7-inch and10-inch Android Indoor Monitor

V1.0.3

Foreword

General

This manual introduces the installation, functions and operations of the 7-inch and 10-inch Android VTH (hereinafter referred to as the "VTH "). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Date
V1.0.3	Revised alarm settings.	June 2024
V1.0.2	Revised "Important Safeguards and Warnings".	December 2022
V1.0.1	Add 7-inch VTH description.	March 2022
V1.0.0	First release.	December 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in

compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Operation Requirements

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Transport, use and store the device under allowed humidity and temperature conditions.
- If the device is powered off for longer than a month, it should be placed in its original package and sealed. Make sure to keep it away from moisture, and store it under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.

Installation Requirements

WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Improper use of the battery might result in a fire or explosion.

- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Install the device on a stable surface to prevent it from falling.
- Install the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

Table of Contents

Foreword I
Important Safeguards and Warnings III
1 Introduction 3
1.1 Overview 3
1.2 Features 3
2 VTO Configuration 5
2.1 Config Tool 5
2.2 Initialization 5
2.3 Configuring Network Parameters 7
2.4 Configuring VTO Number 7
2.5 Configuring SIP Servers 8
2.6 Adding VTOs 10
2.7 Adding Room Number 11
3 VTH Configuration 14
3.1 Initialization 14
3.2 Main Menu Overview 14
3.3 Settings 16
3.3.1 Network & Internet 17
3.3.2 Apps & Notifications 18
3.3.3 Display 18
3.3.4 Sound 18
3.3.5 Storage 18
3.3.6 System 19
3.4 Project Settings 19
3.4.1 Configuring VTH 19
3.4.2 Configuring SIP Server 20
3.4.3 Configuring VTO 21
3.4.4 Searching for Devices 23
3.4.5 Resetting Password 23
3.4.6 Security Settings 24
3.5 User Settings 25
3.5.1 Ring 26
3.5.2 DND 26
3.5.3 Forward 27
3.5.4 Password 27
3.5.5 Themes 29
3.6 Alarm Settings 30
3.6.1 Wire Zone 30
3.6.2 Alarm Output 31
3.6.3 Alarm Mode 32
4 Commissioning 33
4.1 Watching Monitoring Video 33
4.2 Checking Messages 34
4.3 Making Calls 34

4.4 Viewing Alarms Logs 35
4.5 Viewing Information 37
Appendix 1 Cybersecurity Recommendations 39

1 Introduction

1.1 Overview

The 10-inch digital Android VTH, 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 connection

VTHs can connect to the network through Wi-Fi function.

Voice call

Make calls on the VTOs to VTHs.

Monitoring

View videos from fence stations, VTOs, IP cameras on the VTH.

Elevator control

Make the elevator come to your floor through the VTH.

Emergency call

Make emergency calls on the VTH.

Auto snapshot

Take snapshots and save them to the SD card or FTP server during calls or monitoring.

Video recording

Record videos through the VTH if SD card is inserted into the rear panel of the VTH.

Do not disturb

Set period in which you do not want to be disturbed so that you will not receive calls or messages from VTOs or other VTHs.

Remote unlock

Unlock doors remotely.

Arm and disarm

Arm the VTH to enable alarm function in the protection zone, and disarm the function when you do not need it.

Message check

Check text messages and videos left by visitors, or public notices released by the management center.

2 VTO 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.

The snapshots are for reference only, and slight differences might be found in the actual web page of the VTO depending on your model.

2.1 Config Tool

You can use the Config Tool to initialize devices, modify IP address and upgrade system for multiple devices at the same time. For the detailed information, see the Config Tool user's manual.

2.2 Initialization

For first-time login, you need to initialize the VTO.

Step 1 Power on the VTO.

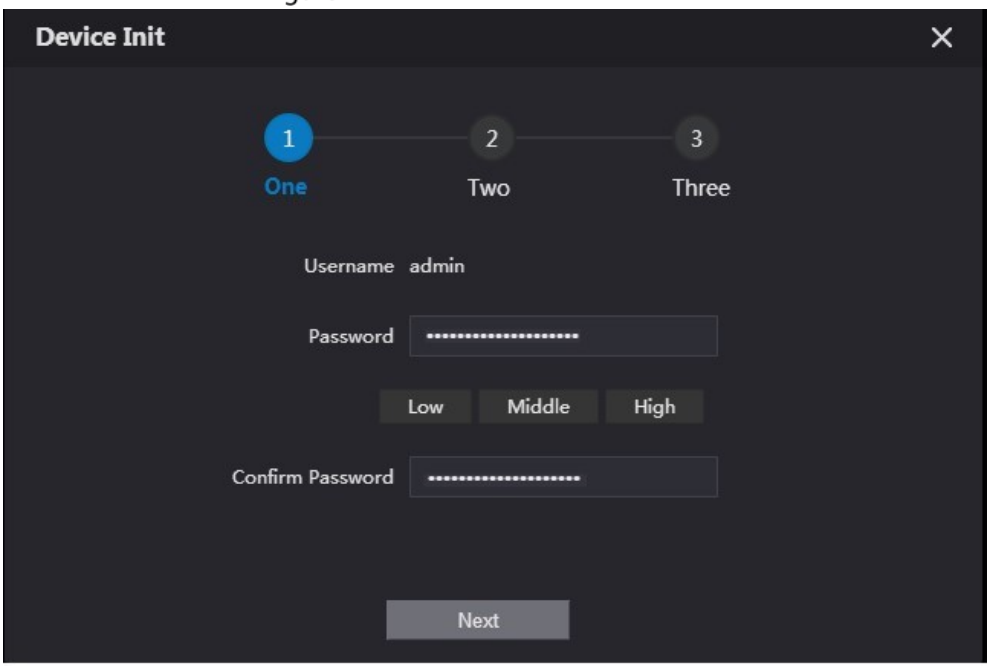
Step 2 Go to the default IP address (192.168.1.108) of the VTO in the browser address bar, and then press the Enter key to go to the web page of the VTO.

- The username is admin by default.
- Make sure that the IP address of the computer is on the same network segment as the VTO.

Step 3 On the **Device Init** page, enter and confirm the password, and then click **Next**.

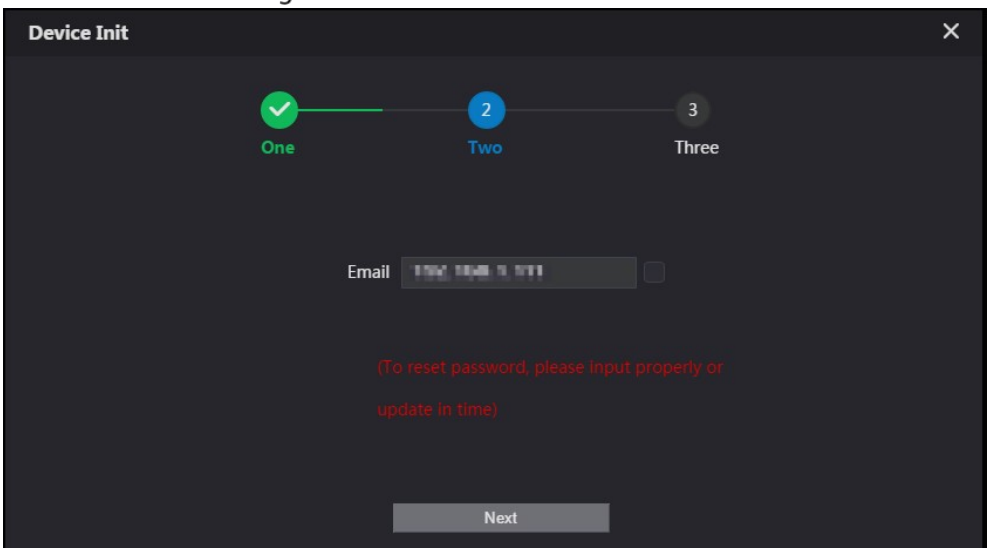
The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).

Figure 2-1 Device initialization



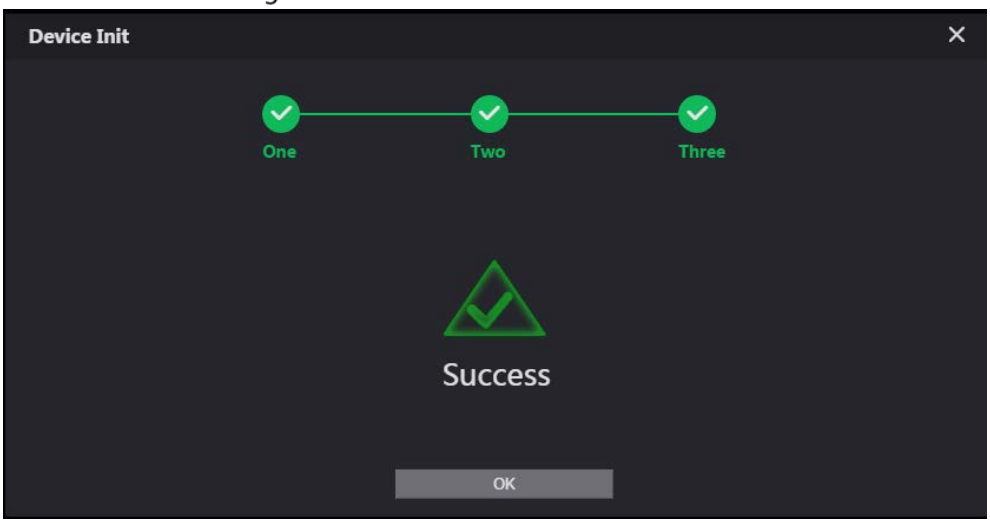
Step 4 Select the **Email** checkbox and enter the email address.

Figure 2-2 Set an email address



Step 5 Click **Next**.

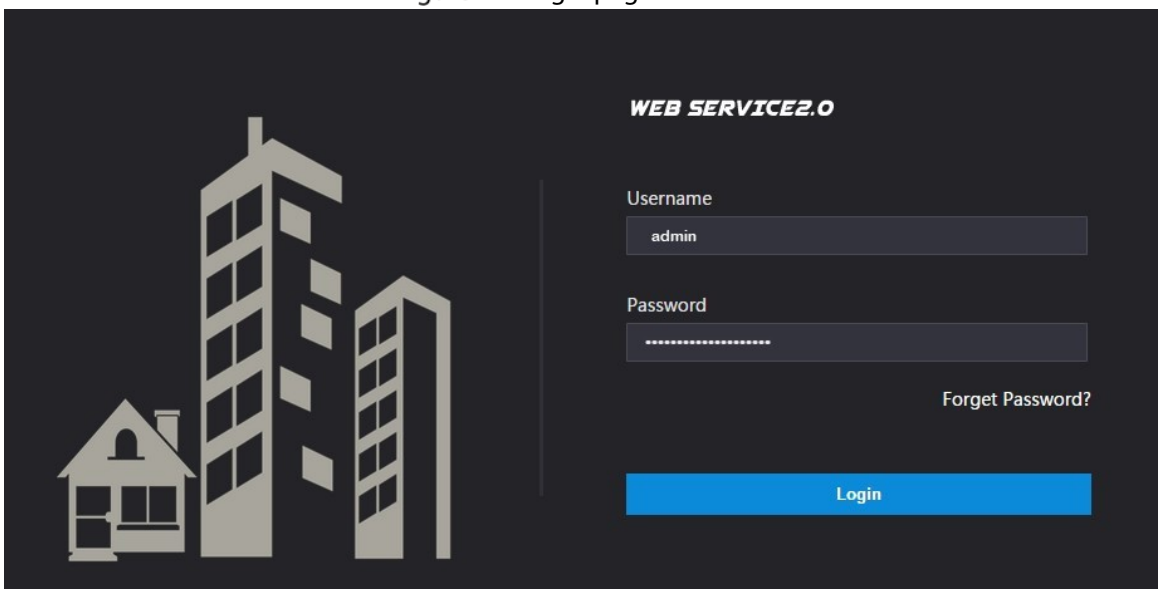
Figure 2-3 Initialization successful



Step 6 Click **OK**.

Enter username (admin by default) and the new password to log in to the web page.

Figure 2-4 Login page

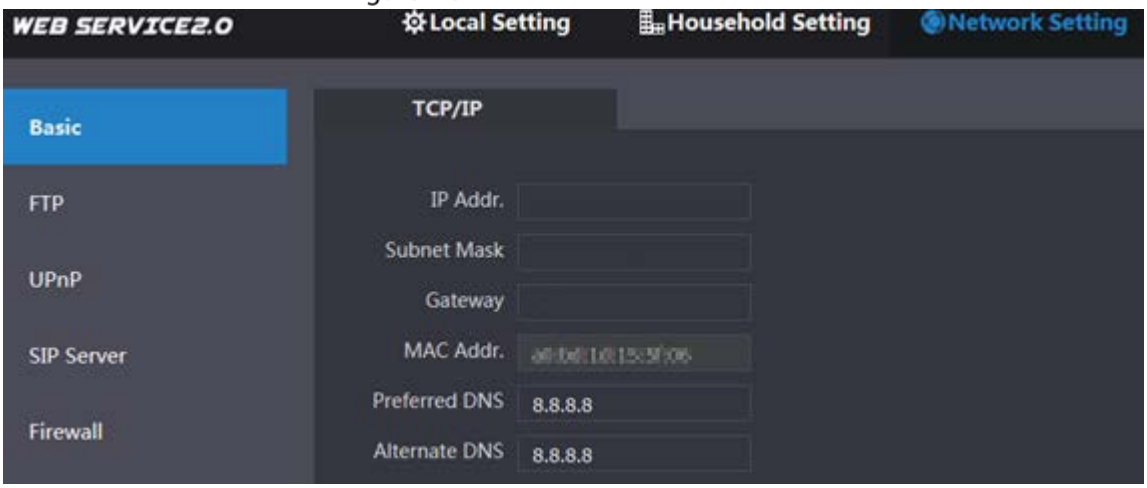


2.3 Configuring Network Parameters

You need to configure the TCP/IP information to connect the VTO to the network.

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

Figure 2-5 TCP/IP information



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

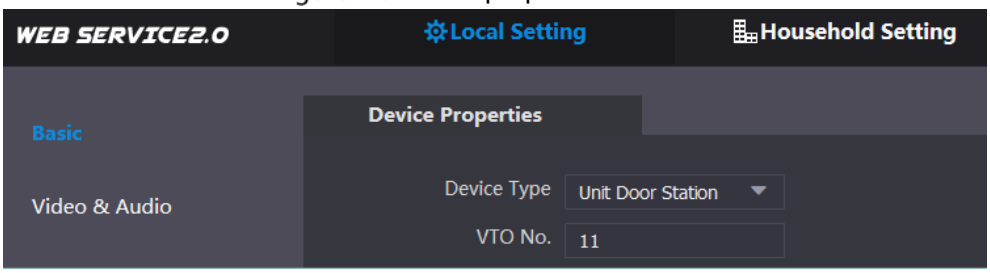
2.4 Configuring VTO Number

Numbers can be used to distinguish each VTO, and it is recommended that you set it according to the unit or building number.

