# IP Indoor Monitor

## Quick Start Guide

V1.0.0

# Foreword

## General

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

## Safety Instructions

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

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

## Revision History

| Version | Revision Content | Release Date |
|---|---|---|
| V1.0.0 | First release | April 2020 |

## About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

# Important Safeguards and Warnings

The following description is the correct application method of the device. Read the manual carefully before use to prevent danger and property loss. Strictly conform to the manual during application and keep it properly after reading.

## Operating Requirement

- Do not place and install the device in an area exposed to direct sunlight or near heat generating device.
- Do not install the device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening.
- Use the device only within rated input and output range.
- Do not dismantle the device arbitrarily.
- The device shall be used with screened network cables.

## Power Requirement

- The product shall use electric wires (power wires) required by the region where the device will be used.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, refer to device labels.
- Appliance coupler is a disconnecting device. During normal use, keep an angle that facilitates operation.
- Do not cut off power supply during device upgrade.

# Table of Contents

# 1 Introduction

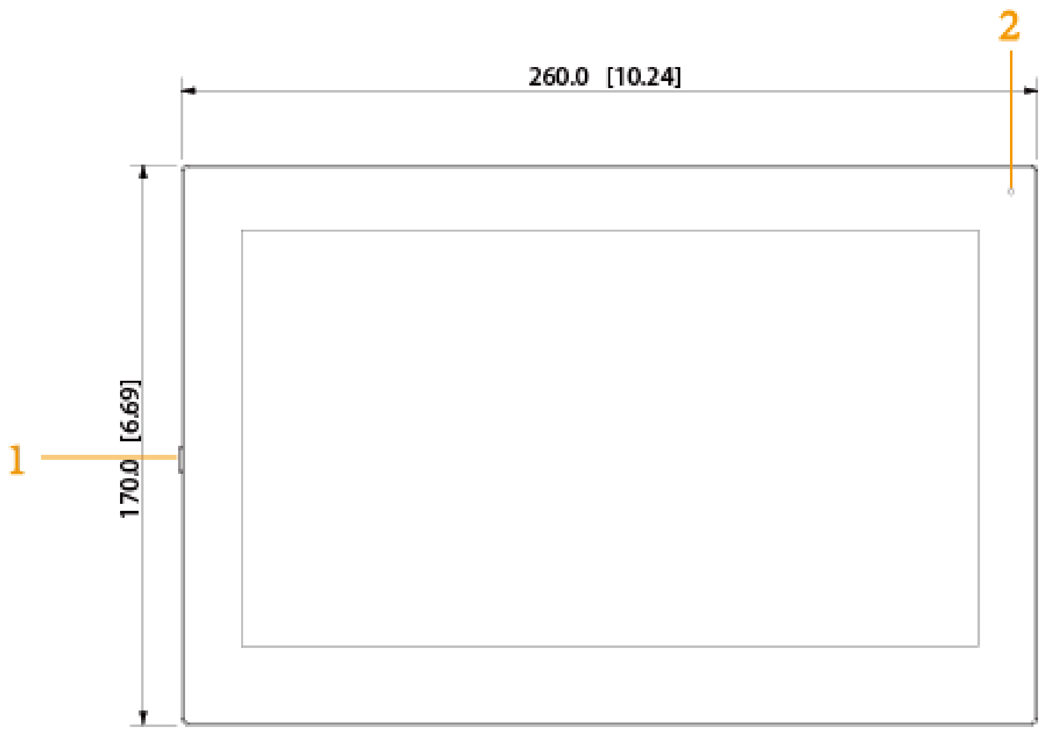
## 1.1 Overview

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

## 1.2 Front Panel

### 10 Inch

Figure 1-1 Front panel [mm (inch)]



## 7 Inch

Figure 1-2 Front panel [mm (inch)]

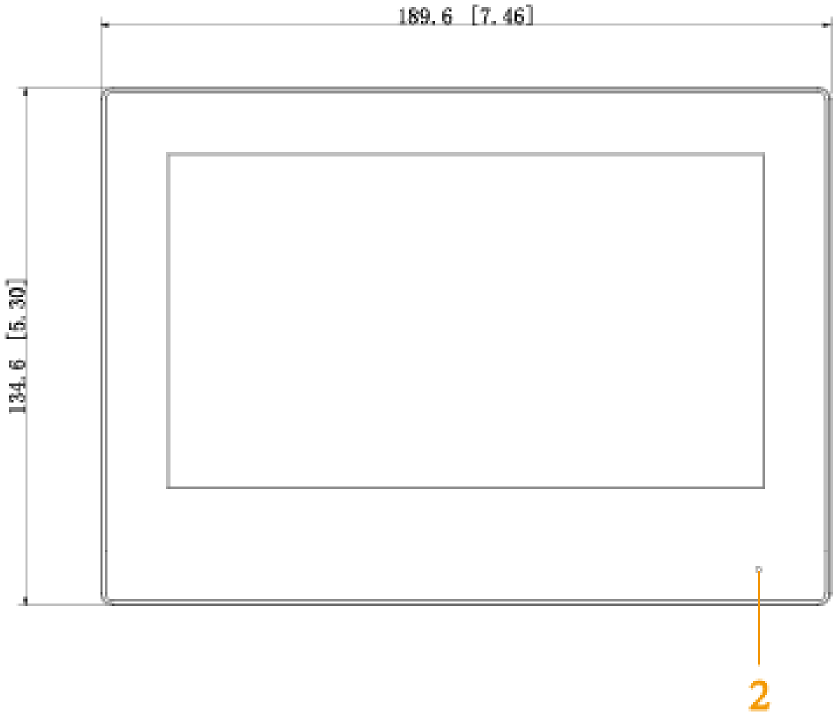


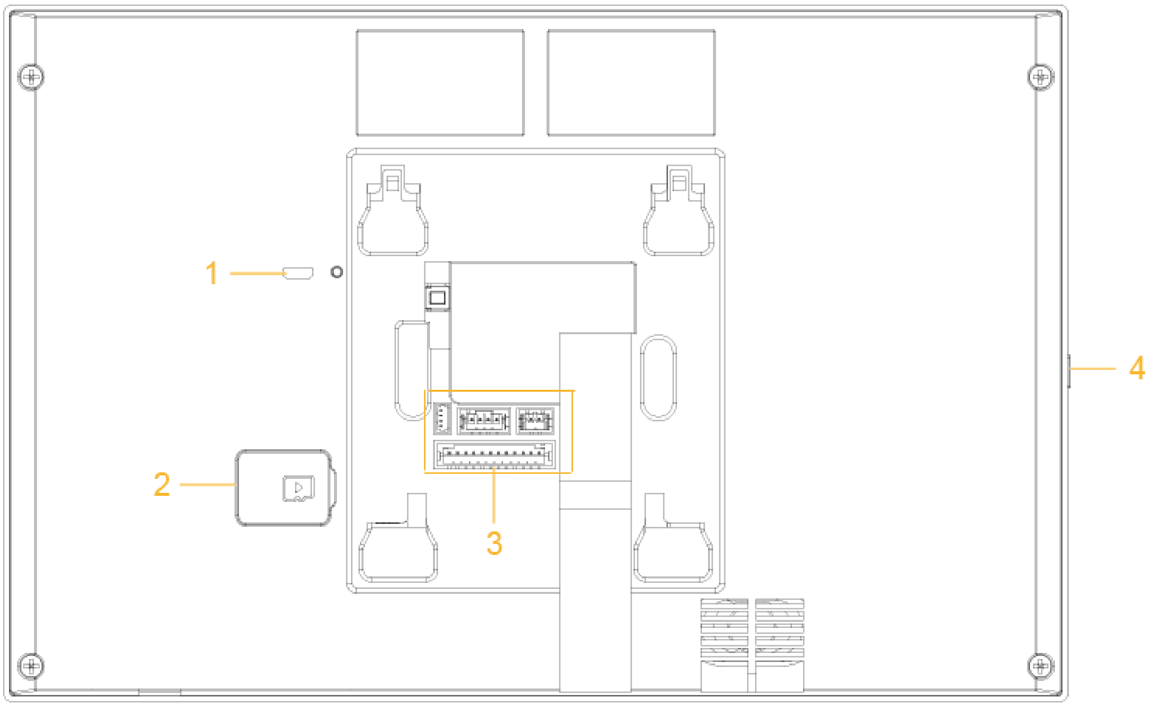
Table 1-1 Components

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

## 1.3 Rear Panel

### 10 Inch

Figure 1-3 Rear panel



### 7 Inch

Figure 1-4 Rear panel

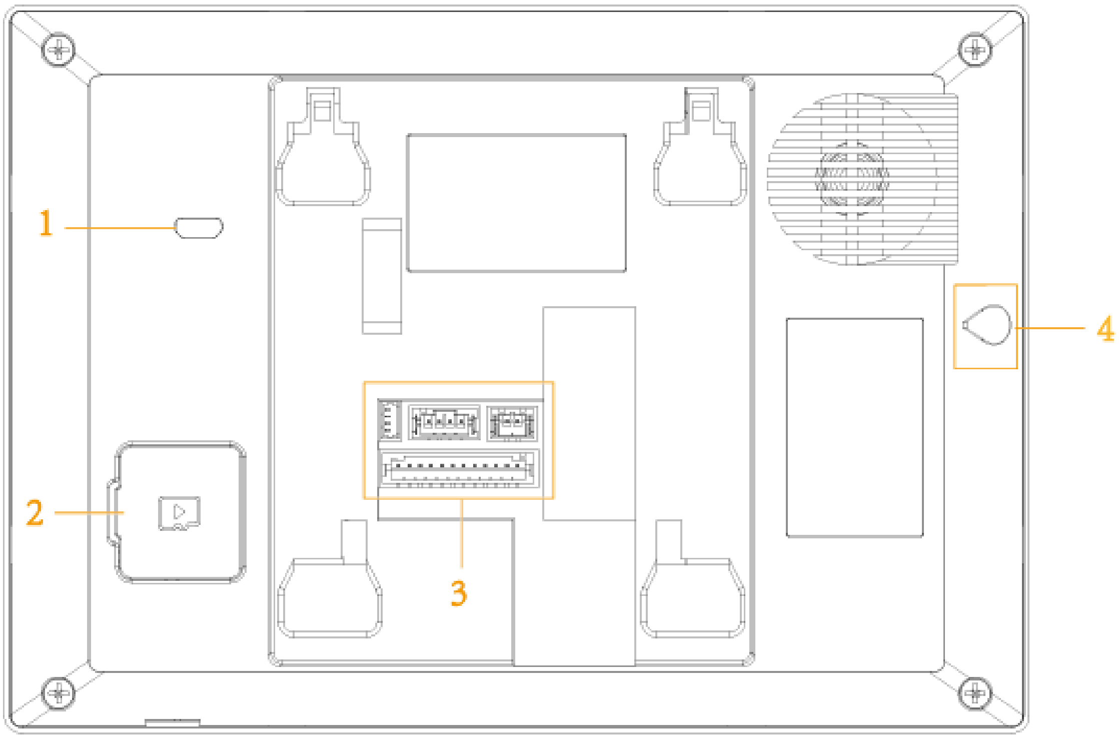
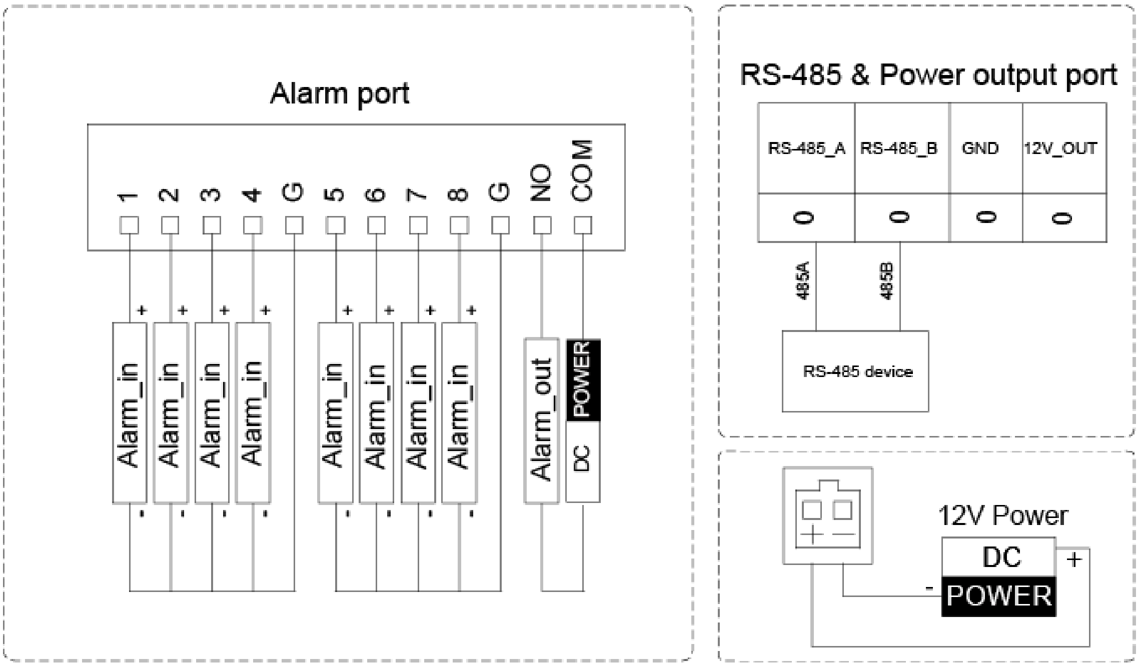


