



VTH Series  
User's Manual

Dahua Technology Co., Ltd

# Foreword

## General

This manual offers reference material and general information about the basic operation, maintenance, and troubleshooting for a Dahua security device. Read, follow, and retain the following safety instructions. Heed all warning on the unit and in the operating instructions before operating the unit. Keep this guide for future reference.

## Safety Instructions

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

Signal Words	Meaning
 <b>WARNING</b>	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 <b>CAUTION</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 <b>NOTE</b>	Provides additional information as the emphasis and supplement to the text.

## Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	January 2019
2	V1.0.1	Revised for North America	July 2019

## Privacy Protection Notice

As the device user or data controller, you may collect personal data such as face images, fingerprints, license plate number, email address, phone number, GPS location and other sensitive or private information. You must ensure that your organization is in compliance with local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact

## About the Guide

- This user guide has been compiled with great care and the information it contains has been thoroughly reviewed and verified.
- The text was complete and correct at the time of printing. This guide may be periodically updated to reflect changes to the product or to correct previous information and the content of this guide can change without notice.
- If you encounter an error or have any questions regarding the contents of this guide, contact customer service for the latest documentation and supplementary information.

- Dahua accepts no liability for damage resulting directly or indirectly from faults, incompleteness, or discrepancies between this guide and the product described. Dahua is not liable for any loss caused by installation, operation, or maintenance inconsistent with the information in this guide.
- All the designs and software are subject to change without prior written notice. The product updates may cause some differences between the actual product and the Guide. Please contact the customer service for the latest program and supplementary documentation.
- Video loss is inherent to all digital surveillance and recording devices; therefore Dahua cannot be held liable for any damage that results from missing video information. To minimize the occurrence of lost digital information, Dahua recommends multiple, redundant recording systems, and adoption of backup procedure for all data.
- All trademarks, registered trademarks and the company names in the Guide 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.
- Contact the supplier or customer service if you encounter any issue while using this unit.

# Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the device, hazard prevention, and prevention of property damage. Read these contents carefully before using the device, comply with them when using, and keep it well for future reference.

## Installation and Maintenance Professionals Requirements

- All installation and maintenance professionals must have adequate qualifications or experiences to install and maintain CCTV systems and electric apparatus, and to work above the ground. The professionals must have the following knowledge and operation skills:
  - Basic knowledge and installation of CCTV systems.
  - Basic knowledge and operation skills of low voltage wiring and low voltage electronic circuit wire connection.
  - Basic knowledge and operation skills of electric apparatus installation and maintenance in hazardous sites.

## Power Requirements

- Install the unit in accordance with the manufacturer's instructions and in accordance with applicable local codes.
- All installation and operation must conform to your local electrical safety codes.
- Do not overload outlets and extension cords, which may cause fire or electrical shock.
- Do not place the camera near or in a place where the camera may contact overhead power lines, power circuits, or electrical lights.
- Ensure power conforms to SELV (Safety Extra Low Voltage) and that the limited power source is rated AC 24V as specified in IEC60950-1. (Power supply requirement is subject to the device label).
- All input/output ports are SELV circuits. Ensure that SELV circuits are connected only to other SELV circuits.
- Ground the unit using the ground connection of the power supply to protect the unit from damage, especially in damp environments.
- Please install easy-to-use device for power off before installing wiring, which is for emergent power off when necessary.
- Protect the plug and power cord from foot traffic, being pinched, and its exit from the unit.
- Do not attempt to service the unit. Opening or removing covers may expose you to dangerous voltage or other hazards. Refer all servicing to qualified personnel.
- If the unit is damaged and requires service, unplug the unit from the main AC power supply and from the PoE supply and refer to qualified service personnel. Damage may include, but is not limited to:
  - The power supply cord or plug is damaged.
  - Liquid has spilled in or on the unit.
  - An object has fallen on the unit.
  - The unit has been dropped and the housing is damaged.

- The unit displays a marked change in performance.
- The unit does not operate in the expected manner when the user correctly follows the proper operating procedures.
- Ensure a service technician uses replacement parts specified by the manufacturer, or that have the same characteristics as the original parts. Unauthorized parts may cause fire, electrical shock, or other hazards. Dahua is not liable for any damage or harm caused by unauthorized modifications or repairs.
- Perform safety checks after completion of service or repairs to the unit.
- Use attachments and accessories only specified by the manufacturer. Any change or modification of the equipment, not expressly approved by Dahua, could void the warranty.
- Incorporate a readily accessible disconnect device in the building installation wiring for quick power disconnect to the camera.
- Dahua assumes no liability or responsibility for any fire or electrical shock caused by improper handling or installation.

## Application Environment Requirements

- Please use the device within the allowed humidity (<95%RH) and altitude (<3000m).
- Transport, use, and store the unit within the specified temperature and humidity range.
- Do not place the unit in a wet, dusty, extremely hot or an extremely cold environment; and avoid environments with strong electromagnetic radiation or unstable lighting.
- Do not use the device in the corrosive environment such as high salt fog area (sea, beach and coastal area), acid gas environment and chemical plants.
- Do not use the device in applications with strong vibrations such as in boats and vehicles.
- Never push objects of any kind into this unit through openings as they may touch dangerous voltage points or cause a short circuit that may result in fire or electrical shock. Take care to not spill any liquid on the unit.
- If your installation environment is subjected to one of the conditions above, contact our sales staff to purchase cameras intended for the particular environment.
- Please don't install the device near the place with heat source, such as radiator, heater, stove or other heating equipment, which is to avoid fire.
- Do not aim the lens at an intense radiation source (such as the sun, a laser, and molten steel for example) to avoid damage to the thermal detector.
- Use the factory default package or material with equal quality to pack the device when transporting.

## Operation and Maintenance Requirements

- Do not touch the heat dissipation component of the unit. This part of the unit is hot and may cause a burn.
- Do not open or dismantle the device; there are no components that a user can fix or replace. Opening the unit may cause water leakage or expose components to direct light. Contact the manufacturer or a qualified service representative to service the camera or to replace a component, including the desiccant.
- Dahua recommends the use of a thunder-proof device in concert with the unit.
- Do not touch the CCD or the CMOS optic sensor. Use a blower to clean dust or dirt on the lens surface. Use a dry cloth dampened with alcohol and gently wipe away any dust on the lens.

- Use a dry soft cloth to clean the unit's housing. If the unit is particularly dusty, use water to dilute a mild detergent, apply the diluted detergent to a soft cloth, then gently clean the device. Finally, use a dry cloth to wipe the unit dry. Do not use a volatile solvent like alcohol, benzene, or thinner; or use a strong detergent with abrasives, which may damage the surface coating or reduce the working performance of the unit.
- Do not touch or wipe a dome cover during installation, this cover is an optical device. Refer to the following methods clean the dome cover:
  - Stained with dirt: Use an oil-free soft brush or blower to gently remove the dirt.
  - Stained with grease or fingerprints: Use a soft cloth to wipe gently the water droplet or the oil from the dome cover. Then, use an oil-free cotton cloth or paper soaked with alcohol or detergent to clean the lens from the center of the dome to outside. Change the cloth several times to ensure the dome cover is clean.



## WARNING

- Modify the default password after login.
- Use attachments and accessories only specified by the manufacturer. Any change or modification of the equipment, not expressly approved by Dahua, could void the warranty.
- Internal and external ground connection should be stable.
- Do not supply power via the Ethernet connection (PoE) when power is already supplied via the power connector.
- Disconnect power before device maintenance and overhaul. It is prohibited to open the cover with power on in an explosive environment.
- Please contact the local dealer or the nearest service center if the device fails to work normally, please don't dismantle or modify the device.

# Cybersecurity Recommendations

## Mandatory actions to be taken towards cybersecurity

- Change Passwords and Use Strong Passwords
  - The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.
- Update Firmware
  - As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

## Recommendations to improve your network security

- Change Passwords Regularly
  - The length should be greater than 8 characters;
  - Include at least two types of characters; character types include upper and lower case letters, numbers, and symbols;
  - Do not use an account name or the account name in reverse order;
  - Do not use sequential characters, such as 123, abc, etc.;
  - Do not use repeated characters, such as 111, aaa, etc.;
- Change Default HTTP and TCP Ports
  - Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
  - These ports can be changed to any set of numbers between 1025 and 65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.
- Update Firmware and Client Software
  - Keep your network-enabled equipment (such as NVRs, DVRs, IP cameras, 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.
  - Download and use the latest version of client software.
- Enable HTTPS/SSL
  - Set up an SSL Certificate and enable HTTPS to encrypt all communication between your devices and recorder.
- Enable IP Filter
  - Enable the IP filter to prevent unauthorized access to the system.

- Change ONVIF Password
  - Older IP camera firmware does not automatically change the ONVIF password when the system credentials are changed. Update the camera's firmware to the latest revision or manually change the ONVIF password.
- Forward Only Ports You Need
  - Forward only the HTTP and TCP ports that are required. Do not forward a wide range of numbers to the device. Do not DMZ the device's IP address.
  - Do not forward any ports for individual cameras if they are all connected to a recorder on site. Simply forward the NVR port.
- Disable Auto-Login on SmartPSS
  - Disable the Auto-Login feature on SmartPSS installed on a computer that is used by multiple people. Disabling auto-login prevents users without the appropriate credentials from accessing the system.
- Use a Different Username and Password for SmartPSS
  - Do not use a username/password combination that you have in use for other accounts, including social media, bank account, or email in case the account is compromised. Use a different username and password for your security system to make it difficult for an unauthorized user to gain access to the IP system.
- Limit Features of Guest Accounts
  - Ensure that each user has rights to features and functions they need to perform their job.
- Disable Unnecessary Services and Choose Secure Modes
  - Turn off specific services, such as SNMP, SMTP, and UPnP, to reduce network compromise from unused services.
  - It is recommended to 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 a mailbox server.
    - FTP: Choose SFTP and use strong passwords.
    - AP hotspot: Choose WPA2-PSK encryption mode and use strong passwords.
- Multicast
  - Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast. Deactivate this feature if not in use to enhance network security.
- Check the Log
  - The information stored in the network log file is limited due to the equipment's limited storage capacity. Enable the network log function to ensure that the critical logs are synchronized to the network log server if saving log files is required.
  - Check the system log if you suspect that someone has gained unauthorized access to the system. The system log shows the IP addresses used to login to the system and the devices accessed.
- Physically Lock Down the Device
  - Perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement access control permission and key management to prevent unauthorized personnel from accessing the equipment.

- Connect IP Cameras to the PoE Ports on the Back of an NVR
  - Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.
- Isolate NVR and IP Camera Network
  - Ensure that the network for the NVR and IP cameras should not be the same network as a public computer network. Separate networks prevent unauthorized users accessing the same network the security system.
- Secure Auditing
  - Check online users regularly to ensure unauthorized accounts are not logged in to a device.
  - Check the equipment log to access the IP addresses used to login to devices and their key operations.

# Table of Contents

<b>Foreword</b> .....	<b>I</b>
<b>Important Safeguards and Warnings</b> .....	<b>III</b>
<b>Cybersecurity Recommendations</b> .....	<b>VI</b>
<b>Table of Contents</b> .....	<b>IX</b>
<b>1 Overview</b> .....	<b>1</b>
<b>2 VTH Panels</b> .....	<b>2</b>
2.1 DHI-VTH1550CH-S / DHI-VTH1550CHW-2-S .....	2
2.2 DHI-VTH5221D-S / DHI-VTH5221DW-S.....	4
<b>3 Installation</b> .....	<b>6</b>
3.1 Planning the Install.....	6
3.2 Inspecting the Device.....	6
3.3 Installing the VTH Device.....	7
3.3.1 Surface Installation .....	7
<b>4 Commissioning</b> .....	<b>8</b>
4.1 Setup .....	8
4.2 Setting VTH Parameters .....	8
4.2.1 Initialize the VTH.....	8
4.2.2 Set VTH Network .....	9
4.2.3 Configure the VTH .....	11
4.2.4 Configure SIP Server.....	12
4.2.5 Add VTO Stations .....	13
4.3 Verify VTH Operation .....	13
4.3.1 Answering a Call from a VTO .....	13
4.3.2 Monitoring a VTO Station .....	14
<b>5 VTH Interface</b> .....	<b>15</b>
5.1 Main Menu .....	15
5.2 Setting VTH Functions .....	16
5.2.1 Setting Ring Tones.....	16
5.2.2 Setting Do Not Disturb.....	17
5.2.3 Setting Alarms.....	18
5.2.4 Mode Setting.....	21
5.2.5 Setting Call Forwarding .....	21
5.2.6 General Settings .....	22
5.2.7 Product Info .....	26
5.2.8 Resetting the Password.....	26
5.2.9 Making and Receiving Calls .....	27
<b>6 Monitoring Locations</b> .....	<b>31</b>
6.1 Monitoring Video from a VTO Station .....	31
6.2 Monitoring a Remote Camera.....	32
6.2.1 Adding a Camera .....	32
6.2.2 Modifying Camera Parameters.....	34

6.2.3 Deleting Cameras .....	34
6.2.4 Monitoring Video from a Connected Device.....	34
6.3 Selecting Favorites .....	35
6.4 VTH Information.....	36
6.4.1 Reviewing Security Alarms.....	36
6.4.2 Reviewing Guest Messages.....	37
6.4.3 Reviewing Published Information.....	37
6.4.4 Viewing Stored Video .....	37
6.5 Arm/Disarm Function .....	38
6.5.1 Arming an Alarm .....	38
6.5.2 Disarming an Alarm .....	38
<b>7 DSS Mobile.....</b>	<b>40</b>
7.1 Downloading the App.....	40
7.2 Registering the App.....	41
7.3 Call Functions .....	43
7.3.1 Configuring Call Forwarding.....	43
7.3.2 Calling Operations .....	44
7.4 Monitoring Video from a VTO .....	45
7.5 Call Records.....	46
7.6 Settings .....	47
7.7 Messages.....	47

# 1 Overview

Dahua VTH devices are indoor monitors that allow tenants to view and talk with visitors, record call sessions, monitor the surroundings from outdoor stations and IP cameras and remotely unlock doors. Visitors can also leave messages, which can be retrieved from the indoor monitor. The VTH series is used as part of a video intercom solution with compatible outdoor stations.