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

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

Figure 2-6 Device properties



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

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

2.5 Configuring SIP Servers

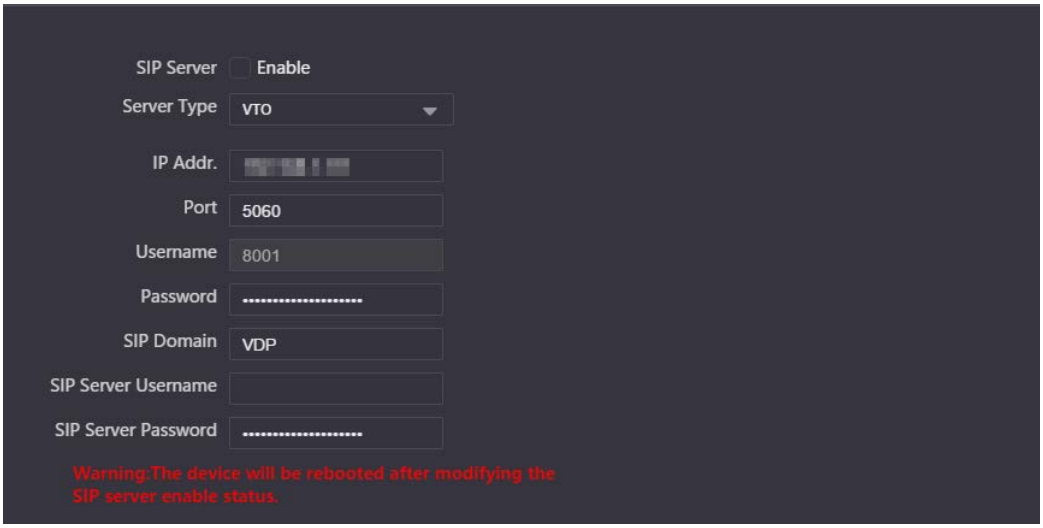
When connected to the same SIP server, all VTOs and VTHs can call each other. You can use a VTO or other servers as the SIP server.

VTO as the SIP server (for One Building)

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

Step 2 Set **Server Type** as **VTO**.

Figure 2-7 VTO as the SIP server



Step 3 Configure the parameters. See Table 2-1.

- If the current VTO you have logged in works as the SIP server, enable **SIP Server**, and then keep other parameters by default.
- If other VTOs work as the SIP server, set **Server Type** as **VTO**, and then configure the parameters.

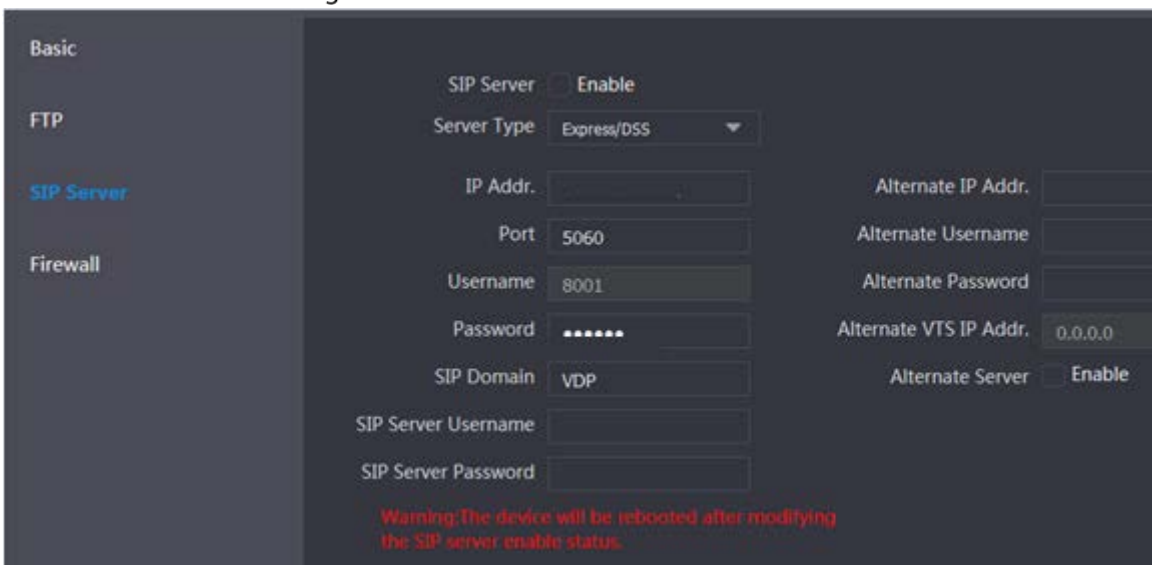
  Do not enable **SIP Server**, otherwise the connection fails.

Step 4 Click **Save**.

Platform (Express/DSS) as the SIP server (for Multiple Buildings or Units)

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

Figure 2-8 Platform as the SIP server



Step 2 Set **Server Type** as **Express/DSS**.

Step 3 Configure the parameters.

Table 2-1 SIP server parameter description

Parameter	Description
IP Addr.	SIP server IP address.
Port	• 5060 by default when another VTO works as the SIP server. • 5080 by default when the platform works as the SIP server.
Username/Password	Leave it as default.
SIP Domain	• Leave it as default when a VTO works as the SIP server. • Leave it as default or keep it null when the platform works as the SIP server.
SIP Server Username/ Password	Used to log in to the SIP server.
Alternate IP Addr.	The alternate server will be used as the SIP server when DSSExpress/DSS pro stops responding. We recommend you configure the alternate IP address. • If you enable **Alternate Server,** the current VTO you have logged in serves as the alternate server. • If you want another VTO serve as the alternate server, you need to enter the IP address of that VTO in the **Alternate IP Addr.** textbox. Do not enable **Alternate Server** in this case.
Alternate Username/ Password	Used to log in to the alternate server.
Alternate VTS IP Addr.	IP address of the alternate VTS.

Step 4 Click **Save**.

When the platform works as the SIP server and you want to configure the building number and building unit number, enable **Support Building** and **Support Unit** first.

2.6 Adding VTOs

You can add VTOs to the SIP server and then they can call each other.

Background Information

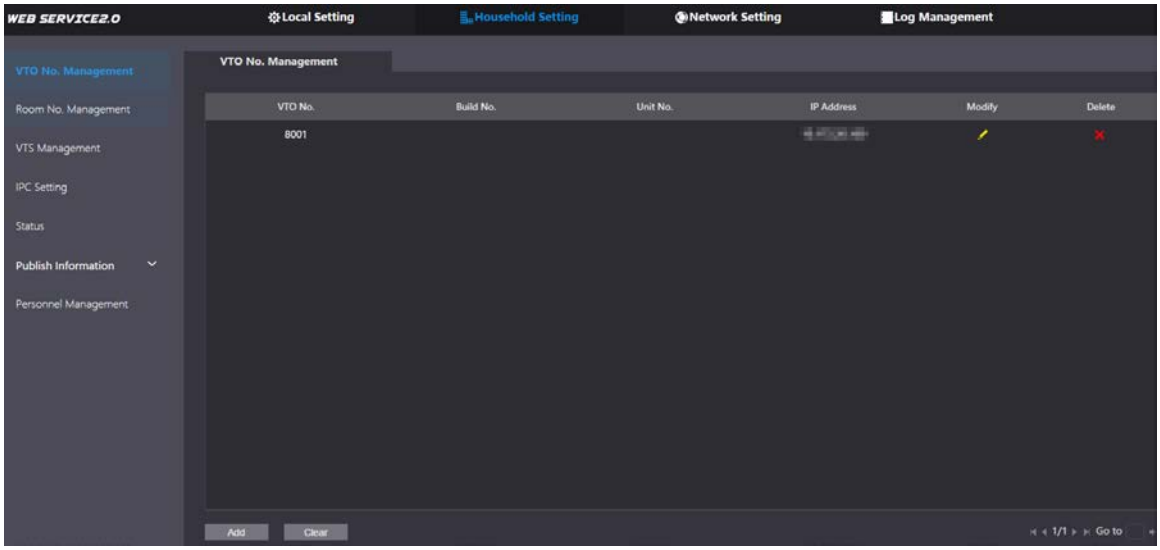
This section applies to the condition in which a VTO works as the SIP server. If you are using other servers as the SIP server, see the corresponding manual for details.

Procedure

Step 1 Log in to the web page of the SIP server.

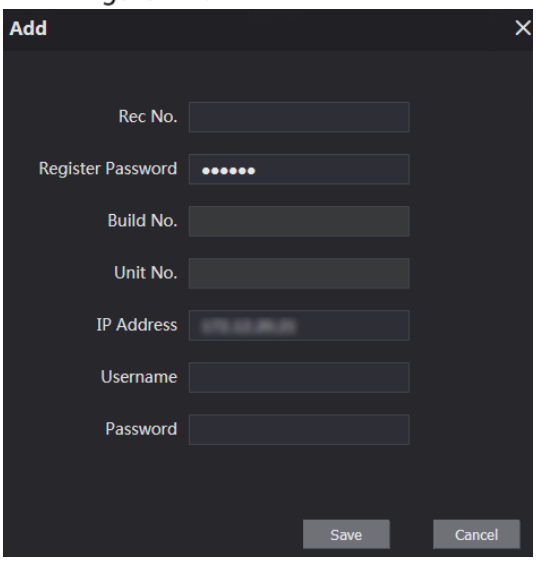
Step 2 Select **Household Setting** > **VTO No. Management**.

Figure 2-9 VTO No. management



Step 3 Click **Add**.

Figure 2-10 Add a VTO



Step 4 Configure the parameters.

Table 2-2 Add a VTO

Parameter	Description
Rec No.	VTO number.
Register Password	Leave it as default.
Build No.	Available only when other servers work as the SIP server.
Unit No.	
IP Address	VTO IP address.
Username/Password	Used to log in to the web page of the VTO.

Step 5 Click **Save**.

2.7 Adding Room Number

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

Background Information

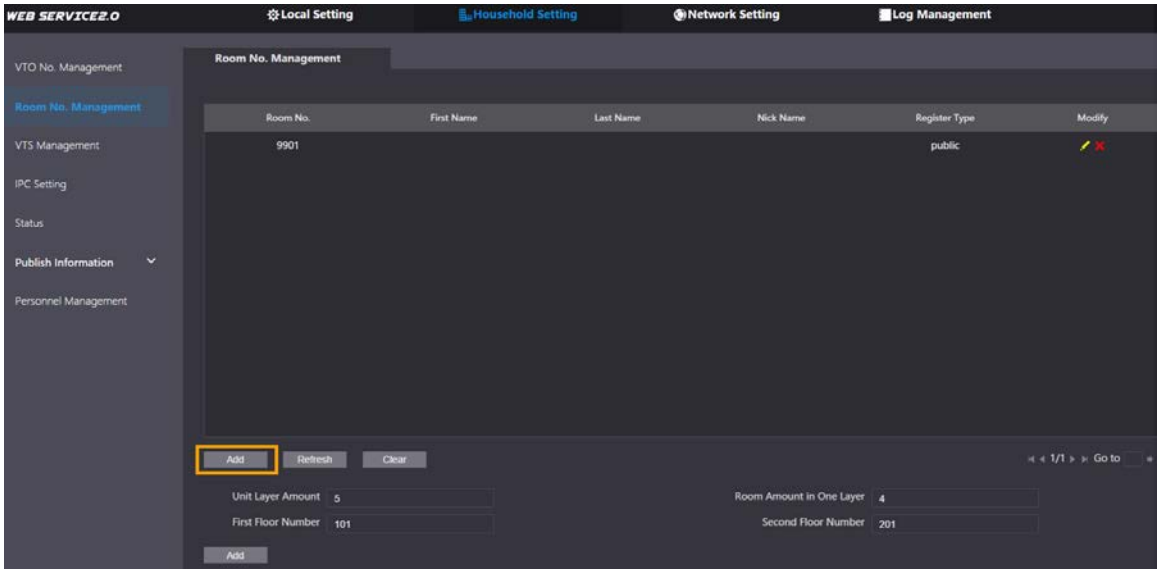
This section applies to the condition in which a VTO works as the SIP server. If you are using other servers as the SIP server, see the corresponding manual for details.

Procedure

Step 1 Log in to the web page of the SIP server.

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

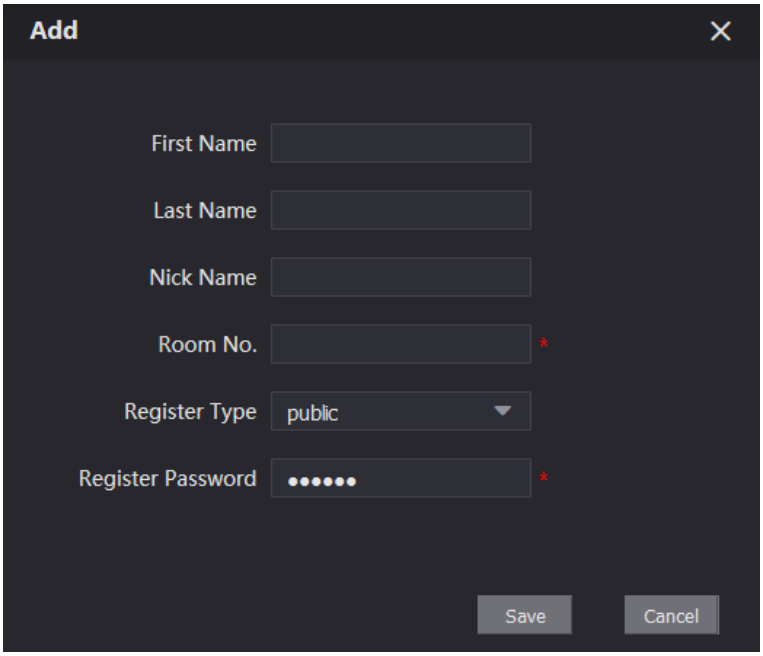
Figure 2-11 Room No. management



Adding a Single Room Number

Step 1 On the **Room No. Management** page, click **Add**.

Figure 2-12 Add a single room number



Step 2 Configure room information.

Table 2-3 Room information

Parameter	Description
First Name	Information used to differentiate each room.
Last Name	
Nick Name	
Room No.	Room number of the VTH. ● When there are multiple VTHs for the group call function, the room number for the main VTH should end with #0, and the room numbers for extension VTHs with #1, #2… ● The room number can contain up to 6 digits of numbers, letters or their combination, and it cannot be the same with any VTO number.
Register Type	Select **public**.
Register Password	Leave it as default.

Step 3 Click **Save**.

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

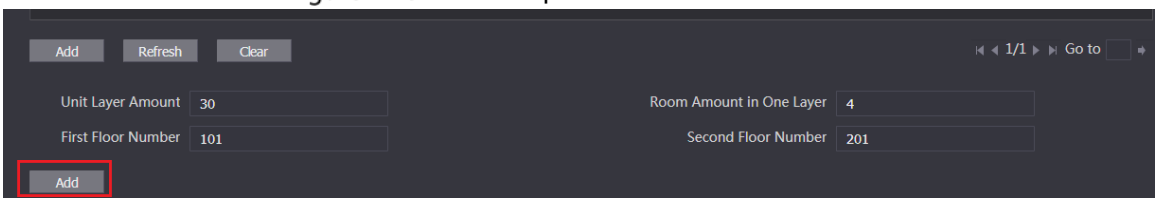
Adding Multiple Room Numbers

Step 1 On the **Room No. Management** page, configure the information in **Unit Layer Amount**, **Room Amount in One Layer**, **First Floor Number**, and **Second Floor Number**.

Step 2 Click **Add**.

All the added room numbers are displayed.

