

Digital VTH (Version 4.2)

Quick Start Guide








Foreword

General

This document mainly introduces the structure, installation and commissioning 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.	September 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 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 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 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

- Use recommended power cables in the region under their rated specification.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, 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 Structure	1
1.1 Front Panel.....	1
1.2 Rear Panel Port	2
1.2.1 VTH5221 Series /VTH5241 Series	2
1.2.2 VTH5221E-H/VTH5221EW-H	2
1.2.3 VTH15XX-S2 Series B/CH & VTH15XX Series B/CH.....	2
1.2.4 VTH5222CH/VTH5222CHW-2	3
1.2.5 VTH1660CH	4
1.2.6 VTH2221A/VTH2221A-S2.....	4
1.2.7 VTH2421FB/VTH2421FS.....	5
2 Installation and Commissioning	6
2.1 Installation	6
2.1.1 Wall-mounted	6
2.1.2 Installation with 86 Box	6
2.1.3 Desktop Installation with Bracket	7
2.2 Preparations.....	8
2.2.1 VTO Settings.....	8
2.2.2 VTH Settings.....	12
2.3 Commissioning.....	17
2.3.1 VTO Calls VTH.....	17
2.3.2 VTH Monitors VTO	18
Appendix 1 Cybersecurity Recommendations	20

1 Structure

1.1 Front Panel

Different models of devices may have different front panel dimensions and key types, but keys or indicators with the same name or icon have the same function.

Table 1-1 Front panel description

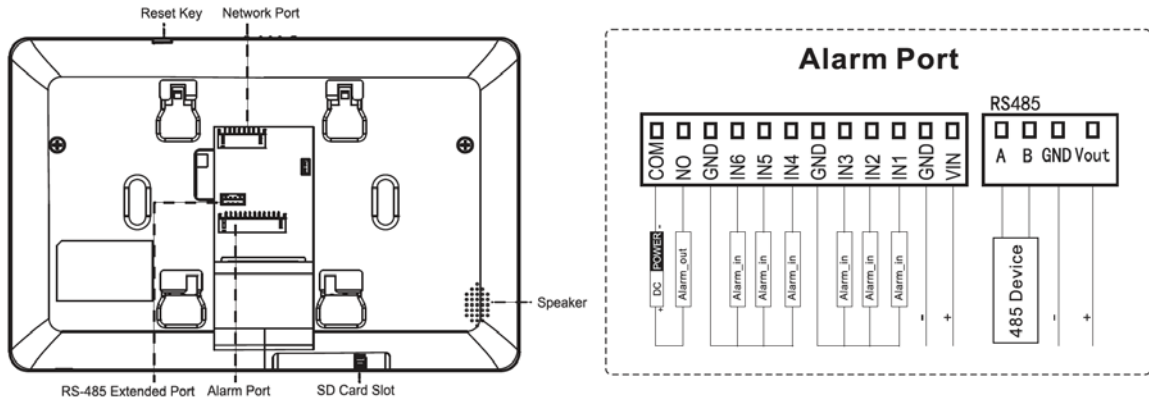
Icon	Name	Description
	SOS	Emergency call.
	Menu	Go to main menu.
	Call	<ul style="list-style-type: none"> ● Answer call. ● During call, press to hang up. ● During monitoring, press to speak to unit VTO, villa VTO, fence station and verifying VTO. ● During speaking, press to exit speaking.
	Monitor	<ul style="list-style-type: none"> ● In standby mode, press to monitor the main VTO. ● During monitoring, press to exit monitoring.
	Unlock	When calling, talking, monitoring and speaking to VTO, press to unlock corresponding VTO.
	Message	If it is on, there are unread messages.
	Power	If it is green, power supply is normal.
Network	Network	<ul style="list-style-type: none"> ● If it is on, communication with VTO is normal. ● If it is off, you cannot speak to VTO.
DND	DND	<p>If it turns green, DND function is enabled.</p>  <p>Refer to the user manual for DND settings by scanning the QR code on the front cover.</p>

1.2 Rear Panel Port

1.2.1 VTH5221 Series /VTH5241 Series

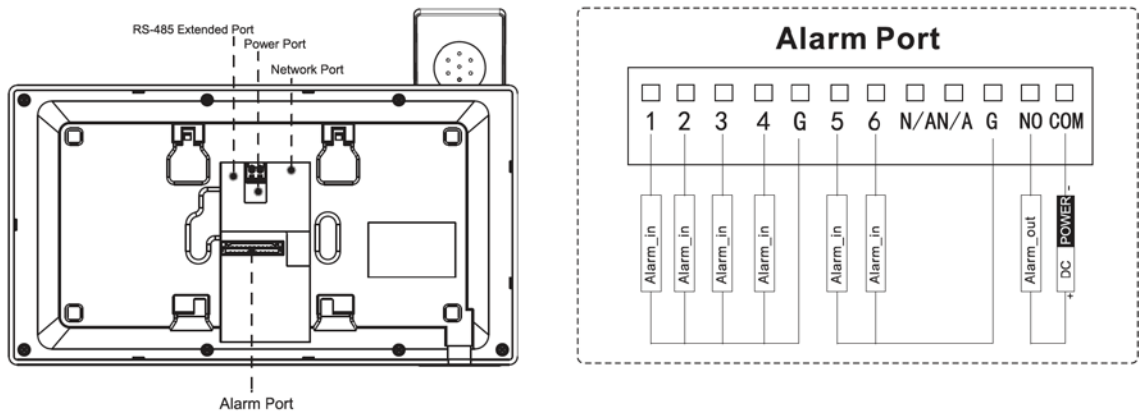
Port positions at the rear panel may differ. Take VTH5221 as an example.

Figure 1-1 Rear panel of VTH5221



1.2.2 VTH5221E-H/VTH5221EW-H

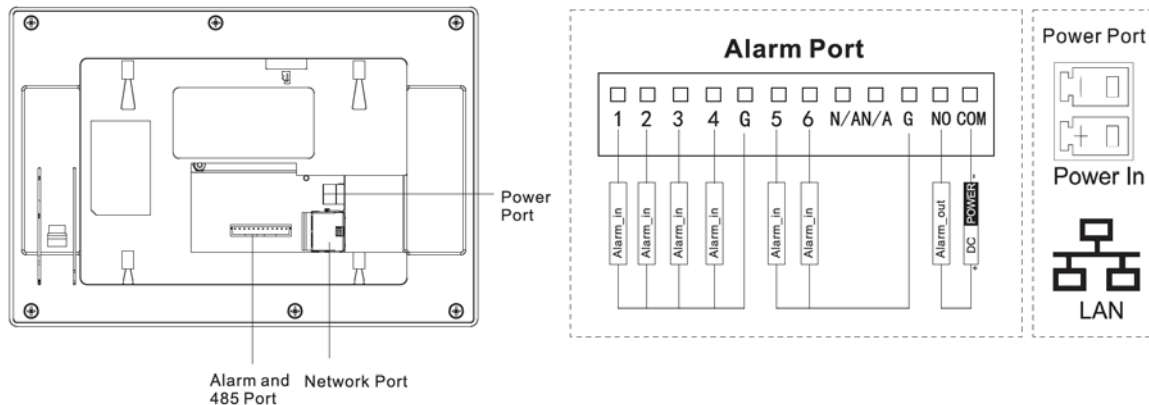
Figure 1-2 Rear panel of VTH5221E-H/VTH5221EW-H



1.2.3 VTH15XX-S2 Series B/CH & VTH15XX Series B/CH

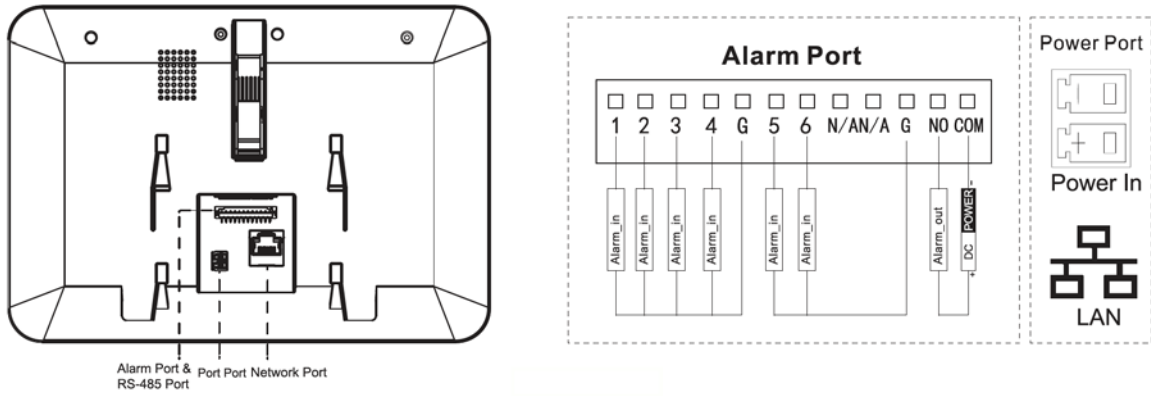
For VTH15XX-S2 CH series, port positions may differ. Take VTH150CH-S2 as an example.

Figure 1-3 Rear panel of VTH150CH-S2



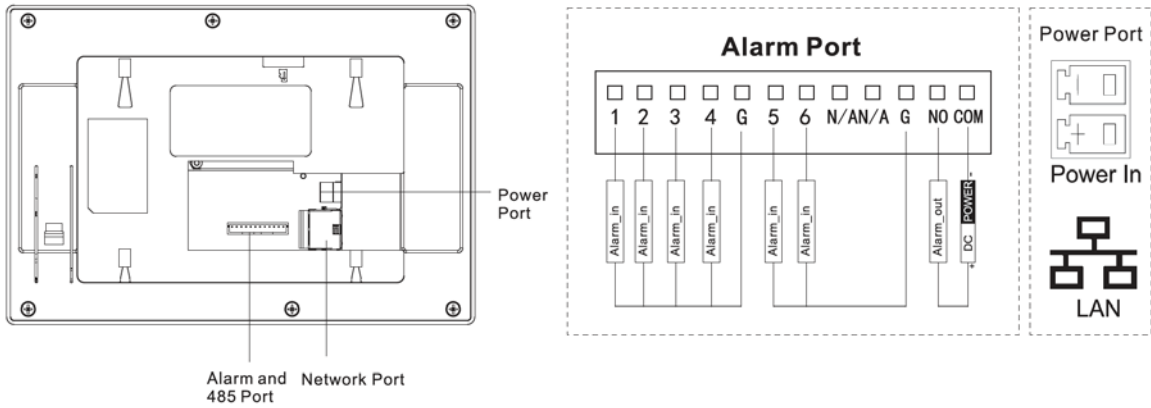
For VTH15XX-S2 B series, port positions may differ. Take VTH1560B-S2 as an example.

Figure 1-4 Rear panel of VTH1560B-S2



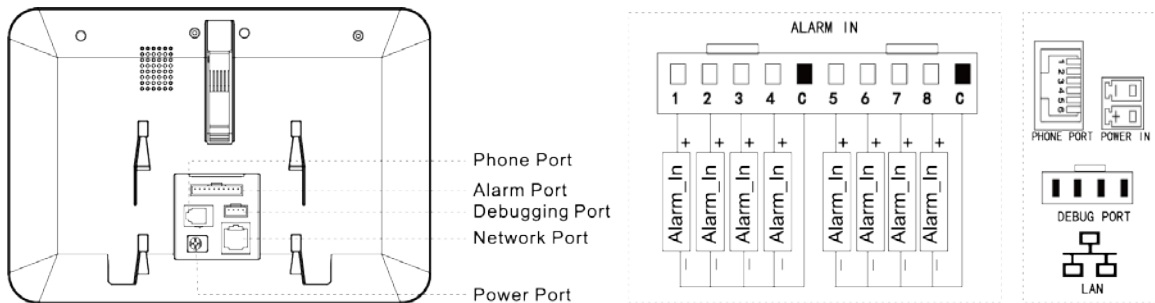
For VTH15XX CH series, port positions may differ, Take VTH1550CH as an example.

Figure 1-5 Rear panel of VTH1550CH



For VTH15XX B series, port positions may differ. Take VTH1560B as an example.

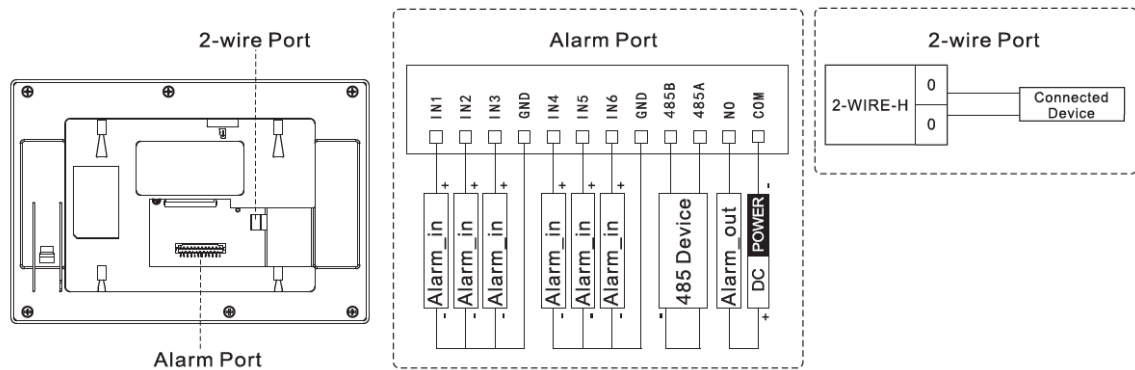
Rear panel of VTH1560B



1.2.4 VTH5222CH/VTH5222CHW-2

VTH5222CH has 1 group of 2-wire port, and VTH1550CHW-2 has 3 groups of 2-wire port.

Figure 1-6 Rear panel of VTH5222CH

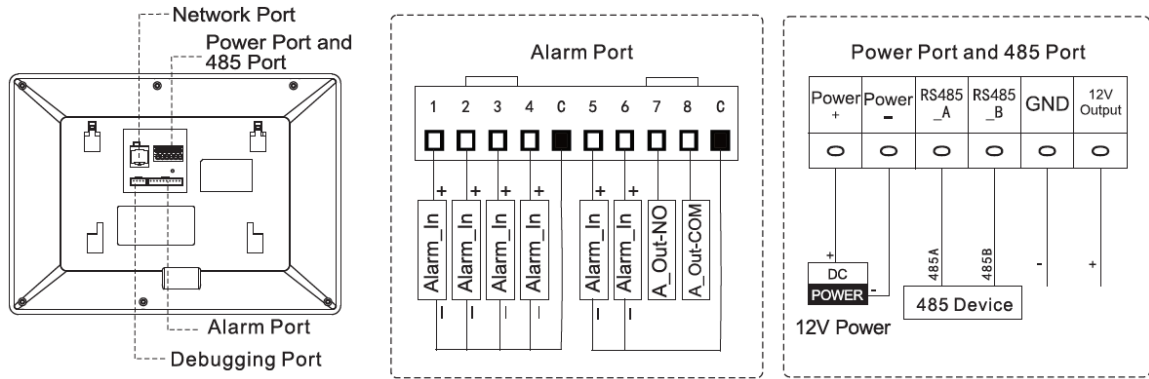




- Provide 1 group of 2-wire port to connect to 2-wire VTHs, VTOs, and networking control and DC power devices. Power devices are connected irrespective of positive and negative poles.
- Every group of ports can connect to multiple devices in parallel, but 3 groups support connecting to 5 devices at most.

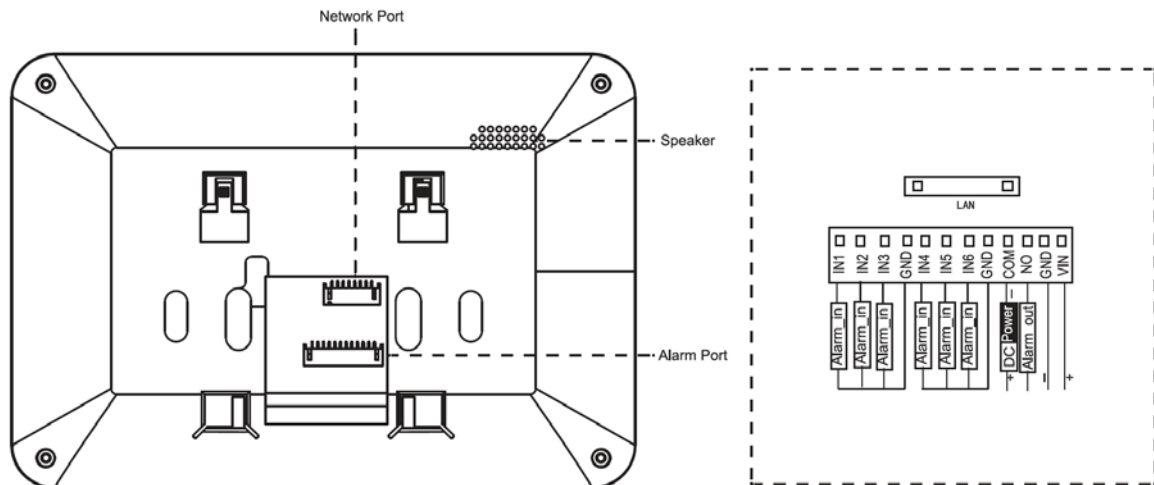
1.2.5 VTH1660CH

Figure 1-7 Rear panel of VTH1660CH



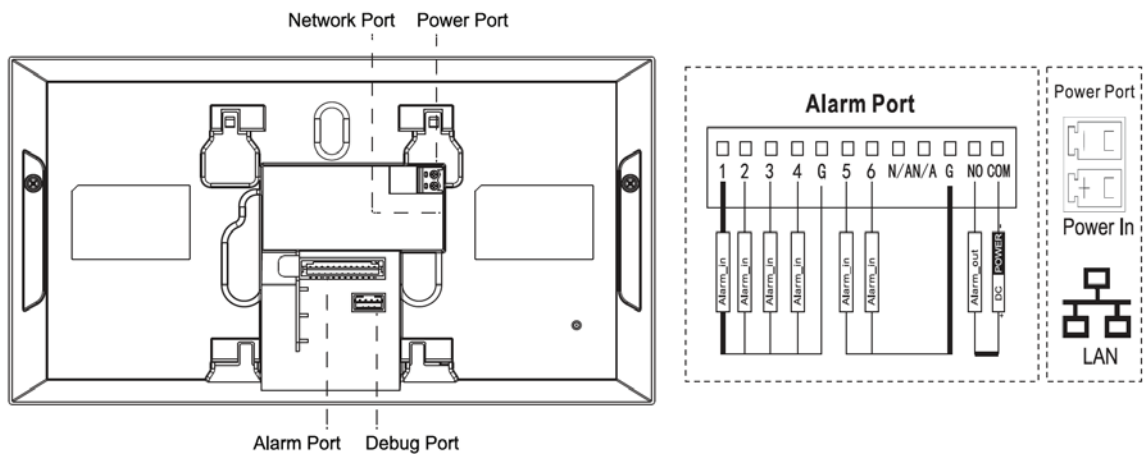
1.2.6 VTH2221A/VTH2221A-S2

Figure 1-8 Rear panel of VTH2221A/VTH2221A-S2



1.2.7 VTH2421FB/VTH2421FS

Figure 1-9 Rear panel of VTH2421FB/VTH2421FS



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 immediately. 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 technical support.
- Device central point height should be 1.4 m–1.6 m above the ground.

2.1.1 Wall-mounted

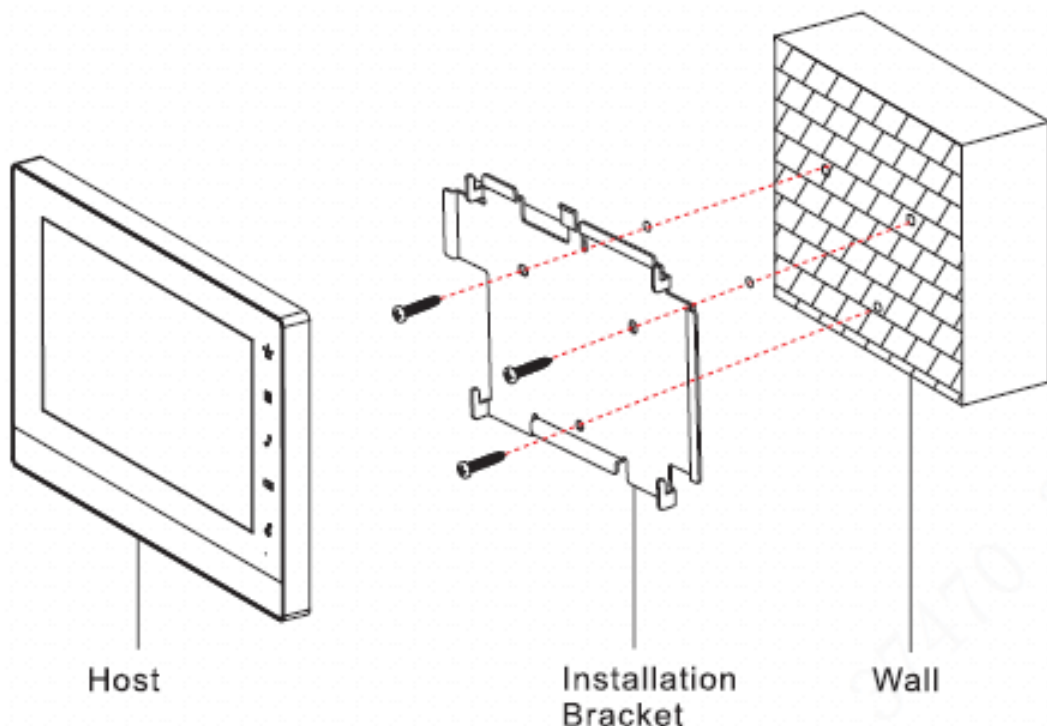
Directly install the device with a bracket on the wall, which is suitable for all types of devices. Take VTH1550CH as an example.

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

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

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

Figure 2-1 Wall-mounted installation



2.1.2 Installation with 86 Box

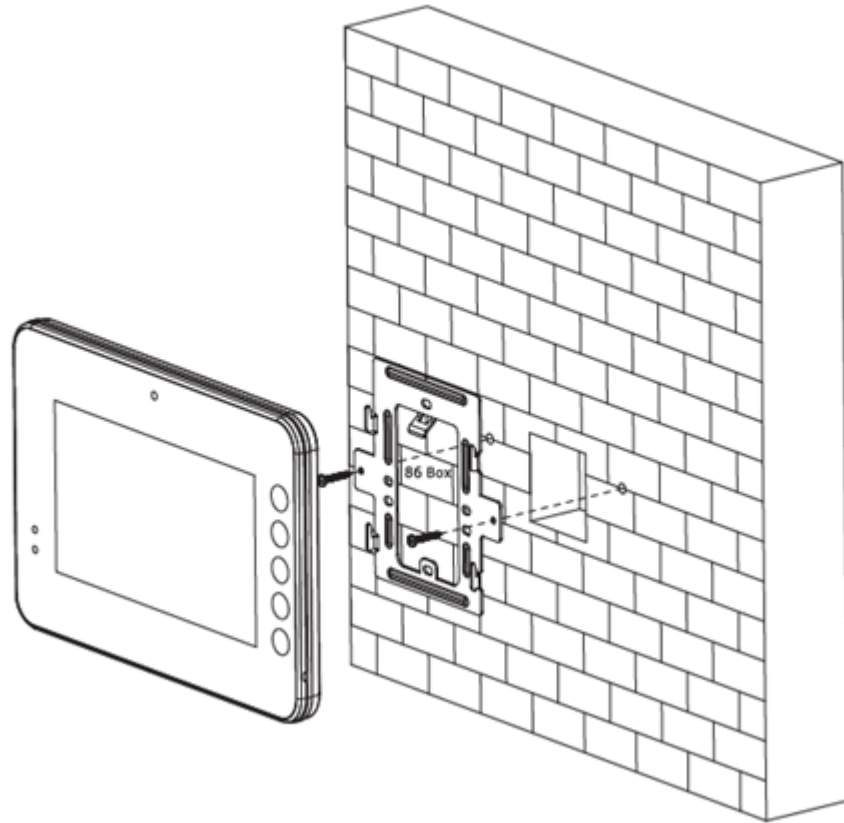
Install the device with 86 box, which is suitable for all types of devices. Take VTH1560B/BW as an example.

Step 1 Embed 86 box into the wall at a proper height.

Step 2 Fix the installation bracket on the 86 box with screws.

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

Figure 2-2 Installation with 86 box



2.1.3 Desktop Installation with Bracket

Install the device with bracket on the desktop, which only applies to handset VTH. Take VTH5221E-H as an example.

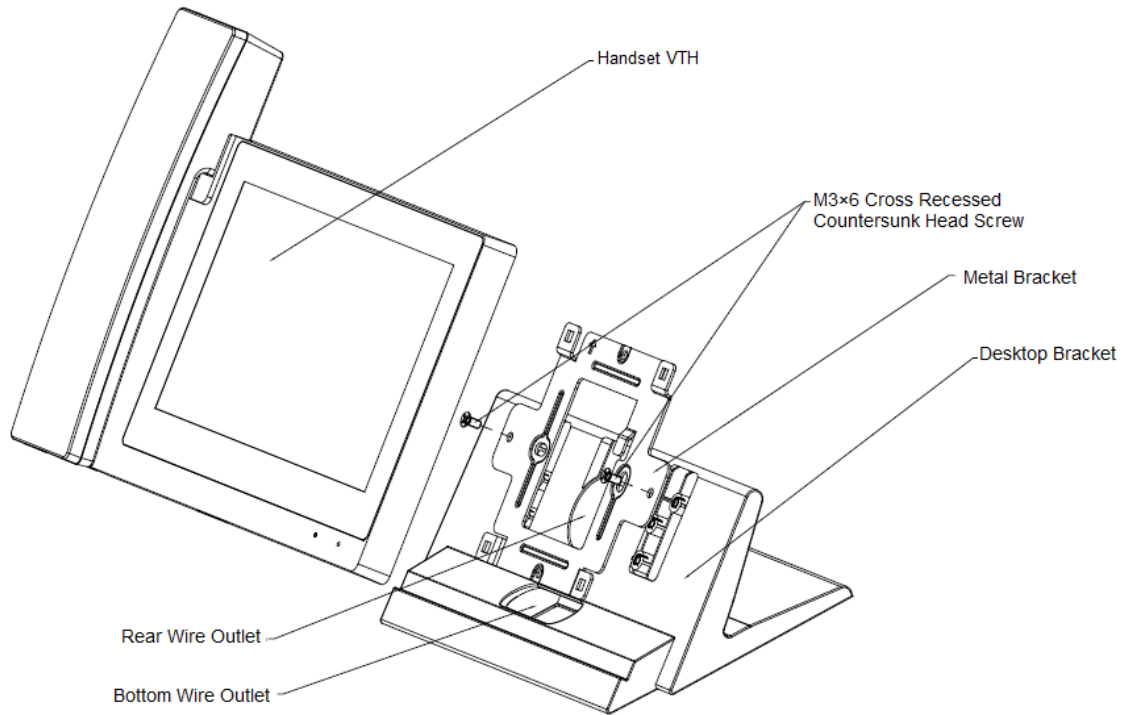
Step 1 With two M3 × 6 cross recessed countersunk head screws, tighten the metal bracket on the top two nuts of the desktop bracket.

Step 2 Connect the wires.

Step 3 Run the wires through outlet in the rear or at the bottom of the desktop bracket.

Step 4 Install the handset VTH in the slot at the top of the metal bracket.

Figure 2-3 Desktop installation with brackets



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.

2.2.1 VTO Settings

VTO interface may differ for different models and the actual interface shall prevail.

For first time use, initialize and change login password.



Make sure that the default IP addresses of PC and VTO are in the same network segment. The default IP address of VTO is 192.168.1.110.

Step 1 Power on the device, and then go to the default IP address of VTO in the browser.

Figure 2-4 Device initialization

Device Init

1 — 2 — 3
One — Two — Three

Username admin

Password

Low Middle High

Confirm Password

Next

Step 2 Enter password and confirm it, and then click **Next**. Select **Email** and enter email address for resetting password.

Step 3 Enter the default address in the browser to log in to WEB interface.



The default username is admin, and the password is the one set just now.

Step 4 Select **Network Setting > Basic**.

Figure 2-5 TCP/IP

WEB SERVICE 2.0 Local Setting Household Setting **Network Setting** Log Management

Basic

FTP

SIP Server

Active Reg.

IP Permissions

TCP/IP

IP Addr.

MAC Addr.

Subnet Mask

Gateway

Preferred DNS

Alternate DNS

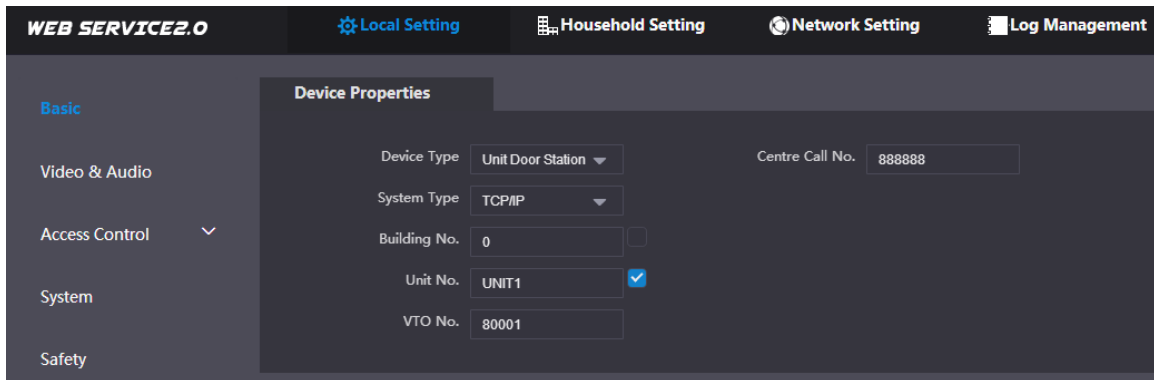
Step 5 Enter IP address, subnet mask and gateway, and then click **OK**.

The VTO will restart automatically, and:

- If PC is in the same network segment, WEB interface jumps to the login interface.
- If PC is not in the same network segment, you cannot access the new IP address. Add PC to the same network segment and try again.

Step 6 Log in to WEB interface again and select **Local Setting > Basic**.

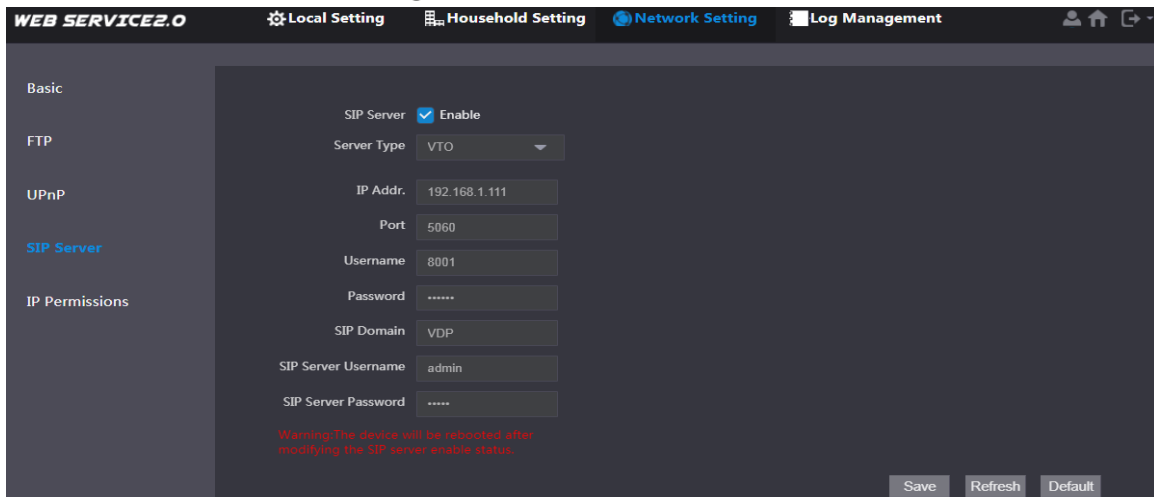
Figure 2-6 Device properties



- 1) Select **System Type** as TCP/IP.
- 2) Click **OK**.
- 3) Restart the device manually or wait for it to automatically restart.

Step 7 Log in to WEB interface, and then select **Network Setting > SIP Server**.

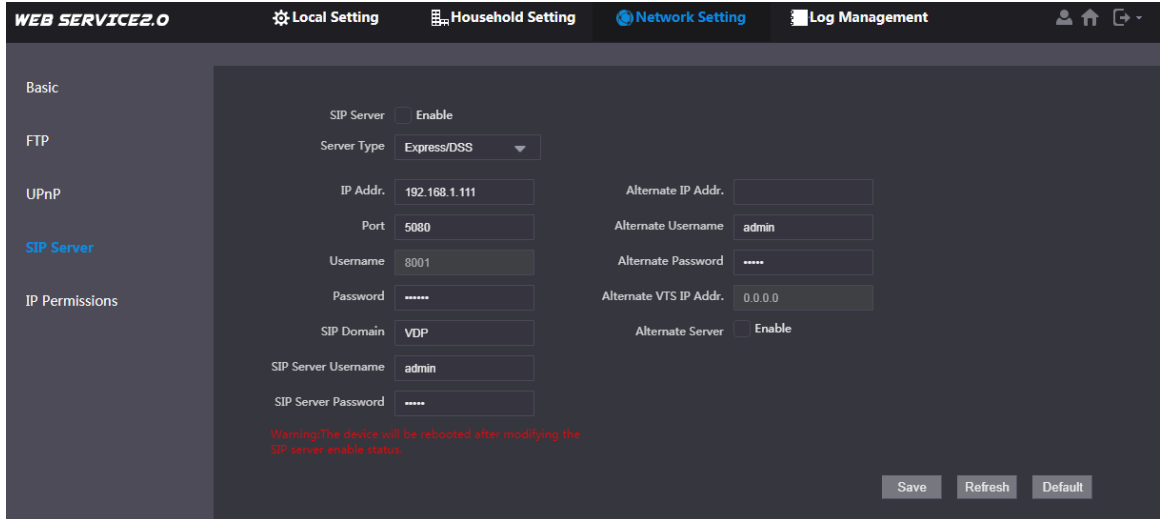
Figure 2-7 SIP server (1)



- 1) Select server type.
 - When VTO works as the SIP server, select **Server Type** as **VTO**. It applies to one building or unit.
 - When the platform (Express/DSS) works as the SIP server, select **Server Type** as **Express/DSS**. It applies to multiple buildings or units.
- 2) Set VTO number and click **Save**.
 - When the platform works as the SIP server, enable **Support Building** and **Support Unit** as needed and configure accordingly.
 - After VTO is set as the SIP server, group call function will appear at the interface. Enable it as needed.

Step 8 Select **Network Setting > SIP Server**.

Figure 2-8 SIP server (2)



- The current VTO works as the SIP server. Enable **SIP Server** and click **Save**. The VTO will automatically restart.
- Another VTO or platform works as the SIP server. Configure the parameters and click **Save**. The VTO will automatically restart.

Table 2-1 Parameter description

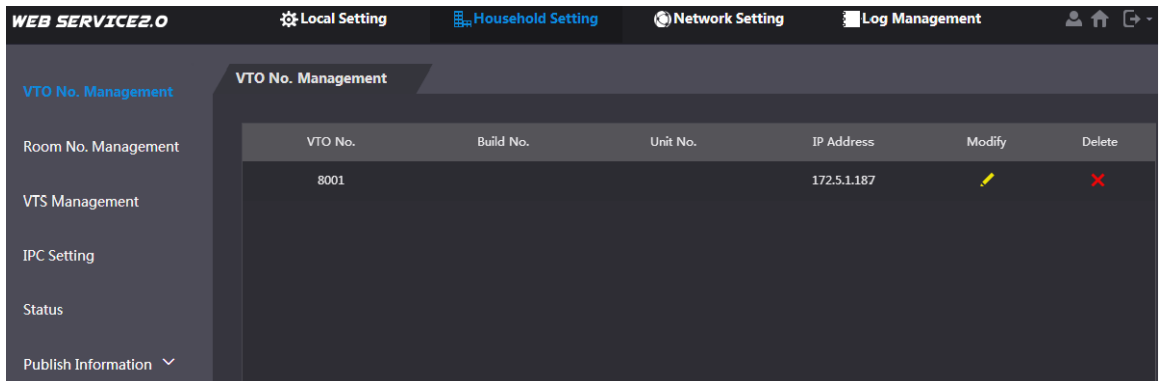
Parameter	Description
IP Addr.	SIP server IP address.
Port	<ul style="list-style-type: none"> • 5060 by default when another VTO works as SIP server. • 5080 by default when platform works as SIP server.
Username/Password	Keep default value.
SIP Domain	<ul style="list-style-type: none"> • Enter VDP when another VTO works as SIP server. • Keep empty or use default value when platform works as SIP server.
Login Username/ Password	Username and password to log in to SIP server.



- VTO settings have been completed when the platform or another VTO works as the SIP server.
- If the current VTO works as the SIP server, go through Step 9 and 10.

Step 9 (Optional) Log in to WEB interface, and then select **Household Setting > VTO No. Management**.

Figure 2-9 VTO No. management



Click **Add**, configure the parameters and click **OK**. Repeat this step to add other VTOs.

Table 2-2 VTO No. management

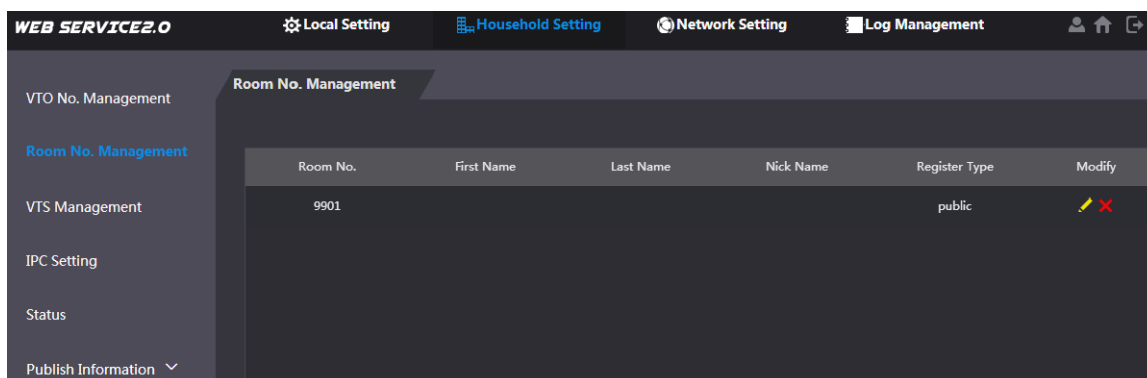
Parameter	Description
VTO No.	VTO number.
Build No.	Number of building where VTO is located.
Unit No.	Number of unit where VTO is located.
IP Address	IP address of VTO.

Step 10 (Optional) Select **Household Setting > Room No. Management**.



Add both when there are master VTH and extension.

Figure 2-10 Room No. management



Click **Add**, configure the parameters and click **OK**. Repeat this step to add other VTHs.

Table 2-3 Room No. management

Parameter	Description
Room No.	<p>Set VTH room number.</p> <ul style="list-style-type: none"> VTH room number consists of 1–6 numbers, letters, or their combinations. It should be the same with room number configured on VTH. See Figure 2-15. When there are master VTH and extensions, end master VTH short no. with #0, and extension VTH short no. with #1, #2 and #3, to achieve group call function. For example, if master VTH is 101#0, extensions should be 101#1, 101#2...
First Name	Set username and nickname for each VTH.
Last Name	
Nick Name	
Register Type	Signaling interactive use in SIP system. Keep the default value.

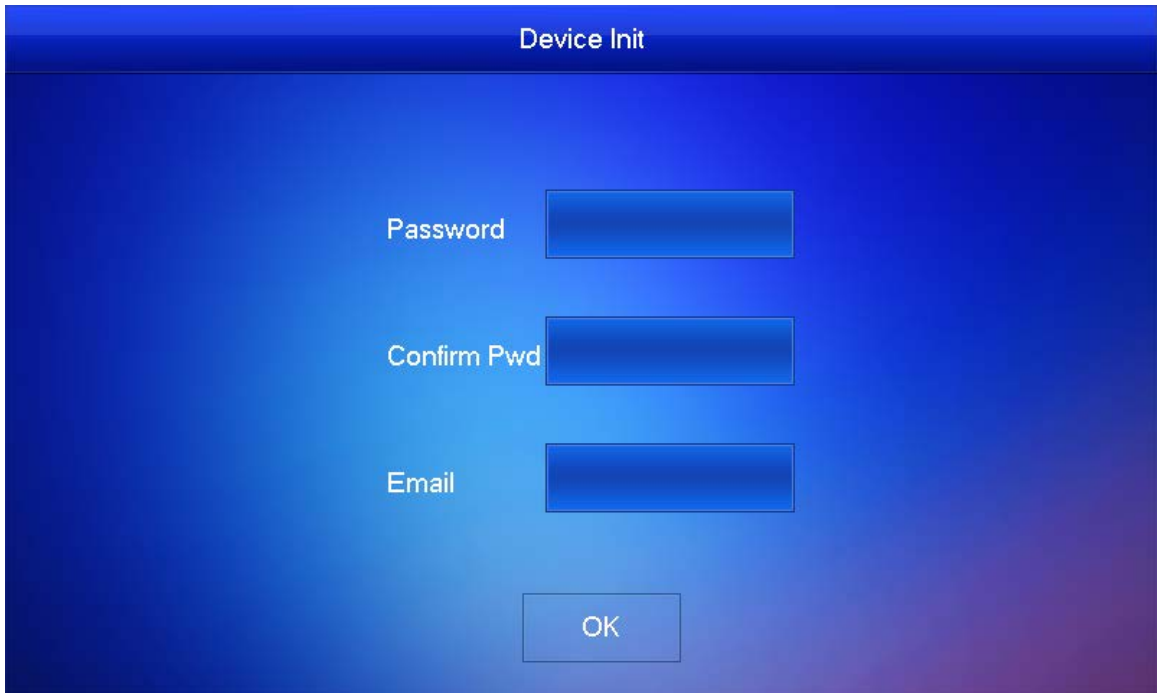
2.2.2 VTH Settings

2.2.2.1 Initialization

For first-time use, set up password and bind email address. 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.

Figure 2-11 Set up password and bind email address



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

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

Step 4 Tap **Network**.



