



Ethernet Switch

Hardware Installation Guide



Foreword

General

This manual mainly introduces the cable connection, and quick operation of the switch (hereinafter referred to as "the device"). The manual is for reference only, and might differ from the actual product. Read carefully before using the device, and keep the manual safe for future reference.

Symbols

The following symbols might appear in the manual.

Symbol	Description
 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
V1.0.0	First release.	April 2026

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.

Table of Contents

Foreword.....	I
1 Cable Connection.....	1
1.1 Connecting the Grounding Cable.....	1
1.2 Connecting the Ethernet Cable to the RJ-45 Ethernet Port.....	3
1.3 Connecting the Ethernet Cable to the PoE Ethernet Port.....	4
1.4 Connecting the Fiber Cable to the Optical Port.....	4
1.5 Connecting the Ethernet Cable to the Management Ethernet Port.....	5
1.6 Connecting the Console Cable to the Console Port.....	6
1.7 Connecting the RS-485 Cable to the RS-485 Port.....	7
1.8 Connecting to the Alarm Port.....	8
1.9 Connecting the Power Cord.....	9
2 Quick Operation.....	13
2.1 First Login through Console Port.....	13
2.2 Logging in to the Webpage.....	15
2.3 Restoring the Device to Factory Settings.....	15
Appendix 1 Security Commitment and Recommendation.....	16

1 Cable Connection

1.1 Connecting the Grounding Cable

Proper grounding is important for ensuring the safe operation of the devices, protecting against lightning strikes, suppressing electromagnetic interference, and preventing electric shock hazards. Always connect the grounding cable before powering on the device, and then disconnect it only after power is turned off.



- Some devices are not shipped with a grounding cable. You need to prepare it separately.
- Use a yellow-green protective grounding cable with the cross-sectional area of at least 4 mm² and the grounding resistance of no more than 4 Ω.
- If the grounding cable is bare, we recommend you using crimped terminals for connection. If crimped terminals are not available, the cable can be formed into a closed loop for use.
- The grounding hole locations shown in the following illustrations are for reference only. Refer to the actual device for accurate positioning.

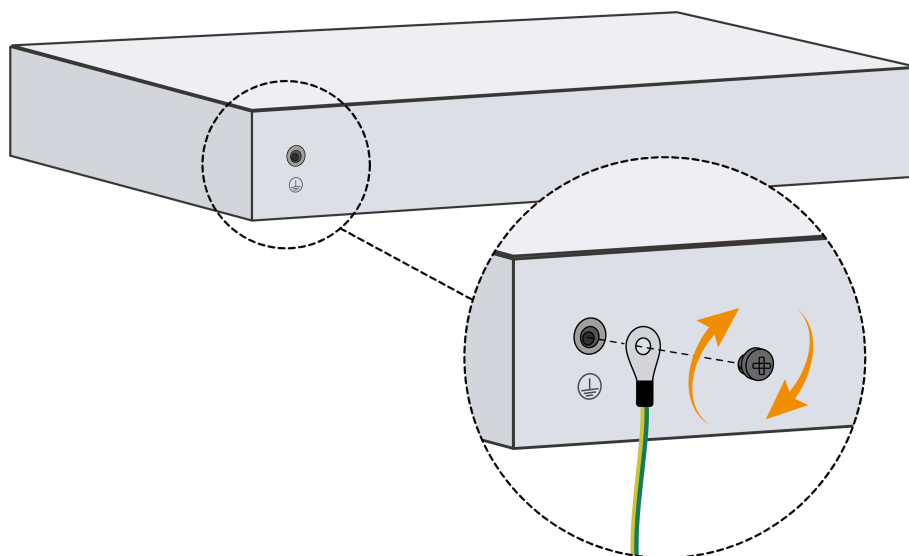
Select an appropriate grounding method based on the device type and installation environment.

Centralized Grounding through Grounding Busbar (Indirect Grounding)

This method is suitable for environments with a unified grounding system, such as machine rooms or distribution rooms. Centralized grounding through a grounding busbar facilitates maintenance and inspection.

1. Use a crosshead screwdriver to remove the screw from the grounding hole on the device panel.
2. Secure one end of the grounding cable to the grounding hole using the removed screw, and then tighten it clockwise.

