# 2-wire Switch

## User's manual

V1.0.0

# Foreword

## General

This manual introduces the structure and installation of the 2-wire switch (hereinafter referred to as the "switch").

## 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 Time |
|---|---|---|
| V1.0.0 | First release. | December 2020 |

# Important Safeguards and Warnings

This chapter introduces the contents covering proper handling of the switch, hazard prevention, and prevention of property damage. Read these contents carefully before using the switch, comply with them when using, and keep the manual well for future reference.

## Operation Requirement

- Change the default password after the switch is armed.
- Do not expose the switch to direct sunlight or near heat source.
- Do not expose the switch to dampness or dust.
- Install the switch horizontally or at a stable place to prevent it from falling.
- Do not drop or splash liquid onto the switch, or put anything filled with liquid onto the switch.
- Install the switch at a well-ventilated place, and do not block its vent.
- Use the switch within the rated range of power input and output.
- Do not dismantle the switch by yourself.
- Use the provided power supply.
- Before connecting cables, read and understand the structure first. See "2 Structure". for details.
- Before power on, make sure that all the cables are correctly connected.
- After powered on, if the POWER indicator is solid red, and RUN indicator flashes green, the switch is working properly.
- Before unplugging the power cable, make sure that the power switch is turned to "OFF".
- For best performance, only the first switch needs to be connected to the Ethernet when cascading multiple switches.
- Do not stack the switches on one another.

## Power Requirement

- The switch must use electric wires that conform to your local requirements and within their rated specifications.
- Use the power adapter provided with the switch; otherwise, it might result in people injury and device damage.
- 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 the label on the switch.
- For type I devices, use a grounded power socket.
- The appliance coupler is a disconnection device. Keep a convenient angle when using it.