Figure 2-13 Add multiple room numbers



3 VTH Configuration

You need to configure IP, Wi-Fi, VTO parameter, SIP server, and more on the VTH, and then the VTH can communicate with VTOs and the management center.

The VTH screen only supports single-touch operation.

3.1 Initialization

The default IP address of the VTH is 192.168.1.108.

Step 1 Power on the VTH.

Step 2 Select a language, and then tap **Next**.

Step 3 Set a quick configuration type either as **Apartment** or **Villa**, and then tap **Next**.

Step 4 Enter the password, confirm password and email.

- Password: Used to go to the project mode.
- Email: Used to reset the password.

Step 5 Tap **OK** to go to the main menu.

3.2 Main Menu Overview

Figure 3-1 Main menu (1)

Figure 3-2 Main menu (2)

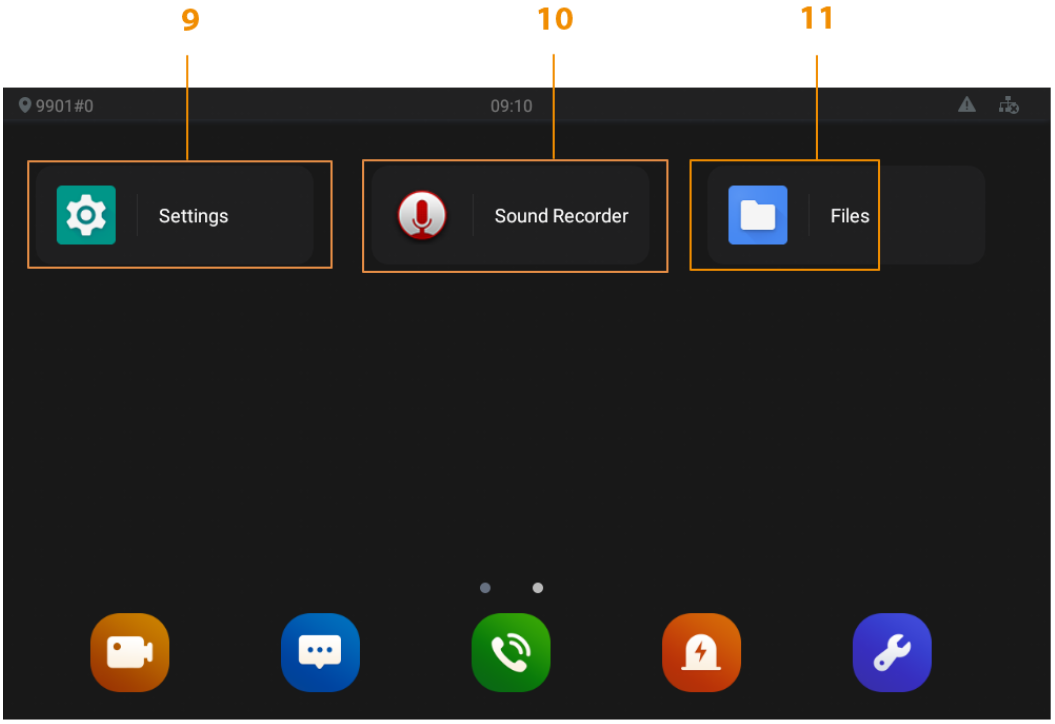


Table 3-1 Menu description

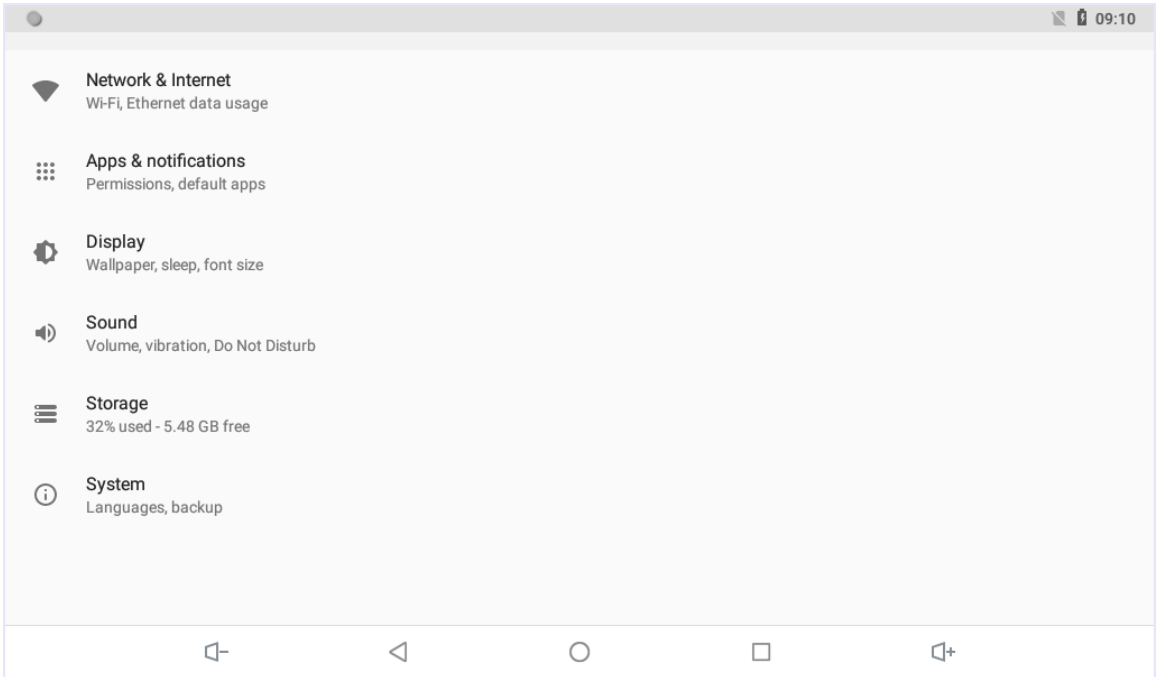
No.	Name	Description
1	Room Number	Number of the room where the VTH is installed.
2	Date and Time	Current time and date.
3	Arm and Disarm	Shortcut icons to arm or disarm.The four icons represent at home mode, away from home mode, sleep mode, and customizable mode. Select **Arm Mode** or **Disarm Mode** first, and then tap the icons to arm or disarm.
4	Status Bar	• : The wired network is not connected. • : The wired network is connected. • : The VTH failed to connect to the SIP server. If this icon does not appear, then the VTH is connected to the SIP server. • : The SD card is inserted and recognized. • : The VTH is in the Do Not Disturb mode.
5	SOS	Tap the icon to call the management center.
6	Do Not Disturb	Tap the icon to set Do Not Disturb period. Enable DND Period first, and then you can configure do-not-disturb.
7	Turn off Screen	Tap the icon to turn off the screen.

No.	Name	Description
8	Function Buttons	• : Tap the icon to watch videos from VTOs and IP cameras. • : Tap the icon to view text messages and videos left by visitors, or public notices released by the management center. • : Tap the icon to make calls to other VTHs and the management center. • : Tap the icon to view alarm logs, do alarm settings for 6 areas. • : Tap the icon to go to the User Settings screen. You can select ringtones for different VTOs, Do Not Disturb period, call forward mode, and other settings. Tap the icon for over 5 seconds to go to the Project Setting screen, where you can configure VTH, VTO and SIP server.
9	Settings	: Tap the icon to configure network settings, app notifications, displays and system.
10	Sound Recorder	: Tap the icon to record voice messages to the SD card or to the VTH.
11	Files	: Tap the icon to view files like images, videos and audio.

3.3 Settings

Tap to go to the **Settings**.

Figure 3-3 User settings



3.3.1 Network & Internet

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

Wired Network

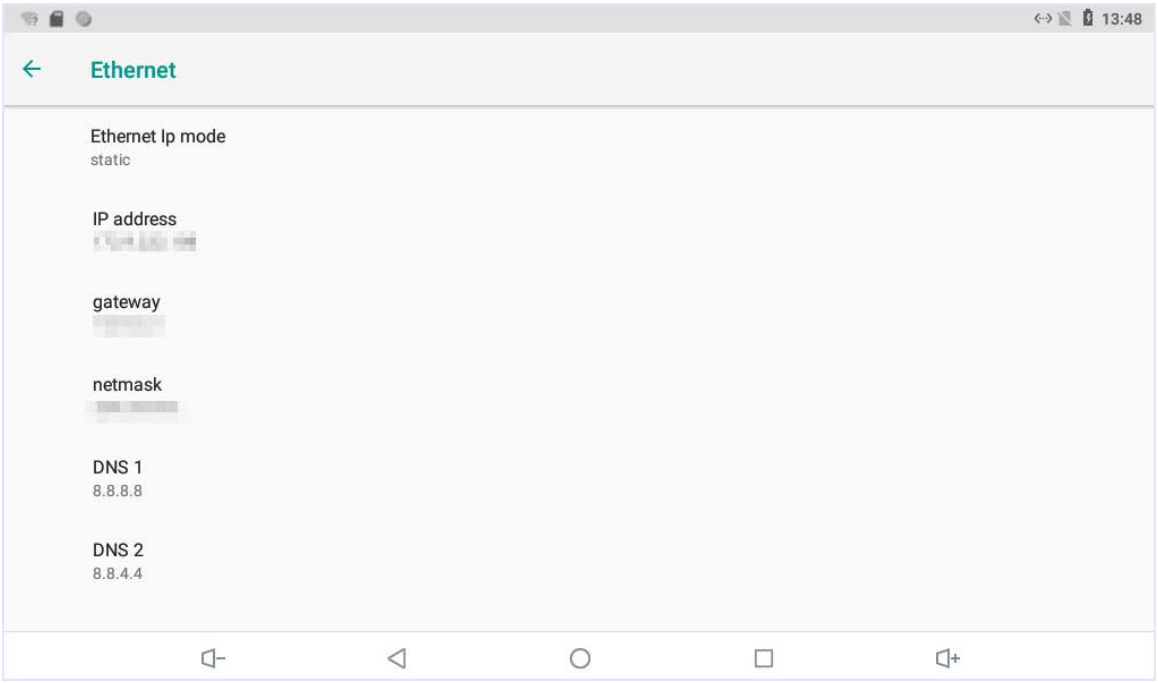
Make sure that IP addresses of the VTH and IP address of VTOs are in the same network segment; otherwise the VTH cannot acquire VTO information.

Step 1 Tap **Settings** > **Network & Internet** > **Ethernet**.

Step 2 Configure parameters.

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

Figure 3-4 Network setting

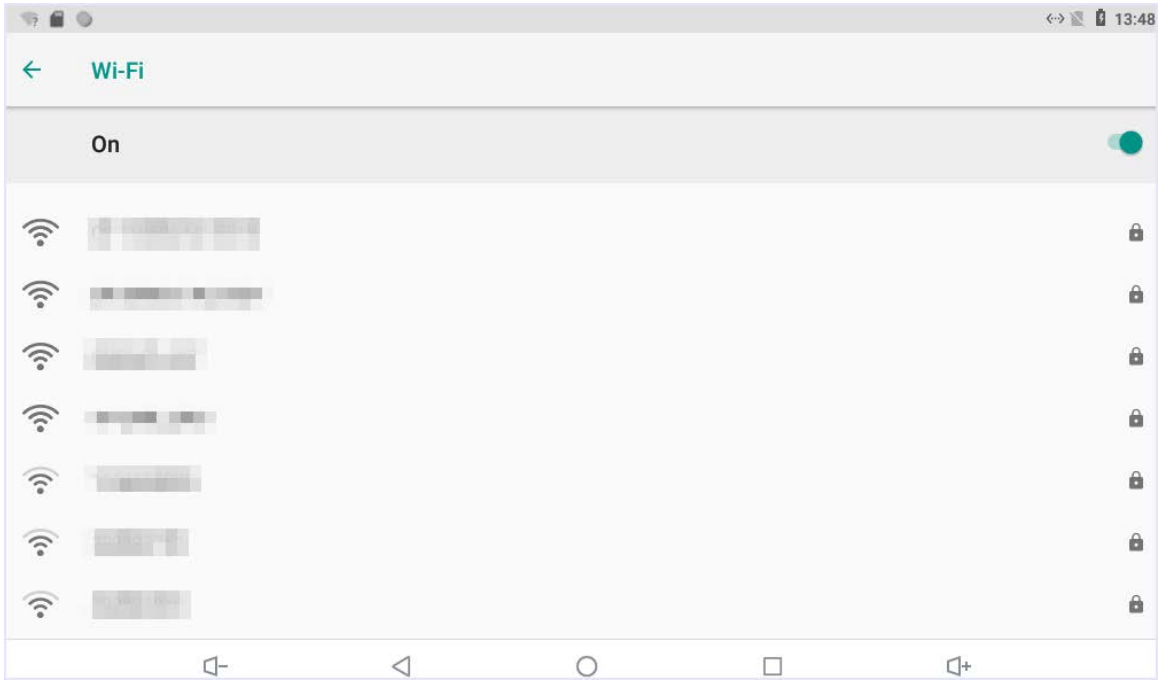


Wireless network

Step 1 Tap **Settings** > **Network & Internet** > **Wi-Fi**.

Step 2 Tap to see all the available networks.

Figure 3-5 Wi-Fi



Step 3 Select a wireless network.

Step 4 Enter the password.

Step 5 Tap **CONNECT.**

3.3.2 Apps & Notifications

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.

3.3.3 Display

You can adjust display brightness, display sleep duration, font size, and display size.

3.3.4 Sound

You can adjust media volume and notification volume. You can also select to use default notification sound and default alarm sound.

3.3.5 Storage

View spaces that are used or still available. You can delete unwanted messages to recover storage spaces.

3.3.6 System

Languages & Input

Languages: You can select languages as needed.

Keyboard & Inputs: You can choose virtual keyboard or physical keyboard

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.

Backup

You can back up the files in the VTH if you do not want to delete them when the storage is full.

Reset options

You can reset Wi-Fi, mobile, and Bluetooth, and app preferences. You can also erase all data, which means restoring the VTH to factory settings.

About tablet

You can see details (battery status, network status, legal information, model, android version, Android security patch level, baseband version, Kernel version, build number, and more) about the VTH.

3.4 Project Settings

Step 1 Tap and hold on the main menu for over 5 seconds.

Step 2 Enter the project password (123456 by default) in the **Password Verification** textbox to go to the **Project Settings** mode.

3.4.1 Configuring VTH

Step 1 Tap **VTH Config** on the **Project Setting** screen.

Step 2 Configure the parameters.

