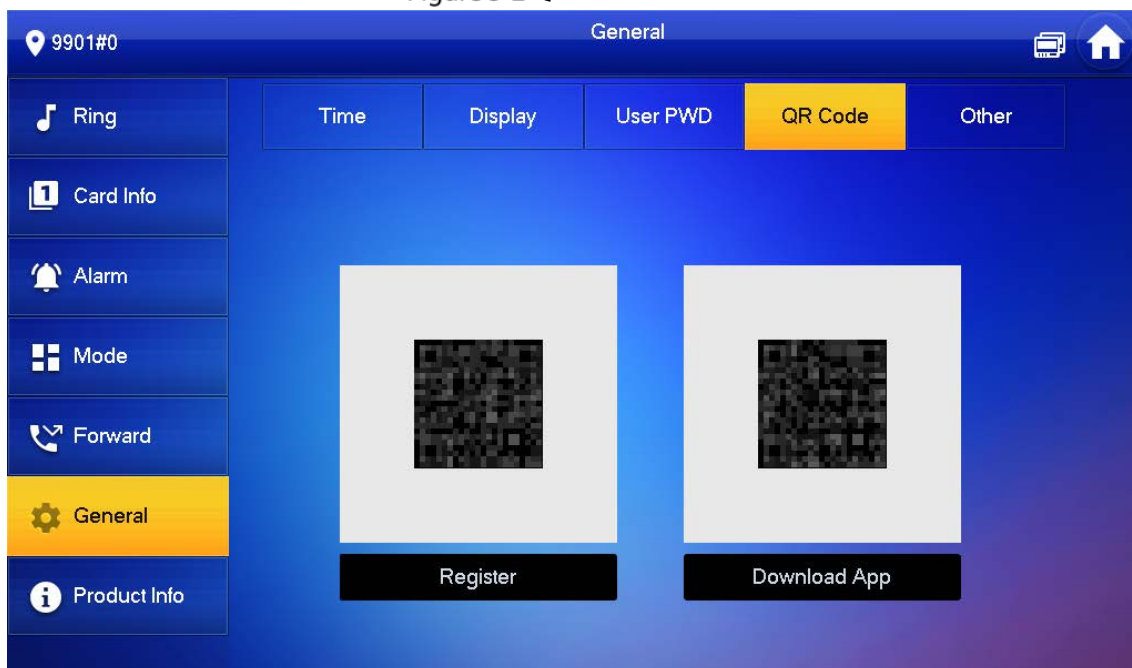
Figure 5-1 Main interface



Step 2 Input the password you configured, and then select **General > QR Code**.

Step 3 Scan the **Download** QR code with your smartphone, and then download and install the app.

Figure 5-2 QR code



5.2 Registration and Login


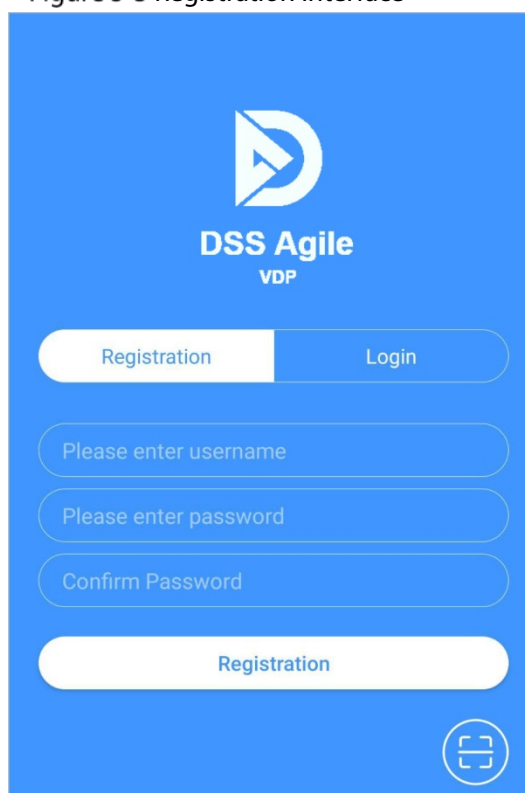
Step 1 Tap  on your smartphone, read the **Software license agreement and Privacy policy**, and then tap **Agree** (only for first-time login).

Figure 5-3 Registration interface




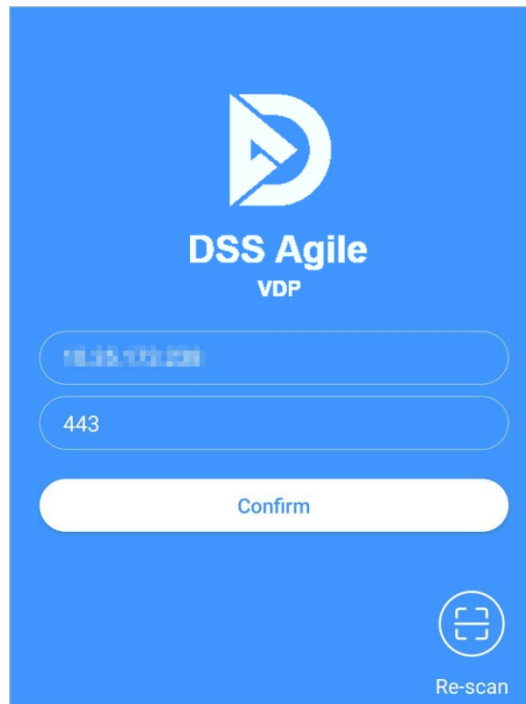
Step 2 Tap , and then scan the **Register** code on the VTH. See Step 2 in "5.1 Downloading the App".

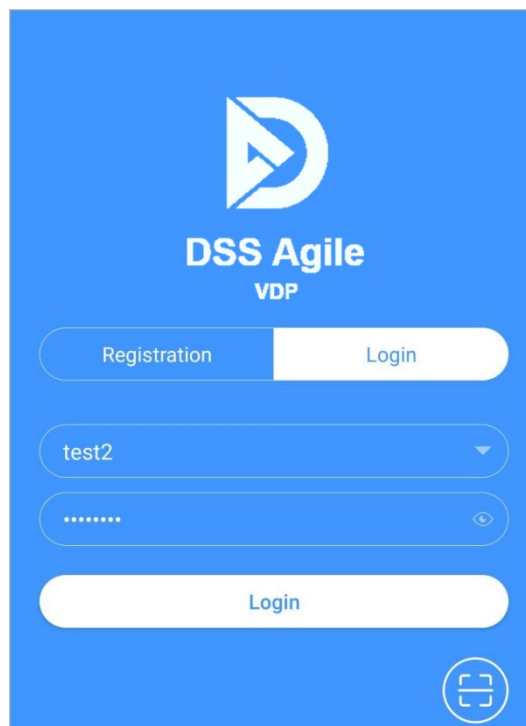
Figure 5-4 Confirm IP address and port number



Step 3 Verify the IP address and port number, and then tap **Confirm**.

Step 4 Enter the username and password, and then tap **Registration**. You can add 5 users to one VTH at most.

Figure 5-5 Login



Step 5 Tap the **Login tab**, enter the username and password you have set, and then tap **Login**.

5.3 Call Functions

You can receive the forwarded calls, remotely unlock the door, view live video of the VTO, and more.



To receive push notifications of call messages on the mobile phone, make sure that notifications of the app are enabled on your smartphone, and you are logged in to the app.

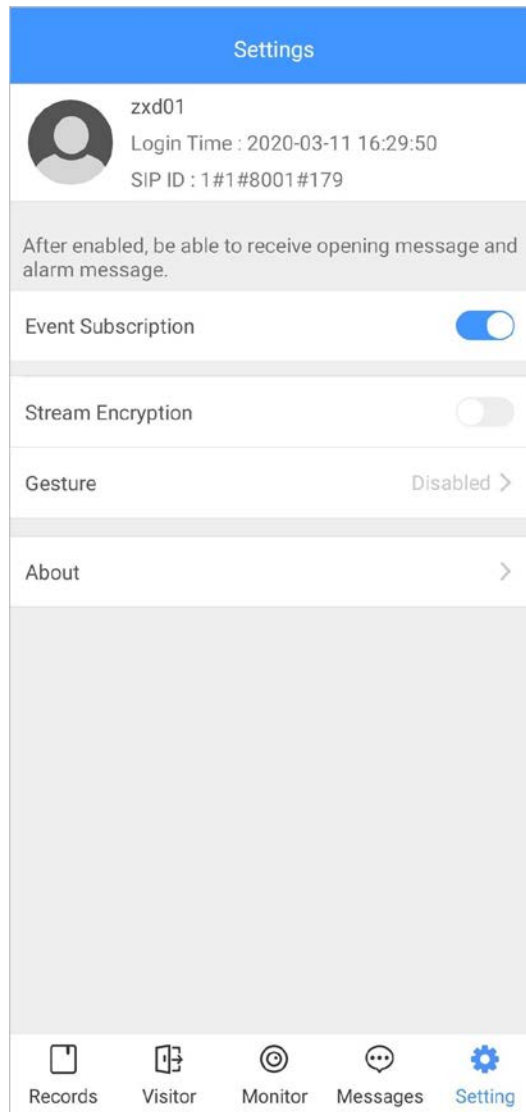
5.3.1 Forwarding Calls

Confirm your SIP ID, and then configure call forwarding on the VTH. If any device calls the VTH, you will receive the call on your smartphone.