VTH series products are digital video intercom home stations that integrate monitoring, two-way communication, and door management. The VTH devices use an IP network, SNMP (Simple Network Management Protocol) technology, and network encryption technology to achieve a stable system, robust functionality, convenient operation, and safer data transmission.

# 2 VTH Panels

Use this process to plan, install, and configure the security network and the IP devices.

## 2.1 DHI-VTH1550CH-S / DHI-VTH1550CHW-2-S

The DHI-VTH1550CH-S indoor monitor allows tenants to view and talk with visitors, record call sessions, monitor the surroundings from outdoor stations and IP cameras, and remotely unlock doors. Visitors can also leave messages, which can be retrieved from the indoor monitor. The DHI-VTH1550CH-S indoor monitor is used as part of a video intercom solution with compatible outdoor stations.

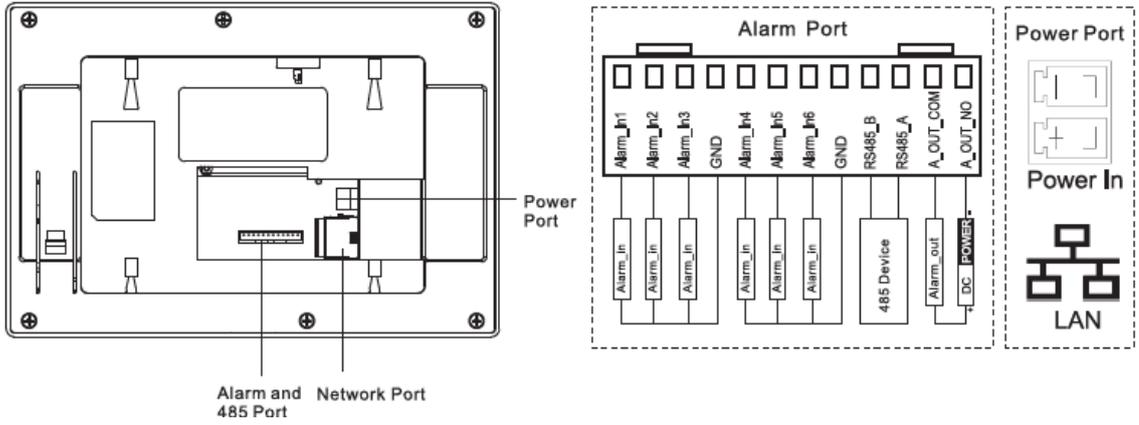
### Front Panel



Icon	Name	Description
	SOS	Calls the central station in case of emergency.
	Menu	Returns to the main menu.
	Call	<ul style="list-style-type: none"><li>• Press to answer an incoming call.</li><li>• Press to hang-up an active call.</li><li>• Press to speak to another intercom device in the same complex or to a fence station.</li></ul>
	Monitor	<ul style="list-style-type: none"><li>• Standby mode: press to monitor the main VTO.</li><li>• Monitoring Mode: press to exit monitoring.</li></ul>
	Unlock	Press to unlock this key during calling, talking, monitoring and speaking of VTO, so corresponding VTO will be unlocked.

Table 2-1: DHI-VTH1550CH-S Front Panel Keys

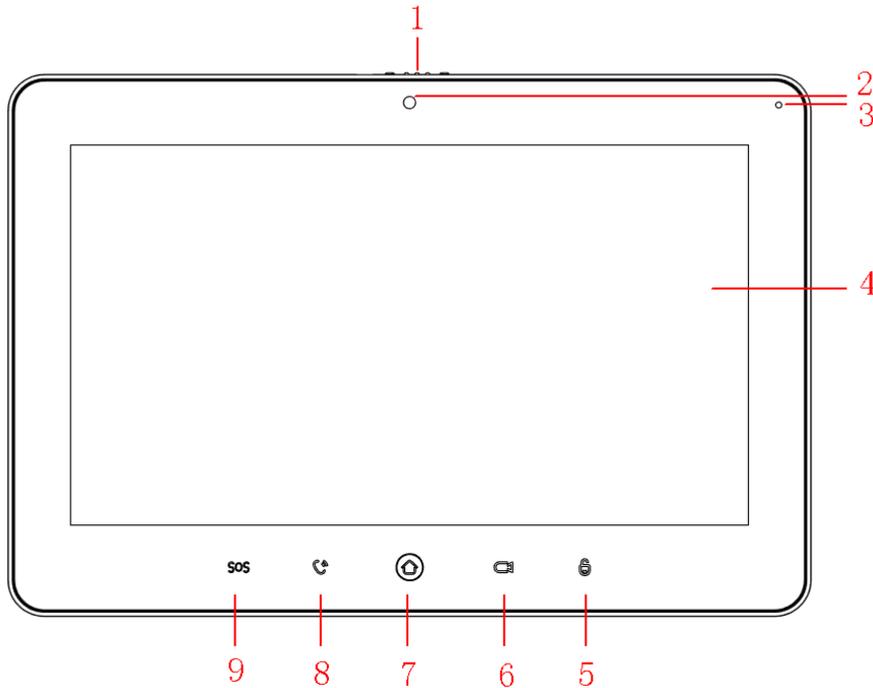
# Rear Panel



## 2.2 DHI-VTH5221D-S / DHI-VTH5221DW-S

The DHI-VTH5221-S Series indoor monitors allow tenants to view and talk with visitors, record call sessions, monitor the surroundings from outdoor stations and IP cameras and remotely unlock doors. Visitors can also leave messages, which can be retrieved from the indoor monitor. The DHI-VTH5221-S Series indoor monitors are used as part of a video intercom solution with compatible outdoor stations.

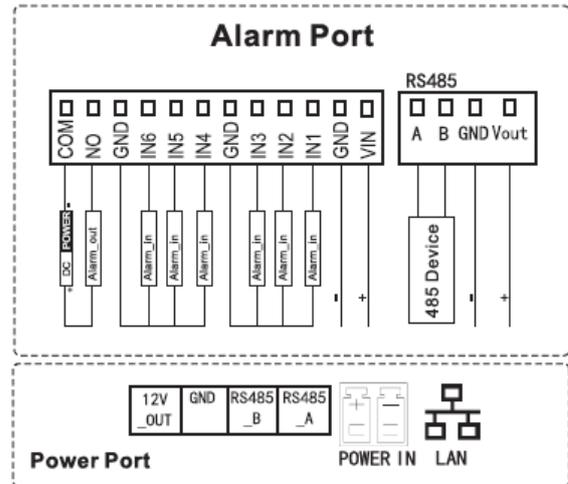
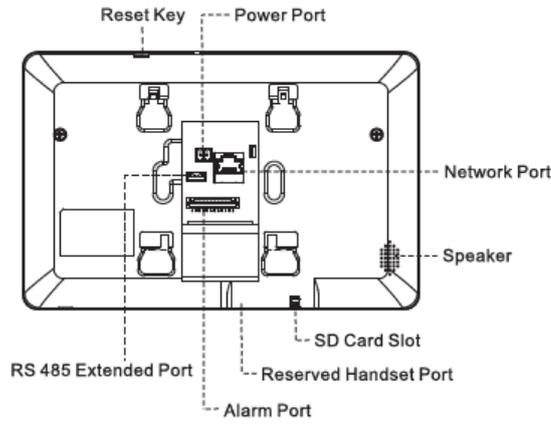
### Front Panel



No.	Name	Description
1,2	Camera	The VTH5221D series does not have a camera.
3	Microphone	Voice input.
4	Display Screen	7-in. TFT Capacitive Touch Screen
5	Unlock	Unlocks the connected VTO calling, talking, monitoring, and talking.
6	Monitor	<ul style="list-style-type: none"> <li>Standby mode: press to monitor the main VTO.</li> <li>Monitoring Mode: press to exit monitoring.</li> </ul>
7	Menu	Returns to the Main Menu.
8	Call	<ul style="list-style-type: none"> <li>Press to answer an incoming call.</li> <li>Press to hang-up an active call or to exit speaking.</li> <li>Press to speak to another intercom device in the same complex or to a fence station.</li> </ul>
9	SOS	Calls the central station in case of emergency.

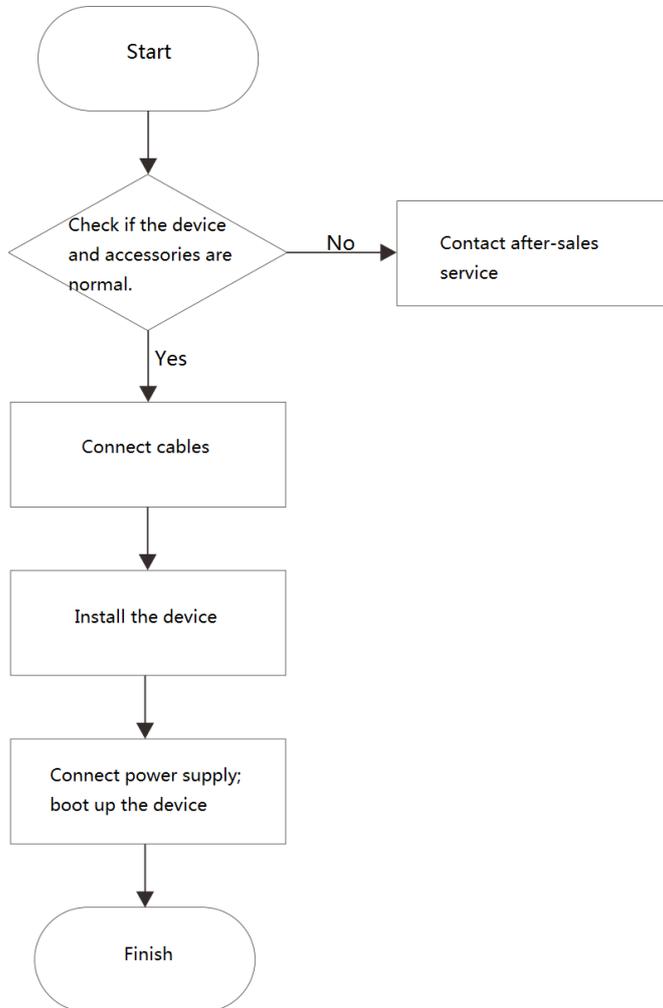
Table 2-2: DHI-VTH5221D-S / DHI-VTH5221DW-S Front Panel Keys

# Rear Panel



# 3 Installation

## 3.1 Planning the Install



## 3.2 Inspecting the Device

Sequence	Item	Content	
1	Overall package	Appearance	Check for obvious damage and check that the fittings and hardware are complete.
		Package	
		Fittings	
2	Model and Label	Device Model	Inspect whether it is consistent with order contract.
		Label on the device	Inspect whether the label is torn or damaged. Do not discard the label. The warranty is voided if the label is not present.
3	Device	Appearance	Check for any damage and loose fittings.

Table 3-1: Device Inspection

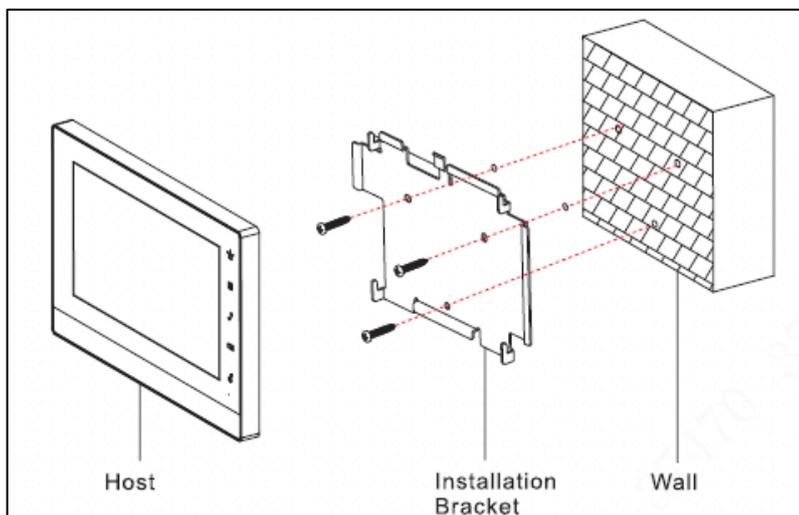
## 3.3 Installing the VTH Device

- Install the device in an appropriate location. Avoid locations that experience condensation, high temperatures, dust, corrosives, and direct sunlight.
- Installation and commissioning shall be performed by professional integrators trained on the latest security devices.
- DO NOT dismantle or repair the device. Contact your local Dahua representative in case of a faulty device.
- The suggested installation height of central point of the device central point is 1.4 cm to 1.6 cm (0.55 in. to 0.63 in.) above the ground.

