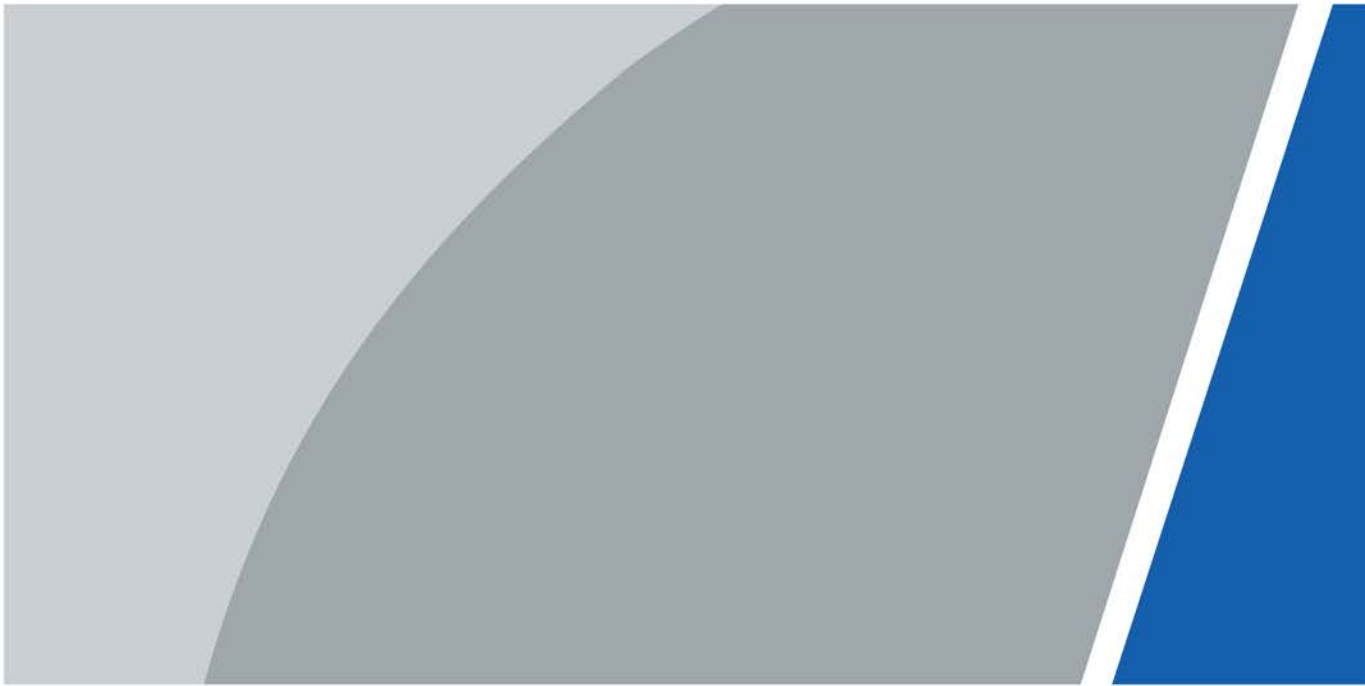# Ethernet Switch (4/8-port Unmanaged Hardened Switch)

Quick Start Guide

V1.0.1

Foreword

General

This manual mainly introduces the hardware, installation, and wiring steps of the 4/8-port unmanaged hardened switch (hereinafter referred to as "the device").

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, reductions in performance, or unpredictable results.
⚿ TIPS	Provides methods to help you solve a problem or save time.
📖 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	● Updated **Important Safeguards and Warnings**. ● Updated **1.1 Introduction**. ● Updated **1.2 Features**. ● Updated **2.1 Front Panel**, added Figure 2-2. ● Updated **2.2 Side Panel**, added Figure 2-4 and Table 2-3. ● Updated Figure 4-1 GND port.	July 2021
V1.0.0	First release.	April 2021

Privacy Protection Notice

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

The manual helps you to use our product properly. To avoid danger and property damage, read the manual carefully before using the product, and we highly recommend you to keep the manual well for future reference.