Step 1 Log in to the app, and then tap **Setting**.

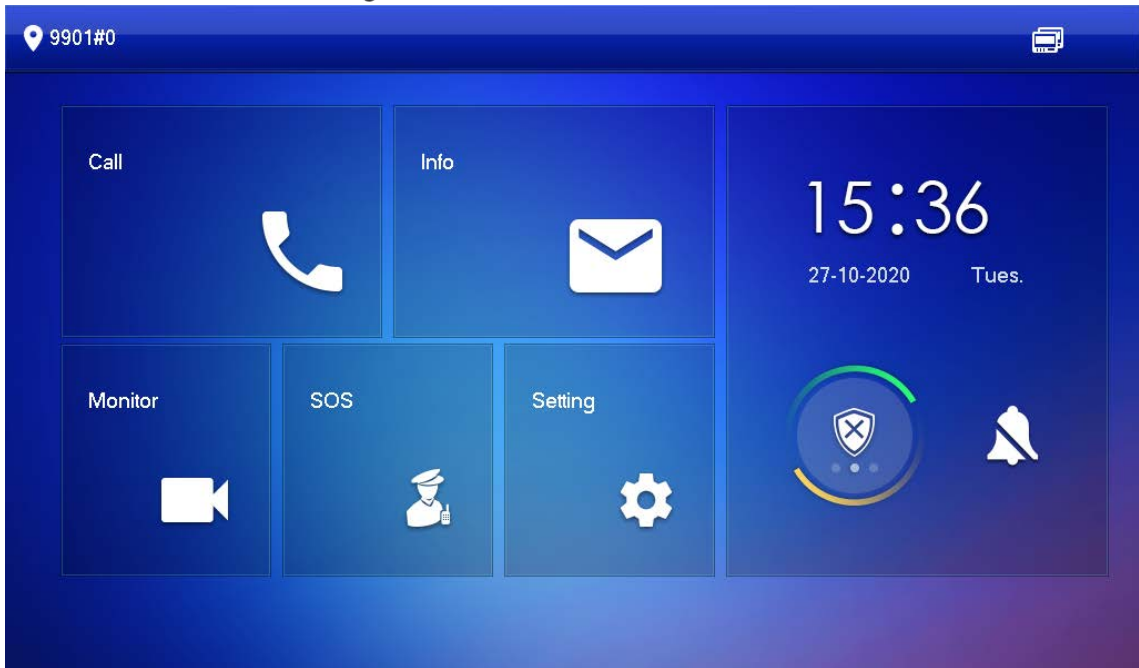
In the following example, the **SIP ID** is **1#1#8001#179**.

Figure 5-6 Settings



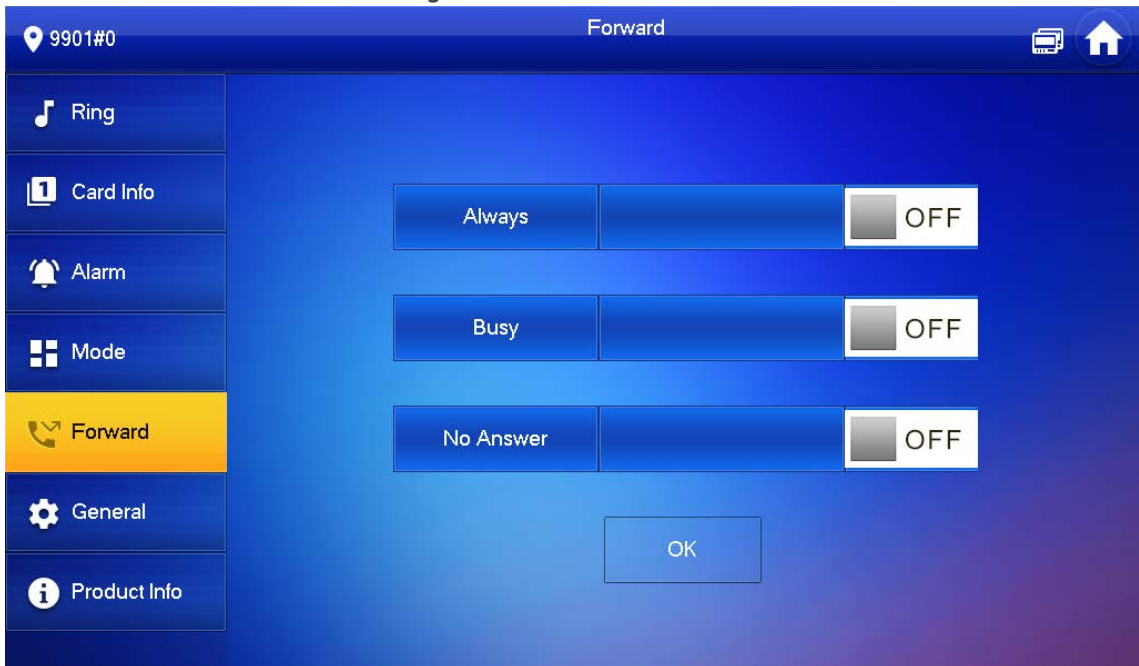
Step 2 On the VTH main interface, tap **Setting**.

Figure 5-7 VTH main interface



Step 3 Enter the password you configured, and then tap **Forward**.

Figure 5-8 Forward



Select forwarding type as needed:

- **Always:** All calls to this VTH will be forwarded.
- **Busy:** If the VTH is busy, the call will be forwarded.
- **No Answer:** Any call that is not answered within the defined ring time will be forwarded. See "4.6.1.4 Other Ring Settings" for details.

Step 4 Enter the SIP ID in the input box.

- Forward calls to a specific user: Enter the SIP ID of the user. For example, enter 1#1#8001#179 from Figure 5-6, and then calls will be forwarded to this user.
- Forward calls to every user: Change the last three numbers of the SIP ID to 100 (1#1#8001#100), and then all users linked to this VTH will receive the call on their smartphones at the same time.

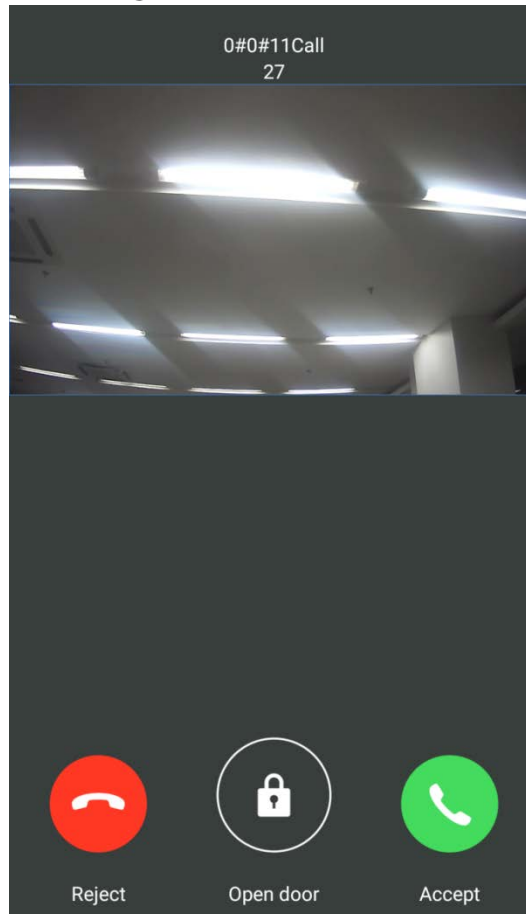
Step 5 Tap OFF to enable the forwarding type you selected, and then tap **OK**.