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

Figure 2-12 Network

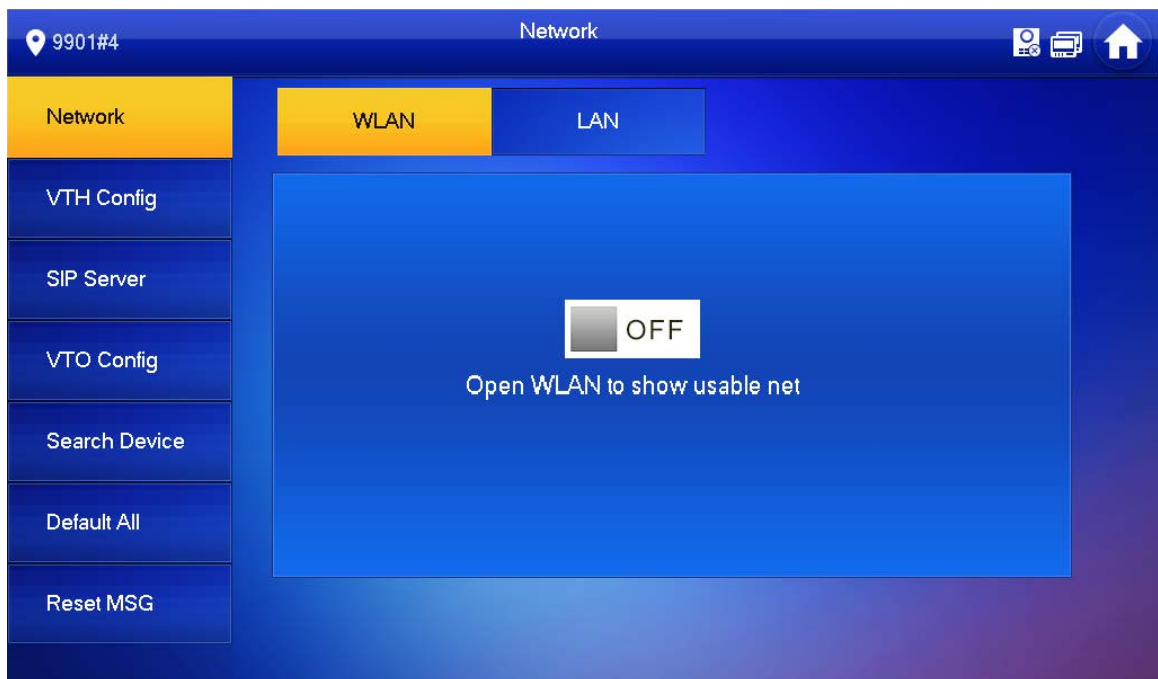
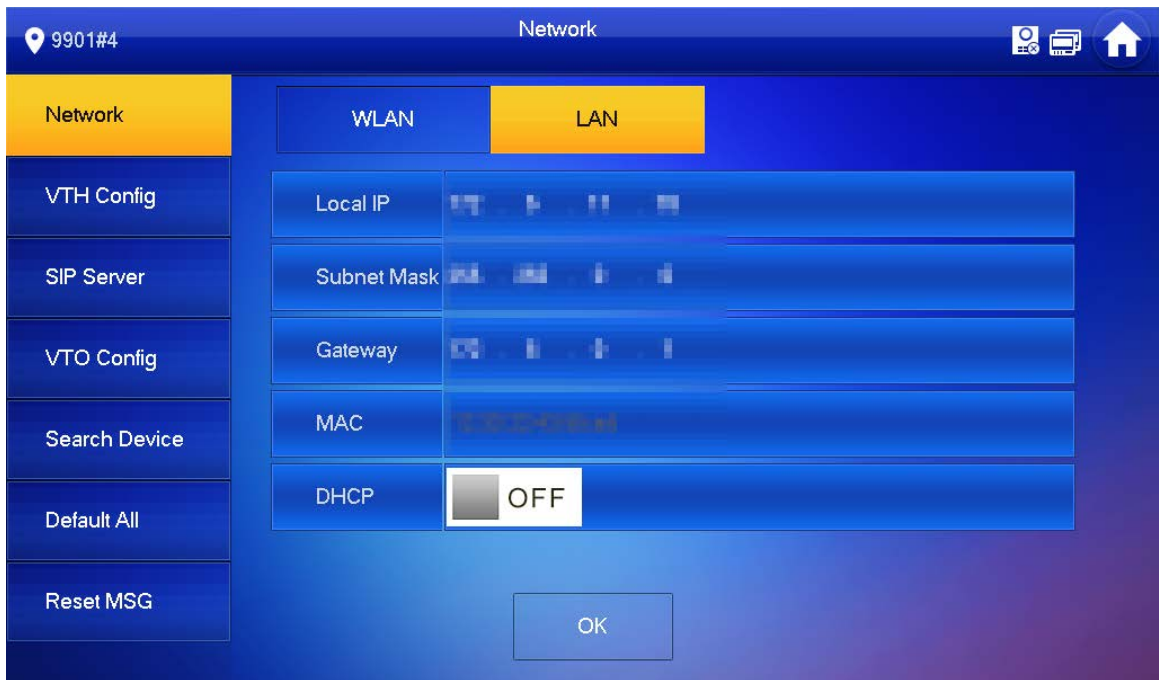


Figure 2-13 LAN



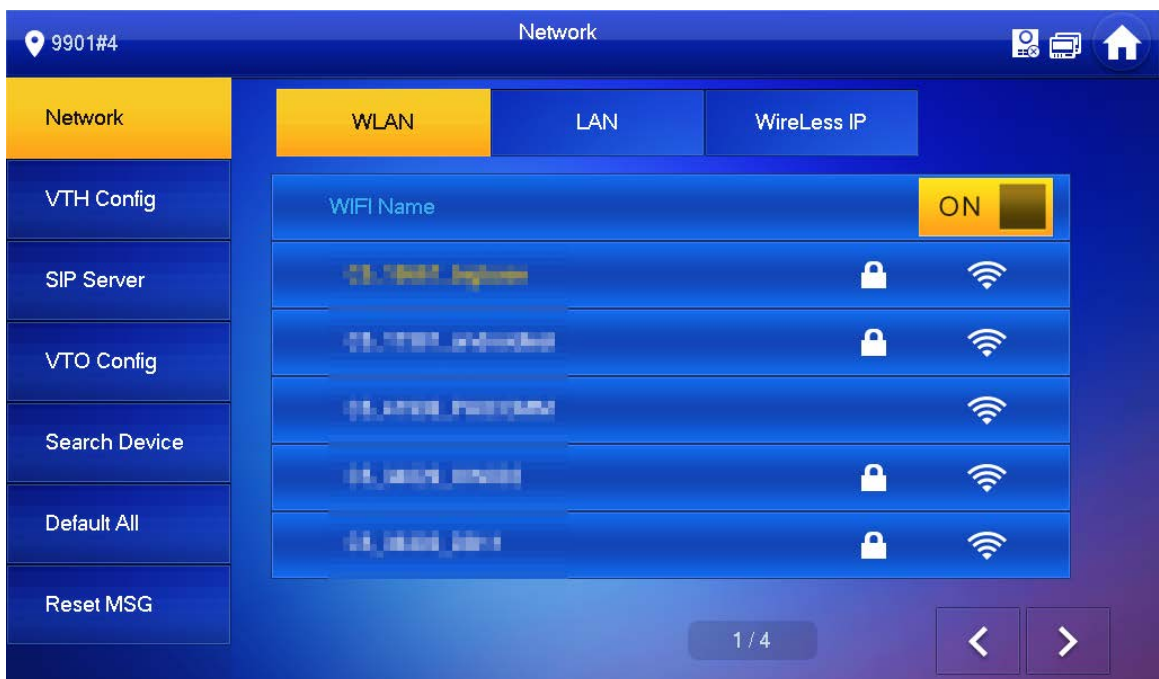
- LAN

Tap **Network** > **LAN**. Enter local IP, subnet mask and gateway, and then tap **OK**. Or tap OFF to enable DHCP function to obtain IP info automatically.

- WLAN

1) Tap **Network** > **WLAN**, and then tap OFF.

Figure 2-14 WLAN



2) Before connecting to a WIFI network, do either of the following first.

- Tap **WireLessIP**, enter local IP, subnet mask and gateway, and then tap **OK**.
- Tap **WireLessIP**, tap OFF to enable DHCP function to obtain IP info automatically.



To enable DHCP function, use a router with DHCP function.

- 3) Connect to a WIFI network.

Step 5 Tap **VTH Config**.

Figure 2-15 VTH configuration

Room No.	9901	Master
Master IP	192.168.1.1	
Master Name	admin	
Master Pwd	*****	
Version	VTH 1.0.0	
SSH	<input type="checkbox"/> OFF	

- Use as a master VTH.

Enter room number (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.

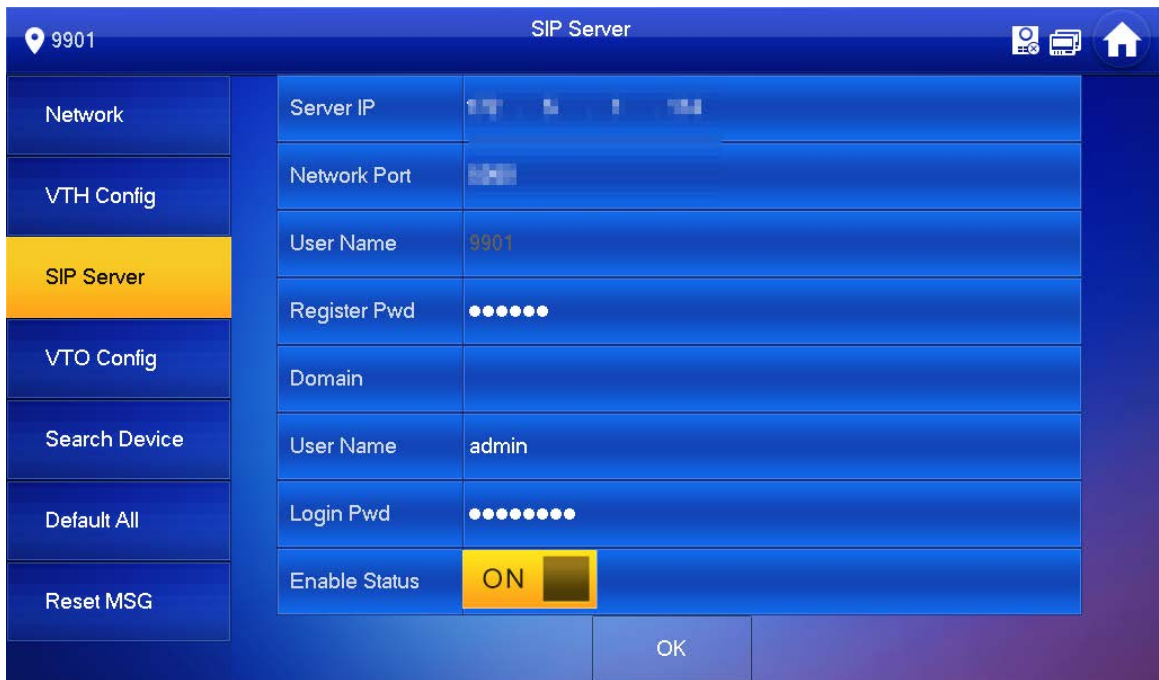
If there is extension VTH, room No. should end with #0. Otherwise, it will fail to connect to VTO.

- Use as an extension VTH.

- 1) Tap **Master** and the icon switches to **Extension**.
- 2) Enter room number (such as 101#1) and the IP address of master VTH.
Master name and password are the username and password of master VTH. Default username is **admin**, and the password is the one set from previous step.
- 3) Tap **OK** to save the settings.

Step 6 Tap **SIP Server**.

Figure 2-16 SIP server



1) Configure parameters of **SIP Server**.

Table 2-4 SIP server

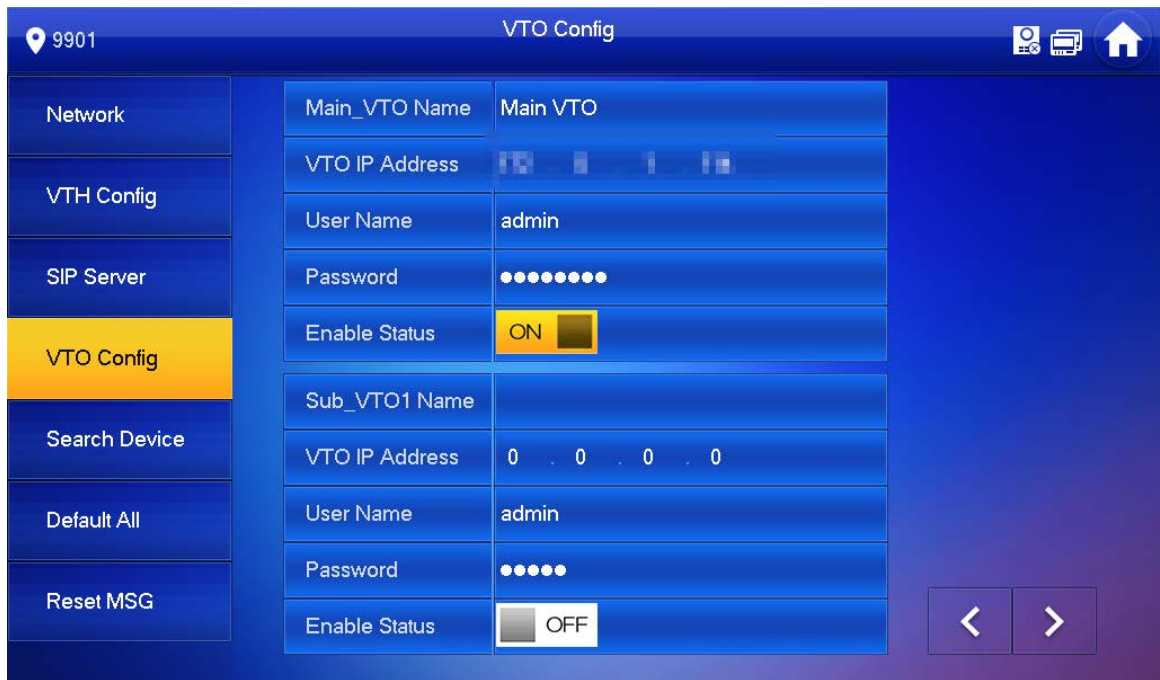
Parameter	Description
Server IP	<ul style="list-style-type: none"> When the platform works as SIP server, server IP is the IP address of the platform. When VTO works as SIP server, server IP is the IP address of the VTO.
Network Port	<ul style="list-style-type: none"> When the platform works as SIP server,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

2) Set **Enable Status** to **ON**.


3) Tap **OK**.

Step 7 Tap **VTO Config**.

Figure 2-17 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 interface 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.



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 2-18 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**, and select the VTO to enter monitoring image.



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 2-19 Door

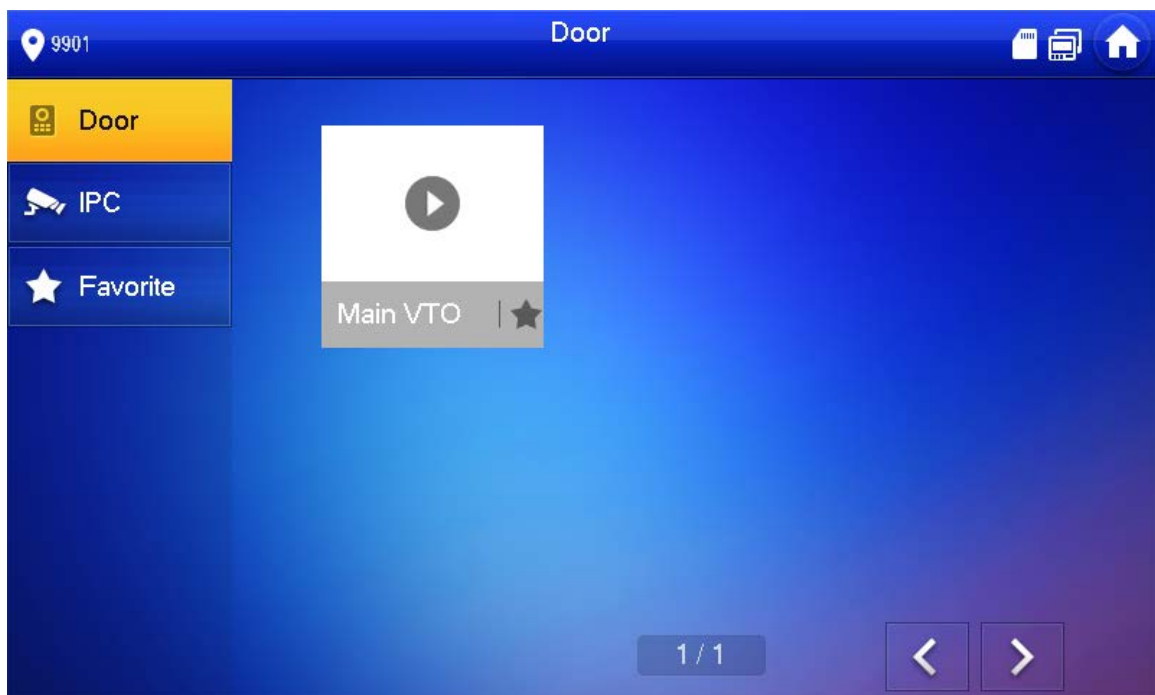
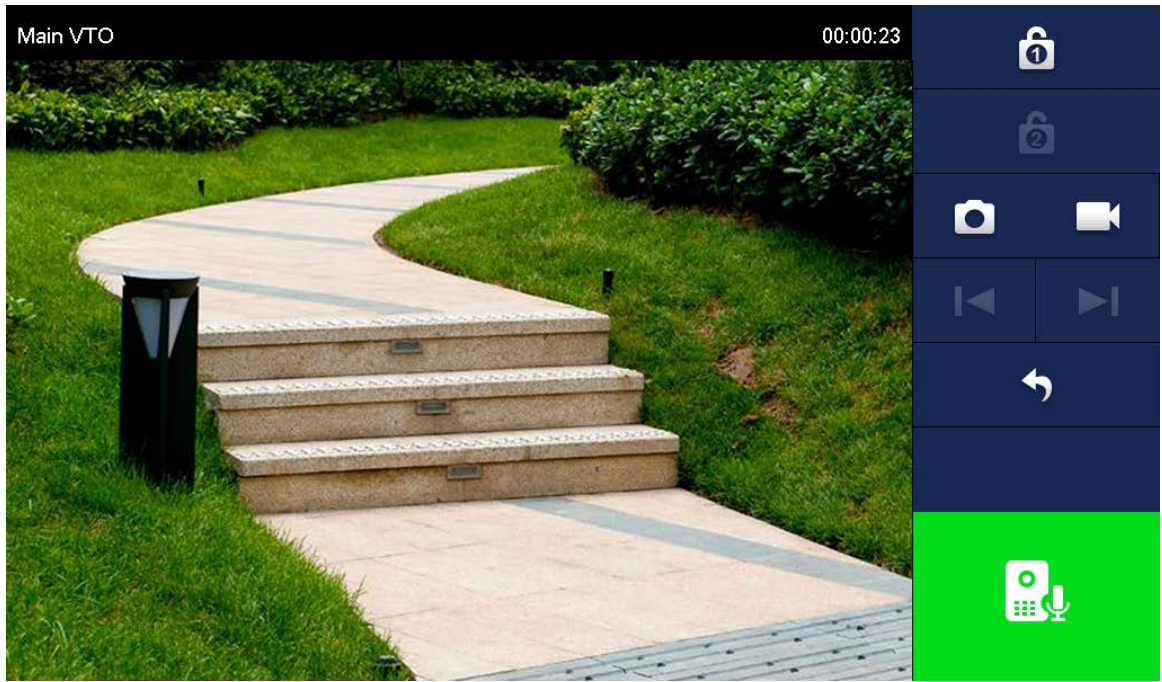


Figure 2-20 Monitoring video



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.

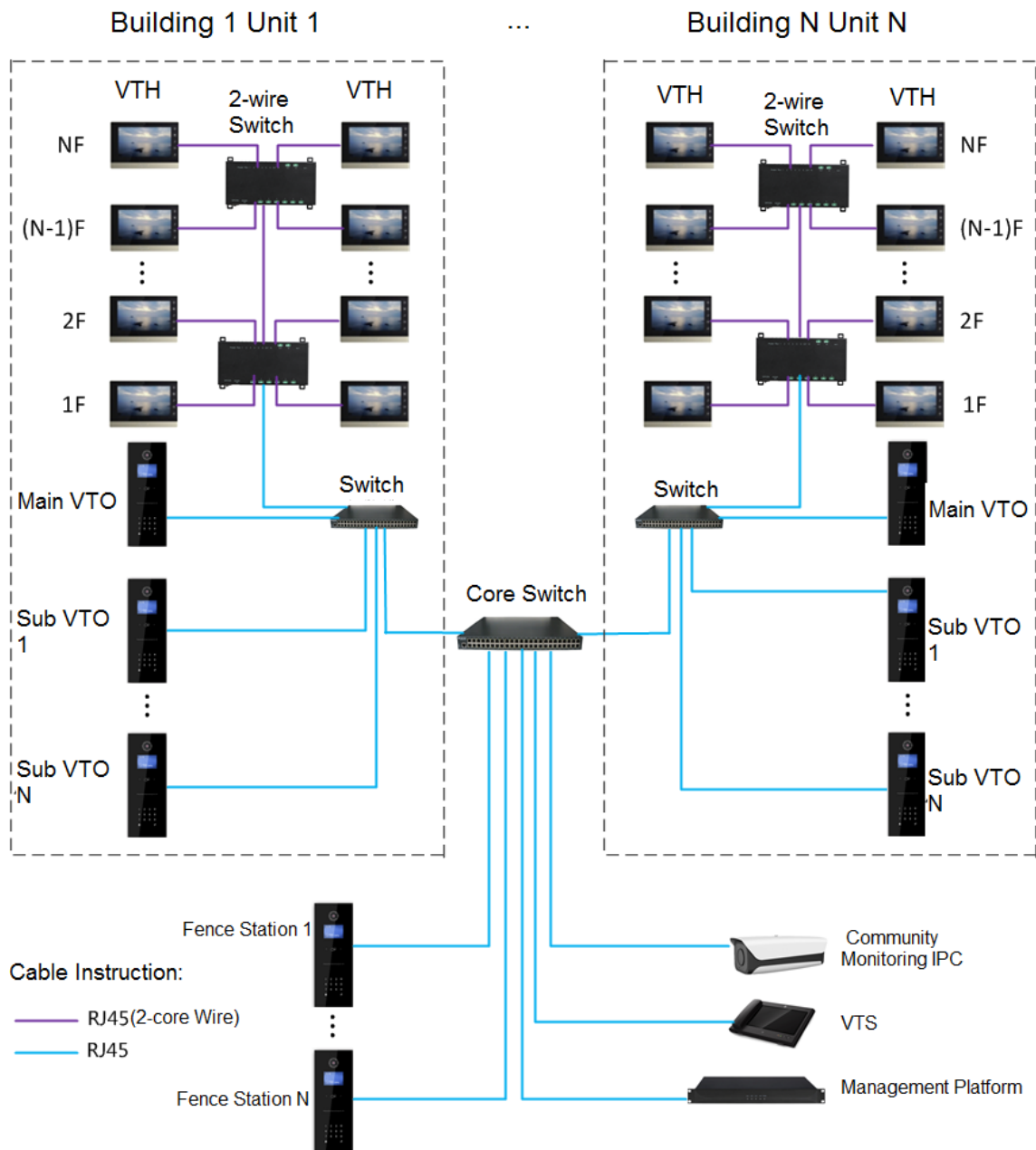
Message

View messages, including videos, pictures and announcements.

2 Network Diagram

2.1 2-wire System

Figure 2-1 Network diagram of 2-wire system

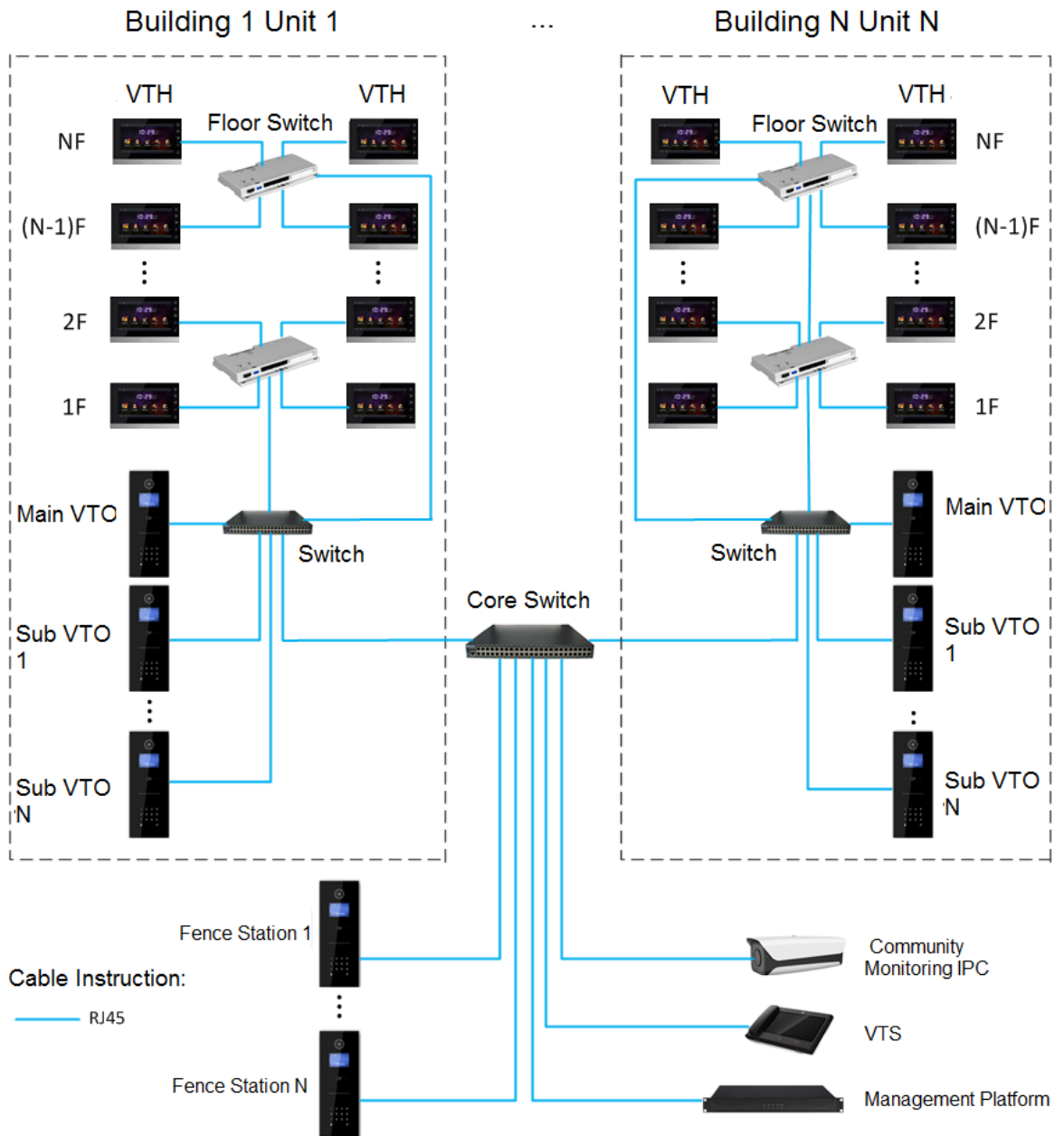


2.2 Digital System

There are two types of digital system network:

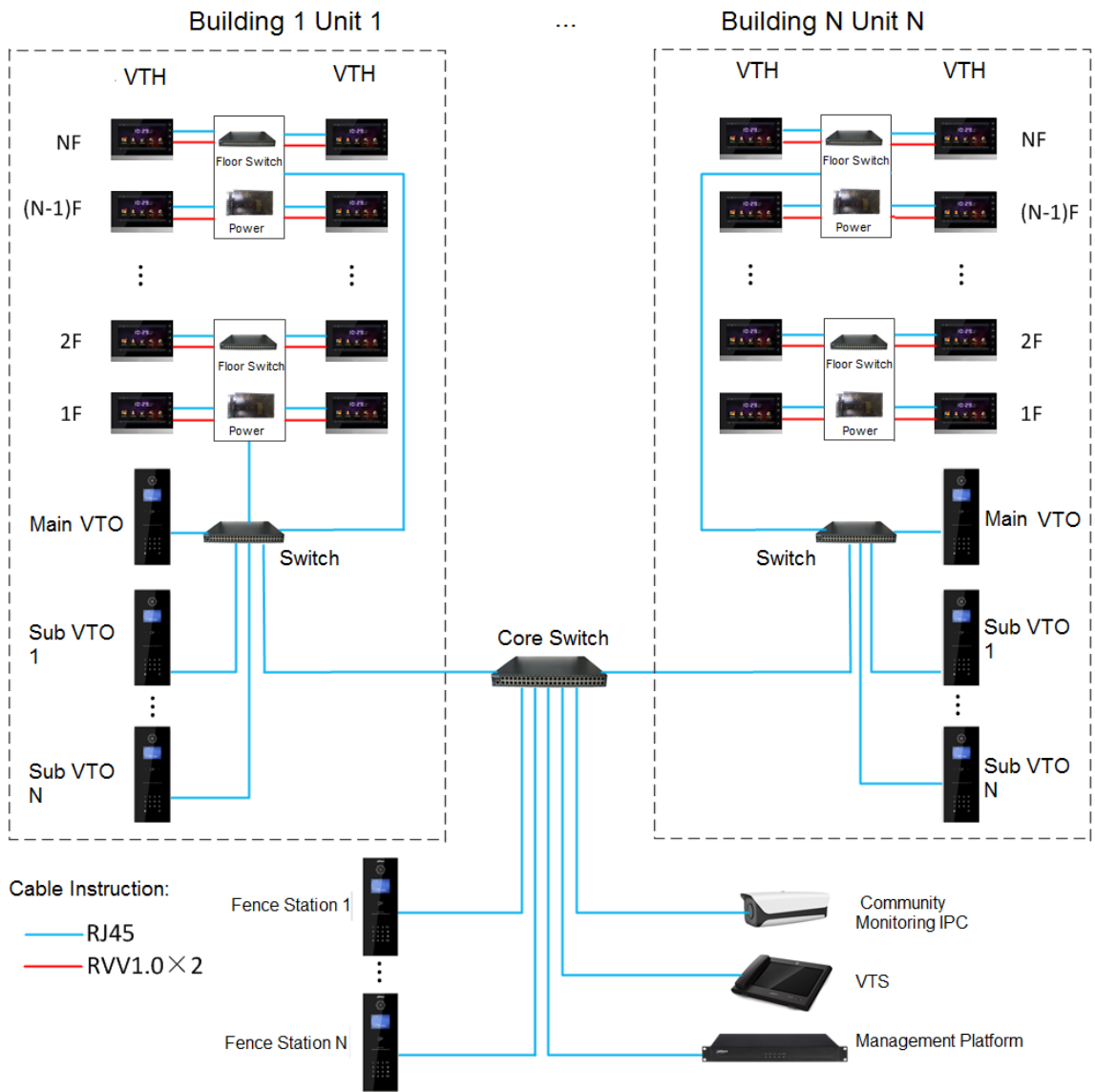
- The VTH powered through PoE from the floor switch.

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

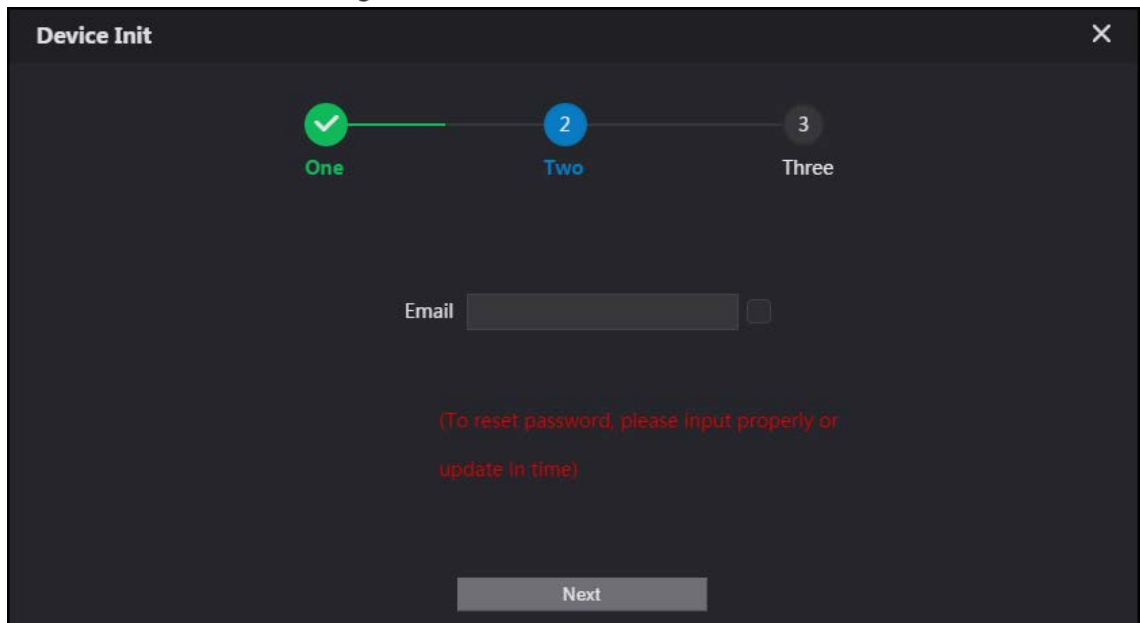
The screenshot shows a web interface titled "Device Init" with a close button (X) in the top right corner. At the top, there is a progress indicator with three steps: "1 One", "2 Two", and "3 Three". Step 1 is highlighted with a blue circle. Below the progress indicator, there are input fields for "Username"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

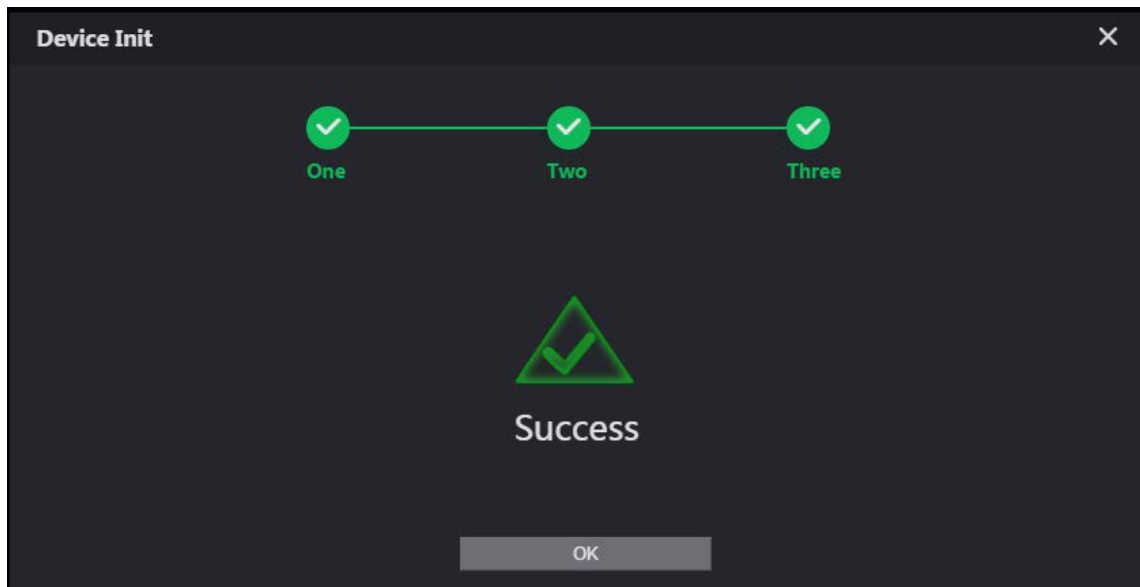
Figure 3-2 Set an email address



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

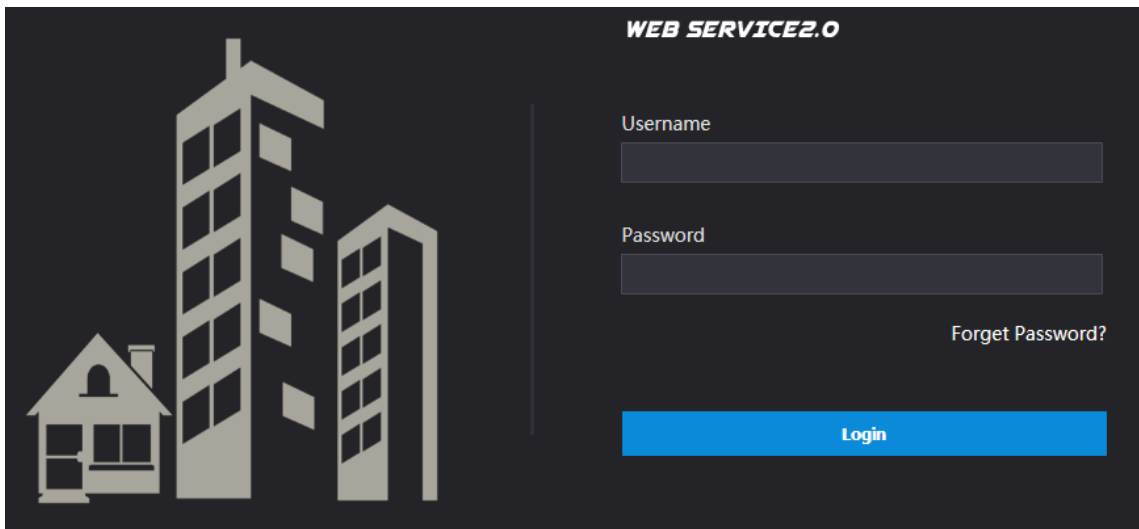
Step 5 Click **Next**.

Figure 3-3 Initialization successful



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

Figure 3-4 Login interface



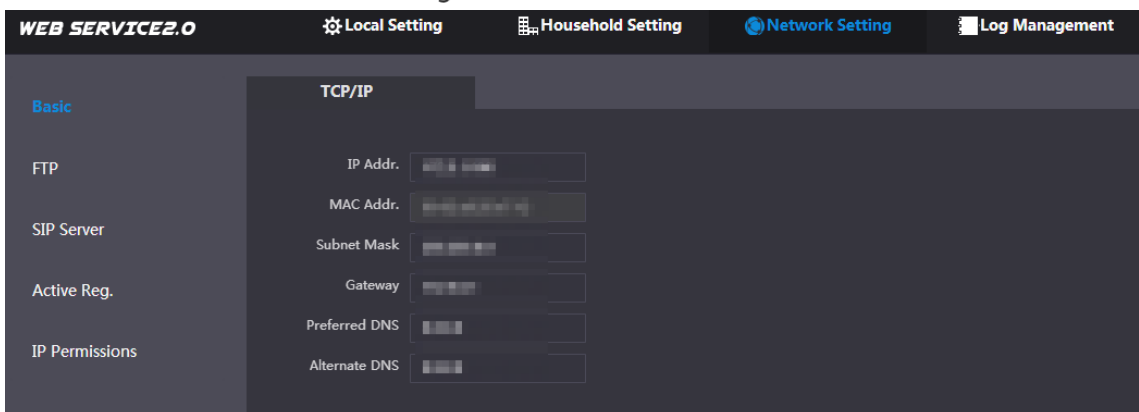
Step 7 Enter username (admin by default) and password, and then click **Login**.

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



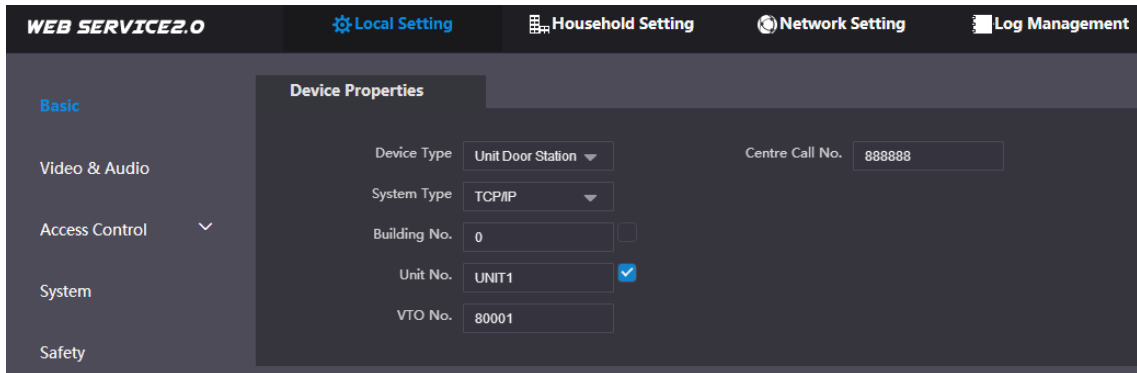
Step 2 Enter the parameters, and then click **OK**.

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**.

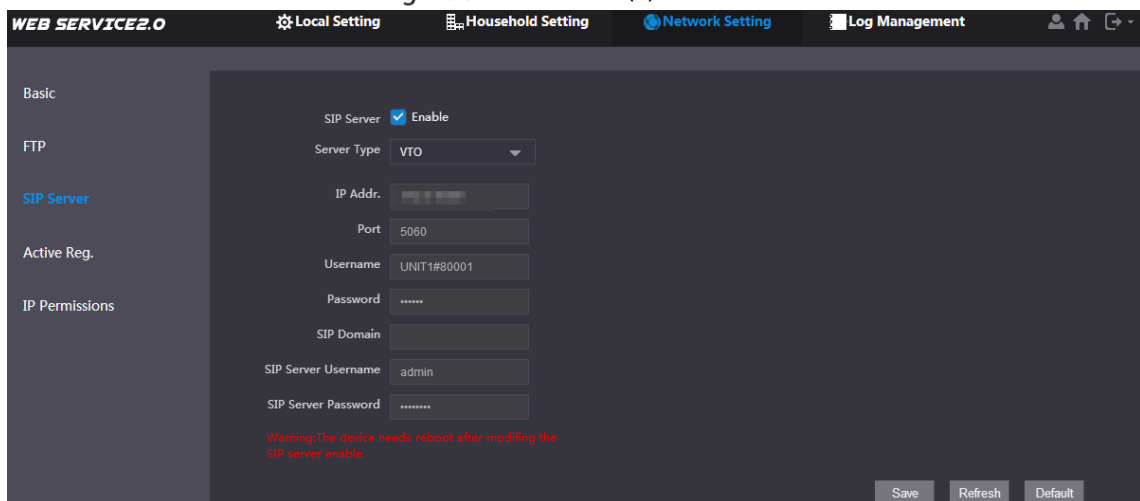
Wait for the device to automatically restart or restart it manually, and then the settings will take effect.

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)



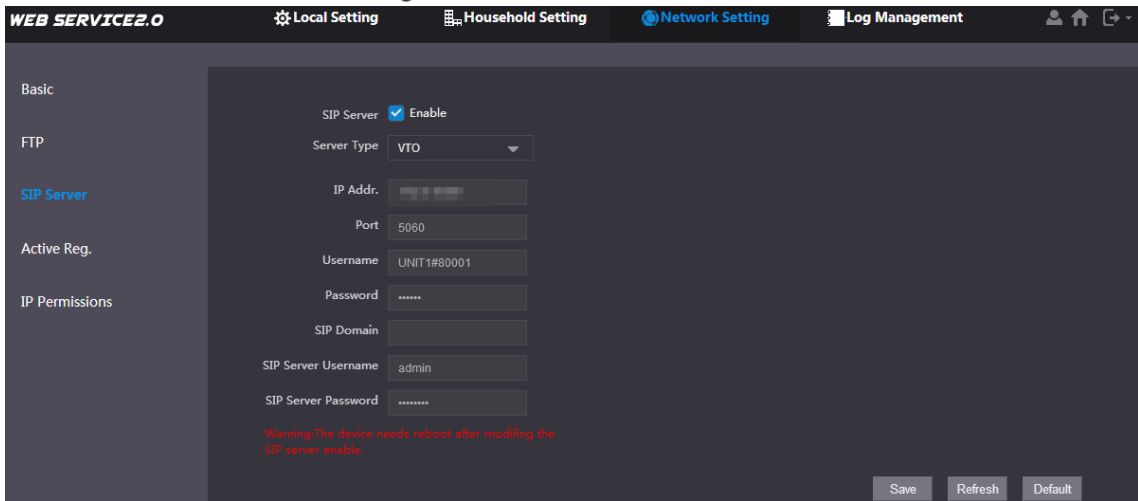
Step 2 Select a server type.

- 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

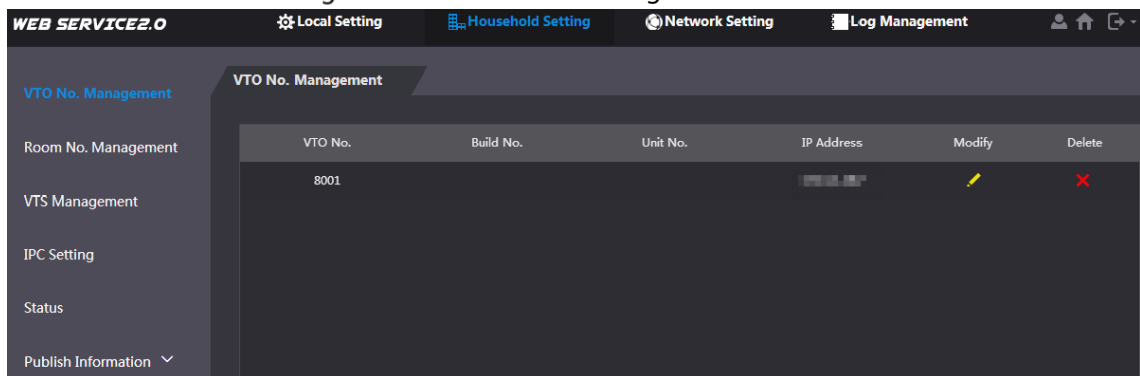


Add VTO only when the current VTO works as the SIP server.

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.

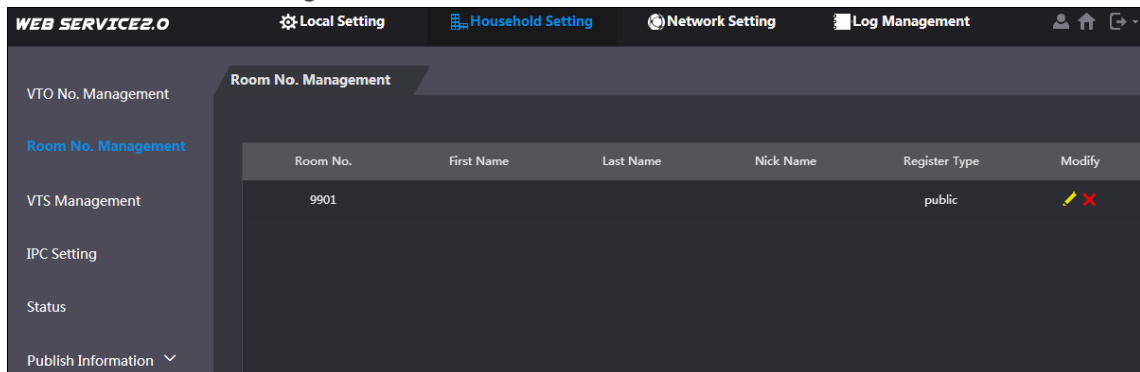
3.1.1.7 Adding VTH



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

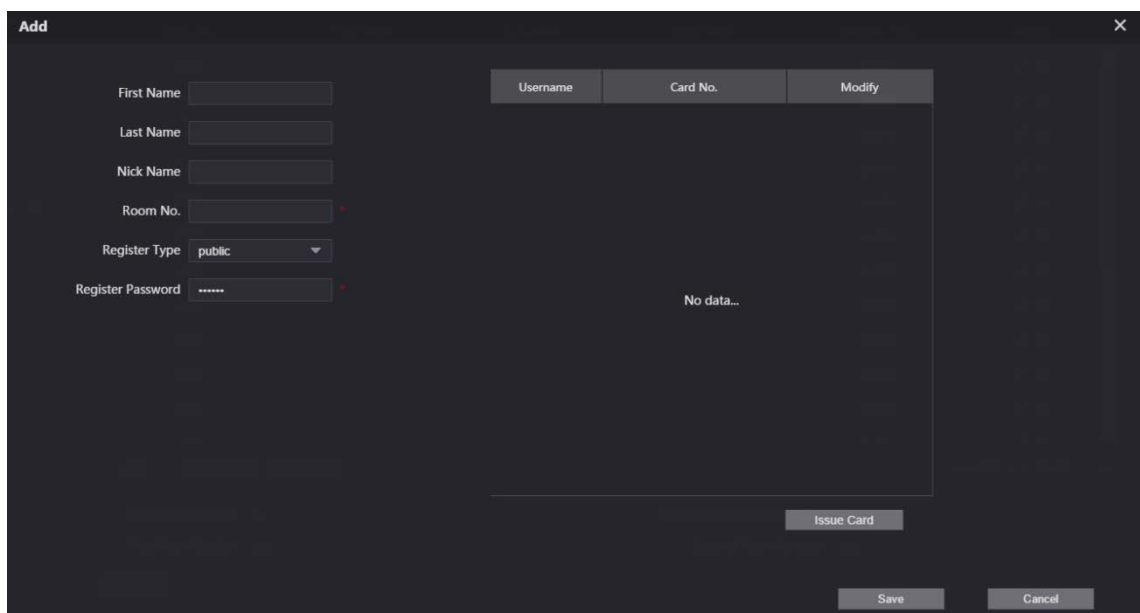
Step 1 Select **Household Setting > Room No. Management**.