Table 1-2 Rear panel description

| No. | Description |
|---|---|
| 1 | USB port, used by project personnel. |
| 2 | SD card slot. |
| 3 | Alarm ports, power cables, RS-485 port, and network ports are under the cover. |
| 4 | On/off button. Press the button, and then you can turn on/off the screen; press and hold the button, you can turn on/off or restart the indoor monitor. |

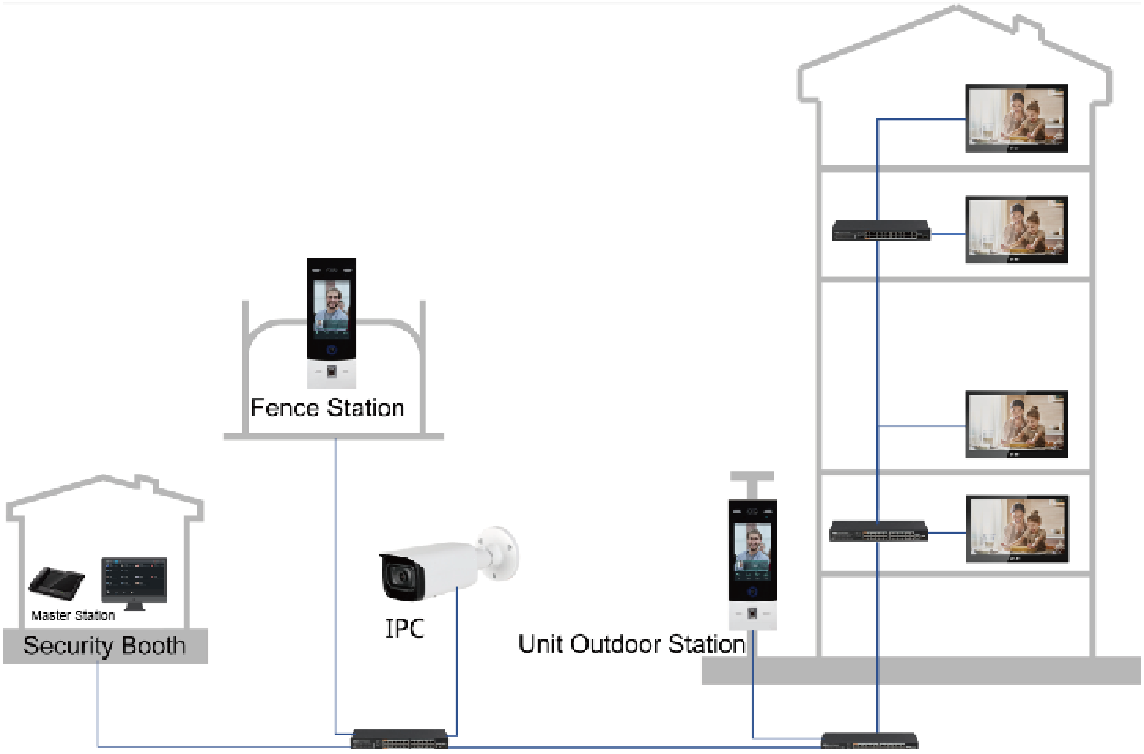
## 1.4 Cable Connection

Figure 1-5 Cable connection



# 2 Network Diagram

Figure 2-1 Network diagram



# 3 Configuration

This chapter introduces initialization, cable connection, and parameter configuration to realize basic functions, including device management, calling, and monitoring.

## 3.1 Configuration Process

Before configuration, make sure that there is no short circuit or open circuit.

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

Step 2 Configure door stations (VTO). For details, see the *IP Indoor Monitor_User's Manual*.

1) Initialize VTO.
2) Configure VTO number.
3) Configure VTO network parameters.
4) Configure SIP Server.
5) Add door stations (VTO) to the SIP server.
6) Add room number to the SIP server.

Step 3 Configure indoor monitor (VTH).

Step 4 Commissioning.

## 3.2 VDPConfig

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

## 3.3 Configuring Indoor Monitor

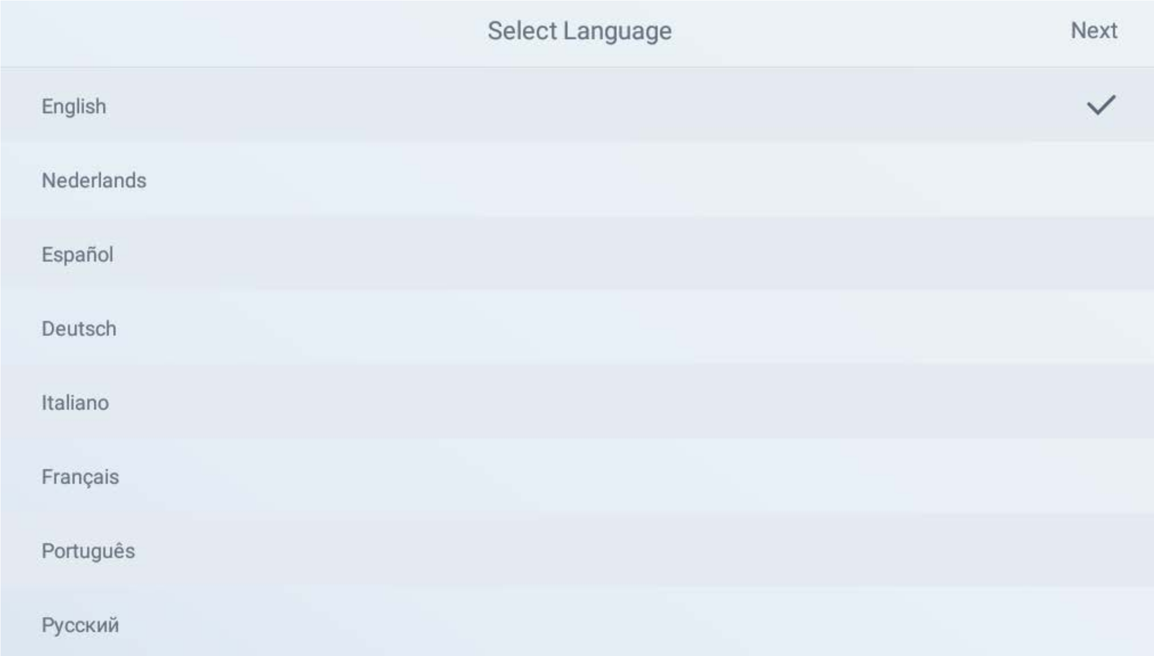
When the indoor monitor is used for the first time, you need to select a language that you prefer, initialize the indoor monitor to get a password to enter project setting interface and an email to reset password. In addition, you need to configure parameters for all door stations (VTO) and indoor monitors that are found on the indoor monitor you are operating.

### 3.3.1 Initialization

#### 3.3.1.1 Quick Configuration for VTH (For Villa)

Step 1 Power on the device.

Figure 3-1 Select a language



Select Language Next

English ✓

Nederlands

Español

Deutsch

Italiano

Français

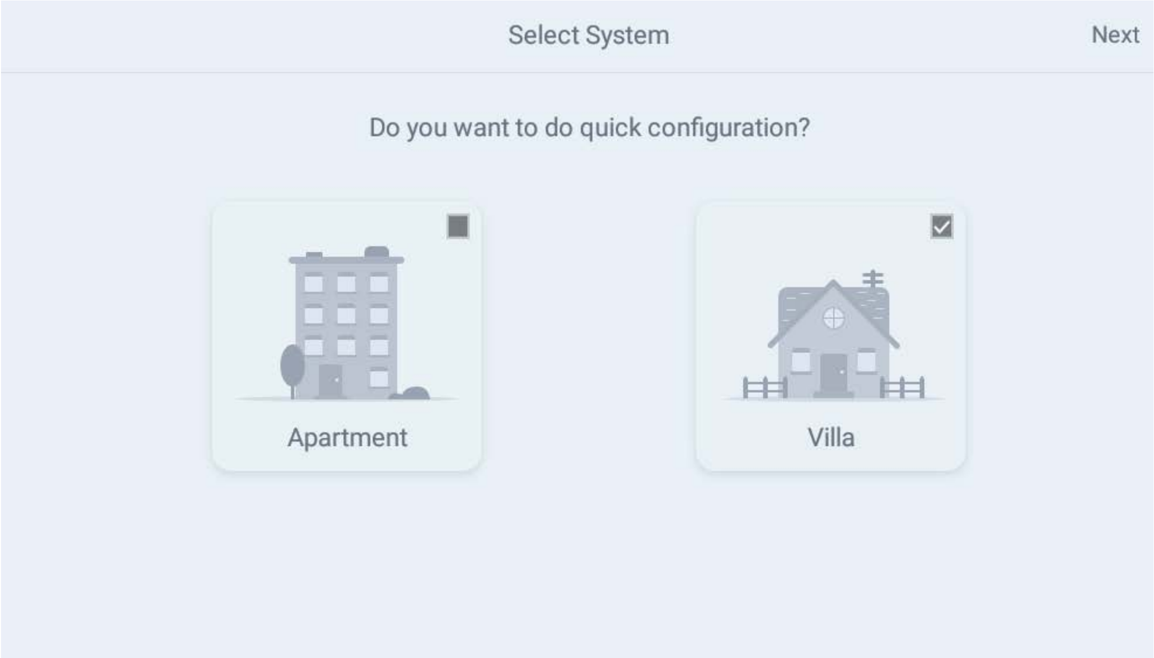
Português

Русский

Step 2 Select a language that you prefer.

Step 3 Tap **OK**.

Figure 3-2 Select apartment or villa



Select System Next

Do you want to do quick configuration?

