Digital VTH

User's Manual

V1.2.0

Foreword

General

This document mainly introduces function, structure, networking, installation process, debugging, UI operation and technical parameter of digital VTH products matched with version 4.2 UI interface.

Models

Type	Model Series		Specific Model
Digital VTH	VTH5221 series		VTH5221DW, VTH5221D, VTH5221DW-C, VTH5221D-C, VTH5221E-H, VTH5221EW-H
	VTH5241 series		VTH5241DW
	VTH15 series	Type A	VTH1520A, VTH1520AS-H, VTH1520AH, VTH1520AS
		Type B	VTH1550B, VTH1560B(W)
		Type CH	VTH1510CH, VTH1520CH, VTH1550CH, VTH1550CHM
	VTH16 series		VTH1660CH
	VTH2X series		VTH2221A
2-wire VTH			VTH1550CHW-2, VTH5222CH

Device Upgrade

Please don’t cut off 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
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

No.	Version	Revision Content	Release Date
1	V1.0.0	First release	2017.1.15
2	V1.1.0	Add VTH5221E-H/VTH5221EW-H panel introduction	2018.5.15

No.	Version	Revision Content	Release Date
		and installation drawing.	

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

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

Power Requirement

- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification!
- Please 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.

Table of Contents

Foreword ..... **I**
Important Safeguards and Warnings ..... **III**
1 Product Overview **1**
1.1 Product Profile 1
1.2 Function 1
2 Product Structure **2**
2.1 Front Panel 2
2.1.1 VTH5221 Series /VTH5241 Series 2
2.1.2 VTH5221E-H/VTH5221EW-H 3
2.1.3 VTH15 Series Type A/B 4
2.1.4 VTH15 Series Type CH /VTH5222CH 6
2.1.5 VTH1660CH 7
2.1.6 VTH2221A 7
2.2 Rear Panel Port 8
2.2.1 VTH5221 Series /VTH5241 Series 8
2.2.2 VTH5221E-H/VTH5221EW-H 8
2.2.3 VTH15 Series Type A/Type B/Type CH 9
2.2.4 VTH5222CH/VTH5222CHW-2 9
2.2.5 VTH1660CH 10
2.2.6 VTH2221A 10
3 Network Diagram **12**
3.1 2-wire System 12
3.2 Digital System 12
4 Device Installation **15**
4.1 Installation Flow Chart 15
4.2 Open-case Inspection 15
4.3 Installation Requirement 16
4.4 Device Installation 16
4.4.1 Surface Installation 16
4.4.2 Installation with 86 Box 17
4.4.3 Desktop Installation with Bracket 17
5 Device Debugging **19**
5.1 Debugging Settings 19
5.1.1 VTO Settings 19
5.1.2 VTH Settings 27
5.2 Debugging Verification 34
5.2.1 VTO Calls VTH 34
5.2.2 VTH Monitors VTO 34
6 Interface Operation **36**
6.1 Main Interface 36
6.2 Setting 38

6.2.1 Ring Settings 38
6.2.2 DND Settings 42
6.2.3 Alarm Setting 43
6.2.4 Mode Setting 47
6.2.5 Forward Setting 48
6.2.6 General Setting 49
6.2.7 Product Info 54
6.3 Project Settings 55
6.3.1 Forget Password 55
6.3.2 Network Settings 56
6.3.3 VTH Config 58
6.3.4 VTO Config 59
6.3.5 Default 60
6.3.6 Reset MSG 60
6.4 Call 61
6.4.1 Contact 61
6.4.2 Call User 62
6.4.3 Call from User 64
6.4.4 Call from VTO 65
6.4.5 Recent Call 66
6.5 Monitor 67
6.5.1 Monitoring of VTO 67
6.5.2 Monitoring of IPC 70
6.5.3 Favorite 73
6.6 SOS 73
6.7 Info 74
6.7.1 Security Alarm 74
6.7.2 Guest Message 75
6.7.3 Publish Info 75
6.7.4 Video Pictures 76
6.8 Unlock Function 76
6.9 Arm and Disarm Function 77
6.9.1 Arm 77
6.9.2 Disarm 77
7 DSS Mobile for VDP 79
7.1 Downloading the App 79
7.2 Registration and Login 79
7.3 Call Functions 84
7.3.1 Configuring Call Forward 84
7.3.2 Calling Operations 86
7.4 Monitor 88
7.5 Call Records 90
7.6 Message 91
7.7 Setting 93
Appendix 1 Cybersecurity Recommendations 94

1 Product Overview

1.1 Product Profile

VTH series product is a digital video intercom home station for numerous homes, integrating monitoring, intercom and unlocking. With embedded technology, all IP network, SNMP (Simple Network Management Protocol) technology and network encryption technology, achieve more stable system operation, richer functional extension, more convenient system management and safer data transmission.

1.2 Function

- Wi-Fi Networking: Realize Wi-Fi networking of devices.
- Video Intercom: Call or connect VTO and VTH; realize talk.
- Monitoring: Monitor fence station, VTO and IPC devices.
- SOS: Press the key to call the Call Center in case of an emergency.
- Auto Snapshot: Snapshot the call picture or monitoring picture, and store them in SD card or FTP.
- DND (Do Not Disturb): Avoid other's incoming call interference.
- Remote Unlock: Realize remote unlock.
- Arm and Disarm: Provide 6-channel area setting, arm and disarm them.
- Playback: Play back videos and pictures in SD card of this device.
- Alarm: After 6-channel area triggers an alarm, pop up an alarm prompt interface, provide linkage alarm output and report to Call Center.
- Record Inquiry: Inquire call records and alarm records.
- Message Inquiry: Inquire guests' message, videos, pictures and announcements issued by Property Management Center.

2 Product Structure

2.1 Front Panel

2.1.1 VTH5221 Series /VTH5241 Series

VTH5221D is a 7″ digital indoor monitor. Their front panels have the same size, as shown in Figure 2-1. Please refer to Table 2-1 for details.

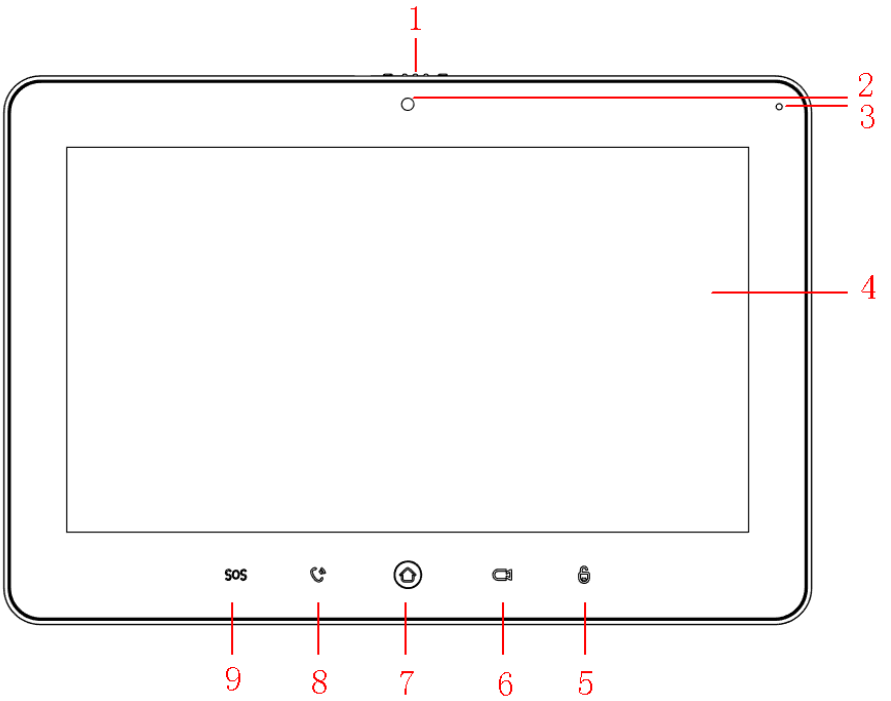


Figure 2-1

No.	Name	Description
1	Camera occlusion switch	Slide it to occlude or open the camera.
2	Camera	Only VTH5221DW-C supports front-facing camera.
3	Microphone	Voice input.
4	Display screen	● 7″ type D digital VTH owns a 7″ high-definition LCD. ● 10″ type D digital VTH owns a 10″ high-definition LCD.
5	Unlock	Press this key during calling, talking, monitoring and speaking of VTO, so corresponding VTO will be unlocked.
6	Monitor	● In standby mode, press this key to monitor the main VTO. ● During monitoring, press this key to exit monitoring.
7	Menu	Press this key to return to main menu.
8	Call	● In case of incoming call, press this key to answer the call. ● During talk, press this key to hang up. ● During monitoring, press this key to speak to unit VTO, villa

No.	Name	Description
		VTO and fence station. ● During speaking, press this key to exit speaking.
9	SOS	Press this key to call the Call Center in case of emergency.

Table 2-1

2.1.2 VTH5221E-H/VTH5221EW-H

VTH5221E-H/VTH5221EW-H is two types of digital VTH with handset. They are the same except appearance color, as shown in Figure 2-2 and Figure 2-3.

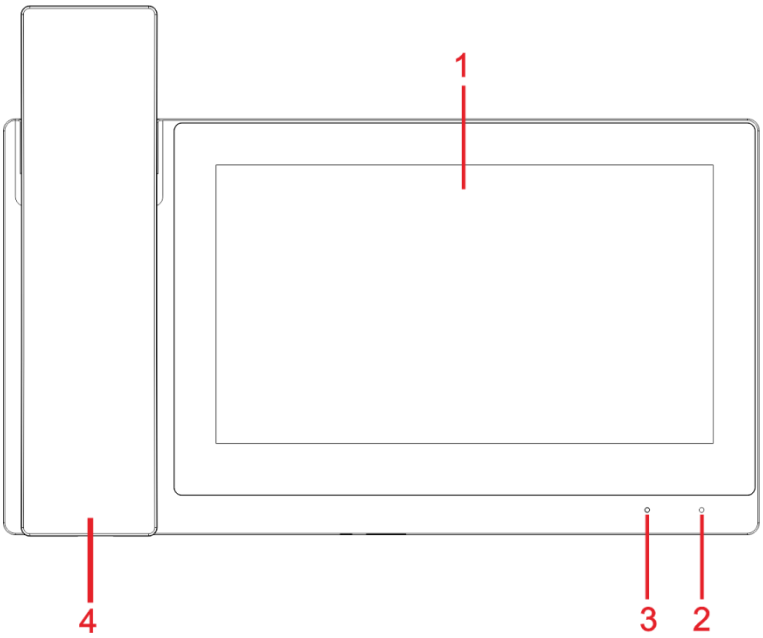


Figure 2-2

No.	Name	Description
1	Display screen	7″ high-definition LCD.
2	Microphone	Voice input.
3	Indicator	The indicator light is normally on after power-on.
4	Handset	Pick up the handset, and dial pad will be displayed.

Table 2-2

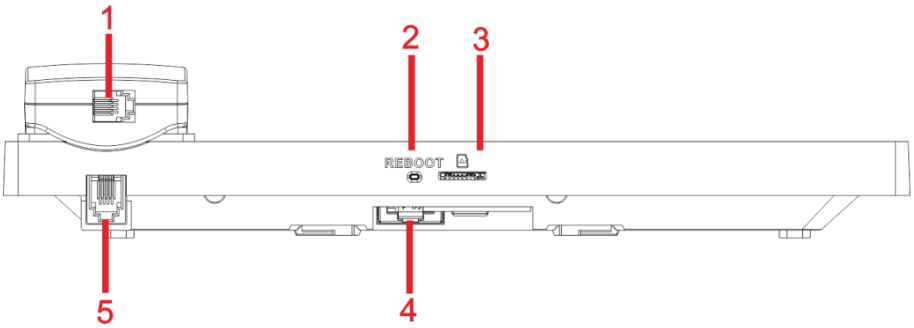


Figure 2-3

No.	Name	Description
1	RJ11 port	Port of connecting cable between handset and VTH.
2	Reboot button	Long press the button to reboot VTH.

No.	Name	Description
3	TF card slot	TF card slot, max. 64GB.
4	RJ45 port	RJ45 network cable port.
5	RJ11 port	Port of connecting cable between handset and VTH.

Table 2-3

2.1.3 VTH15 Series Type A/B

In VTH15 series, different types of devices have different front panels.

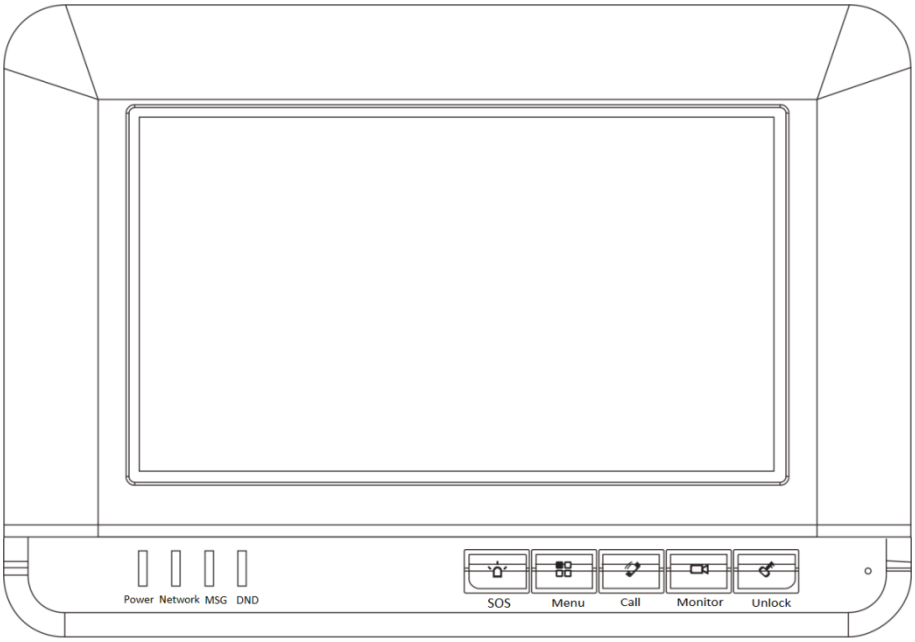


Figure 2-4 VTH15 Series Type A

Icon	Name	Description
SOS	SOS	Press this key to call the Call Center in case of emergency.
Menu	Menu	Press this key to return to main menu.
Call	Call	● In case of incoming call, press this key to answer the call. ● During talk, press this key to hang up. ● During monitoring, press this key to speak to apartment VTO, villa VTO and fence station. ● During speaking, press this key to exit speaking.
Monitor	Monitor	● In standby mode, press this key to monitor the main VTO. ● During monitoring, press this key to exit monitoring.
Unlock	Unlock	Press this key during calling, talking, monitoring and speaking of VTO, so corresponding VTO will be unlocked.
Power	Power indicator	If this indicator turns on in green, it represents normal power supply.

Icon	Name	Description
Network	Network indicator	● If this indicator turns on, it represents normal communication with VTO. ● If this indicator turns off, it represents abnormal communication with VTO.
MSG	Message indicator	If this indicator turns on, it represents that there are unread messages.
DND	DND indicator	If this indicator turns on in green, it represents that DND function is enabled. For DND settings, please refer to “6.2.2 DND Settings“.

Table 2-4

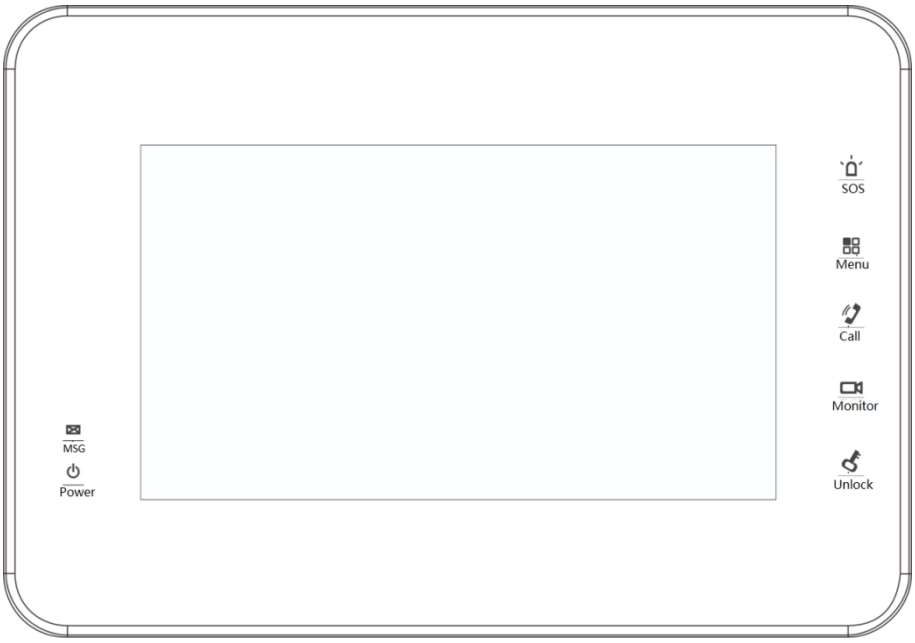


Figure 2-5 VTH15 Series Type B

Icon	Name	Description
SOS	SOS	Press this key to call the Call Center in case of emergency.
Menu	Menu	Press this key to return to main menu.
Call	Call	● In case of incoming call, press this key to answer the call. ● During talk, press this key to hang up. ● During monitoring, press this key to speak to apartment VTO, villa VTO and fence station. ● During speaking, press this key to exit speaking.
Monitor	Monitor	● In standby mode, press this key to monitor the main VTO. ● During monitoring, press this key to exit monitoring.

Icon	Name	Description
Unlock	Unlock	Press this key during calling, talking, monitoring and speaking of VTO, so corresponding VTO will be unlocked.
MSG	Message indicator	If this indicator turns on, it represents that there are unread messages.
Power	Power indicator	If this indicator turns on in green, it represents normal power supply.

Table 2-5

2.1.4 VTH15 Series Type CH /VTH5222CH

Figure 2-6

Icon	Name	Description
	SOS	Press this key to call the Call Center in case of emergency.
	Menu	Press this key to return to main menu.
	Call	• In case of incoming call, press this key to answer the call. • During talk, press this key to hang up. • During monitoring, press this key to speak to apartment VTO, villa VTO and fence station. • During speaking, press this key to exit speaking.
	Monitor	• In standby mode, press this key to monitor the main VTO. • During monitoring, press this key to exit monitoring.
	Unlock	Press this key during calling, talking, monitoring and speaking of VTO, so corresponding VTO will be unlocked.

Table 2-6

2.1.5 VTH1660CH

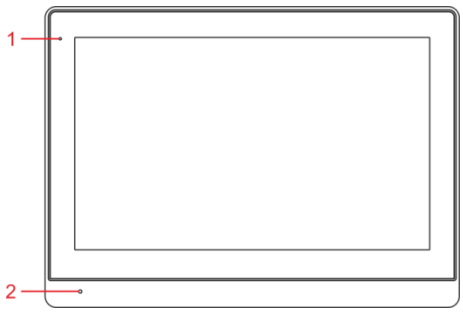


Figure 2-7

No.	Name	Description
1	Power indicator	If this indicator turns on in green, it represents normal power supply.
2	Microphone	Audio input.

Table 2-7

2.1.6 VTH2221A

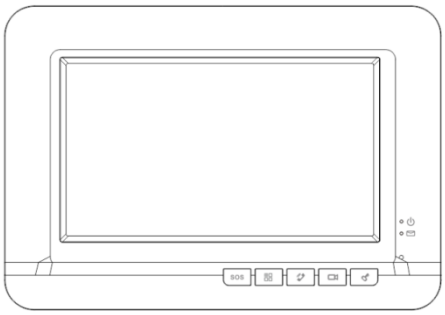


Figure 2-8

Icon	Name	Description
SOS	SOS	Press this key to call the Call Center in case of emergency.
	Menu	Press this key to return to main menu.
	Call	● In case of incoming call, press this key to answer the call. ● During talk, press this key to hang up. ● During monitoring, press this key to speak to apartment VTO, villa VTO and fence station. ● During speaking, press this key to exit speaking.
	Monitor	● In standby mode, press this key to monitor the main VTO. ● During monitoring, press this key to exit monitoring.
	Unlock	Press this key during calling, talking, monitoring and speaking of VTO, so corresponding VTO will be unlocked.
	Power indicator	If this indicator turns on in green, it represents normal power supply.
	Message indicator	If this indicator turns on, it represents that there are unread messages.

Table 2-8

2.2 Rear Panel Port

2.2.1 VTH5221 Series /VTH5241 Series

Port positions are slightly different on the rear panel of VTH5221 series and VTH5241 series, but the same port owns the same function. Taking VTH5221 as an example, specific functions of ports are introduced, as shown in Figure 2-9.

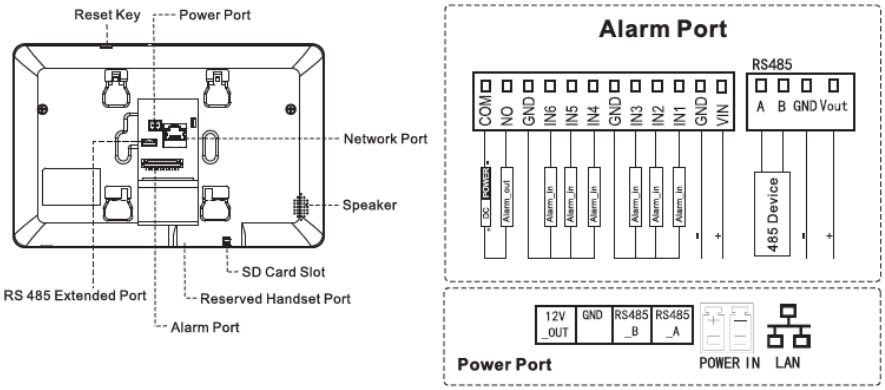


Figure 2-9

2.2.2 VTH5221E-H/VTH5221EW-H

Port positions are slightly different on the rear panel, but the same port owns the same function. VTH5221E-H/VTH5221EW-H front panels are shown in Figure 2-10.

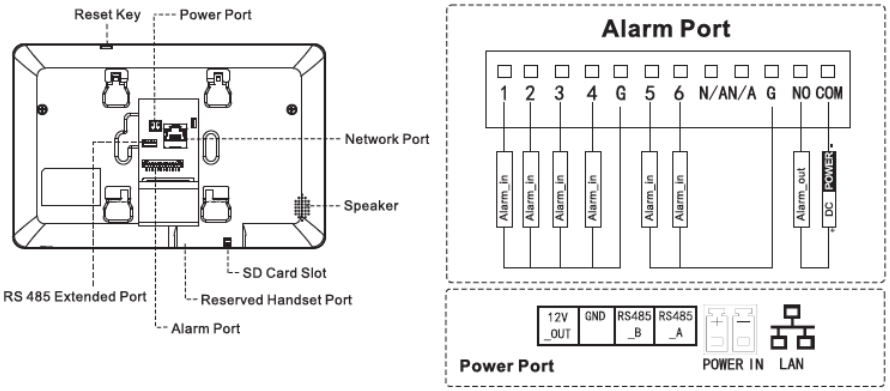


Figure 2-10

2.2.3 VTH15 Series Type A/Type B/Type CH

In VTH15 series, different types of digital VTH have different port positions, but the same port provides the same function. Taking VTH1550CH as an example, specific functions of ports are introduced, as shown in Figure 2-12.

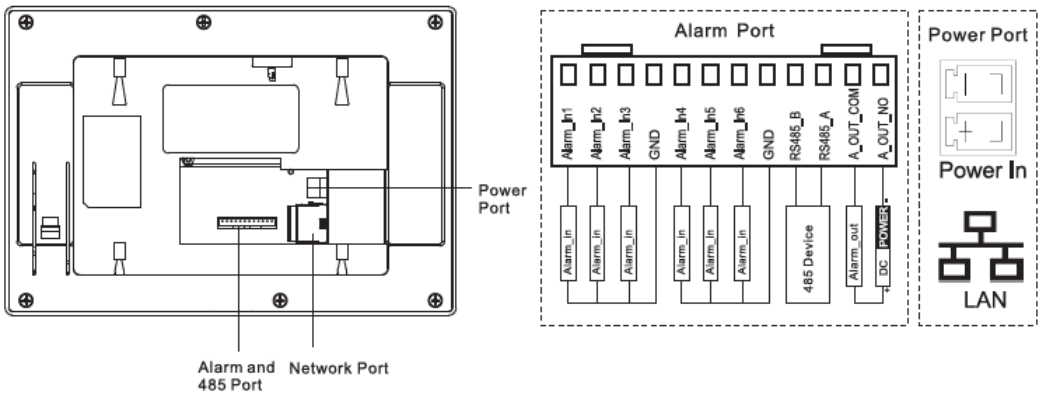


Figure 2-11

In VTH15 type A/type B series, different types of digital VTH have different port positions, but the same port provides the same function. Taking VTH1560B as an example, specific functions of ports are introduced, as shown in Figure 2-12.

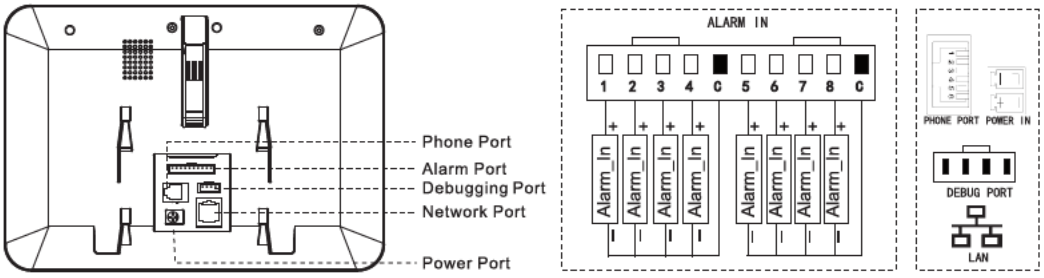


Figure 2-12

2.2.4 VTH5222CH/VTH5222CHW-2

Except different numbers of 2-wire port, VTH5222CH and VTH5222CHW-2 are the same in other aspects. VTH5222CH has 1 group of 2-wire port, while VTH1550CHW-2 has 3 groups of 2-wire port. VTH5222CH provides 6-ch alarm input ports, 1-ch alarm output port, 1-ch RS485 port and 1 group of 2-wire port, as shown in Figure 2-13.

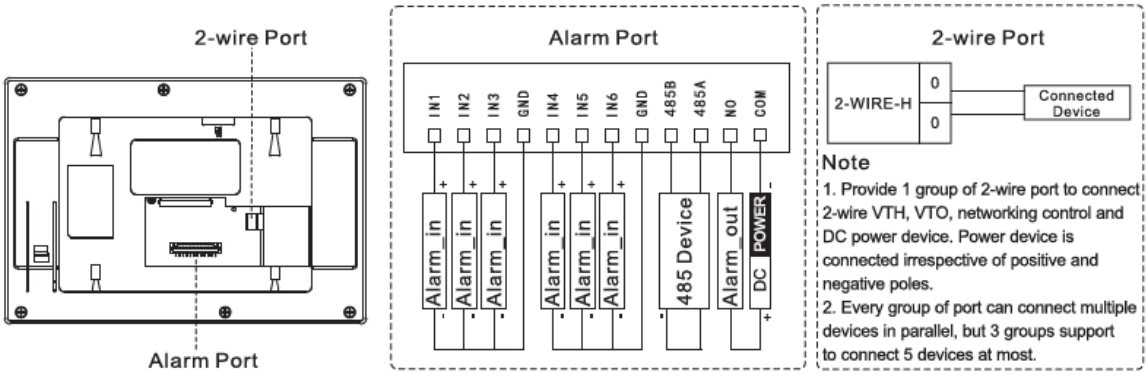


Figure 2-13

2.2.5 VTH1660CH

VTH1660CH provides 6-ch alarm input ports, 1-ch RS485 port, 1-ch debugging port, 1-ch network port and power port, as shown in

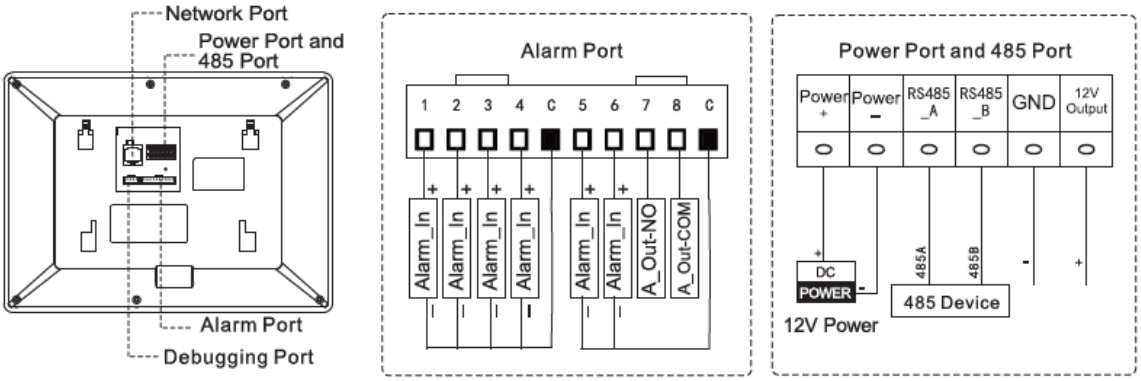


Figure 2-14.

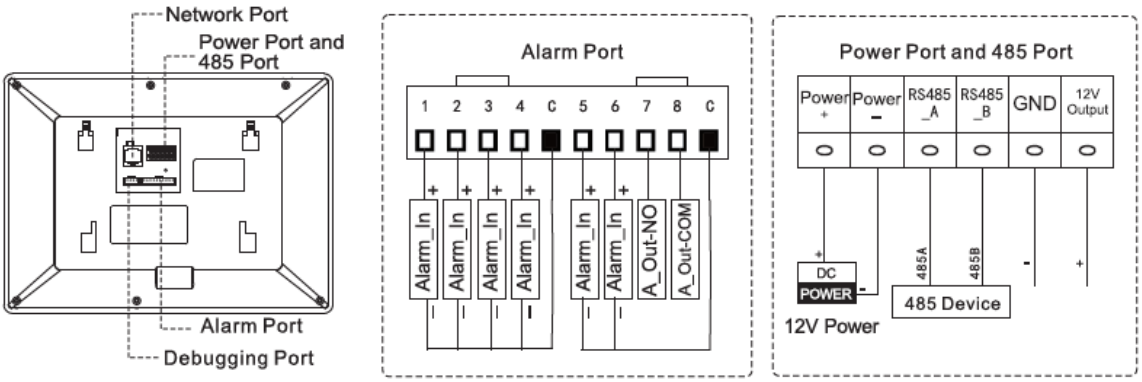


Figure 2-15

2.2.6 VTH2221A

VTH2221A provides 8-ch alarm input ports, 1-ch network port and power port, as shown in Figure 2-16.

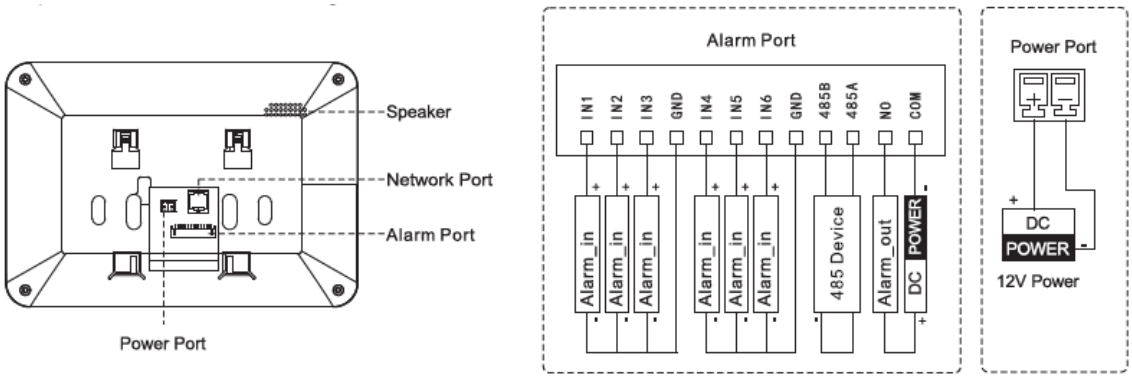

Speaker
Network Port
Alarm Port
Power Port
Alarm Port
IN1
IN2
IN3
GND
IN4
IN5
IN6
GND
485B
485A
NO
COM
Alarm_in
Alarm_in
Alarm_in
Alarm_in
Alarm_in
Alarm_in
485 Device
Alarm_out
DC
POWER
Power Port
DC
POWER
12V Power

Figure 2-16

3 Network Diagram

3.1 2-wire System

Network diagram of 2-wire system is shown in Figure 3-1.

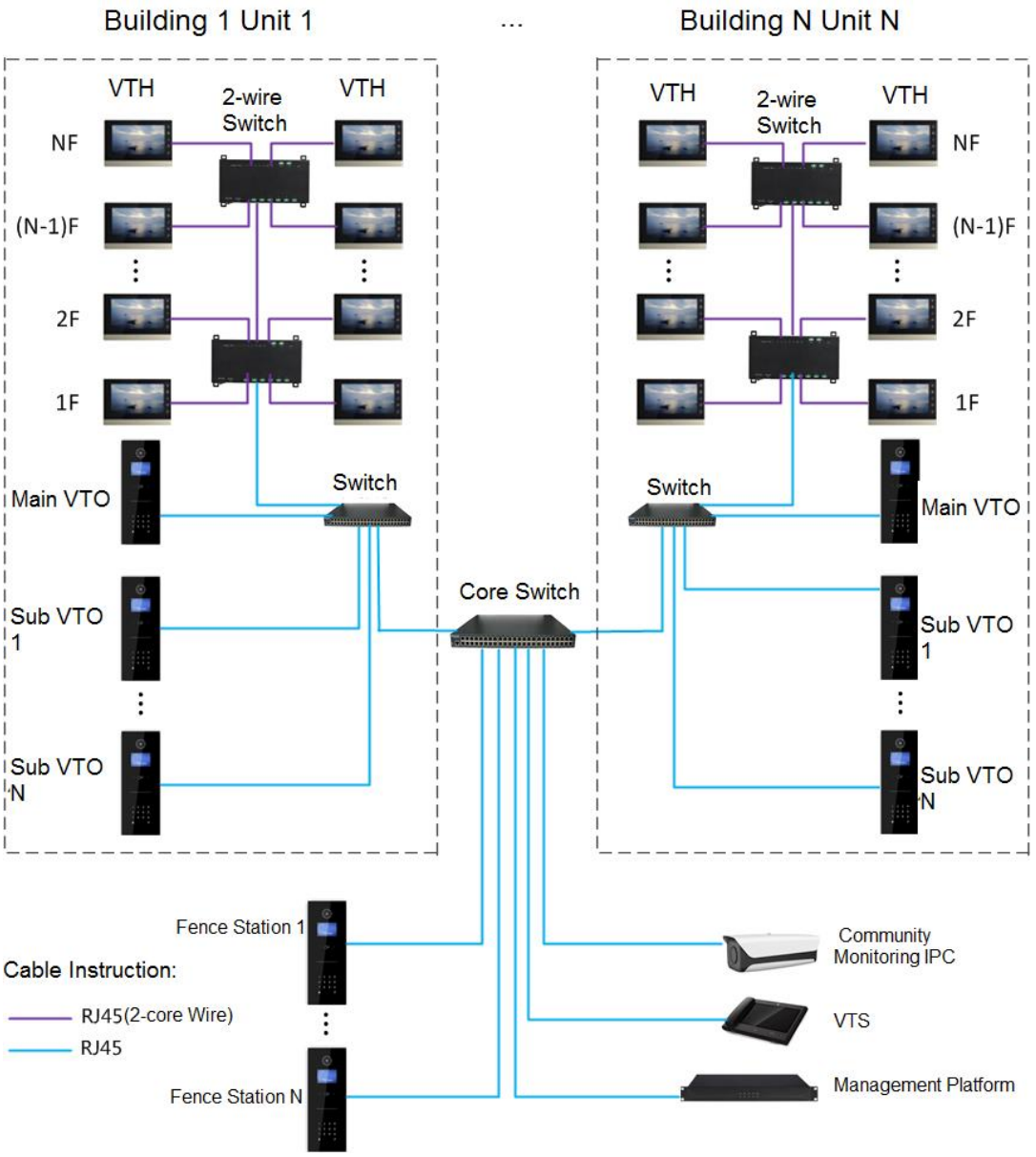


Figure 3-1

3.2 Digital System

Digital system network consist of two types:

- VTH adopts PoE power supply from floor switch, as shown in Figure 3-2.