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**.

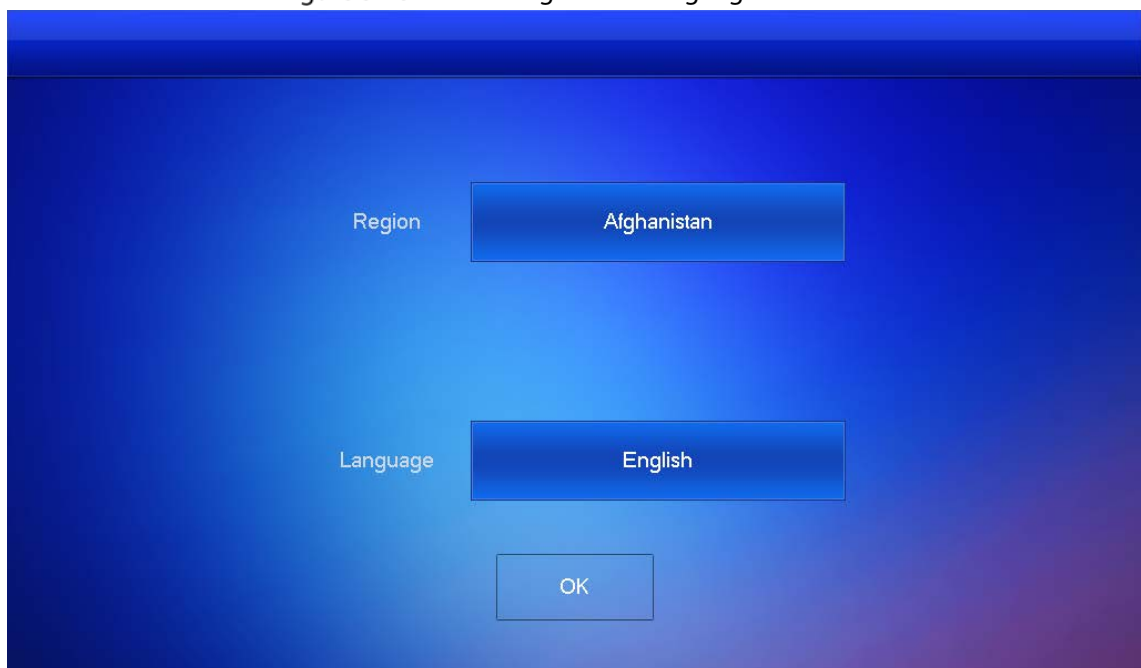
Do Step 2–Step 4 to add other VTHs.

3.1.2 VTH Settings

3.1.2.1 Initialization

Step 1 Select a region and language.

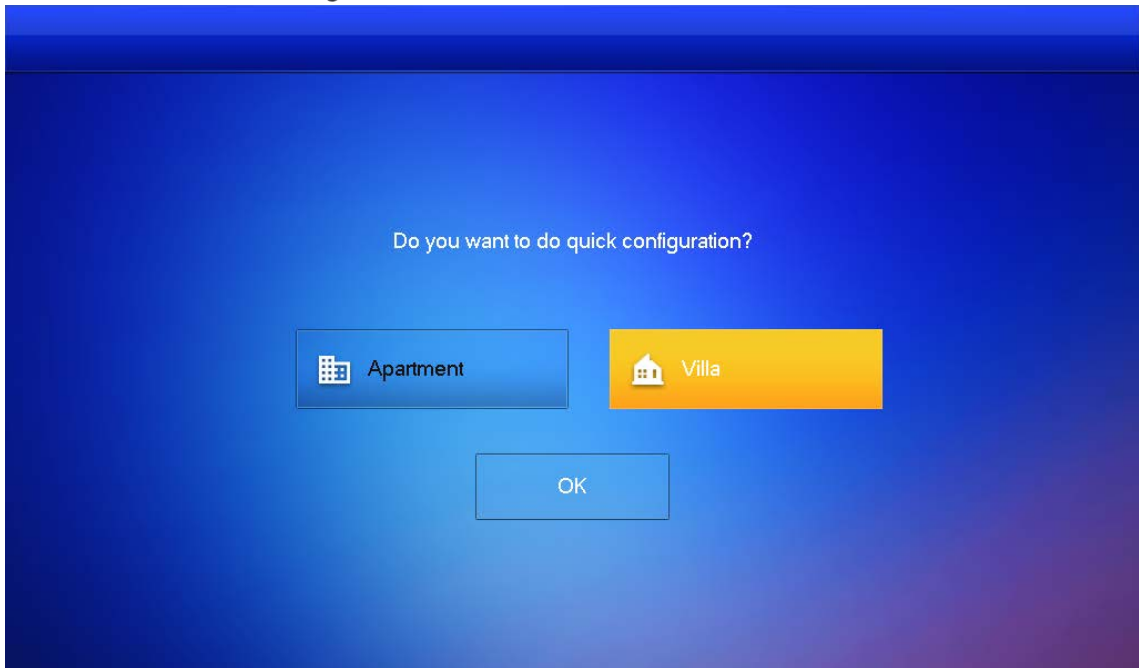
Figure 3-13 Select a region and language



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

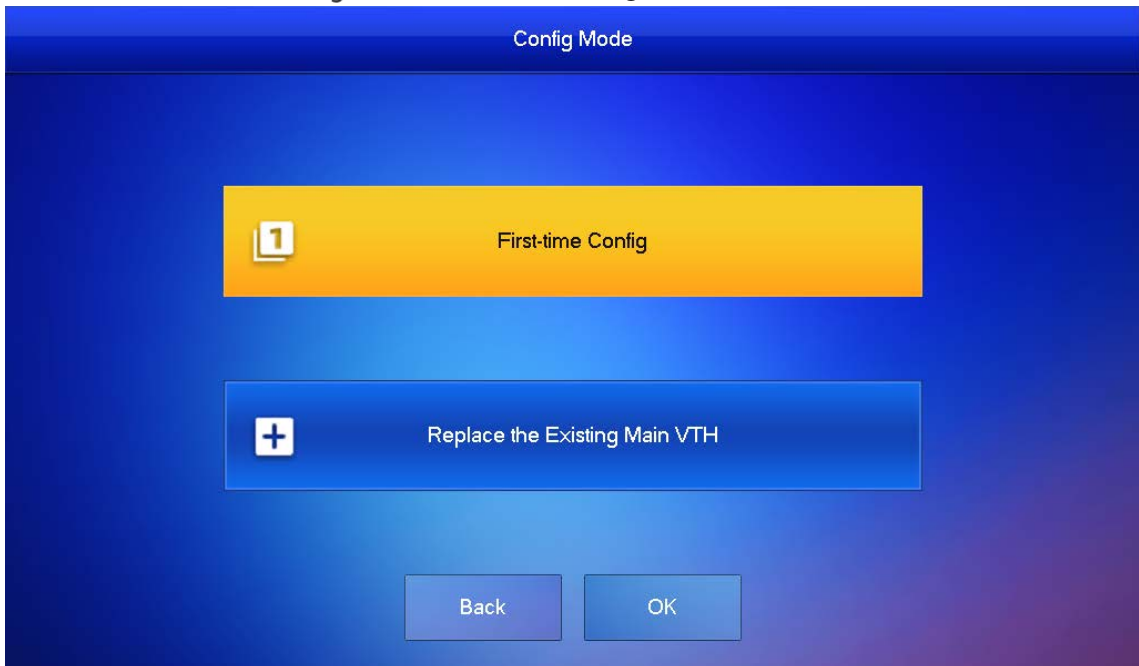
This section takes **Villa** as an example.

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

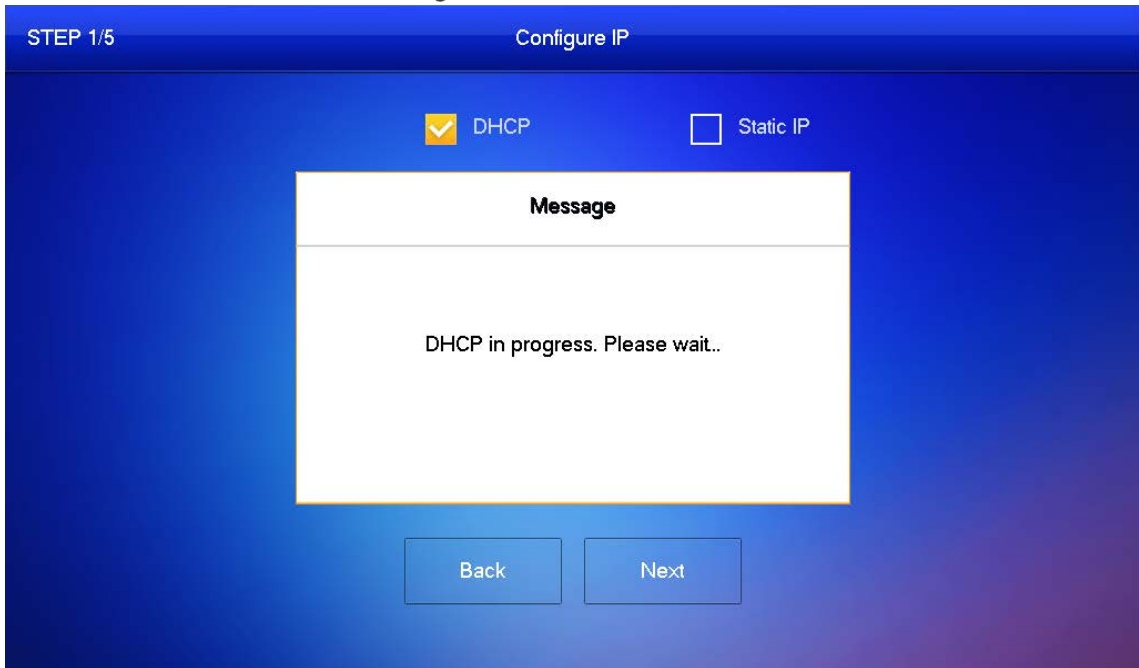
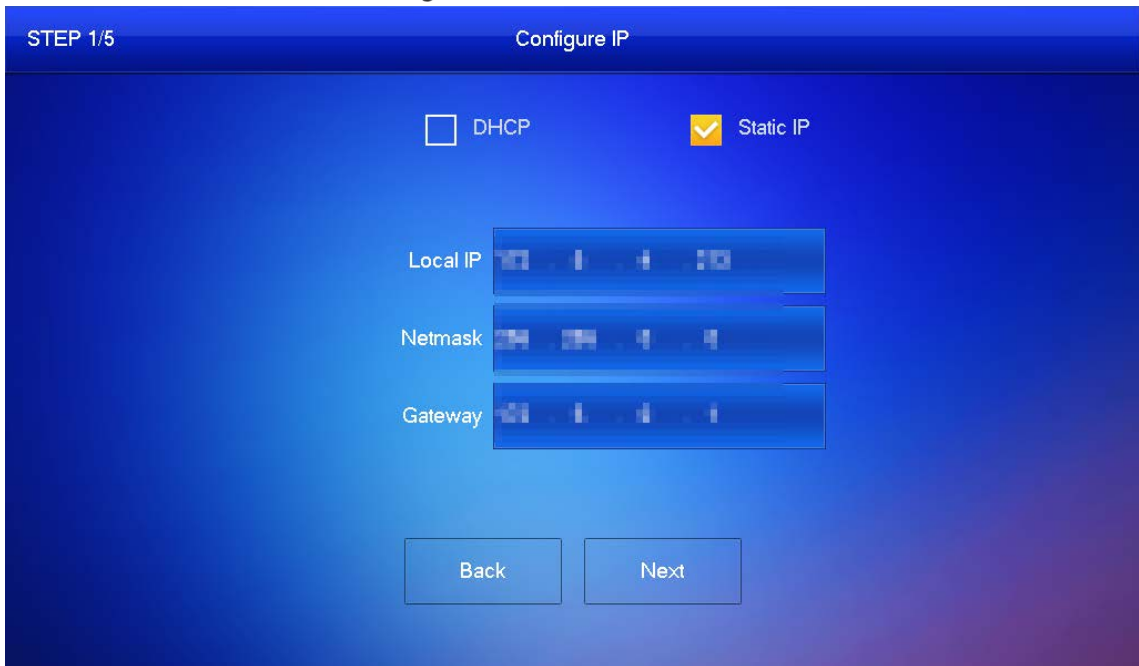


Figure 3-17 Static IP




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

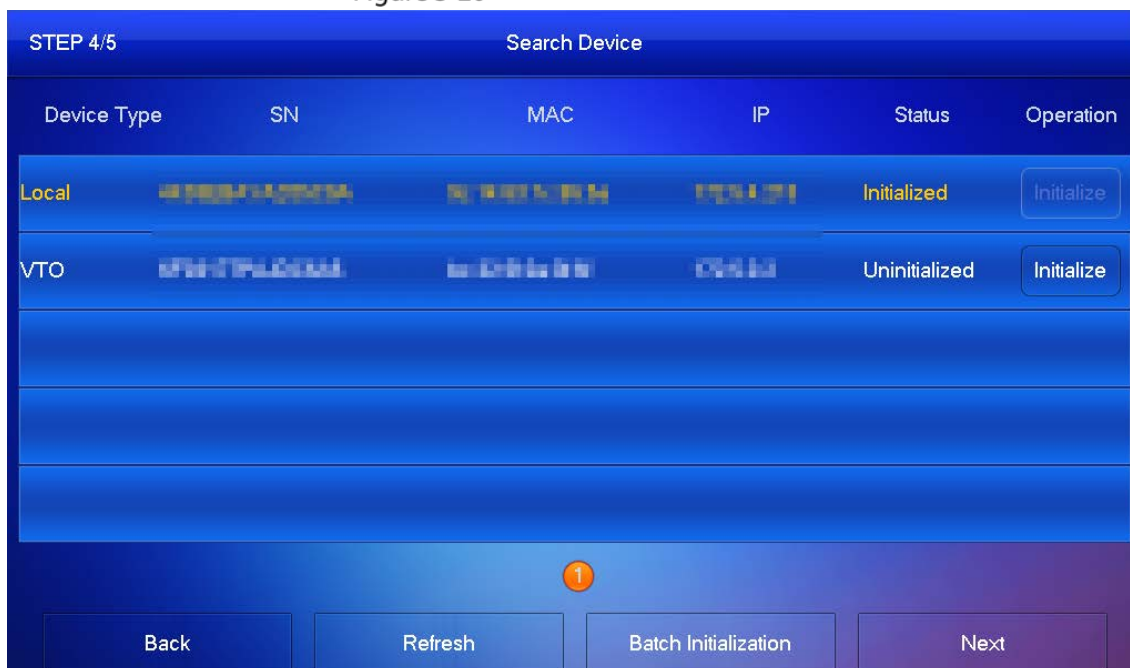
Confirm PWD 
8-32 characters password

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

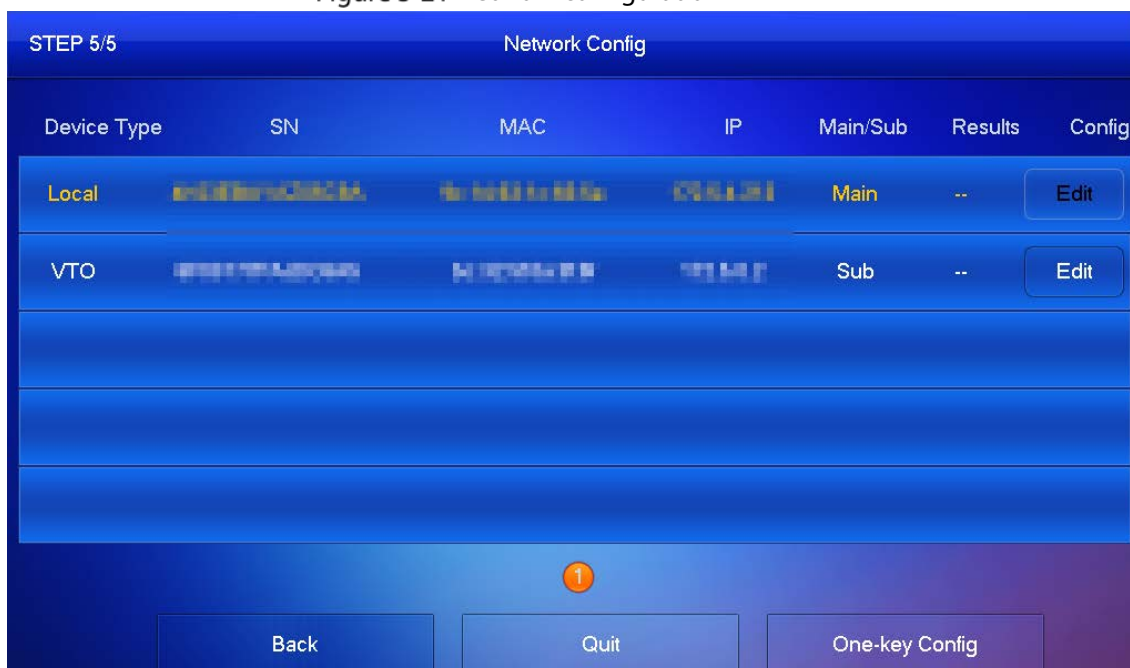
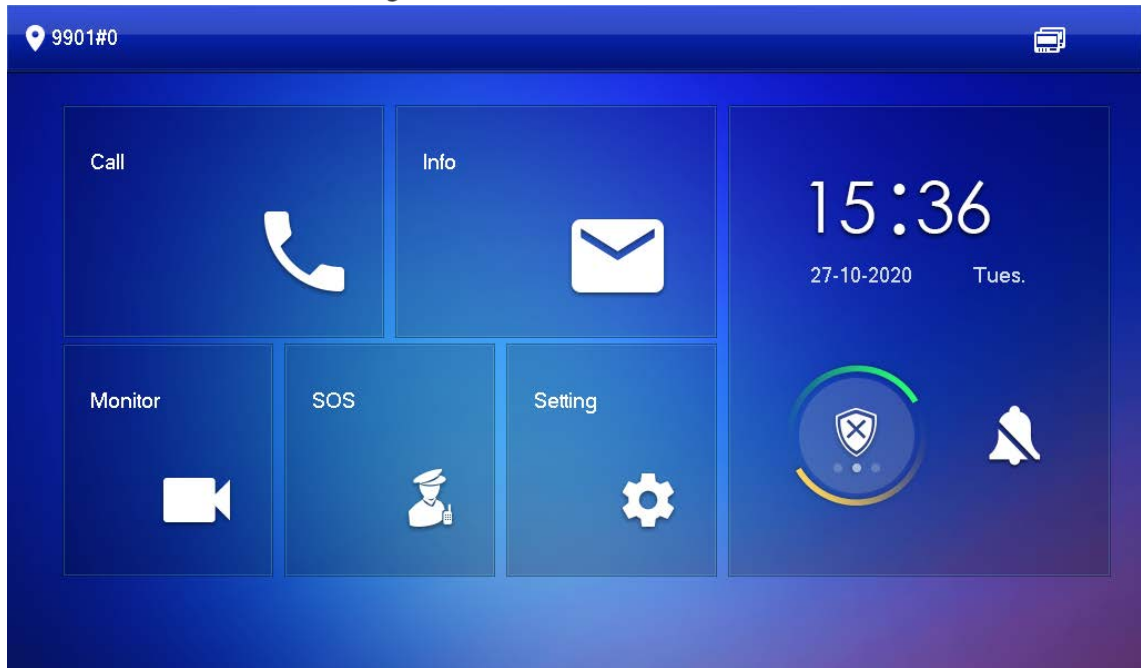


Figure 3-22 Main interface



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**.

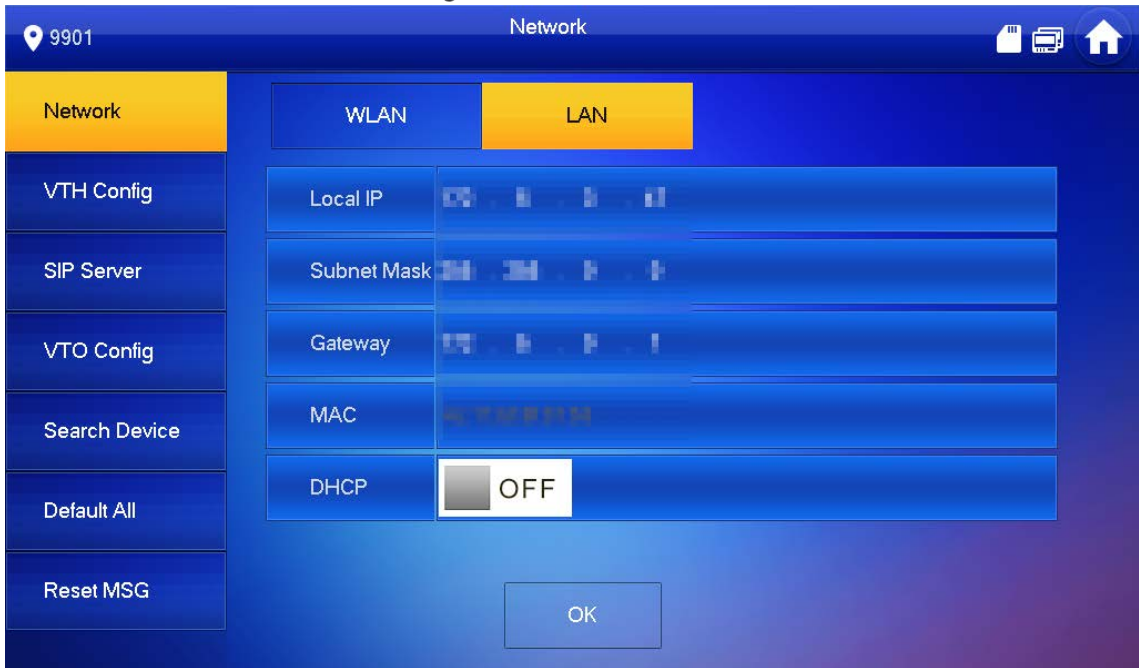
Step 3 Tap **Network**.

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



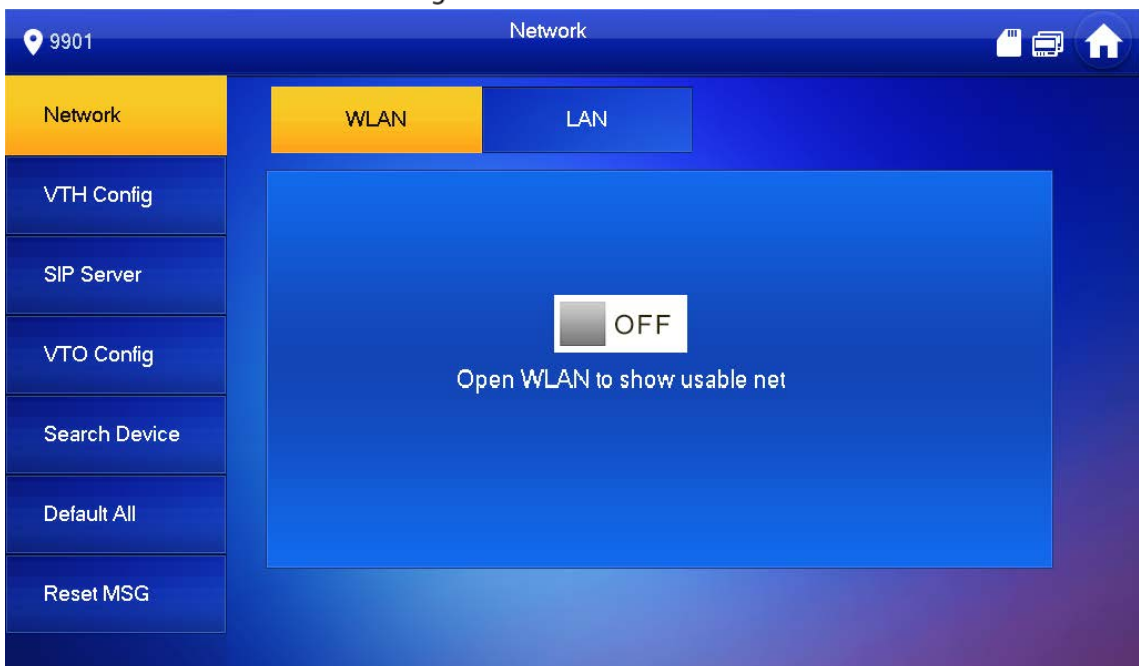
- WLAN



- 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.

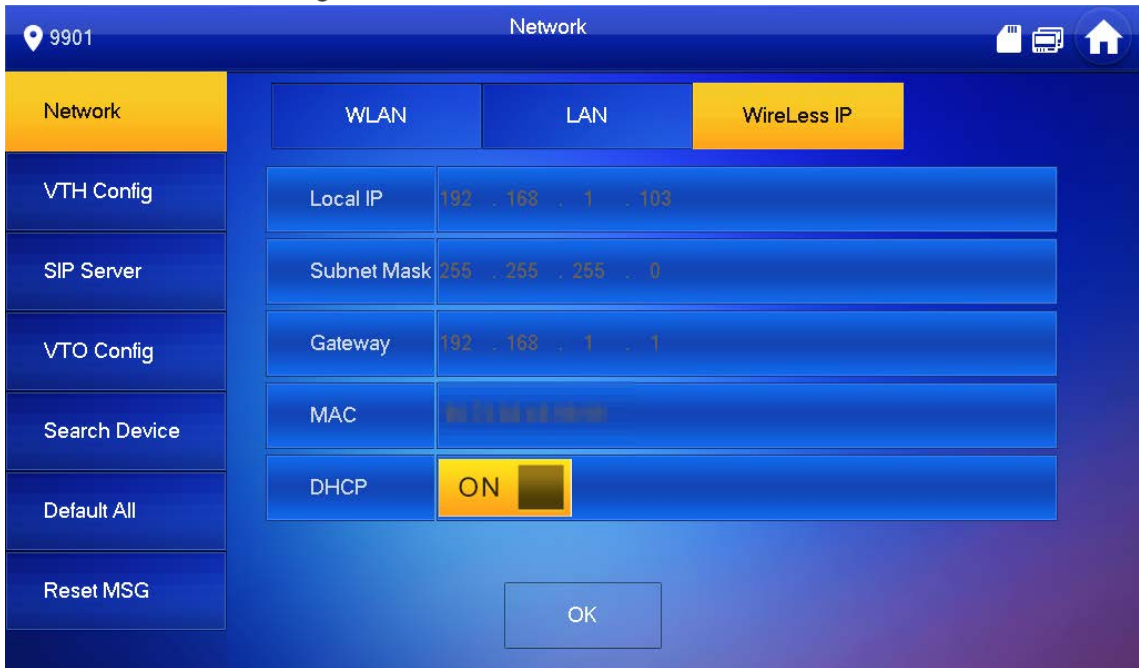
The system has 2 access ways as follows.

- ◇ 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

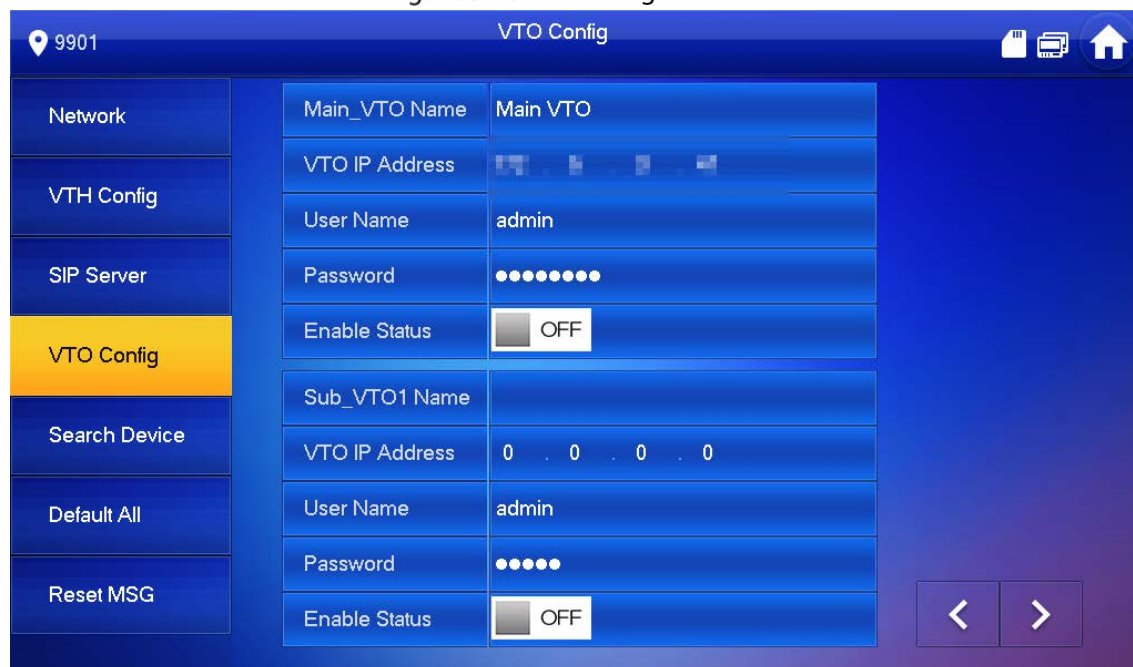
Add VTOs and fence stations to bind them with the VTH.

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

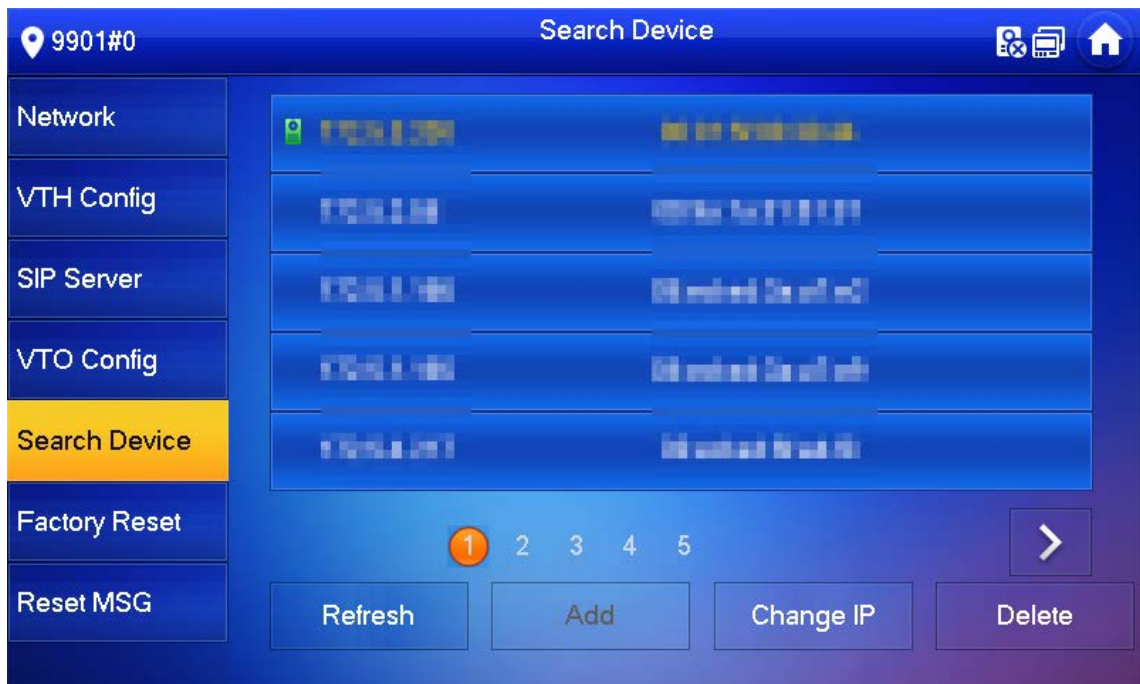
You can search for VTOs in the same network, and then add them or change their information.

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

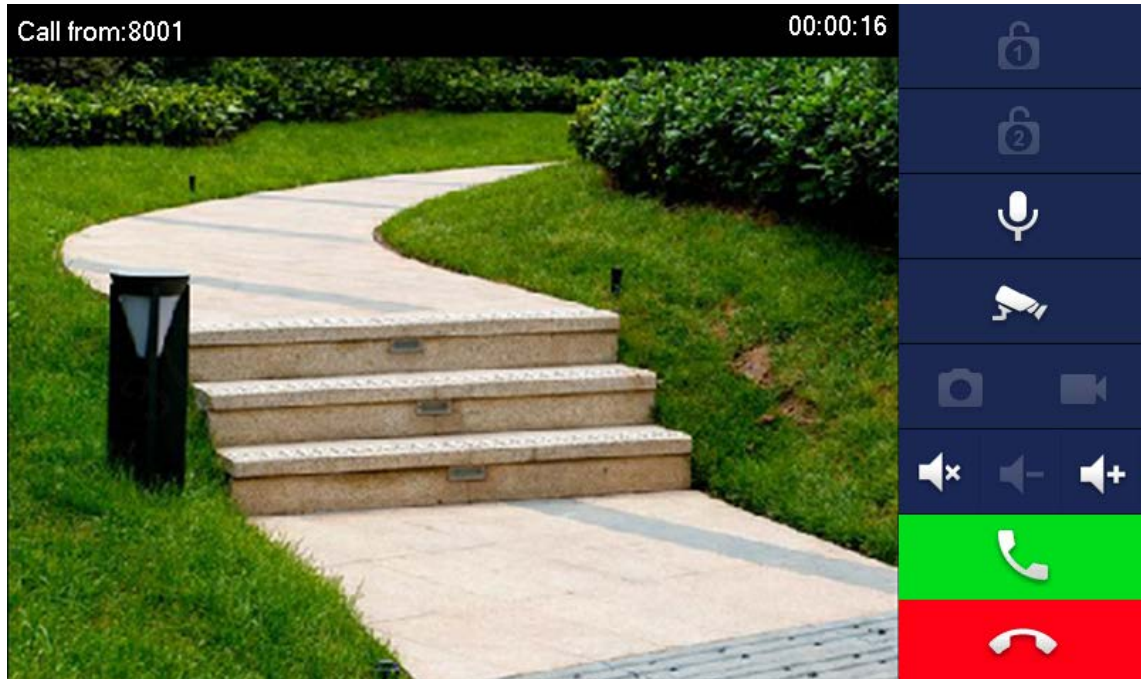
Delete

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

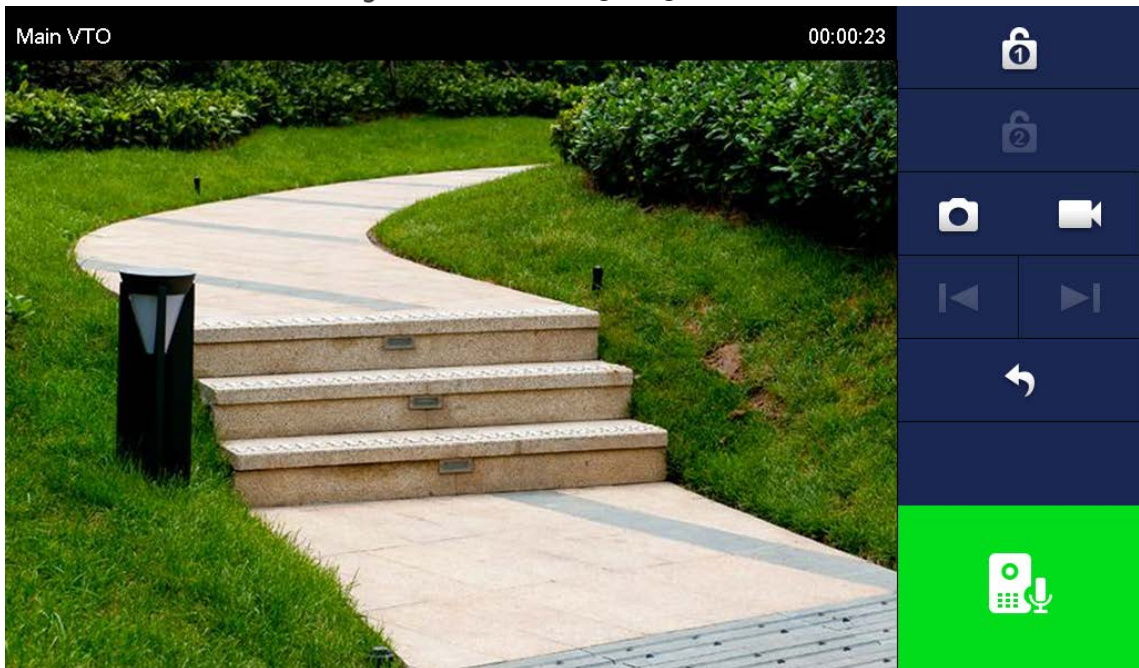
VTH can monitor VTO, fence station or IPC. This section takes monitoring VTO as an example.

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

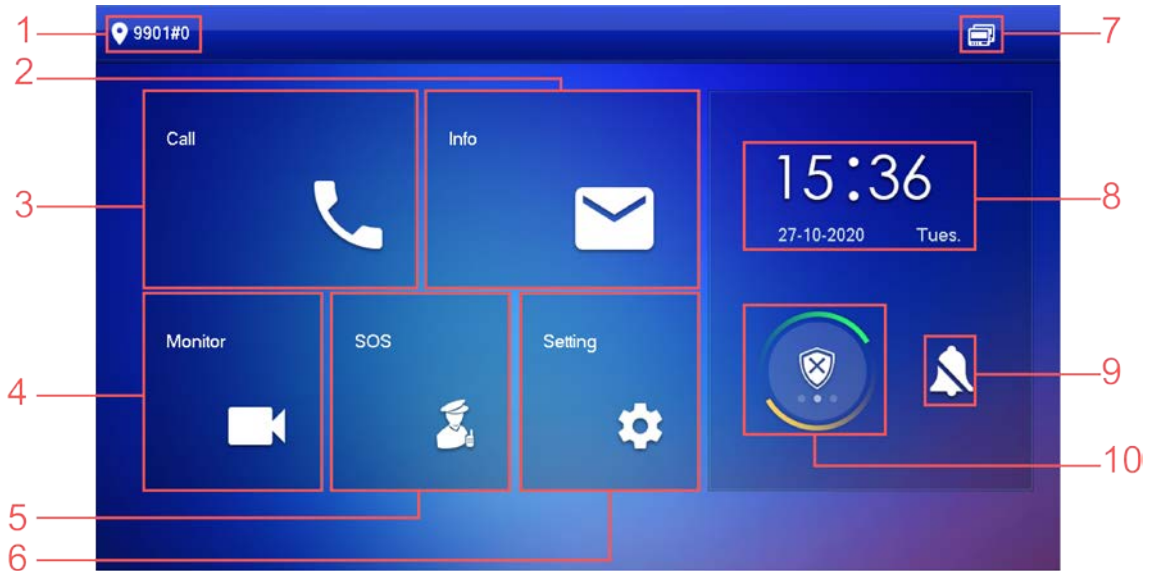








Table 4-1 Main interface description

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.

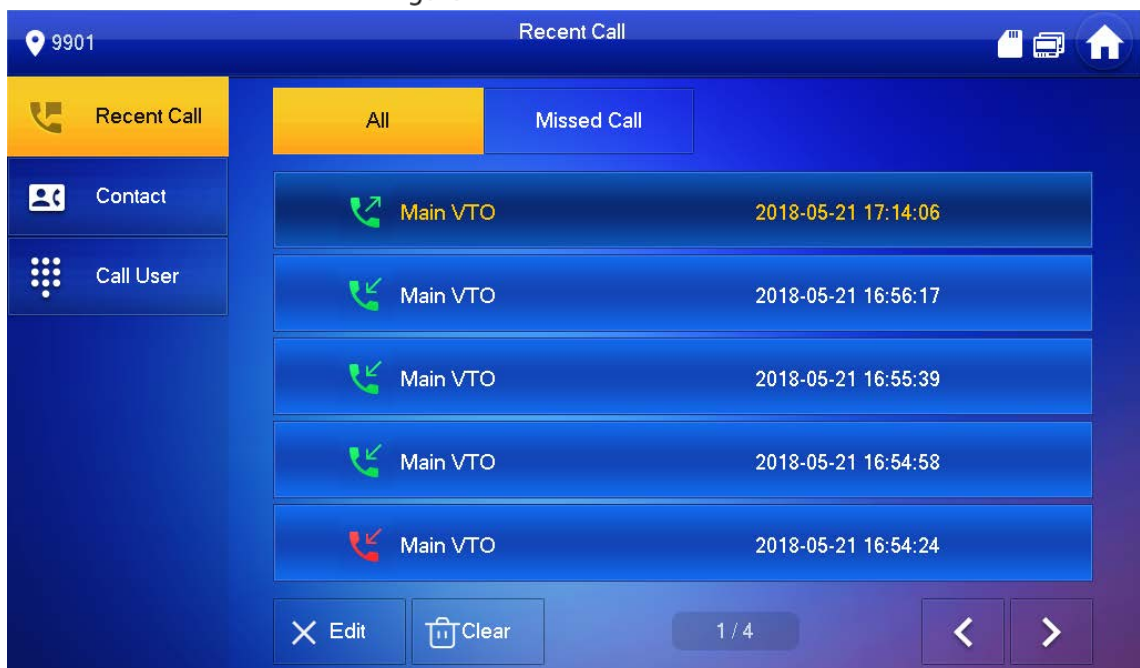
4.2.1 Recent Call

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**).

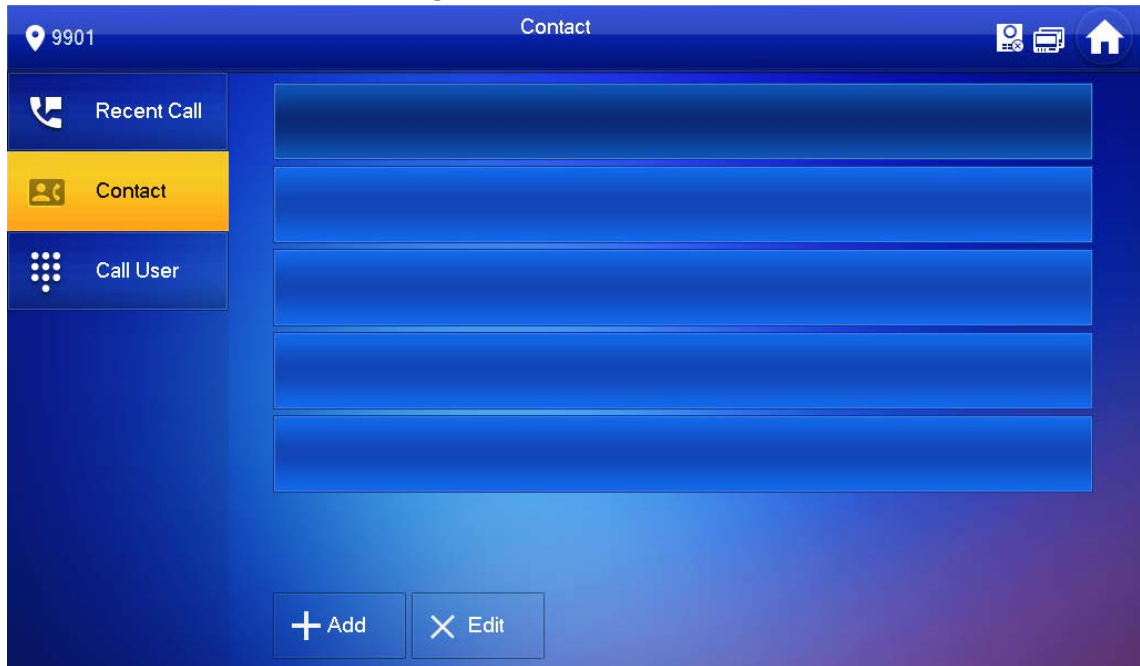


If storage is full, the oldest records will be overwritten. Back up the records as needed.