# 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.

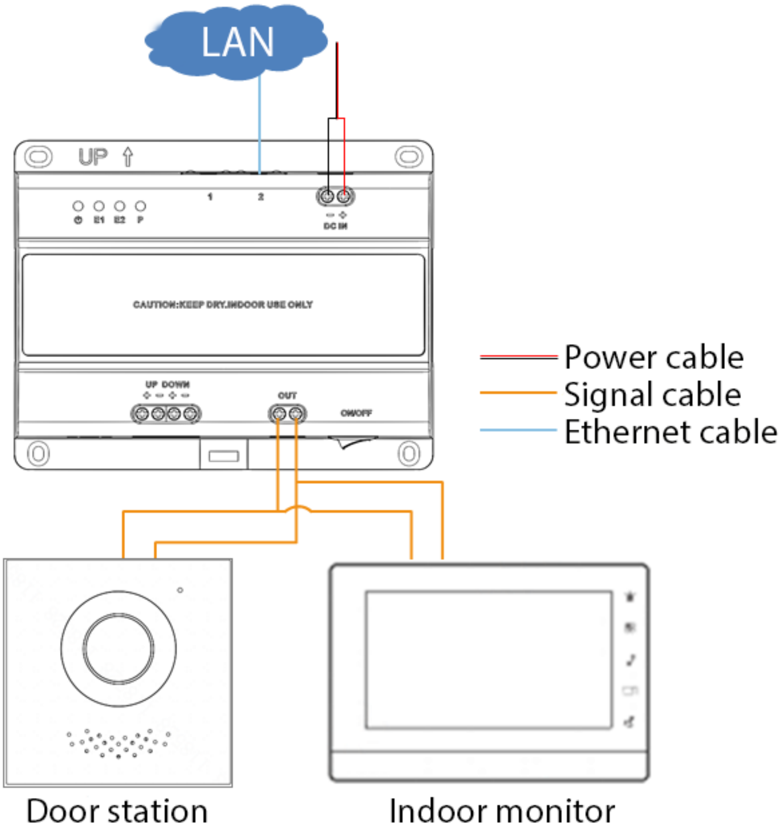
## 1.2 Application

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

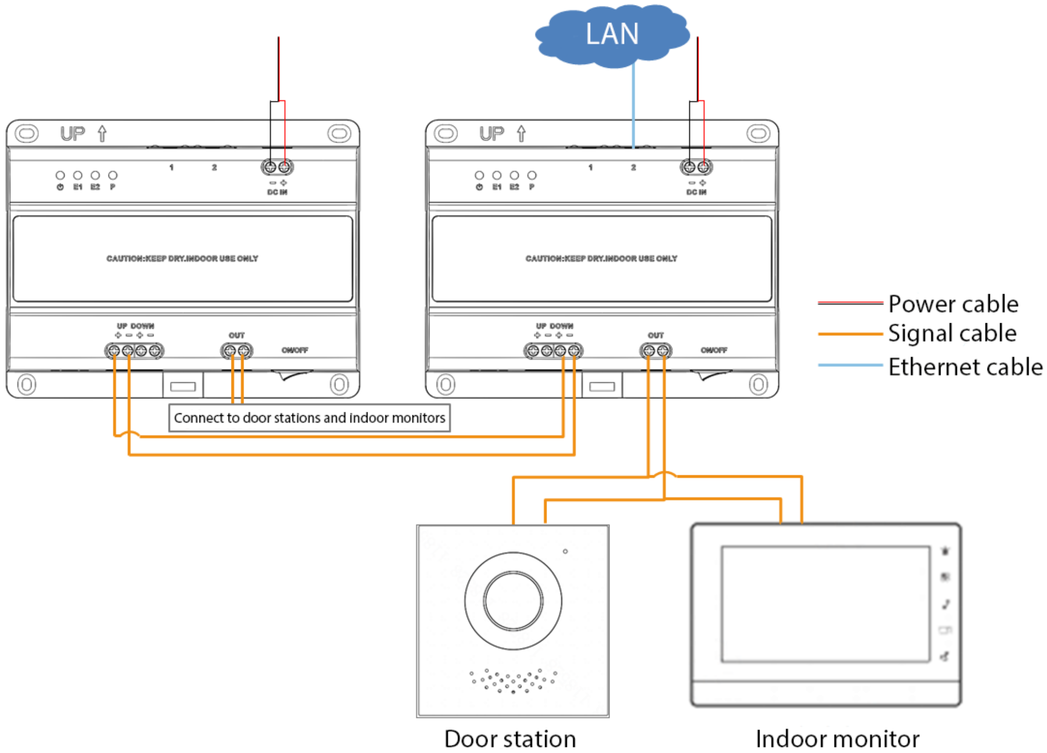


### Apartment

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 | 20 VTHs and 2 VTOs. | 50 m：<br>● Between 2 switches.<br>● Between 1 switch and 1 VTH/VTO. |
| 4-core cable | | |
| Ethernet cable | 12 VTHs and 2 VTOs. | ● 50 m.<br>Between 2 switches.<br>● 30 m.<br>Between the switch and VTO when there is only 1 VTO.<br>● 5 m and 30m.<br>The distance from the 2 VTOs to the switch. |

