

10-Inch Android Indoor Monitor

User's Manual





Foreword

General

This document mainly introduces structure, installation process, and basic configuration of the 10-Inch Android Indoor Monitor (hereinafter referred to as the "indoor monitor").

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Date
V1.0.0	First release	January 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. 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 to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- The device shall be used with screened network cables.

Power Requirement

- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification!
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.
- Do not cut off power supply during device upgrade. Power supply can be cut off only after the device has completed upgrade and has restarted.

Table of Contents

Foreword	I
Important Safeguards and Warnings	II
1 Introduction	1
1.1 Overview	1
1.2 Features	1
1.3 Front Panel.....	2
1.4 Rear Panel	2
1.5 Cable Connections.....	3
2 Installation	4
3 Network Diagram	6
4 Configuration	7
4.1 Configuration Process.....	7
4.2 VDPCONFIG	7
4.3 Configuring Door Station.....	7
4.3.1 Initialization	7
4.3.2 Configuring VTO Number	9
4.3.3 Configuring Network Parameters	9
4.3.4 Selecting SIP Servers.....	10
4.3.5 Adding VTO Devices.....	13
4.3.6 Adding Room Number	14
4.4 Configuring Indoor Monitor	16
4.4.1 Initialization	16
4.4.2 Network Settings.....	18
4.4.3 Project Settings.....	21
4.4.4 General Settings	27
4.4.5 Alarm Settings.....	32
4.4.6 Elevator Control	35
4.5 Commissioning.....	35
4.5.1 Watching Monitoring Video.....	35
4.5.2 Checking Messages	37
4.5.3 Making Calls	37
4.5.4 Viewing Alarms Logs	38
4.5.5 Viewing Information	39
Appendix 1 Cybersecurity Recommendations	41

1 Introduction

1.1 Overview

The 10-inch digital Android indoor monitor, widely used in intelligent buildings, integrates functions of monitoring, voice/video call, and unlock. Technologies like embedded technology, IP communication methods, simple network management protocol (SNMP), network encryption, and more are applied to make the whole system more stable, safer, and easier to be managed.

1.2 Features

- Wi-Fi: Provides wireless network for devices.
- Voice call: You can make calls on the door stations to indoor monitors.
- Monitoring: Videos captured by fence stations, door stations, IP cameras, and more can be watched on the indoor monitor.
- Elevator control: You can make the elevator come to your floor through the indoor monitor.
- Emergency call: Emergency calls can be made on the indoor monitor.
- Auto snapshot: During calls, or during monitoring, images can be captured, and the images can be stored in the SD card or FTP.
- Video recording: You can record videos through the indoor monitor if SD card is inserted into the rear panel of the indoor monitor.
- Do not disturb: You can set period in which you do not want to be disturbed.
- Remote unlock: You can unlock doors remotely.
- Arm and disarm: You can set protection zones, and then arm and disarm.
- Record search: Call records and alarm records can be viewed.
- Message check: You can check text messages and videos left by visitors, or public notices released by the management center.
- App: You can install app on your mobile phone.

1.3 Front Panel

Figure 1-1 Appearance



Table 1-1 Components

No.	Name
1	On/off button. Press the button, and then you can turn on/off the screen; press and hold the button, you can turn on/off or restart the indoor monitor.
2	MIC, inputs audio.

1.4 Rear Panel

Figure 1-2 Rear panel

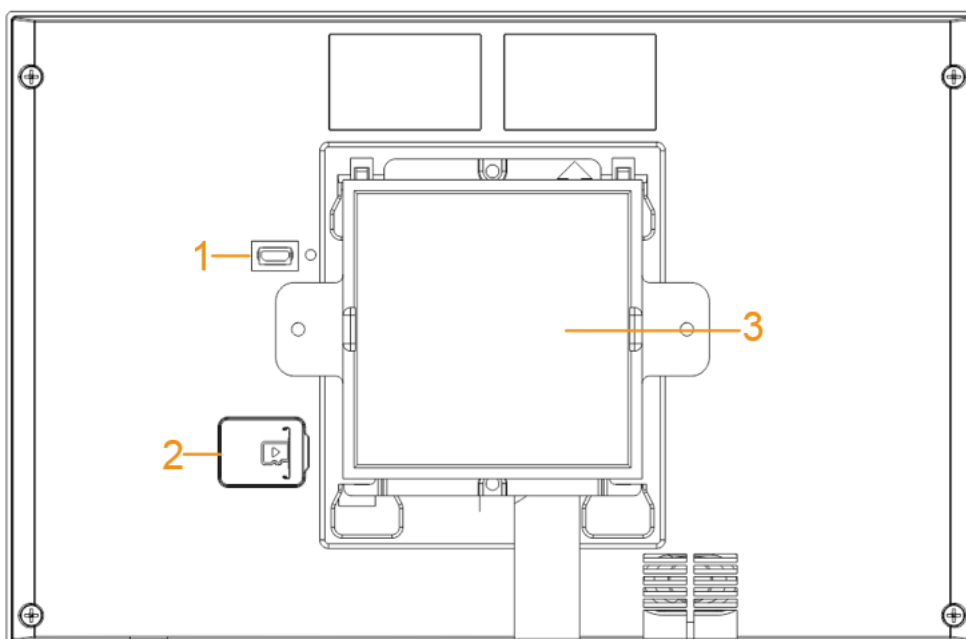
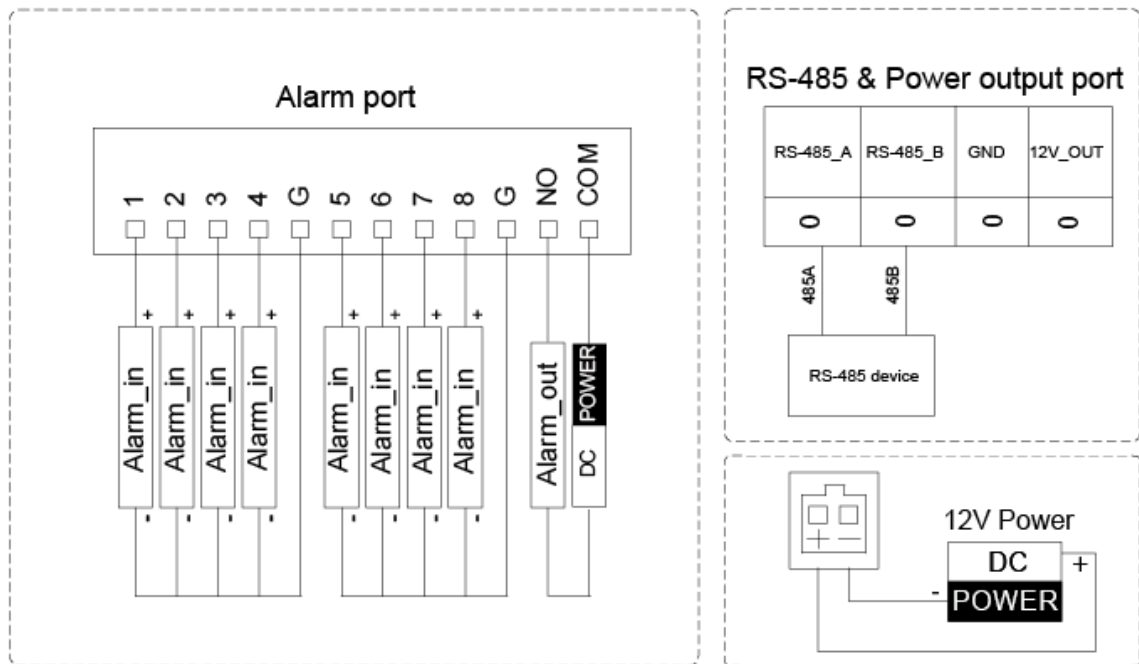


Table 1-2 Rear panel description

No.	Description
1	USB port, used by project personnel.
2	SD card slot.
3	Alarm ports, power cables, RS-485 port, and network ports are under the cover. For details, see Figure 1-3.

1.5 Cable Connections

Figure 1-3 Cable connection



2 Installation

Figure 2-1 Installation

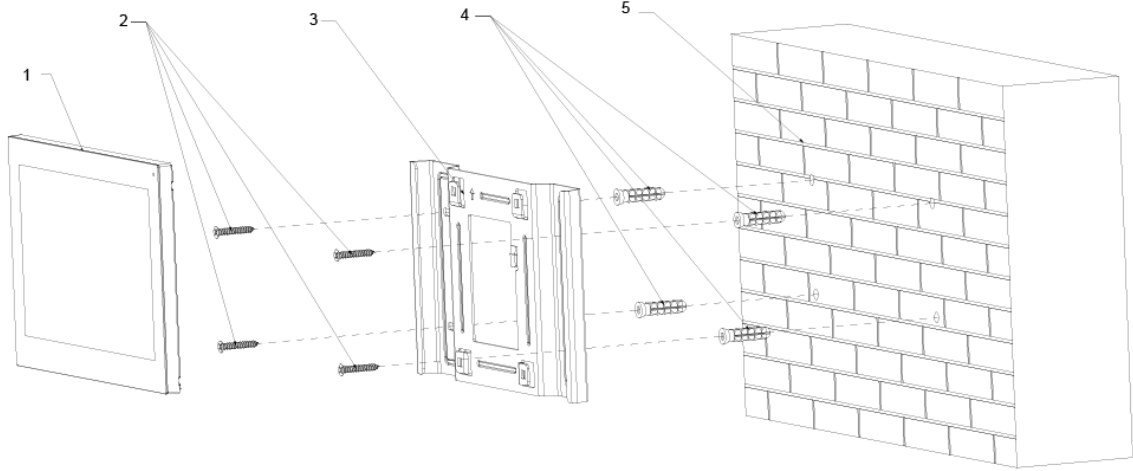


Table 2-1 Components

No.	Name	No.	Name
1	Indoor monitor	4	Anchor bolt
2	ST3 self-tapping screws	5	Wall
3	Bracket	—	—

Figure 2-2 Screw hole distances and diameters

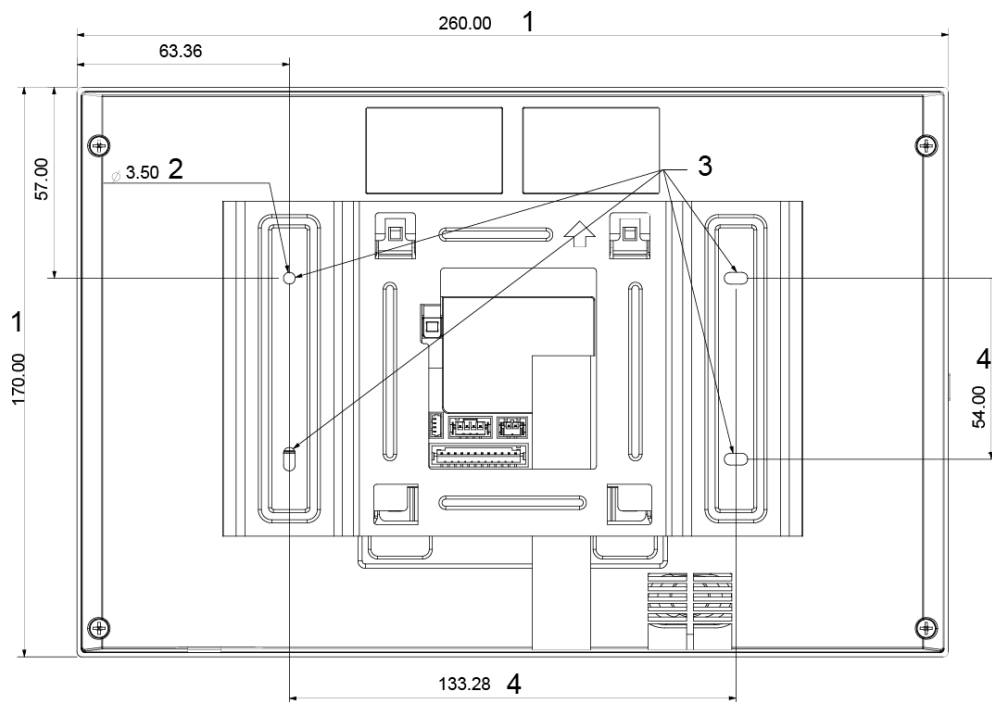


Table 2-2 Description of screw hole distances and diameters

No.	Description
1	Indoor monitor dimension
2	Bracket screw hole diameter
3	Bracket oval hole position
4	Screw hole distance

Step 1 Drill four screw holes in the wall according to holes on the bracket.

Step 2 Put anchor bolts into the screw holes.

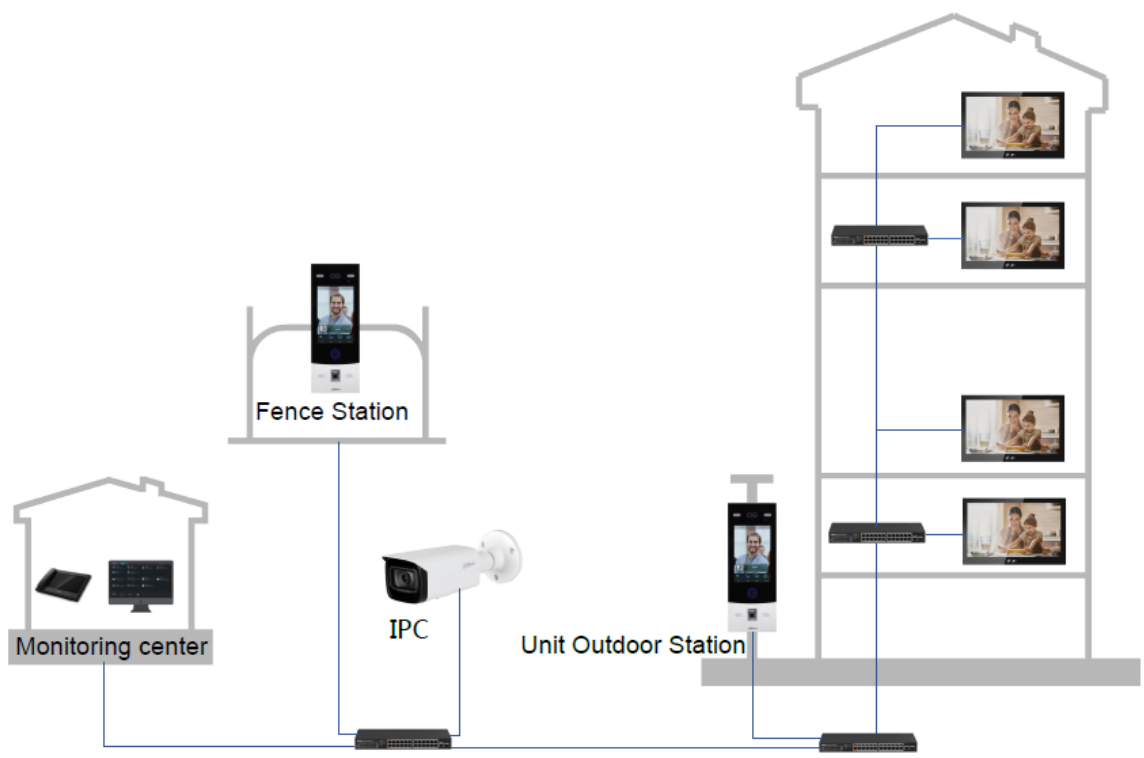
Step 3 Fix the indoor monitor on the wall with screws.

