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	Janauary 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.

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 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 RF Radiation Exposure Statement:

  This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body.

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

Important Safeguards and Warnings

The following description is the correct application method of the device. Read the manual carefully before use, in order 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; doo 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) recommended by this area, which shall be used within its rated specification!
- 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. Power supply can be cut off only after the device has completed upgrade and has restarted.

Table of Contents

1 Introduction

1.1 Overview

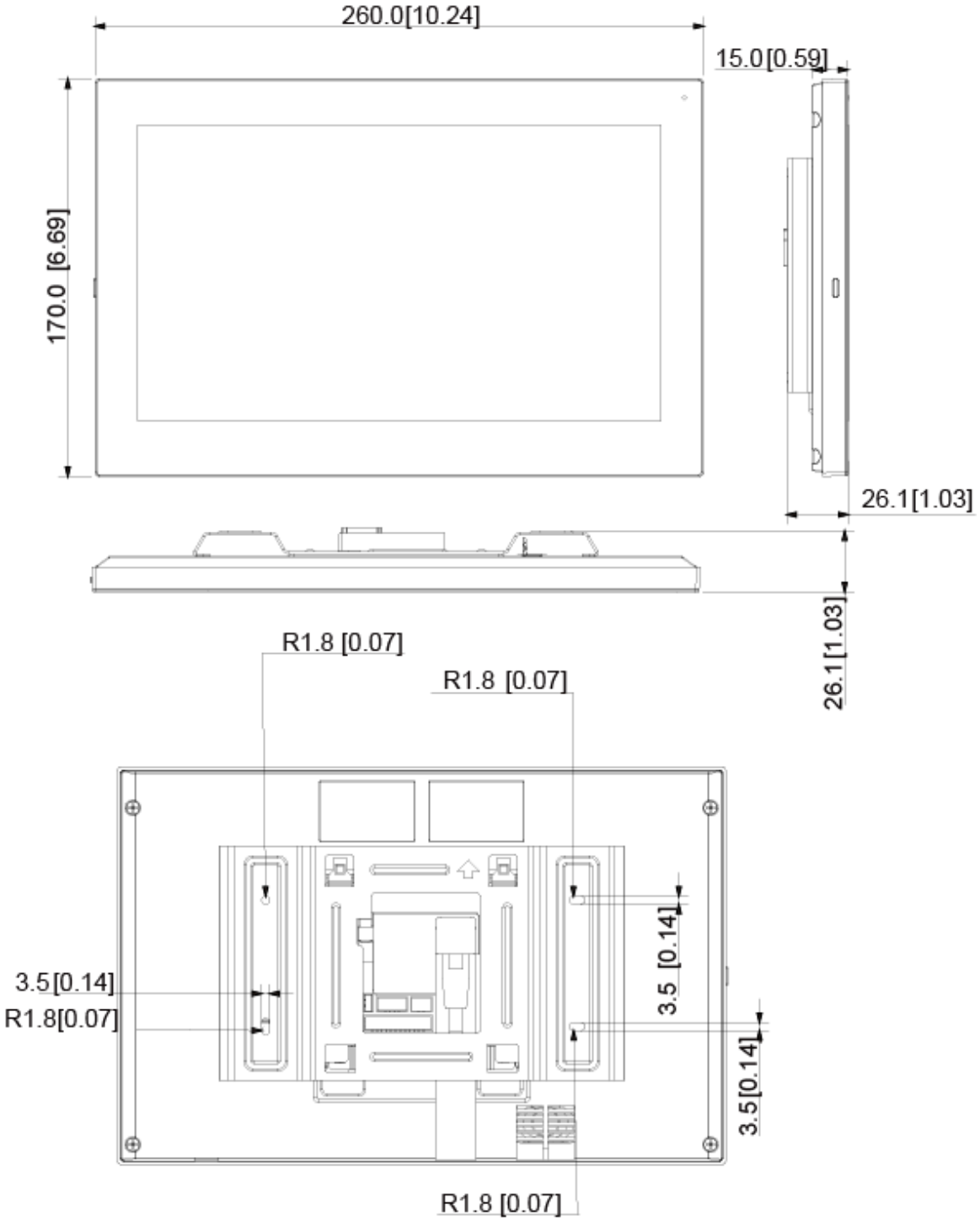
The IP indoor monitor, widely used in intelligent buildings, integrates functions of monitoring, voice communication, and unlock. Technologies like embedded technology, IP communication methods, simple network management protocol (SNMP), network encryption, and more are applied to make the whole system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

1.2 Features

- Wi-Fi: Provides wireless network for devices.
- Voice call: You can make calls on the outdoor stations to indoor monitors.
- Monitoring: Videos captured by fence stations, outdoor stations, IP cameras, and more can be watched on the indoor monitor.
- Emergency call: Emergency calls can be made on the indoor monitor.
- Auto snapshot: During calls, or during monitoring, images can be captured, and the images can be stored in the SD card or FTP.
- Do not disturb: You can set period in which you do not want to be disturbed.
- Remote unlock: You can unlock doors remotely.
- Arm and disarm: You can set protection zones, and then arm and disarm.
- Record search: Call records and alarm records can be viewed.
- Message check: You can check text messages and videos left by visitors, or public notices released by the management center.
- App: You can install app on your mobile phone.