Figure 1-1 Secure the grounding cable to the device

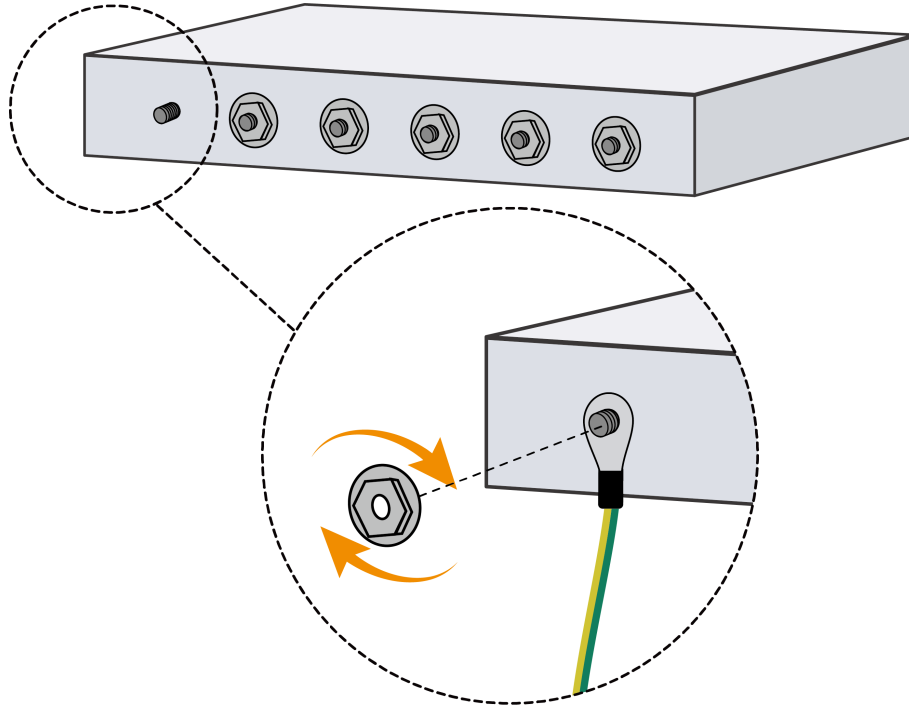


3. Place the other end of the grounding cable onto the grounding post of the grounding busbar. Use a wrench to tighten the hex nut clockwise, ensuring the grounding cable is securely fixed to the post.



The grounding busbar shown in the illustration is for reference only. Refer to the actual grounding busbar in your installation environment for specific operations.

Figure 1-2 Secure the grounding cable to the grounding busbar

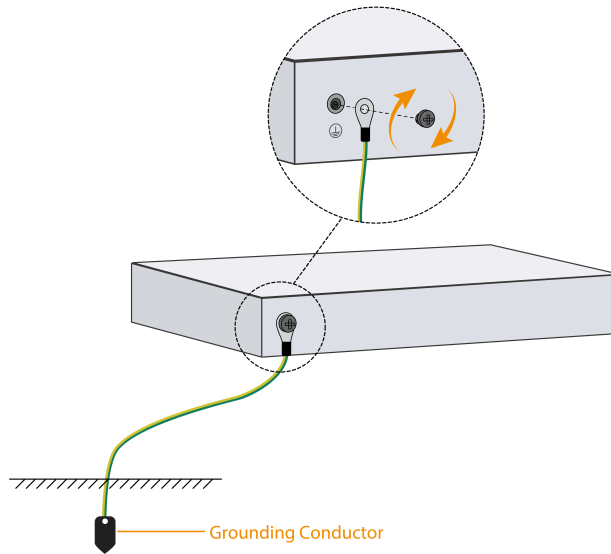


Chassis Grounding (Direct Grounding)

This method is suitable for standalone installation scene.

1. Use a crosshead screwdriver to remove the screw from the grounding hole on the device panel.
2. Secure one end of the grounding cable to the grounding hole using the removed screw, and then tighten it clockwise.
3. Connect the other end of the grounding cable to the ground, ensuring the grounding path is smooth.