■ Apartment

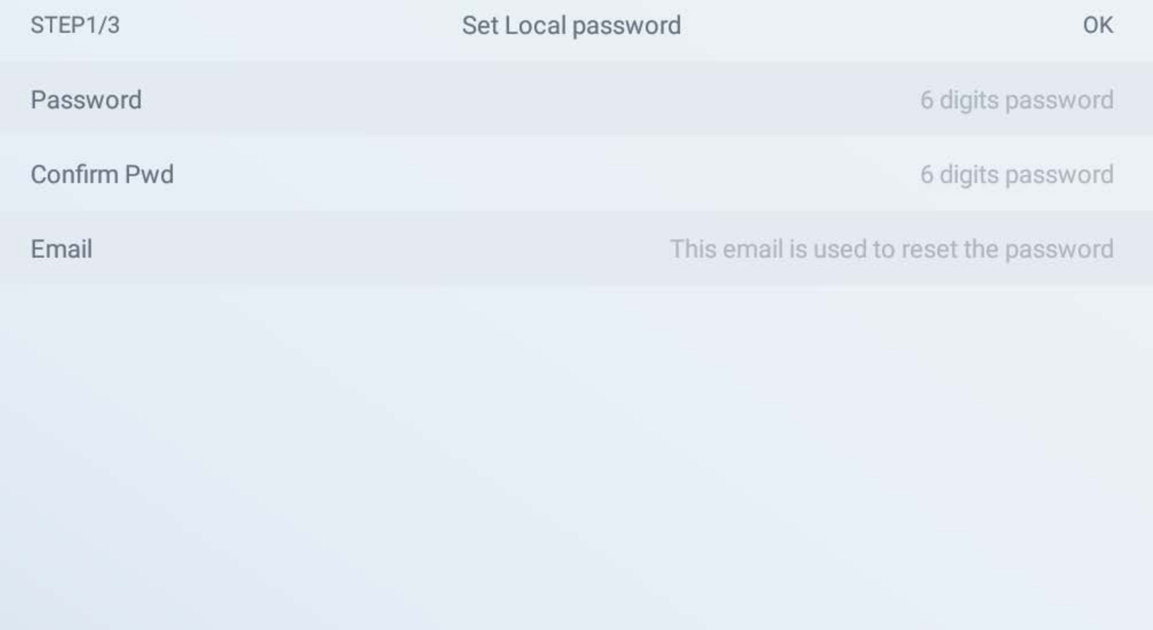
☑ Villa

- Apartment: Select **Apartment** when the door stations and indoor monitors are installed in apartments. Quick configuration is not available when you select apartment.
- Villa: Select **Villa** when the door stations and indoor monitors are installed in villas. Quick configuration is available when you select villa.

Step 4 Select **Villa**.

Step 5 Tap **OK**.

Figure 3-3 Set local password



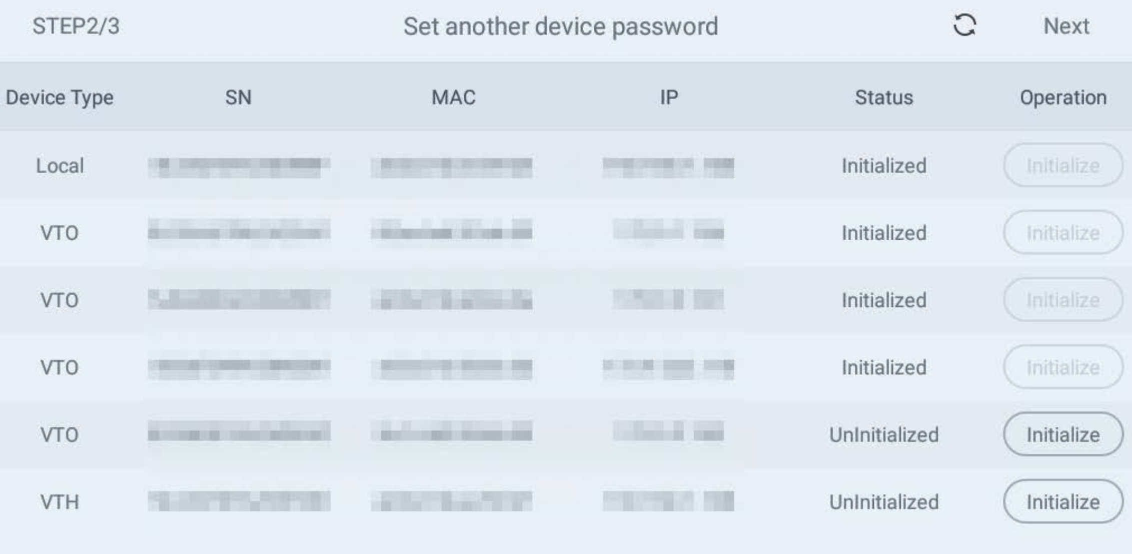
STEP1/3 Set Local password OK

| | |
|---|---|
| Password | 6 digits password |
| Confirm Pwd | 6 digits password |
| Email | This email is used to reset the password |

Step 6 Enter password, confirm password, and email for the VTH you are to initialize.

Step 7 Tap **OK**.

Figure 3-4 Set another device password

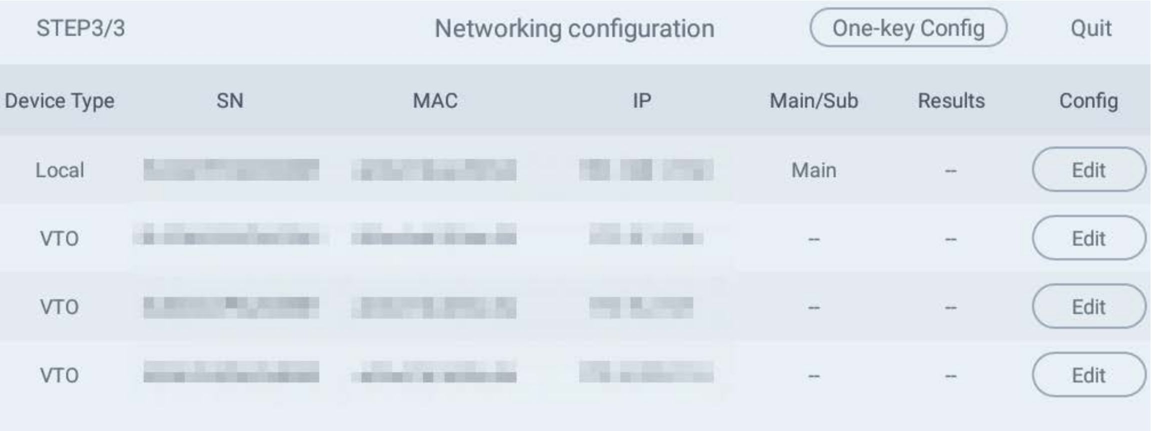


STEP2/3 Set another device password Next

| Device Type | SN | MAC | IP | Status | Operation |
|---|---|---|---|---|---|
| Local | [redacted] | [redacted] | [redacted] | Initialized | Initialize |
| VTO | [redacted] | [redacted] | [redacted] | Initialized | Initialize |
| VTO | [redacted] | [redacted] | [redacted] | Initialized | Initialize |
| VTO | [redacted] | [redacted] | [redacted] | Initialized | Initialize |
| VTO | [redacted] | [redacted] | [redacted] | UnInitialized | Initialize |
| VTH | [redacted] | [redacted] | [redacted] | UnInitialized | Initialize |

Step 8 Tap **Refresh**, and then tap **Next**.

Figure 3-5 Networking configuration



STEP3/3 Networking configuration One-key Config Quit

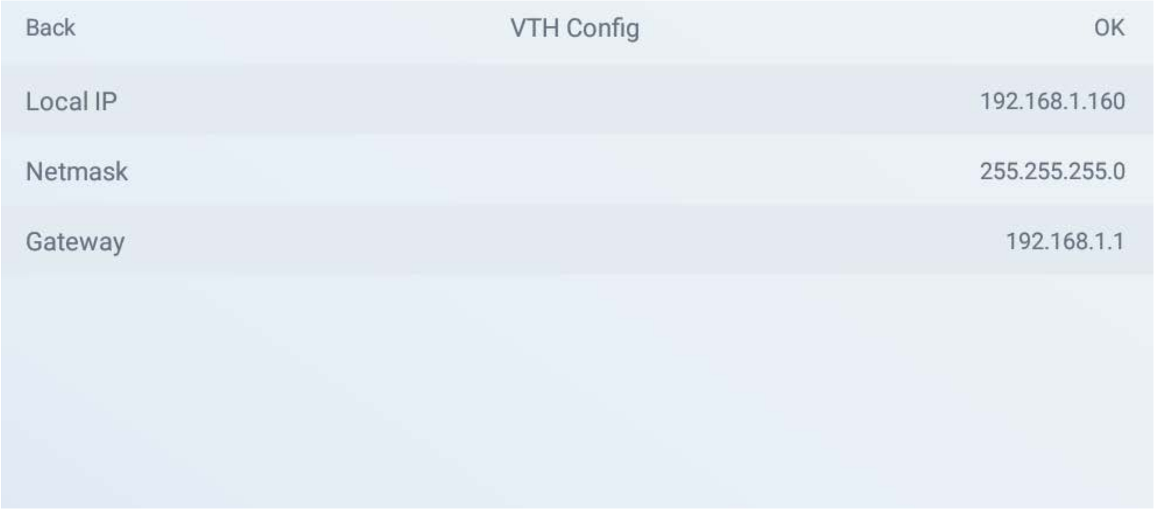
| Device Type | SN | MAC | IP | Main/Sub | Results | Config |
|---|---|---|---|---|---|---|
| Local | [redacted] | [redacted] | [redacted] | Main | -- | Edit |
| VTO | [redacted] | [redacted] | [redacted] | -- | -- | Edit |
| VTO | [redacted] | [redacted] | [redacted] | -- | -- | Edit |
| VTO | [redacted] | [redacted] | [redacted] | -- | -- | Edit |

Step 9 Tap **Edit** behind each device to do configurations.

- Configure indoor monitor (VTH).

1) Select an indoor monitor (VTH).

Figure 3-6 VTH config



| Back | VTH Config | OK |
|---|---|---|
| Local IP | | 192.168.1.160 |
| Netmask | | 255.255.255.0 |
| Gateway | | 192.168.1.1 |

2) Enter local IP, Network, and gateway.

3) Tap **OK**.

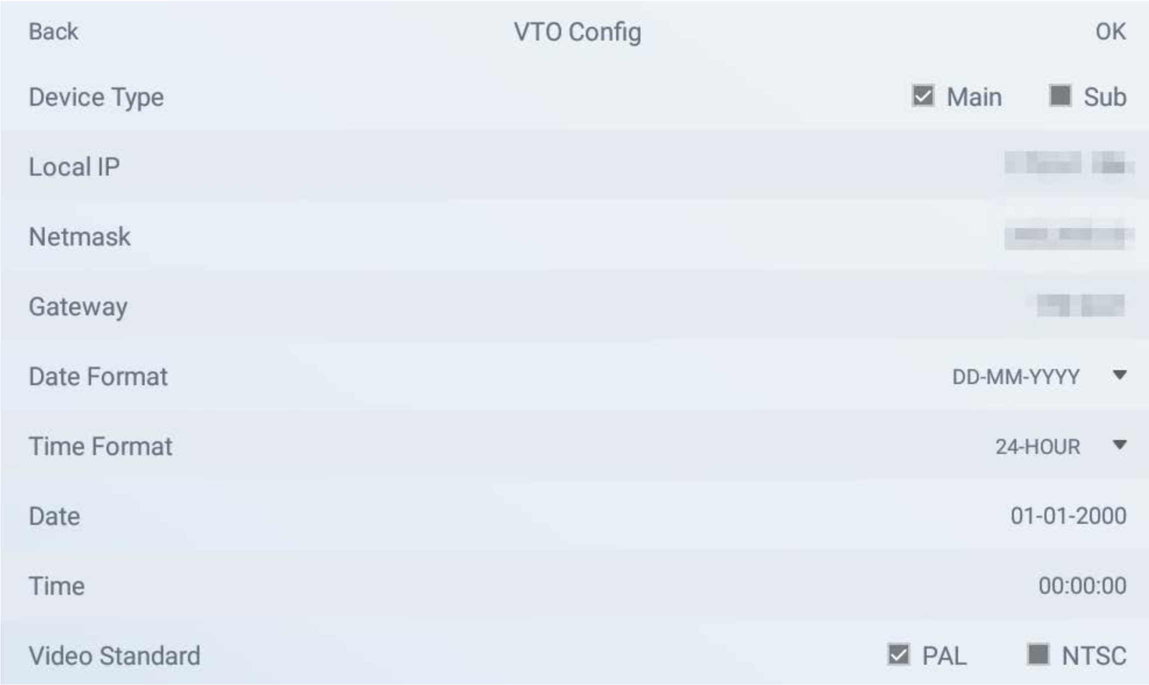
The indoor monitor (VTH) configuration is completed.

- Configure Main VTO and Sub VTO. There must be only one main VTO and one or more sub VTOs.

If there are no sub door stations (VTO), then you do not need to do sub door station (VTO) configurations.