Step 4 Connect cables (power cable, network cables, and more).

The installation is completed.

3 Network Diagram

Figure 3-1 Network diagram



4 Configuration

This chapter introduces how to initialize, connect, and make primary configurations to the VTO and VTH devices to realize basic functions, including device management, calling, and monitoring.

4.1 Configuration Process



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

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

Step 2 Configure VTO. See "4.3 Configuring Door Station."

- 1) Initialize VTO. See "4.3.1 Initialization."
- 2) Configure VTO number. See "4.3.2 Configuring VTO Number."
- 3) Configure VTO network parameters. See "4.3.3 Configuring Network Parameters."
- 4) Configure SIP Server. See "4.3.4 Selecting SIP Servers."
- 5) Add VTO devices to the SIP server. See "4.3.5 Adding VTO Devices."
- 6) Add room number to the SIP server. See "4.3.6 Adding Room Number."

Step 3 Configure VTH. See the VTH users' manual.

Step 4 Verify configuration. See "4.5 Commissioning."

4.2 VDPConfig

You can download the "VDPConfig" and initialize device, modify IP address and upgrade system for multiple devices at the same time. For the detailed information, see the VDPConfig user's manual.

4.3 Configuring Door Station

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

4.3.1 Initialization

The default IP address of VTO is 192.168.1.110, and make sure that 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 browser on the PC, then enter the default IP address of the VTO in the address bar, and then press Enter on the keyboard.

The **Device Init** interface is displayed.

Figure 4-1 Device initialization

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

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 is finished.

Step 6 Click **OK**.

The login interface is displayed.

Figure 4-2 Login interface

The screenshot shows the 'WEB SERVICE2.O' login interface. At the top, the text 'WEB SERVICE2.O' is displayed in a stylized font. Below it are two input fields: 'Username' and 'Password'. To the right of the 'Password' field is a link that says 'Forget Password?'. At the bottom of the interface is a large blue button with the text 'Login' in white.

4.3.2 Configuring VTO Number

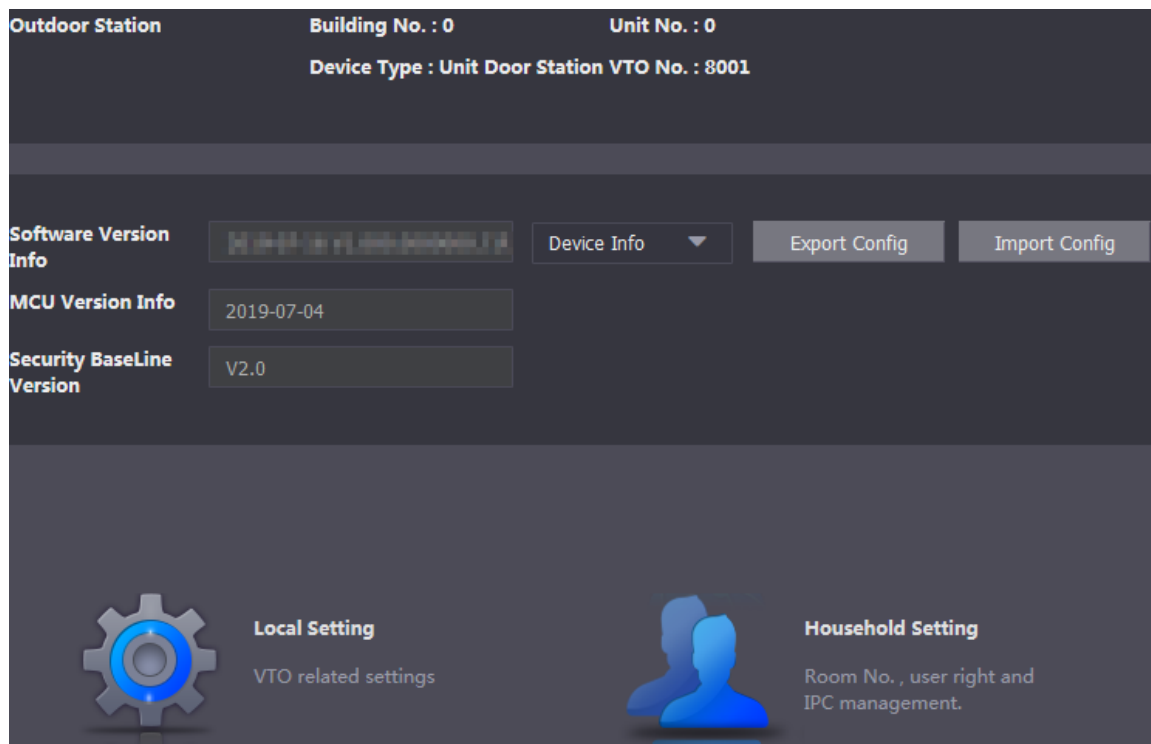
The VTO number can be used to differentiate each VTO, and it is normally configured according to building number.



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

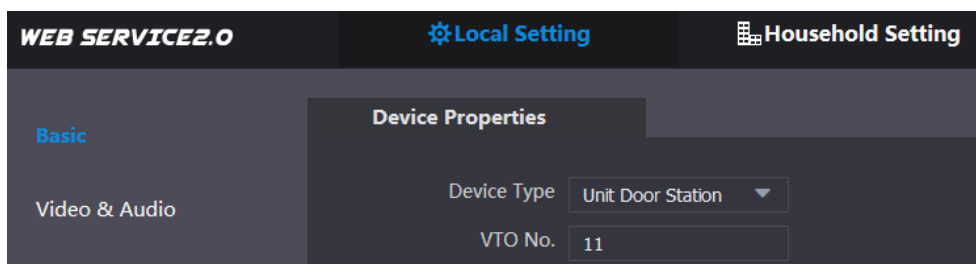
Step 1 Log in to the web interface of the VTO.

Figure 4-3 Main interface



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

Figure 4-4 Device properties



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

4.3.3 Configuring Network Parameters

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

The TCP/IP information is displayed.

Figure 4-5 TCP/IP information



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

The VTO will restart.



Make IP addresses of your PC and VTO are in the same network segment.

4.3.4 Selecting SIP Servers

The Session Initiation Protocol (SIP) is used for signaling and controlling multimedia communication sessions in applications of voice and video calls. A SIP server is an application provides information or direction to a user agent.

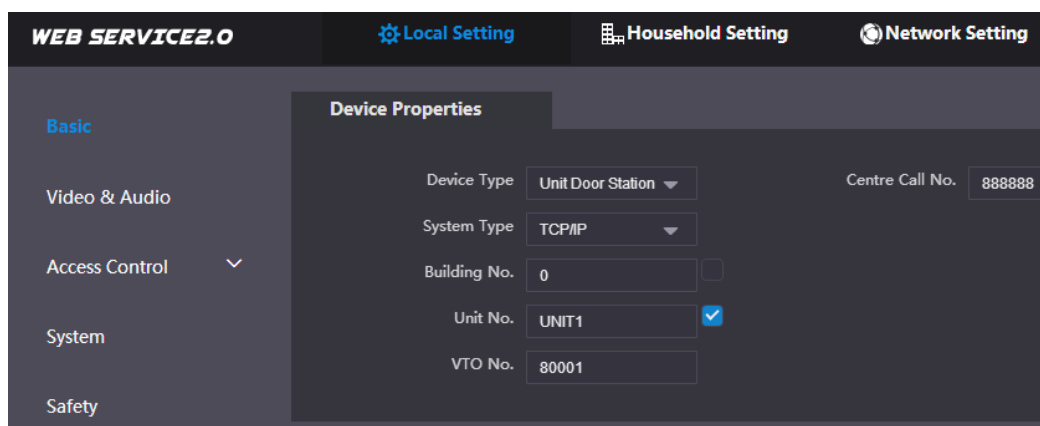
- When this VTO or another VTO works as SIP server, select **VTO** from the **Server Type** drop-down list. It applies to a scenario where there is only one building.
- When the platform (Express/DSS) works as SIP server, select **Express/DSS** from the **Server Type** drop-down list. It applies to a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

Step 1 Log in to the web page.

Step 2 On the homepage, select **Local Setting > Basic**.

The **Device Properties** interface is displayed.

Figure 4-6 Device properties



- 1) Select **TCP/IP** from the **System Type** drop-down list.



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

- 2) Click **OK** to save the settings.
- 3) Restart the device manually, or wait for auto restart to make the settings effective.

Step 3 Log in to web interface again.

Step 4 Select **Network Setting > SIP Server**.

The **SIP Server** interface is displayed.

Figure 4-7 SIP server (1)

Step 5 Select a SIP server.

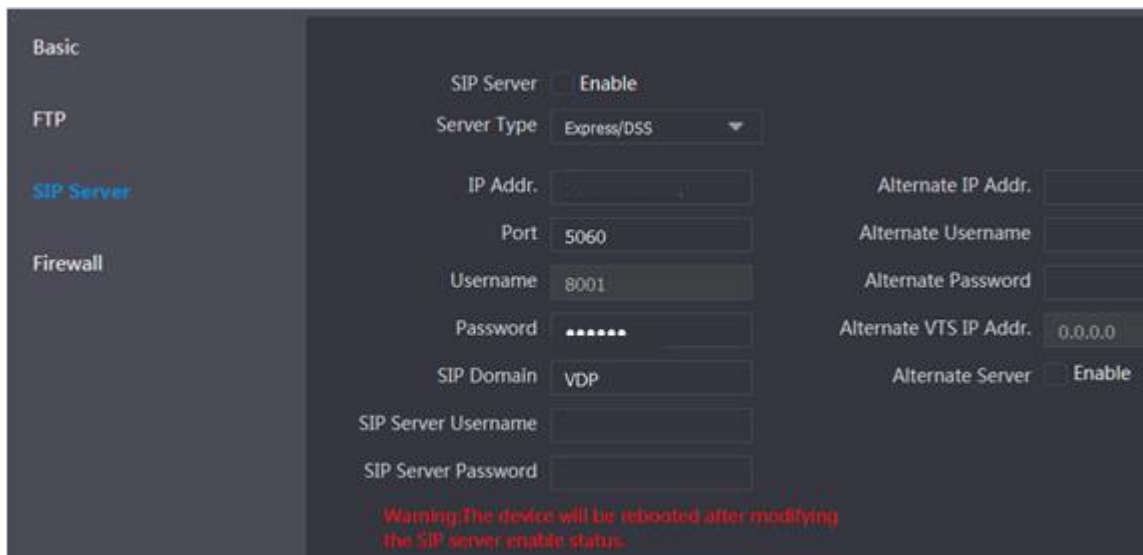
VTO as SIP server

- Step 1 Select **Enable** next to **SIP Server**.
- Step 2 Select **VTO** from the **Server Type** drop-down list
- Step 3 Configure parameters (see Table 4-1 for details).
- Step 4 Click **Save**.
The VTO will restart automatically.

Platform (Express/DSS) as a SIP server

- Step 1 Select **Network Setting > SIP Server**.
The **SIP Server** interface is displayed.


Figure 4-8 SIP server (2)



Step 2 Select **Express/DSS** from the **Server Type** drop-down list.

Step 3 Set parameters according to Table 4-1.

Table 4-1 SIP server parameter description

Parameter	Description
IP Address	IP address of SIP server.
Port	<ul style="list-style-type: none"> It is 5060 by default when another VTO works as SIP server. It is 5080 by default when the platform works as SIP server.
Username/Password	Use default value.
SIP Domain	<ul style="list-style-type: none"> It shall be VDP when another VTO works as SIP server. It can be null or keep default value when the platform works as SIP server.
Login Username/Password	Username and password to log in to SIP server.
Alternate IP Addr.	IP address of the alternate server.  If alternate server is enabled and Express or DSS works as SIP server, when Express or DSS cannot work normally, the VTO will be used as SIP server.
Alternate Username	Username and password for logging in to the alternate server.
Alternate Password	
Alternate VTS IP Addr.	IP address of the alternate VTS.
Alternate Server	After entering alternate IP address, username, password, and VTS IP address, you need to select the Enable checkbox to enable the alternate server.

Step 4 Click **OK** to save the configuration.

The VTO will restart automatically.



When the platform works as SIP server, if it is necessary to set Building No. and Building Unit No., enable **Support Building** and **Support Unit** first.

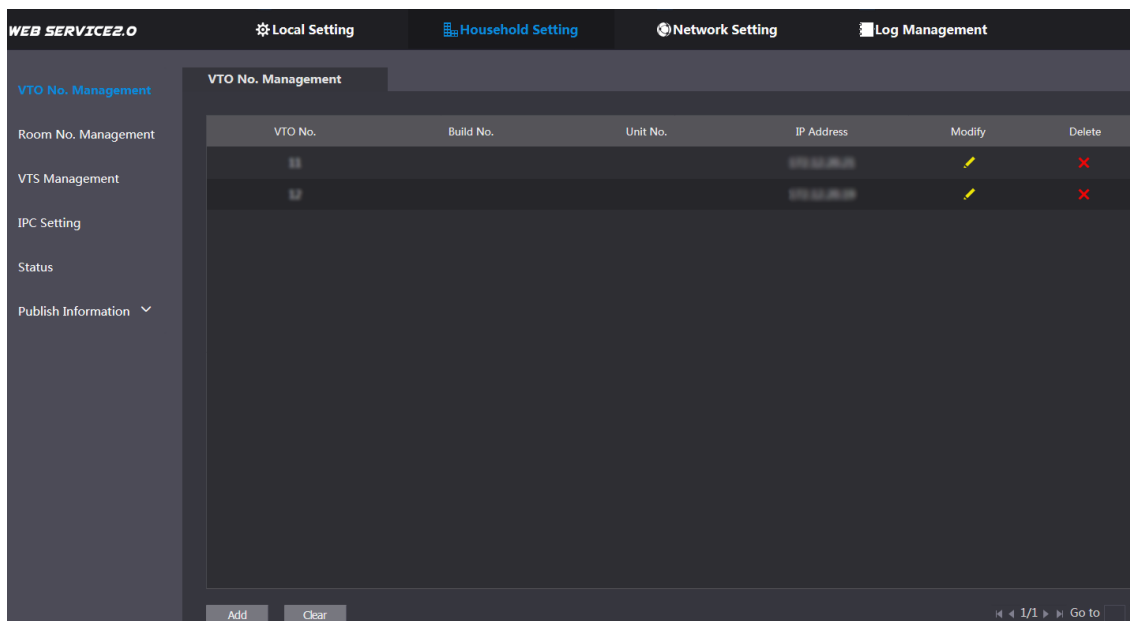
4.3.5 Adding VTO Devices

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

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

The **VTO No. Management** interface is displayed.

Figure 4-9 VTO No. management



Step 2 Click **Add**.

The **Add** interface is displayed.

Figure 4-10 Add VTO

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

Table 4-2 Add VTO configuration

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

Step 4 Click **Save**.

