Wireless Bridge

Quick Start Guide

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.1.0

Foreword

General

This manual introduces the installation, functions and operations of the wireless bridge (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.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.1.0	Updated the initialization.	May 2026
V1.0.1	Content improvement.	June 2025
V1.0.0	First release.	January 2024

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

- 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.
- When installing the device outdoors on a rooftop pole, securely mount the device to the pole. Do not extend it so that it projects outward without support.

- Do not place the device in a place exposed to sunlight or near heat sources.
- 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.
- 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.
- 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.

- For outdoor installation, securely fasten the device to its bracket on a vertical pole. The installation height and position must comply with design specifications. To prevent corrosion, apply anti-rust paint to all iron components.
- When installing the device outdoors on a rooftop, select a location with minimal or no direct sunlight to prevent overheating from prolonged sun exposure. Take appropriate protective measures if necessary.
- When installing the device outdoors, set it so the Ethernet port faces downward. Also, route all the cables in a downward direction.

Operating Requirements

WARNING

- 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.
- Operating temperature: -30 °C to +65 °C (-22 °F to +149 °F).

Maintenance Requirements

DANGER

Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

Preventive measures (including but not limited to):

- Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
- Dispose of the old batteries as instructed.

WARNING

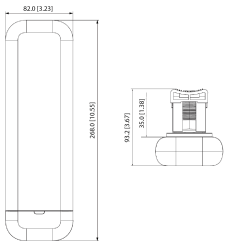
Power off the device before maintenance.

Table of Contents

1 Device Structure

1.1 Dimensions

Figure 1-1 Dimensions (Unit: mm [inch])



1.2 Structure

1.2.1 Indicators

Figure 1-2 Indicators

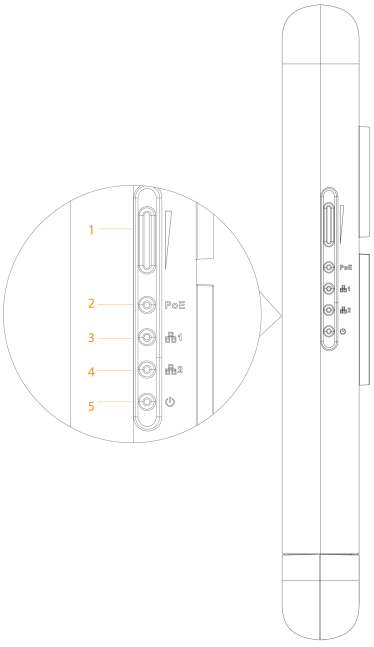


Table 1-1 Description of indicators

No.	Name	Status	Description
1	LED 1/LED 2/LED 3	Off	Not connected to any device.

No.	Name	Status	Description
		On	• LED 1, LED 2, LED 3 are on: strong wireless signal. • LED 1, LED 2 are on, and LED 3 is off: normal wireless signal. • LED 1 is on, and LED 2 and LED 3 are off: poor wireless signal. You need to adjust the direction or position between bridges.
2	PoE indicator	Off	The PoE OUT function is disabled.
		On	The PoE OUT function is enabled.
3	LAN 1 indicator	Off	The port is not properly connected.
		Flicker	Wireless data transmission is in progress.
		On	The port is properly connected.
4	LAN 2 indicator	Off	The port is not properly connected.
		Flicker	Wireless data transmission is in progress.
		On	The port is properly connected.
5	Power indicator	Off	Power supply is abnormal.
		On	Power supply is normal.

1.2.2 Ports and Button

Figure 1-3 Ports and button

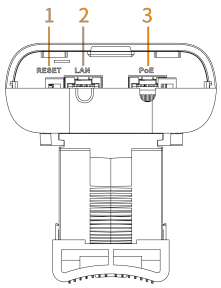


Table 1-2 Description of the items

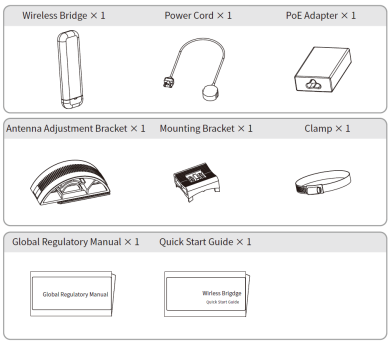
No.	Item	Description
1	RESET	After the Device is powered on for 1 minute, press and hold it for about 5 seconds and then release it. If the indicator light is on and off again, it means that the Device has been restored to factory settings.
2	LAN	Ethernet data transmission port, which can be connected to terminal device or switch.
3	PoE	PoE power input port/data transmission reuse port: The PoE power supply adapter or PoE switch can be connected to supply power to the Device.

