Digital VTH

User's Manual

V1.0.0

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.

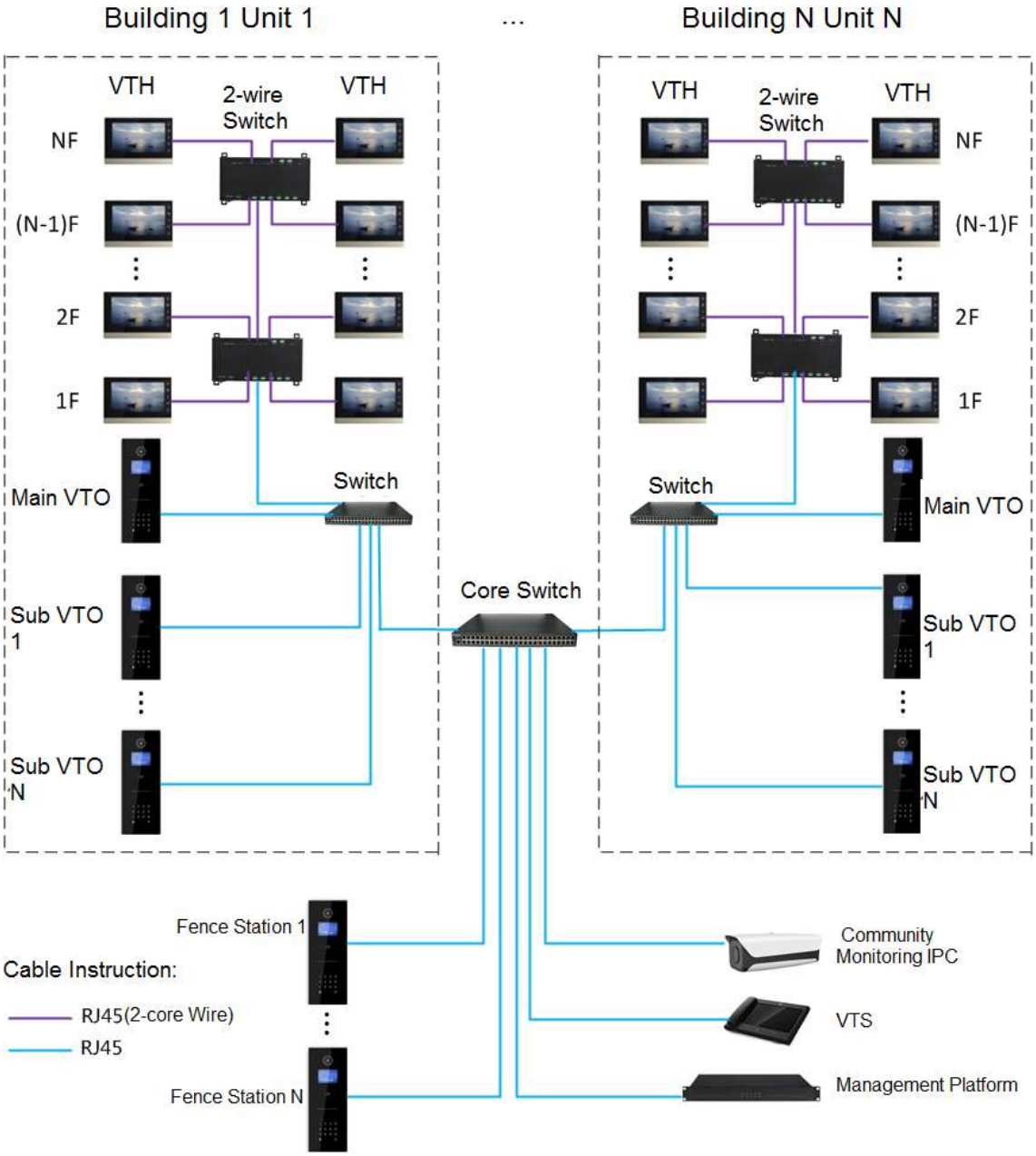
Message

View messages, including videos, pictures and announcements.

2 Network Diagram

2.1 2-wire System

Figure 2-1 Network diagram of 2-wire system

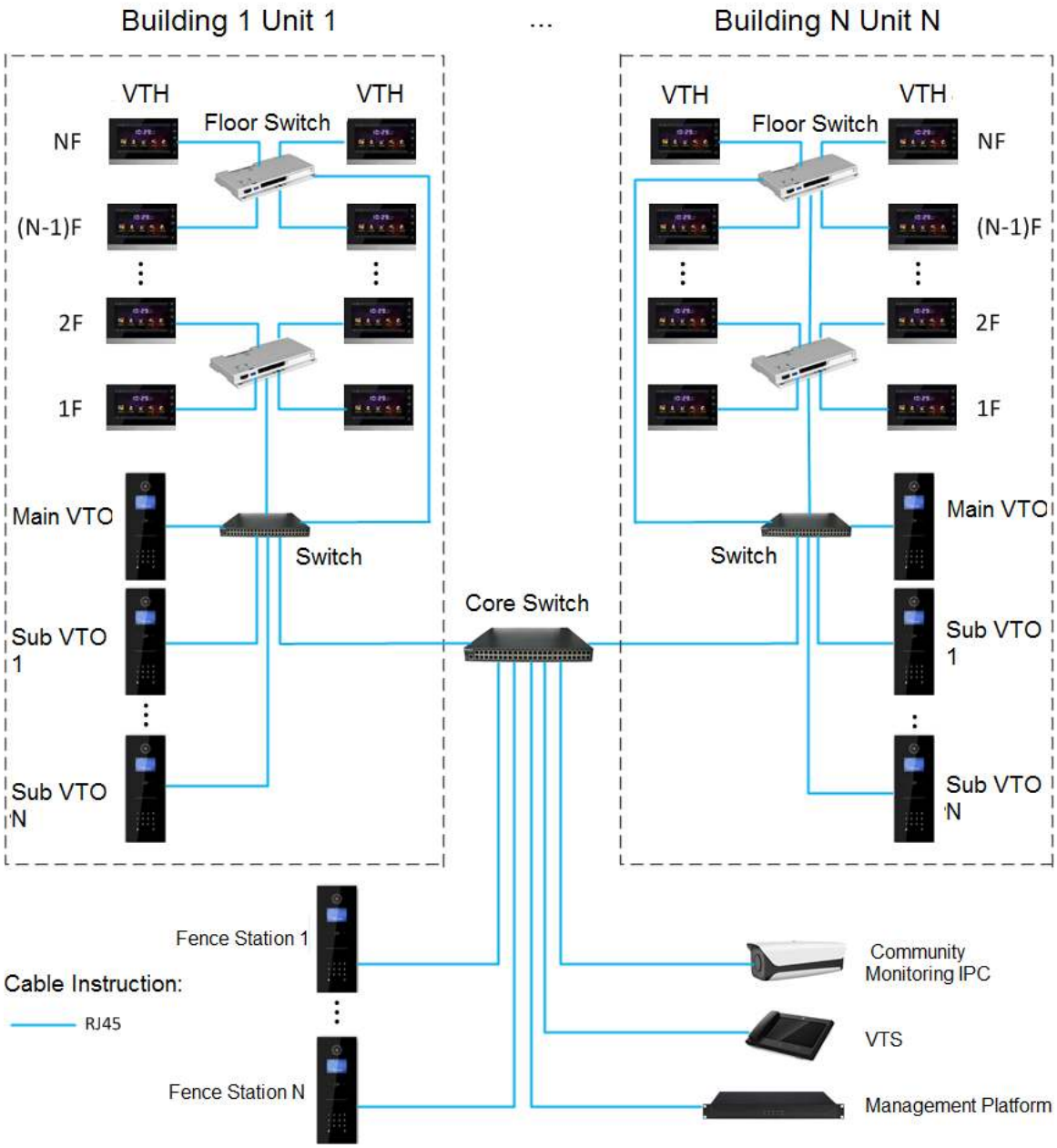


2.2 Digital System

There are two types of digital system network:

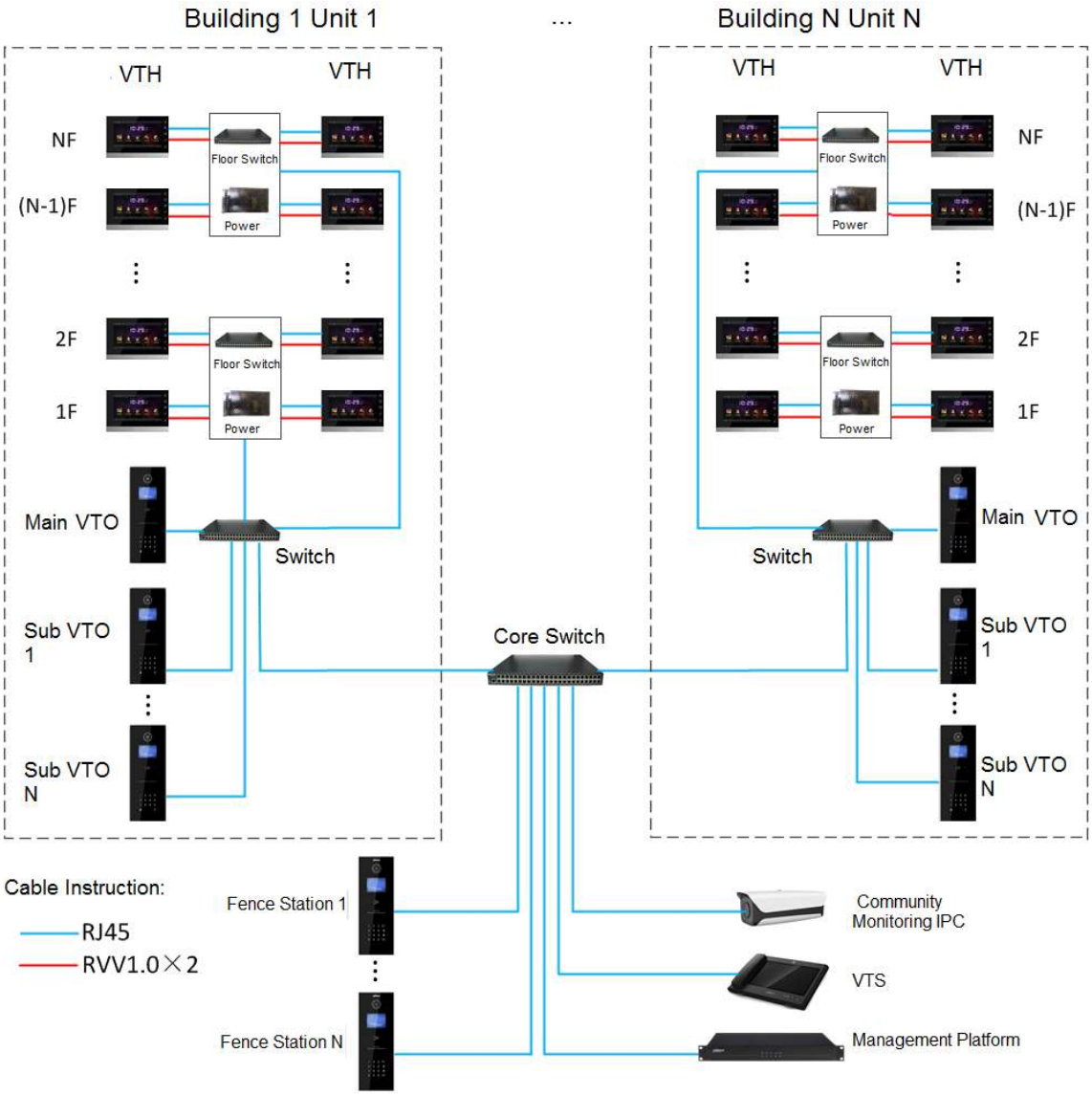
- The VTH powered through PoE from the floor switch.

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

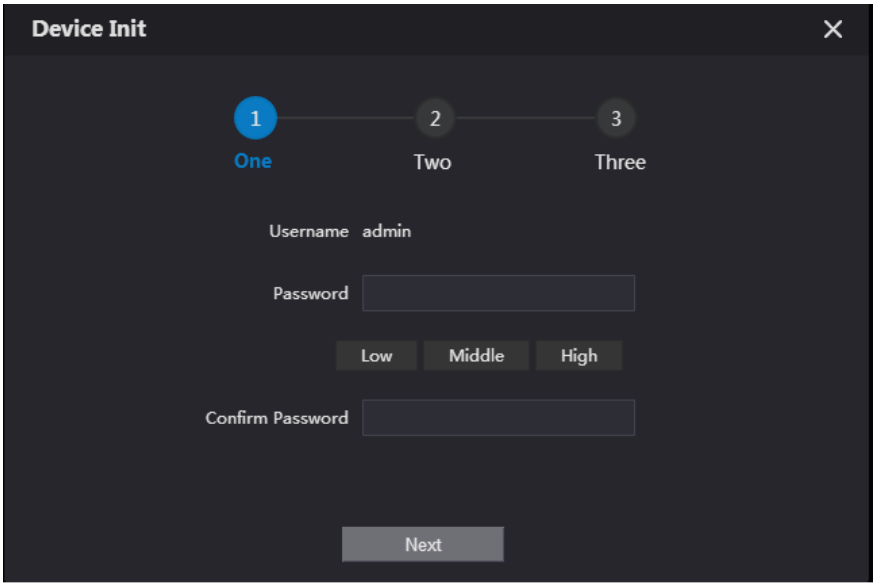
For first-time use, you must initialize the device.

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.

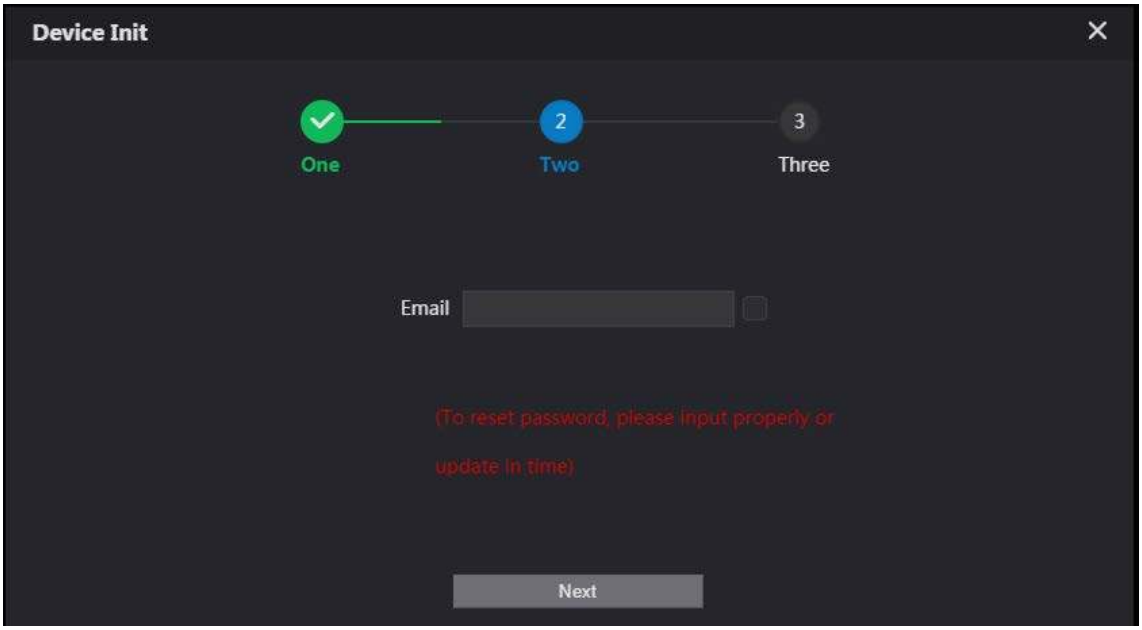
Figure 3-1 Device initialization



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.

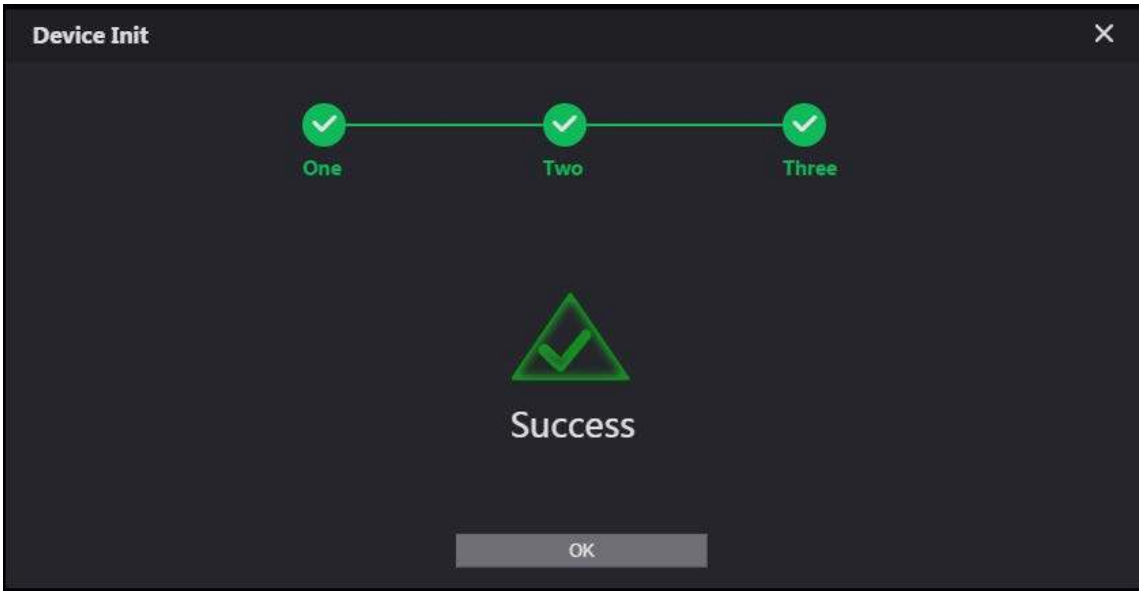
Figure 3-2 Set an email address



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

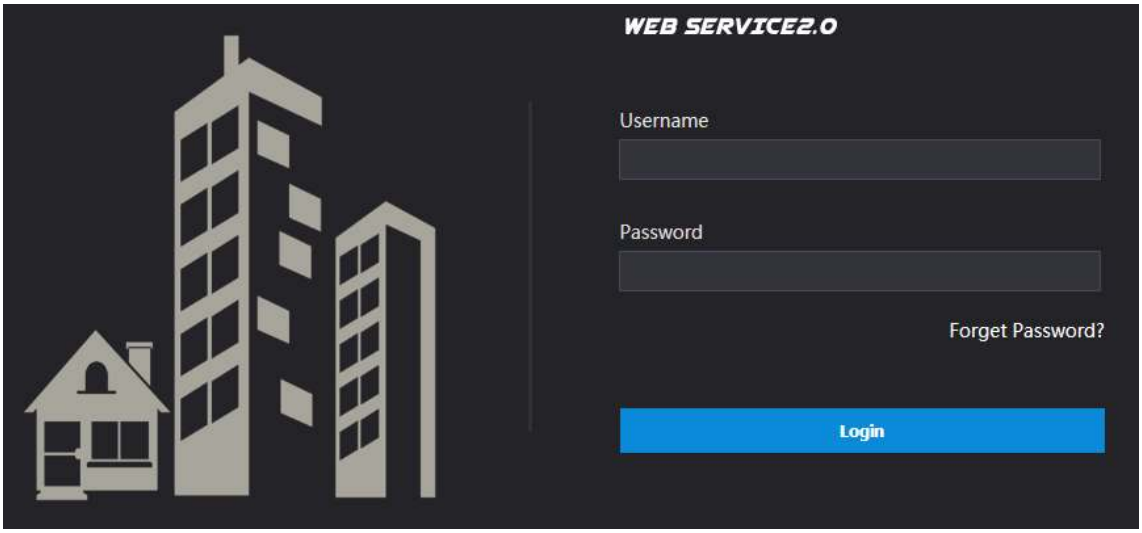
Step 5 Click **Next**.

Figure 3-3 Initialization successful



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

Figure 3-4 Login interface



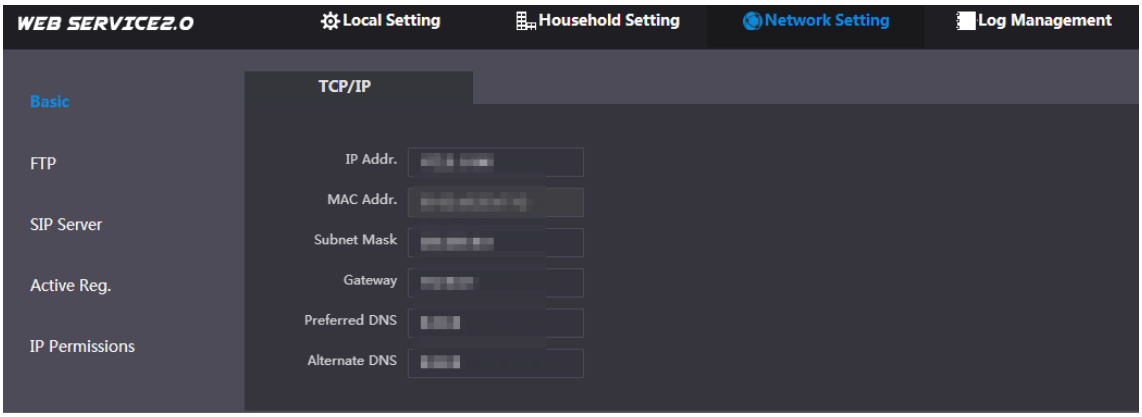
Step 7 Enter username (admin by default) and password, and then click **Login**.

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



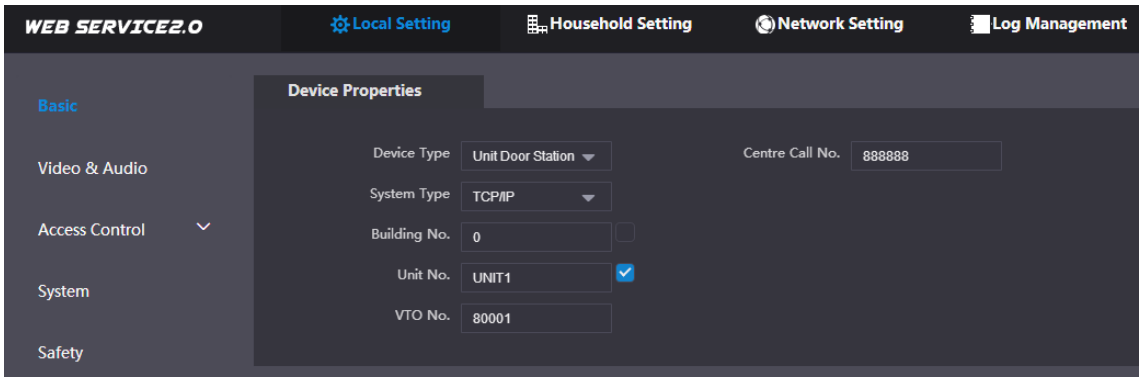
Step 2 Enter the parameters, and then click **OK**.

