

# **Analog 4-Wire Video Intercom**

## **Quick Start Guide**



# Foreword

## General






This manual mainly introduces structure, installation, wiring and menu operations of the analog 4-wire video intercom. Read carefully before using the device, and keep the manual safe for future reference.

## Model

7-inch and 4.3-inch VTH

## Safety Instructions

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

Signal Words	Meaning
 <b>DANGER</b>	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 <b>CAUTION</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 <b>TIPS</b>	Provides methods to help you solve a problem or save time.
 <b>NOTE</b>	Provides additional information as a supplement to the text.

## Revision History

Version	Revision Content	Release Time
V1.2.4	Revised "Important Safeguards and Warnings".	December 2022
V1.2.3	Revised wiring description.	November 2022
V1.2.2	Revised wire color description.	January 2022
V1.2.1	Added the recommended installation height of the device.	January 2022
V1.2.0	Added new model 4.3-inch VTH.	October 2021
V1.1.0	<ul style="list-style-type: none"><li>Added description of the functions of 7-inch VTH.</li><li>Added Factory Reset function.</li></ul>	March 2021
V1.0.0	First release.	August 2020

## Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face,

fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

## About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

# Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, comply with the guidelines when using it.

## Operation Requirements



- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Transport, use and store the device under allowed humidity and temperature conditions.
- If the device is powered off for longer than a month, it should be placed in its original package and sealed. Make sure to keep it away from moisture, and store it under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.

## Installation Requirements



### WARNING

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- Improper use of the battery might result in a fire or explosion.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Install the device on a stable surface to prevent it from falling.
- Install the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

# Table of Contents

<b>Foreword</b> .....	<b>I</b>
<b>Important Safeguards and Warnings</b> .....	<b>III</b>
<b>1 Structure</b> .....	<b>1</b>
1.1 Introduction.....	1
1.2 Features .....	1
1.3 Front Panel.....	1
1.3.1 7-inch VTH.....	1
1.3.2 4.3-inch VTH.....	2
1.4 Rear Panel .....	4
<b>2 Installation</b> .....	<b>5</b>
2.1 VTH .....	5
2.2 VTO .....	6
<b>3 Wiring</b> .....	<b>8</b>
3.1 Preparations.....	8
3.1.1 Port Connection Rules .....	8
3.1.2 Cord Specification.....	9
3.2 Wiring One VTO and One VTH.....	9
3.3 Wiring One VTO and Three VTHs .....	10
3.4 Wiring Two VTOs and Three VTHs .....	11
<b>4 Menu Operations</b> .....	<b>12</b>
4.1 Snapshots.....	12
4.2 Time.....	14
4.3 Restoring to Default Settings .....	14
<b>Appendix 1 Cybersecurity Recommendations</b> .....	<b>16</b>

# 1 Structure

## 1.1 Introduction

The analog 4-wire video intercom consists of a door station ("VTO") and an indoor monitor ("VTH"). It is applicable to buildings, such as residential buildings, for people to do voice and video calls. The VTO is installed outdoors and VTH is installed indoors.

## 1.2 Features

### VTH

- Real-time video/voice communication
- Can be connected to three VTOs
- Can be connected to cameras (CVBS)
- Plug-and-play

