Ethernet Switch (Cloud-Managed Desktop Switch)

Quick Start Guide



ZHEJIANG DAHUA VISION TECHNOLOGY CO.,LTD. V1.0.1

Foreword

General

This manual mainly introduces the features, indicators and installation of the switch (hereinafter referred to as "the device"). 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
V1.0.1	Updated the front panel description.	September 2026
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.

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

 **DANGER**

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.

 **WARNING**

- 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 °C (+14 °F to +131 °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
2 Port and Indicator 2
2.1 Front Panel 2
2.2 Rear Panel 5
3 Installation 7
3.1 Preparations 7
3.2 Desktop Mount 7
3.3 Rack Mount 7
3.4 Wall Mount 8
Appendix 1 Security Commitment and Recommendation 10

1 Overview

The device is a cloud-managed desktop switch. The cloud managed device is a layer-2 commercial device. With a full-metal design, the device has great heat dissipation capabilities on its shell surface.

In addition, through cloud management, webpage management, the device can be remotely managed. The device is applicable for uses in different scenarios, including buildings, homes, factories and offices.

Cloud management refers to managing this device through the DoLynk apps and webpages.

2 Port and Indicator

The following description uses a typical device as an example. The actual device might only include a subset of the ports or features described. For details, refer to the port introduction and the physical device.

2.1 Front Panel

The PoE device complies with the IEEE 802.3af and IEEE 802.3at standards. The red ports comply with the IEEE 802.3bt standard, while the orange ports comply with the Hi-PoE standard.

Figure 2-1 Front panel (1)

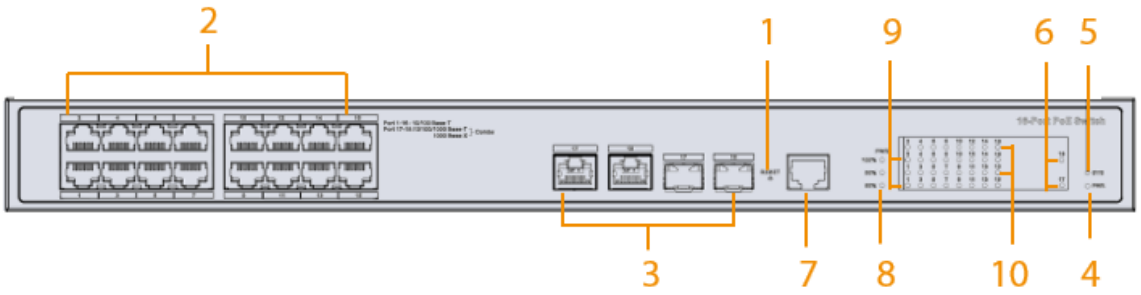


Figure 2-2 Front panel (2)

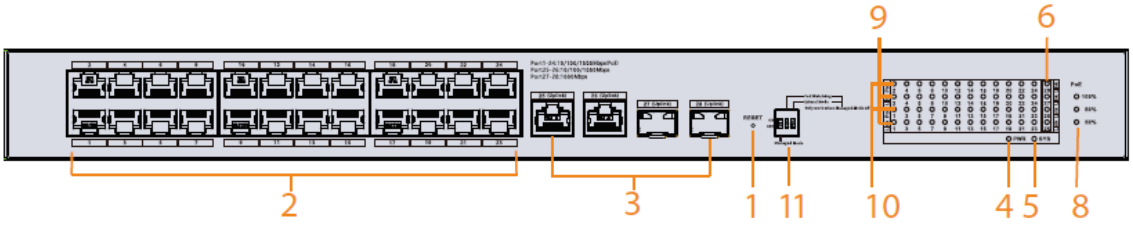


Table 2-1 Front panel introduction

No.	Description
1	Reset button (Reset). Press and hold for longer than 5 seconds, wait until all the indicators are solid on, and then release. The device restores to the default settings. Only effective in the managed mode.

No.	Description
2	10/100/1000 Mbps self-adaptive PoE Ethernet ports. • The self-adaptive PoE Ethernet port is available on select models. • Different models support different data rates. Please refer to the actual specifications of the device.
3	Uplink port (Uplink). Includes 10/100/1000 Mbps self-adaptive uplink Ethernet ports, and 1000 Mbps uplink optical ports. • The number of the ports might differ from different models. • 10/100/1000 Mbps Ethernet ports and 1000 Mbps optical ports are available on select devices. • The uplink ports are combo ports on select models.
4	Power indicator (PWR). • On: Power on. • Off: Power off.
5	System indicator (SYS). • Flashes: The system is running. • Off: The system is experiencing issues.
6	Uplink port status indicator (Link/Act). • On: Connected to device. • Off: Not connected to device. • Flashes: Data transmission is in progress.
7	Console port (Console). Only supported by select models.
8	PoE output power indicator (PWR). • Only solid green: PoE output power < 50%. • Solid green and yellow: 50% ≤ PoE output power < 80%. • Solid green, yellow and red: PoE output power ≥ 80%.