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**.

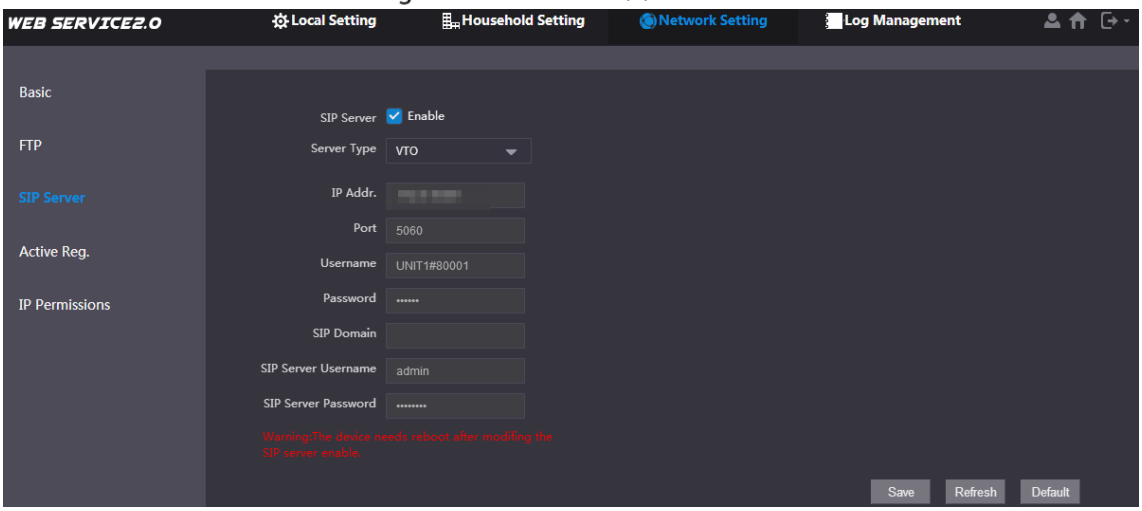
Wait for the device to automatically restart or restart it manually, and then the settings will take effect.

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)



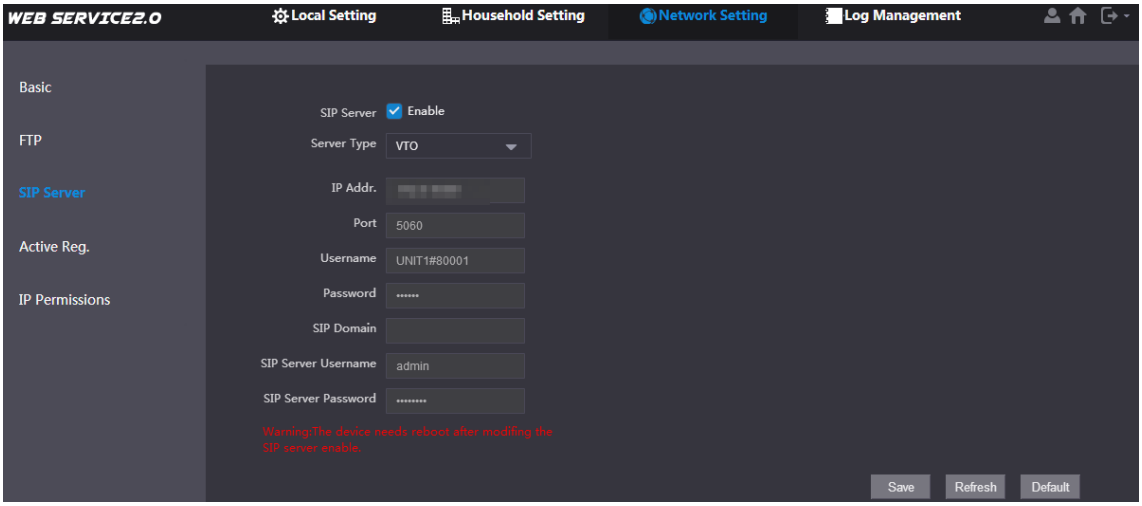
Step 2 Select a server type.

- 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.

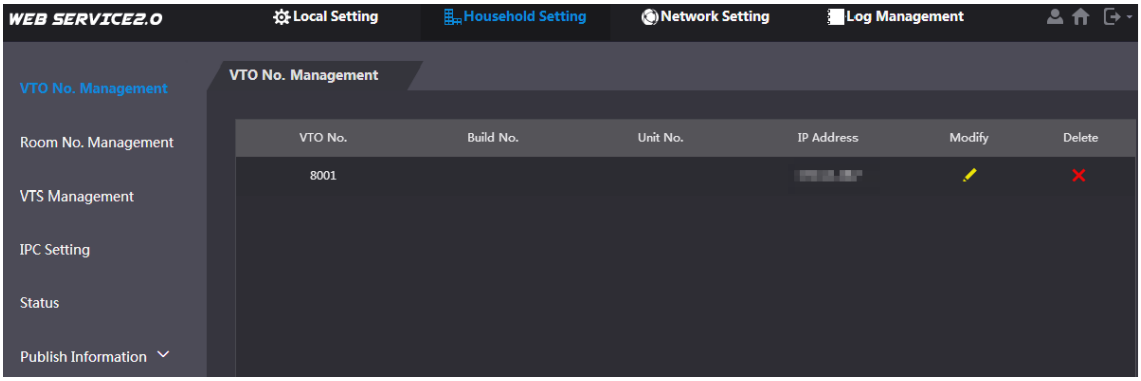
3.1.1.6 Adding VTO

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

Step 1 Log in to the web interface.

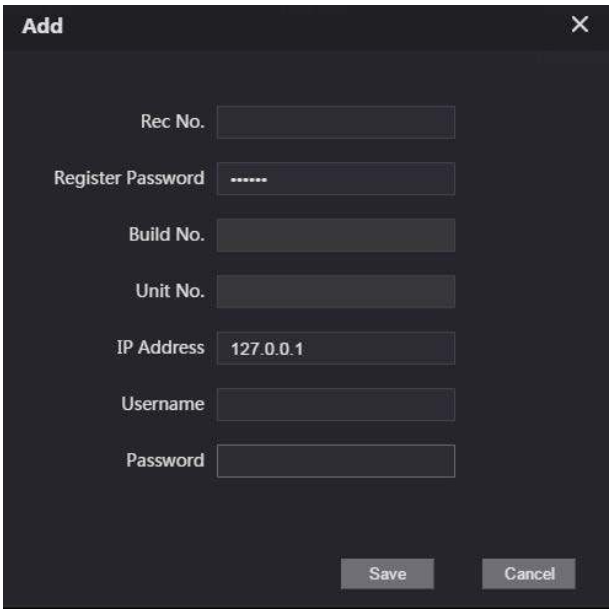
Step 2 Select **Household Setting > VTO No. Management**.

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**.

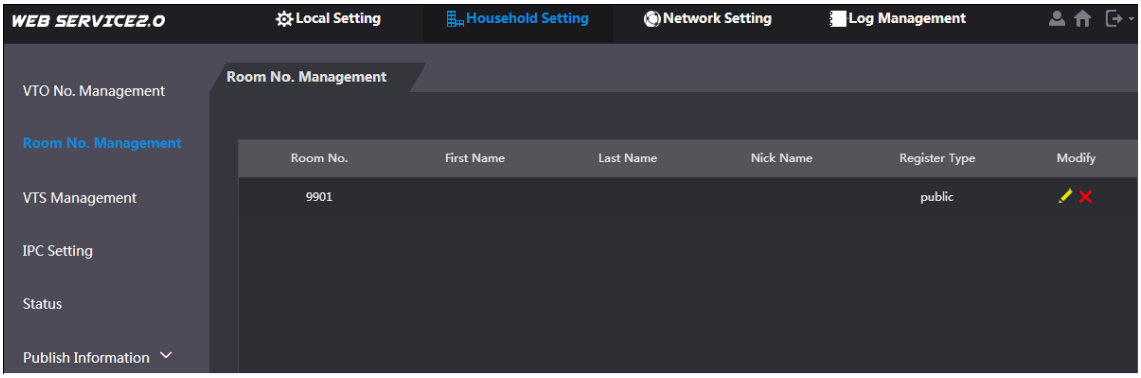
Do Step 3–Step 5 to add other VTOs.

3.1.1.7 Adding VTH

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

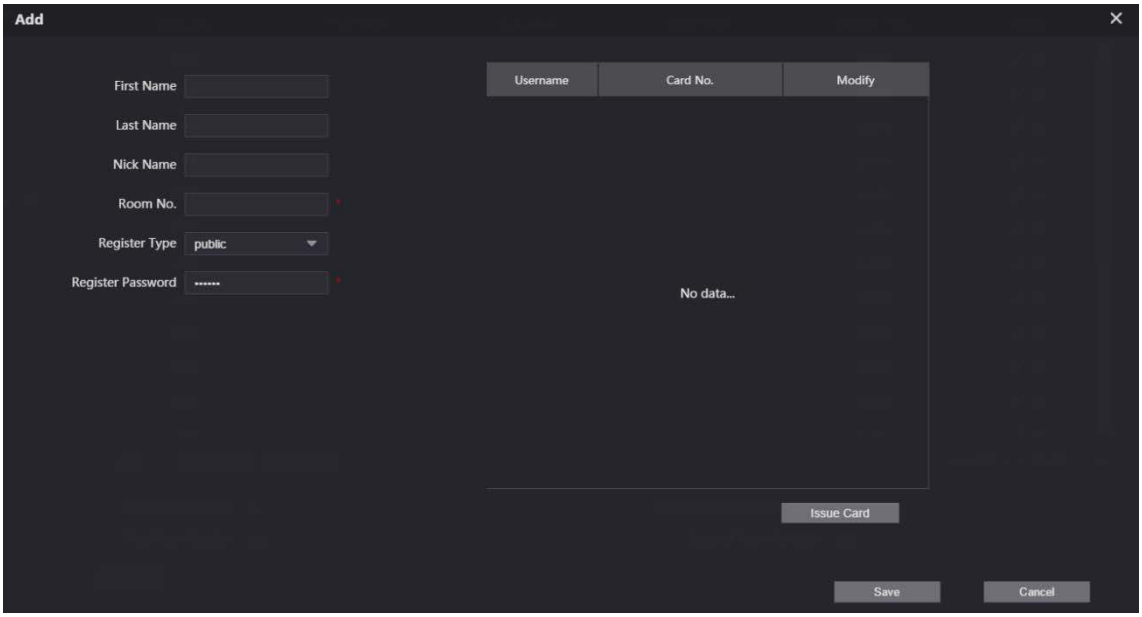
Step 1 Select **Household Setting** > **Room No. Management**.

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.	● 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**.

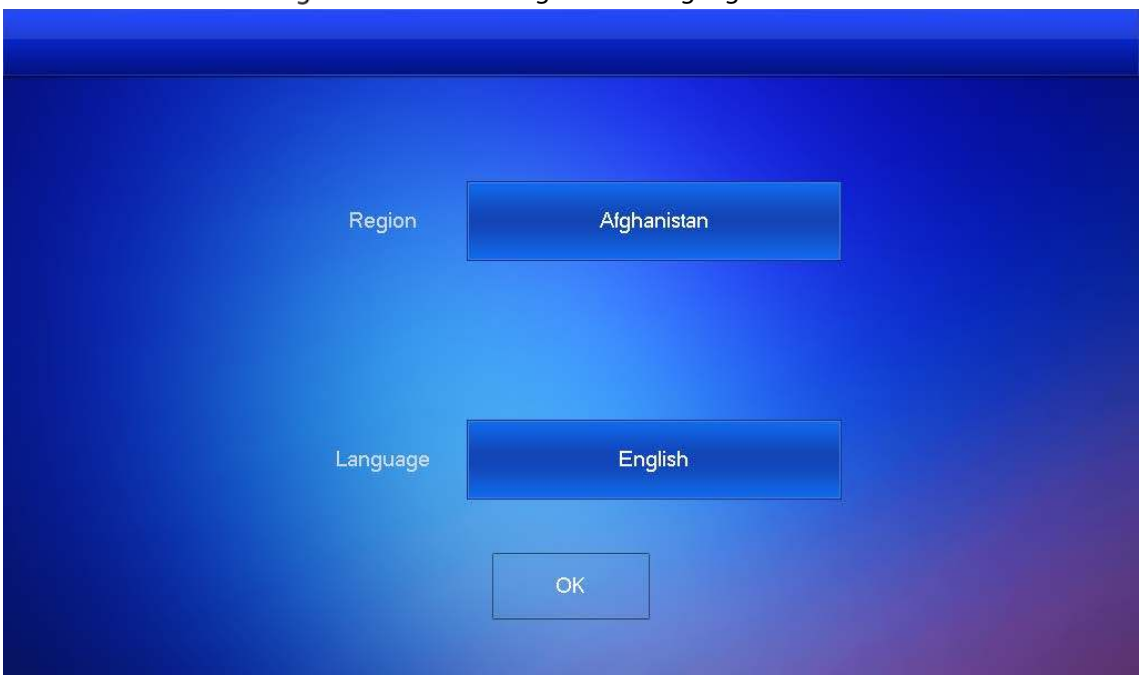
Do Step 2–Step 4 to add other VTHs.

3.1.2 VTH Settings

3.1.2.1 Initialization

Step 1 Select a region and language.

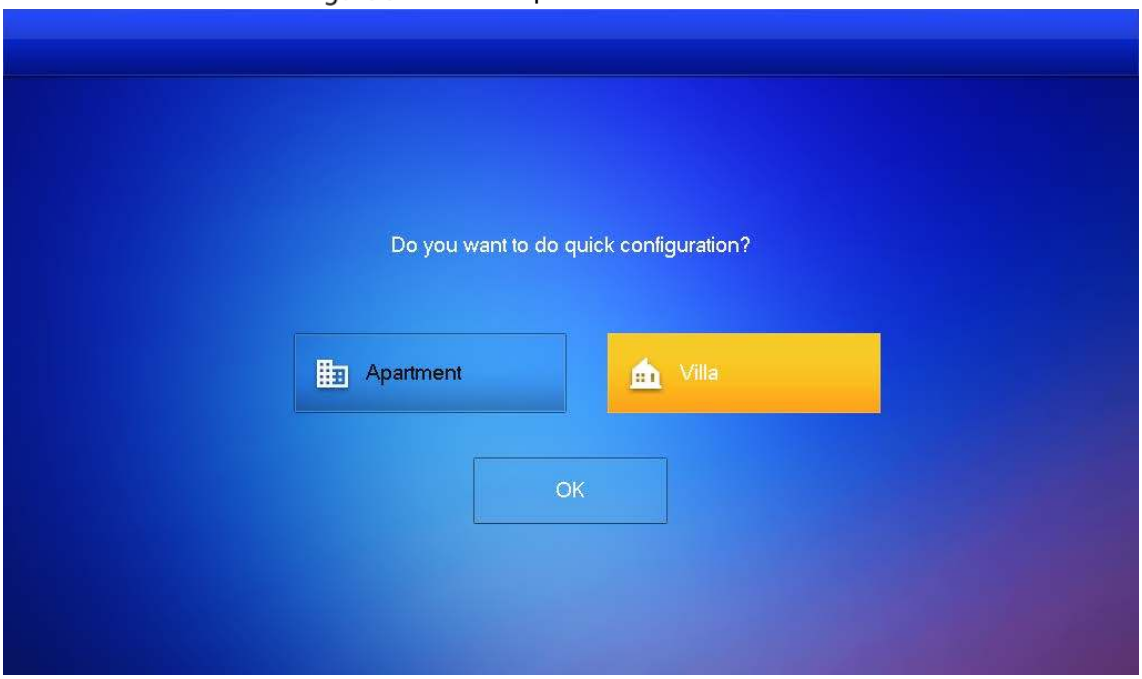
Figure 3-13 Select a region and language



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

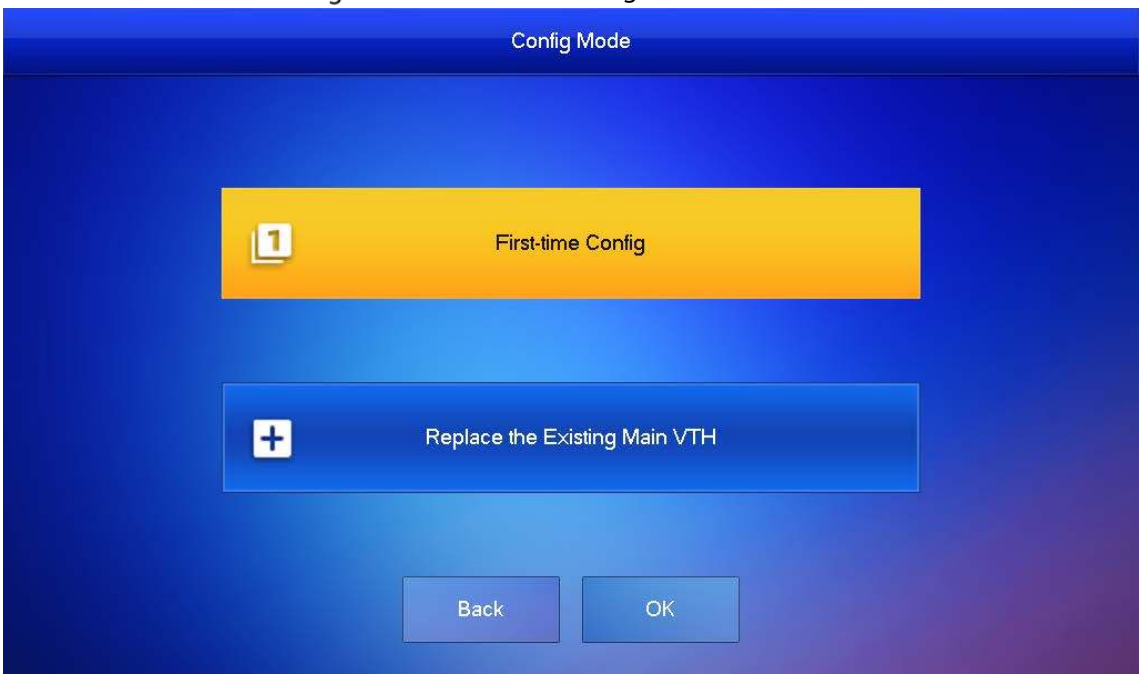
This section takes **Villa** as an example.

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

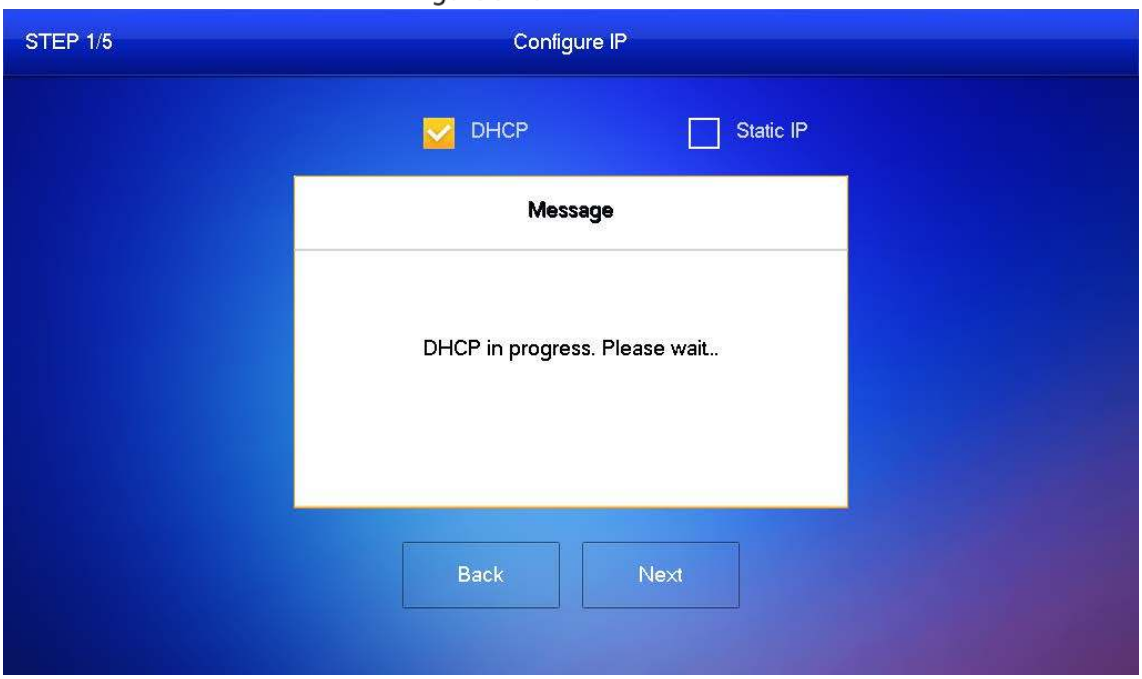
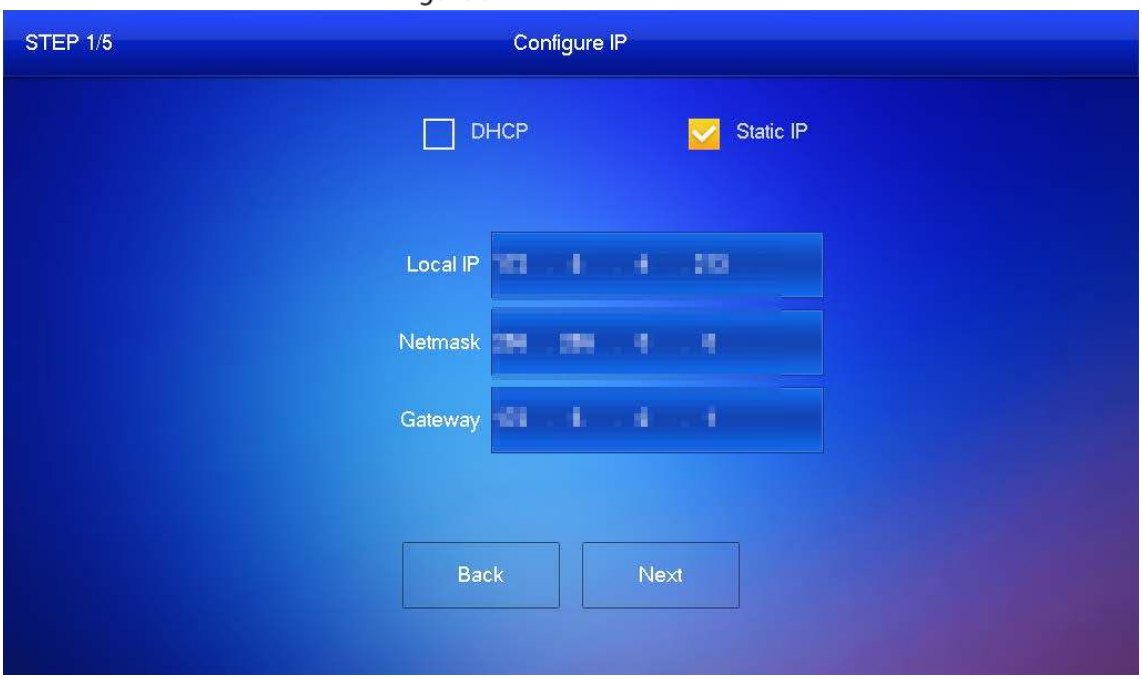