2 Installation and Connection

2.1 Packing List

For tools or accessories not listed, purchase them as needed.

Figure 2-1 Packing list



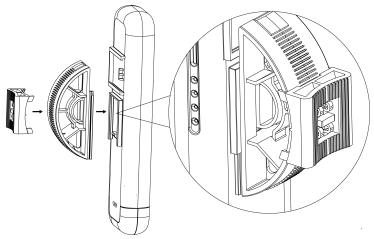
2.2 Device Installation

2.2.1 Vertical Installation

Procedure

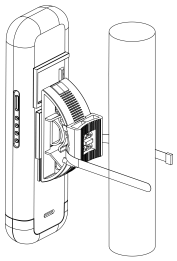
Step 1 Put the mounting bracket into the vertical slot on the back of the Device.

Figure 2-2 Vertical installation of the bridge



Step 2 After crossing the mounting bracket on the back of the Device with the clamp, fix the Device to the mounting rod, and then tighten the clamp.

Figure 2-3 Fixing the bridge

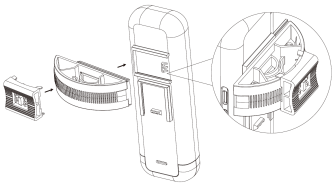


2.2.2 Horizontal Installation

Procedure

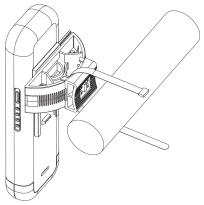
Step 1 Put the mounting bracket into the horizontal slot on the back of the Device.

Figure 2-4 Horizontal installation of the bridge



Step 2 After crossing the mounting bracket on the back of the Device with clamp, fix the Device to the mounting rod, and then tighten the clamp.