Figure 1-3 Connect to the ground

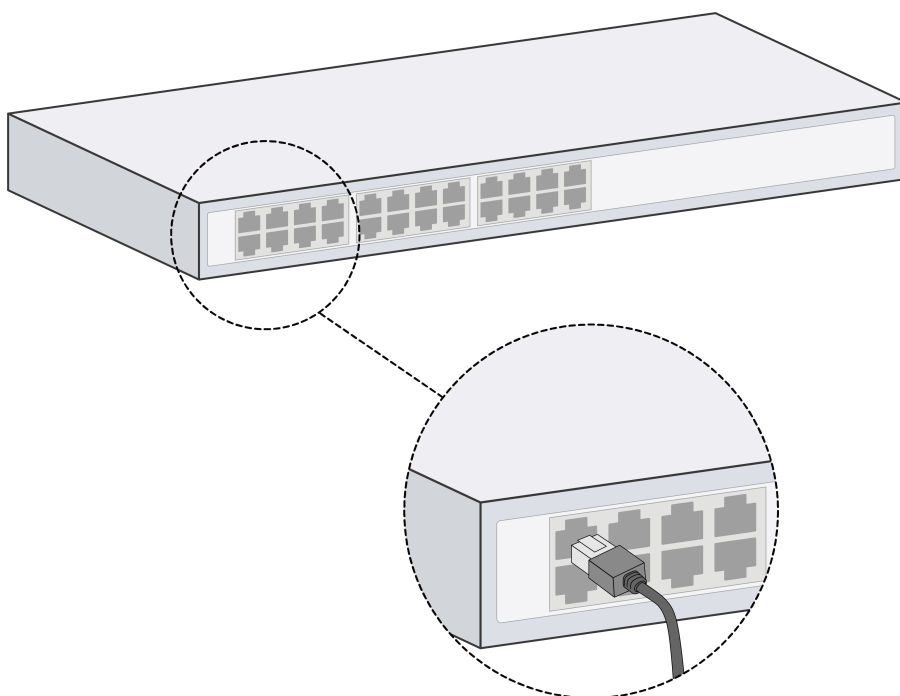


1.2 Connecting the Ethernet Cable to the RJ-45 Ethernet Port

This device is equipped with multiple adaptive RJ-45 Ethernet ports, which automatically negotiate and switch to the optimal full-duplex or half-duplex operating mode. The ports also support MDI/MDI-X auto recognition, eliminating the need to distinguish between straight-through and crossover Ethernet cables.

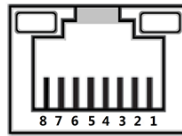
This allows direct connection to various end devices or network equipment, offering flexible and convenient deployment.

Figure 1-4 Connect an Ethernet cable



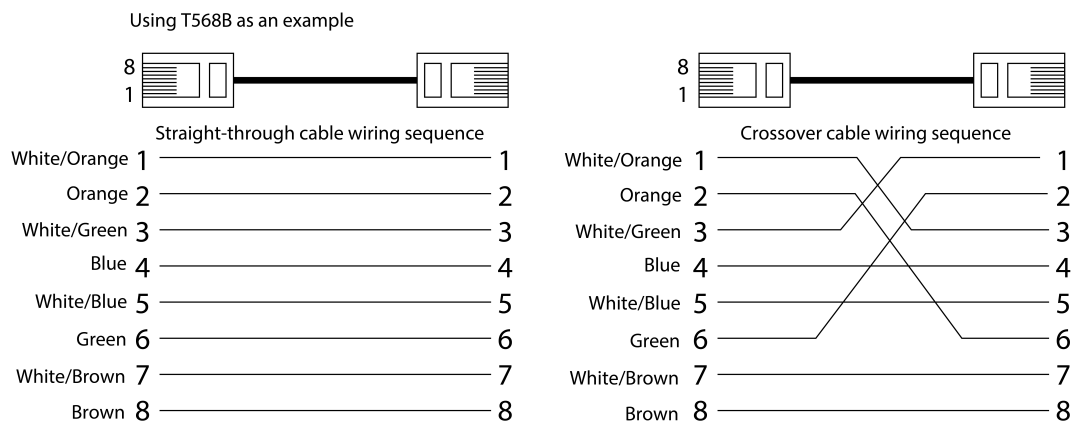
Description of Ethernet Port Pins

Figure 1-5 Ethernet port pin numbers (from left to right are 8 to 1)



The RJ-45 connectors at both ends of the cable can be wired according to the following diagram.

Figure 1-6 Standard 568B interface pin definition



1.3 Connecting the Ethernet Cable to the 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 network cable to achieve synchronized network connection and power supply. When the long-distance power supply is disabled, we recommend using Ethernet cables no longer than 100 meters.



For non-PoE end devices, ensure they are externally powered to establish normal communication.

1.4 Connecting the Fiber Cable to the Optical Port

Background Information



WARNING

The device uses laser to transmit signal through fiber cable. Do not look directly into the optical module when the device is powered on, as it might cause permanent eye damage.

Procedure

- Step 1** Wear an anti-static wrist strap or gloves.
- When wearing only an anti-static wrist strap, ensure the conductive band maintains direct and continuous contact with your skin.
 - When using both ESD gloves and a wrist strap, first put on the gloves and then secure the wrist strap over them, ensuring the conductive surface maintains uninterrupted contact through the glove material.
- Step 2** Install the optical module.



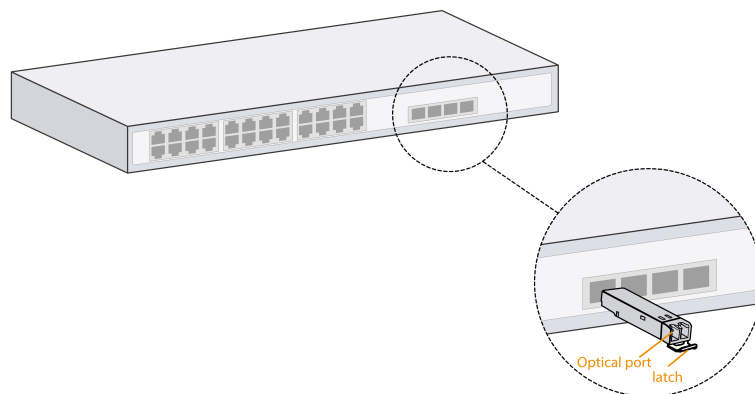
- Do not touch the golden fingers of the optical module directly with hands.
- Do not remove the dust plug of the optical module before connecting the fiber.
- Do not install an optical module that has fiber cables attached to it.