No.	Description
9	Single port connection/data transmission status indicator (Link/Act). • On: Connected to device. • Off: Not connected to device. • Flashes: Data transmission is in progress. The Link/Act indicators are located on either the left or right side of each Ethernet port on select models.
10	PoE network port power supply status indicator (PoE). • On: Powered by PoE. • Off: Not powered by PoE. The PoE power supply indicators are located on either the left or right side of each Ethernet port on select models.
11	DIP Switch. • The managed mode. ◇ On: The managed mode is enabled, which supports both local management and cloud management. It is enabled by factory default. ◇ Off: The management mode is disabled. ◇ Every time the DIP switch flipped, the device would reboot. ◇ When the managed mode is disabled, the configuration under the managed mode will be reserved. The device has no IP address and may serve as an unmanaged switch, with plug-and-play functionality. • **PoE Watchdog**: The **PoE Watchdog** is enabled through the DIP switch. When terminal device crash is detected, power down and restart the terminal device. • **Extend Mode**: The **Extend Mode** extends the maximum transmission distance to 250 m, but reduces average transmission speed to 10 Mbps. ◇ Only works when **Managed Mode** is off. ◇ The actual transmission distance depends on the PoE power and wire mass. The advertised distance is only the laboratory test distance.

2.2 Rear Panel

Standard Socket Outlet

Figure 2-3 Rear panel

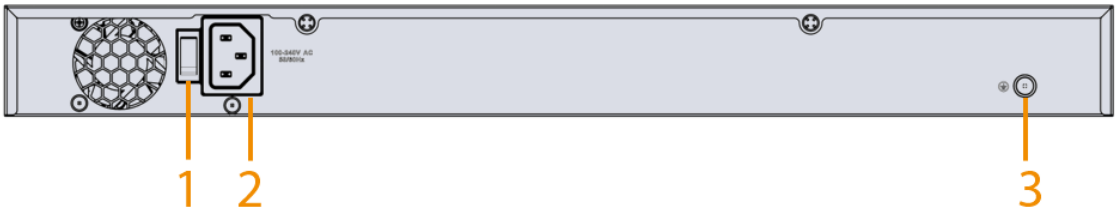


Table 2-2 Rear panel introduction

No.	Description
1	Power Button. Supported by select models.
2	Power port. Power specifications might vary by device. For the actual specifications, refer to the label on the device.
3	Ground terminal.

DC Power Jack

Figure 2-4 Rear panel

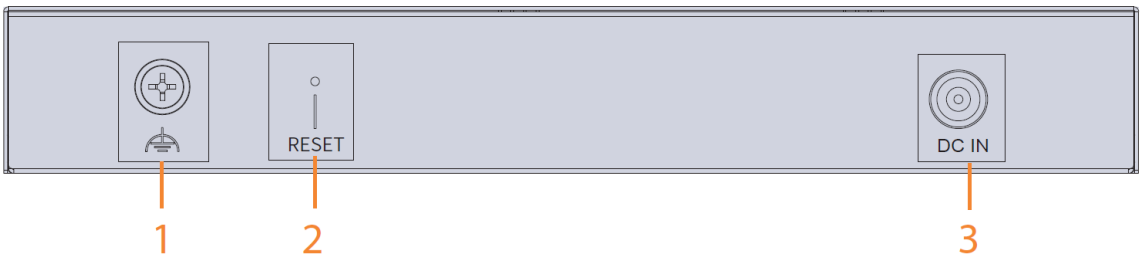


Table 2-3 Rear panel introduction

No.	Description
1	Ground terminal.

No.	Description
2	Reset button (Reset). Press and hold for longer than 5 seconds, wait until all the indicators are solid on, and then release. The device restores to the default settings. Only effective in the managed mode.
3	Power port. Power specifications might vary by device. For the actual specifications, refer to the label on the device.

3 Installation

3.1 Preparations

- Select a proper installation method according to your actual needs.
- Make sure that the working platform is stable and steady.
- Leave about 10 cm space on both sides of the device for heat dissipation to ensure good ventilation.

