

PoE Switch (16-and-24-Port Managed Desktop Switch)

Quick Start Guide



V1.1.0

Foreword

General

This manual mainly introduces the hardware, installation, wiring steps, and quick configurations of the switch (hereinafter referred to as "the device").

Symbols

The following symbols might appear in the manual.

Symbol	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
V1.1.0	Updated the Important Safeguards and Warnings.	April 2026
V1.0.3	Updated the initializing and adding the device.	January 2024
V1.0.2	Updated the images.	September 2023
V1.0.1	Updated the features.	August 2021
V1.0.0	First release.	July 2021

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

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



Stability Hazard

Possible result: The device might fall down and cause serious personal injury.

Preventive measures (including but not limited to):

- Before extending the rack to the installation position, read the installation instructions.
- When the device is installed on the slide rail, do not place any load on it.
- Do not retract the slide rail while the device is installed on it.



- 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.
- The power supply must meet the rated voltage requirements as indicated on the device label.
- If the device uses a power adapter, ensure it meets the following requirements:
 - ◇ If a power adapter was shipped with your device, we recommend you use it. If you need to buy a separate adapter, make sure it meets the following requirements.
 - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
 - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
 - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
 - ◇ Do not connect the power adapter to the device while the adapter is powered on.
- 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 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.
- When installing the device, make sure that the power plug can be easily reached to cut off the power.
- 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.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.

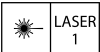
Operating Requirements



WARNING

- Operating the device in a domestic environment may cause radio interference.
- 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.
- Ground the device to protective ground before you power it on.
- The device must be reliably grounded by professionals. They must install the grounding conductor in the building floor and verify the grounding connection of the output receptacle.



- 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: -10°C to $+55^{\circ}\text{C}$ ($+14^{\circ}\text{F}$ to $+131^{\circ}\text{F}$).
- 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.
-  This is a Class 1 laser device. In accordance with IEC 60825-1:2014, EN 60825-1:2014+A11:2021, IEC 60825-2:2021, and EN 60825-2:2004+A1:2007+A2:2010, it must only be used with compatible Class 1 SFP modules. You may only insert modules that meet the Class 1 laser safety requirement.

Maintenance Requirements



WARNING

Power off the device before maintenance.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Overview.....	1
1.1 Introduction.....	1
1.2 Features.....	1
2 Port and Indicator.....	2
2.1 Front Panel.....	2
2.2 Rear Panel.....	3
3 Installation.....	4
4 Wiring.....	5
4.1 Connecting GND.....	5
4.2 Connecting Power Cord.....	5
4.3 Connecting Ethernet Port.....	5
4.4 Connecting SFP Ethernet Port.....	6
4.5 Connecting PoE Ethernet Port.....	7
5 Quick Operation.....	8
5.1 Login through Web.....	8
5.2 Restoring to Factory Settings.....	8
Appendix 1 Security Recommendation.....	9

1 Overview

1.1 Introduction

The Device is a layer-2 commercial switch. It provides a high-performance switching engine and large buffer memory to ensure smooth video stream transmission. With a full-metal design, the Device has great heat dissipation capabilities on its shell surface, and is able to work in environments that range from -10°C (14°F) to $+55^{\circ}\text{C}$ (131°F). With its DIP design, it provides a variety of work modes that suit different scenarios. The Device also supports power consumption management, which allows it to adapt to fluctuations in the power consumption of terminal devices. This ensures stable operation. With web management, SNMP and other functions, the Device can be remotely managed. It can directly connect to iLinksView.

The Device is applicable for use in different scenarios, including homes, offices, small malls and on server farms.

