

IP Indoor Monitor

Quick Start Guide





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

Foreword	I
Important Safeguards and Warnings	II
1 Introduction	1
1.1 Overview	1
1.2 Front Panel.....	1
1.3 Rear Panel	3
1.4 Cable Connection	4
2 Network Diagram	5
3 Configuration	6
3.1 Configuration Process	6
3.2 VDPCongig.....	6
3.3 Configuring Indoor Monitor	6
3.3.1 Initialization	6
3.3.2 Network Settings	12
3.3.3 Project Settings.....	15
3.4 Unlocking.....	21
3.5 Commissioning	22
3.5.1 Watching Monitoring Videos	22
3.5.2 Making Calls.....	23
Appendix 1 Cybersecurity Recommendations	26

1 Introduction

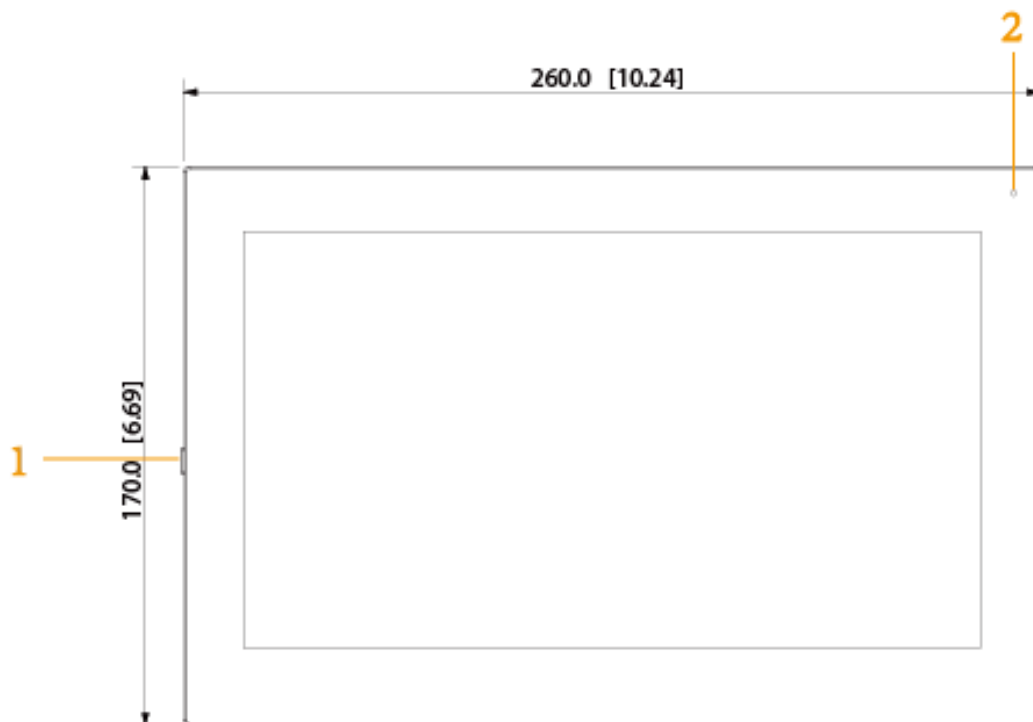
1.1 Overview

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)]