5.3.2 Calling Operations

After call forwarding is configured, you can receive and answer phone calls from the VTO or the management center.

For example, when a VTO is calling, you can answer the call, view live video, and remotely unlock the door if the VTO is connected to a lock.

Figure 5-9 A call from a VTO

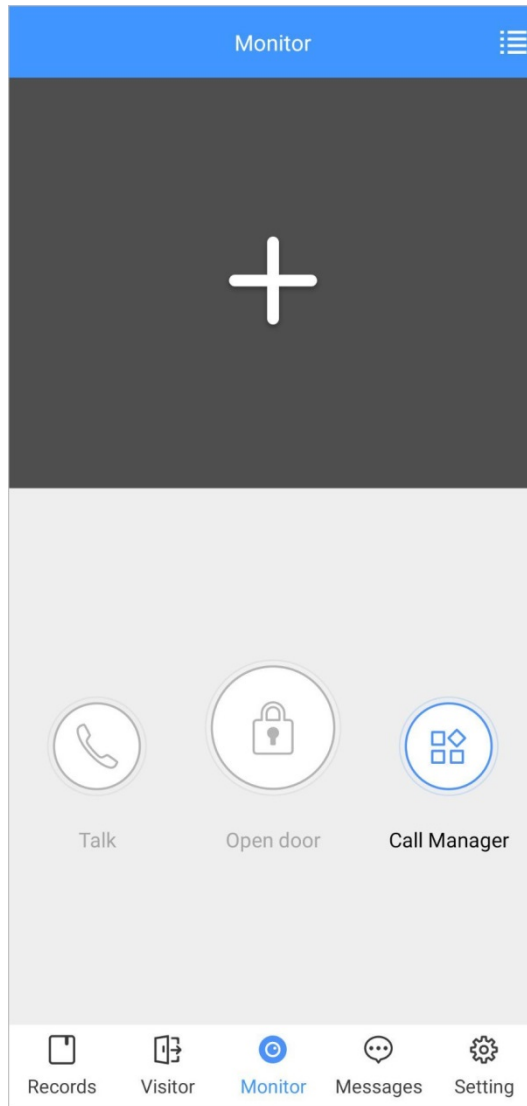


5.4 Monitoring

After a VTO is added, you can view its live video, have two-way audio talk, call management center, and remotely unlock the door.

Step 1 Log in to the app, and then tap **Monitor**.

Figure 5-10 Monitor interface




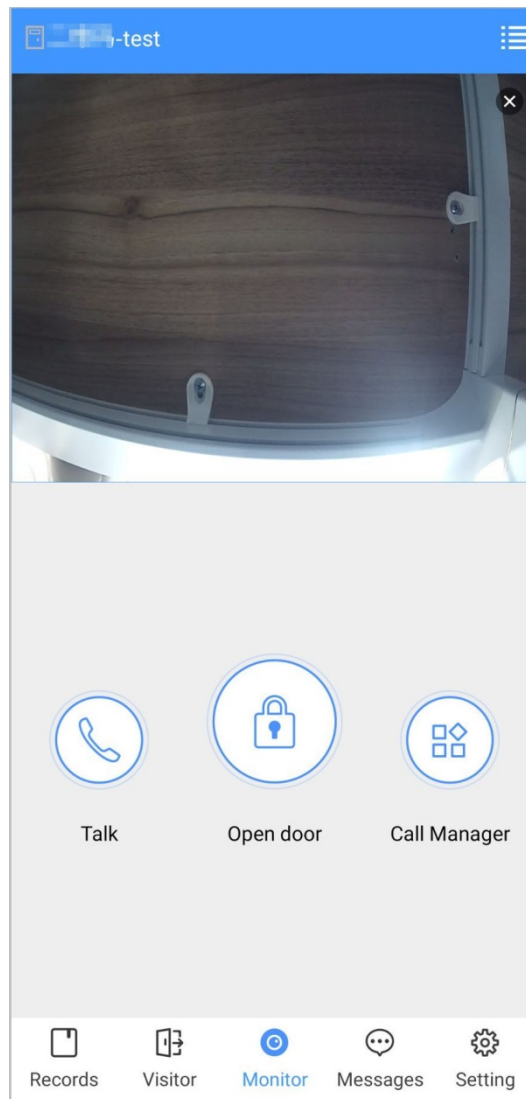




Step 2 Tap , select the VTO from the channel list as needed.

Figure 5-11 Live video



- : Switch to another VTO.
- : Unlock the door remotely.
- : Have a two-way audio talk with the VTO.
- : Call management center.

5.5 Call Records

View the incoming and outgoing call records.

Log in to the APP, and then tap **Records**.

Figure 5-12 Call records

Missed		All	Edit
	888888 Not Opened		09:01:39
	888888 Not Opened		16:45:53
	888888 Not Opened		16:46:12
	8888881000 Not Opened		16:56:54
	VT011 Not Opened		16:57:06
	888888 Not Opened		2020-02-18 19:11:30
	888888 Not Opened		2020-02-18 13:49:28
	888888 Not Opened		2020-02-18 11:35:05

Records Visitor Monitor Messages Setting

- Red phone icon: The call is missed or not answered.
- Green phone icon: The call is answered.
- **Not Opened/Opened:** Indicates whether the door is unlocked.
- **Edit:** Delete the record one by one, or tap **Edit > Empty** to delete all records.

5.6 Message

You can view the unlocking records and alarm messages, and search for history messages.

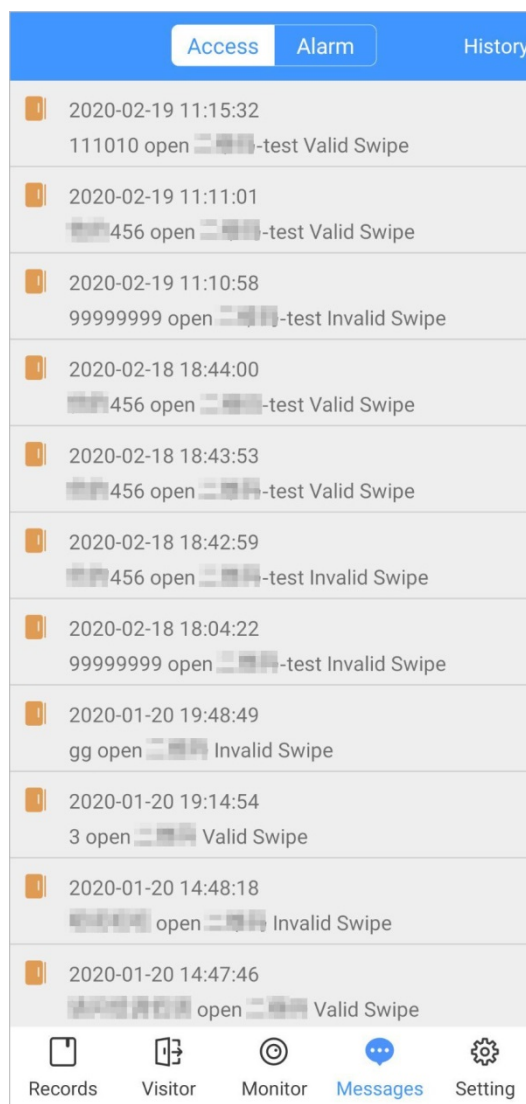


- You need to enable **Event Subscription** in **Setting** of the App first. See "5.7 Setting" for details.
- To receive messages on your smartphone, make sure that notifications of the app are enabled on your smartphone and the you are logged in to the app.

Viewing Messages

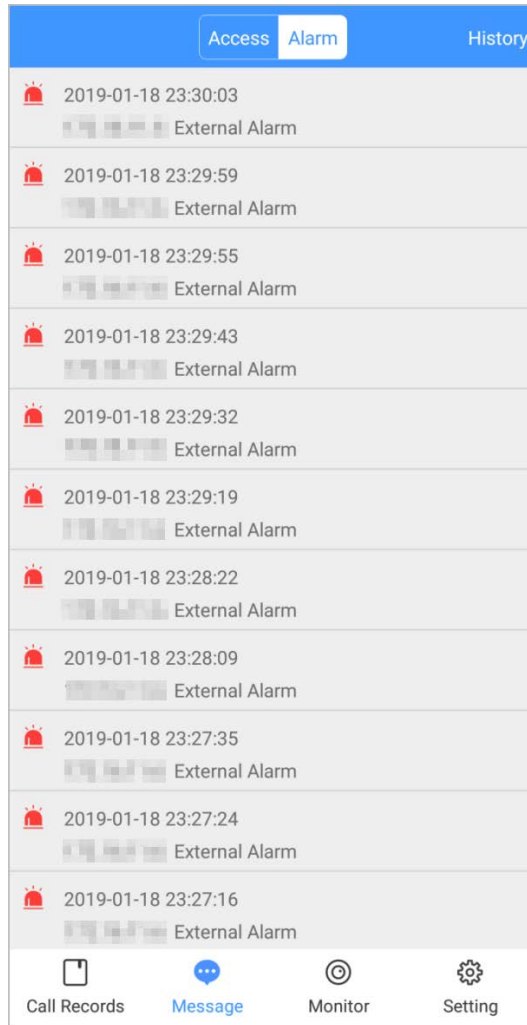
- Log in to the app, tap **Messages > Access**, and then you can view unlocking records, such as unlocking method, which user unlocked the door, and when the door is unlocked.