1.2 Features

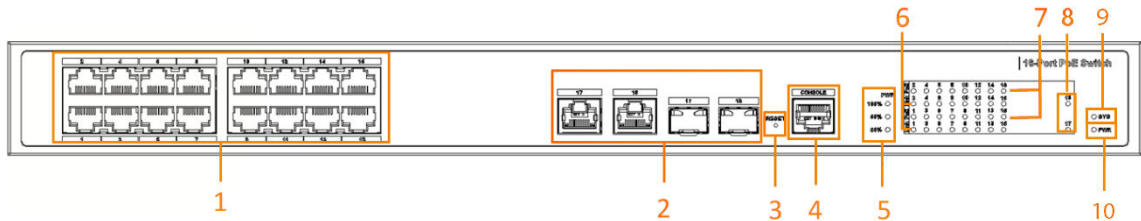
- 16/24 × 100 Mbps PoE Ethernet ports, uplink ports support gigabit optical ports or Ethernet ports.
- All ports meet the requirements of IEEE802.3af and IEEE802.3at standards. The red ports also conform with Hi-PoE and IEEE802.3bt standards, and the orange ports conform with Hi-PoE standard.
- 250 m long-distance PoE transmissions, which can be configured on the webpage.
- PoE watchdog for real-time detection of terminal device status, which can be configured on the webpage.
- Supports STP, RSTP, and MSTP.
- IEEE802.1Q-based VLAN configuration.
- Manual link aggregation and static LACP.
- Desktop mount and rack mount.

2 Port and Indicator

2.1 Front Panel

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

Figure 2-1 Front panel



Following are all the ports and indicators on the front panel of the 16/24-port managed desktop switch. Your actual device might only have some of them.

Table 2-1 Description of the front panel

No.	Description
1	10/100 Mbps self-adaptive PoE Ethernet ports.
2	Uplink port, including 10/100/1000 Mbps self-adaptive Ethernet ports and 1000 Mbps optical port.
3	Reset button. Press and hold it for more than 5 seconds, and release after the panel status indicators all turn on to restore the device to its default settings.
4	Console port.
5	PoE output power indicators. ● Solid green: Total power $\leq 50\%$. ● Solid green and yellow: $50\% < \text{total power} \leq 80\%$. ● Solid green, yellow and red: $80\% < \text{total power}$.
6	Single-port connection status indicators (Link). ● On: Connected to device. ● Off: Not connected to device.
7	PoE port status indicators. ● On: Powered by PoE. ● Off: Not powered by PoE.
8	Uplink port connection status indicators (Link). ● On: Connected to device. ● Off: Not connected to device.

No.	Description
9	System status indicator (SYS). ● Flashing: Operation is normal. ● Off: Operation is not normal.
10	Power indicator. ● On: Power on. ● Off: Power off.

2.2 Rear Panel

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

Figure 2-2 Rear Panel

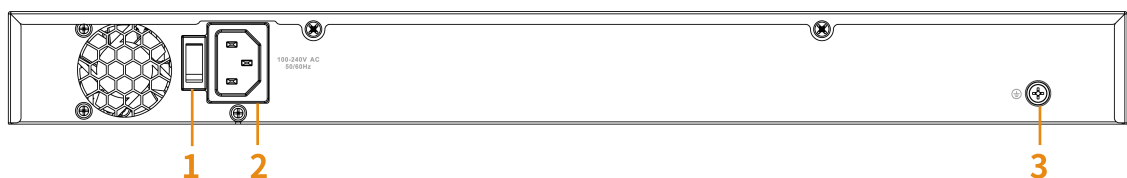


Table 2-2 Description of the rear panel

No.	Description
1	Power switch.
2	Power port, supports 100–240 VAC.
3	Ground terminal.

3 Installation

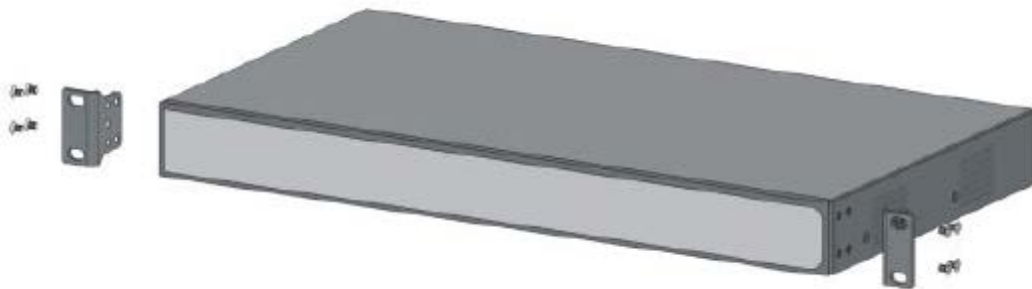
Background Information

The Device supports rack mount.

