2-wire Switch

User’s manual

V1.0.1

Foreword

General

This manual introduces basic operations of the digital door station (hereinafter referred to as "VTO").

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Date
V1.0.1	Revise the Structure chapter.	October 2021
V1.0.0	First release.	December 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.

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interfaces used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

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, and keep the manual safe for future reference.

Operation Requirements

- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.
- Please use battery properly to avoid fire, explosion and other dangers.
- Please replace used battery with battery of the same type.
- If you use power plug or appliance coupler as disconnecting device, please maintain the disconnecting device available to be operated all the time.

Installation Requirements

 **WARNING**

- Connect the device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might become damaged.

- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.
- The device must be installed on solid and flat surface in order to guarantee safety under load and earthquake. Otherwise, it may cause Device to fall off or turnover.

Table of Contents

1 Introduction

1.1 Product Overview

The switch provides one 2-wire P port, two 2-wire cascading ports and two RJ-45 ports. You can connect up to 10 switches together to bring as many as 200 devices into the network. This is applicable to an apartment where there are many tenants. When connected to network through the switch, 2-wire indoor monitors (VTH) can make calls, unlock doors and monitor.

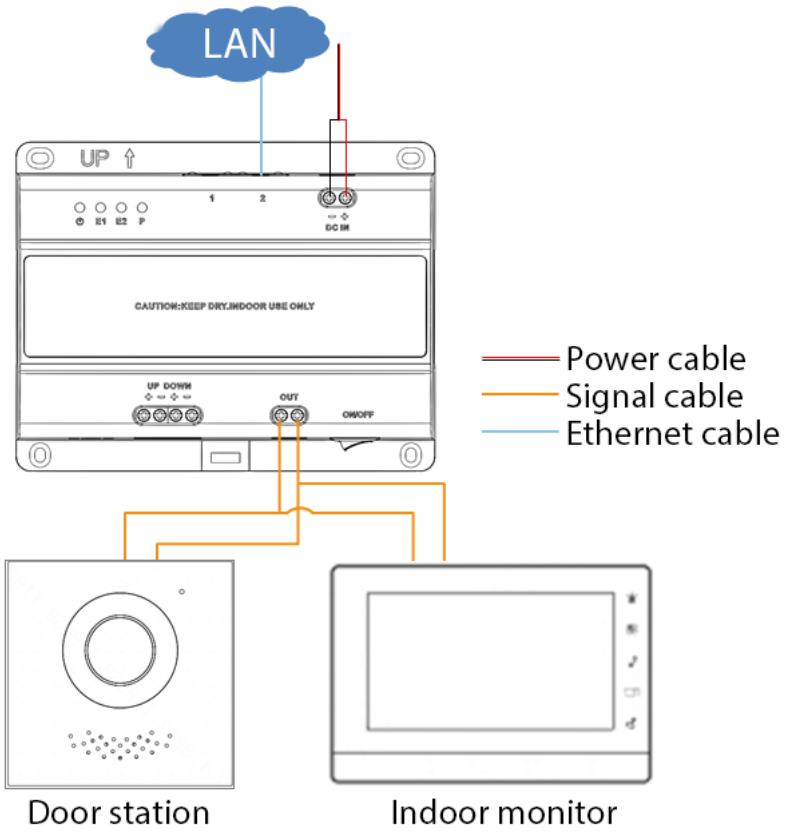
1.2 Application

A single 2-wire switch can connect at most 20 VTHs and 2 door stations (VTOs). Based on the total number of devices, we have villa and apartment.

Villa

If there are no more than 20 VTHs and 2 VTOs, they can all connect to the same switch.