Figure 5-13 Access messages



- Log in to the App, tap **Messages > Alarm**, and then you can view alarm messages.

Figure 5-14 Alarm messages

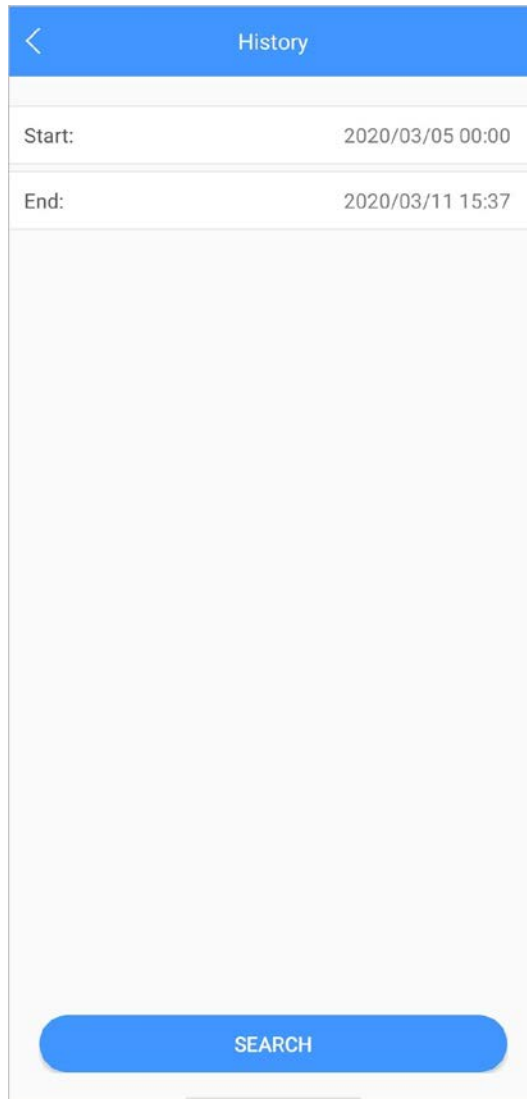


Searching for History Messages

Tap **History**, set the start and end time, and then tap **SEARCH**.

You search for messages within up to 7 days.

Figure 5-15 History messages



5.7 Visitor

You can create a pass for a visitor to have access permission. The pass is invalid after it is manually invalidated, the visiting period expires, or the visit is ended. You can also view visit records.

5.7.1 Creating Pass

Step 1 Log in to the APP, and then tap **Visitor**.

Figure 5-16 Visitor information

Pass		Record
Resident		
3#1#2002#101		
Visitor	Mike	
Vehicle	12345678	<input checked="" type="checkbox"/>
Phone No.	88888888	
Visit Time	2020-03-11 15:14:43	
	2020-03-12 15:14:43	
Credential	ID Card	Select >
Credential No.	[REDACTED]	
Remark	VIF	
Generate Pass		

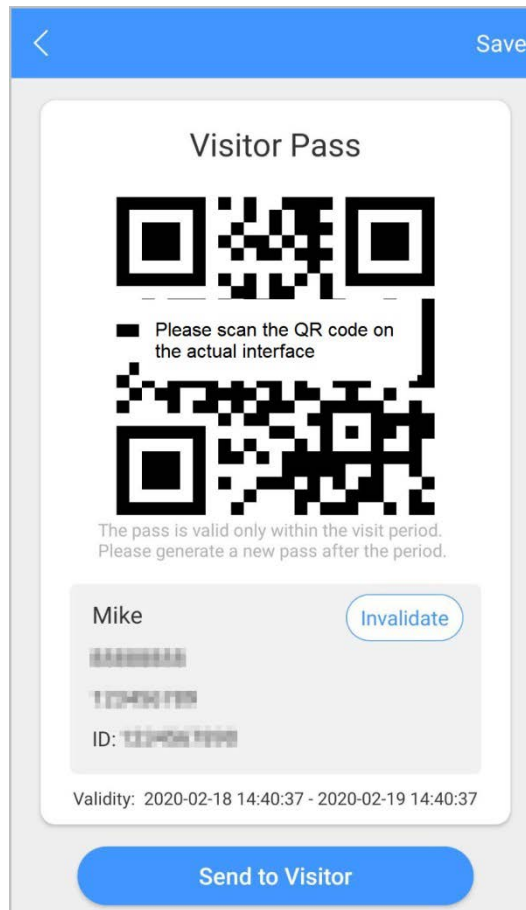
Records Visitor Monitor Messages Setting

Step 2 Enter the information of the visitor, and then tap **Generate Pass**.



Each visitor can only register one plate number.

Figure 5-17 Visitor pass



Step 3 Tap **Send to Visitor** to send the QR code to the visitor.



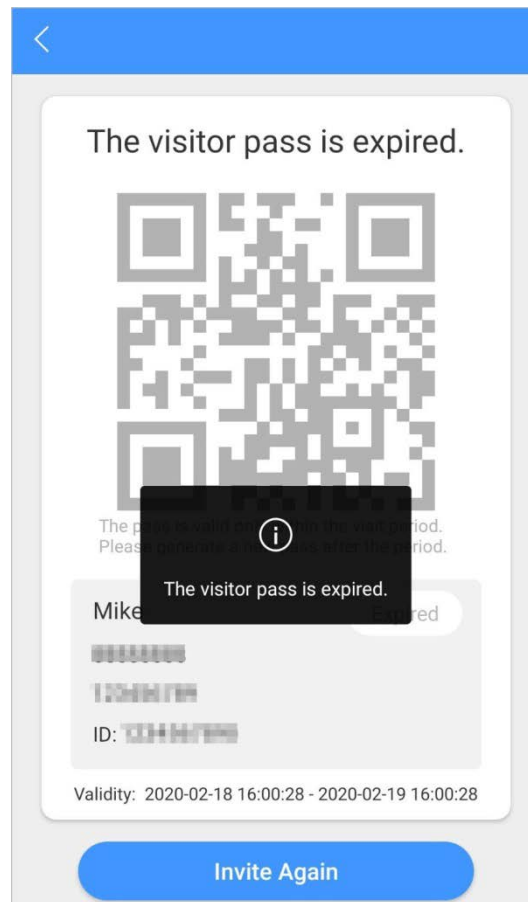
Tap **Save** to save the QR code to your smartphone.

Step 4 (Optional) Tap **Invalidate** to cancel the appointment, and then the QR code will not have access permissions.



Tap **Invite Again** to generate a new pass for the visitor.

Figure 5-18 Invalidate the pass



5.7.2 Visit Records

You can view visitor status such as having an appointment, on a visit, ending the visit, and cancelling the appointment. You can also view and modify the pass.

- View visitor status: Log in to the APP, tap **Visitor > Record**.
- View and modify a pass: Tap a visitor in the list, and then you can view detailed information of the pass, invalidate the appointment, invite the visitor again, and more. For details, see "5.7.1 Creating Pass".