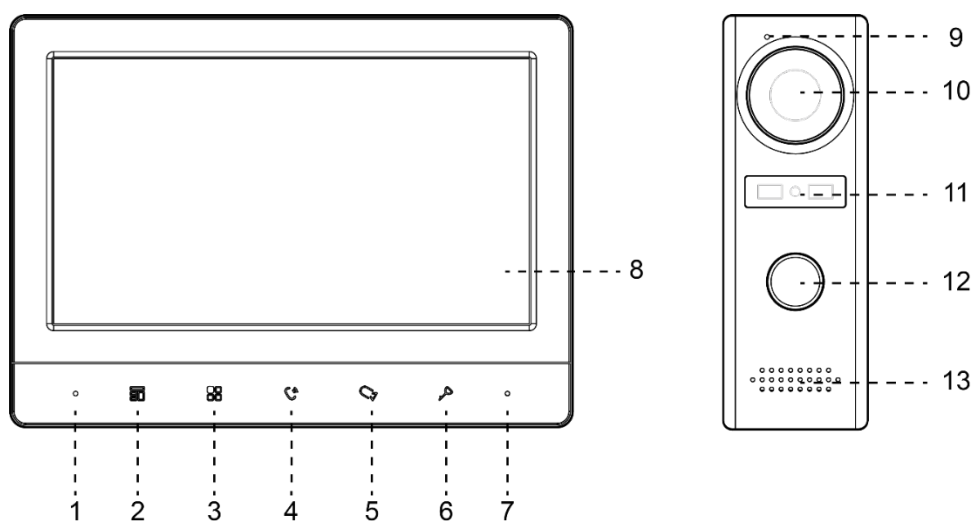
### VTO

- Real-time voice communication
- Self-adaptive IR illumination

## 1.3 Front Panel

### 1.3.1 7-inch VTH

Figure 1-1 Front panel



### 1.3.2 4.3-inch VTH

Figure 1-2 Front panel

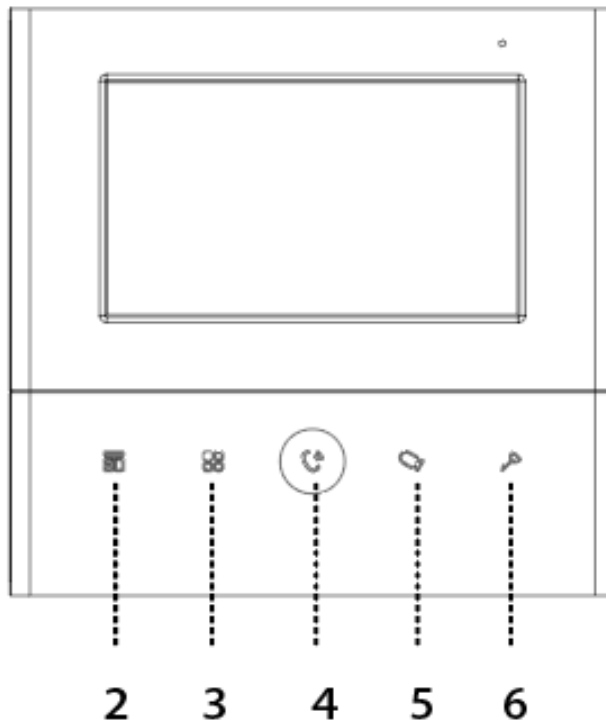








Table 1-1 Front panel description

No.	Icon	Description
1	–	Microphone.
2		<ul style="list-style-type: none"> <li>● Press to hang up the incoming call.</li> <li>● Take snapshots during monitoring (only supported by VTH1020J-T).</li> </ul>
3		<p>Wake up the screen, and bring up the menu.</p>  <p>For how to operate the menu, see "4 Menu Operations".</p>
4		<p>When someone is calling from the VTO:</p> <ul style="list-style-type: none"> <li>● Press once to do voice communication with the person.</li> <li>● Press twice quickly to hang up.</li> </ul>
5		<p>When someone is calling from the VTO:</p> <ul style="list-style-type: none"> <li>● Press to talk to the person (only supported by VTH1020J).</li> <li>● Press to take snapshots (only supported by VTH1020J-T).</li> </ul> <p>When no one is calling:</p> <ul style="list-style-type: none"> <li>● Press once, twice, three times and four times to view live video of: VTO1, VTO2, analog camera 1 and analog camera 2 respectively.</li> <li>● On any live video, press to take snapshots (only supported by VTH1020J-T).</li> </ul>
6		When someone is calling, press to open the door where the VTO is installed.
7	–	Power indicator.
8	–	LCD screen.
9	–	Microphone.
10	–	Built-in camera.
11	–	Power indicator.
12	–	<p>Call button.</p> <ul style="list-style-type: none"> <li>● Press once to call the VTH.</li> <li>● Press and hold for 10 seconds to change the bell type of the VTO. The power indicator will flash.</li> <li>● Press and hold for 15 seconds to turn up the bell volume of the VTO. The power indicator will flash. When the volume reaches maximum, this step will set it to minimum. Repeat this step to set appropriate volume.</li> <li>● Press and hold for 20 seconds to change to DWDR (digital wide dynamic range)/normal mode for the VTO. The power indicator will flash.</li> </ul>
13	–	Speaker.



## 1.4 Rear Panel

There might be slight differences in the rear panel among different models. But they have the same function ports.