### 3.3.1 Surface Installation

Install the device with a bracket directly onto a wall.

1. Drill holes in the wall using the bracket as a guide to mark the hole positions.
2. Secure the bracket to the wall with screws.
3. Slide the VTH device onto the bracket from the top and slide down.



# 4 Commissioning

Confirm that all devices are complete and that they work properly prior to installation and configuration.

## 4.1 Setup

Prior to commissioning and configuring the VTH unit, ensure the unit conforms to the following:

- Check that the unit is connected to the proper power supply. Power on the device only after the circuit is confirmed to be normal.
- Plan the list of IP Addresses and the ID numbers for each VTO and VTH unit.
- Check the deployment position of SIP server.
- Install and configure the VTO SIP system before commissioning and configuring a VTH device. Refer to the VTO User Manual for instructions on installing and configuring VTO devices.
- Use the VTO Web interface to set VTO and VTH information. Then set the VTH and VTO information at each VTH device.

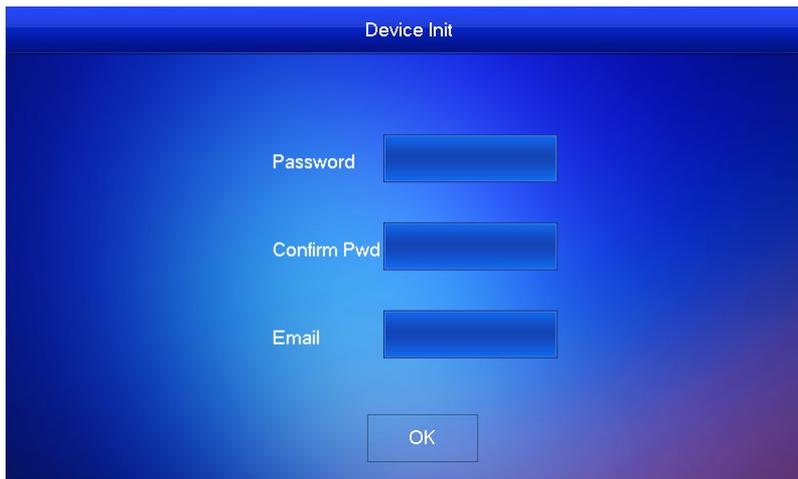
## 4.2 Setting VTH Parameters

### 4.2.1 Initialize the VTH

You must supply the following information before configuring the VTH:

- Password
  - Email address (used to retrieve password)
1. Power on the device.

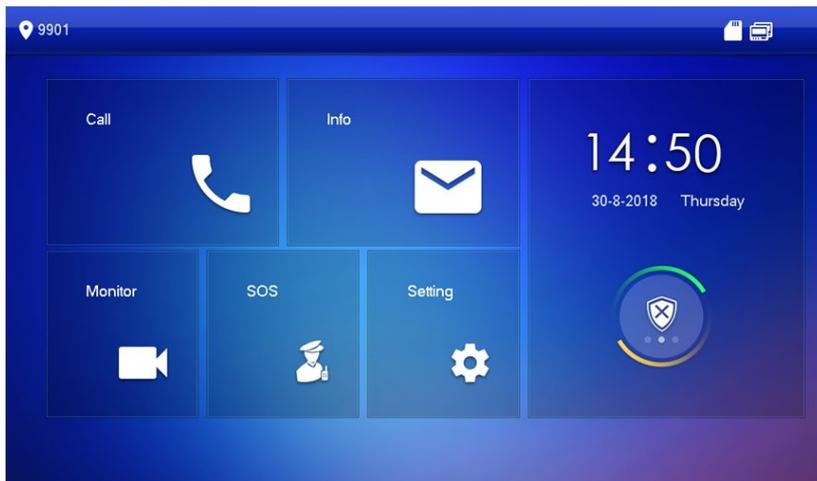
The system displays the Device Initialization interface.



The screenshot shows a web-based interface titled "Device Init" with a blue gradient background. It contains three input fields: "Password", "Confirm Pwd", and "Email". Below these fields is an "OK" button.

2. Type your Password, then type the same password in Confirm Pwd box.
3. Type a valid email address.
4. Press OK.

The system displays main interface if all credentials are input successfully.



## 4.2.2 Set VTH Network

Configure the VTH network information. The VTH must be part of the same network segment as the VTO and the other VTH devices in the system.

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press [OK].
3. Press Network.

The system displays the Network interface. Note, only devices with wireless functionality can access a WLAN.

4. Set the Network credentials according to the type of network: LAN or WLAN.

- LAN



- a) Enter the following addresses: Local IP, Subnet Mask, and Gateway.  
Press Off to enable DHCP functionality and to obtain an IP address automatically.
- b) Press OK.

- WLAN

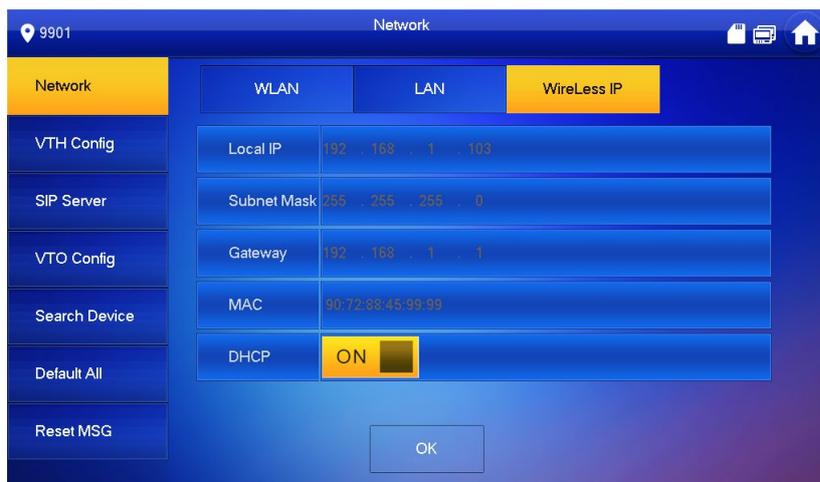
a) Press Off to enable the WiFi Function.

The system list the available WiFi networks.



b) Connect to a WiFi network in one of the following ways:

- Select Wi-Fi, then press the Wireless IP tab. Enter the Local IP, Subnet Mask and, Gateway addresses. Then [OK].
- Select Wi-Fi, then press the Wireless IP tab. Press OFF to enable DHCP functionality and to obtain an IP address automatically. To obtain IP info with DHCP function, use a router with DHCP function.



### 4.2.3 Configure the VTH

Follow these steps to set VTH room number, type and, Master IP address. VTH devices can be configured as a master unit or as an extension unit. Typically, there is one master unit and each master can support several extension units. A master unit uses a four-digit room number.

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Press VTH Config.



The screenshot shows the 'VTH Config' screen on a device. The top bar displays '9901' and 'VTH Config'. A left sidebar contains menu items: Network, VTH Config (highlighted), SIP Server, VTO Config, Search Device, Default All, and Reset MSG. The main area contains a form with the following fields:

Room No.	9901	Master
Master IP	0 . 0 . 0 . 0	
Master Name	admin	
Master Pwd	*****	
Version	V4.000.0000000.2.R.20180825	
SSH	<input type="checkbox"/> OFF	

An 'OK' button is located at the bottom center of the screen.

4. Set the VTH information based on the type of VTH device: Master or Extension.
  - Set a Master VTH:
    - a) Enter "Room No." and press OK to save.

This number must be the same number as the "VTH Short No." set when adding the VTH device at the WEB interface.
  - Set an Extension VTH:
    - a) Press Master to switch the unit to Extension mode.
    - b) Enter the "Room No." and the Master IP (IP address of master VTH).
    - c) Enter the Master Name and the Master Password.

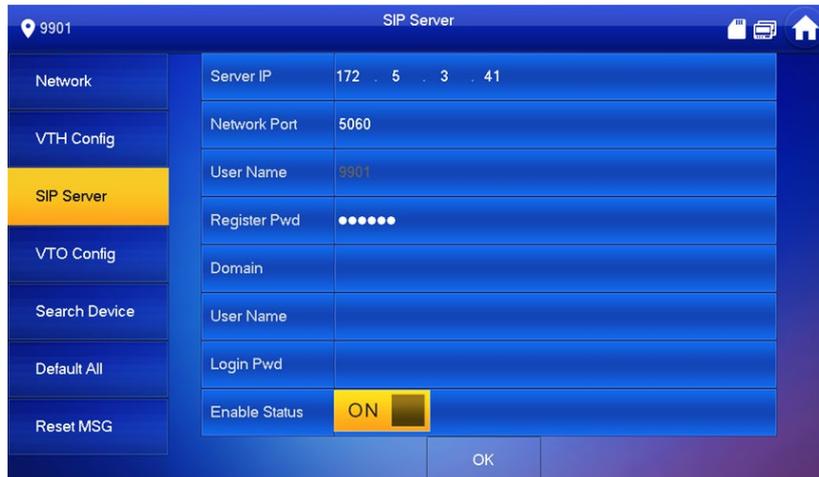
"Master Name" and "Master Pwd" are the user name and password for the master VTH. Default user name is admin, and the password is the one set during device initialization.

5. Press OFF to enable SSH (optional). After SSH is enabled, the debugging terminal connects VTH through SSH protocol, so as to operate and debug it.
6. Press OK to save the configuration.

## 4.2.4 Configure SIP Server

Configure SIP server on VTH and build connections.

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Press SIP Server.



4. Set the parameters for the SIP server using the following information.

Parameter	Description
Server IP	This IP Address is either: <ul style="list-style-type: none"> <li>• the IP Address of the separate SIP server.</li> <li>• the IP address of the VTO, if the VTO is acting as the SIP server.</li> </ul>
Network Port	Standalone SIP server: network port is 5080. VTO as SIP server: network port is 5060.
User Name	Use default value.
Register Pwd	
Domain	Registration domain of the SIP server. This value can be left blank. If the VTO is the SIP server, use VDP as the domain
User Name	User name and password to login to the SIP server.
Login Pwd	

Table 4-1: SIP Server Parameters

5. Set Enable Status to ON to activate SIP Server functions.
6. Press OK to save SIP server configuration.

## 4.2.5 Add VTO Stations

VTO stations are the external devices that VTH units connect to for two-way communication. VTO stations typically contain a camera to send video information and can unlock doors and gates from a command from VTH devices.

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Press VTO Config.



4. Add a main VTO or a VTO sub-station:
  - Add Main VTO
    - a) Enter the Main VTO Name, the VTO IP Address, User Name, and Password.
    - b) Switch the Enable Status to ON.
  - Add a VTO sub-station:
    - a) Enter Sub VTO/Fence Station Name, Sub VTO/Fence Station IP address, User Name and Password.
    - b) Switch the Enable Status to ON.
    - c) Press the Left or Right Arrow to add additional VTO sub-stations.

## 4.3 Verify VTH Operation

### 4.3.1 Answering a Call from a VTO

To verify that a VTH unit is configured properly, make a test call from a VTO unit.

- Dial the VTH room number from the VTO unit.  
The VTH unit displays the video feed and the operating keys from the VTO if all settings are configured properly.

Note in the image below that the Snapshot and Record keys are active. These active functions indicate that the VTH has an SD card inserted in the unit.



### 4.3.2 Monitoring a VTO Station

- Select Monitor > Door, and then select the VTO you wish to monitor. Press the Star icon to add this VTO to the Favorite List.



# 5 VTH Interface

## 5.1 Main Menu

All interaction with the VTH features starts from the Menu.



No.	Name	Description
1	Room Number	Number of the room where the VTH is located.
2	Call	<ul style="list-style-type: none"> <li>• Call another VTH or a VTO unit.</li> <li>• Manage contacts.</li> <li>• View and manage call records.</li> </ul>
3	Info	<ul style="list-style-type: none"> <li>• View, delete, and clear notices issued by Property Management Center.</li> <li>• View, delete and clear security alarm information.</li> <li>• View, delete, and clear VTO messages (if VTH does not have an SD card installed or the VTO enables the video-audio message upload function).</li> <li>• View, delete, and clear videos and pictures (if VTH has an SD installed).</li> </ul>
4	Status Bar	<ul style="list-style-type: none"> <li>• : VTH not connected to a wired network</li> <li>• : VTH is connected to wired network</li> <li>• : VTH connected to a WiFi network</li> <li>• : VTH is not connected to the Master VTO</li> <li>• : SD card installed in the VTH</li> <li>• : Do Not Disturb is active for the VTH.</li> </ul>
5	Time	Displays the current date, day of the week, and time.

No.	Name	Description
6	Arm/disarm	<ul style="list-style-type: none"> <li>Displays the last unread alarm message.</li> <li>Press the icon to enter arming mode.</li> </ul>
7	Setting	Press here to access the VTH settings. Press and hold until the Password Verification dialog box opens.
8	SOS	Calls the Management Center.
9	Monitor	Monitor the Master VTO, VTO sub-station, IP camera, and other connected devices.