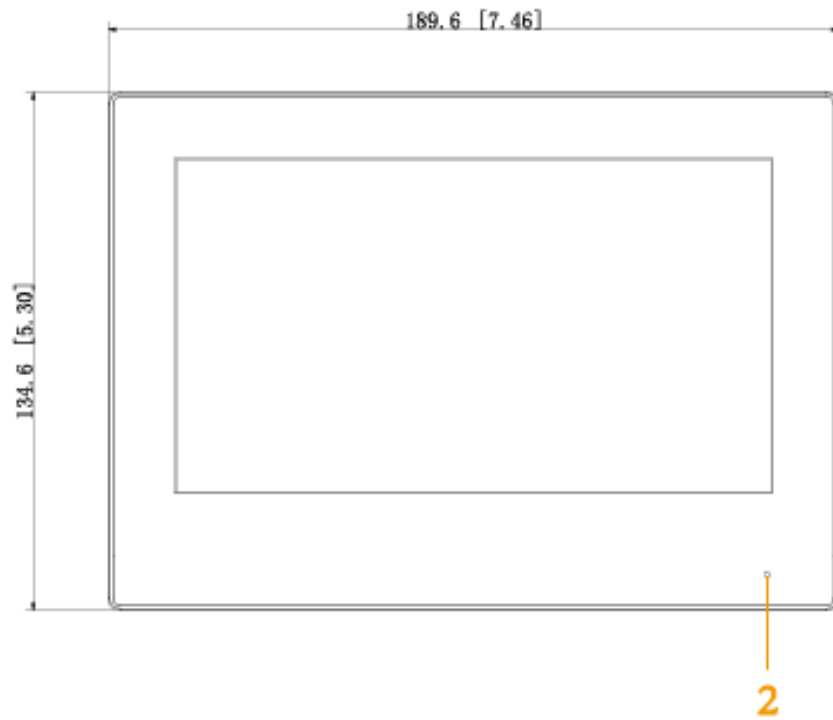


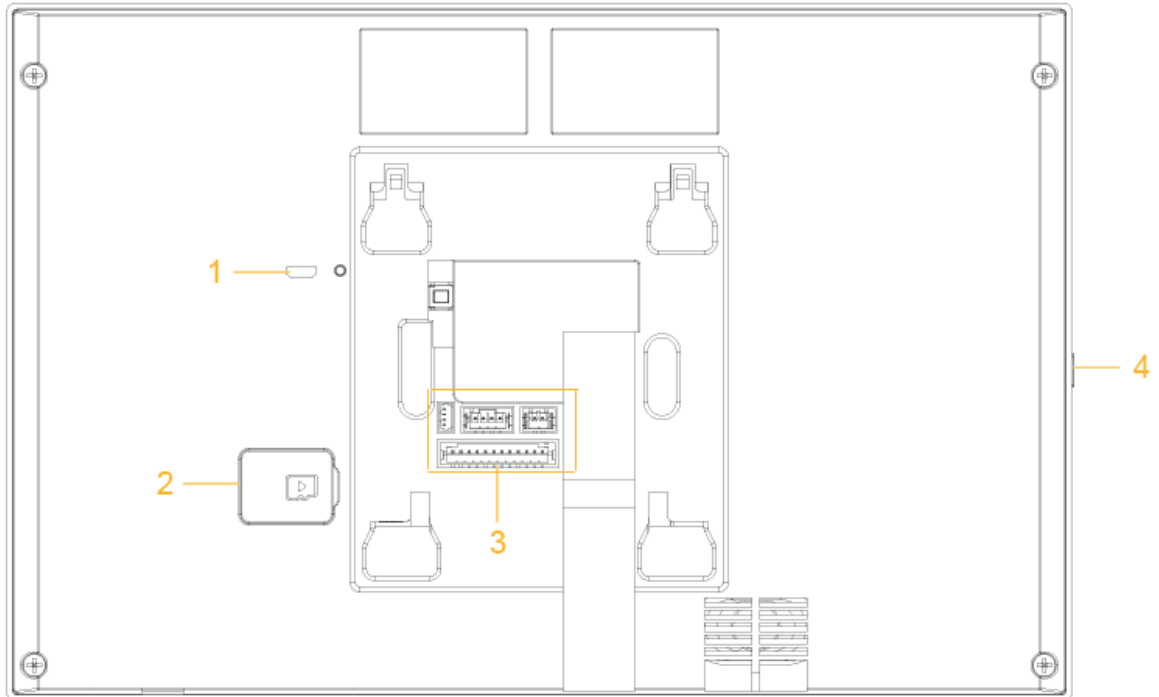
Table 1-1 Components

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

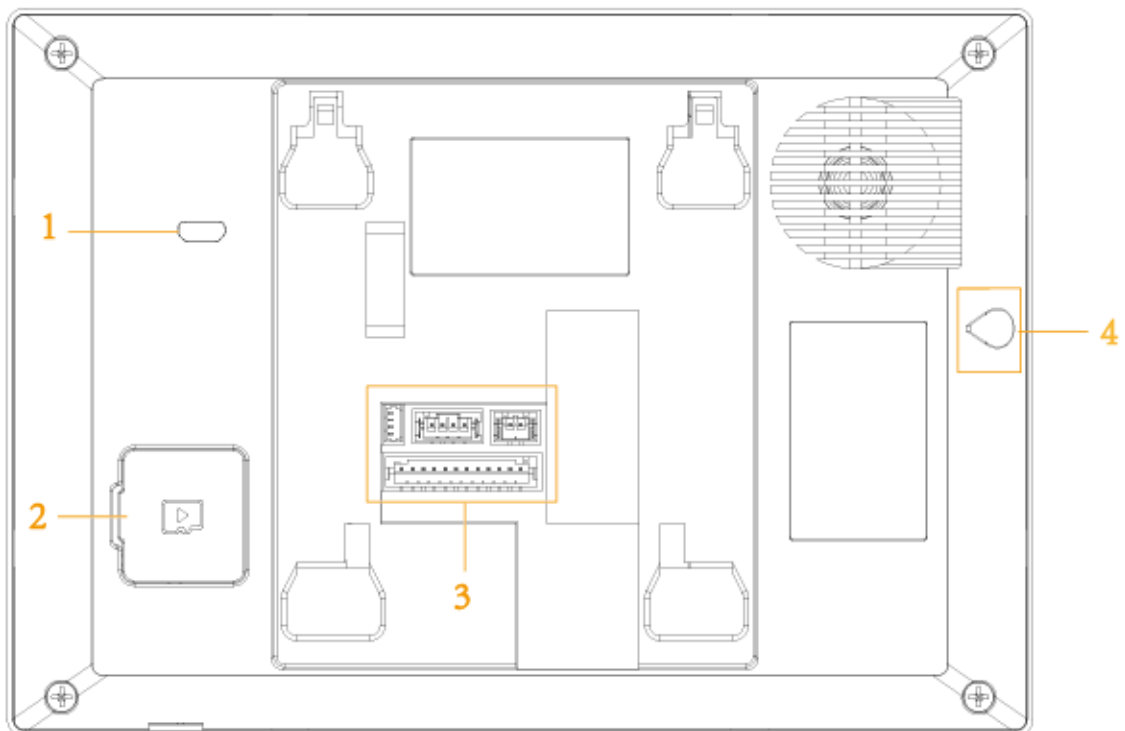
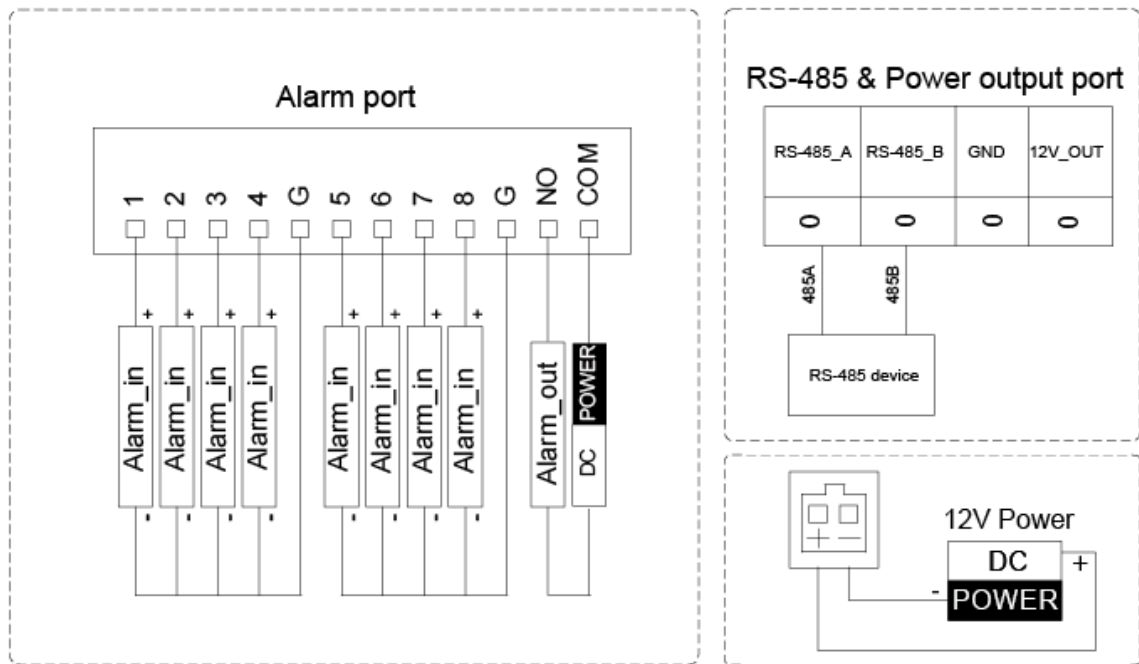


Table 1-2 Rear panel description

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.

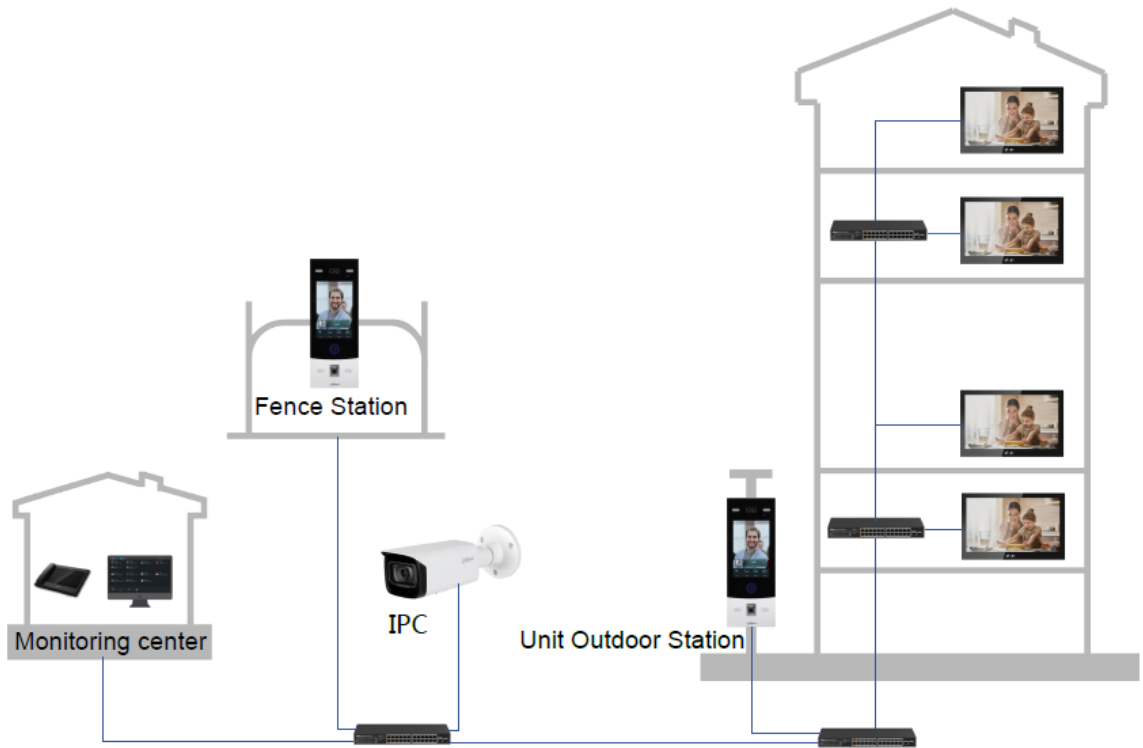
1.4 Cable Connection

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.

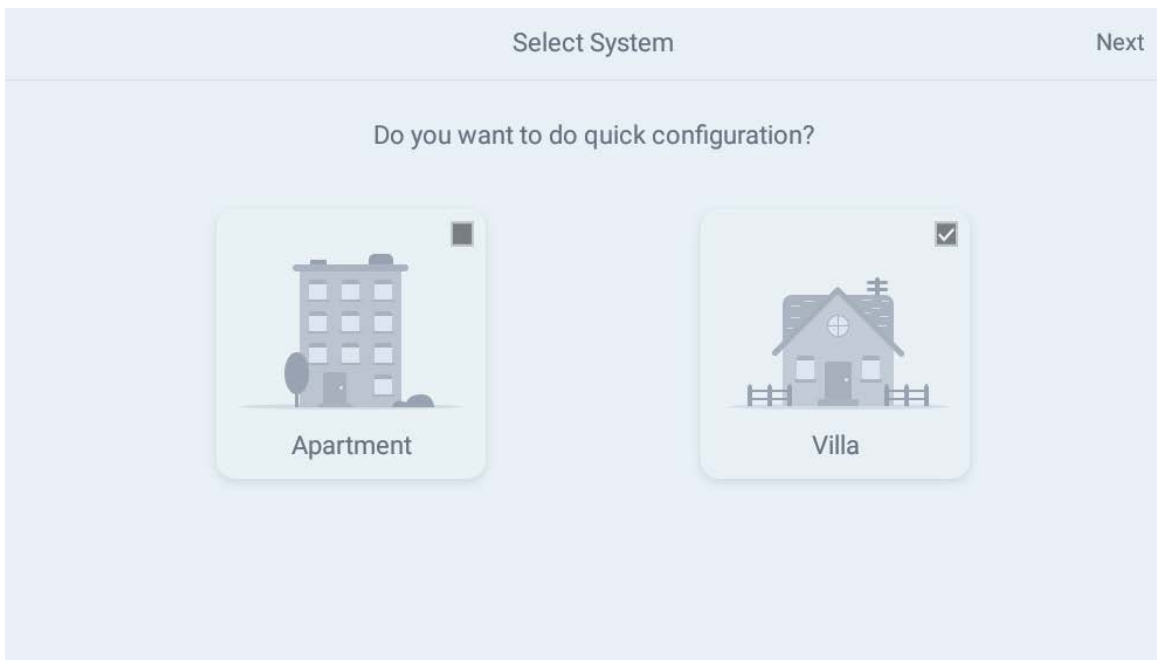
Figure 3-1 Select a language



Step 2 Select a language that you prefer.

Step 3 Tap **OK**.