Figure 3-6 VTH configuration

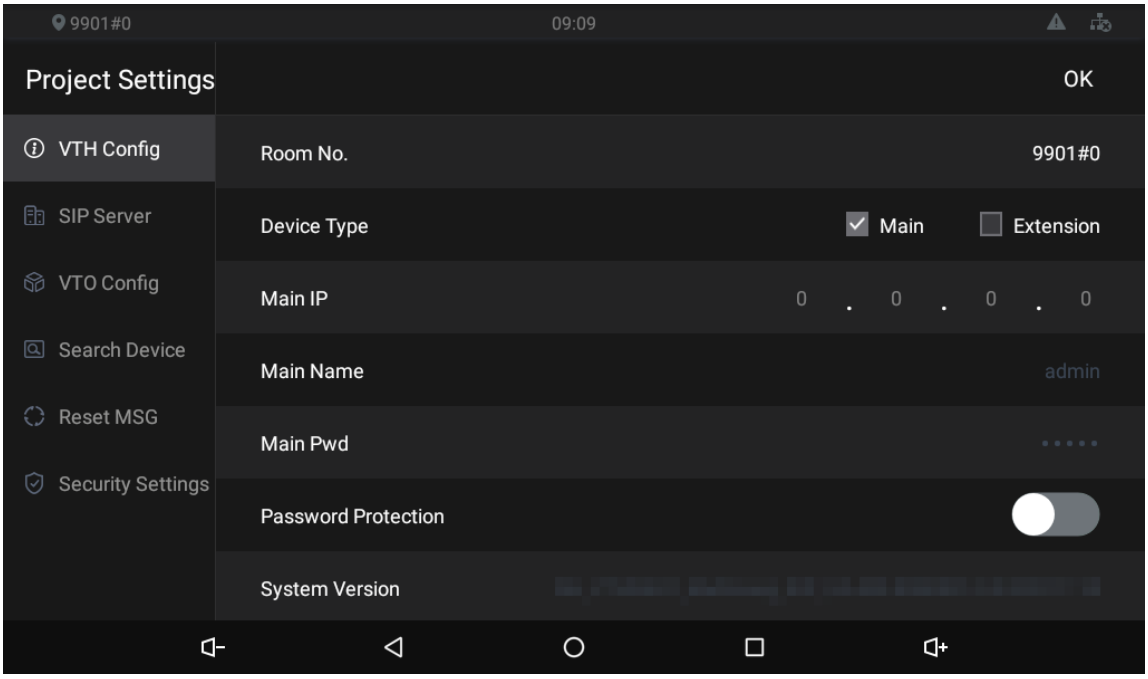


Table 3-2 Parameter description

Parameter	Description
Room No.	Number of the room where the VTH is installed. When there are multiple VTHs, the room number for the main VTH should end with #0, and the room numbers for extension VTHs with #1, #2…
Device Type	• Select **Main** if the VTH you are operating works as the main VTH. • Select **Extension** if the VTH works as an extension.
Main IP	The planned IP address for the VTH.
Main Name/Pwd	Leave it as default.
Password Protection	We recommend you enable this function to avoid potential security risks.
System Version	You can view system version of the VTH.

3.4.2 Configuring SIP Server

You need to configure the SIP server information to make sure that the intercom function works.

Step 1 Tap **SIP Server** on the **Project Setting** screen.

Step 2 Configure the parameters.

Figure 3-7 SIP server

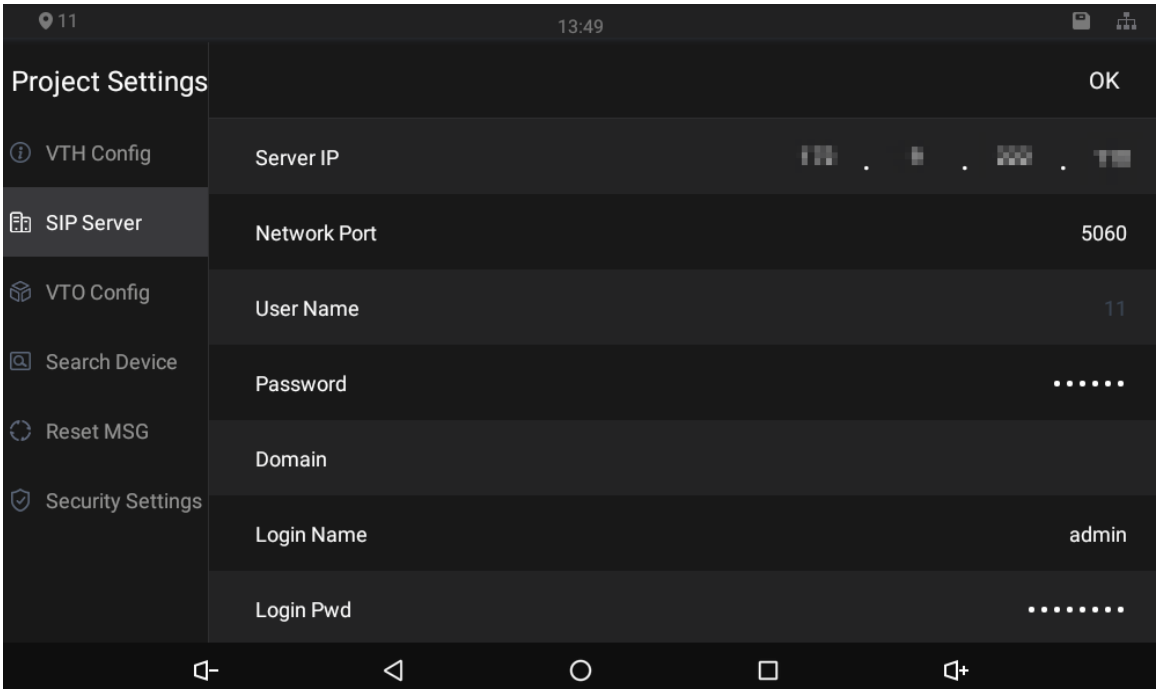


Table 3-3 SIP server description

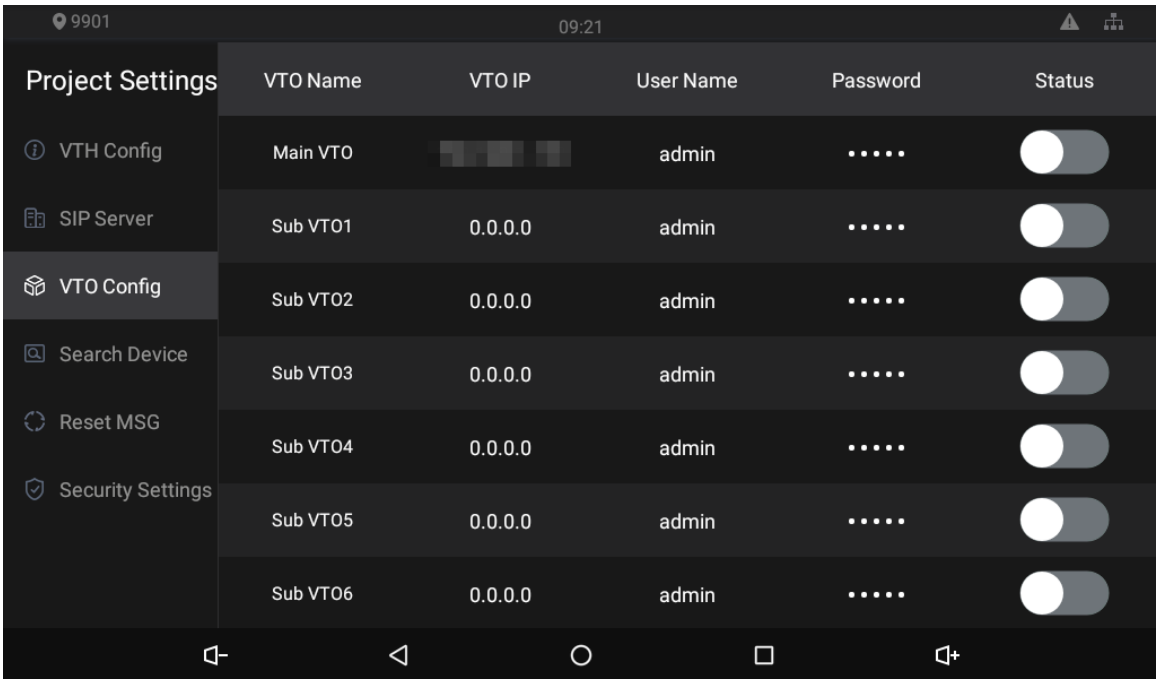
Parameter	Description
Server IP	• IP address of the platform that works as the SIP server. • IP address of the VTO that works as the SIP server.
Network Port	• 5060 by default when a VTO works as the SIP server. • 5080 by default when the platform works as the SIP server.
User Name/ Password	Leave it as default.
Domain	Leave it as default.
Login Name	Username and password to log in to the web page of the SIP server.
Login Pwd	
Status	Enable the SIP server status, and then the VTH can connect to the SIP server.

3.4.3 Configuring VTO

You can add VTOs to the VTH to achieve the intercom function.

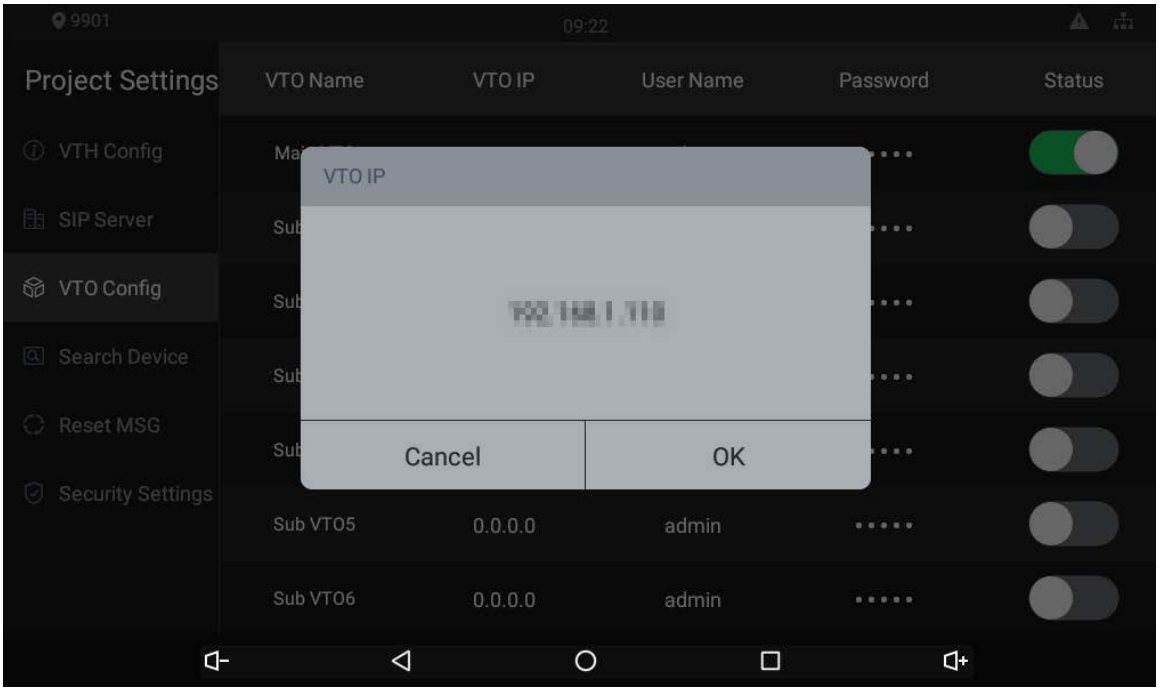
Step 1 Tap **VTO Config** on the **Project Setting** screen.

Figure 3-8 VTO configuration



Step 2 Tap **VTO IP** of a VTO that you plan to configure.

Figure 3-9 VTO IP



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

Step 4 Enter the VTO IP, user name, and password (used to log in to the VTO web page.

- You can add up to 20 VTOs (one main VTO and 19 sub VTOs) to the VTH.
- 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 VTO web page.

Step 5 Tap to enable the VTO.

3.4.4 Searching for Devices

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

Figure 3-10 Searching device (1)

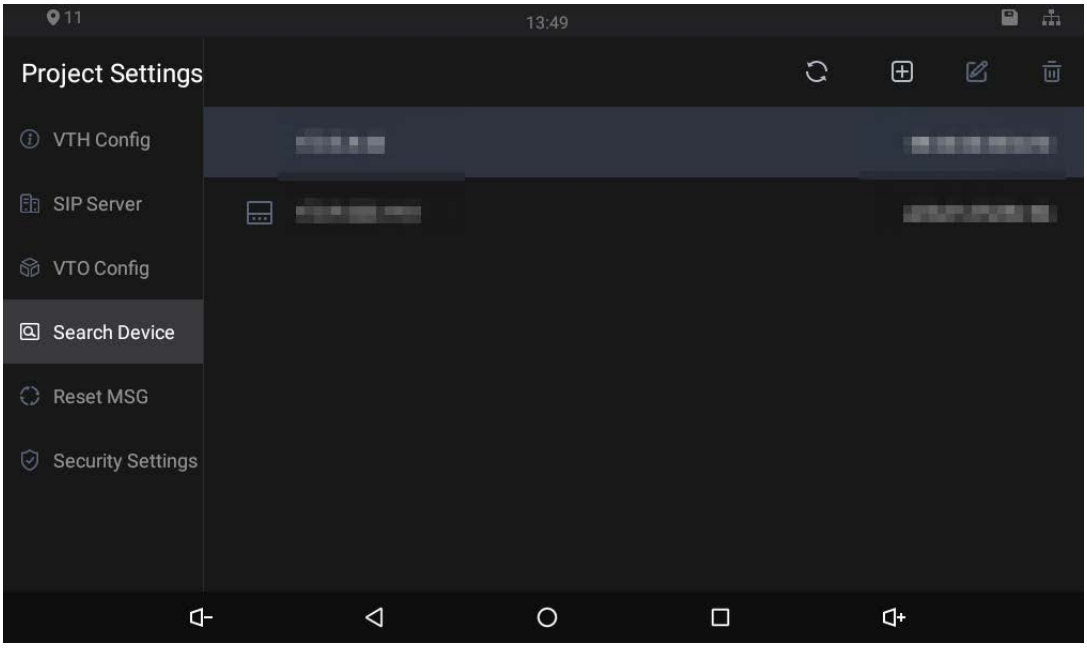
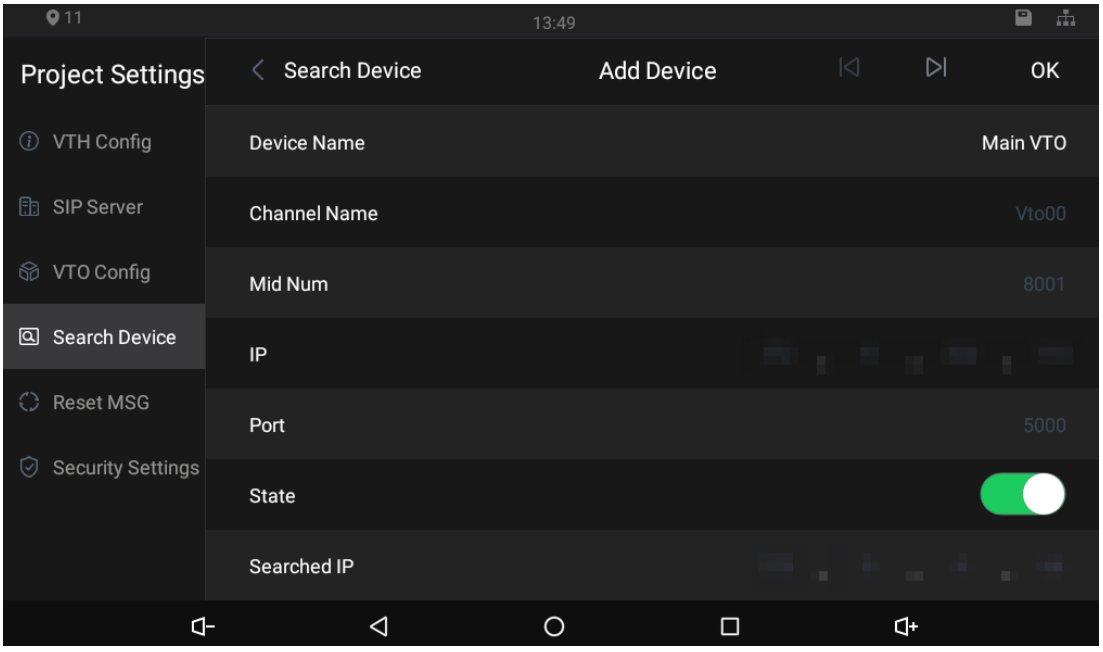


Figure 3-11 Searching device (2)



3.4.5 Resetting Password

You need to enable the **Resst Password** first on the **Reset MSG** tab on the **Project Settings** screen if you want to reset the password.

