

# Hardened Managed Switch

## Quick Start Guide








# Foreword

## General

This manual introduces the installation, functions and operations of the hardened managed switch (hereinafter referred to as "the Device"). Read carefully before using the device, and keep the manual safe for future reference.

## Safety Instructions

The following signal words 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 you time.
 <b>NOTE</b>	Provides additional information as a supplement to the text.

## Revision History

Version	Revision Content	Release Time
V1.0.1	Updated the description of the introduction and the laser product.	June 2022
V1.0.0	First release.	February 2022

## 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, and comply with the guidelines when using it.

## Transportation Requirements



Transport the device under allowed humidity and temperature conditions.

## Storage Requirements



Store the device under allowed humidity and temperature conditions.

## Installation Requirements



- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- 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.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- 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.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- 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.
- The device must be grounded by a copper wire with a cross-sectional area of 2.5 mm<sup>2</sup> and a ground resistance no more than 4 Ω.
- Voltage stabilizer and lightning surge protector are optional depending on the actual power supply on site and the ambient 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.

## Operation Requirements



- Do not disassemble the device without professional instruction.
- Operate the device within the rated range of power input and output.
- Make sure that the power supply is correct before use.
- Make sure the device is powered off before disassembling wires to avoid personal injury
- Do not unplug the power cord on the side of the device while the adapter is powered on.



- Use the device 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.
- Operating temperature:  $-30\text{ }^{\circ}\text{C}$  ( $-22\text{ }^{\circ}\text{F}$ ) to  $+65\text{ }^{\circ}\text{C}$  ( $+149\text{ }^{\circ}\text{F}$ ).
- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- Do not block the ventilator of the device with objects, such as a newspaper, table cloth or curtain.
- Do not place an open flame on the device, such as a lit candle.

## Maintenance Requirements



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

# Table of Contents

<b>Foreword</b> .....	I
<b>Important Safeguards and Warnings</b> .....	III
<b>1 Overview</b> .....	1
<b>1.1 Introduction</b> .....	1
<b>1.2 Features</b> .....	1
<b>2 Port and Indicator</b> .....	2
<b>2.1 Front Panel</b> .....	2
<b>2.2 Side Panel</b> .....	3
<b>3 Installation</b> .....	4
<b>4 Wiring</b> .....	5
<b>4.1 Connecting GND</b> .....	5
<b>4.2 Connecting Power Cord</b> .....	5
<b>4.3 Connecting SFP Ethernet Port</b> .....	6
<b>4.4 Connecting Ethernet Port</b> .....	8
<b>4.5 Connecting PoE Port</b> .....	8
<b>5 Quick Operation</b> .....	9
<b>5.1 Login through Web</b> .....	9
<b>5.2 Restoring to Factory Settings</b> .....	9
<b>Appendix Cybersecurity Recommendations</b> .....	10

# 1 Overview

## 1.1 Introduction

The product is a professional device. The Device is layer-2 hardened switch. Equipped with high performance switching engine and large buffer memory, it features low transmission delay and high reliability. The full-metal and fanless design and efficient surface heat dissipation enable it to work in the environment from  $-30\text{ }^{\circ}\text{C}$  ( $-22\text{ }^{\circ}\text{F}$ ) to  $+65\text{ }^{\circ}\text{C}$  ( $+149\text{ }^{\circ}\text{F}$ ). With web management and direct connection to iLinksView, the Device can offer multiple working modes and meet different requirements under different scenarios.

The Device is applicable for use in different scenarios, including corridors, factories and offices.

## 1.2 Features

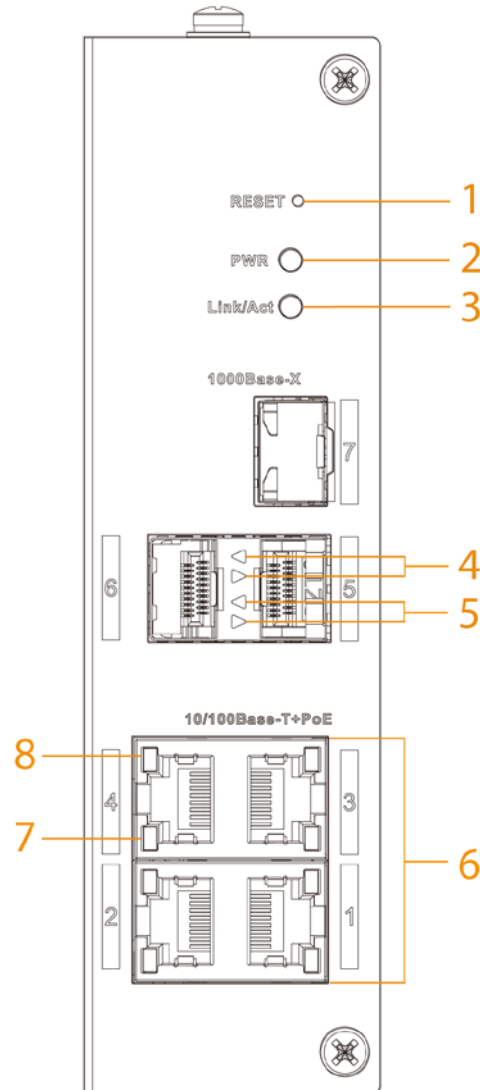
- $4 \times 100$  Mbps Ethernet ports, and  $3 \times 1000$  Mbps uplink optical ports.
- All ports meet the requirements of IEEE802.3af and IEEE802.3at standards. The red ports also conform to Hi-PoE and IEEE802.3bt standards.
- 4 kV/CM, 2 kV/DM, lightning and surge protection.
- IEEE802.1Q-based VLAN configuration.
- 250 m long-distance PoE transmission (10 Mbps).
- PoE watchdog.
- 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