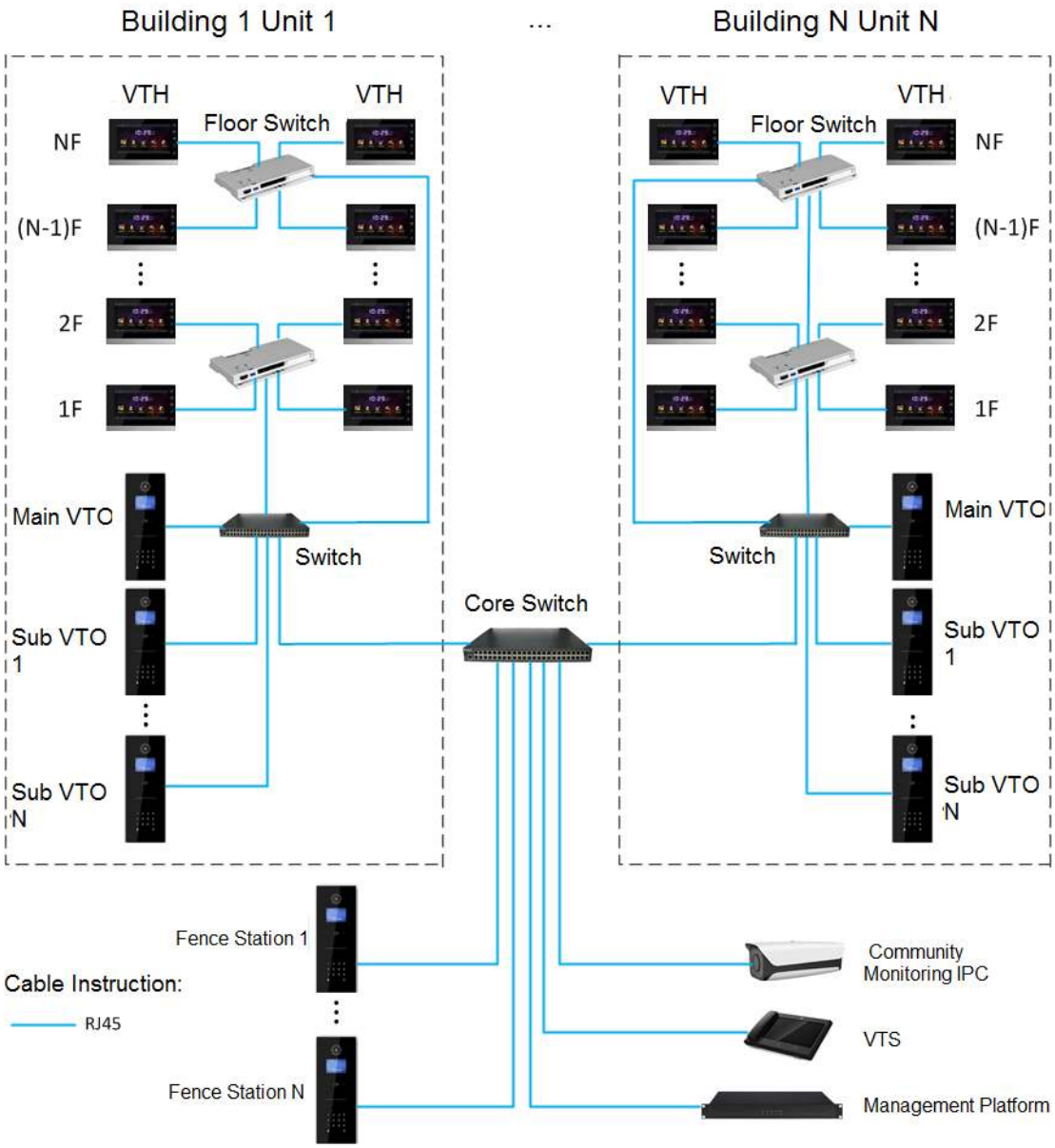


Figure 3-2

- VTH adopts independent power supply from power supply device, as shown in Figure 3-3.

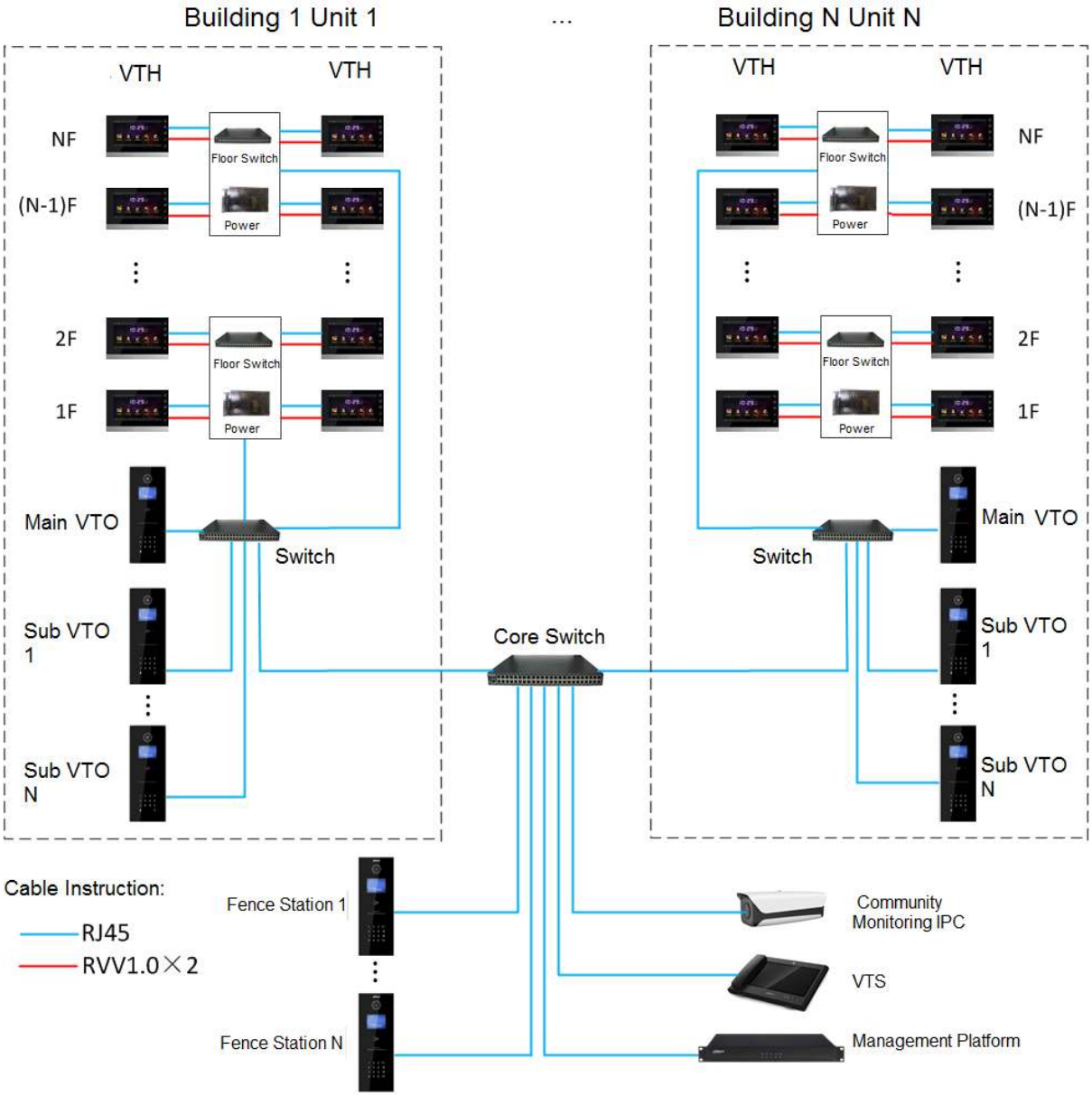

Building 1 Unit 1
...
Building N Unit N
VTH
VTH
NF
(N-1)F
2F
1F
Floor Switch
Power
Main VTO
Switch
Sub VTO 1
Sub VTO N
Core Switch
Cable Instruction:
RJ45
RVV1.0×2
Fence Station 1
Fence Station N
Community Monitoring IPC
VTS
Management Platform

Figure 3-3

4 Device Installation

4.1 Installation Flow Chart

VTH installation flow chart is shown in Figure 4-1 Please install VTH in the following steps.

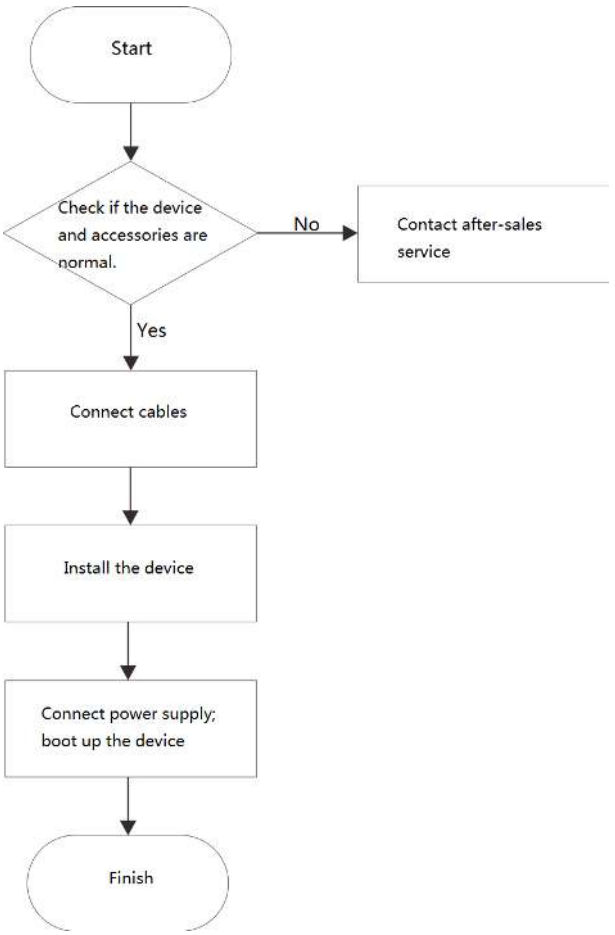


Figure 4-1

- For cable connection, please refer to “2.2 Rear Panel Port“.
- For device installation, please refer to “4.4 Device Installation“.

4.2 Open-case Inspection

Please carry out open-case inspection when receiving the device. Please timely contact our after-sales service personnel in case of any problems.

Sequence	Item		Content
1	Overall package	Appearance	Inspect whether there are obvious damages.
		Package	Inspect whether there are accidental impacts.
		Fittings	Inspect whether fittings are complete.
2	Model and label	Device model	Inspect whether it is consistent with order contract.

Sequence	Item		Content
		Label on the device	Inspect whether it is torn or damaged. Don't tear or discard the label, otherwise warranty service won't be provided. When dialing our after-sales hotline, please provide serial number of the product.
3	Device	Appearance	Inspect whether there are obvious damages.

Table 4-1

4.3 Installation Requirement

- Don't install VTH in bad environment, such as condensation, high temperature, stained, dusty, chemically corrosive and direct sunshine environment.
- Engineering installation and debugging shall be done by professional teams. Please don't dismantle or repair arbitrarily in case of device failure.

4.4 Device Installation

It is suggested that installation height of device central point shall be 1.4cm～1.6cm above the ground.

4.4.1 Surface Installation

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

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

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

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

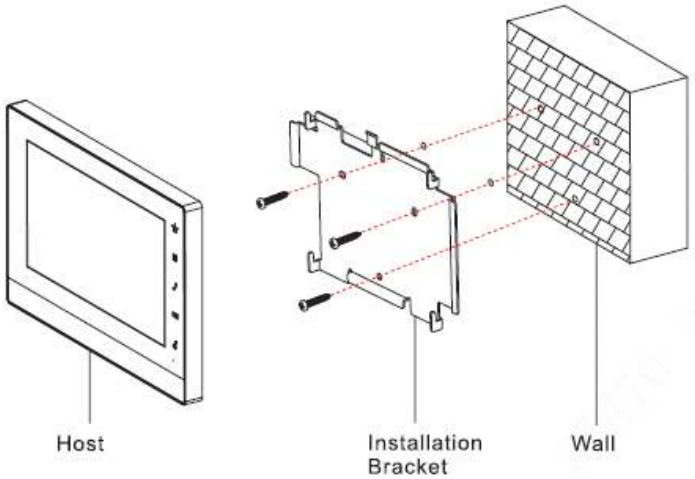


Figure 4-2

4.4.2 Installation with 86 Box

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

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

Step 2 Fix installation bracket onto 86 box with screws.

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

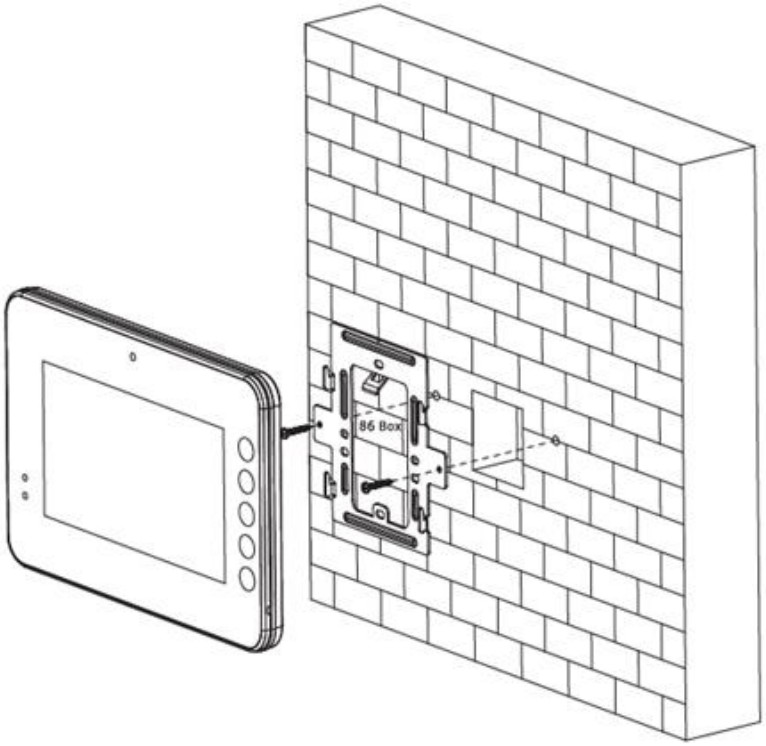


Figure 4-3

4.4.3 Desktop Installation with Bracket

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

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

Step 2 Please connect wire by reference to Figure 2-10.

Step 3 After wiring, guide the wire through wire outlet in the rear or at the bottom of desktop bracket.

Step 4 Put the handset VTH along slot at the top of metal bracket, and install it into the bracket.

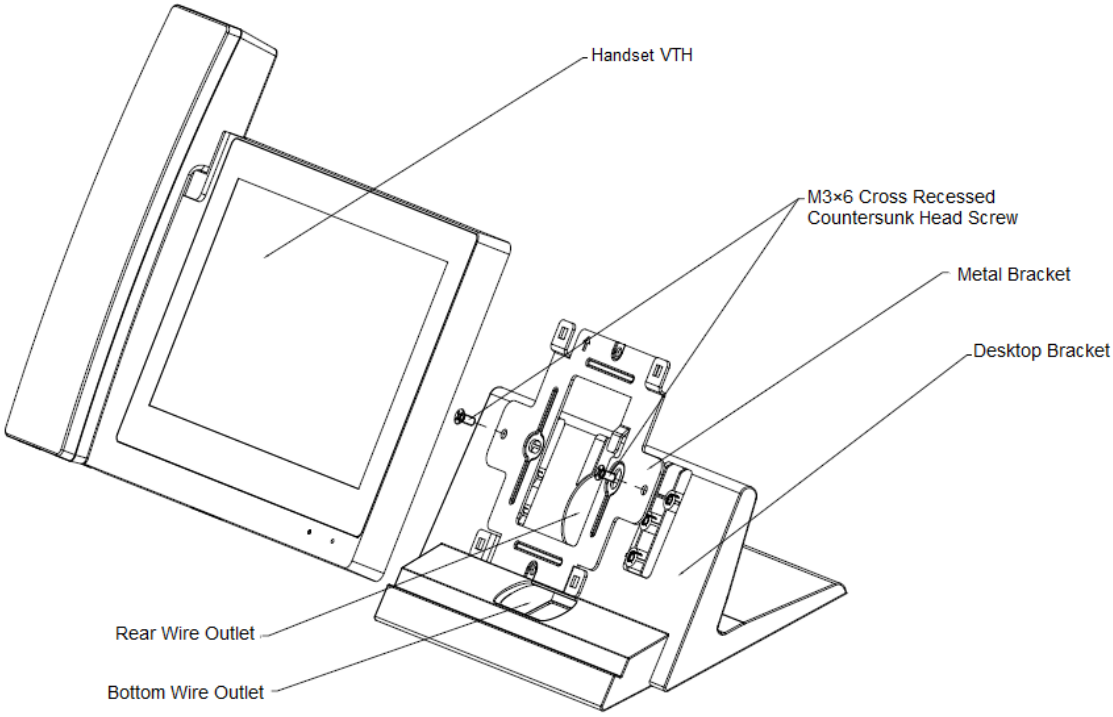


Figure 4-4

5 Device Debugging

Carry out debugging to ensure that the device can realize basic network access, call and monitoring functions after installation. Before debugging, please check whether the following work has been completed.

- Check whether there is short circuit or open circuit. Power on the device only after the circuit is confirmed to be normal.
- IP and no. of every VTO and VTH have been planned.
- Check deployment position of SIP server.

5.1 Debugging Settings

- This device shall be used with VTO of SIP system. This manual introduces “Unit VTO” as an example. Please refer to matched user’s manuals for other types of VTO.
- Set VTO info and VTH info at WEB interface of every VTO, set VTH info, network info and VTO info on every VTH, and thus realize video intercom function.

5.1.1 VTO Settings

5.1.1.1 Initialization

For the first time, please initialize and modify login password.

Please ensure that default IP addresses of PC and VTO are in the same network segment. Default IP address of VTO is 192.168.1.110.

Step 1 Connect VTO power and boot up.

Step 2 Enter default IP address of VTO at the address bar of PC browser.

The system displays “Device Ini” interface, as shown in Figure 5-1.

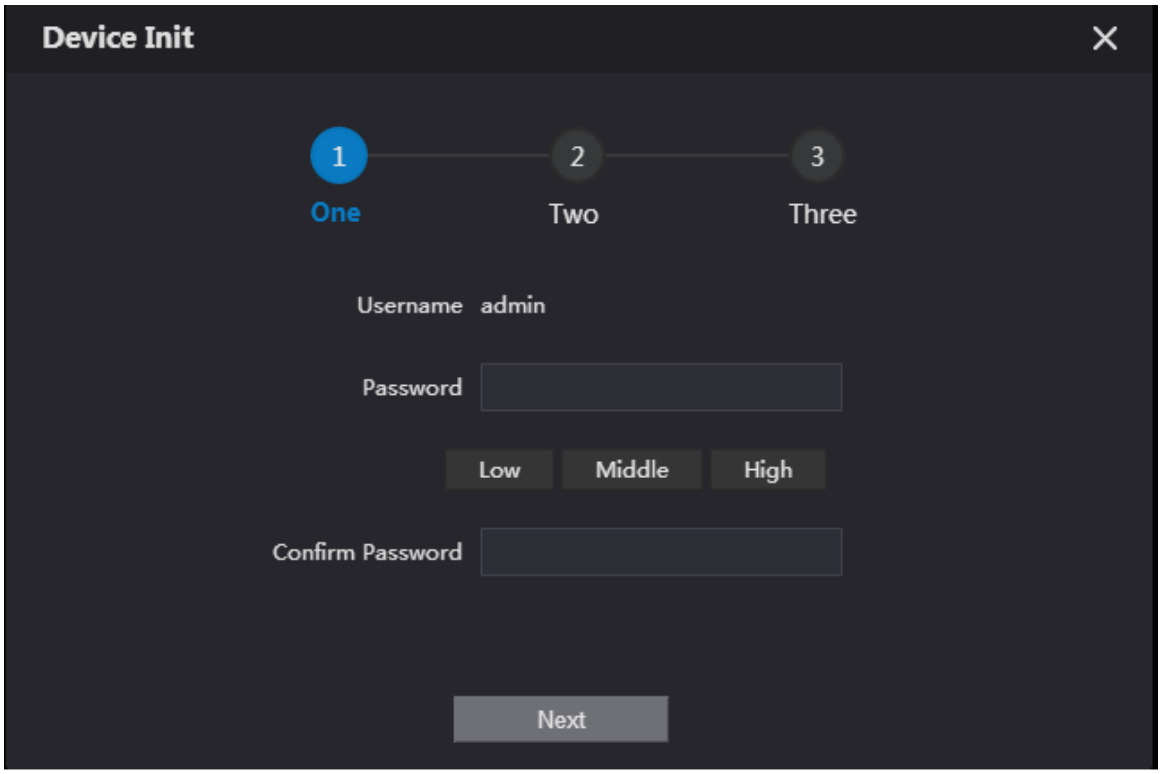


Figure 5-1

Step 3 Enter “Password” and “Confirm Password”, and click “Next”.

The system displays “step two”, as shown in Figure 5-2.

This password is used to login WEB interface. It shall be at least 8 characters, and shall include at least two types of number, letter and symbol.

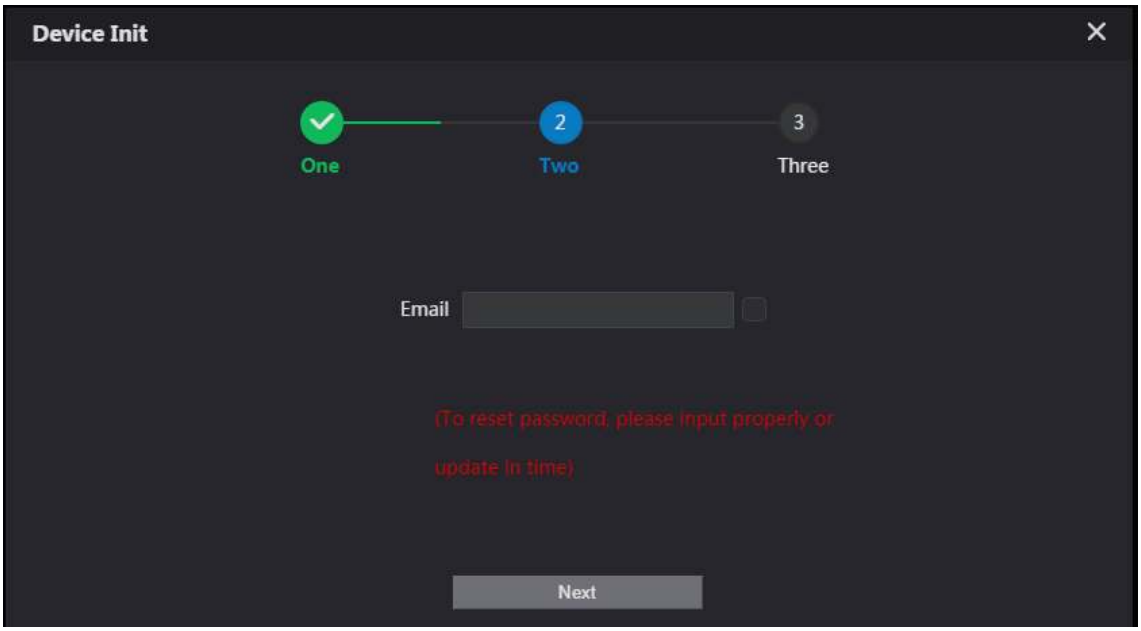


Figure 5-2

Step 4 Select “Email” and enter your Email address. This Email address is used to reset the password, so it is recommended that it should be set.

Step 5 Click “Next”.

The system displays “OK” interface, as shown in Figure 5-3, and shows “Success”

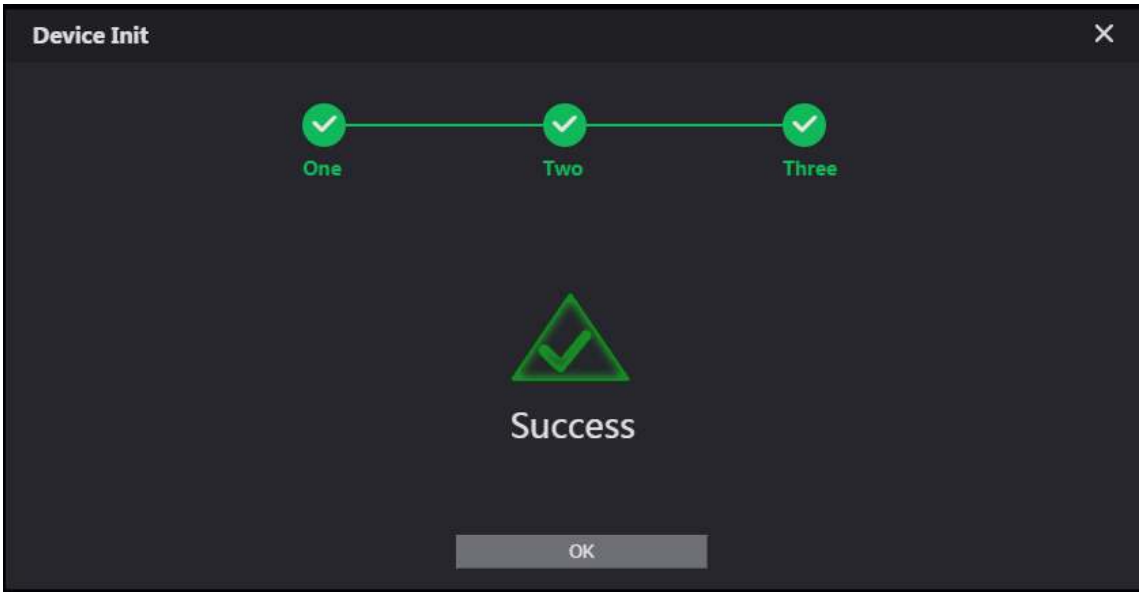


Figure 5-3

Step 6 Click “OK”.

The system displays WEB login interface, as shown in Figure 5-4.

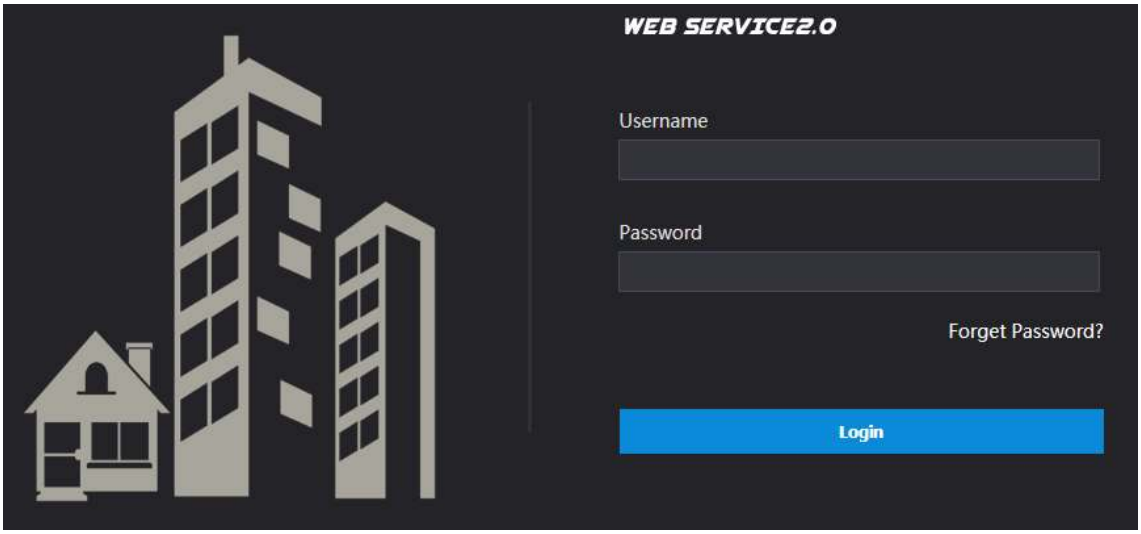


Figure 5-4

Step 7 Enter user name and password, and click “Login”.

Log in the WEB interface of the device.

- Default user name is admin.
- Password is the one set during initialization.

5.1.1.2 Network Config

Modify IP address of VTO to be planned IP address.

Step 1 Select “Network Setting > Basic”.

The system displays “TCP/IP” interface, as shown in Figure 5-5.

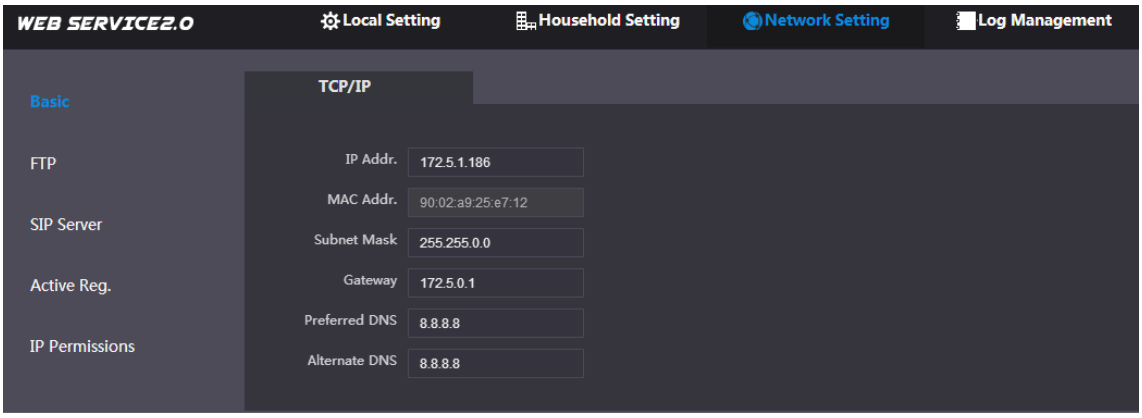


Figure 5-5

Step 2 Enter the planned “IP Address”, “Subnet Mask” and “Default Gateway”, and click “OK”. After modification is completed, VTO reboots automatically, while the following two cases occur at WEB interface.

- If PC is in the planned network segment, WEB interface jumps to new IP login interface automatically.
- If PC is not in the planned network segment, the webpage cannot be displayed. Please add PC into the planned network segment and login WEB interface again.

5.1.1.3 Set System Type

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

Step 1 Select “Local Setting > Basic”.

The system displays “Device Properties” interface, as shown in Figure 5-6.

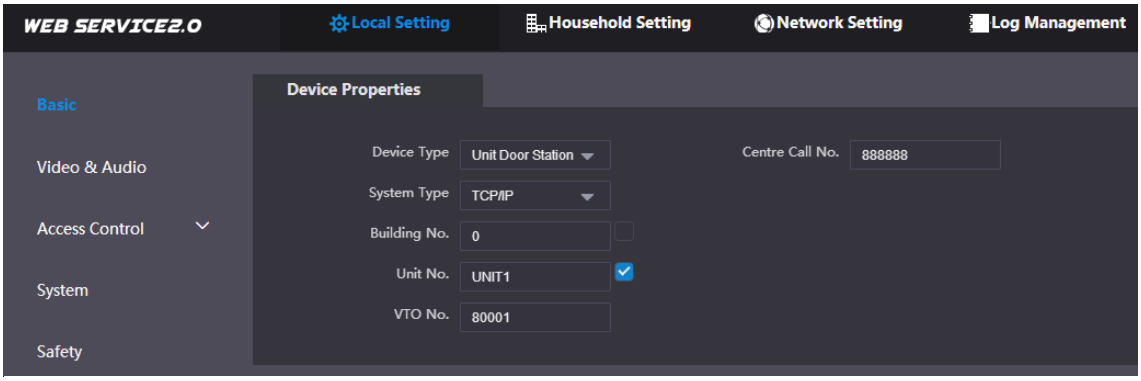


Figure 5-6

Step 2 Select system type to be “TCP/IP”.

Step 3 Click “OK” to save config.

Reboot the device manually or wait the device to reboot automatically, and the settings will take effect.

5.1.1.4 Set Server Type

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

Step 1 Select “Network Setting > SIP Server”.

The system displays “SIP Server” interface, as shown in Figure 5-7.

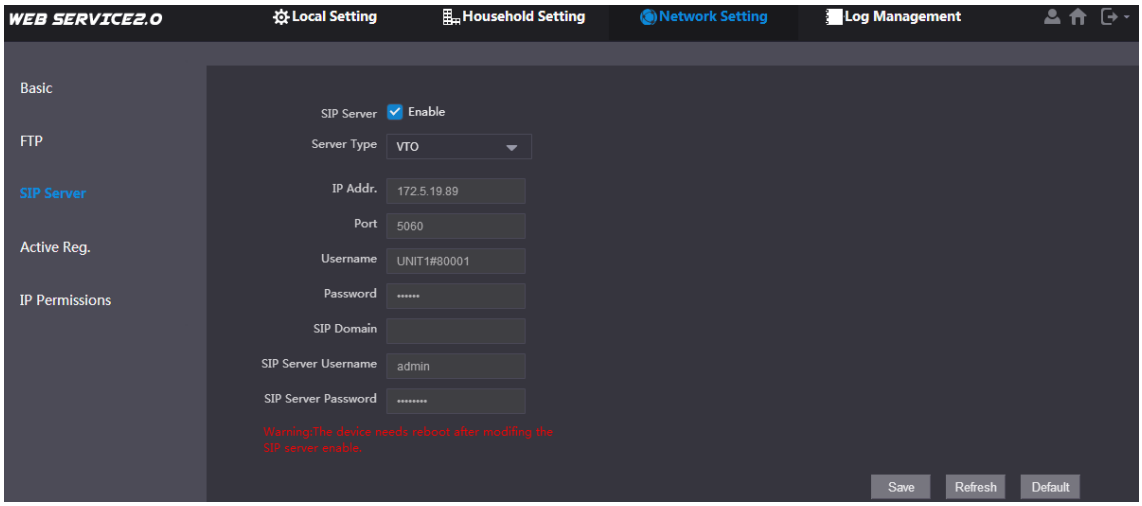


Figure 5-7

Step 2 Select server type.

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

5.1.1.5 SIP Server Config

Configure SIP server info.

Step 1 Select “Network Setting > SIP Server”.

The system displays “SIP Server” interface, as shown in Figure 5-8.

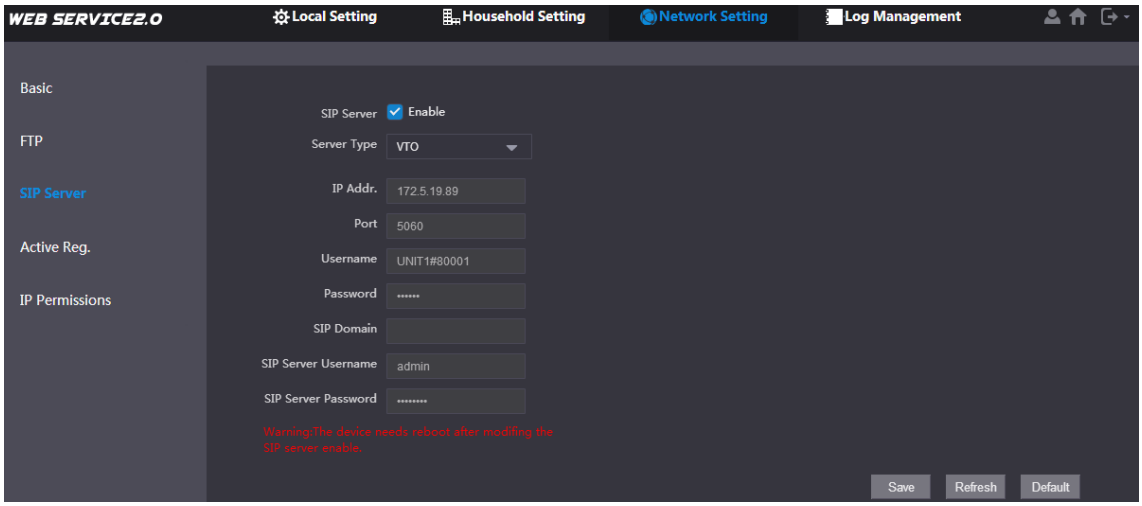


Figure 5-8

Step 2 Configure SIP server.

- This VTO works as SIP server.

  Select “Enable”, and click “OK” to save config. The VTO reboots automatically, and WEB interface jumps to login interface.

If the VTO you are visiting is not configured as SIP server, do not select the **Enable** check box at **SIP Server**, otherwise the connection will fail.

- Another VTO works as SIP server.

Set parameters by reference to Table 5-1 and click “OK”. The VTO reboots automatically, and web interface jumps to login interface.