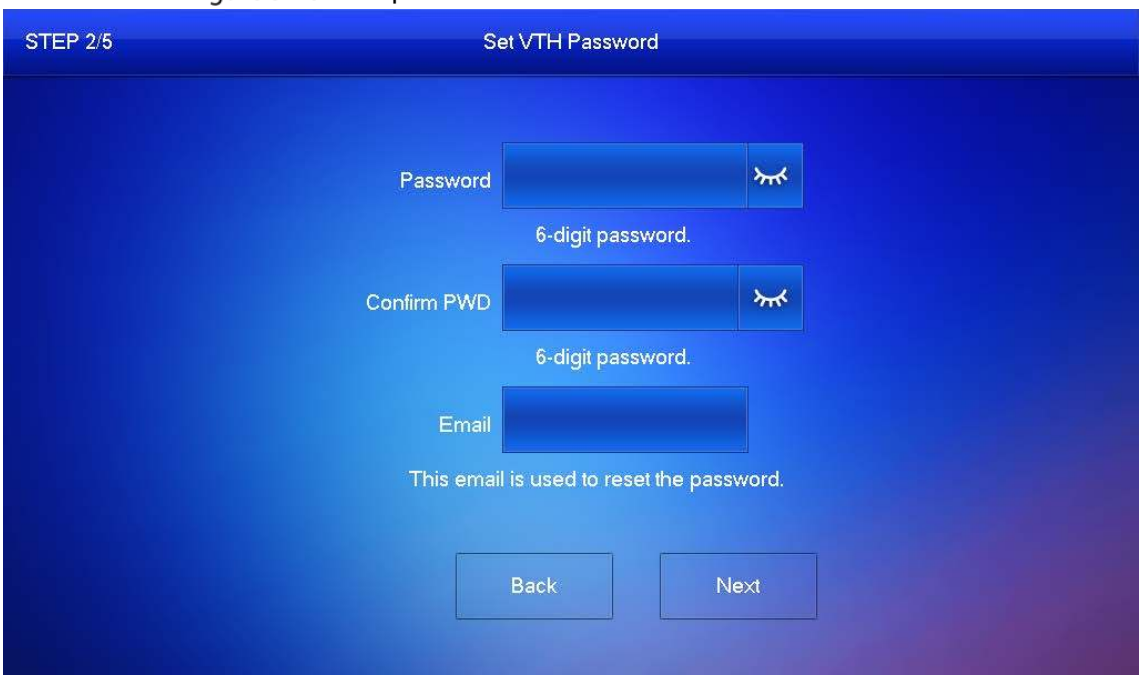
Figure 3-17 Static IP



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.

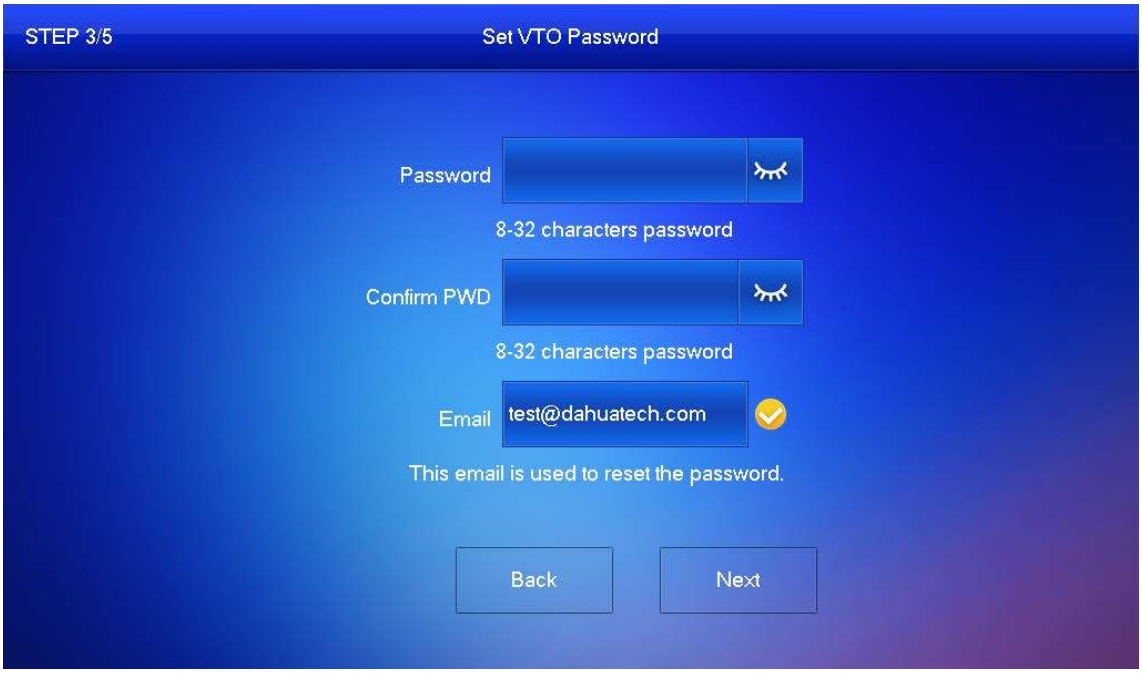
Figure 3-18 Set a password an email address for the VTH



Step 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



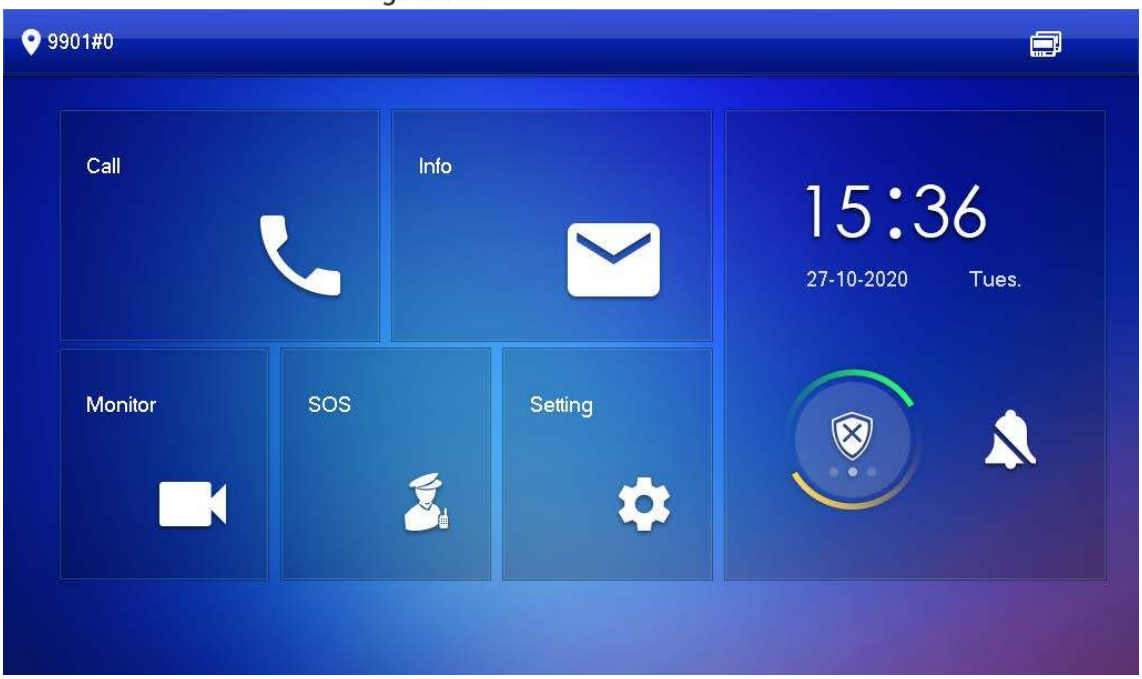
Step 7 Click **Initialize** to initialize a single device or **Batch Initialization** to initialize all available devices, and then click **Next**.

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.

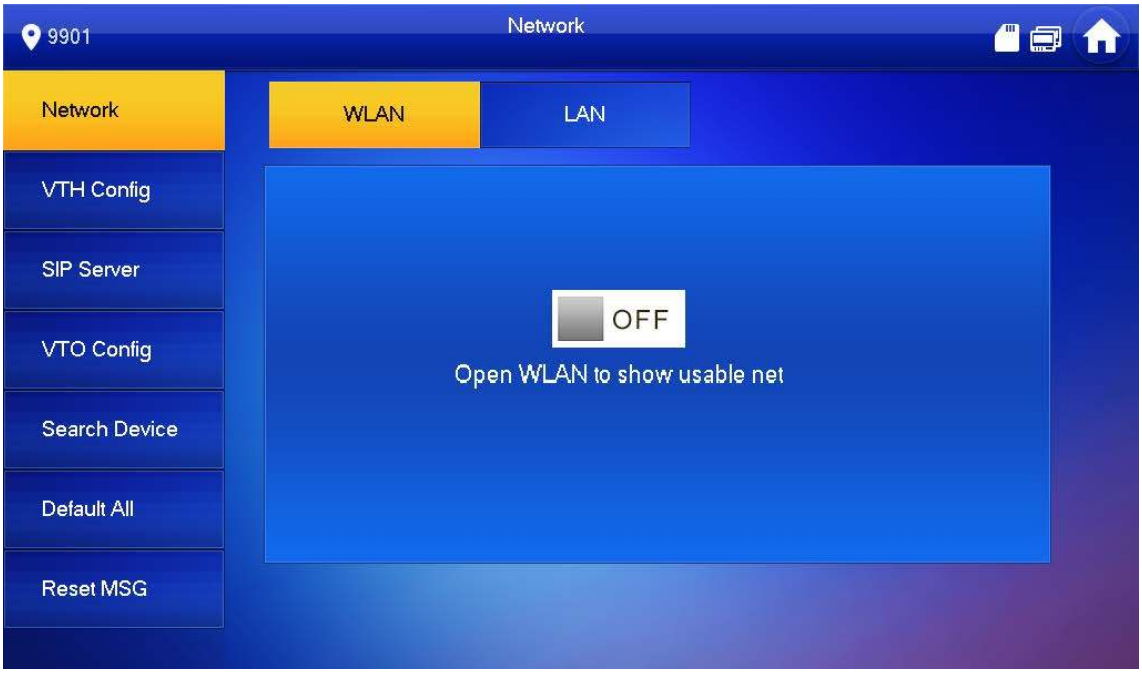
Figure 3-23 LAN

- 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	● 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	● 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

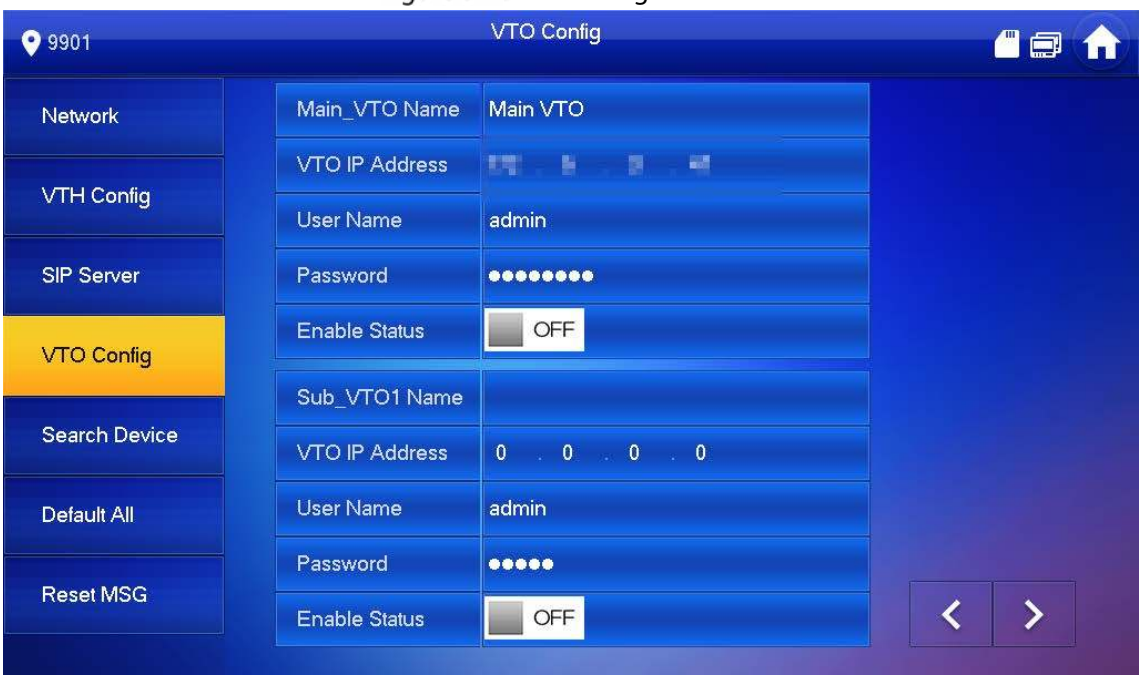
Add VTOs and fence stations to bind them with the VTH.

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.

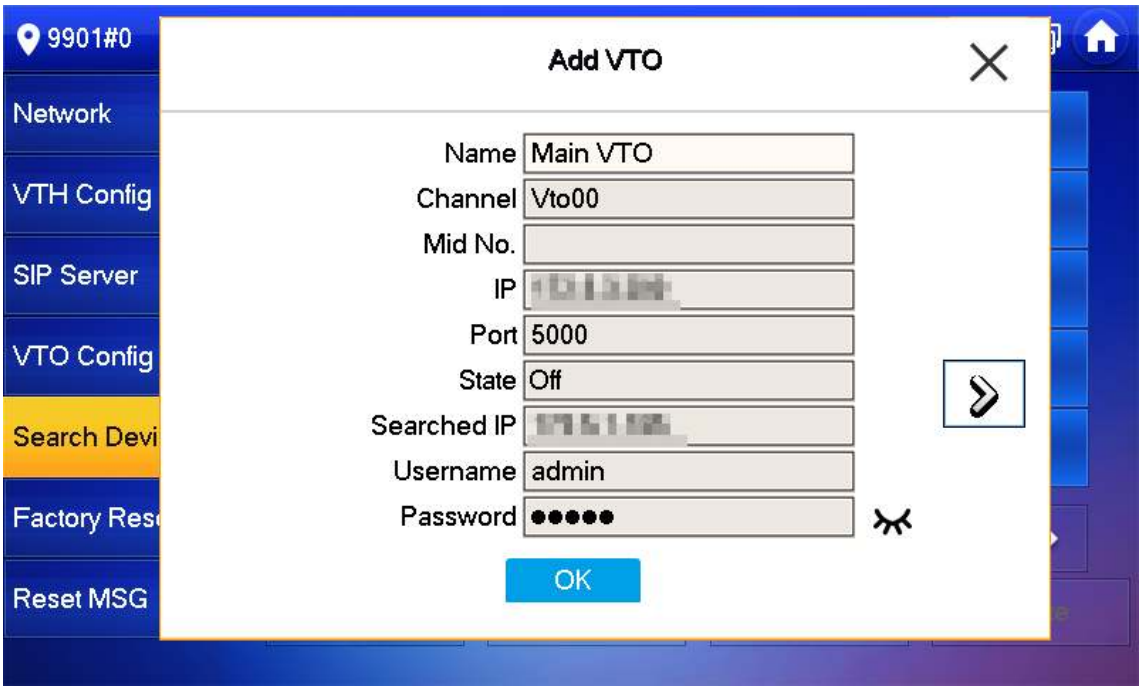
Figure 3-29 Search device

Step 2 Tap a device.

You can only add or edit villa VTOs.

- Click **Add**.