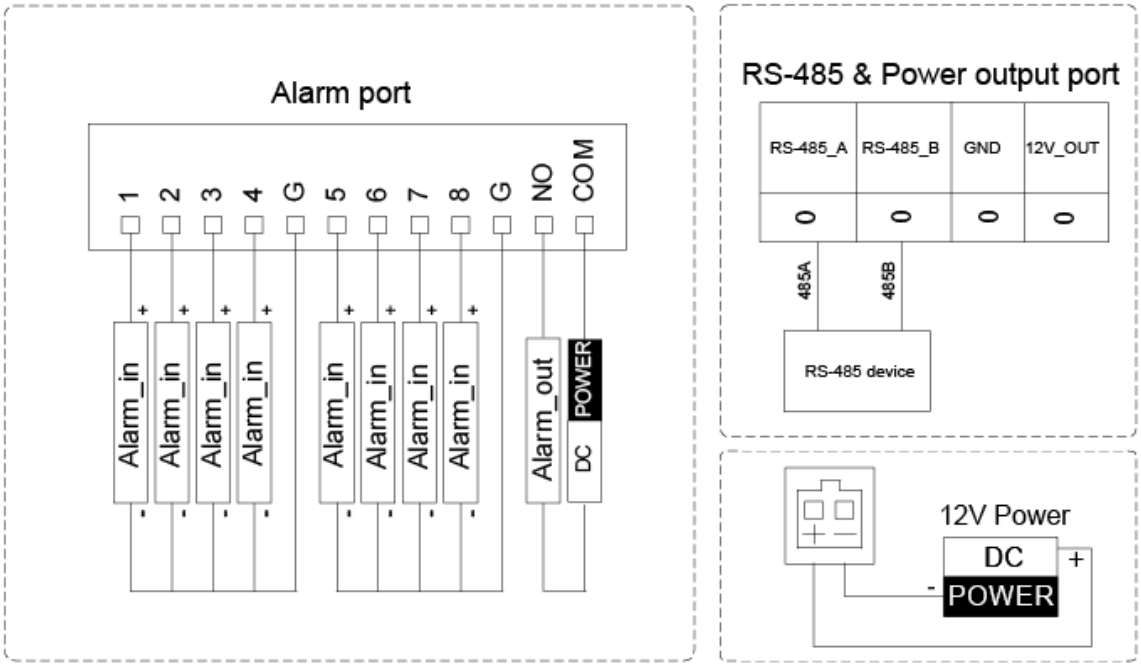
1.3 Dimensions

Figure 1-1 Dimensions (mm [inch])



1.4 Cable Connections

Figure 1-2 Cable connection



2 Installation

Figure 2-1 Installation

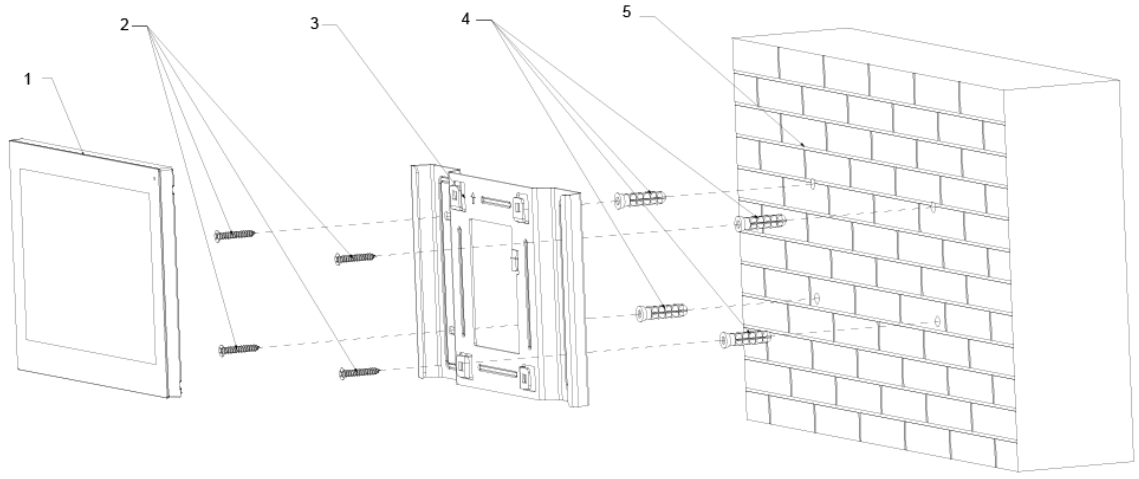


Table 2-1 Components

No.	Name
1	Indoor monitor
2	ST3 self-tapping screws
3	Bracket
4	Anchor bolt
5	Wall