4.2.2 Contact

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

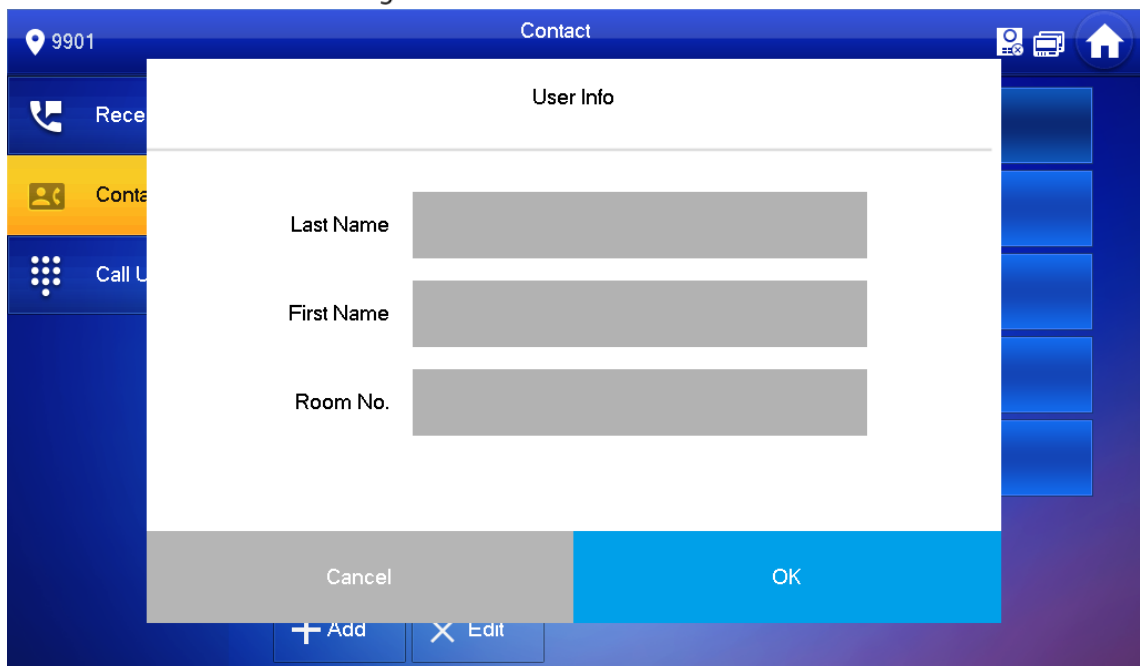
Figure 4-3 Contact



- 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



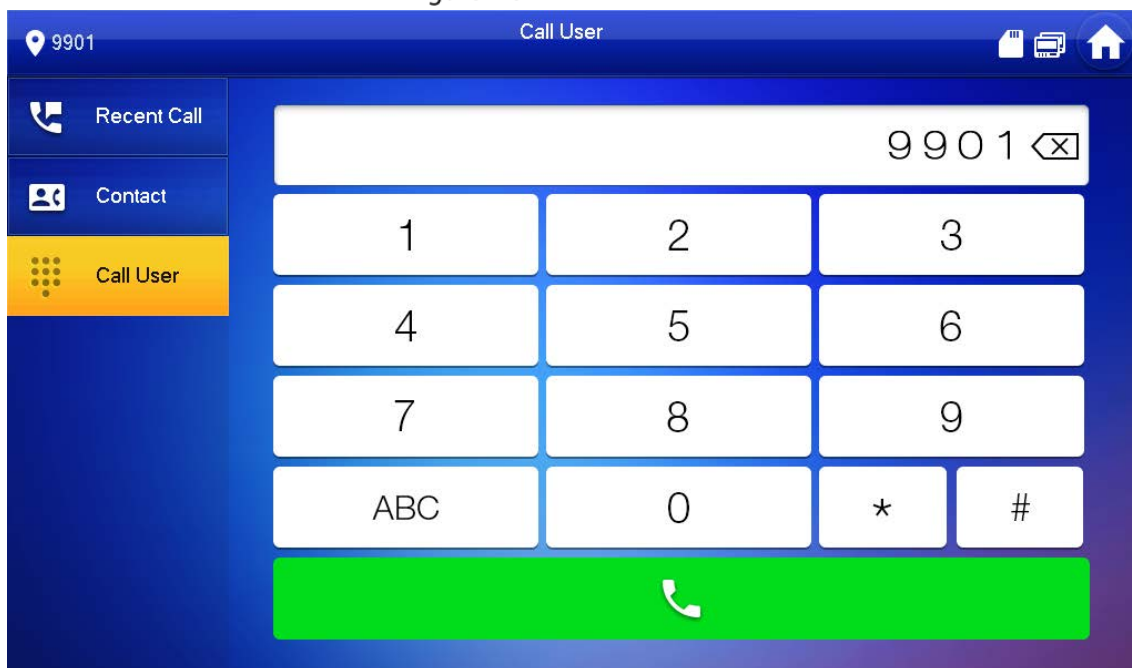
- Make sure that resident-to-resident call function has been enabled. See "4.6.6.4 QR Code" for details.
- Call function is used by VTH to call VTH.
- If both VTHs have a camera, bilateral video call can be provided.

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

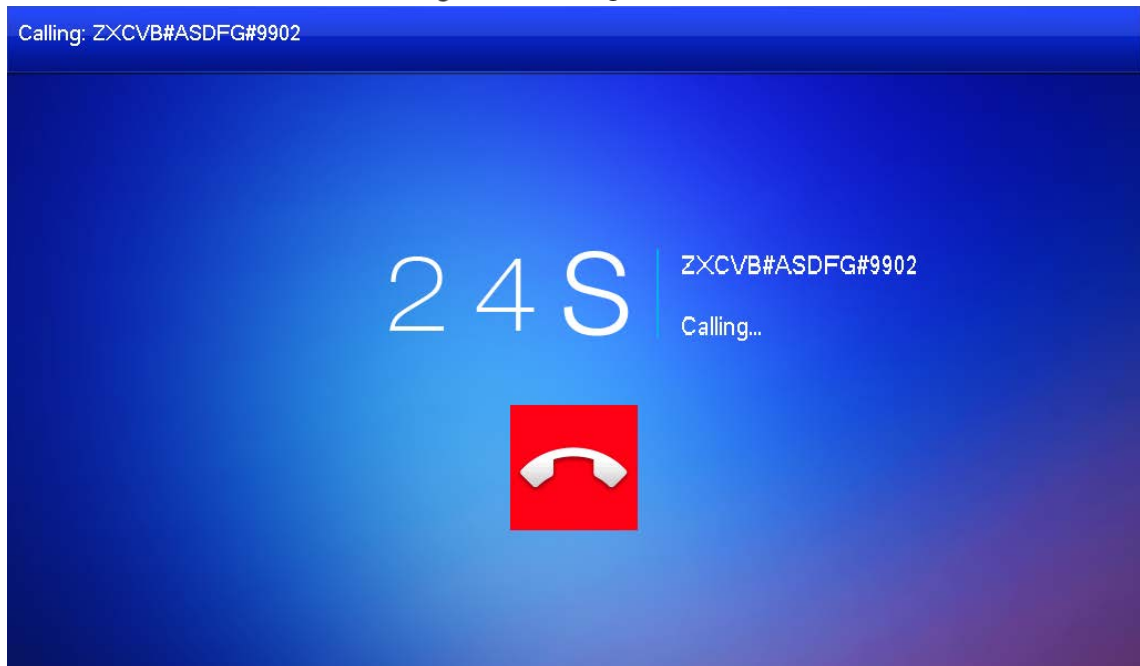
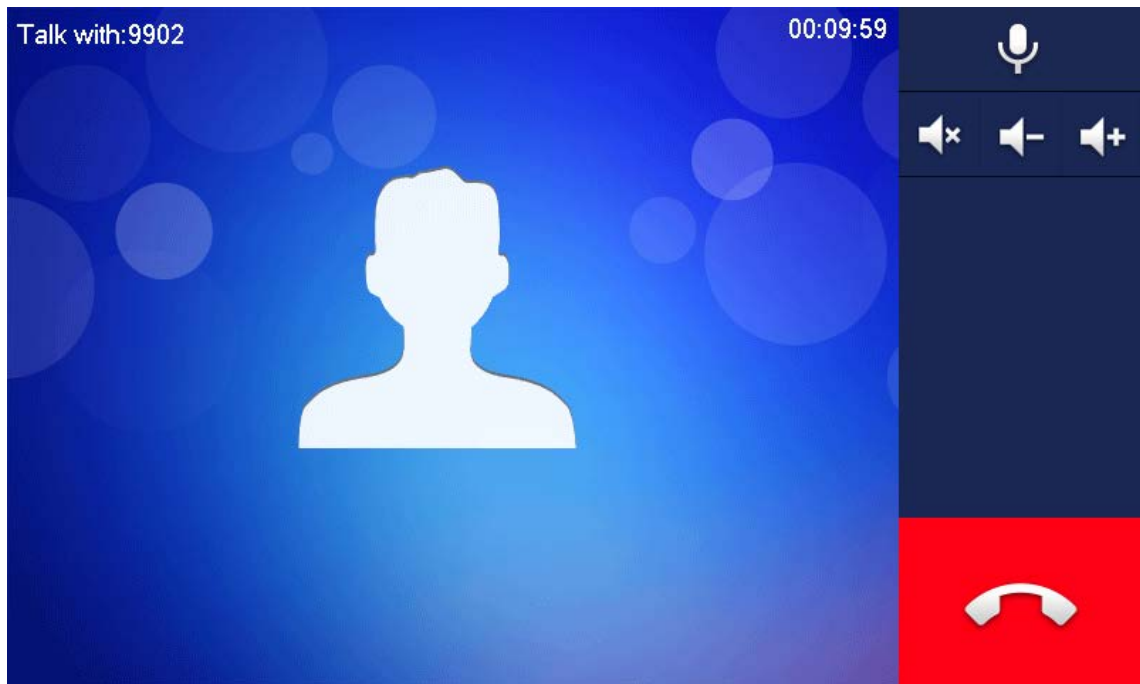


Figure 4-7 Call in progress



4.2.3.2 From Contact



Add contacts first. See 4.2.2 Contact.

Step 1 Select **Call > Contact**.

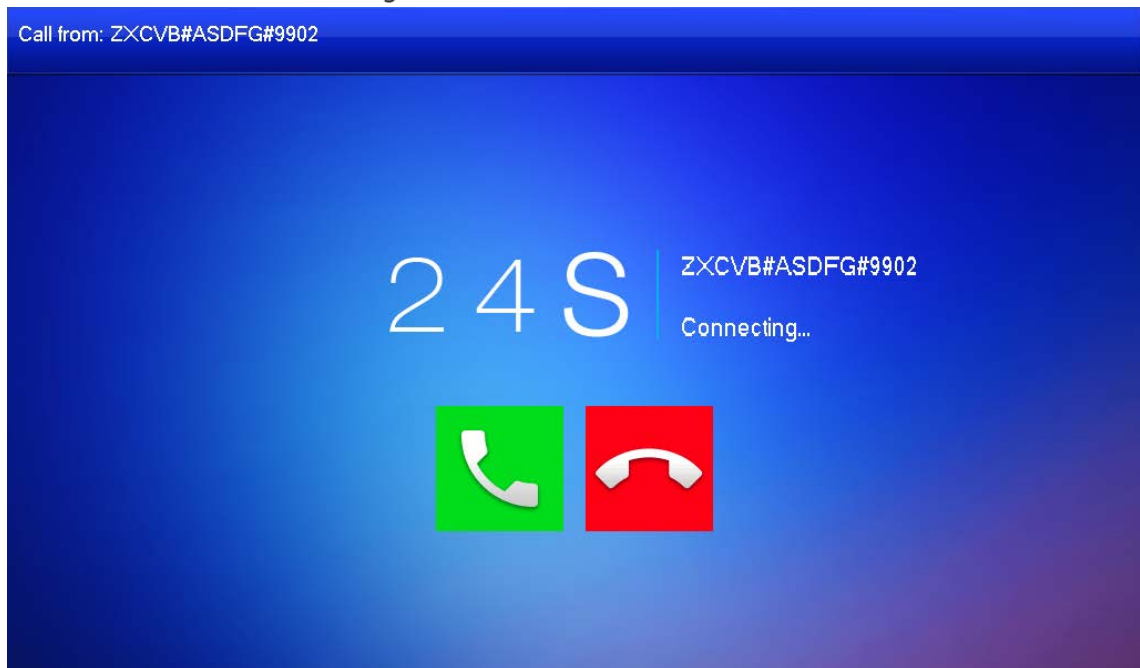
Step 2 Select the one you want to call.

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)





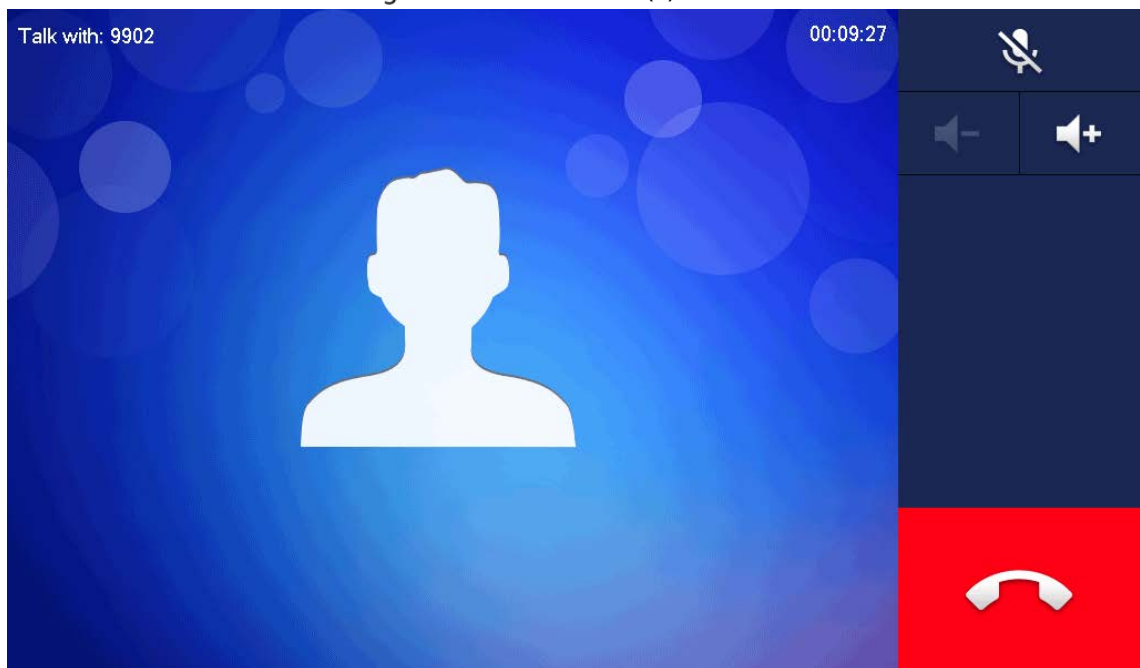
- : Answer.
- : Hang up.

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

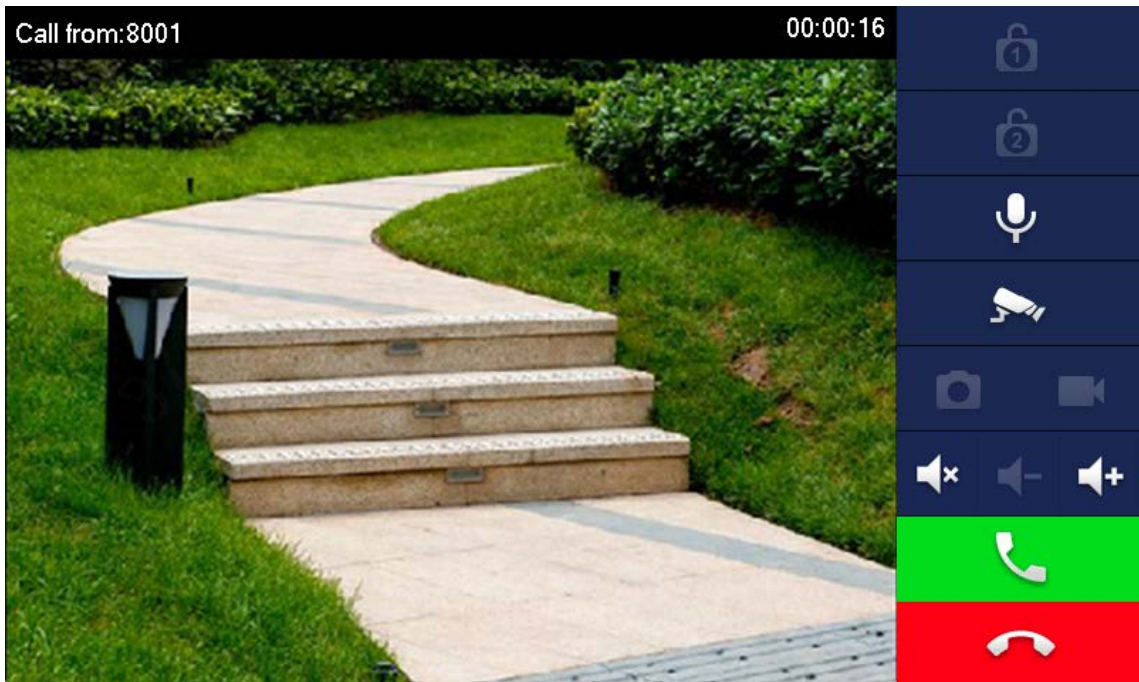






Table 4-2 Interface description

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.

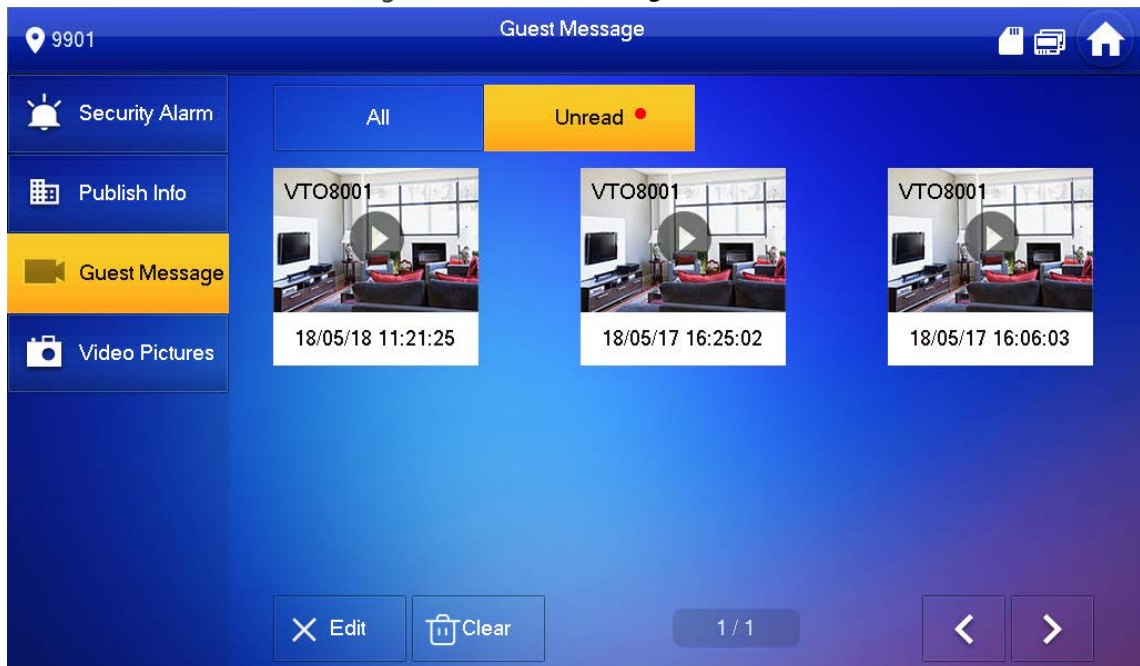
Figure 4-12 Security alarm



4.3.2 Guest Message

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

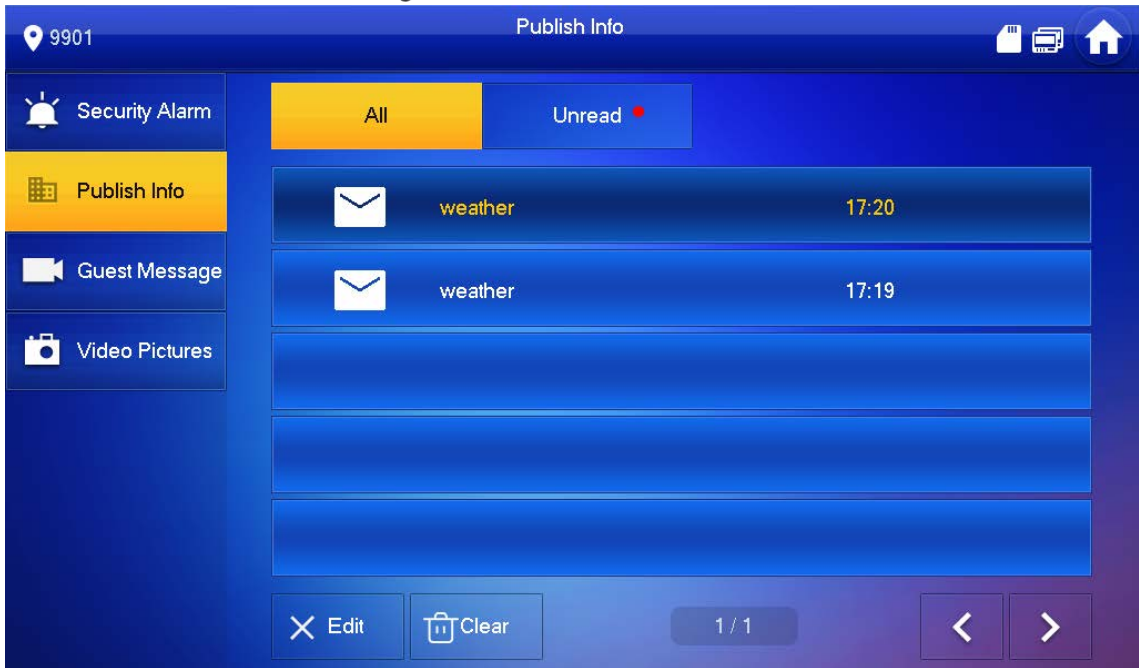
Figure 4-13 Guest message



4.3.3 Publish Info

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

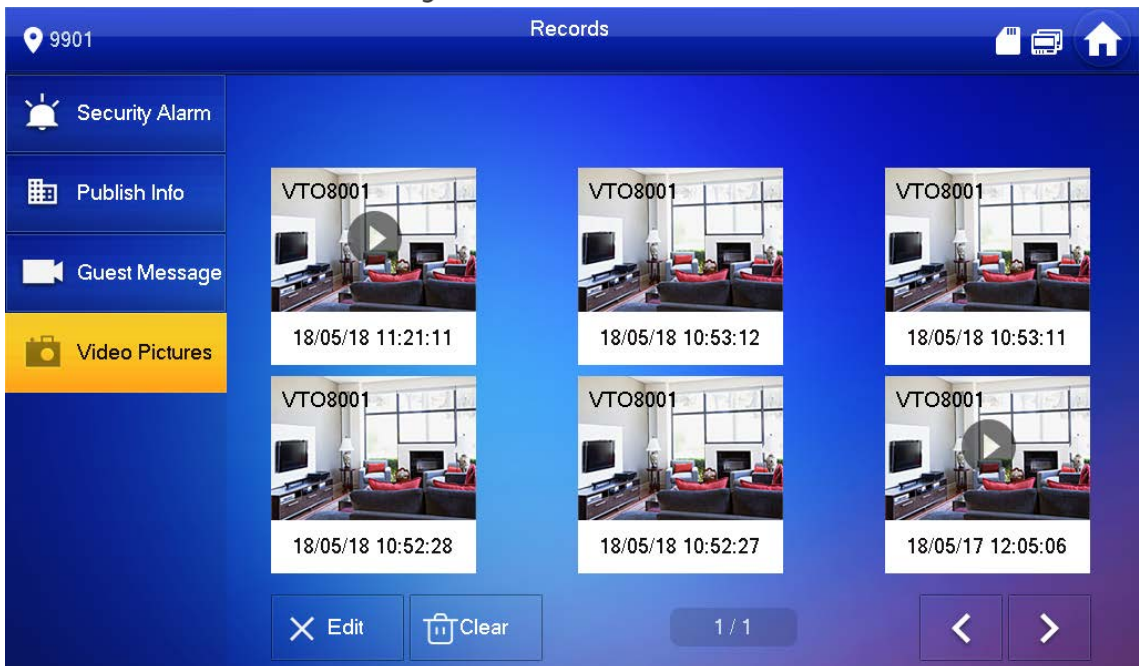
Figure 4-14 Publish info



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

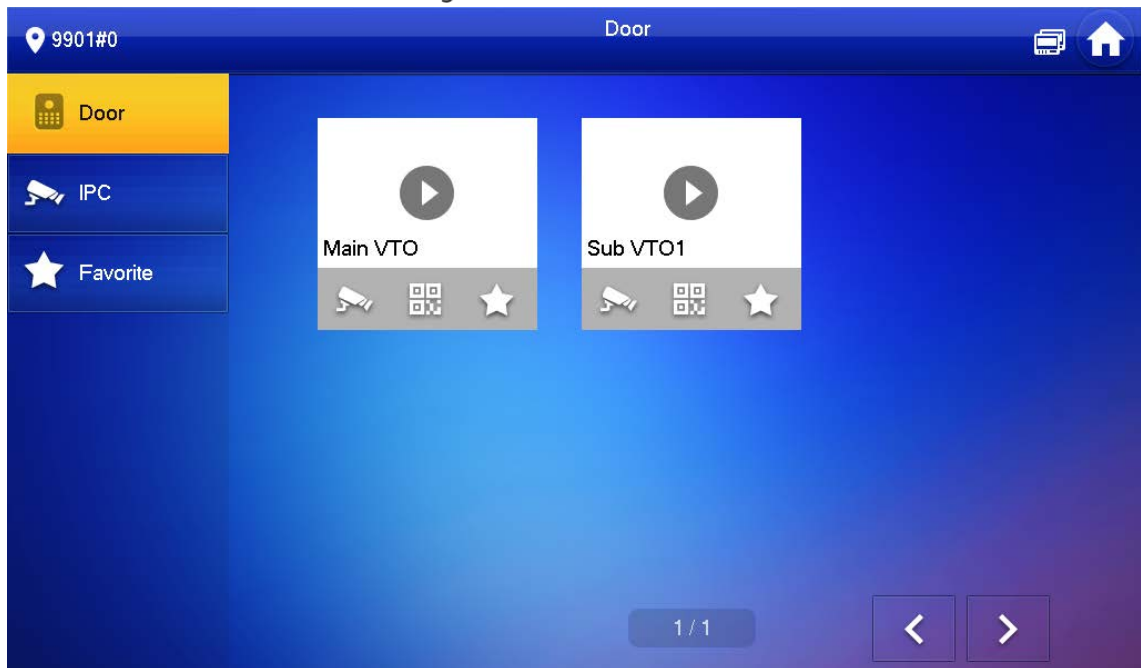


Table 4-3 Function description

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

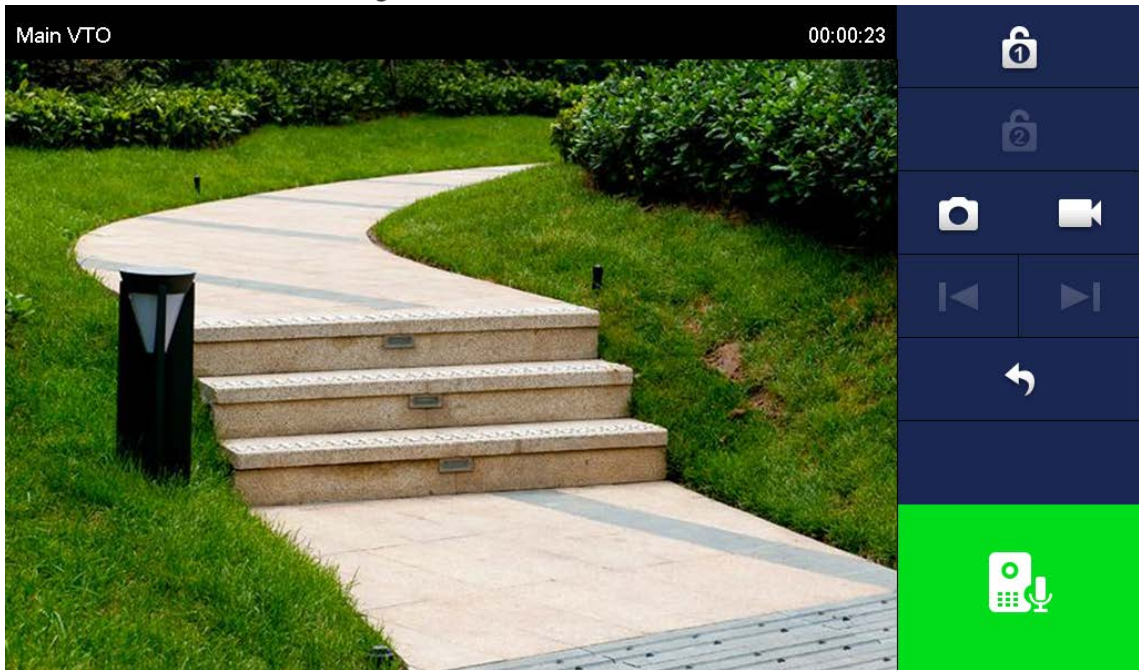


Table 4-4 Interface description

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/IPCs, 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**.


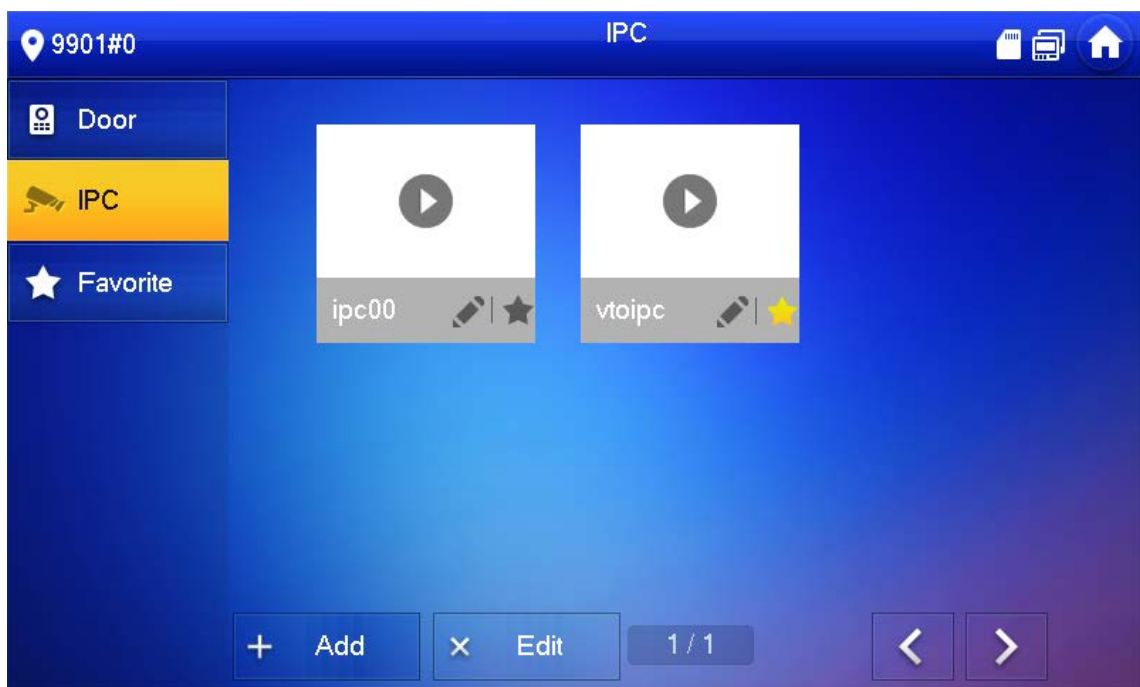
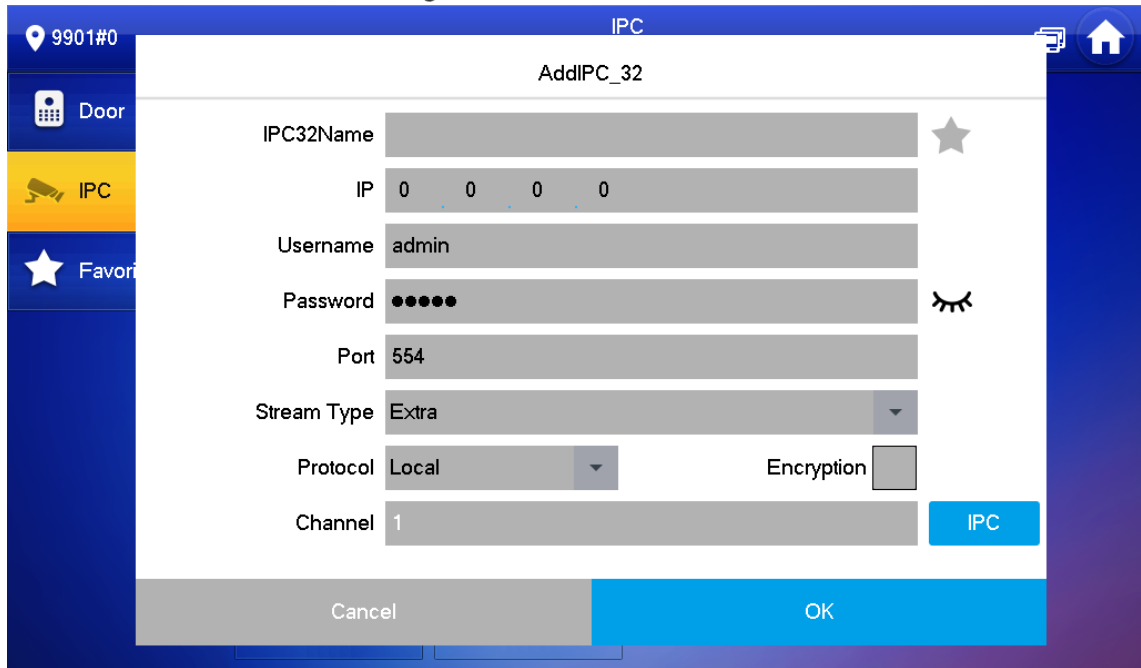
You can tap  to add the IPC to **Favorites**.

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

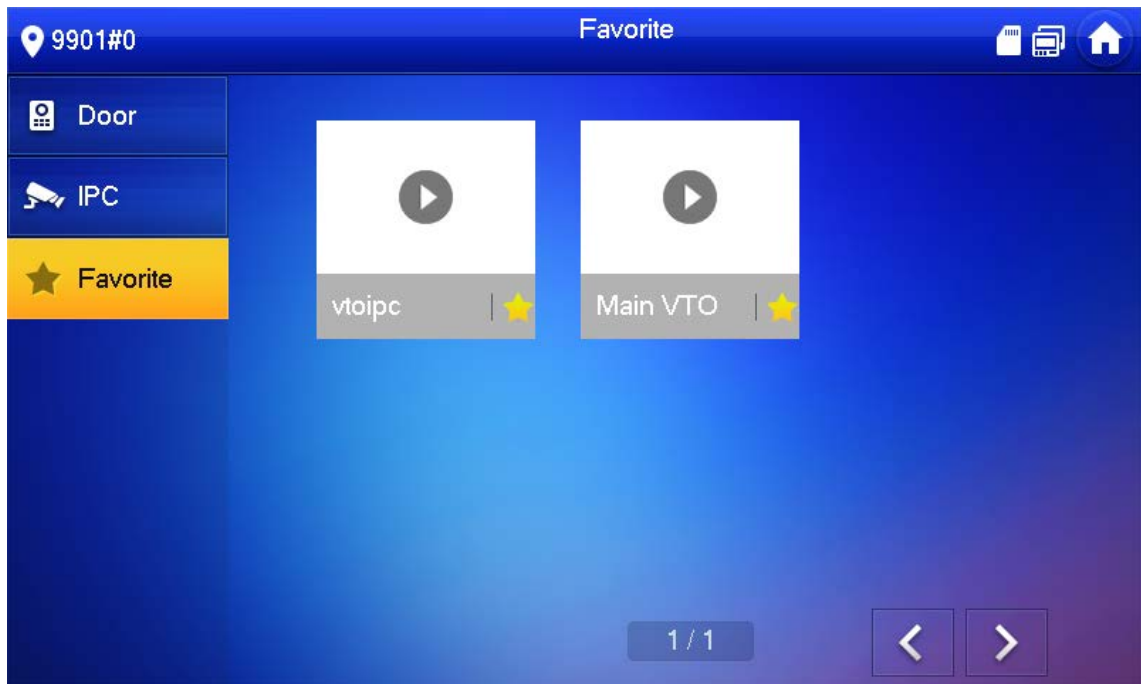
Displays VTO, fence stations or IPC that have been added to favorites.






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.

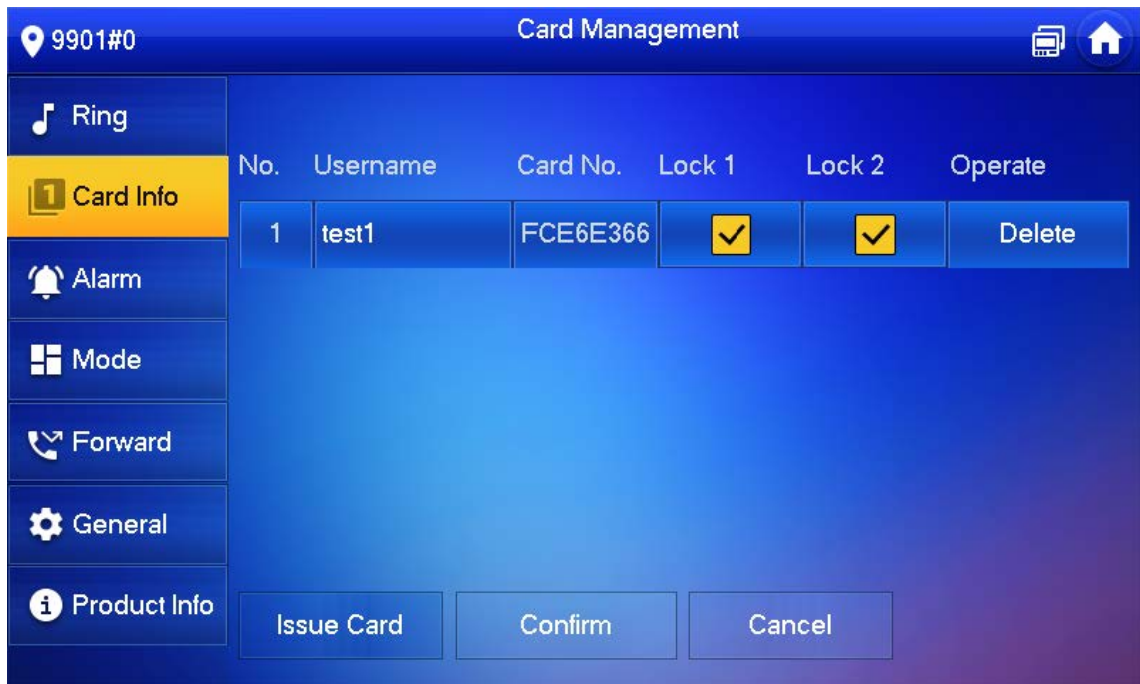
4.6.2 Card Information

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.

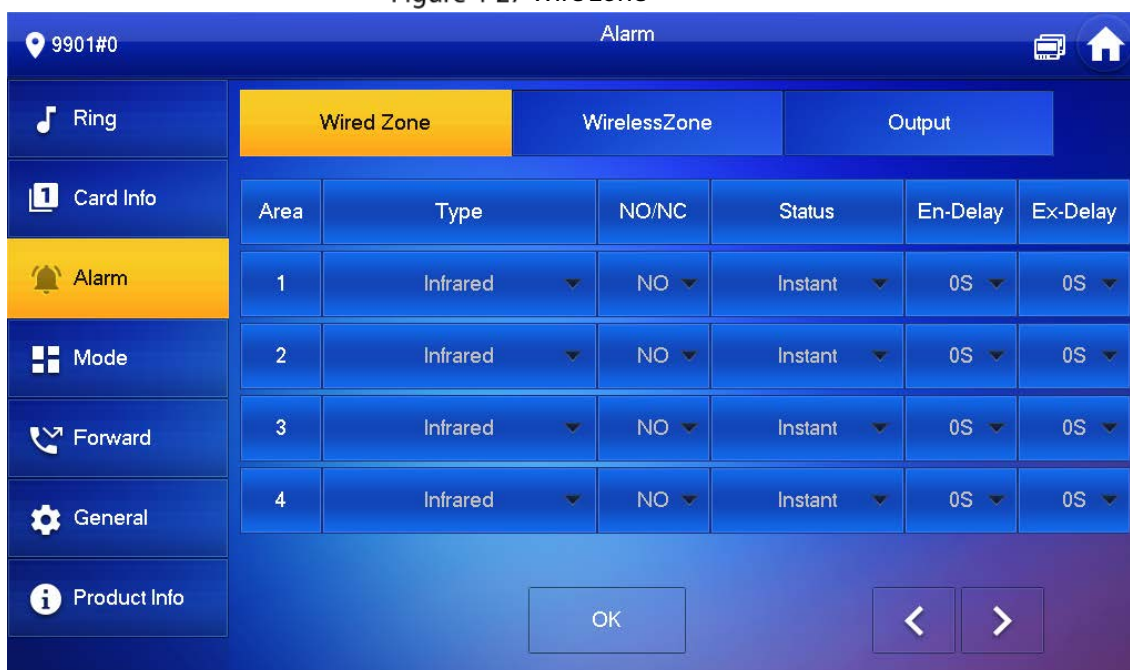
Step 2 Enter login password and tap OK.



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**.

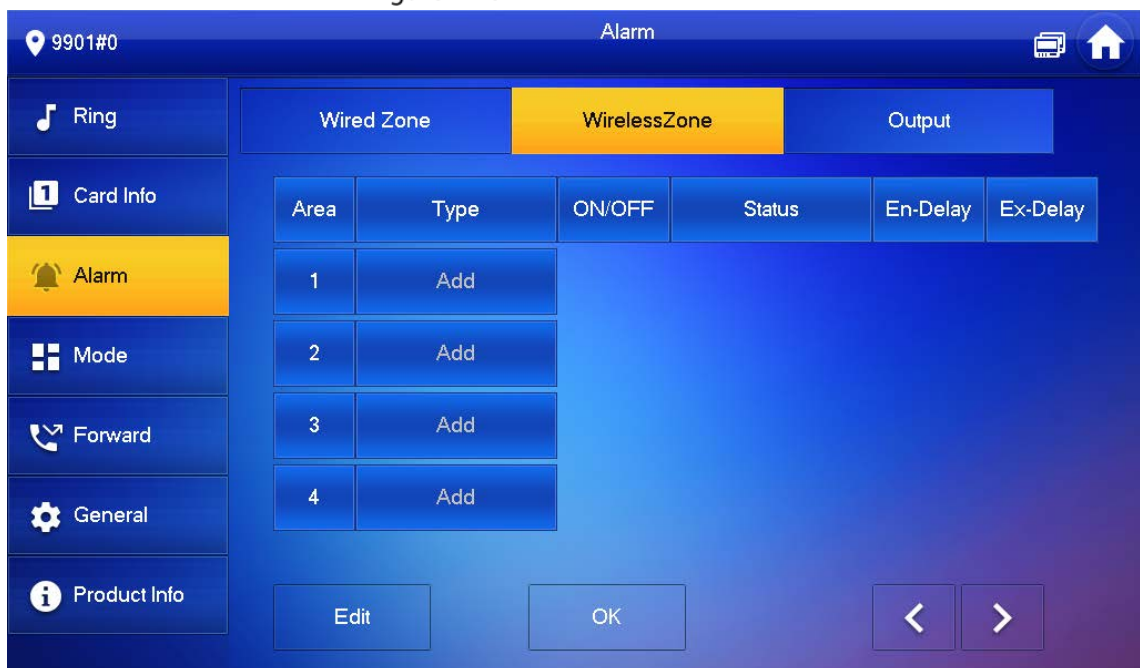
Step 2 Enter login password and tap **OK**.



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**.

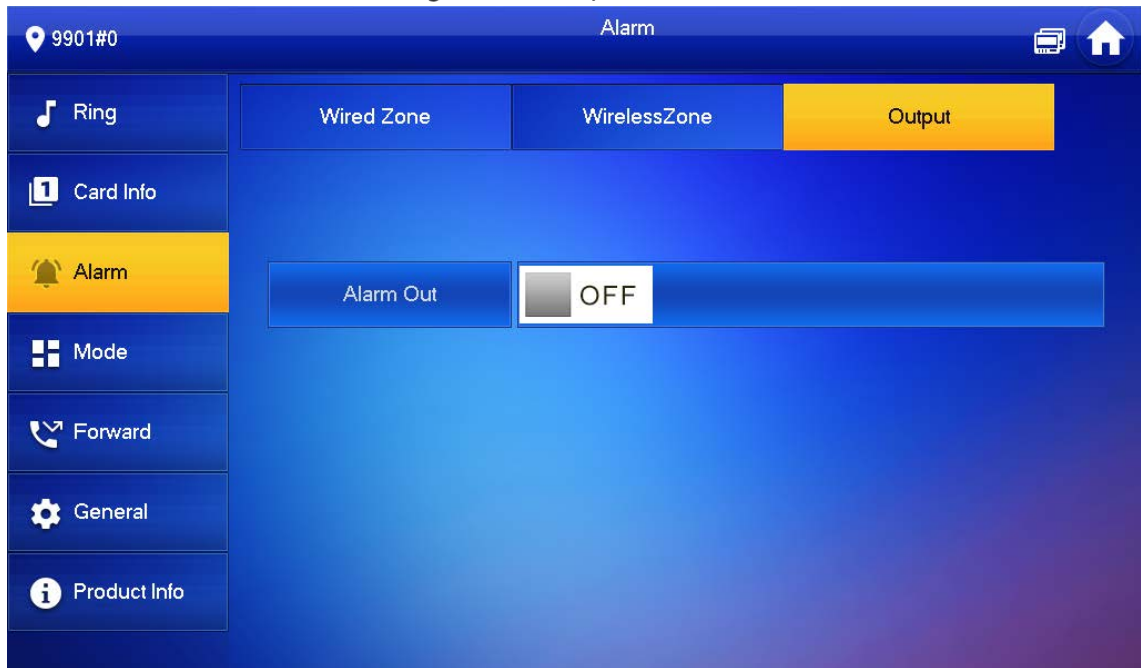
Step 2 Enter login password and tap **OK**.



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**.