4.3.6 Adding Room Number

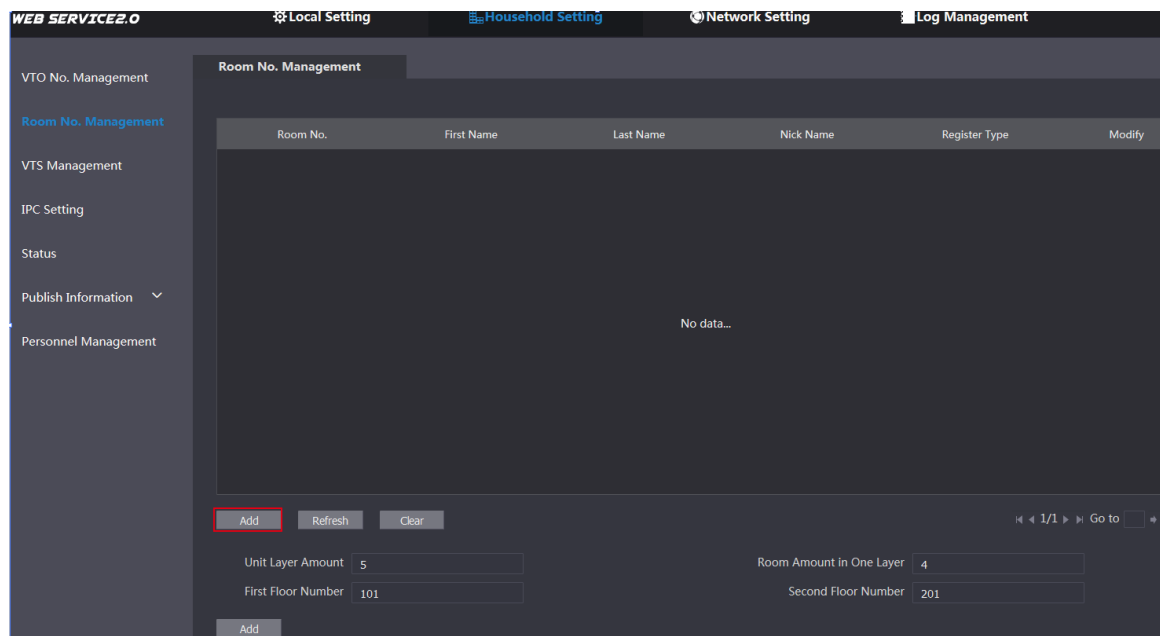
You can add the planned room number to the SIP server, and then configure the room number on VTH devices to connect them to the network. VTO works as SIP server will be taken as an example, and if you use other servers as SIP server, see the corresponding manual for the details.



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

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

Figure 4-11 Room No. management




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

- Add single room number
- 1) Click **Add**. See Figure 4-11.
The **Add** interface is displayed. See Figure 4-12.

Figure 4-12 Add single room number

2) Configure room information.

Table 4-3 Room information

Parameter	Description
First Name	Enter the information you need to differentiate each room.
Last Name	
Nick Name	
Room No.	<p>The room number you planned.</p>  <ul style="list-style-type: none"> If you use multiple VTH devices, the room number of the master VTH should be "room number#0", and the room number of the extension VTH should be "room number#1", "room number#2", and so on. You can have 10 extension VTH devices at most for one master VTH.
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.

- Add room number in batch

- Configure the Unit Layer Amount, Room Amount in One Layer, First Floor Number, and Second Floor Number according to the actual condition.
- Click **Add** at the bottom left of the interface. See Figure 4-13.

Figure 4-13 Add in batch

All the added room numbers are displayed. Click **Refresh** to view the latest status, and click **Clear** to delete all the room numbers.

4.4 Configuring Indoor Monitor

You need to configure IP, Wi-Fi, door station parameter, SIP server, and more on the indoor monitor, and then the indoor monitor can communicate with door stations and the management center.

4.4.1 Initialization

Set password and email.

- Password: The password is used when administrators need to go to the project mode.
- Email: The email is used when you need to reset the password.



The default IP address of the indoor monitor is 192.168.1.108.

Step 1 Connect the indoor monitor to power source.

WELCOME is displayed, and then the initialization interface is displayed.

Step 2 Enter the password, confirm password, and email.

Step 3 Tap **OK**.







The main menu is displayed.

Figure 4-14 Main menu



Table 4-4 Description of screw hole distances and diameters

No.	Name	Description
1	Room number	Number of the room where the indoor monitor is installed.
2	Date and time	Current time and date are displayed here.
3	Arm and disarm	Shortcut icons to arm or disarm are displayed here. The four icons represent at home mode, away from home mode, sleep mode, and customizable mode. Select Arm Mode or Disarm Mode first, and then tap the icons to arm or disarm.
4	Status bar	<ul style="list-style-type: none"> • : The wired network is not connected. • : The wired network is connected. • : The indoor monitor failed to be connected to the SIP server. If this icon does not appear, then the indoor monitor is connected to the SIP server. • : The SD card is inserted and recognized. • : The indoor monitor is in the Do not disturb mode. It is disabled by default.
5	SOS	Tap the SOS icon, the indoor monitor will call the management center.
6	Do not disturb	Tap the icon, and then you can set do not disturb period. You need to enable DND Period first, and then you can do do-not-disturb

No.	Name	Description
		settings. For details, see DND by tapping  .
7	Turn off screen	Tap the icon, and then the screen will be turned off.
8	Function buttons	<ul style="list-style-type: none"> • : Tap the icon, and then you can watch videos from door stations and IP cameras. • : Tap the icon, and then text messages and videos left by visitors, or public notices released by the management center will be displayed. • : Tap the icon, and then you can make calls to other indoor monitors and the management center; and you can also view call logs and your contacts on this interface. • : Tap the icon, and then you can view alarm logs, do alarm settings for 6 areas as needed. • : Tap the icon, and then you can select ringtones for different door stations, Do Not Disturb period, call forward mode (there are three options: Always, Busy, and No Answer), and other settings. • Sound Recorder: You can record your voice messages to the SD card or to the indoor monitor. • Calculator: You can do calculations through the calculator. • Files: You can view files like images, videos, audio, and recently produced files. • Calendar: You can view date through the indoor monitor, and create notes, schedules, and plans. • Gallery: You can view images captured by door stations (VTO) or IP cameras.

4.4.2 Network Settings

Connect the indoor monitor to the network, and then the indoor monitor can communicate with other devices.

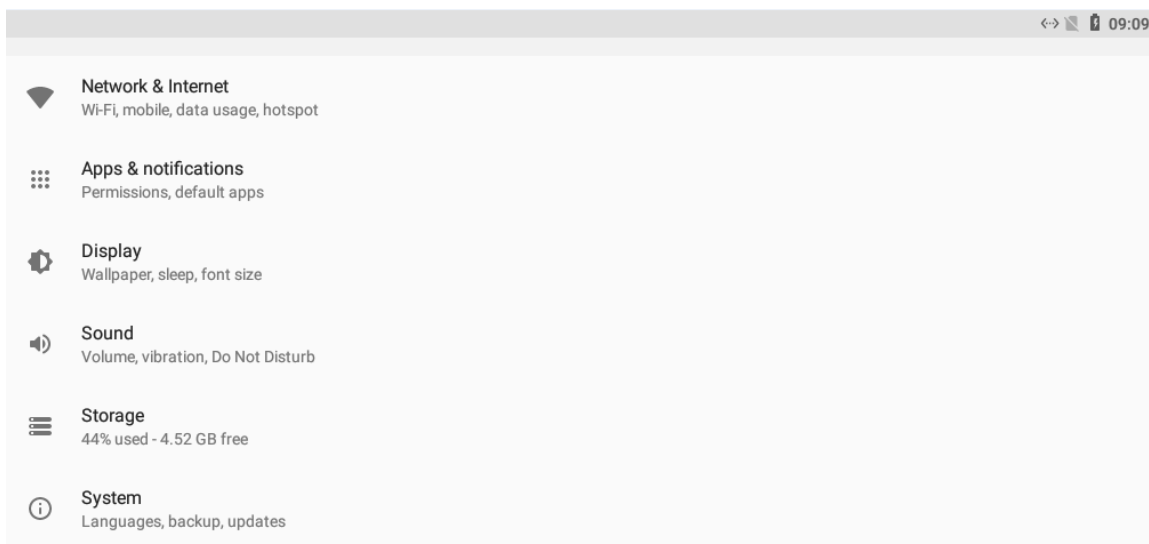
Wired Network

Make sure that IP address of the indoor monitor and IP address of door stations are in the same network segment; otherwise the indoor monitor cannot acquire door station information.

Step 1 Tap the **Settings** icon.



The network settings interface is displayed.

Figure 4-15 Network settings



Step 2 Configure parameters.

Table 4-5 Parameter description

Parameter	Description	
Network & Internet	<p>You can choose to enable Wi-Fi or not by tapping .</p> <ul style="list-style-type: none"> Tap , and then available Wi-Fi networks will be displayed. You can select Ethernet IP mode. There are two options: Static and DHCP. 	
Apps & notifications	<p>You can view the recently opened apps, apps opened by default, app permissions (apps using location, microphone, and camera), app notifications, and special app access.</p>	
Display	<p>You can adjust display brightness, display sleep duration, font size, and display size.</p>	
Sound	<p>You can adjust media volume and notification volume. You can also select to use default notification sound and default alarm sound.</p>	
Storage	<p>Spaces used and spaces left can be viewed. You can delete unwanted files as needed.</p>	
System	Languages & Input	<p>Languages: You can select languages as needed.</p> <p>Keyboard & Inputs: There are two options: Virtual keyboard and physical keyboard.</p> <p>Input assistance: You can use spell checker, autofill service (not available at present), personal dictionary, and text-to-speech output as needed. Pointer speed can also be adjusted.</p>
	Backup	<p>You can use backup storage as needed.</p>
	Reset options	<p>You can reset Wi-Fi, mobile, and Bluetooth, and app preferences. You can also erase all data, which means restoring the indoor monitor to factory settings.</p>
	About tablet	<p>You can see details (battery status, network status, legal information, model, android version, Android security patch</p>

Parameter	Description
	level, baseband version, Kernel version, build number, and more) about the indoor monitor.

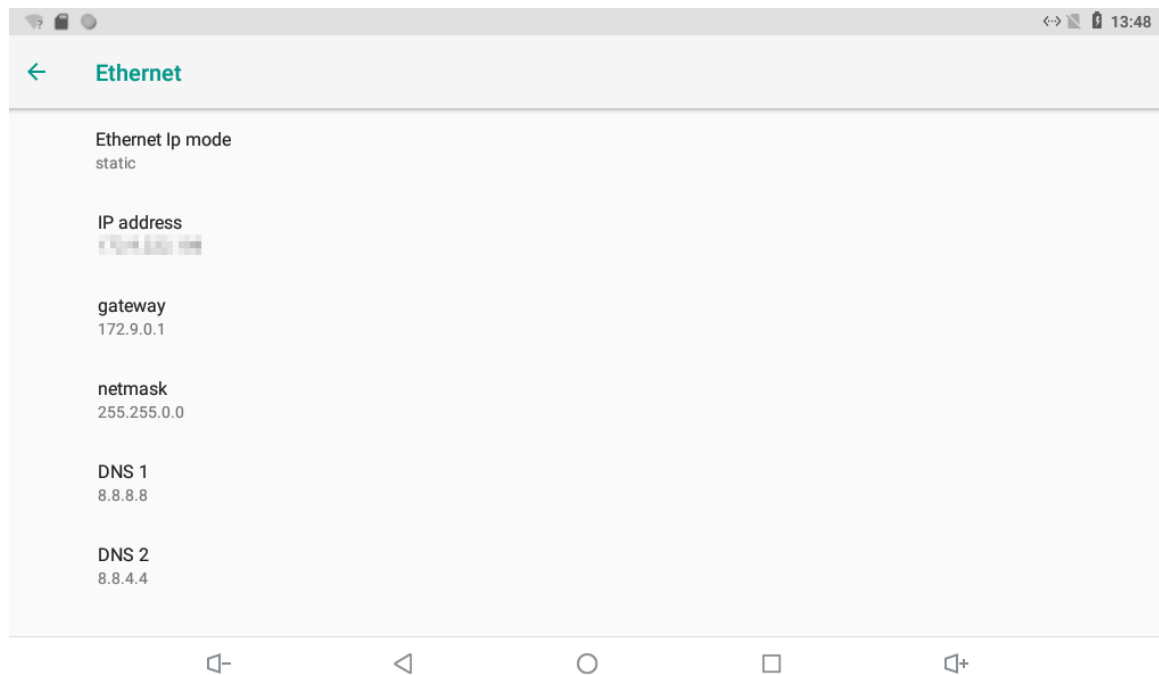
Step 3 Tap Network & Internet.

The **Network & Internet** interface is displayed.

Step 4 Tap Ethernet.

The **Ethernet** interface is displayed.

Figure 4-16 Network setting



Step 5 Tap Ethernet Ip mode.

- Select static: Enter IP address, gateway, netmask, and then tap **CONNECT**.
- Select dhcp: Tap dhcp, the IP information will be automatically acquired.


Wireless network

Step 1 Tap the **Settings** icon.

The network settings interface is displayed.

Step 2 Tap Network & Internet.

The **Network & Internet** interface is displayed.

Step 3 Tap , the Wi-Fi is enabled.


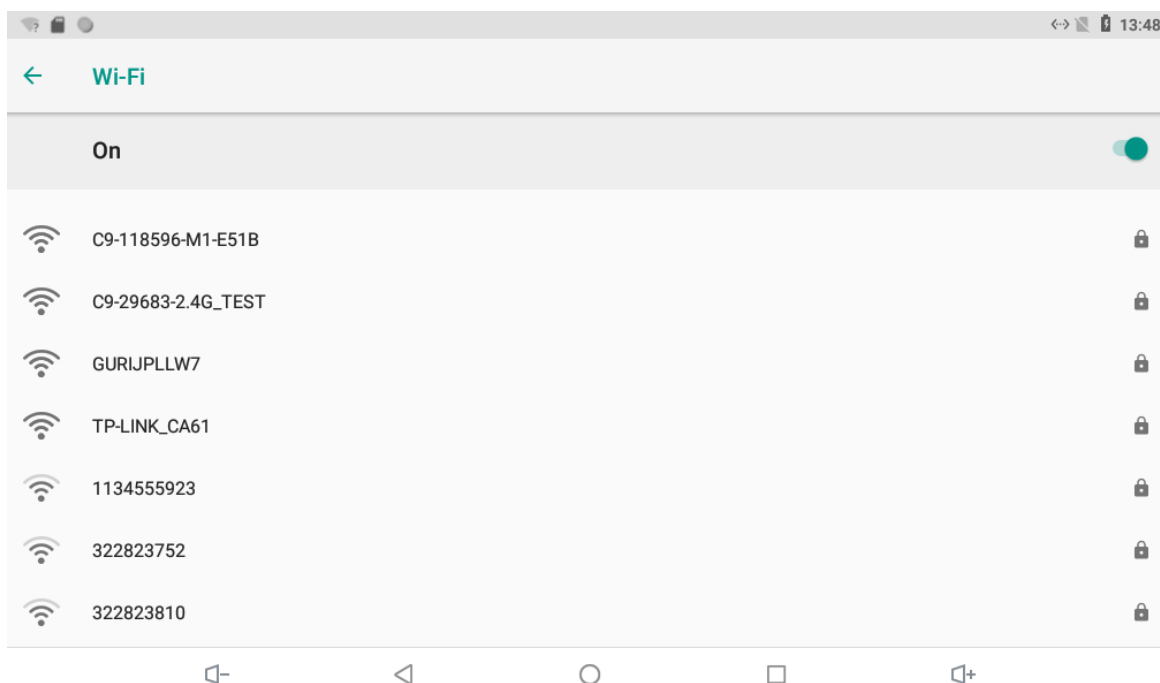
Step 4 Tap , the available wireless networks are displayed.