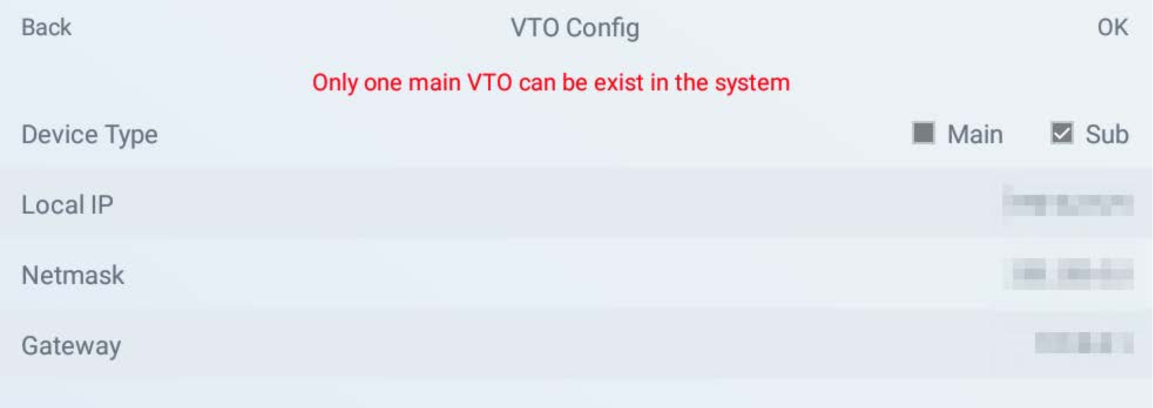
1) Select a door station (VTO).

Figure 3-7 VTO config (1)



| Back | VTO Config | OK |
|---|---|---|
| Device Type | | ☑ Main ■ Sub |
| Local IP | | [redacted] |
| Netmask | | [redacted] |
| Gateway | | [redacted] |
| Date Format | | DD-MM-YYYY ▼ |
| Time Format | | 24-HOUR ▼ |
| Date | | 01-01-2000 |
| Time | | 00:00:00 |
| Video Standard | | ☑ PAL ■ NTSC |

Figure 3-8 VTO config (2)



Only one main VTO can be exist in the system

Device Type ■ Main ☑ Sub

Local IP

Netmask

Gateway

2) Select **Main** or **Sub**.

   Enter local IP, Network, gateway; select video standard, date format, time format; set date and time.

3) Tap **OK**.

4) Tap **One-key Config**.

   The VTO configuration will be completed in a few seconds.

### 3.3.1.2 Normal Configuration for VTH (For Apartment)

Step 1 Tap **Apartment** on Figure 3-2.

Step 2 Connect the indoor monitor to power source.

Step 3 Enter the password, confirm password, and email.

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

Step 4 Tap **OK**.

Figure 3-9 Main menu

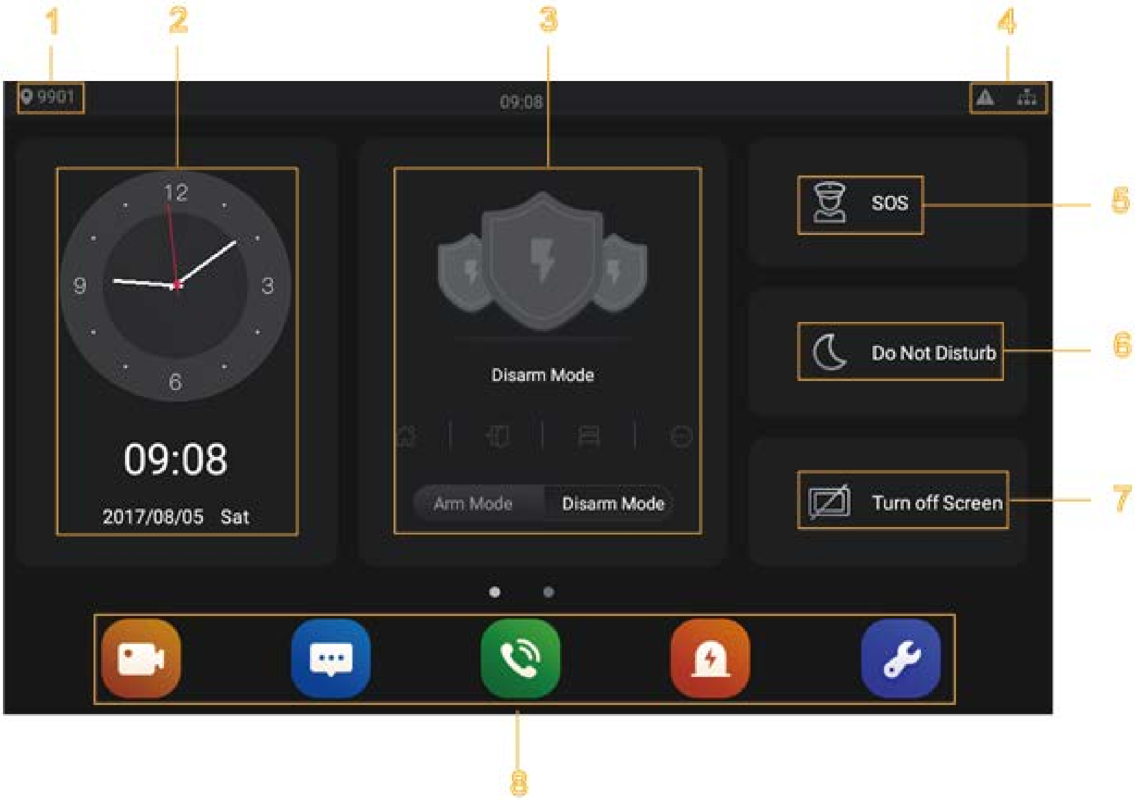


Table 3-1 Description of the main menu

| No. | Name | Description |
|---|---|---|
| 1 | Room number | Number of the room where the indoor monitor Is installed. |
| 2 | Date and time | Current time and date are displayed here. |
| 3 | Arm and disarm | Shortcut icons to arm or disarm are displayed here. The four icons represent at home mode, away from home mode, sleep mode, and customizable mode. Select **Arm Mode** or **Disarm Mode** first, and then tap the icons to arm or disarm. |
| 4 | Status bar | ● : The wired network is not connected.<br>● : The wired network is connected.<br>● ⚠: The indoor monitor failed to be connected to the SIP server. If this icon does not appear, then the indoor monitor is connected to the SIP server.<br>● : The SD card is inserted and recognized.<br>● ☾: The indoor monitor is in the Do not disturb mode. It is disabled by default.<br>● Door Status<br>◇ : Door closed.<br>◇ : Door open.<br>◇ : Unknown. |

| No. | Name | Description |
|---|---|---|
| 5 | SOS | Tap the SOS icon, the indoor monitor will call the management center. |
| 6 | Do not disturb | Tap the icon, and then you can set do not disturb period. You need to enable DND Period first, and then you can do do-not-disturb settings.<br>For details, see DND after tapping 🔧 and entering the password (123456 by default; for password changing, see the *IP Indoor Monitor_User's Manual*).<br>📖<br>It is recommended that the password be changed during the first use. |
| 7 | Turn off screen | Tap the icon, and then the screen will be turned off. |
| 8 | Function buttons | ● 📹: Tap the icon, and then you can watch videos from door stations and IP cameras.<br>● 💬: Tap the icon, and then text messages and videos left by visitors, or public notices released by the management center will be displayed.<br>● 📞: Tap the icon, and then you can make calls to other indoor monitors and the management center; and you can also view call logs and your contacts on this interface.<br>● ⚠: Tap the icon, and then you can view alarm logs, do alarm settings for 6 areas as needed.<br>● 🔧: Tap the icon, enter the password (123456 by default) and then you can select ringtones for different door stations, Do Not Disturb period, call forward mode (there are three options: Always, Busy, and No Answer), and other settings.<br>● Sound Recorder: You can record your voice messages to the SD card or to the indoor monitor.<br>● Calculator: You can do calculations through the calculator.<br>● Files: You can view files like images, videos, audio, and recently produced files.<br>● Calendar: You can view date through the indoor monitor, and create notes, schedules, and plans.<br>● Gallery: You can view images captured by door stations (VTO) or IP cameras. |

## 3.3.2 Network Settings

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

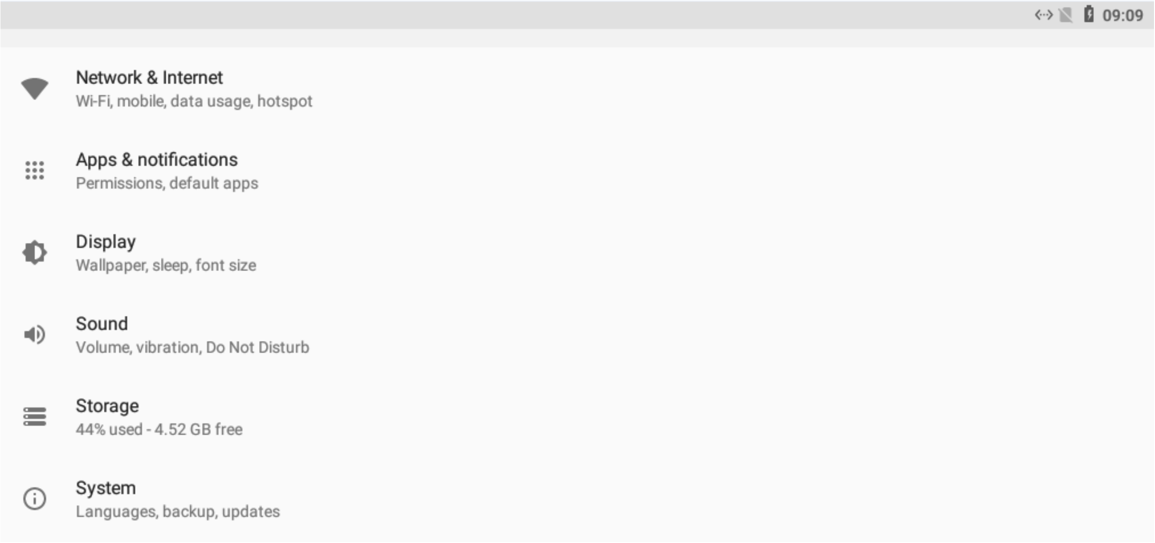
### Wired Network

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

Step 1 Tap the **Settings** icon.

Step 2 Enter the password (123456 by default; for password changing, see the *IP Indoor Monitor_User's Manual*).

Figure 3-10 Network settings



09:09

Network & Internet
Wi-Fi, mobile, data usage, hotspot

Apps & notifications
Permissions, default apps

Display
Wallpaper, sleep, font size

Sound
Volume, vibration, Do Not Disturb

Storage
44% used - 4.52 GB free

System
Languages, backup, updates

Step 3 Configure parameters.