Figure 1-3 Rear panel

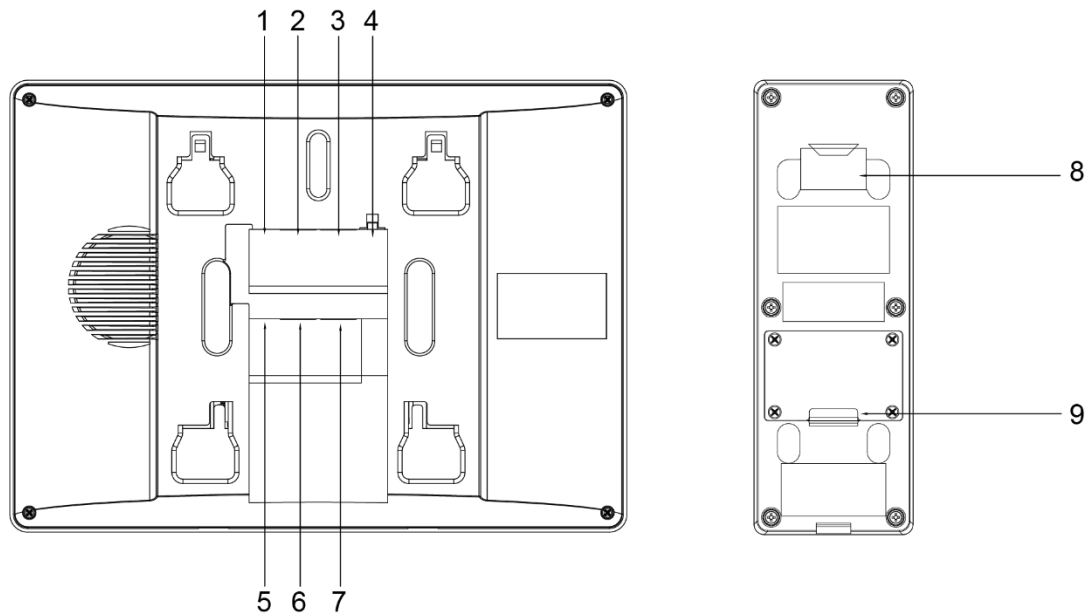


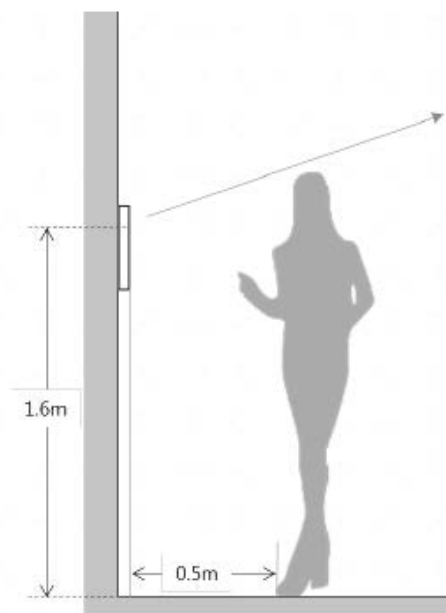
Table 1-2 Rear panel

No.	Description	No.	Description
1	Analog camera port 1.	6	VTH cascading port 1.
2	VTO port 1.	7	VTH cascading port 2.
3	VTO port 2.	8	VTO hanging slot.
4	Power input.	9	Wires: The color of the wires represents different port functions. <ul style="list-style-type: none"> <li>● Red: power.</li> <li>● Yellow: video.</li> <li>● White: audio.</li> <li>● Black: GND.</li> <li>● Green: exit button.</li> <li>● Orange: feedback.</li> <li>● Purple: NO.</li> <li>● Blue: COM.</li> <li>● Brown: NC.</li> </ul>
5	Analog camera port 2.	-	-

## 2 Installation

- Do not install devices in harsh environment with condensation, high temperature, dust, corrosive substance and direct sunlight.
- In case of abnormality after powering on the device, cut off the power supply at once, and unplug the network cable. Power on after troubleshooting.
- Installation should be done by professional teams. Do not dismantle or repair the device by yourself in case of device failure. Contact after-sales service if you need any help.
- The recommended installation height of the device is 1.6 m from the ground.

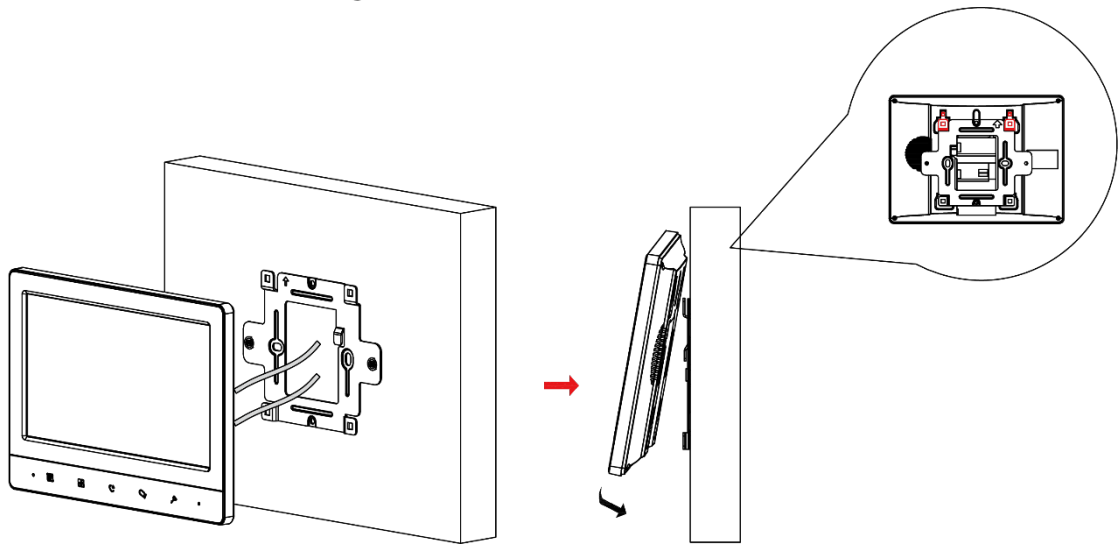
Figure 2-1 Installation height



### 2.1 VTH

Fix the bracket on the wall by screws, hang the VTH on the bracket, and then apply silicone sealant to the gap between the device and the wall.