Table 5-1: VTH Main Menu Selections

## 5.2 Setting VTH Functions

### 5.2.1 Setting Ring Tones

The VTH allows you to set the ring tone incoming calls from the VTO, another VTH, alarms, and other communications. Setting custom ring tones helps to identify the source of the incoming call or alert.

You can upload custom ring tones into the VTH via an SD card. Follow these guidelines to import tones:

- Ring tones must be stored on the SD card in this directory path: `/mnt/sd/Ring/`.
- The audio file must be an .mp3 file. You cannot simply change the extension of another audio file, the file must be encoded as an MP3.
- Audio file size must be less than 100kB.
- Ring tone format: 16K, 16BIT, or .mp3.
- You can add 10 ring tones.

#### 5.2.1.1 Setting a Ring Tone

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Press Ring. Then press VTO Ring Setup, VTH Ring Setup, or Alarm Ring Setup.

The system displays the corresponding interface. Press the Left or the Right arrow button to page through the available ring tones.



4. Press the tone name box to select the ring tone, then press the “+” or the “-” button to set the volume.

### 5.2.1.2 Setting Ring Tone Preferences

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Select “Ring > Other”.



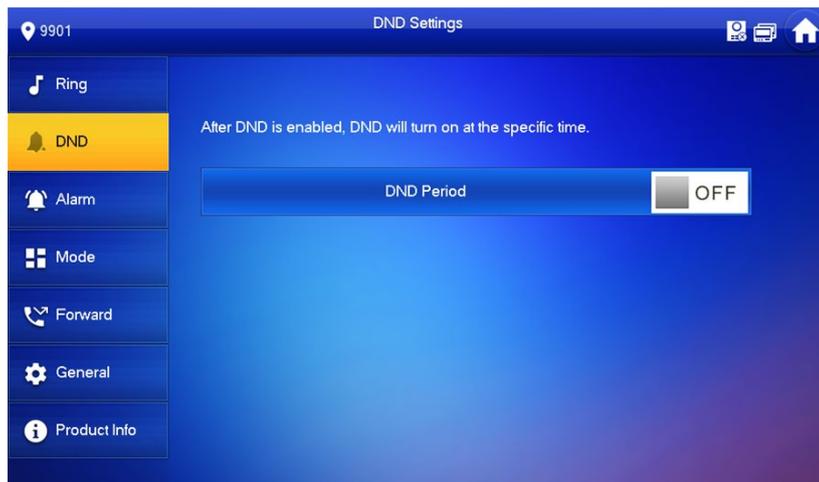
4. Set the following parameters:
  - VTO Ring Time: Amount of time, in seconds, that the unit plays the ring tone from an incoming call from a VTO unit.
  - VTH Ring Time: Amount of time, in seconds, that the unit plays the ring tone from an incoming call from another VTH unit.
  - MIC Volume: Use the “+” or “-” buttons to set the outgoing voice volume.
  - Talk Volume: Use the “+” or “-” buttons to set the speaker volume.
5. Press the OFF button to mute all ring tones. Press the button again to activate all ring tones.

### 5.2.2 Setting Do Not Disturb

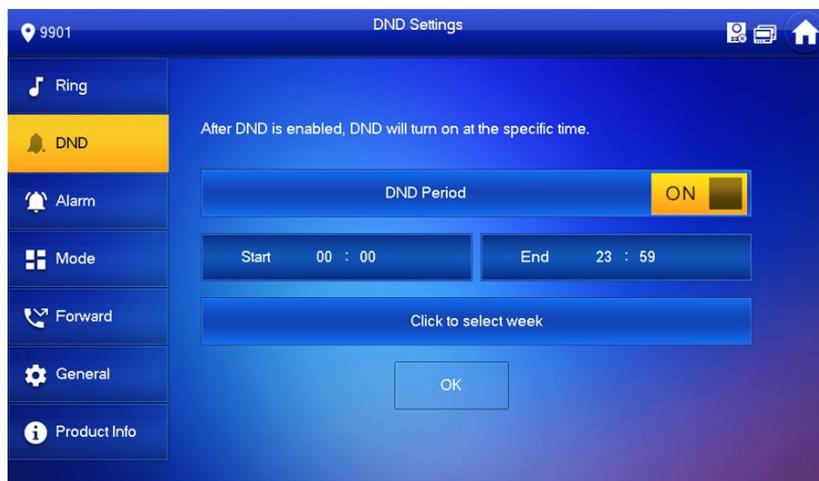
Use this setting to silence incoming calls during a specified time period. Note the following about the Do Not Disturb (DND) function:

- DND function is off by default.
- In DND mode, the VTH does not save a call reminder, but it does record the call information.
- DND parameters are set only at the Master VTH. The Master VTH synchronizes the settings with Extension VTH units.

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Press DND.



4. Press OFF to activate the Do Not Disturb function.



5. Press the Start box and enter the start time to activate Do Not Disturb.
6. Press the End box and enter the time the VTH disables Do Not Disturb.
7. Press Click to select week and select the days of the week when the Start and End times are active.
8. Press OK to save settings.

### 5.2.3 Setting Alarms

The VTH allows you to configure the types of alarms, status, and the actions of an incoming alarm.

### 5.2.3.1 Configuring Wired Alarm Zones

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Select Alarm > Wire Zone.



4. Press a corresponding position to set area type, NO/NC, alarm status, enter delay, and exit delay.

Parameter	Description
Area	Alarm identifier, cannot be modified.
Type	Select the type of the alarm according to the detector type: IR, gas or smoke detector; emergency call button, door alarm, burglar alarm, perimeter, or doorbell.
NO/NC	Select Normally Open (NO) or Normally Closed (NC) according to the detector type.
Status	Select one of the following options: <ul style="list-style-type: none"> <li>Instant Alarm: Sounds a tone immediately when an alarm is triggered and enters alarm status mode.</li> <li>Delay Alarm: Sounds a tone and enters alarm mode after a specified delay time. You can disarm and cancel the alarm during the delay period.</li> <li>Bypass: Area is not armed.</li> <li>Remove: Area is invalid during arm/disarm. Status cannot be bypassed.</li> </ul>
Enter Delay	After entering delay, when armed area triggers an alarm, entering armed area from non-armed area within the delay time period will not lead to linkage alarm. Linkage alarm will be produced if delay time comes to an end and it is not disarmed.
Exit Delay	After arm, "delay alarm" area will enter arm status at the end of "exit delay". If multiple areas set the exit delay, interface prompt will conform to maximum delay time.

Table 5-2: Alarm Zone Parameters

5. Press OK to save the settings.

### 5.2.3.2 Configuring Wireless Alarm Zones

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Select Alarm > Wireless Zone.

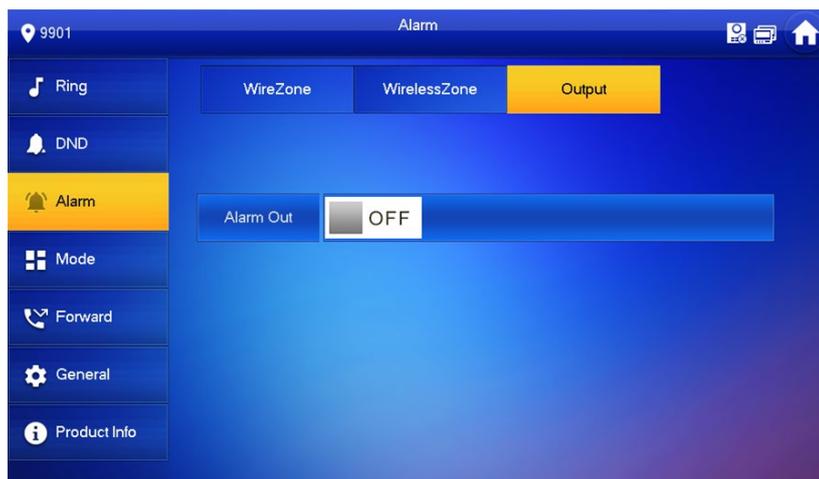


4. Press Add.
5. Press the wireless code button on the wireless device. Please refer to the documentation for the wireless device for instructions.
6. Press a corresponding position to set alarm status, enter delay, and exit delay. Refer to Table 5-2: Alarm Zone Parameters for details.
7. Press Edit to select a zone and press Delete to delete the selected area.

### 5.2.3.3 Configuring Alarm Output

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

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Select Alarm > Output.



4. Press OFF to enable alarm output function.

## 5.2.4 Mode Setting

Set area on/off status under different modes. Area mode can be set only in disarm status.

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Press Mode.

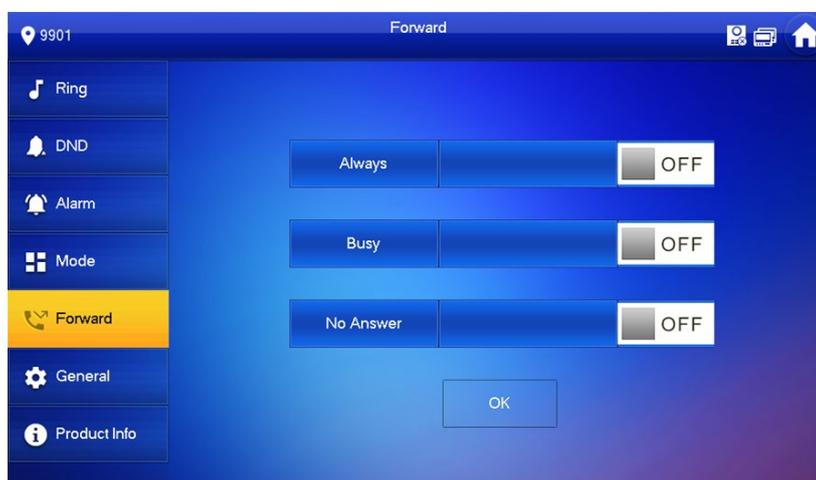


4. Select the arm mode in every tab.
5. Press OFF in every area to add it into arm mode. Multiple areas can be added into one arm mode simultaneously, whereas one area can be added into different modes.

## 5.2.5 Setting Call Forwarding

The VTH allows you to forward incoming calls to another VTH device. Call forwarding is configured only on the Master VTH, and the Master VTH synchronizes the setting to its Extension VTH devices.

- To forward a call to a VTH device in another building or unit on the same system, you must format the call forwarding number as: Building Number + Unit Number + VTH Room Number. For example, input "0101101" Builder 1, Unit 1, Room 101.
  - To forward a call to a VTH in the same unit, simply use the VTH Room Number.
1. Press and hold Setting until the system displays the Password Verification dialog box.
  2. Type your password and press OK.
  3. Press Forward.



- Input the VTH number in the corresponding forward mode; then press OFF to enable the forward function.

Parameter	Description
Always	All incoming calls will be forwarded to preset number.
Busy	When the user is busy, incoming call from the third party is forwarded to the preset number. If “No Answer” is not set, when the user refuses to answer, the incoming call will be deemed as busy forwarding.
No Answer	If no one answers after VTH ring time, the incoming call is forwarded to the preset number.

Table 5-3: Call Forwarding Options

- Press OK to save settings.

## 5.2.6 General Settings

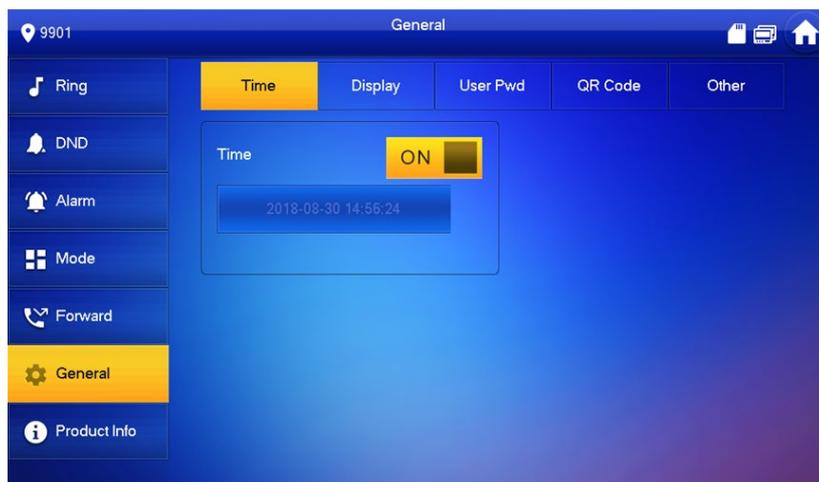
Set VTH time, display, password, and other parameters. .