Table 3-2 Parameter description

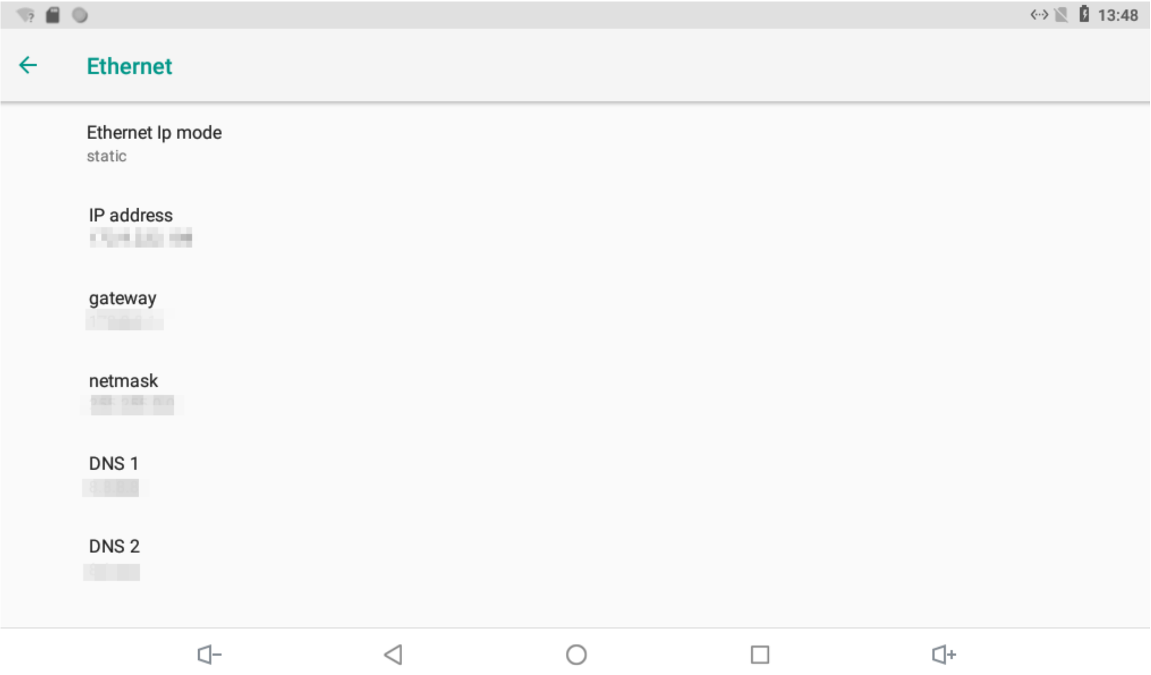
| **Parameter** | **Description** | |
|---|---|---|
| Network & Internet | You can choose to enable Wi-Fi or not by tapping ○.<br>● Tap ▼, and then available Wi-Fi networks will be displayed.<br>● You can select Ethernet IP mode. There are two options: Static and DHCP. | |
| Apps & notifications | You can view the recently opened apps, apps opened by default, app permissions (apps using location, microphone, and camera), app notifications, and special app access. | |
| Display | You can adjust display brightness, display sleep duration, font size, and display size. | |
| Sound | You can adjust media volume and notification volume. You can also select to use default notification sound and default alarm sound. | |
| Storage | Spaces used and spaces left can be viewed. You can delete unwanted files as needed. | |
| System | Languages & Input | ● Languages: You can select languages as needed.<br>● Keyboard & Inputs: There are two options: Virtual keyboard and physical keyboard.<br>● Input assistance: You can use spell checker, autofill service (not available at present), personal dictionary, and text-to-speech output as needed. Pointer speed can also be adjusted. |
| | Backup | You can use backup storage as needed. |
| | Reset options | You can reset Wi-Fi, mobile, and Bluetooth, and app preferences. You can also erase all data, which means restoring the indoor monitor to factory settings. |
| | About tablet | You can see details (battery status, network status, legal |

| Parameter | Description | |
|---|---|---|
| | | information, model, android version, Android security patch level, baseband version, Kernel version, build number, and more) about the indoor monitor. |

Step 4 Tap Network & Internet.

Step 5 Tap Ethernet.

Figure 3-11 Network setting



Ethernet

Ethernet Ip mode
static

IP address
[redacted]

gateway
[redacted]

netmask
[redacted]

DNS 1
[redacted]

DNS 2
[redacted]

Step 6 Tap Ethernet Ip mode.

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

## Wireless Network

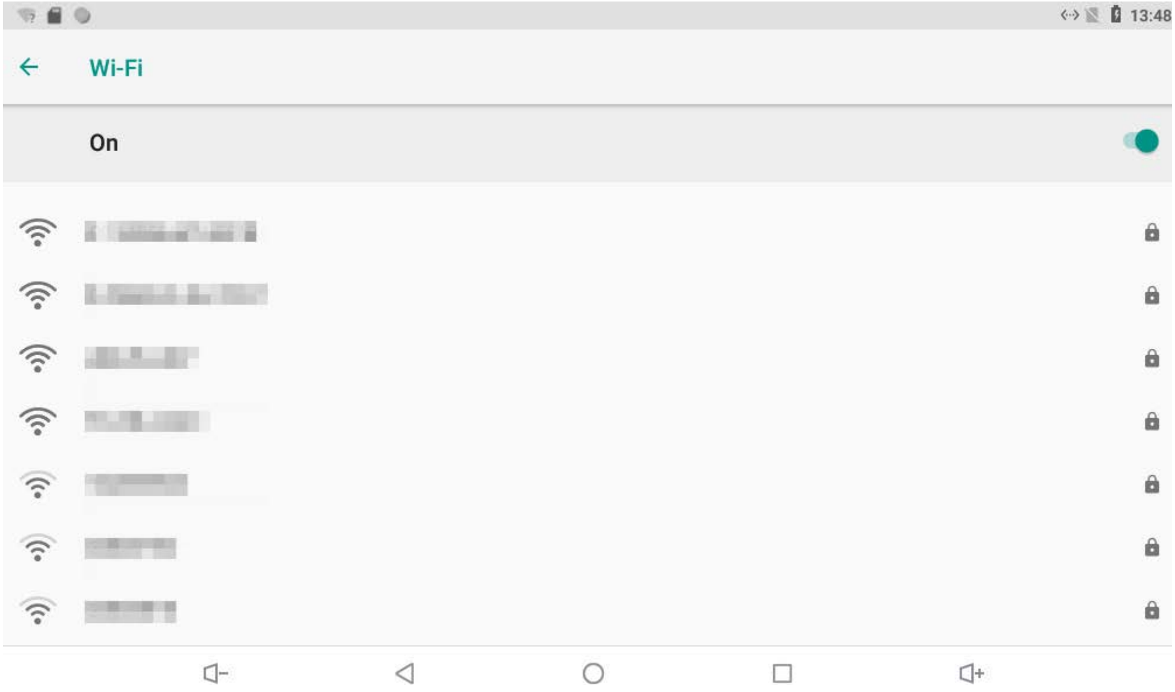
Step 1 Tap the **Settings** icon.

Step 2 Tap Network & Internet.

Step 3 Tap ○, the Wi-Fi is enabled.

Step 4 Tap ▼, the available wireless networks are displayed.

Figure 3-12 Wi-Fi



Step 5 Select a wireless network.

Step 6 Enter the password.

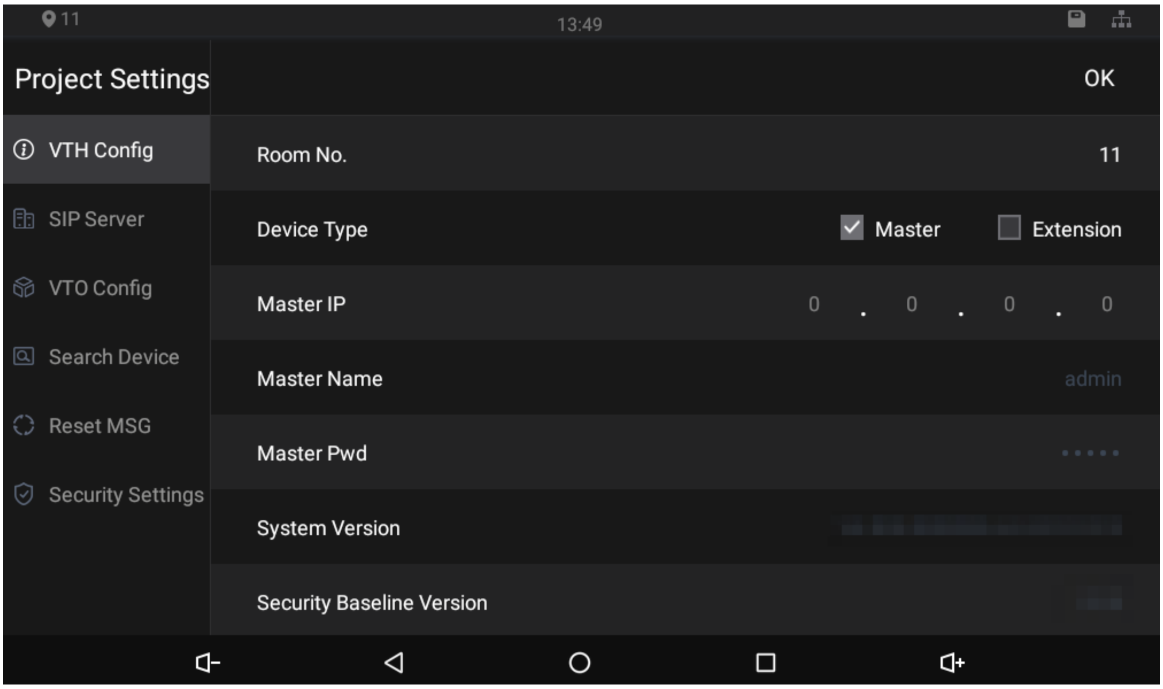
Step 7 Tap CONNECT.

The network is connected.

### 3.3.3 Project Settings

Tap and hold 🔧, enter the password (the password set during initialization), and then the **Project Settings** interface will be displayed.

Figure 3-13 Project settings



| | |
|---|---|
| Room No. | 11 |
| Device Type | ☑ Master □ Extension |
| Master IP | 0 . 0 . 0 . 0 |
| Master Name | admin |
| Master Pwd | ••••• |
| System Version | |
| Security Baseline Version | |

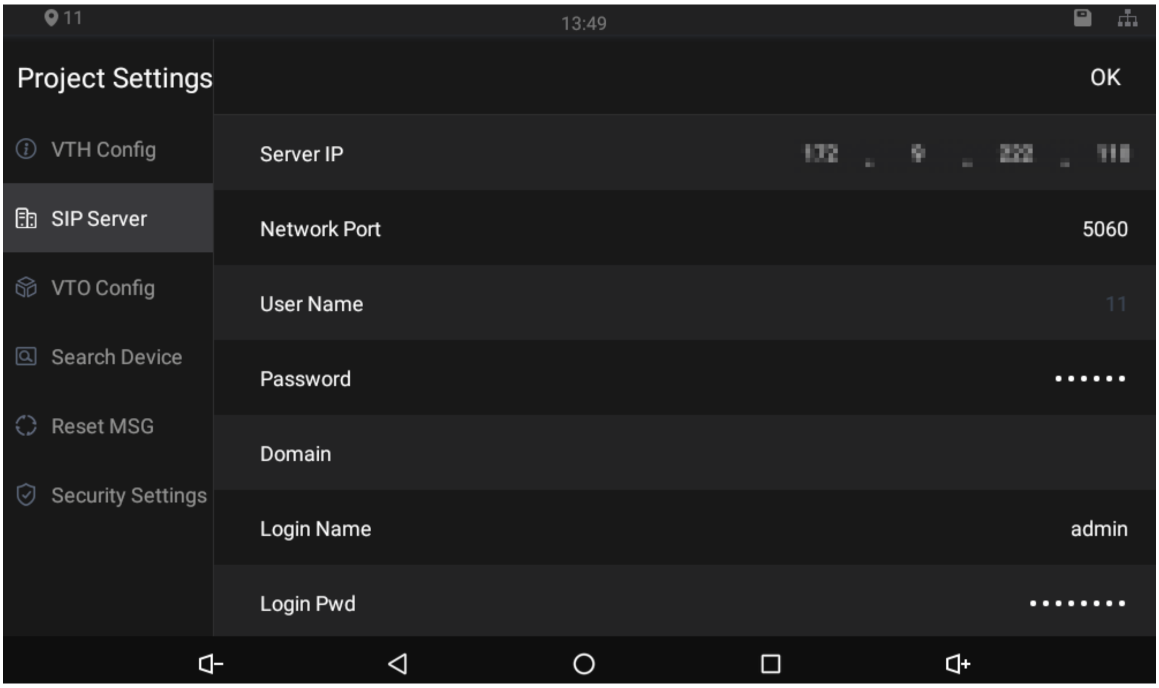
### 3.3.3.1 VTH Config

- Room No.: Number of the room where the indoor monitor is installed.
- Device Type: There are two options: **Master** and **Extension**.
  - ◇ Master: If the indoor monitor that you are operating works as the master station, you need to select **Master**.
  - ◇ Extension: If the indoor monitor works as an extension, you need to select Extension.
- Master IP: When the indoor monitor works as an extension, you need to enter IP address of the master station.
- Master Name: Keep the default value.
- Master Pwd: The password you set during initialization (6 characters).
- System Version: You can view system version of the indoor monitor.
- Security Baseline Version: You can view security baseline version of the indoor monitor.