Operating Requirements

- Transport, use, and store the device in allowed humidity and temperature ranges.
- Avoid liquids splashing on the device. Do not place objects full of liquid on the device to avoid liquid flowing into the device.
- Do not disassemble the device without professional instruction.
- Use the device at rated input and output voltage.
- 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.
- When removing the cable, power off the device first to avoid personal injury.
- Operating temperature range: −30 °C (-22 °F) to +65 °C (149 °F).
- This is a class A product. In a domestic environment this may cause radio interference in which case the user may be required to take adequate measures.

Installation Requirements

- Observe all safety procedures and wear required protective equipment provided for your use while working at height.
- Use the battery properly to avoid fire, explosions, and other dangers.
- Do not expose the device directly to sunlight, and keep it away from heat.
- Do not install the device in a damp environment, and keep it away from dust and soot.
- Install the device in a well-ventilated environment. Do not block the vent of the device.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to power requirements of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- Connect the device with the adapter before power on.
- Do not connect the device to more than one power supply. Otherwise, the device might be damaged.
- 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.
- Be sure to ground the device (cross section of copper wire: > 2.5 mm^2; resistance to ground: ≤ 4 Ω).
- Voltage stabilizers and lightning protection devices are optional according to the power supply and surrounding environment.
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 10 cm on the sides and 10 cm on top of the device.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- Do not block the ventilator of the device with objects, such as newspaper, table cloth or curtains.
- Do not put open flames, such as a lit candle, on the device.

Maintenance Requirements

- Power off the device before maintenance.
- Mark key components on the maintenance circuit diagram with warning signs.

Table of Contents

1 Overview

1.1 Introduction

The device is a hardened switch. It provides a high-performance switching engine and large buffer memory to ensure smooth video stream transmission. With its full-metal and fanless design, the device has great heat dissipation capabilities on its shell surface, and is able to work in environments that range from–30 ℃ (-22 ℉) to +65 ℃149 ℉). With its DIP design, it provides a variety of work modes that suit different scenarios, including corridors and offices.

1.2 Features

- 4/8 × 10 Mbps/100 Mbps or 10 Mbps/100 Mbps/1000 Mbps Ethernet ports.
- Uplink ports include Ethernet ports and optical ports.
- All ports meet the requirements of IEEE802.3af and IEEE802.3at standards. The red ports also conform to Hi-PoE and IEEE802.3bt standards, and the orange ports conform to Hi-PoE standard.
- 250 m long-distance PoE transmission, which can be enabled by the DIP switch.
- PoE watchdog for real-time detection of terminal device status.
- Fanless.
- Desktop mount and DIN-rail mount.

2 Port and Indicator

2.1 Front Panel

The following figures are for reference only, and might differ from the actual product.

Figure 2-1 Front panel (with PoE)
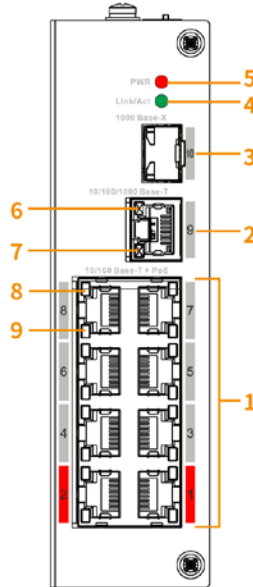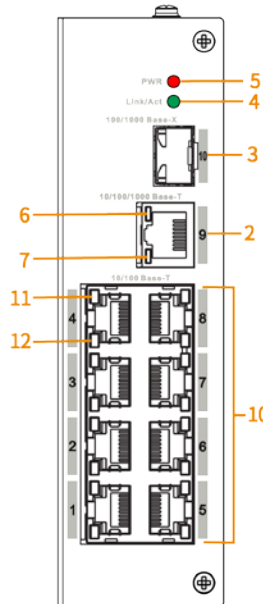

Figure 2-2 Front panel (without PoE)

Following are all the ports and indicators on the front panel of the 4/8-port unmanaged hardened switch. The actual device might only have some of these ports and indicators.

Table 2-1 Description of front panel

No.	Description
1	10 Mbps/100 Mbps or 10 Mbps/100 Mbps/1000 Mbps self-adaptive PoE Ethernet ports.