Parameter	Description
IP Address	IP address of VTO, which works as SIP server.
Port	It is 5060 by default.
Username	Use default value.
Password	
SIP Domain	SIP domain shall be VDP.
Login Username	Username and password to login SIP server.
Login Pwd	

Table 5-1

- The platform (Express/DSS) works as SIP server.
  Select “Server Type” to be “Express/DSS” and set parameters by reference to Table 5-2 and click “OK”. The VTO reboots automatically, and web interface jumps to login interface.

Parameter	Description
IP Address	IP address of the platform.
Port	It is 5080 by default.
Username	Use default value.
Password	
SIP Domain	SIP domain can be null or default.
SIP Server Username	Username and password to login SIP server.
SIP Server Password	

Table 5-2

- VTO settings have been completed if the platform or another VTO works as SIP server.
- If this VTO works as SIP server, “Device Manager” appears in the left parameter tab. Please add VTO and VTH by reference to “5.1.1.6 Add VTO“ and “5.1.1.7 Add VTH“.

5.1.1.6 Add VTO

Add info about all outdoor stations (VTO).

It is necessary to add VTO only when this VTO works as SIP server.

Step 1 Login web interface again.

Step 2 Select “Household Setting > VTO No. Management”.

The system displays “VTO No. Management” interface, as shown in Figure 5-9.

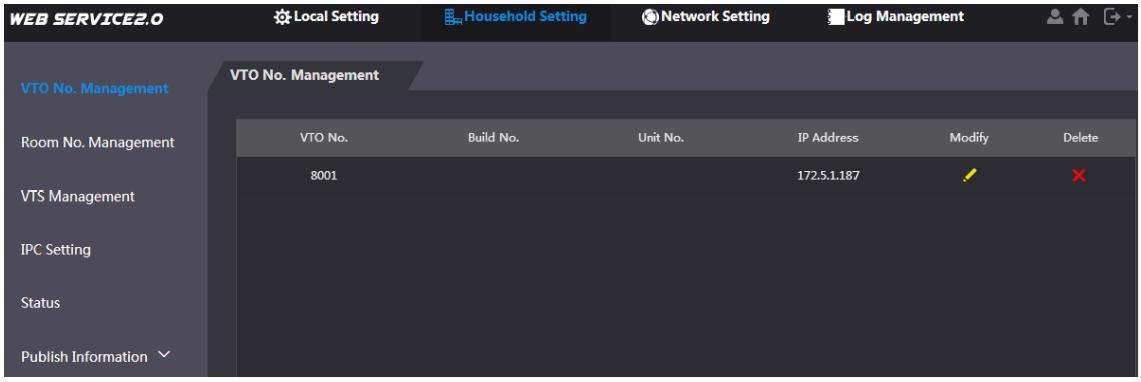


Figure 5-9

Step 3 Click “Add”.

The system displays “Add” interface, as shown in Figure 5-10.

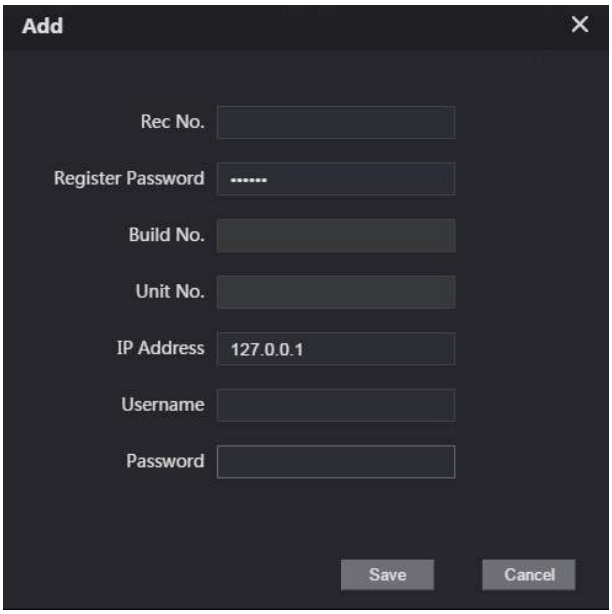


Figure 5-10

Step 4 Set VTO parameters by reference to Table 5-3.

Parameter	Description
Rec No.	VTO number.
Register Password	Signaling interactive use in SIP system. Adopt default value.
IP Address	IP address of VTO.
Username	Username and password to login WEB interface of this VTO.
Password	

Table 5-3

Step 5 Click “OK” to complete adding.

Repeat these steps to add other outdoor stations in the group.

5.1.1.7 Add VTH

Add info about all indoor stations (VTH).

- It is necessary to add VTH only when this VTO works as SIP server.
- When there are master VTH and extension, both shall be added.

Step 1 Select “Household Setting > Room No. Management”.

The system displays “Room No. Management” interface, as shown in Figure 5-11.

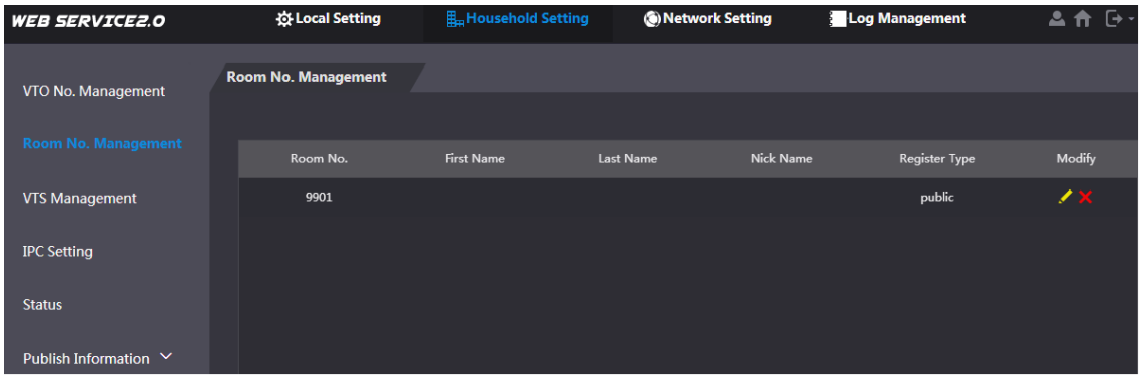


Figure 5-11

Step 2 Click “Add”.

The system displays “Add” interface, as shown in Figure 5-12.

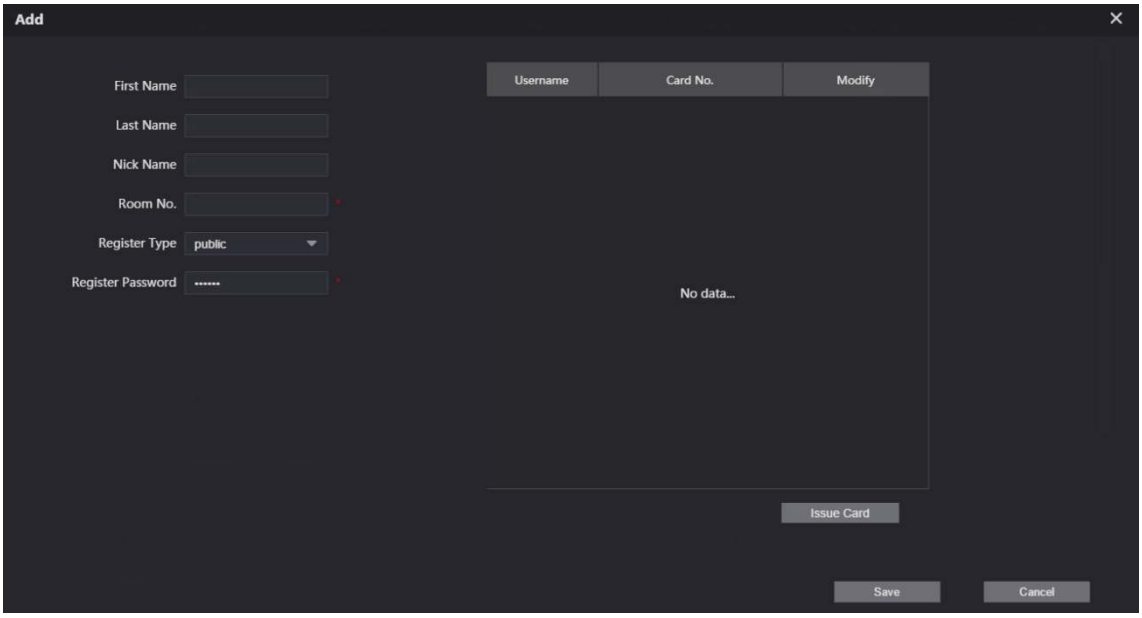


Figure 5-12

Step 3 Set VTH parameters by reference to Table 5-4.

Parameter	Description
First Name	Set VTH username and nickname, in order to distinguish.
Last Name	
Nick Name	
Room No.	Set VTH room number. ● VTH short number consists of 1～6 numbers, which may include number and “#”. It shall be consistent with room number configured at VTH. ● When there are master VTH and extensions, to realize group call function, master VTH short no. shall end with “#0”, whereas extension VTH short no. shall end with #1, #2 and #3. For example, if master VTH is 101#0, extensions will be 101#1, 101#2…
Register Password	Signaling interactive use in SIP system. Adopt default value.
Register Type	

Table 5-4

Step 4 Click “OK” to complete adding.
Repeat these steps to add other indoor stations in the group.

5.1.2 VTH Settings

5.1.2.1 Initialization

Set the password and bind your Email.

- Password: it is used to enter project setting interface.
- Email: it is used to retrieve your password when you forget it.

Step 1 Power on the device.
The system displays “Welcome” and enters “Device Initialization” interface, as shown in Figure 5-13.

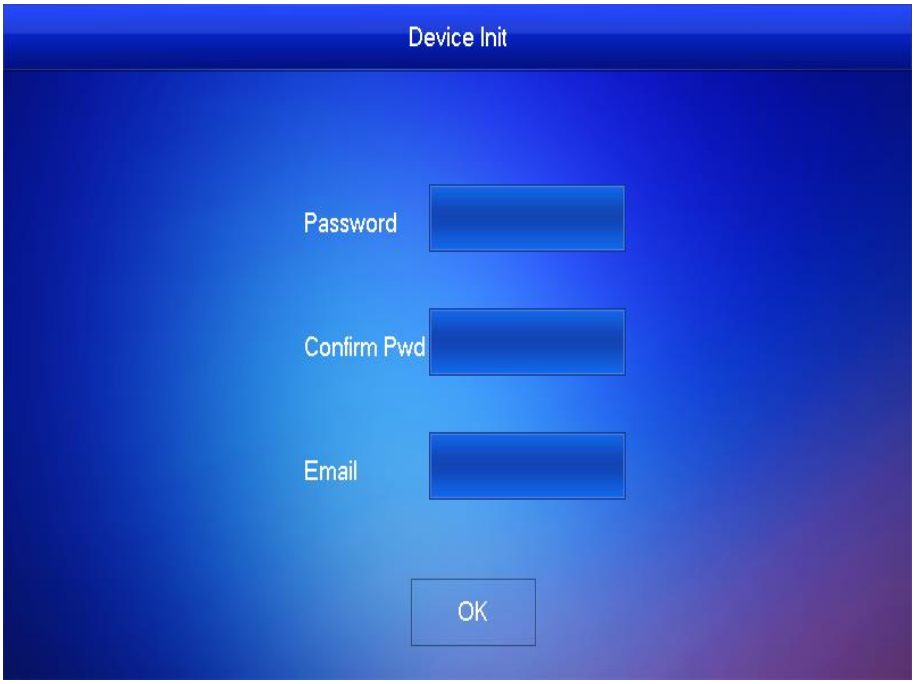


Figure 5-13

Step 2 Enter “Password”, “Confirm Pwd” and “Email”.

Step 3 Press [OK].

The system displays main interface, as shown in Figure 5-14.

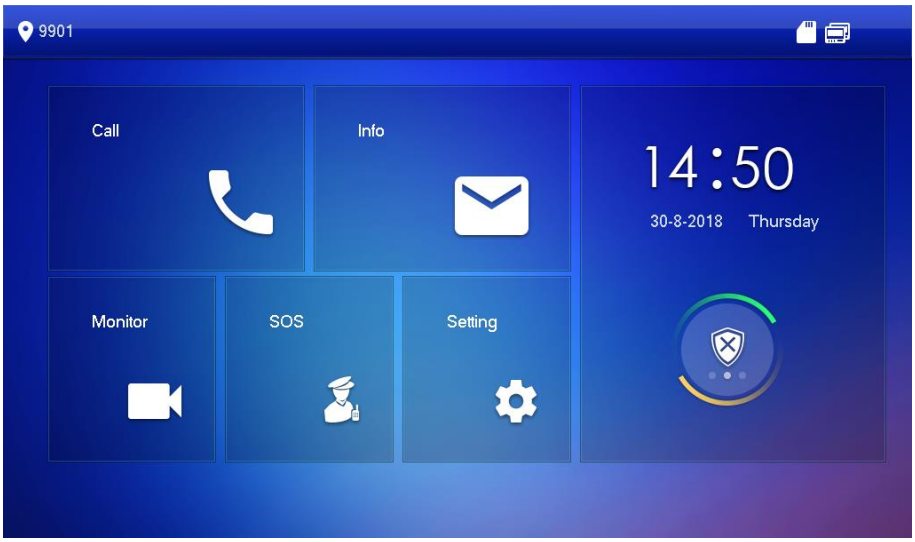


Figure 5-14

5.1.2.2 Set Device Network

According to available network connection modes, configure VTH network information.

IP addresses of VTH and VTO shall be in the same network segment. Otherwise, VTH will fail to obtain VTO info after configuration.

Step 1 Press [Setting] for more than 6 seconds.

The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and press [OK].

Step 3 Press [Network].

The system displays “Network” interface, as shown in Figure 5-15 or Figure 5-16.

Only devices with the wireless function can access to wireless network.

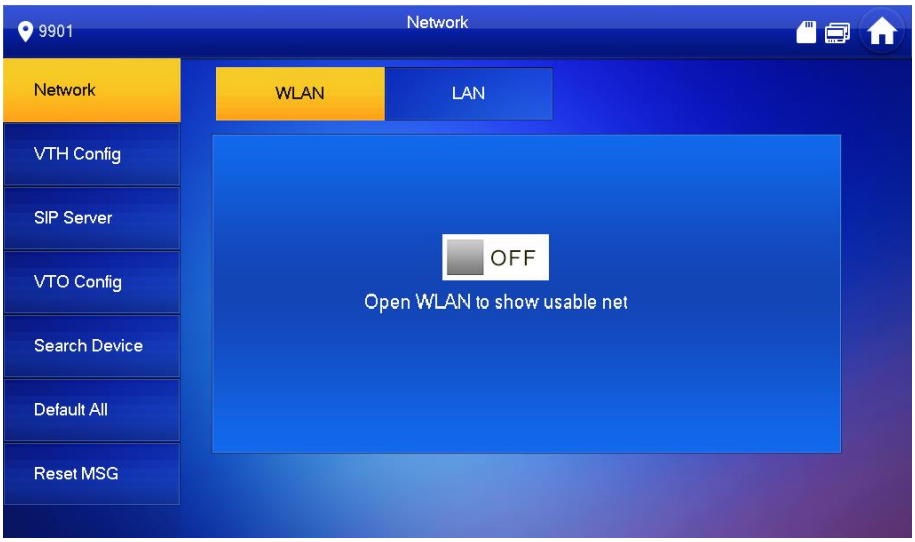


Figure 5-15

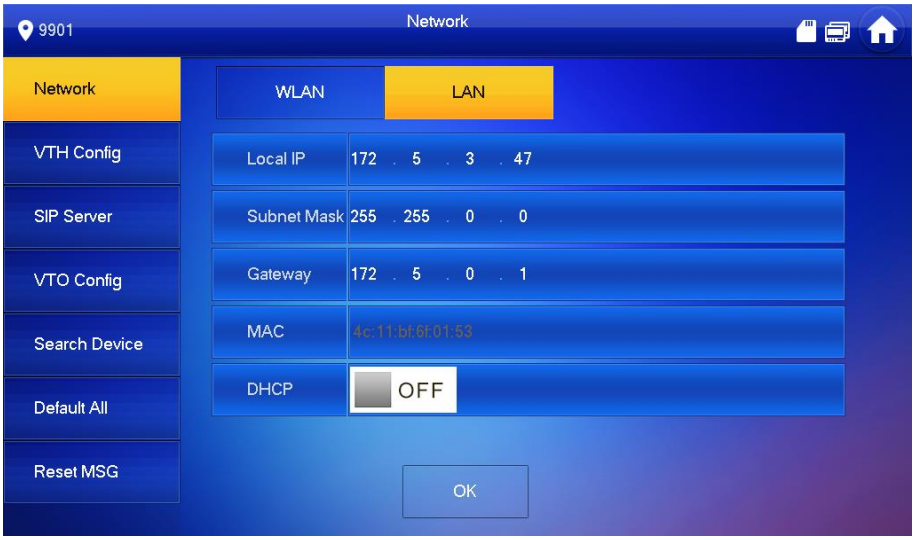


Figure 5-16

Step 4 Set according to actual network access mode.

- LAN

Enter “Local IP”, “Subnet Mask” and “Gateway”, press [OK]. Or press OFF to enable DHCP function and obtain IP info automatically.

If the device has WLAN function, please click “WLAN” tab to set it.

- WLAN

1) Press OFF to enable Wi-Fi function.

The system displays available Wi-Fi list, as shown in Figure 5-17.

Figure 5-17

2) Connect Wi-Fi.

The system has 2 access ways as follows.

◇ At “WLAN” interface, select Wi-Fi, click “Wireless IP” tab to enter “Local IP”, “Subnet Mask” and “Gateway”, and press [OK].

◇ At “WLAN” interface, select Wi-Fi, click “Wireless IP” tab, press OFF to enable DHCP function and obtain IP info automatically, as shown in Figure 5-18.

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

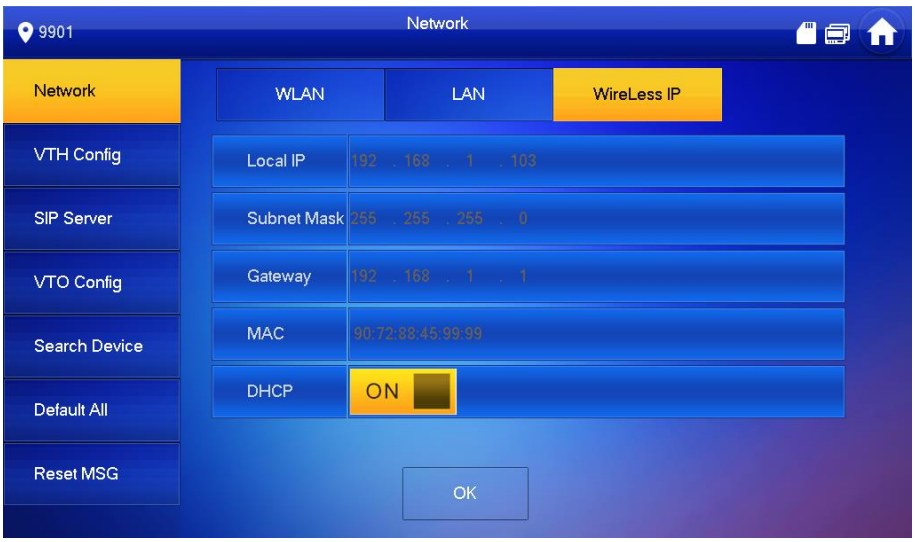


Figure 5-18

5.1.2.3 VTH Config

Set VTH “Room No.”, type and “Master IP”.

Step 1 At main interface, press [Setting] for more than 6 seconds.
The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and press [OK].

Step 3 Press [VTH Config].

The system displays “VTH Config” interface, as shown in Figure 5-19.

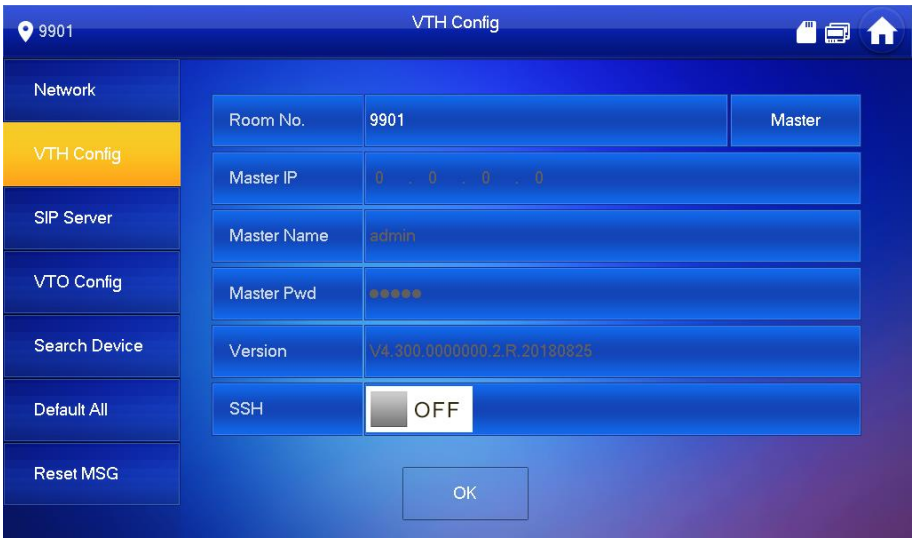


Figure 5-19

Step 4 Set VTH info.

- Be used as a master VTH.

Enter “Room No.” (such as 9901 or 101#0) and press “OK” to save.

- “Room no.” shall be the same with “VTH Short No.”, which is set when adding VTH at WEB interface. Otherwise, it will fail to connect VTO.
- In case of extension VTH, room no. shall end with #0. Otherwise, it will fail to connect VTO.

- Be used as an extension VTH.

1) Press [Master] and switch to “Extension”.
2) Enter “Room No.” (such as 101#1) and “Master IP” (IP address of master VTH).

“Master Name” and “Master Pwd” are the user name and password of master VTH. Default user name is admin, and the password is the one set during device initialization.

Step 5 (Optional) Press OFF to enable SSH.

After SSH is enabled, the debugging terminal connects VTH through SSH protocol, so as to operate and debug it.

Step 6 Press [OK] to save config.

5.1.2.4 SIP Server

Configure SIP server on VTH, and build connection.

Step 1 At main interface, press [Setting] for more than 6 seconds.

The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and press [OK].

Step 3 Press [SIP Server].

The system displays “SIP Server” interface, as shown in Figure 5-20.

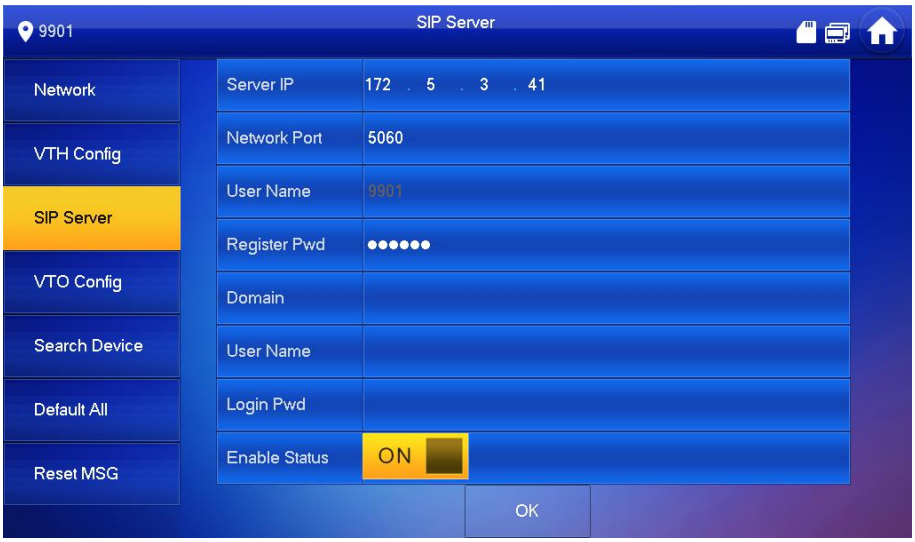


Figure 5-20

Step 4 Set parameters of SIP server by reference to Table 5-5.

Parameter	Description
Server IP	When the platform works as SIP server, server IP is IP address of the platform. When VTO works as SIP server, server IP is IP address of the VTO.
Network Port	When the platform works as SIP server, network port is 5080. When VTO works as SIP server, network port is 5060
User Name	Use default value.
Register Pwd	
Domain	Registration domain of SIP server, which can be null. When VTO works as SIP server, registration domain of SIP server shall be VDP.
User Name	User name and password to login SIP server.
Login Pwd	

Table 5-5

Parameter	Description
Server IP	• When the platform works as SIP server, server IP is IP address of the platform. • When VTO works as SIP server, server IP is IP address of the VTO.
Network Port	• When the platform works as SIP server, network port is 5080. • When VTO works as SIP server, network port is 5060.
User Name	Use default value.
Register Pwd	
Domain	Registration domain of SIP server, which can be null. When VTO works as SIP server, registration domain of SIP server shall be VDP.
User Name	User name and password to login SIP server.
Login Pwd	

Table 5-6

Step 5 Set “Enable Status” to be ON.

Enable SIP server function.

Step 6 Press [OK] to save config.

5.1.2.5 VTO Config

Add VTO and fence station info; at VTH interface, bind VTH with VTO.

Step 1 At main interface, press [Setting] for more than 6 seconds.

The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and press [OK].

Step 3 Press [VTO Config].

The system displays “VTO Config” interface, as shown in Figure 5-21.

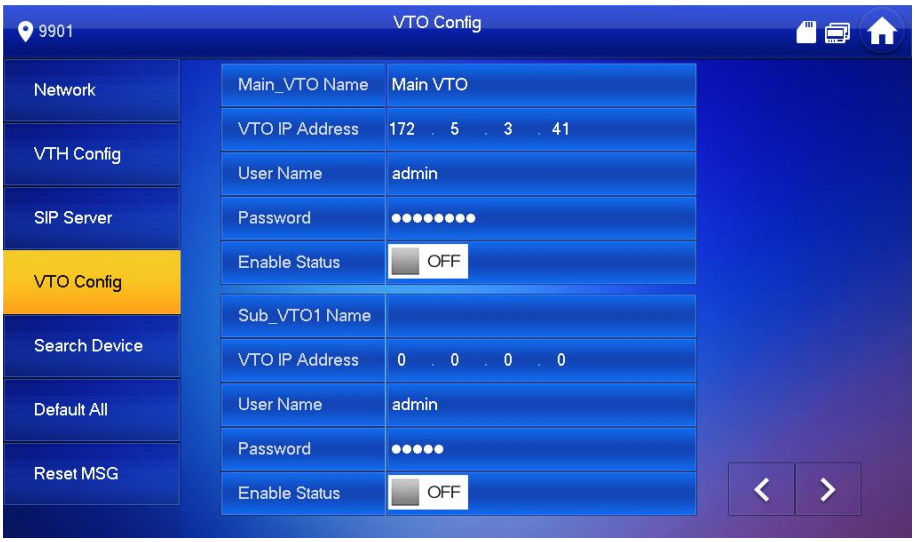


Figure 5-21

Step 4 Add VTO or fence station.

- Add main VTO.

1) Enter “Main VTO Name”, “VTO IP Address”, “User Name” and “Password”.

2) Switch the “Enable Status” to be ON.

“User Name” and “Password” shall be consistent with WEB login user name and password of VTO. Otherwise, it will fail to connect.

- Add sub VTO or fence station.

1) Enter “Sub VTO/Fence Station Name”, “Sub VTO/Fence Station IP address”, “User Name” and “Password”.

2) Switch the “Enable Status” to be ON.

Press < / > to turn page and add more sub VTO/fence stations.

5.2 Debugging Verification

5.2.1 VTO Calls VTH

Dial VTH room no. (such as 101) at VTO, and thus call VTH. VTH pops up monitoring image and operating keys, as shown in Figure 5-22. It represents successful debugging.

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 5-22

5.2.2 VTH Monitors VTO

VTH is able to monitor VTO, fence station or IPC. Take “VTO” for example.

Select “Monitor > Door”, as shown in Figure 5-23. Select the VTO to enter monitoring image, as shown in Figure 5-24.

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

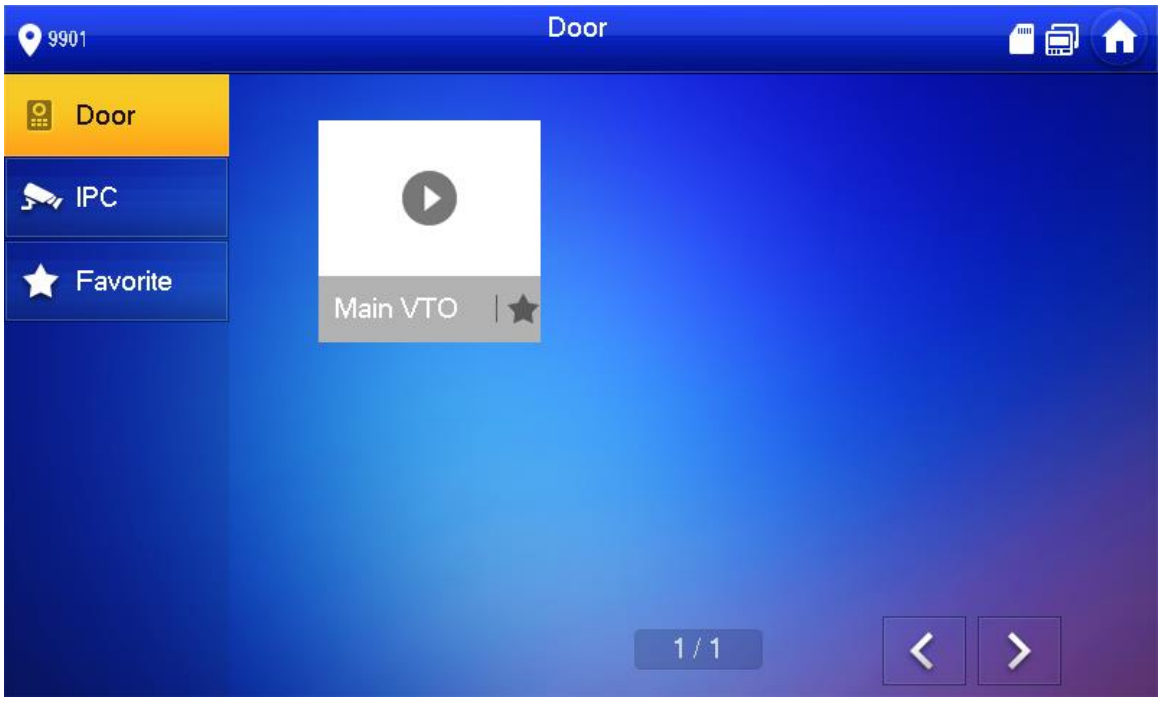


Figure 5-23

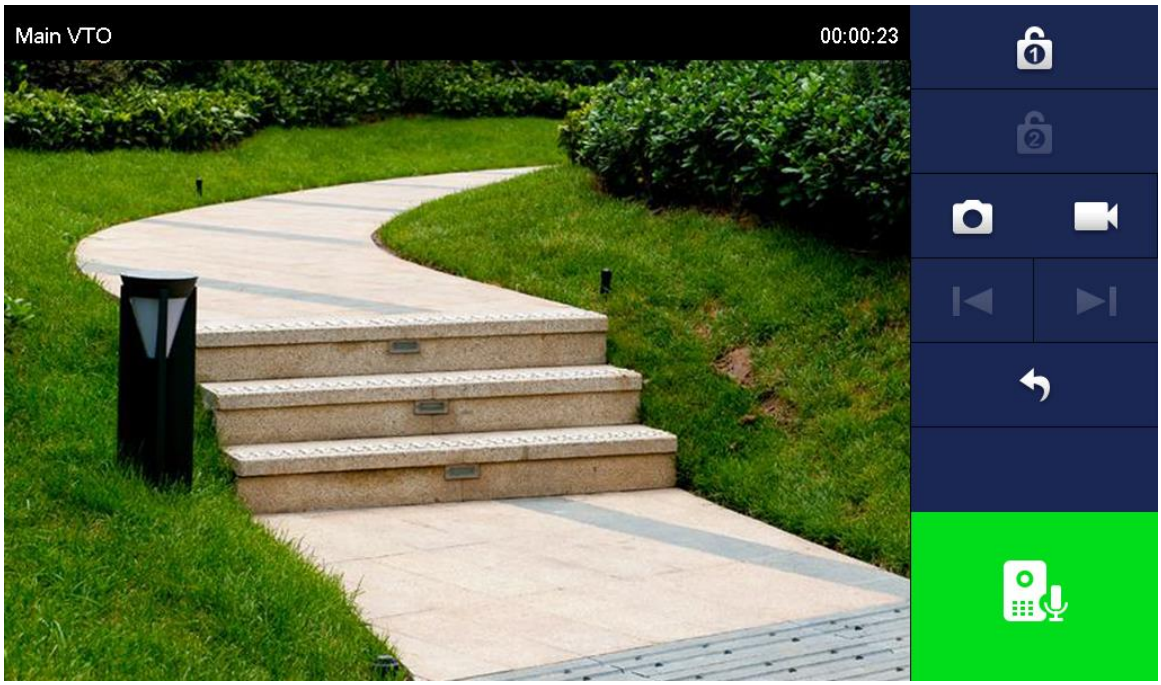


Figure 5-24

6 Interface Operation

6.1 Main Interface

There are six items at the main interface, namely, call, info, monitor, SOS, setting and arm/disarm, as shown in Figure 6-1. For description of every item, please refer to Table 6-1.

No.	Name	Description
1	Room No.	Number of the room where VTH is located.
2	Call	Call a user. Manage the contacts. View and manage the call records.
3	Info	View, delete and clear notices issued by Property Management Center. View, delete and clear security alarm info. When VTH doesn't have a SD card or VTO enables video-audio message uploading function, "Guest Message" tab will be displayed. View, delete and clear messages of VTO. When VTH owns a SD card, "Video Pic" tab will be displayed. View, delete and clear videos and pictures.
4	Status Bar	: Wired network connection icon, meaning that the device isn't connected with network. : Wired network connection icon, meaning that the device has connected with network in a wired way. : Wi-Fi network connection icon, meaning that the device has connected with network in a wireless way. : Main VTO connection icon, meaning that the device failed to connect main VTO; without this icon, the device has connected with main VTO successfully. : SD card icon, meaning that SD card has been inserted into the device; without this icon, the SD card has not been inserted or the device doesn't support SD card. : DND (Do Not Disturb) icon, meaning that the device has enabled DND function. It is not enabled by default.
5	Time	Display date, day of the week and time.
6	Arm/disarm	Display the last unread alarm info.

No.	Name	Description
		: press this icon to enter arm mode selection.
7	Setting	Press [Setting], input login password and enter system setting interface. Press [Setting] for over 6 seconds, input the password set during initialization, and enter project setting interface.
8	SOS	Press this icon to call Management Center.
9	Monitor	Monitor the VTO, fence station, IPC, NVT, HCVR and XVR.

Table 6-1

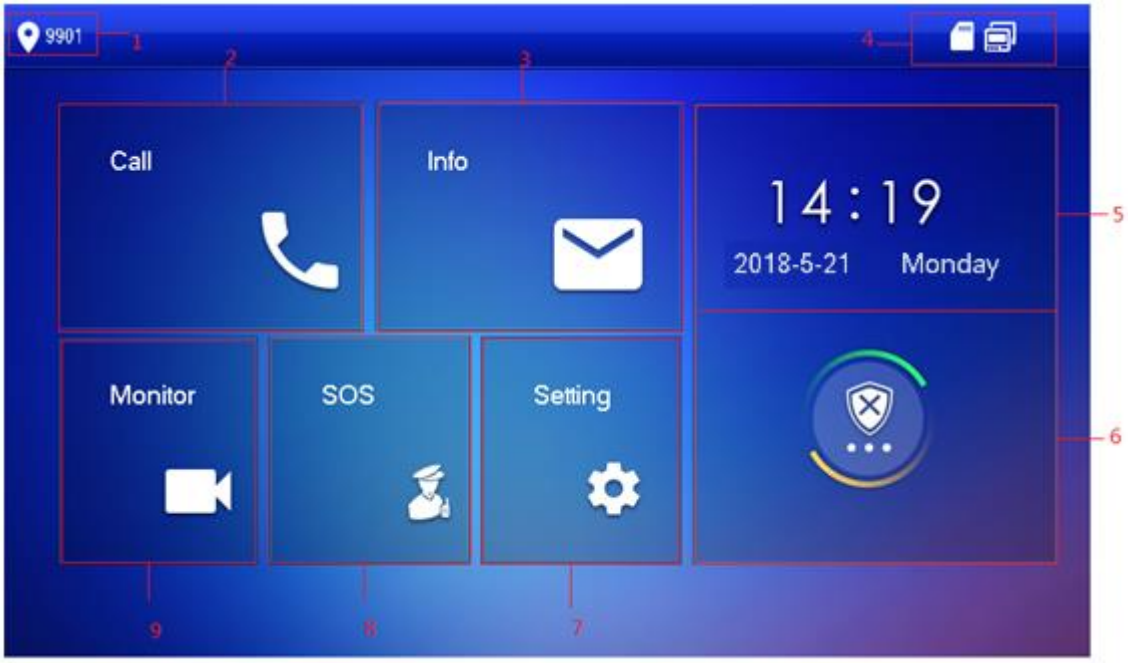


Figure 6-1

No.	Name	Description
1	Room No.	Number of the room where VTH is located.
2	Call	● Call a user. ● Manage the contacts. ● View and manage the call records.
3	Info	● View, delete and clear notices issued by Property Management Center. ● View, delete and clear security alarm info. ● When VTH doesn't have a SD card or VTO enables video-audio message uploading function, "Guest Message" tab will be displayed. View, delete and clear messages of VTO. ● When VTH owns a SD card, "Video Pic" tab will be displayed. View, delete and clear videos and pictures.