Figure 3-2 Select apartment or 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			Refresh	Next
Device Type	SN	MAC	IP	Status	Operation	
Local	5L04270YAZD088F	a0:bd:1d:ee:59:b4	192.168.1.160	Initialized	Initialize	
VTO	5L02A61PAZACDA1	08:ed:ed:20:de:59	172.9.1.136	Initialized	Initialize	
VTO	5J044DAPAZ02B87	a0:bd:1d:a8:2a:3a	172.9.2.121	Initialized	Initialize	
VTO	5G06704PAZ84EB9	a0:bd:1d:5d:8c:6b	172.9.222.110	Initialized	Initialize	
VTO	5C05DE1PAZ4DD9C	9c:14:63:99:46:99	172.9.2.130	UnInitialized	Initialize	
VTH	5L04270YAZ097DB	a0:bd:1d:ee:59:b7	192.168.1.108	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	5L04270YAZD088F	a0:bd:1d:ee:59:b4	192.168.1.160	Main	--	Edit
VTO	5L02A61PAZACDA1	08:ed:ed:20:de:59	172.9.1.136	--	--	Edit
VTO	5J044DAPAZ02B87	a0:bd:1d:a8:2a:3a	172.9.2.121	--	--	Edit
VTO	5G06704PAZ84EB9	a0:bd:1d:5d:8c:6b	172.9.222.110	--	--	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	<input checked="" type="checkbox"/> Main <input type="checkbox"/> Sub	
Local IP		172.9.1.136
Netmask		255.255.0.0
Gateway		172.9.0.1
Date Format		DD-MM-YYYY ▼
Time Format		24-HOUR ▼
Date		01-01-2000
Time		00:00:00
Video Standard	<input checked="" type="checkbox"/> PAL <input type="checkbox"/> NTSC	

Figure 3-8 VTO config (2)

Back	VTO Config	OK
Only one main VTO can be exist in the system		
Device Type	<input type="checkbox"/> Main	<input checked="" type="checkbox"/> Sub
Local IP	172.9.2.121	
Netmask	255.255.0.0	
Gateway	172.9.0.1	

- 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

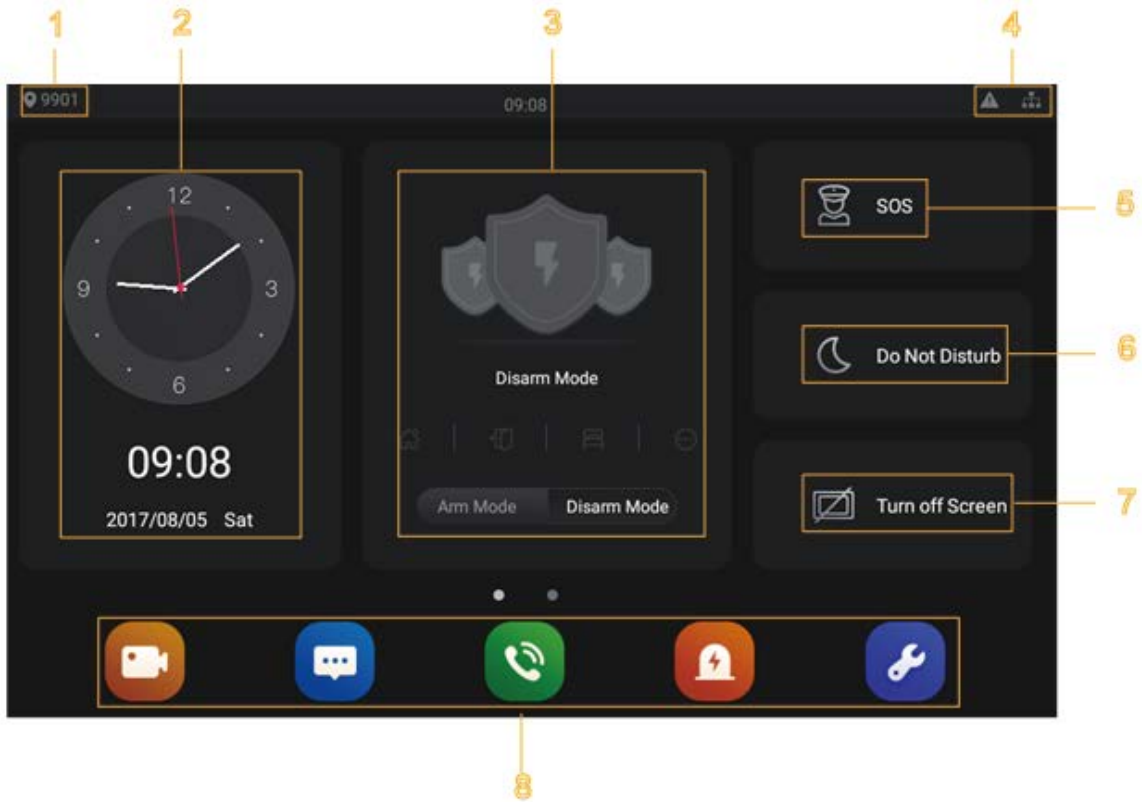









Table 3-1 Description of the main menu

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	<ul style="list-style-type: none"> ● : The wired network is not connected. ● : The wired network is connected. ● : The indoor monitor failed to be connected to the SIP server. If this icon does not appear, then the indoor monitor is connected to the SIP server. ● : The SD card is inserted and recognized. ● : The indoor monitor is in the Do not disturb mode. It is disabled by default. ● Door Status <ul style="list-style-type: none"> ◇ : Door closed. ◇ : Door open. ◇ : Unknown.

No.	Name	Description
5	SOS	Tap the SOS icon, the indoor monitor will call the management center.
6	Do not disturb	<p>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.</p> <p>For details, see DND after tapping  and entering the password (123456 by default; for password changing, see the <i>IP Indoor Monitor_User's Manual</i>).</p> <p></p> <p>It is recommended that the password be changed during the first use.</p>
7	Turn off screen	Tap the icon, and then the screen will be turned off.
8	Function buttons	<ul style="list-style-type: none"> ● : Tap the icon, and then you can watch videos from door stations and IP cameras. ● : Tap the icon, and then text messages and videos left by visitors, or public notices released by the management center will be displayed. ● : Tap the icon, and then you can make calls to other indoor monitors and the management center; and you can also view call logs and your contacts on this interface. ● : Tap the icon, and then you can view alarm logs, do alarm settings for 6 areas as needed. ● : Tap the icon, 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. ● Sound Recorder: You can record your voice messages to the SD card or to the indoor monitor. ● Calculator: You can do calculations through the calculator. ● Files: You can view files like images, videos, audio, and recently produced files. ● Calendar: You can view date through the indoor monitor, and create notes, schedules, and plans. ● Gallery: You can view images captured by door stations (VTO) or IP cameras.

3.3.2 Network Settings

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

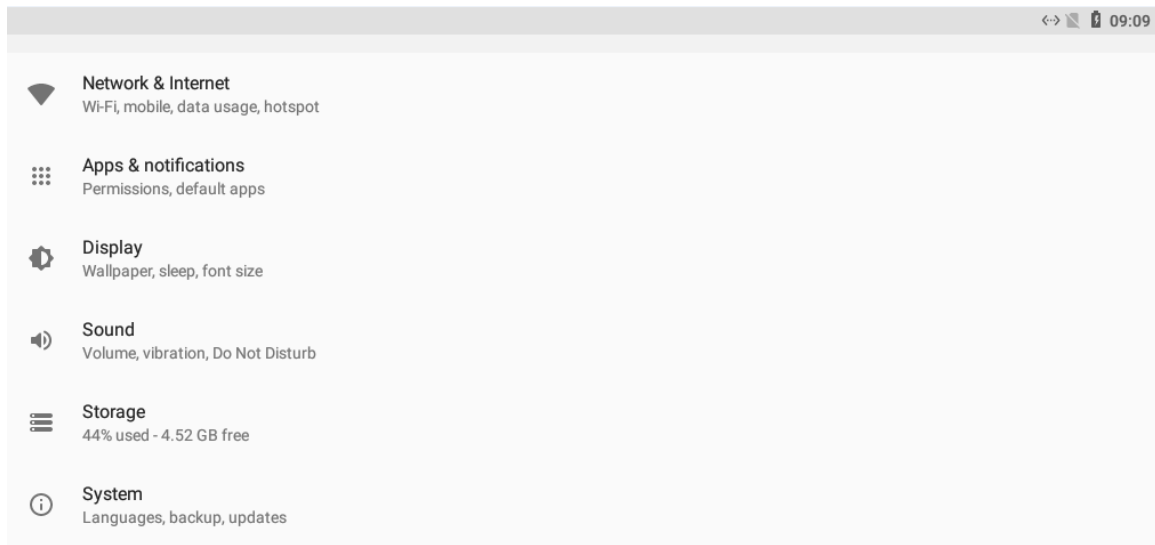
Wired Network

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



Step 3 Configure parameters.