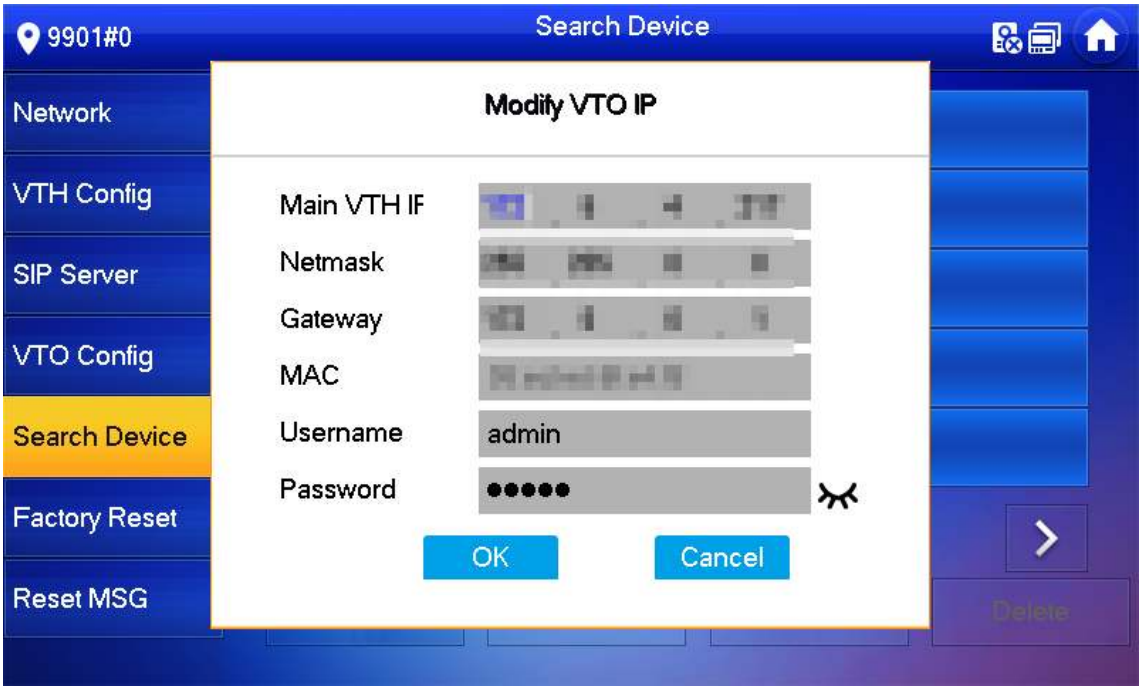
Figure 3-30 Add a VTO



- 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

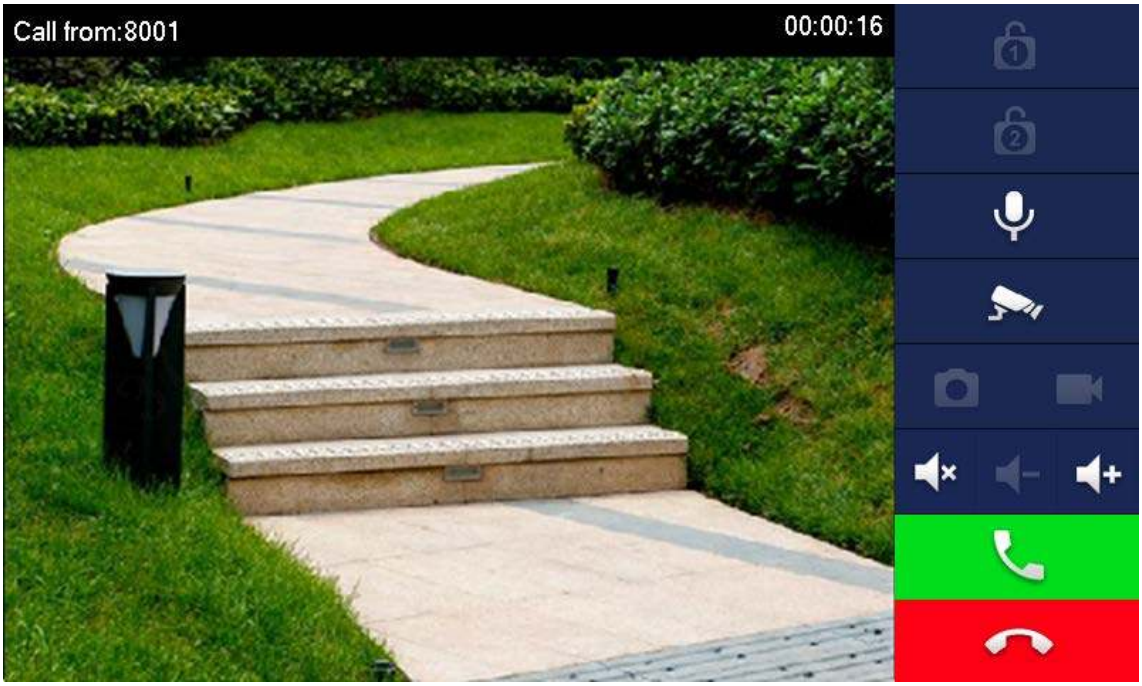


3.2 Commissioning

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

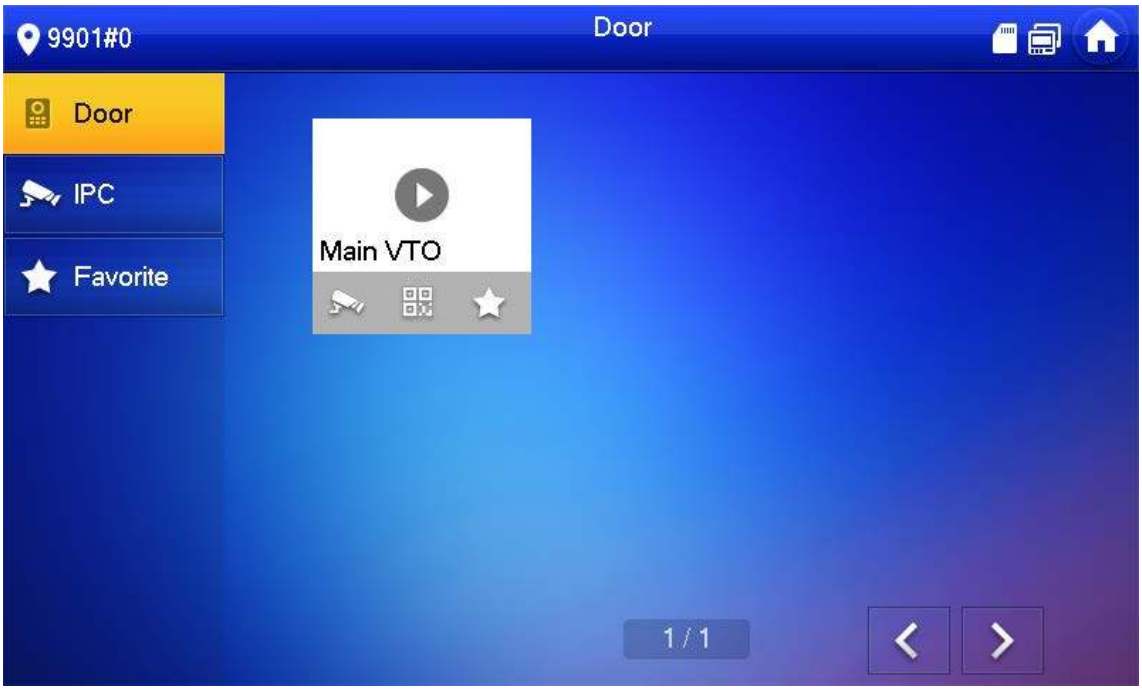
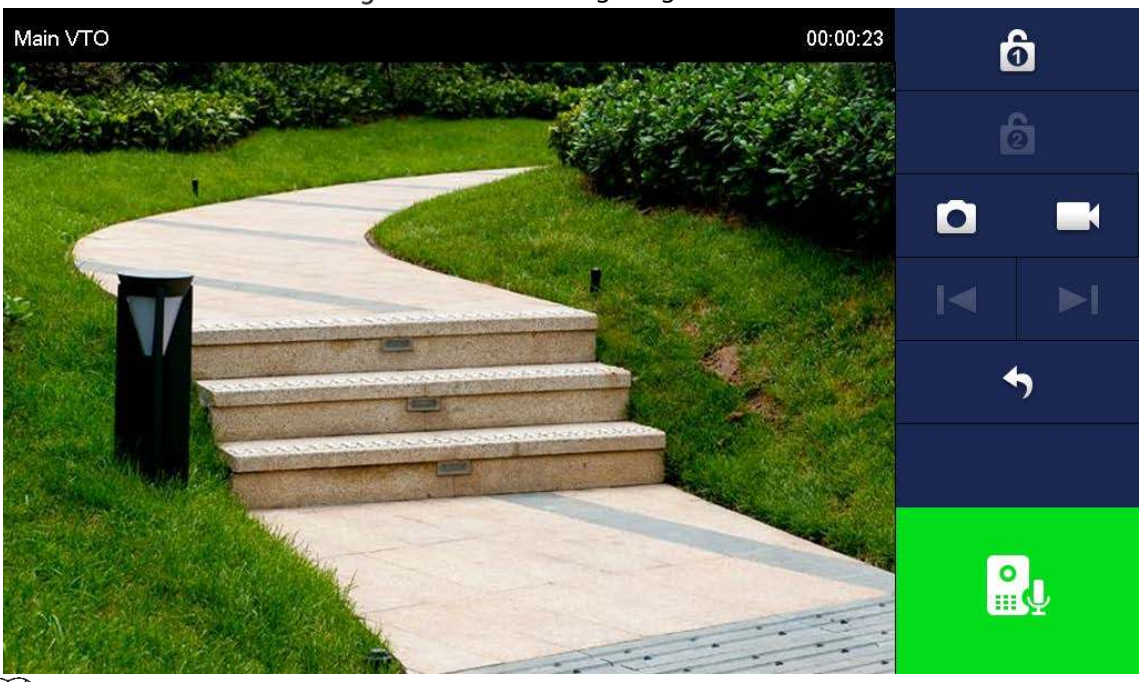


Figure 3-34 Monitoring image



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

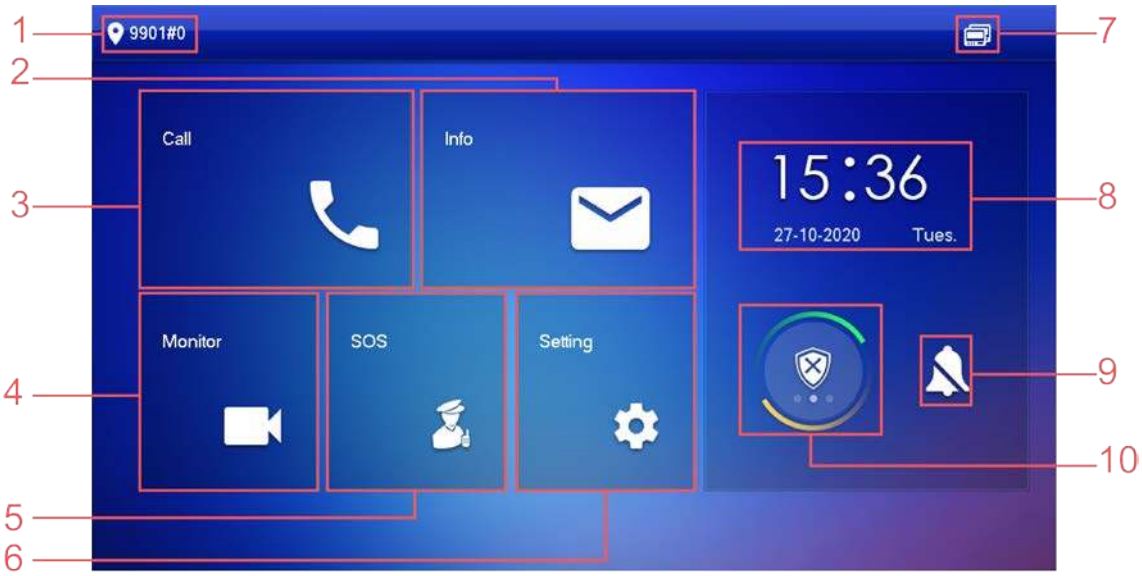


Table 4-1 Main interface description

No.	Name	Description
1	Room number	Number of the room where the VTH is located.
2	Info	● 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	● 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	● Tap to enter system setting. ● Tap for more than 6 seconds, input the password set during initialization, and then enter project setting.
7	Status	● : Not connected to the network. ● : Connected to the network through a cable. ● : Wirelessly connected to the network.

No.	Name	Description
		• : 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	• Display unread alarm information. • Tap to select an arm mode.

4.2 Call

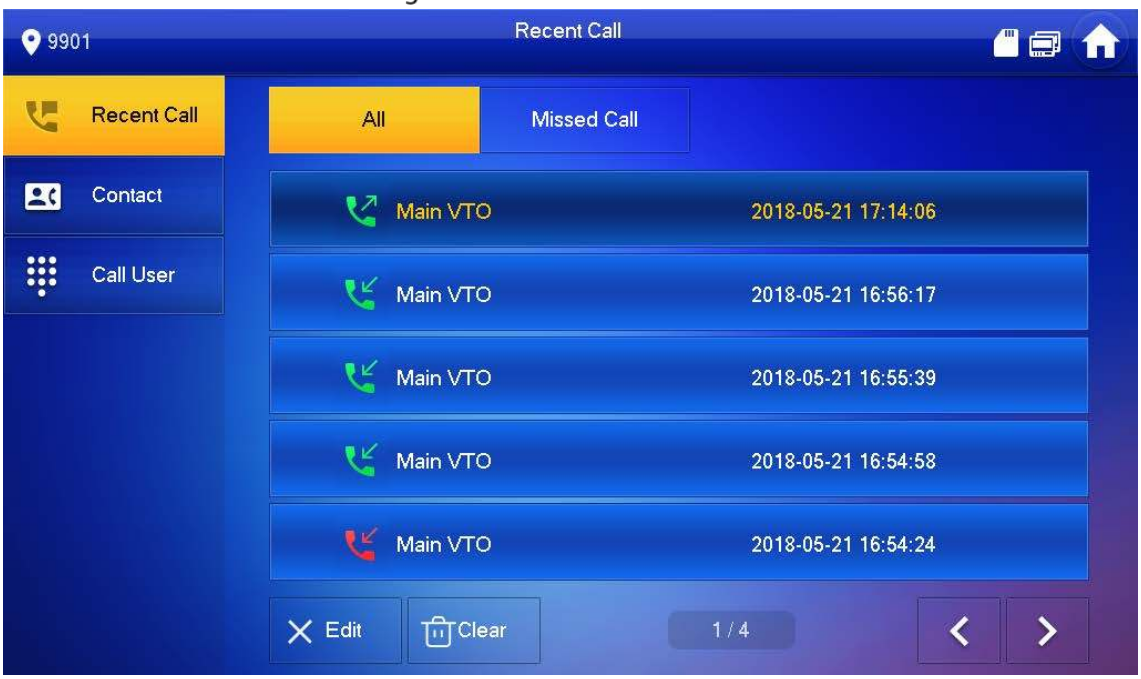
Manage contact, call and view call records.

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.

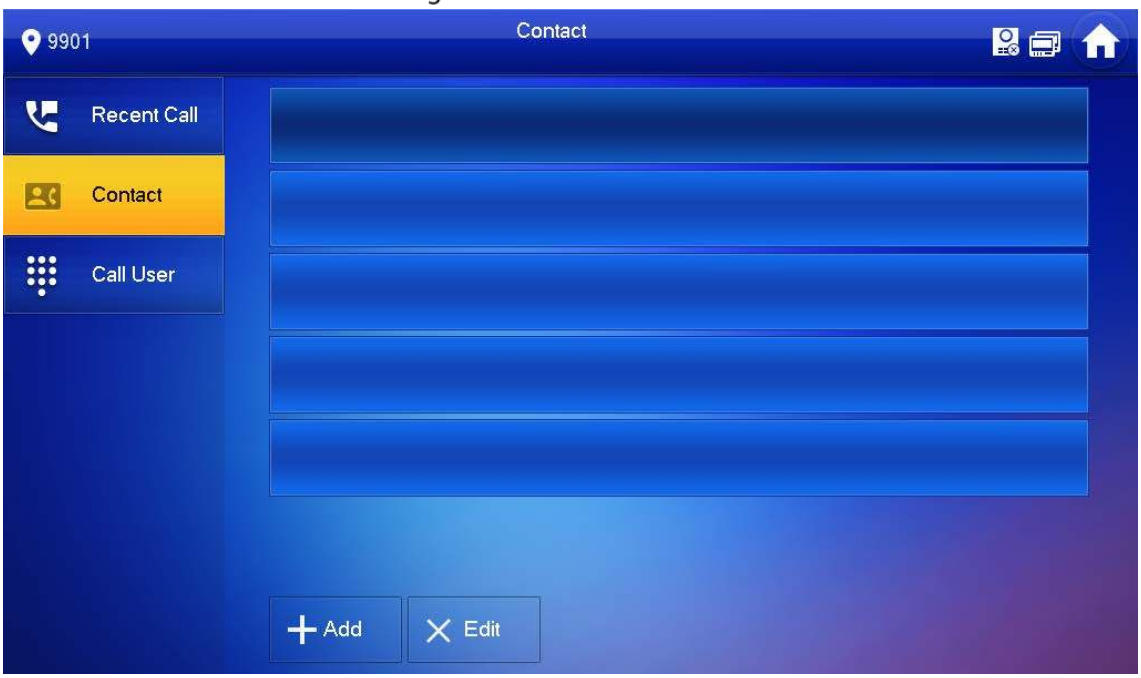
- **Clear**: Clear all record in the current tab (**All** or **Missed Call**).

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.

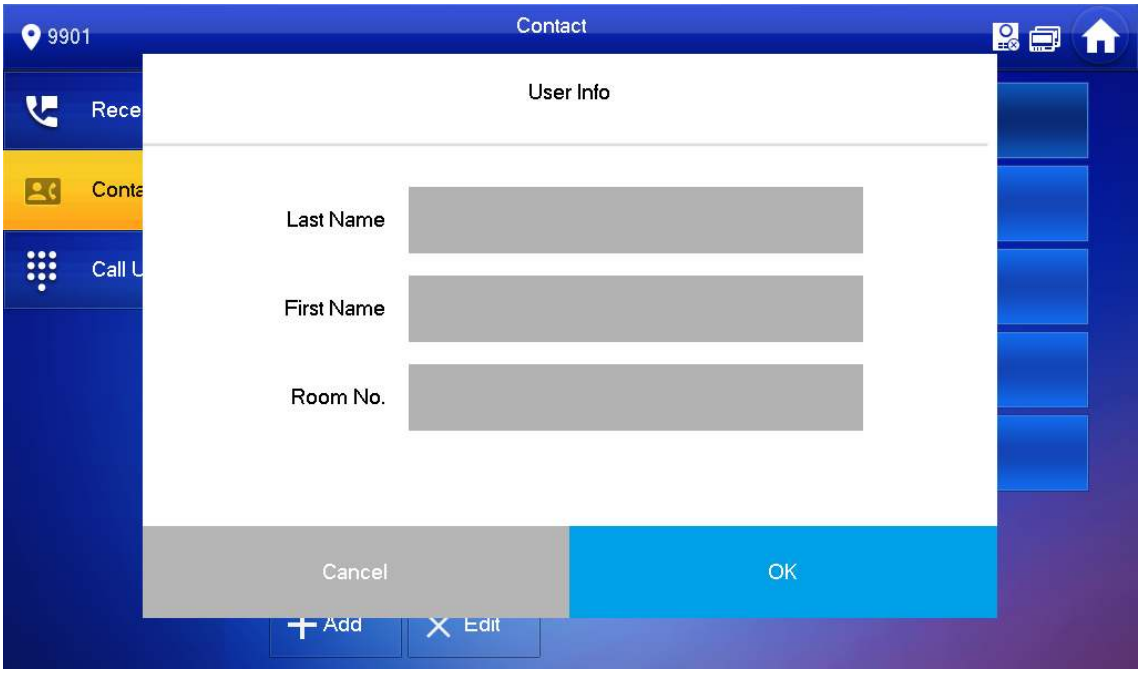
Figure 4-3 Contact



- 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

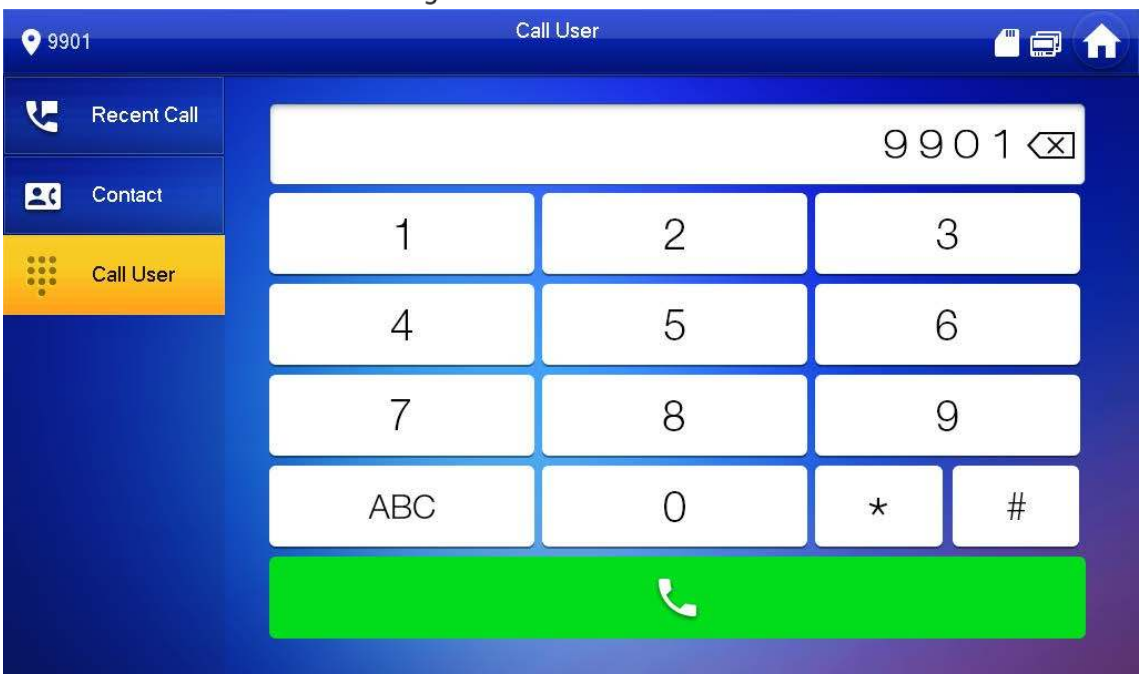
- Make sure that resident-to-resident call function has been enabled. See "4.6.6.4 QR Code" for details.
- Call function is used by VTH to call VTH.
- If both VTHs have a camera, bilateral video call can be provided.

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

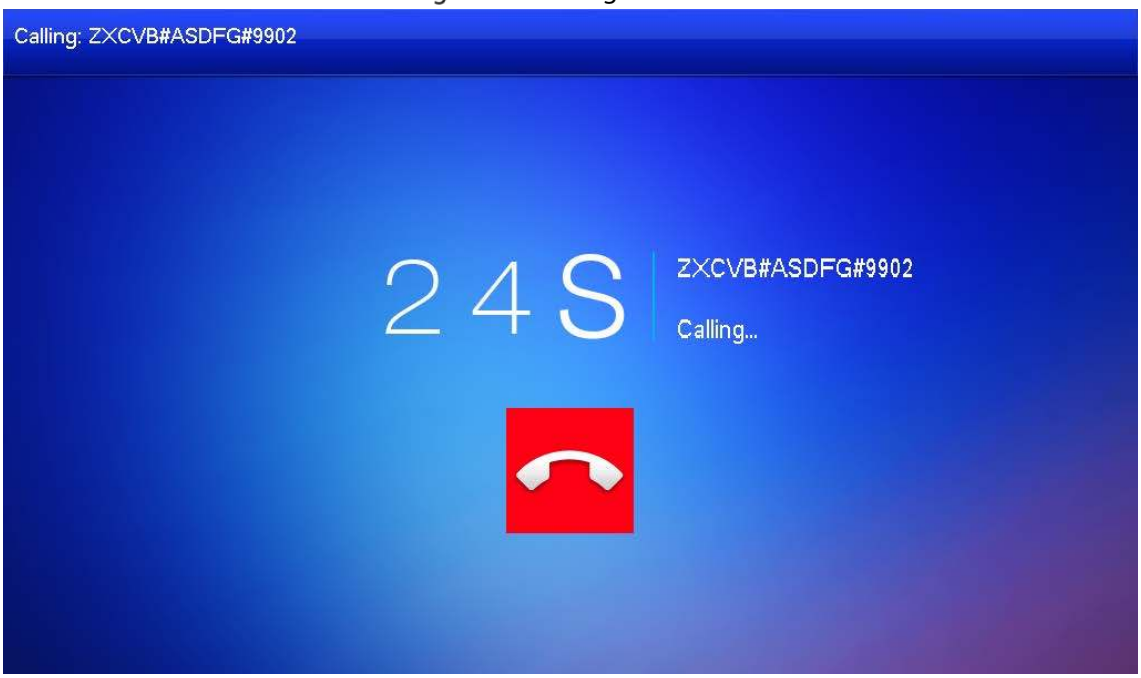
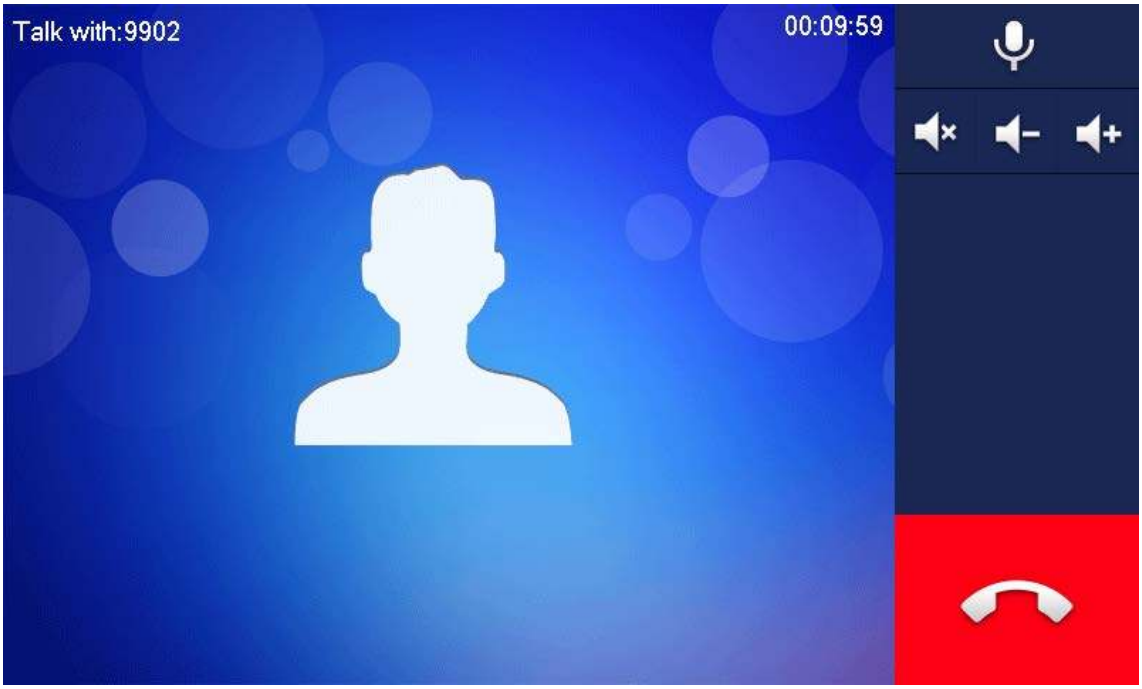


Figure 4-7 Call in progress



4.2.3.2 From Contact

Add contacts first. See 4.2.2 Contact.

Step 1 Select **Call** > **Contact**.