### 5.2.6.1 Setting Time

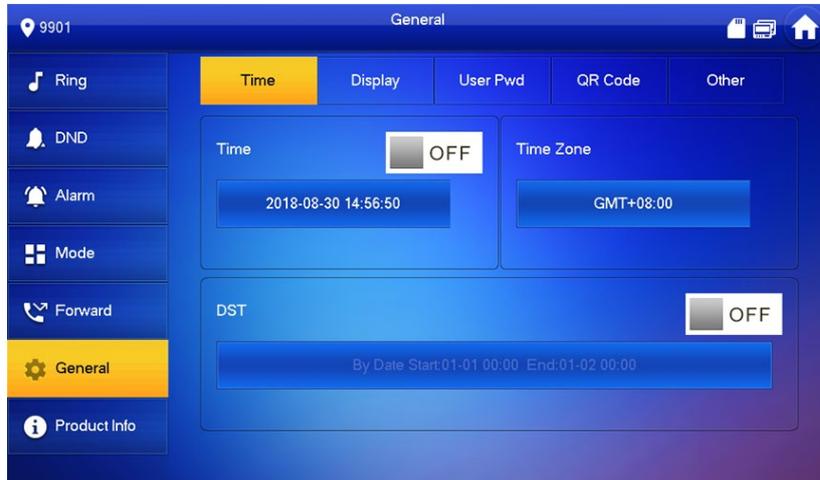
Set the VTH system time, time zone, and daylight savings time (DST).

These parameters are set only on the Master VTH, and the Master VTH synchronizes the settings to its Extension VTH devices.

- Press and hold Setting until the system displays the Password Verification dialog box.
- Type your password and press OK.
- Select General > Time.



4. Set the time parameter.
  - Manual system time:
    - a) Press ON.
    - b) Press time text box to set system time.
  - Set time zone:
    - a) Press ON.
    - b) Press the Time Zone text box and select the local time zone.

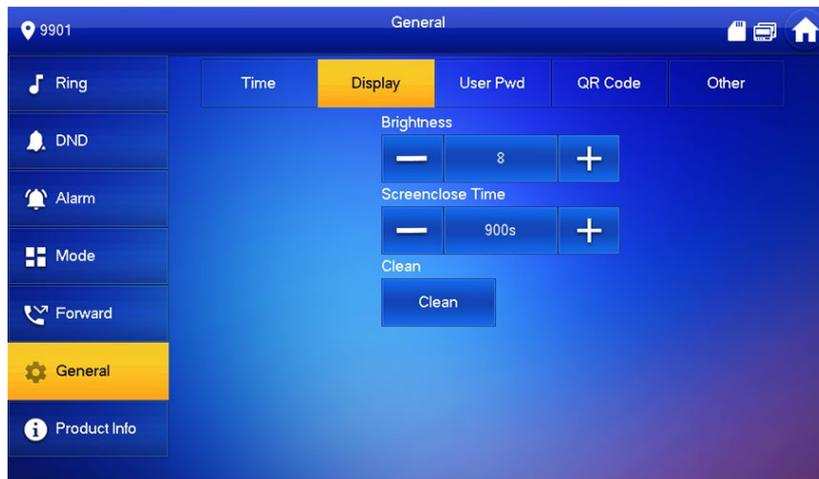


- Set DST:
  - a) Press OFF in the DST box to enable DST.
  - b) Press DST text box and select DST start time and end time.

### 5.2.6.2 Display Setting

Set VTH screen brightness, screensaver time, and clean time.

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Select General > Display.



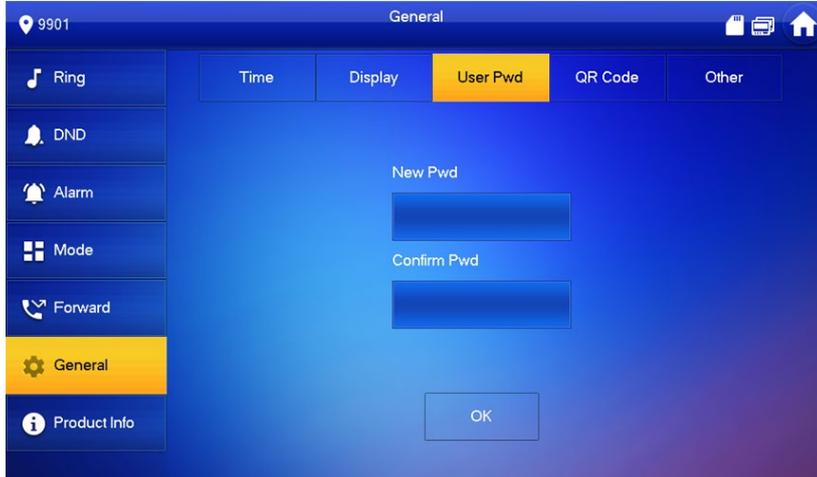
4. Set parameters.
  - a) Press the "+" or the "-" to set the Brightness and Screensaver Time.
  - a) Press Clean to lock the screen for 10 seconds in order to clean the touchscreen.

### 5.2.6.3 Setting the Password

Use this dialog box to set the login password.

These parameters are set only on the Master VTH, and the Master VTH synchronizes the settings to its Extension VTH devices.

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Select General > User Password.



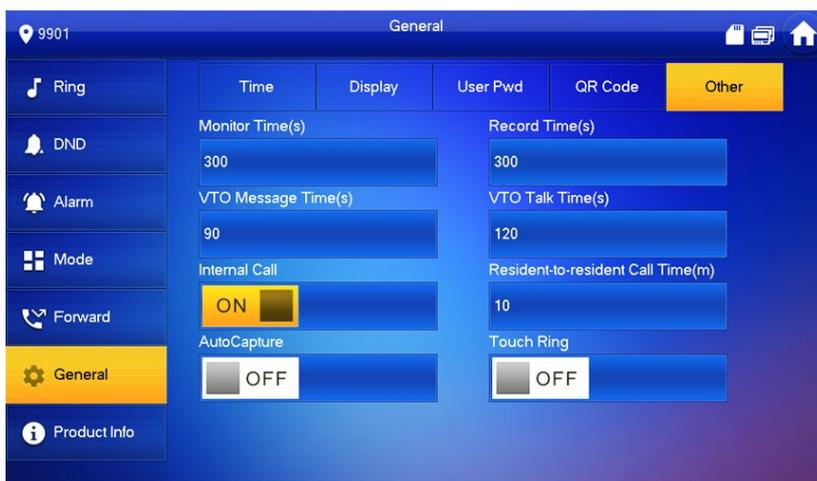
4. Type a New Password and confirm the password in the Confirm Pwd box.
5. Press OK to complete password modification.

### 5.2.6.4 Configuring Other Settings

Set monitor time, record time, VTO message time, VTO talk time, resident-to-resident call enable, resident-to-resident call time, auto capture and touch ring.

You can set Auto Capture and Touch Ring at both Master and Extension VTH devices, other parameters are set only on the Master VTH and then synchronizes with its Extension VTH devices.

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Select General > Other.



4. Set the following parameters:

Parameter	Description
Monitor Time	Maximum time to monitor the video from a VTO, VTO sub-station, IP camera or another device.
Record Time	Maximum recording time of videos during call, talk, monitoring, and speaking. The system stops recording at the end of recording time.
VTO Message Time	<ul style="list-style-type: none"> <li>• When VTO message time is not 0:</li> <li>• If VTH with SD card doesn't answer when VTO calls, enter message status according to prompt, and save the message in SD card of VTH.</li> <li>• If VTH doesn't have SD card, but VTO has enabled "Leave Message Upload" and set FTP server, "Message" tab will appear at VTH info interface. If VTH doesn't answer when VTO calls, enter message status according to prompt, and upload the message to FTP server.</li> <li>• If VTH doesn't have SD card, and VTO has not enabled "Leave Message Upload", if VTH doesn't answer when VTO calls, hang up automatically.</li> <li>• When VTO message time is 0:</li> <li>• Hang up automatically if VTH doesn't answer when VTO calls, no matter whether VTH has SD card or not, no matter whether VTO has enabled "Leave Message Upload" or not.</li> </ul> <p>If VTO sets to forward the call to management center, if VTH doesn't answer when VTO calls, and there is no message prompt, the call will be forwarded to management center.</p>
Resident-to-resident Call Time	Maximum talk time between VTH and another VTH.
VTO Talk Time	Maximum talk time when a VTO calls a VTH.
Resident-to-resident Call Enable	<p>After resident-to-resident call is enabled, VTH can call another VTH.</p> <p>The called party enables internal call, to realize this function.</p>
Auto Capture	<p>After auto capture is enabled, 3 pictures will be captured automatically when VTO calls VTH. View them at "Info &gt; Record and Picture" interface.</p> <p>This function is valid only when SD card is inserted.</p>
Touch Ring	After enabling touch ring, there will be a ring when touching the screen.

Table 5-4: Other VTH Setting Parameters

## 5.2.7 Product Info

This box lets you reboot the system and format the SD card, if installed.

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Press Product Info.



4. Press Reboot and press OK at the prompt to reboot the VTH.
5. Press SD Format and press OK at the prompt to format the SD card.

## 5.2.8 Resetting the Password

1. Press and hold Setting until the system displays the Password Verification dialog box.
2. Type your password and press OK.
3. Press Forget Password.



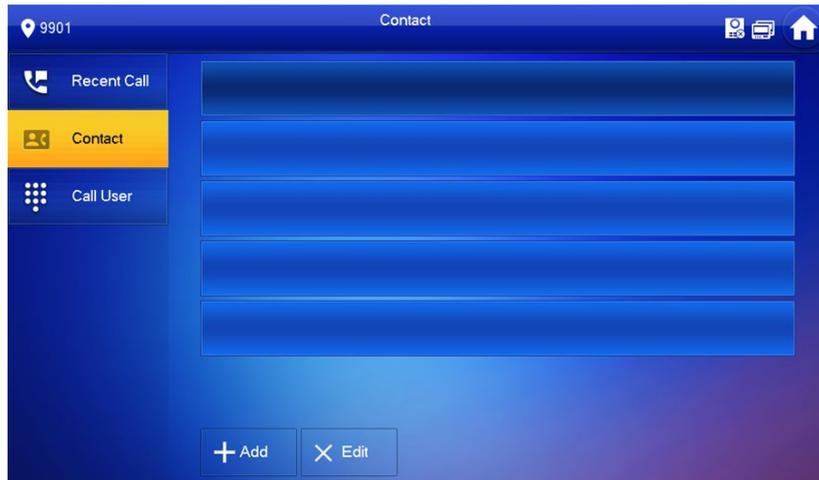
4. Scan the QR code with any code-scanning APP, bind your email box, send it by email to support\_cpwd@htmicrochip.com, and thus obtain security code.
5. Press Next.
6. Enter “Password”, “Confirm Password” and obtained “Security Code”.
7. Press OK to reset the password.

## 5.2.9 Making and Receiving Calls

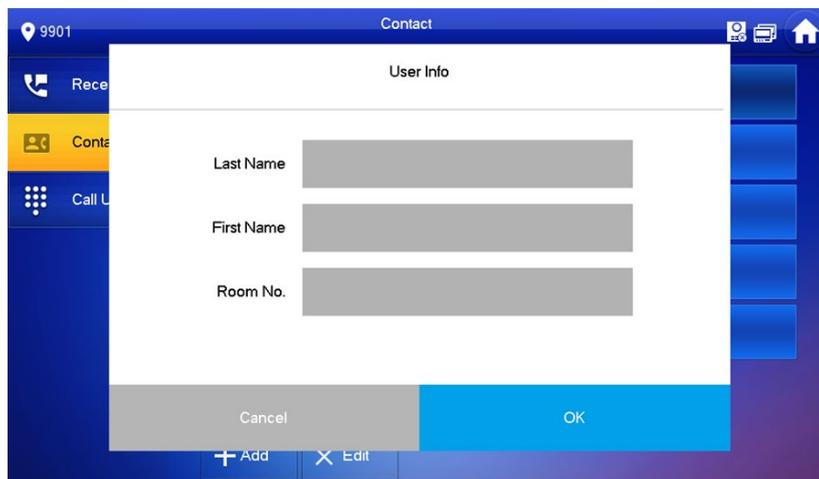
### 5.2.9.1 Adding Contacts

Add and edit VTH and extension number.

1. Select Call > Contact.



2. Press Add.



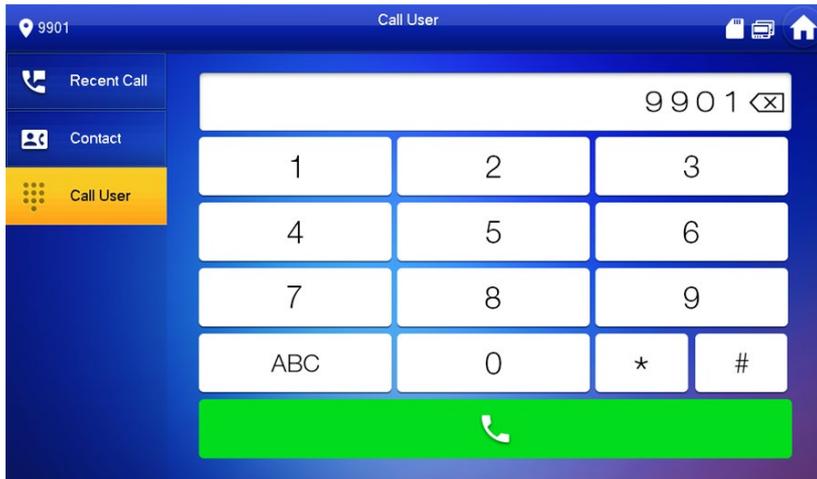
3. Enter the Last Name, First Name, and the Room Number of the contact person.
4. Press OK to add the contact.