Procedure

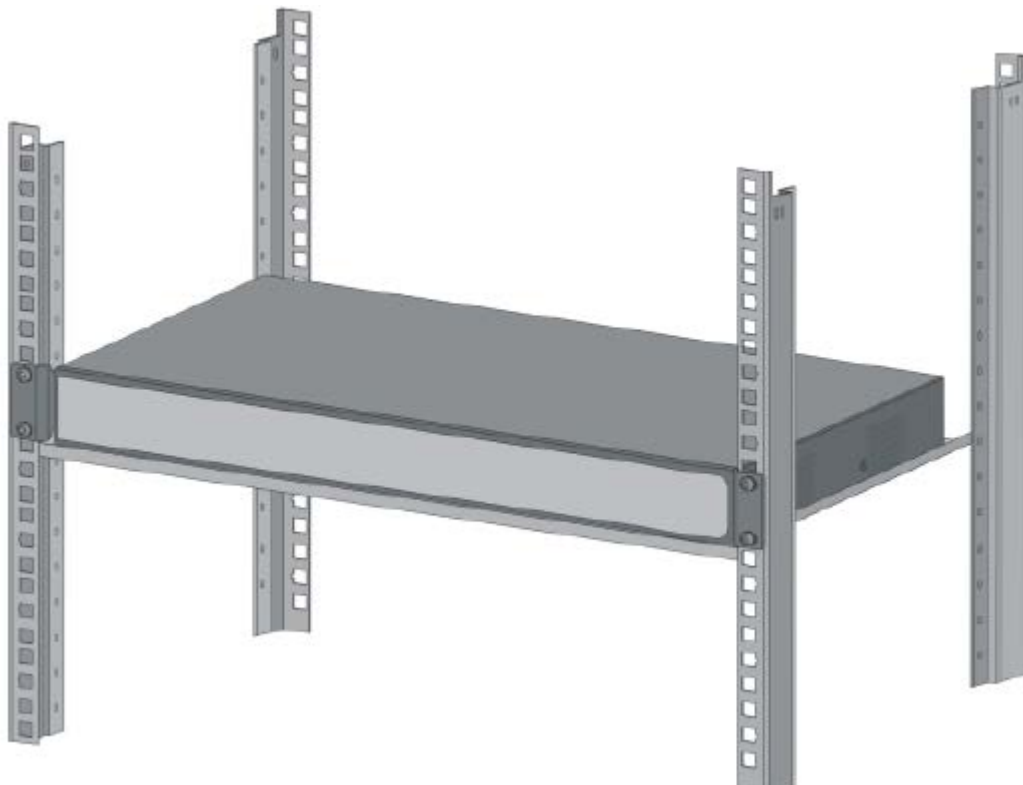
- Step 1 Attach the mounting bracket to the Device side panel (one on each side) and secure it with the screws provided with the rack.

Figure 3-1 Install the bracket



- Step 2 Attach the Device to the rack with screws.

Figure 3-2 Install the device



4 Wiring

4.1 Connecting GND

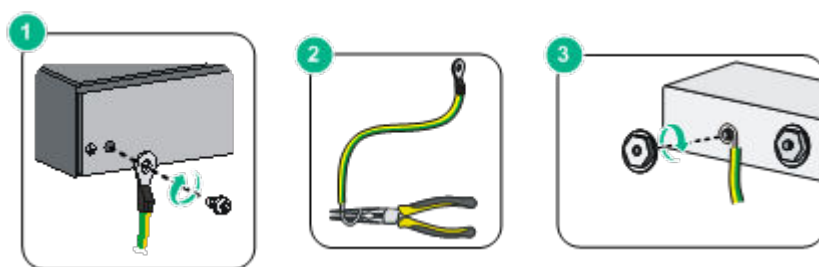
Background Information

Grounding the Device can protect it against lightning and interference.