Step 1 Tap and hold until the **Password Verification** screen is displayed.

Step 2 Tap **Forgot password?** to go to the warning screen.

Step 3 Tap **OK**, and then the QR code appears.

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

A string will be displayed after you scanned the QR code.

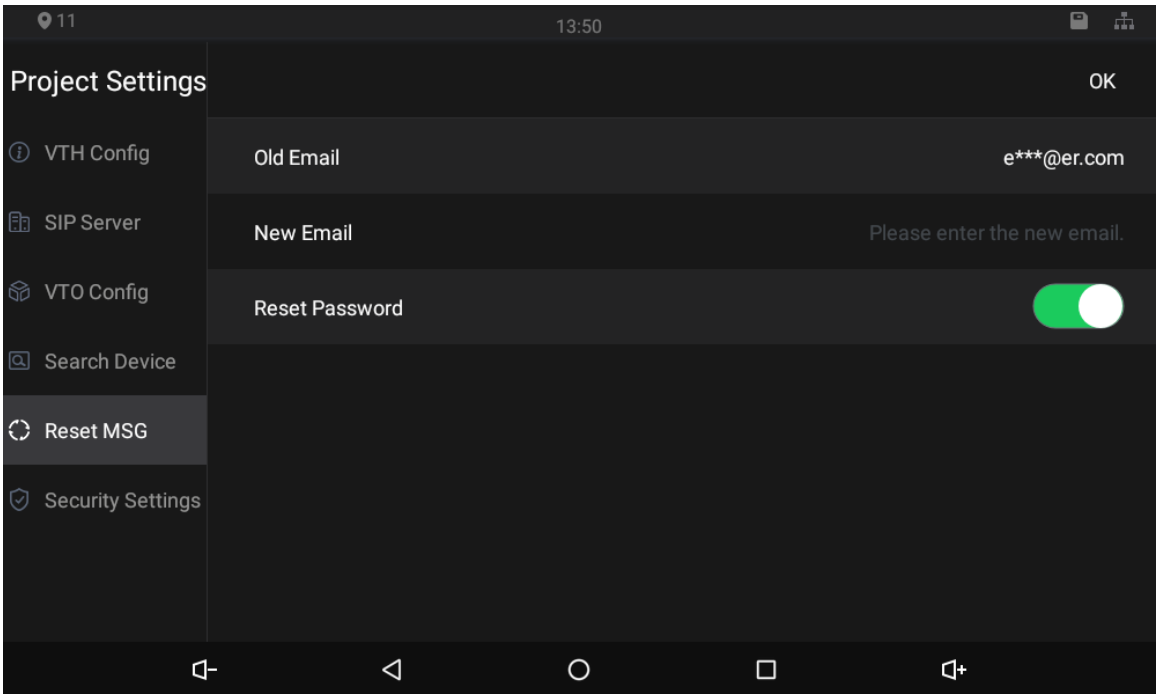
Step 5 Send the string to required email box with the email address you set on the **Reset MSG** screen.

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 3-12 Reset password



3.4.6 Security Settings

With the trusted list, you can only add devices that you trust to the VTH. Devices that are not on the list cannot be added to the VTH. The Dshell allows you to develop analysis modules to help you understand cyber intrusion events.

Figure 3-13 Enable trusted list

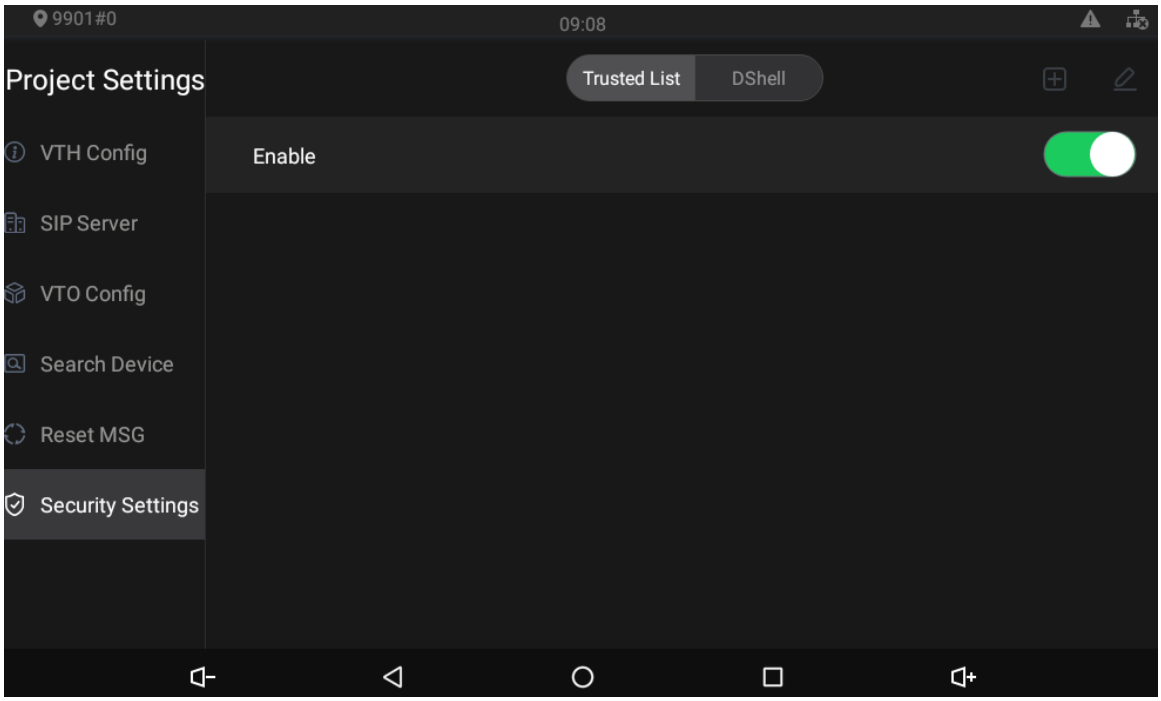
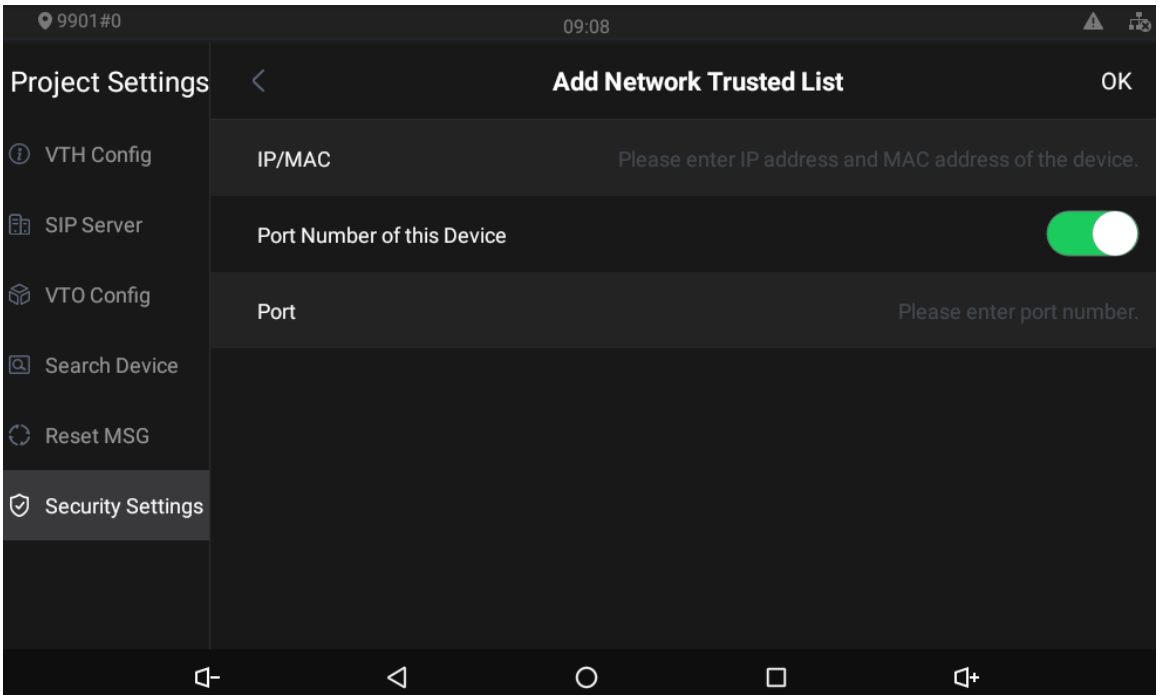


Figure 3-14 Add network trusted list



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

3.5 User Settings

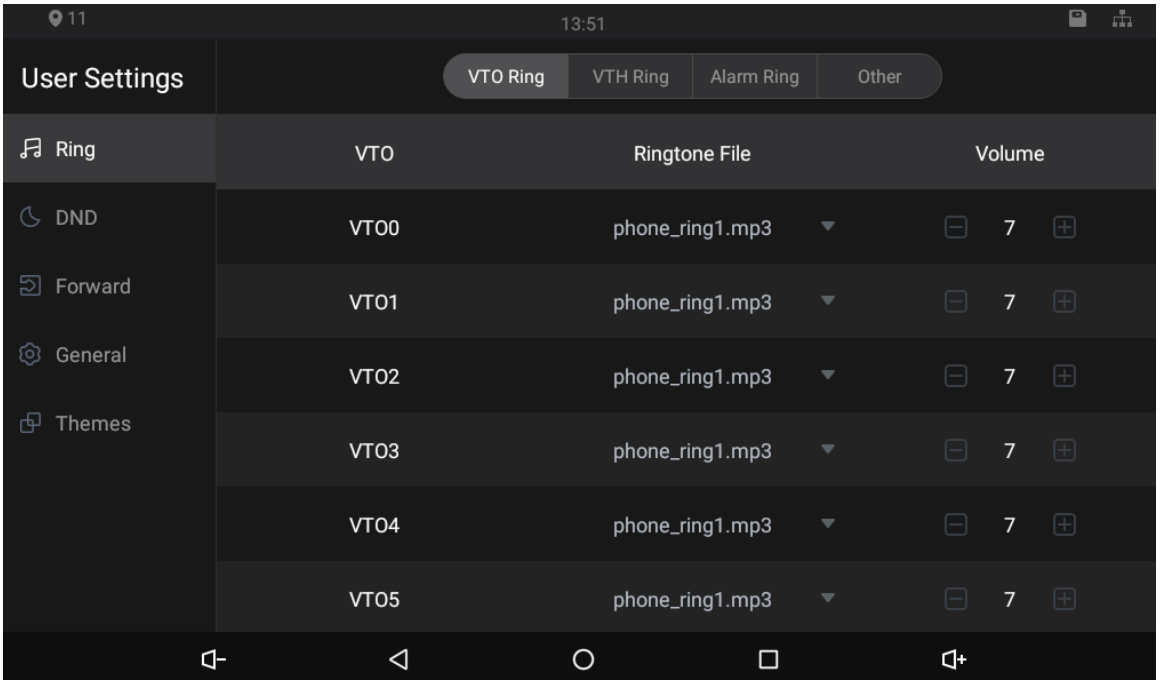
Tap , and then the user setting screen is displayed. You can select ringtones for different VTOs, Do Not Disturb period, call forward mode (there are three options: Always, Busy, and No Answer), and

other settings.

3.5.1 Ring

On this screen, you can select ringtones for different VTOs.

