

7-inch and 10-inch Android Indoor Monitor








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
V1.0.2	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, 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



- 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
2 Introduction	1
2.1 Overview	1
2.2 Features	1
2.3 Dimensions.....	3
2.3.1 7-inch VTH	3
2.3.2 10-inch VTH.....	4
2.4 Cable Connections.....	5
3 Installation	6
3.1 Preparations.....	6
3.2 Installation Guide.....	6
4 Configuration	8
4.1 Configuration Overview	8
4.2 Configuring VTH.....	8
4.2.1 Initialization	8
4.2.2 Configuring Network Parameters.....	9
4.2.3 Entering Project Settings	11
4.2.4 Configuring VTH.....	11
4.2.5 Configuring SIP Server	12
4.2.6 Configuring VTO.....	13
5 Commissioning	15
5.1 Watching Monitoring Video	15
5.2 Checking Messages.....	15
5.3 Making Calls.....	15
5.4 Viewing Alarms Logs.....	16
5.5 Viewing Information	16
Appendix 1 Cybersecurity Recommendations	18

1 Introduction

1.1 Overview

The 10-inch digital Android VTH, widely used in intelligent buildings, integrates functions of monitoring, voice communication, 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.

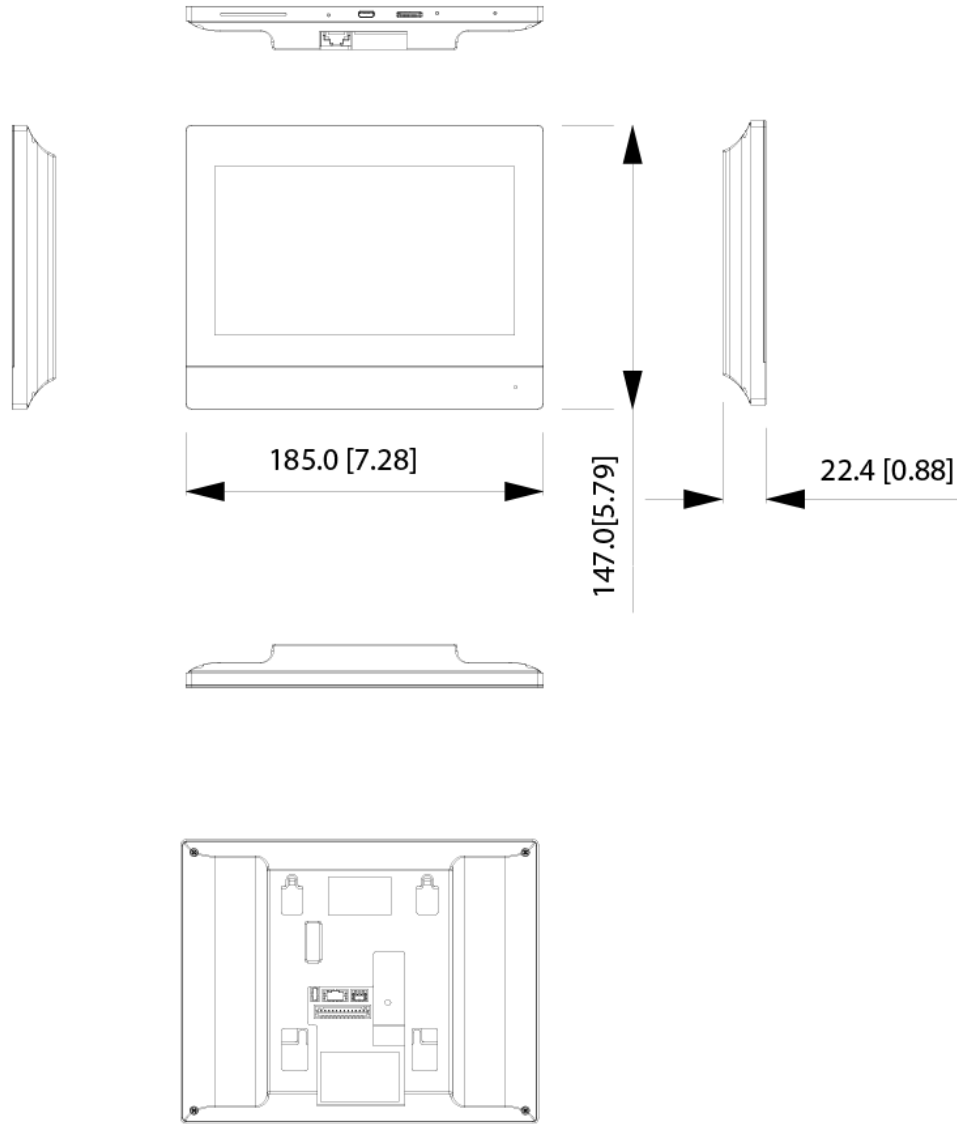
Message check

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

1.3 Dimensions

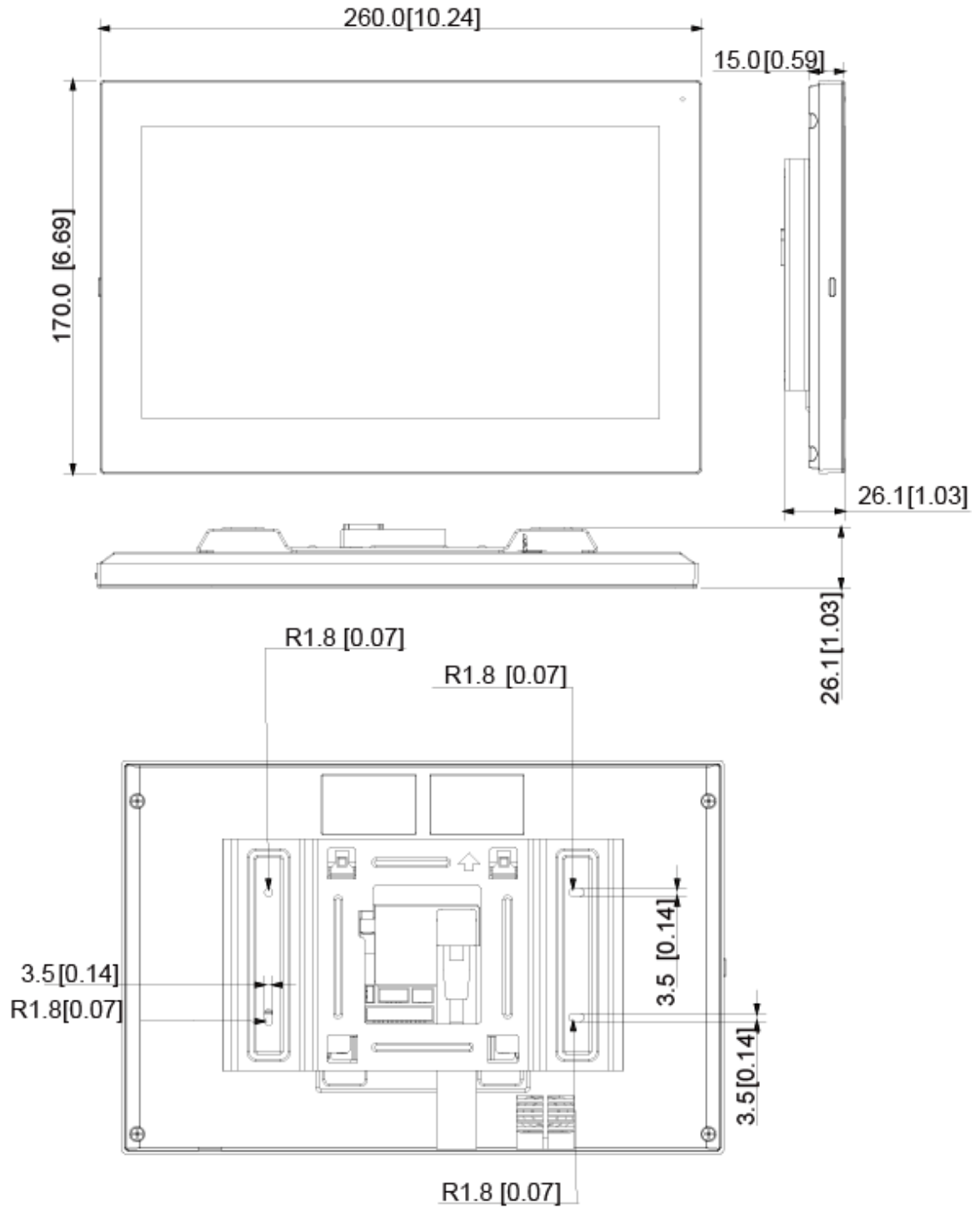
1.3.1 7-inch VTH

Figure 1-1 Dimensions (mm [inch])



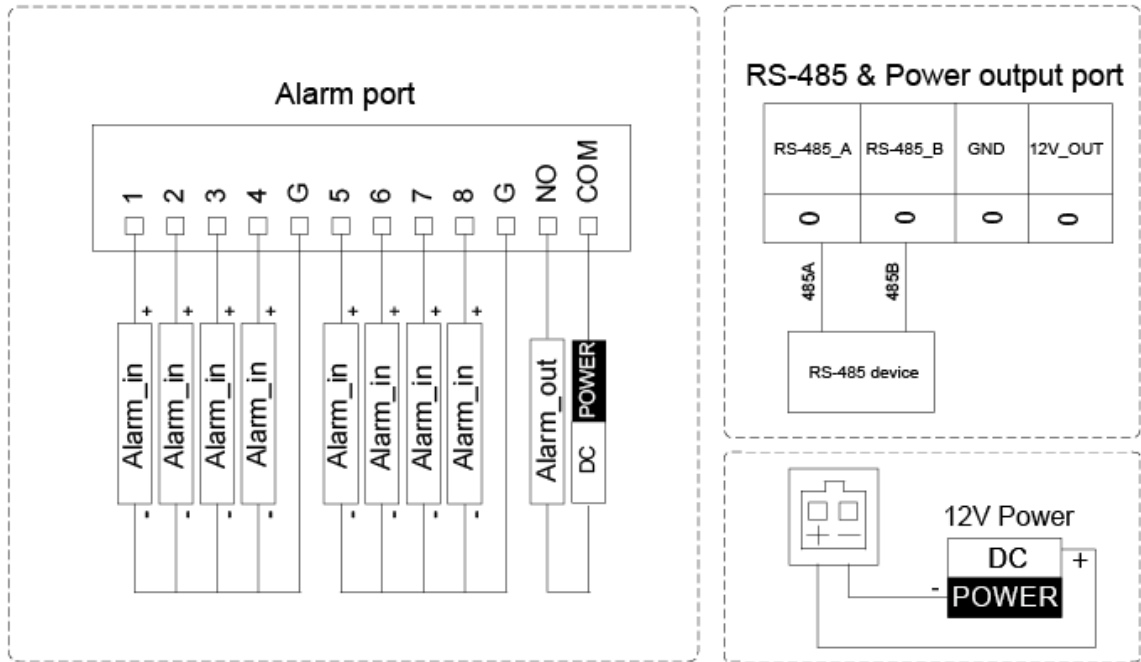
1.3.2 10-inch VTH

Figure 1-2 Dimensions (mm [inch])



1.4 Cable Connections

Figure 1-3 Cable connection



2 Installation

2.1 Preparations



- Do not install the VTH in harsh environment with condensation, high temperature, dust, corrosive substance and direct sunlight.
- In case of abnormality after powering on the VTH, cut off the power supply at once, and unplug the network cable. Power on after troubleshooting.
- Installation should be done by professional teams. Do not dismantle or repair the device by yourself in case of device failure. Contact after-sales service if you need any help.

2.2 Installation Guide

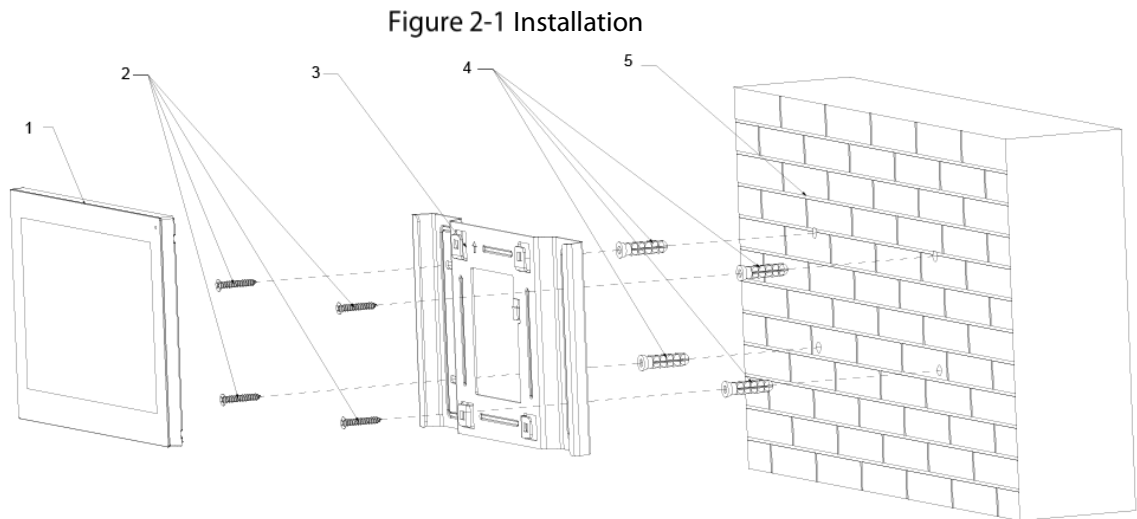


Table 2-1 Components

No.	Name
1	VTH
2	ST3 self-tapping screws
3	Bracket
4	Anchor bolts
5	Wall

Figure 2-2 Screw hole distances and diameters (10-inch VTH)