### 3.3.3.2 SIP Server

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

Figure 3-14 SIP server (1)



Server IP [redacted]
Network Port 5060
User Name 11
Password ••••••
Domain
Login Name admin
Login Pwd •••••••••

Table 3-3 SIP server description

| Parameter | Description |
|---|---|
| Server IP | ● When the platform works as SIP server, server IP is IP address of the management platform.<br>● When a door station works as SIP server, server IP is IP address of the door station. |
| Network Port | ● When the platform works as SIP server, network port is 5080.<br>● When VTO works as SIP server, network port is 5060. |
| User Name | Keep default value. |

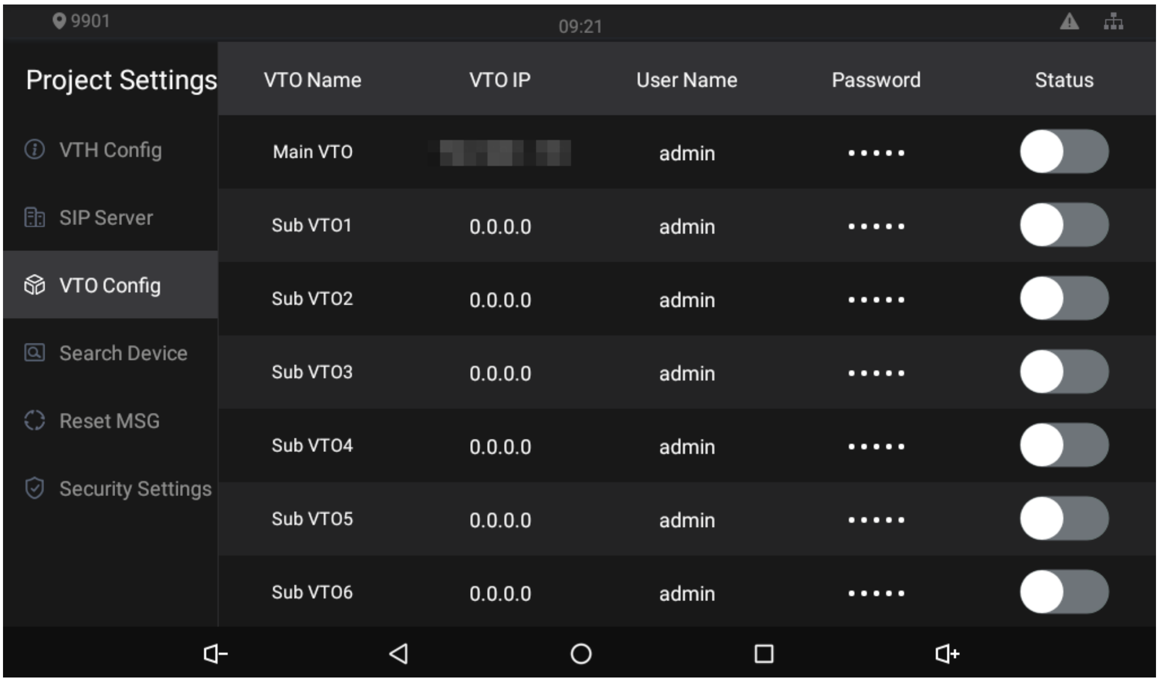
| Parameter | Description |
|---|---|
| Password | |
| Domain | Registration domain of SIP server, which can be null.<br>When VTO works as SIP server, registration domain of SIP server shall be VDP. |
| Login Name | Username and password to log in to web of the SIP server. |
| Login Pwd | |
| Status | Enable the SIP server status, and then the SIP server can start to work. |

### 3.3.3.3 VTO Config

You need to add door stations to the indoor monitor, and then calls can be made among door stations and indoor monitors.

Step 1 Tap VTO Config,

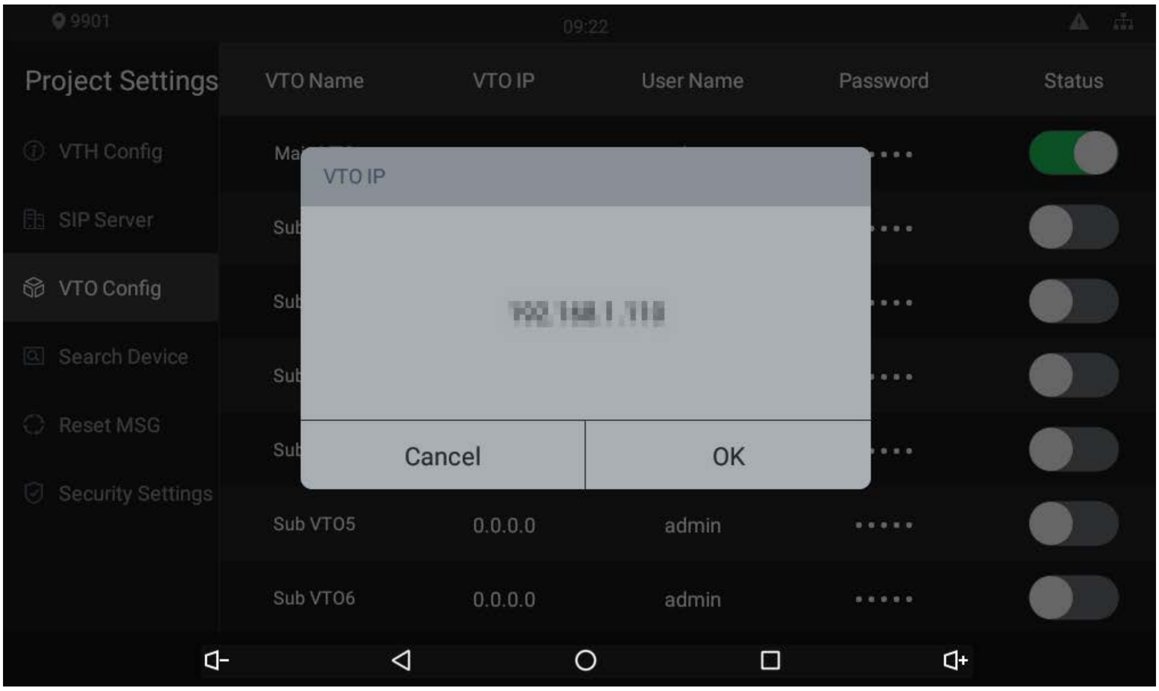
Figure 3-15 Door station (VTO) configuration



| VTO Name | VTO IP | User Name | Password | Status |
|---|---|---|---|---|
| Main VTO | [redacted] | admin | •••••• | ○ |
| Sub VTO1 | 0.0.0.0 | admin | •••••• | ○ |
| Sub VTO2 | 0.0.0.0 | admin | •••••• | ○ |
| Sub VTO3 | 0.0.0.0 | admin | •••••• | ○ |
| Sub VTO4 | 0.0.0.0 | admin | •••••• | ○ |
| Sub VTO5 | 0.0.0.0 | admin | •••••• | ○ |
| Sub VTO6 | 0.0.0.0 | admin | •••••• | ○ |

Step 2 Tap a door station (VTO).

Figure 3-16 VTO IP



| VTO Name | VTO IP | User Name | Password | Status |
|---|---|---|---|---|
| Sub VTO5 | 0.0.0.0 | admin | ••••• | |
| Sub VTO6 | 0.0.0.0 | admin | ••••• | |

Step 3 Tap the default IP.

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

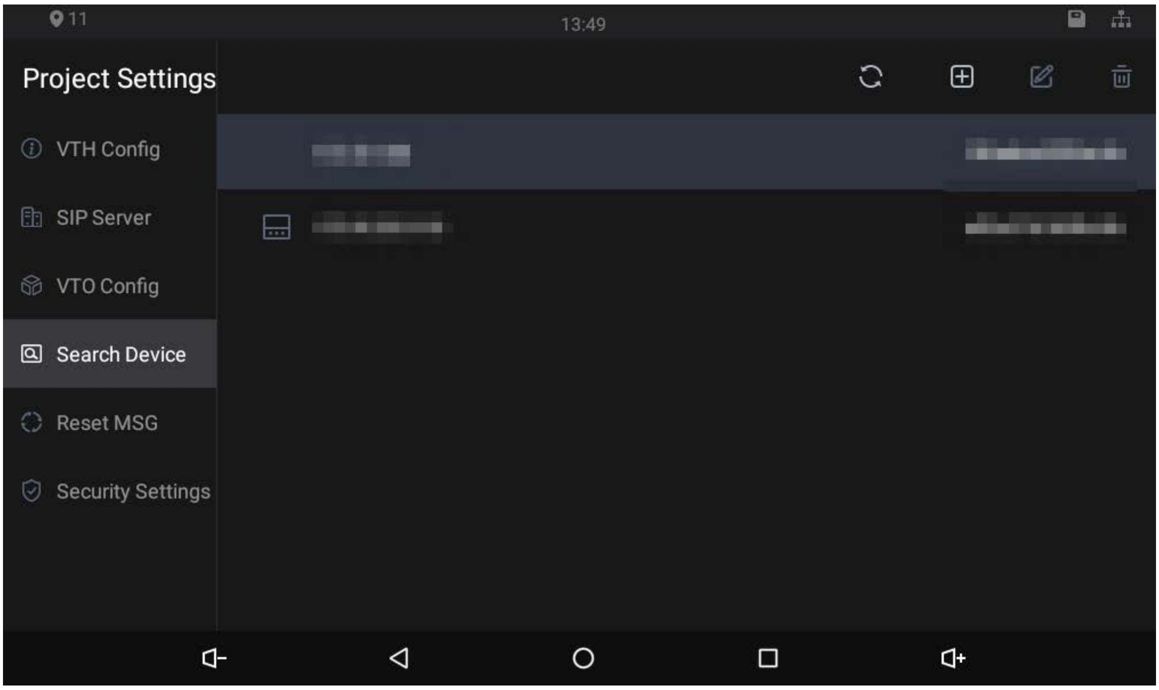
- You can add 20 door stations (one main door station and 19 sub door stations) to the indoor monitor.
- Make sure that user name and password that you entered here are the same as the user name and password used when logging in to the door station web interface.

Step 5 Tap ○ to enable the door station.

## 3.3.3.4 Searching Device

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

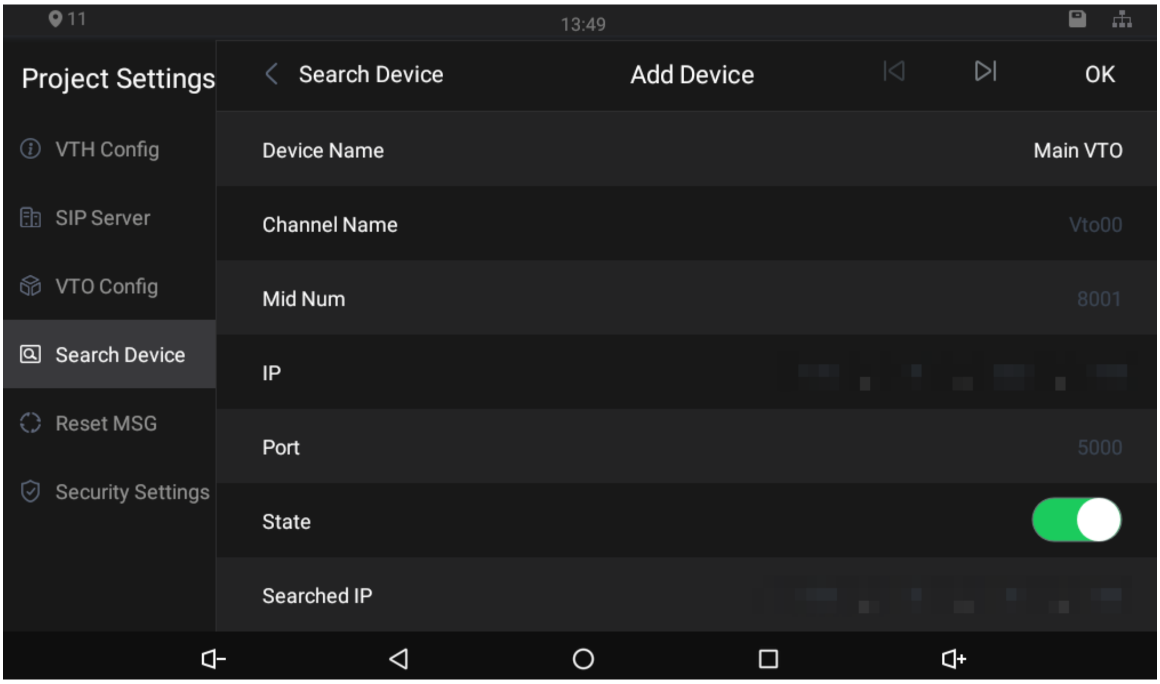
Figure 3-17 Searching device (1)



[redacted] [redacted]

[redacted] [redacted]

Figure 3-18 Searching device (2)



Device Name Main VTO

Channel Name Vto00

Mid Num 8001

IP [redacted]

Port 5000

State

Searched IP [redacted]

### 3.3.3.5 Resetting Password

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

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

Step 1 Tap and hold 🔧.