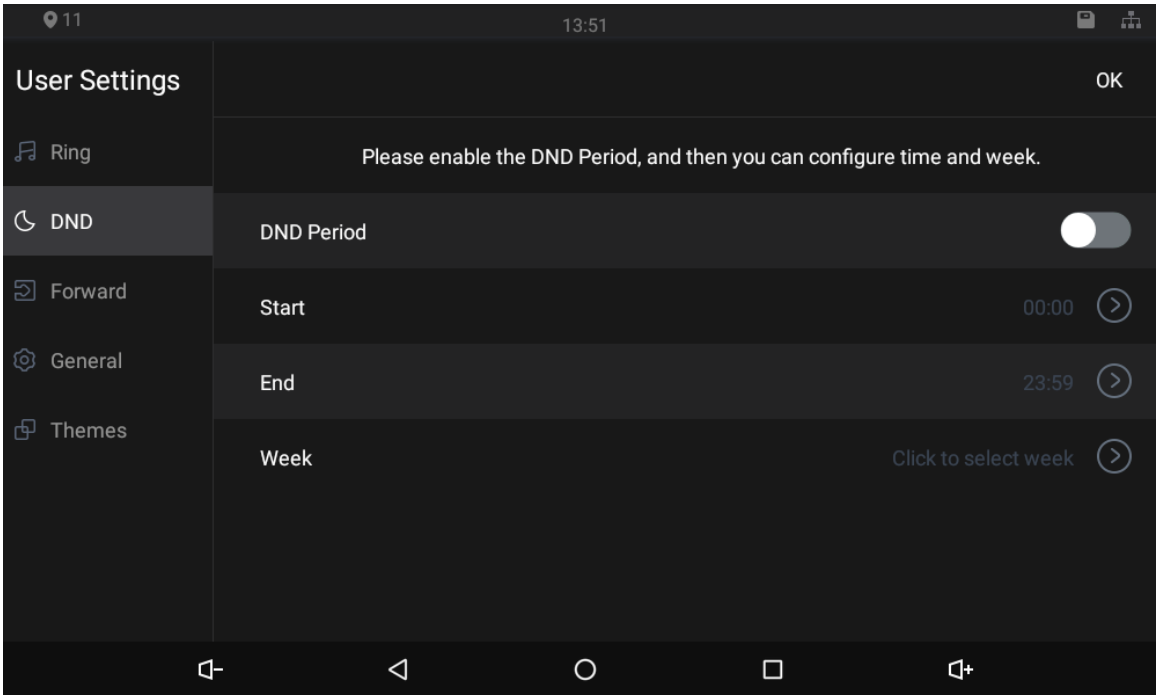
Figure 3-15 Ring



3.5.2 DND

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

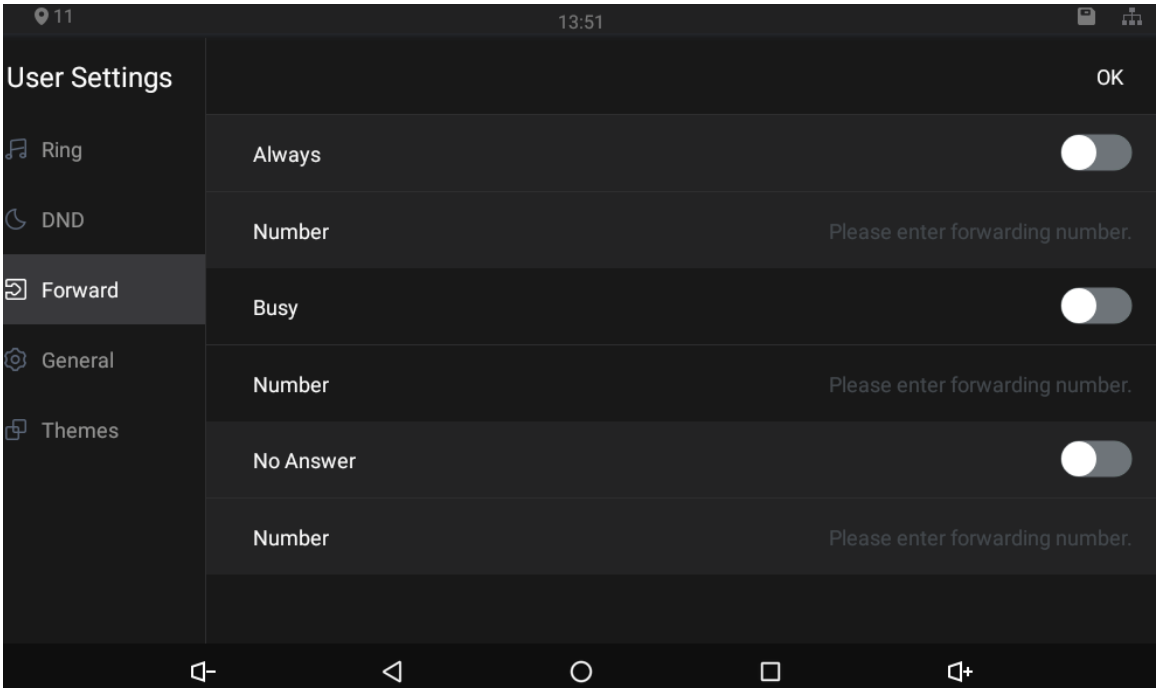
Figure 3-16 DND



3.5.3 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 3-17 Forward



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

3.5.4 Password

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

Figure 3-18 Password

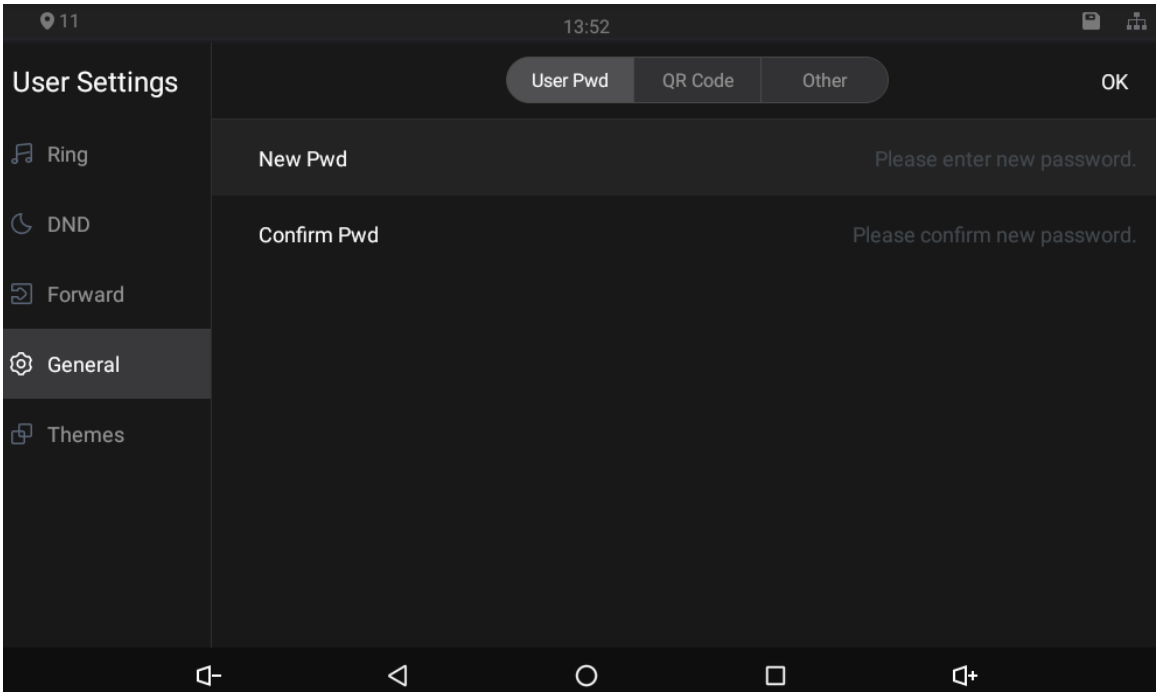


Figure 3-19 QR code

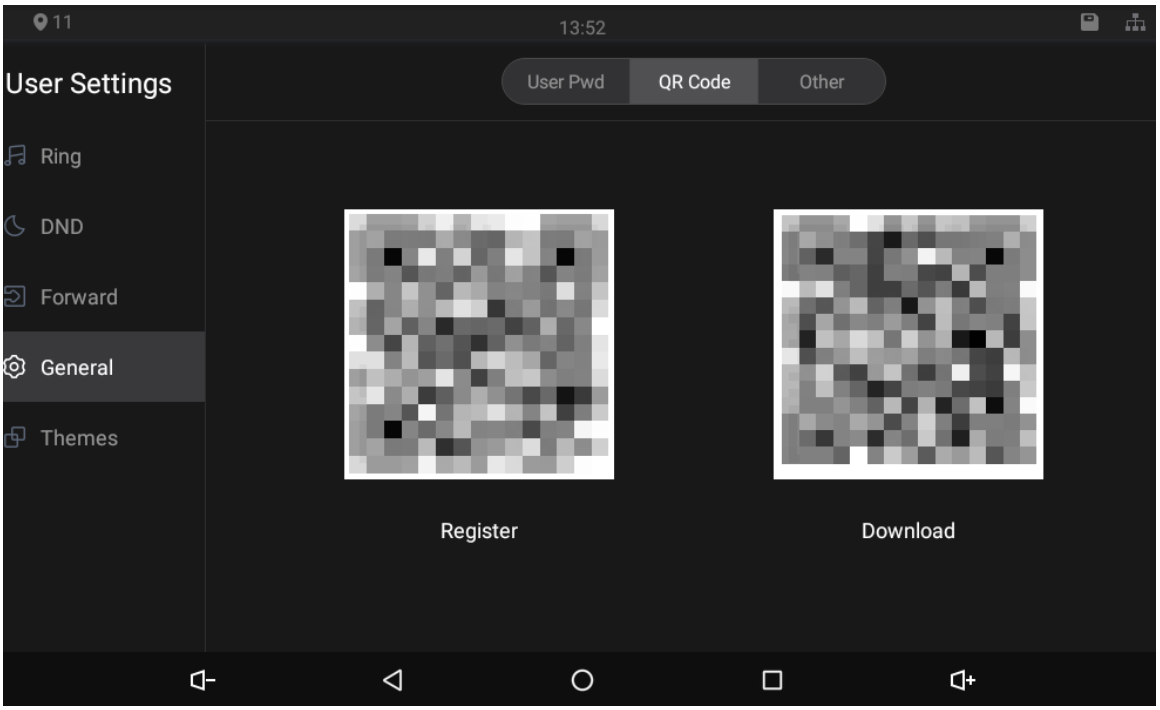
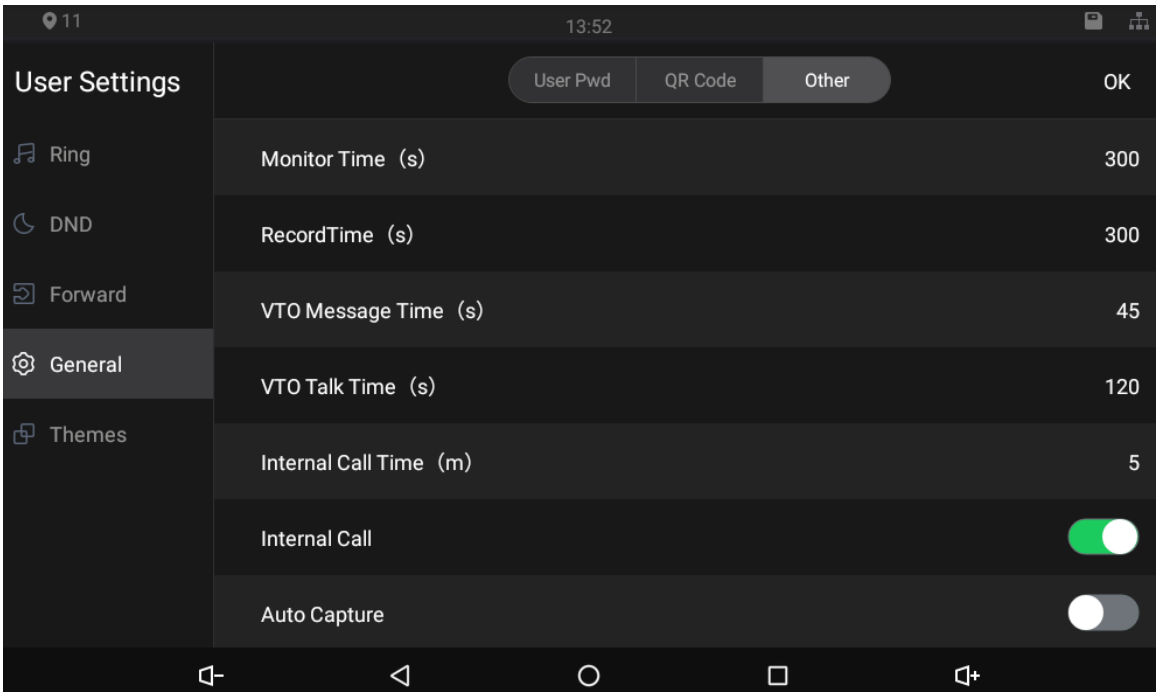


Figure 3-20 Other

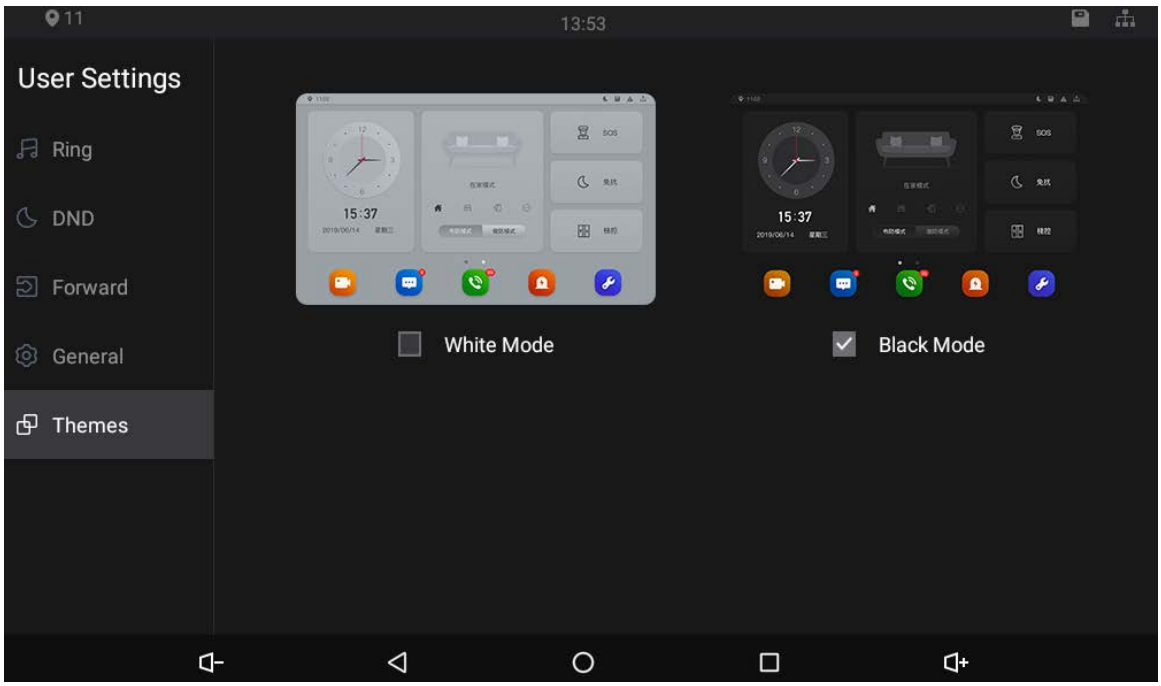


- **Monitor Time (s)**: You can watch monitoring images from the VTH for at most 300 seconds a time.
- **Record Time (s)**: You can record for up to 300-second audio files a time on the VTH.
- **VTO Message Time (s)**: Visitors can only leave up to 90-second message a time on the VTO (VTO).
- **VTO Talk Time (s)**: Visitors can talk to you through the VTO (VTO) for at most 300 seconds at a time.
- **Internal Call Time (s)**: You can talk to other VTHs for at most 60 seconds a time.
- **Internal Call**: After the Internal Call is enabled, you can call other VTHs from the VTH 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 VTO (VTO) would take three images of the visitor standing in front of the VTO.