Table 3-2 Parameter description

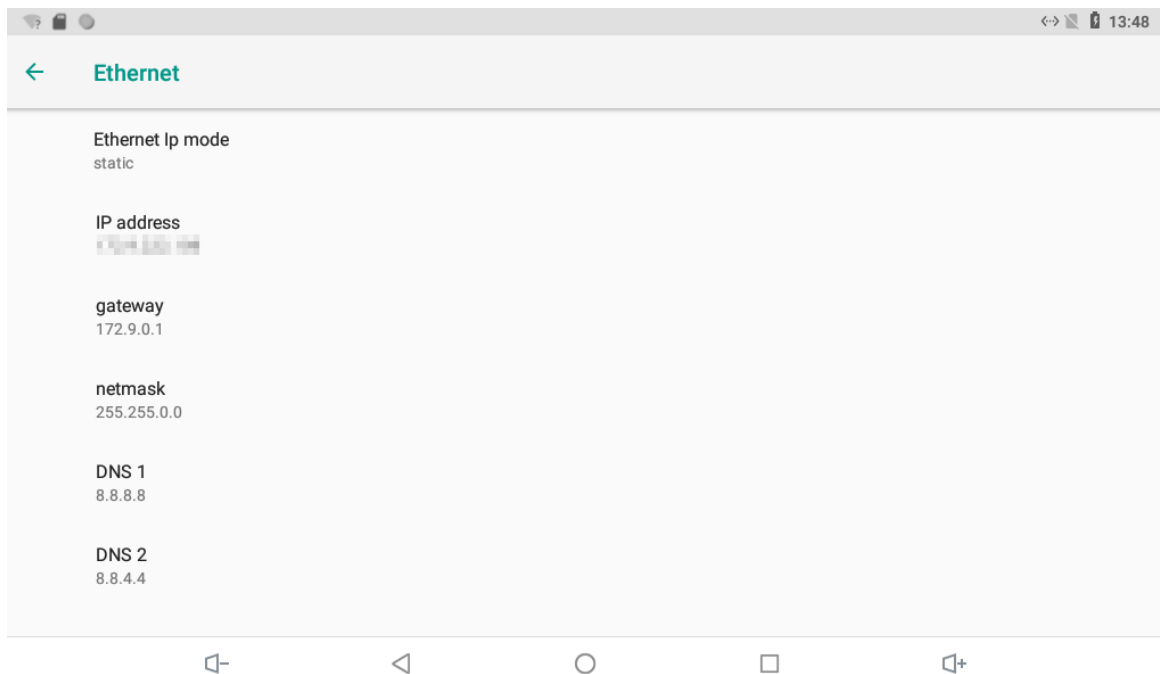
Parameter	Description	
Network & Internet	<p>You can choose to enable Wi-Fi or not by tapping .</p> <ul style="list-style-type: none"> Tap , and then available Wi-Fi networks will be displayed. You can select Ethernet IP mode. There are two options: Static and DHCP. 	
Apps & notifications	<p>You can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

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




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.


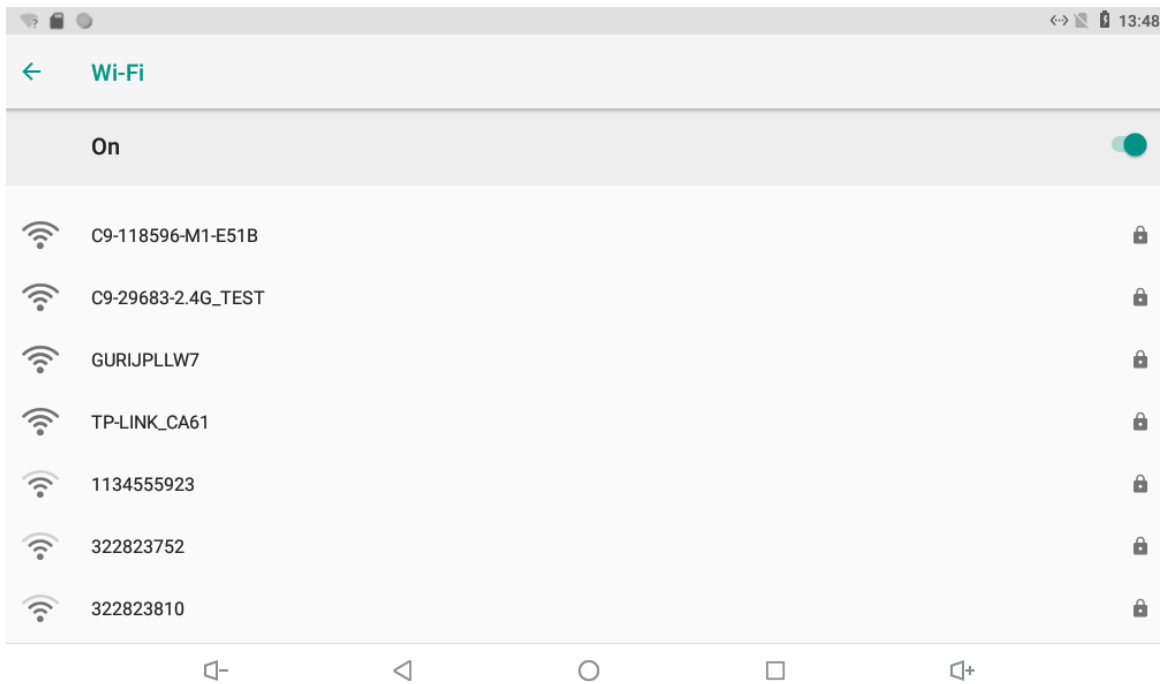
Step 4 Tap , the available wireless networks are displayed.

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


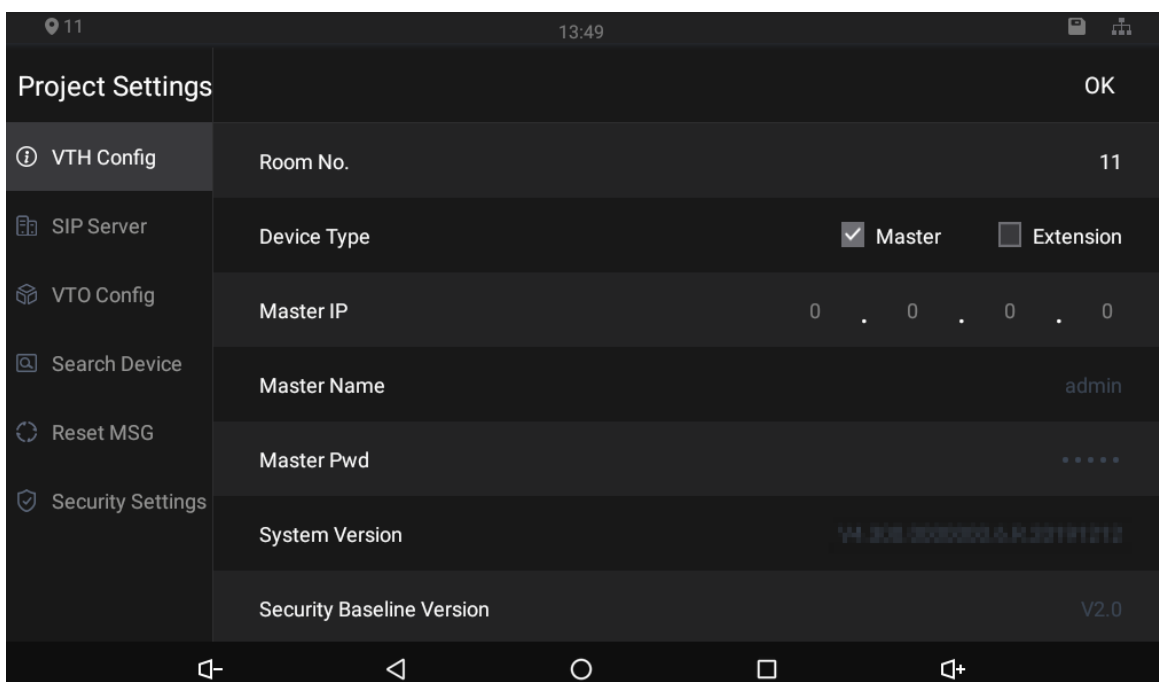
Tap and hold , enter the password (the password set during initialization), and then the **Project Settings** interface will be displayed.

Figure 3-13 Project settings



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)