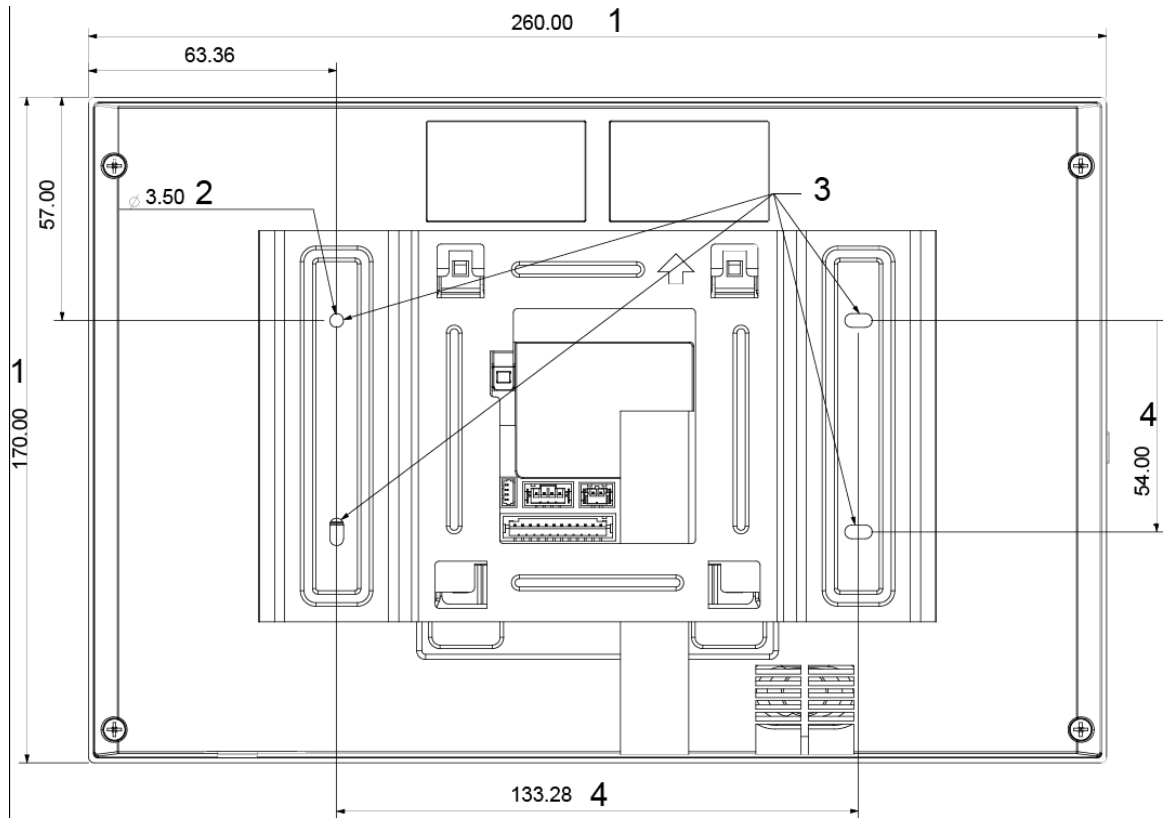


Table 2-2 Description of screw hole distances and diameters

No.	Description
1	VTH 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 VTH on the wall with screws.

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

3 Configuration

You need to configure IP, Wi-Fi, VTO parameters, SIP server information on the VTH, and then the VTH can call the VTO and the management center.



The VTH screen only supports single-touch operation.

3.1 Configuration Overview

- Step 1 Plan the location for the SIP server and plan IP and numbers for each VTO and VTH.
- Step 2 Make sure that there is no short circuit and open circuit.
- Step 3 Configure parameters for VTO.
- Step 4 Add VTH to the SIP server.
- Step 5 Configure parameters for VTH.
- Step 6 Commissioning.

3.2 Configuring VTH

3.2.1 Initialization



The default IP address of the VTH is 192.168.1.108.

You need to initialize the VTH when you log in for the first time.

- 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.

Figure 3-1 Main menu (1)