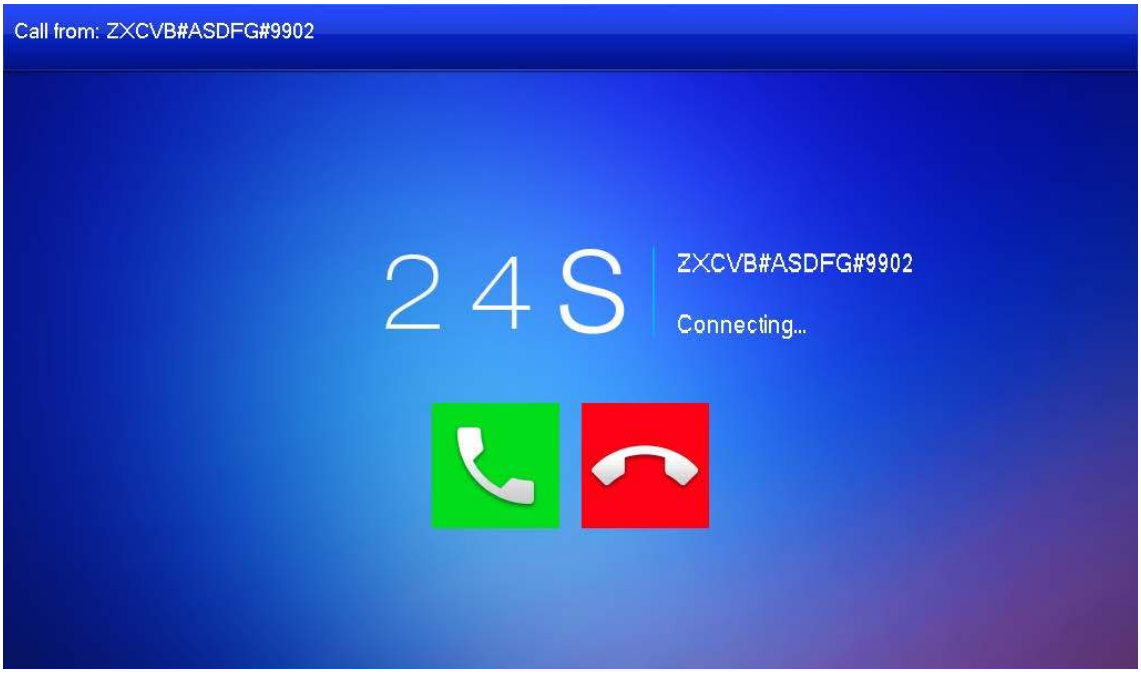
Step 2 Select the one you want to call.

Step 3 Tap to start.

4.2.4 Call from User

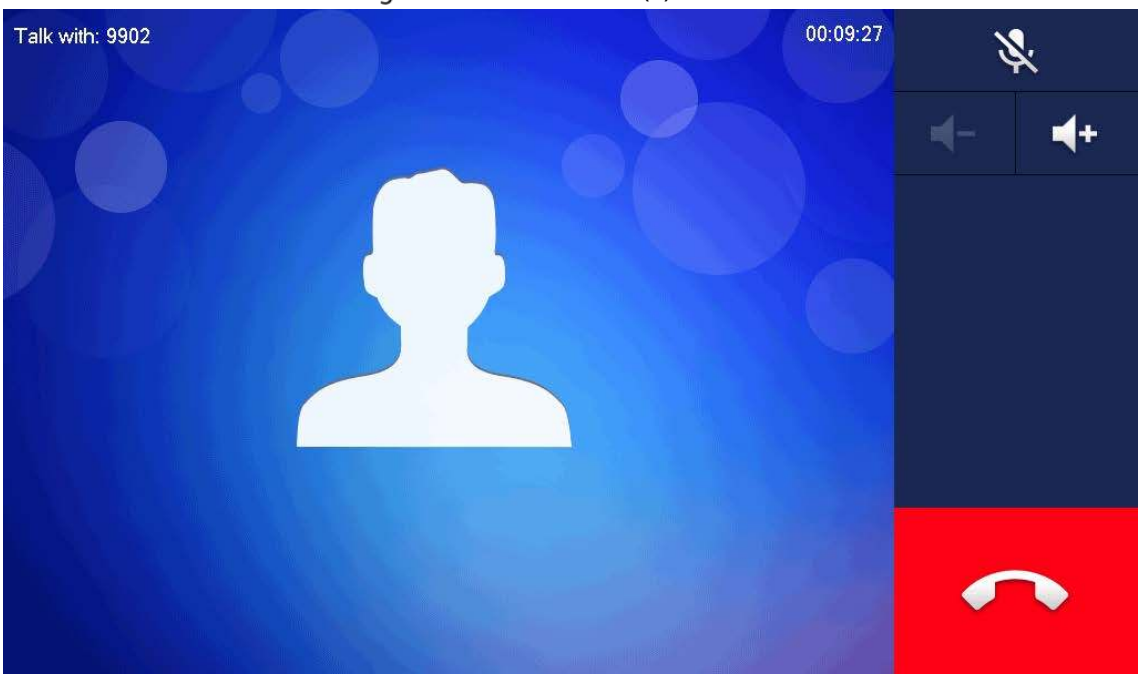
When receiving calls from other VTHs, the following interface will be displayed.

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

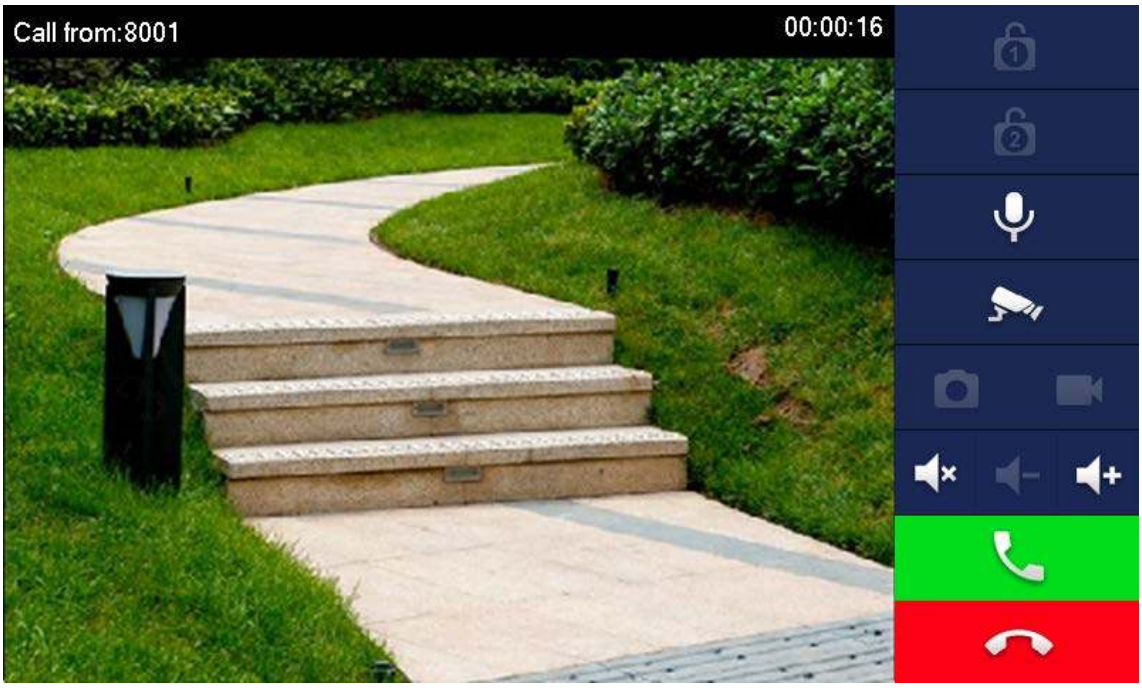


Table 4-2 Interface description

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 . ● 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

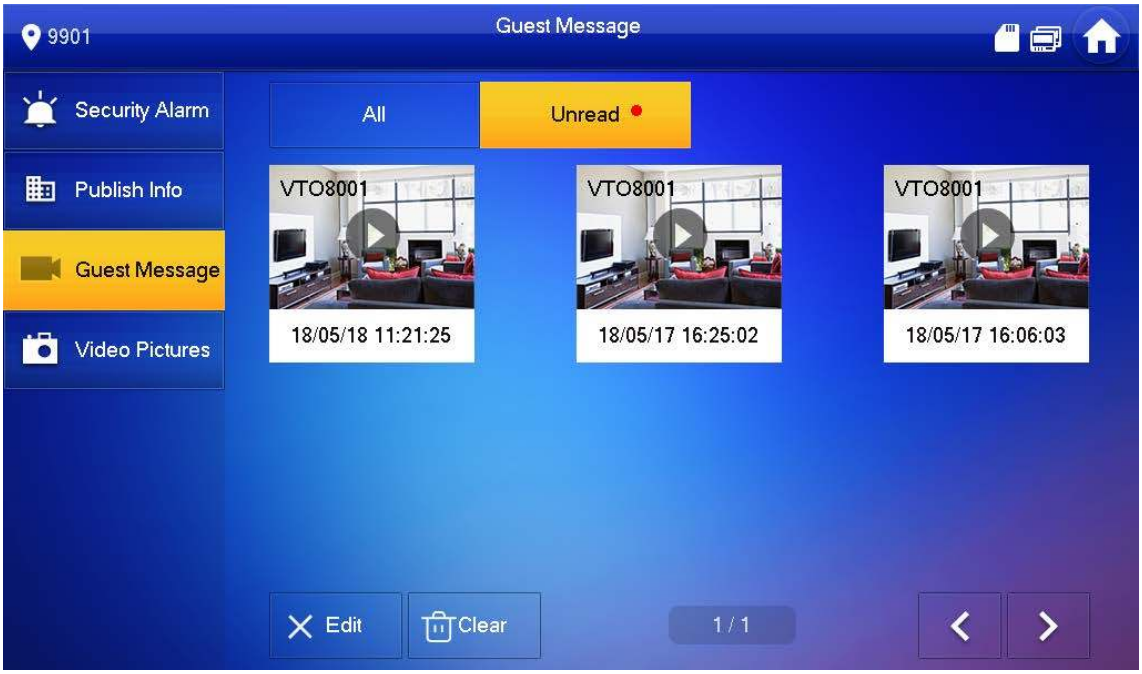
Select **Info** > **Security Alarm**, and then you can view and manage all alarm records.

Figure 4-12 Security alarm

4.3.2 Guest Message

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

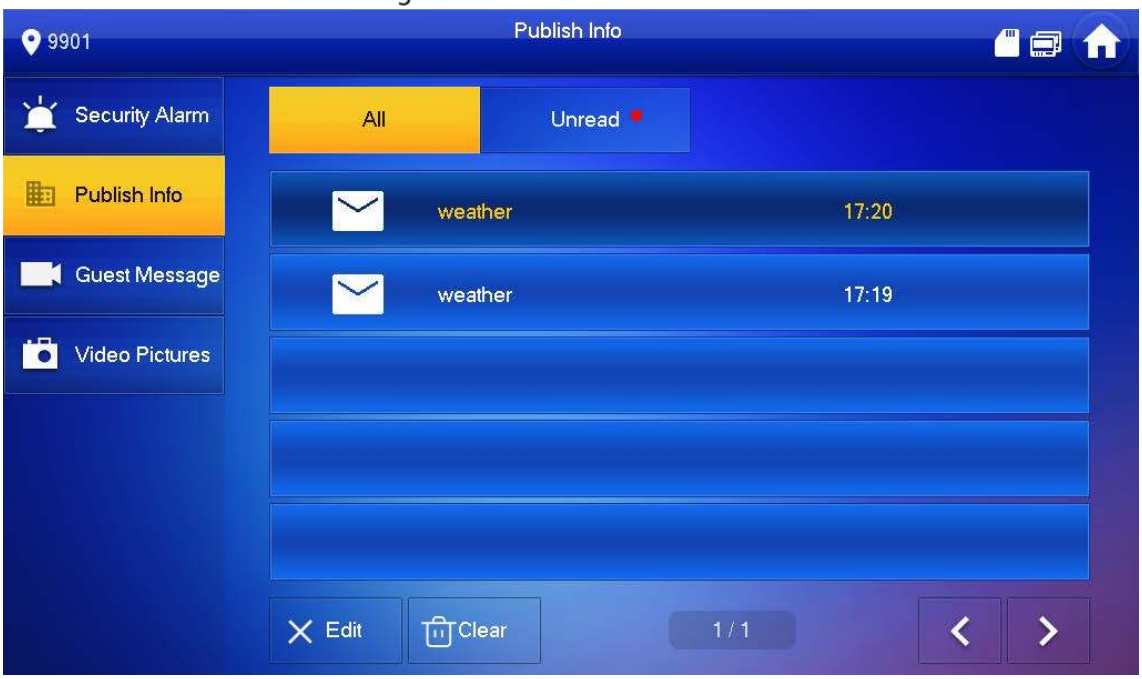
Figure 4-13 Guest message



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

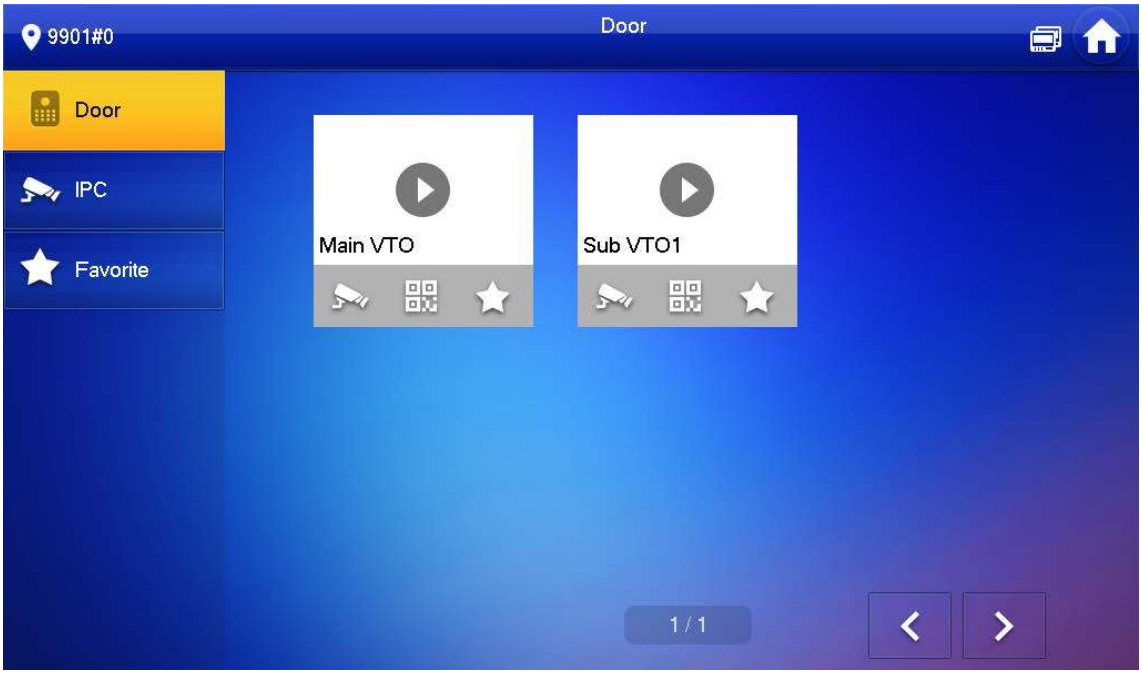


Table 4-3 Function description

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

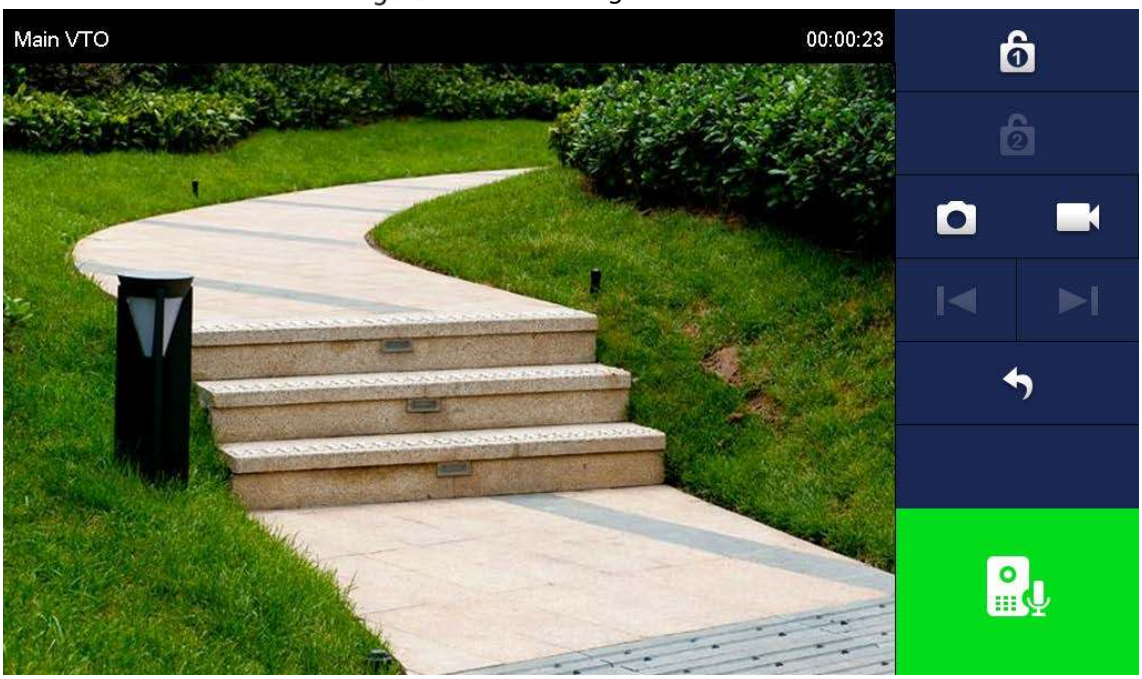


Table 4-4 Interface description

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

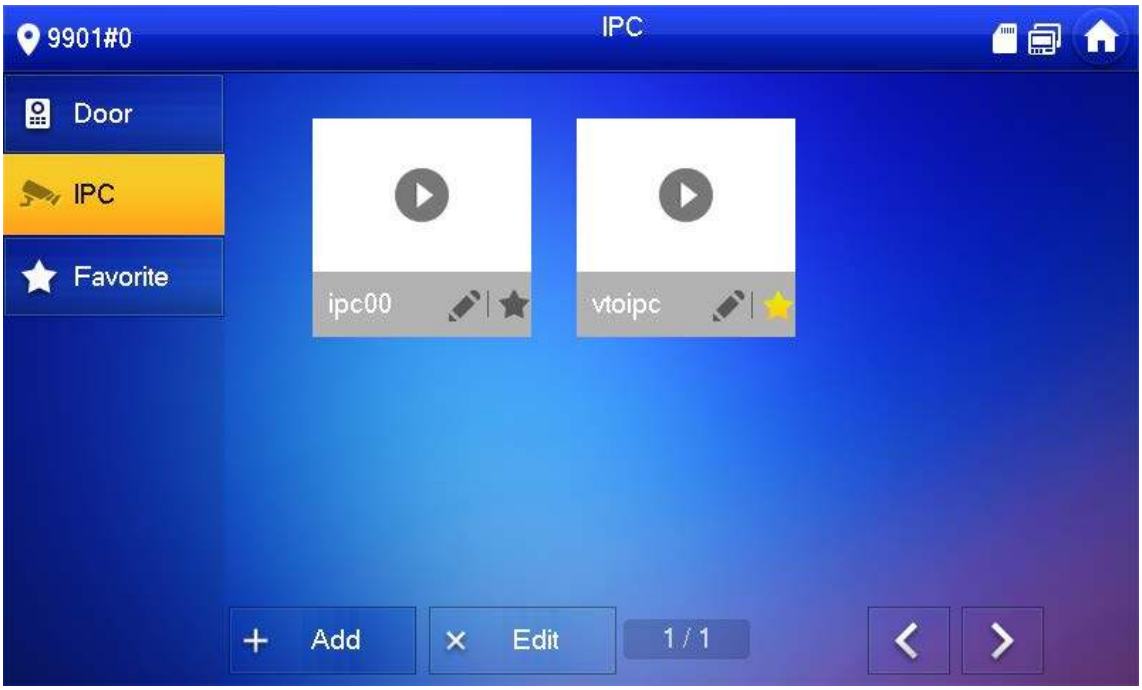
4.4.2.1 Adding IPC

- 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**.

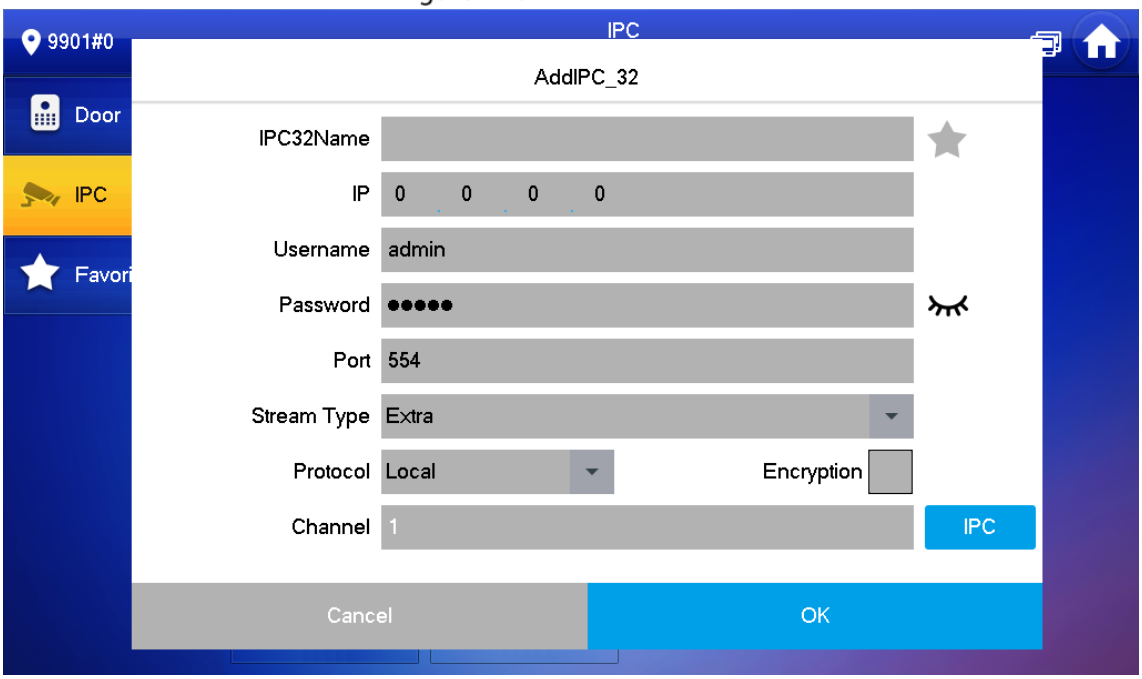
You can tap ★ to add the IPC to **Favorites**.

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	• 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	• 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.