Figure 2-2 VTH installation



## 2.2 VTO

Install the VTO bracket on the wall, and then hang the VTO on the bracket; or install the VTO cover on the wall, and then hang the VTO on the cover. Finally, apply silicone sealant to the gap between the device and the wall.

Figure 2-3 VTO installation

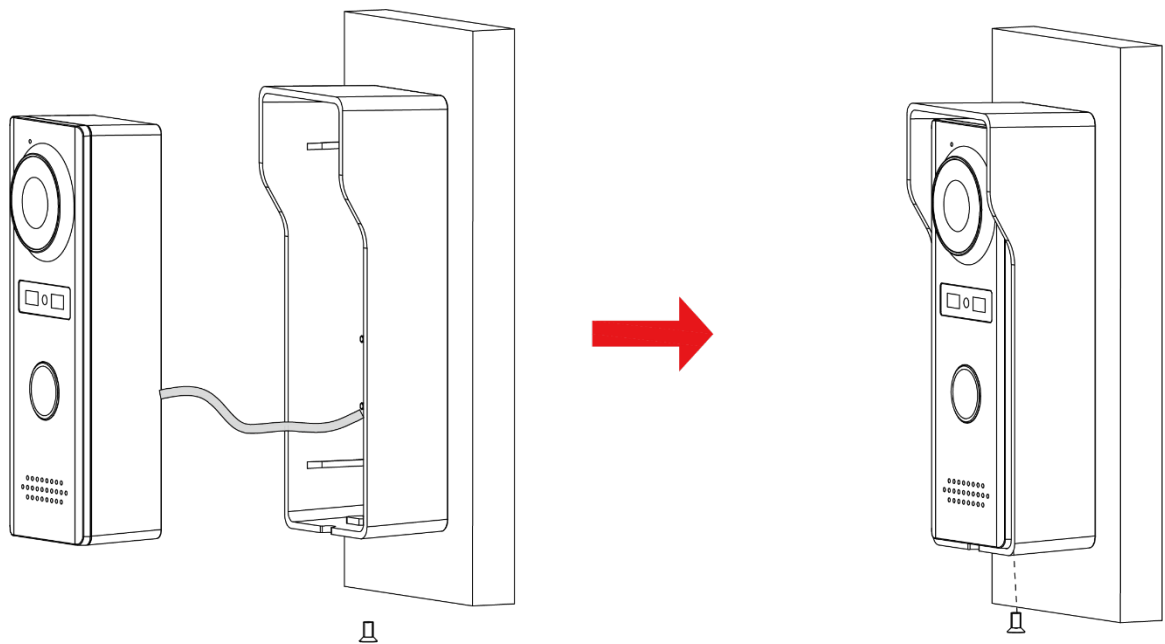
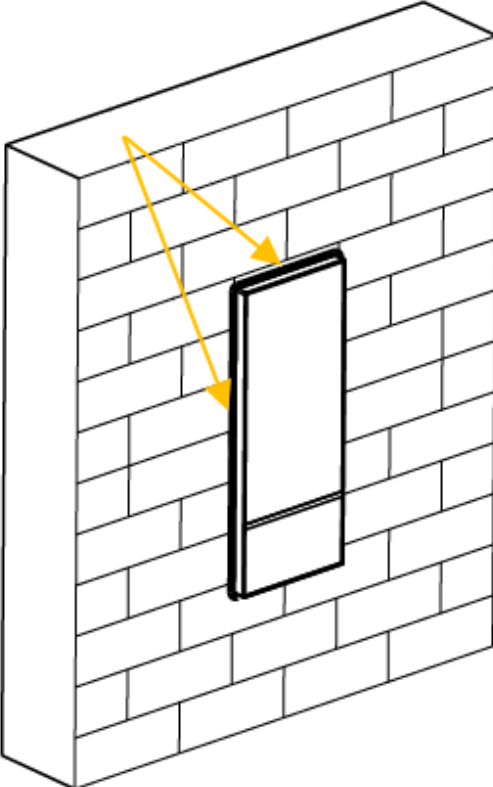