Figure 2-2 Screw hole distances and diameters

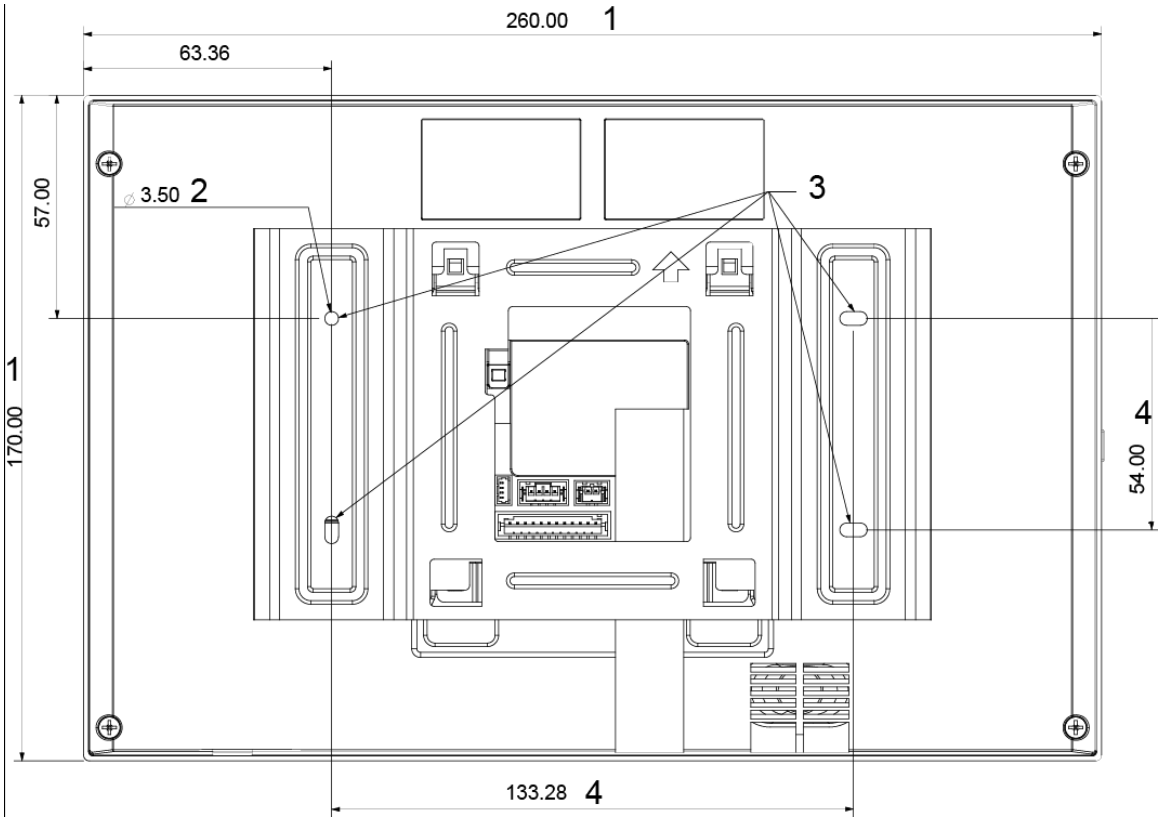


Table 2-2 Description of screw hole distances and diameters

No.	Description
1	Indoor monitor dimension
2	Bracket screw hole diameter
3	Bracket oval hole position
4	Screw hole distance

Step 1 Drill four screw holes in the wall according to holes on the bracket.

Step 2 Put anchor bolts into the screw holes.

Step 3 Fix the indoor monitor on the wall with screws.

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

The installation is completed.

3 Configuration

You need to configure IP, Wi-Fi, door station parameter, SIP server, and more on the indoor monitor, and then the indoor monitor can communicate with door stations and the management center.