1. Lift the optical module's latch until it engages the retaining clip.
2. Grip both sides of the optical module and insert it smoothly into the optical port slot.
3. Ensure the module is fully seated and properly aligned with the slot.



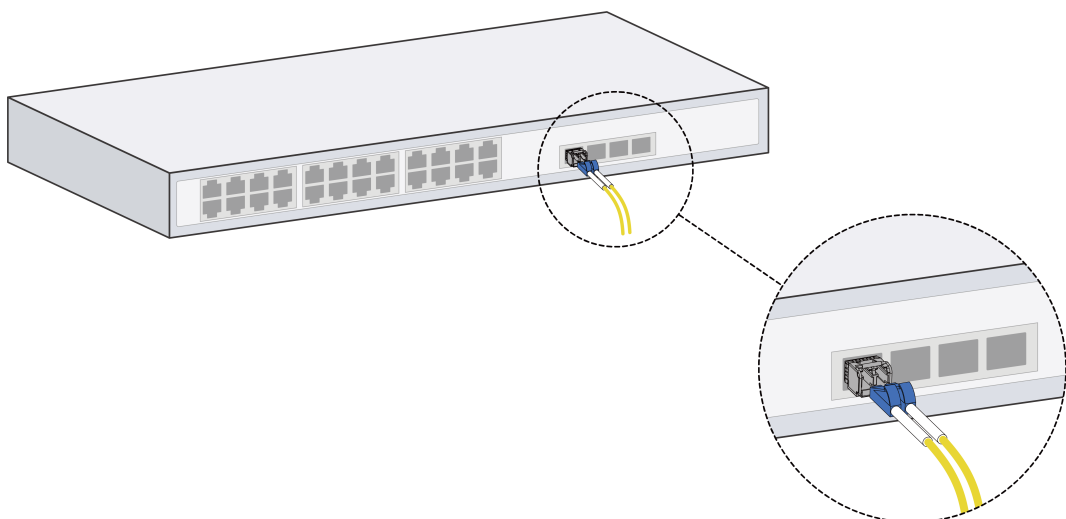
Installation methods might vary for different optical ports and modules. Refer to the actual device.

Figure 1-7 Install the optical module



- Step 3** Remove the dust plug from the optical module, align the fiber with the interface, and then gently insert it until fully seated.

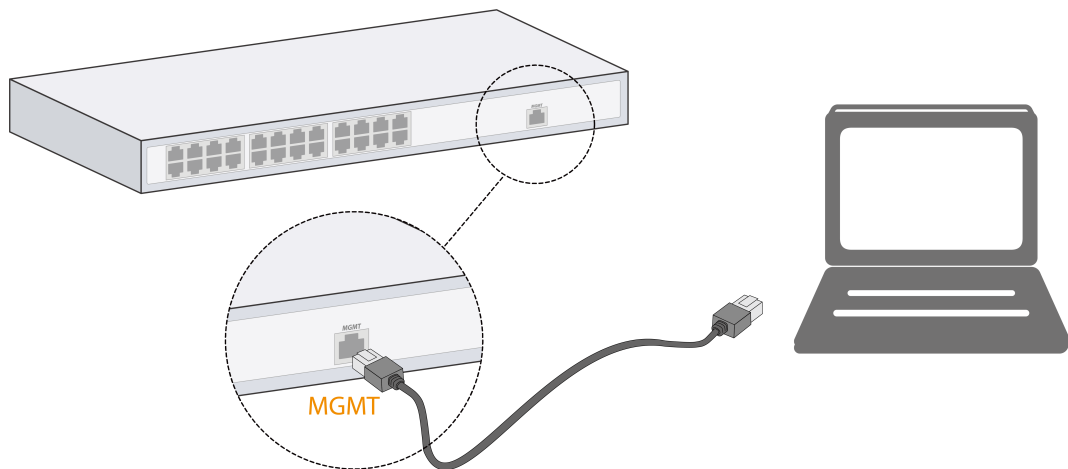
Figure 1-8 Insert the optical fiber



1.5 Connecting the Ethernet Cable to the Management Ethernet Port

The management Ethernet port (MGMT) supports local or remote computer connections for device maintenance, debugging, and upgrades.

Figure 1-9 Connect the management Ethernet port



1.6 Connecting the Console Cable to the Console Port

Prerequisites

Prepare a USB console cable featuring an RJ-45 connector on one end and a USB connector on the other, or an RJ-45-to-DB-9 serial cable with an RJ-45 connector on one end and a DB-9 connector on the other.