5. To edit a contact, select the contact and press .
6. To delete a contact, press Edit and select the contact. Then press Delete to remove the contact. Multiple contacts can be selected and deleted at one time.
7. To place a call to a contact:
  - a) Select “Call > Contact” and select the contact.
  - b) Press  to place the call.

### 5.2.9.2 Calling Other VTH Units

Make sure that resident-to-resident call function has been enabled. If both VTHs have a camera, bilateral video call can be provided.

1. Select Call > Call User.

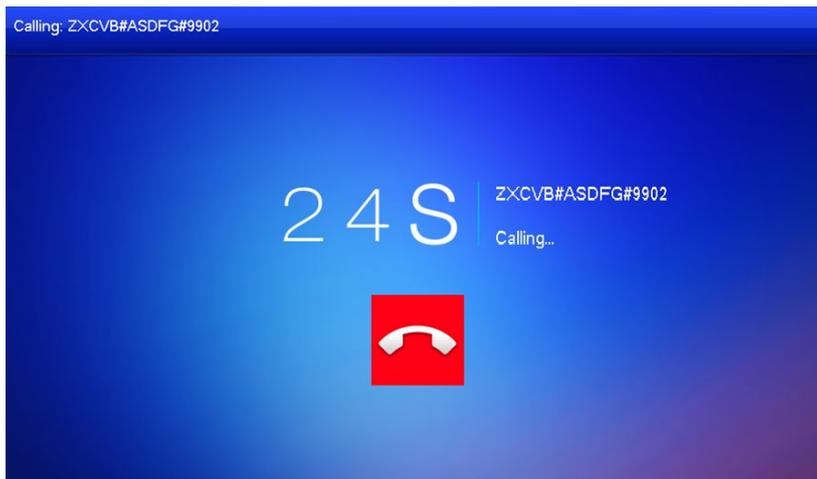


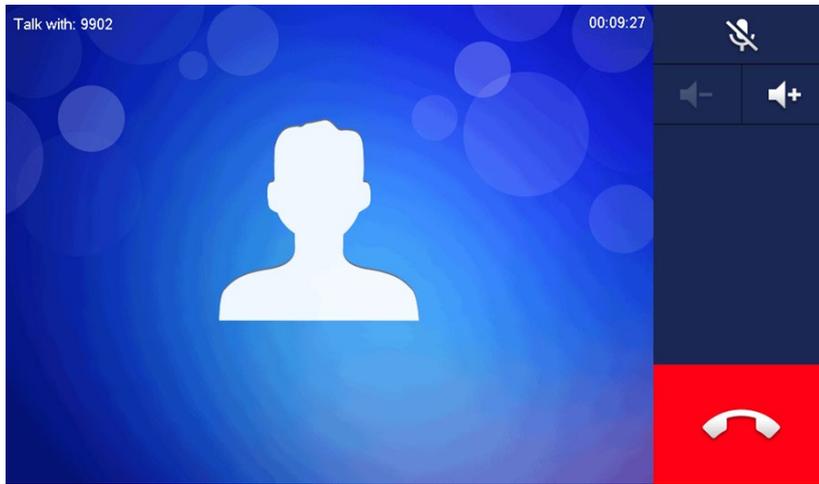
2. Enter the room number for the VTH you wish to call.
  - If VTO works as SIP server, dial room no. directly.
  - If the platform works as SIP server:
    - To call a user in the same unit and building, dial the room number directly.
    - To call a user in another buildings or unit, dial the complete address: Building Number + Unit Number + Room Number. For example, to call Building 1 Unit 1 Room 101 dial 1#1#101 to call.

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

3. Press  to place the call.

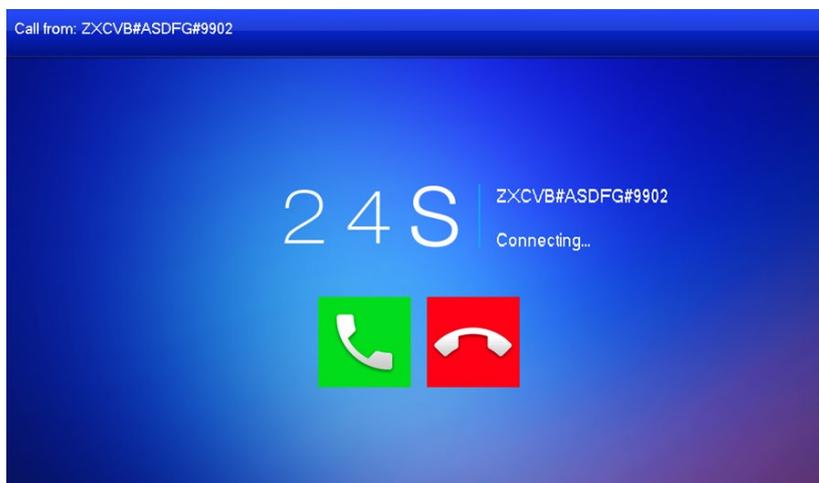
The system displays calling interface. If VTH owns a camera, there will be videos after answering the call.





### 5.2.9.3 Answering a Call

When another VTH calls this VTH, the call interface will be displayed.



- Press  to answer the call.
- Press  to hang up.

### 5.2.9.4 Managing Recent Calls

View and manage missed calls, accepted calls, and the call log of the VTH.

To call back a recent contact, select Call > Recent Call. Select the list of all calls or a list of only missed calls.



- Select the recent call of required VTH, press Call to call the contact.
- Press Edit, select a recent call record, and press Delete to remove the record.
- Press Clear to clear all recent calls in this tab.

# 6 Monitoring Locations

VTH master and extension devices are capable of displaying live video feeds from Main VTO stations, VTO sub-stations, and from IP cameras connected to the same network.

## 6.1 Monitoring Video from a VTO Station

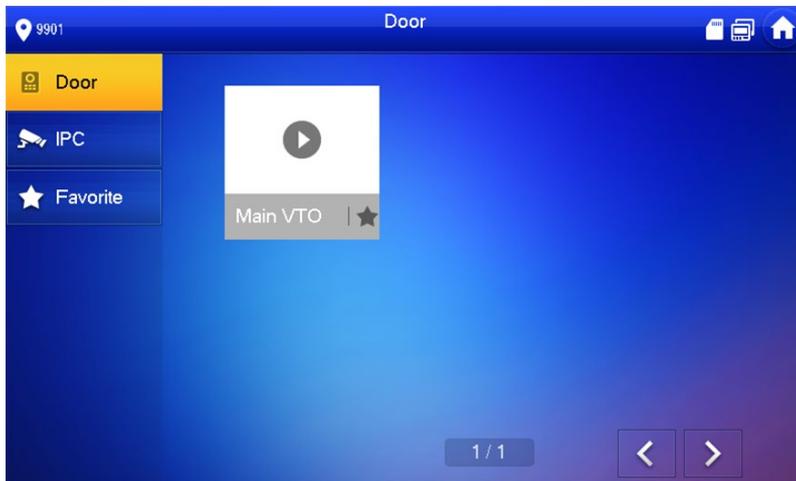
VTH devices can monitor video from a main VTO station and from a VTO sub-station. In monitoring mode, you can press the Call Key (📞) on the VTH front panel to transmit audio to the monitored VTO.

Note that the VTH user name and password must be set in each VTO that you need to monitor.

1. Select Monitor > VTO.

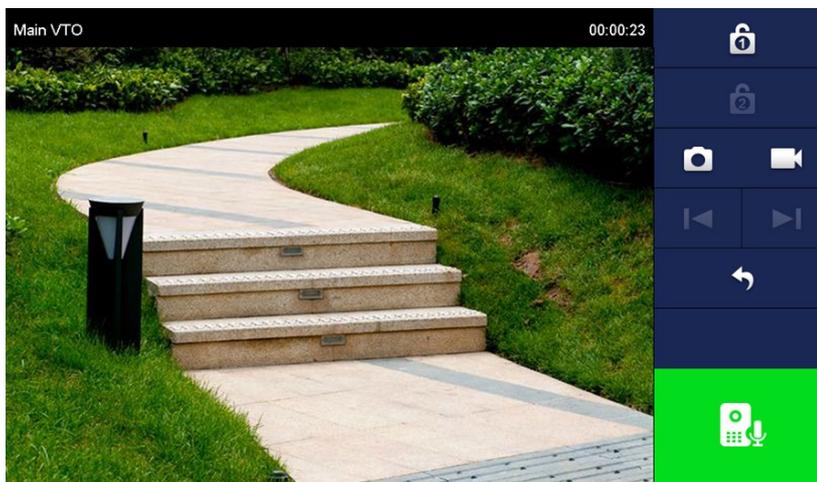
The system displays the list of added VTO main and substations.

2. Press the Star icon to add the VTO station to the Favorite list.



3. Press  to display the video from the VTO.

The device enters monitoring mode.



You can take the following actions:

Icon	Description
	Unlock the VTO remotely. The system provides 2-channel unlock function. If the icon is gray, then the unlock function for this VTO is not available.
	Take a snapshot. This key is gray if an SD card is not installed in the VTH.
	Start recoding video. Videos are stored in the installed SD card. If the SD card is full, then the VTH overwrites older video. This key is gray if an SD card is not installed in the VTH.
	Press  or  to switch to between multiple connected VTO devices to view that specific video feed
	Cancel monitoring.
	Speak to a person at the monitored device. Press the key again to disconnect.

Table 6-1: VTH Video Monitoring Actions

## 6.2 Monitoring a Remote Camera

In addition to displaying video from a VTO station, the VTH can also display video from an IP camera that is configured on the same network as the VTH device.

### 6.2.1 Adding a Camera

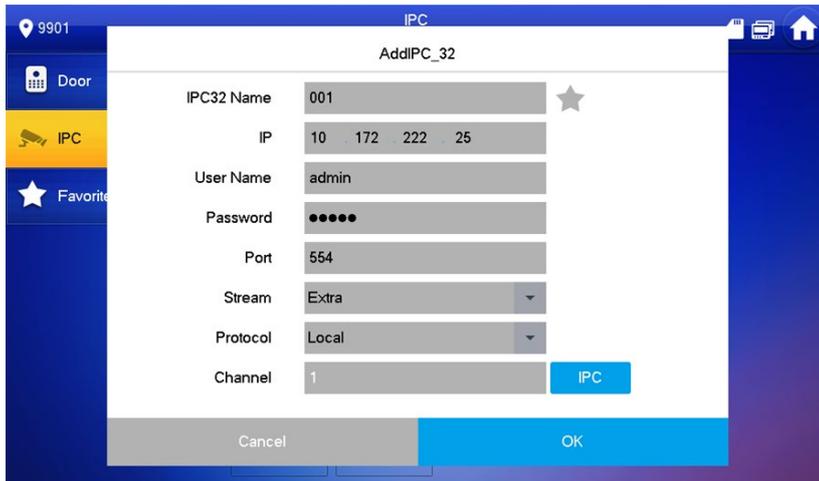
An IP camera that is added to the intercom system at the main VTO or via the mobile application interface is automatically synchronized to each VTH in the system.

Note, ensure the IP camera is powered and connected to the same intercom network prior to adding to the intercom system.

1. Select Monitor > IPC.



2. Press +Add.



3. Configure the camera parameters using the table below.

Parameter	Description
IPC	<p>Press this key to select the source of the incoming video feed: IPC, NVR, DVR, or HDCVI DVR (HCVR).</p> <ul style="list-style-type: none"> <li>• Select IPC if the video feed streams from a connected IPC directly.</li> <li>• Select NVR/DVR/HCVR if the video feed streams via a central recording device to which the IP camera is connected.</li> </ul>
IPC32 Name	Enter a name for the connected camera or recording device.
IP	Enter the IP Address for the connected camera or recording device.
User Name	Enter the User Name and the Password to login into the e connected camera or recording device.
Password	
Port	Default port is 554.
Stream	<p>Select the stream type:</p> <ul style="list-style-type: none"> <li>• Main stream: high-definition video that consumes a portion of bandwidth, suitable for local storage.</li> <li>• Extra stream: relatively smooth image with less bandwidth consumption, suitable for network transmission with low bandwidth.</li> </ul>
Protocol	Select either the video transmission protocol that the camera or device uses to transmit video. Choose Local or ONVIF.
Channel	<ul style="list-style-type: none"> <li>• IP Camera: Channel is always 1.</li> <li>• Recording Device: Channel number is the same channel assigned to the IP camera connected to the recording device.</li> </ul>

Table 6-2: Remote Video Fee Parameters

4. Press OK to accept and save the settings.
5. Press the Star icon to add the device to the Favorite list.

## 6.2.2 Modifying Camera Parameters

1. Select Monitor> IPC.
2. Press  for the connected IP camera or recording device.
3. Modify IPC parameters. Refer to Table 6.2 for details.
4. Press OK to accept and save the changes.

## 6.2.3 Deleting Cameras

1. Select Monitor> IPC.
2. Press Edit.
3. Select the desired IP camera or recording device.
4. Press Delete to remove the device from the IPC list.

## 6.2.4 Monitoring Video from a Connected Device

1. Select Monitor> IPC.
2. Select the IP camera or recording device and press .



3. Refer to Table 6.2 for camera monitoring functions.

## 6.3 Selecting Favorites

The VTH maintains a list of favorite VTO stations and IP cameras/recording devices so you can quickly display video from a device.