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

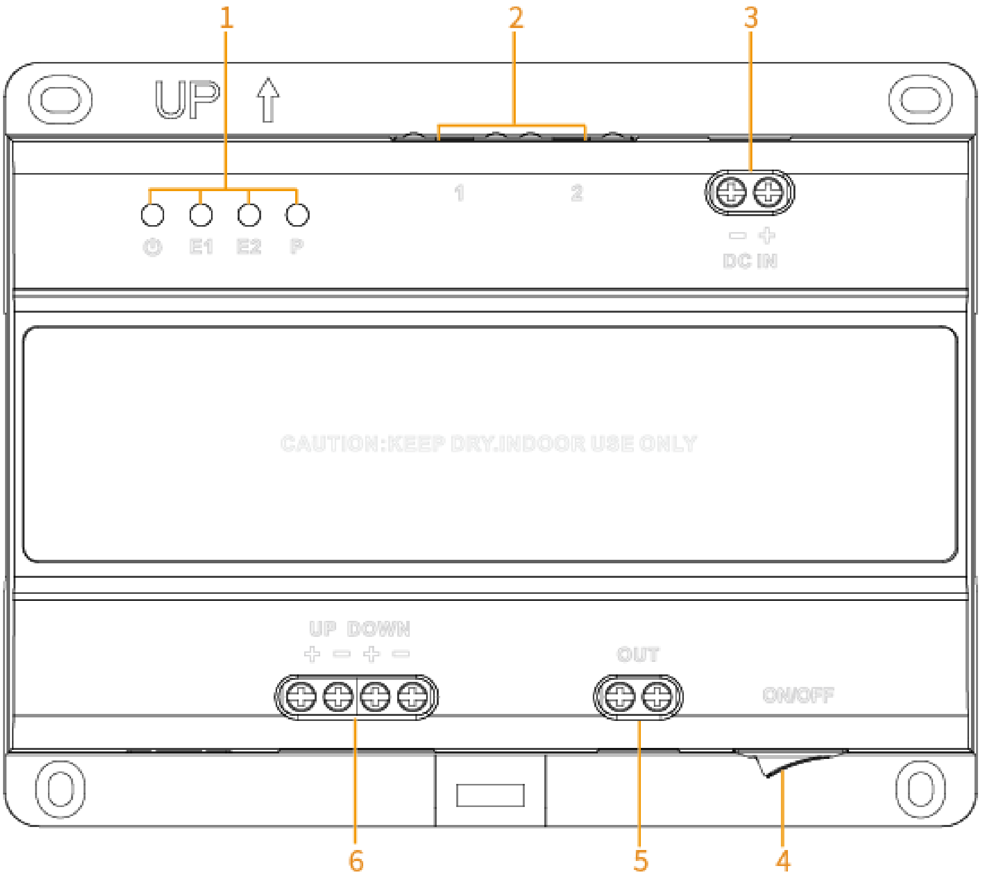


Table 2-1 Structure description

| No. | Item | Description |
|---|---|---|
| 1 | Indicator | From left to right:<br>● POWER.<br>◇ Red: Powered on.<br>◇ Off: No power.<br>● E1.<br>◇ Green flashes: The device is properly connected to uplink port.<br>◇ Solid green: No signal from the uplink port.<br>◇ Off: The device is powered off or malfunctioning.<br>● E2.<br>◇ Green flashes: The device is properly connected to downlink port.<br>◇ Solid green: No signal from the downlink port.<br>◇ Off: The device is powered off or malfunctioning.<br>● P.<br>◇ Green flashes: Received PLC signal that either the VTH or VTO that is properly connected to the switch.<br>◇ Solid green: All VTHs and VTOs are not properly connected.<br>◇ Off: The devices are powered off or malfunctioning. |

| No. | Item | Description |
|---|---|---|
| 2 | Network | 2 RJ-45 ports. |
| 3 | Power input | Use 48V DC 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. |
| 6 | Uplink and downlink ports | ● UP.<br>Connect the positive pole to that of the downlink port of the previous switch, and the same for the negative pole.<br>● DOWN.<br>Connect the positive pole to that of the uplink port of the subsequent switch, and the same for the negative pole.<br>📖<br>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