3.1 Configuration Overview

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

3.2 Indoor Monitor Configuration

3.2.1 Initialization

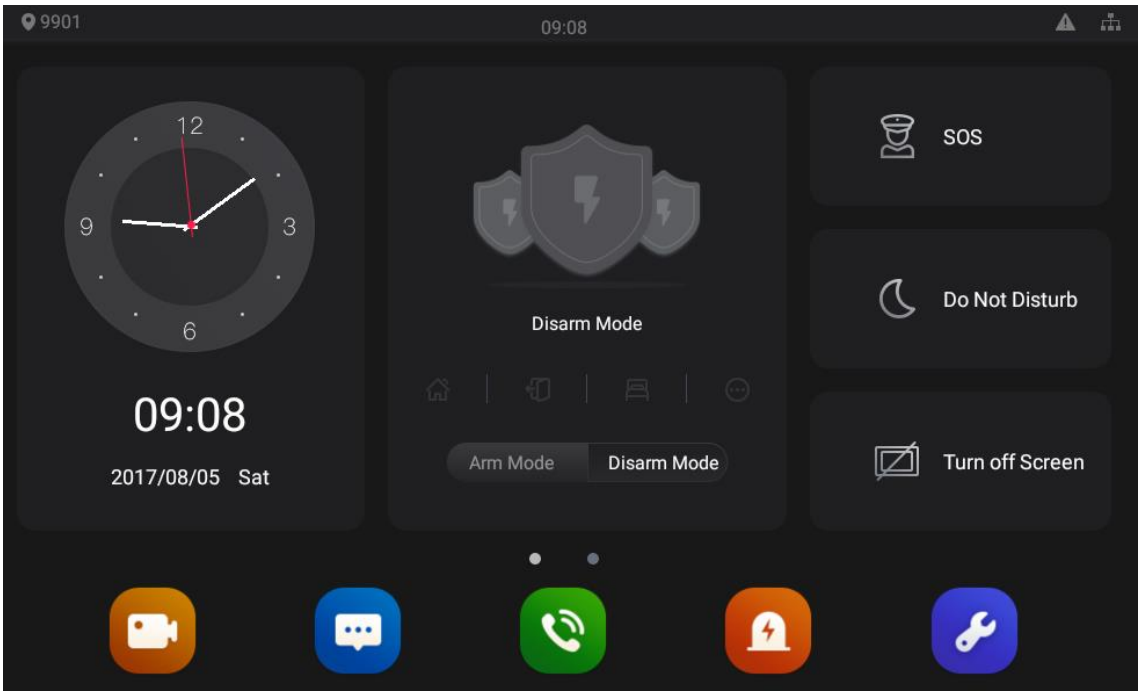
Set password and email.

- Password: Used when administrators need to go to the project mode.
- Email: Used when you need to reset the password.

The default IP address of the indoor monitor is 192.168.1.108.

Step 1 Connect the indoor monitor to power source.
WELCOME is displayed, and then the initialization interface is displayed.
Step 2 Enter the password, confirm password, and email.
Step 3 Tap **OK**.
The main menu is displayed.

Figure 3-1 Main menu



Room No.

Room No. is displayed at the upper left corner of the main menu.

Time and Date

On the main menu, time and date is displayed.

Arm Mode/Disarm Mode

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.

Network Status

Network status and SIP server status are displayed at the upper right corner of the main menu.

If the SIP server works normally, the icon will disappear.

SOS

Tap the SOS icon, the indoor monitor will call the management center.

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. For details, see DND by tapping .

Turn off Screen

Tap the icon, and then the screen will be turned off.

User Settings

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

Ring

On this interface, you can select ringtones for different outdoor stations.

DND

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

Forward

When calls come in, they will be forwarded to the management center during the hours that you have set. There are three options: Always, Busy, and No Answer.

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

General

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

- Monitor Time (s): You can watch monitoring images from the indoor monitor for at most 300 seconds a time.
- Record Time (s): You can record at most 300-second audio files a time on the indoor monitor.
- VTO Message Time (s): Visitors can only leave an at most 90-second message a time on the outdoor station (VTO).
- VTO Talk Time (s): Visitors can talk to you through the outdoor station (VTO) for at most 300 seconds a time.
- Internal Call Time (s): You can talk to other indoor monitors for at most 60 seconds a time.
- Internal Call: After the Internal Call is enabled, you can call other indoor monitors from the indoor monitor you are operating.
- Auto Capture: After the Auto Capture function is enabled, if a visitor called you but you did not answer the call, the outdoor station (VTO) would take three images of the visitor standing in front of the outdoor station.

Themes

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

Calendar

You can view date through the indoor monitor, and create notes, schedules, and plans.