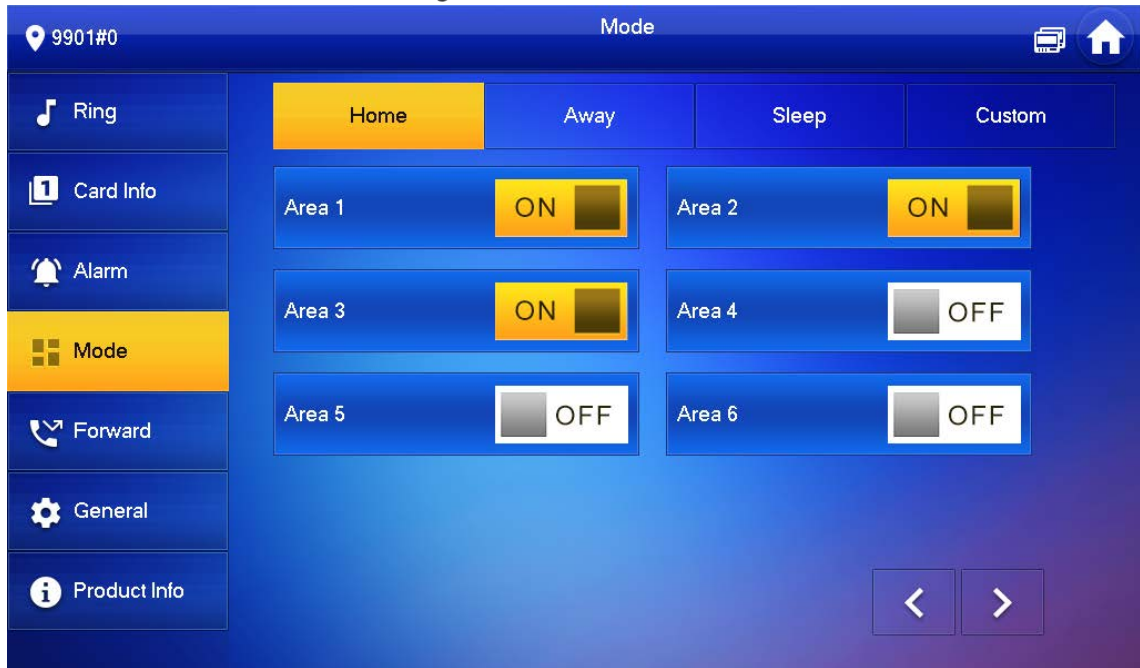
Step 2 Enter login password and tap **OK**.



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**.

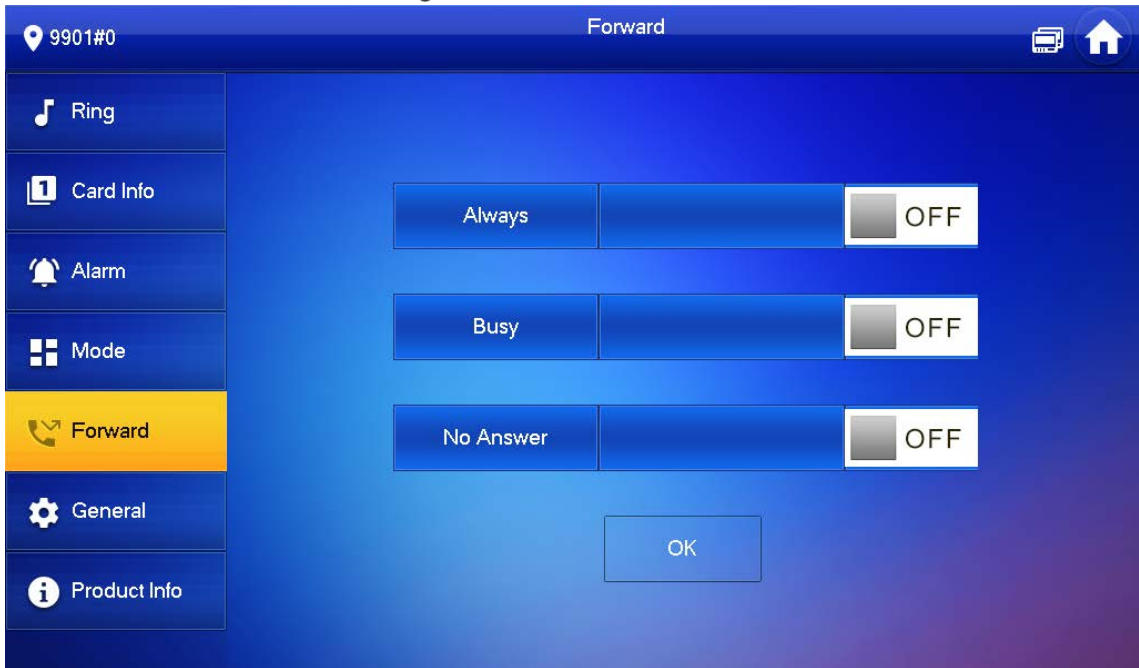
Step 2 Enter login password and tap **OK**.



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**.

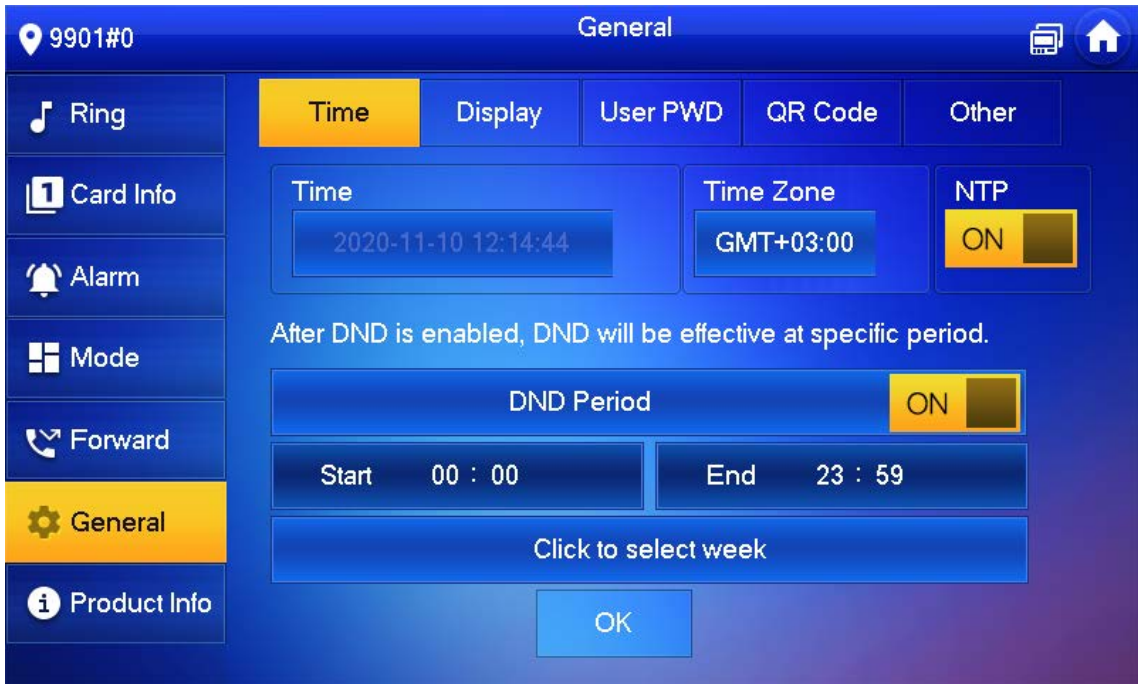
Figure 4-32 Set time and time zone



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**.

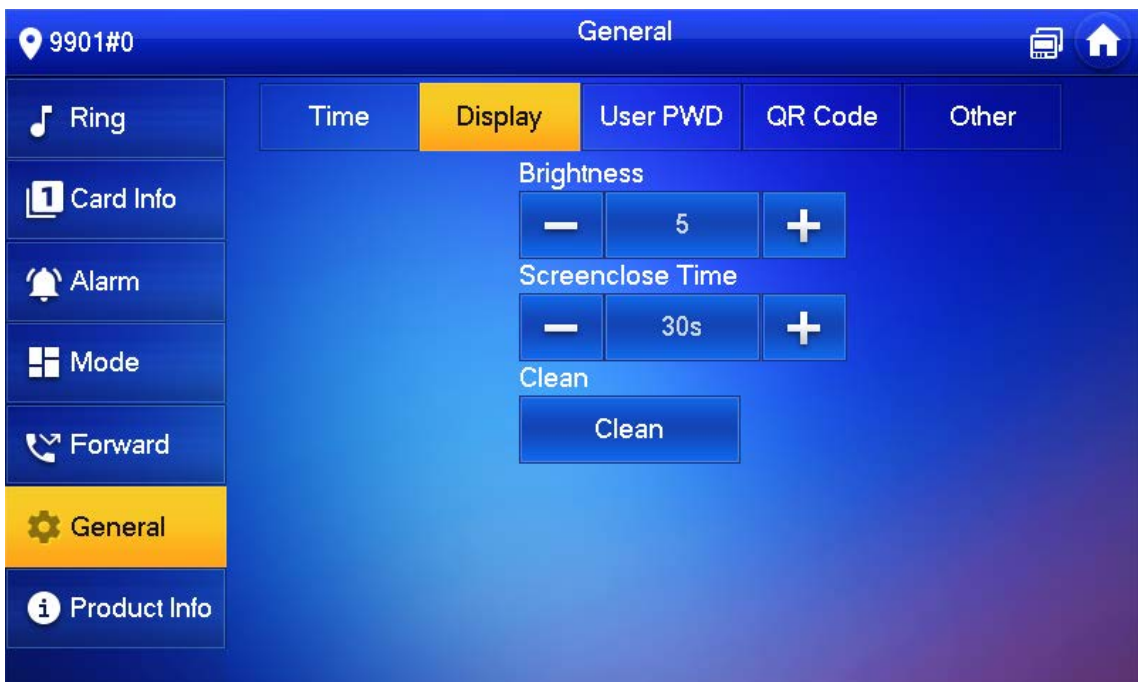
Step 2 Input login password and tap **OK**.





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.



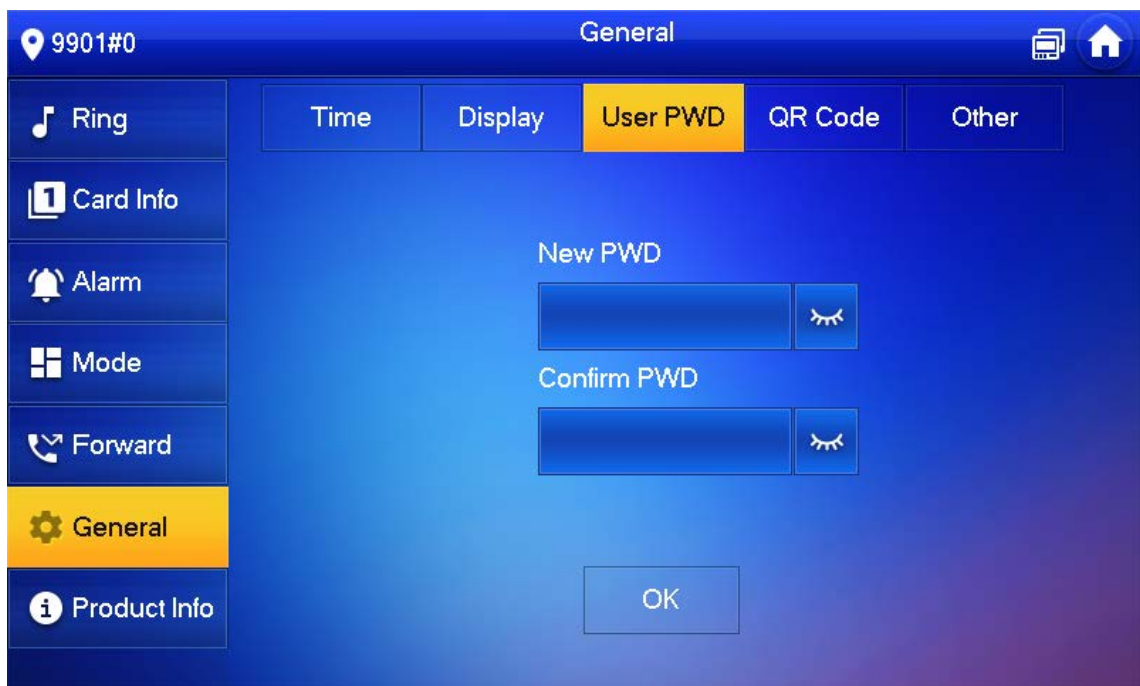
Parameters at this interface are set on main VTH only, and extension VTH synchronizes with main VTH.

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**.

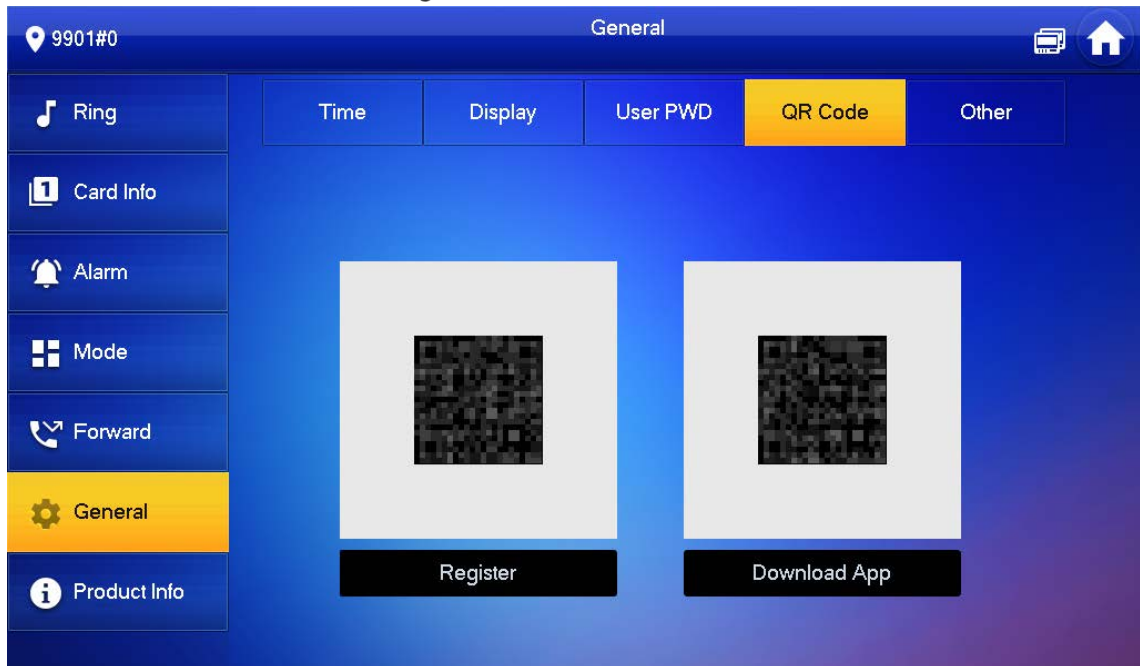
Step 2 Input login password and tap **OK**.



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

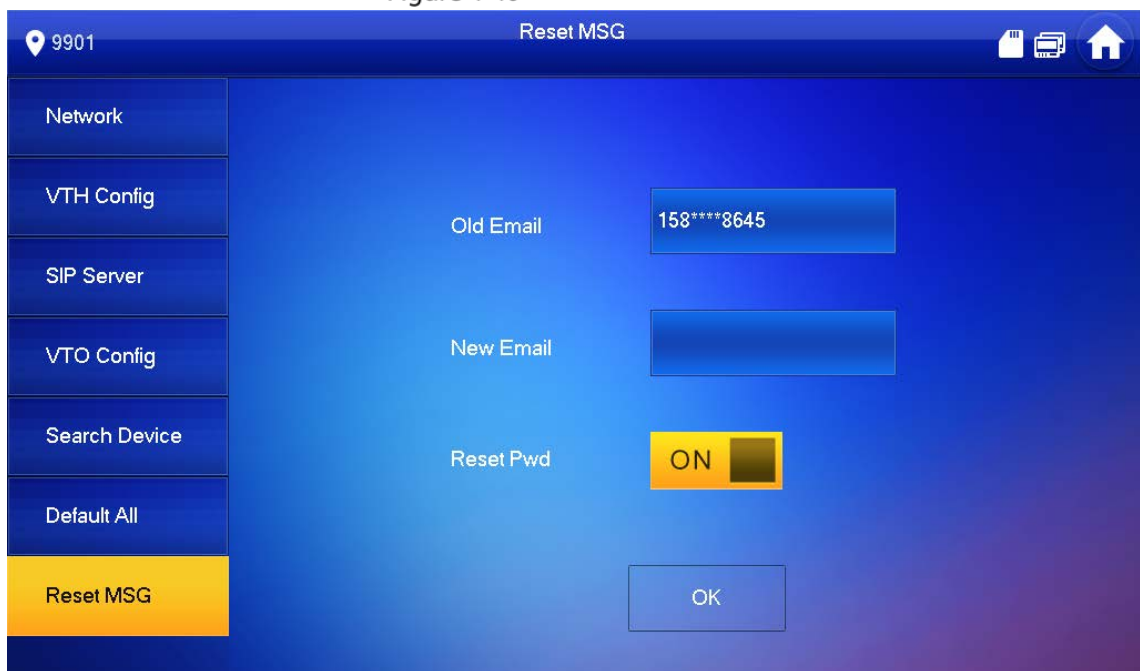
Modify the bonded Email.

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.

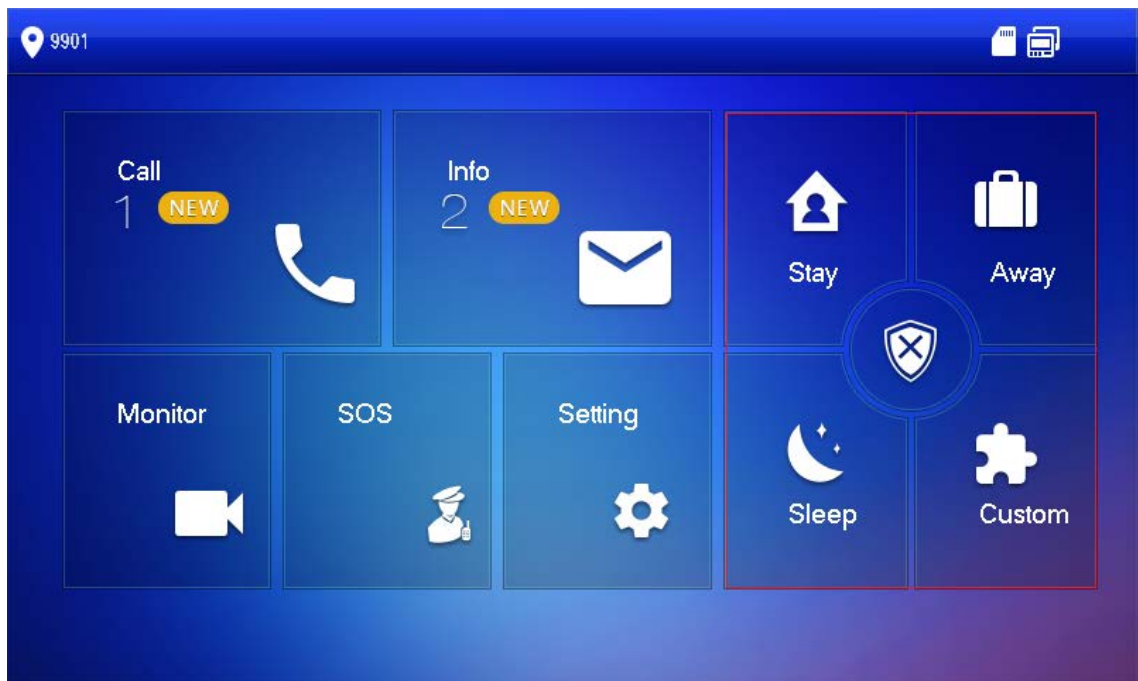


- Please ensure that the area has been added into arm mode. Otherwise, there will be no alarm triggering after arm.
- Please ensure that it is in disarmed status. Otherwise, arm will fail.



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.



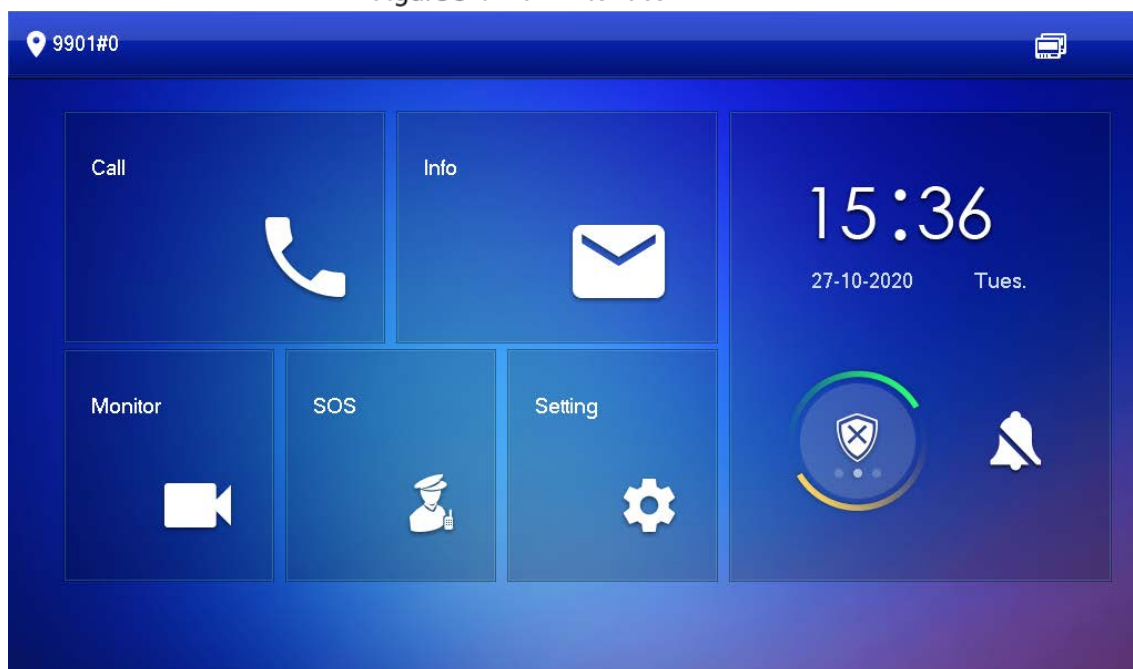
Interfaces and operations might vary between iOS and Android OS. This section takes Android OS as an example.

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**.

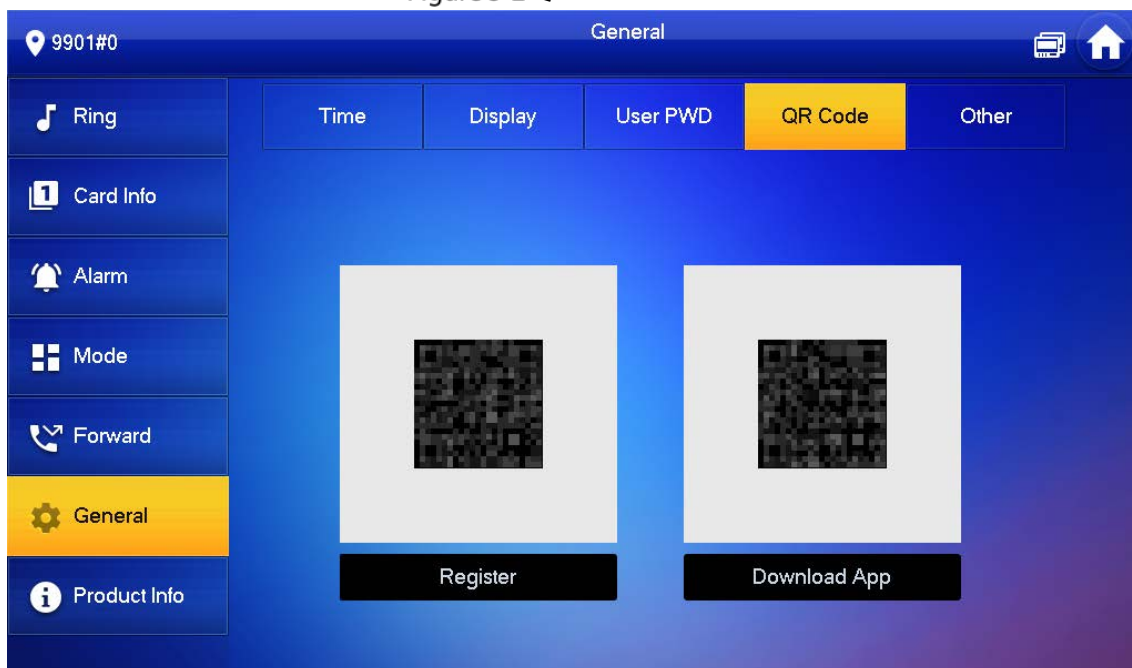
Figure 5-1 Main interface



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


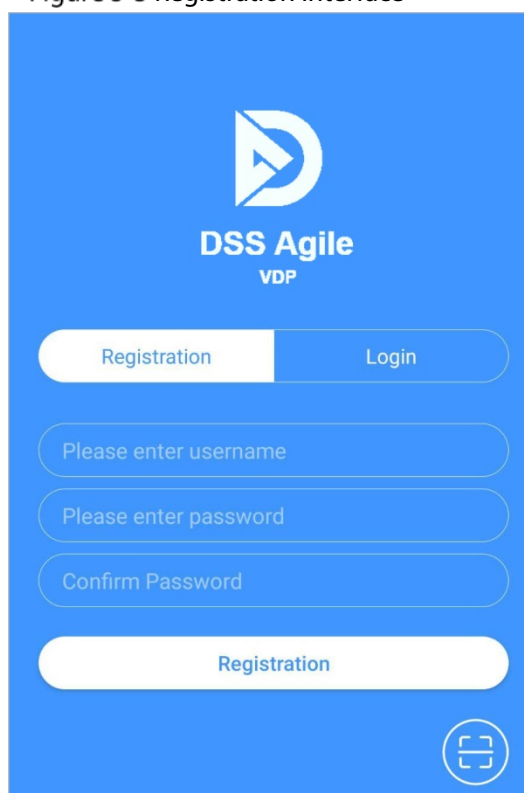
Step 1 Tap  on your smartphone, read the **Software license agreement and Privacy policy**, and then tap **Agree** (only for first-time login).

Figure 5-3 Registration interface




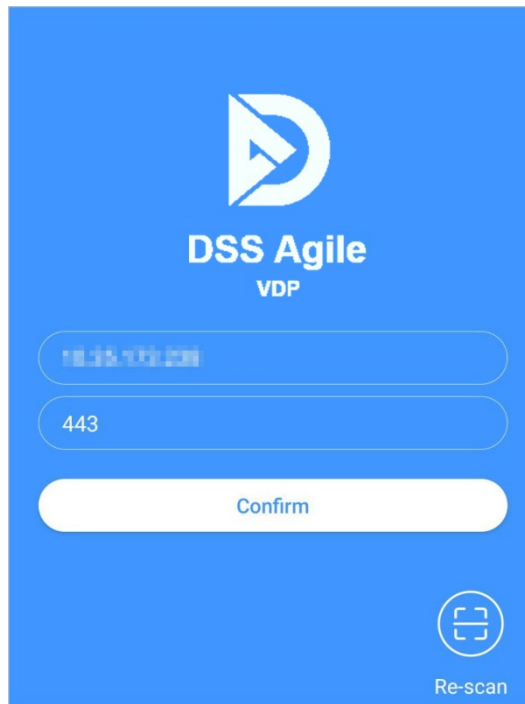
Step 2 Tap , and then scan the **Register** code on the VTH. See Step 2 in "5.1 Downloading the App".

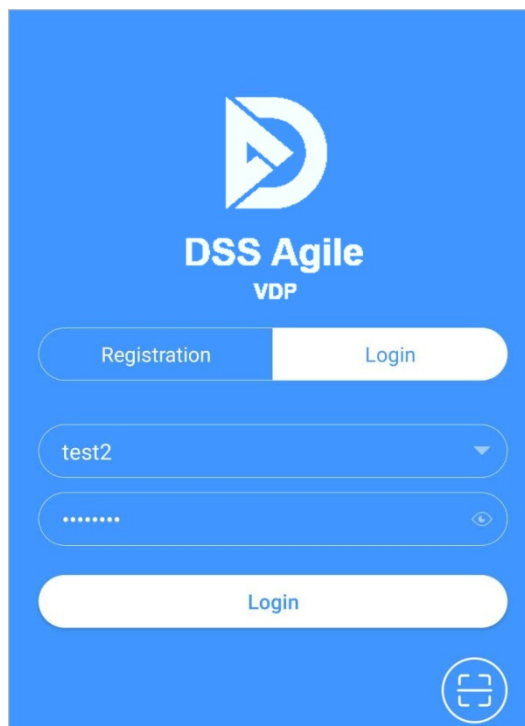
Figure 5-4 Confirm IP address and port number



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.

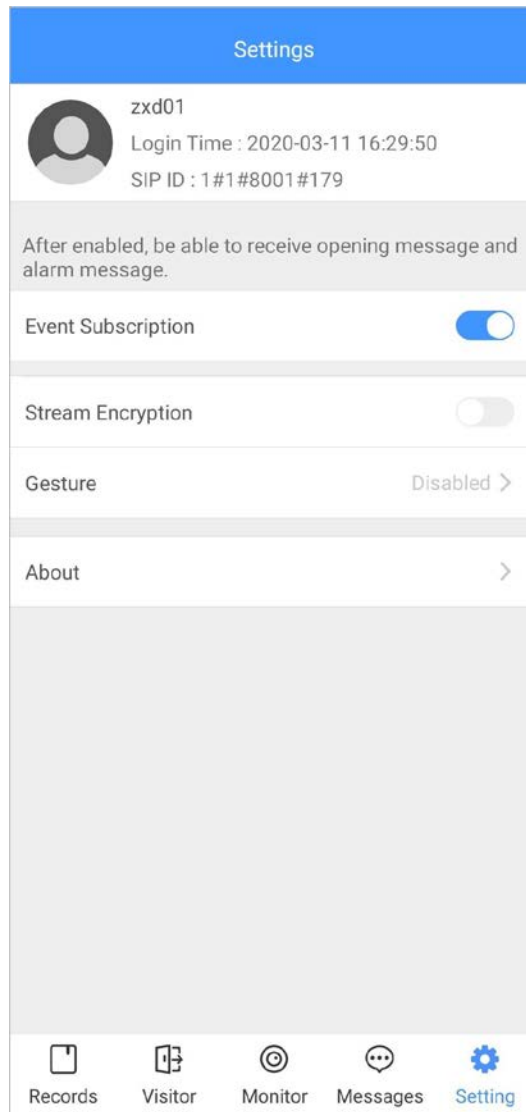
5.3.1 Forwarding Calls

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**.

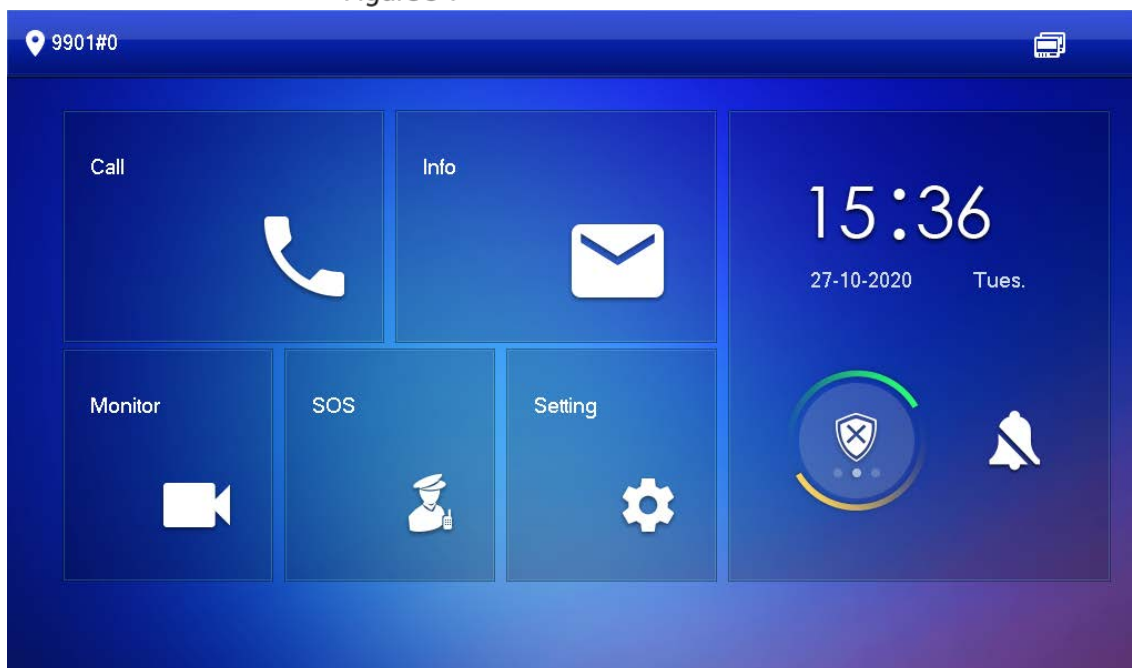
In the following example, the **SIP ID** is **1#1#8001#179**.

Figure 5-6 Settings



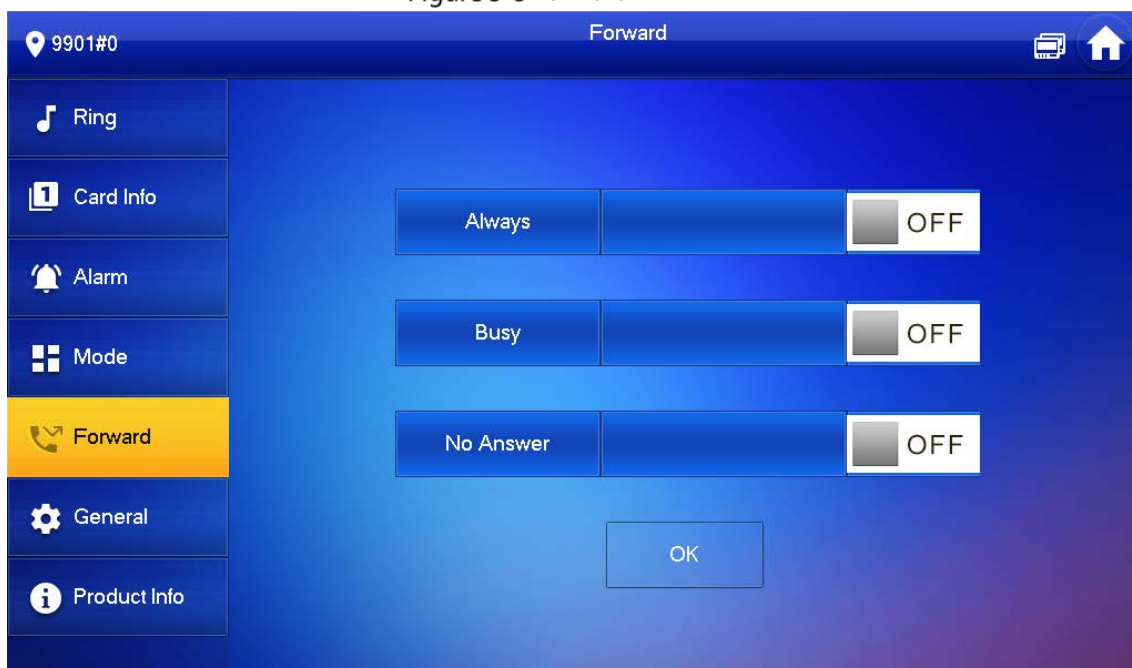
Step 2 On the VTH main interface, tap **Setting**.

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.

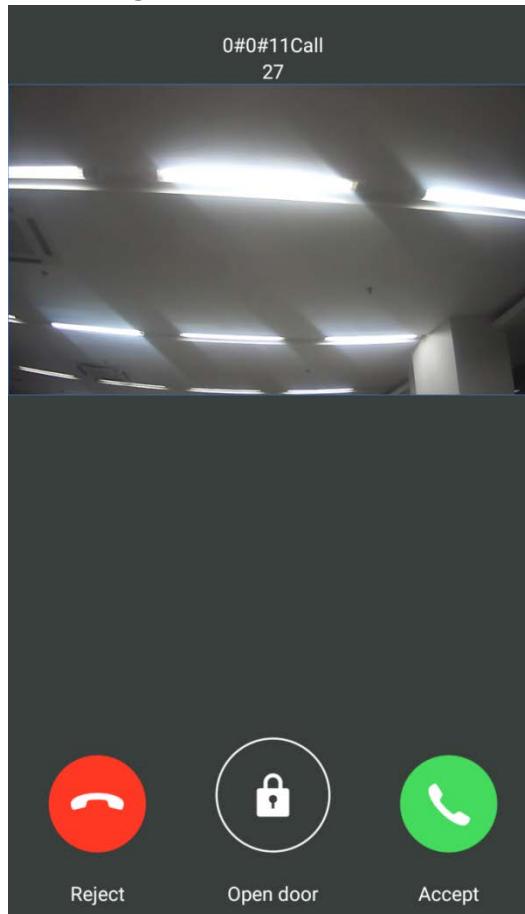
Step 5 Tap OFF to enable the forwarding type you selected, and then tap **OK**.

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

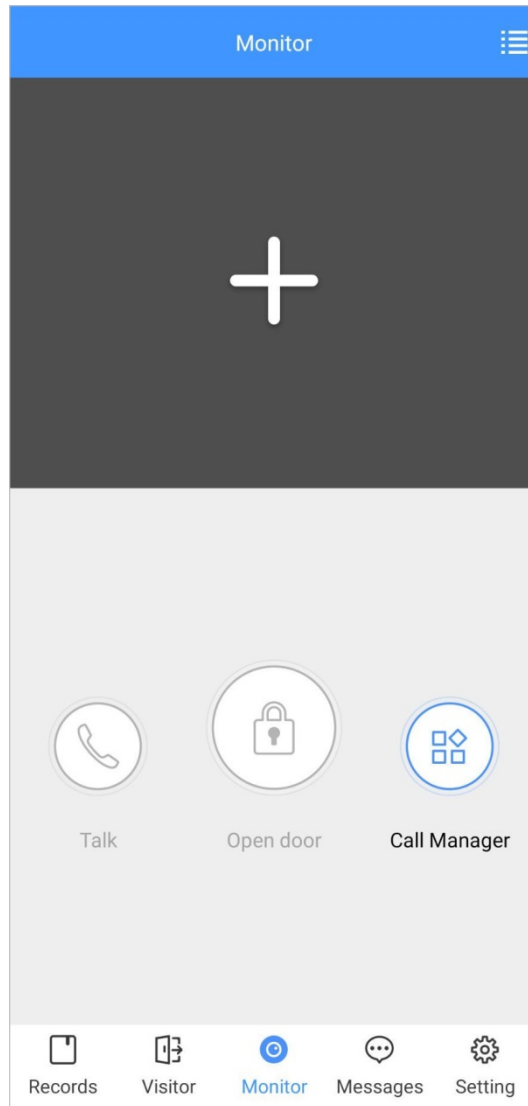


5.4 Monitoring

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




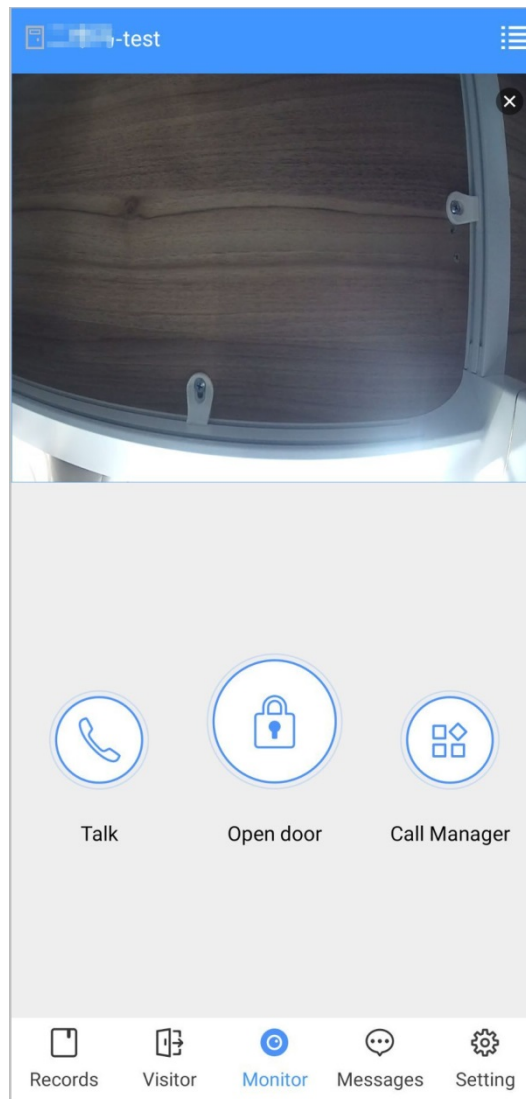




Step 2 Tap , select the VTO from the channel list as needed.

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.

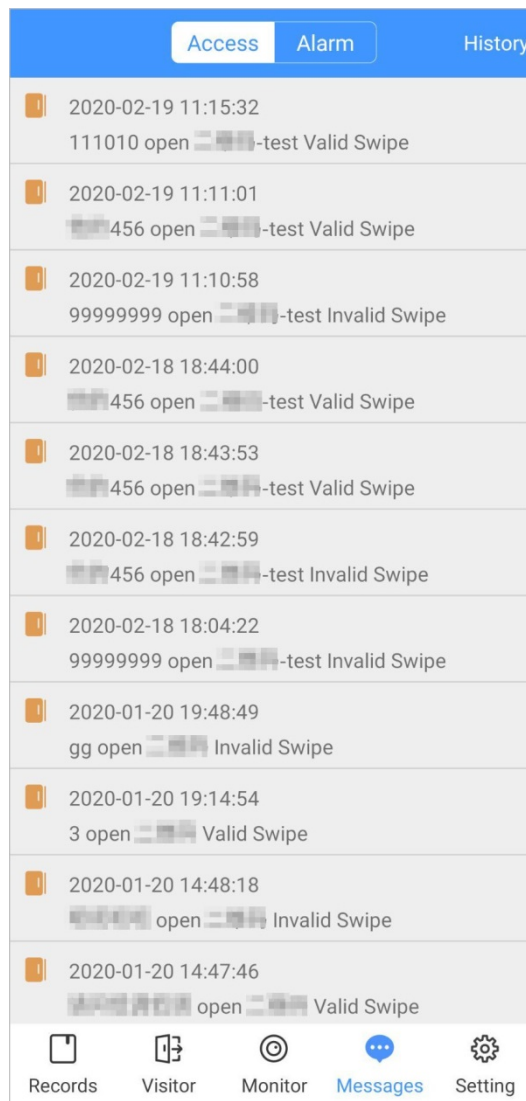


- You need to enable **Event Subscription** in **Setting** of the App first. See "5.7 Setting" for details.
- To receive messages on your smartphone, make sure that notifications of the app are enabled on your smartphone and the you are logged in to the app.

Viewing Messages

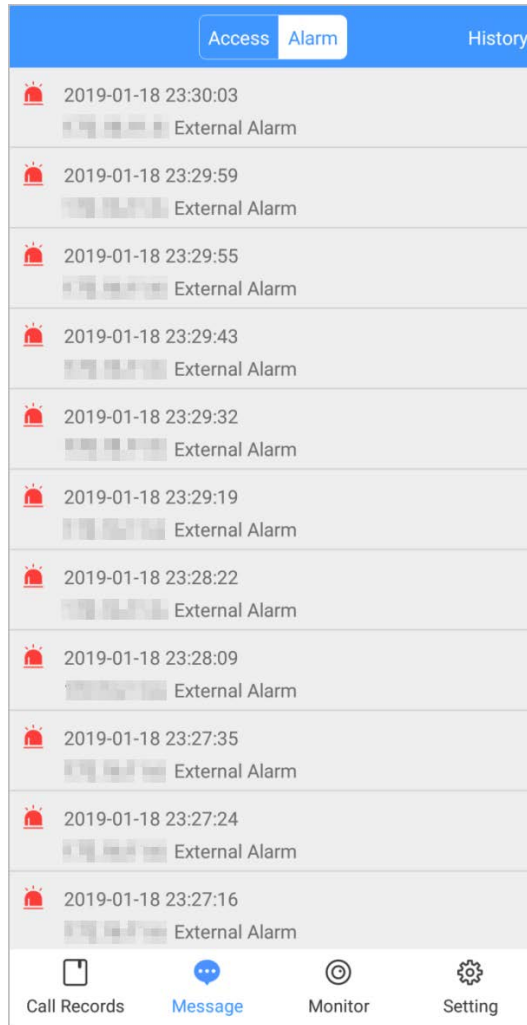
- Log in to the app, tap **Messages > Access**, and then you can view unlocking records, such as unlocking method, which user unlocked the door, and when the door is unlocked.