3.5.5 Themes

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

Figure 3-21 Themes



3.6 Alarm Settings

3.6.1 Wire Zone

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

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

Figure 3-22 Wire zone

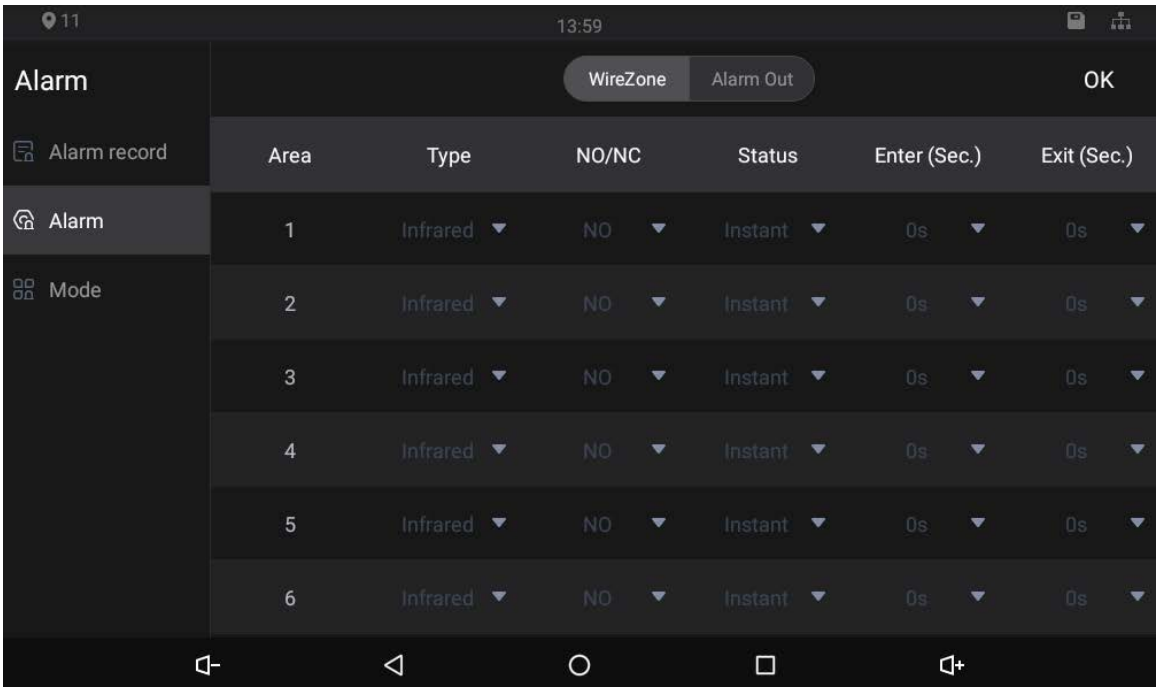


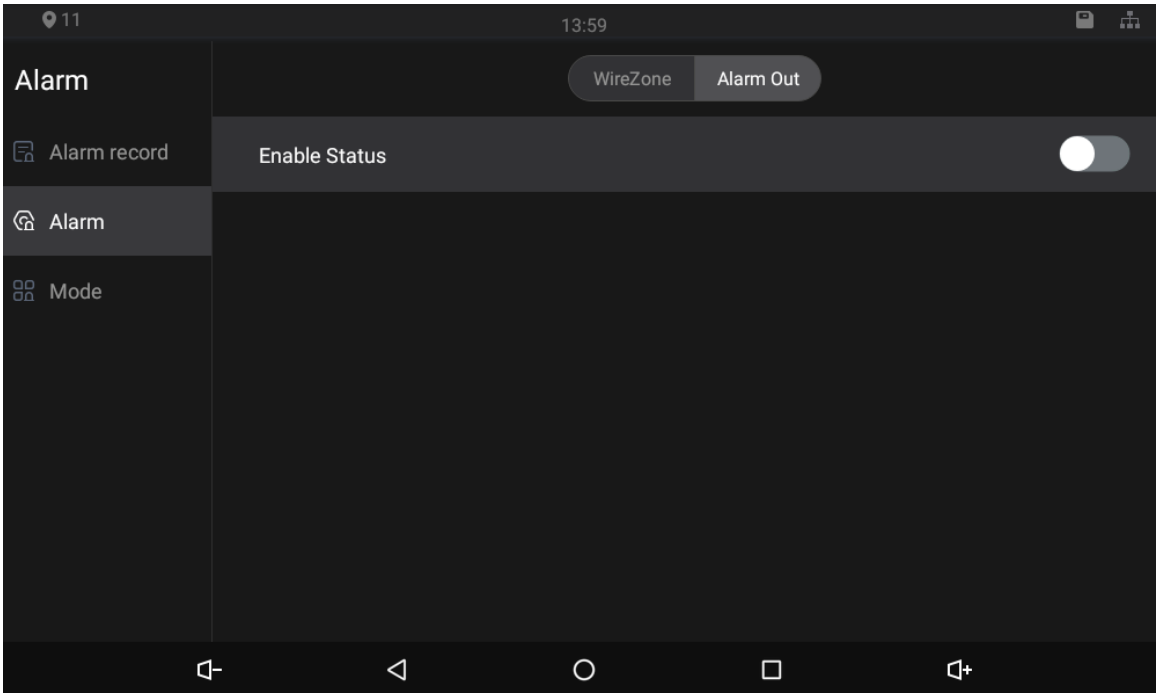
Table 3-4 Alarm settings

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 must be the same as detector type.
Status	There are 5 statuses: instant, delay, bypass, remote, and 24-hour protection zone. ● Instant: In Arm Mode, if you selected this status for an area, once alarms are triggered, the VTH will give out voice prompt immediately. ● Delay: In Arm Mode, if you selected this status for an area, once alarms are triggered, the VTH 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. ● Remote: 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.)	Configure the time. After configuring the **Delay Alarm** status for the area, if you enter the area from an unarmed area within the delay time, a linkage alarm will not be triggered. If the delay time comes to an end and the area is not disarmed, a linkage alarm will be triggered. The configured time is only effective in areas with **Delay Alarm**.
Exit (Sec.)	Configure the time. After configuring the **Delay Alarm** status for the area, if the delay time comes to an end, the area will enter the arming status. ● The configured time is only effective in areas with **Delay Alarm**. ● If multiple areas have an exit delay time configured, a prompt will appear stating the maximum delay time.

3.6.2 Alarm Output

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

Figure 3-23 Alarm output

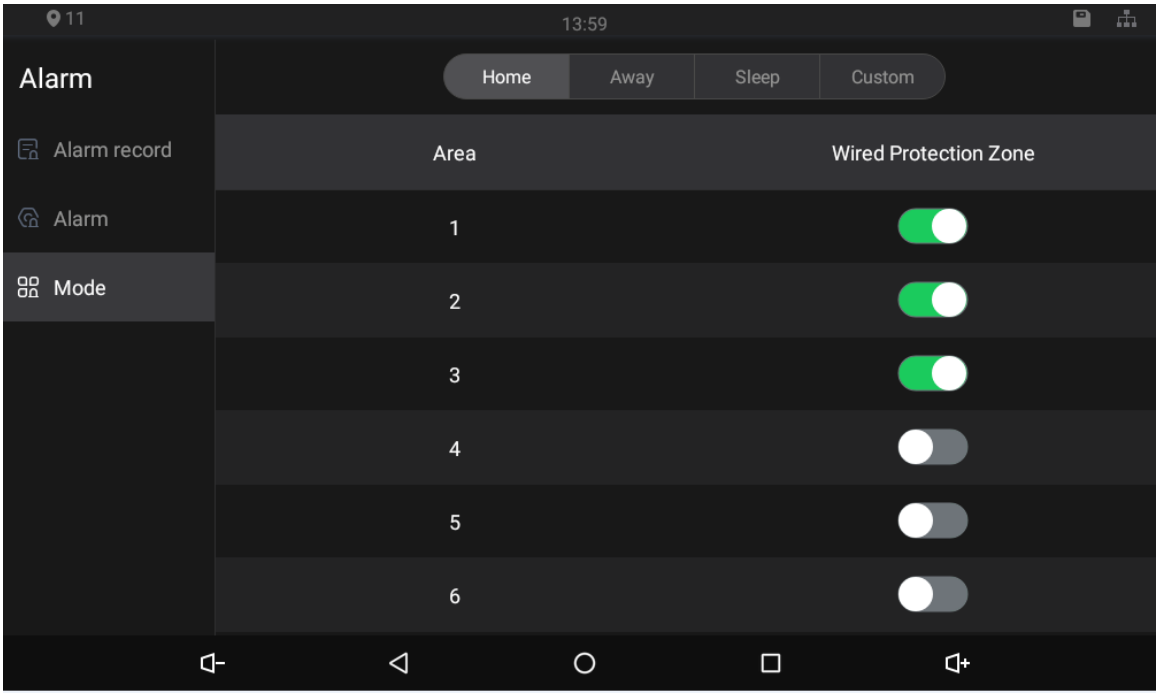


3.6.3 Alarm Mode

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

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

Figure 3-24 Alarm mode



4 Commissioning

4.1 Watching Monitoring Video

Tap , and the **Monitor** screen is displayed.

On the VTH, you can view videos captured by VTOs and IP cameras. You can also put VTOs and IP cameras that you like into the **Favorite** folder by tapping at the lower right corner of each device.

Figure 4-1 Monitor (1)

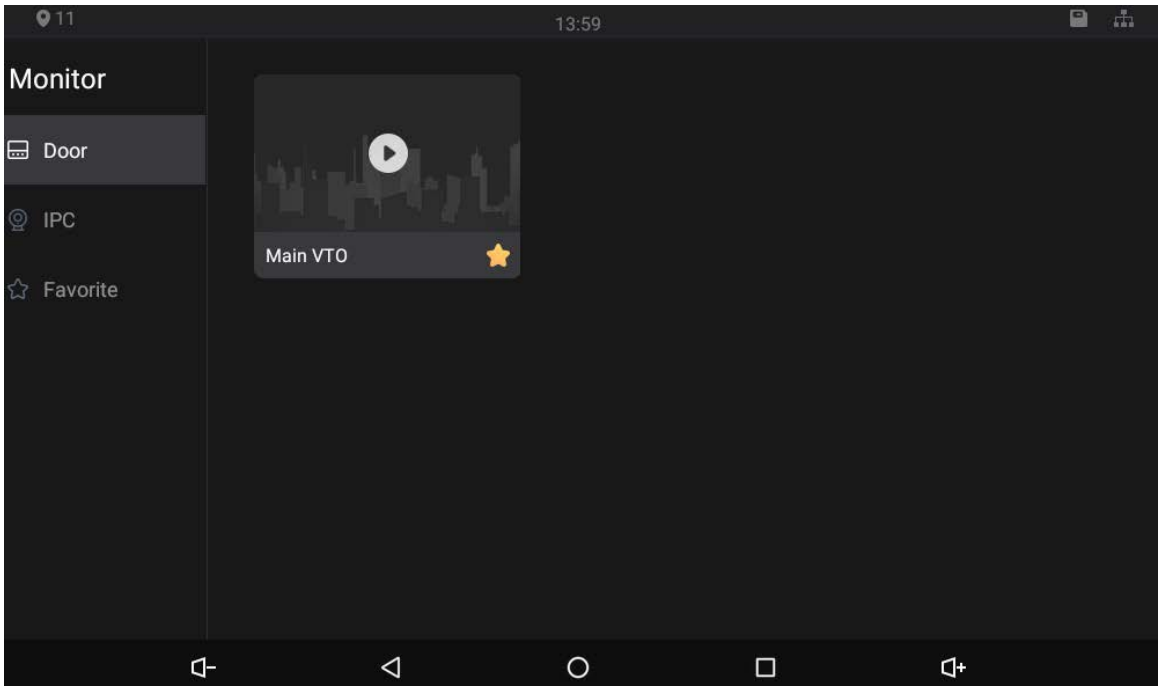


Figure 4-2 Monitor (2)

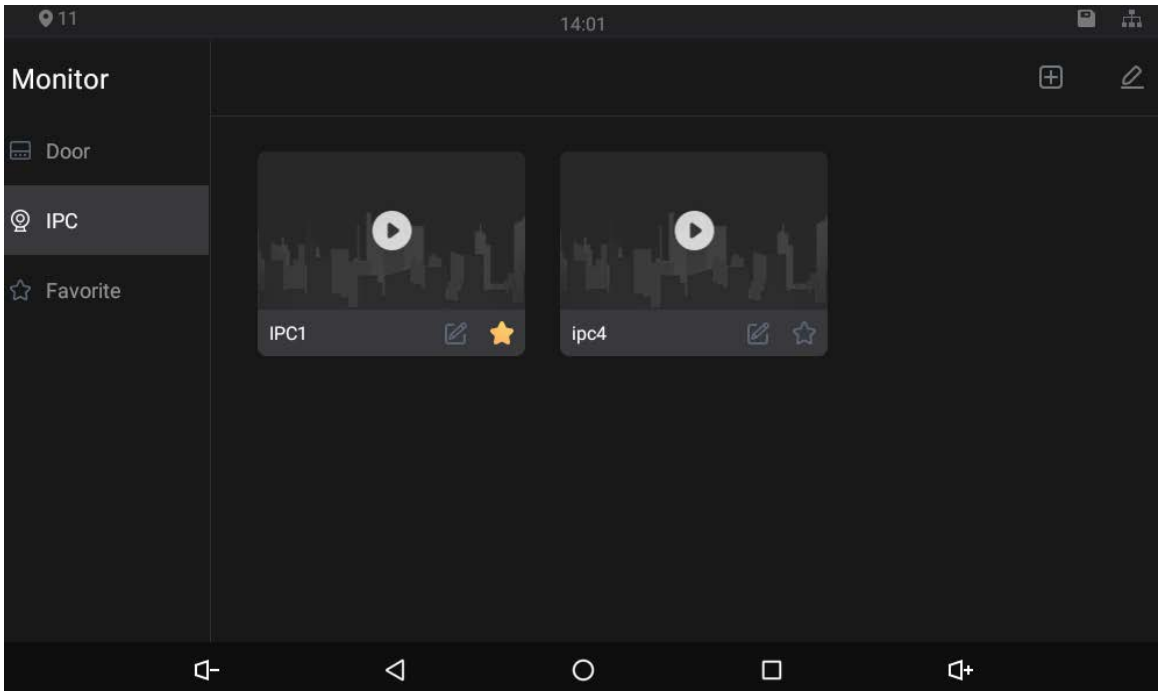
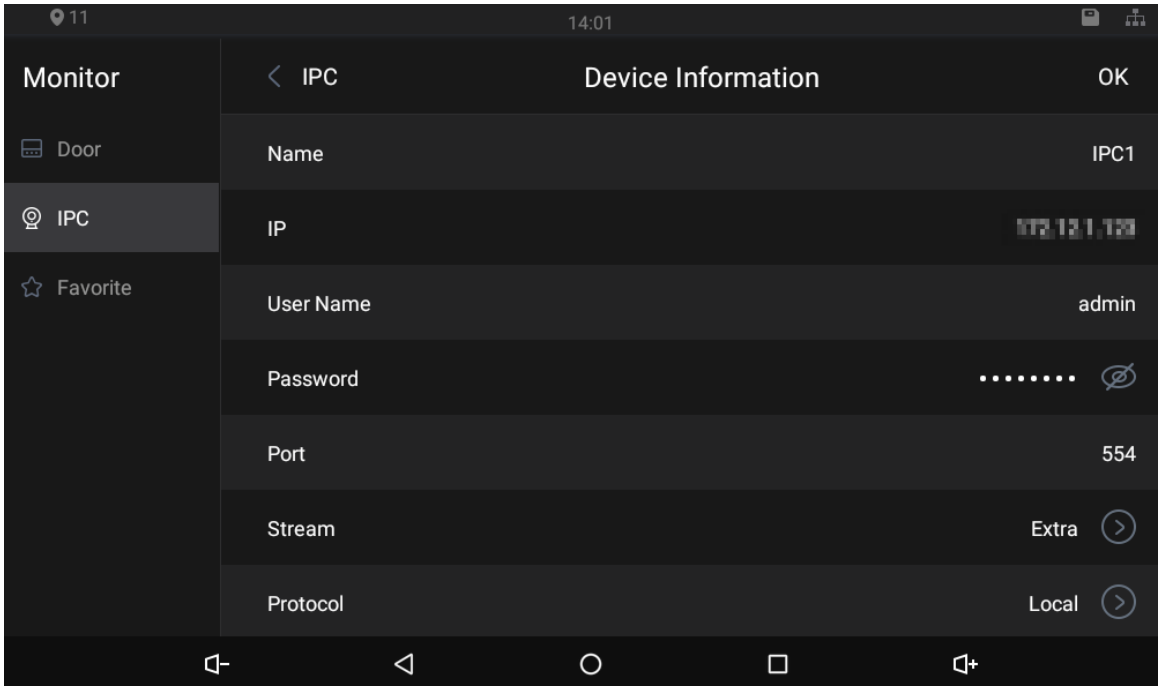


Figure 4-3 IPC information



- Tap to turn down the volume.
- Tap to go to the previous page.
- Tap to go to the main menu.
- Tap to se all thumbnails of screens you have opened. Select a screenand slide it to the left or right to close the screen.
- Tap to turn up the volume.

4.2 Checking Messages

Tap to view messages and videos left by visitors, or public notices released by the management center.

4.3 Making Calls

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

You can also call the VTH from VTOs.