Figure 2-4 Apply silicone sealant to the gap between the device and the wall



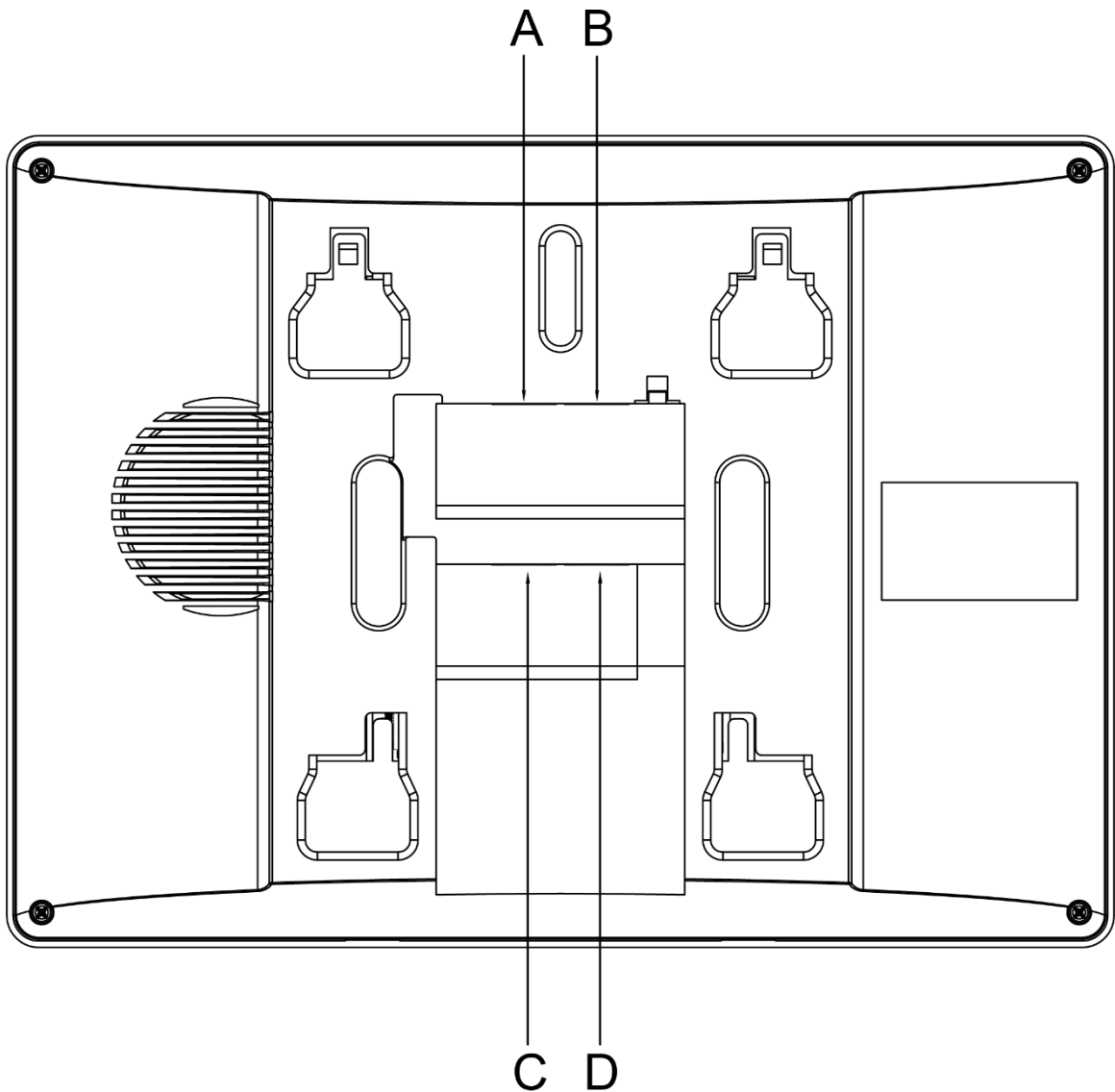
# 3 Wiring

At most 2 VTOs and 3 VTHs can be wired in one communication system.

## 3.1 Preparations

### 3.1.1 Port Connection Rules

Figure 3-1 Port connection rules



- Port A of an VTH can be connected to Port C of another VTH to do data communication.
- Port B of an VTH can be connected to Port D of another VTH to do data communication.
- Port A of an VTH cannot be connected to Port B or D of another VTH to do data communication.
- Port C of an VTH cannot be connected to Port B or D of another VTH to do data communication.

### 3.1.2 Cord Specification

Depending on the distance between the VTO and VTH, you need to select RVV4 cords of different specifications.

Table 3-1 Cord specification

Transmission Distance (TD)	RVV4 Cord Specification
TD ≤ 10 m	RVV4 × 0.3 mm <sup>2</sup>
10 m < TD ≤ 30 m	RVV4 × 0.5 mm <sup>2</sup>
30 m < TD ≤ 50 m	RVV4 × 0.75 mm <sup>2</sup>