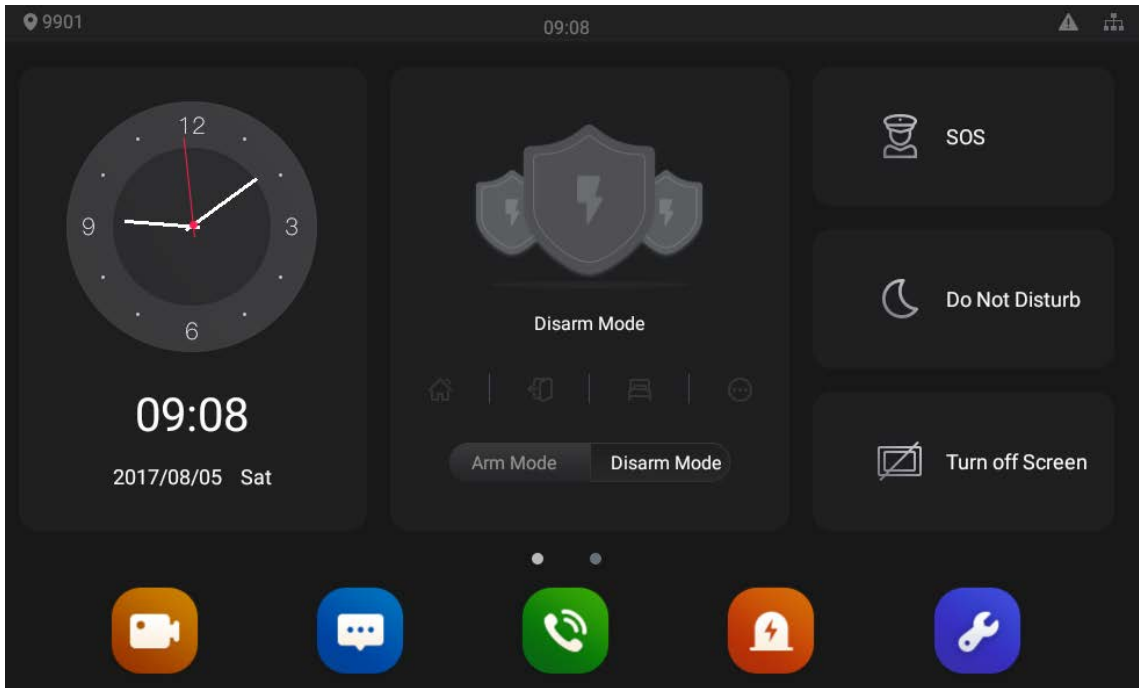
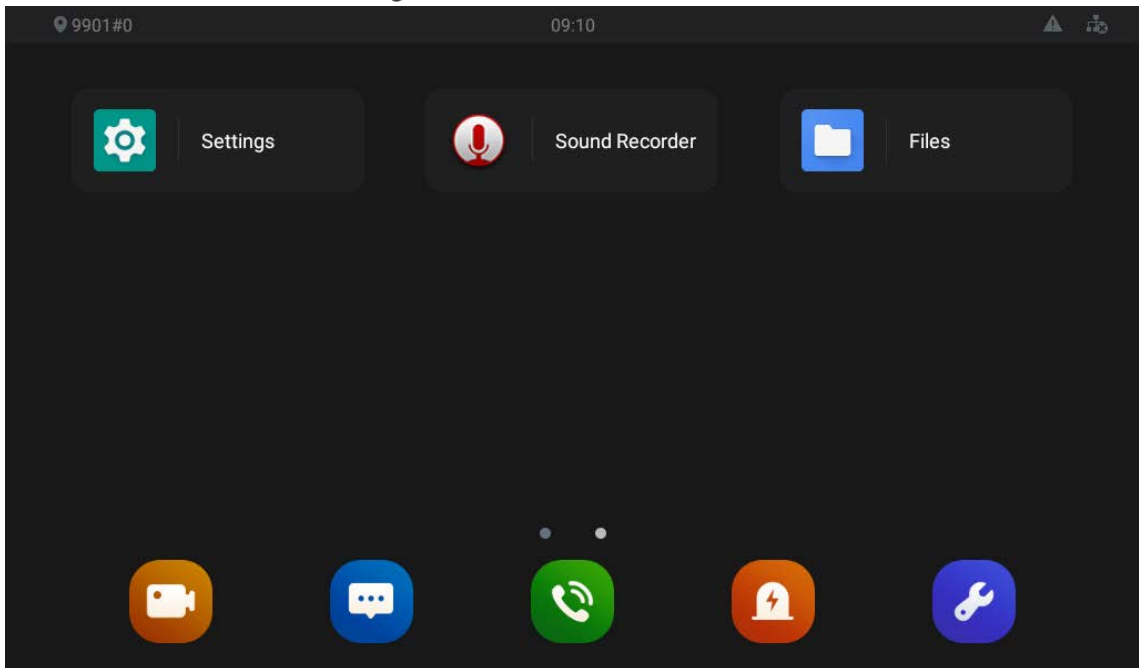


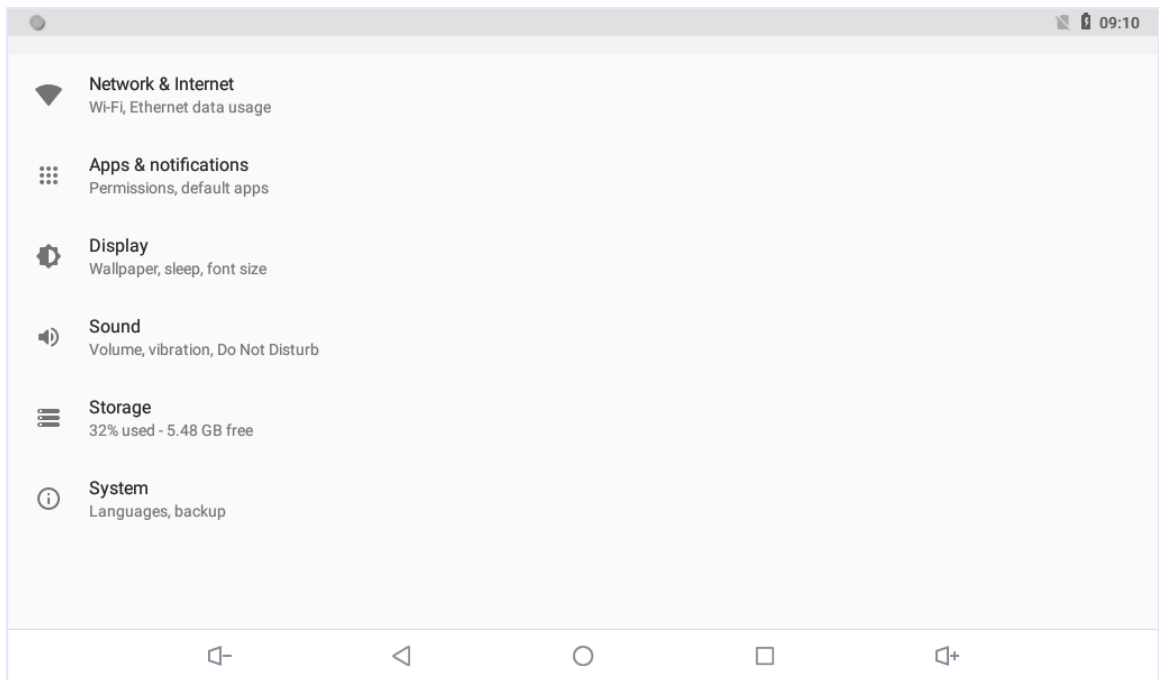
Figure 3-2 Main menu (2)