Figure 5-19 Visitor records

The screenshot shows a mobile application interface for 'Visitor records'. At the top, there is a blue header with two tabs: 'Pass' and 'Record'. Below the header is a list of visitor records. Each record consists of a name, a timestamp, and an action button. The records are as follows:

Name	Timestamp	Action
Mike	2020-02-18 16:01:57	Cancel Appointment >
Mike	2020-02-18 15:59:01	Cancel Appointment >
TOM	2020-02-18 15:58:45	Appointment >
TOM	2020-02-18 15:46:54	Cancel Appointment >
TOM	2020-02-18 15:46:43	Cancel Appointment >
TOM	2020-02-18 15:46:11	Cancel Appointment >
Mike	2020-02-18 15:36:32	Appointment >
Mike	2020-02-18 15:34:37	Cancel Appointment >
w1	2020-01-20 09:19:44	Cancel Appointment >
rft2	2020-01-20 09:01:24	End Visit >
rft	2020-01-20 08:58:53	End Visit >

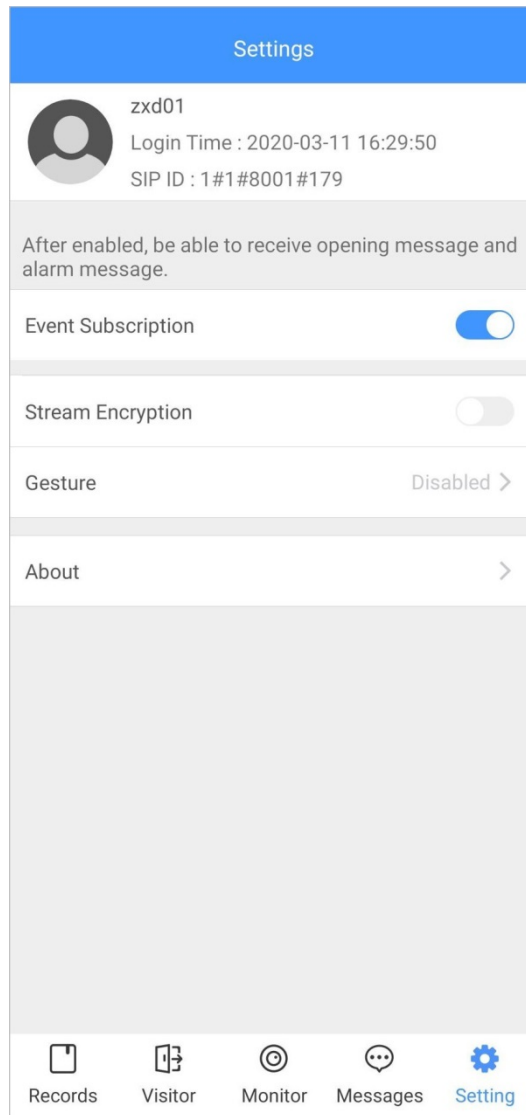
At the bottom of the screen is a navigation bar with five icons and their corresponding labels: 'Records' (document icon), 'Visitor' (blue person icon), 'Monitor' (target icon), 'Messages' (speech bubble icon), and 'Setting' (gear icon). The 'Visitor' icon is highlighted in blue.

5.8 Setting

You can view SIP ID, and enable message subscription, stream encryption, message sound, login by pattern, and more.

Log in to the app, and then tap **Setting**.

Figure 5-20 Setting



- **Event Subscription:** Enable it, and then you can receive unlocking messages and alarm messages. See "5.6 Message" for details.
- **Stream Encryption:** Enable it to enhance security, but stream acquisition speed might slow down.
- **Gesture:** Draw a pattern, and then you can log in by that pattern.
- **About:** View app version, software license and privacy policy, help document, or log out of the current account.

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.

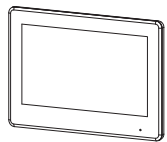
13. Construct a Safe Network Environment

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

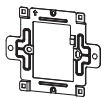
- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, 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.



① × 1



② × 1



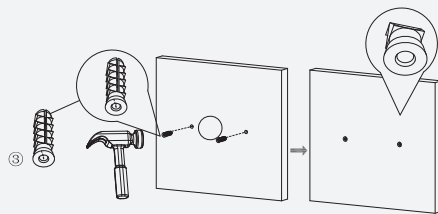
③ × 4



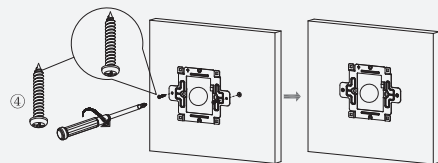
④ × 4



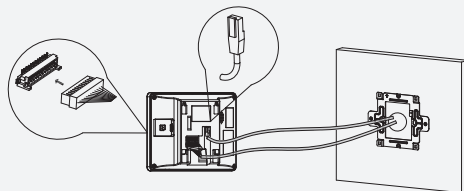
1.2



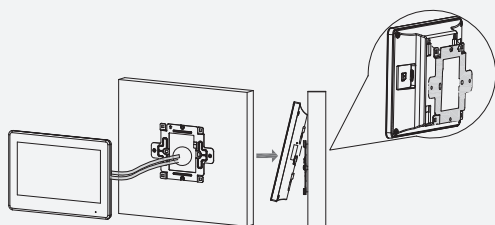
1.3



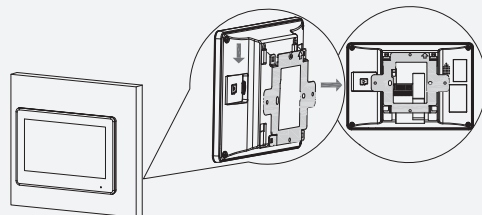
1.4



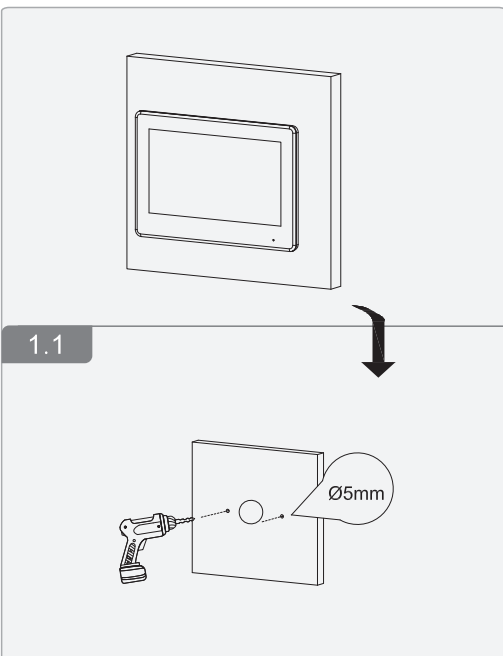
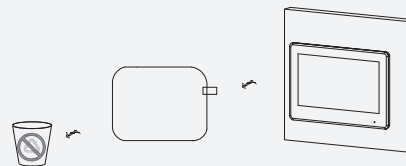
1.5



1.6



1.7



1.1

2-wire Switch

User's manual








Foreword

General

This manual introduces the structure and installation of the 2-wire switch (hereinafter referred to as the "switch").

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

Important Safeguards and Warnings

This chapter introduces the contents covering proper handling of the switch, hazard prevention, and prevention of property damage. Read these contents carefully before using the switch, comply with them when using, and keep the manual well for future reference.

Operation Requirement

- Change the default password after the switch is armed.
- Do not expose the switch to direct sunlight or near heat source.
- Do not expose the switch to dampness or dust.
- Install the switch horizontally or at a stable place to prevent it from falling.
- Do not drop or splash liquid onto the switch, or put anything filled with liquid onto the switch.
- Install the switch at a well-ventilated place, and do not block its vent.
- Use the switch within the rated range of power input and output.
- Do not dismantle the switch by yourself.
- Use the provided power supply.
- Before connecting cables, read and understand the structure first. See "2 Structure". for details.
- Before power on, make sure that all the cables are correctly connected.
- After powered on, if the POWER indicator is solid red, and RUN indicator flashes green, the switch is working properly.
- Before unplugging the power cable, make sure that the power switch is turned to "OFF".
- For best performance, only the first switch needs to be connected to the Ethernet when cascading multiple switches.
- Do not stack the switches on one another.

Power Requirement

- The switch must use electric wires that conform to your local requirements and within their rated specifications.
- Use the power adapter provided with the switch; otherwise, it might result in people injury and device damage.
- 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 the label on the switch.
- For type I devices, use a grounded power socket.
- The appliance coupler is a disconnection device. Keep a convenient angle when using it.

Table of Contents

- Foreword..... I**
- Important Safeguards and Warnings..... II**
- 1 Introduction..... 1**
 - 1.1 Product Overview 1
 - 1.2 Application 1
- 2 Structure 3**
 - 2.1 Front panel 3
 - 2.2 Rear Panel 4
- 3 Installation..... 6**
 - 3.1 Installing with Screws..... 6
 - 3.2 Installing with a Guide Rail 6
- Appendix 1 Cybersecurity Recommendations 8**

1 Introduction

1.1 Product Overview

The switch provides one 2-wire P port, two 2-wire cascading ports and two RJ-45 ports. You can connect up to 10 switches together to bring as many as 200 devices into the network. This is applicable to an apartment where there are many tenants. When connected to network through the switch, 2-wire indoor monitors (VTH) can make calls, unlock doors and monitor.