Figure 4-17 Wi-Fi



Step 5 Select a wireless network.

Step 6 Enter the password.

Step 7 Tap CONNECT.

The network is connected.

4.4.3 Project Settings


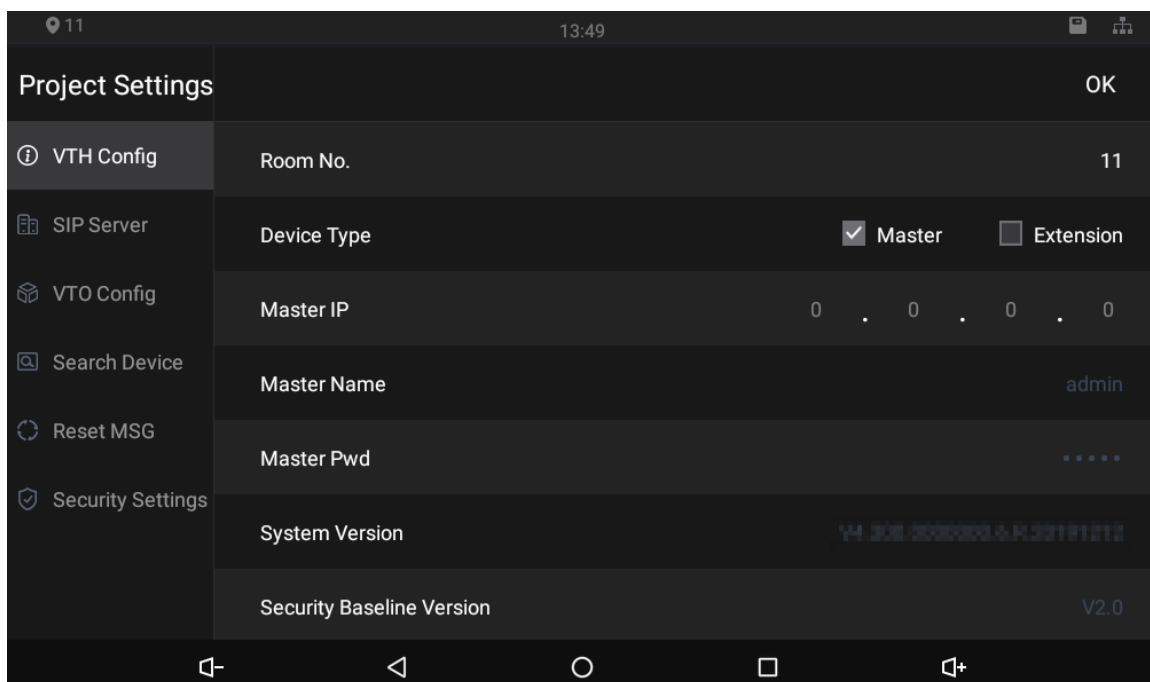
Tap and hold the icon , enter the password (123456 by default), and then the **Project Settings** interface will be displayed.

Figure 4-18 Project settings



4.4.3.1 VTH Config

- Room No.: Number of the room where the indoor monitor is installed.
- Device Type: There are two options: Master and Extension.
 - ◇ Master: If the indoor monitor that you are operating works as the master station, you need to select **Master**.
 - ◇ Extension: If the indoor monitor works as an extension, you need to select Extension.
- Master IP: When the indoor monitor works as an extension, you need to enter IP address of the master station.
- Master Name: Keep the default value.
- Master Pwd: Keep the default value.
- System Version: You can view system version of the indoor monitor.
- Security Baseline Version: You can view security baseline version of the indoor monitor.

4.4.3.2 SIP Server

You need to enter SIP server information, and then the whole video door phone system can communicate with each other.

Tap **SIP Server**, and then the SIP server interface is displayed.

Figure 4-19 SIP server (1)

Parameter	Description
Server IP	172 232 . 111
Network Port	5060
User Name	11
Password
Domain	
Login Name	admin
Login Pwd

Table 4-6 SIP server description

Parameter	Description
Server IP	<ul style="list-style-type: none"> ● When the platform works as SIP server, server IP is IP address of the management platform. ● When a door station works as SIP server, server IP is IP address of the door station.
Network Port	<ul style="list-style-type: none"> ● When the platform works as SIP server, network port is 5080. ● When VTO works as SIP server, network port is 5060.

Parameter	Description
User Name	Use default value.
Password	
Domain	Registration domain of SIP server, which can be null. When VTO works as SIP server, registration domain of SIP server shall be VDP.
Login Name	User name and password to login to web page of the SIP server.
Login Pwd	
Status	Enable the SIP server status, and then the SIP server can start to work.

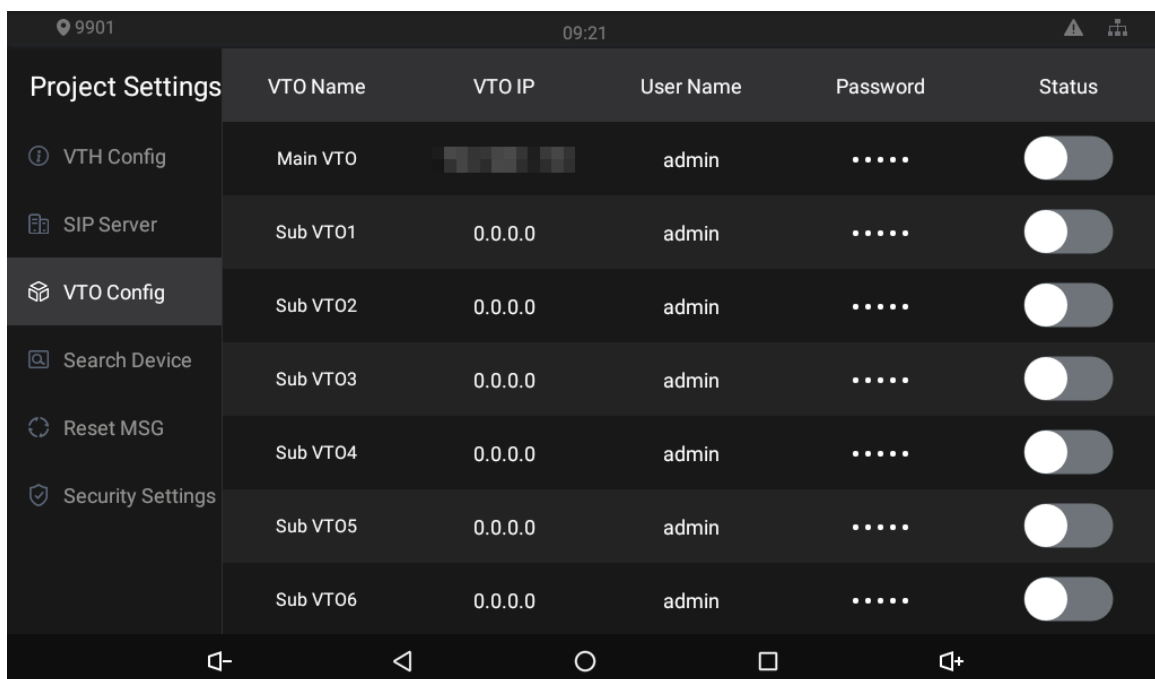
4.4.3.3 VTO Config

You need to add door stations to the indoor monitor.

Step 1 Tap VTO Config,

The **VTO Config** interface is displayed.

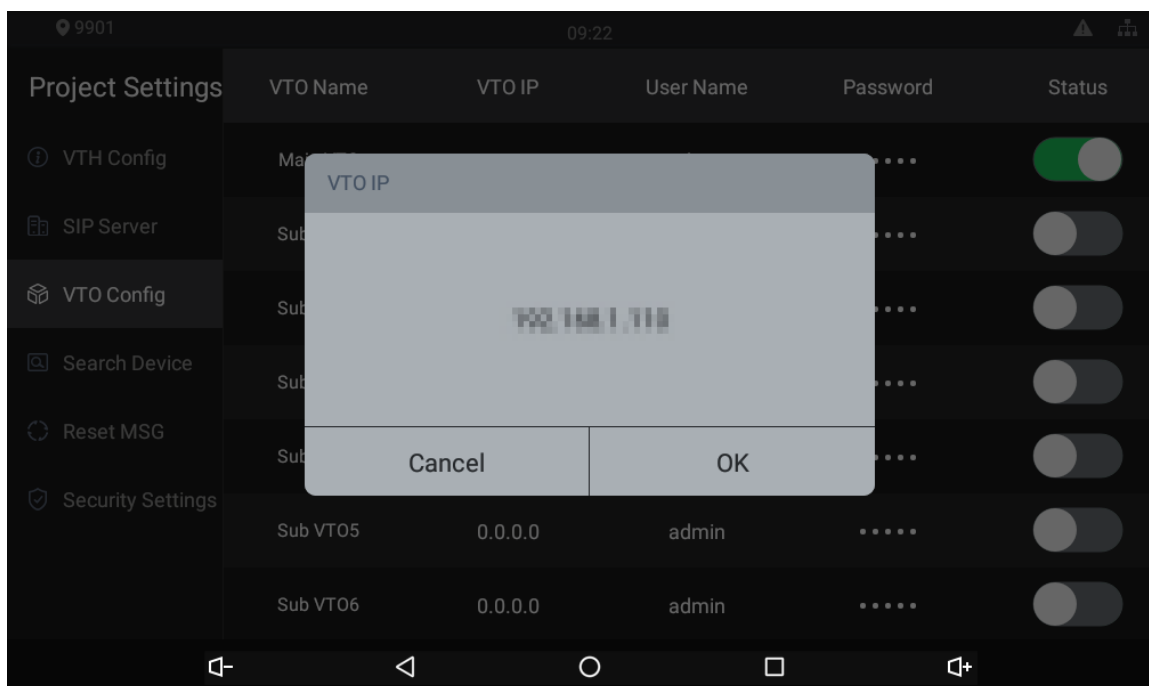
Figure 4-20 Door station (VTO) configuration



Step 2 Tap a door station (VTO).

The **VTO IP** interface is displayed.

Figure 4-21 VTO IP



Step 3 Tap the default IP, and then the on-screen keyboard appears.

Step 4 Enter the door station (VTO) IP, user name, and password (used to log in to the door station web interface).



- You can add 20 door stations (one main door station and 19 sub door stations) to the indoor monitor.
- Make sure that user name and password you entered here are the same as the user name and password used when logging in to the door station web interface.

Step 5 Tap to enable the door station.

4.4.3.4 Searching Device

Tap the **Search Device** icon, and then the system starts to search devices automatically. You can add the device found to the indoor monitor.

Figure 4-22 Searching device (1)

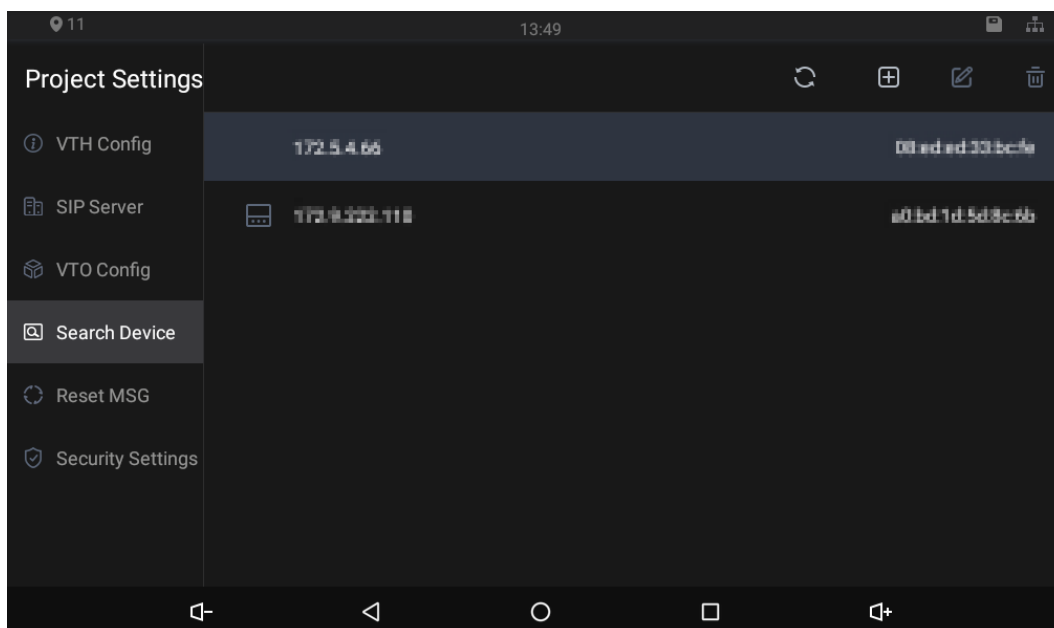
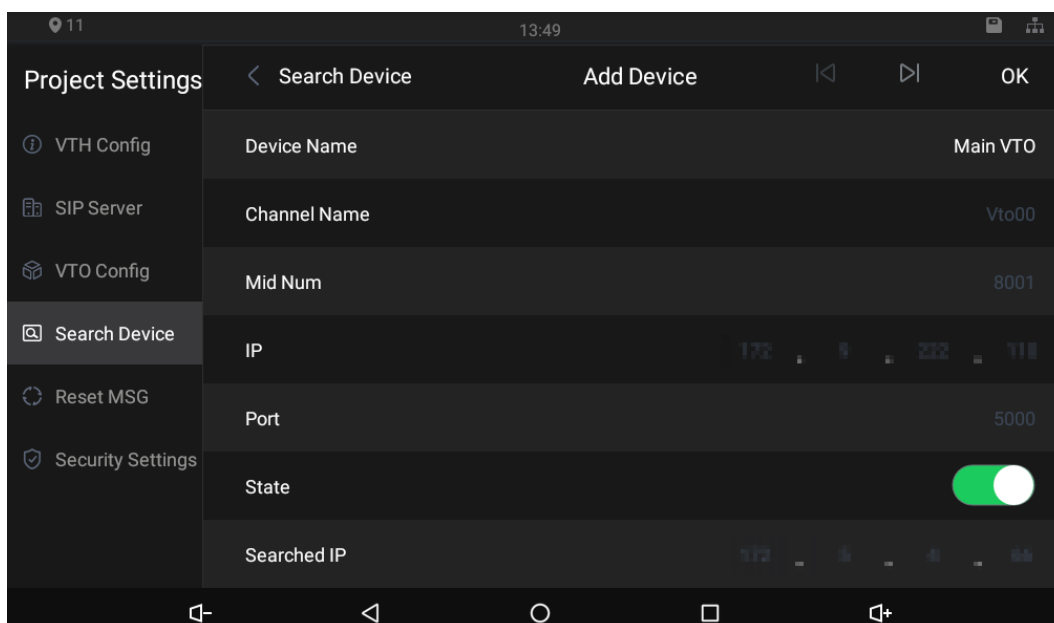


Figure 4-23 Searching device (2)




4.4.3.5 Resetting Password

You can change the email address that you use to reset your password.