No.	Name	Description
4	Status Bar	● : Wired network connection icon, meaning that the device isn't connected with network. ● : Wired network connection icon, meaning that the device has connected with network in a wired way. ● : Wi-Fi network connection icon, meaning that the device has connected with network in a wireless way. ● : Main VTO connection icon, meaning that the device failed to connect main VTO; without this icon, the device has connected with main VTO successfully. ● : SD card icon, meaning that SD card has been inserted into the device; without this icon, the SD card has not been inserted or the device doesn't support SD card. ● : DND (Do Not Disturb) icon, meaning that the device has enabled DND function. It is not enabled by default.
5	Time	Display date, day of the week and time.
6	Arm/disarm	● Display the last unread alarm info. ● : press this icon to enter arm mode selection.
7	Setting	● Press [Setting], input login password and enter system setting interface. ● Press [Setting] for over 6 seconds, input the password set during initialization, and enter project setting interface.
8	SOS	Press this icon to call Management Center.
9	Monitor	Monitor the VTO, fence station, IPC, NVT, HCVR and XVR.

Table 6-2

6.2 Setting

6.2.1 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 at the path/mnt/sd/Ring/.
- Audio file extension name must be .mp3; audio files must be MP3 files (audio files of other formats cannot be played if you modify their extension names).
- Audio file size must be less than 100kB.
- Ring tone format: 16K, 16BIT, mp3.

- You can only customize 10 ring tones. Other ring tones will not be displayed at the VTH.

6.2.1.1 VTO Ring

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

Step 1 Press [Setting].

The system pops up “Password” prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to “6.2.6.3 Password Setting“ for details.

Step 3 Select “Ring > VTO Ring Setup”.

The system displays “VTO Ring Setup” interface, as shown in Figure 6-2. Press or to page up and down.

Figure 6-2

Step 4 Press text box to select rings, and press and to set the volume.

6.2.1.2 VTH Ring

Set the ring of this VTH.

Step 1 Press [Setting].

The system pops up “Password” prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to “6.2.6.3 Password Setting“ for details.

Step 3 Select “Ring > VTH Ring Setup”.

The system displays “VTH Ring Setup” interface, as shown in Figure 6-3.

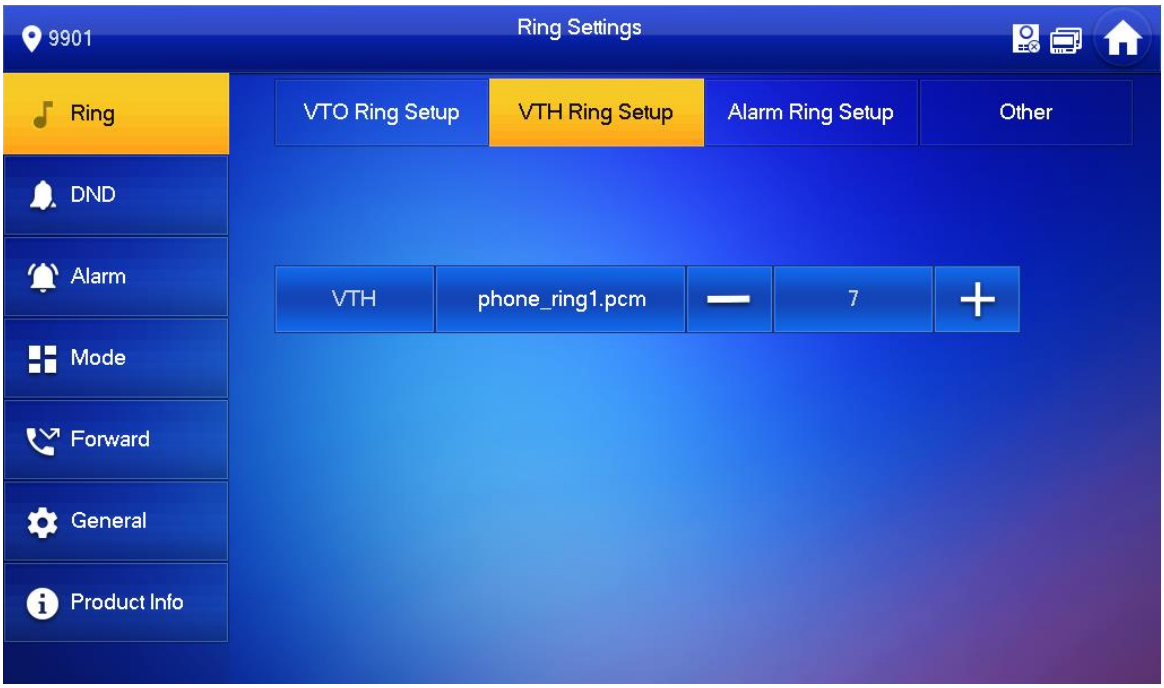


Figure 6-3

Step 4 Press text box to select rings, and press + and − to set the volume.

6.2.1.3 Alarm Ring

Set the ring when VTH gives an alarm.

Step 1 Press [Setting].

The system pops up “Password” prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to “6.2.6.3 Password Setting“ for details.

Step 3 Select “Ring > Alarm Ring Setup”.

The system displays “Alarm Ring Setup” interface, as shown in Figure 6-4.

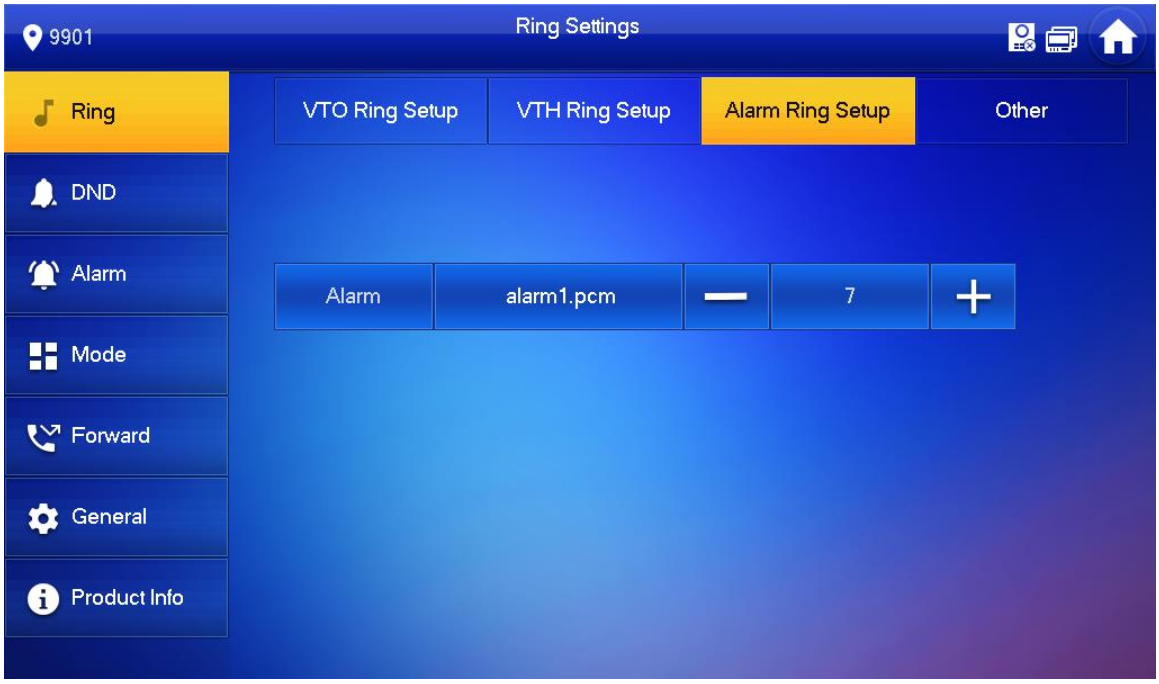


Figure 6-4

Step 4 Press text box to select rings, and press + and − to set the volume.

6.2.1.4 Other

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 master VTH, and cannot be set.

Step 1 Press [Setting].

The system pops up "Password" prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to "6.2.6.3 Password Setting" for details.

Step 3 Select "Ring > Other".

The system displays "Other" interface, as shown in Figure 6-5.

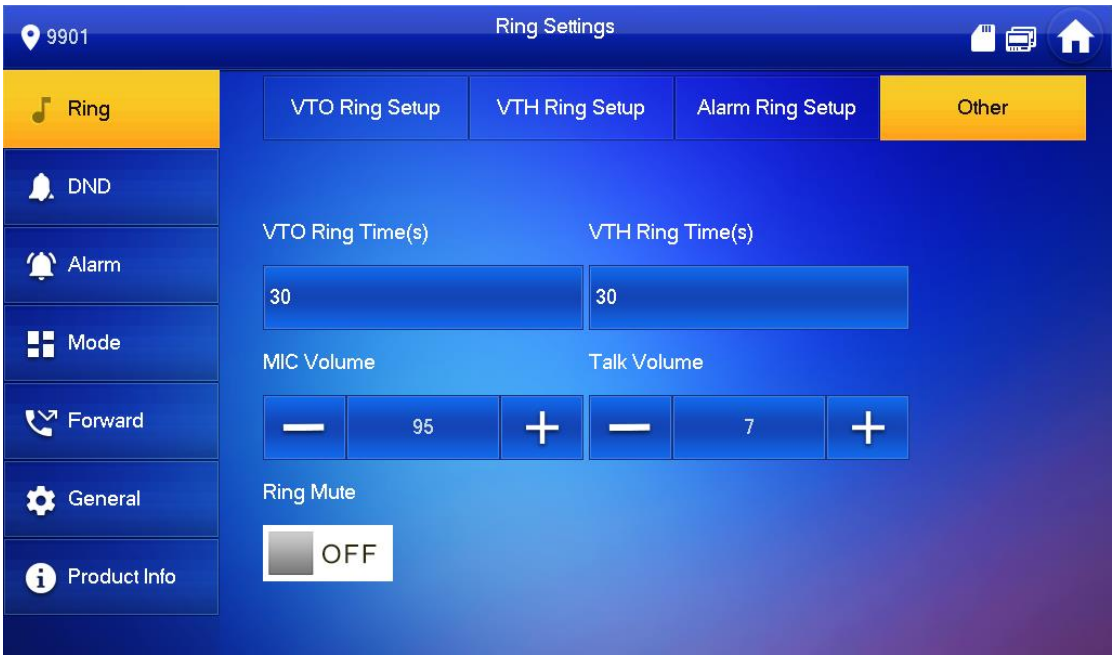


Figure 6-5

Step 4 Press + and − to set the time or volume. Press OFF to enable "Ring Mute", and the icon becomes ON.

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

6.2.2 DND Settings

Set to avoid incoming calls within a time period.

- DND function is not enabled by default.
- Under DND mode, there is no call reminder when VTH is called, but call info is recorded.
- Parameters at this interface are set on master VTH only, and extension VTH synchronizes with master VTH.

Step 1 Press [Setting].

The system pops up "Password" prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to "6.2.6.3 Password Setting" for details.

Step 3 Press [DND].

The system displays "DND Settings" interface, as shown in Figure 6-6.

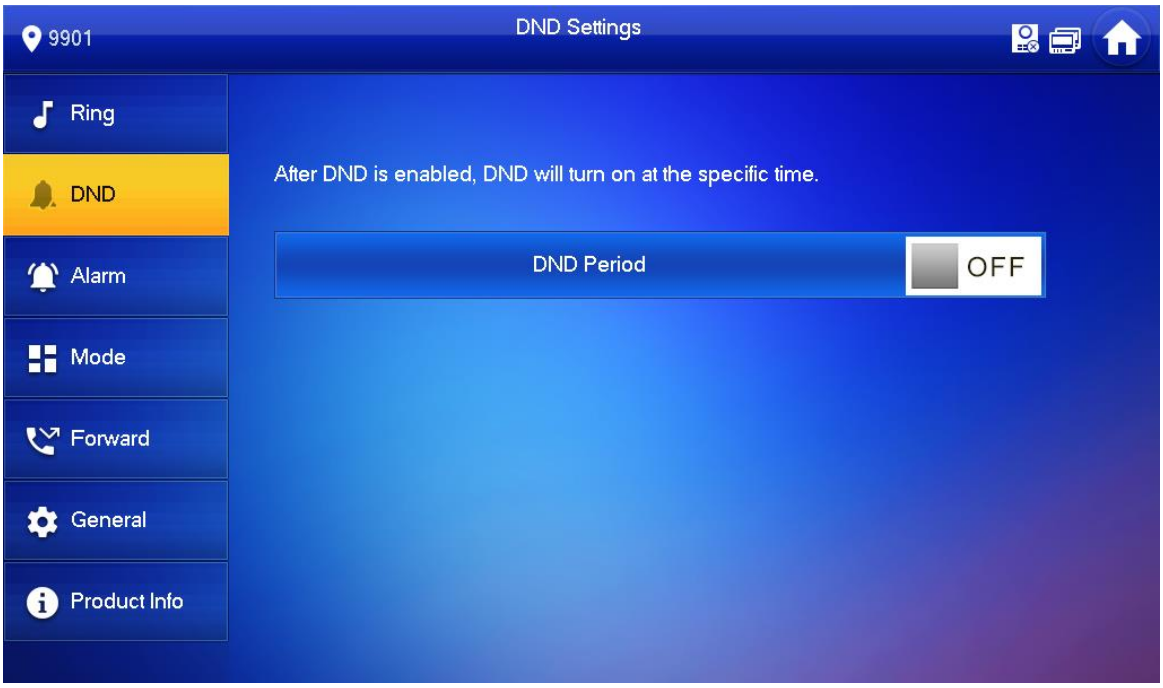


Figure 6-6

Step 4 Press OFF to enable DND function, and the icon becomes ON.

The system displays DND period, as shown in Figure 6-7.

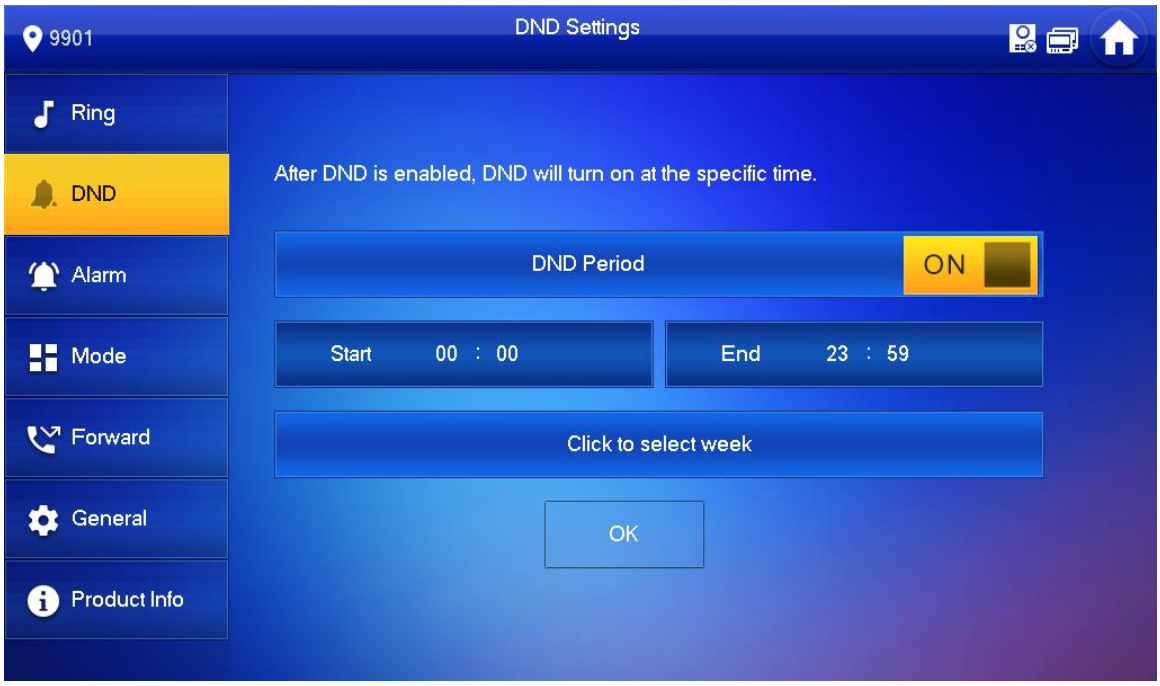


Figure 6-7

Step 5 Press time text box; set start time and end time.

Step 6 Press [Click to select week] and select DND week.

Step 7 Press [OK] to save settings.

6.2.3 Alarm Setting

Set wire zone, wireless zone and alarm output.

Zones can be set under disarm mode.

6.2.3.1 Wire Zone

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

Step 1 Press [Setting].

The system pops up “Password” prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to “6.2.6.3 Password Setting“ for details.

Step 3 Select “Alarm > Wire Zone”.

The system displays “Wire Zone” interface, as shown in Figure 6-8.

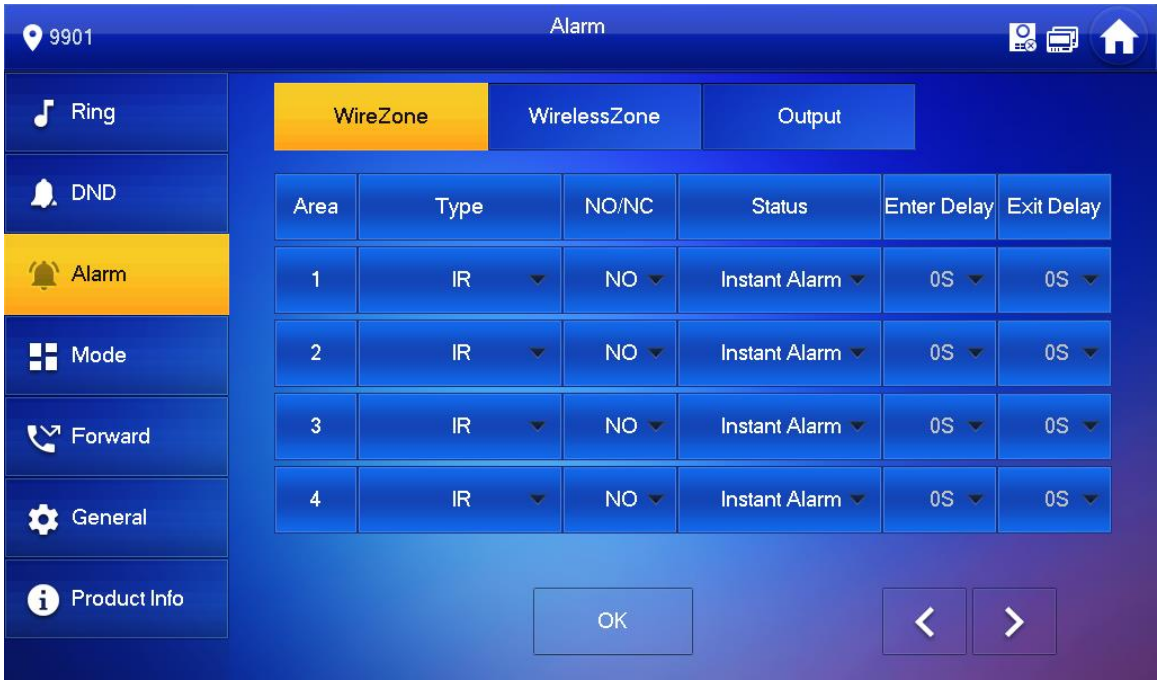


Figure 6-8

Step 4 Press corresponding positions to set area type, NO/NC, alarm status, enter delay and exit delay. Please refer to Table 6-3 for details.

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.

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>Status</td><td colspan="2">It includes instant alarm, delay alarm, bypass and remove.
● Instant alarm: in case of alarm after arm, produce alarm sound at once and enters alarm status.
● Delay alarm: in case of alarm after arm, enter alarm status after some time. Within the time period, you can disarm and cancel the alarm.
● Bypass: this area is shielded from this arm. After disarm, this area will restore normal working status.
● Remove: this area is invalid during arm/disarm.
Note
An zone under “Remove” status cannot be bypassed.</td></tr>
<tr><td>Enter Delay</td><td>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.</td><td rowspan="2">Delay is only valid to the areas of “delay alarm”.</td></tr>
<tr><td>Exit Delay</td><td>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.</td></tr>
</table>

Table 6-3

Step 5 Press [OK] to complete setting.

6.2.3.2 Wireless Zone

Only devices with wireless function have this function.

Add, delete and set wireless zones.

Step 1 Press [Setting].

The system pops up “Password” prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to “6.2.6.3 Password Setting“ for details.

Step 3 Select “Alarm > Wireless Zone”.

The system displays “Wireless Zone” interface, as shown in Figure 6-9.

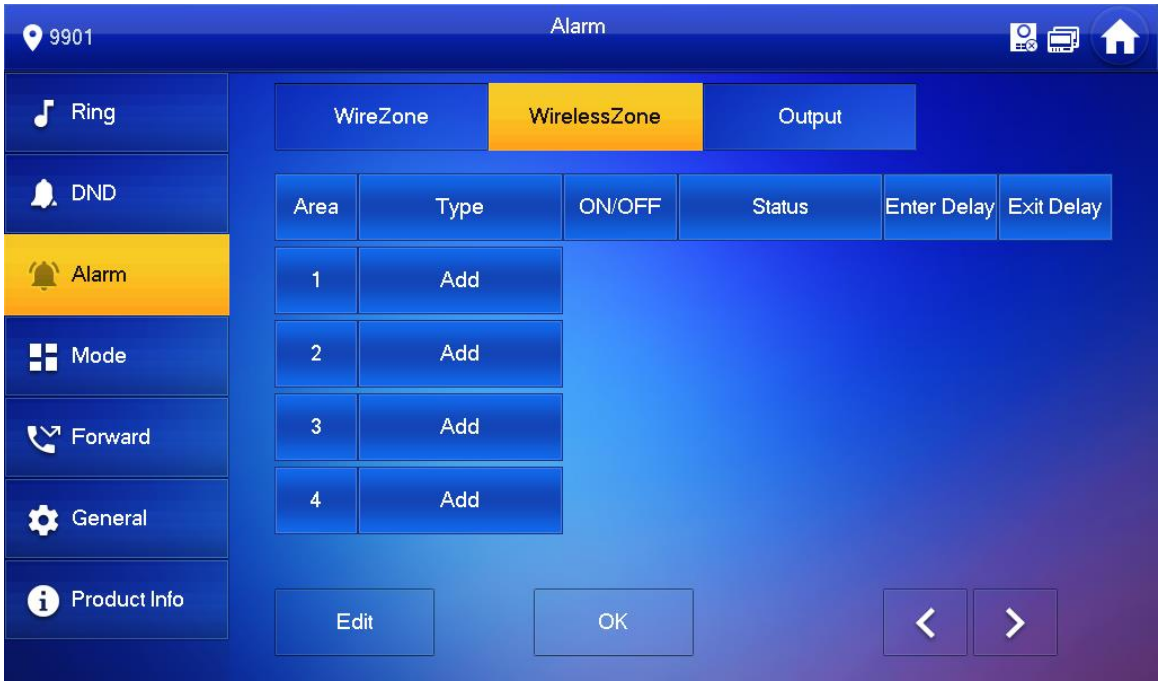


Figure 6-9

Step 4 Press [Add].

Step 5 Press wireless code button of wireless device. Please refer to wireless device user's manual for details.

After successful coding, display area info.

Step 6 Press corresponding positions to set alarm status, enter delay and exit delay. Please refer to Table 6-3 for details.

Press [Edit] to select a zone and press [Delete] to delete the selected area.

6.2.3.3 Alarm Output

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

Step 1 Press [Setting].

The system pops up "Password" prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to "6.2.6.3 Password Setting" for details.

Step 3 Select "Alarm > Output".

The system displays "Output" interface, as shown in Figure 6-10.

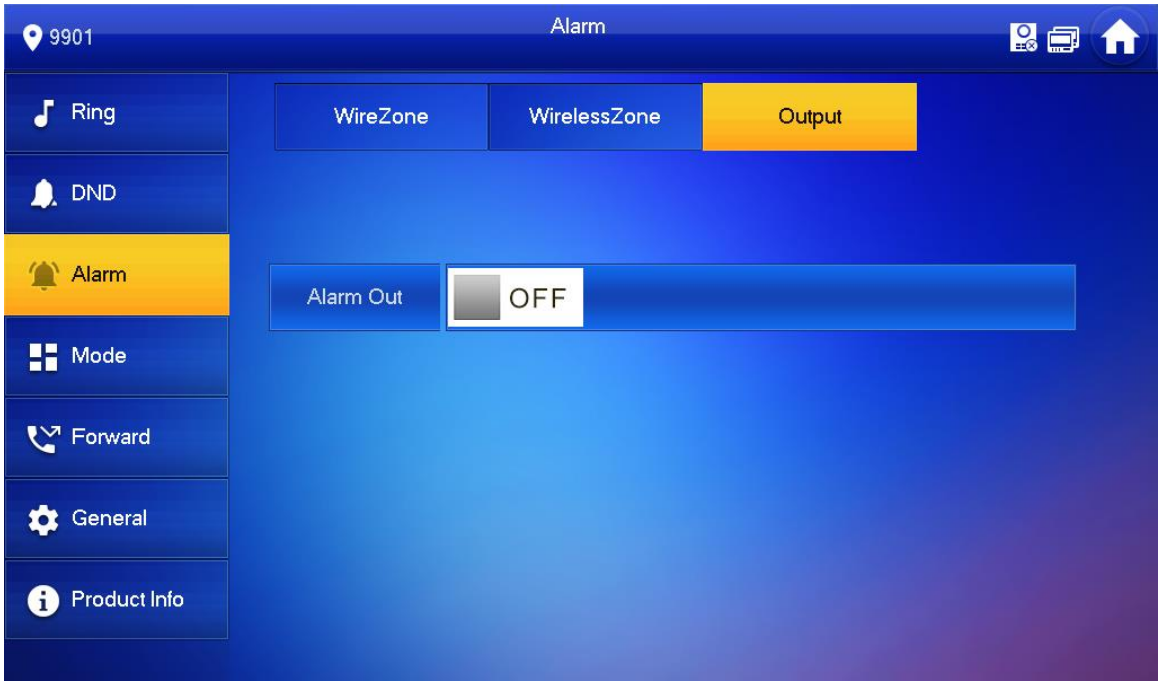


Figure 6-10

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

6.2.4 Mode Setting

Set area on/off status under different modes.

Area mode can be set only in disarm status.

Step 1 Press [Setting].

The system pops up “Password” prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to “6.2.6.3 Password Setting“ for details.

Step 3 Press [Mode].

The system displays “Mode” interface, as shown in Figure 6-11.

Figure 6-11

Step 4 Select arm mode in every tab.

Step 5 Press 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.

6.2.5 Forward Setting

Forward incoming calls.

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

Step 1 Press [Setting].

The system pops up “Password” prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to “6.2.6.3 Password Setting“ for details.

Step 3 Press [Forward].

The system displays “Forward” interface, as shown in Figure 6-12.

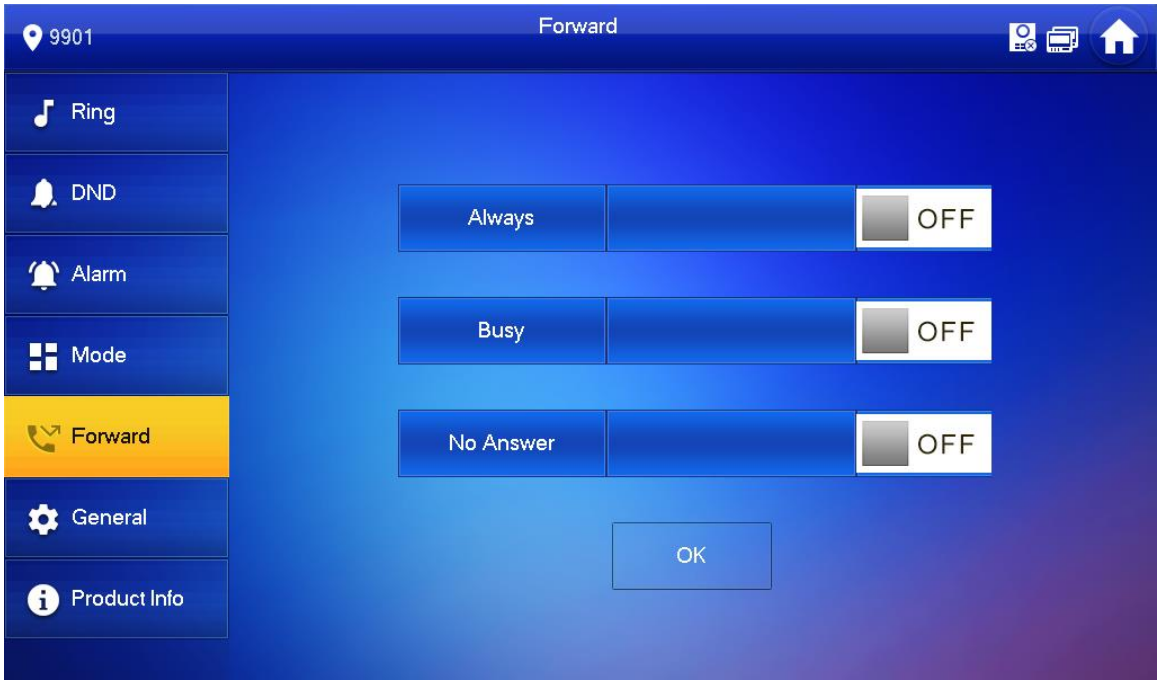


Figure 6-12

Step 4 Input VTH no. in the corresponding forward mode, press OFF to enable the forward function. Please refer to Table 6-4 for details.

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.

Table 6-4

- To forward to an user of another building or unit, the forward number is “Building + Unit + VTH room number”. For example, input 0101101 for 101 of Unit 1, Building 1.
- To forward to an user of the same unit, the forward number is VTH room number.

Step 5 Press [OK] to save settings.

6.2.6 General Setting

Set VTH time, display, password and others.

6.2.6.1 Time Setting

Set VTH system time, time zone and DST.

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

Step 1 Press [Setting].

The system pops up “Password” prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to “6.2.6.3 Password Setting“ for details.

Step 3 Select “General > Time”.

The system displays “Time” interface, as shown in Figure 6-13.

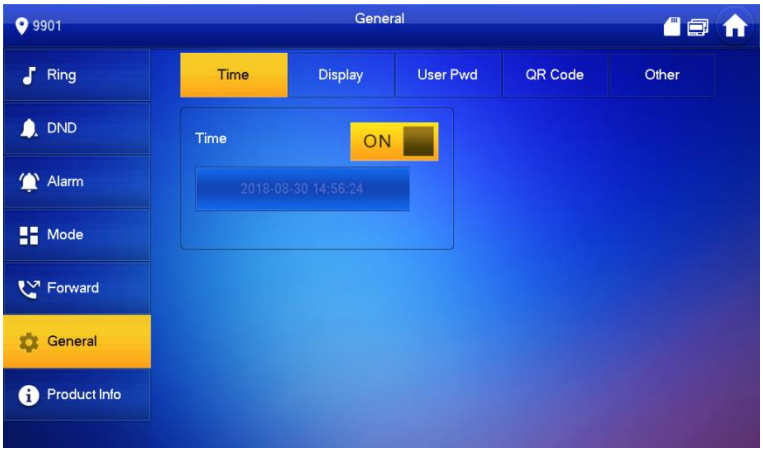


Figure 6-13

Step 4 Set time parameter.

When system time switch is ON, obtain server time by default; when it is OFF, set system time, time zone and DST manually.

- Manual setting of system time

1) Press ON of system time and the icon becomes OFF, so as to enable manual setting function.
2) Press time text box to set system time.

- Setting of time zone

1) Press ON of system time and the icon becomes OFF, so as to enable manual setting function.
2) Press time zone text box, and select local time zone, as shown in Figure 6-14.

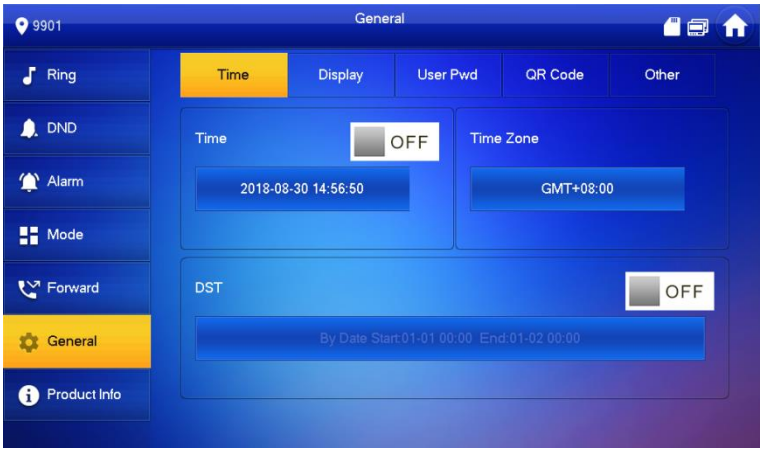


Figure 6-14

- DST setting

1) Press ON of system time and the icon becomes OFF, so as to enable manual setting function.

2) Press OFF to enable DST.

3) Press DST text box, and select DST start time and end time.

6.2.6.2 Display Setting

Set VTH screen brightness, screensaver time and clean.

Step 1 Press [Setting].

The system pops up “Password” prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to “6.2.6.3 Password Setting“ for details.

Step 3 Select “General > Display”.

The system displays “Display” interface, as shown in Figure 6-15.

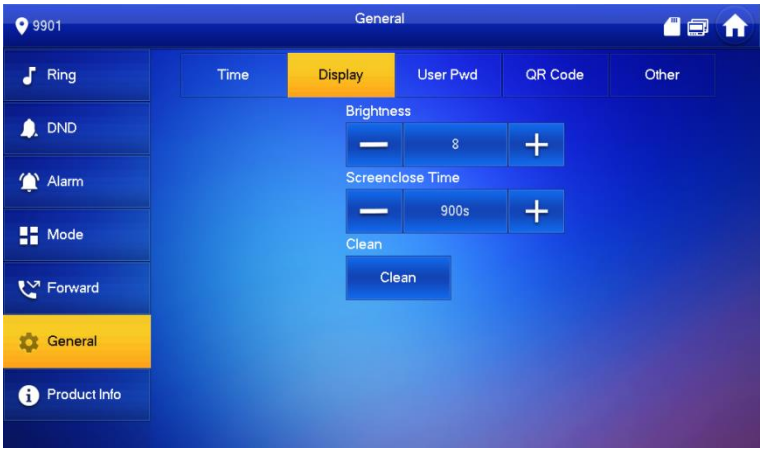


Figure 6-15

Step 4 Set parameters.

- Press + and −; set “Brightness” and “Screensaver Time”.

- Press [Clean] and the screen will be locked for 10 seconds. During the period, clean the screen. It restores after 10 seconds.

6.2.6.3 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 master VTH only, and extension VTH synchronizes with master VTH.

Step 1 Press [Setting].
The system pops up “Password” prompt box.

Step 2 Input login password and press [OK].

Step 3 Select “General > User Password”.
The system displays “User Password” interface, as shown in Figure 6-16.

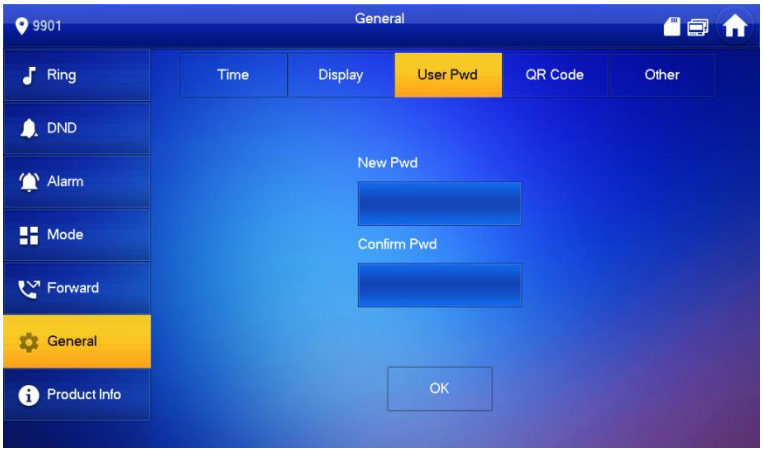


Figure 6-16

Step 4 Enter “New Password” and “Confirm Password”.