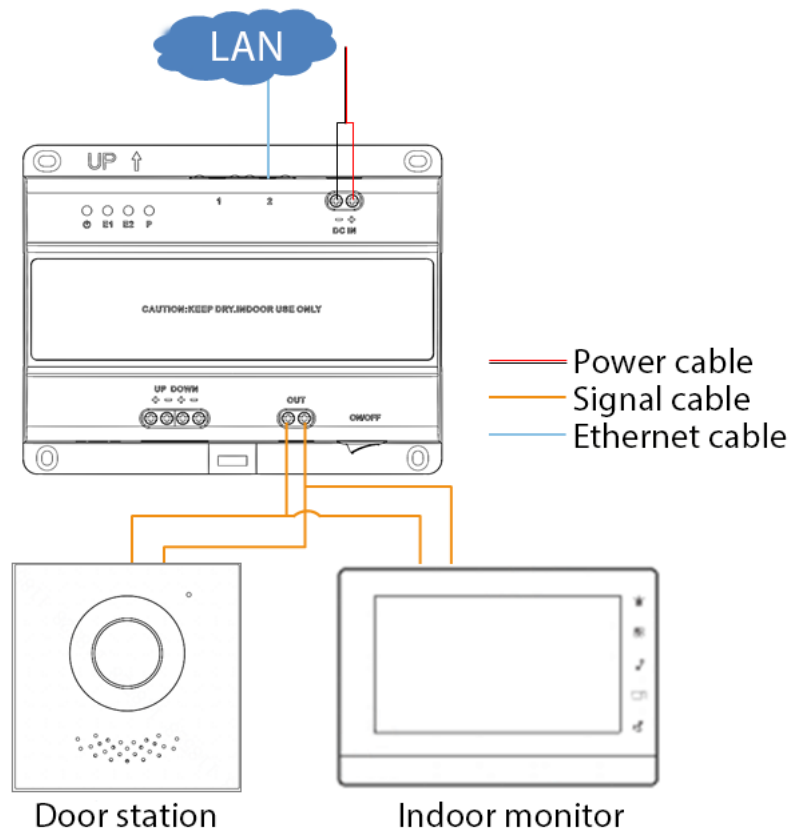
1.2 Application

A single 2-wire switch can connect at most 20 VTHs and 2 door stations (VTOs). Based on the total number of devices, we have villa and apartment.

Villa

If there are no more than 20 VTHs and 2 VTOs, they can all connect to the same switch.

Figure 1-1 Villa network diagram



Apartment

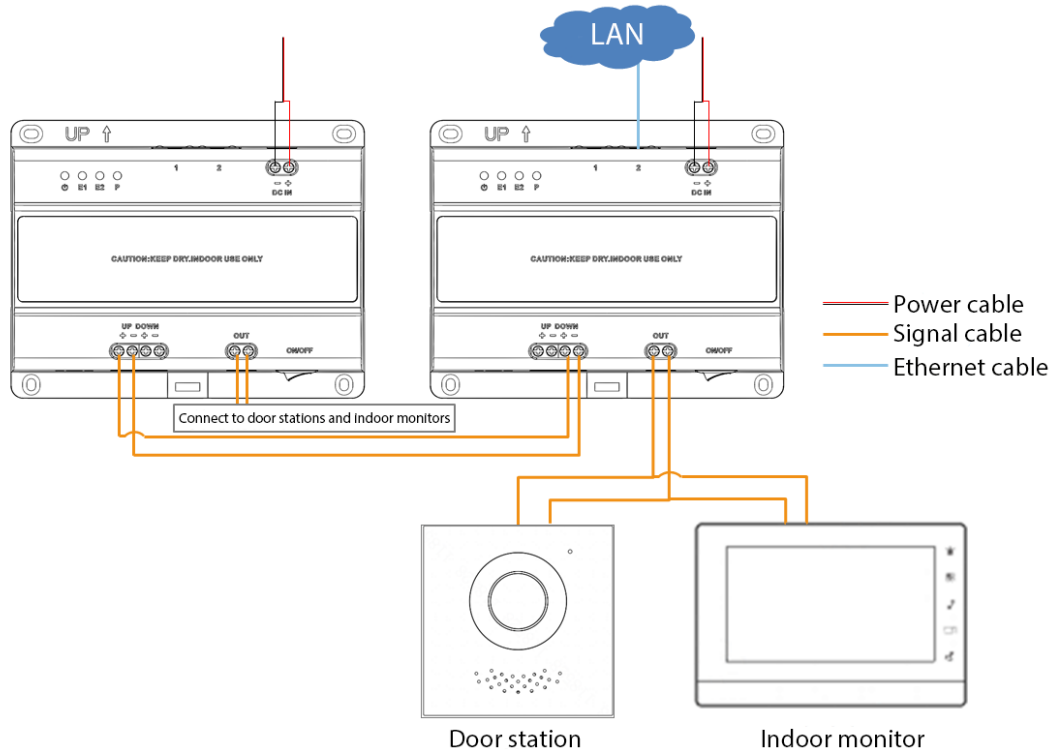
If there are more than 20 VTHs and 2 VTOs, you need more than one switch to connect them all to the network. Use the 2-wire cascading ports or RJ-45 ports to connect the switches as needed, and

make sure that all the switches are connected to the same network. Take cascading with the 2-wire cascading ports as an example.



The cable connection of cascading with RJ-45 ports is the same as villa.

Figure 1-2 Apartment network diagram with 2-wire cascading ports



See the instruction below when choosing the right signal cables for the amount of devices you have:

$$R \text{ (total resistance)} = 6V / \text{the number of VTHs} / 0.1A \text{ (the average current for each VTH)}$$

For example, the total resistance of the cables for 5 VTHs must be less than $6V / 5 / 0.1A = 12\Omega$.

Table 1-1 Description of using different cables

Cable Type for Cascading	Supported Quantity	Device	Maximum Distance
2-core cable	20 VTHs and 2 VTOs.		50 m:
4-core cable			<ul style="list-style-type: none"> Between two switches. Between one switch and one VTH/VTO.
Ethernet cable	12 VTHs and 2 VTOs.		<ul style="list-style-type: none"> 50 m. Between two switches. 30 m. Between one switch and one VTH/VTO. <p>Because each core in an Ethernet cable has a relatively large impedance, we recommend that the cable should not be longer than 30 m.</p>



- The cable between 1 switch and one VTO/VTH must be longer than 1 m.
- When using multiple switches, make sure that each switch is at least 3 m from the other ones.