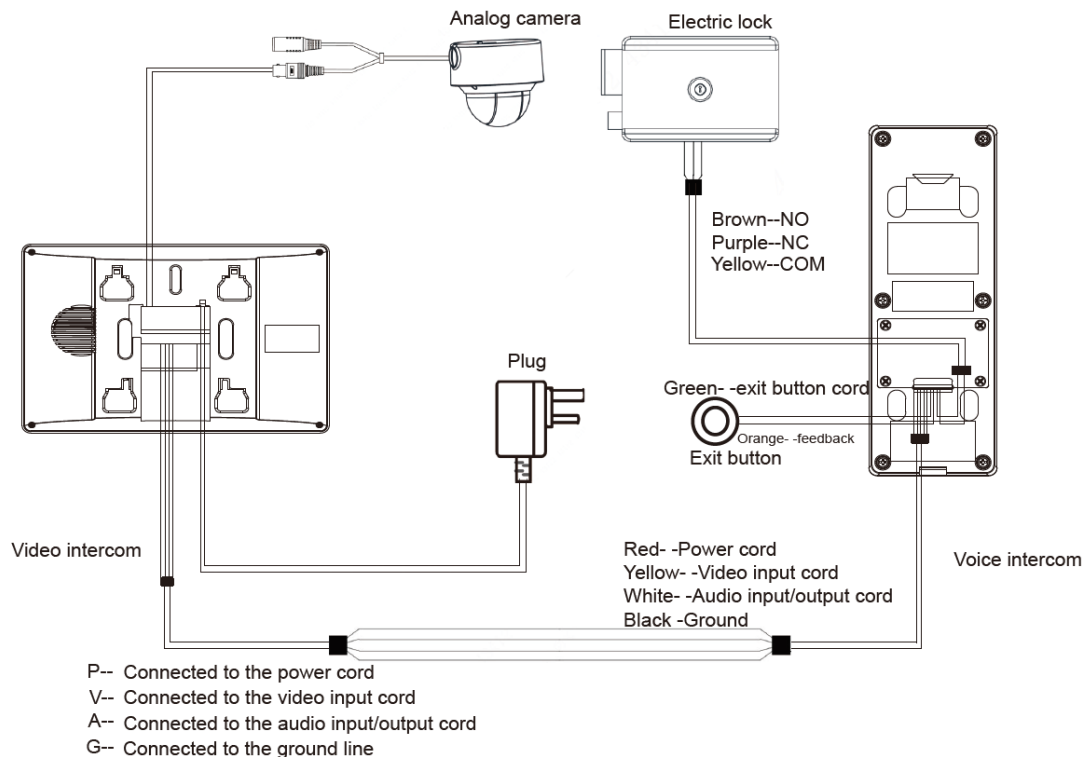
If the distance between the VTO and VTH is more than 50 m, use coaxial cables.



- Do not pull the cords violently.
- During wiring, wrap the cord joints with insulated rubber tape to prevent short circuit.