Note, you must add devices to the Favorite list by pressing the Star icon on the device icon.

1. Select Monitor> Favorite

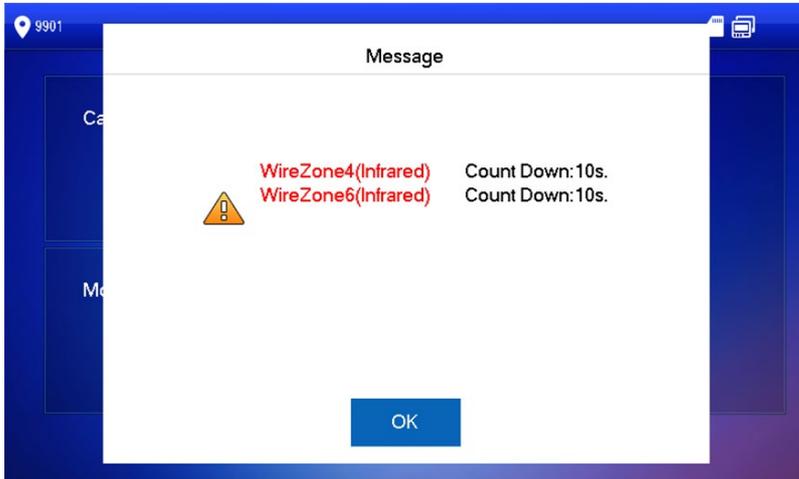


2. Select the device to be monitored and press  .  
The system displays the monitoring interface.

## 6.4 VTH Information

### 6.4.1 Reviewing Security Alarms

The VTH plays a 15 second sound after an alarm is triggered and displays a prompt interface, as shown below. The VTH also uploads the alarm information to the alarm record interface and to the management platform.



To view all alarm messages, select Info > Security Alarm to access the Security Alarm interface, as shown below. The All tab displays all alarm message stored in the system, and the Unread tab displays only those alarms messages that have not been read.

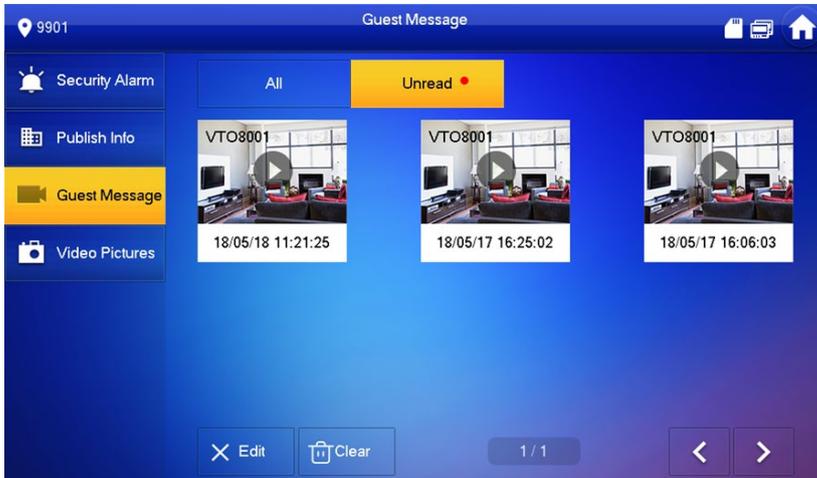
- Press Edit to select a message.
- Press Delete to delete the selected message.
- Press Clear to delete all records after confirmation.



## 6.4.2 Reviewing Guest Messages

A VTH device with an installed SD card can store guest messages (all messages stored on the SD card) recorded at a VTO station. The VTH can also retrieve messages from the VTO if the VTO device has FTP enabled and the “Video-audio Message Uploading” feature is enabled. Refer to the VTO User Manual for more information.

To retrieve guest messages, select Info > Guest Message.



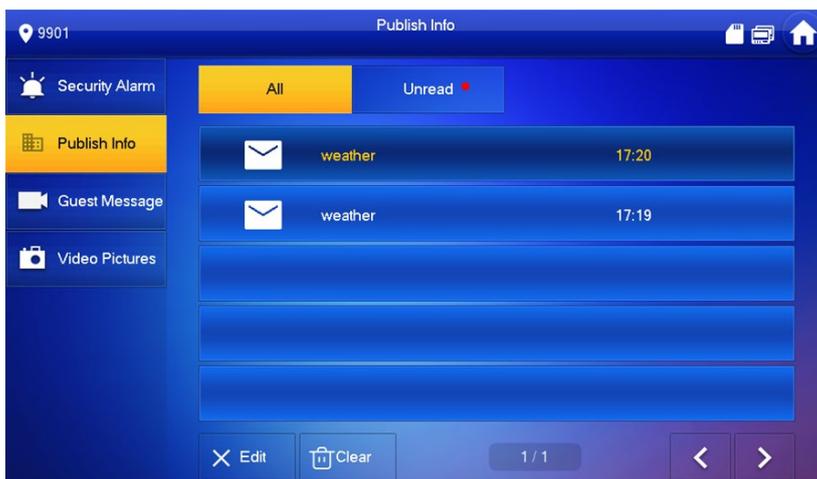
The All tab displays all messages stored on the system, the Unread tab displays only those messages not yet viewed.

- Press Edit to select a message.
- Press Delete to delete the selected message.
- Press Clear to delete all records after confirmation.

## 6.4.3 Reviewing Published Information

Published information are messages sent by the management center and in VTH the device.

To retrieve published information, select Info > Publish Info.

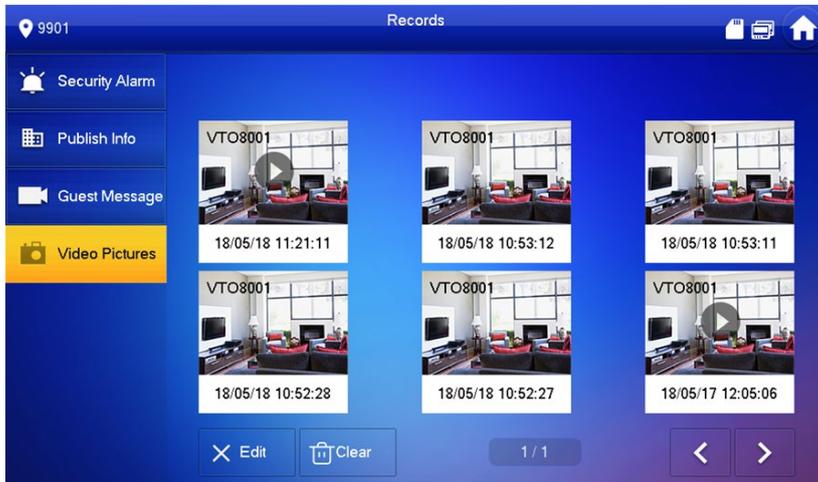


- Press Edit to select a message.
- Press Delete to delete the selected message.
- Press Clear to delete all records after confirmation.

## 6.4.4 Viewing Stored Video

The VTH can store videos and snapshots when an SD card is installed in the device.

To view these videos or snapshots, select Info > Video Pictures.



- Press Edit to select a message.
- Press Delete to delete the selected message.
- Press Clear to delete all records after confirmation.

## 6.5 Arm/Disarm Function

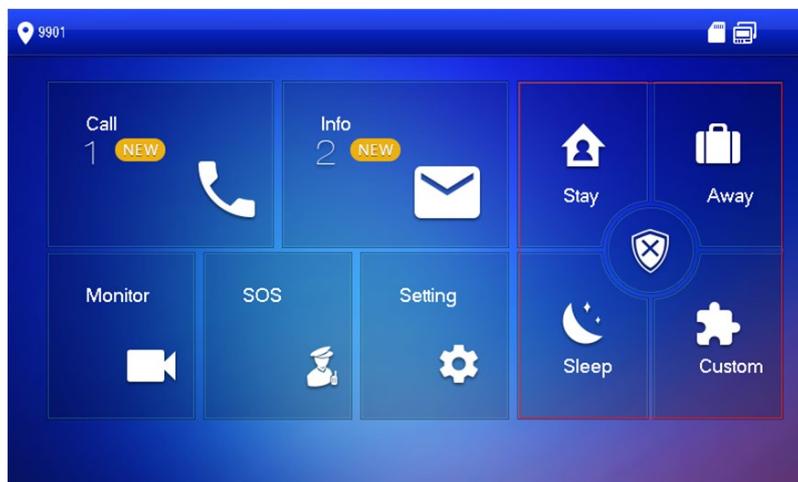
### 6.5.1 Arming an Alarm

In case of triggering alarm after arm, produce linkage alarm and upload alarm info.

- Please ensure that the area has been added into arm mode. Otherwise, there will be no alarm triggering after arm.
- Please ensure that it is in disarmed status. Otherwise, arm will fail.



1. Press  at the main interface.



2. Select arm mode. The system displays password input interface.
3. Enter arm and disarm password; press [OK].  
The device beeps continuously, which represents successful arm. The key displays corresponding arm mode.

### 6.5.2 Disarming an Alarm

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

1. Press disarm symbol at the lower right corner of the main interface.
2. Enter arm and disarm password; press [OK].

If you are forced to enter disarm password in case of emergencies, enter anti-hijacking password, which is the reversed arm password. The system will disarm, and at the same time, upload alarm info to management center/platform.

# 7 DSS Mobile

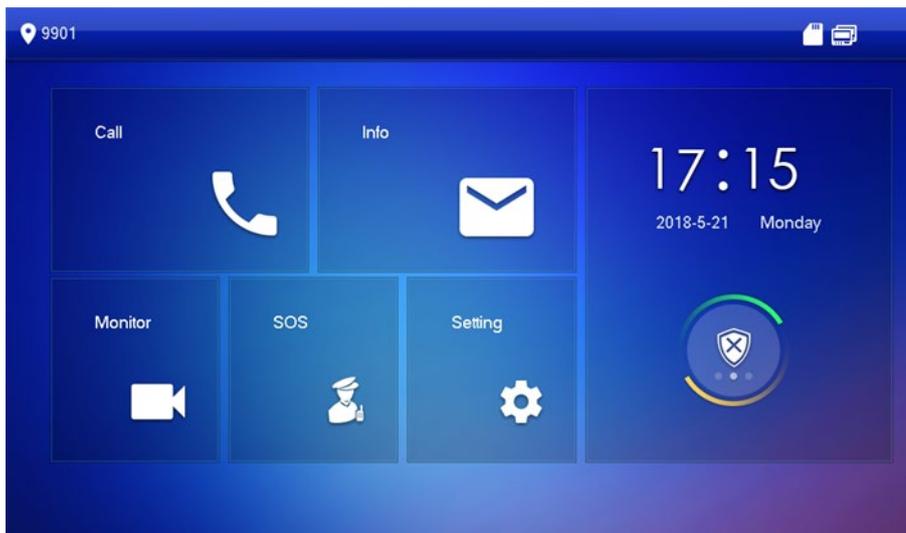
The VTH device is compatible with the Dahua DSS Mobile for VDP mobile application. From DSS you can unlock doors, talk to connected VTO devices, call the management center, and view call records and messages.

## 7.1 Downloading the App

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

1. On the VTH main interface, press Setting.

The Password Verification dialog box is displayed.

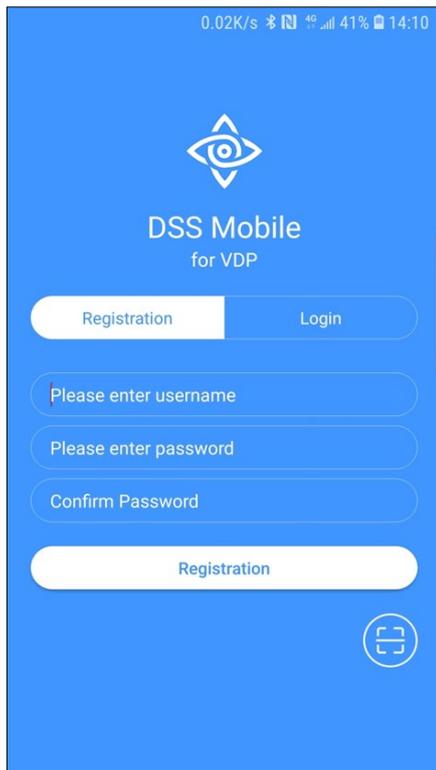


2. Input the password you configured, and then select General > QR Code. The Register code and Download code are displayed.
3. Scan the Download code with your smart phone to download and install the app. You can also search for “DSS Mobile for VDP” in the Apple App Store or in Google Play.



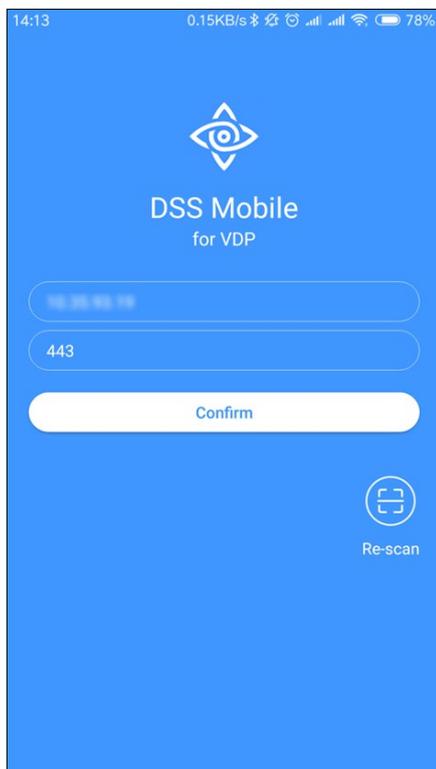
## 7.2 Registering the App

1. Run the app, accept the End-User License Agreement, and then allow the permissions for the app. The Registration interface is displayed.