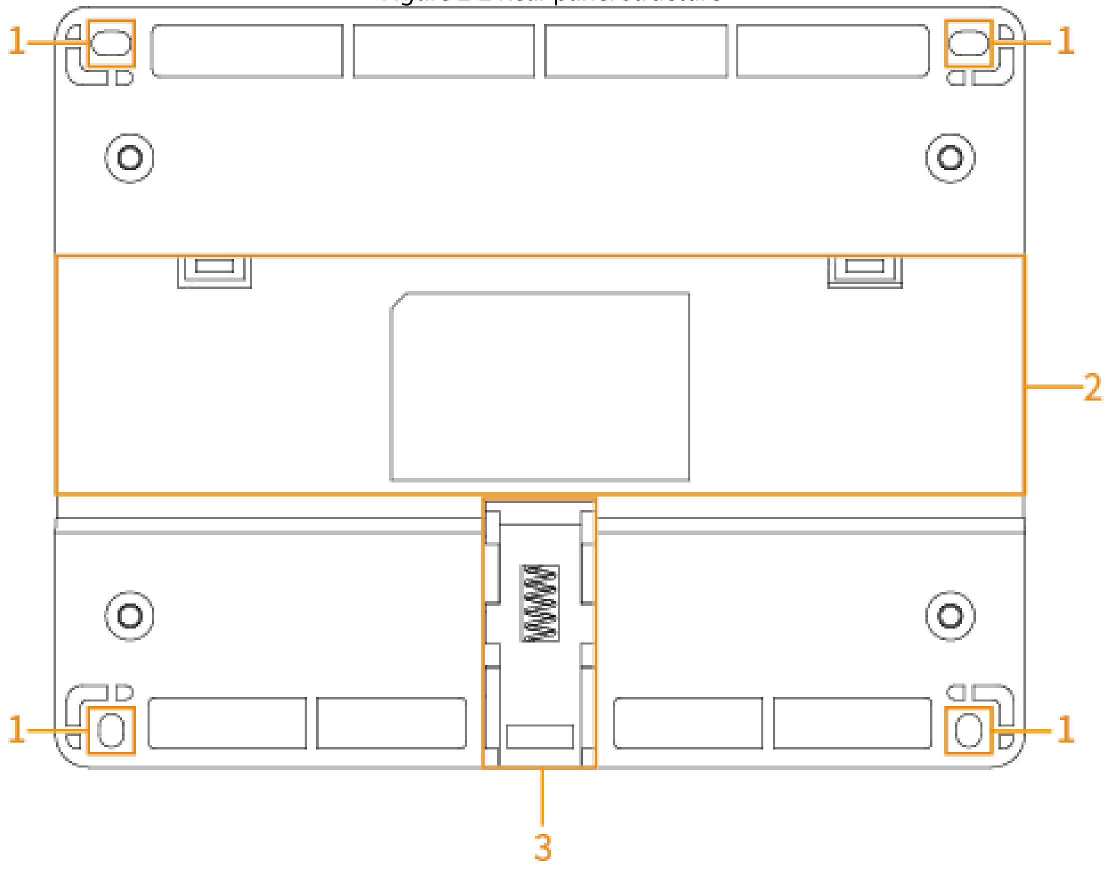


Table 2-2 Structure description

| 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. |

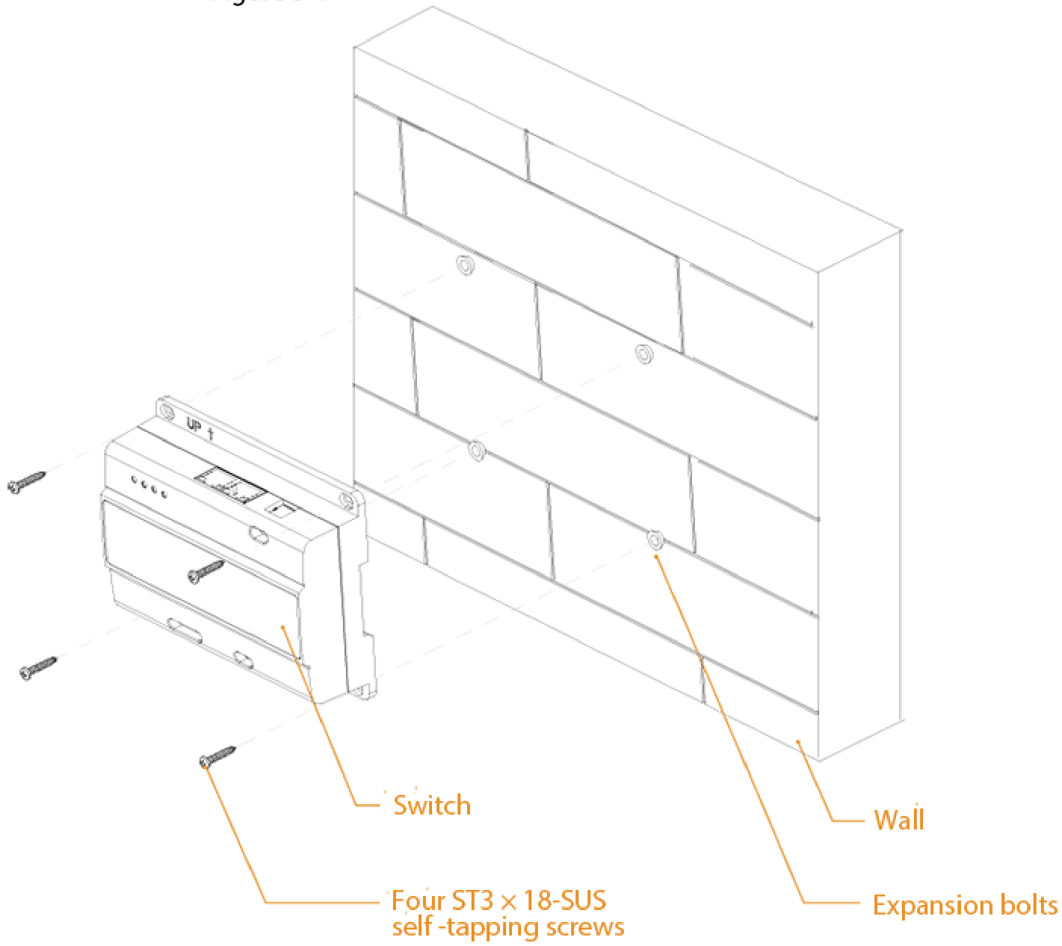
# 3 Installation

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.