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

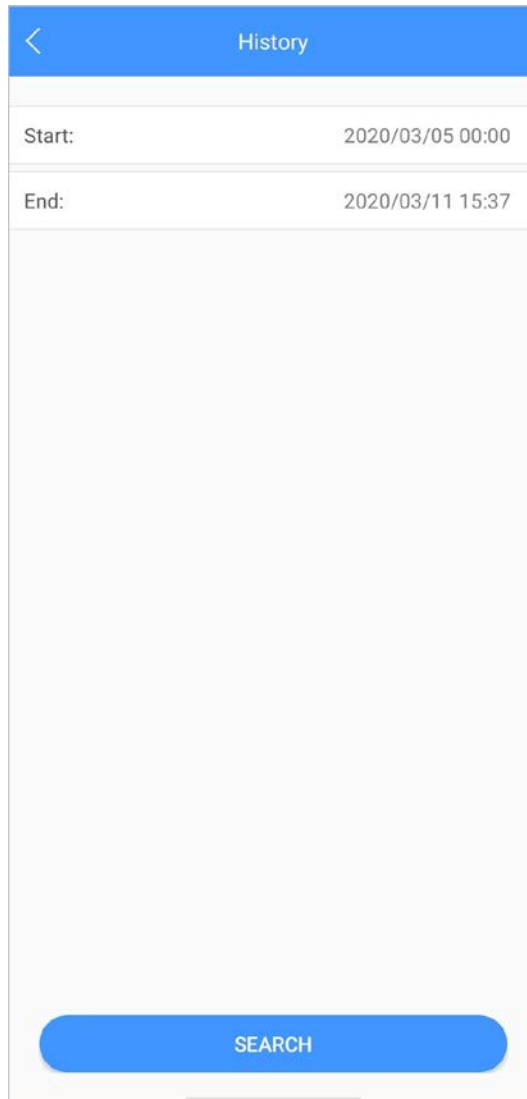


Searching for History Messages

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		

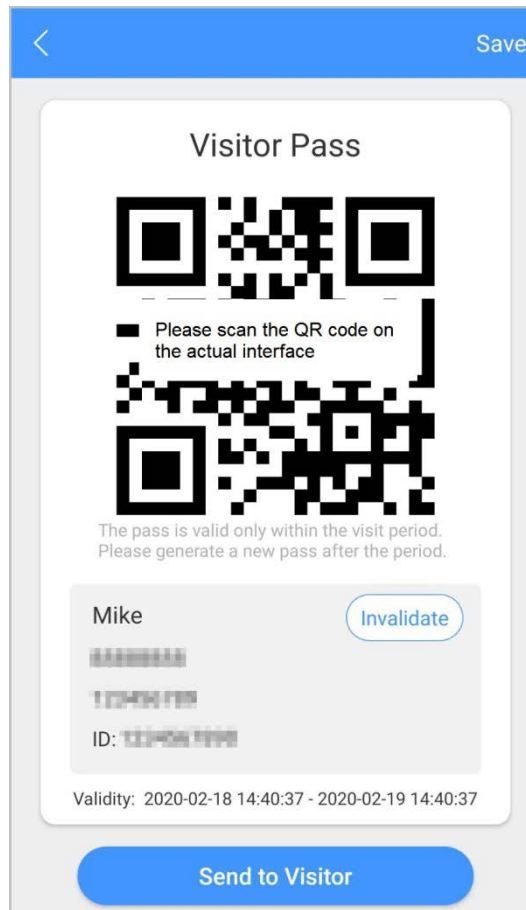
Records Visitor Monitor Messages Setting

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.



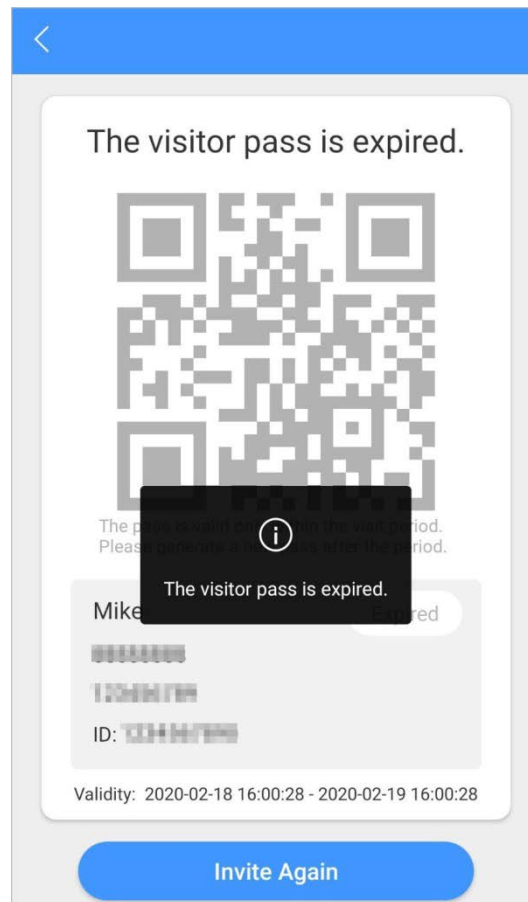
Tap **Save** to save the QR code to your smartphone.

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 displays the 'Visitor records' app interface. At the top, there are two tabs: 'Pass' and 'Record', with 'Record' being the active tab. Below the tabs is a list of visitor records, each consisting 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 >

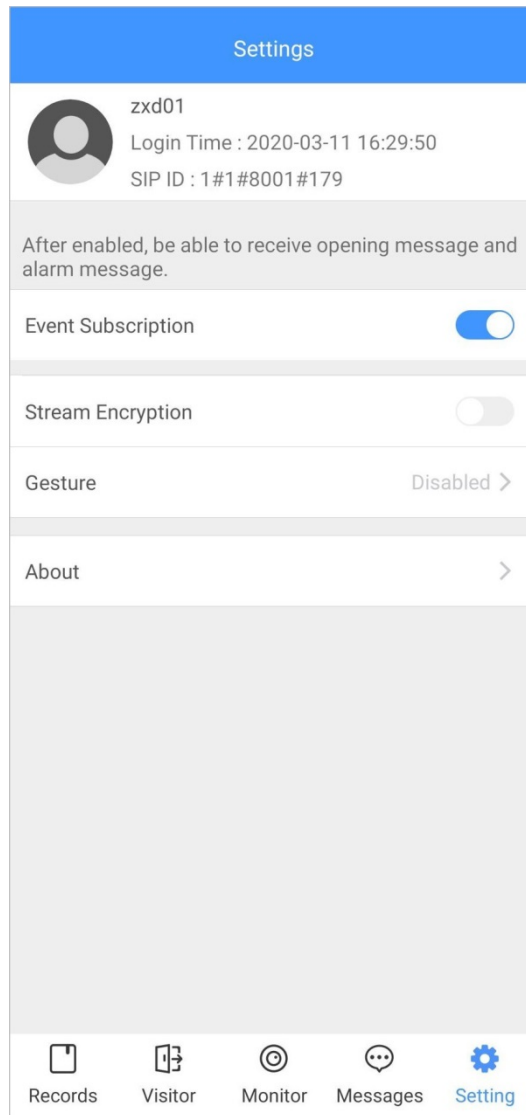
At the bottom of the screen is a navigation bar with five icons and their corresponding labels: 'Records' (document icon), 'Visitor' (blue person icon, highlighted), 'Monitor' (target icon), 'Messages' (speech bubble icon), and 'Setting' (gear icon).

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.

Villa Door Station (Version 4.3)

Quick Start Guide






Foreword

General

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

Safety Instructions

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

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

Revision History

Version
V1.0.0

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

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

Operating Requirement

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

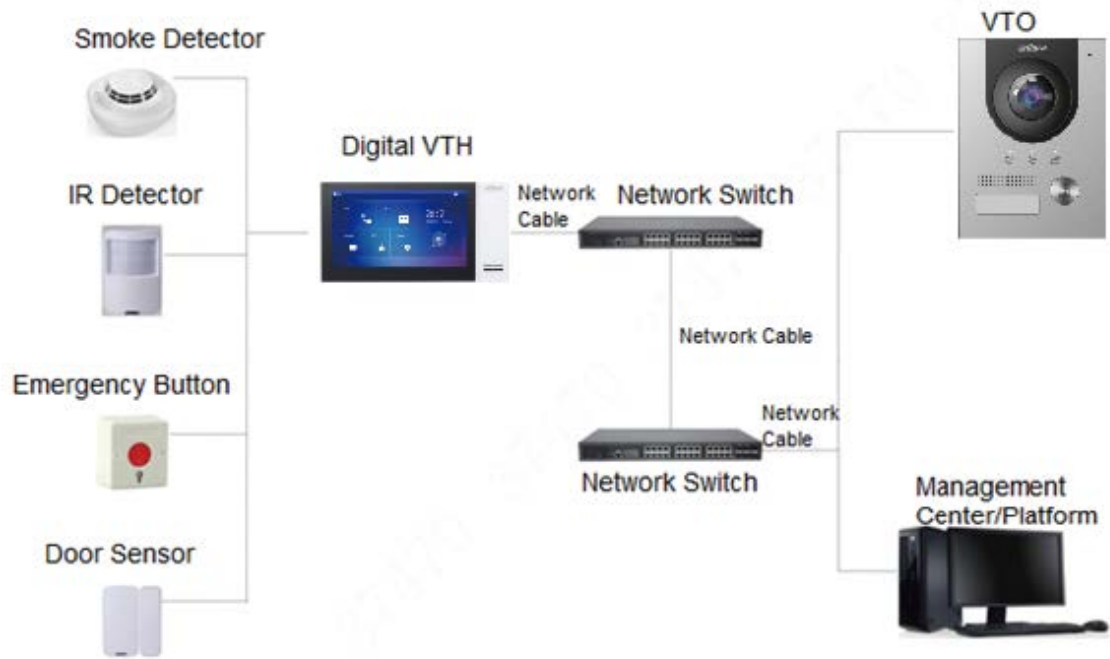
Power Requirement

- The product shall use electric wires (power wires) required by the region where the device will be used.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.

Table of Contents

Foreword	I
Important Safeguards and Warnings	II
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 VTO3211D-P	3
2.2.1 Front Panel	3
2.2.2 Rear Panel	4
2.3 VTO2211G/VTO1201G.....	6
2.3.1 Front Panel	6
2.3.2 Rear Panel	7
3 Installation	10
3.1 Notice	10
3.2 Guidance	10
4 Configuration	11
4.1 Configuration Process	11
4.2 VDPConfig.....	11
4.3 Configuring VTOs.....	11
4.3.1 Initialization	11
4.3.2 Configuring VTO Number	12
4.3.3 Configuring Network Parameters.....	13
4.3.4 Configuring SIP Server	14
4.3.5 Configuring Call No. and Group Call.....	15
4.3.6 Adding VTO	15
4.3.7 Adding Room Number.....	16
4.4 Verifying Configuration.....	18
4.4.1 Calling VTH from VTO	18
4.4.2 Watching Monitoring Videos on the VTH	18
5 App Installation and Adding Device	20
5.1 Adding through Wired Network.....	22
5.2 Adding through Soft Access Point (AP)	23
Appendix 1 Cybersecurity Recommendations	31

1 Network Diagram



2 Appearance

2.1 VTO2101E-P

2.1.1 Front Panel

Figure 2-1 VTO2101E-P

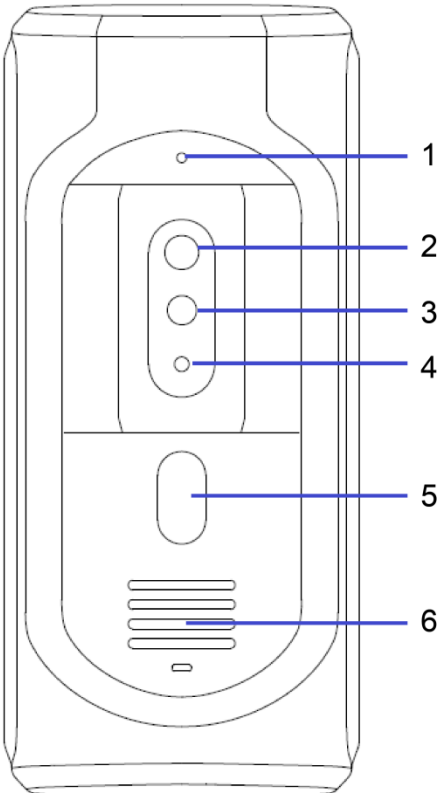


Table 2-1 Front panel description

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

2.1.2 Rear Panel

Figure 2-2 VTO2101E-P

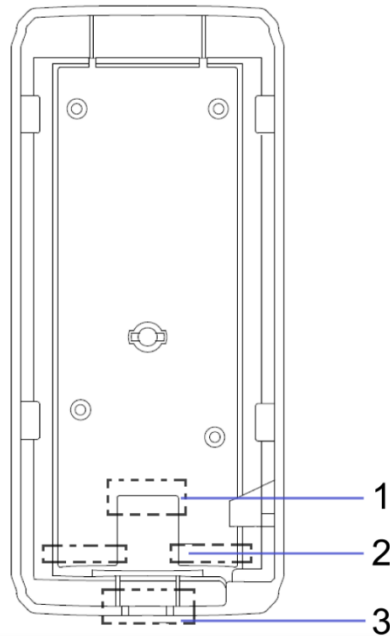


Table 2-2 Rear panel description

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

Figure 2-3 Cable connection

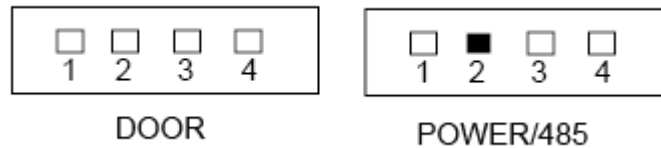


Table 2-3 Port description

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

2.2 VTO3211D-P

2.2.1 Front Panel

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

Figure 2-4 VTO3211D-P

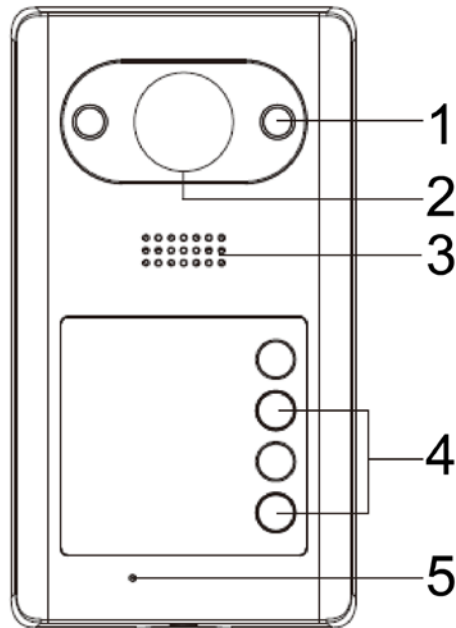


Table 2-4 Front panel description

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

2.2.2 Rear Panel

Figure 2-5 VTO3211D-P

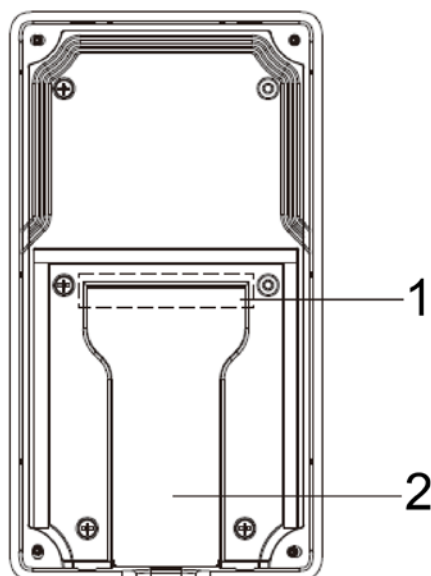


Table 2-5 Rear panel description

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

Figure 2-6 Cable connection

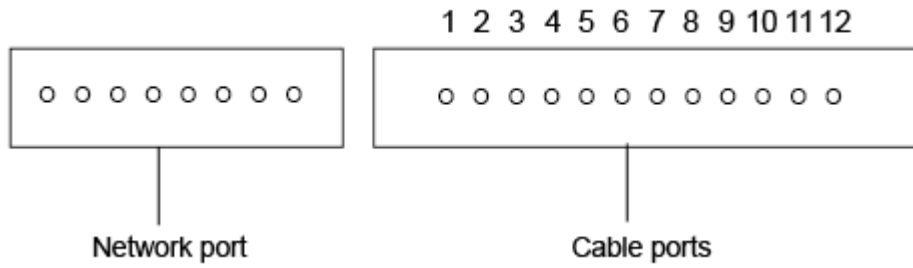


Table 2-6 Cable port description

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

2.3 VTO2211G/VTO1201G

2.3.1 Front Panel

Figure 2-7 Front panel of VTO2211G/VTO1201G

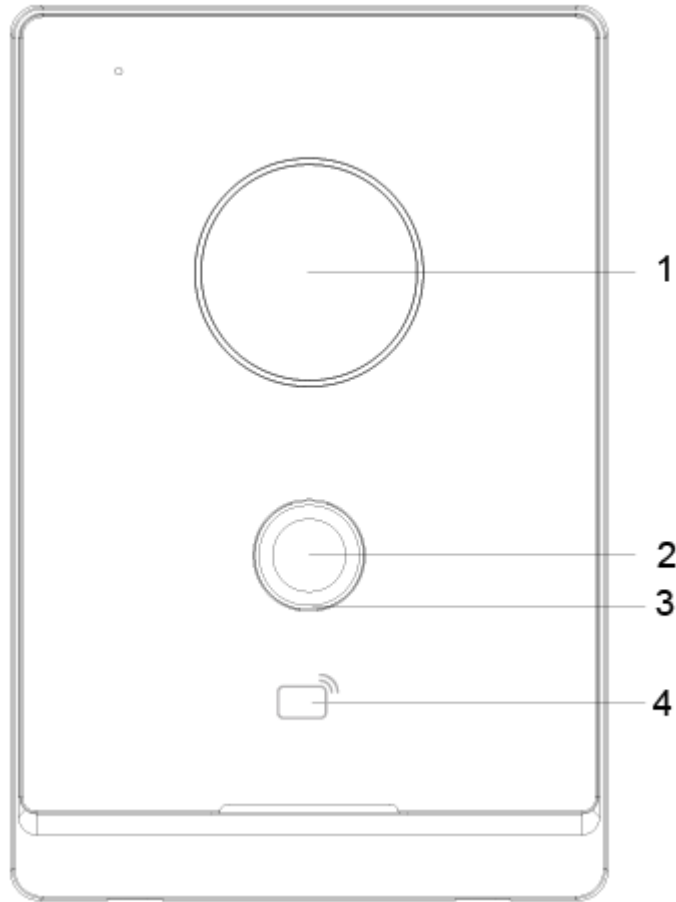


Table 2-7 Front panel description

No.	Description
1	Camera
2	Press the button to call an indoor monitor VTH or the management center.
3	Indicator light. <ul style="list-style-type: none">● Off: The device in standby mode;● Solid green: VTO making a call;● Solid blue: VTO during a call;● Yellowish green: When you unlock the door through VTH while VTO is making a call.● Bluish red: When you unlock the door through VTH while you are having a call with the VTO;● Green breathing light: The network is disconnected.
4	Card reader (only for VTO2211G).

2.3.2 Rear Panel

Figure 2-8 Rear panel of VTO2211G/VTO1201G

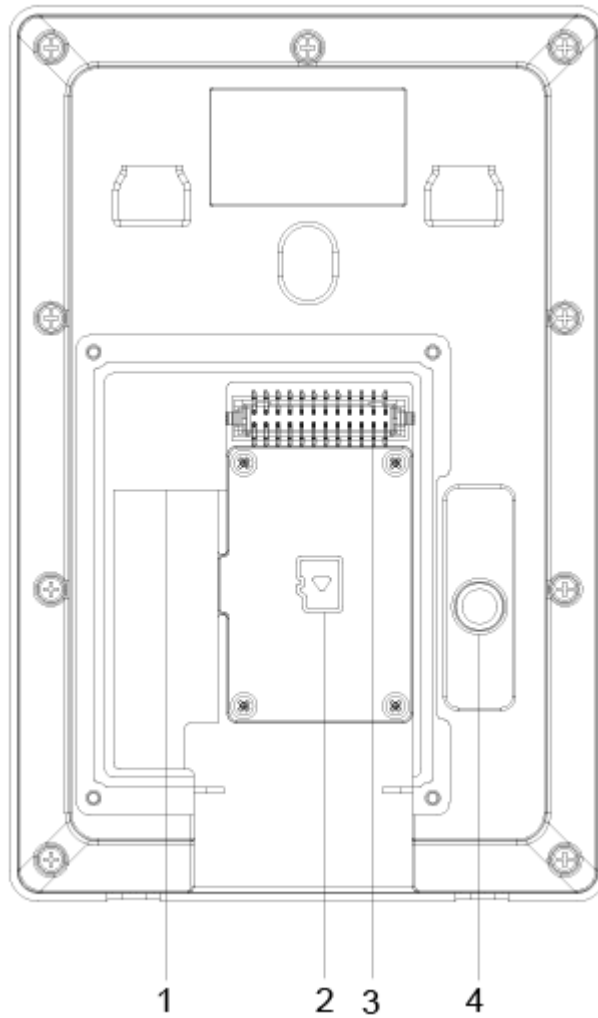


Table 2-8 Rear panel description

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

Figure 2-9 VTO2211G cable connection

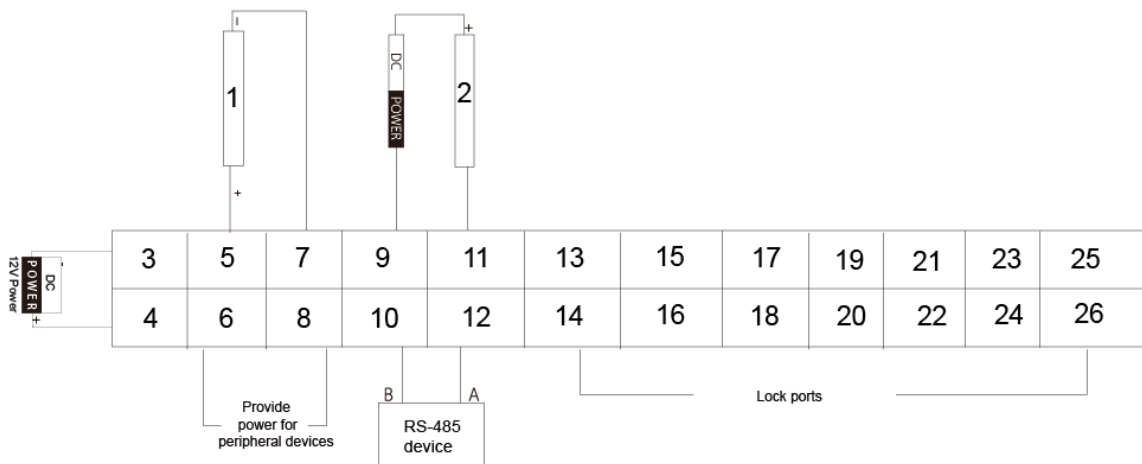


Table 2-9 Port description

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

Figure 2-10 VTO1201G cable connection

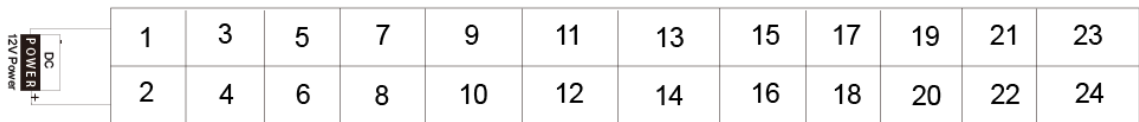


Table 2-10 Port description

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

Figure 2-11 Connecting lock cables

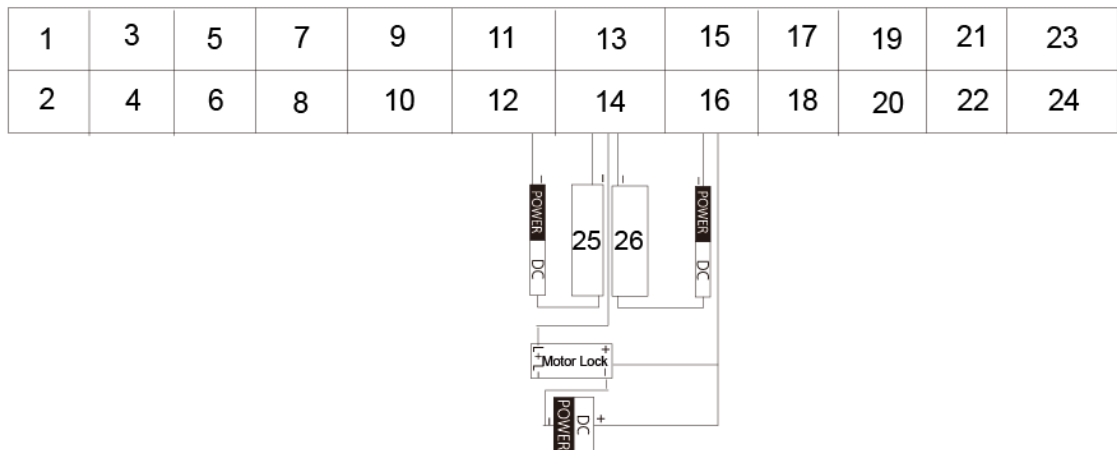


Table 2-11 Port description

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

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

3 Installation

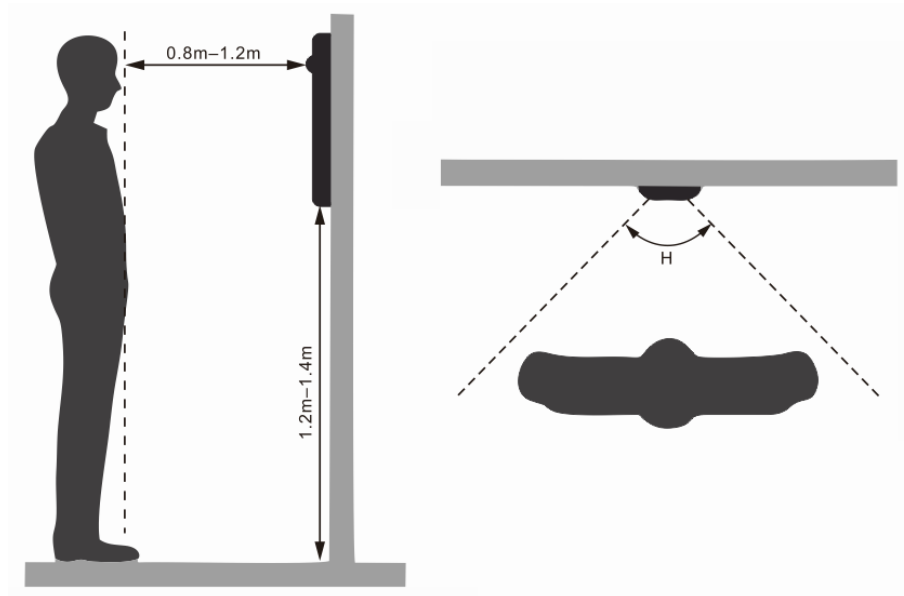
3.1 Notice

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

3.2 Guidance

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

Figure 3-1 Installation position reference



4 Configuration

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

4.1 Configuration Process



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

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

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

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

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

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

4.2 VDPConfig

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

4.3 Configuring VTOs

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

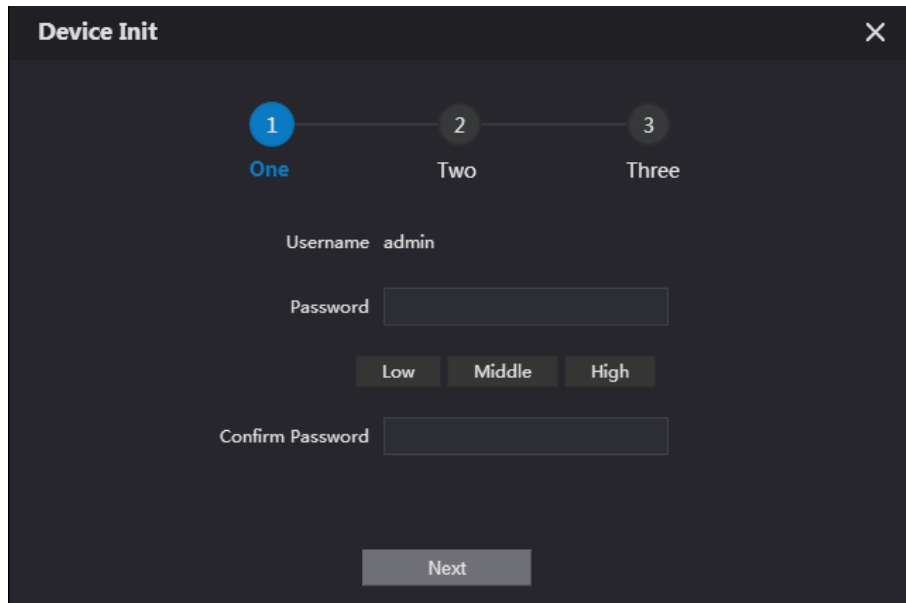
4.3.1 Initialization

The default IP address of VTO is 192.168.1.110, and make sure the PC is in the same network segment as the VTO.

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

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

Figure 4-1 Device initialization



Device Init

1 One 2 Two 3 Three

Username admin

Password

Low Middle High

Confirm Password

Next

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

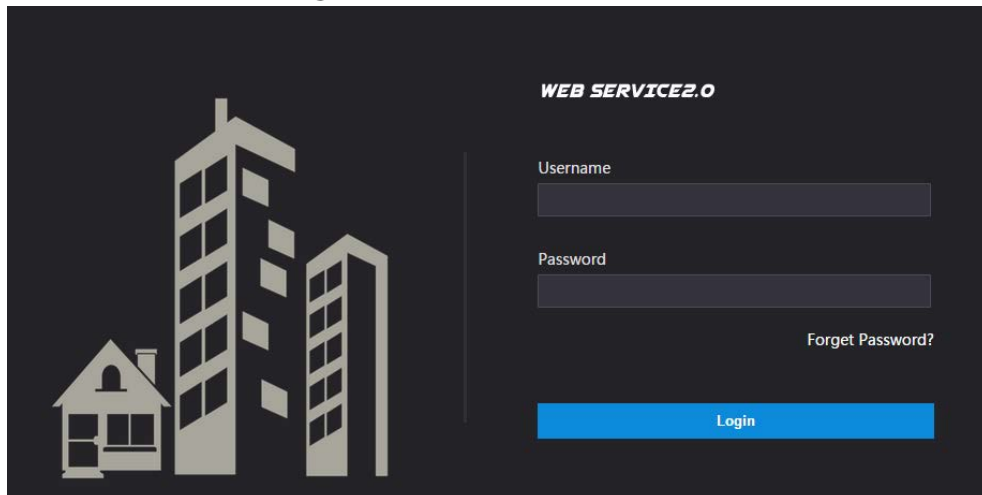
The email setting interface is displayed.

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

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

Step 6 Click **OK**.

Figure 4-2 Login interface



WEB SERVICE2.0

Username

Password

[Forget Password?](#)

Login

4.3.2 Configuring VTO Number

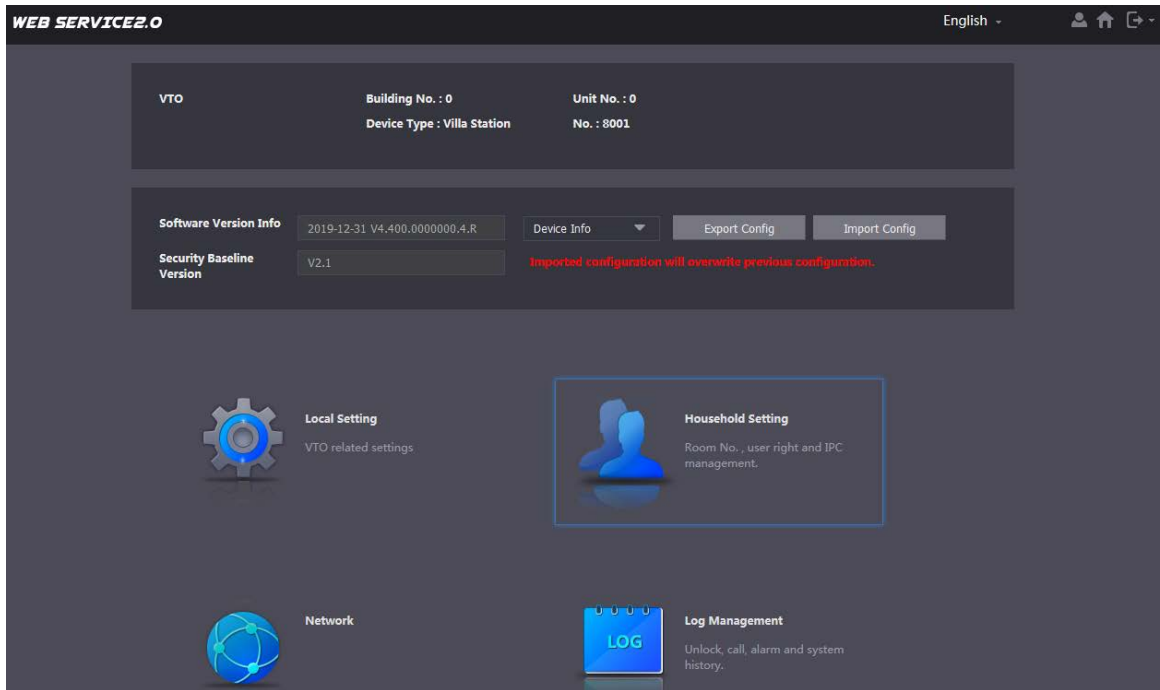
The VTO number can be used to differentiate each VTO, and it is normally configured according to apartment or building number.



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

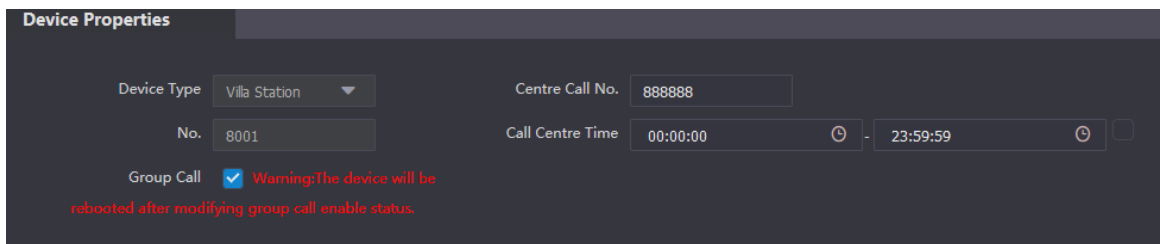
Step 1 Log in to the web interface of the VTO, and then the main interface is displayed.

Figure 4-3 Main interface



Step 2 Select Local Setting > Basic.

Figure 4-4 Device properties

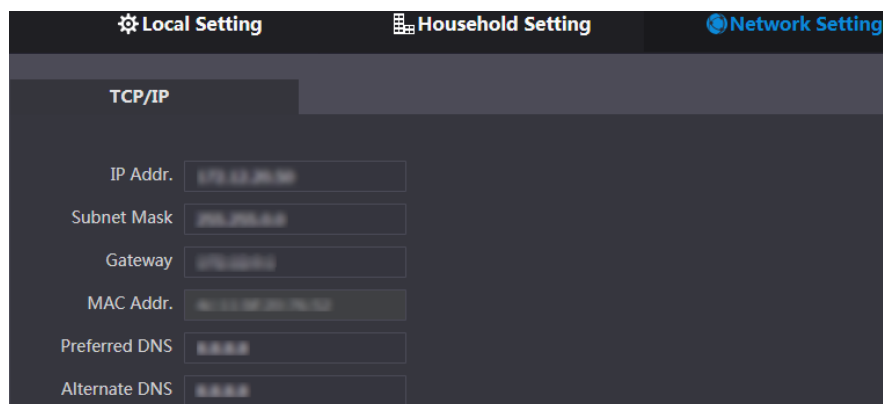


Step 3 In the **No.** input box, enter the VTO number you planned for the VTO you are operating, and then click **Confirm** to save.

4.3.3 Configuring Network Parameters

Step 1 Select Network Setting > Basic.

Figure 4-5 TCP/IP information



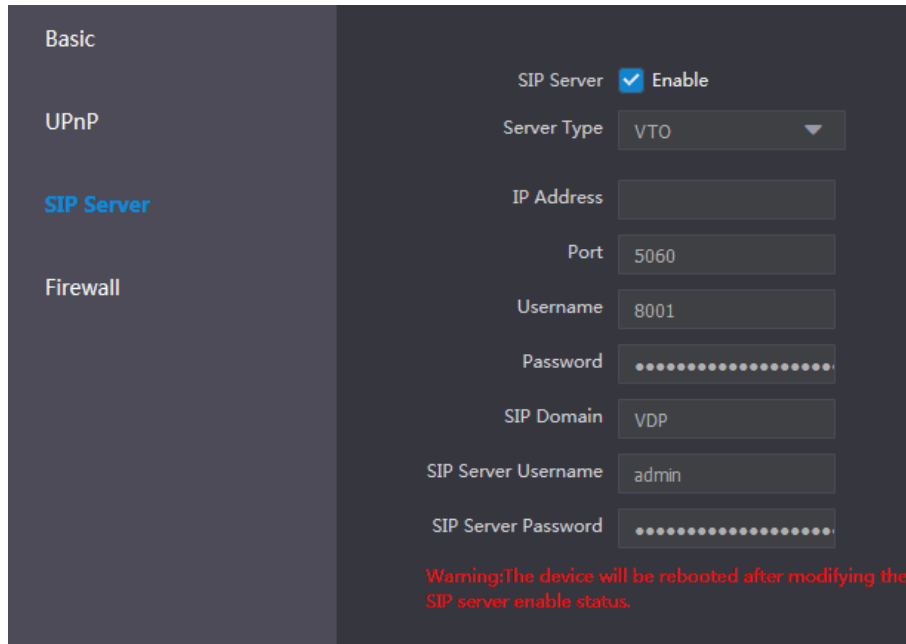
Step 2 Enter the network parameters you planned, and then click **Save**.
The VTO will restart, and you need to modify the IP address of your PC to the same network segment as the VTO to log in again.

4.3.4 Configuring SIP Server

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

Step 1 Select Network Setting > SIP Server.

Figure 4-6 SIP server



Step 2 Select the server type you need.


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

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

Table 4-1 SIP server configuration

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

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

4.3.5 Configuring Call No. and Group Call

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



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

Step 1 Select Local Setting > Basic.

Figure 4-7 Device properties

Device Properties

Device Type: Villa Station

No.: 8001

Centre Call No.: 888888

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 VTO web interface.

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

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

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

4.3.6 Adding VTO

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

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

Figure 4-8 VTO No. management

WEB SERVICE 2.0

Local Setting Household Setting Network Setting Log Management

VTO No. Management

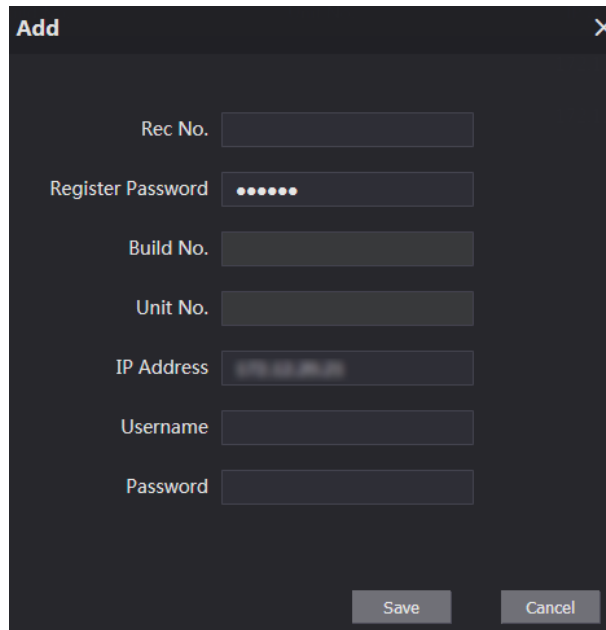
VTO No.	Build No.	Unit No.	IP Address	Modify	Delete
41			192.168.1.101		
51			192.168.1.102		

Add Clear

1/1 Go to

Step 2 Click **Add**.

Figure 4-9 Add VTOs



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

Table 4-2 Add VTOs

Parameter	Description
Rec No.	The VTO number you configured for the target VTO. See the details in "4.3.2 Configuring VTO Number."
Register Password	Keep default value.
Build No.	Available only when other servers work as SIP server.
Unit No.	
IP Address	The IP address of the target VTO.
Username	The user name and password for the web interface of the target VTO.
Password	

Step 4 Click **Save**.

4.3.7 Adding Room Number

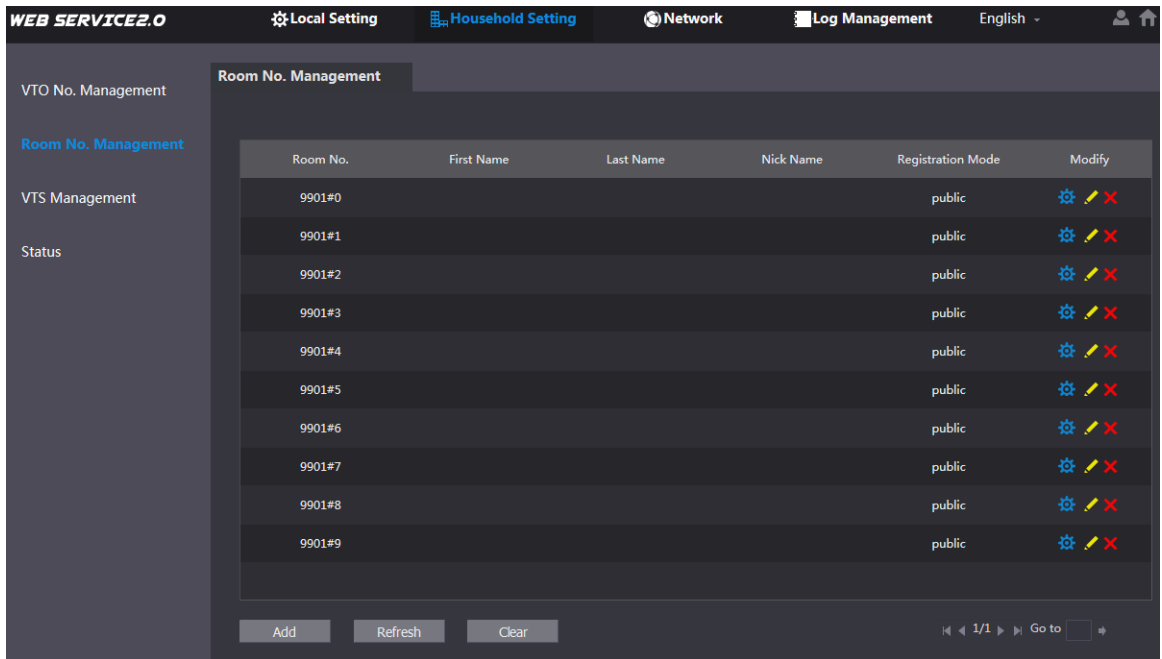
You can add the planned room number to the SIP server, and then configure the room number on VTHs to connect them to the network. This section applies to the condition in which a VTO works as SIP server, and if you use other servers as SIP server, see the corresponding manual for the detailed configuration.



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

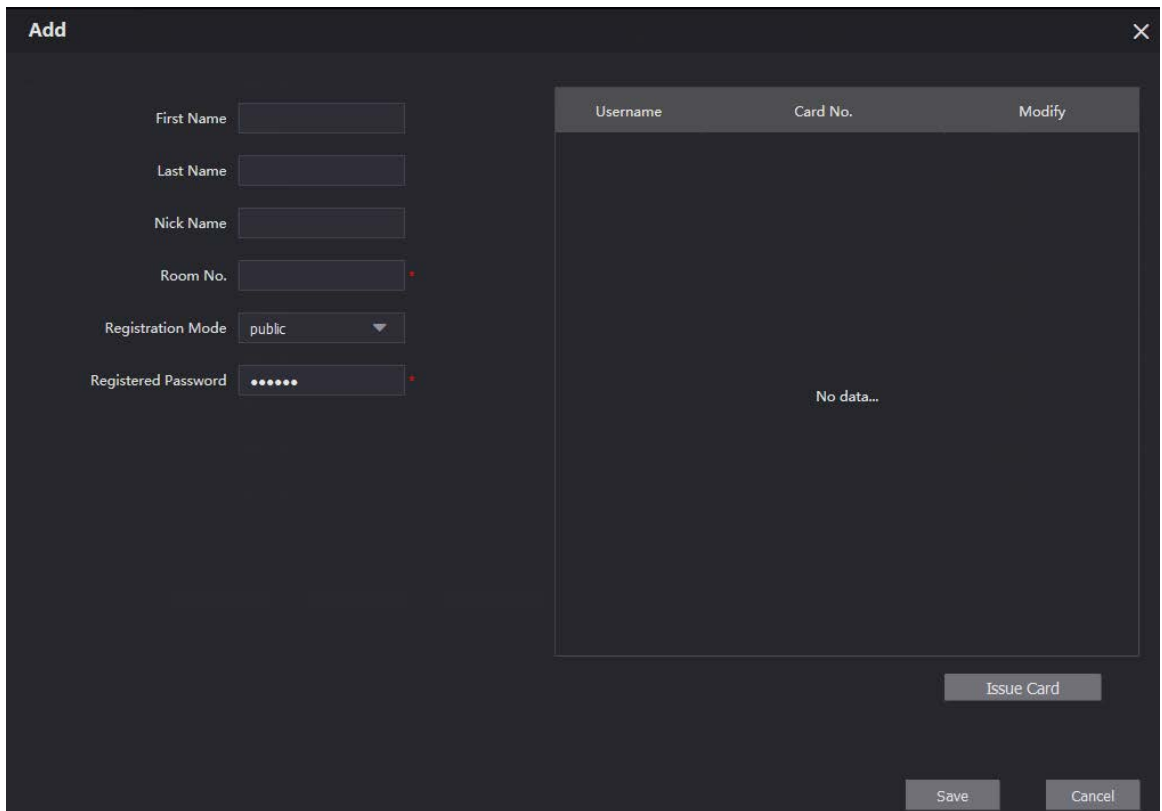
Step 1 Log in to the web interface of the SIP server, and then select **Household Setting > Room No. Management**.