The following are all the ports and indicators on the front panel of the Device.

Table 2-1 Description of front panel

No.	Description
1	Reset button. Press and hold it for more than 5 s, and release after the panel status indicators are all on to restore the Device to default settings.
2	Power Indicator. <ul style="list-style-type: none"> <li>● On: Power on.</li> <li>● Off: Power off.</li> </ul>



No.	Description
3	Optical-port connection or data transmission status indicator (Link/Act). <ul style="list-style-type: none"> <li>● On: Connected to device.</li> <li>● Off: Not connected to device.</li> <li>● Flashes: Transmitting 1000 Mbps data.</li> </ul>
4	Optical-port connection status indicator (Link). <ul style="list-style-type: none"> <li>● On: Connected to device.</li> <li>● Off: Not connected to device.</li> </ul>
5	Optical-port connection or data transmission status indicator (Link/Act). <ul style="list-style-type: none"> <li>● On: Connected to device.</li> <li>● Off: Not connected to device.</li> <li>● Flashes: Transmitting 1000 Mbps data.</li> </ul>
6	10/100 Mbps adaptive PoE port.
7	Single-port connection or data transmission status indicator (Link/Act). <ul style="list-style-type: none"> <li>● On: Connected to device.</li> <li>● Off: Not connected to device.</li> <li>● Flashes: Transmitting data.</li> </ul>
8	Single-port PoE status indicator. <ul style="list-style-type: none"> <li>● On: Powered by PoE.</li> <li>● Off: Not powered by PoE.</li> </ul>

## 2.2 Side Panel

The following figure is for reference only, and might differ from the actual product.

Figure 2-2 Side panel

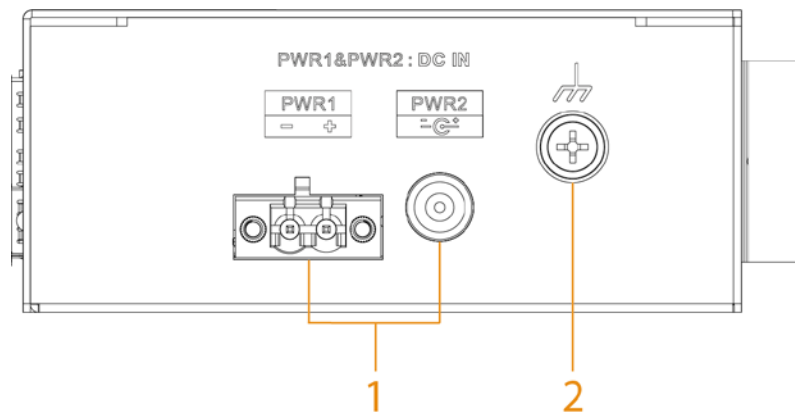


Table 2-2 Port description

No.	Description
1	Power port (dual power backup). Supports 48–57 VDC.
2	GND screw.

# 3 Installation

The Device supports DIN-rail mount. Hang the hook on the rail, press the Device to make the buckle stuck into the rail.



The width of the guide rail supported by the Device is 50 mm.