Gallery

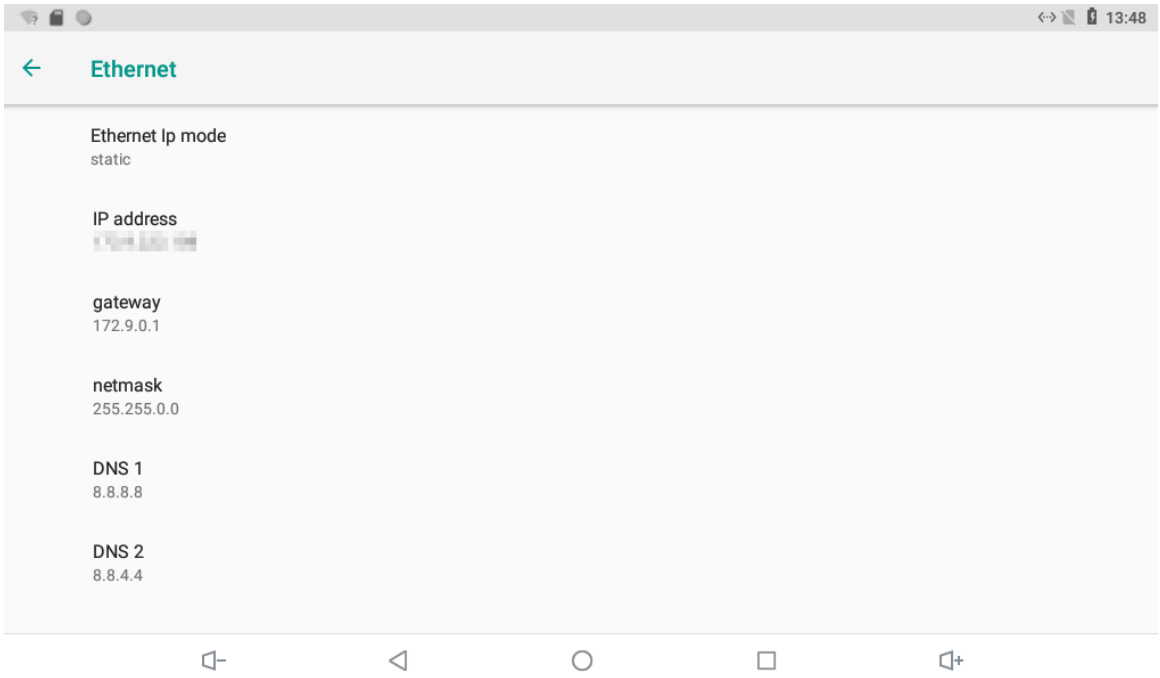
You can view images captured by outdoor stations (VTO) or IP cameras.

3.2.2 Network Settings

Step 1 Tap the **Settings** interface.

The settings interface is displayed.

Figure 3-2 Setting



Step 2 Configure parameters.

Table 3-1 Parameter description

Parameter	Description
Network & Internet	You can choose to enable Wi-Fi or not by tap . ● Tap , and then available Wi-Fi network will be displayed. ● 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.

Parameter	Description	
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. 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	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 restore the indoor monitor to factory settings.
	About tablet	You can see details (battery status, network status, legal information, model, android version, Android security patch level, baseband version, Kernel version, build number, and more) about the indoor monitor.

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.