Step 5 Press [OK] to complete password modification.

6.2.6.4 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 master VTH and cannot be set.

Step 1 Press [Setting].
The system pops up “Password” prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to “6.2.6.3 Password Setting“ for details.

Step 3 Select “General > Other”.

The system displays “Other” interface, as shown in Figure 6-17.

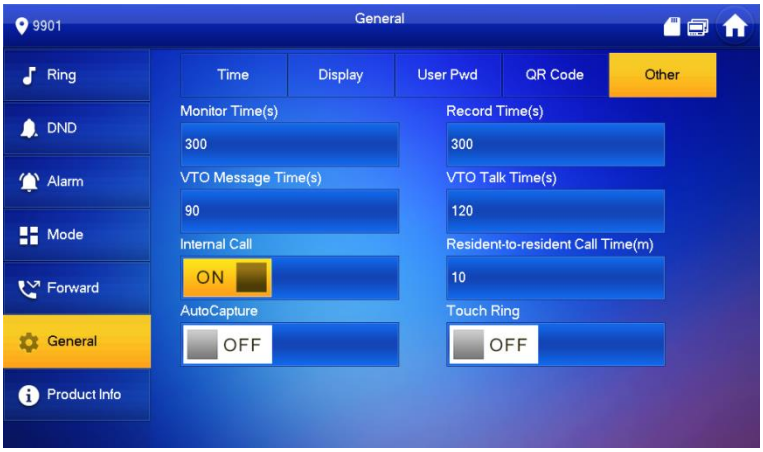


Figure 6-17

Step 4 Set parameters. Please refer to Table 6-5 for details.

Parameter	Description	Operation
Monitor Time	Maximum time to monitor VTO, IPC, fence station, HCVR, NVR and DVR.	Press + 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.	
TO Message Time	• When VTO message time is not 0: • If VTH with SD card doesn’t answer when VTO calls, enter message status according to prompt, and save the message in SD card of VTH. • If VTH doesn’t have SD card, but VTO has enabled “Leave Message Upload” and set FTP server, “Message” tab will appear at VTH info interface. If VTH doesn’t answer when VTO calls, enter message status according to prompt, and upload the message to FTP server. • If VTH doesn’t have SD card, and VTO has not enabled “Leave Message Upload”, if VTH doesn’t answer when VTO calls, hang up automatically. • When VTO message time is 0: Hang up automatically if VTH doesn’t answer when VTO calls, no matter whether VTH has SD card or not, no matter whether VTO has enabled “Leave Message Upload” or not. ⚠ 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.	

Parameter	Description	Operation
Resident-to-resident Call Time	Maximum talk time between VTH and VTH.	
VTO Talk Time	Maximum talk time when VTO calls VTH.	
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.	Press OFF to enable the function. The icon becomes ON.
Auto Capture	After auto capture is enabled, 3 pictures will be captured automatically when VTO calls VTH. View them at “Info > Record and Picture” interface. This function is valid only when SD card is inserted.	
Touch Ring	After enabling touch ring, there will be a ring when touching the screen.	

Table 6-5

6.2.7 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 Press [Setting].

The system pops up “Password” prompt box.

Step 2 Input login password and press [OK].

Default login password is 123456. Please refer to “6.2.6.3 Password Setting“ for details.

Step 3 Press [Product Info].

The system displays “Product Info” interface, as shown in Figure 6-18.

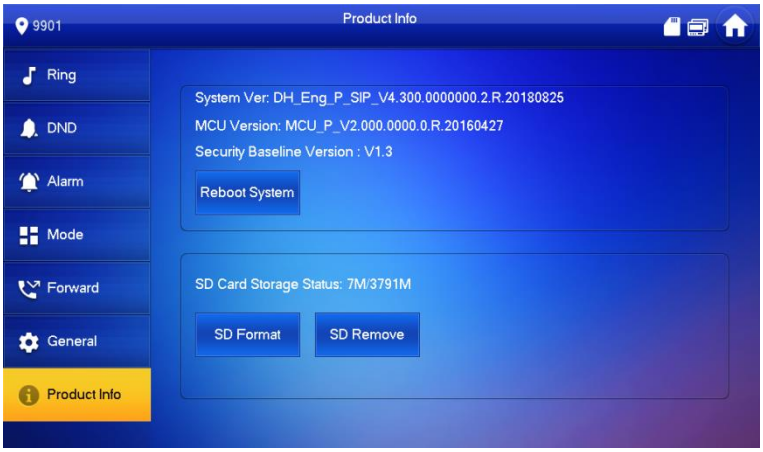


Figure 6-18

- Reboot

Press [Reboot] and press [OK] at prompt interface. The device will reboot.

- SD Format

Press [SD Format] and press [OK] at prompt interface. The SD card will be formatted.

6.3 Project Settings

6.3.1 Forget Password

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

6.3.1.1 Reset the Password at the Interface

Step 1 Press [Setting] for over 6 seconds.
The system pops up “Password” prompt box.

Step 2 Press [Forget Password].
The system displays “QR Code” interface, as shown in Figure 6-19.

Figure 6-19

Step 3 Scan the QR code with any code-scanning APP, bind your email box, send it by email to support_cpwd@htmicrochip.com, and thus obtain security code.

Step 4 Press [Next].

Step 5 Enter “Password”, “Confirm Password” and obtained “Security Code”.

Step 6 Press [OK] to complete resetting the password.

6.3.1.2 Reset the Password in VDPconfig

Use VDPconfig tool to export XML file (ExportFile.xml), send it by email to support_cpwd@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.

6.3.2 Network Settings

Set VTH network info according to actual conditions, since different types of devices support different access modes.

IP addresses of VTH and VTO shall be in the same network segment. Otherwise, VTH will fail to obtain VTO info after configuration.

Step 1 Press [Setting] for over 6 seconds.
The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and press [OK].

Step 3 Press [Network].
The system displays “Network” interface, as shown in Figure 6-20 or Figure 6-21.

Only devices with the wireless function can access to wireless network.

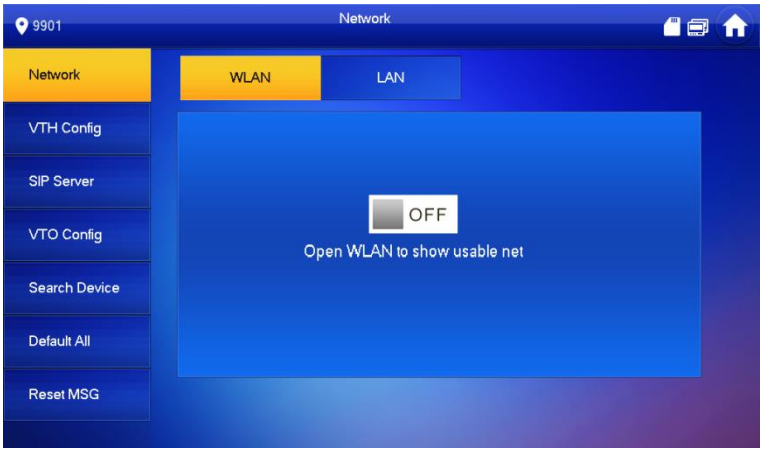


Figure 6-20

Figure 6-21

Step 4 Set according to actual network access mode.

- LAN

Enter “Local IP”, “Subnet Mask” and “Gateway” manually, press [OK]. Or press OFF to enable DHCP function and obtain IP info automatically.

If the device has wireless function, please click “LAN” tab to set it.

- WLAN

1) Press OFF to enable Wi-Fi function.

The system displays available Wi-Fi list, as shown in Figure 6-22.

Figure 6-22

2) Connect Wi-Fi.

The system has 2 access ways as follows.

◇ At “WLAN” interface, select Wi-Fi, click “Wireless IP” tab to enter “Local IP”, “Subnet Mask” and “Gateway”, and press [OK].

◇ At “WLAN” interface, select Wi-Fi, click “Wireless IP” tab, press OFF to enable DHCP function and obtain IP info automatically, as shown in Figure 6-23.

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

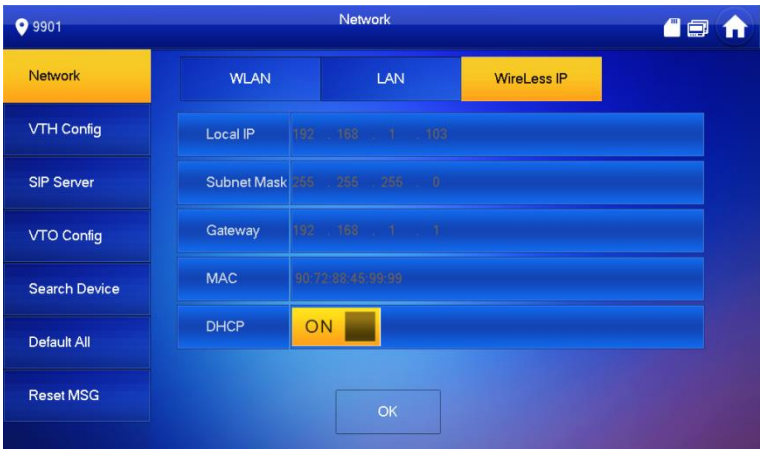


Figure 6-23

6.3.3 VTH Config

Configure VTH info.

VTH “Room No.” shall be the same with “VTH Short No.”, which is set at VTO WEB interface or Express/DSS platform server.

Step 1 Press [Setting] for over 6 seconds.

The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and press [OK].

Step 3 Press [VTH Config].

The system displays “VTH Config” interface, as shown in Figure 6-24.

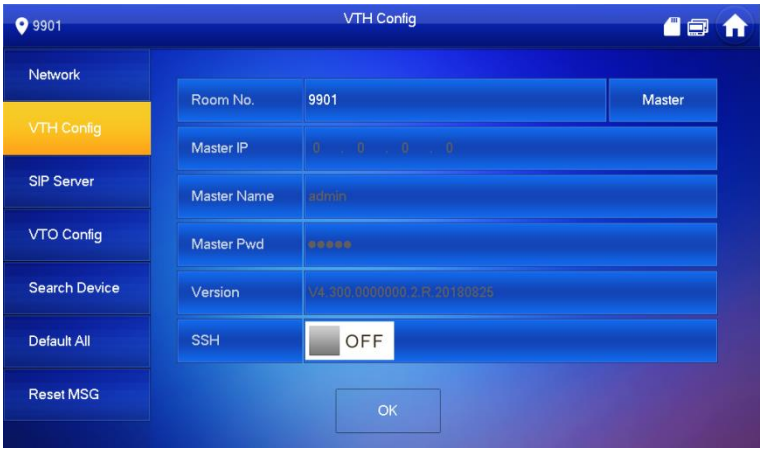


Figure 6-24

Step 4 Set VTH info.

- Be used as a master VTH.

Enter “Room No.” (such as 9901 or 101#0).

- “Room no.” shall be the same with “VTH Short No.”, which is set when adding VTH at WEB interface. Otherwise, it will fail to connect VTO.
- In case of extension VTH, room no. shall end with #0. Otherwise, it will fail to connect VTO.

- Be used as an extension VTH.

1) Press [Master] and switch to “Extension”.
2) Enter “Room No.” (such as 101#1) and “Master IP” (IP address of master VTH).

“User Name” and “Password” are the user name and password of master VTH. Default user name is admin, and the password is the one set during initialization.

Step 5 (Optional) press OFF to enable SSH.

After SSH is enabled, the debugging terminal connects VTH through SSH protocol, so as to operate and debug it.

Step 6 Press [OK] to save settings.

6.3.4 VTO Config

Add VTO and fence station info, and bind VTH with VTO on the VTH side.

Step 1 Press [Setting] for over 6 seconds.

The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and press [OK].

Step 3 Press [VTO Config].

The system displays “VTO Config” interface, as shown in Figure 6-25.

Figure 6-25

Step 4 Add VTO or fence station.

- Add main VTO.

1) Enter main VTO name, VTO IP, “User Name” and “Password”.

2) Switch the “Enable Status” to be ON.

“User Name” and “Password” shall be consistent with WEB login user name and password of VTO. Otherwise, it will fail to connect.

- Add sub VTO or fence station.

1) Enter sub VTO/fence station name, IP address, “User Name” and “Password”.

2) Switch the “Enable Status” to be ON.

Press < / > to add more sub VTOs/ fence stations.

6.3.5 Default

All parameters of the device, except IP address, can be restored to initial default values.

Step 1 Press [Setting] for over 6 seconds.
The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and press [OK].

Step 3 Press [Default].
The system displays “Default” interface.

Step 4 Press [OK].
The device reboots and enters initialization interface, representing successful restoration.

6.3.6 Reset MSG

Modify the bonded Email.

Step 1 Press [Setting] for over 6 seconds.
The system pops up “Password” prompt box.

Step 2 Enter the password set during initialization, and press [OK].

Step 3 Press [Reset MSG].

The system displays “Reset MSG” interface, as shown in Figure 6-26.

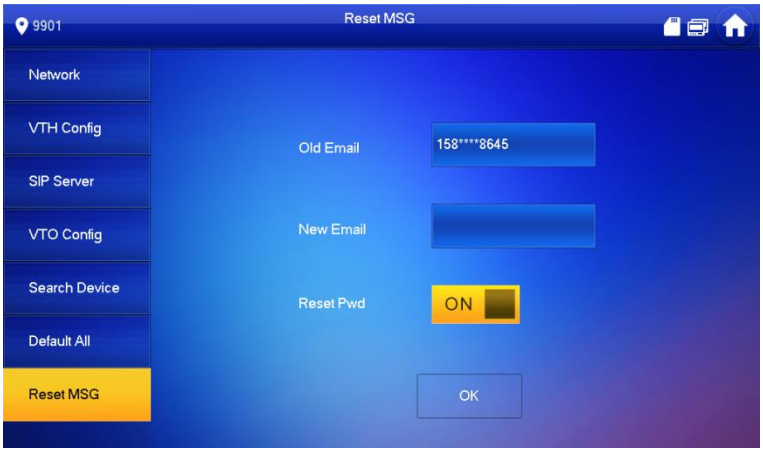


Figure 6-26

Step 4 Enter “New Email” and press [OK].

The Email will obtain security code during password resetting. For details, please refer to “6.3.1 Forget Password“.

6.4 Call

Manage contact, call users and view the latest call log.

6.4.1 Contact

Add and edit VTH and extension number.

Select “Call > Contact”, and the system displays “Contact” interface, as shown in Figure 6-27.

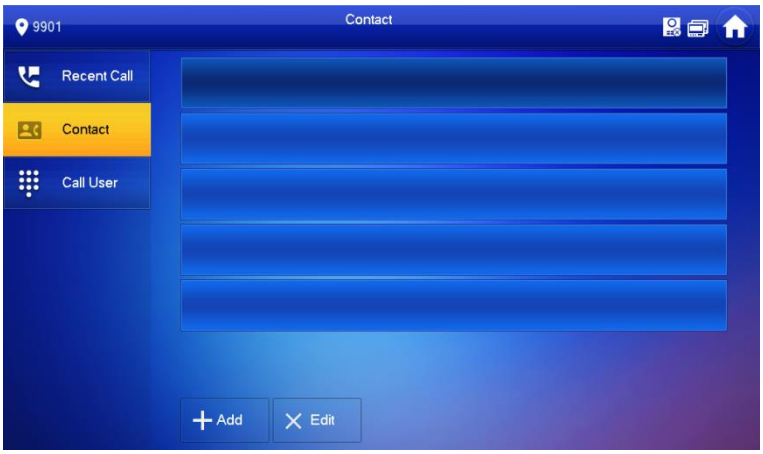


Figure 6-27

6.4.1.1 Add User

Step 1 Press [Add].

The system displays “User Info” interface, as shown in Figure 6-28.

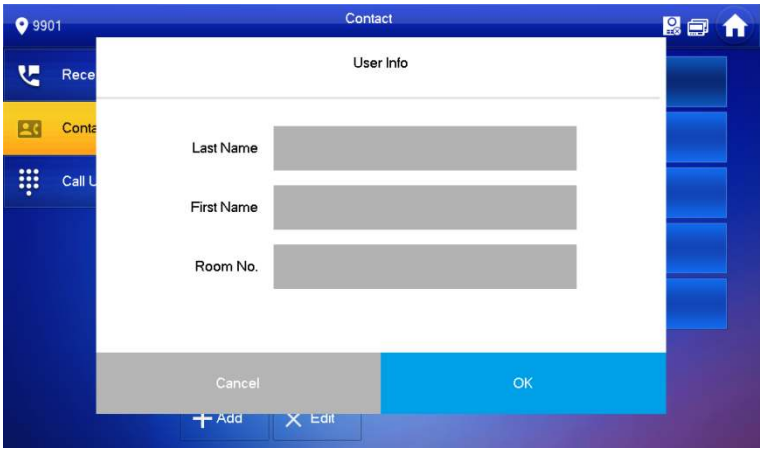


Figure 6-28

Step 2 Enter “Last Name”, “First Name” and “Room No.” of contact person.

Step 3 Press [OK] to complete adding.

6.4.1.2 Edit Contact Info

Select the contact person, press to edit the info.

6.4.1.3 Delete Contact Person

Press [Edit], select the contact person and press [Delete] to delete the contact person.

Multiple contact persons can be selected once.

6.4.2 Call User

- Make sure that resident-to-resident call function has been enabled. Please refer to “6.2.6.4 Other Settings“ for details.
- Call function is used by VTH to call VTH.
- If both VTHs have a camera, bilateral video call can be provided.

6.4.2.1 Dial and Call User directly

At “Call User” interface, dial and call the user.

Step 1 Select “Call > Call User”.

The system displays “Call User” interface, as shown in Figure 6-29.

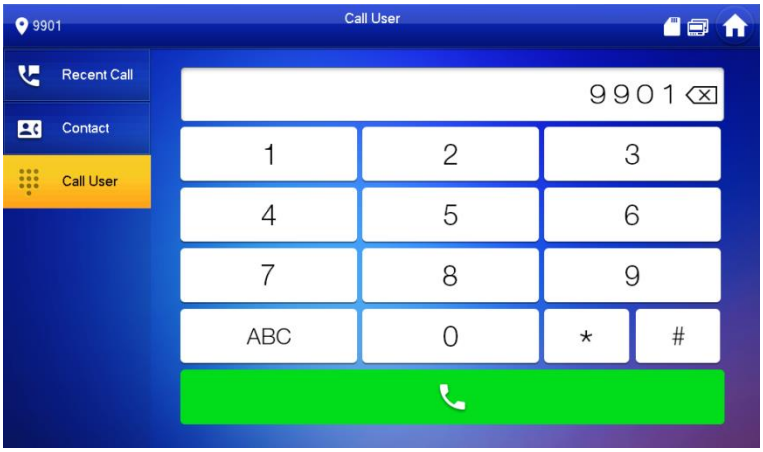


Figure 6-29

Step 2 Enter the user's room no. (VTH room no.).

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

Step 3 Press to start.

The system displays calling interface, as shown in Figure 6-30. After the user answers the call, both parties talk to each other, as shown in
Figure 6-31. For interface key description, please refer to Table 6-6.

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

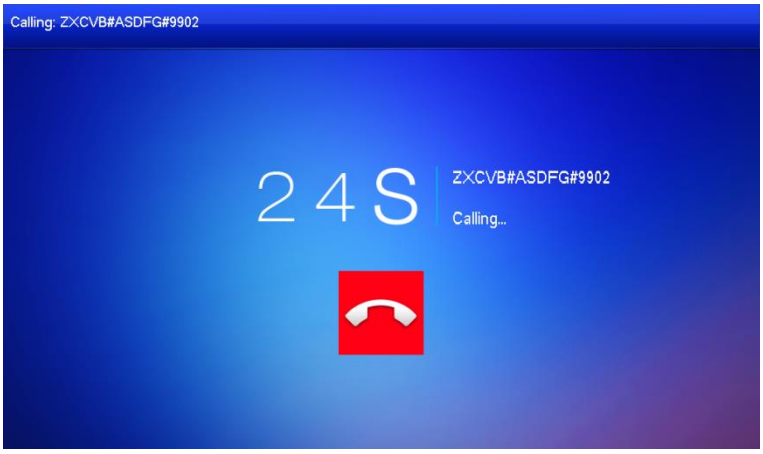


Figure 6-30

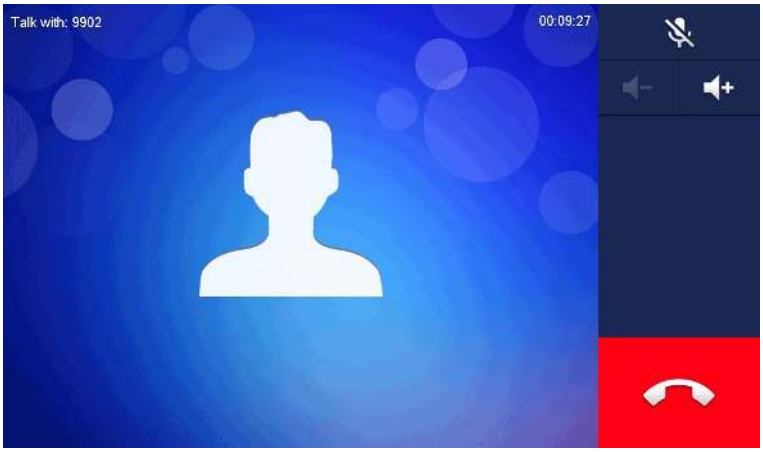


Figure 6-31

6.4.2.2 Call User in Contact

Please add contact persons to the contact, by reference to “6.4.1.1 Add User“.

Step 1 Select “Call > Contact”.

Step 2 Select the one you want to call.

Step 3 Press to start.

6.4.3 Call from User

When another VTH calls this VTH, the call interface will be displayed, as shown in Figure 6-32.

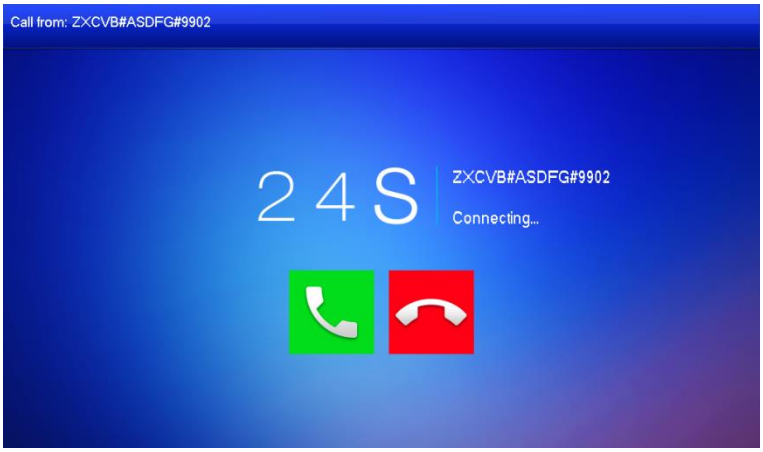


Figure 6-32

- Press to talk with each other, as shown in Figure 6-33. For key description, please refer to Table 6-6.
- Press to hang up.

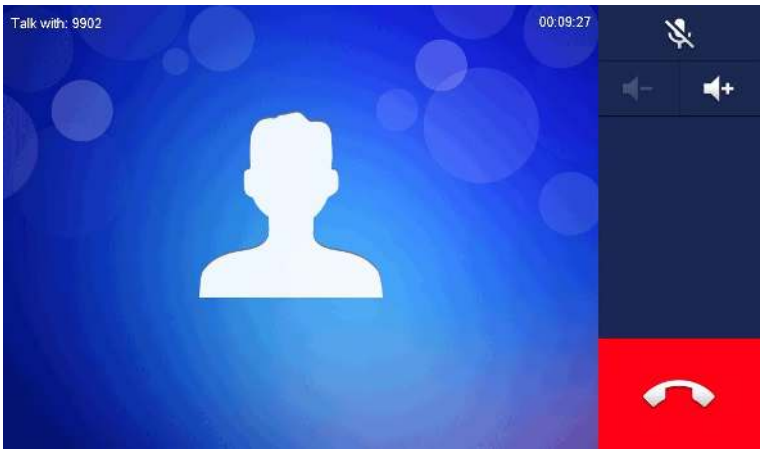


Figure 6-33

6.4.4 Call from VTO

Step 1 Dial VTH room no. (such as 9901) at VTO, to call VTH.
VTH pops up a waiting picture, as shown in Figure 6-34.

Step 2 At VTH interface, press [Answer].
Answer the call and talk with each other. For key description, please refer to Table 6-6.

Figure 6-34

Key	Description
	Press this key to unlock the VTO remotely. The system provides 2-channel unlock function. If the icon is gray, it means that unlock function of this channel is not available.
	This key means to talk with the opposite end device. Press this key to prohibit talking; press it again to switch back to talking status.
	Press this key to select IPC in “Favorite” that shall be monitored.
	Press this key to snapshot. This key is gray if SD card is not installed.
	Press this key to record. Complete recording when the call is completed or by pressing . Videos are stored in SD card of this VTH. If SD card is full, the earlier videos will be covered. This key is gray if SD card is not installed.
	Press this key to reduce volume.
	Press this key to increase volume.
	Press this key to answer and talk.
	Press this key to refuse.

Table 6-6

6.4.5 Recent Call

View and manage the missed call, accepted call and called log of this VTH. Meanwhile, call back the contact persons. Select “Call > Recent Call”, and the system displays “Recent Call” interface.

In case of missed call, press on the front panel and enter recent call interface.

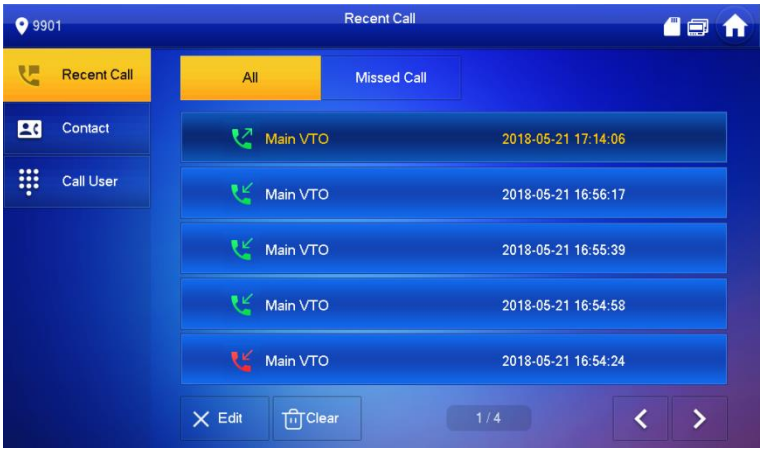


Figure 6-35

6.4.5.1 Callback

Select the recent call of required VTH, press [Call] to call the contact person.

6.4.5.2 Delete

Press [Edit], select a recent call record and press [Delete] to delete it.

6.4.5.3 Clear

Press [Clear] to clear all recent calls in this tab.

6.5 Monitor

VTH is able to monitor VTO, fence station or IPC.

6.5.1 Monitoring of VTO

Please confirm user name and password in VTH, which are set when adding VTO. They shall be consistent with WEB login user name and password of VTO. Otherwise, it will fail to obtain videos during monitoring.

VTH is able to monitor VTO or fence station. Under the condition of monitoring, press call key on the front panel to talk to VTO. VTO will pick up the call automatically.

Step 1 Select “Monitor > VTO”.

The system displays the list of added VTO and fence station, as shown in Figure 6-36.

Press to add frequently-used VTO or fence station to favorite, which will be displayed in “Favorite” tab, so as to switch videos during monitoring.

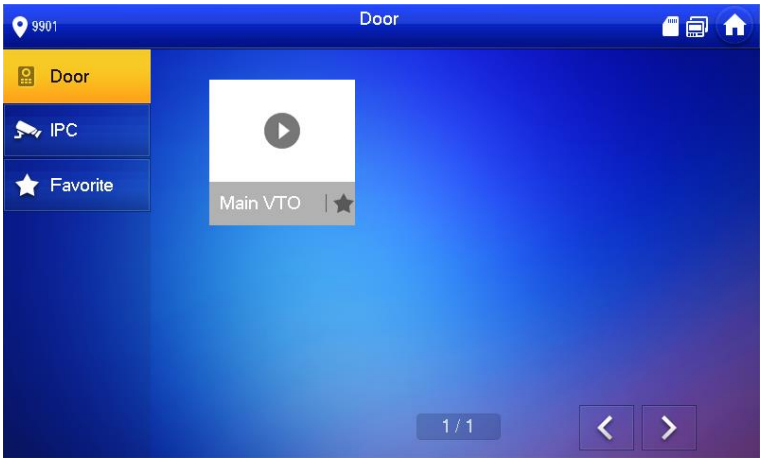


Figure 6-36

Step 2 Press to select VTO that shall be monitored.

The device enters monitoring, as shown in Figure 6-37. For relevant monitoring operations, please refer to Table 6-7.

Icon	Description	
/	Press this key to unlock VTO remotely. The system provides 2-channel unlock function. If the icon is gray, it means that unlock function of this channel is not available.	
	Press this key to snapshot. This key is gray if SD card is not installed.	
	Press this key to record. Complete recording when the call is completed or by pressing . Videos are stored in SD card of this VTH. If SD card is full, the earlier videos will be covered. This key is gray if SD card is not installed.	
/	If VTH connects multiple VTO/IPC, press and to switch to last/next channel.	
	Press this key to cancel monitoring.	
	Press this key to speak to the other end device. Press this key to start and the icon becomes . Press it again to complete.	

Table 6-7

Speak to VTO directly after successful monitoring.

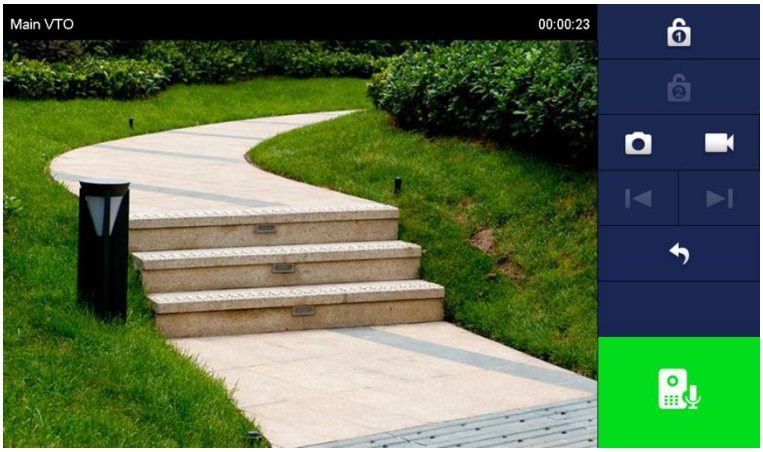


Figure 6-37

Icon	Description
/	Press this key to unlock VTO remotely. The system provides 2-channel unlock function. If the icon is gray, it means that unlock function of this channel is not available.
	Press this key to snapshot. This key is gray if SD card is not installed.
	Press this key to record. Complete recording when the call is completed or by pressing . Videos are stored in SD card of this VTH. If SD card is full, the earlier videos will be covered. This key is gray if SD card is not installed.
/	If VTH connects multiple VTO/IPC, press and to switch to last/next channel.
	Press this key to cancel monitoring.
	Press this key to speak to the other end device. Press this key to start and the icon becomes . Press it again to complete.

Table 6-8

6.5.2 Monitoring of IPC

Please add IPC before monitoring of IPC.

6.5.2.1 Add IPC

- IPC added at main VTO and Express/DSS “IPC” interface will be synchronized to VTH. The synchronized IPC cannot be deleted.
- Before adding IPC, please ensure that IPC has been powered on, and connected to the same network with VTH.

Step 1 Select “Monitor > IPC”.

The system displays “IPC” interface, as shown in Figure 6-38. Press to add frequently-used IPC to favorites, which will be displayed in “Favorite” tab, so as to switch videos during monitoring.

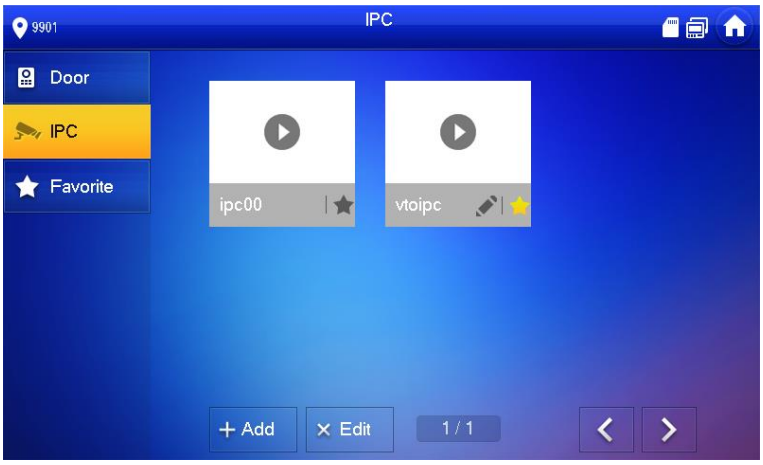


Figure 6-38

Step 2 Press [Add].

The system displays “Add IPC” interface, as shown in Figure 6-39.

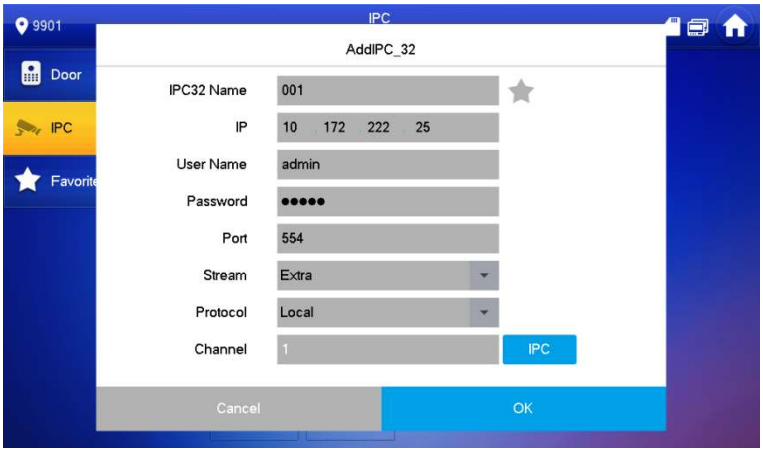


Figure 6-39

Step 3 Please refer to Table 6-9 to configure camera parameters.

Parameter	Description
IPC	Press this key to select IPC, NVR, DVR and HCVR. ● Select IPC, meaning that VTH obtains video stream from the connected IPC directly. It is necessary to configure IPC info. ● Select NVR/DVR/HCVR, meaning that VTH obtains IPC video stream from the connected device. It is necessary to configure info about the connected device.
IPC32 Name	Input IPC/NVR/DVR/HCVR name.
IP	Input IP address of the connected IPC/NVR/DVR/HCVR.
User Name	Input user name and password to login WEB interface of IPC/NVR/DVR/HCVR.
Password	
Port	Default port is 554.
Stream	Select stream type according to needs, including main stream and extra stream. ● Main stream: large stream, high definition, large occupied bandwidth, suitable for local storage. ● Extra stream: relatively smooth image, small occupied bandwidth, suitable for network transmission with low bandwidth.

Parameter	Description
Protocol	It includes local protocol and Onvif protocol. Please select according to the protocol of the connected device.
Channel	● If IPC is connected, default setting is 1. ● If NVR/XVR/HCVR is connected, set channel number of IPC on NVR/XVR/HCVR.

Table 6-9

Step 4 Press [OK] to finish.

6.5.2.2 Modify IPC

Modify IPC info.

Step 1 Select “Monitor> IPC”.

The system displays “IPC” interface.

Step 2 Press of IPC.

Step 3 Modify IPC parameters. Please refer to Table 6-9 for details.

Step 4 Press [OK] to finish.

6.5.2.3 Delete IPC

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

Step 1 Select “Monitor> IPC”.

The system displays “IPC” interface.

Step 2 Press [Edit].

Step 3 Select IPC.

Step 4 Press [Delete] to delete the selected IPC.

6.5.2.4 Monitor IPC

Monitor the IPC.

Step 1 Select “Monitor> IPC”.

The system displays “IPC” interface.

Step 2 Select IPC to be monitored, and press .

The system displays monitoring interface, as shown in Figure 6-40.