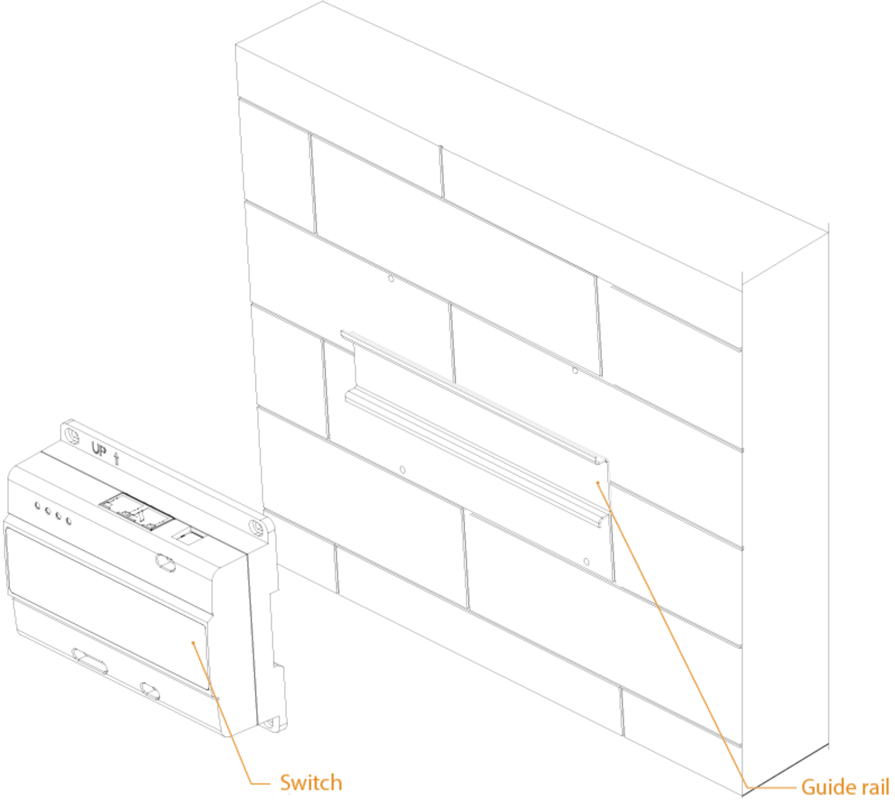
📖

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)

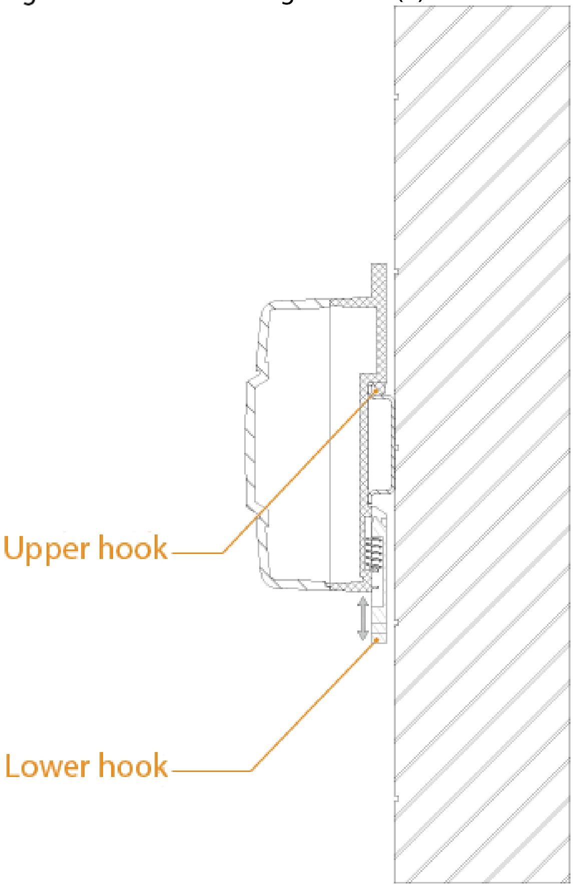


Step 2 Fix the upper hooks inside the slot of the guide rail.

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.