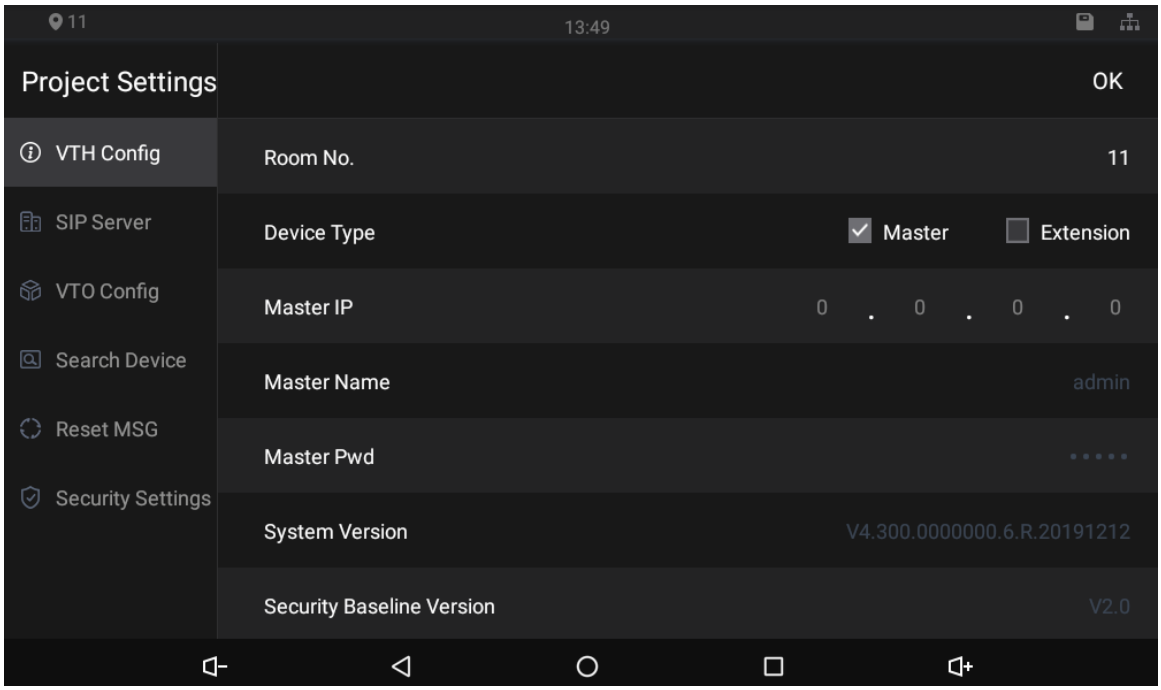
Files

You can view files like images, videos, audio, and recently produced files.

3.2.3 Project Settings

Tap and hold  for over 5 seconds, enter the password (123456 by default), and then the **Project Settings** interface will be displayed.

Figure 3-3 Project settings



VTH Config

- Room No.: No. of the room where the indoor monitor is installed.
- Device Type: There are two options: Master and Extension.
  - ◇ Master: If the indoor monitor 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: Keep the default value.
- System Version: You can view system version of the indoor monitor.
- Security Baseline Version: You can view security baseline version of the indoor monitor.

SIP Server

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

Tap **SIP Server**, and then the SIP server interface is displayed.

Figure 3-4 SIP server (1)

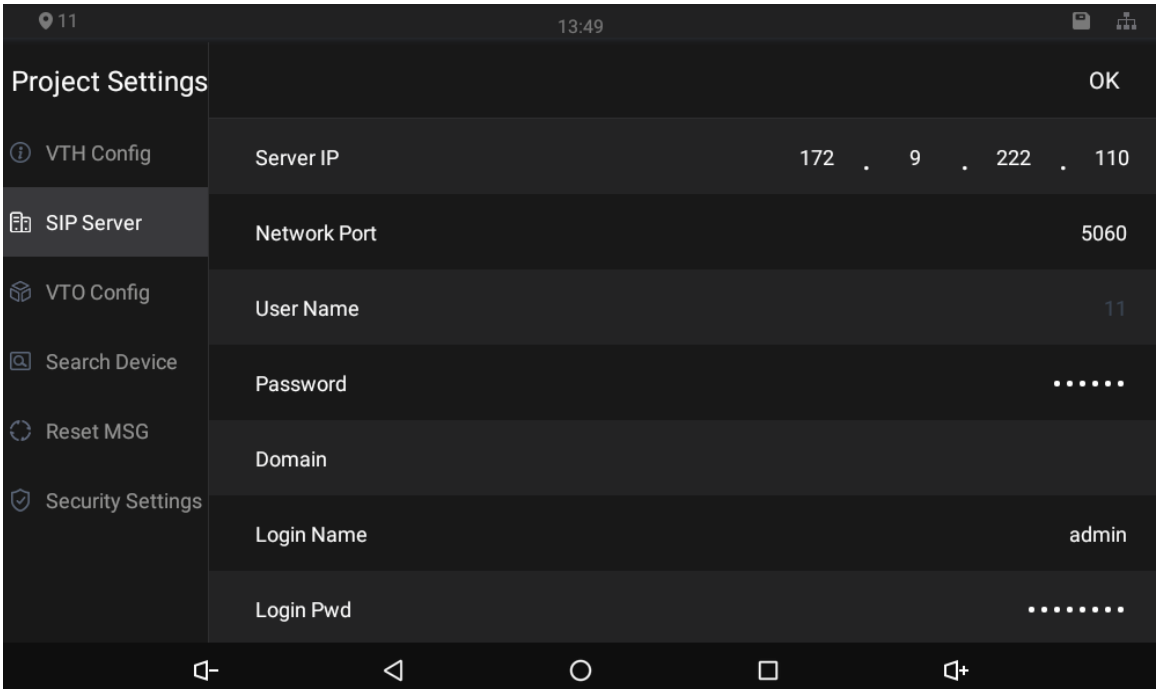


Table 3-2 SIP server description

Parameter	Description
Server IP	● When the platform works as SIP server, server IP is IP address of the management platform. ● When an outdoor station works as SIP server, server IP is IP address of the outdoor station.
Network Port	● When the platform works as SIP server, network port is 5080. ● When VTO works as SIP server, network port is 5060.
User Name	Use default value.
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	User name and password to login to web page of the SIP server.
Login Pwd	
Status	Enable the SIP server status, and then the SIP server can start to work.