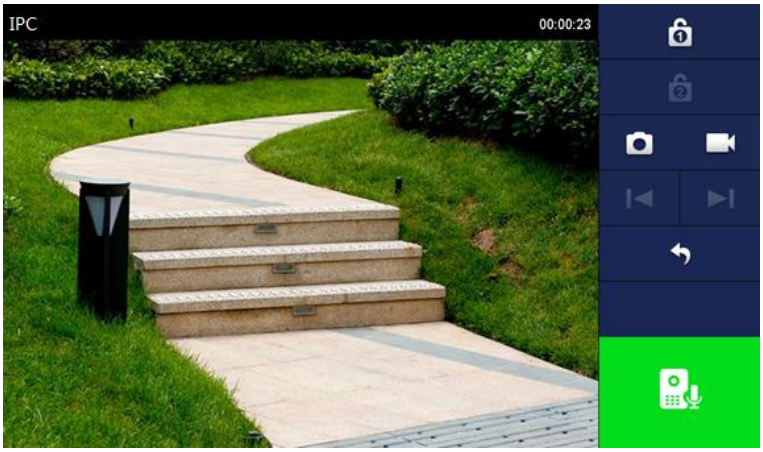


Figure 6-40

Step 3 Please monitor the VTO by reference to Table 6-8.

6.5.3 Favorite

Display 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 null.

Step 1 Select “Monitor> Favorite”.

The system displays “Favorite” interface, as shown in Figure 6-41.

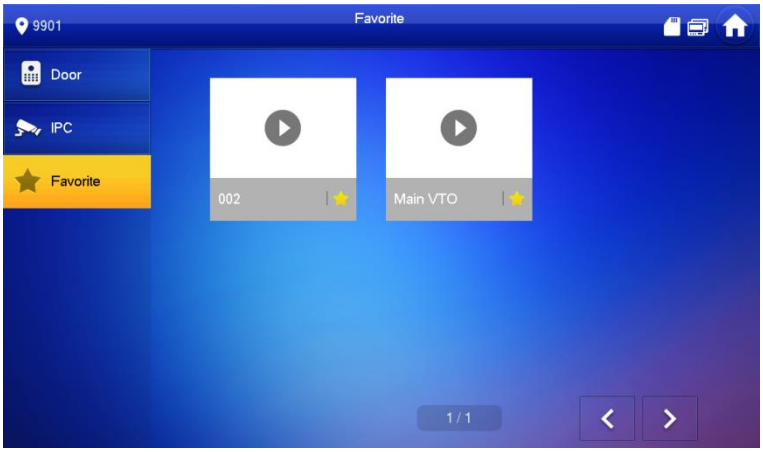


Figure 6-41

Step 2 Select the device to be monitored, and press .

The system displays monitoring interface. In case of multiple devices in “Favorite” tab, press / to switch and monitor them.

6.6 SOS

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

In emergency, press SOS button on the front panel, or press [SOS] at the main interface to call management center.

6.7 Info

6.7.1 Security Alarm

All alarm info is stored in the device.

When an alarm is triggered, there will be 15s alarm sound. Pop up alarm prompt interface, as shown in Figure 6-42, and upload the alarm info to alarm record interface and management platform.

Figure 6-42

Alternatively, select “Info > Security Alarm”, and the system displays “Security Alarm” interface, as shown in 错误!未找到引用源。. “All” tab displays all alarm info of the system, whereas “Unread” tab displays unread alarm info.

- Press [Edit] to select the info; press [Delete] to delete the selected info.
- Press [Clear] to delete all records after confirmation.

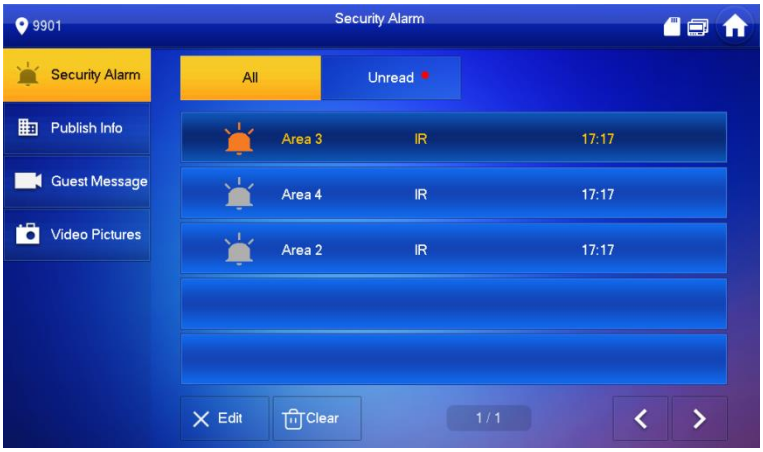


Figure 6-43

6.7.2 Guest Message

- When a SD card is inserted into the device, this function is valid. All messages are stored in SD card.
- If SD card is not inserted, but VTO WEB has set FTP and selected “Video-audio Message Uploading”, this function is valid too. All messages will be uploaded to FTP.

Select “Info > Guest Message”, and the system displays “Guest Message” interface, as shown in Figure 6-44. “All” tab displays all messages of the system, whereas “Unread” tab displays unread messages.

- Press [Edit] to select the info; press [Delete] to delete the selected info.
- Press [Clear] to delete all messages after confirmation.

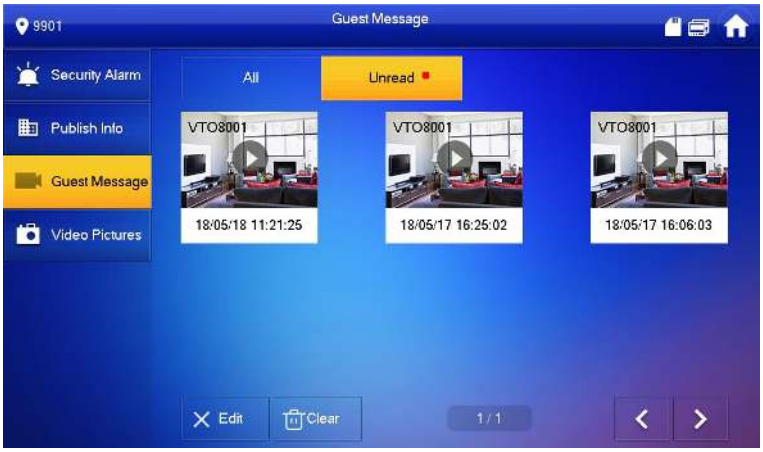


Figure 6-44

6.7.3 Publish Info

Info released by the management center is stored in the device, and pictures, if any, are stored in FTP card.

Select “Info > Publish Info”, and the system displays “Publish Info” interface, as shown in Figure 645. “All” tab displays all info of the system, whereas “Unread” tab displays unread info.

- Press [Edit] to select the info; press [Delete] to delete the selected info.
- Press [Clear] to delete all info after confirmation.

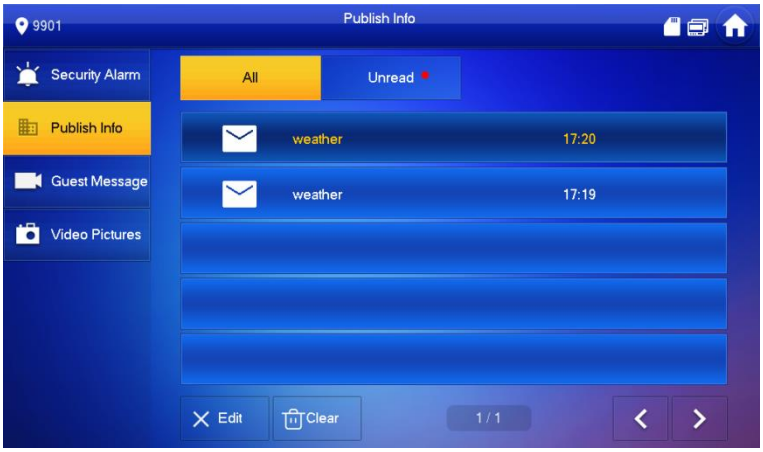


Figure 6-45

6.7.4 Video Pictures

When a SD card is inserted into the device, this function is valid. All videos and pictures are stored in SD card.

Select “Info > Video Pictures”, and the system displays “Video Pictures” interface, as shown in Figure 6-.

- Press [Edit] to select the video or picture; press [Delete] to delete the selected video or picture.
- Press [Clear] to delete all videos and pictures after confirmation.

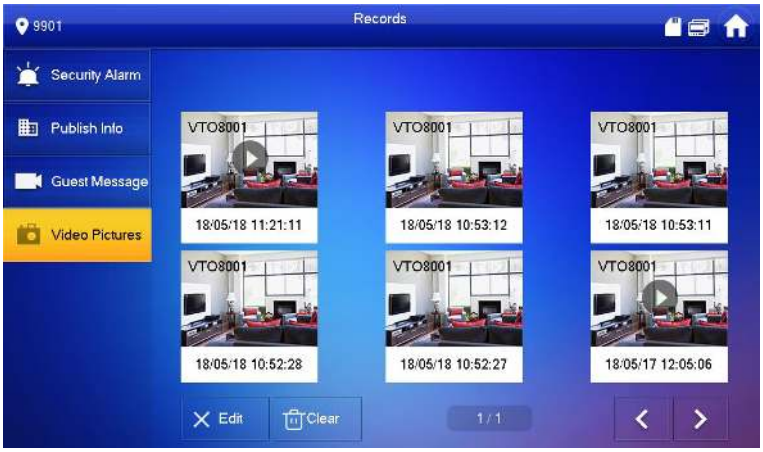


Figure 6-46

6.8 Unlock Function

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

6.9 Arm and Disarm Function

6.9.1 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 Press at the main interface.

The system displays arm mode, as shown in Figure 6-47.

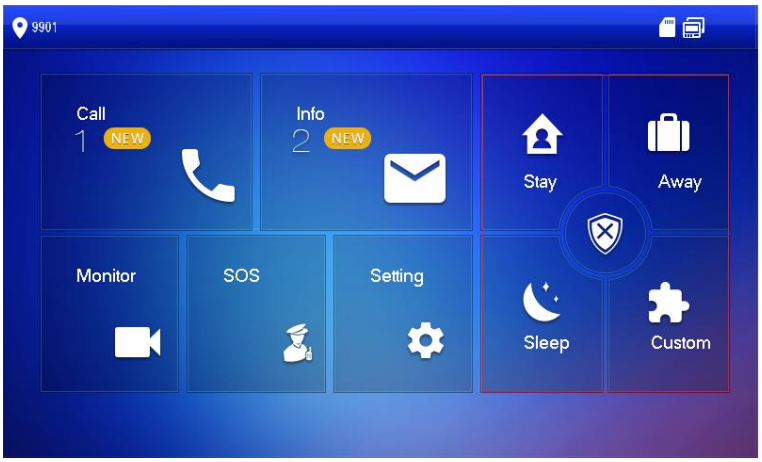


Figure 6-47

Step 2 Select arm mode.

The system displays password input interface.

Step 3 Enter arm and disarm password; press [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 “6.2.6.3 Password Setting“ for details.
- If delay alarm is set in the area, the device will beep continuously at the end of exit delay time.

6.9.2 Disarm

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

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

The system displays password input interface.

Step 2 Enter arm and disarm password; press [OK].

The system displays successful disarm.

- Default password of arm and disarm is 123456. Please refer to “6.2.6.3 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.

7 DSS Mobile for VDP

You can download the DSS mobile app and bind your VTH to the app to unlock the door, talk to the connected VTO devices, call the management center, and view call records and messages.

7.1 Downloading the App

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

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

The **Password Verification** dialog box is displayed.

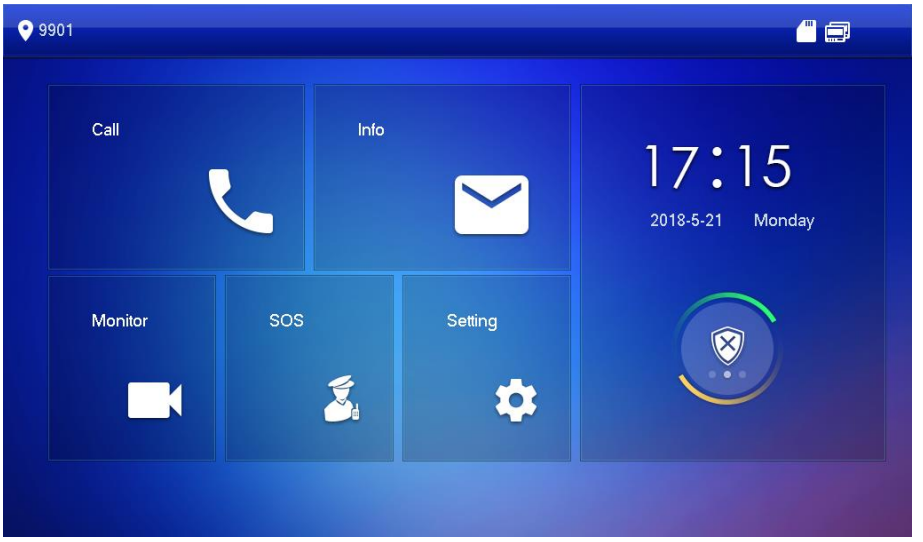


Figure 7-1

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

The **Register** code and **Download** code are displayed.

Step 3 Scan the **Download** code with your smart phone to download and install the app.

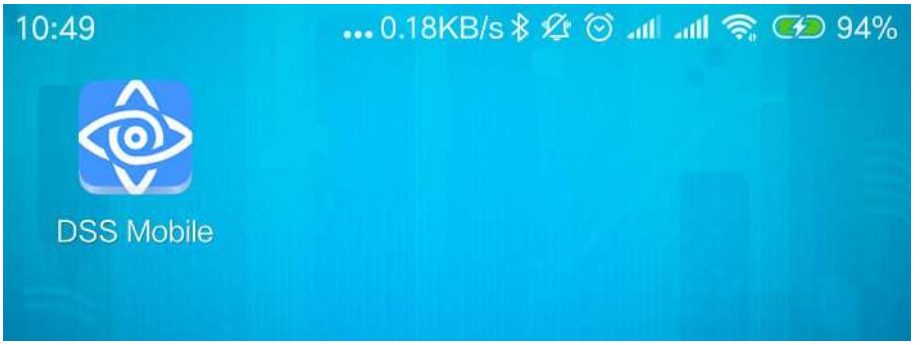


Figure 7-2

7.2 Registration and Login

Step 1 Run the app, then accept the **End-User License Agreement**, and then allow the permissions for the app.

The **Registration** interface is displayed.

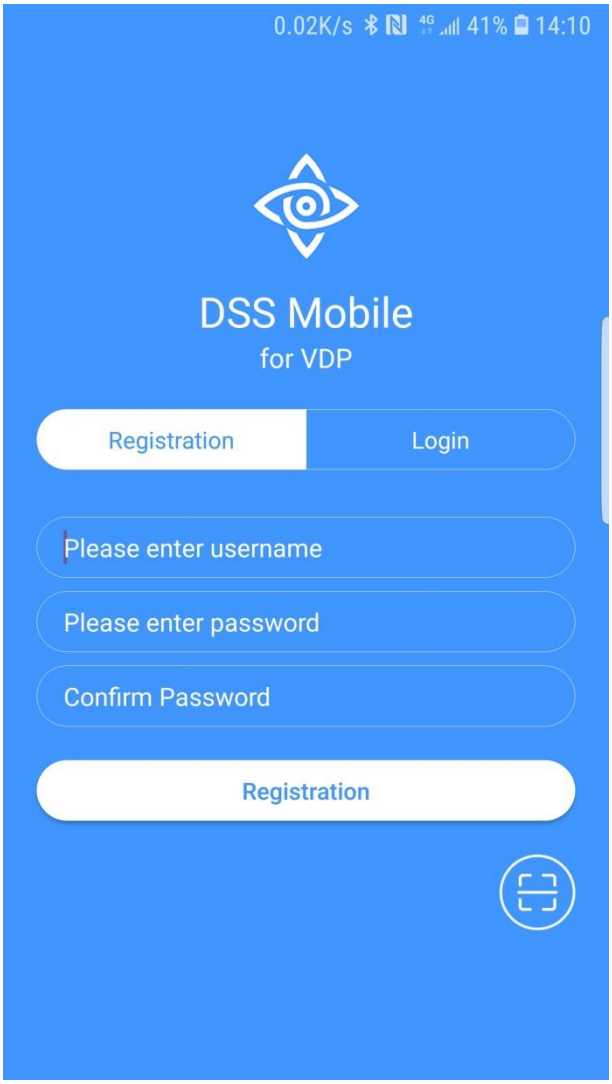


Figure 7-3

Step 2 Tap , and then scan the **Register** code on the VTH. See “Step 2“ in “7.1 Downloading the App“.

The IP address and port number of your DSS server is displayed.

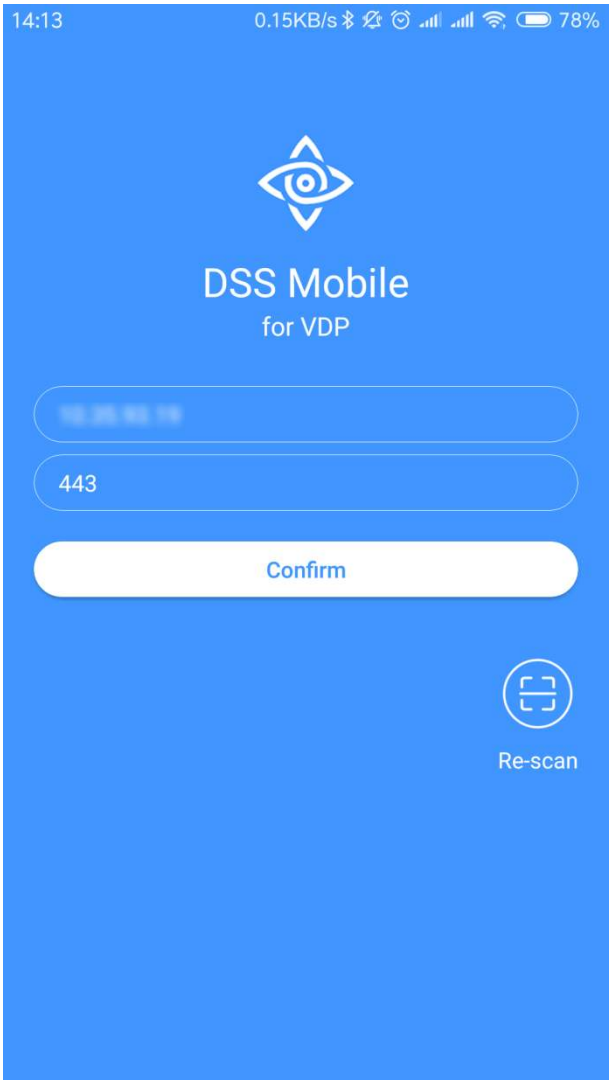


Figure 7-4

Step 3 Tap **Confirm**, then Input the user name and password you need, and then tap **Registration**. You can register 5 users on a VTH at most.

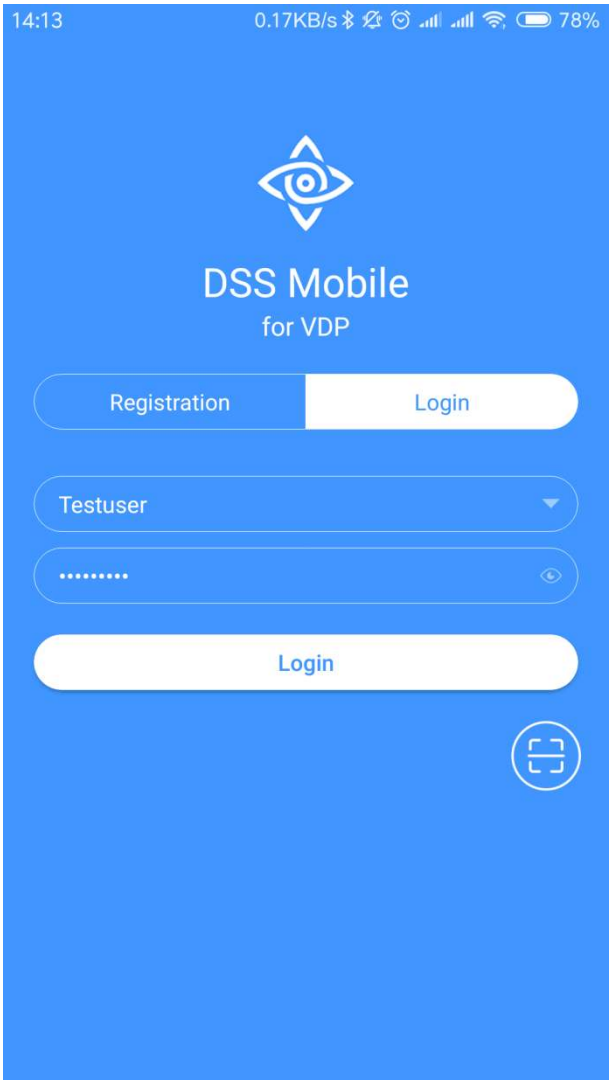


Figure 7-5

Step 4 Tap **Login**.

The **Login** interface is displayed.

Step 5 Input the user name and password you registered, and then tap **Login**.

The **Call Records** interface is displayed.

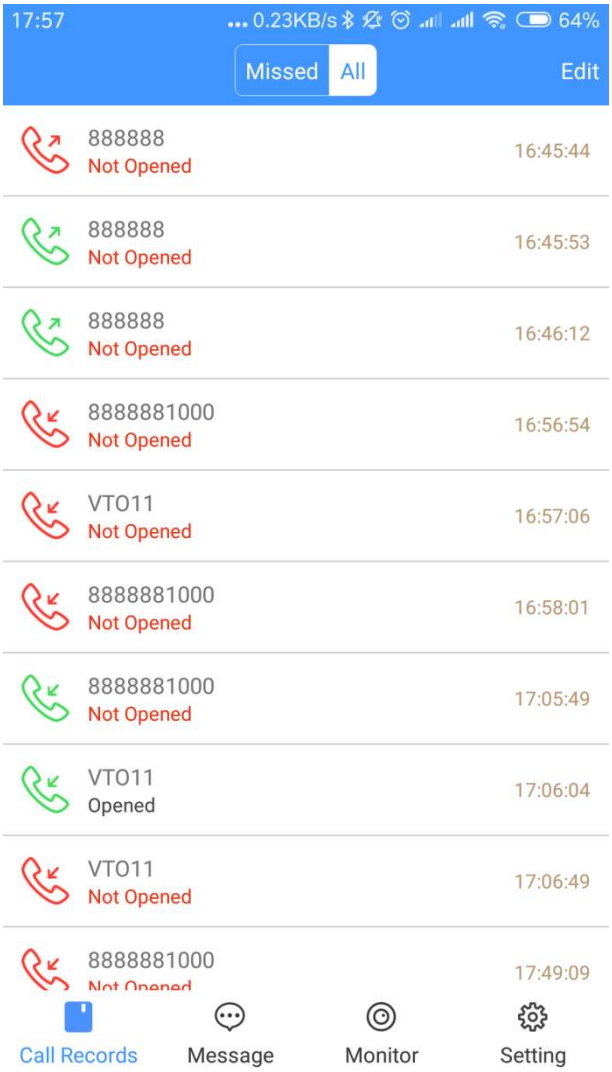

17:57
0.23KB/s
64%
Missed
All
Edit
888888
Not Opened
16:45:44
888888
Not Opened
16:45:53
888888
Not Opened
16:46:12
8888881000
Not Opened
16:56:54
VTO11
Not Opened
16:57:06
8888881000
Not Opened
16:58:01
8888881000
Not Opened
17:05:49
VTO11
Opened
17:06:04
VTO11
Not Opened
17:06:49
8888881000
17:49:09
Call Records
Message
Monitor
Setting

Figure 7-6

7.3 Call Functions

7.3.1 Configuring Call Forward

Confirm your SIP ID, and then configure call forward on the VTH. If any device is calling the VTH, you will receive the call on the phone.

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

The **Settings** interface is displayed, and the **SIP ID** here is **3#1#1001#115**.

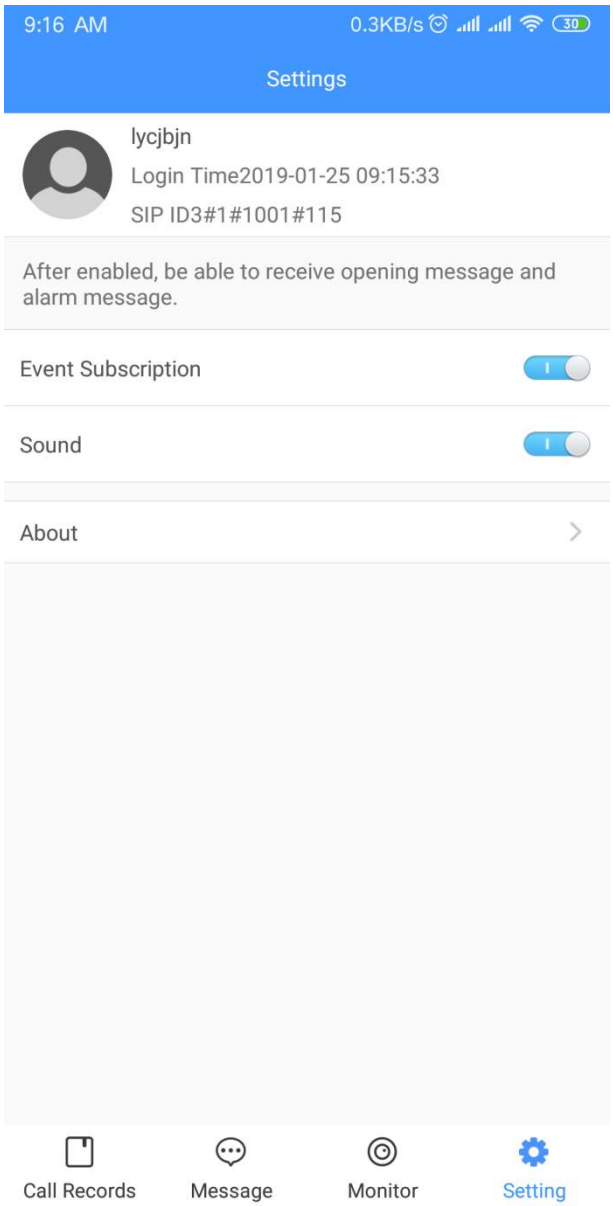


Figure 7-7

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

The **Password Verification** dialog box is displayed.

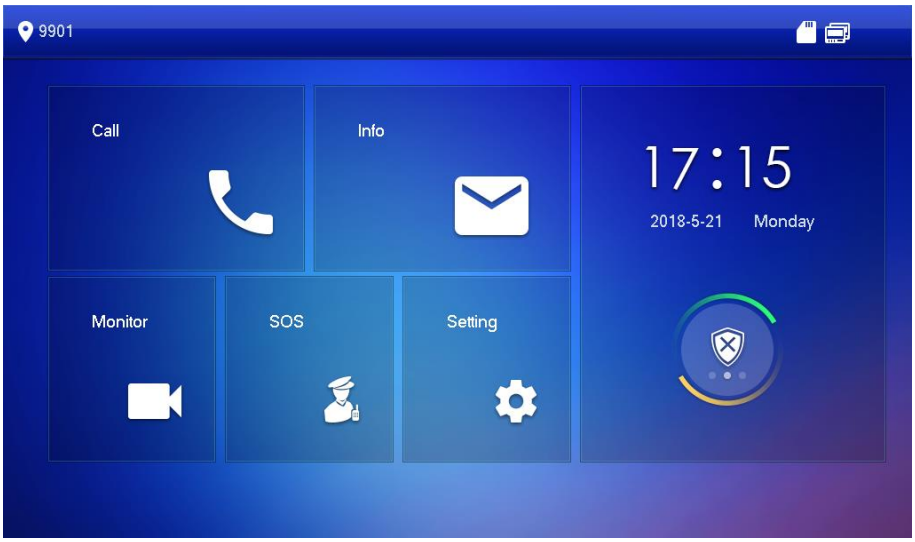


Figure 7-8

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

The **Forward** interface is displayed.

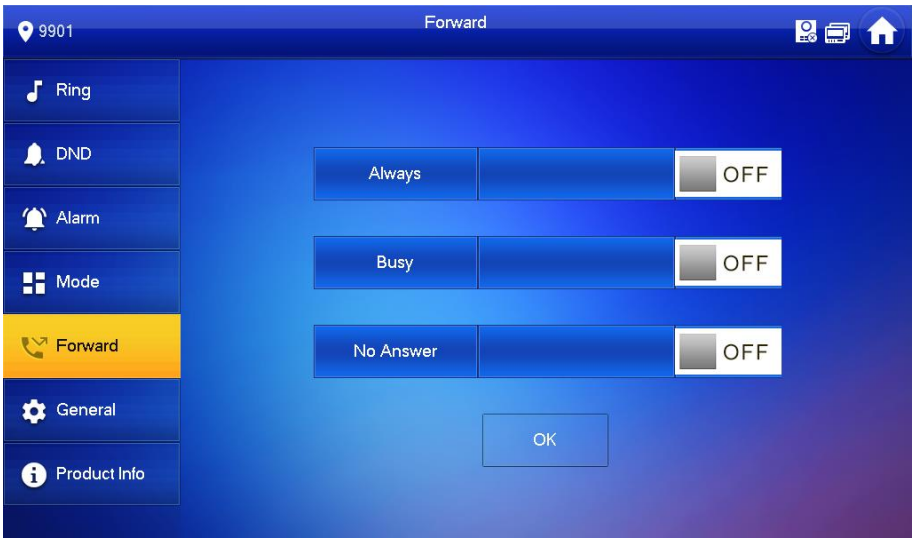


Figure 7-9

You can select the forward type you need:

- **Always**: All the calls come to this VTH will be forwarded.
- **Busy**: If the VTH is busy, then the call will be forwarded.
- **No Answer**: Any call that has not been answered within 15 s will be forwarded.

Step 4 In the input box behind the forward type you need, input the SIP code.

- If you want to forward the calls to a specific user, input the SIP code of that user. For example, if you input **3#1#1001#115**, then all the calls will be forwarded to that specific user.
- If you want to forward the calls to every user of the VTH, change the last three numbers into **100**, in this case, you need to input **3#1#1001#100**, then all the users will receive the forwarded call on their phone at the same time.

Step 5 Tap

to enable the function, and then it changes to

. Tap **OK** to save.

7.3.2 Calling Operations

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

- When the VTO is making video call, you can answer the call and unlock the door remotely.

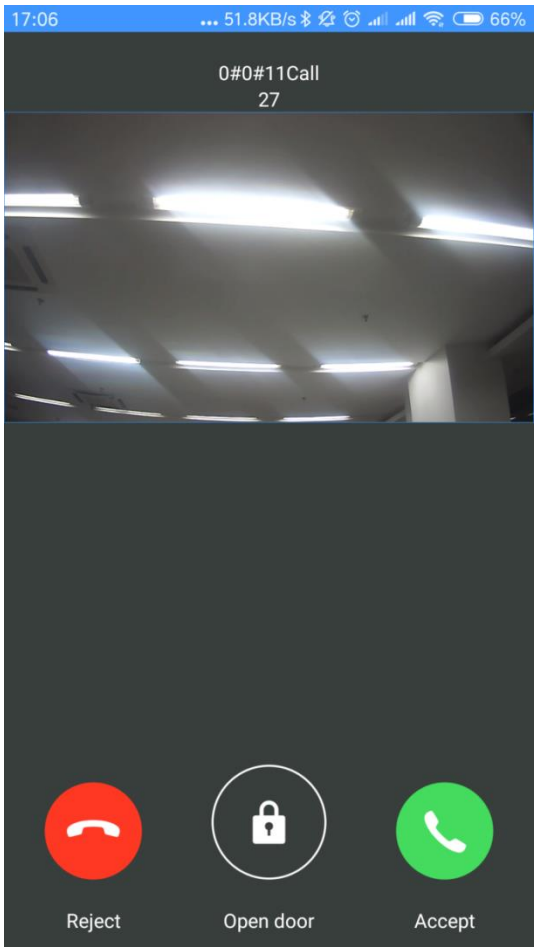


Figure 7-10

- You can also receive the call from the management center.

Figure 7-11

7.4 Monitor

You can add the connected VTO manually to do monitor, voice communication, and unlock.

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

The **Monitor** interface is displayed.

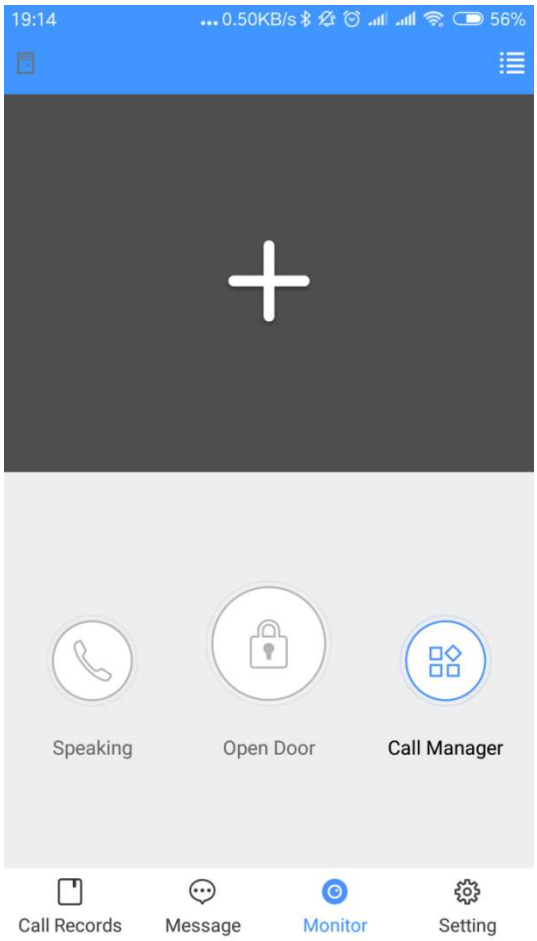


Figure 7-12

You can tap **Call Manager** to call the management center.

Step 2 Tap the “+” sign, and then select the VTO you need from the Channel List.

The live video is displayed.

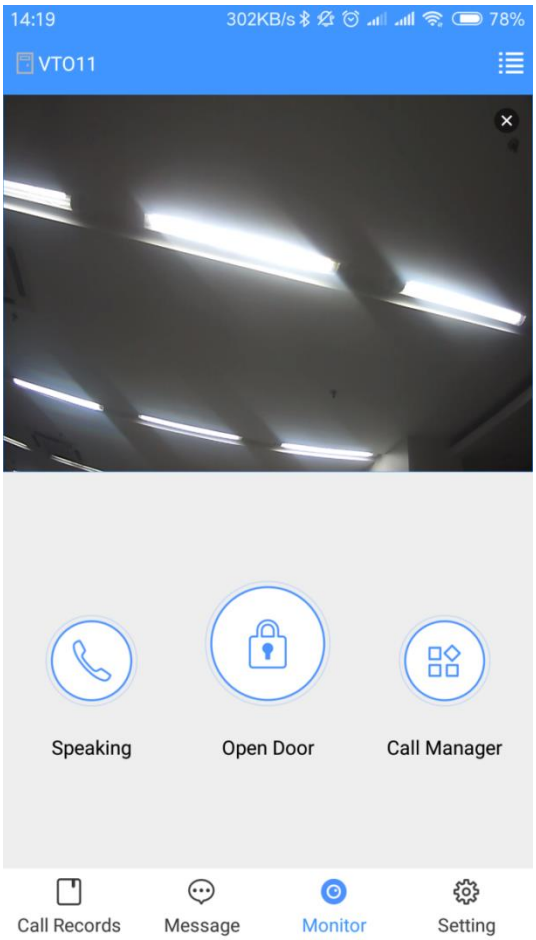


Figure 7-13

- Tap **Open Door** to unlock the door.
- Tap **Speaking** to do voice communication with the VTO.

7.5 Call Records

After call forward is properly configured (See “7.3.1 Configuring Call Forward“), you can view the call records from the VTO or the management center.

Step 1 Log in the app, and then Tap **Call Records**.

The **Call Records** interface is displayed.