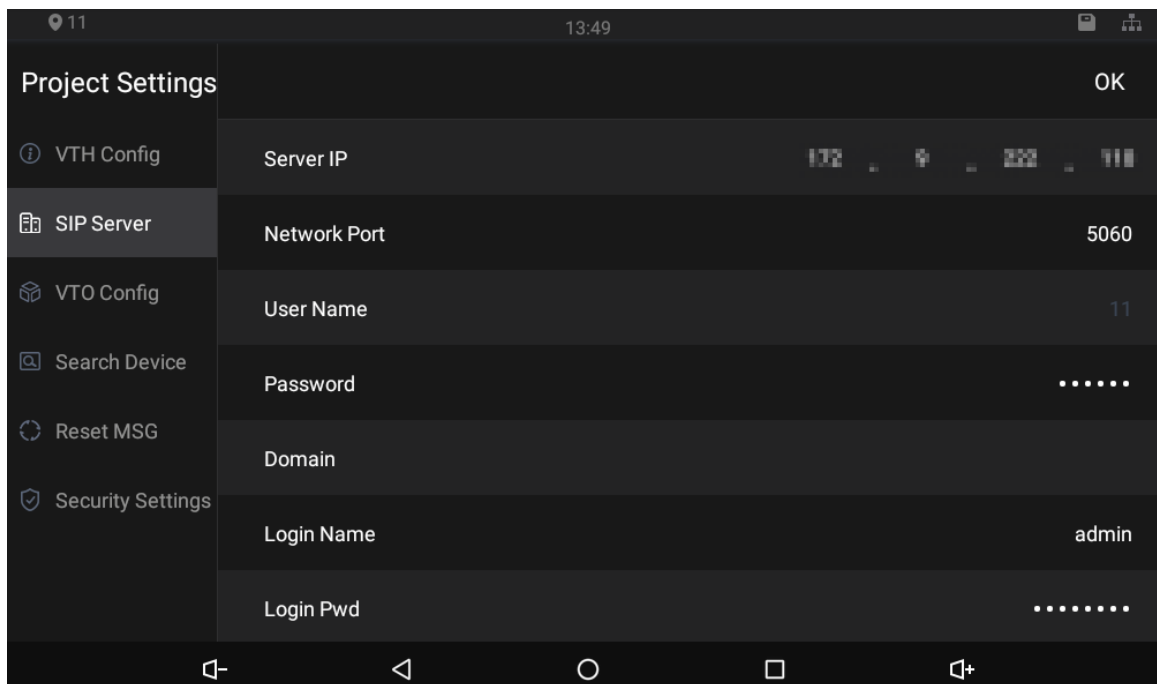


Table 3-3 SIP server description

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

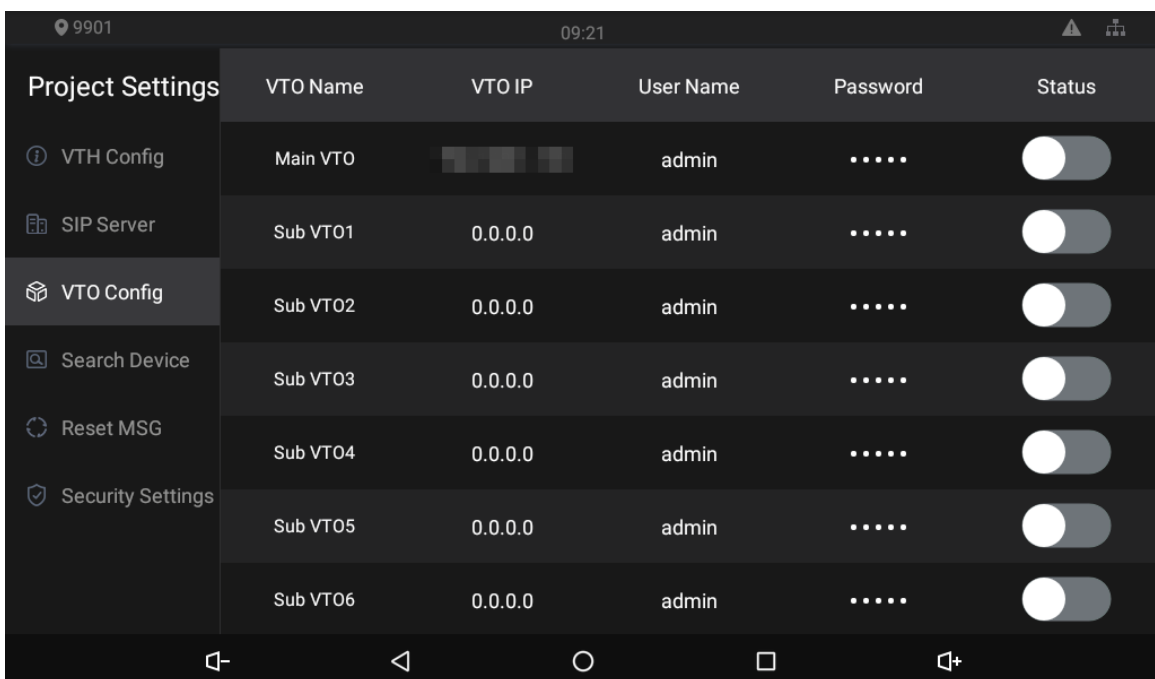
Parameter	Description
Password	
Domain	Registration domain of SIP server, which can be null. When VTO works as SIP server, registration domain of SIP server shall be VDP.
Login Name	Username and password to log in to web of the SIP server.
Login Pwd	
Status	Enable the SIP server status, and then the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

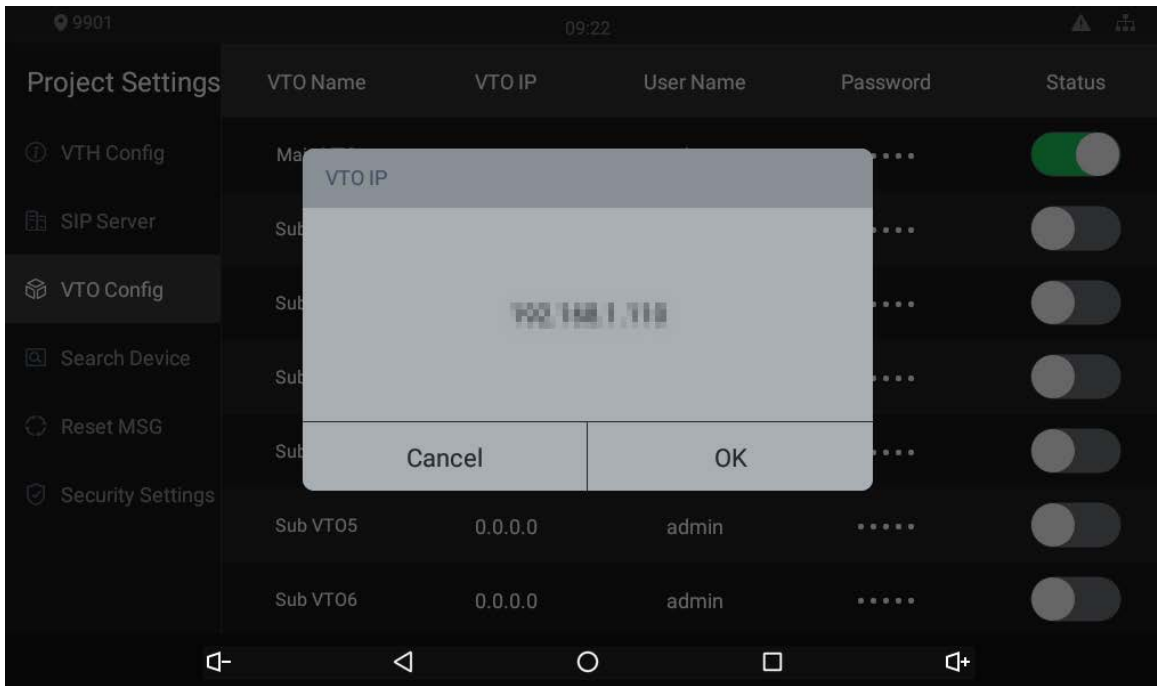
Step 1 Tap VTO Config,

Figure 3-15 Door station (VTO) configuration



Step 2 Tap a door station (VTO).

Figure 3-16 VTO IP



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)

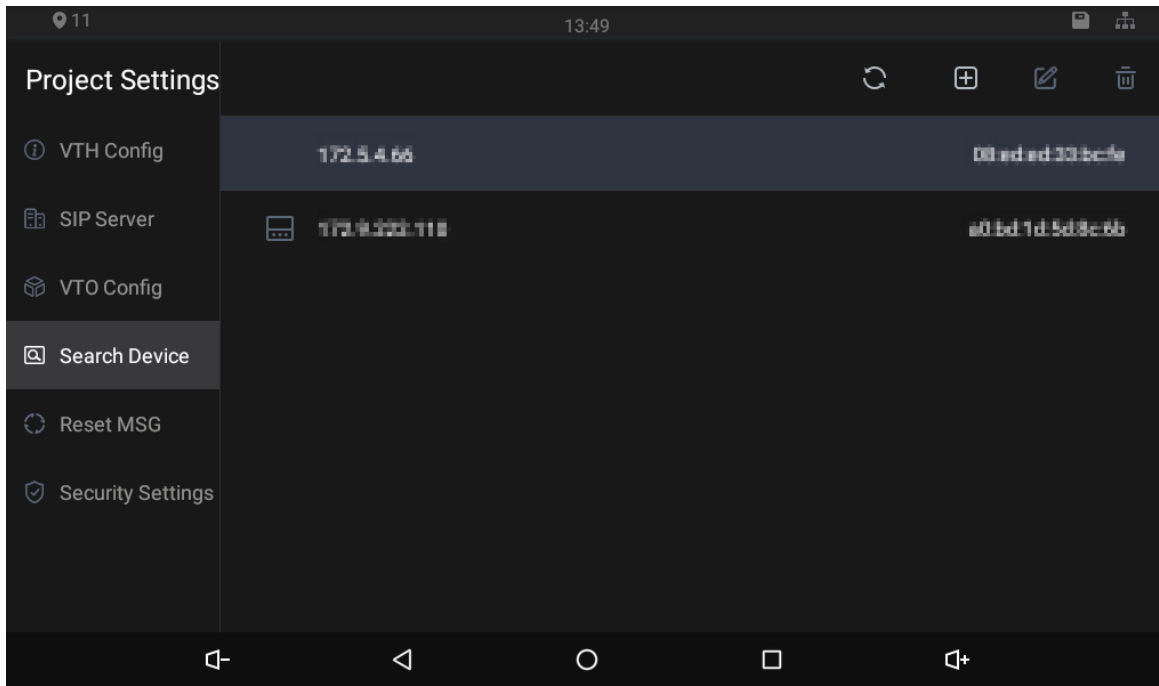
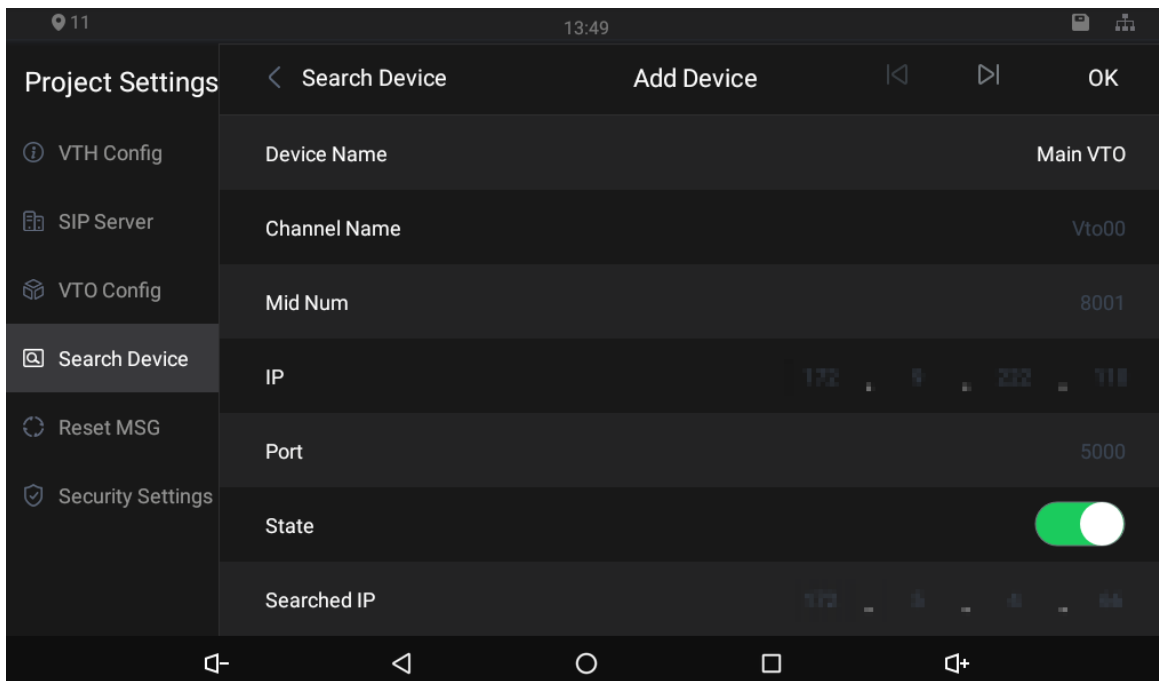