3.2.2 Configuring Network Parameters

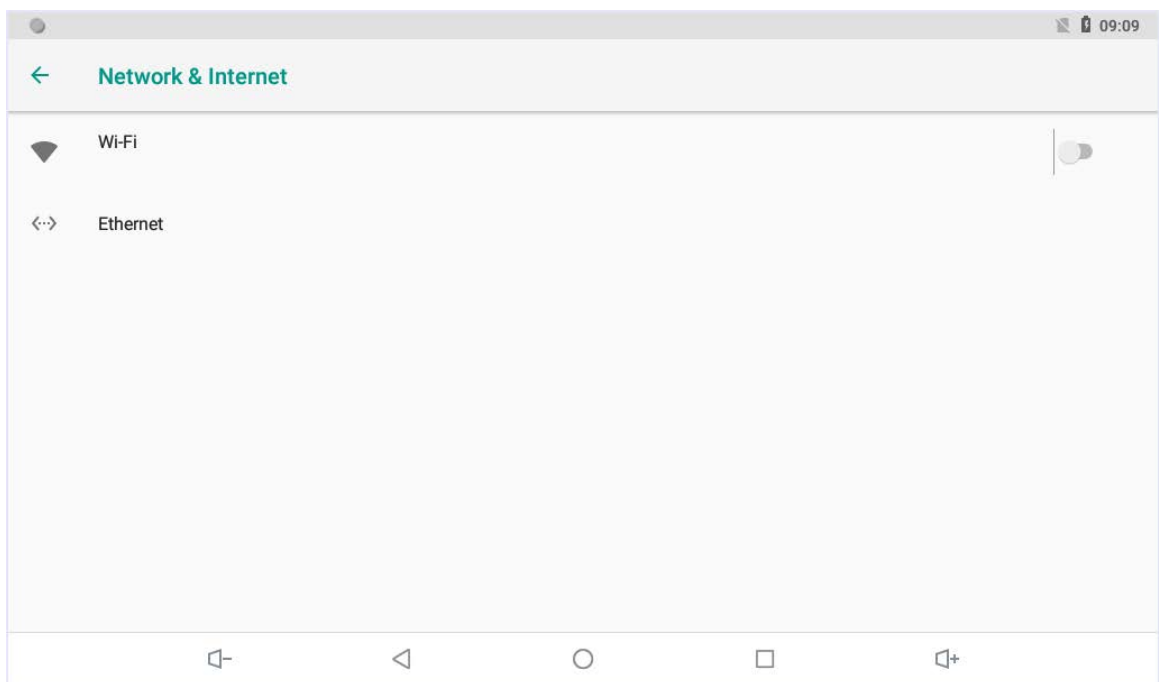
Step 1 Select **Settings** > **Network & Internet** on the main menu.

Figure 3-3 Network settings (1)



Step 2 Select either **Wi-Fi** or **Ethernet** to connect to the network.

Figure 3-4 Network settings (2)

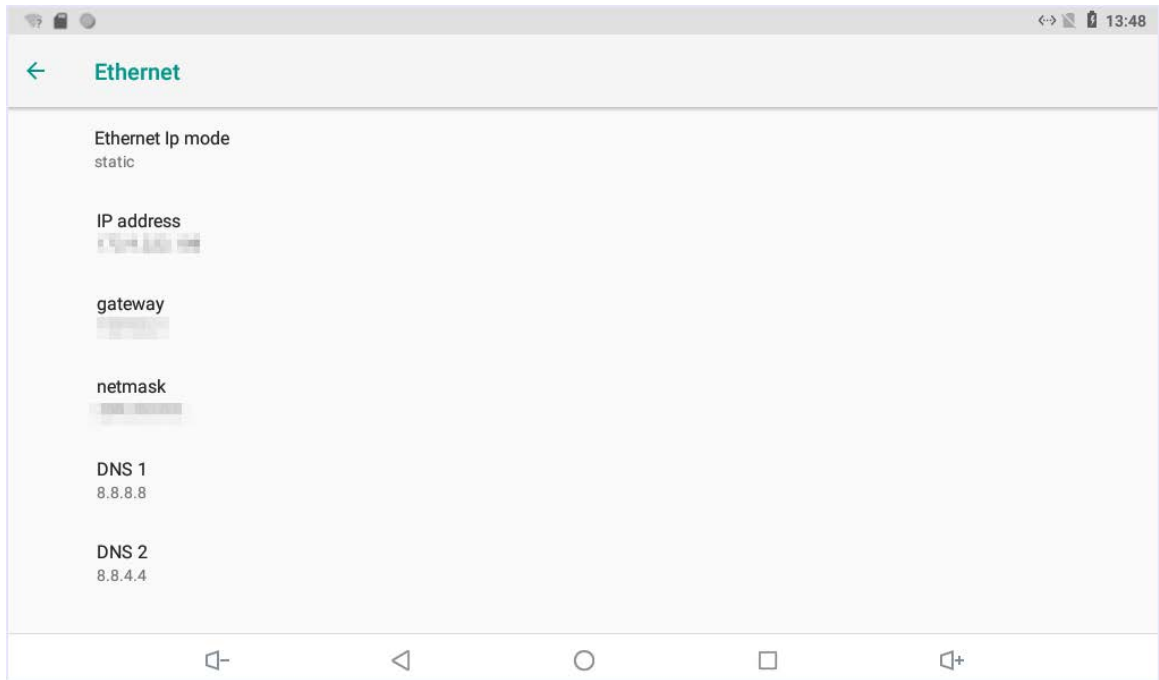


- **Wi-Fi**
Click to see all the available networks. Tap the Wi-Fi name, and then enter password to connect to the network.
- **Ethernet**
Tap **Ethernet** to go to the configuration screen. Configure the parameters including IP address, gateway, net mask and DNS.




The **Ethernet IP mode** is static by default. You can also change it to DHCP to get the allocated IP address.

Figure 3-5 Ethernet



3.2.3 Entering 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.

3.2.4 Configuring VTH

- Step 1** Tap **VTH Config** on the **Project Setting** Screen.
- Step 2** Configure the parameters.

Figure 3-6 VTH configuration

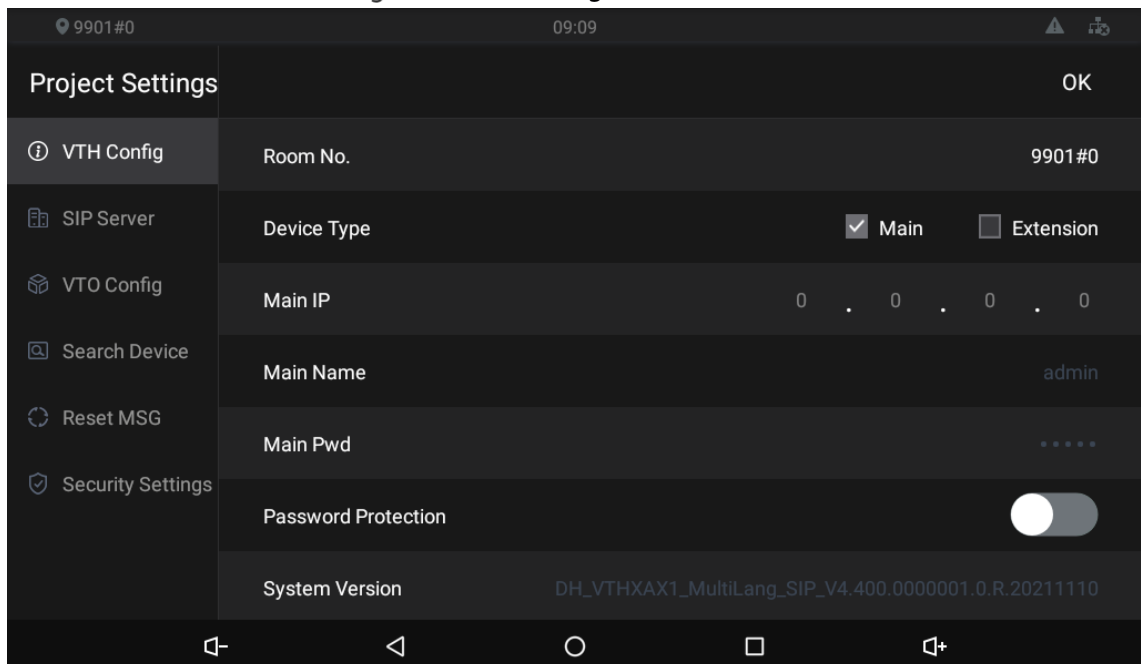



Table 3-1 Parameter description

Parameter	Description
Room No.	<p>Number of the room where the VTH is installed.</p>  <p>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...</p>
Device Type	<ul style="list-style-type: none"> • 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.