Figure 1-10 USB console cable



Figure 1-11 Cable sequence of RJ-45-DB-9

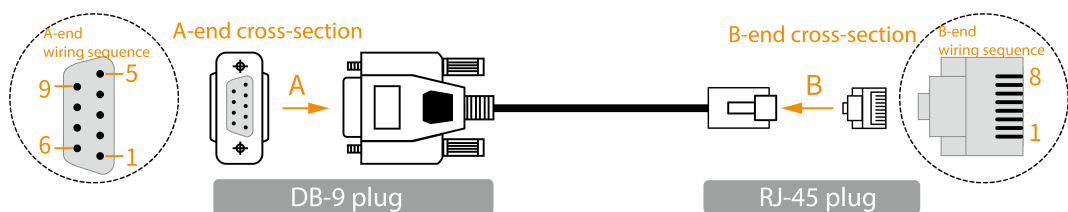


Table 1-1 Pin correspondence and description for both ends

DB-9 Connector Pin Number	RJ-45 Connector Pin Number	Signal	Function
3	6	RXD	Receive data
2	3	TXD	Transmit data
5	4 or 5	GND	Ground

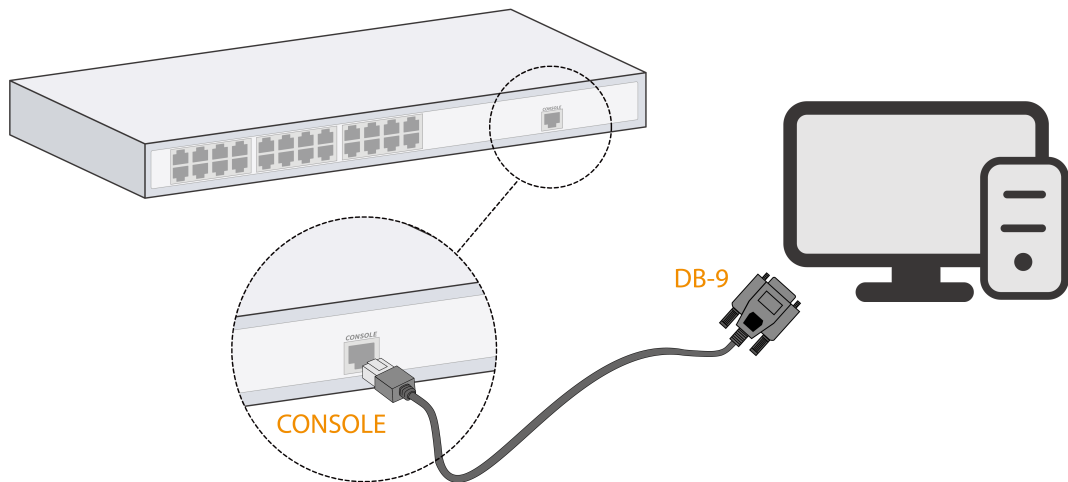
Procedure



The DB-9 connector is shown as an example of the computer-side interface in the following steps and diagrams.

1. Insert the RJ-45 connector of the configuration cable into the console port on the device.
2. Insert the DB-9 connector of the configuration cable into the 9-pin serial port on the computer.
3. Run a terminal emulation program on the computer, for example on the Windows operating system, to configure, maintain, and manage the device.

Figure 1-12 Connect the configuration cable

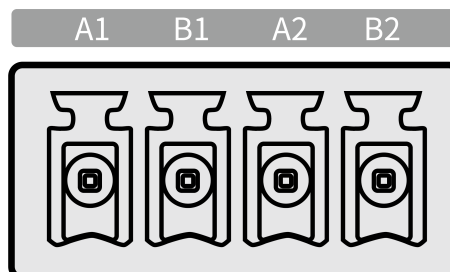


1.7 Connecting the RS-485 Cable to the RS-485 Port

The RS-485 port enables bidirectional protocol conversion between industry standard serial data and Ethernet data. It supports converting RS-485 serial signals into IP network packets based on TCP or UDP protocols, and can be used to connect to PTZ (Pan-Tilt-Zoom) devices.

Each RS-485 port consists of 2 terminals labeled A and B. During installation, terminals with the same identifier must be connected as a pair.

Figure 1-13 RS-485 port



1.8 Connecting to the Alarm Port

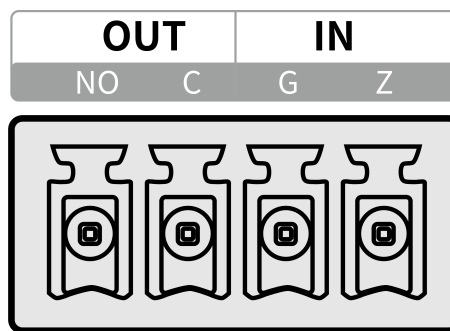
The alarm port of the device supports external alarm signal input and can achieve linkage output through a built-in relay. When a valid alarm input is detected, the relay will activate automatically, outputting a switching signal that can be used to trigger alarms or interconnect with other devices.

Background Information

The device provides 2 sets of ports:

- The alarm output (OUT) includes a common terminal (C) and a normally open terminal (NO), forming a set of normally open contact outputs.
- The alarm input (IN) includes a ground terminal (G) and a signal terminal (Z), designed to receive external alarm signals.