Procedure

- Step 1 Remove the ground screw from the Device and pass the ground screw through the round hole of the OT terminal of the ground cable. Turn the ground screw clockwise with a cross screwdriver to fasten the OT terminal of the ground cable.
- Step 2 Wind the other end of the ground cable into a circle with the needle-nose pliers.
- Step 3 Connect the other end of the ground cable to the ground bar, then turn the hex nut clockwise with a wrench to fasten the other end of the ground cable to the ground terminal.

Figure 4-1 Connect GND



4.2 Connecting Power Cord

Background Information

Before connecting the power cord, make sure that the Device is securely grounded.

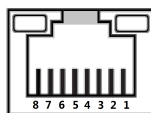
Procedure

- Step 1 Connect one end of the power cord to the power jack of the Device.
- Step 2 Connect the other end of the power cord to the external power socket.

4.3 Connecting Ethernet Port

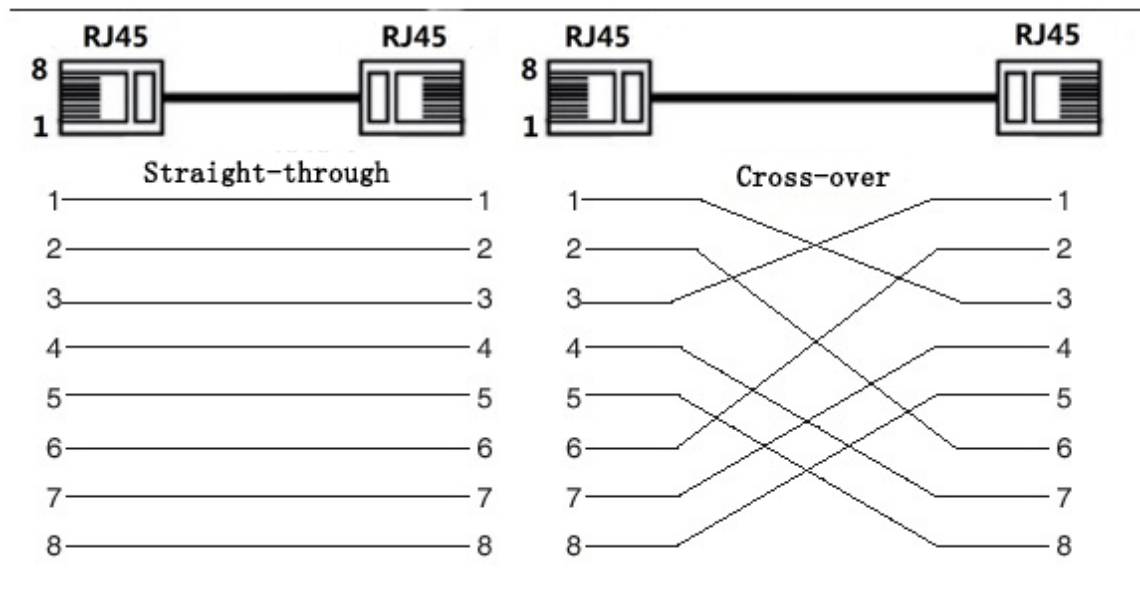
The Ethernet port is a standard RJ-45 port. With its self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode. It supports MDI/MDI-X self-recognition of the cable, allowing you to use a cross-over cable or straight-through cable to connect the terminal device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