3.2.5 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

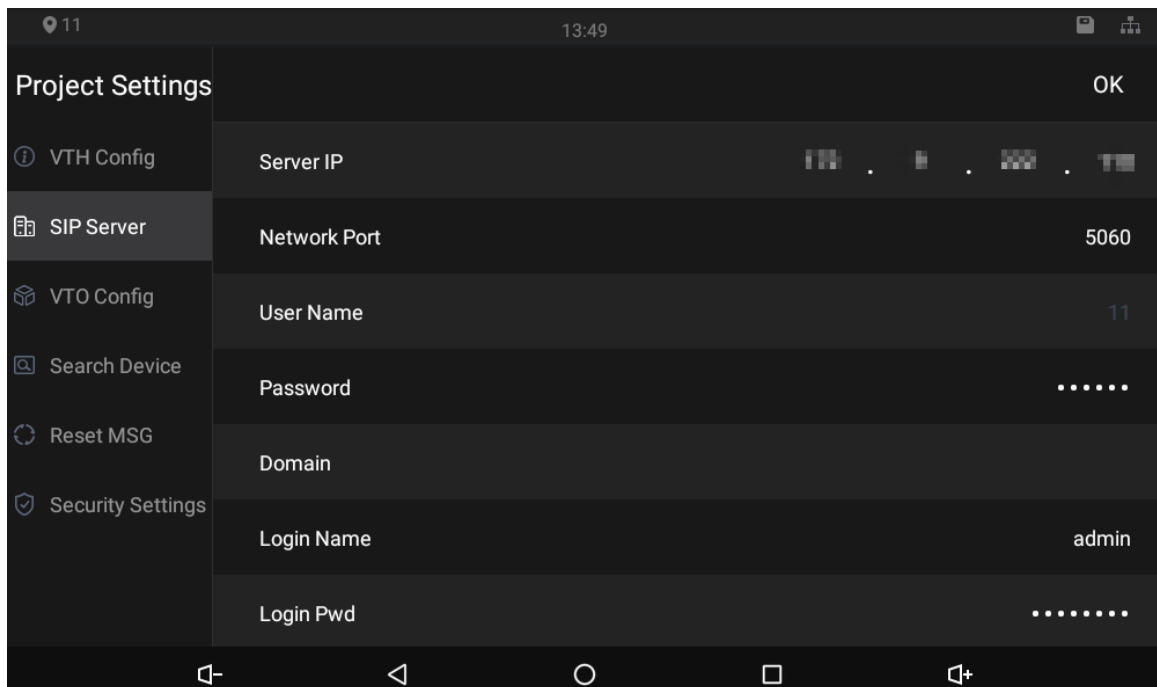


Table 3-2 SIP server description

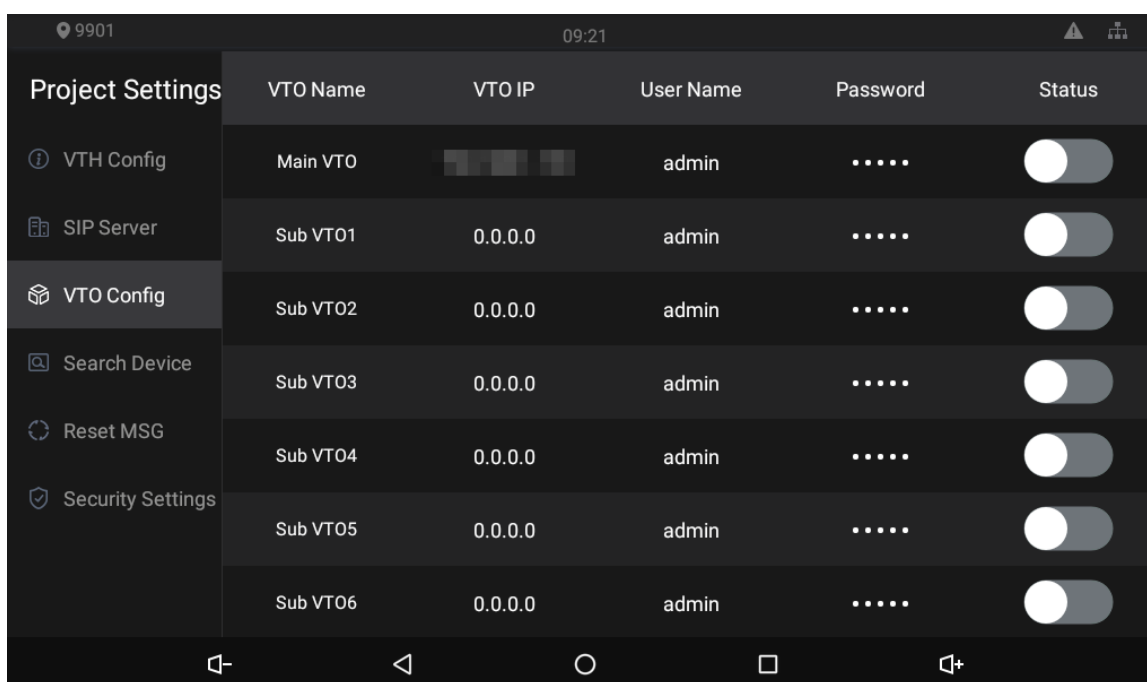
Parameter	Description
Server IP	<ul style="list-style-type: none"> ● IP address of the platform that works as the SIP server. ● IP address of the VTO that works as the SIP server.
Network Port	<ul style="list-style-type: none"> ● 5060 by default when a VTO works as the SIP server. ● 5080 by default when 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.