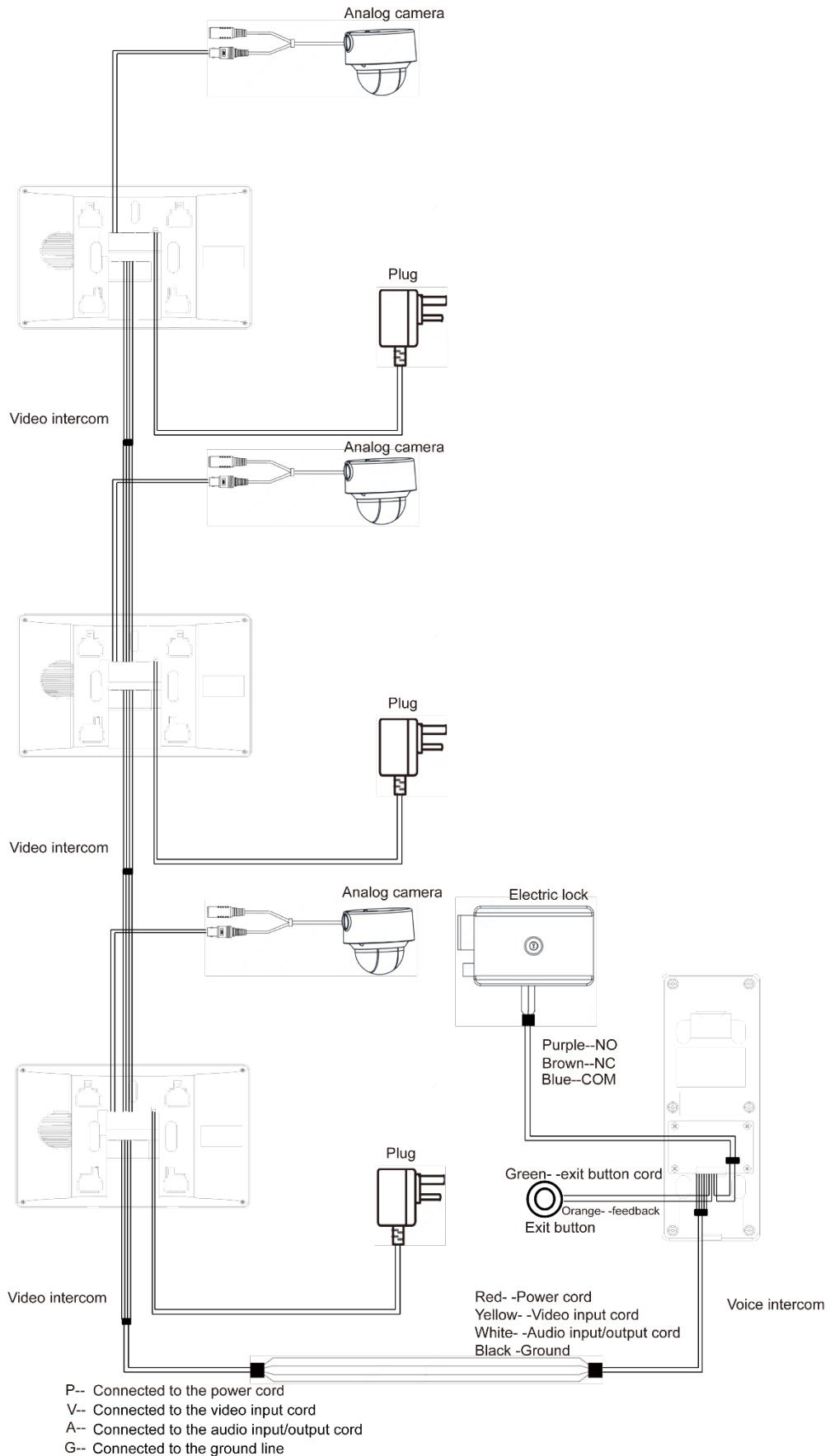
### 3.2 Wiring One VTO and One VTH

Figure 3-2 Wiring (1)



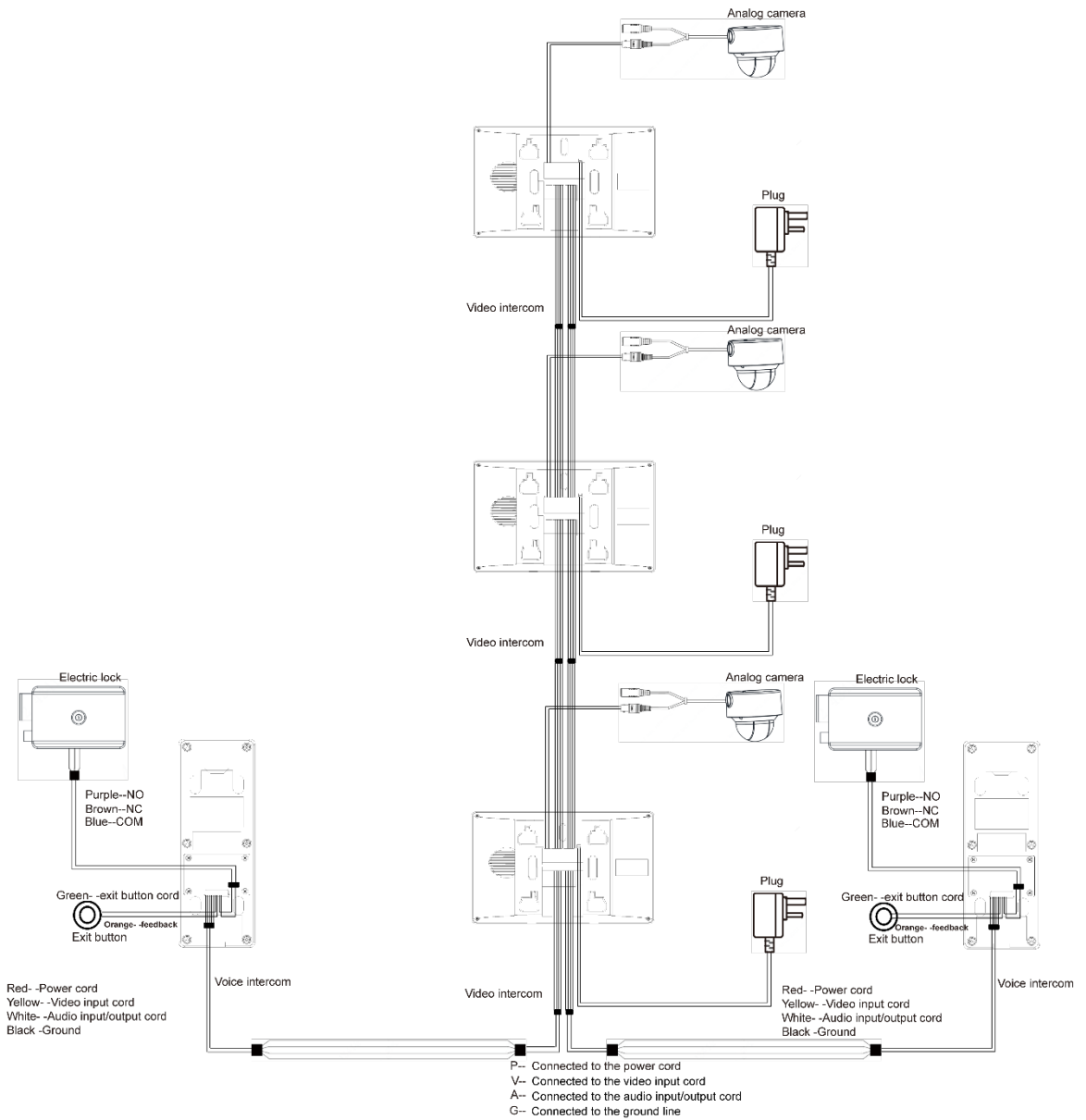
### 3.3 Wiring One VTO and Three VTHs

Figure 3-3 Wiring (2)



### 3.4 Wiring Two VTOs and Three VTHs

Figure 3-4 Wiring (3)



The recommended analog cameras (CVBS) are HAC 1230 series.