Figure 1-14 Alarm port



- During normal operation, the common terminal (C) and the normally open terminal (NO) remain in a disconnected state.
- When the alarm input port detects a low-level signal, the device identifies an alarm event. The common terminal (C) and the normally open terminal (NO) then switch to a conducting state. The disconnected state is sustained for approximately 5 seconds and then automatically restored, meaning the alarm output level remains low for 5 seconds before being pulled high again.
- Alarm ports are available on select models.

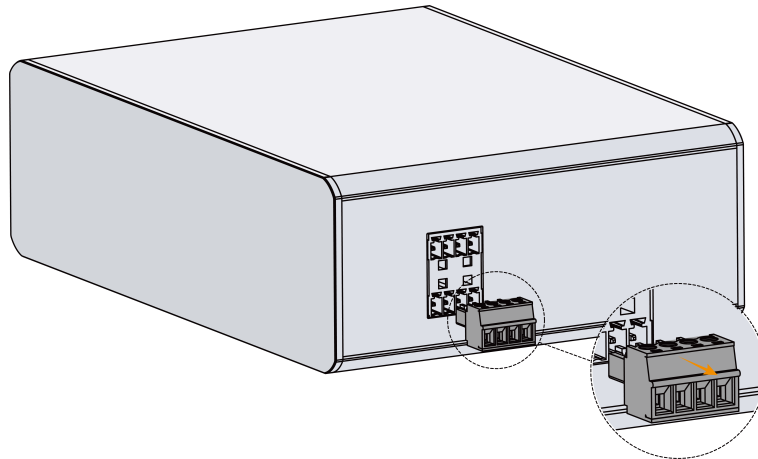
Table 1-2 Relay output contact specifications

Parameter	Value
Maximum voltage	125 VAC/60 VDC
Maximum current	2 A
Maximum power	60 W
Maximum withstanding voltage	2 kV

Procedure

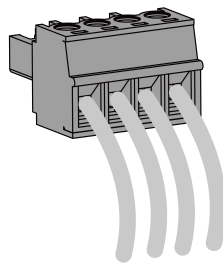
- Step 1** Use a screwdriver to remove the alarm port connector from the device.

Figure 1-15 Remove the alarm port connector



Step 2 Insert the alarm input and output signal wires into the corresponding terminals of the connector according to the interface pin. Ensure all connections are secure.

Figure 1-16 Connect the alarm signal wires



Step 3 Insert the wired alarm port connector back into the device and tighten it using a screwdriver.

1.9 Connecting the Power Cord

The power port of the device can be one of the following types: Standard socket, DC power jack, or terminal block. Select the appropriate connection method based on your device.



Make sure that the device is reliably grounded before connecting the power cord.



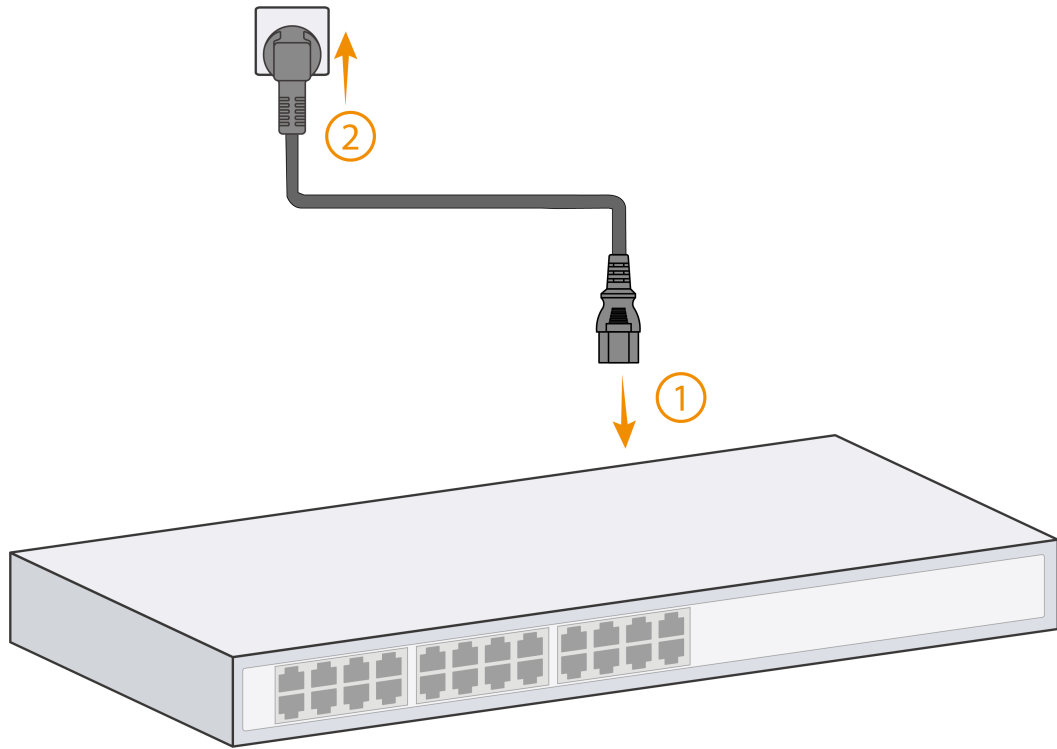
- Verify that the power supply matches the voltage and current requirements specified on the device label to avoid damage.
- For PoE switches powered by an external adapter, an isolated power adapter is required.
- Some devices support redundant power supplies. If one power supply fails, the system can switch to the alternate power source to maintain network reliability.
- The power cable shown in the diagram is for reference only. The actual cable might vary.