3.2.6 Configuring VTO

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

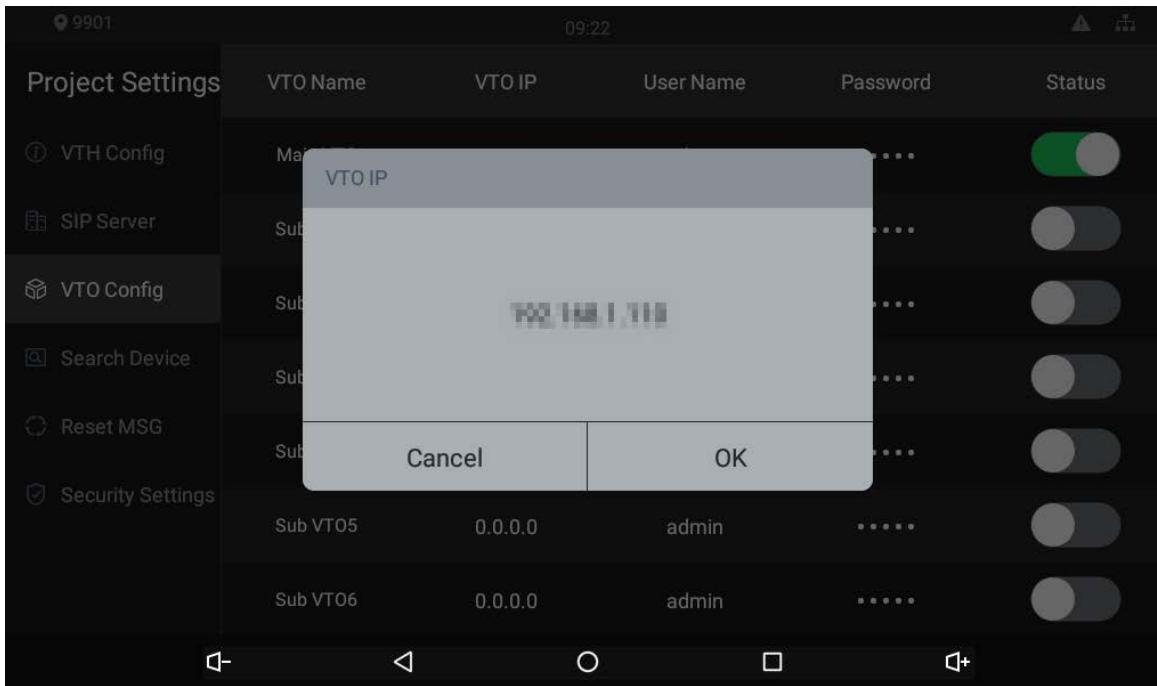
Step 1 Tap **VTO Config** on the **Project Setting** screen.

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 IP address that you planned for the VTO.

Step 5 Tap **OK** to save the configuration.



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

Step 6 Tap at the **Status** bar of the VTO you just configured to make it work.

4 Commissioning

4.1 Watching Monitoring Video

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


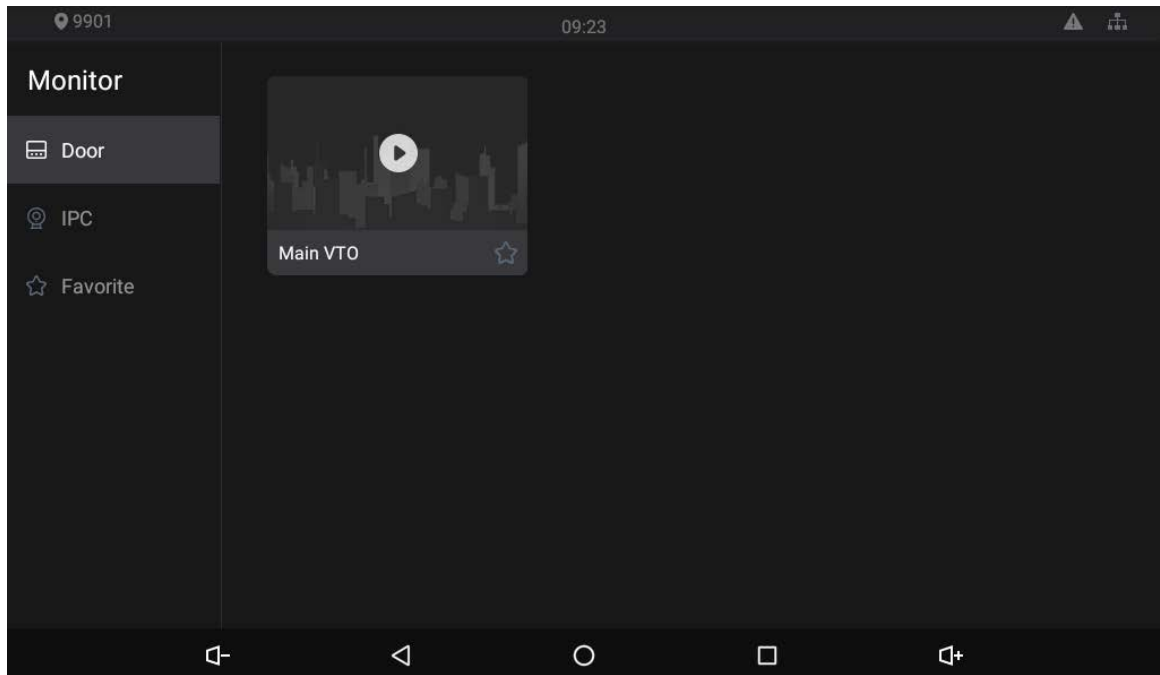

On the VTH, you can view videos from VTO and IP cameras. You can also put VTO and IP cameras that you like into the **Favorite** folder by tapping  at the lower right corner of each device.


Figure 4-1 Monitor




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 make calls to other VTH and the management center; you can also view call logs and your contacts on this screen.

4.4 Viewing Alarms Logs

Tap , and then the **Alarm** screen 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.