You need to enable the **Resst Password** first if you want to reset the password.

Step 1 Tap and hold .

The password Verification interface is displayed.

Step 2 Tap **Forgot password?**.

The warning interface is displayed.

Step 3 Tap **OK**.

The QR code appears.

Step 4 Scan the QR code with any app that is with scanning function.

A string will be displayed.

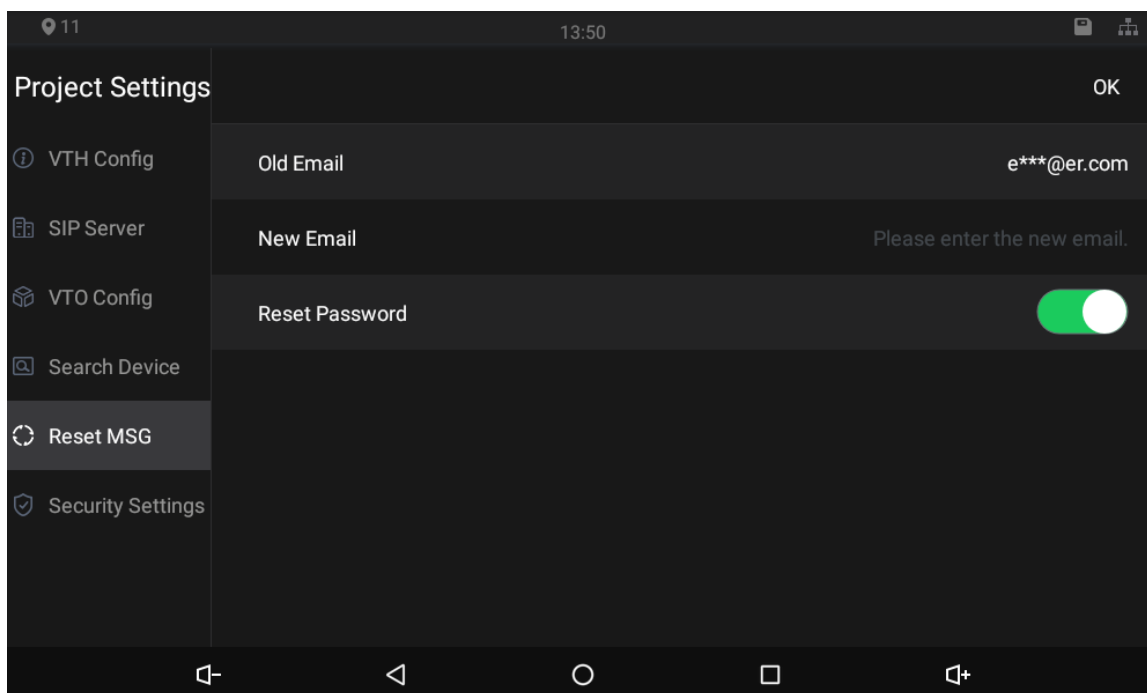
Step 5 Send the string to support_gpwd@htmicrochip.com with the email address you set on the **Reset MSG** interface.

A safe number will be sent to your email address.

Step 6 Tap **Next** and then enter the new password, confirm password, and safe number.

The password is reset.

Figure 4-24 Reset password



4.4.3.6 Security Settings

You need to enable the trusted list, and then trusted devices can be added. You can also use Dshell to provide you with the ability to develop custom analysis modules which help you understand events of cyber intrusion.

Figure 4-25 Enable trusted list

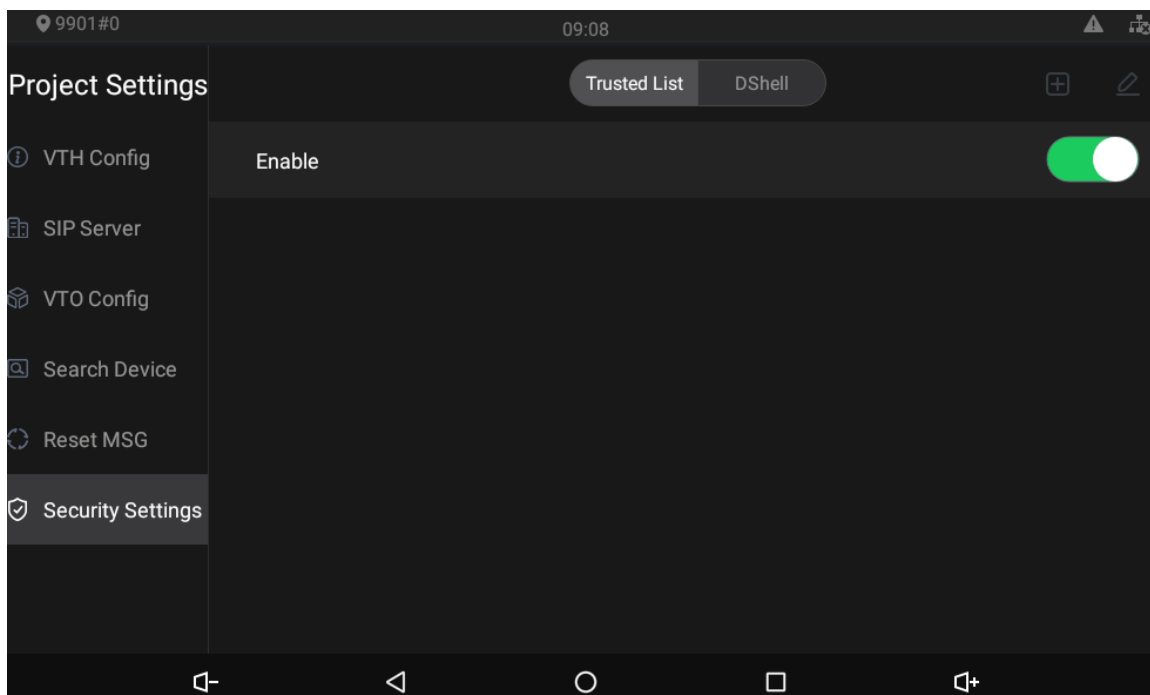
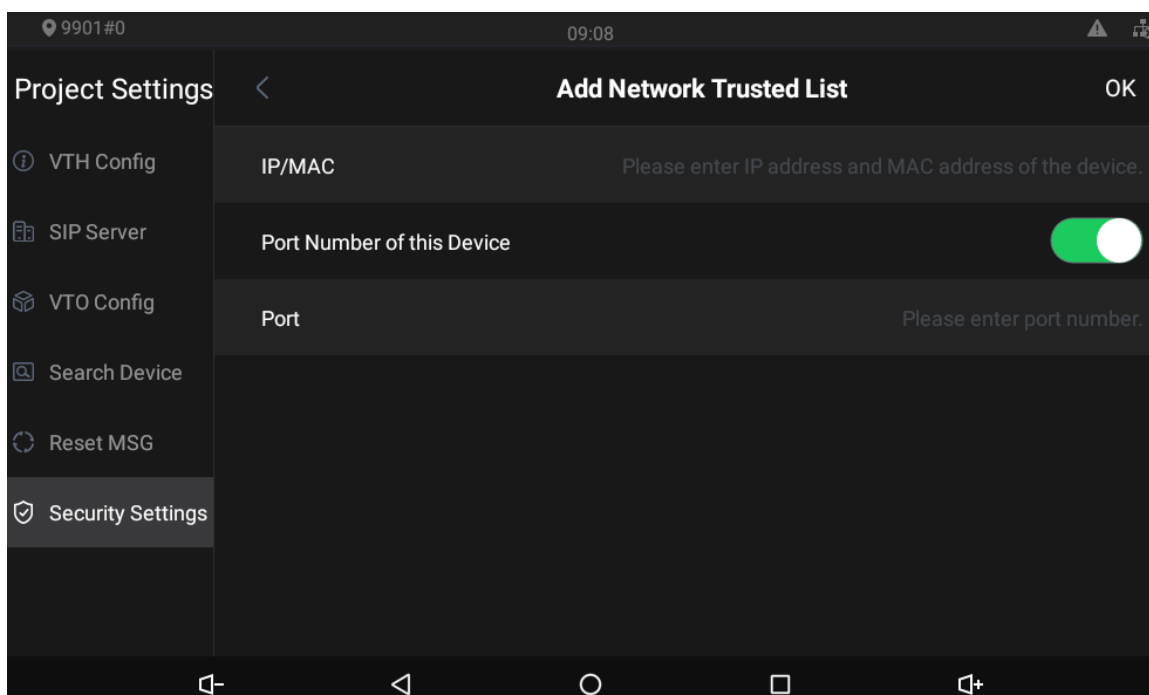




Figure 4-26 Add network trusted list



You need to tap  on the Enable trusted list interface, and then the **Add Network Trusted List** will be displayed.

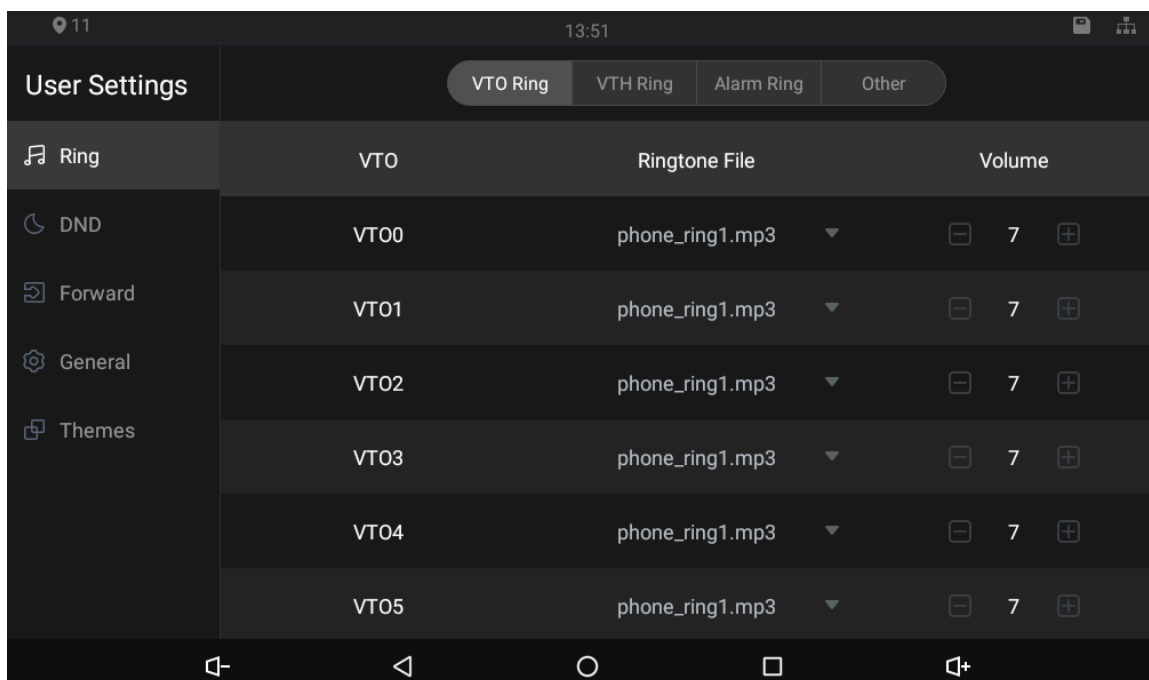
4.4.4 General Settings

Tap , and then the user setting interface is displayed. You can select ringtones for different door stations, Do Not Disturb period, call forward mode (there are three options: Always, Busy, and No Answer), and other settings.

4.4.4.1 Ring

On this interface, you can select ringtones for different door stations.

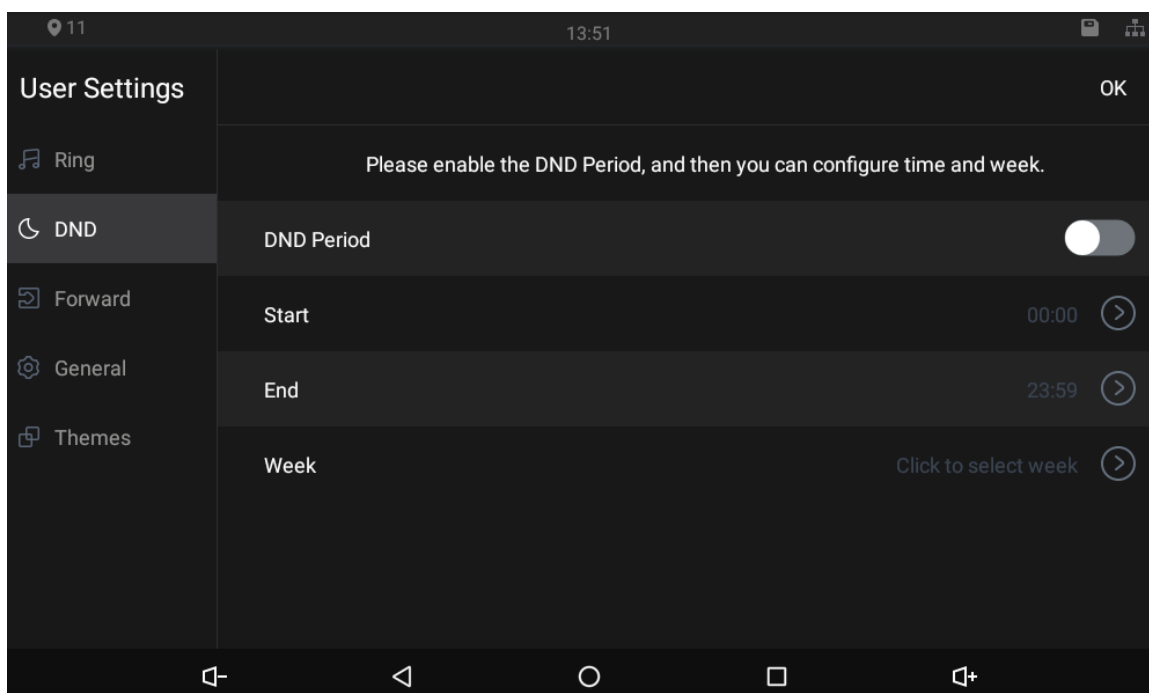
Figure 4-27 Ring



4.4.4.2 DND

Enable **DND Period** first, and then you can set do not disturb period for each day.