Figure 3-18 Searching device (2)




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.

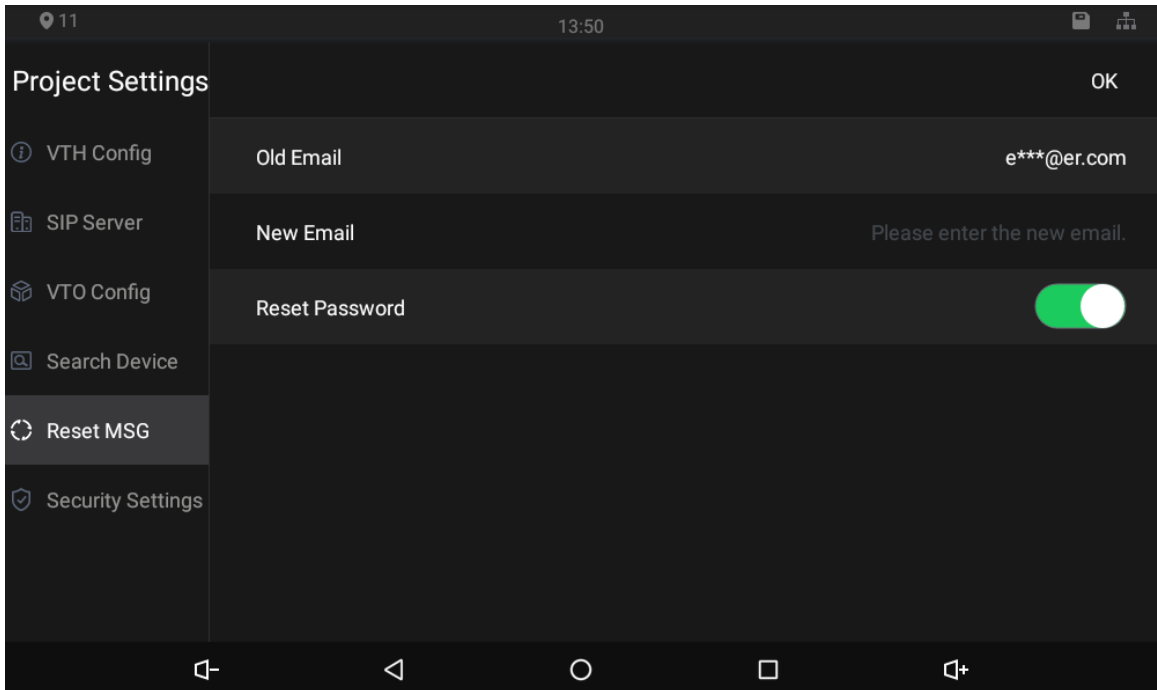
Step 5 Send the string to the email address displayed on your device interface with the email address you set on the **Reset MSG** interface.

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



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

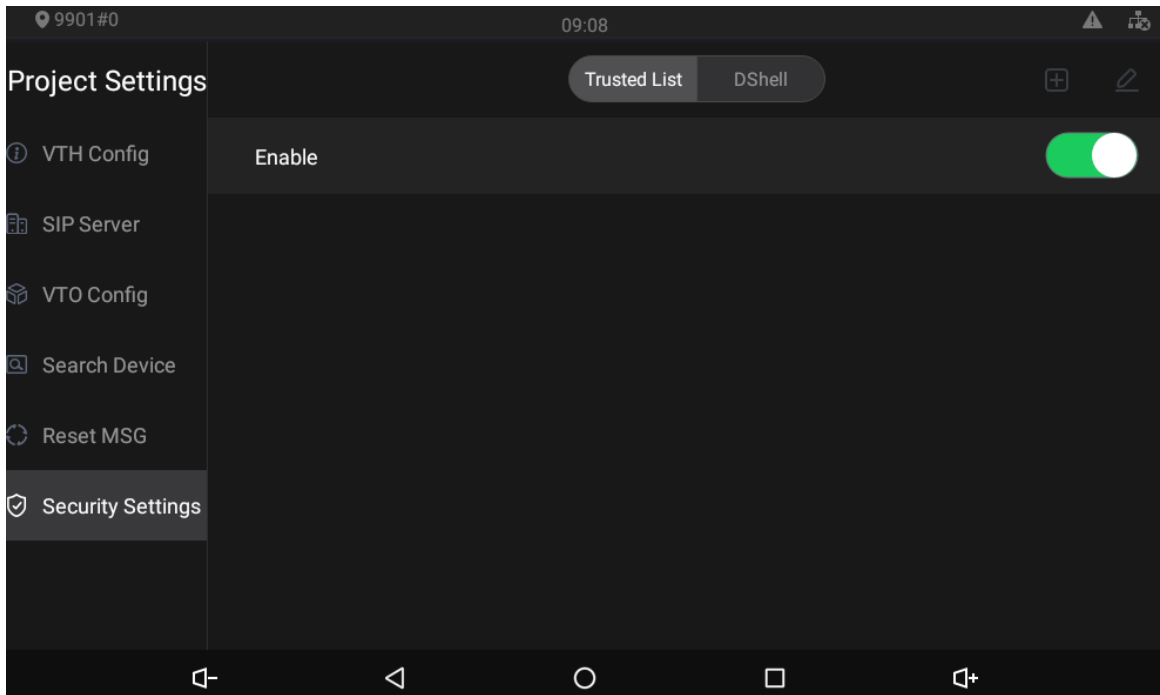
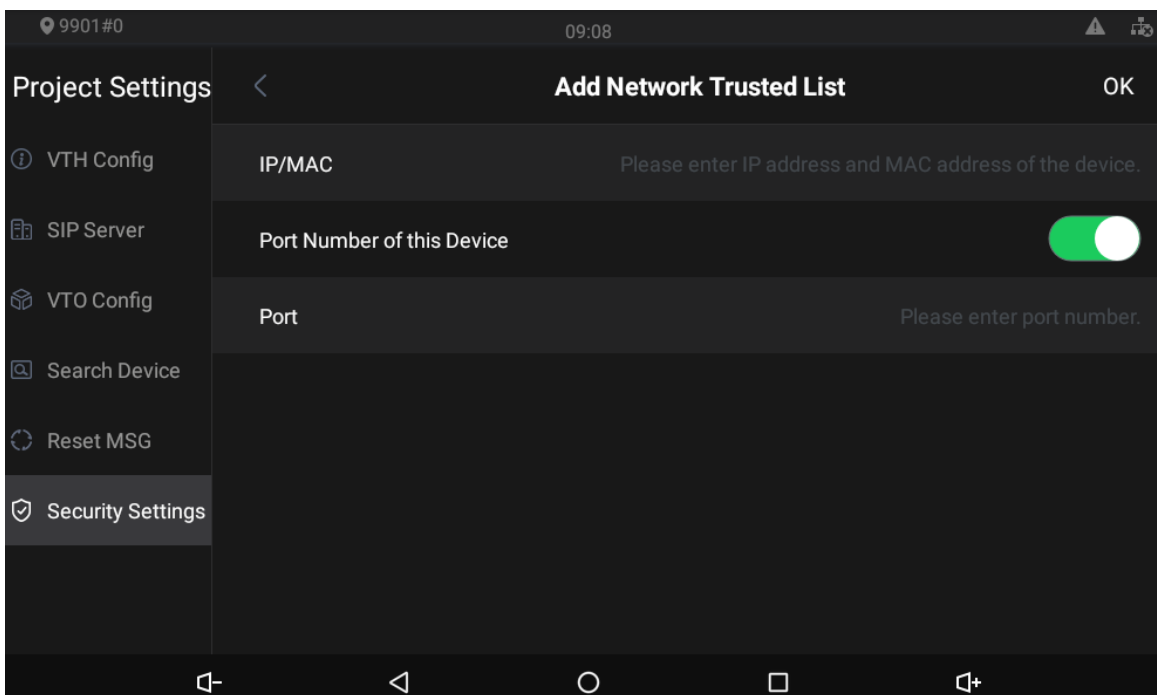