No.	Description
2	10 Mbps/100 Mbps/1000 Mbps self-adaptive uplink Ethernet port.
3	1000 Mbps self-adaptive uplink optical port.
4	Optical port connection or data transmission status indicator (Link/Act). ● On: Connected to device. ● Off: Not connected to device. ● Flashes: Transmitting data (1000 Mbps).
5	Power indicator. ● On: Power on. ● Off: Power off.
6	Uplink Ethernet port connection status indicator (Link). ● On: Connected to device. ● Off: Not connected to device.
7	Uplink Ethernet port data transmission status indicator (Act). ● Flashes: Transmitting data (10 Mbps/100 Mbps/1000 Mbps). ● Off: No data transmission.
8	PoE Ethernet ports status indicator. ● On: Powered by PoE. ● Off: Not powered by PoE.
9	Single-port connection or data transmission status indicator (Link/Act). ● On: Connected to device. ● Off: Not connected to device. ● Flashes: Transmitting data.
10	10 Mbps/100 Mbps or 10 Mbps/100 Mbps/1000 Mbps self-adaptive Ethernet ports.
11	Uplink Ethernet port connection status indicator (Link). ● On: Connected to device. ● Off: Not connected to device.
12	Uplink Ethernet port data transmission status indicator (Act). ● Flashes: Transmitting data (10 Mbps/100 Mbps/1000 Mbps). ● Off: No data transmission.

2.2 Side Panel

The following figures are for reference only, and might differ from the actual product.

Figure 2-3 Side panel (with PoE)
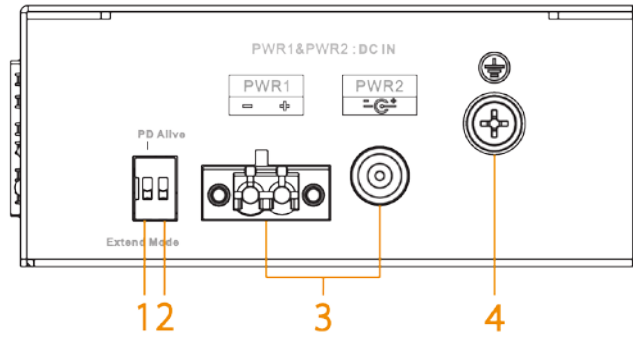
Table 2-2 Port description (with PoE)

No.	Description
1	PD Alive: When a terminal device crash is detected, the device will power down and restart the terminal device.
2	Extend Mode: Extends the maximum transmission distance to 250 m, but reduces average transmission speed to 10 Mbps.
3	Power port (dual power backup): Supports 48–57 VDC.
4	GND terminal.

Figure 2-4 Side panel (without PoE)
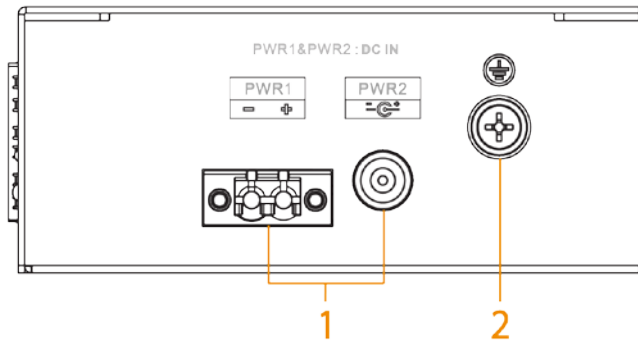
Table 2-3 Port description (without PoE)

No.	Description
1	Power port (dual power backup): Supports 12 VDC.
2	GND terminal.