3.2 Desktop Mount

The device supports desktop mount. Place it on a steady and stable desktop.

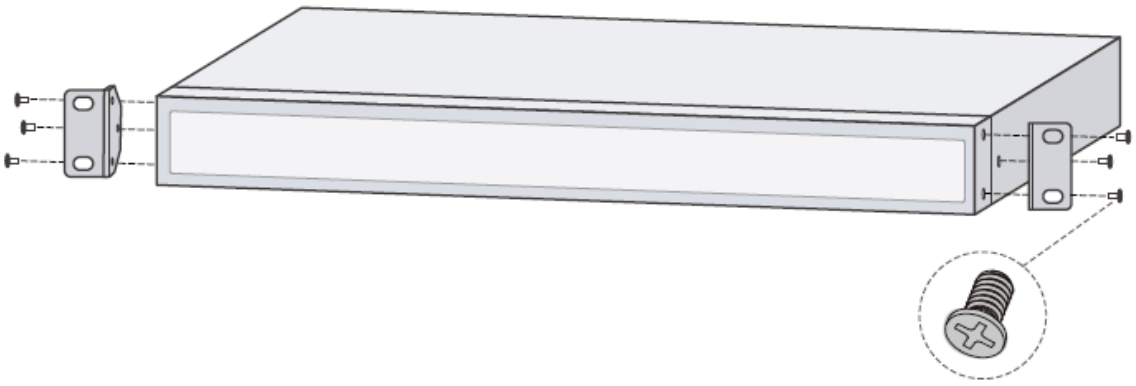
3.3 Rack Mount

The 16-port and 24-port devices support rack mount.

Procedure

Step 1 Attach the rack-mounting kit to the device side panel (one on each side), and then secure it with the screws provided with the rack.

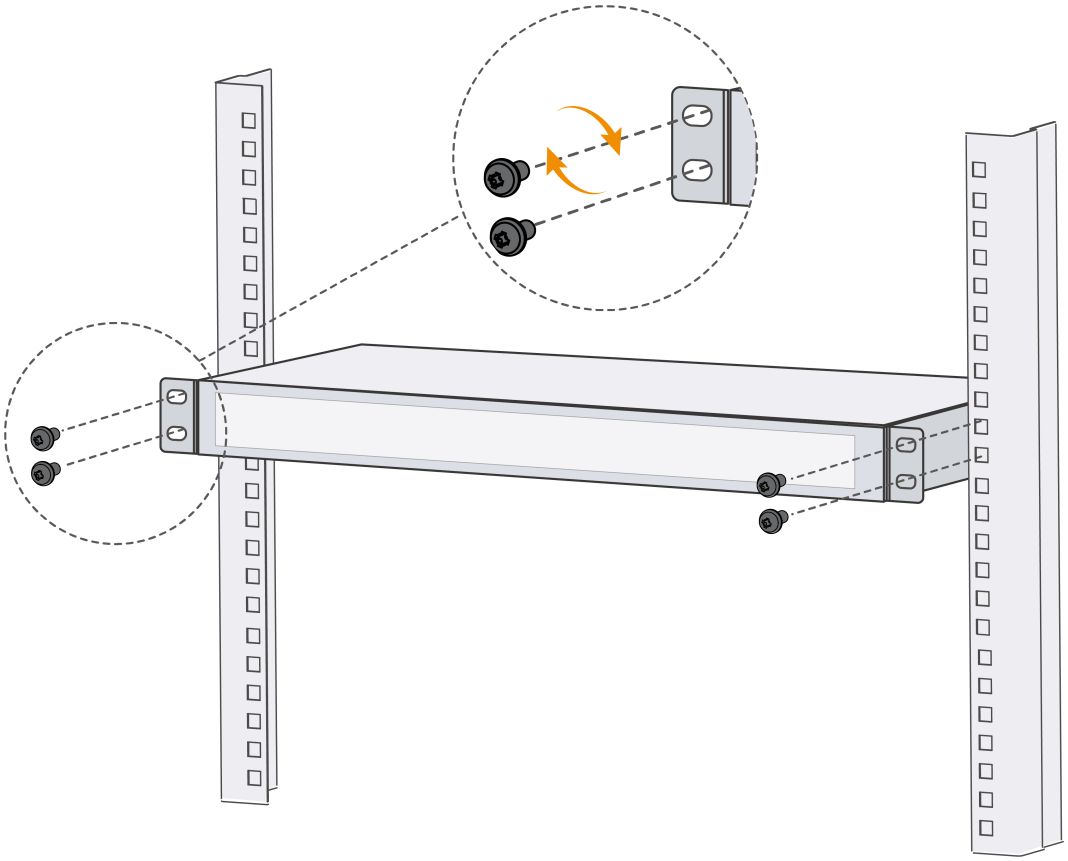
Figure 3-1 Install the rack-mounting kit



Step 2 Mount the device to the rack using the rack screws.