2 Structure

2.1 Front Panel

Figure 2-1 Front panel structure

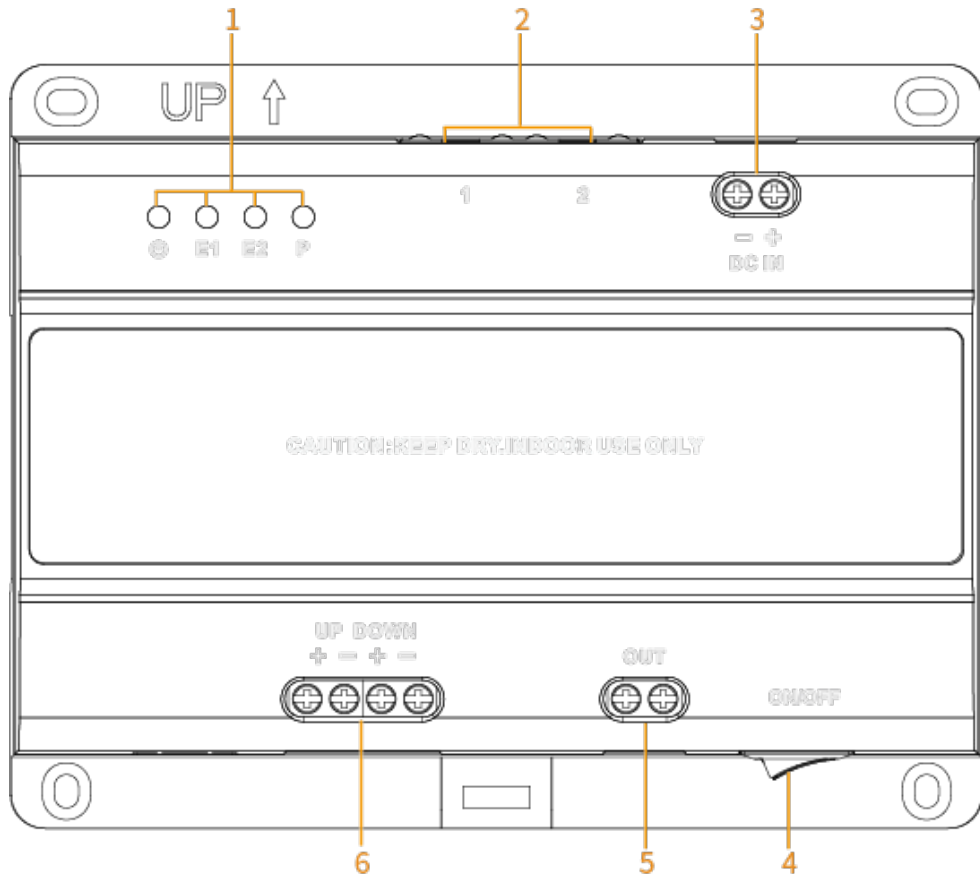



Table 2-1 Structure description

No.	Item	Description
1	Indicator	<p>From left to right:</p> <ul style="list-style-type: none"> ● POWER. <ul style="list-style-type: none"> ◇ Red: Powered on. ◇ Off: No power. ● E1. <ul style="list-style-type: none"> ◇ Green flashes: The device is properly connected to uplink port. ◇ Solid green: No signal from the uplink port. ◇ Off: The device is powered off or malfunctioning. ● E2. <ul style="list-style-type: none"> ◇ Green flashes: The device is properly connected to downlink port. ◇ Solid green: No signal from the downlink port. ◇ Off: The device is powered off or malfunctioning. ● P. <ul style="list-style-type: none"> ◇ Green flashes: Received PLC signal that either the VTH or VTO that is properly connected to the switch. ◇ Solid green: All VTHs and VTOs are not properly connected. ◇ Off: The devices are powered off or malfunctioning.

No.	Item	Description
2	Network	2 RJ-45 ports.
3	Power input	Use 48V DC power supply.
4	OFF/ON	Power switch.
5	2-wire ports	Connect up to 20 VTHs and 2 VTOs with no positive or negative poles.
6	Uplink and downlink ports	<ul style="list-style-type: none"> • UP. Connect the positive pole to that of the downlink port of the previous switch, and the same for the negative pole. • DOWN. Connect the positive pole to that of the uplink port of the subsequent switch, and the same for the negative pole.  <p>Under certain conditions, these two ports can be connected to the EOC port of a VTO, and you also need to connect the two positive poles together and the same for the negative poles.</p>



Before connecting cables, power off the switch first to avoid damaging it.

2.2 Rear Panel

Figure 2-2 Rear panel structure

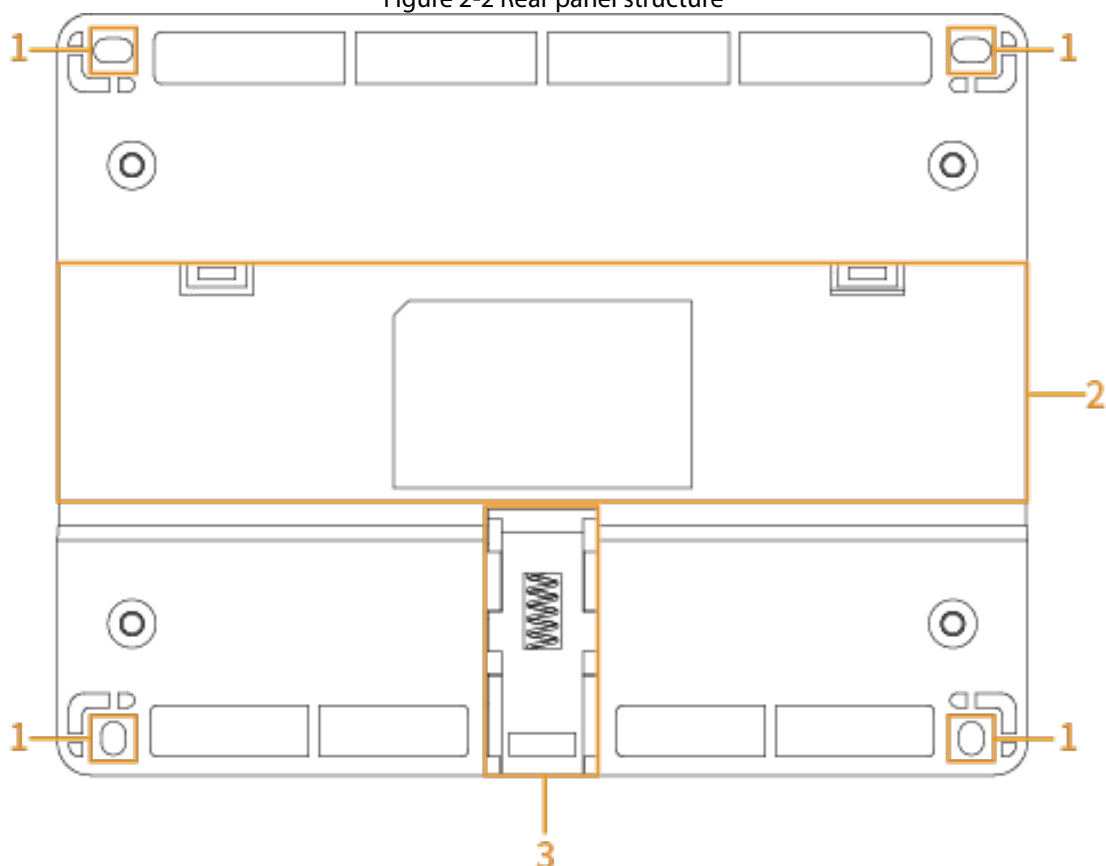


Table 2-2 Structure description

No.	Item	Description
1	Screw holes	Use four ST3 × 18-SUS to install the switch. See "4.1 Installing with Screws".
2	Rail	Use a guide rail to install the switch. See "4.2 Installing with Slide Rail".
3	Lower hook	Fix the switch when installing with a guide rail.

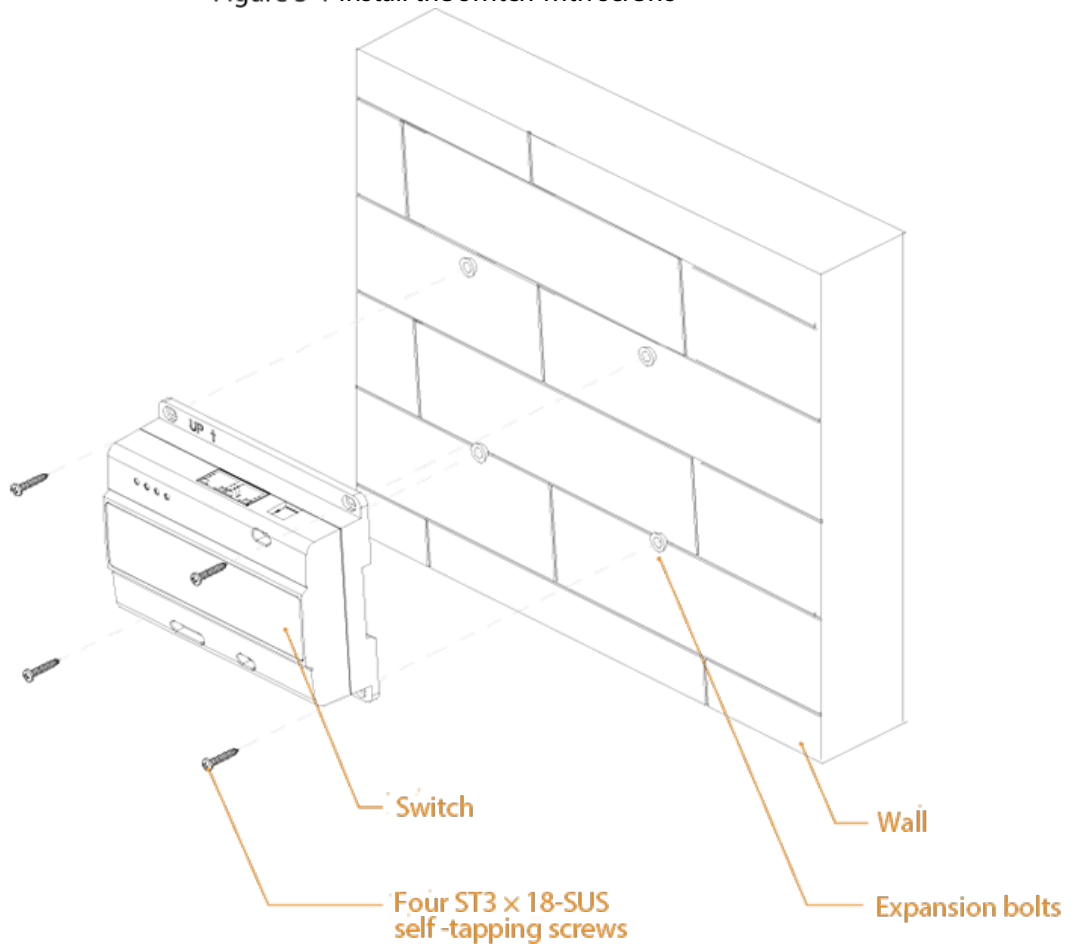
3 Installation

The chapter introduces how to install the switch on the wall with screws or a guide rail.