Figure 3-21 Add network trusted list



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)

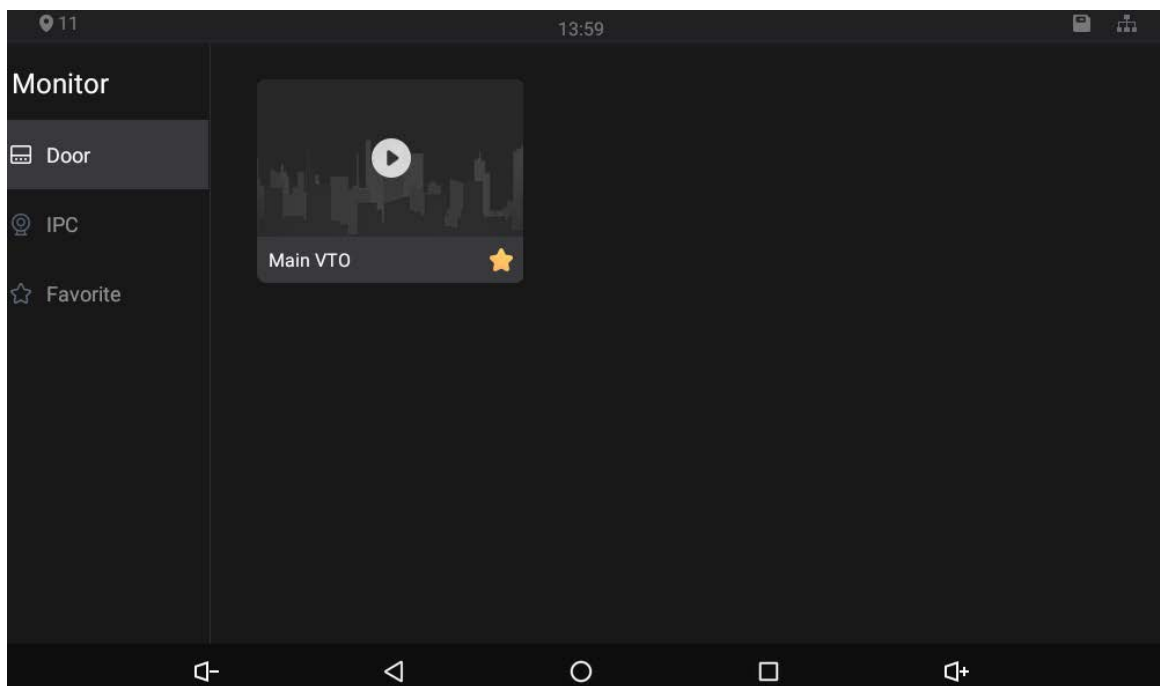


Figure 3-23 Monitor (2)

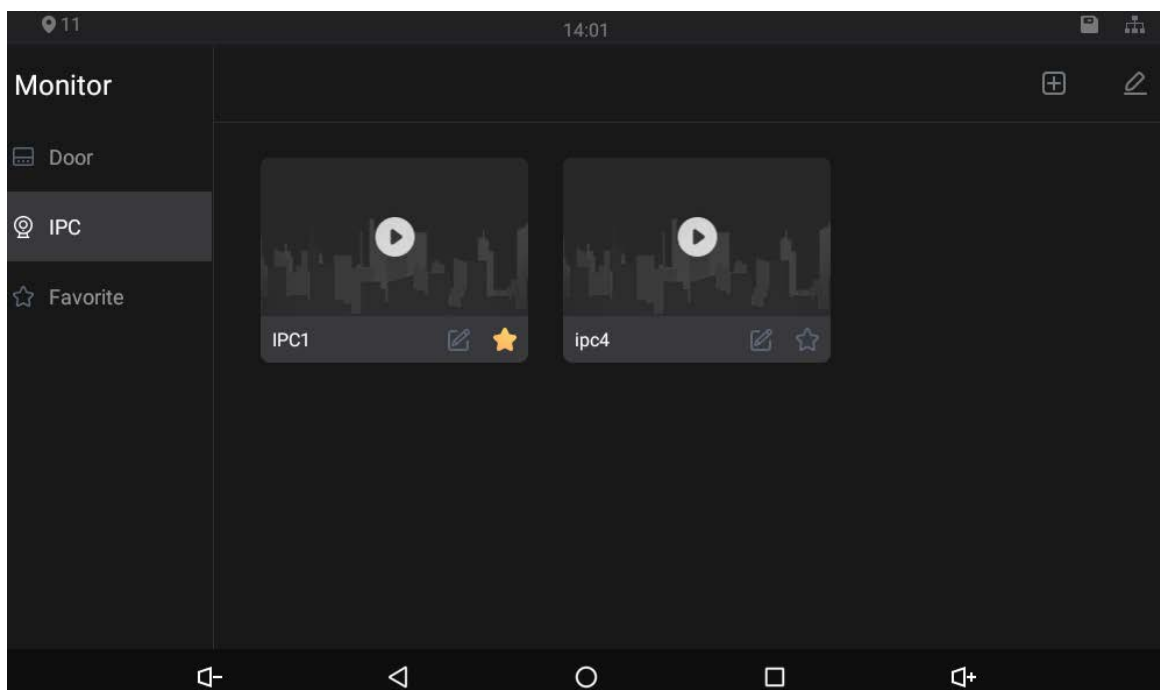
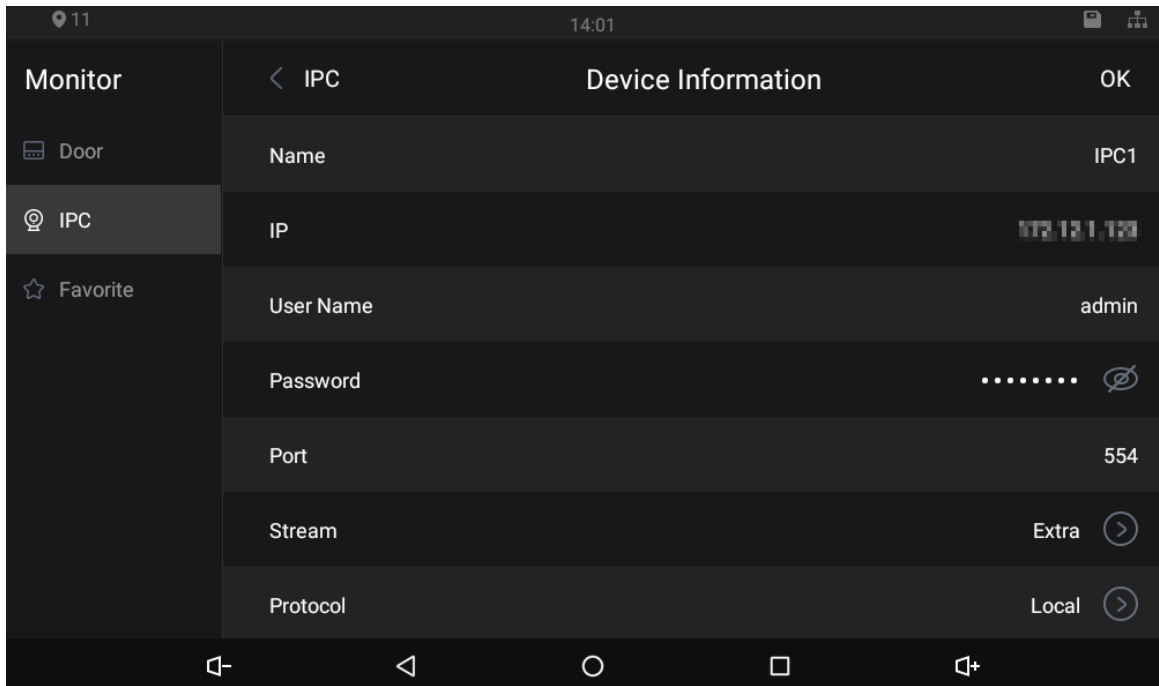