Figure 2-5 Fixing the bridge

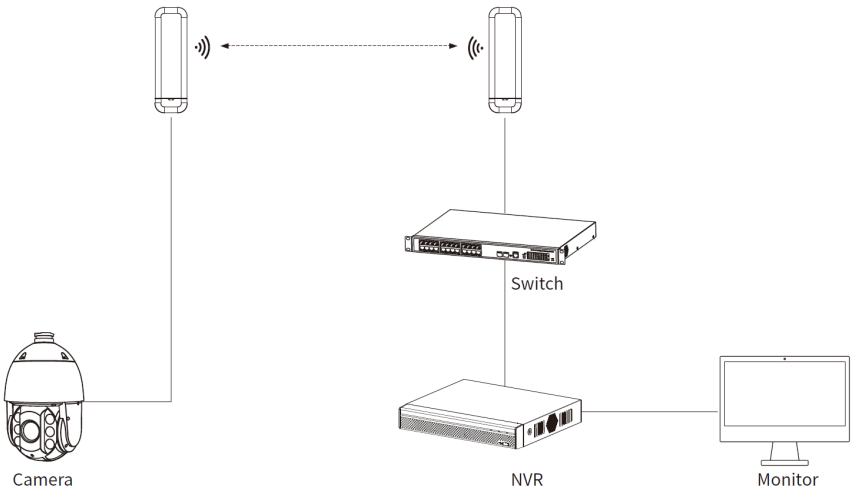


2.3 Device Connection

2.3.1 Connection Mode

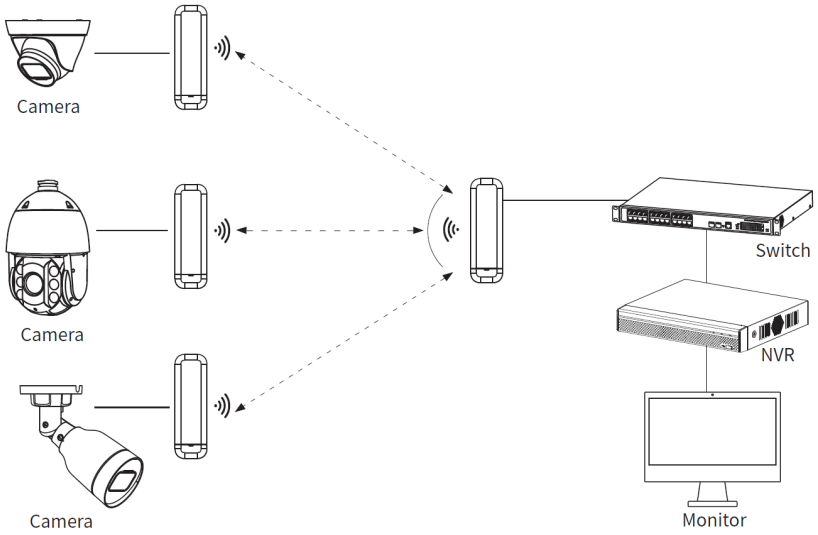
Point to Point

Figure 2-6 Point-to-point connection



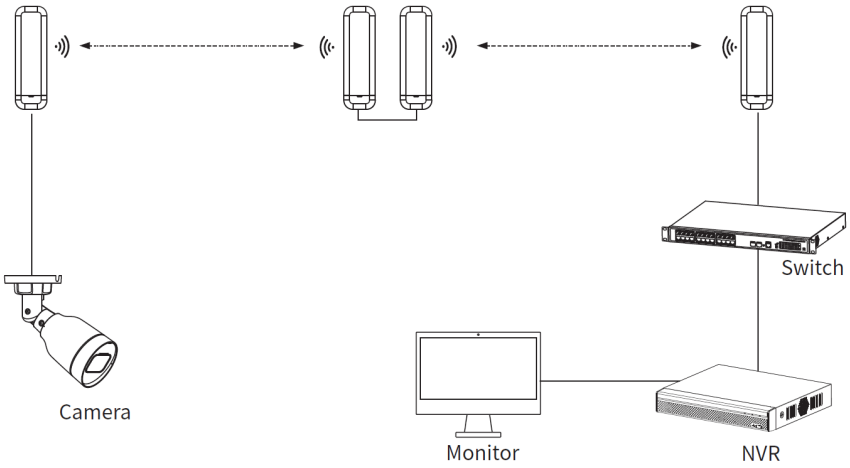
Point to Points

Figure 2-7 Point-to-points connection



Back to Back

Figure 2-8 Back-to-back connection

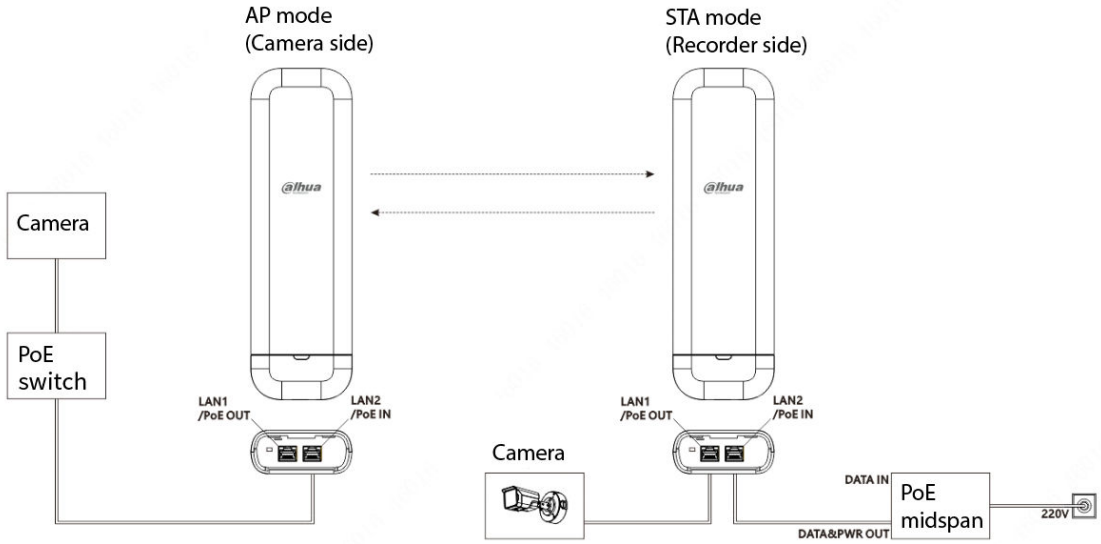


2.3.2 Connecting the Device

Access Point Bridge Directly Connected to PoE Switch

1. Connect the NVR to the PoE switch.
2. Connect the PoE switch to the LAN2/PoE IN port of the access point bridge.
3. Connect the IPC to the LAN1/PoE OUT port of the STA bridge.
4. Connect the midspan to the DATA&PWR OUT port of the STA bridge.
5. Power on the midspan with a supply voltage of 220 V.