Figure 1-1 Villa network diagram



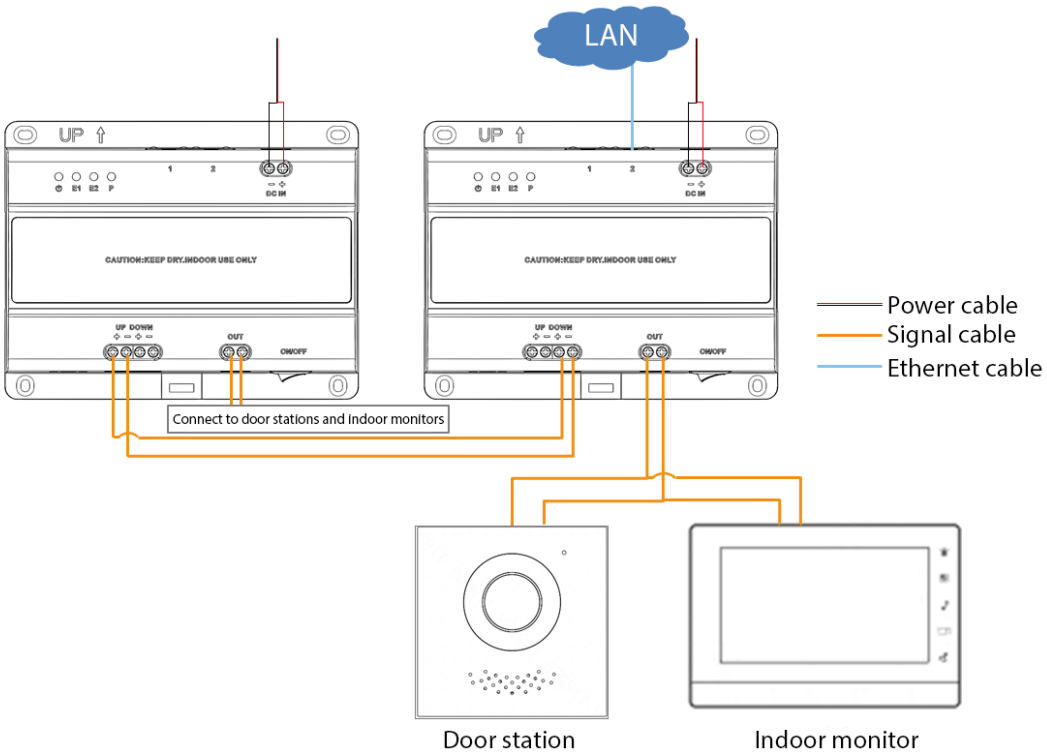
Apartment

If there are more than 20 VTHs and 2 VTOs, you need more than one switch to connect them all to the network. Use the 2-wire cascading ports or RJ-45 ports to connect the switches as needed, and make

sure that all the switches are connected to the same network. Take cascading with the 2-wire cascading ports as an example.

The cable connection of cascading with RJ-45 ports is the same as villa.

Figure 1-2 Apartment network diagram with 2-wire cascading ports



See the instruction below when choosing the right signal cables for the amount of devices you have:

R (total resistance) = 6V/the number of VTHs/0.1A (the average current for each VTH)

For example, the total resistance of the cables for 5 VTHs must be less than 6V/5/0.1A = 12Ω.

Table 1-1 Description of using different cables

Cable Type for Cascading	Supported Device Quantity	Maximum Distance
2-core cable 4-core cable	20 VTHs and 2 VTOs.	50 m: ● Between two switches. ● Between one switch and one VTH/VTO.
Ethernet cable	12 VTHs and 2 VTOs.	● 50 m. Between two switches. ● 30 m. Between one switch and one VTH/VTO. Because each core in an Ethernet cable has a relatively large impedance, we recommend that the cable should not be longer than 30 m.

- The cable between 1 switch and one VTO/VTH must be longer than 1 m.
- When using multiple switches, make sure that each switch is at least 3 m from the other ones.