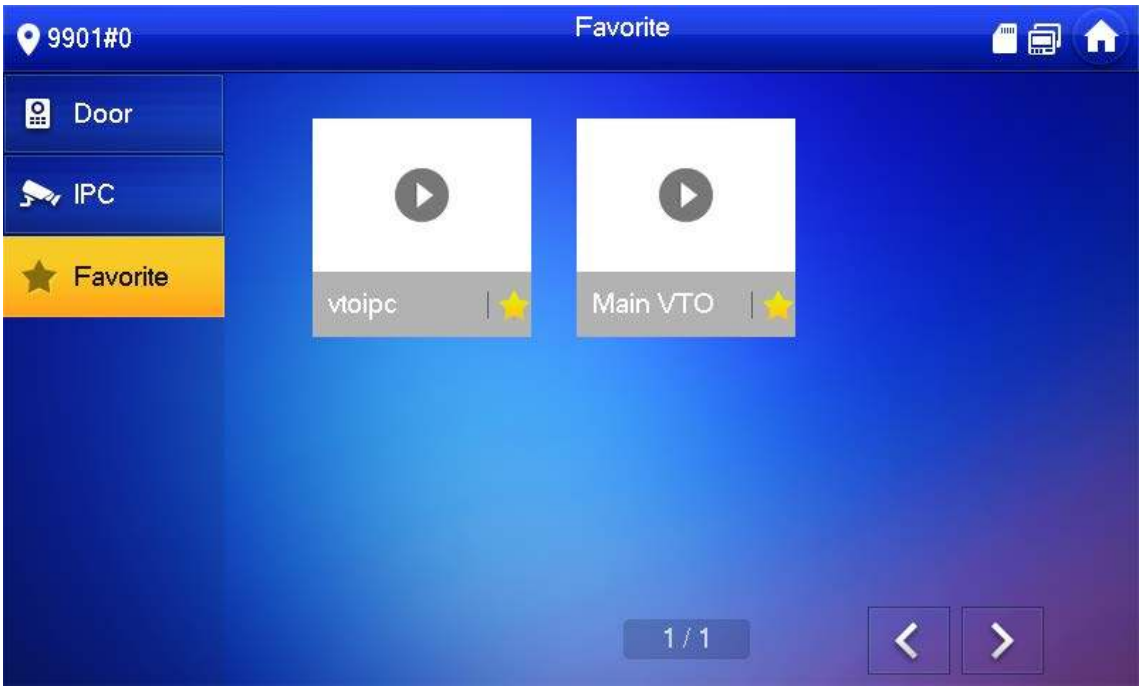
4.4.3 Favorite

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.

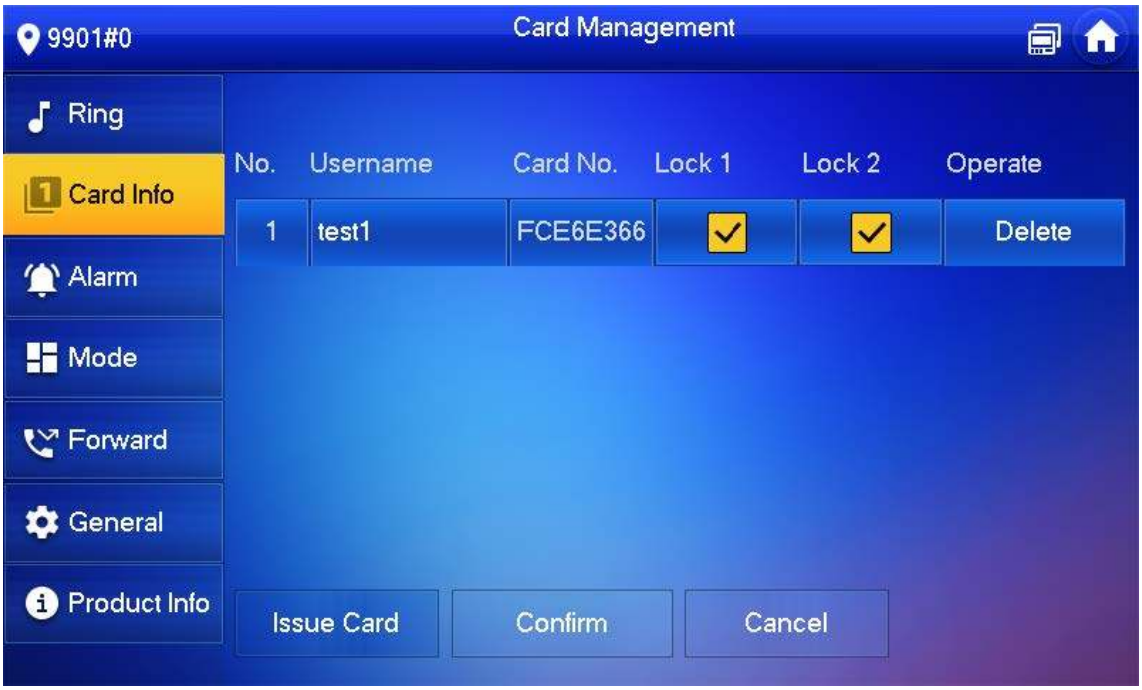
- VTO ring time: ring time when a VTO calls this VTH.
- VTH ring time: ring time when another VTH calls this VTH.

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.

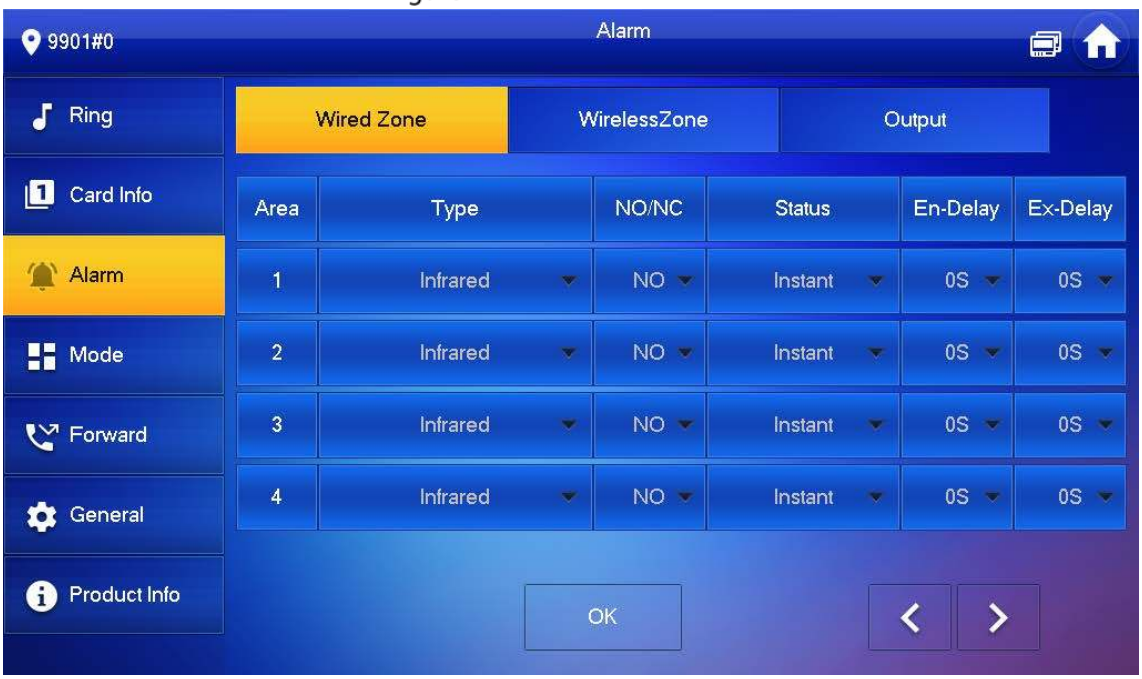
Step 1 Tap Setting.

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	• **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. A zone in **Remove** status cannot be bypassed.	
Enter Delay	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.	Delay is only valid to the areas of **Delay Alarm**.
Exit Delay	After arm, **Delay Alarm** area will enter arm status at the end of **Exit Delay**. If multiple areas set the exit delay, interface prompt will conform to maximum delay time.	

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.

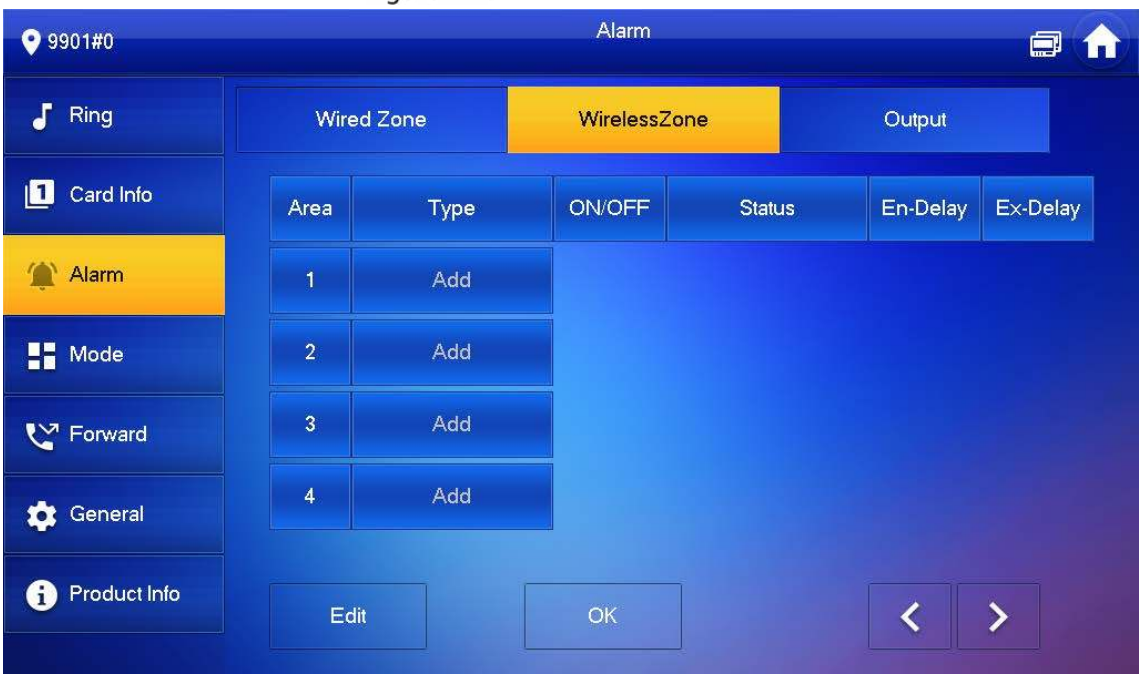
Step 1 Tap **Setting**.

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.

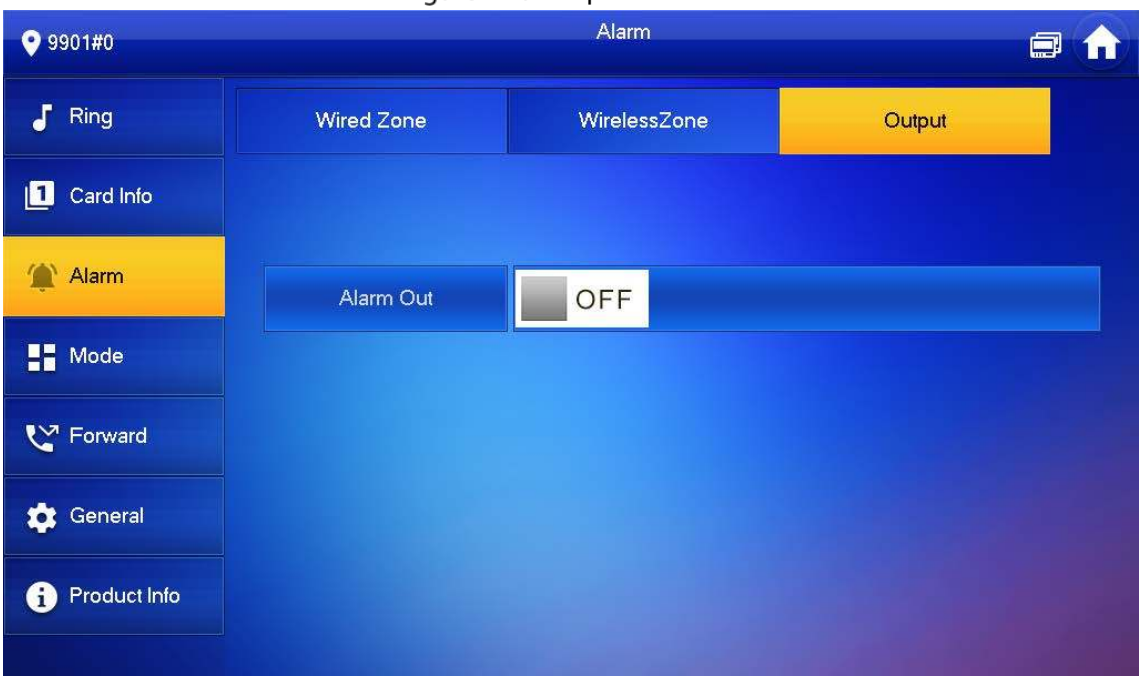
Step 1 Tap **Setting**.

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.

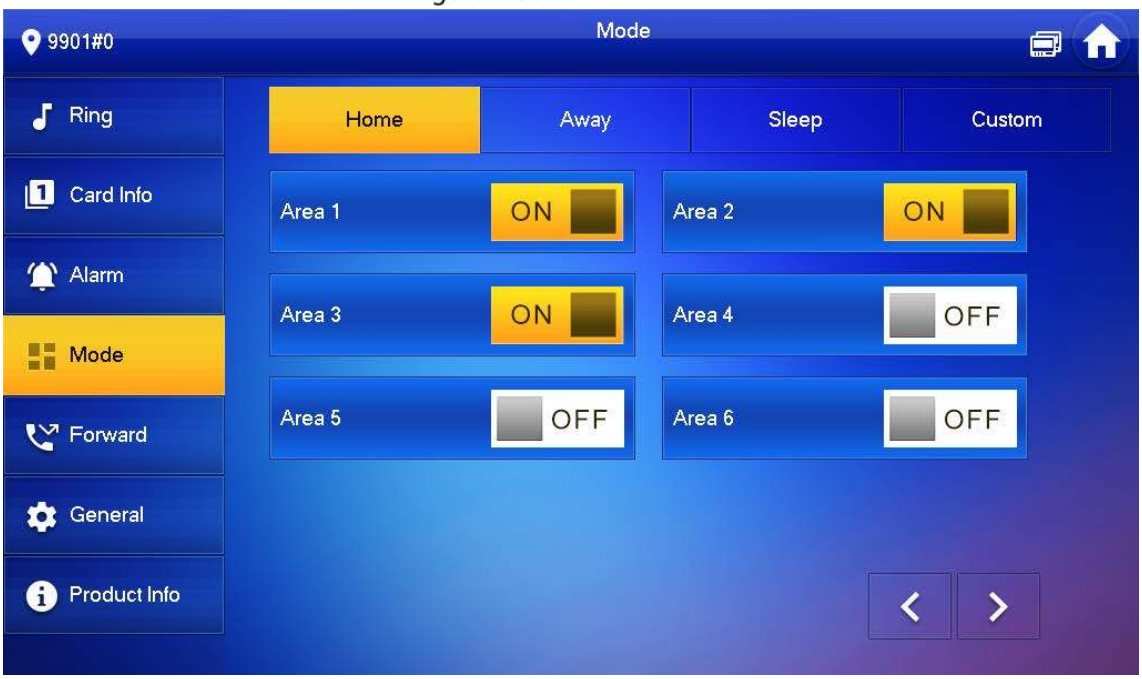
Step 1 Tap **Setting**.

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.

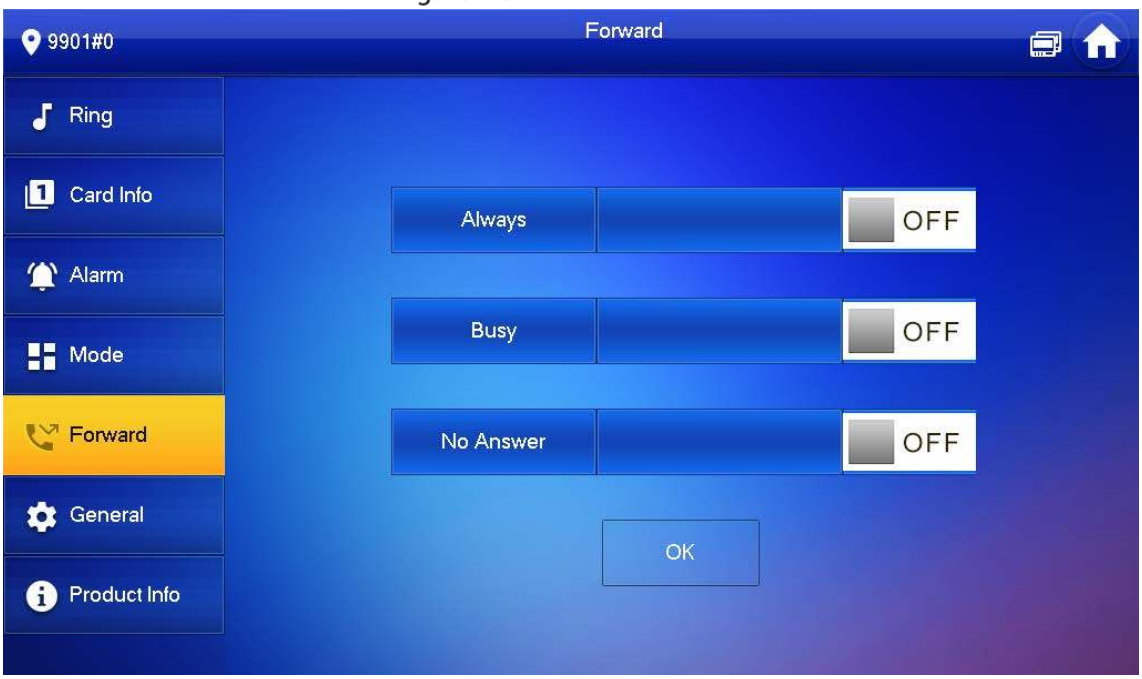
Step 1 Tap **Setting**.

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.

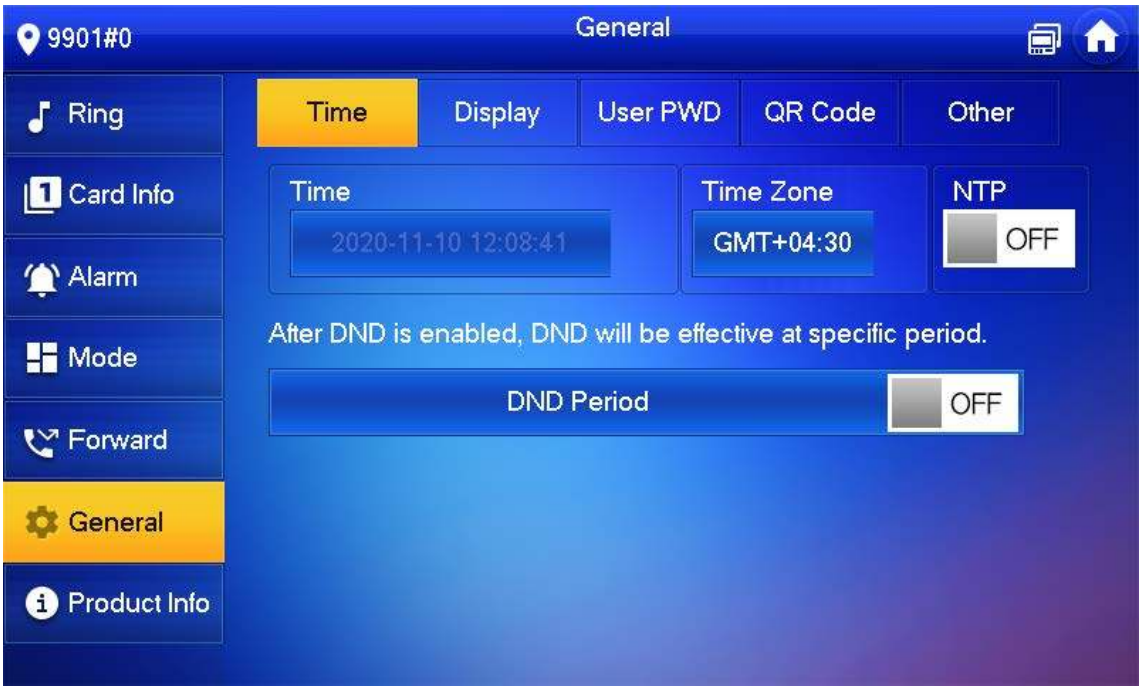
Step 1 Tap **Setting**.

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**.

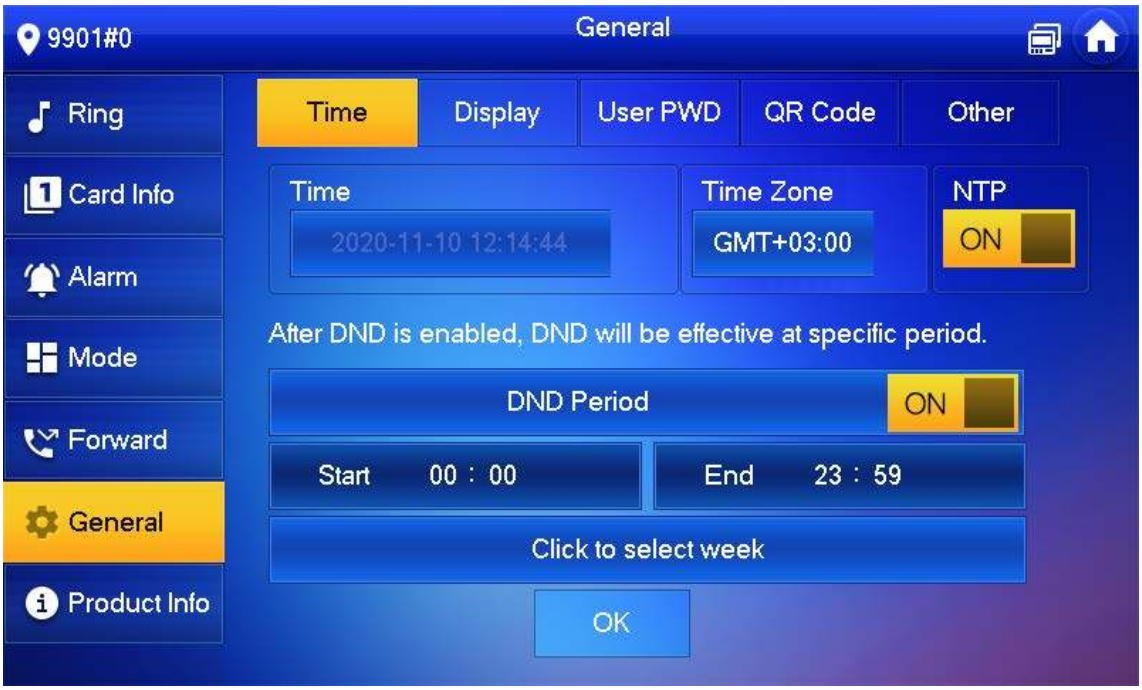
Figure 4-32 Set time and time zone



Step 4 Set time parameter.