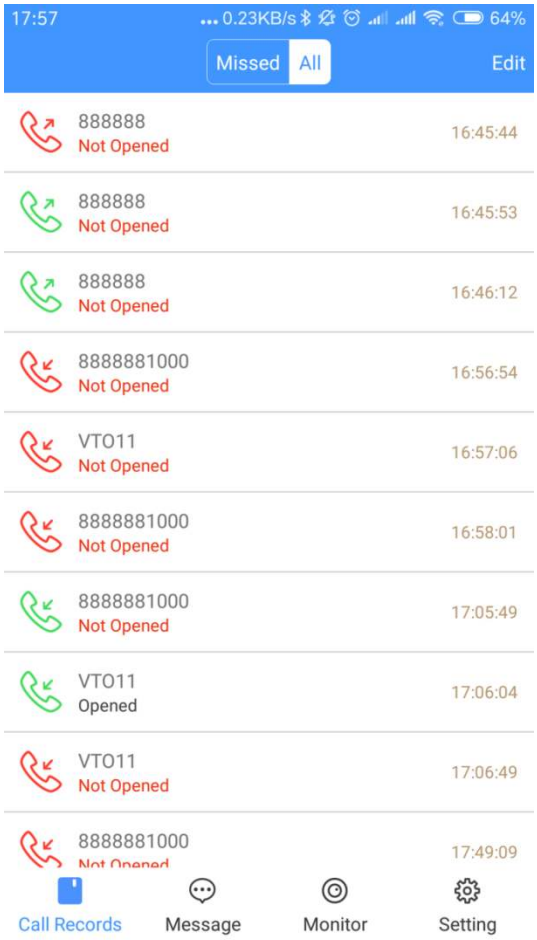


Figure 7-14

Step 2 You can view the missed calls and all the records.

- Tap **Edit** to delete call record one by one.
- Tap **Edit** > **Empty** to delete all the records.

7.6 Message

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

The **Message** interface is displayed. You can view the access messages and alarm messages.

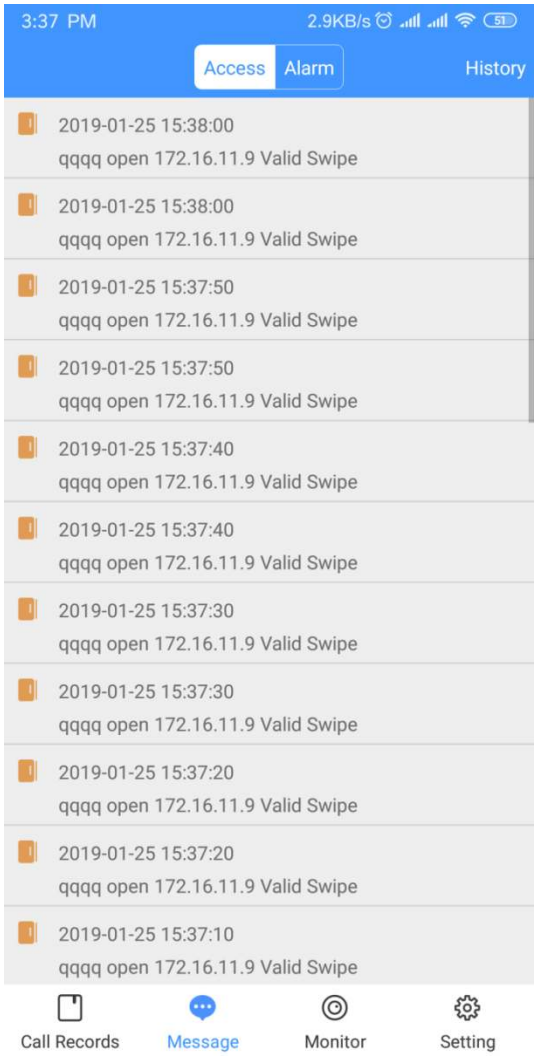


Figure 7-14

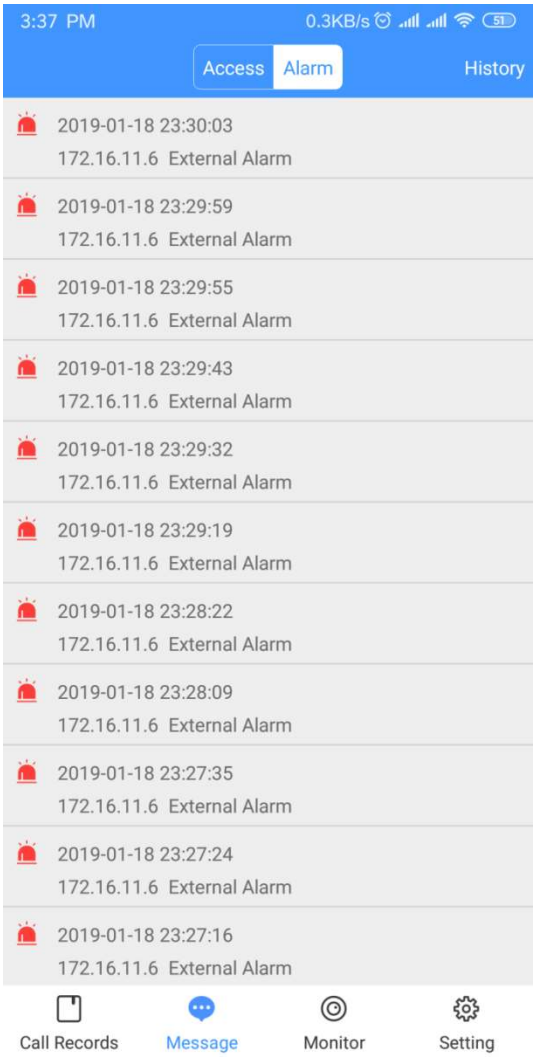


Figure 7-15

You need to enable event subscription first. See “7.7 Setting.”

Villa VTO

User’s Manual

V1.0.0

Foreword

General

This Manual introduces the operation of the web interface.

Safety Instructions

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

Signal Words	Meaning
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
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	Janauary 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) recommended by this area, which shall be used within its rated specification!
- Please 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.

Table of Contents

Foreword ..... **I**
Important Safeguards and Warnings ..... **II**
1 Initialization **1**
2 Login Interface **2**
2.1 Logging In 2
2.2 Resetting Password 2
3 Main Interface **4**
4 Local Setting **5**
4.1 Basic 5
4.2 Video & Audio 6
4.3 Access Control 8
4.4 System 9
4.5 Security 10
5 Household Setting **11**
5.1 VTO No. Management 11
5.1.1 Adding VTO 11
5.1.2 Modifying VTO Information 12
5.1.3 Deleting VTO 13
5.2 Room No. Management 13
5.2.1 Adding Room Number 13
5.2.2 Modifying Room Number 15
5.2.3 Issuing Access Card 15
5.3 VTS Management 16
5.4 IPC Setting 17
5.5 Status 19
5.6 Publish Information 19
5.6.1 Send Info 19
5.6.2 History Info 20
6 Network Setting **21**
6.1 Basic 21
6.1.1 TCP/IP 21
6.1.2 HTTPS 21
6.2 SIP Server 21
6.3 IP Permissions 22
7 Log Management **24**
7.1 Call 24
7.2 Unlock 24
Appendix 1 Cybersecurity Recommendations **25**

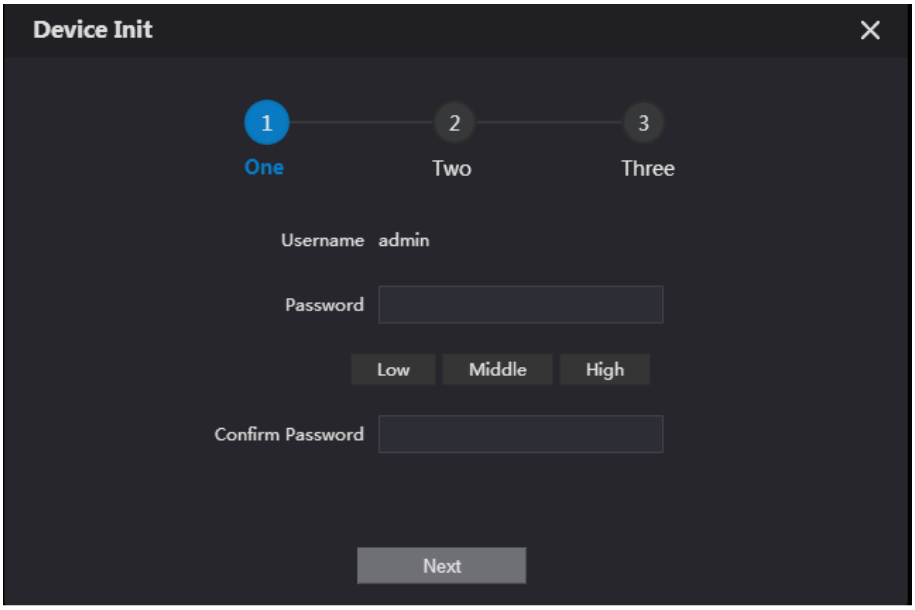
1 Initialization

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 192.168.1.110, 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 1-1 Device initialization



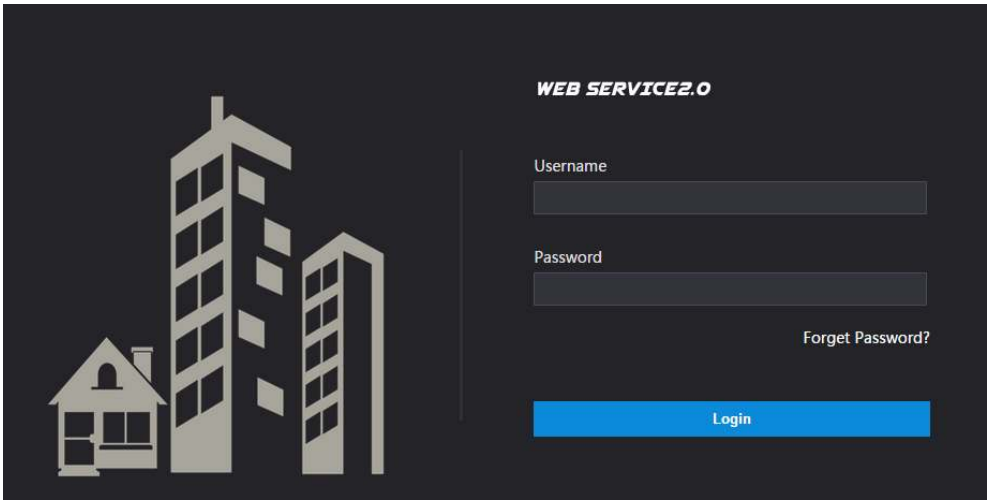
Step 3 Enter and confirm the password, and then click **Next**.
The email setting interface is displayed.

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



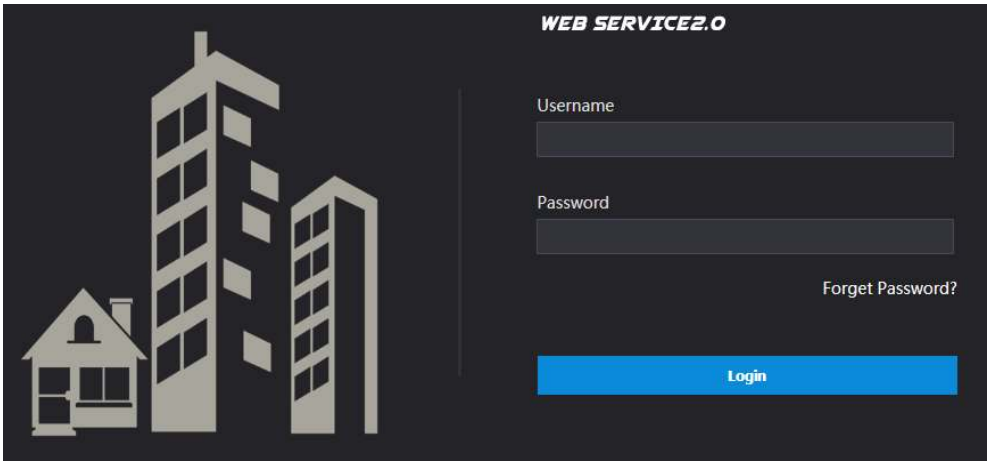
2 Login Interface

2.1 Logging In

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

Step 1 Open internet browser on the PC, then enter the VTO IP address in the address bar, and then press **Enter**.

Figure 2-1 Login interface

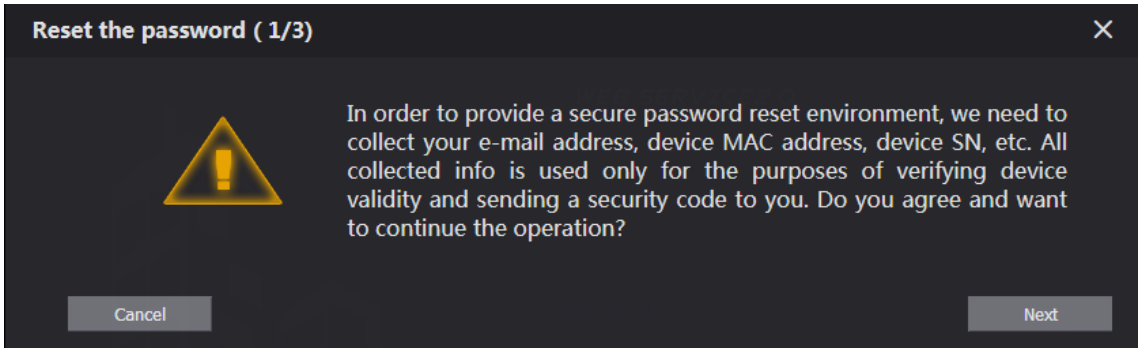


Step 2 Enter "admin" as username, then the password you set during initialization, and then click **Login**.

2.2 Resetting Password

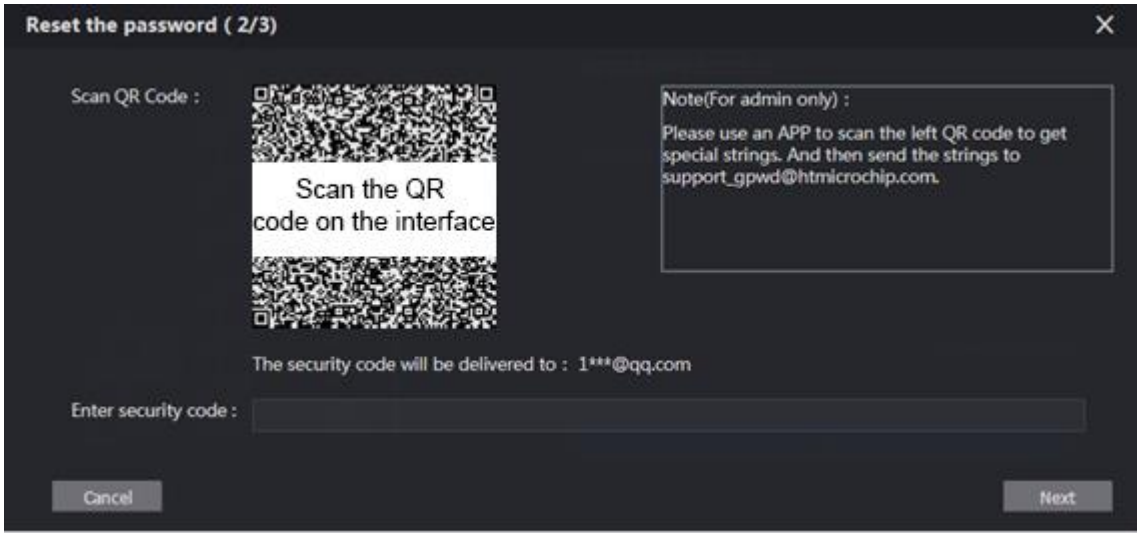
Step 1 On the login interface (Figure 2-1), click **Forgot Password?**.

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

Figure 3-1 Main interface

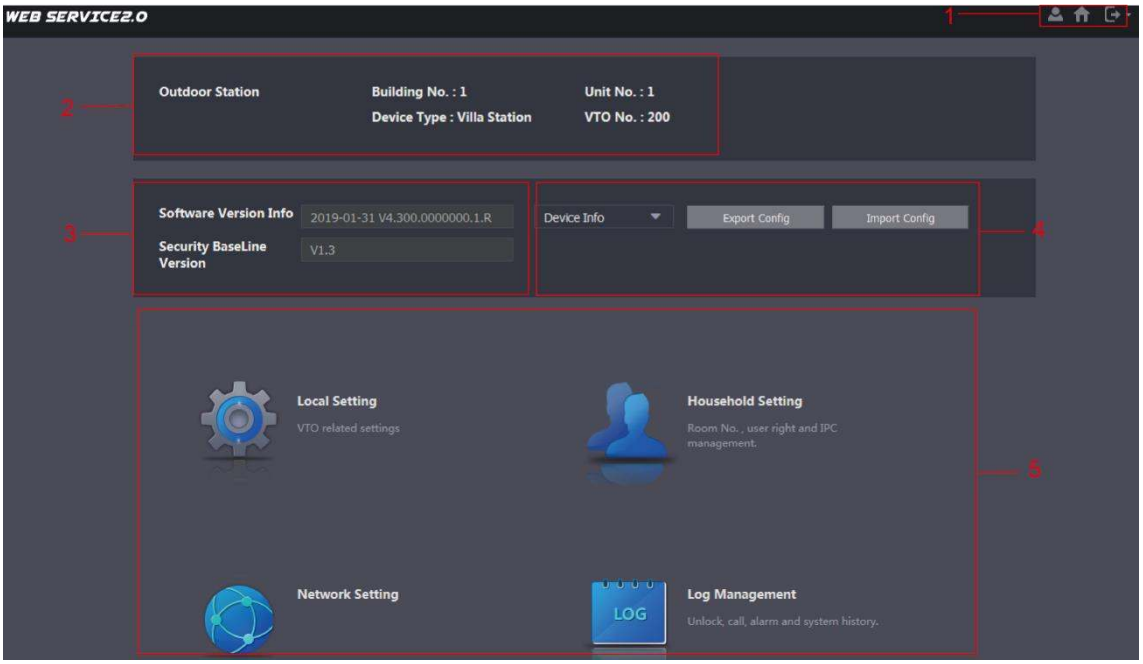


Table 3-1 Main interface introduction

No.	Function	Description
1	General function	• 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:

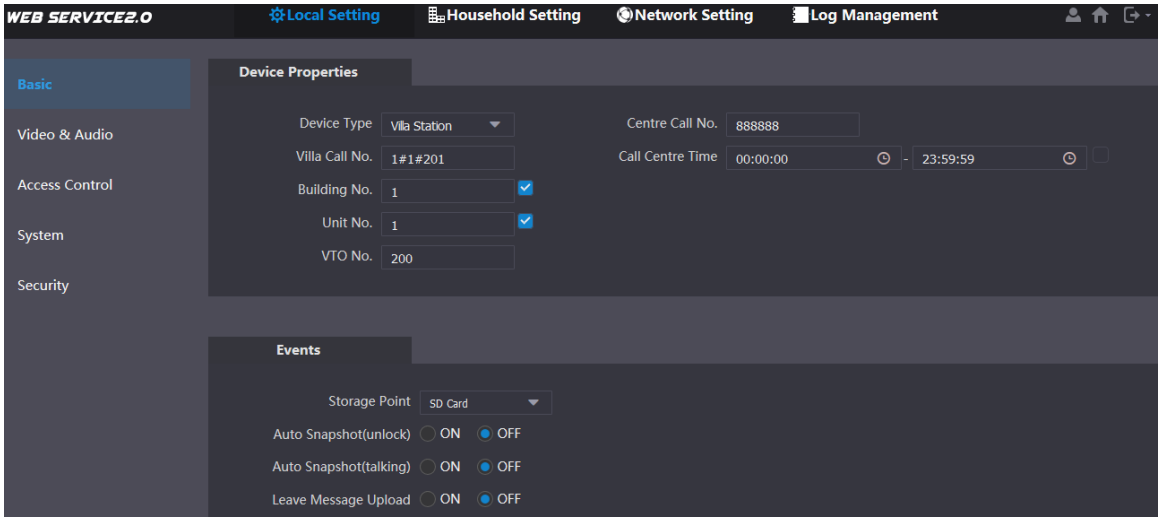
- After every configuration, click **Confirm** to save, and click **Refresh** to view the latest change.
- If you click **Default**, all the configurations in the current page would be restored to the default, and you need to click **Confirm** to save.

4.1 Basic

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	You can select Villa Station or Second Confirmation. ● Building number and unit number are available only when other servers work as SIP server. See "6.2 SIP Server." ● 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

Parameter	Description
	configured according to unit or building number. You can add VTO devices to the SIP server with their numbers.
Storage Point	All the snapshots would be saved to the SD card automatically. ● 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. ● Leave Message Upload Select **ON** to enable this function, and then the system uploads the messages from visitors to the SD card automatically. ● 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.

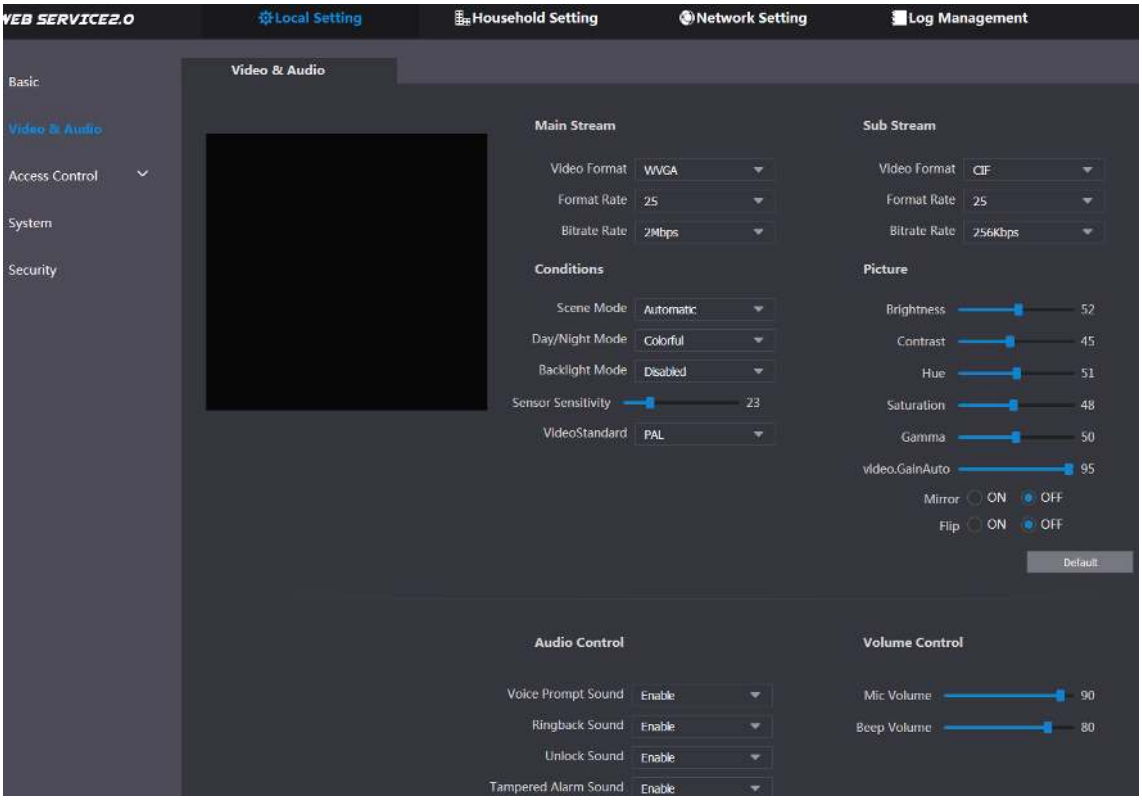
Step 3 Click **Confirm**.

4.2 Video & Audio

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

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

Figure 4-2 Video & audio



Step 2 Configure parameters, and these configurations 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 Rate	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**, 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 Rate	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.
Conditions	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 **Automatic**, **Colorful** or **Black White** mode.
	BackLight Mode	You can select from the following modes: ● **Disabled**: no back light. ● **Backlight**: the camera gets clearer image of the dark areas on the target when shooting against light. ● **Wide dynamic**: the system dims bright areas and compensates dark areas to ensure the clarity of all the area. ● **Inhibition**: the system constrains bright areas and reduces halo size to dim the overall brightness.
	Sensor Sensitivity	Adjust the value, and the larger the value is, the easier the sensor will be triggered.
	Video Standard	Select from **PAL** or **NTSC** according to your display device.
Picture	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 configured too big.
	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 set too big, the dark area would be too dark and bright area easier to get overexposed. The picture might be hazy if the value is set too small.

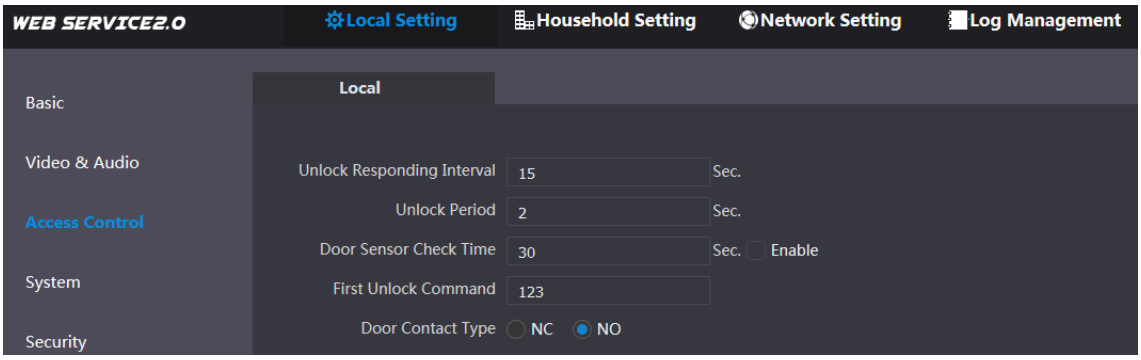
Parameter		Description
	Hue	Makes the color deeper or lighter. The default value is made by the light sensor, and it is recommended.
	Saturation	Makes the color deeper or lighter. The larger the value is, the deeper the color will be, and the lower the lighter. Saturation value doesn't change image brightness.
	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.
	Video.GainAuto	Amplify the video signal to increase image brightness. If the value is too large, there will be more noise in the image.
	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	Mic Volume	Adjust the value, and the larger the value is, the louder the microphone on the VTO will be.
	Beep Volume	Adjust the value, and the larger the value is, the louder the system sounds 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.

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

Figure 4-3 Local



Step 2 Configure parameters, and for the detailed description.

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.

Parameter	Description
Door Sensor Check Time	If you have installed door sensor, then you can 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. ● 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.

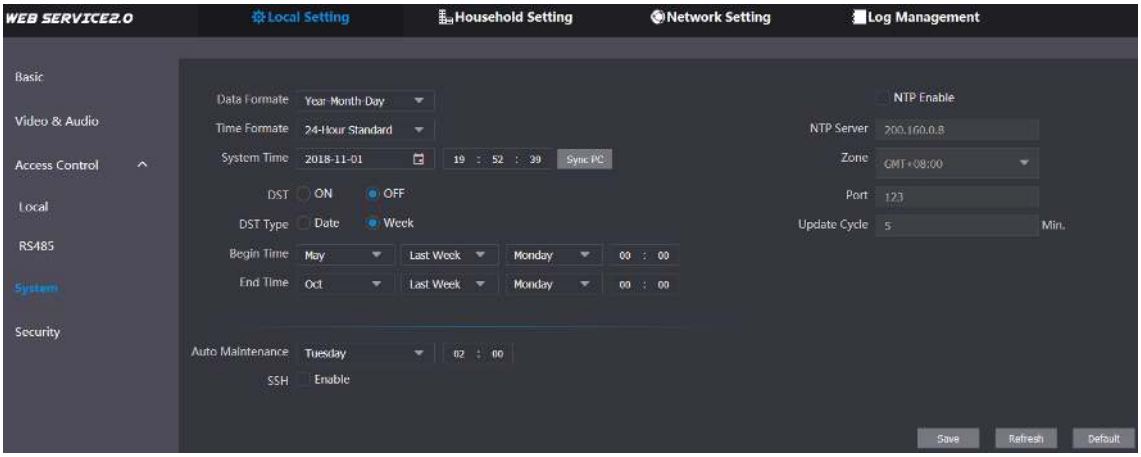
Step 3 Click **Save**.

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 4-4 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**.
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.

Parameter	Description
Begin Time	Configure the begin time and end time for DST.
End Time	
NTP Enable	Select the check box to enable NTP timing.
NTP Server	Enter the domain name of the NTP server.
Zone	The time zone of the current area.
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.
Auto Maintenance	Select the day and time for the auto maintenance, and the VTO will reboot 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 4-5 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.
Reset Password	Select the check box to enable, and then the password resetting is available.

Step 3 Click **Save** to save.

5 Household Setting

This chapter applies to the condition in which the VTO works as SIP server (see 6.2 SIP Server), and it introduces 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.

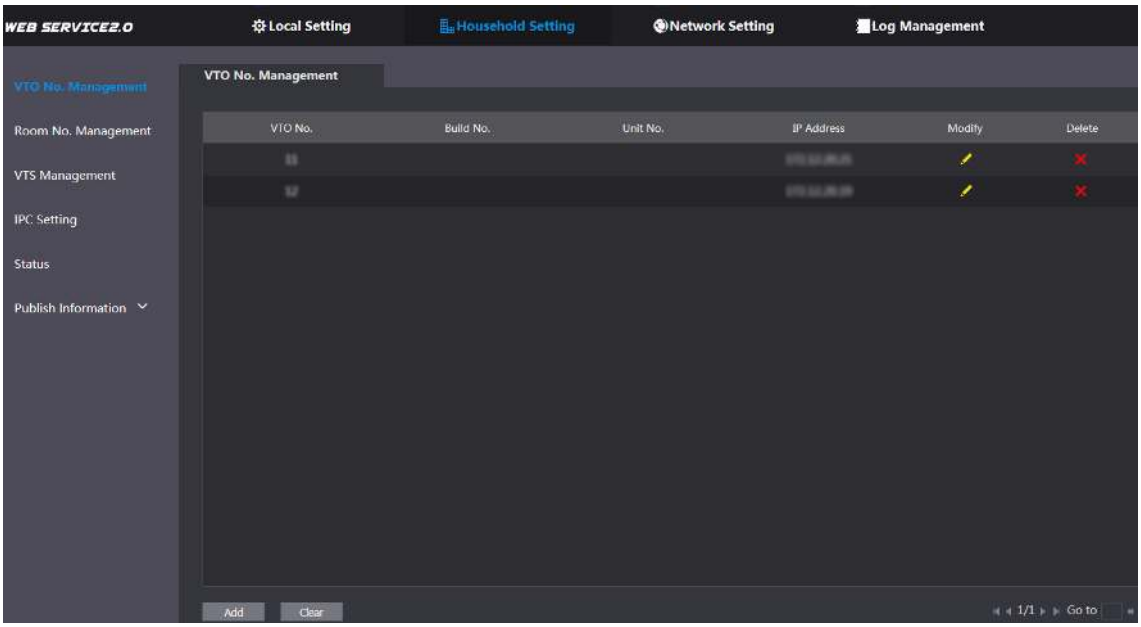
5.1 VTO No. Management

5.1.1 Adding VTO

You can add VTO devices to the SIP server, and all the VTO devices connected to the same SIP server can make video call between each other.

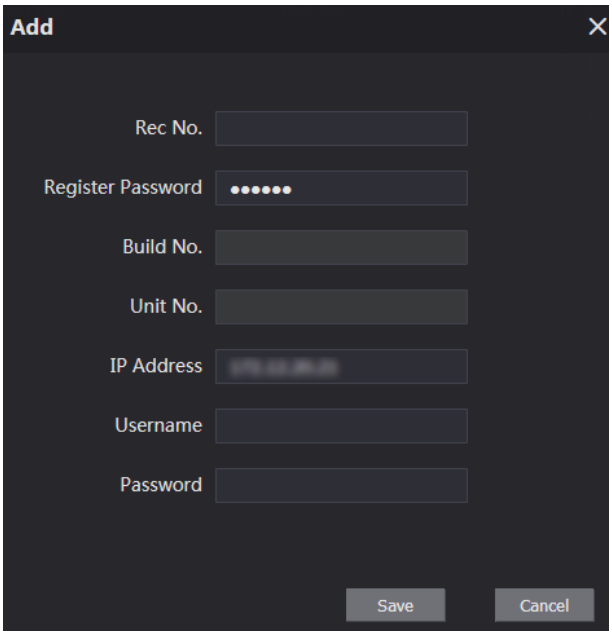
Step 1 Log in the web interface of the SIP server, and then select **Household Setting > VTO No. Management**.

Figure 5-1 VTO No. management



Step 2 Click **Add**.

Figure 5-2 Add VTO



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

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	

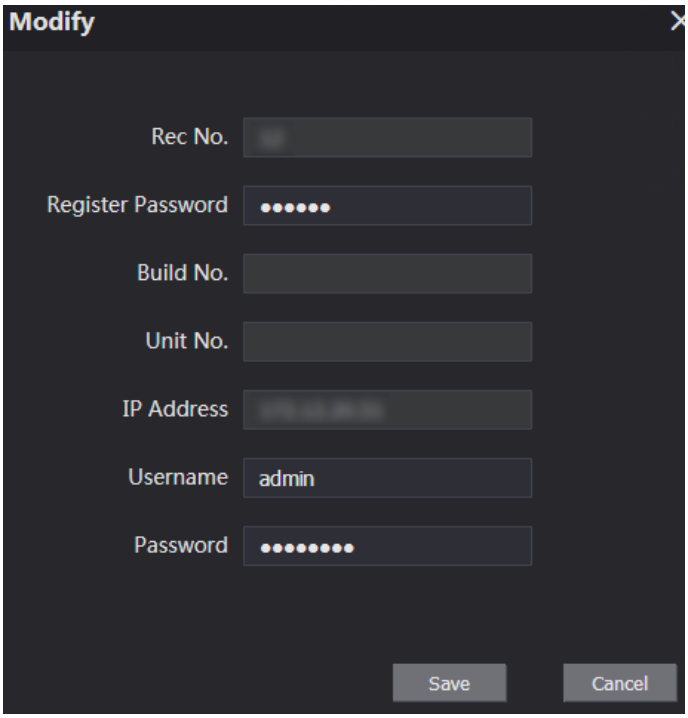
Step 4 Click **Save**.

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



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

Step 3 Click **Save**.

5.1.3 Deleting VTO

The VTO that is currently at 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.

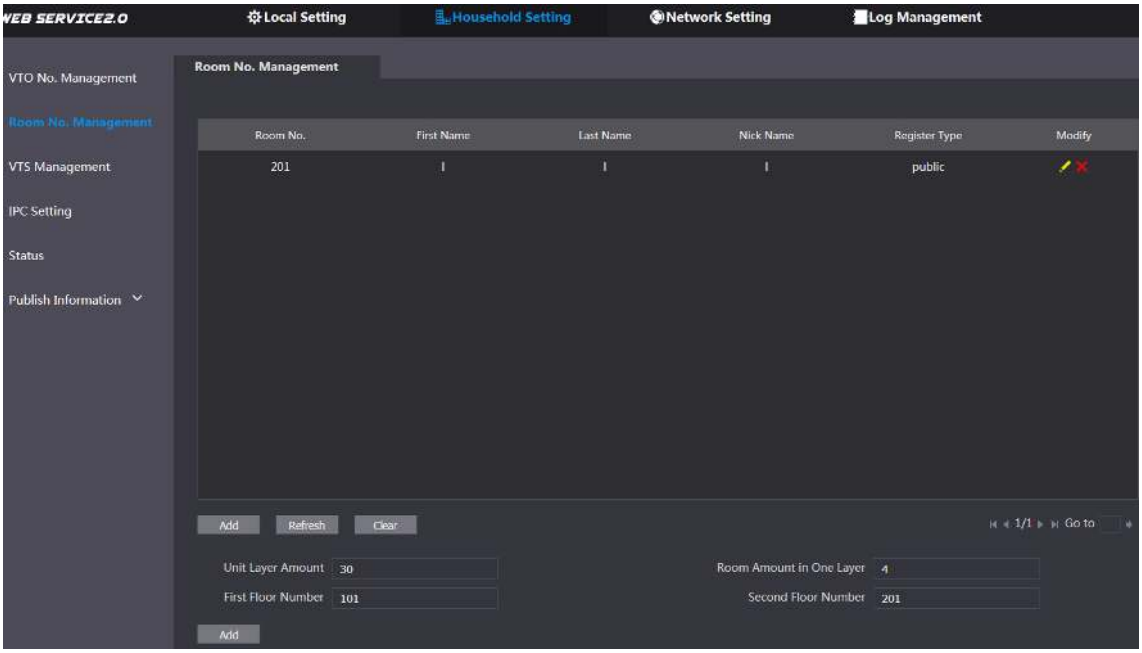
5.2 Room No. Management

5.2.1 Adding Room Number

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

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

Figure 5-4 Room No. Management

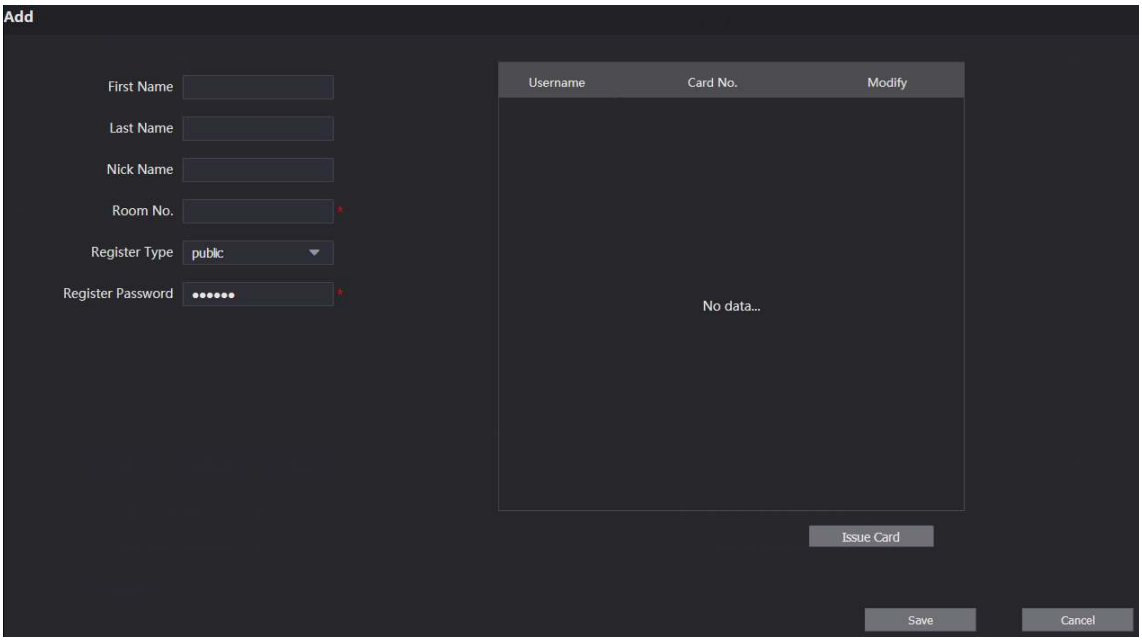


Step 2 You can add single room number or do it in batch.