2 Structure

2.1 Front Panel

Figure 2-1 Front panel structure

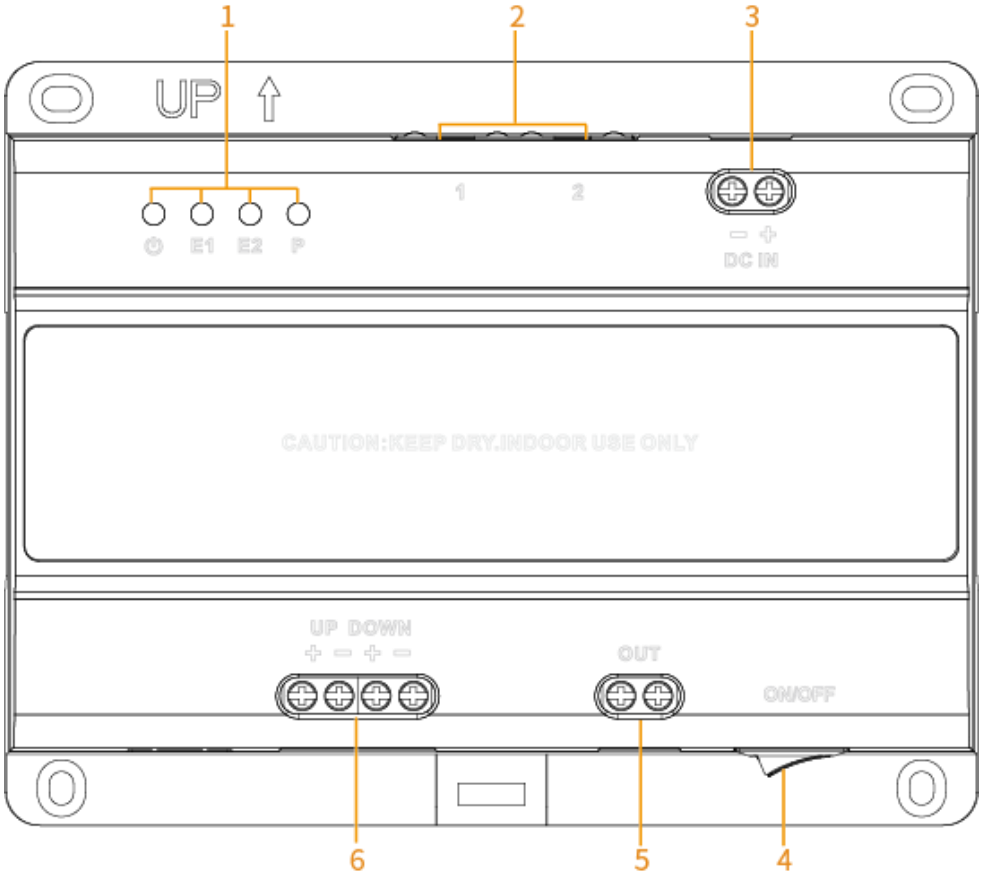


Table 2-1 Structure description

No.	Item	Description
1	Indicator	From left to right: ● POWER. ◇ Red: Powered on. ◇ Off: No power. ● E1. ◇ Green flashes: The device is properly connected to uplink port. ◇ Solid green: No signal from the uplink port. ◇ Off: The device is powered off or malfunctioning. ● E2. ◇ Green flashes: The device is properly connected to downlink port. ◇ Solid green: No signal from the downlink port. ◇ Off: The device is powered off or malfunctioning. ● P. ◇ Green flashes: Received PLC signal that either the VTH or VTO that is properly connected to the switch. ◇ Solid green: All VTHs and VTOs are not properly connected. ◇ Off: The devices are powered off or malfunctioning.
2	Network	2 RJ-45 ports.
3	Power input	Use 48 VDC power supply.
4	OFF/ON	Power switch.
5	2-wire ports	Connect up to 20 VTHs and 2 VTOs with no positive or negative poles (OUT 48 VDC).
6	Uplink and downlink ports	● UP. Connect the positive pole to that of the downlink port of the previous switch, and the same for the negative pole. ● DOWN. Connect the positive pole to that of the uplink port of the subsequent switch, and the same for the negative pole. Under certain conditions, these two ports can be connected to the EOC port of a VTO, and you also need to connect the two positive poles together and the same for the negative poles.