Step 2 Tap Forgot password?.

Step 3 Tap **OK**.

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

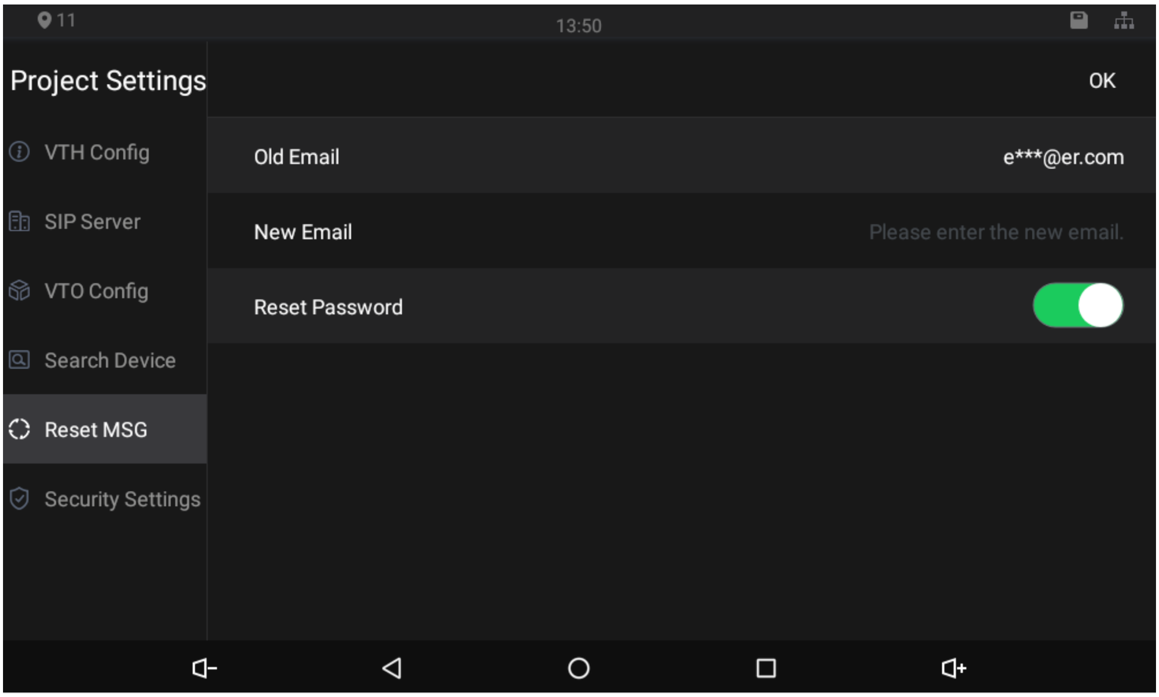
Step 5 Send the string to the email address displayed on your device interface with the email address you set on the **Reset MSG** interface.

A safe number will be sent to your email address.

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

The password is reset.

Figure 3-19 Reset password



Project Settings

OK

Old Email e***@er.com

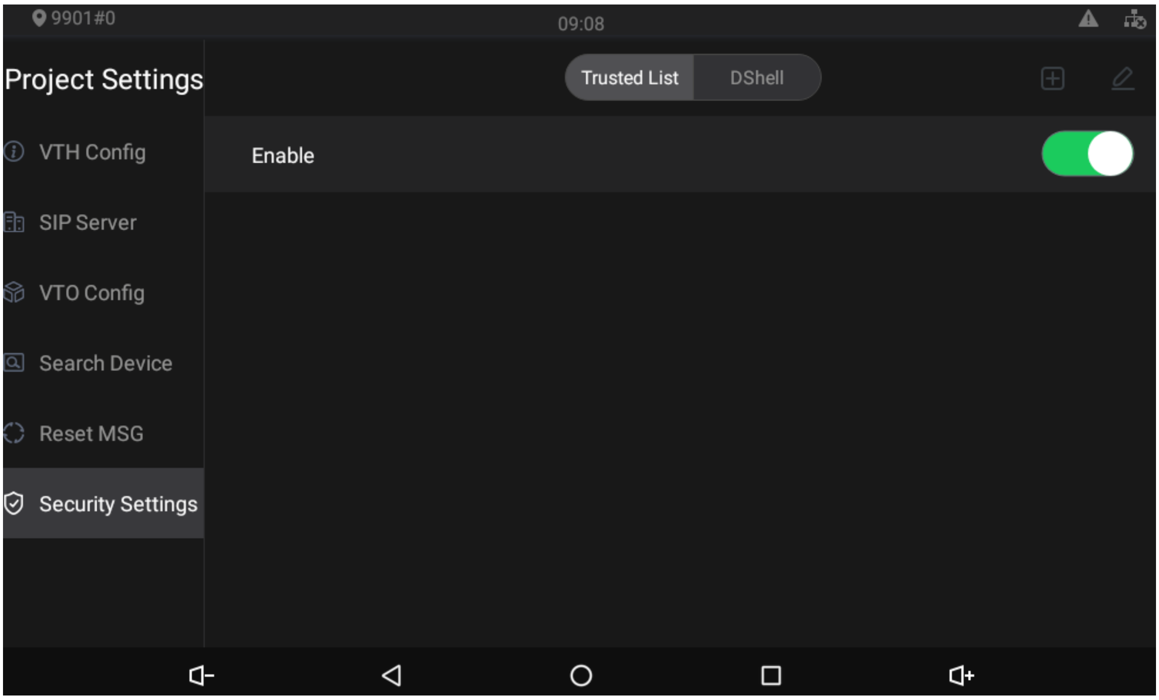
New Email Please enter the new email.

Reset Password

### 3.3.3.6 Security Settings

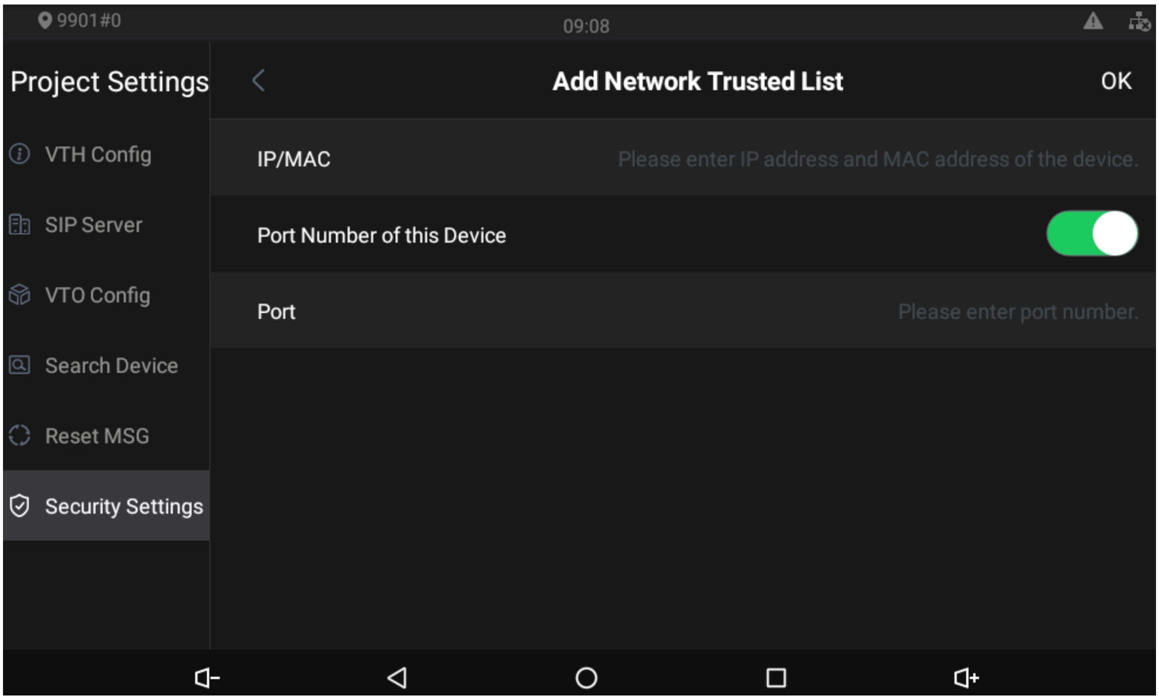
You need to enable the trusted list, and then trusted devices can communicate with the indoor monitor. You can also use Dshell to get the ability to develop custom analysis modules which help you understand events of cyber intrusion.

Figure 3-20 Enable trusted list



Enable: on

Figure 3-21 Add network trusted list



IP/MAC: Please enter IP address and MAC address of the device.

Port Number of this Device: on

Port: Please enter port number.

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

## 3.4 Unlocking

You can unlock doors connected to the door stations through the indoor monitor when watching monitoring videos, when someone is calling you from the door station, or when talking to the people at the door station over the indoor monitor.

# 3.5 Commissioning

## 3.5.1 Watching Monitoring Videos

Tap 📹, and the **Monitor** interface is displayed.

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

During the call with a door station, you can watch the real-time videos capture by door stations or IP cameras.

Figure 3-22 Monitor (1)

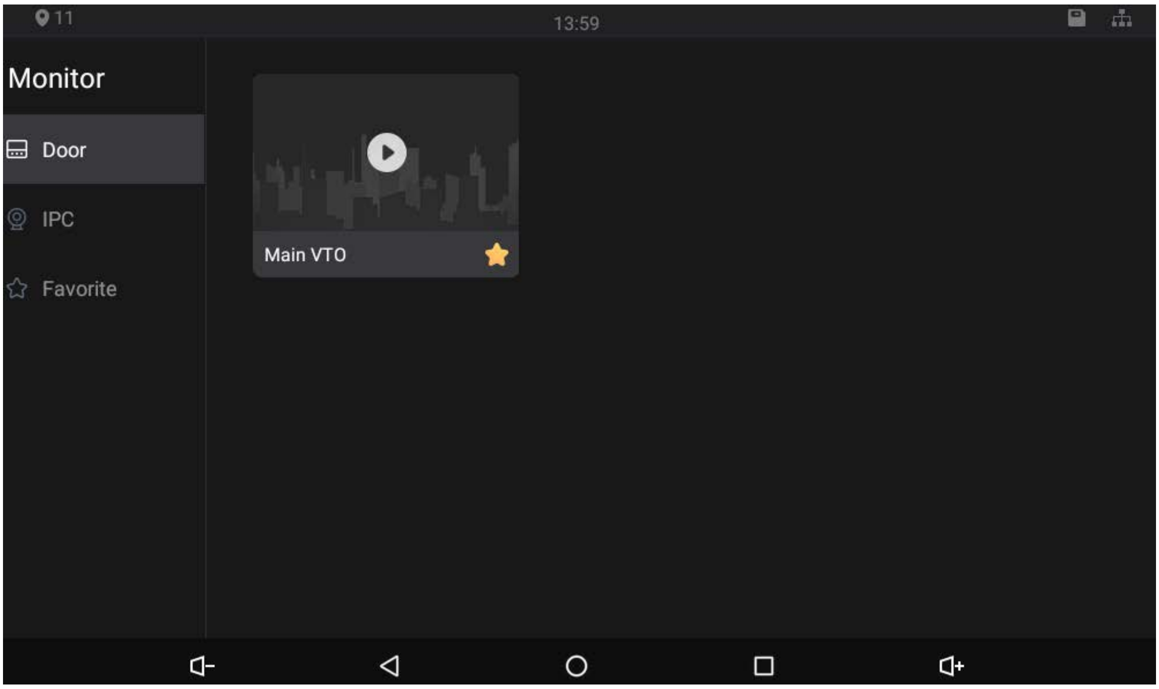


Figure 3-23 Monitor (2)