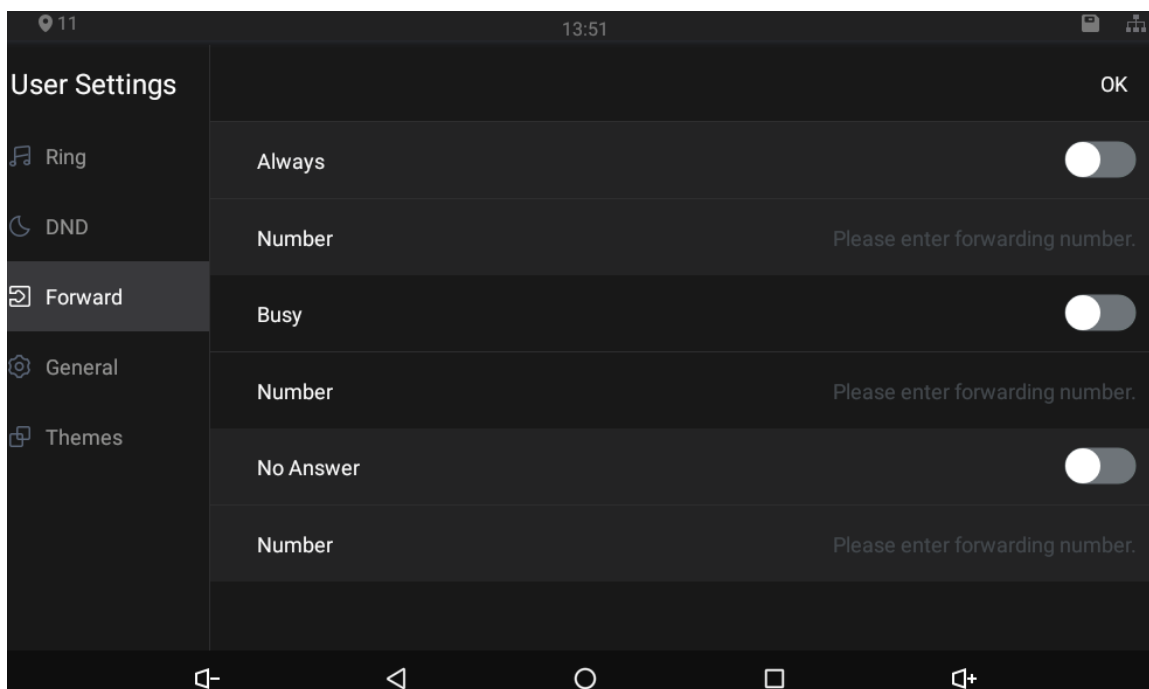
Figure 4-28 DND



4.4.4.3 Forward

When calls come in, they will be forwarded to the management center during the hours that you have set. There are three options: **Always**, **Busy**, and **No Answer**.

Figure 4-29 Forward



- **Always:** Whenever calls come in, they will always be forwarded.
- **Busy:** If calls come in when you are talking to others over the indoor monitor, the calls will be forwarded.
- **No Answer:** When the coming calls are not answered, they will be forwarded.

4.4.4.4 Password

On the **General** interface, you can set new passwords for arm and disarm. Register new users and download apps by scanning QR codes, and set other parameters.

Figure 4-30 Password

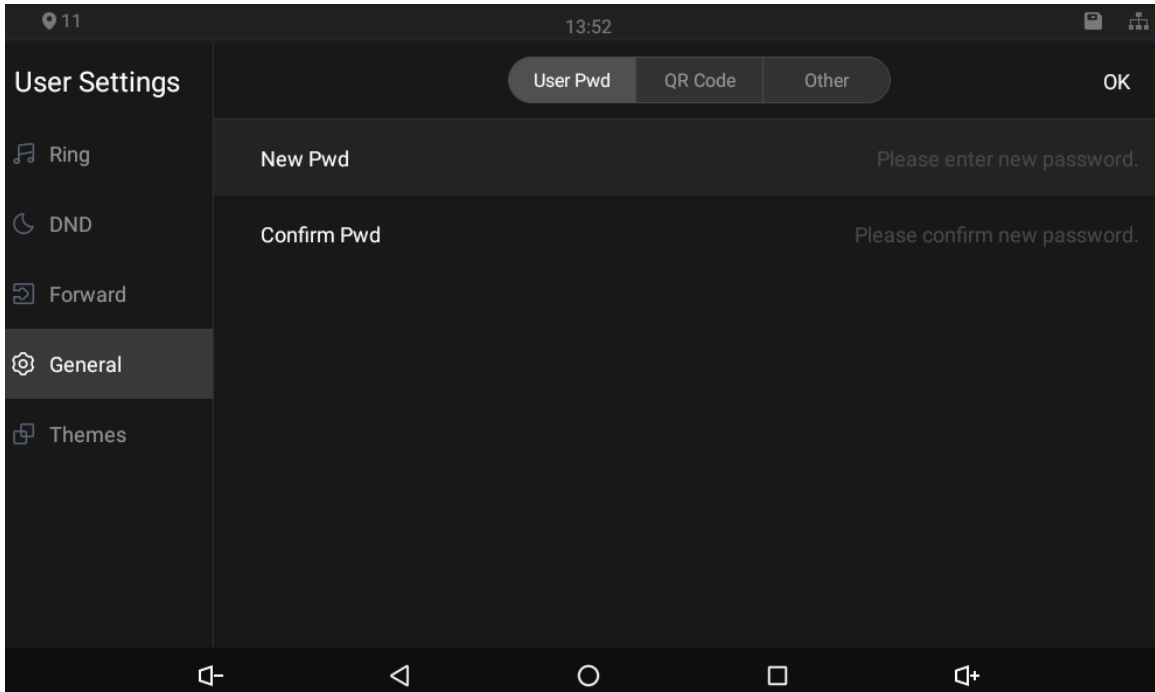


Figure 4-31 QR code

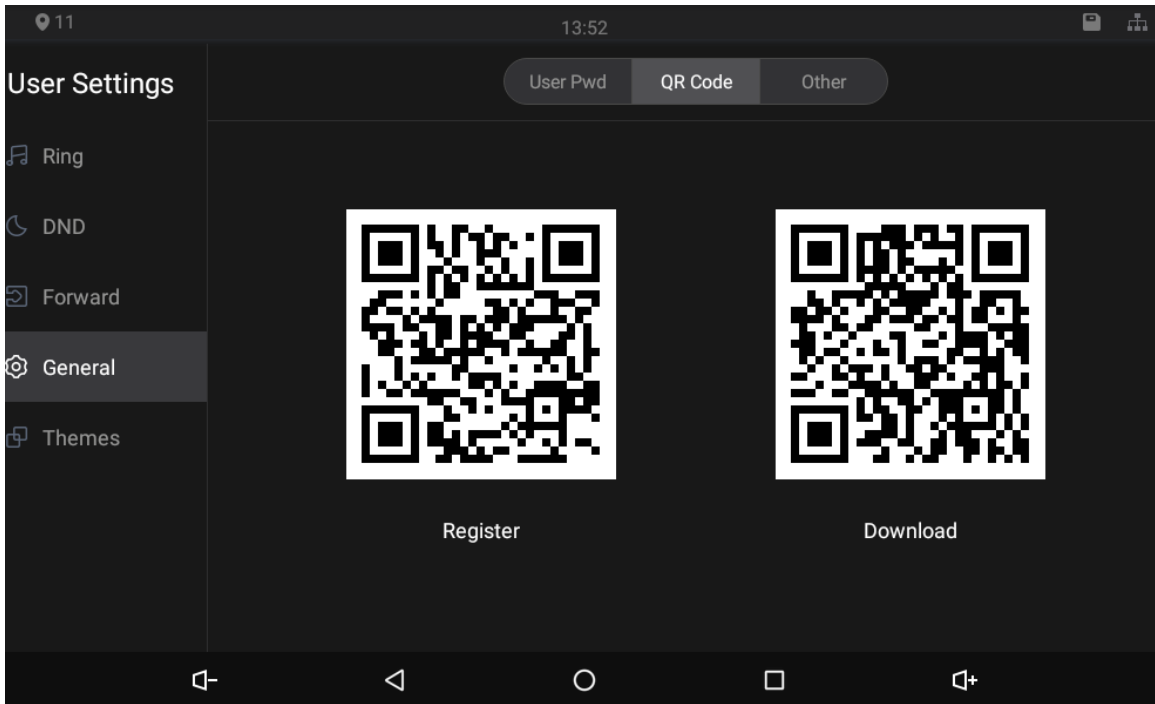
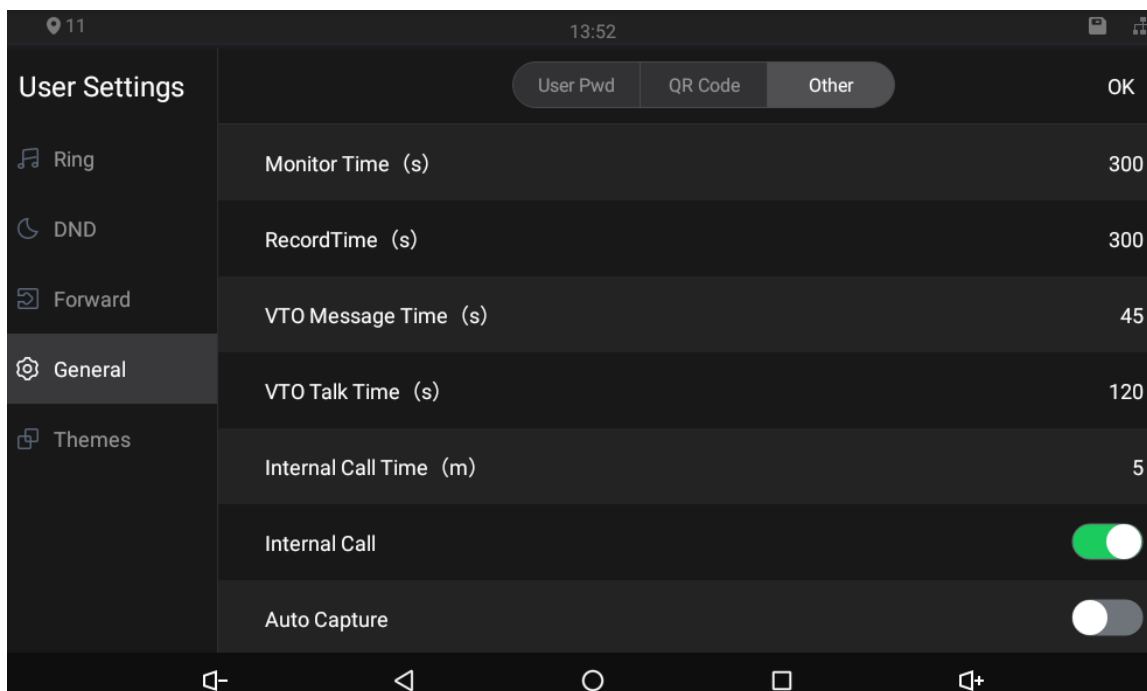


Figure 4-32 Other

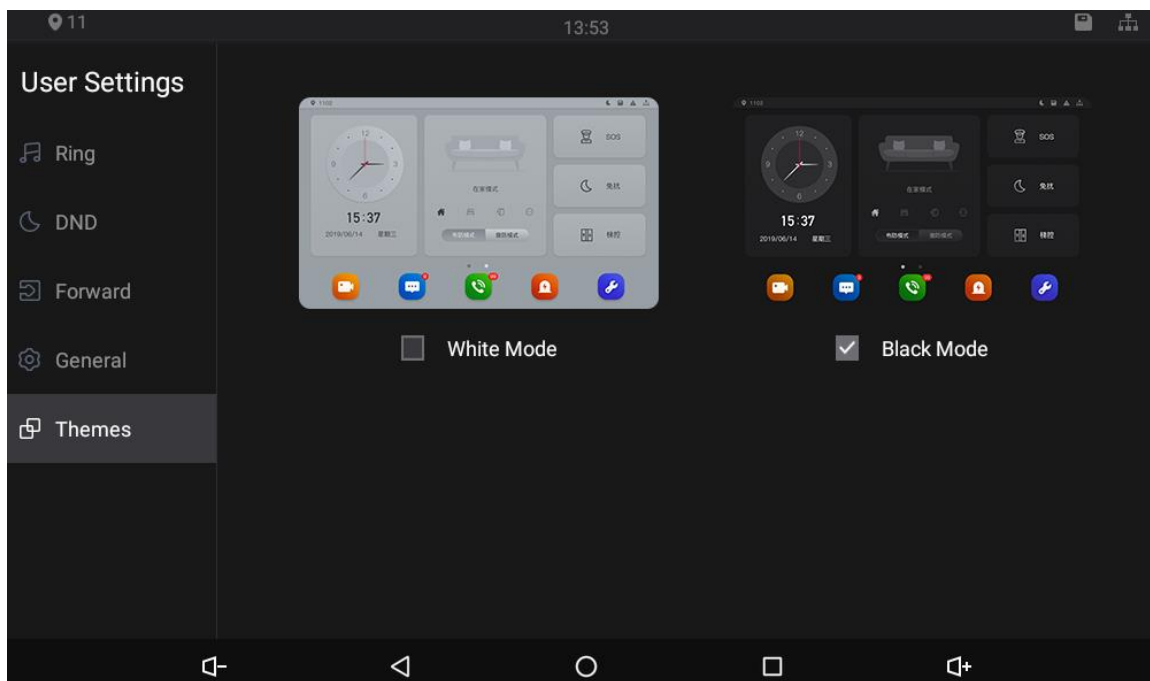


- Monitor Time (s): You can watch monitoring images from the indoor monitor for at most 300 seconds a time.
- Record Time (s): You can record at most 300-second audio files a time on the indoor monitor.
- VTO Message Time (s): Visitors can only leave an at most 90-second message a time on the door station (VTO).
- VTO Talk Time (s): Visitors can talk to you through the door station (VTO) for at most 300 seconds a time.
- Internal Call Time (s): You can talk to other indoor monitors for at most 60 seconds a time.
- Internal Call: After the Internal Call is enabled, you can call other indoor monitors from the indoor monitor you are operating.
- Auto Capture: After the Auto Capture function is enabled, if a visitor called you but you did not answer the call, the door station (VTO) would take three images of the visitor standing in front of the door station.

4.4.4.5 Themes

You can select a theme for your indoor monitor. There are two options: **White Mode** and **Black Mode**.

Figure 4-33 Themes



4.4.5 Alarm Settings

4.4.5.1 Wire Zone

Set alarm settings for six areas, and then if emergencies happen, alarms will be triggered.



Tap , the **Alarm** interface is displayed.