Before connecting cables, power off the switch first to avoid damaging it.

2.2 Rear Panel

Figure 2-2 Rear panel structure

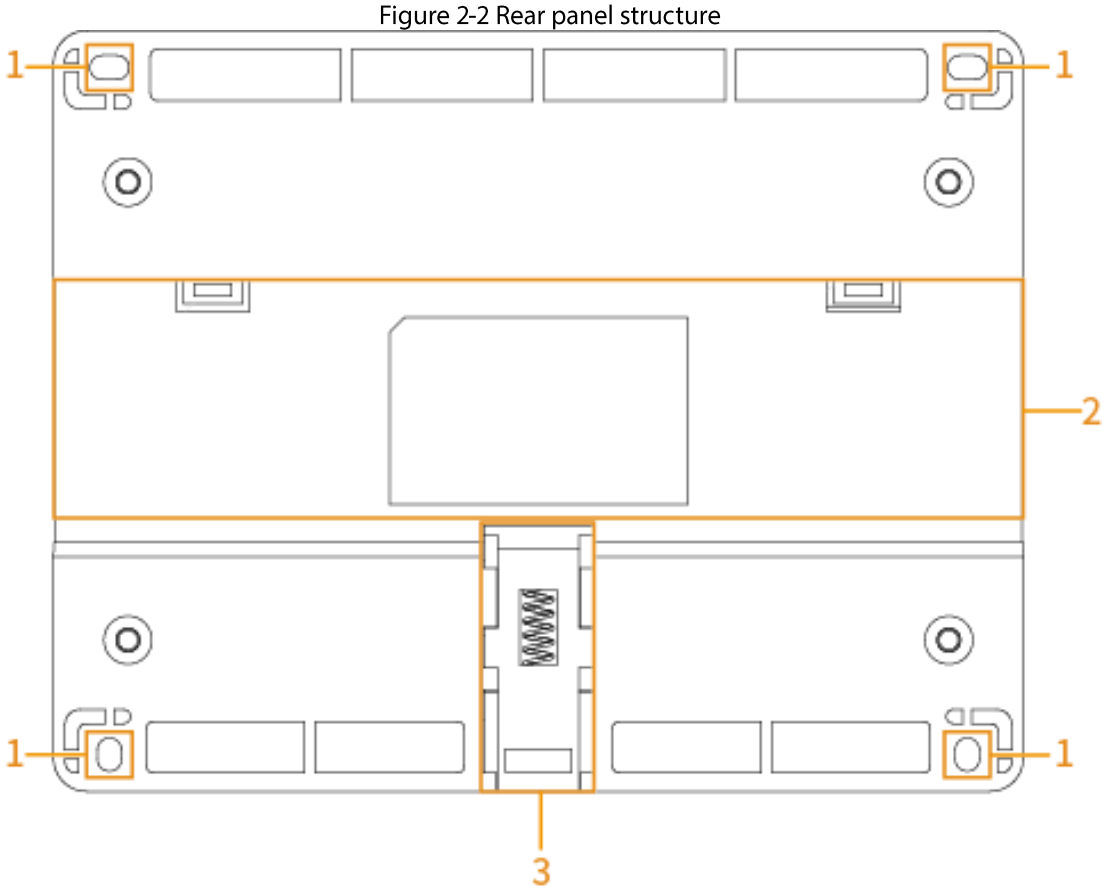


Table 2-2 Structure description

No.	Item	Description
1	Screw holes	Use four ST3 × 18-SUS to install the switch. See "4.1 Installing with Screws".
2	Rail	Use a guide rail to install the switch. See "4.2 Installing with Slide Rail".
3	Lower hook	Fix the switch when installing with a guide rail.