Figure 4-2 Ethernet port pin number



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

Figure 4-3 Connect cable



4.4 Connecting SFP Ethernet Port

Background Information



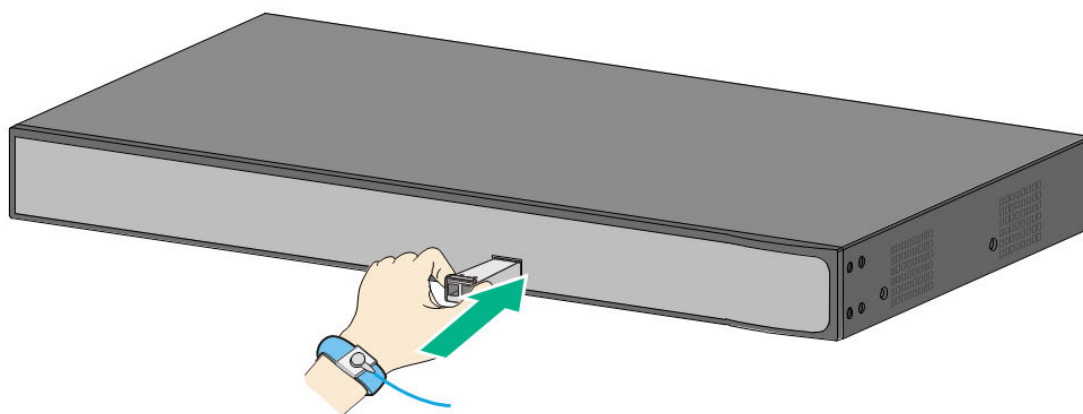
WARNING

- 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 fiber.
- Do not directly insert the SFP optical module into the slot while the optical fiber is inserted in it. Unplug the optical fiber before installing it.

Procedure

- Step 1 Wear the antistatic wrist band, and confirm that the antistatic wrist band is in good contact with your skin and the Device is reliably grounded.
- Step 2 Turn up the handle of the SFP optical module vertically and hold the optical module on both sides with your hands.
- Step 3 Push the optical module gently into the slot in the horizontal direction until the SFP optical module is firmly connected to the slot.

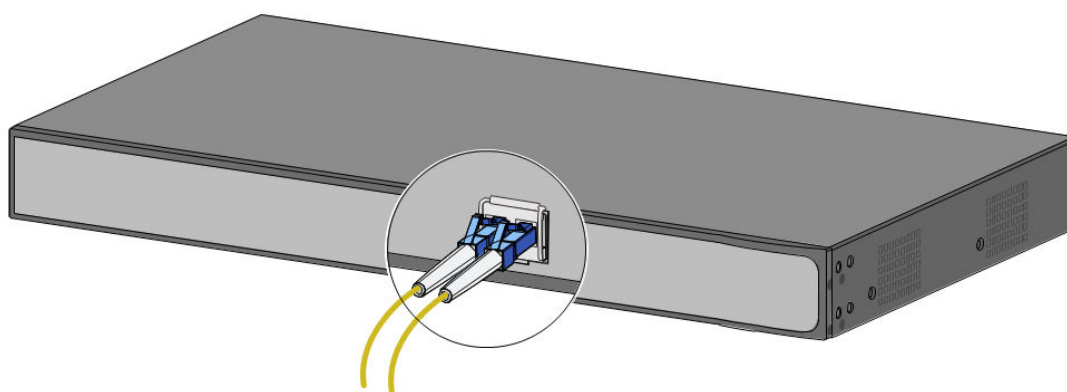
Figure 4-4 Install SFP module



Step 4 Remove the dust cap of the LC connector of the optical fiber and the dust plug of the SFP optical module.

Step 5 Connect the LC connector of the optical fiber to the SFP optical module.

Figure 4-5 Connect optical fiber



4.5 Connecting PoE Ethernet Port

If the terminal device has a PoE Ethernet port, you can directly connect this port to the Device PoE Ethernet port through the network cable to achieve synchronized network connection and power supply. The maximum distance between the Device 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 the web for management and operation. For details, see web operation manual.



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

Table 5-1 Default factory configuration

Parameter	Description
IP address	192.168.1.110/255.255.255.0
Username	admin
Password	• Web: No initial password, user-defined during initialization. • iLinksView : lt_91_il_02_nmp  When using iLinksView for device management, ensure that the username and password of the Device matches that of iLinksView, otherwise iLinksView will not be able to discover the Device.

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 seconds 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 1 Security Recommendation

Account Management

1. Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account logout function

The account logout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up complex passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.

4. Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.

2. **MAC address binding**

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).