Figure 4-34 Wire zone

Alarm		WireZone					Alarm Out	OK
Alarm record	Area	Type	NO/NC	Status	Enter (Sec.)	Exit (Sec.)		
Alarm	1	Infrared	NO	Instant	0s	0s		
Mode	2	Infrared	NO	Instant	0s	0s		
	3	Infrared	NO	Instant	0s	0s		
	4	Infrared	NO	Instant	0s	0s		
	5	Infrared	NO	Instant	0s	0s		
	6	Infrared	NO	Instant	0s	0s		

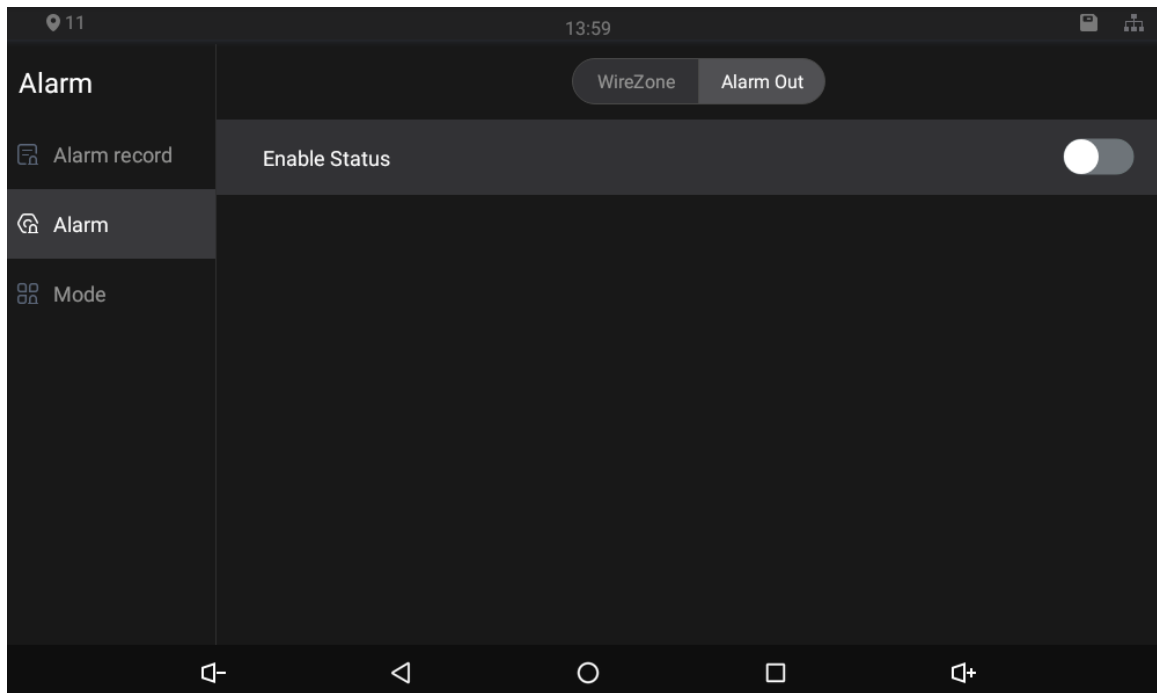
Table 4-7 SIP server description

Parameter	Description
Area	Area numbers. There are 8 areas in total. They cannot be modified.
Type	There are 8 types of alarms: Infrared, gas sensor, smoke sensor, urgency button, door sensor, stolen, perimeter, and doorbell. Select alarm types according to detector types.
NO/NC	Select NO (normally open) or NC (normally closed) according to detector types. It shall be the same as detector type.
Status	<p>There are 5 statuses: instant, delay, bypass, remote, and 24-hour protection zone.</p> <ul style="list-style-type: none"> Instant: In Arm Mode, if you selected this status for an area, once alarms are triggered, the indoor monitor will give out voice prompt immediately. Delay: In Arm Mode, if you selected this status for an area, once alarms are triggered, the indoor monitor will give out voice prompt a period later. Bypass: If you selected the bypass status for an area, after the area has been armed and alarms are triggered; there will be no voice prompt. Once the area is disarmed, alarm status will be back to normal. Remove: When you select Arm Mode and Disarm Mode for an area in "at home mode", "away from home mode", "sleep mode", and "customizable mode", the status of this area will not be changed. 24-hour protection zone: If you selected this status for an area, whenever alarms are triggered, voice prompt will always be given out.
Enter (Sec.)	In the Arm Mode, after you have selected this status for an area, there will be no voice prompt when you enter the area from a disarmed area within the period you set; after that period has passed in the Arm Mode, voice prompt will be given out.
Exit (Sec.)	<p>In the Arm Mode, after you have selected this status for an area, there will be no voice prompt unit you have exit the area within the period you set. After that period has passed in the Arm Mode, voice prompt will be given out when alarms are triggered.</p>  <p>If you have selected this status for more than one area, and then prompts of the area with the longest period will be displayed on the indoor monitor.</p>

4.4.5.2 Alarm Output

After you have enabled the alarm output function, when there are people making calls to the indoor monitor from other devices, alarm devices will send alarms.

Figure 4-35 Alarm output



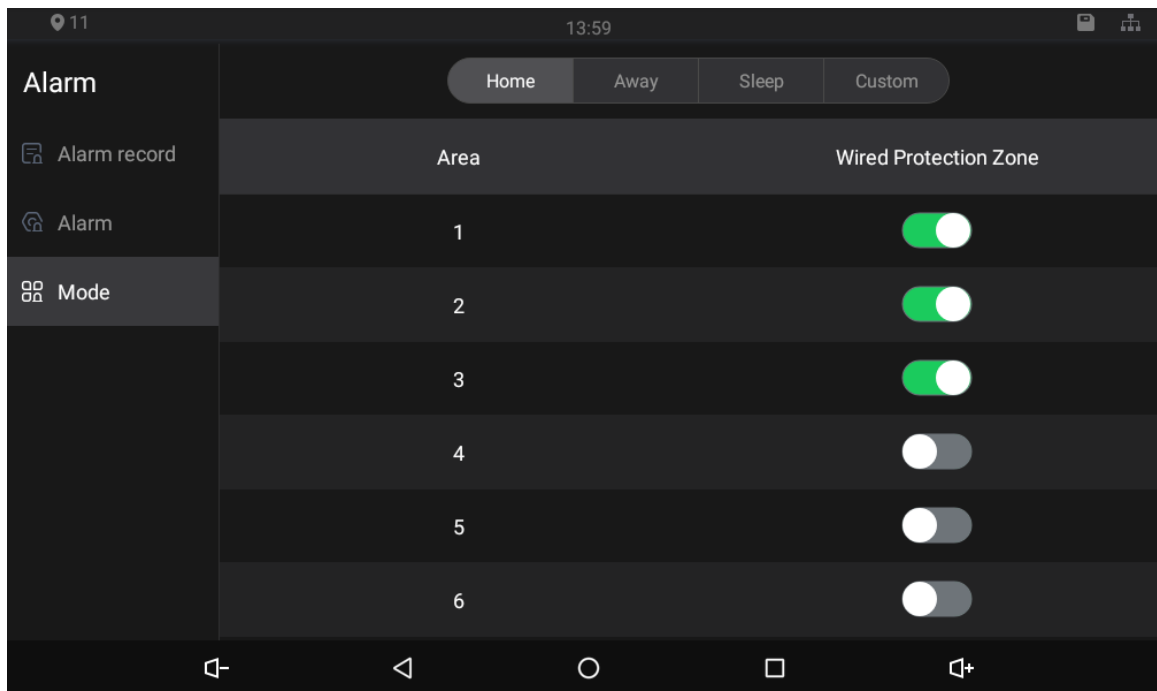
4.4.5.3 Alarm Mode

There are four modes: Home, away, sleep, and custom. Select modes as needed.



Only in the Disarm Mode can you enable alarm modes for the areas.

Figure 4-36 Alarm mode



4.4.6 Elevator Control

Elevator control modules can be connected to the indoor monitor. You can make the elevator come to your floor through the indoor monitor. Once elevator control module is connected, there is an elevator control button on the main menu of the indoor monitor

4.5 Commissioning

4.5.1 Watching Monitoring Video

Tap , and the Monitor interface is displayed.


On the indoor monitor, you can watch videos captured by door stations and IP cameras. You can also put door stations and IP cameras that you like into the **Favorite** folder by tapping  at the lower right corner of each device.

Figure 4-37 Monitor (1)

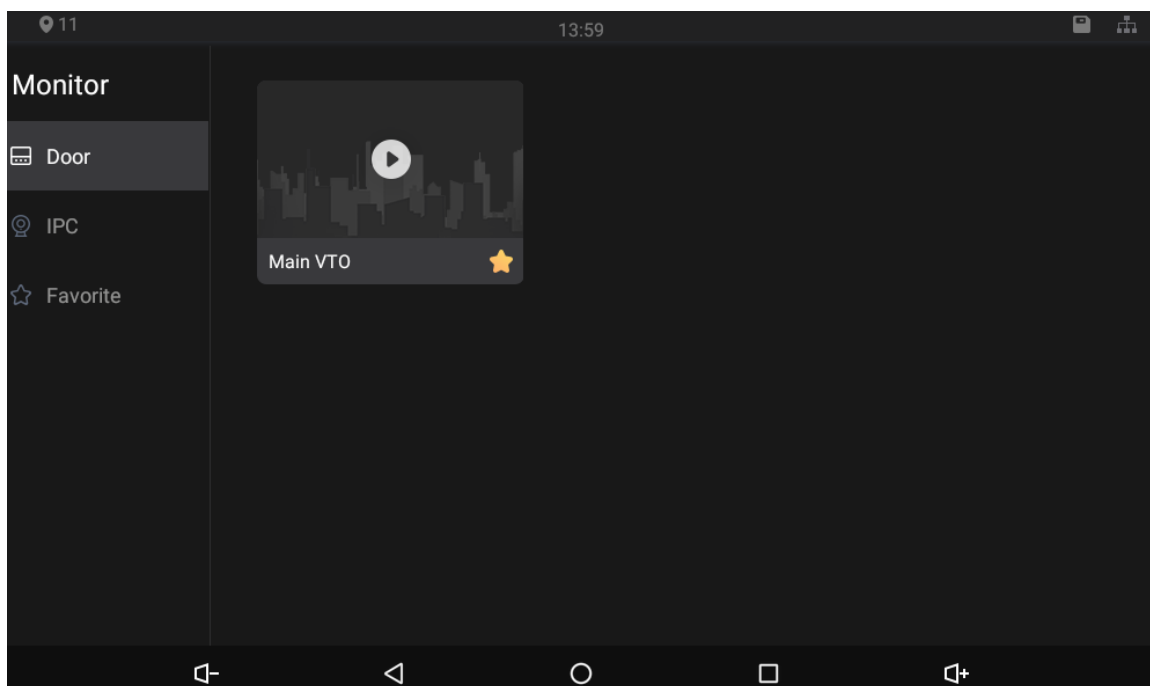


Figure 4-38 Monitor (2)

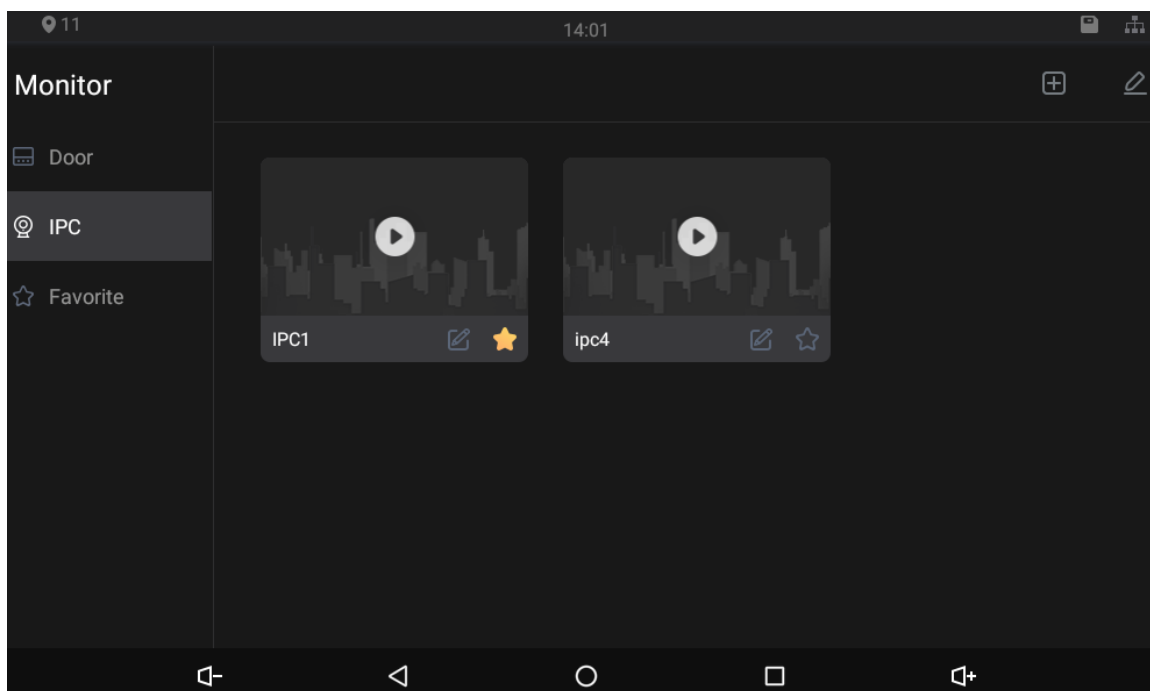
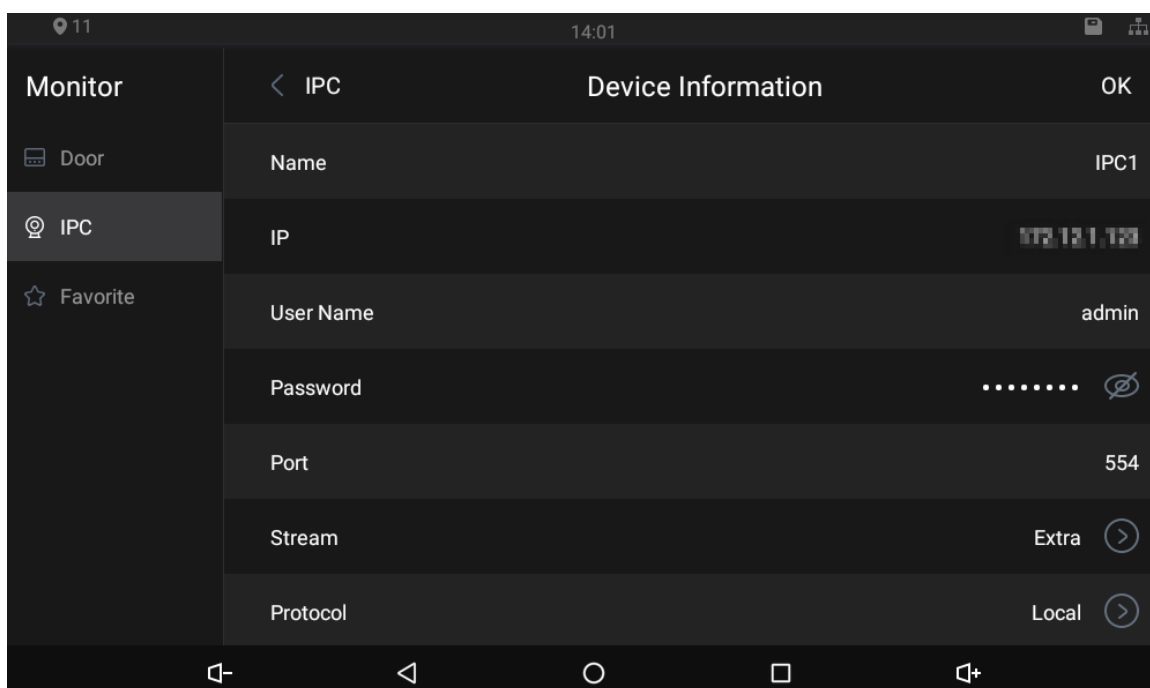








Figure 4-39 IPC information




- : Tap the icon to turn down the volume.
- : Tap the icon to go to the previous page.
- : Tap the icon to go to the main menu.
- : Tap the icon, and all thumbnails of interfaces you have opened will be displayed. Select an interface and slide it to the left or right to close the interface.
- : Tap the icon to turn up the volume.

4.5.2 Checking Messages

Tap , and then text messages and videos left by visitors, or public notices released by the management center will be displayed.

4.5.3 Making Calls

Tap , and then you can call other indoor monitors and the management center; and you can also view call logs and your contacts on this interface.