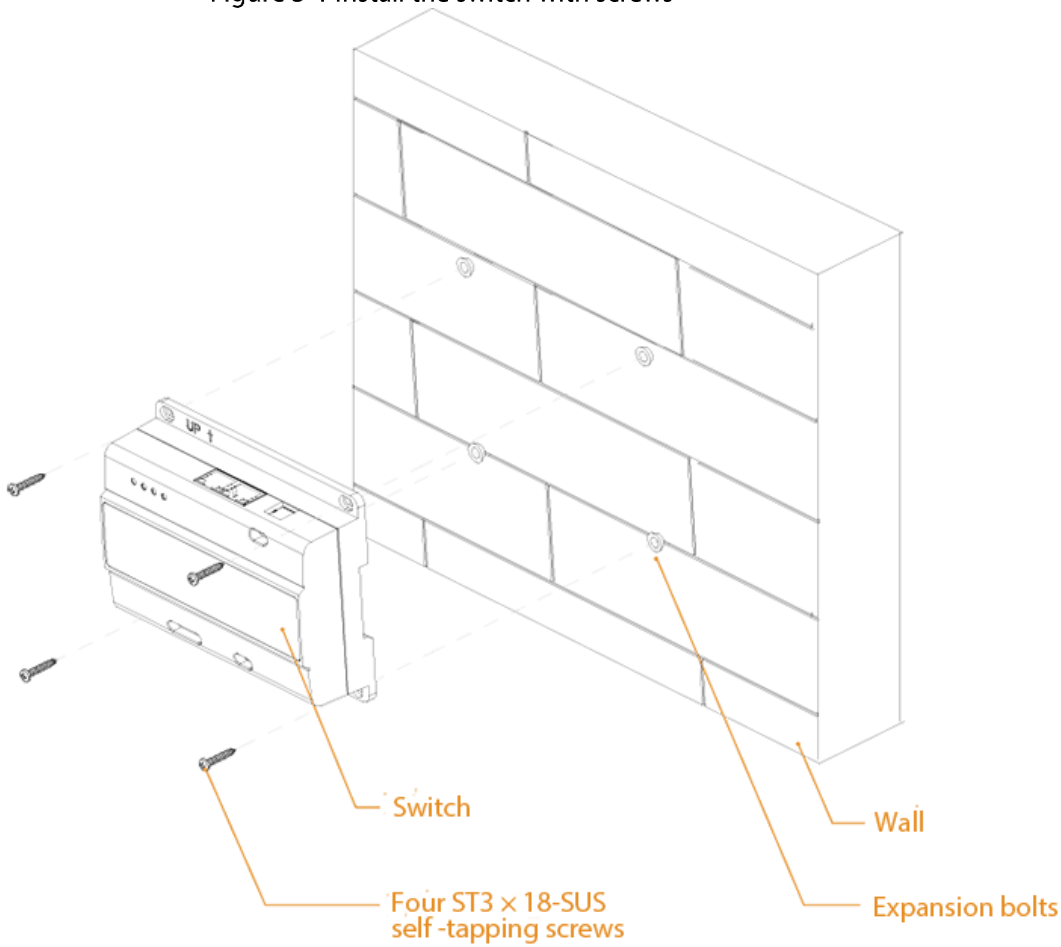
3 Installation

The chapter introduces how to install the switch on the wall with screws or a guide rail.

3.1 Installing with Screws

Use screws to fix the switch at a proper location on the wall.