Figure 4-4 Making calls

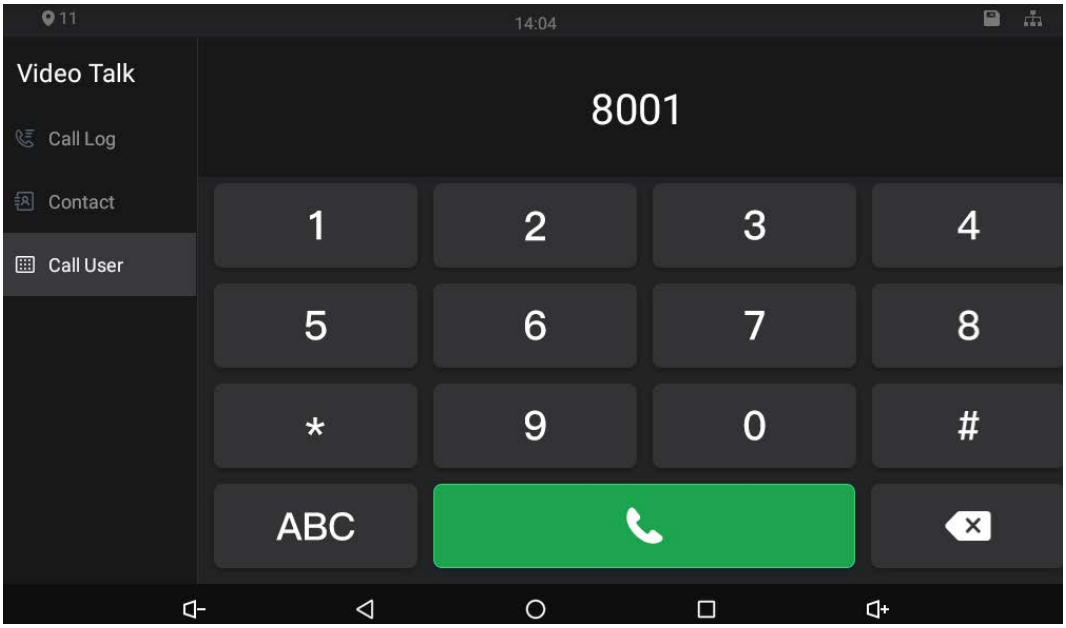


Figure 4-5 Calling

- When Figure 4-28 appears, it means that SD card has been inserted into the VTH. 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.

4.4 Viewing Alarms Logs

Tap , and then the **Alarm** screen is displayed. Peripheral alarm modules can be connected to the VTH. 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 4-6 View alarm prompt

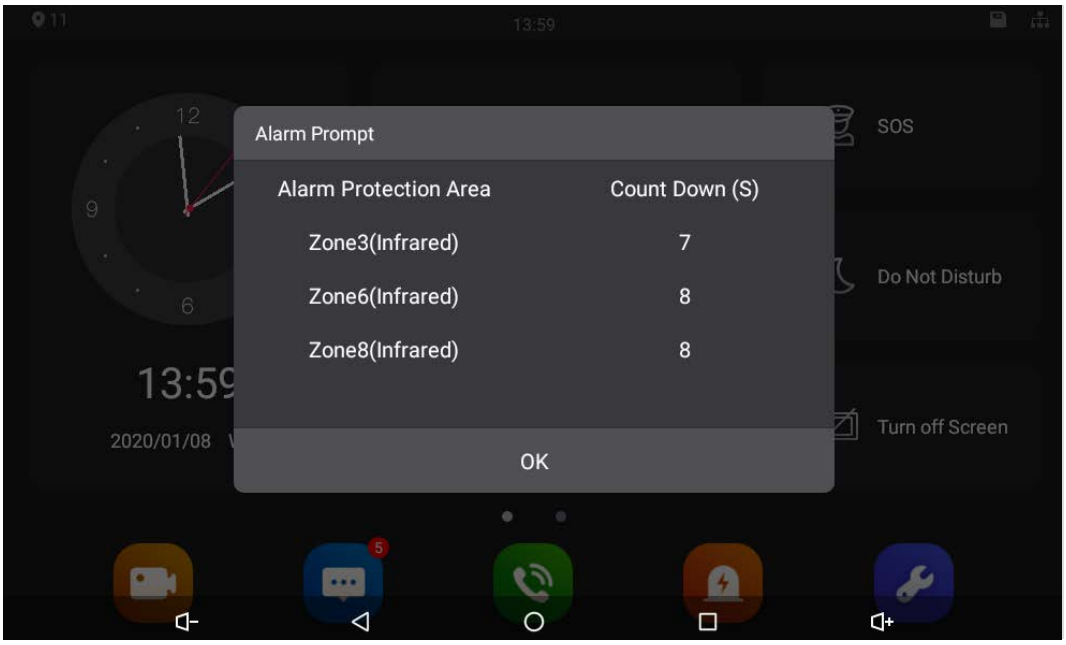
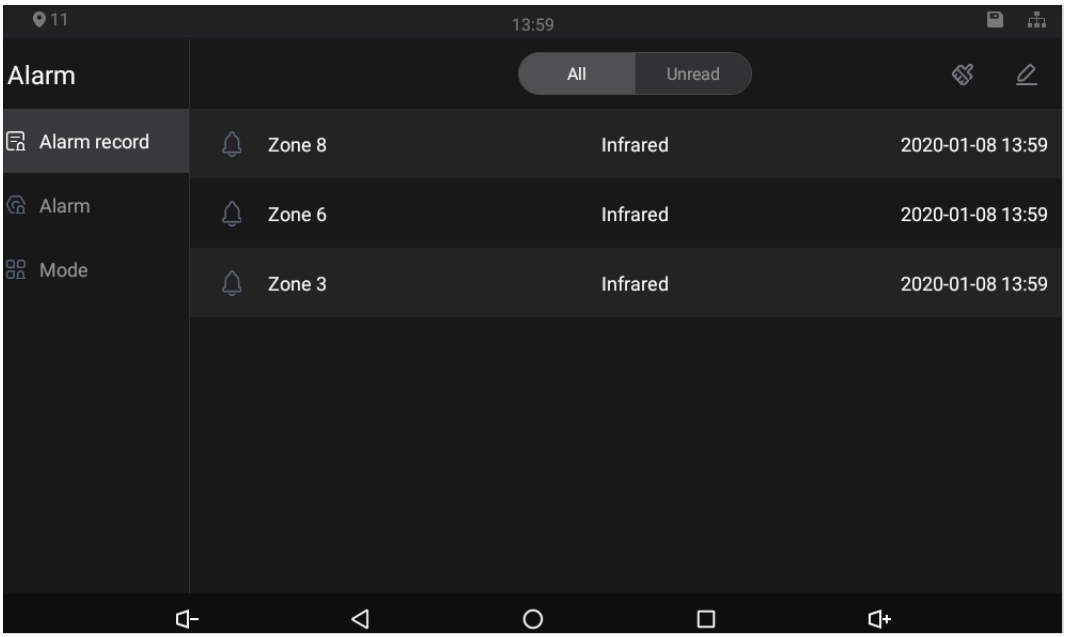


Figure 4-7 Viewing alarm record



4.5 Viewing Information

Figure 4-8 Viewing guest message

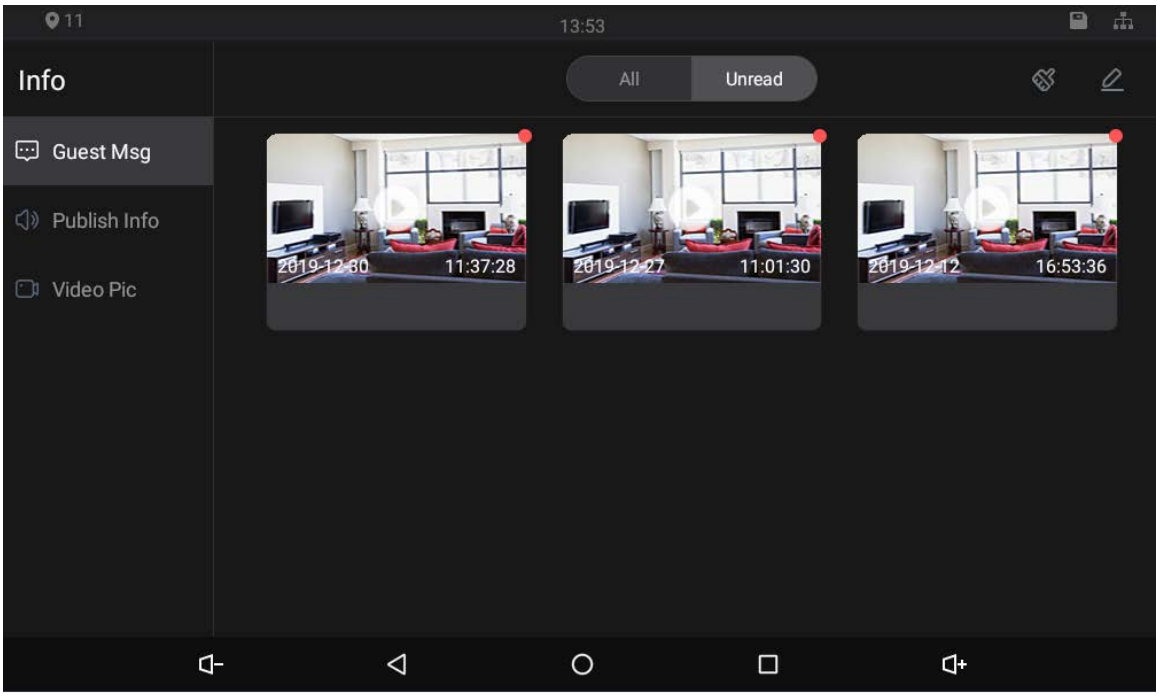


Figure 4-9 Viewing publish information

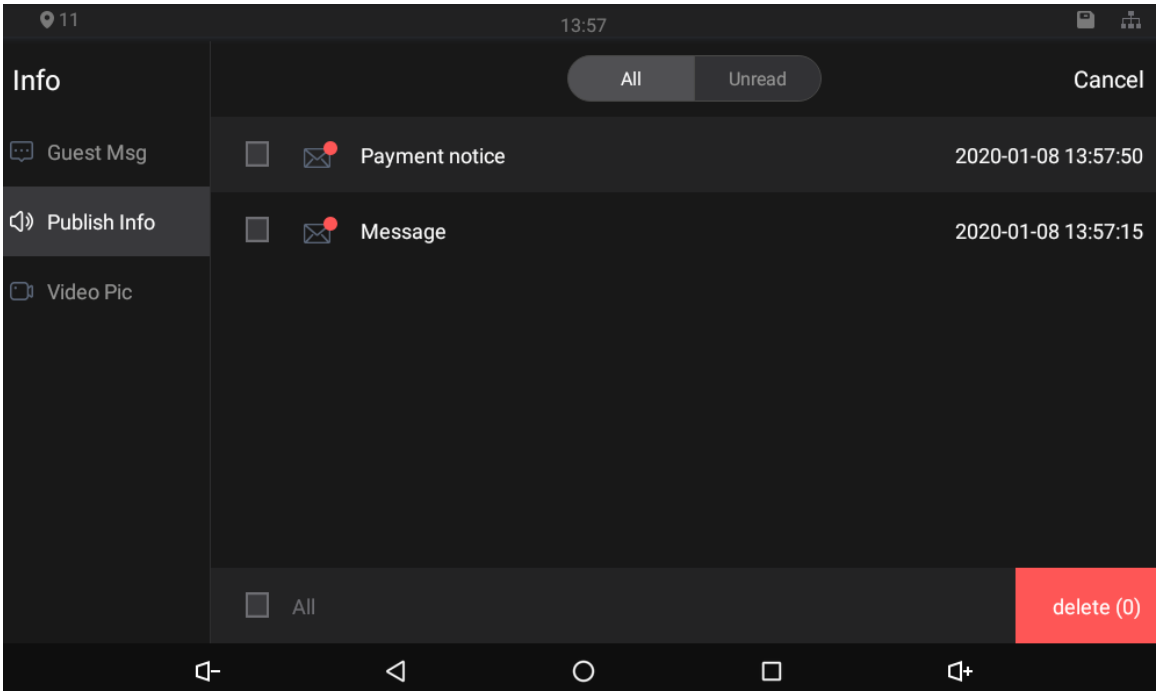
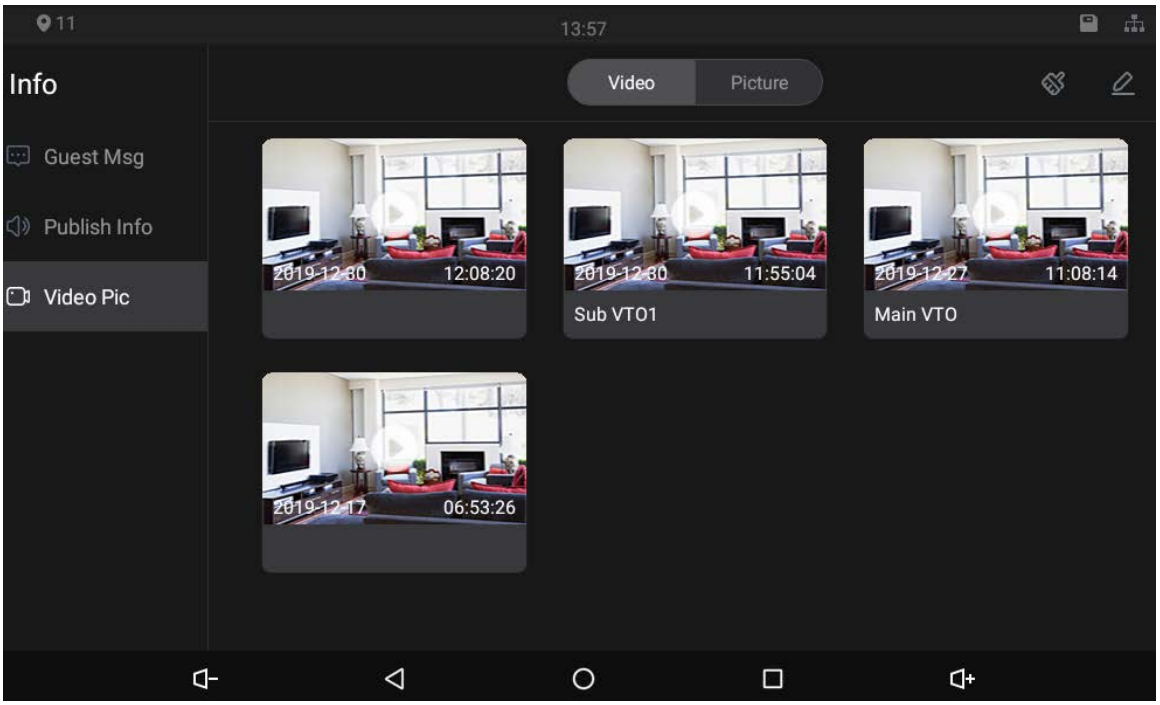


Figure 4-10 Viewing video pictures



Appendix 1 Cybersecurity Recommendations

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

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

1. Physical Protection

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

2. Change Passwords Regularly

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

3. Set and Update Passwords Reset Information Timely

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

4. Enable Account Lock

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

5. Change Default HTTP and Other Service Ports

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

6. Enable HTTPS

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

7. MAC Address Binding

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

the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

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

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

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

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