Figure 4-10 Room No. Management



Step 2 Click **Add**.


Figure 4-11 Add single room number





Step 3 Configure room information.

Table 4-3 Room information

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

Parameter	Description
First Name	Enter the information you need to differentiate each room.
Last Name	
Nick Name	
	 <ul style="list-style-type: none"> If you use multiple VTHs, the room number of the master VTH should be "room number#0", and the room number of the extension VTH should be "room number#1", "room number#2", and so on. You can have 9 extension VTHs at most for one master VTH.
Registration Mode	Select public , and local is reserved for future use.
Registered Password	Keep the default value.

Step 4 Click **Save**.

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

4.4 Verifying Configuration

4.4.1 Calling VTH from VTO

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

Figure 4-12 Call screen



Tap  on the VTH to answer the call.

4.4.2 Watching Monitoring Videos on the VTH

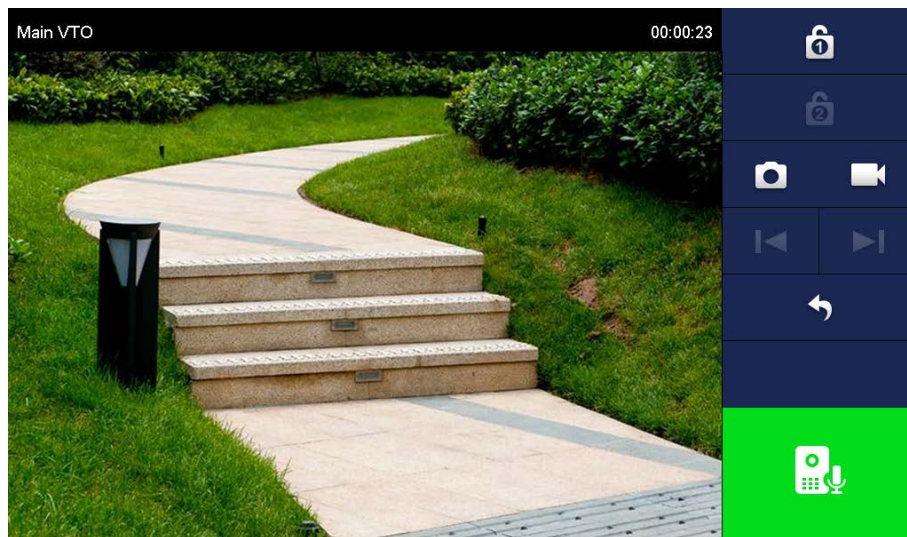
Step 1 In the main interface of the VTH, select **Monitor > Door**.

Figure 4-13 Door



Step 2 Select a VTO to watch monitoring videos.

Figure 4-14 Watching monitoring videos



5 App Installation and Adding Device

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



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


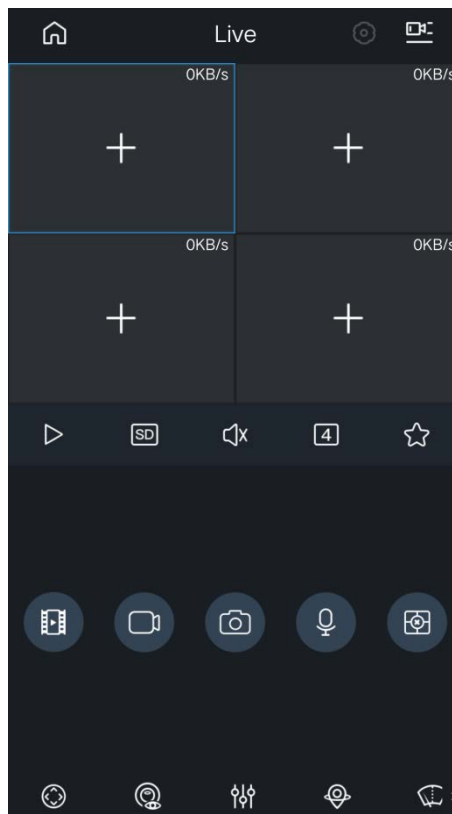
- Step 1** On your mobile phone, tap , and then follow the onscreen instructions until the region selection interface is displayed.
- Step 2** Select a region.
- Step 3** Tap **Done** on the upper right corner of the interface.

Figure 5-1 Live




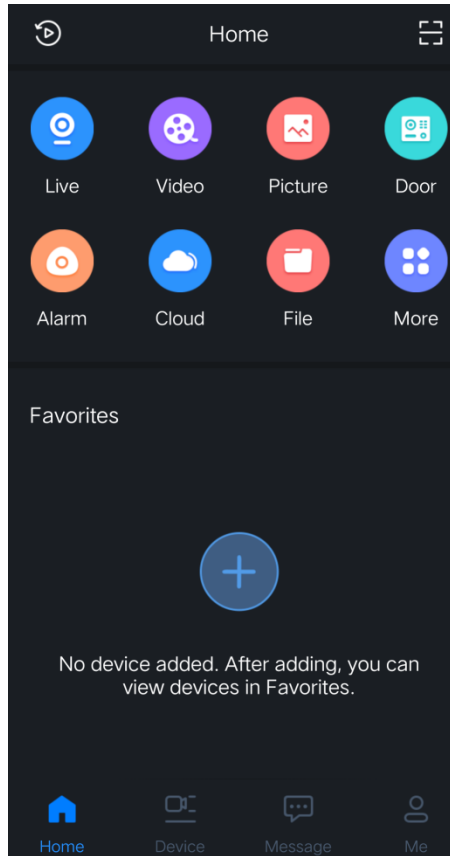
- Step 4** Tap  on the upper left corner of the **Live** interface.

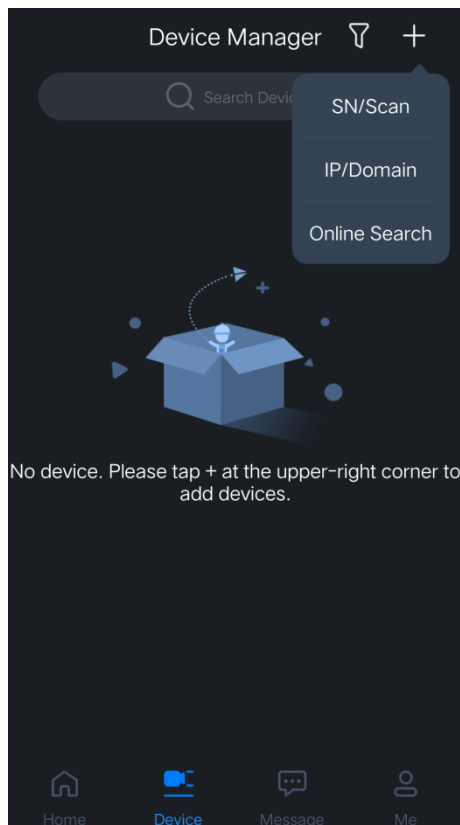
Figure 5-2 Home



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

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

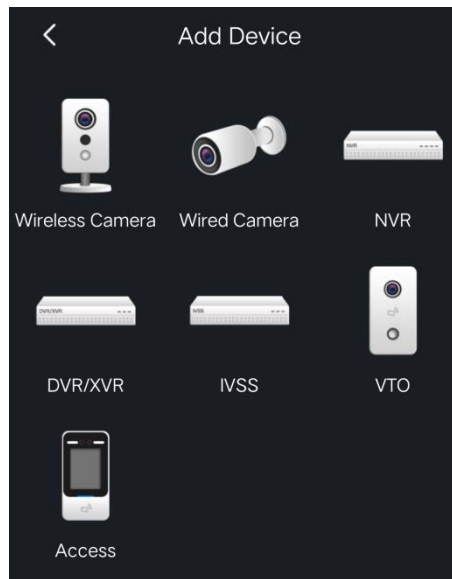
Figure 5-3 Device manager



5.1 Adding through Wired Network

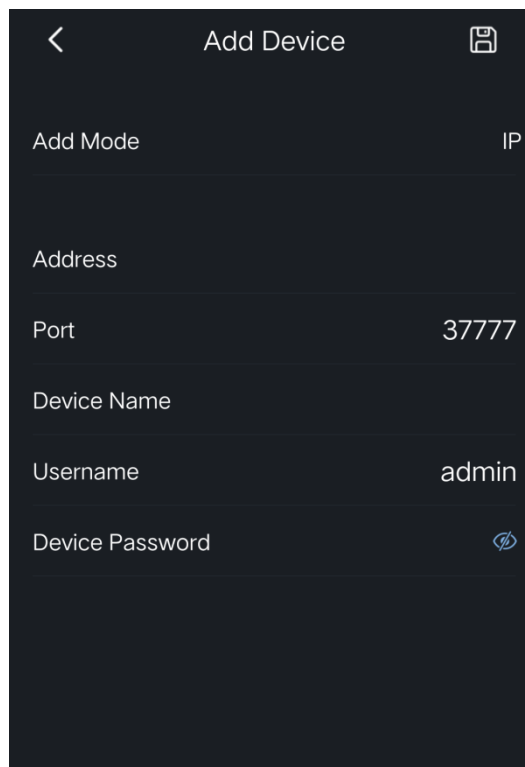
Step 1 Tap **IP/Domain** on Figure 5-3.

Figure 5-4 Add device



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

Figure 5-5 Add device

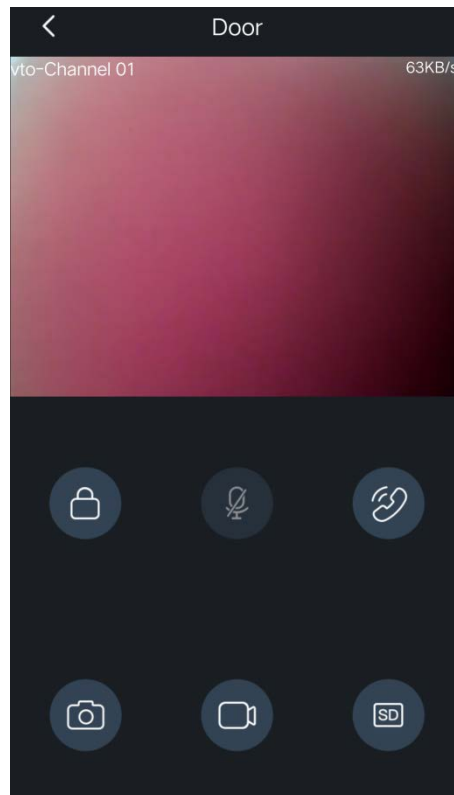


Step 3 Enter Address (IP address of the VTO), Device Name, and Device Password.

Step 4 Tap .

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

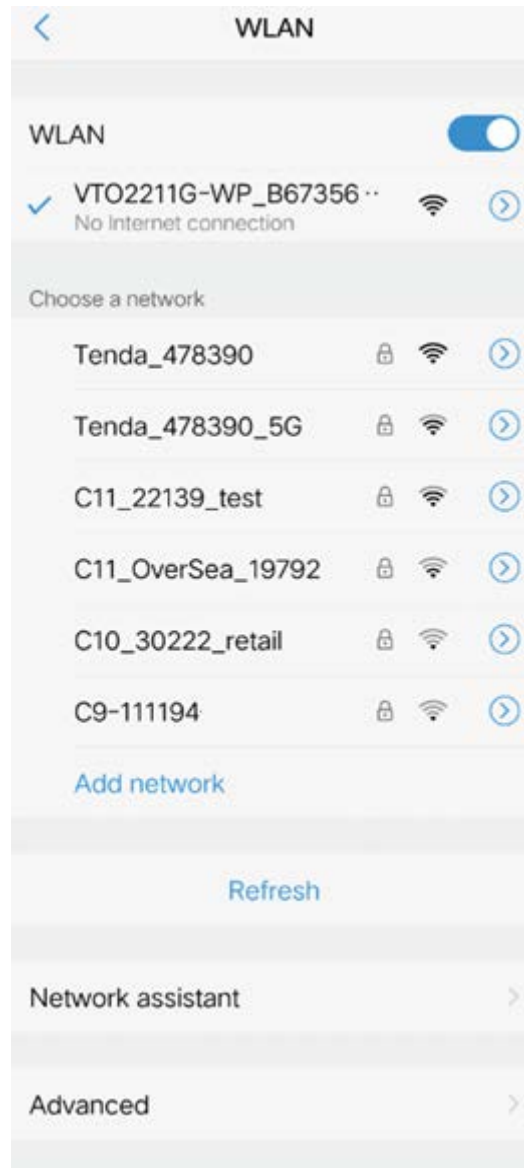
Figure 5-6 Door



5.2 Adding through Soft Access Point (AP)

- Step 1 Connect the door station to the power source.
- Step 2 Go to the **WLAN** interface of your mobile phone.
- Step 3 Press and hold the call button on the door station for over 5 seconds until you hear a beep.
- Step 4 Connect your phone to the **VTO2211G-WP_b67356..** network.

Figure 5-7 Mobile phone WLAN



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

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

Figure 5-8 Scan the QR code



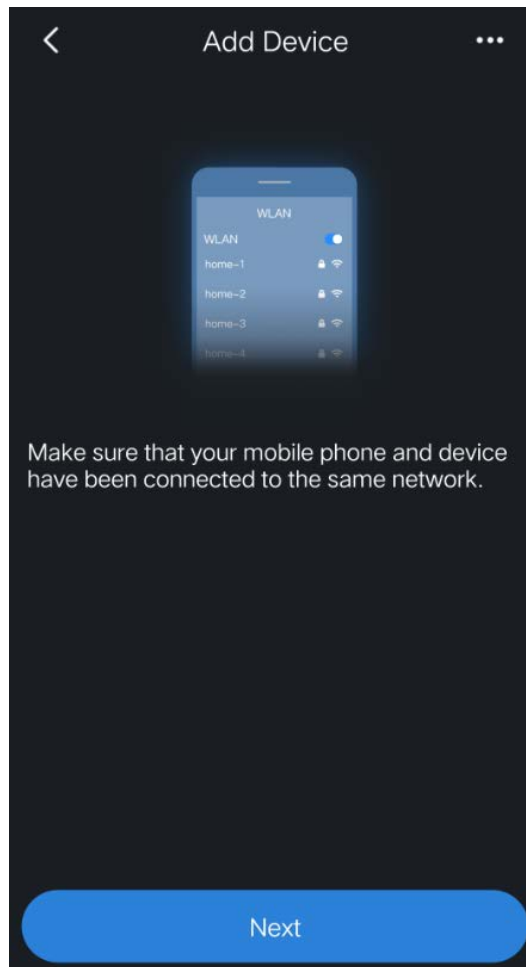
Step 7 Scan the QR code at the rear cover of the door station.



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

Step 8 Tap **Next**.

Figure 5-9 Add device




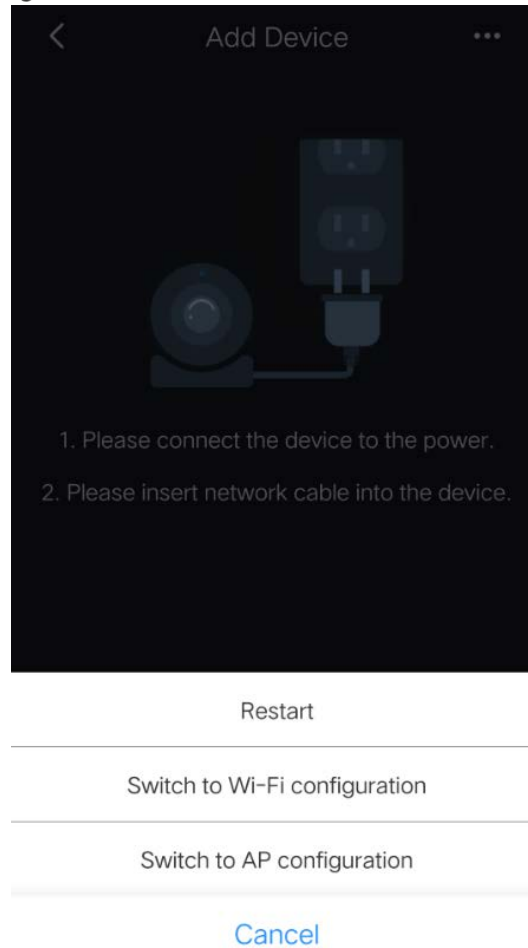
Step 9 Tap  on the upper-right corner.

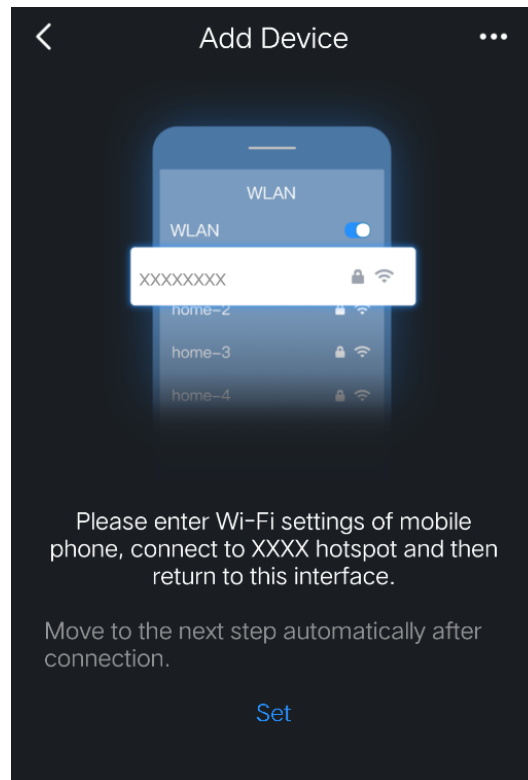
Figure 5-10 Select network configuration mode



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

Step 11 Tap **Next**.

Figure 5-11 Set phone network



Step 12 Tap **Set**.

Figure 5-12 Select a Wi-Fi



Step 13 Tap a Wi-Fi name.

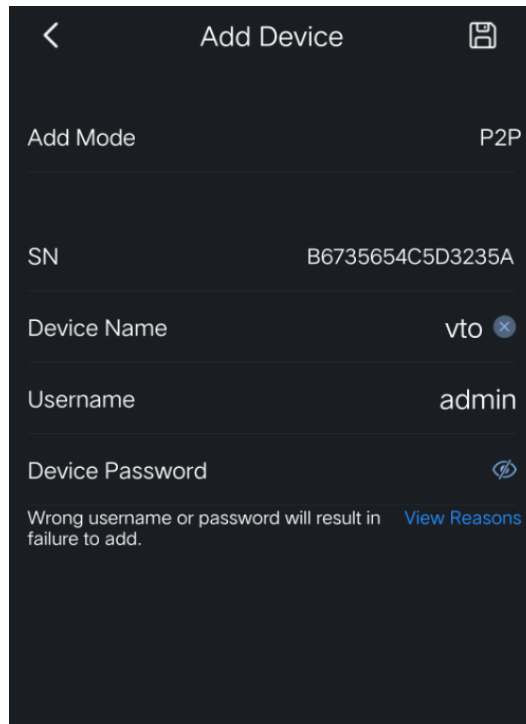
Figure 5-13 Enter Wi-Fi password




Step 14 Enter the Wi-Fi password.

Step 15 Tap **Next**.

Figure 5-14 Add device



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

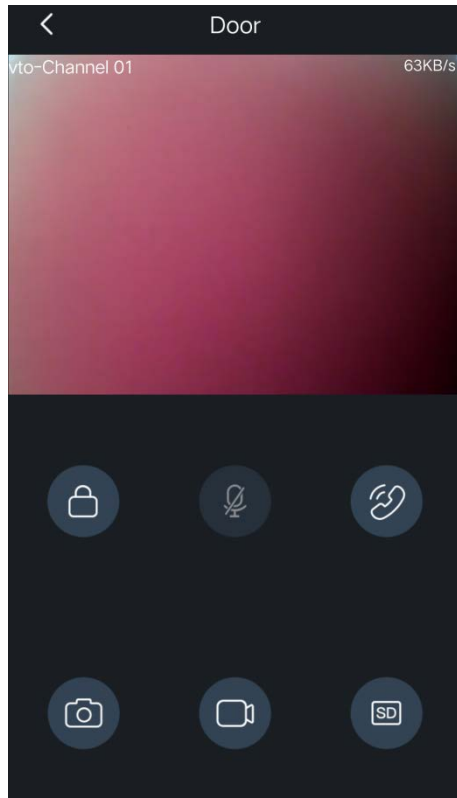
Step 17 Tap .

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



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

Figure 5-15 Door



Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

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

2. Update Firmware and Client Software in Time

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

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

1. Physical Protection

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

2. Change Passwords Regularly

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

3. Set and Update Passwords Reset Information Timely

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

4. Enable Account Lock

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

5. Change Default HTTP and Other Service Ports

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

6. Enable HTTPS

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

7. MAC Address Binding

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

8. Assign Accounts and Privileges Reasonably

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

9. Disable Unnecessary Services and Choose Secure Modes

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

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

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

10. Audio and Video Encrypted Transmission

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

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

11. Secure Auditing

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

12. Network Log

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

13. Construct a Safe Network Environment

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

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

Villa VTO

User's Manual






Foreword

General

This Manual introduces the operation of the villa station (VTO) 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.
 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	April 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, in order to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

Operating Requirement

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

Power Requirement

- The product shall use electric wires (power wires) required by the region where the device will be used.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.

Table of Contents

Foreword	I
Important Safeguards and Warnings	II
1 Initialization	1
2 Login Interface	2
2.1 Login	2
2.2 Resetting Password	2
3 Main Interface	4
4 Local Setting	5
4.1 Basic	5
4.1.1 Device Properties & Events.....	5
4.1.2 Façade Layout (Only for VTO3211D).....	6
4.2 Video & Audio	7
4.3 Access Control.....	8
4.3.1 Local.....	9
4.3.2 RS-485	9
4.4 System	10
4.5 Security	11
4.6 Onvif User.....	12
5 Household Setting	13
5.1 VTO No. Management	13
5.1.1 Adding VTO	13
5.1.2 Modifying VTO Information	14
5.1.3 Deleting VTO.....	15
5.2 Room No. Management	15
5.2.1 Adding Room Number.....	15
5.2.2 Modifying Room Number.....	17
5.2.3 Issuing Access Card	17
5.3 VTS Management.....	18
5.4 Status	19
6 Network Setting	20
6.1 Basic	20
6.1.1 TCP/IP	20
6.1.2 Port.....	20
6.1.3 HTTPS	21
6.1.4 P2P.....	21
6.2 SIP Server	21
6.3 Firewall	22
7 Log Management	24
7.1 Call	24
7.2 Alarm	24
7.3 Unlock	24
7.4 Log.....	25
Appendix 1 Cybersecurity Recommendations	26

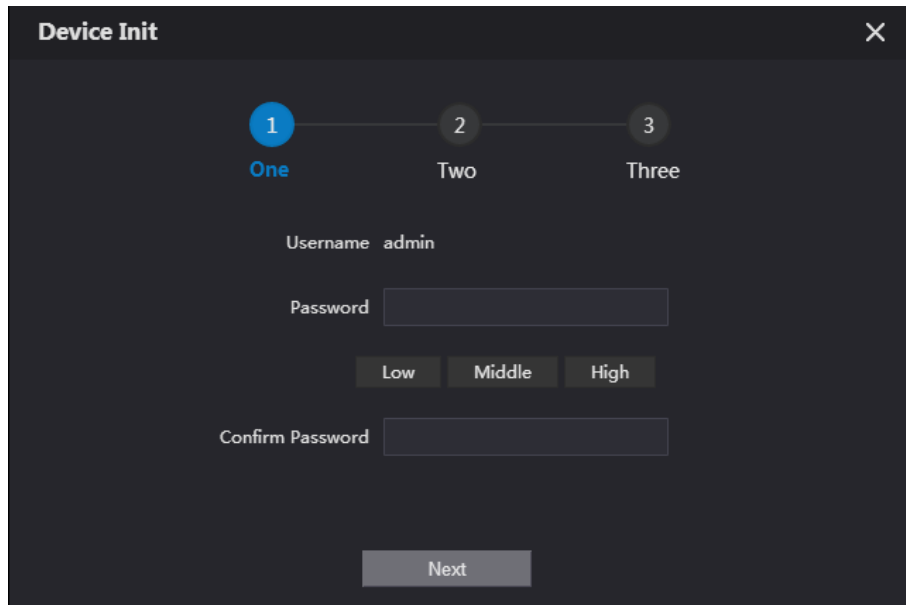
1 Initialization

For first time login or after the VTO being reset, you need to initialize the web interface. The default IP address of the VTO is 192.168.1.108, and make sure the PC is in the same network segment as the VTO.

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

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

Figure 1-1 Device initialization



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

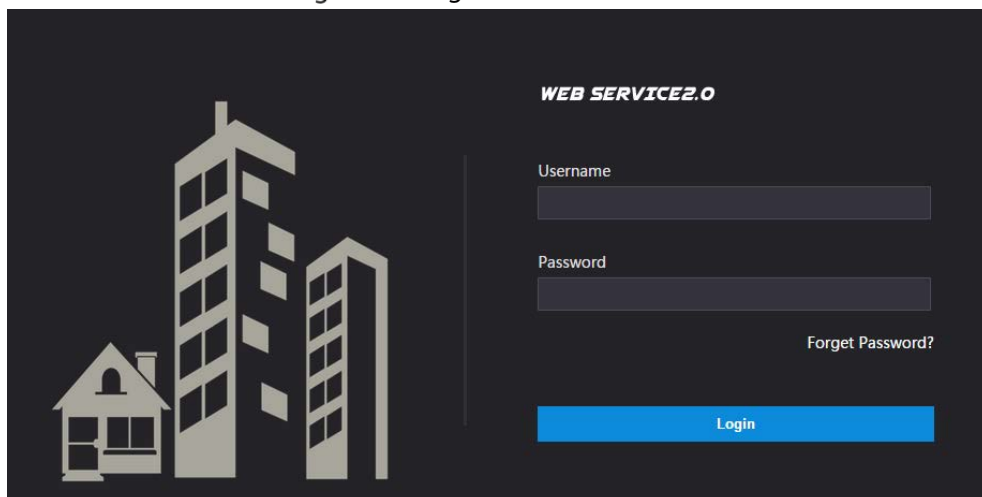
The email setting interface is displayed.

Step 4 Select the **Email** check box, and then enter your email address. This email address can be used to reset the password.

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

Step 6 Click **OK**.

Figure 1-2 Login interface



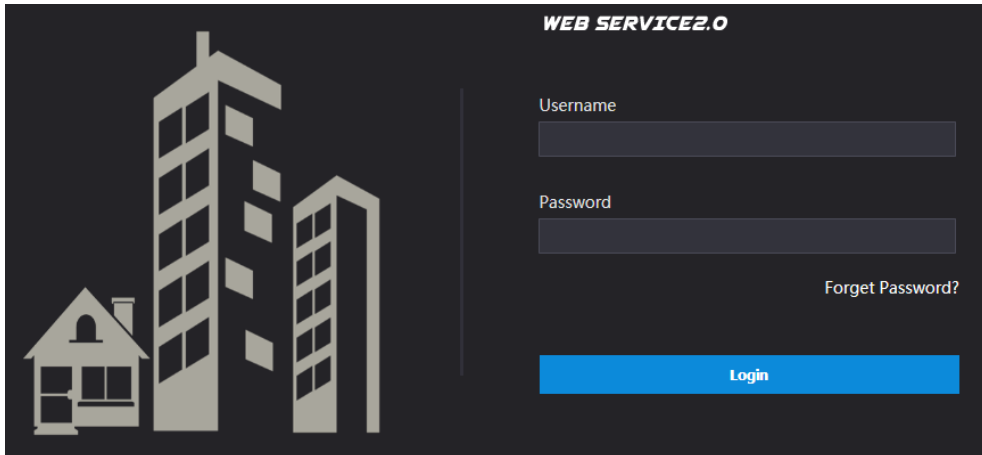
2 Login Interface

2.1 Login

Before login, make sure that the PC and VTO are in the same network segment.

Step 1 Enter the VTO IP address in the browser address bar, and then press **Enter**.

Figure 2-1 Login interface

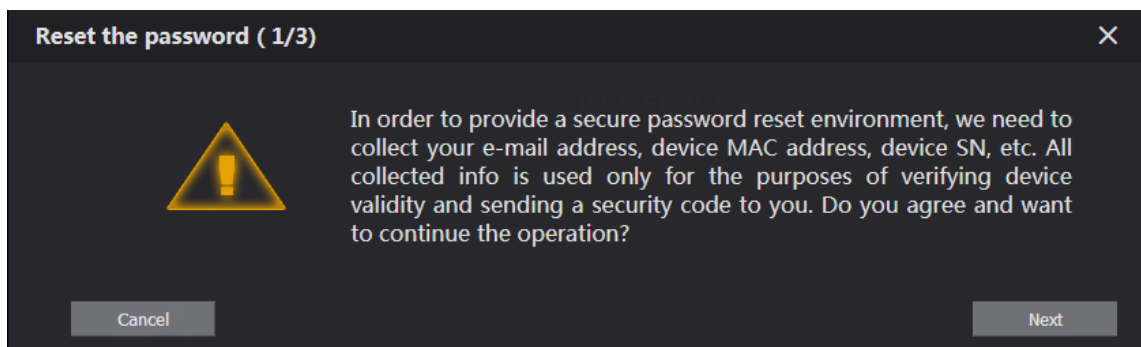


Step 2 Enter "admin" as username, then the password you set during initialization, and then click **Login**.

2.2 Resetting Password

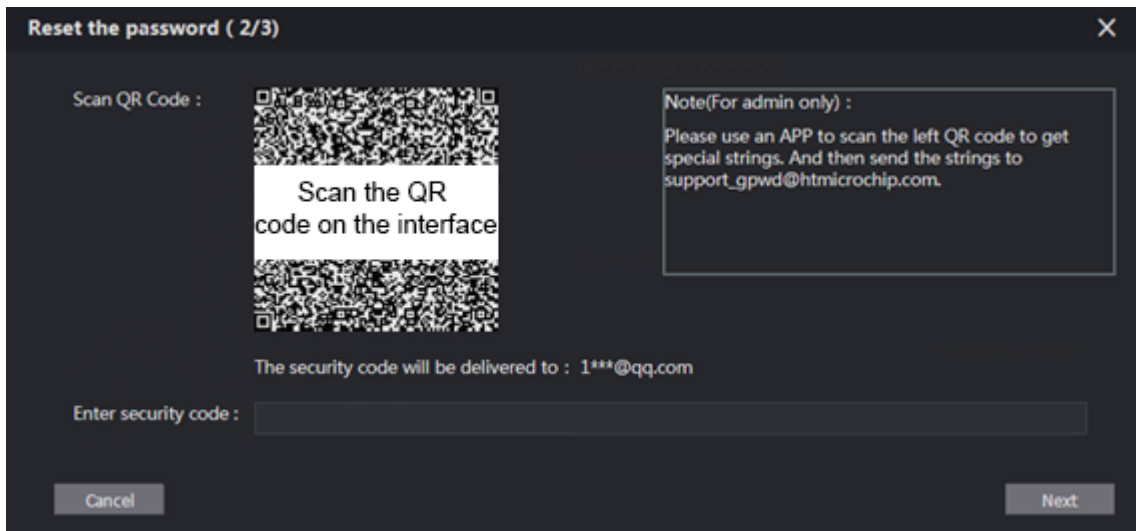
Step 1 On the login interface (Figure 2-1), click **Forgot Password?**.

Figure 2-2 Reset the password (1/3)



Step 2 Click **Next**.

Figure 2-3 Reset the password (2/3)



Step 3 Scan the QR code on the web interface to obtain the security code in your mailbox, and then enter the security code in the input box.



- If you did not configure email during initialization, contact the supplier or customer service for help.
- To obtain security code again, refresh QR code interface.
- Use the security code within 24 hours after receiving it. Otherwise, it will become invalid.
- If wrong security code is entered for 5 times continuously, this account will be locked for 5 min.

Step 4 Click **Next**, and then the **Reset the password (3/3)** dialog box is displayed.

Step 5 Set and confirm the new password as instructed, and then click **OK**.

3 Main Interface

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

Figure 3-1 Main interface

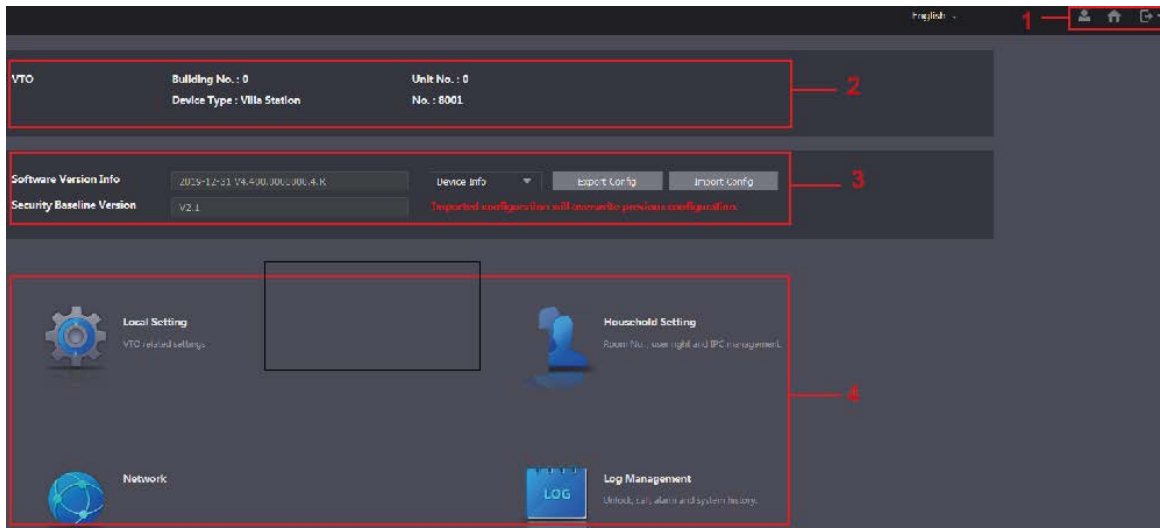





Table 3-1 Main interface introduction

No.	Function	Description
1	General function	<ul style="list-style-type: none"> Click  to change the password and your email address. Click  to go to the main interface. Click  to log out, reboot the VTO or restore the VTO to factory settings.
2	VTO information	You can view the general information of the VTO, including building No., unit No., device type, and VTO No..
3	System information	You can view the software version, MCU version, and security baseline version.
4	Config manager	Select Device Info or User Info , and then you can export the VTO configuration or user information to the PC or import them from it.
5	Function area	Click the buttons to go to the corresponding menu.

4 Local Setting

This chapter introduces how to configure VTO type, VTO No., video and audio, access password, system time, and security function.

General operations:

- After configuration, click **Confirm** to save, and click **Refresh** to view the latest change.
- If you click **Default**, all the configurations in the current page would be restored to the default, and you need to click **Confirm** to save.

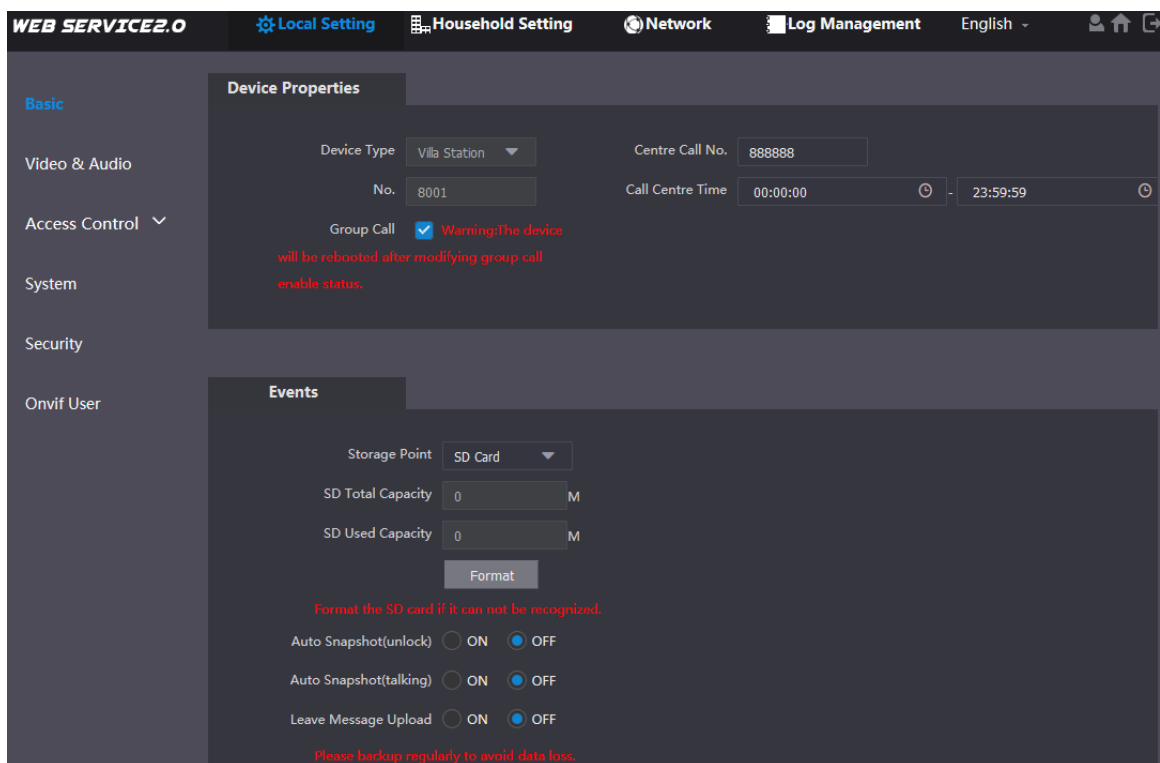
4.1 Basic

4.1.1 Device Properties & Events

This section introduces the configuration of VTO device type, VTO number, and auto storage.


Step 1 On the main interface (Figure 3-1), select **Local Setting > Basic**.


Figure 4-1 Basic



Step 2 Configure parameters.

Table 4-1 Basic parameter description

Parameter	Description
Device Type	<p>Keep the default value.</p> <p></p> <ul style="list-style-type: none"> • Building number and unit number are available only when other servers work as SIP server. See "6.2 SIP Server."

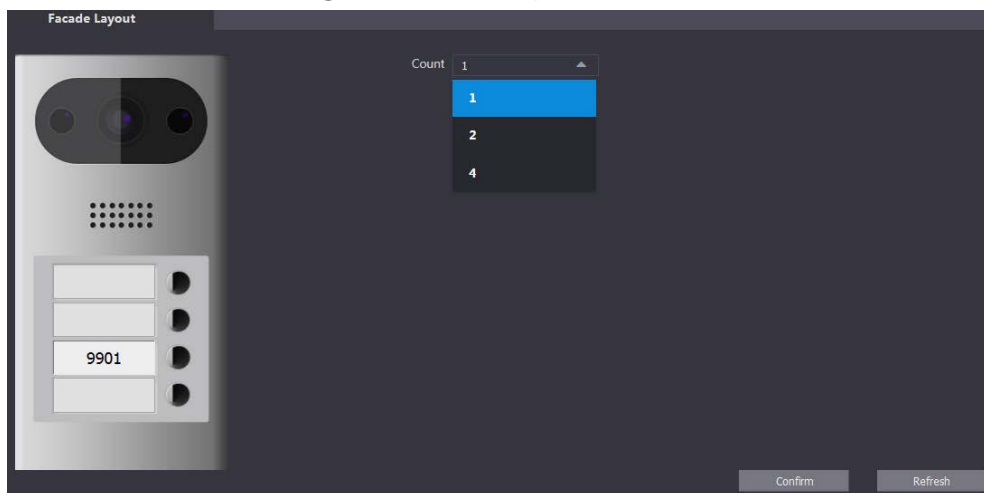
Parameter	Description
	<ul style="list-style-type: none"> Fence station is normally used when other servers work as SIP server.
Centre Call No.	Configure the number of the management centre, and you can call the management centre on every VTO or VTH in the network. The default number is 888888.
Call Centre Time	Time period in which you are allowed to call the management centre.
VTO No.	The VTO number can be used to differentiate each VTO, and it is normally configured according to unit or building number. You can add VTO devices to the SIP server with their numbers.
Storage Point	<p>All the snapshots would be saved to the SD card in the villa station automatically.</p> <ul style="list-style-type: none"> Auto Snapshot (unlock) Select ON to enable this function, and then the system takes snapshot every time when the door is unlocked. Auto Snapshot (talking) Select ON to enable this function, and then the system takes snapshot every time when VTH user answers a call from the VTO. Messages Select ON to enable this function, and then the system uploads the messages from visitors to the SD card automatically. <p></p> <ul style="list-style-type: none"> If there is an SD card in the main VTH, the left messages would be saved to the SD card of the main VTH by default. To receive message, the VTO Message Time must be configured to be more than 0. See the VTH user's manual.

Step 3 Click **Confirm**.

4.1.2 Façade Layout (Only for VTO3211D)

If you select 1 from the **Count** drop-down list, only the third button will be valid; if you select 2, only the second and the fourth buttons will be valid; and if you select 4, all the four buttons will be valid.

Figure 4-2 Façade layout

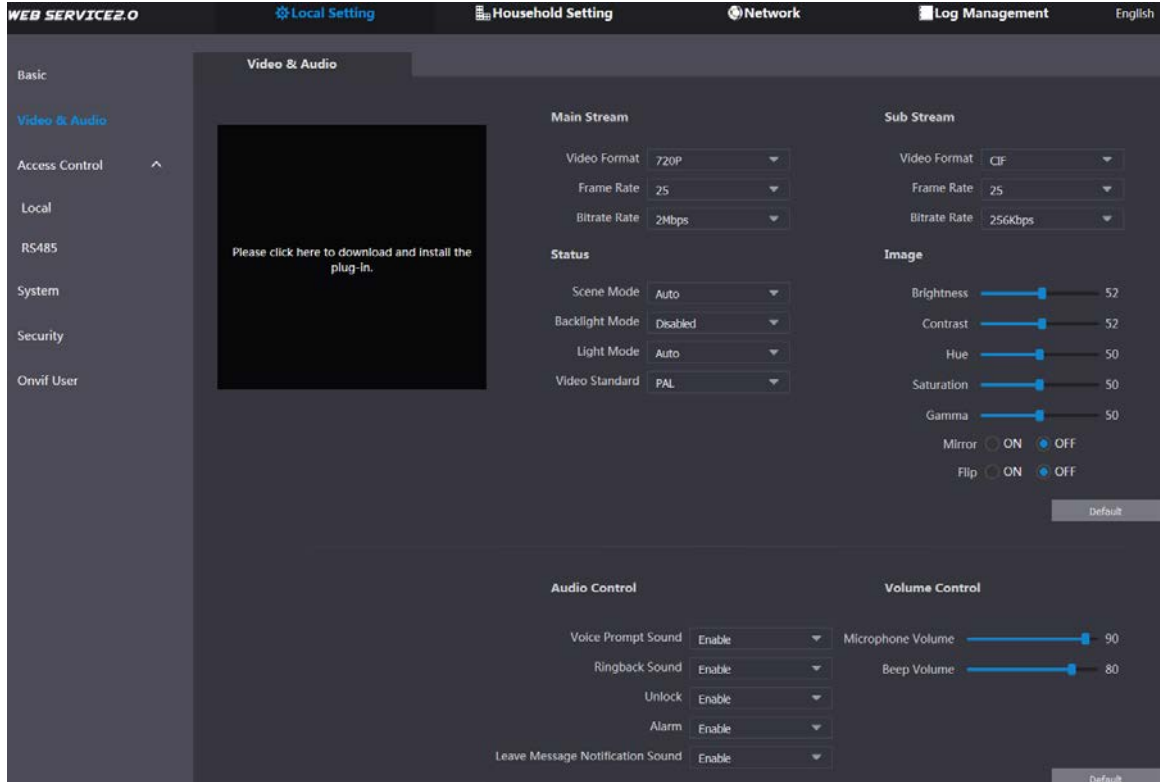


4.2 Video & Audio

This section introduces how to configure the format and quality of video that captured by VTO, and the audio control settings.

Step 1 On the main interface (Figure 3-1), select **Local Setting > Video & Audio**.

Figure 4-3 Video & audio



Step 2 Configure parameters, and these configurations will take effect immediately.

Table 4-2 Video parameter description

Parameter	Description	
Main Stream	Video Format	Select the video resolution from 720P, WVGA, and D1 .
	Format Rate	Configure the number of frames in 1 second. You can select from 1 to 25 under PAL , and 1 to 30 under NTSC video standard. The larger the value is, the smoother the video will be.
	Bitrate	Configure the data amount that transmitted in 1 second. You can select as needed. The larger the value is, the better the video quality will be.
Sub Stream	Video Format	Select the video resolution from CIF, WVGA, QVGA, D1, and 1080P .
	Format Rate	Configure the number of frames in 1 second. You can select from 1 to 25 under PAL , and 1 to 30 under NTSC video standard. The larger the value is, the smoother the video will be.
	Bitrate	Configure the data amount that transmitted in 1 second. The larger the value is, the better the video quality will be.
Status	Scene Mode	Adjust the video to adapt to different scenarios. You can select from Automatic, Sunny, Night and Disabled . It is Automatic by default.
	Day/Night Mode	You can select from Disabled, Auto, Sunny or Night .