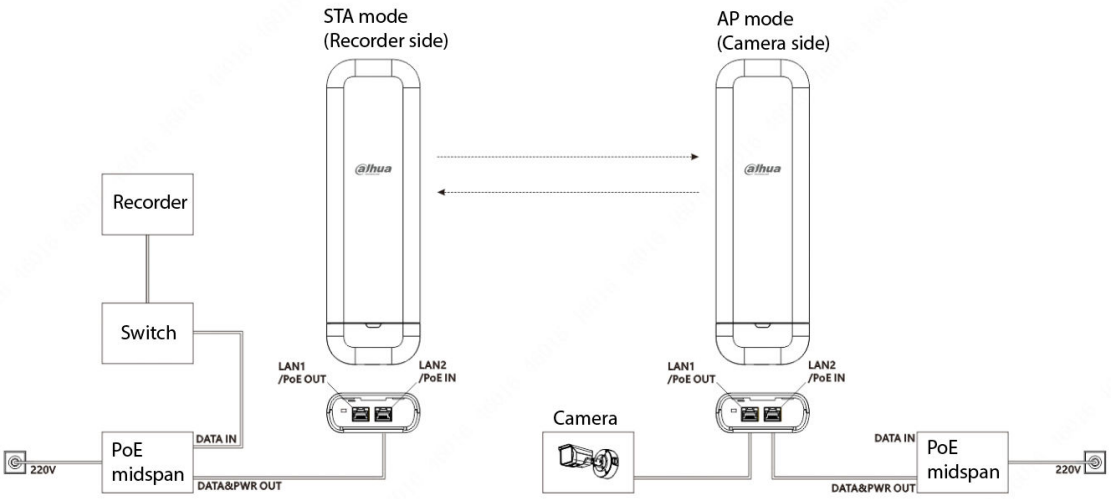
Figure 2-9 Connecting the device (1)



Access Point Bridge Directly Connected to Non-PoE Switch

1. Connect the NVR to the non-PoE switch.
2. Connect the non-PoE switch to the DATA IN port of the access-point-side midspan, and then connect the access point bridge to the DATA&PWR OUT port of the access-point-side midspan.
3. Power on the access-point-side midspan with a supply voltage of 220 V.
4. Connect the IPC to the LAN1/PoE OUT port of the STA bridge, and then connect the DATA&PWR OUT port of the STA-side midspan to the LAN2/PoE IN port of the STA bridge.
5. Power on the STA-side midspan with a supply voltage of 220 V.

Figure 2-10 Connecting the device (2)



3 Initialization

Background Information

- For wireless bridge kit, it has been wirelessly paired by default. To configure and manage the wireless bridge, the device must be initialized firstly.
- For single-packed wireless bridge, initialize the device firstly, and then pair it.
- You can use the DoLynk Care app to initialize and add the Device when the Device is connected to Internet. For details, see the corresponding quick configuration manual.
- You can log in to the webpage to initialize the Device when the Device is not connected to Internet.

Here takes initialization on the webpage as an example.

Procedure

Step 1 Prepare a computer, and then connect to the device through its management SSID.

The SSID is in the format "DAHUA_Wireless_XXXXXX", where "XXXXXX" is the last six digits of the device's serial number. You can find this management SSID on the device label.

Step 2 After the computer is connected, open a browser, and then enter 192.168.177.36 to access the management webpage.

Step 3 Enter the default password **admin123** , reset and confirm the login password of the admin account, and then click **Next** to finish the initialization.

Related Operations

You can also connect the management computer to the bridge in the wired way.

1. Configure a 192.168.1.0/24 network segment IP on the computer, such as 192.168.1.100/24.
2. Open the browser on the computer, and then enter 192.168.1.35 (the default management IP address of the AP mode) or 192.168.1.36 (the default management IP address of the STA mode) to log in to the webpage of the bridge for initialization or management.

Through the ConfigTool, the wireless bridge can only be initialized via a wired connection.

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