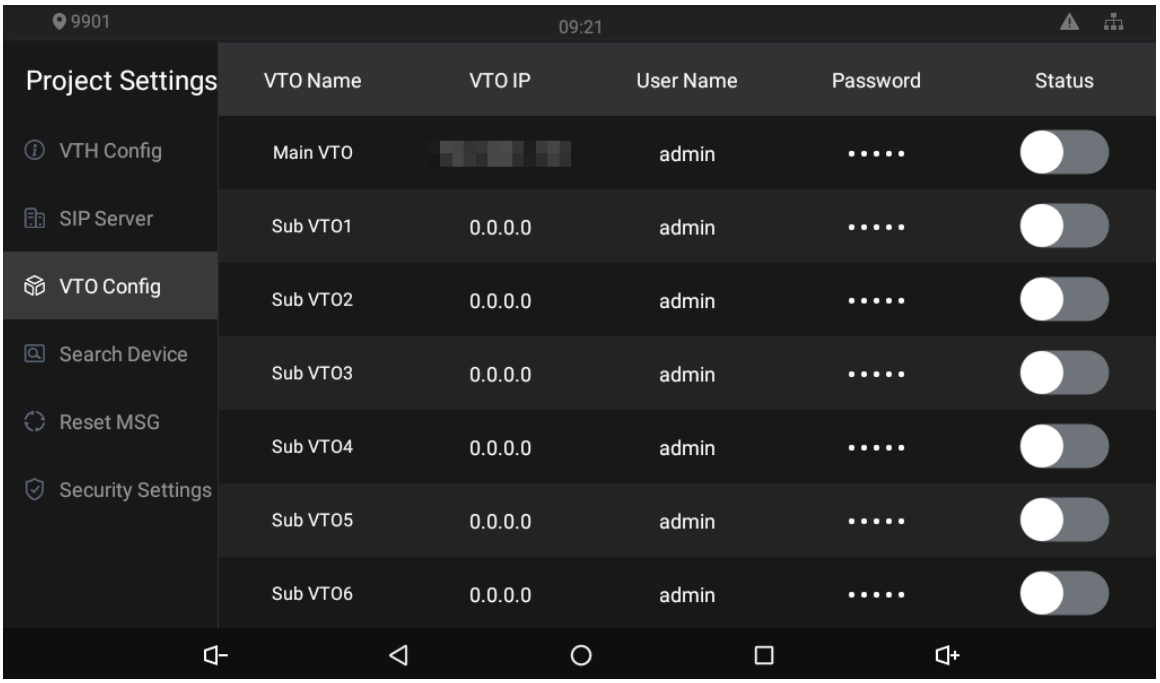
VTO Config

You need to add outdoor stations to the indoor monitor.

Step 1 Tap VTO Config.

The **VTO Config** interface is displayed.

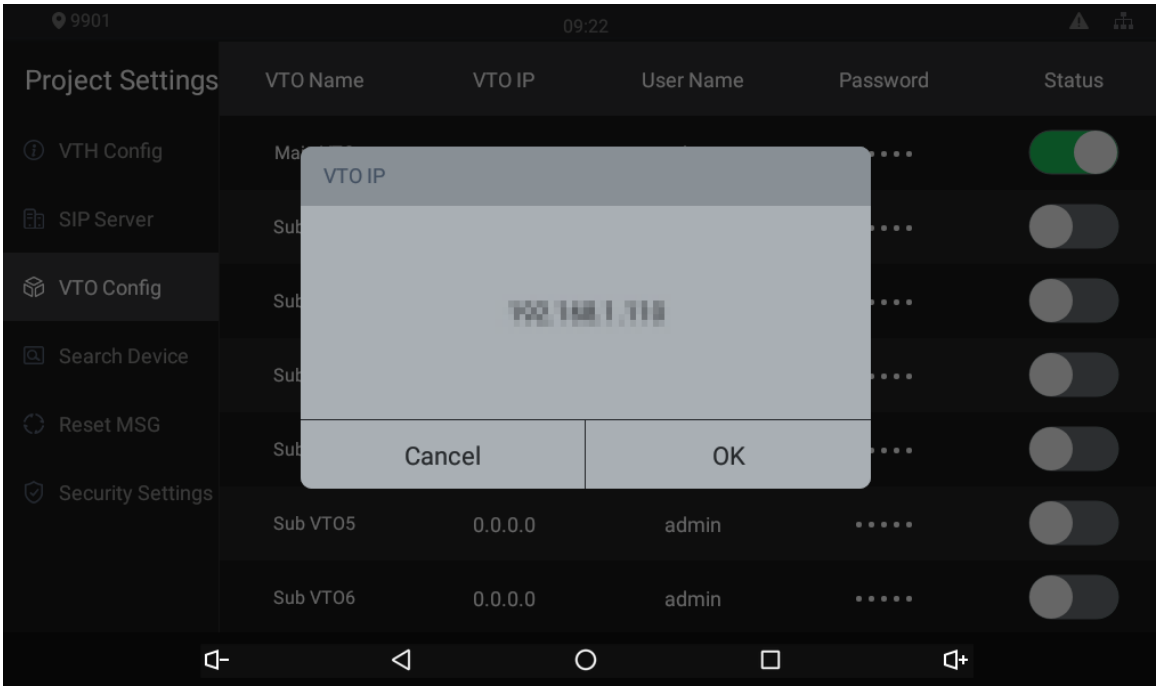
Figure 3-5 Outdoor station (VTO) configuration



Step 2 Tap an outdoor station (VTO).