Figure 3-1 DIN rail

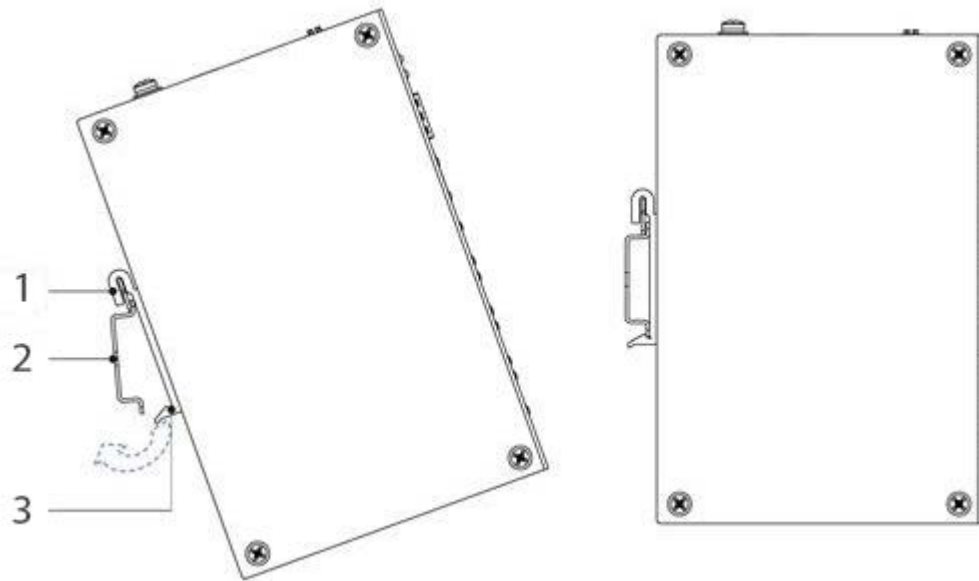


Table 3-1 Component description

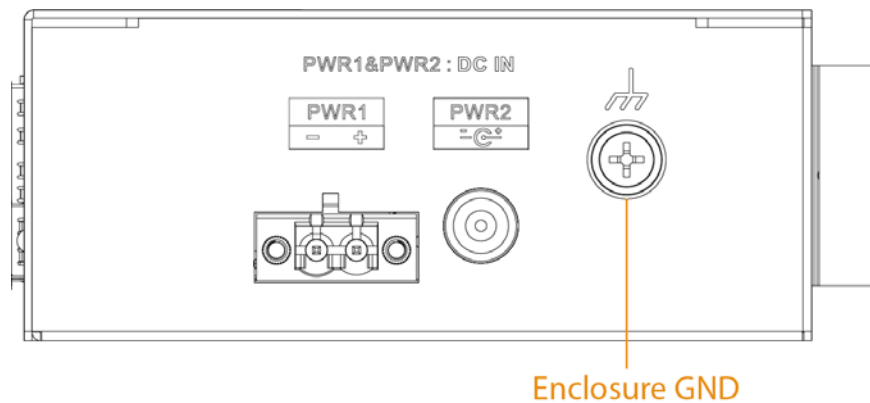
No.	Description
1	Hook
2	Rail
3	Buckle

# 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, which is called enclosure GND.

Figure 4-1 GND port



- Step 1** Remove the GND screw at the enclosure GND with a cross screwdriver.
- Step 2** Connect one end of the GND cable with the cold-pressed terminal, and fix it on 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 needs to be more than 2.5 mm<sup>2</sup>, and the GND resistance needs to be less than 4 Ω.

## 4.2 Connecting Power Cord

Redundant power input supports two-channel power, which are PWR2 and PWR1. You can select the other power for continuous power supply when one channel of power breaks down, which greatly improves the reliability of network operation.

 **WARNING**

To avoid personal injury, do not touch any exposed wire, terminal and areas with danger voltage of the Device and do not dismantle parts or plug connector 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.

Figure 4-2 Power terminal

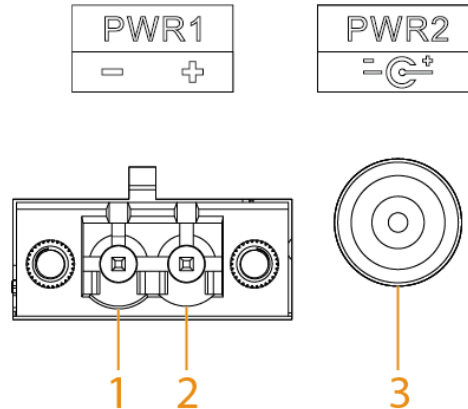


Table 4-1 Power terminal description

No.	DC Wiring Definition
1	PWR1-
2	PWR1+
3	PWR2

Step 1 Connect the Device to 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 the requirement.



The sectional area of power cable needs to be more than 0.75 mm<sup>2</sup> (max sectional area 2.5 mm<sup>2</sup>).

Step 4 Insert the plug which is connected to power cable back to the corresponding power terminal socket of the Device.

Step 5 Connect the other end of power cable to the corresponding external power supply system according to the power supply requirement marked on the Device, and check if the corresponding power indicator light of the Device is on, it means power connection is correct if the light is on.

## 4.3 Connecting SFP Ethernet Port

We recommend wearing antistatic gloves, then the antistatic wrist before installing SFP module. Make sure that the antistatic wrist and the surface of the gloves are in good contact.

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

Step 2 Hold the SFP module on both sides and push it gently into the SFP slot until the SFP

module is firmly connected to the slot (You can feel that both the top and bottom spring strip of the SFP module are firmly stuck with the SFP slot).