Figure 3-1 Install the switch with screws



3.2 Installing with a Guide Rail

Preparation

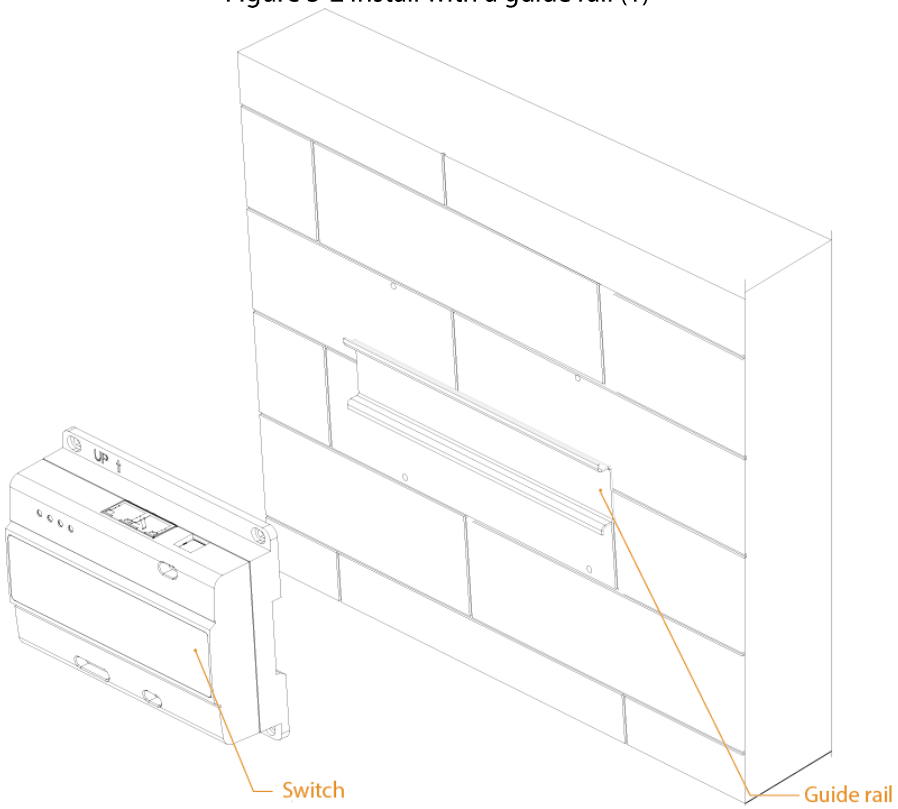
Prepare a standard 35 mm guide rail.

The switch does not come with a guide rail.

Procedure

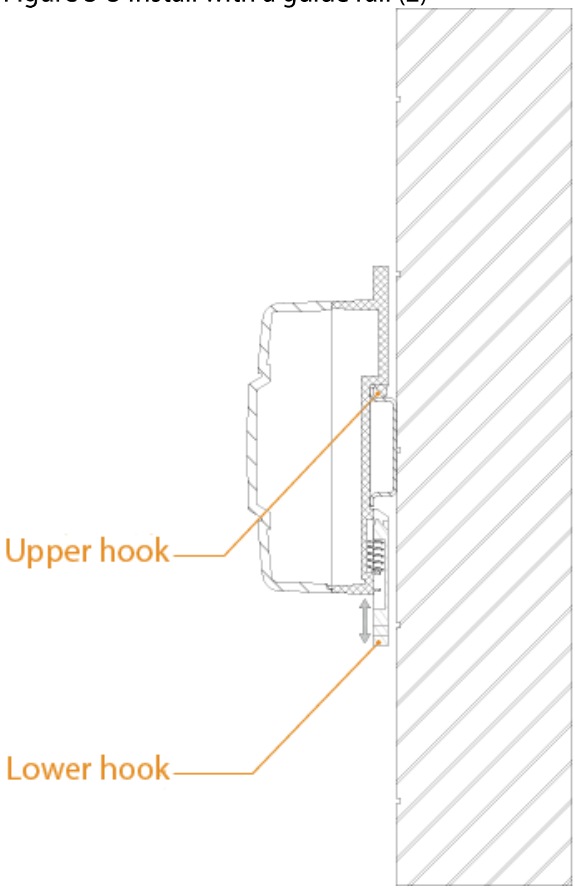
Step 1 Fix the guide rail at a proper location on the wall.

Figure 3-2 Install with a guide rail (1)



Step 2 Fix the upper hooks inside the slot of the guide rail.
Step 3 Pull down the lower hook and press the switch close to the guide rail.
Step 4 Let go of the lower hook.

Figure 3-3 Install with a guide rail (2)



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.