Users need to provide their own rack screws.

Figure 3-2 Install the device



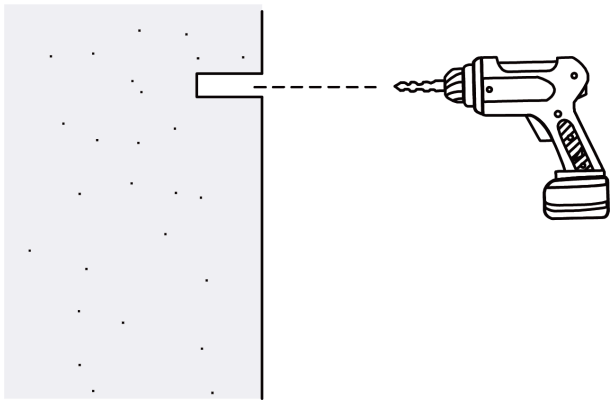
3.4 Wall Mount

The 4-port and 8-port devices support wall mount.

Procedure

Step 1 Mark and drill 2 wall-mounting holes in the wall according to the spacing of the device's wall-mounting holes.

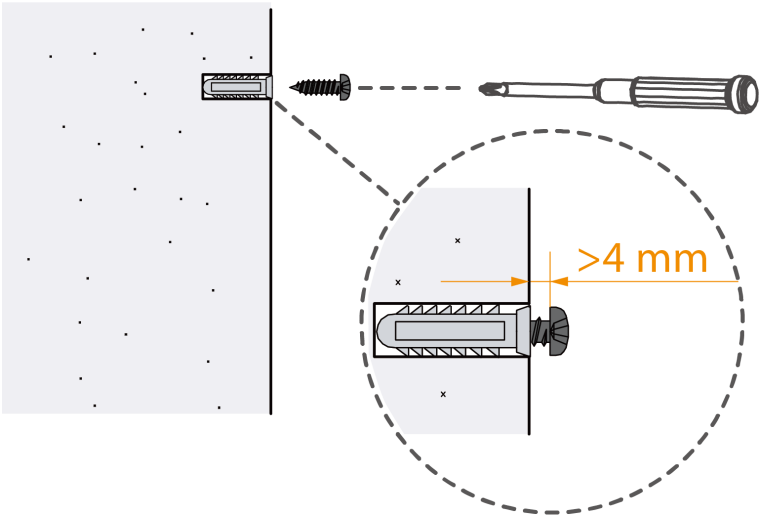
Figure 3-3 Drill the hole



Step 2 Insert the expansion tube into the wall-mounting holes, and then fasten them with two ST3 screws.

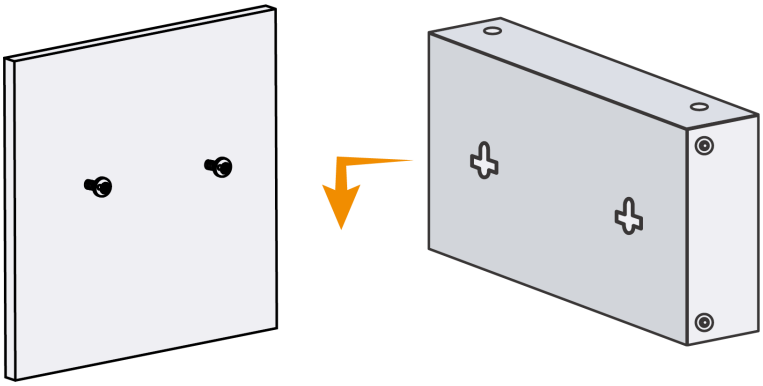
- Some devices do not include standard installation accessories such as screws. Purchase them as needed.
- After tightening the screws, leave 4 mm of the screw exposed for mounting the device.

Figure 3-4 Fasten the screw



Step 3 Align the wall-mounting holes on the back cover with the screws, and then mount the device onto them.

Figure 3-5 Mount the device on the wall



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