- Turn on **NTP**, the VTH will syncronize 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.

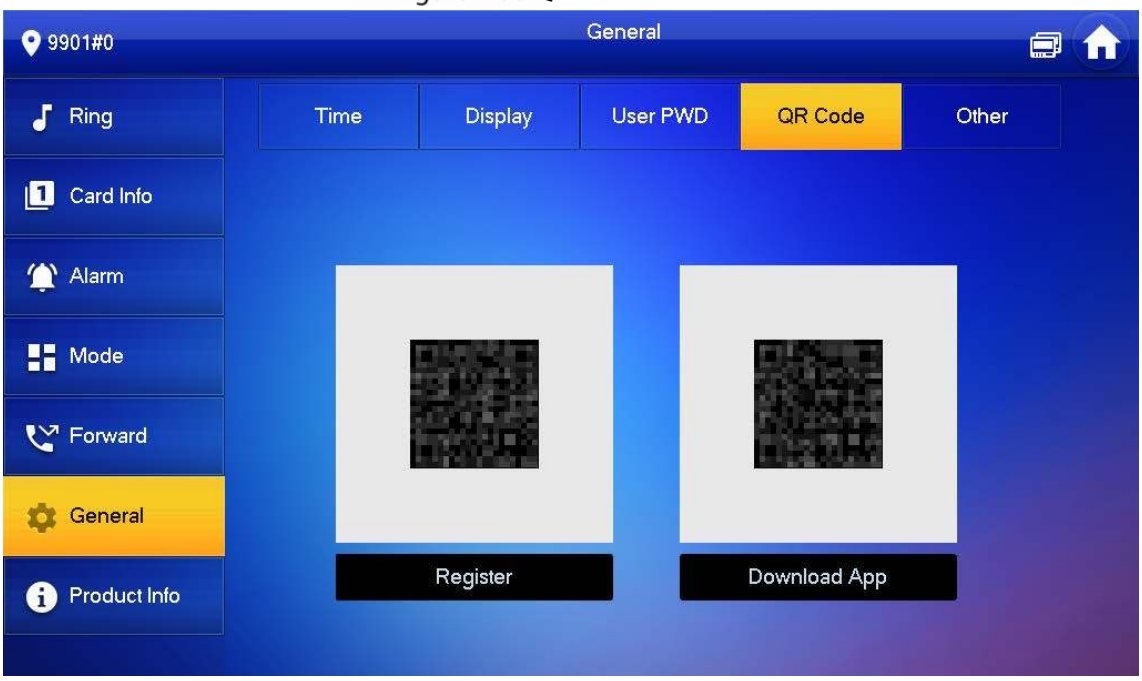
Step 1 Tap **Setting**.

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	● When **VTO Message Time(s)** is not 0: ◇ 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: In any situation, the call will be hung up automatically if the VTH does not answer the VTO. ⚠ 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.	
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	After resident-to-resident call is enabled, VTH can call another VTH. ⚠ The called party enables internal call, to realize this function.	Tap OFF to enable the function. The icon becomes ON.
Auto Capture	After enabled, 3 pictures will be captured automatically when the VTO calls the VTH. Tap **Info** > **Record and Picture** to view them. ⚠ ● 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	After enabling touch ring, there will be a ring when touching the screen.	

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

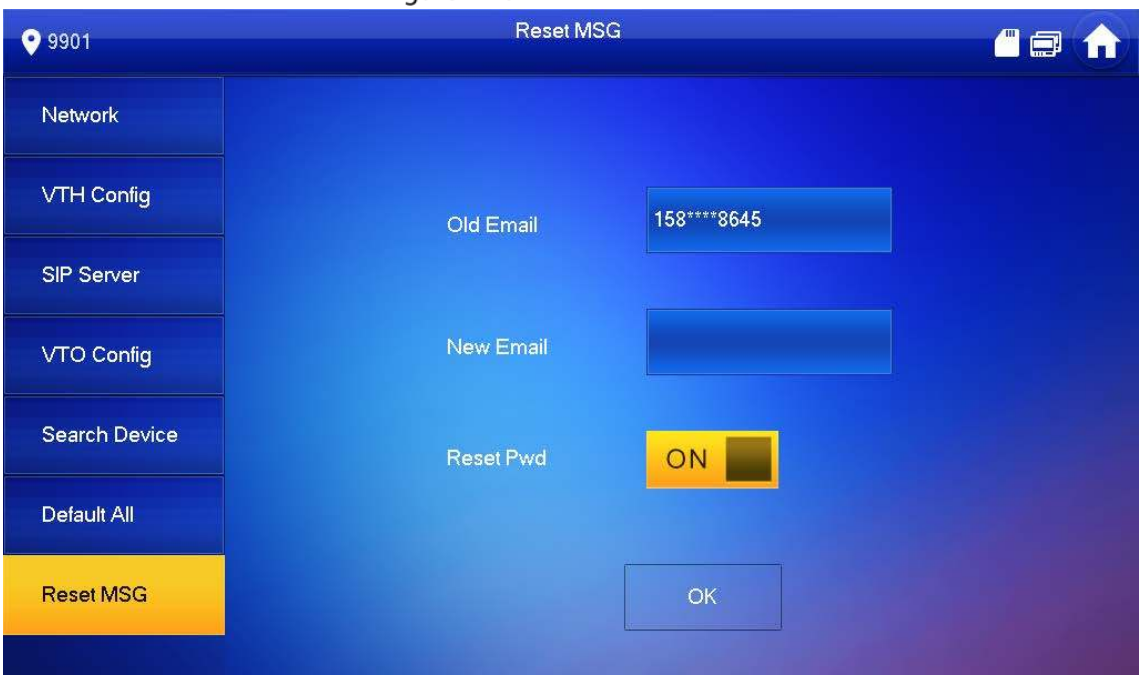
Modify the bonded Email.

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

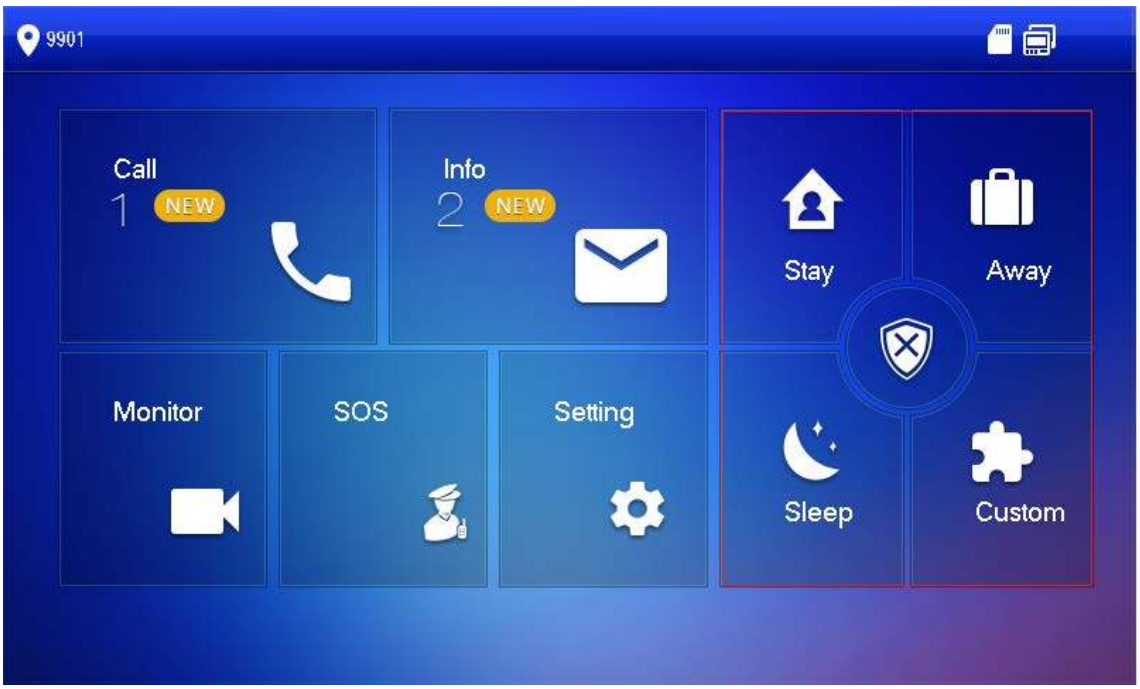
4.9.1 Arm

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.

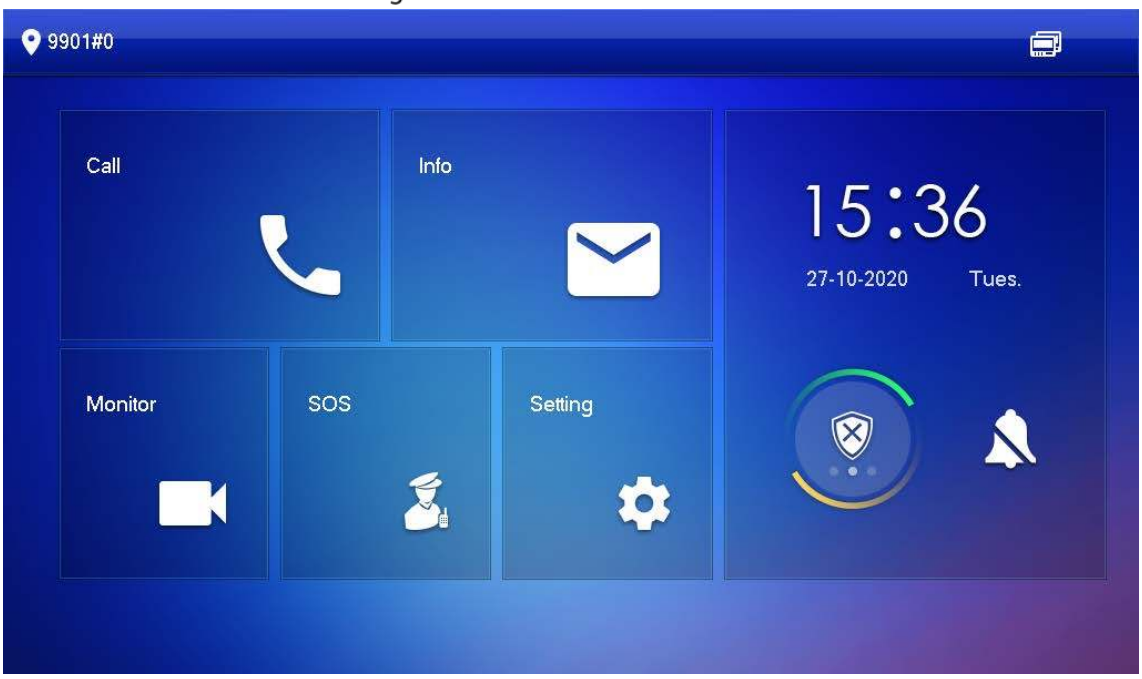
Interfaces and operations might vary between iOS and Android OS. This section takes Android OS as an example.

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**.

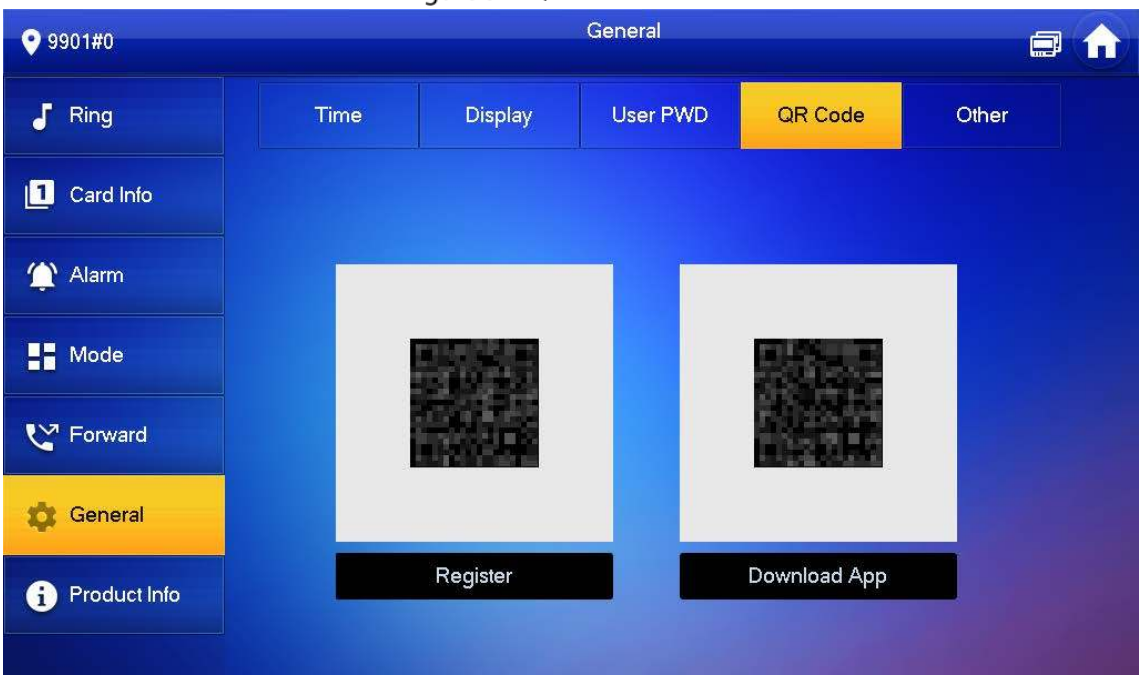
Figure 5-1 Main interface



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.

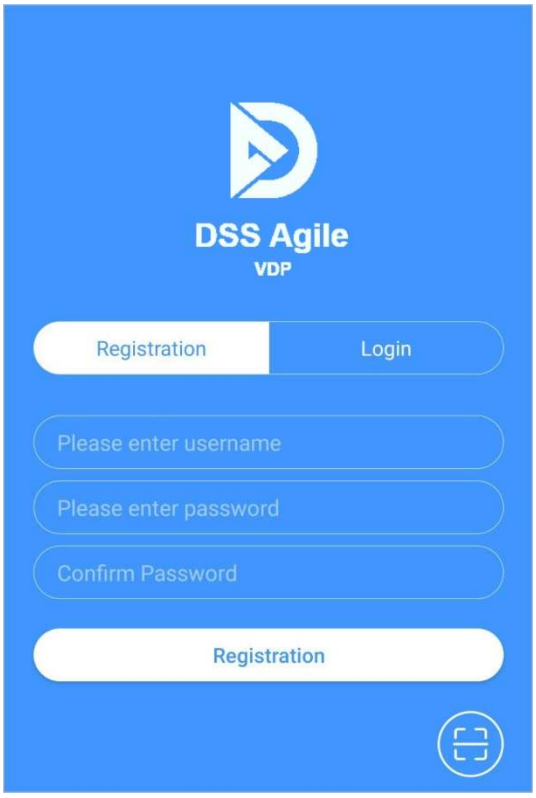
Figure 5-2 QR code



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



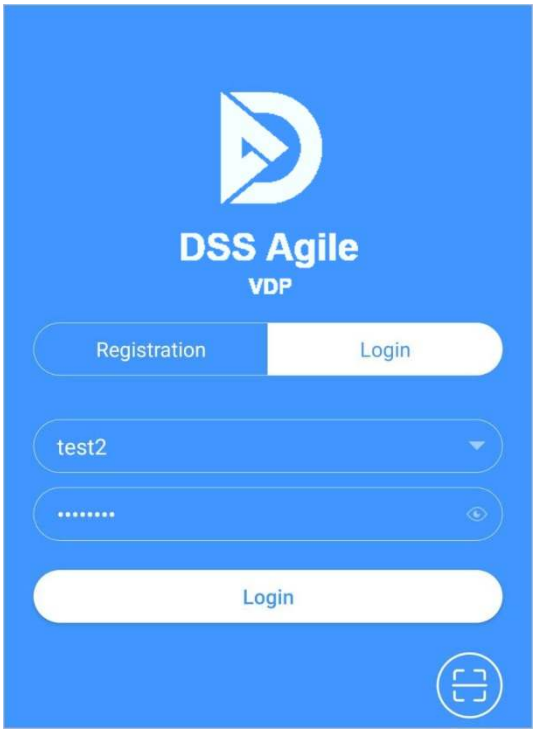
Step 2 Tap , and then scan the **Register** code on the VTH. See Step 2 in "5.1 Downloading the App".

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.

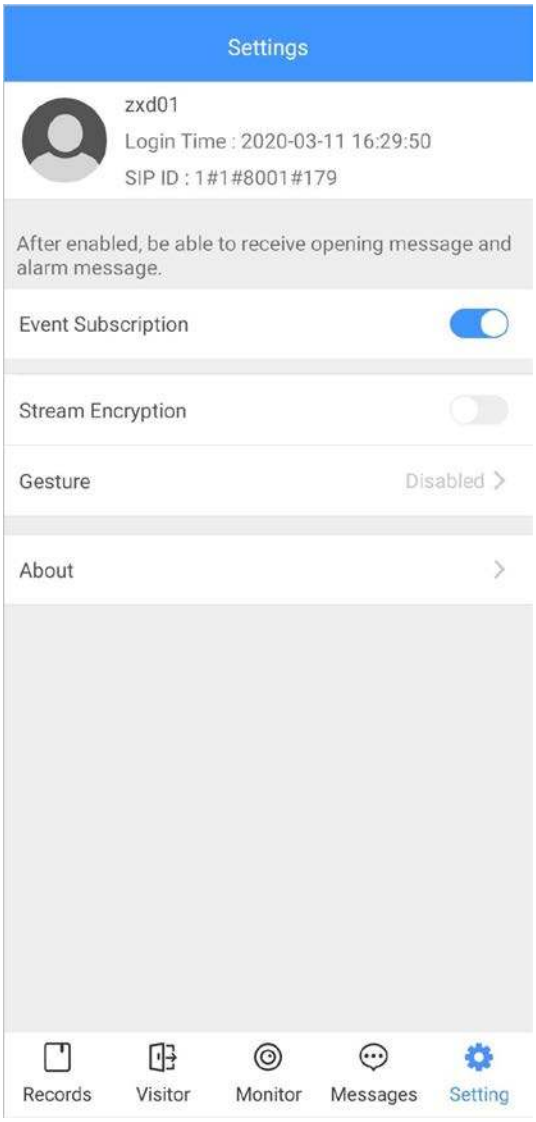
5.3.1 Forwarding Calls

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**.

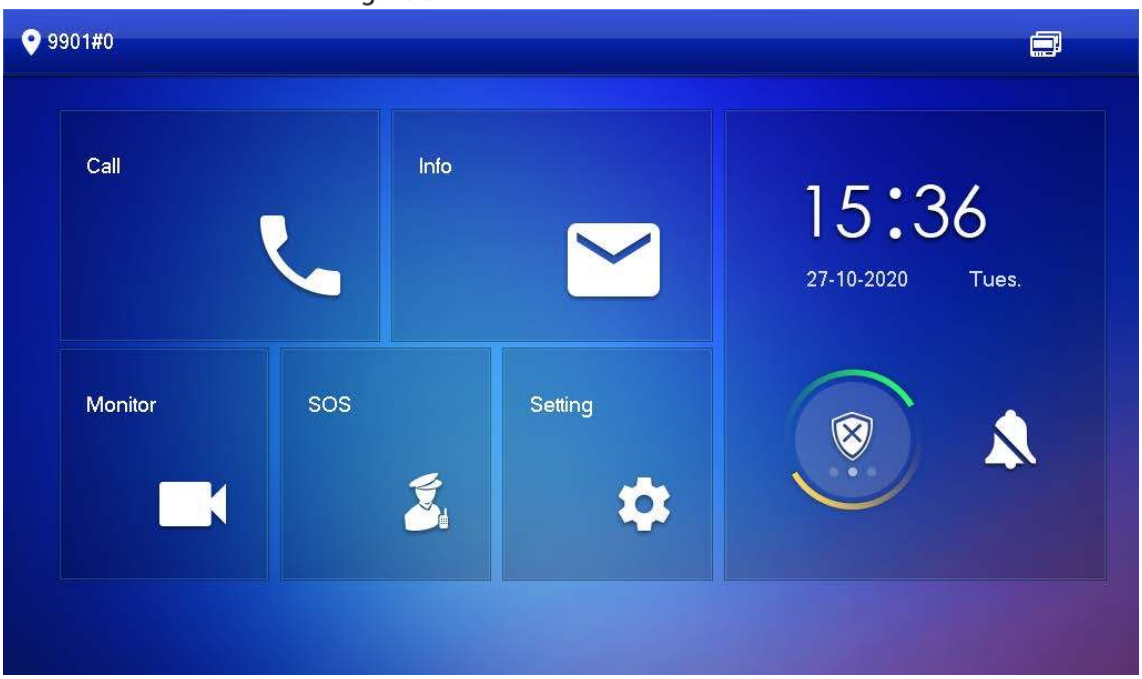
In the following example, the **SIP ID** is **1#1#8001#179**.

Figure 5-6 Settings



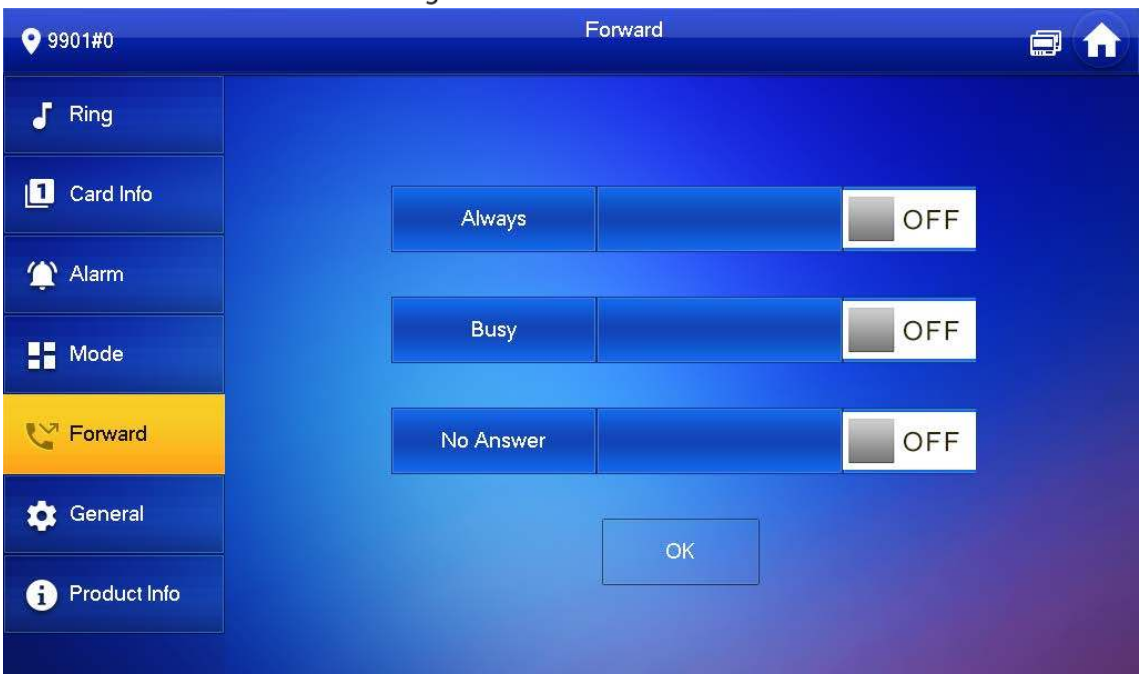
Step 2 On the VTH main interface, tap **Setting**.