Connecting a Standard Socket Power Port

1. Firmly plug one end of the power cable into the device's power socket until fully seated.
2. Attach the other end of the cable to an external power outlet.

3. Ensure both ends of the power cable are securely connected without looseness.

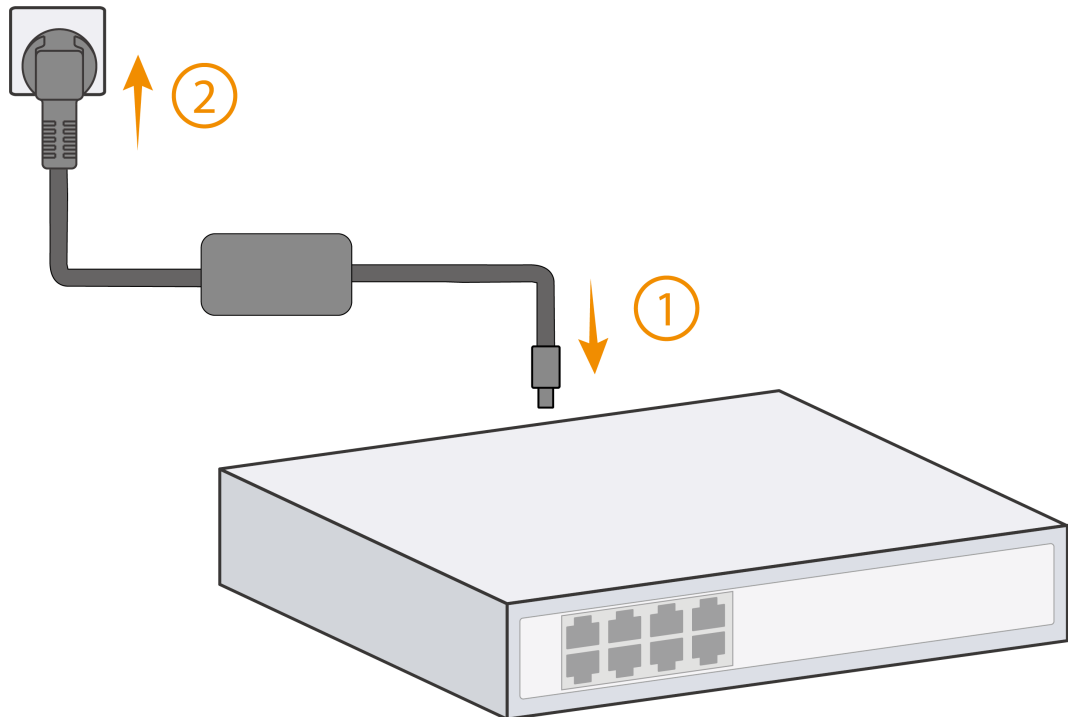
Figure 1-17 Connect a standard socket power port



Connecting a DC Power Jack

1. Firmly plug one end of the power cable into the device's power socket until fully seated.
2. Attach the other end of the cable to an external power outlet.
3. Ensure both ends of the power cable are securely connected without looseness.

Figure 1-18 Connect a DC power jack



Connecting a Terminal Block Power Port

WARNING

Do not touch exposed wires, terminals, or any components marked with high-voltage symbols to avoid personal injury. Do not remove parts or disconnect cables during power-on.

1. Remove the terminal block plug from the device.
2. Insert the positive (+) and negative (-) wires into the terminal block plug and tighten the screws securely with a screwdriver.



The power cable must have a cross-sectional area of at least 0.75 mm², with a maximum allowable cross-section of 2.5 mm².

Figure 1-19 Insert the power terminal plug

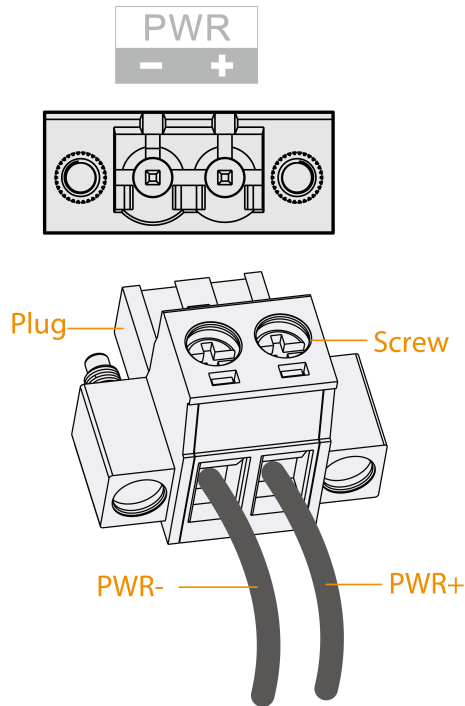


Table 1-3 Description of the power terminal pin

Signal Name	Definition
PWR-	DC power input (Negative)
PWR+	DC power input (Positive)