Parameter		Description
	BackLight Mode	<p>You can select from the following modes:</p> <ul style="list-style-type: none"> ● Disabled: No back light. ● BLC: The camera gets clearer image of the dark areas on the target when shooting against light. ● WDR: The system dims bright areas and compensates dark areas to ensure the clarity of all the area. ● HLC: The system constrains bright areas and reduces halo size to dim the overall brightness.
	Light Mode	There are four light modes: NO, NC, Auto, and Scheduled. Select as needed.
	Video Standard	Select from PAL or NTSC according to your display device.
Image	Brightness	Changes the value to adjust the picture brightness. The larger the value is, the brighter the picture will be, and the smaller the darker. The picture might be hazy if the value is too large.
	Contrast	Changes the contrast of the picture. The larger the value is, the more the contrast will be between bright and dark areas, and the smaller the less. If the value is too large, the dark area would be too dark and bright area easier to get overexposed. The picture might be hazy if the value is too small.
	Hue	Makes the color deeper or lighter. The default value is made by the light sensor.
	Saturation	Makes the color deeper or lighter. The larger the value is, the deeper the color will be, and the lower the lighter. Saturation value does not change image brightness.
	Gamma	Changes the picture brightness and improves the picture dynamic range in a non-linear way. The larger the value is, the brighter the picture will be, and the smaller the darker.
	Mirror	Select On , and then the image is displayed with left and right side reversed.
	Flip	Select On , and then the image is displayed upside down.
Audio Control	Select Enable or Disabled to turn on or off each sound.	
Volume Control	Microphone Volume	Adjust the value, and the larger the value is, the louder the VTO microphone volume will be.
	Beep Volume	Adjust the value, and the larger the value is, the louder the system volume will be.

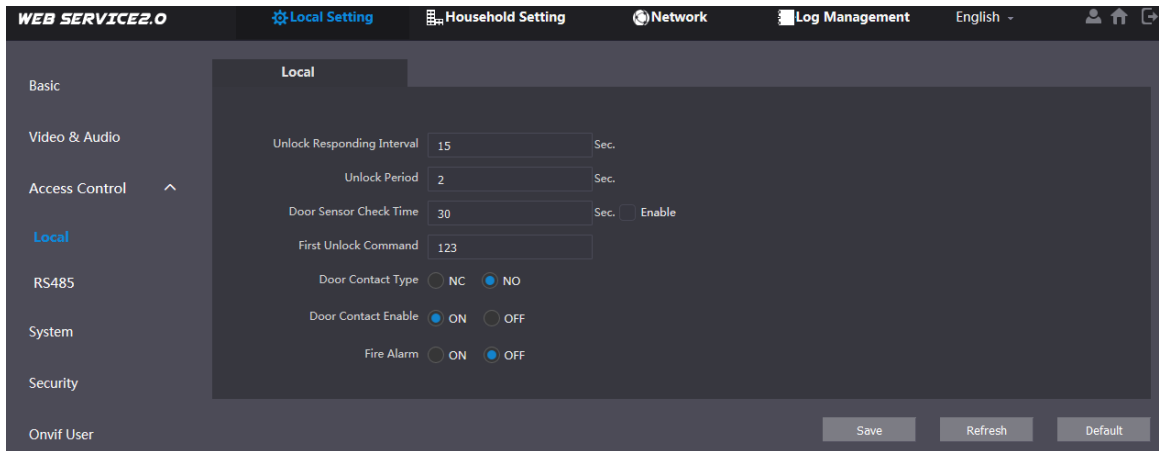
4.3 Access Control

This section introduces how to configure the lock, including unlock responding interval, open door command, door sensor check time, first unlock command and door contact type.

4.3.1 Local

Step 1 On the main interface (Figure 3-1), select **Local Setting > Access Control > Local**.

Figure 4-4 Local



Step 2 Configure parameters.

Table 4-3 Local access control parameter description

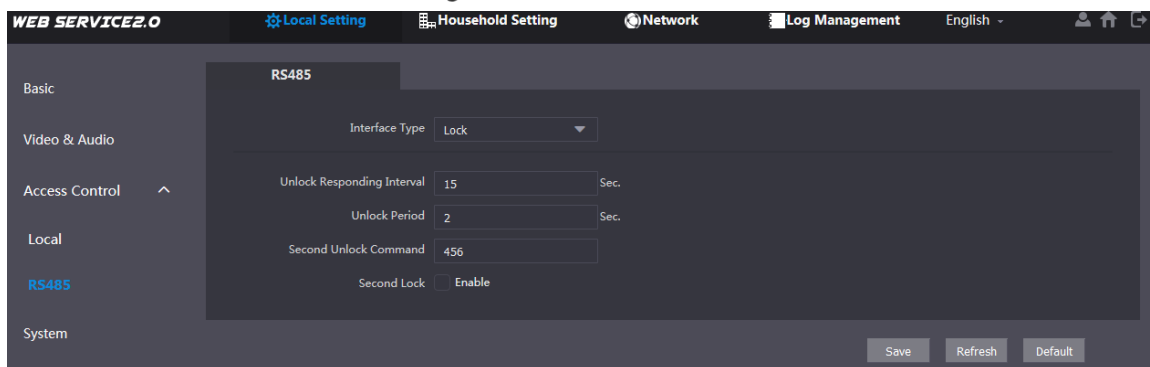
Parameter	Description
Unlock Responding Interval	The time interval to unlock again after the previous unlock, and the unit is second.
Unlock Period	The time amount for which the lock stays open after unlock, and the unit is second.
Door Sensor Check Time	If you have installed door sensor, you need to configure the time period, and if the unlock time exceeds the Door Sensor Check Time , the door sensor alarm is triggered, and the alarm will be sent to the management center. <ul style="list-style-type: none"> ● Select the Enable check box, and the door will not be locked until the door sensor contacts each other. ● If you do not select the Enable check box, the door will be locked after the Unlock Period finishes.
First Unlock Command	You can connect a third-party phone such as SIP phone to your VTO, and use the command to open the door remotely.
Door Contact Type	Select NC or NO according to the lock you use.
Door Contact Enable	After door contact is enabled, if doors are not locked at certain period, alarms will be triggered, and alarm messages will be pushed to the indoor monitor (VTH).
Fire Alarm	Select as needed.

Step 3 Click **Save**.

4.3.2 RS-485

You can set unlock responding interval, unlock period, and second unlock command.

Figure 4-5 RS-485

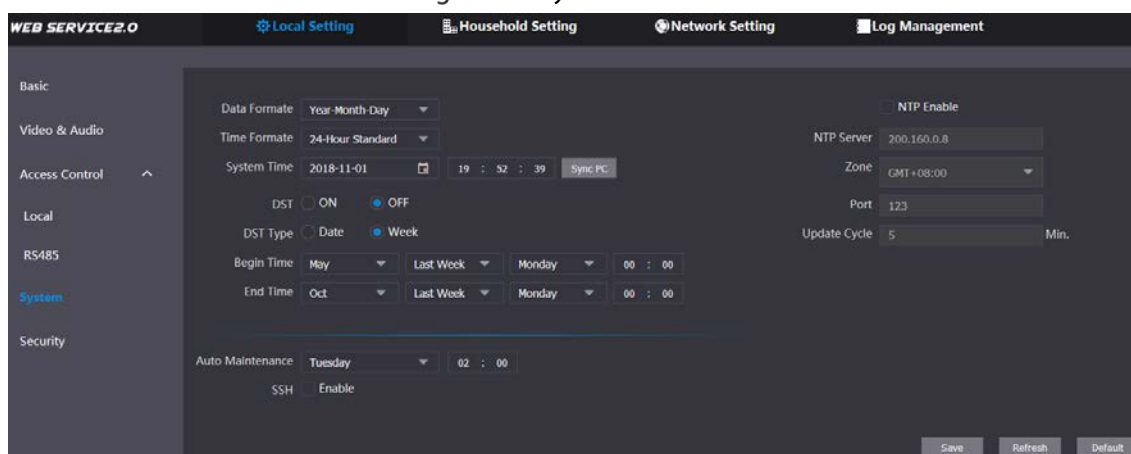


4.4 System

This section introduces how to configure the date format, time format, and the NTP server.


Step 1 On the main interface (Figure 3-1), select **Local Setting > System**.

Figure 4-6 System



Step 2 Configure parameters.

Table 4-4 System parameter description

Parameter	Description
Date Format	You can select from Year-Month-Day, Month-Day-Year, and Day-Month-Year.
Time Format	Configure the time format, and you can select from 12-Hour or 24-Hour .
Time Zone	Select a time zone as needed.
System Time	Configure the VTO system date, time and time zone.  Do not change the system time arbitrarily; it might cause problems on video searching and publishing snapshot or notice. Before changing the system time, turn off video recording or auto snapshot.
Sync PC	Click to sync the VTO system time and the PC system time.
DST	Select ON to enable DST.
DST Type	Select Date to define a specific date for DST or select Week for it.
Start Time	Configure the begin time and end time for DST.
End Time	
NTP Enable	Select the check box to enable NTP timing.

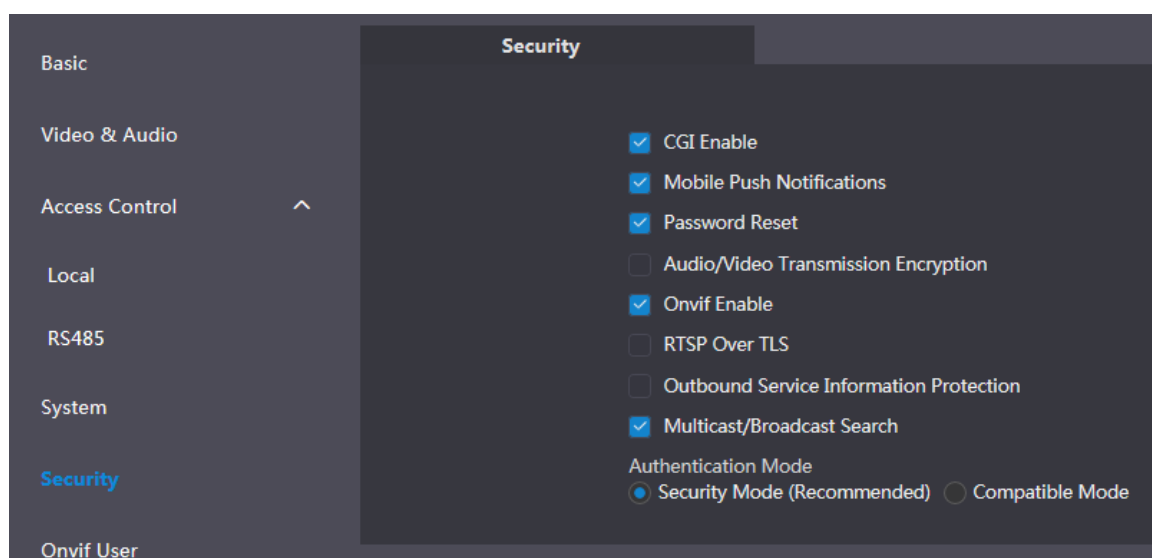
Parameter	Description
NTP Server	Enter the domain name of the NTP server.
Port	The port number of the NTP server.
Update Cycle	The time interval that the VTO syncs time with the NTP server, and it is 30 min at most.
Maintenance	Select the day and time for the auto maintenance, and the VTO will restart then.
SSH	Select the Enable check box, and then you can connect debugging devices to the VTO through SSH protocol.

Step 3 Click **Save**.

4.5 Security

Step 1 On the main interface (Figure 3-1), select **Local Setting > Security**.

Figure 4-7 Security



Step 2 Configure parameters.

Table 4-5 Security parameter description

Parameter	Description
CGI Enable	Select the check box to enable, and then you can use CGI command.
Mobile Push Notification	After you have enabled this, nifications will be pushed to the app installed on your phone.
Password Reset	Select the check box to enable, and then the password resetting is available.
Audio/Video Transmission Encryption	If you have enabled this, transmission of audio and video will be encrypted.
Onvif Enable	After Onvif is enabled, videos from devices manufactured by other companies can be displayed on the door station web interface.
RTSP Over TLS	RTSP is the abbreviation of real time streaming protocol, it's a network control protocol designed for use in entertainment and communications systems to control streaming media servers. The protocol is used for

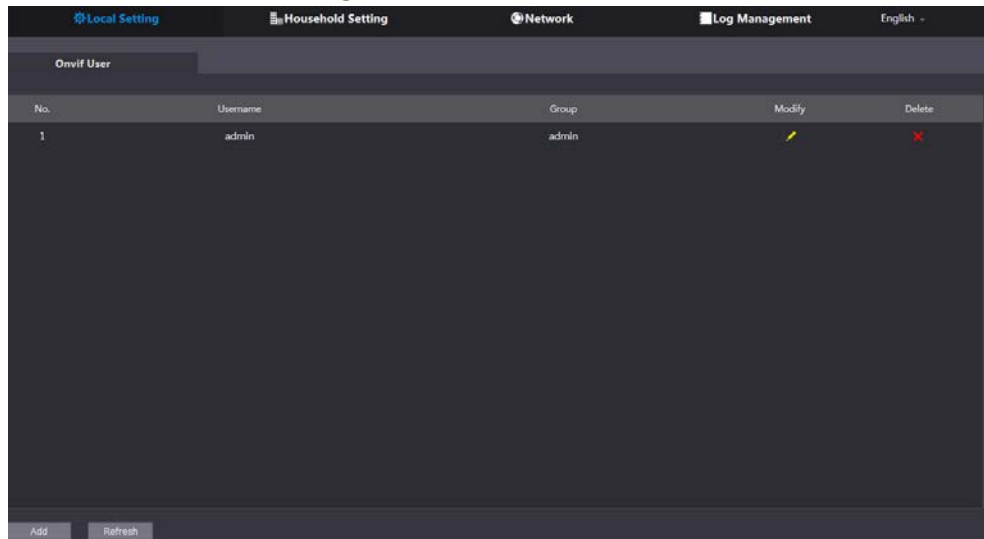
Parameter	Description
	establishing and controlling media sessions between end points.
Outbound Service Information	After it is enabled, service password information cannot be sent to others.
Multicast/Broadcast Search	If you have disabled this, VDP configure tools cannot find this device.
Authentication Mode	There are two modes: Security Mode (Recommended) and compatible mode.

Step 3 Click **Save** to save.

4.6 Onvif User

Onvif user is only for engineers. You can add, delete, and modify ONVIF user information. The Onvif username is admin by default.

Figure 4-8 Onvif user



5 Household Setting

This chapter is about configurations to the door stations (VTO) that work as SIP servers (see 6.2 SIP Server). You will know how to add, modify, and delete VTO, VTH, VTS, and IPC devices, and how to send messages from the SIP server to other VTO and VTH devices. If you are using other servers as SIP server, see the corresponding manual for the detailed configuration.

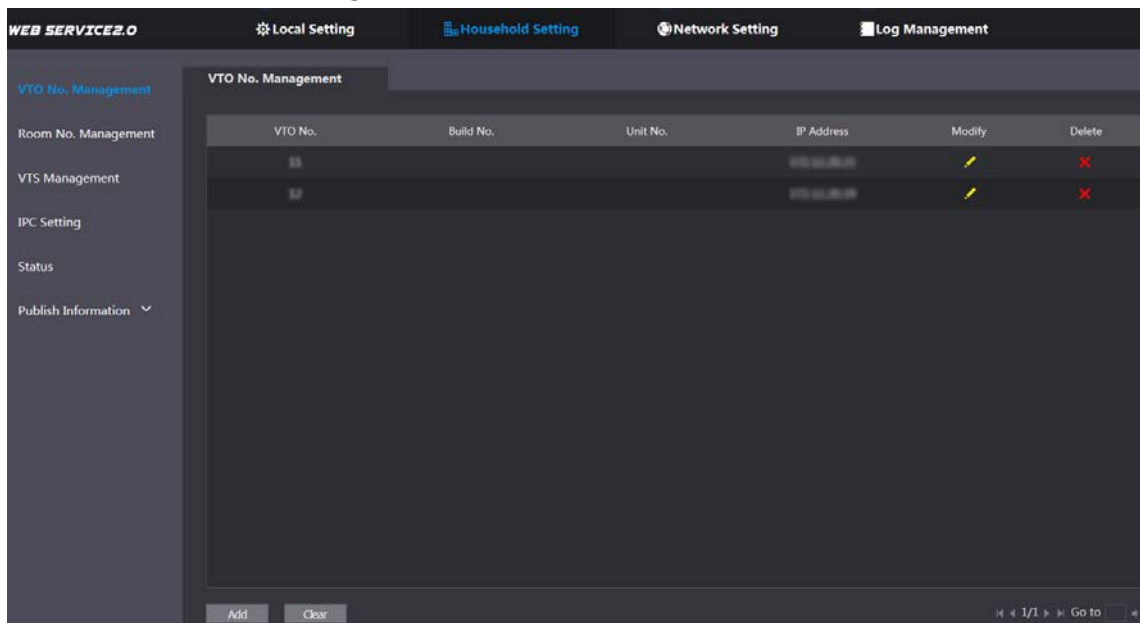
5.1 VTO No. Management

5.1.1 Adding VTO

You can add VTO to the SIP server, and then you can make video calls among video door phones that are connected to the same SIP server.

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

Figure 5-1 VTO No. management



Step 2 Click **Add**.

Figure 5-2 Add VTO

Step 3 Configure the parameters.

Table 5-1 Add VTO configuration

Parameter	Description
Rec No.	The VTO number you configured for the target VTO. See the details in "Table 4-1."
Register Password	Keep default value.
Build No.	Available only when other servers work as SIP server.
Unit No.	
IP Address	The IP address of the target VTO.
Username	The user name and password for the WEB interface of the target VTO.
Password	

Step 4 Click **Save**.

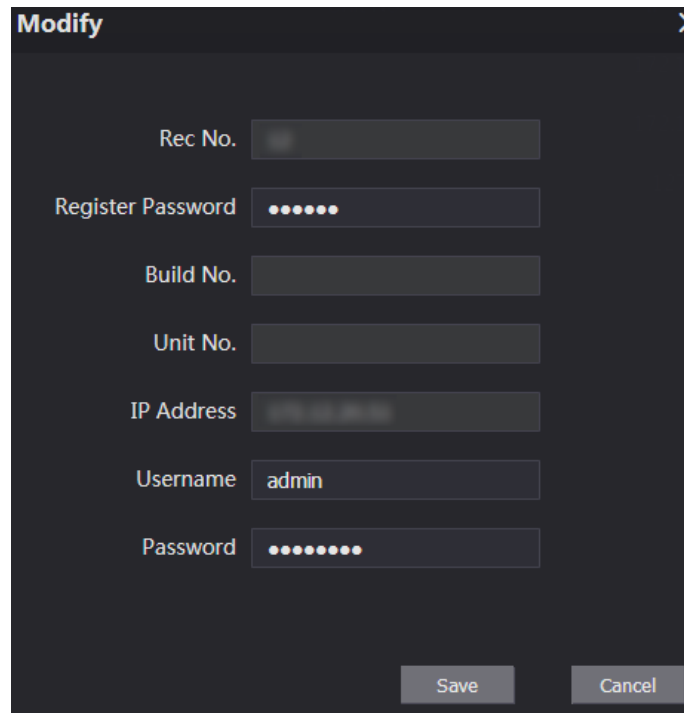
5.1.2 Modifying VTO Information



The VTO that is currently at use cannot be modified or deleted.

Step 1 On the **VTO No. Management** interface (Figure 5-1), click .

Figure 5-3 Modify VTO



The screenshot shows a dark-themed 'Modify' dialog box with a close button (X) in the top right corner. It contains several input fields: 'Rec No.', 'Register Password' (masked with dots), 'Build No.', 'Unit No.', 'IP Address', 'Username' (containing 'admin'), and 'Password' (masked with dots). At the bottom right, there are 'Save' and 'Cancel' buttons.


Step 2 You can modify the **Rec No.**, **Username**, and **Password**.

Step 3 Click **Save**.

5.1.3 Deleting VTO



The VTO that is in use cannot be modified or deleted.

On the **VTO No. Management** interface (Figure 5-1), click  to delete VTO one by one; and click **Clear** to delete all the VTO.

5.2 Room No. Management

5.2.1 Adding Room Number

You can add the planned room numbers to the SIP server, and then configure room numbers on VTH devices so that you can connect them to the network.

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

Figure 5-4 Room No. Management

Room No.	First Name	Last Name	Nick Name	Registration Mode	Modify
9901#0				public	
9901#1				public	
9901#2				public	
9901#3				public	
9901#4				public	
9901#5				public	
9901#6				public	
9901#7				public	
9901#8				public	
9901#9				public	

Step 2 Add room numbers.

- 1) Click **Add**.

Figure 5-5 Add room numbers

- 2) Configure room information.

Table 5-2 Room information

Parameter	Description
First Name	Enter the information that helps to differentiate each room.
Last Name	
Nick Name	
Room No.	The room number you planned.
Register Type	Select public , and local is reserved for future use.
Register Password	Keep the default value.

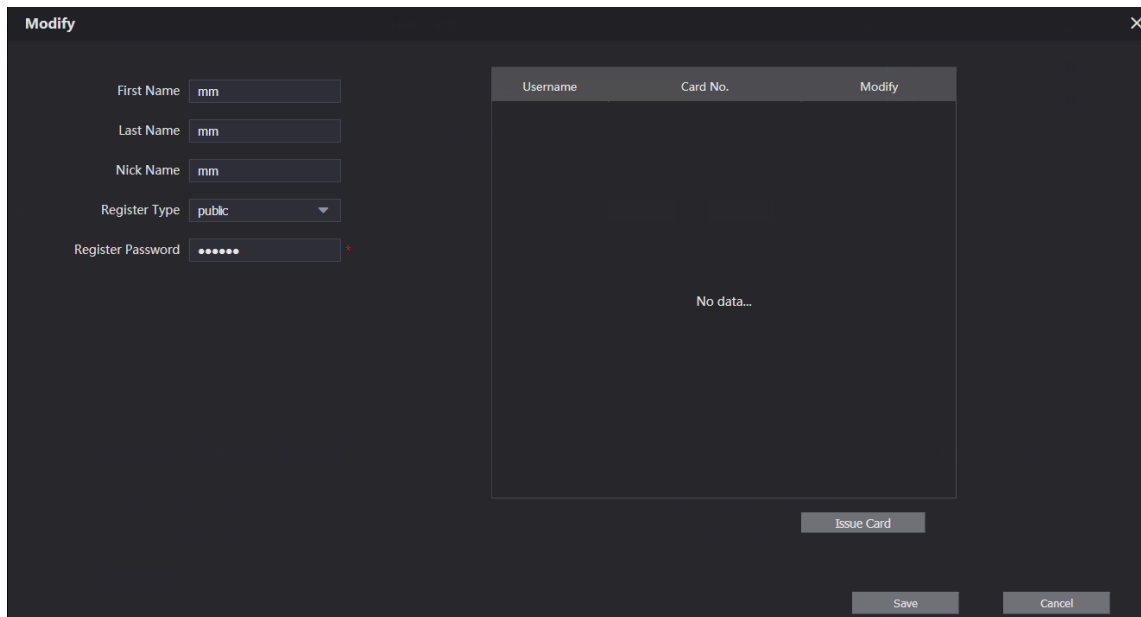
- 3) Click **Save**.

The room numbers added are displayed. Click to modify room information, click to view the device serial number, and click to delete a room. Click **Refresh** to view the latest status, and click **Clear** to delete all the room numbers.

5.2.2 Modifying Room Number

Step 1 On the **Room No. Management** interface (Figure 5-4), click .

Figure 5-6 Modify room number



Username	Card No.	Modify
No data...		

Step 2 You can modify the names for the room.

Step 3 Click **Save**.

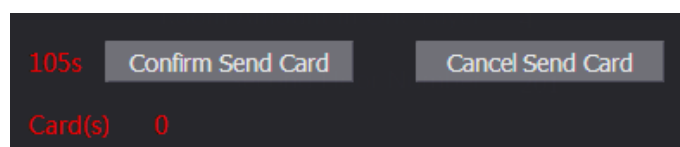
5.2.3 Issuing Access Card

You can issue card to a room, and can also set the card as the main card, or set the card to the lost state. Main cards are used to issue cards for other rooms.

Step 1 On the **Modify room number** interface (Figure 5-6), click **Issue Card**.

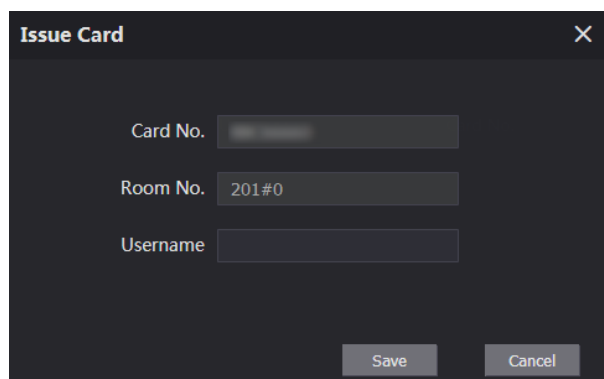
The countdown notice is displayed.

Figure 5-7 Countdown notice



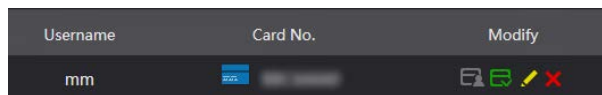
Step 2 Swipe the card that needs to be authorized on the VTO, and then the **Issue Card** dialogue box is displayed.






Figure 5-8 Issue card









Step 3 Enter a username, click **Save**, and then click **Confirm Send Card** at the countdown notice (Figure 5-7).

Figure 5-9 Issued access card



Username	Card No.	Modify
mm	 [masked]	   

Step 4 You can modify card information.

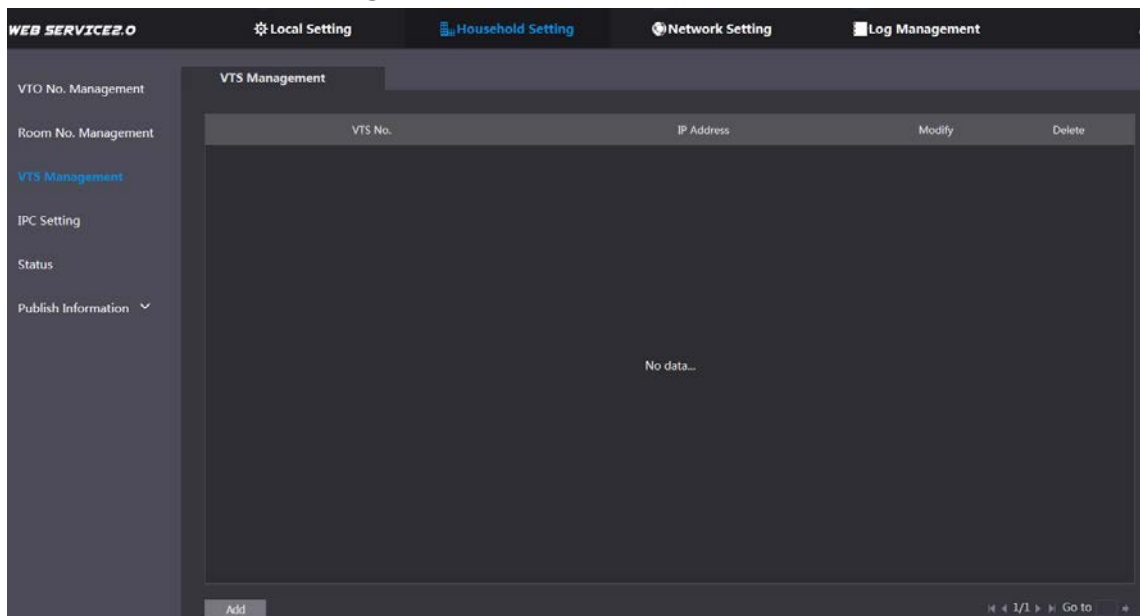
- Click  to set it to the main card, and then the icon turns into . The main card can be used to issue access card for this room on the VTO. Click again to resume.
- Click  to set the card to the lost state, and then the icon turns to . The card under lost state cannot be used to open the door. Click again to resume.
- Click  to modify the user name.
- Click  to delete the card.

5.3 VTS Management

You can add VTS device to the SIP server, and the VTS can be used as the management center. It can manage all the video door phones in the network, make or receive video calls, and make basic configurations. For details, see the VTS user's manual.

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

Figure 5-10 VTS management





Step 2 Click **Add**.

Figure 5-11 Add VTS

Step 3 Configure the parameters, and for the detailed description.

Table 5-3 Add VTS configuration

Parameter	Description
VTS No.	The VTS number you configured for the target VTS.
Register Password	Keep default value.
IP Address	The IP address of the target VTS.

Step 4 Click **Save**, and then the added VTS is displayed. Click  to modify IP address, and click  to delete.

5.4 Status

You can view the working state and IP address of all the connected devices.

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

Figure 5-12 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

6 Network Setting

This chapter introduces how to configure IP address, SIP server, DDNS, and UPnP.

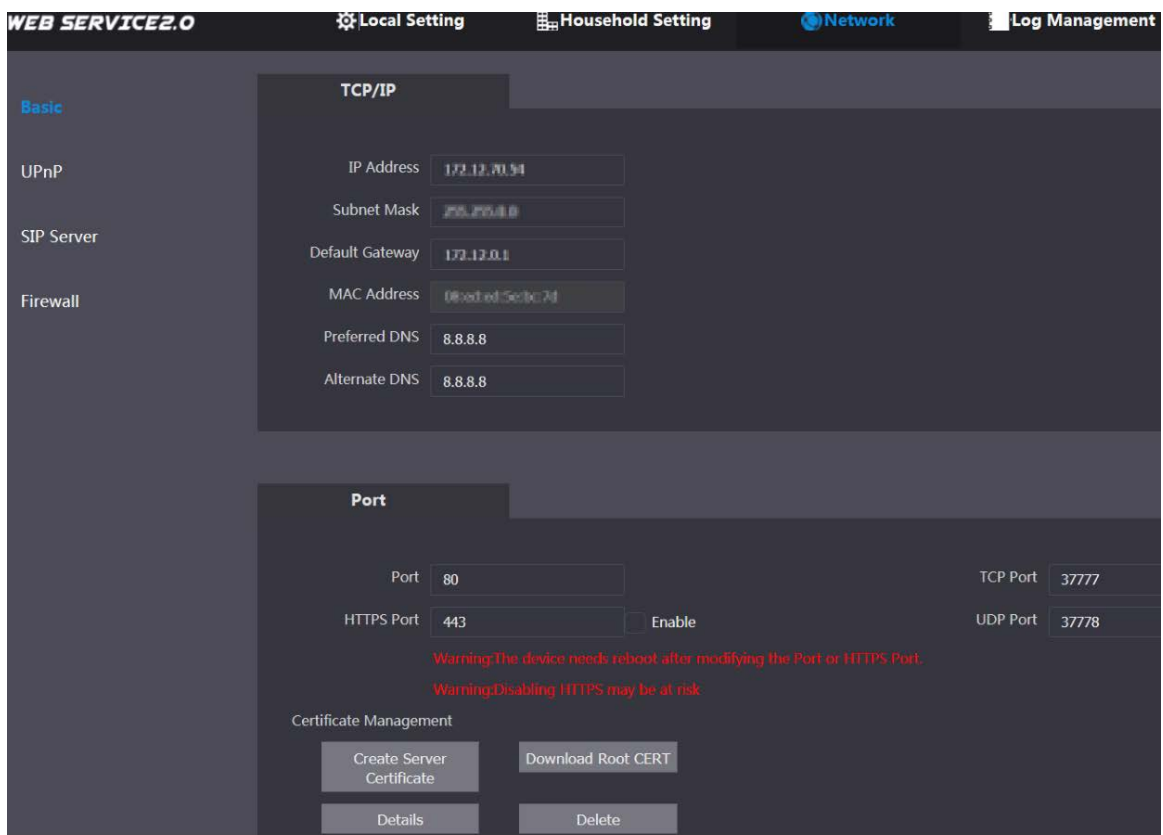
6.1 Basic

6.1.1 TCP/IP

You can modify the IP address and port number of the VTO.

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

Figure 6-1 TCP/IP and port



Step 2 Enter the network parameters and port number, 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

6.1.2.1 Creating Server Certificate

Click **Create Server Certificate**, enter needed information, click **Save**, and then the terminal will restart.

6.1.2.2 Downloading Root Certificate

- Step 1 Click **Download Root Certificate**.
- Step 2 Select a path to save the certificate on the Save File dialog box.
- Step 3 Double-click **Root Certificate** that you have downloaded to install the certificate. Install the certificate by following the onscreen instructions.

6.1.3 HTTPS

Select the **Enable** check box at **HTTPS Port**, and then the VTO will reboot. After restart, you can log in to the VTO by entering "https:// VTO IP address" in the address bar of the explorer.

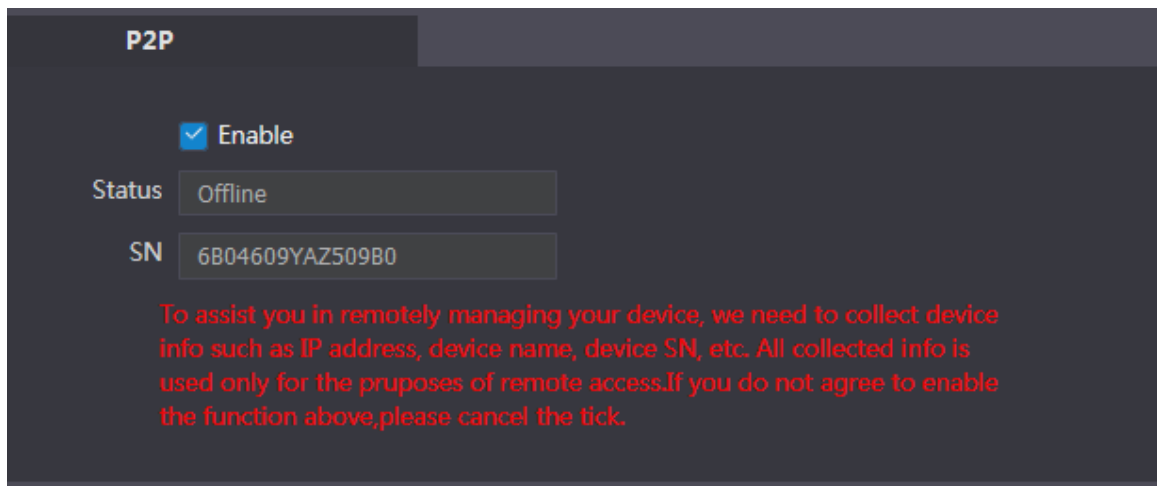


- You can use the default value, and you can also modify the port number as needed.
- When HTTPS Port is enabled, you can enter https://VTO IP address:HTTPS port number/#/Login to log in to the web interface; or you can enter http://VTO IP address:port number, and the address will be automatically changed to https://VTO IP address: HTTPS port number/#/Login.

6.1.4 P2P

P2P network is one in which two or more PCs share files and access to devices such as printers without requiring separate server computer or server software.

Figure 6-2 P2P

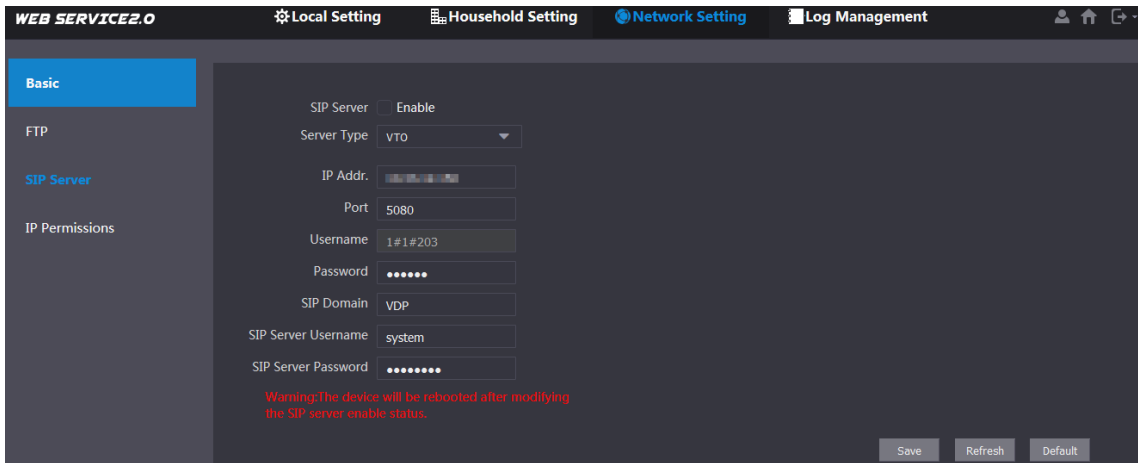


6.2 SIP Server

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

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

Figure 6-3 SIP server



Step 2 Select the server type you need.


- If the VTO you are visiting works as SIP server
 Select the **Enable** check box at **SIP Server**, and then click **Save**.
 The VTO will reboot, and after rebooting, you can then add VTO and VTH devices to this VTO. See the details in "5 Household Setting."

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

Table 6-1 SIP server configuration

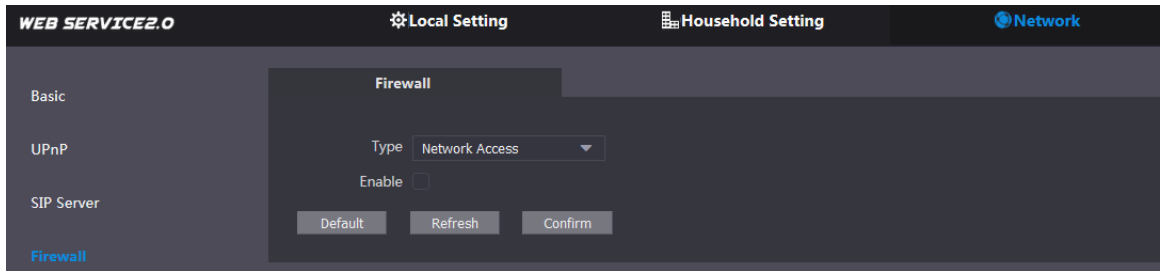
Parameter	Description
IP Addr.	The IP address of the VTO which works as SIP server.
Port	5060
Username	Keep the default value.
Password	
SIP Domain	VDP
SIP Server Username	The user name and password for the web interface of the SIP server.
SIP Server Password	

- If other servers work as SIP server
 Select the server type you need at **Server Type**, and then see the corresponding manual for the detailed configuration.

6.3 Firewall

Firewall is only for engineers. Select as needed.

Figure 6-4 Firewall



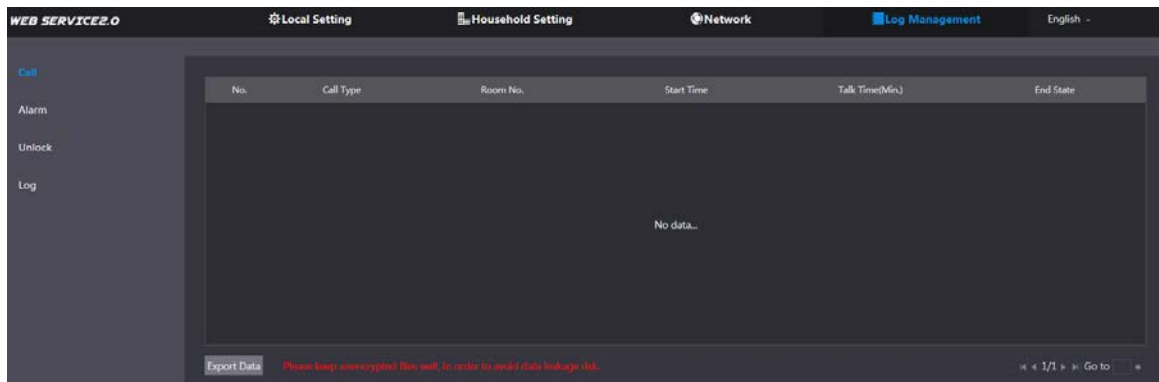
7 Log Management

You can view call history, alarm records, unlock records and system logs.

7.1 Call

You can view call logs, including call types, room numbers, start time, talk time, and end state.

Figure 7-1 Call

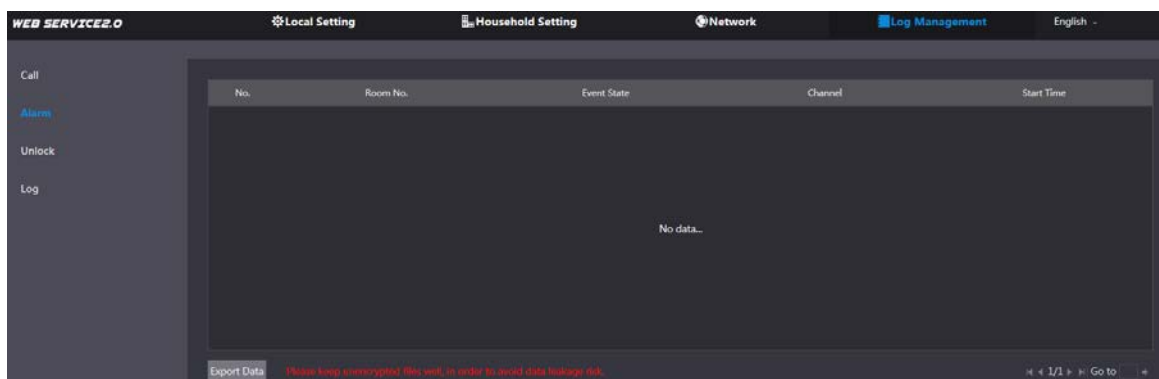


Click **Export Data** to export the records to your PC.

7.2 Alarm

You can view and export alarm logs.

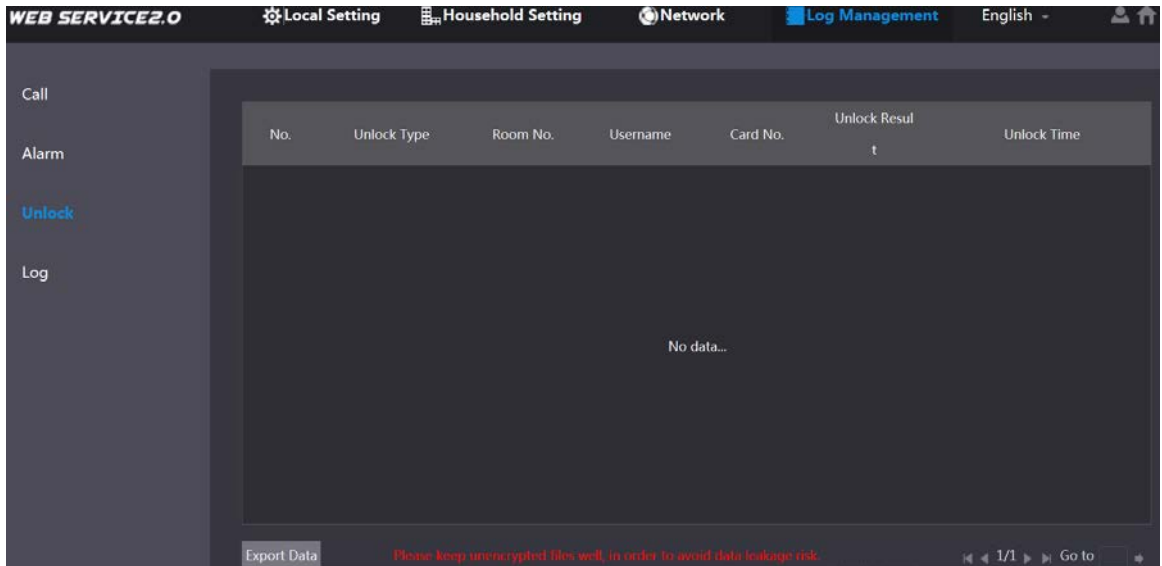
Figure 7-2 Alarm



7.3 Unlock

You can view and export unlocking records, including access card unlock, password unlock, remote unlock, and press button unlock.

Figure 7-3 Unlock

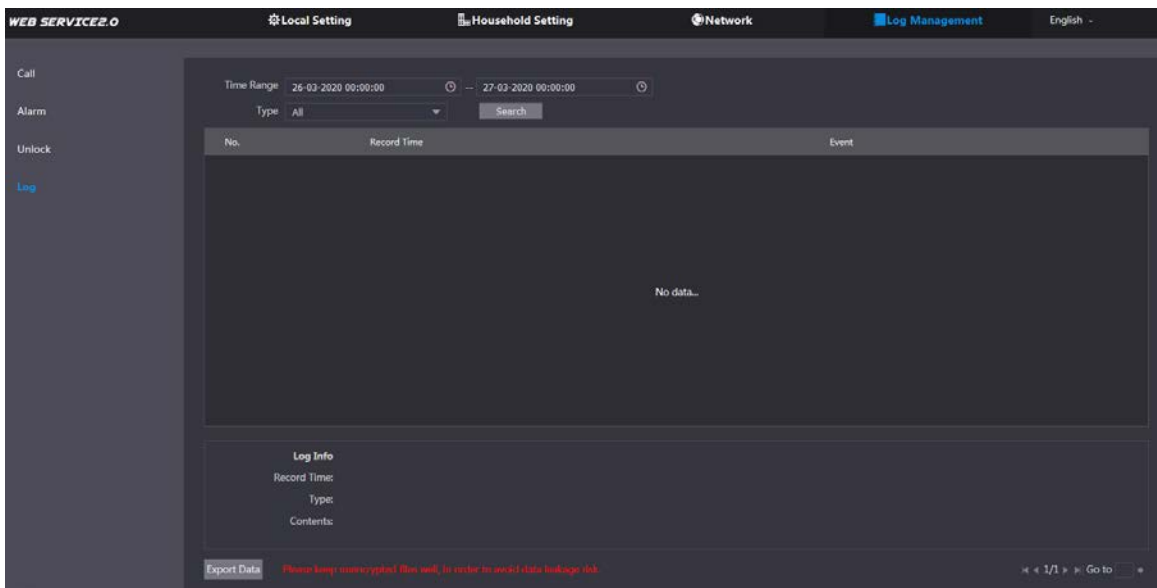


Click **Export Data** to export the records to your PC.

7.4 Log

You can search, view, and view logs of events in specific periods.

Figure 7-4 Log



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.