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

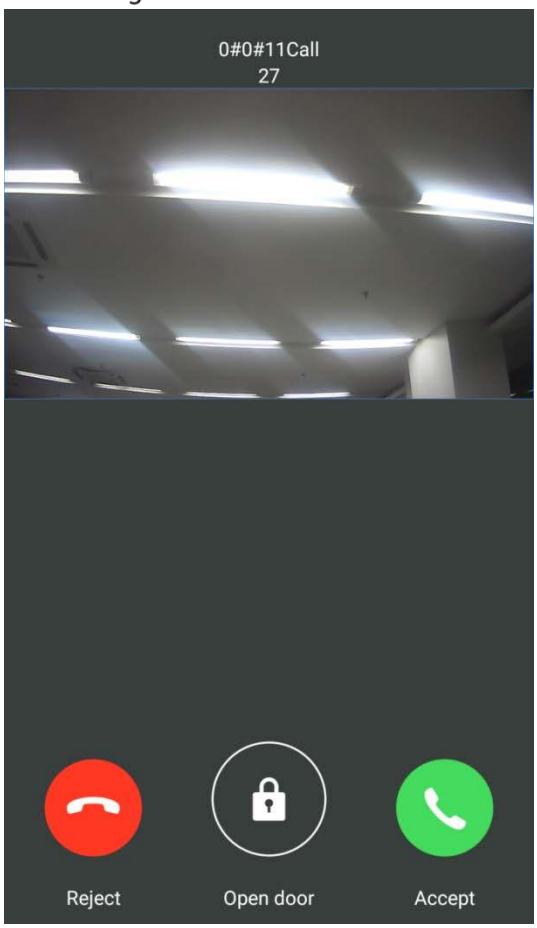
to enable the forwarding type you selected, and then tap **OK**.

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

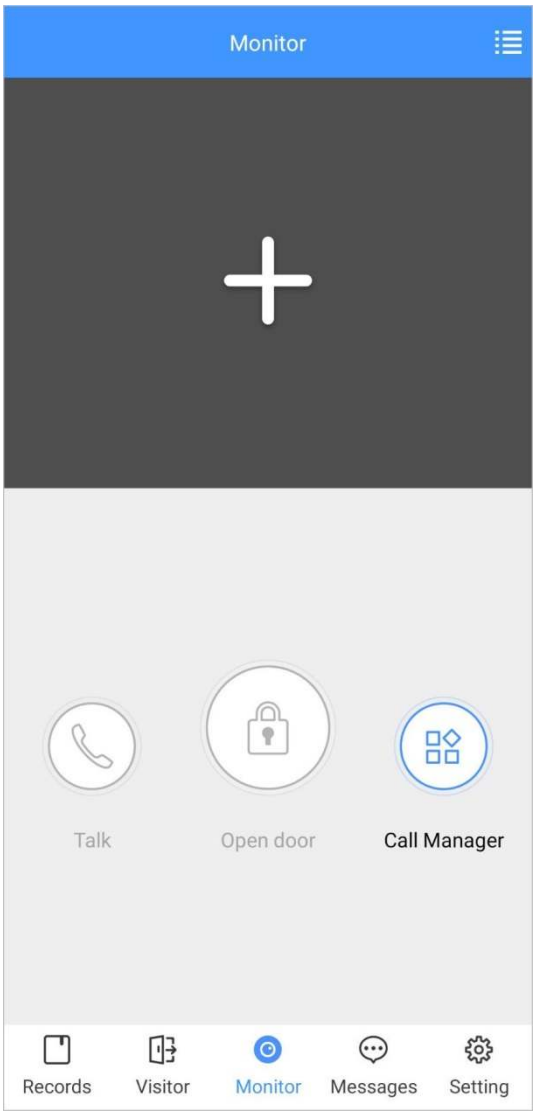


5.4 Monitoring

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

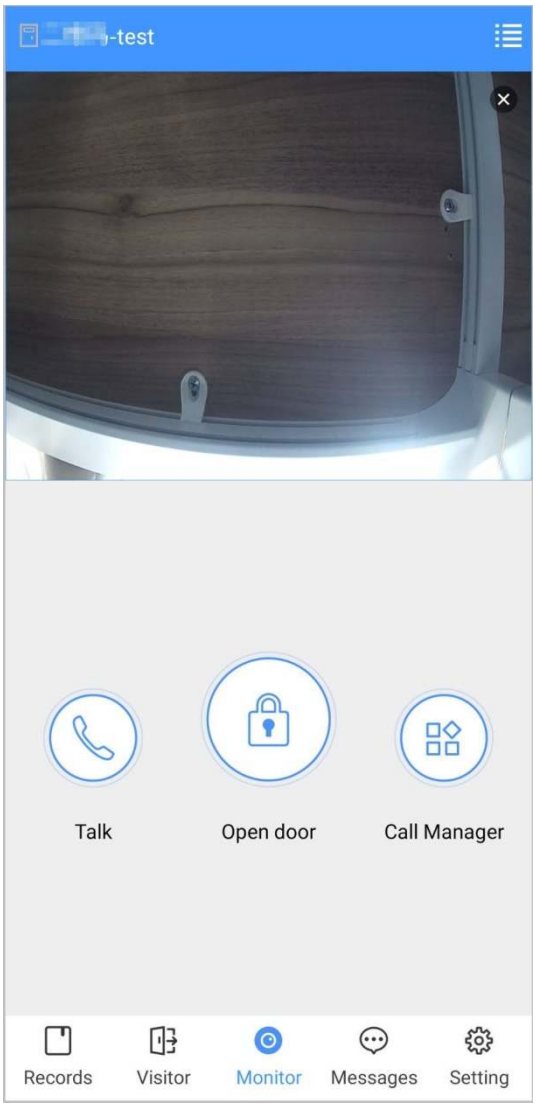
Step 1 Log in to the app, and then tap **Monitor**.

Figure 5-10 Monitor interface



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

Figure 5-11 Live video



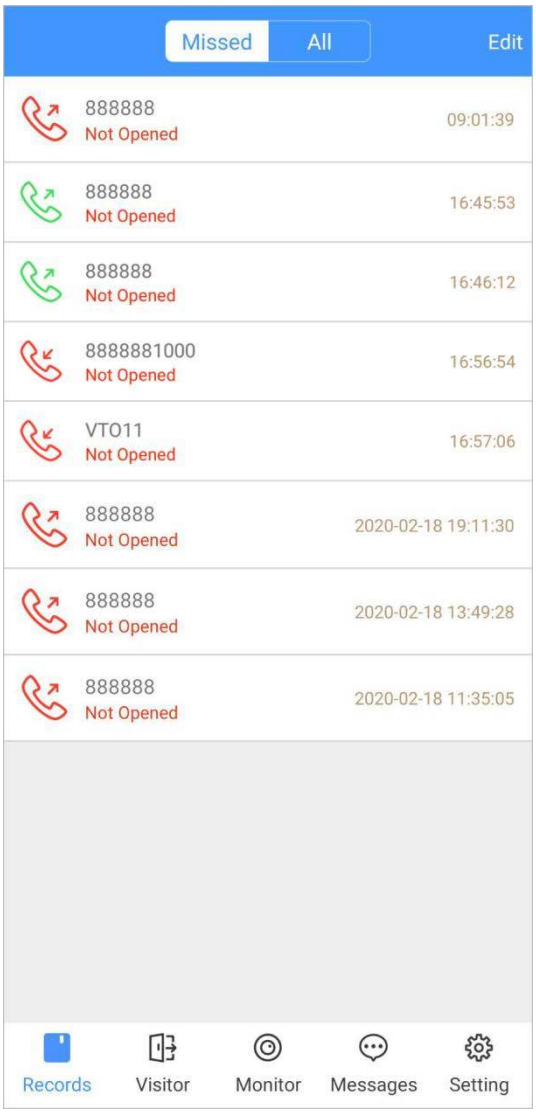
- : Switch to another VTO.
- : Unlock the door remotely.
- : Have a two-way audio talk with the VTO.
- : Call management center.

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



- 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

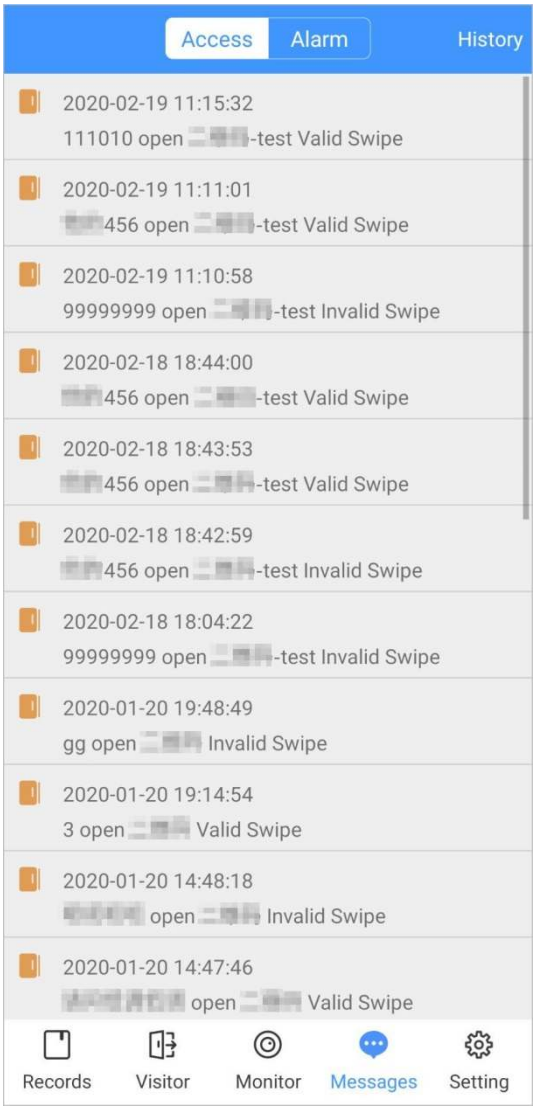
You can view the unlocking records and alarm messages, and search for history messages.

- 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

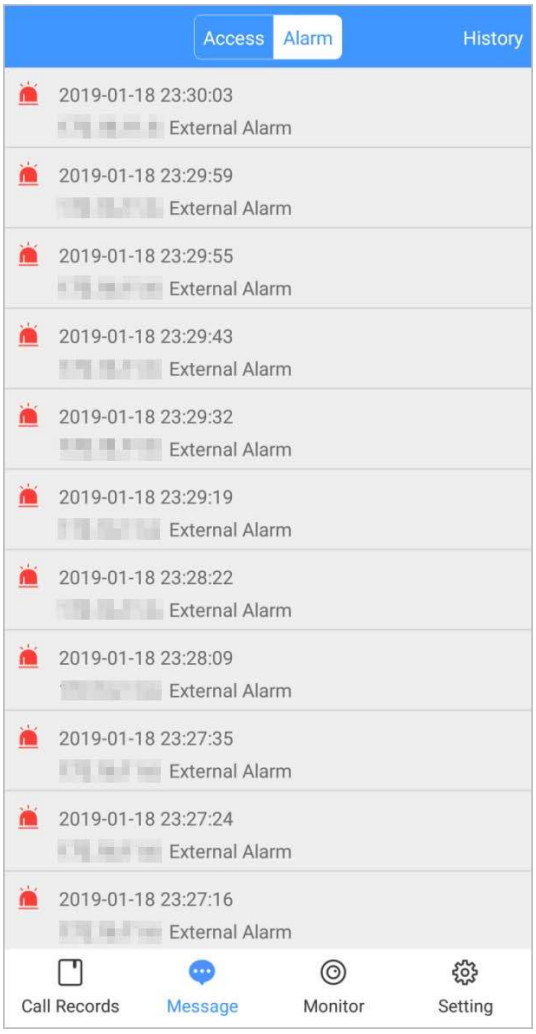
- Log in to the app, tap **Messages** > **Access**, and then you can view unlocking records, such as unlocking method, which user unlocked the door, and when the door is unlocked.

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

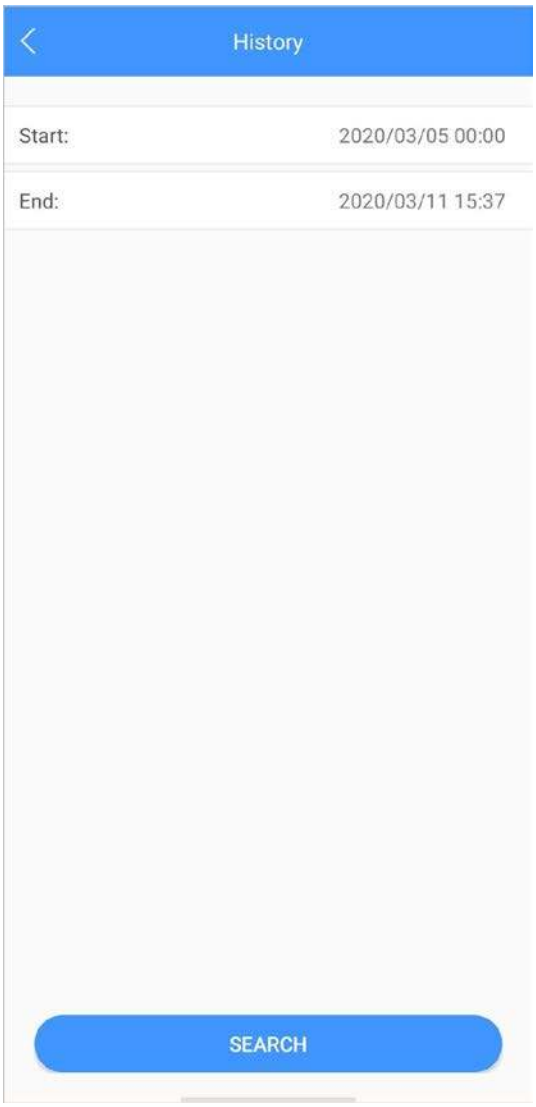


Searching for History Messages

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



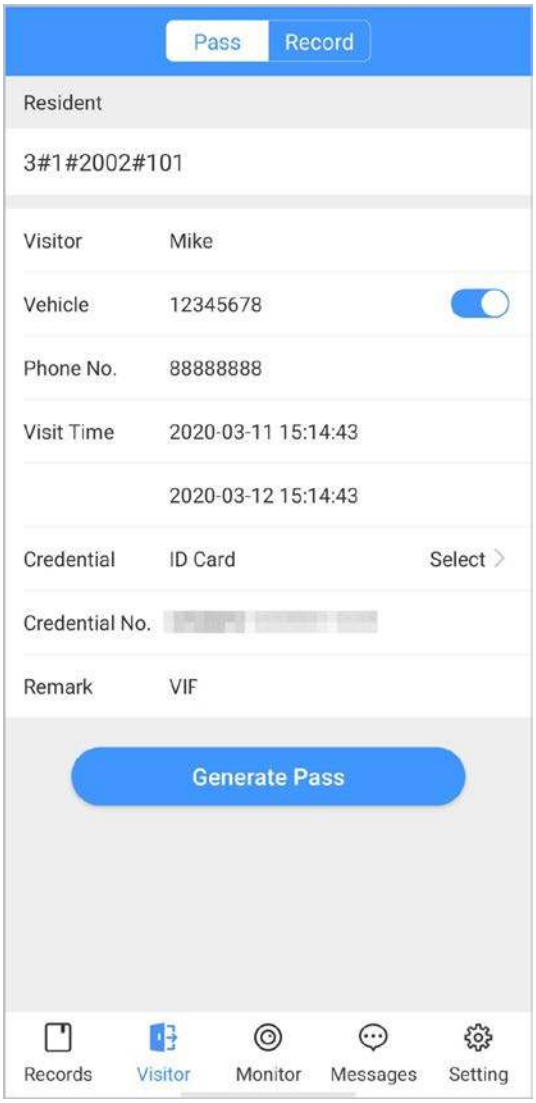
5.7 Visitor

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



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

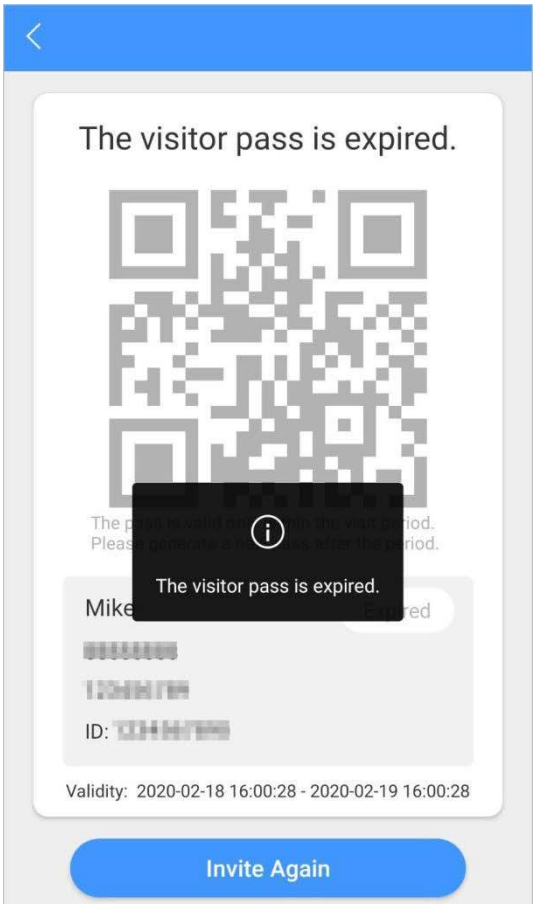
Step 3 Tap **Send to Visitor** to send the QR code to the visitor.

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

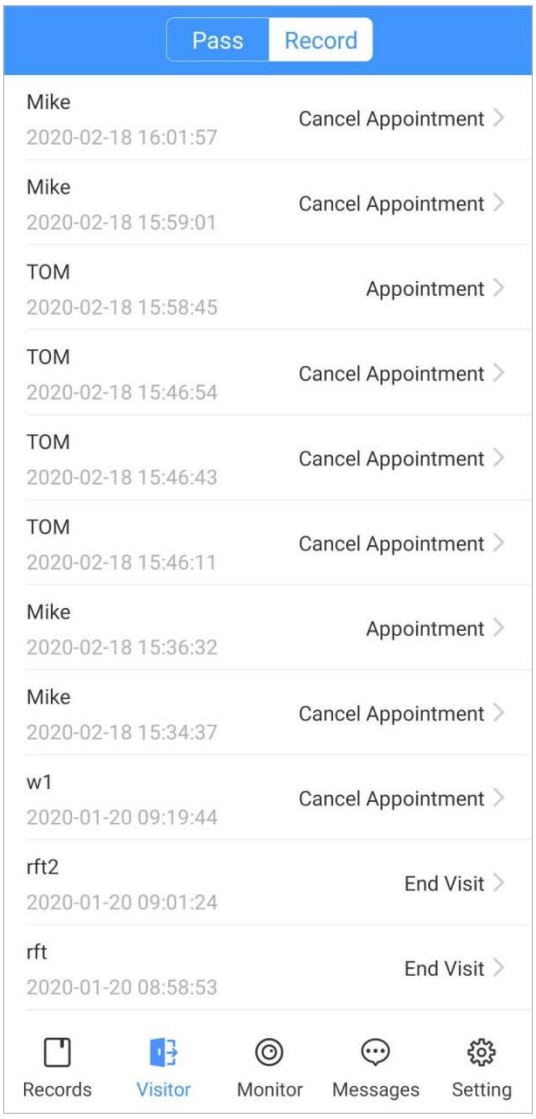


5.7.2 Visit Records

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

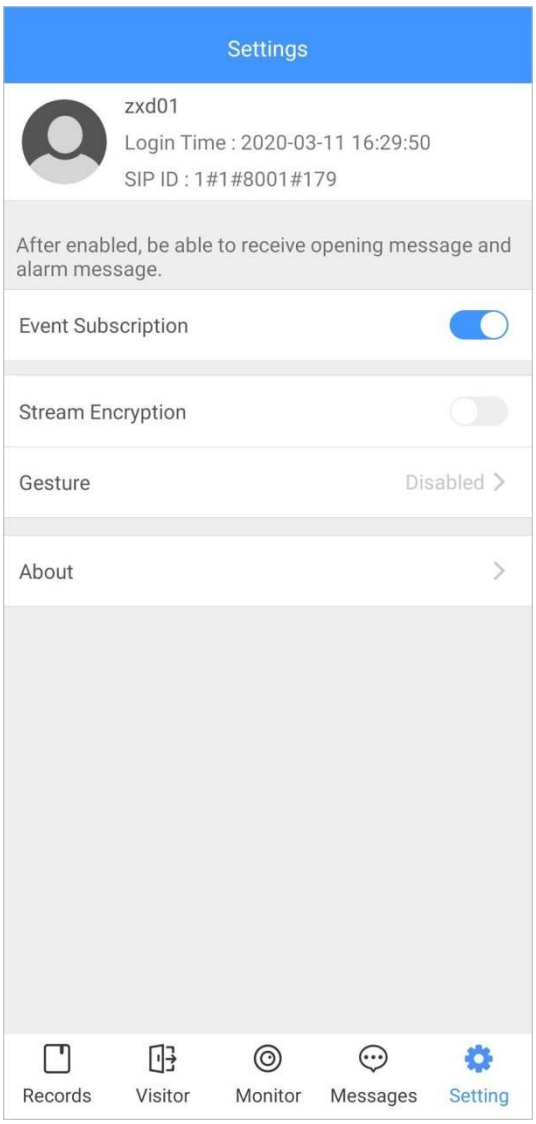


5.8 Setting

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.