3. Firmly reconnect the wired terminal block plug to the device's power terminal port.
4. Attach the other end of the power cable to the external power supply system, ensuring compliance with the device's labeled voltage/current requirements.
5. Check if the power indicator light is on. Light on means the power connection is correct.

2 Quick Operation

2.1 First Login through Console Port

Accessing the local page through the console port is the most basic method for logging into the device.

Background Information



Only some devices support management through the console port.

Procedure

Step 1 Connect the computer and the device using a console configuration cable.



Check the port label before connecting to prevent misconnection.

Step 2 Power on the computer and run the terminal emulation program. Select the serial port connected to the device, and then configure the terminal communication parameters.

The parameter values must match those on the device.



- For computers running Windows Server 2003, add the HyperTerminal program through Windows components, and then log in and manage the device as described in this document.
- For computers running Windows Server 2008, Windows 7, or other operating systems, obtain third-party terminal control software. For usage instructions, refer to the software's user guide or online help.

Figure 2-1 Configure the parameter

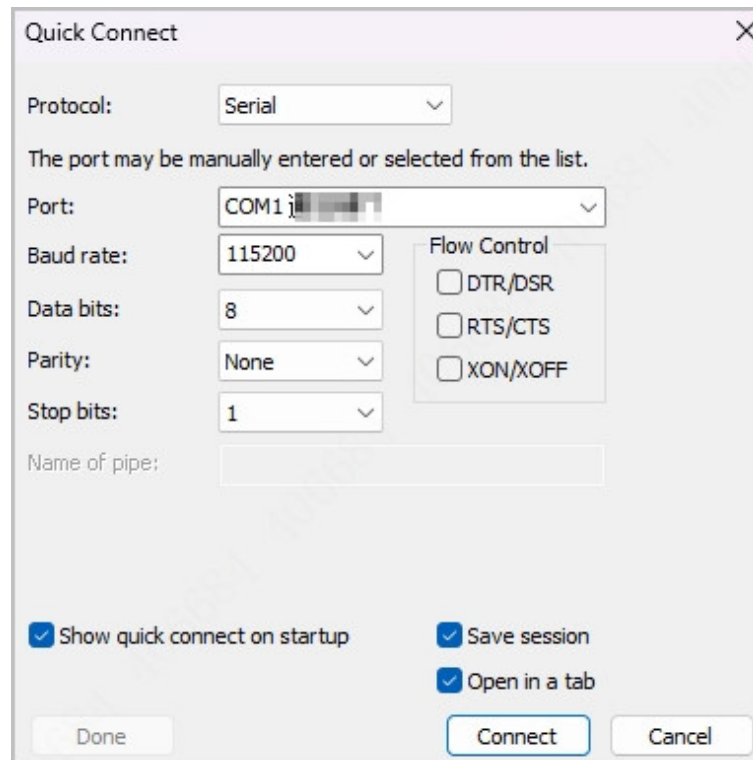


Table 2-1 Communication configuration parameter description

Parameter	Default Setting
Port	Select the port according to the device conditions.
Baud rate	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None  Do not select RTS/CTS.

Step 3 Power on the device. The terminal displays device self-test information. After self-test completion, press the Enter key.

Step 4 Enter the username, and then press the Enter.



The default username is admin.

Step 5 Enter the password, and then press the Enter.

The <dahua> command prompt indicates successful login.

Press ENTER to get started

Username: admin

Password:

<dahua>

Step 6 (Optional) Enter commands to configure the device or view its operational status. For help, type "?" at any time.

2.2 Logging in to the Webpage

You can log in to the webpage to perform operations on the device and manage it.



For first-time login, follow the on-screen prompts to set your password.

Table 2-2 Description of default factory settings

Parameter	Description
IP address/Subnet mask	192.168.1.110/255.255.255.0
Username	admin
Password	You need to set the password for first-time login.

2.3 Restoring the Device to Factory Settings

The following methods are supported for restoring the device to factory default settings.



Restoring factory defaults will cause data loss. Please be advised.

- Press and hold the **RESET** button for 5 seconds.
- To restore defaults through the device webpage, refer to the corresponding web user manual.
- To restore defaults through the command line, refer to the corresponding command line user manual.



Supported features and operations might differ between device models. Refer to the actual device.

Appendix 1 Security Commitment and Recommendation

Zhejiang Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

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 lockout function

The account lockout 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

Dahua 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, we recommend you 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**

We recommend you 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).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188