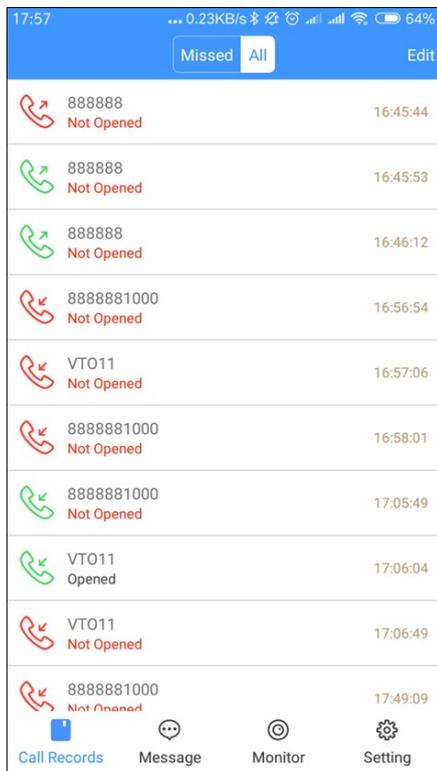


2. Tap  and then scan the Register code on the VTH.

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



3. Tap Confirm, enter the user name and password you need, and then tap Registration. You can register 5 users on a VTH at most.
4. Tap Login.
5. Enter the user name and password you registered, and then tap Login. The Call Records interface is displayed.



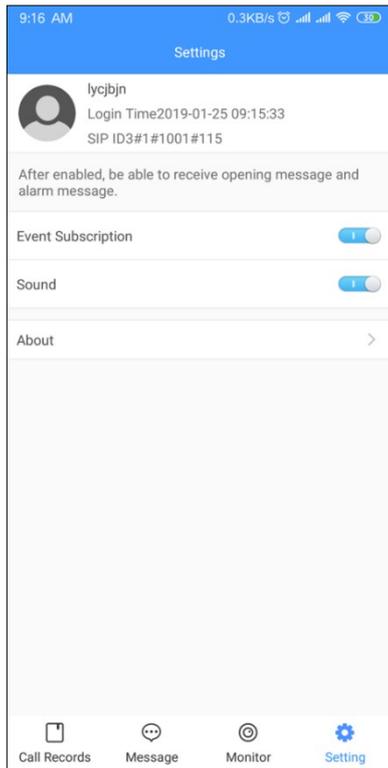
## 7.3 Call Functions

### 7.3.1 Configuring Call Forwarding

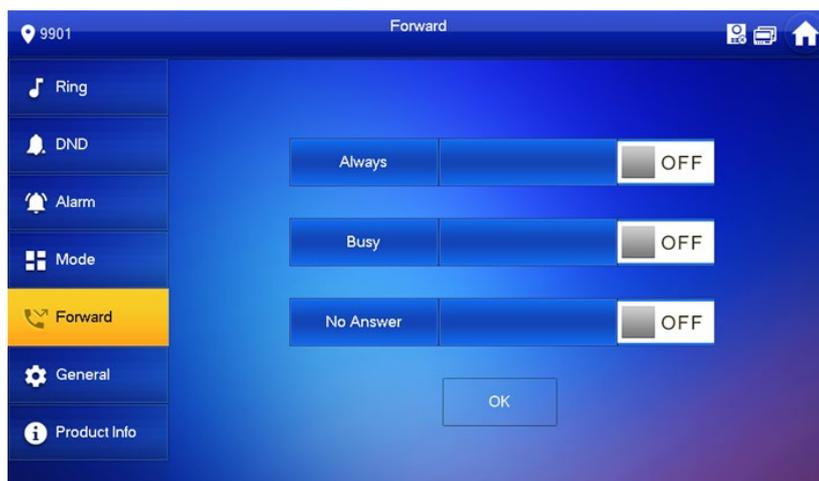
The VTH device can forward incoming calls to your mobile device.

1. Log into the app and tap Setting.
2. Note the SIP ID.

The Settings interface is displayed. The SIP ID is 3#1#1001#115.



3. On the VTH main interface, press Setting.
4. Enter your password and press Forward.

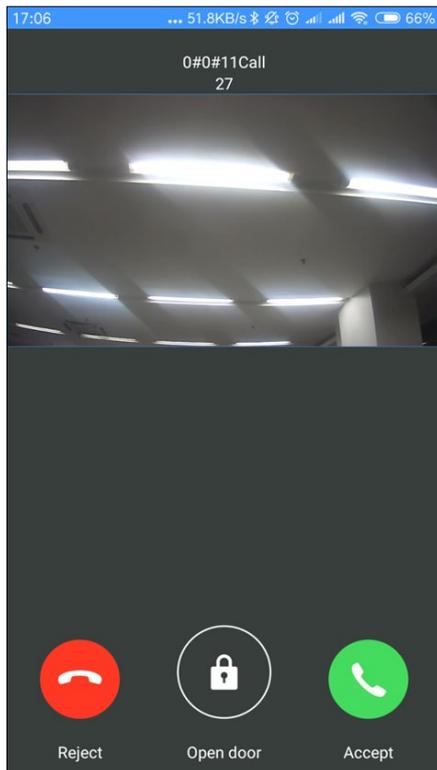


5. Select one of the following forwarding options:
  - Always: VTH forwards all calls.
  - Busy: VTH forwards calls if the VTH is busy with another call.
  - No Answer: VTH forwards any call that has not been answered within 15 seconds.
6. Type the SIP ID in the appropriate input box for the specific forwarding method.
  - To forward the calls to a specific user, enter the SIP ID for that user. For example, if you enter SIP ID 3#1#1001#115 all calls are forwarded to the user associated with the SIP ID.
  - To forward calls to every user associated with a VTH, enter “100” as the last three digits for the SIP ID. For example, if you enter SIP ID 3#1#1001#100 all calls are forwarded to each VTH user’s cell phone at the same time.
7. Press OFF to enable the function and press OK to save.

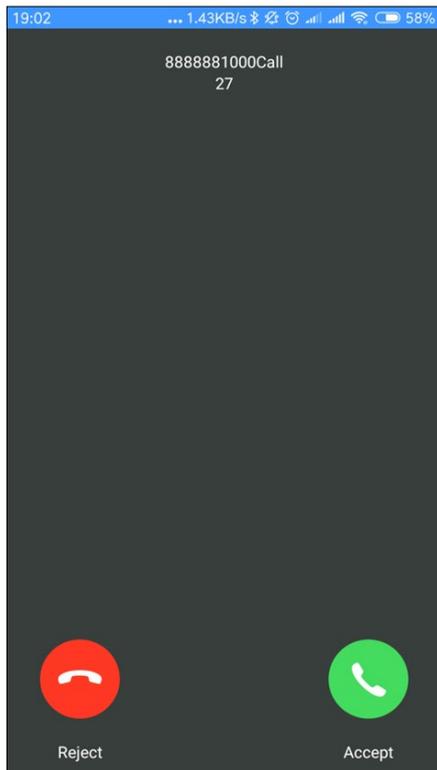
### 7.3.2 Calling Operations

After configuring the call forwarding, you can receive and answer phone calls from a VTO or from the management center.

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



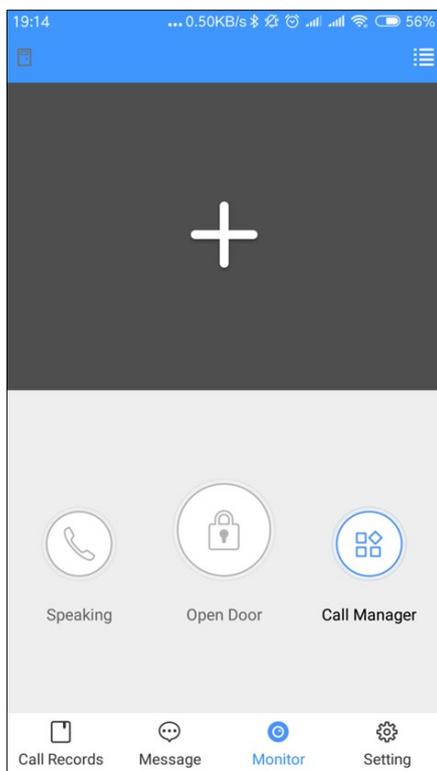
- You can also receive the call from the management center.



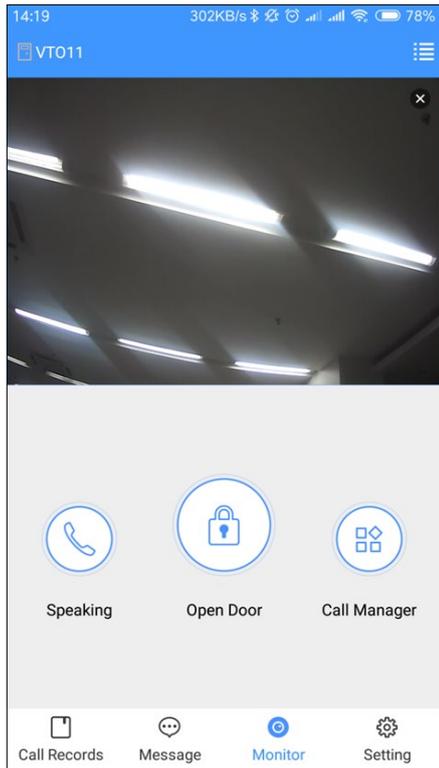
## 7.4 Monitoring Video from a VTO

The mobile application can display streaming video from an associated VTO device.

1. Log into the app and tap Monitor.



2. Tap Call Manager to call the management center.
3. Tap the "+" sign, and then select the VTO video feed you want to display.

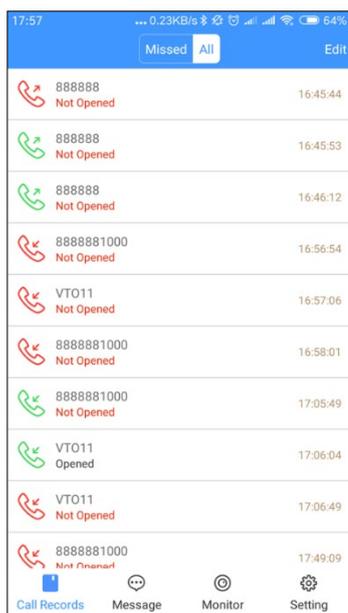


4. Tap Open Door to unlock the door.
5. Tap Speaking to communicate with a person at the VTO station.

## 7.5 Call Records

The mobile application stores call information from a VTO station or from the management center.

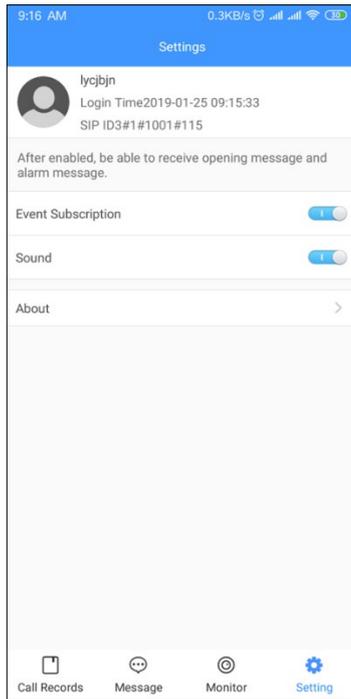
1. Log into the app and tap Call Records.



- Tap Edit to delete a single call record.
- Tap Edit > Empty to delete all the records.

## 7.6 Settings

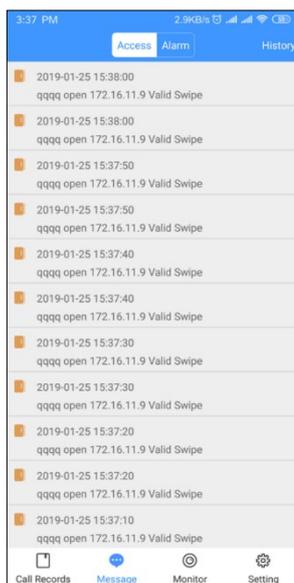
1. Log into the app and tap Setting.



2. Tap  to enable the specific function.
  - Event Subscription: View the access and alarm messages.
  - Sound: Phone rings when receiving a call.
3. Tap About to view the version information and the online help. In addition, you can logout the current account.

## 7.7 Messages

1. Log in the app, and then tap Message to view the access messages and alarm messages.





Dahua Technology USA  
23 Hubble  
Irvine, CA 92618  
Tel: (949) 679-7777  
Fax: (949) 679-5760  
Support: 877-606-1590  
Sales: [sales.usa@dahuatech.com](mailto:sales.usa@dahuatech.com)  
Support: [support.usa@dahuatech.com](mailto:support.usa@dahuatech.com)