The **VTO IP** interface is displayed.

Figure 3-6 VTO IP



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

Step 4 Enter the outdoor station (VTO) IP that you planned.

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

You can add 20 outdoor stations (one main outdoor station and 19 sub outdoor stations) to the indoor monitor.

Search Device

Tap the **Search Device** icon, and then the system starts to search devices automatically.

Reset MSG

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

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

Security Settings

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

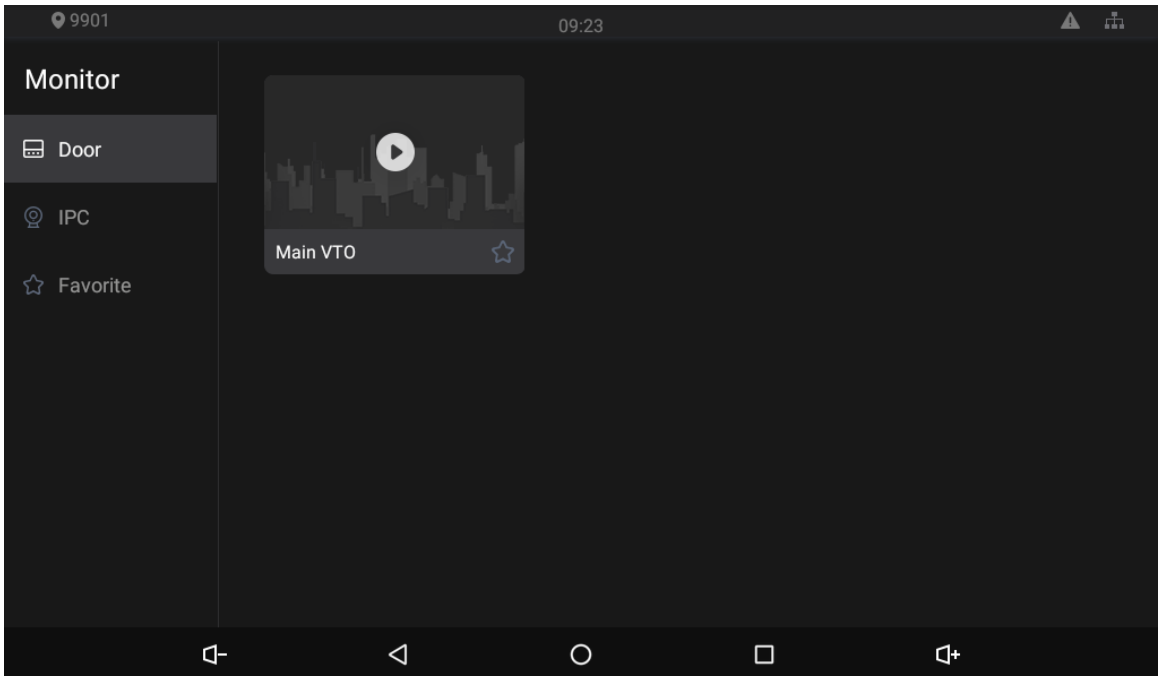
3.3 Commissioning

3.3.1 Watching Monitoring Video

Tap , and the Monitor interface is displayed.

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

Figure 3-7 Monitor



- : Tap the icon to turn down the volume.

- : Tap the icon to go to the previous page.
- : Tap the icon to go to the main menu.
- : Tap the icon, and 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.
- : Tap the icon to turn up the volume.

3.3.2 Checking Messages

Tap , and then text messages and videos left by visitors, or public notices released by the management center will be displayed.

3.3.3 Making Calls

Tap , 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.

3.3.4 Viewing Alarms Logs

Tap , and then the **Alarm** interface is displayed. Peripheral alarm modules can be connected to the indoor monitor. You can view alarm logs, do alarm settings for 6 areas as needed. There are 7 types of alarms: infrared, gas sensor, smoke sensor, urgency button, door sensor, stolen, and perimeter.

Disarm all alarms first, and then you can do alarm settings.

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 equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (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 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.
- We suggest that you download and use the latest version of client software.

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

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. **Assign Accounts and Privileges Reasonably**

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

10. **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.

11. **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.

12. **Secure Auditing**

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

13. **Network Log**

    Due to the limited storage capacity of the equipment, 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.

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment 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.