You can also call the indoor monitor from door stations.

Figure 4-40 Making calls

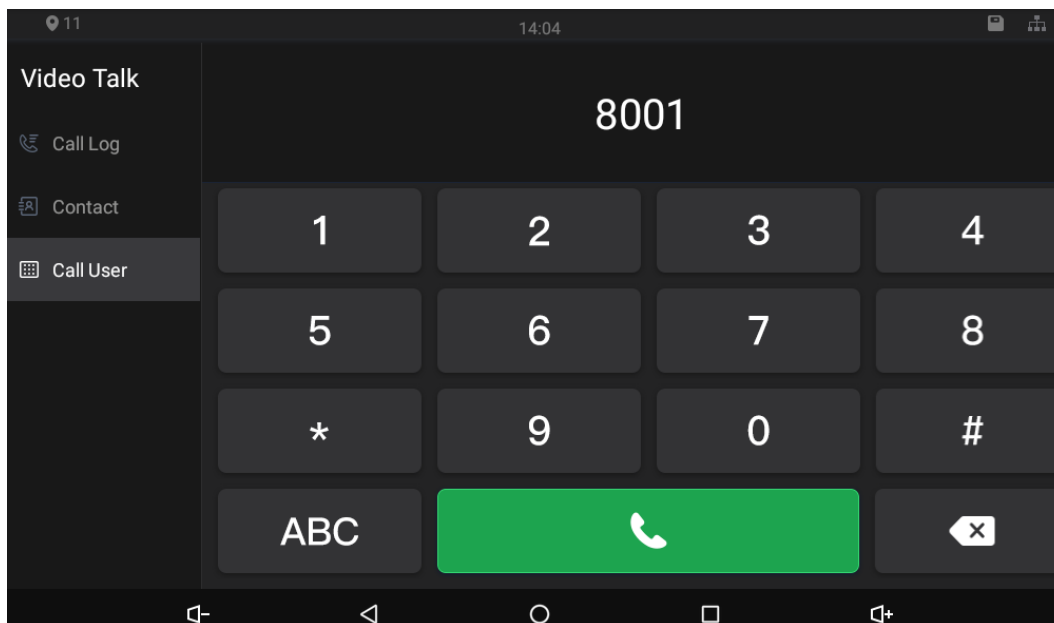







Figure 4-41 Calling





- When Figure 4-28 appears, it means that SD card has been inserted into the indoor monitor. If SD card is not inserted, the video recording icon  and snapshot icon  cannot be used.
- You can tap the unlock icon   to unlock doors. If the icons turn grey, the unlock function cannot be used.

4.5.4 Viewing Alarms Logs

Tap , and then the **Alarm** interface is displayed. Peripheral alarm modules can be connected to the indoor monitor. You can view alarm logs, do alarm settings for 6 areas as needed. There are 7 types of alarms: Infrared, gas sensor, smoke sensor, urgency button, door sensor, stolen, and perimeter.



Disarm all alarms first, and then you can do alarm settings.

Figure 4-42 Viewing alarm prompt

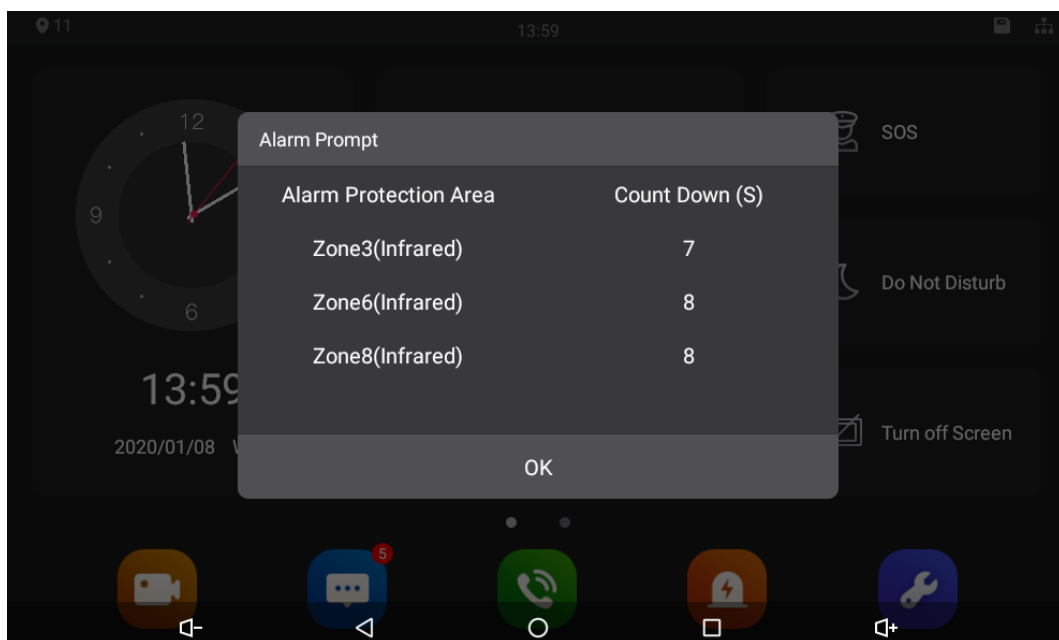
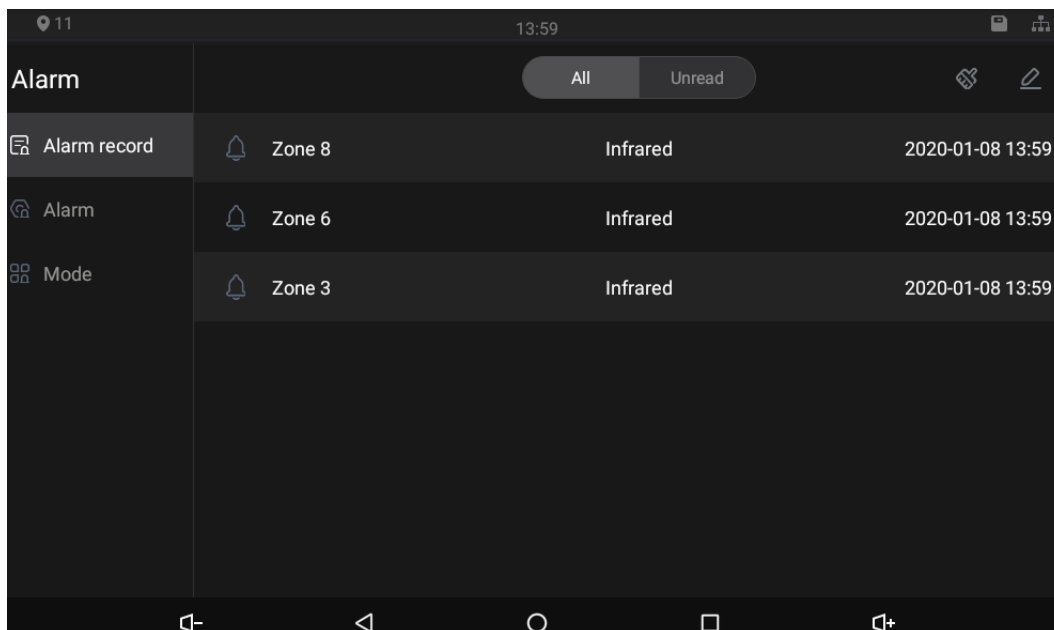


Figure 4-43 Viewing alarm record



4.5.5 Viewing Information

Figure 4-44 Viewing guest message

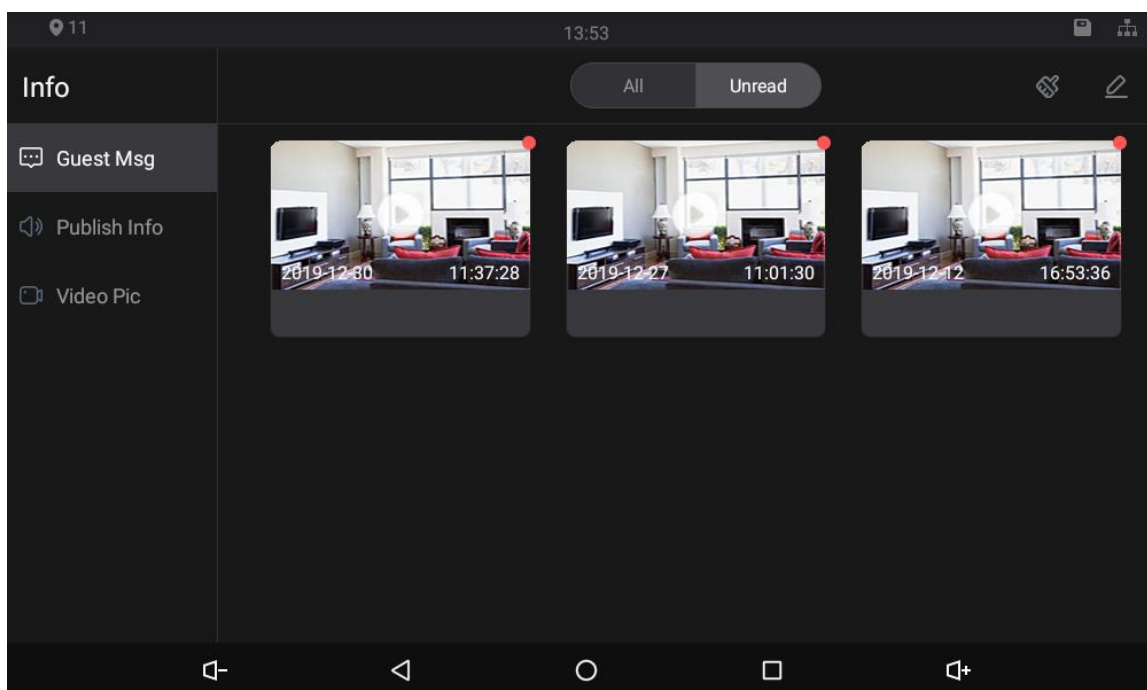


Figure 4-45 Viewing publish information

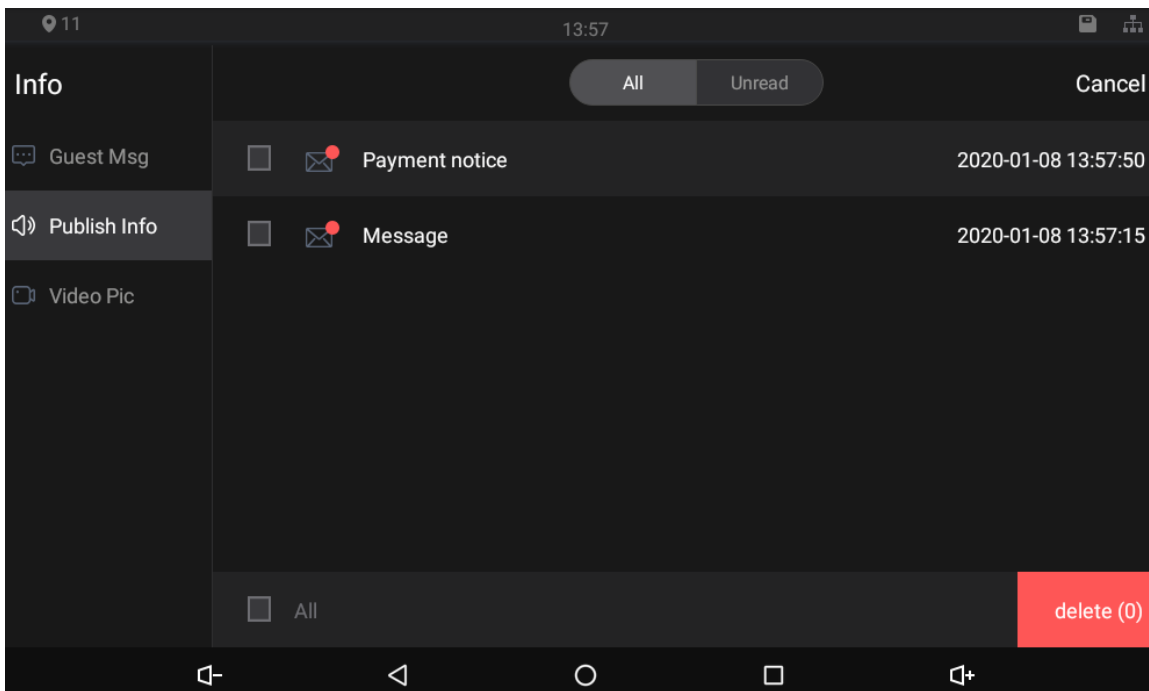
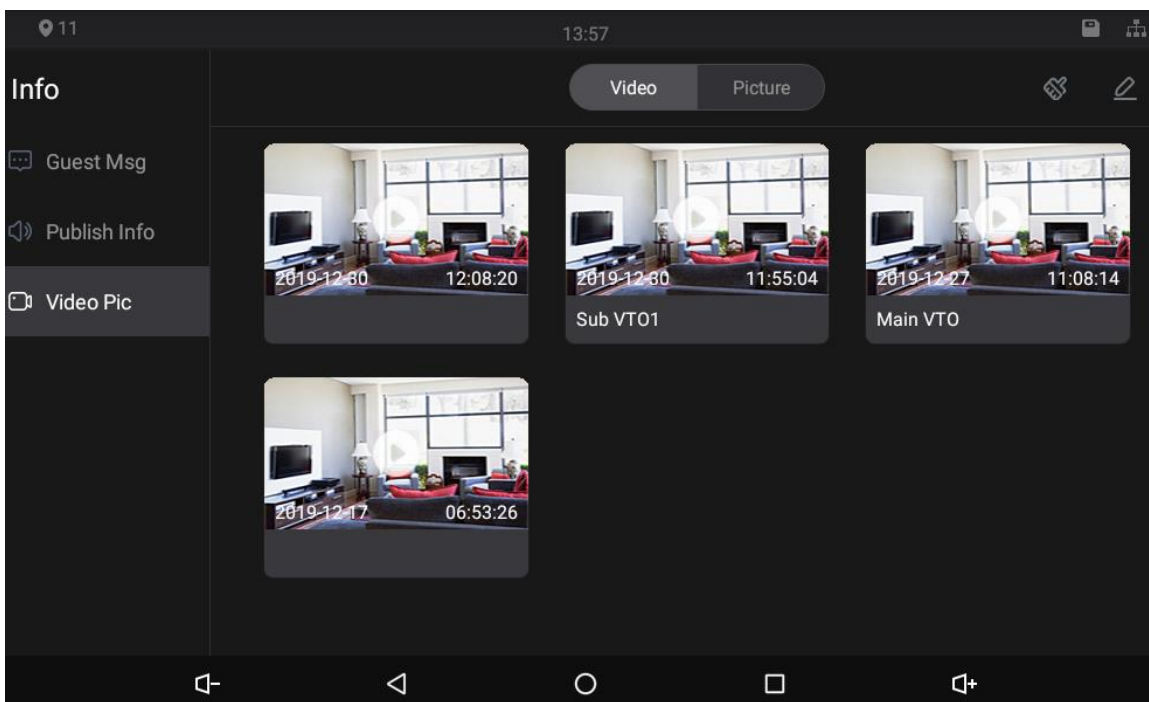


Figure 4-46 Viewing video pictures



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.