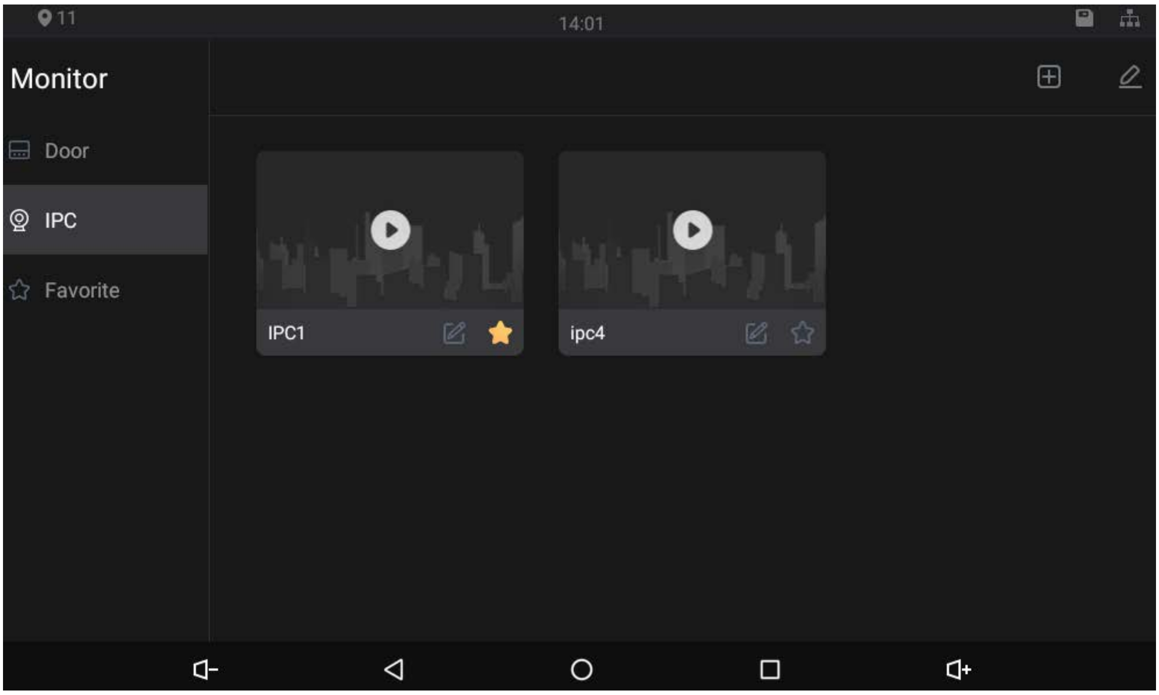
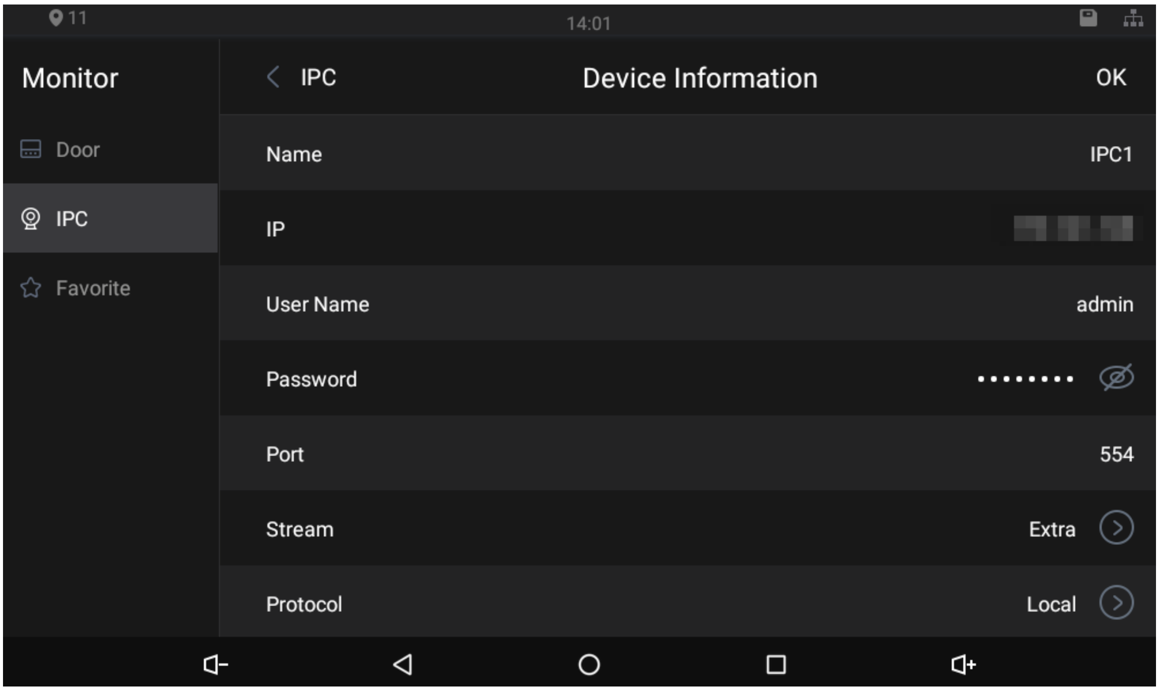


Figure 3-24 IPC information



Device Information OK

| | |
|---|---|
| Name | IPC1 |
| IP | [redacted] |
| User Name | admin |
| Password | ••••••••• |
| Port | 554 |
| Stream | Extra |
| Protocol | Local |

- 🔉: Turn down the volume.
- ◁: Go to the previous page.
- ○: Go to the main menu.
- □: All thumbnails of interfaces you have opened will be displayed. Select an interface and slide it to the left or right to close the interface.
- 🔊: Turn up the volume.

### 3.5.2 Making Calls

Tap ☎, and then you can call other indoor monitors and the management center; and you can also view call logs and your contacts on this interface. You can also call the indoor monitor from door stations.

Figure 3-25 Making calls

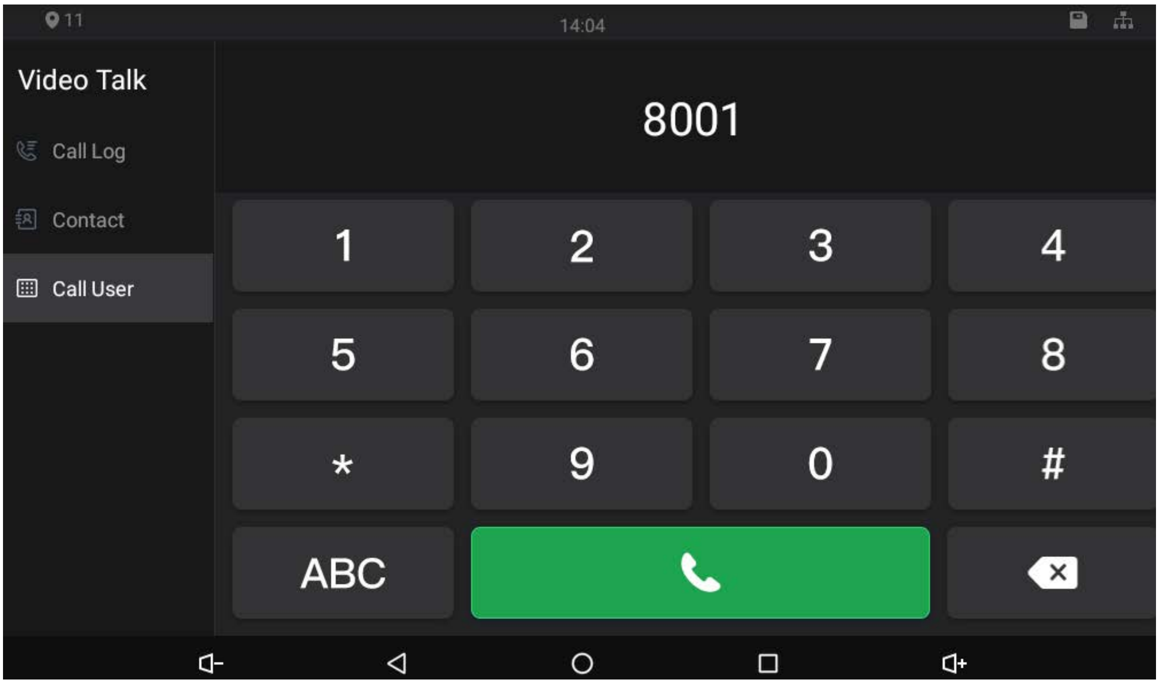
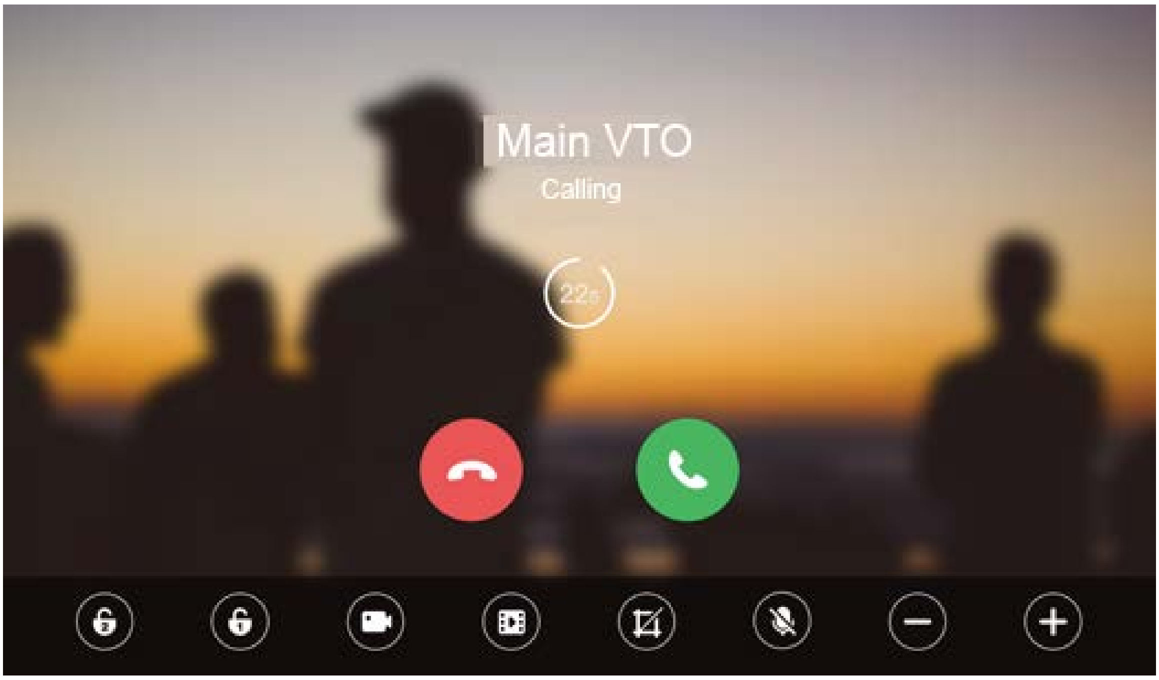


Figure 3-26 Calling



- If SD card is not inserted, the video recording icon and snapshot icon cannot be used.
- You can tap the unlock icon / to unlock doors. If the icons turn grey, the unlock function cannot be used.

## Call Residents through Dialing Numbers

Step 1 Tap ☎.

Step 2 Tap Call User.

Step 3 Enter room number (room number you entered in the indoor monitor), and then tap 📞.

- If door station (VTO) works as SIP server, enter a room number.
- If management platform like DSS Pro or DSS Express works as SIP server.
  - ◇ Call residents in your apartment or your building, enter a room number.
  - ◇ Call residents in other apartments and buildings, enter 1#1#101 for apartment 1 building 1 room 101.

    🕮

    - If you call the extensions (101#1) from the main indoor monitor (101#0), just enter -1.
    - If you call the main indoor monitor from the extensions, just enter -0.

## Call Residents through Contacts

You can also call residents through contacts.

## Call through Call Logs

You can make calls through tapping call records.

# Appendix 1 Cybersecurity Recommendations

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

**Mandatory actions to be taken for basic device 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 device 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.