3 Installation

The device supports DIN-rail mount. Hang the switch hook on the rail, and press the switch to make the buckle latch on to the rail.
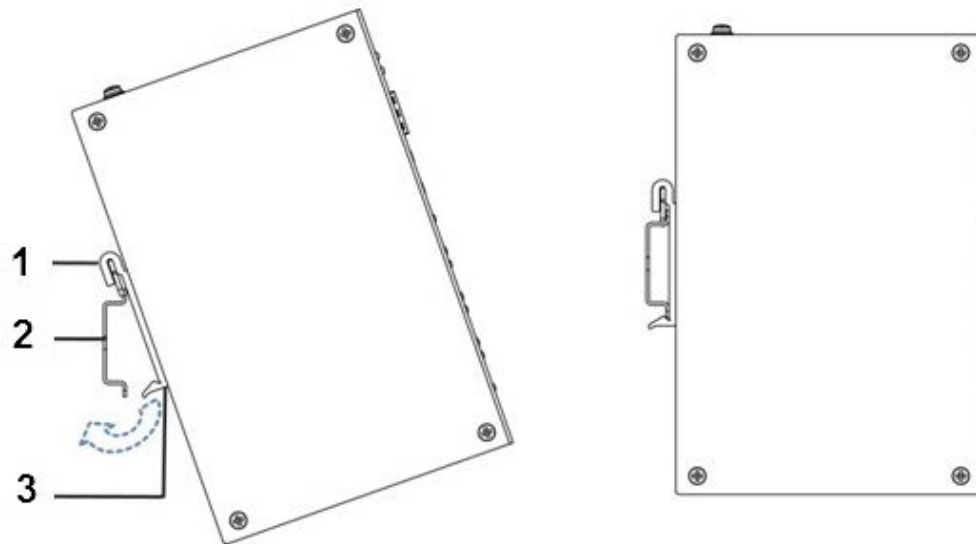
The width of the guide rail supported by the device is 50 mm.

Figure 3-1 DIN rail

No.	Name
1	Hook.
2	Rail.
3	Buckle.

4 Wiring

4.1 Connecting GND

Device GND connection helps ensure device lightning protection and anti-interference. You should connect the GND cable before powering on the device, and power off the device before disconnecting the GND cable. There is a GND screw on the device cover board for the GND cable. It is called enclosure GND.

Figure 4-1 GND port
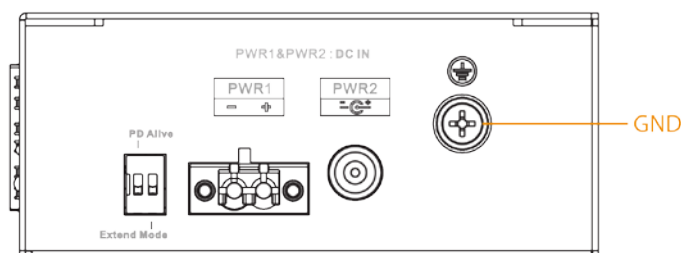
Step 1   Remove the GND screw from the enclosure GND with a cross screwdriver.

Step 2   Connect one end of the GND cable to the cold-pressed terminal, and attach it to the enclosure GND with the GND screw.

Step 3   Connect the other end of the GND cable to the ground.

The sectional area of the GND cable must be more than 2.5 mm^2, and the GND resistance must be less than 4 Ω.

4.2 Connecting Power Cord

Models with PoE support two power inputs: PWR1 and PWR2. You can select a backup power supply to ensure power is continuously provided, even if one channel of power breaks down. This greatly improves the reliability of network operations. Models without PoE only support power supplies through 12 VDC power adapters.

⚠ WARNING

To avoid personal injury, do not touch any exposed wires, terminals or areas of the device that have dangerous voltage levels. Do not dismantle parts or plug connectors into the device during power on.

⚠

Before connecting power, make sure that the power supply conforms to the power supply requirements on the device label. Otherwise, it might cause device damage.

The sectional area of the power cable must be more than 0.75 mm^2 (maximum sectional area 2.5 mm^2); ground resistance is required to be less than 4 Ω.

Table 4-1 Power terminal description

No.	Name
1	DIN rail port (–).
2	DIN rail port (+).
3	Power adapter port.

Step 1   Connect the device to the ground.

Step 2   Take off the power terminal plug from the device.

Step 3   Insert one end of the power cable into the power terminal plug according to requirements.

The sectional area of the power cable must be more than 0.75 mm^2 (maximum sectional area is 2.5 mm^2).

Step 4   Insert the plug that is connected to the power cable back into the corresponding power terminal socket of the device.

Step 5   Connect the other end of the power cable to the corresponding external power supply system according to the power supply requirements marked on the device, and check the power indicator of the device. If the indicator is on, then the power connection is correct.

4.3 Connecting SFP Ethernet Port

We recommend wearing antistatic gloves before installing the SFP module, and wearing an antistatic wrist, and confirm that the antistatic wrist is securely linked to the surface of the gloves.