**WARNING**

### Class 1 Laser Product

The Device uses laser to transmit signal via optical fiber cable. The laser conforms to the requirements of Class 1 laser products. To avoid injury upon eyes, do not look at the 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 4-3 SFP module structure

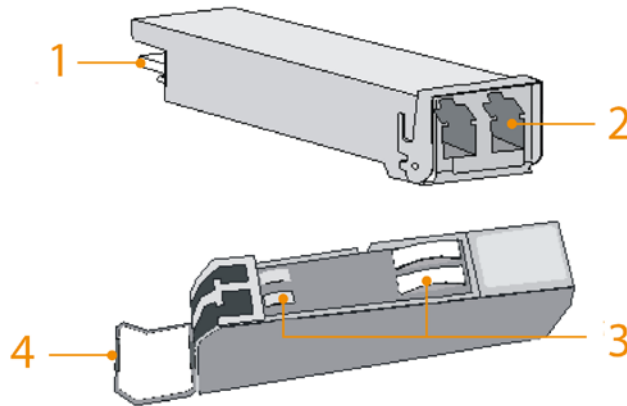
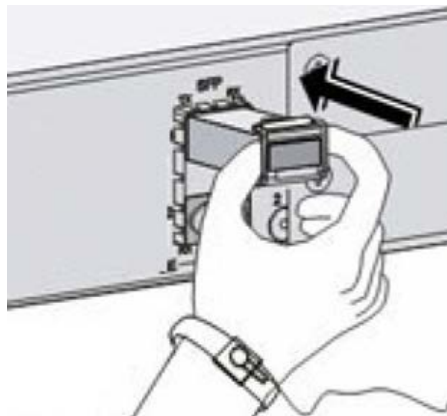


Table 4-2 Structure description

No.	Description
1	Gold finger
2	Optical fiber port
3	Spring strip
4	Handle

Figure 4-4 SFP module installation



## 4.4 Connecting Ethernet Port

Ethernet port is a standard RJ-45 port. With 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 cross-over cable or straight-through cable to connect terminal device to network device.

Figure 4-5 Ethernet port pin number

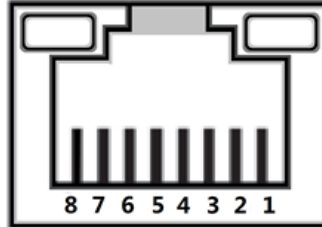
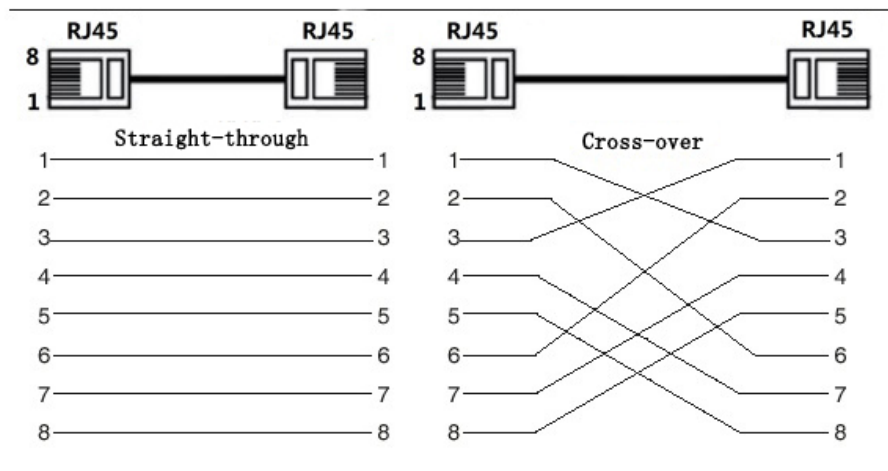


Figure 4-6 Cable connection



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).

## 4.5 Connecting PoE Port

If the terminal device has a PoE port, you can directly connect the terminal device PoE port to the switch PoE port through 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.

# 5 Quick Operation

## 5.1 Login through Web

You can log in to the Device through web for management and operation. For details, see web operation manual.



For first login, you need to change the password according to the prompt.

Table 5-1 Default factory configuration

Parameter	Description
IP address	192.168.1.110/255.255.255.0
Username	admin
Password	<ul style="list-style-type: none"><li>• Web: admin</li><li>• iLinksView : lt_91_il_02_nmp</li></ul> <p>When using the iLinksView to manage the Device, make sure that the username and password must be the same as that you have set in the iLinksView, otherwise the iLinksView cannot discover the Device.</p>

## 5.2 Restoring to Factory Settings

There are two ways to restore the Device to factory settings.

- Press and hold the Reset button for 5 s to restore the Device to factory settings.
- Log in to web or use command line. For details, see the web operation manual or command line reference manual.

# Appendix 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.