Figure 3-24 IPC information



- : 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

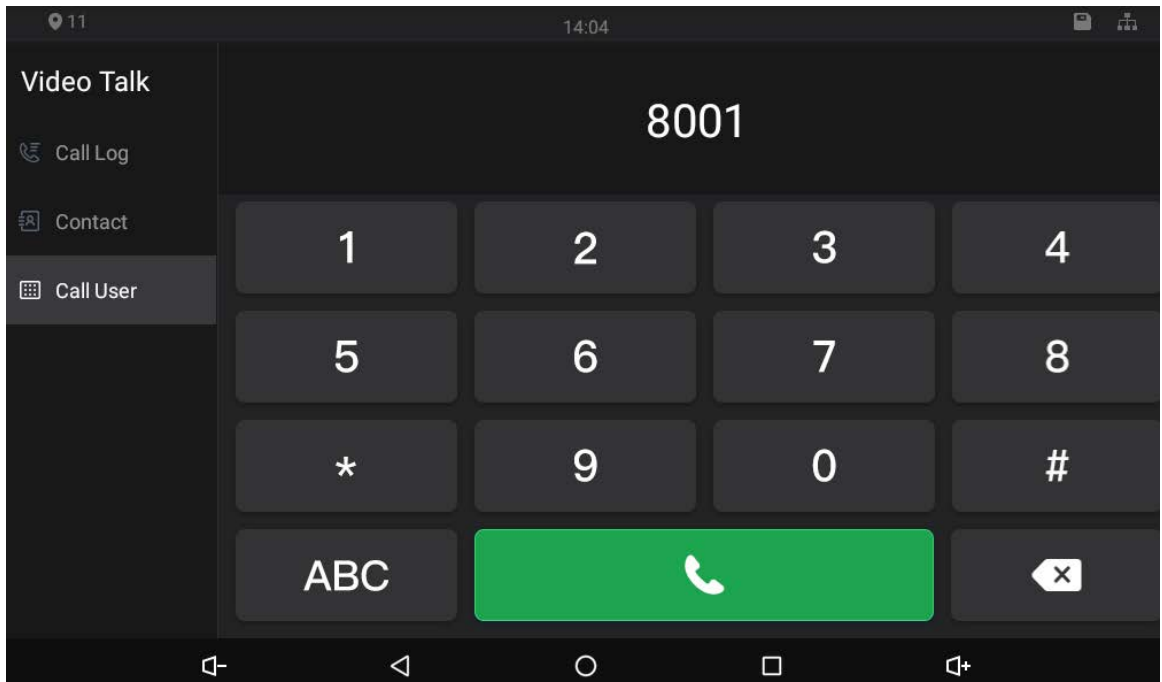






Figure 3-26 Calling




- 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.

Legal and Regulatory Information

Legal Considerations

Video surveillance can be regulated by laws that vary from country to country. Check the laws in your local region before using this product for surveillance purposes.

Disclaimer

Every care has been taken in the preparation of this document. Please inform your nearest Dahua office of any inaccuracies or omissions. Dahua Technology shall not be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Dahua Technology makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Dahua Technology shall not be liable or responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material. This product is only to be used for its intended purpose.

Intellectual Property Rights

Dahua Technology retains all intellectual property rights relating to technology embodied in the product described in this document.

Equipment Modifications


This equipment must be installed and used in strict accordance with the instructions given in the user documentation. This equipment contains no user-serviceable components. Unauthorized equipment changes or modifications will invalidate all applicable regulatory certifications and approvals.

Trademark Acknowledgments

 are registered trademarks or trademark applications of Dahua Technology in various jurisdictions. All other company names and products are trademarks or registered trademarks of their respective companies.

Regulatory Information

European Directives Compliance

 This product complies with the applicable CE marking directives and standards:

- Low Voltage (LVD) Directive 2014/35/EU.
- Electromagnetic Compatibility (EMC) Directive 2014/30/EU.
- Restrictions of Hazardous Substances (RoHS) Directive 2011/65/EU and its amending Directive (EU) 2015/863.

A copy of the original declaration of conformity may be obtained from Dahua Technology.

The most up to date copy of the signed EU Declaration of Conformity (DoC) can be downloaded from: www.dahuasecurity.com/support/notice/

CE-Electromagnetic Compatibility (EMC)

This digital equipment is compliant with Class B according to EN 55032.

CE-Safety

This product complies with IEC/EN/UL 60950-1 or IEC/EN/UL 62368-1, Safety of Information Technology Equipment.

Declaration of Conformity CE

(Only for the product has RF function)

Hereby, Dahua Technology declares that the radio equipment is compliant with Radio Equipment Directive (RED) 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: www.dahuasecurity.com/support/notice/

USA Regulatory Compliance

FCC

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation.

Attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This product has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This product generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a

- we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and 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 occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Support

Should you require any technical assistance, please contact your Dahua distributor. If your questions cannot be answered immediately, your distributor will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can:

- Download user documentation and software updates.
- Search by product, category, or phrase.
- Report problems to Dahua support staff by logging in to your private support area.
- Chat with Dahua support staff.
- Visit Dahua Support at www.dahuasecurity.com/support.

Contact Information

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199, Bin'an Road, Binjiang District, Hangzhou, P.R. China
Postcode: 310053
Tel: +86-571-87688883
Fax: +86-571-87688815
Email: overseas@dahuatech.com
Website: www.dahuasecurity.com

English

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.

Safety Instructions

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

particular installation. If this product does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC SDOC Statement can be downloaded from: <https://us.dahuasecurity.com/support/notices/>

RF exposure warning

(Only for the product has RF communication function)

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Canada Regulatory Compliance

ICES-003

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.






This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

- (1) This device may not cause interference, and
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

RF exposure warning

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

Safety Requirement

- Abide by local electrical safety standards to ensure that the voltage is stable and complies with the power supply requirement of the device.
- Transport, use, and store the device under the allowed humidity and temperature conditions. Refer to the corresponding technical specifications of device for specific working temperature and humidity.
- Do not place the device in a location exposed to dampness, dust, extreme hot or cold, strong electronic radiation, or unstable lighting conditions.
- Do not install the device in a place near the heat source, such as radiator, heater, furnace, or other heat generating device to avoid fire.
- Prevent liquid from flowing into the device to avoid damage to internal components.
- Install the device horizontally or install on the stable place to prevent it from falling.
- Install the device in a well-ventilated place, and do not block the ventilation of the device.
- Do not disassemble the device arbitrarily.
- Avoid heavy stress, violent vibration, and soaking during during transportation, storage, and installation. Complete package is necessary during the transportation.
- Use the factory package or the equivalent for transportation.

Battery

Low battery power affects the operation of the RTC, causing it to reset at every power-up. When the battery needs replacing, a log message will appear in the product's server report. For more information about the server report, see the product's setup pages or contact Dahua support.



- Risk of explosion if the battery is incorrectly replaced.
- Replace only with an identical battery or a battery which is recommended by Dahua.
- Dispose of used batteries according to local regulations or the battery

(Only for the product has RF communication function)

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Japan Regulatory Compliance

VCCI

These products comply with the requirements of VCCI Class B Information Technology Equipment.

Batteries

Correct disposal of batteries in this product



This marking on the battery indicates that the batteries in this product should not be disposed of with other household waste at the end of their working life. Where marked, the chemical symbols Hg, Cd or Pb indicate that the battery contains mercury, cadmium or lead above the reference levels in Directive 2006/66/EC and its amending Directive 2013/56/EU. If batteries are not properly disposed of, these substances can cause harm to human health or the environment.



Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

Safety

The product complies with IEC/EN/UL 60950-1, Information Technology Equipment – Safety – Part 1: General Requirements; or complies with IEC/EN/UL 62368-1, Audio/Video, information and communication technology equipment – Part 1: Safety requirements.

manufacturer's instructions.






Français

Précautions et avertissements importants

Le contenu de ce chapitre aborde la bonne manipulation de l'appareil, la prévention des risques et la prévention des dommages matériels. Lisez ce contenu soigneusement avant d'utiliser l'appareil, respectez-le lorsque vous l'utilisez, et conservez-le pour vous y référer ultérieurement.

Précautions d'emploi

Les mentions d'avertissement catégorisées suivantes ayant un sens défini sont susceptibles d'apparaître dans le manuel.

Mentions d'avertissement	Signification
 DANGER	Indique un danger à risque élevé qui entraînera la mort ou des blessures graves si les instructions données ne sont pas respectées.
 AVERTISSEMENT	Indique une situation moyennement ou faiblement dangereuse qui entraînera des blessures faibles ou modérées si les instructions données ne sont pas respectées.
 AVERTISSEMENT	Indique une situation potentiellement dangereuse qui pourra entraîner des dommages de la propriété, des pertes de données, une performance moindre ou des résultats imprévisibles, si les instructions données ne sont pas respectées.
 ASTUCES	Fournit des instructions qui vous permettront de résoudre un problème ou de vous faire gagner du temps.
 REMARQUE	Fournit des informations supplémentaires pour mettre en évidence et compléter le texte.

Exigences de sécurité

- Respectez les normes de sécurité électrique locales pour vous assurer que la tension est stable et conforme aux exigences d'alimentation de l'appareil.
- Transportez, utilisez et stockez l'appareil dans les conditions d'humidité et de température autorisées. Consultez les spécifications techniques correspondantes de l'appareil pour connaître la température et l'humidité de fonctionnement spécifiques.
- Ne placez pas l'appareil dans un lieu exposé à l'humidité, à la poussière, à une chaleur ou un froid extrême, à de forts rayonnements électroniques, ou à des conditions d'éclairage instables.

If the power supply to the product is from external power adaptor without connecting to AC Mains, and the product is not shipped with power adaptor, customers are required to use the external power adaptor that must fulfill the requirements for Safety Extra Low Voltage (SELV) and Limited Power Source (LPS).

Waste Electrical and Electronic Equipment (WEEE) statements

Disposal and Recycling

When this product has reached the end of its useful life, dispose of it according to local laws and regulations. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. In accordance with local legislation, penalties may be applicable for incorrect disposal of this waste.



This symbol means that the product shall not be disposed of together with household or commercial waste. Directive 2012/19/EU on waste electrical and electronic equipment (WEEE) is applicable in the European Union member states. To prevent potential harm to human health and the environment, the product must be disposed of in an approved and environmentally safe recycling process. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. Businesses should contact the product supplier for information about how to dispose of this product correctly.

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures, including but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

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 jurisdictions. For detailed information, refer to 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,