4.5 Viewing Information

Figure 4-2 View guest message

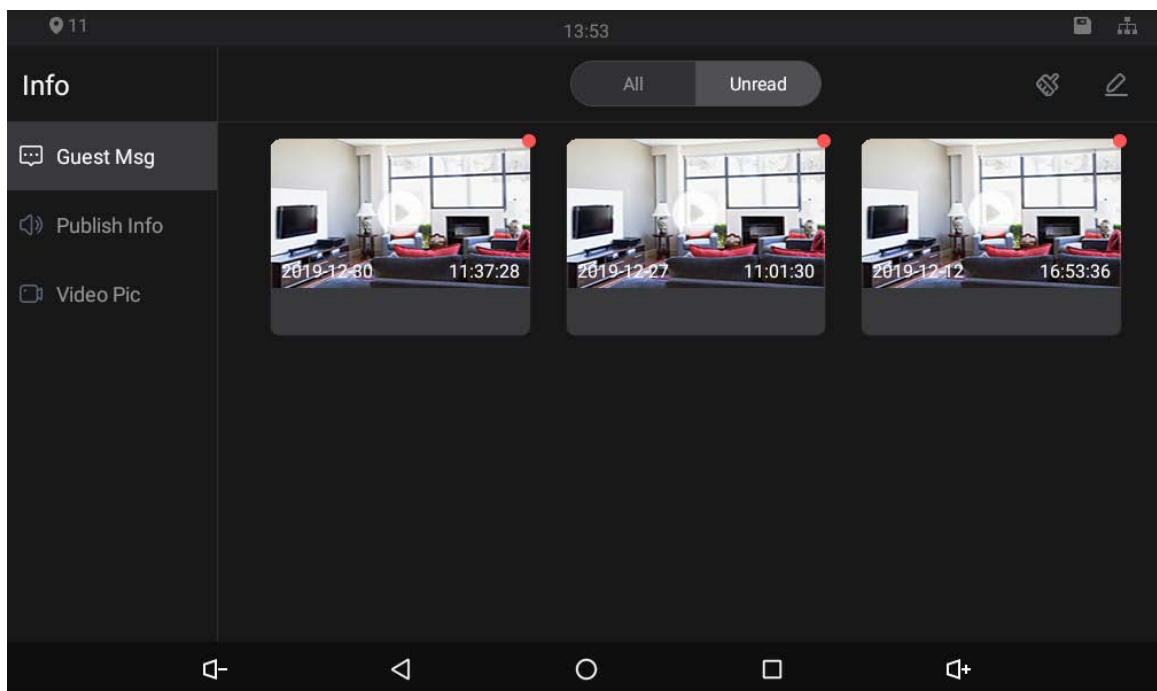


Figure 4-3 Viewing publish information

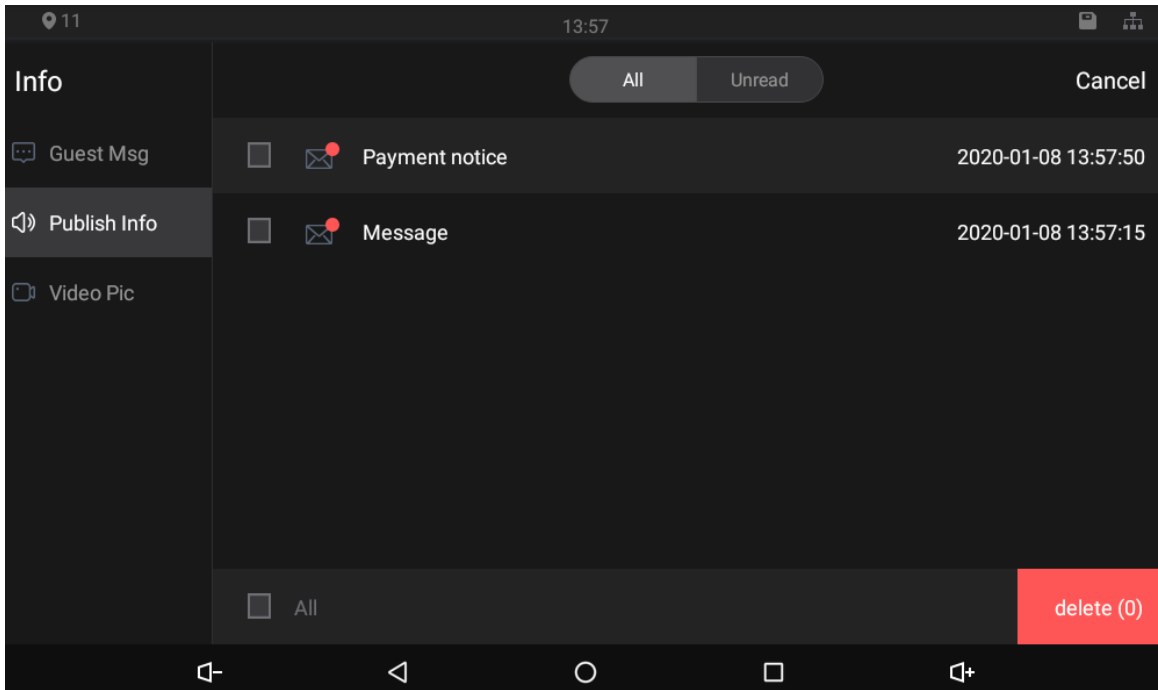
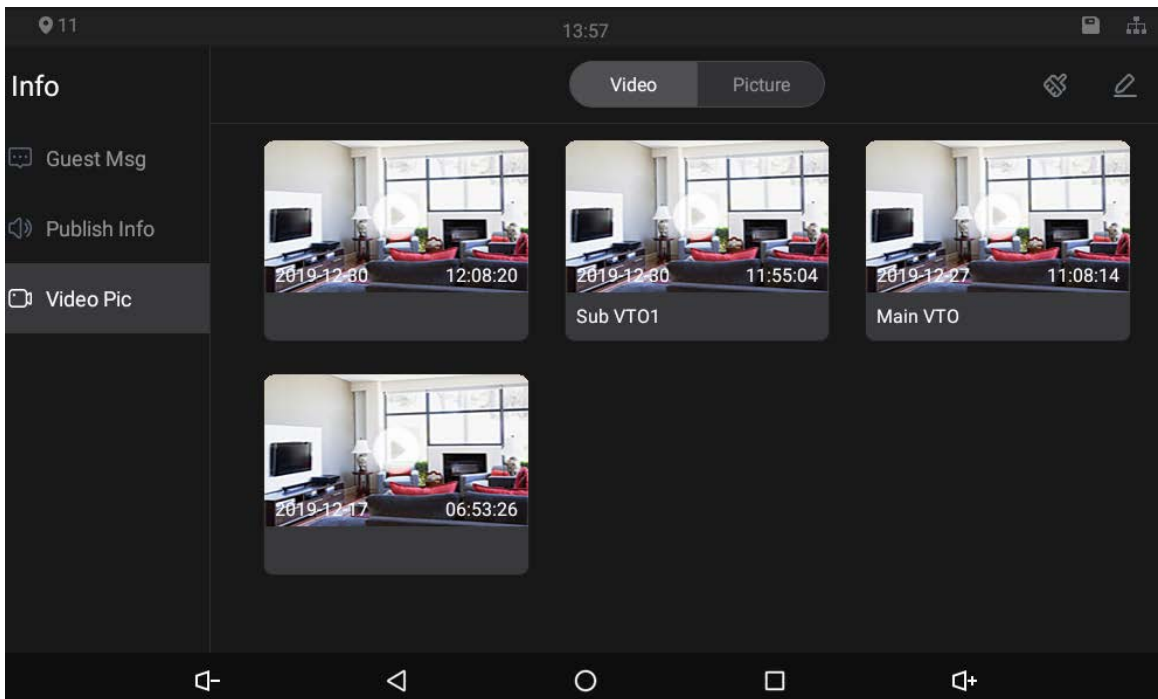


Figure 4-4 Viewing video pictures



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.