- Add single room number

1) Click the **Add** at the mid lower position.

Figure 5-5 Add single room number



2) Configure room information.

Table 5-2 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.
Register Type	Select **public**, and **local** is reserved for future use.
Register Password	Keep the default value.

3) Click **Save**.

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

- Adding room number in batch

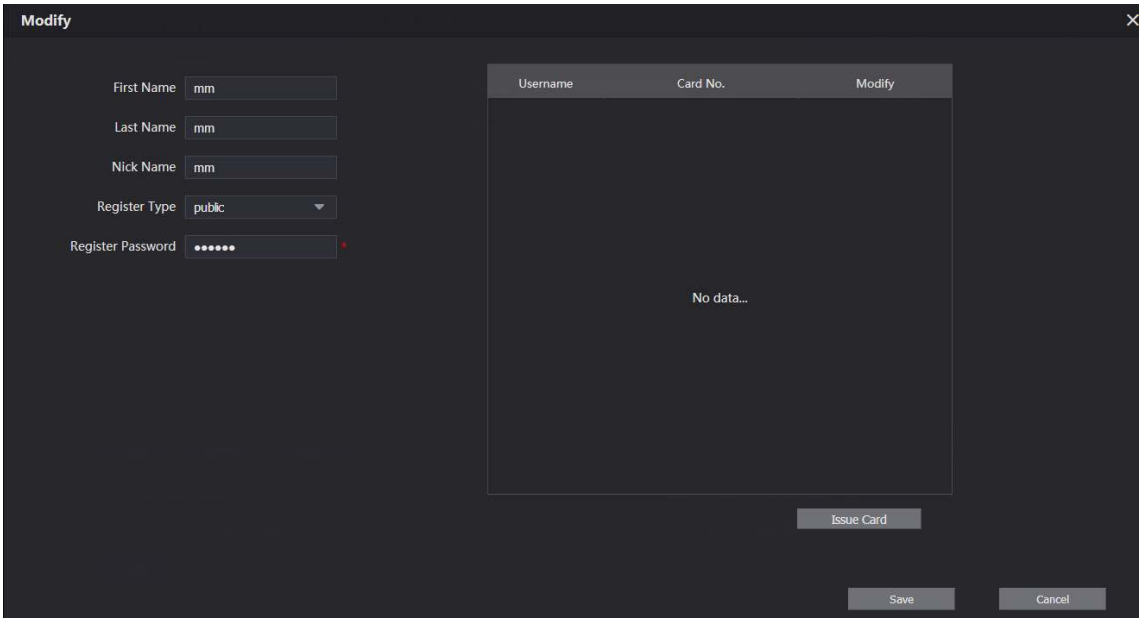
1) Configure the Unit Layer Amount, Room Amount in One Layer, First Floor Number, and Second Floor Number according to the actual condition.
2) Click the **Add** at the bottom position.

All the added room numbers are displayed. 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



Step 2 You can modify the names for the room.

Step 3 Click **Save**.

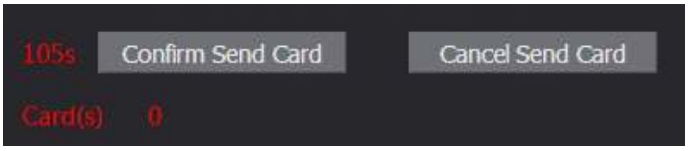
5.2.3 Issuing Access Card

You can issue card to a room, and can also set it to be the main card, or to the lost state.

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

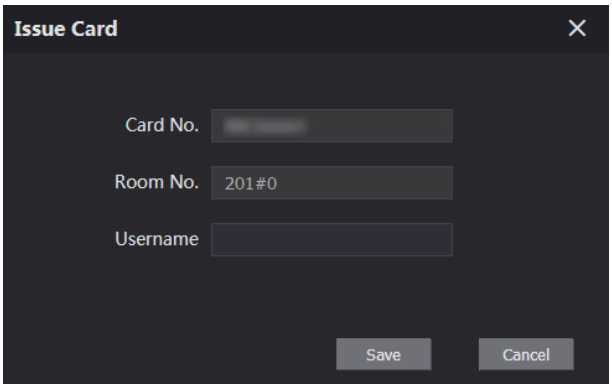
The countdown notice is displayed.

Figure 5-7 Countdown notice



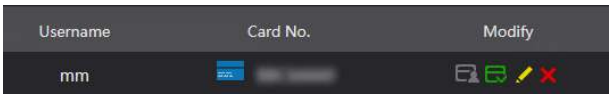
Step 2 Swipe the card that needs to be authorized on the VTO, and then the **Issue Card** dialogue box is displayed.

Figure 5-8 Issue card



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

Figure 5-9 Issued access card



Step 4 You can configure the access card.

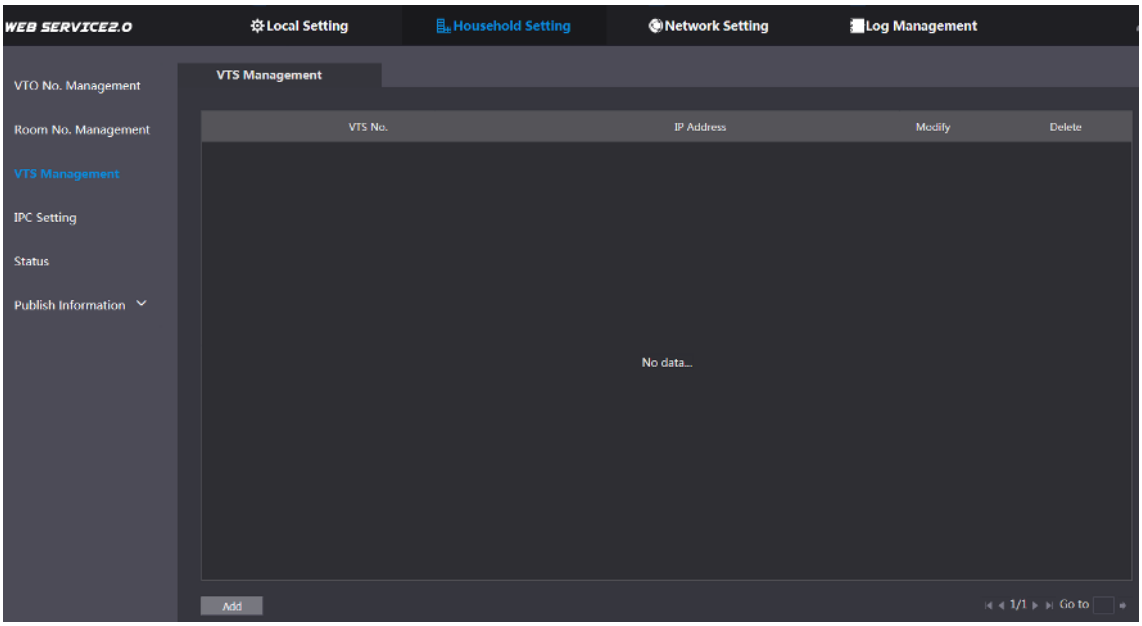
- Click to set it to the main card, and then the icon turns into . The main card can be used to issue access card for this room on the VTO. Click again to resume.
- Click to set it to the lost state, and then the icon turns into . The card under lost state cannot be used to open the door. Click again 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 VTO and VTH devices in the network, make or receive video call from them, and make basic configurations. For the detailed introduction, see the corresponding user's manual.

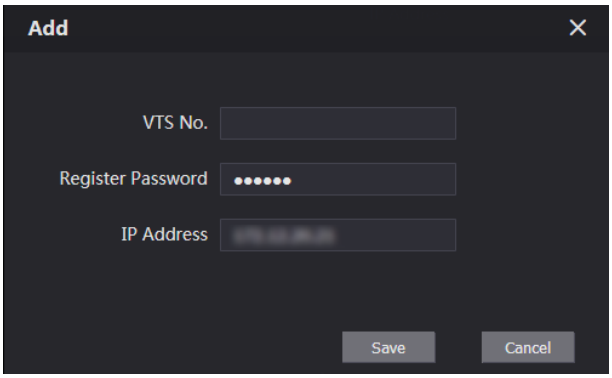
Step 1 Log in the web interface of the SIP server, and then select **Household Setting > VTS Management**

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.

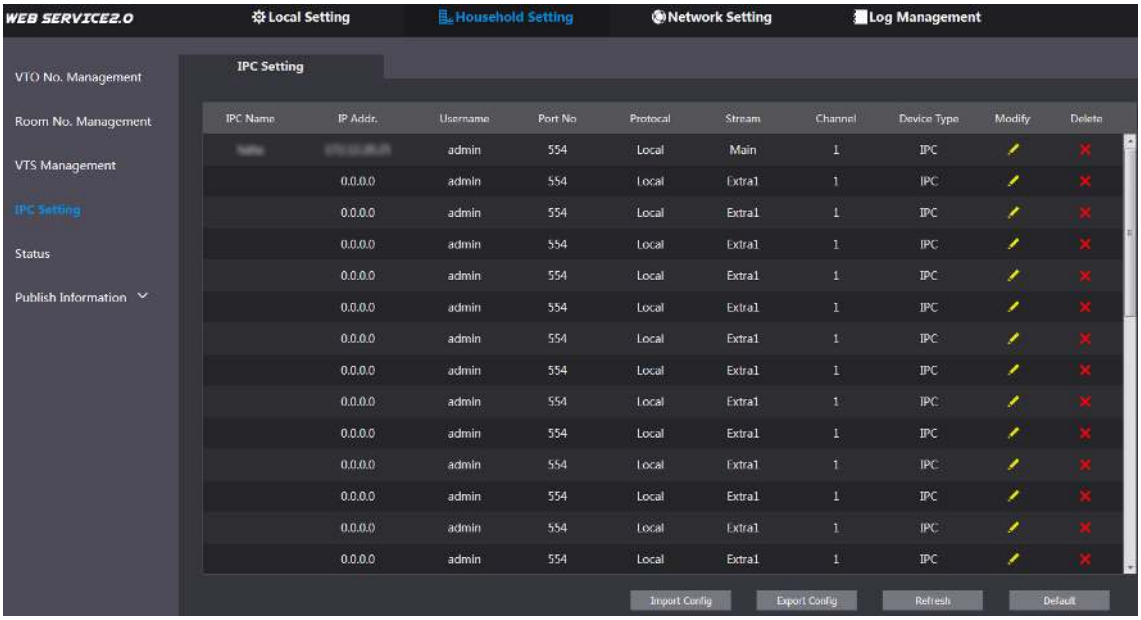
Step 4 Click **Save**, and then the added VTS is displayed. Click to modify IP address, and click to delete.

5.4 IPC Setting

You can add IPC, NVR, HCVR, and XVR to the SIP server, and then all the connected VTH can do monitor with the added cameras.

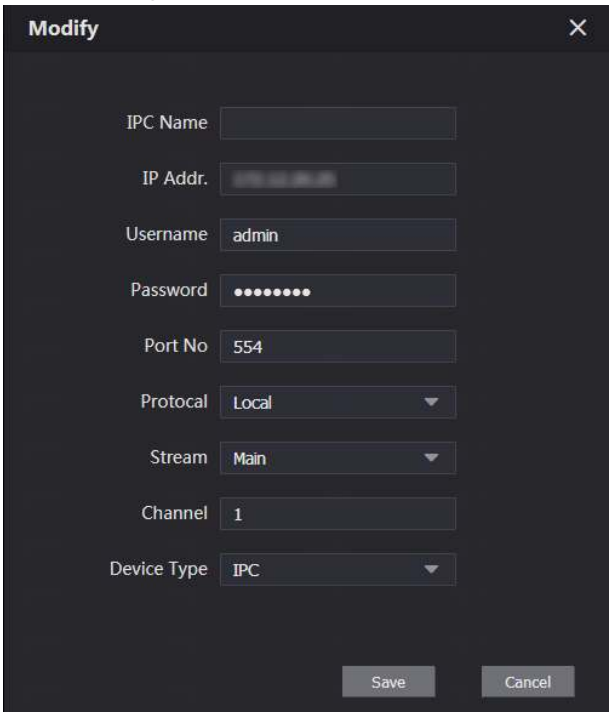
Step 1 Log in the web interface of the SIP server, and then select **Household Setting > IPC Setting**

Figure 5-12 IPC setting



Step 2 The total quantity of the device you can add is fixed. You can click to add the device you need.

Figure 5-13 Add IPC



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

Table 5-4 Add IPC configuration

Parameter	Description
IPC Name	Enter the name of the device you need.
IP Addr.	The IP address of the device.
Username	The user name and password for the web interface of the device.
Password	
Port No.	Keep default value.
Protocol	Select from **Local** or **Onvif**.

Parameter	Description
Stream	Select from **Main** or **Extra1**, and the main stream has better image quality, but also costs more bandwidth.
Channel	Define a channel for the device.
Device Type	Select from **IPC**, **NVR**, **HCVR**, and **XVR** as needed.

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

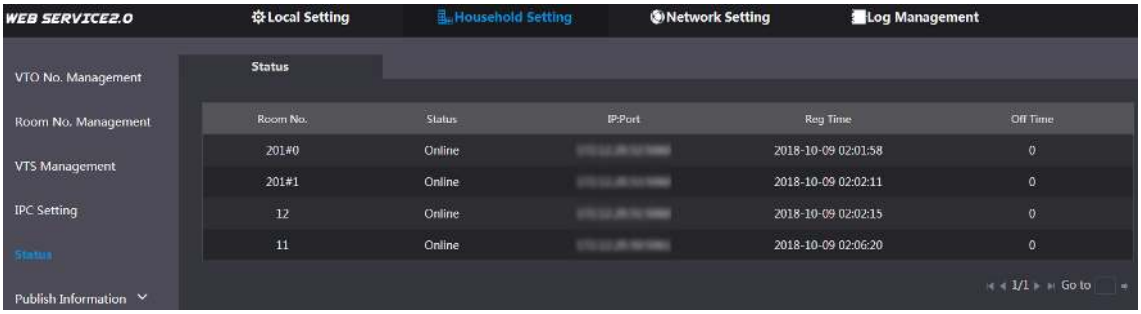
You can also click **Export Config** to export the current devices to the local PC, or click **Import Config** to import the existed configuration.

5.5 Status

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

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

Figure 5-14 Status



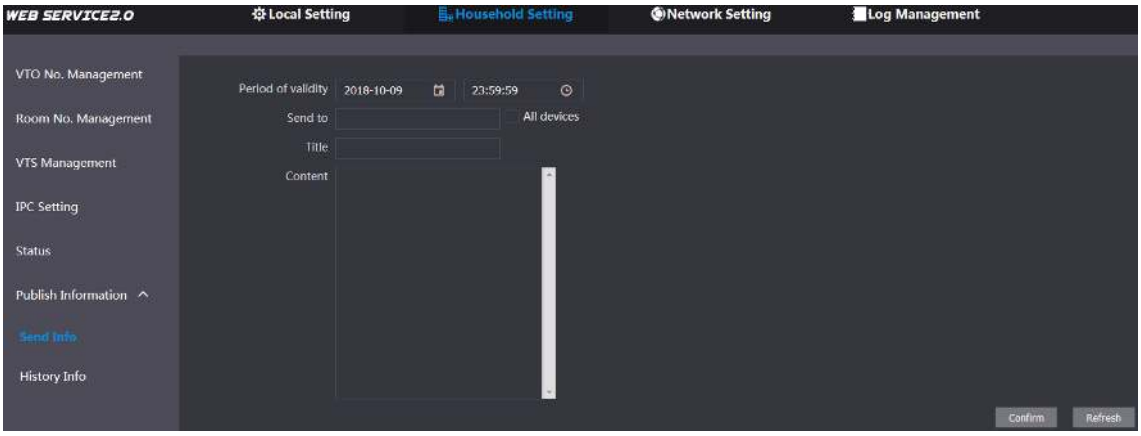
5.6 Publish Information

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

5.6.1 Send Info

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

Figure 5-15 Send Info



Step 2 Enter the target VTO No. or select **All device** to send the message to all the devices in the network, and then the title and content of your message.

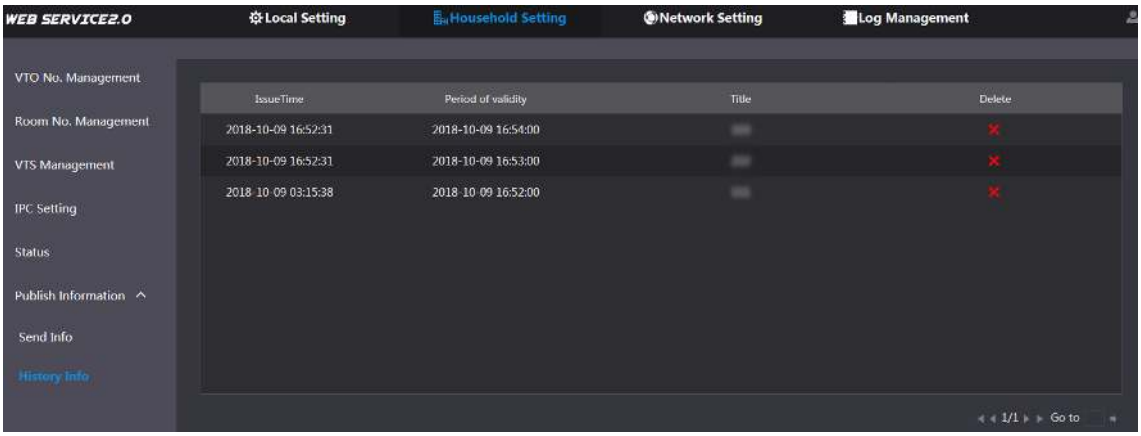
The Period of validity is reserved for future use.

Step 3 Click **Confirm**.

5.6.2 History Info

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

Figure 5-16 History info



You can view the time and title of the sent messages.

6 Network Setting

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

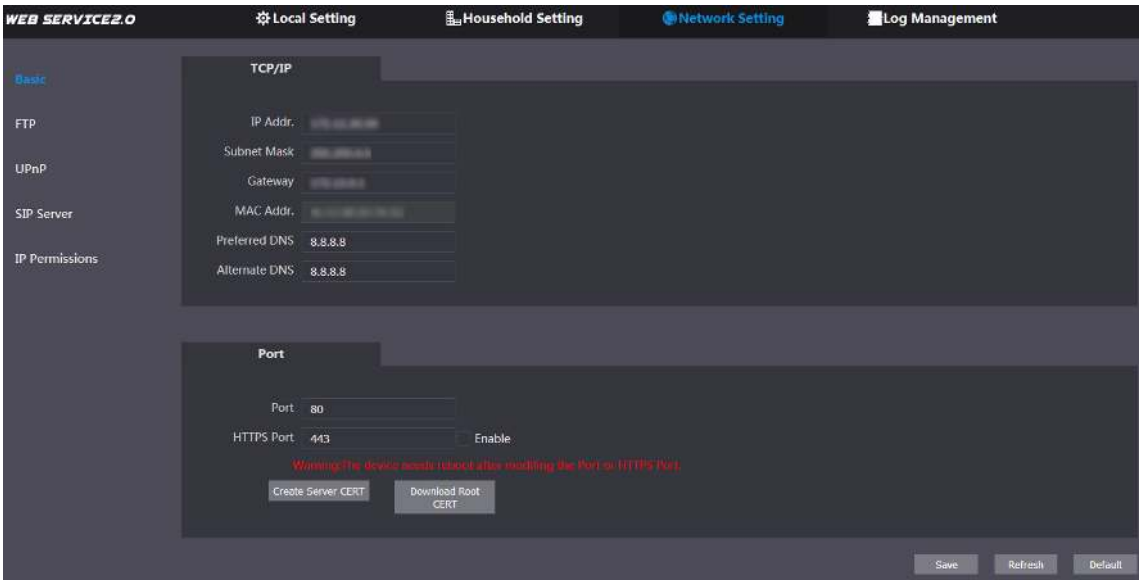
6.1 Basic

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

6.1.2 HTTPS

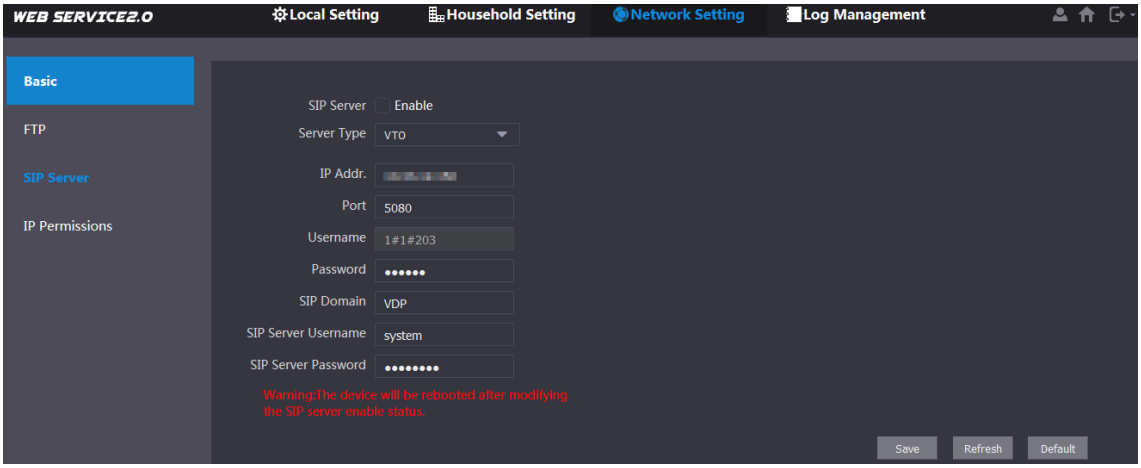
Select the **Enable** check box at **HTTPS Port**, and then the VTO will reboot. After rebooting, you can log in the VTO by entering "https:// VTO IP address" in the address bar of the explorer.

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 call between each other. You can use VTO device or other servers as SIP server.

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

Figure 6-2 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	

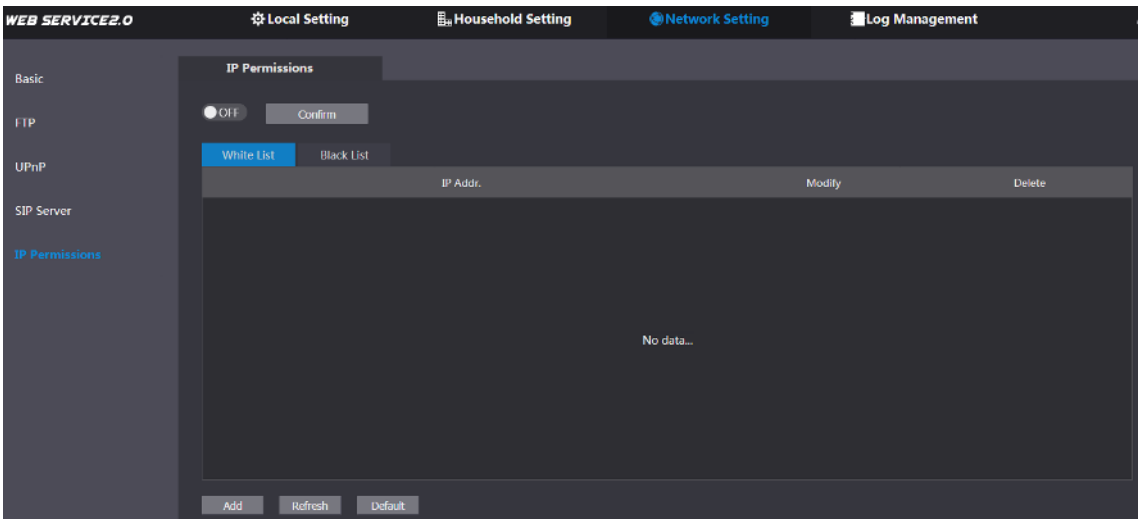
- If other servers work as SIP server
  Select the server type you need at **Server Type**, and then see the corresponding manual for the detailed configuration.

6.3 IP Permissions

To enhance network and data security, you need to configure access authority for different IP addresses.

Step 1 Select **Network Setting > IP Permissions**.

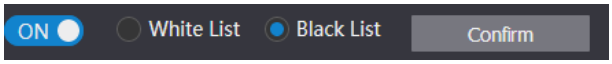
Figure 6-3 IP Permissions



Step 2 Click .

The **White List** option and **Black List** option are displayed.

Figure 6-4 White List and Black List



You can only use one of them at the same time.

- **White list**: only the IP addresses in the list can login the VTO.
- **Black list**: all the IP addresses in the list are prohibited from logging in the VTO.

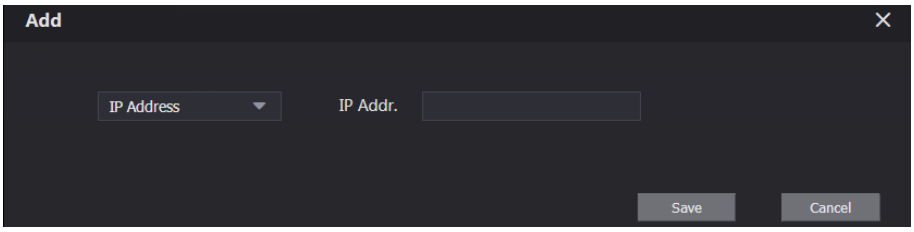
Step 3 Select **White List** or **Black List**.

- If you need to use black list, select **Black List**, and then click **Confirm**.
- If you need to use white list, select **White List**, and then add an IP address or IP section in the white list before clicking **Confirm**.

Step 4 Click **Add**.

The **Add** interface is displayed.

Figure 6-5 Add IP address



Step 5 You can select and enter single IP address or an IP section, and then click **Save**.

7 Log Management

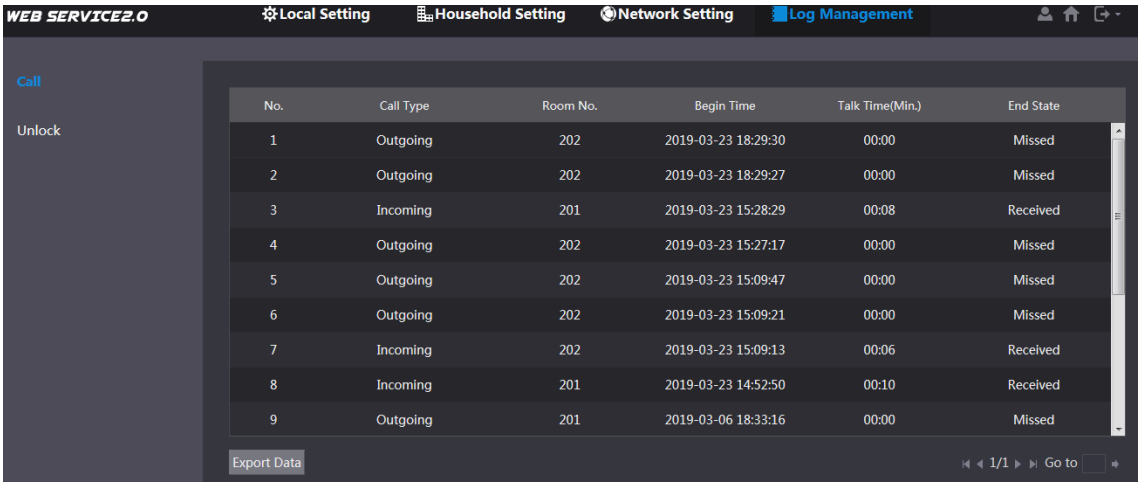
You can view call history, alarm record, unlock record and various system logs.

7.1 Call

You can view the call type, room number, begin time, talk time, and end state.

Select **Log Management > Call**.

Figure 7-1 Call



No.	Call Type	Room No.	Begin Time	Talk Time(Min.)	End State
1	Outgoing	202	2019-03-23 18:29:30	00:00	Missed
2	Outgoing	202	2019-03-23 18:29:27	00:00	Missed
3	Incoming	201	2019-03-23 15:28:29	00:08	Received
4	Outgoing	202	2019-03-23 15:27:17	00:00	Missed
5	Outgoing	202	2019-03-23 15:09:47	00:00	Missed
6	Outgoing	202	2019-03-23 15:09:21	00:00	Missed
7	Incoming	202	2019-03-23 15:09:13	00:06	Received
8	Incoming	201	2019-03-23 14:52:50	00:10	Received
9	Outgoing	201	2019-03-06 18:33:16	00:00	Missed

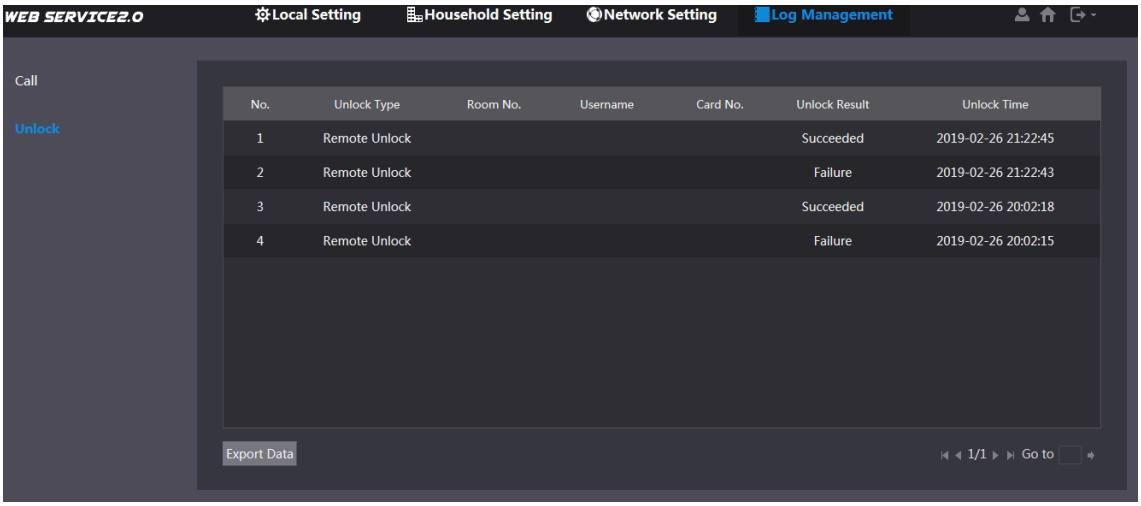
Click **Export Data** to export the records to your PC.

7.2 Unlock

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

Select **Log Management > Unlock**.

Figure 7-2 Unlock



No.	Unlock Type	Room No.	Username	Card No.	Unlock Result	Unlock Time
1	Remote Unlock				Succeeded	2019-02-26 21:22:45
2	Remote Unlock				Failure	2019-02-26 21:22:43
3	Remote Unlock				Succeeded	2019-02-26 20:02:18
4	Remote Unlock				Failure	2019-02-26 20:02:15

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

Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

2. **Update Firmware and Client Software in Time**

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

3. **Set and Update Passwords Reset Information Timely**

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

4. **Enable Account Lock**

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

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers

between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

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

7. **Enable Whitelist**

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

8. **MAC Address Binding**

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

9. **Assign Accounts and Privileges Reasonably**

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

10. **Disable Unnecessary Services and Choose Secure Modes**

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

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

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

11. **Audio and Video Encrypted Transmission**

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

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

12. **Secure Auditing**

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

13. **Network Log**

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

14. **Construct a Safe Network Environment**

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

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

so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

7.7 Setting

Step 1 Log in the app, and then tap **Setting**.
The **Settings** interface is displayed.

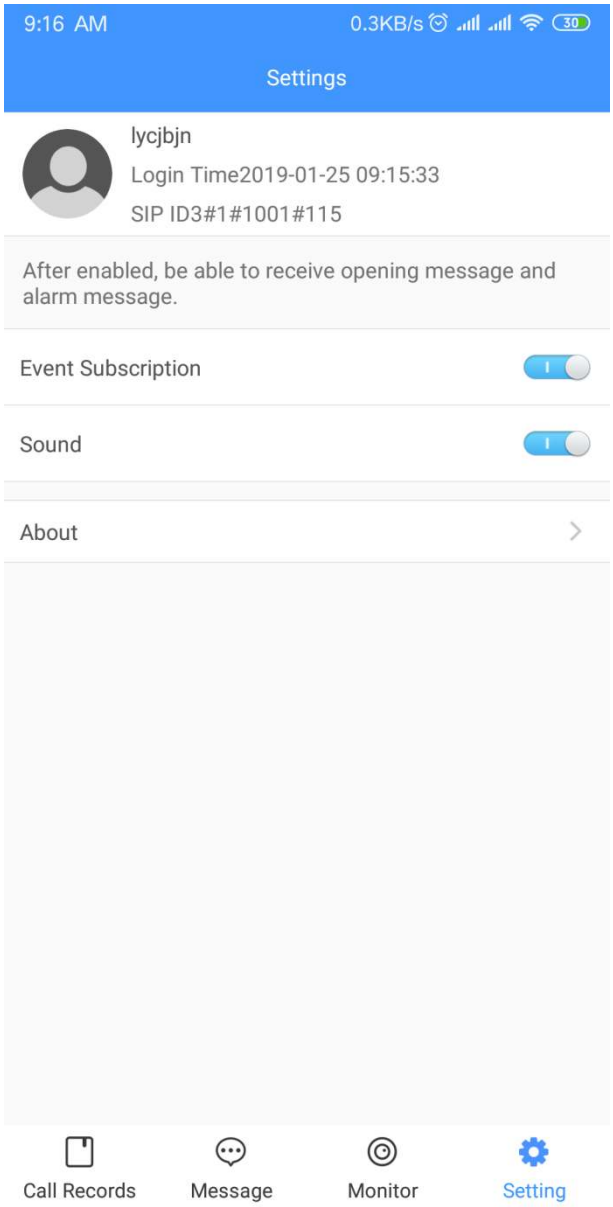


Figure 7-16

Step 2 Tap to enable the function you need, and then it changes to .

- Enable **Event Subscription**, and then you can view the access messages and alarm messages. See “7.6 Message.”
- Enable **Sound**, and then the phone rings when receiving a call.

Step 3 Tap **About**, and then you can view the version information or the help document, and you can logout 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 equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

2. **Update Firmware and Client Software in Time**

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

3. **Set and Update Passwords Reset Information Timely**

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

4. **Enable Account Lock**

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

5. **Change Default HTTP and Other Service Ports**

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

6. **Enable HTTPS**

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

7. **Enable Whitelist**

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

8. **MAC Address Binding**

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

9. **Assign Accounts and Privileges Reasonably**

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

10. **Disable Unnecessary Services and Choose Secure Modes**

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

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

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

11. **Audio and Video Encrypted Transmission**

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

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

12. **Secure Auditing**

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

13. **Network Log**

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

14. **Construct a Safe Network Environment**

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

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

use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.