# 4 Menu Operations

You can configure the functions of the VTH, such as volume, brightness, and more.



- Only VTH1020J-T supports the **Snapshots** and **Time** functions.
- All configurations will be saved after you exit the menu.

Figure 4-1 Menu



Table 4-1 Menu operations

Icon	Function
	Used to confirm your operation when you are using the <b>Snapshots</b> and <b>Time</b> functions (only supported by VTH1020J-T).
	Adjust <b>Vol</b> (volume), <b>Bright</b> (brightness), <b>Contrast</b> and <b>BellVol</b> (bell volume), change <b>Bell</b> and turn off <b>DND</b> (do not disturb).
	Turn up <b>Vol</b> (volume), <b>Bright</b> (brightness), <b>Contrast</b> and <b>BellVol</b> (bell volume), change <b>Bell</b> , turn off <b>DND</b> (do not disturb), and adjust the time.
	Select an item.
	<ul style="list-style-type: none"> <li>• Exit the menu and lock the screen.</li> <li>• Go back to the previous interface.</li> </ul>

## 4.1 Snapshots


You can take snapshots during monitoring, and view the snapshots you have taken.




The VTH can store up to 200 snapshots. If storage is full, the earlier ones will be overwritten.

### Taking Snapshots

- During monitoring.

**Step 1** Press  to go to the monitoring image that you want.


**Step 2** Press , and then **Successful** will appear on the screen.

- When a VTO is calling or in a call with a VTO, press , and then **Successful** will appear on the screen.



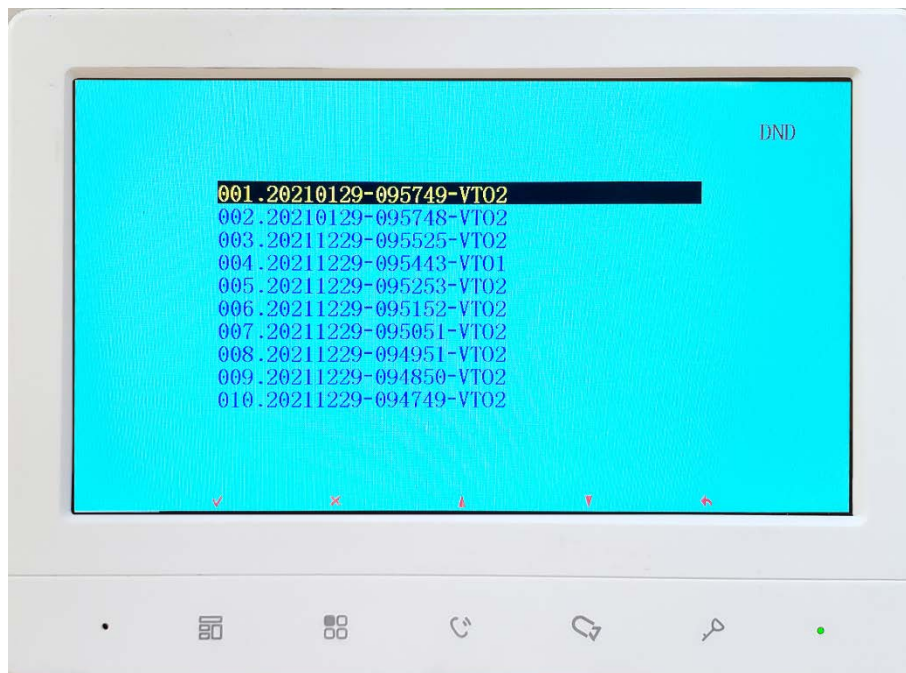
If the calling lasts more than 1 second, a snapshot will be automatically taken.



## Viewing Snapshots

**Step 1** Press  to bring up the menu.

**Step 2** Press , select **Snapshots**, and then press .

Figure 4-2 List of snapshots



**Step 3** Press  to select the one that you need, and then press .










To delete a snapshot, press , **Delete?** will appear on the screen, and then press  to confirm.

Figure 4-3 View a snapshot





Step 4 Press  or  to view the previous or next snapshot. Or you can press  to go back to the list of snapshots, and then select the one that you need.



To delete a snapshot, press , **Delete?** will appear on the screen, and then press  to confirm.


## 4.2 Time

Step 1 Press  to bring up the menu.

Step 2 Press  to select the part of the time that you want.

Step 3 Press  to or  to adjust the number.

## 4.3 Restoring to Default Settings

Step 1 Press  to bring up the menu.



Step 2 Press  to select **FactoryReset**.

Figure 4-4 Confirm your operation



Step 3 Press , and then the device will restart.

# Appendix 1 Cybersecurity Recommendations

## **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.