Step 1   Lift the handle of SFP module vertically upward and attach it to the top hook.

Step 2   Hold the SFP module on both sides and push it gently into the SFP slot untill the SFP module is firmly connected to the slot (You will feel that both the top and bottom spring strip of the SFP module are securely attached with the SFP slot).

⚠ WARNING

The device uses laser to transmit signals via optical fiber cables. The laser conforms to the requirements of level 1 laser products. To avoid injury to your eyes, do not look at the 1000 Base-X optical port directly when the device is powered on.

⚠

● When installing the SFP optical module, do not touch the gold finger of the SFP optical module.

● Do not remove the dust plug of the SFP optical module before connecting the optical port.

● Do not directly insert the SFP optical module with the optical fiber inserted into the slot. Unplug the optical fiber before installing it.

Figure 4-2 SFP module structure
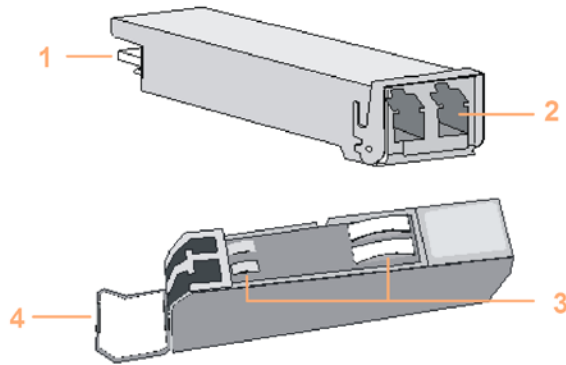
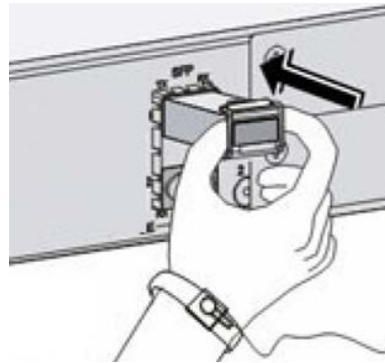| No.	Name
1	Gold finger.
2	Optical port.
3	Spring strip.
4	Handle.

Figure 4-3 SFP module installation

4.4 Connecting Ethernet Port

Ethernet port is a standard RJ-45 port. With its self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode. It supports MDI/MDI-X self-recognition of the cable, therefore, you can use a cross-over cable or straight-through cable to connect the terminal device to network device.

Figure 4-4 Ethernet port pin number
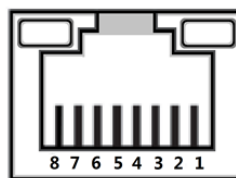
The cable connection of RJ-45 connector conforms to the standard 568B (1-orange white, 2-orange, 3-green white, 4-blue, 5-blue white, 6-green, 7-brown white, 8-brown).

Figure 4-5 Cable connection
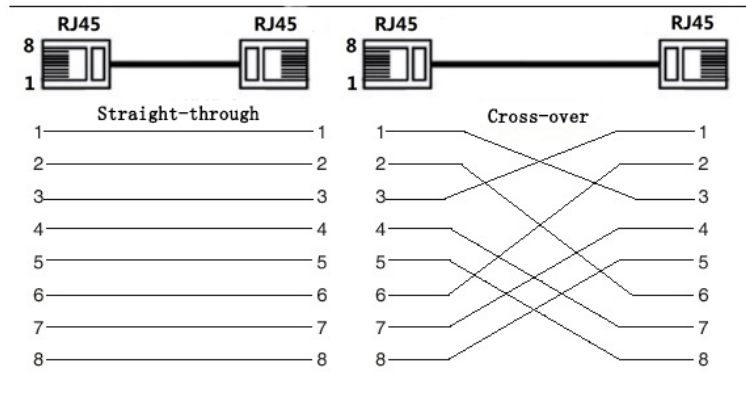
4.5 Connecting PoE Ethernet Port

If the terminal device has a PoE Ethernet port, you can directly connect the terminal device PoE Ethernet port to the switch PoE Ethernet port through the network cable to achieve synchronized network connection and power supply. The maximum distance between the switch and the terminal device is about 100 m.

⚠️

When connecting to a non-PoE device, the device needs to be used with an isolated power supply.

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.