3.1 Installing with Screws

Use screws to fix the switch at a proper location on the wall.

Figure 3-1 Install the switch with screws



3.2 Installing with a Guide Rail

Preparation

Prepare a standard 35 mm guide rail.

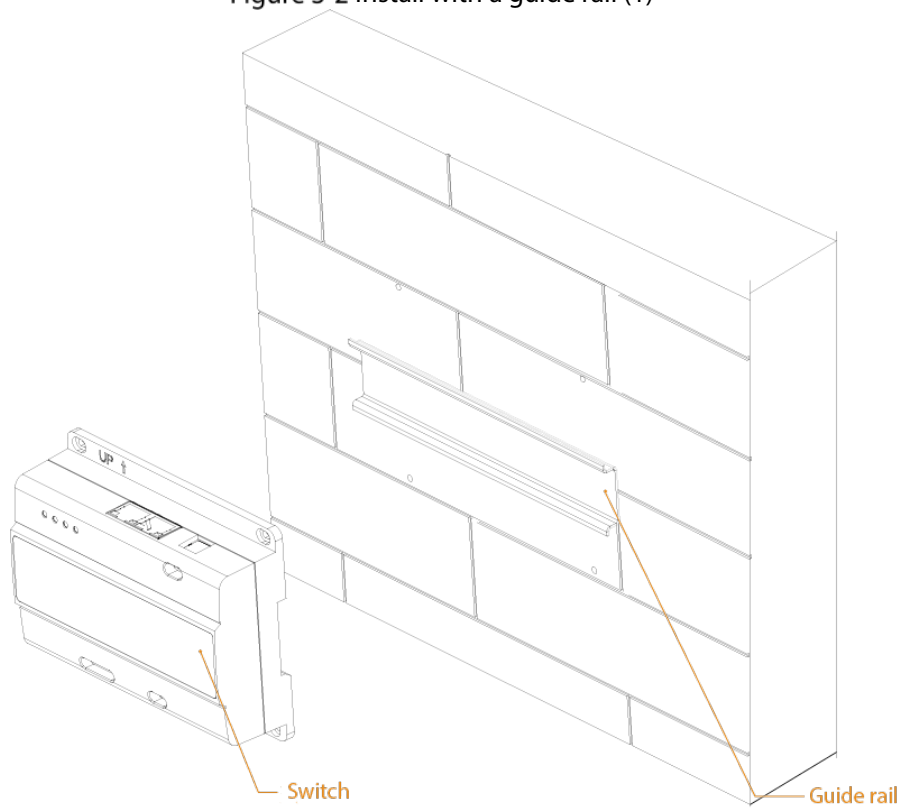


The switch does not come with a guide rail.

Procedure

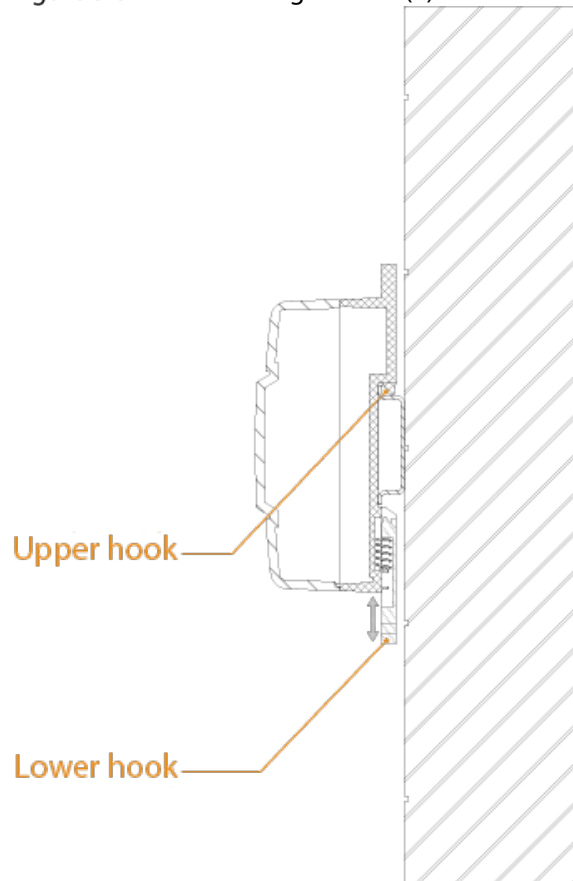
Step 1 Fix the guide rail at a proper location on the wall.

Figure 3-2 Install with a guide rail (1)



- Step 2** Fix the upper hooks inside the slot of the guide rail.
- Step 3** Pull down the lower hook and press the switch close to the guide rail.
- Step 4** Let go of the lower hook.

Figure 3-3 Install with a guide rail (2)



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

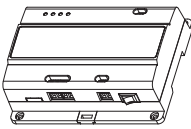
Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

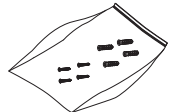
13. Construct a Safe Network Environment

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

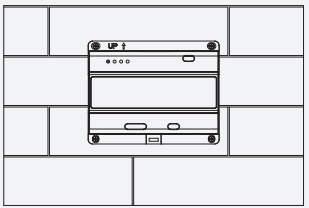
- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, 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.

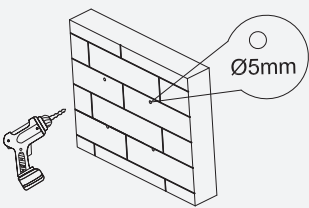


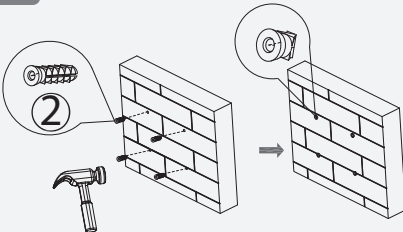
①  × 1

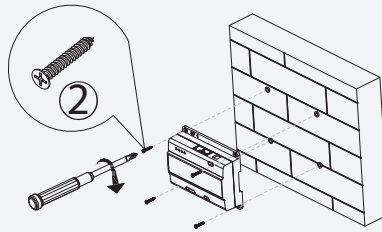
②  × 2

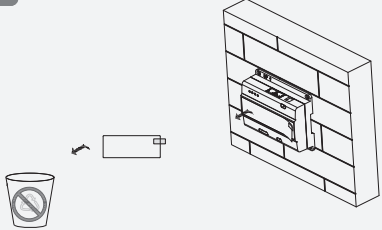
A

1.1 

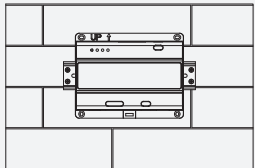


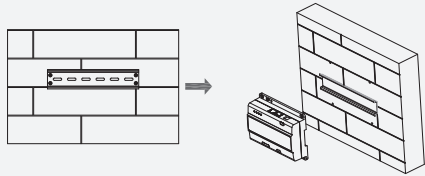
1.2 

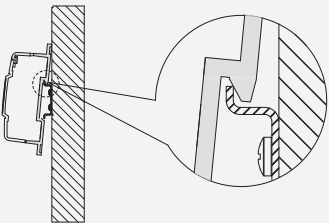
1.3 

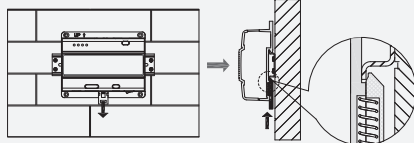
1.4 

B



2.1 

2.2 

2.3 

2.4 