Ethernet Switch (Cloud Managed Switch)

User Manual

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

Foreword

This manual introduces the functions and operations of the Ethernet switch (hereinafter referred to as the "device"). Please read carefully before using the product. After reading, please save the document properly for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	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
V1.0.1	• Updated Initialization and Login, Switch Configuration, Network Settings, Security and System. • Added cable test.	February 2026
V1.0.0	First release.	August 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

1 Initialization and Login

The Managed Switch provides WEB access functionality. You can log in to the web page to manage and configure the device.

1.1 Initializing the Device

Prerequisites

- Make sure that the device is connected to the power supply.
- Make sure that the device is connected to the computer, and the IP addresses of the computer and the device are on the same network.
- By default, DHCP is enabled on the device. When connected to a network, the device typically obtains an IP address from a DHCP server, and then you can obtain the IP address of the device from the upstream device, such as a router. If a DHCP server is not available, the IP address of the device is 192.168.1.110 by default.

You can use **ConfigTool** to obtain the IP address on select models of devices.

Procedure

Step 1 Enter the IP address of the device in the address bar of the web browser, and then press the Enter key.

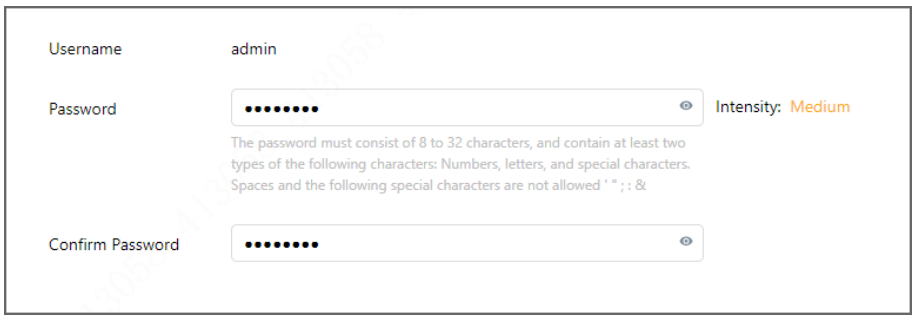
Step 2 Select the language, and then click **Next**.

Step 3 Read the legal statement, select **I have read and agree to the terms of the Software License Agreement and Privacy Policy** , and then click **Next**.

Step 4 Configure the password.

- The default user name is admin.
- Configure a high security password according to the prompt of password strength. A password must be 8-32 characters containing at least 2 types among numbers, letters and common characters (any visible characters other than' " ; : &).

Figure 1-1 Configure password



Step 5 Click **Complete**.

1.2 Login the Device

Prerequisites

- The device has been initialized.

- Make sure that the device is connected to the computer, and the IP addresses of the computer and the device are on the same network.

Procedure

Step 1 Enter the IP address of the device in the address bar of the web browser, and then press the Enter key.

Step 2 Enter the password.

Step 3 Click **Login**.

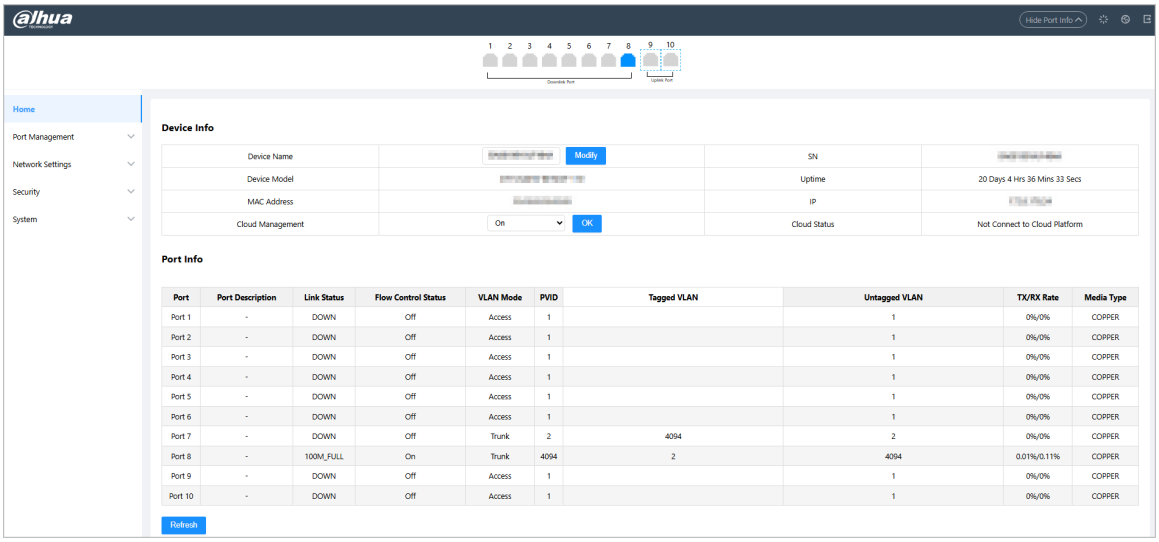
1.3 Home Page

Log in to access the home page.

The left side of the page consists of a menu bar. At the top, there is a graphical display of the port status. In the upper-right corner, supports hiding or showing the port information, logging out, restarting the device, switching the system languages, and scanning QR codes to access information.

The page might vary depending on the product model. Please refer to the actual device.

Figure 1-2 Home page

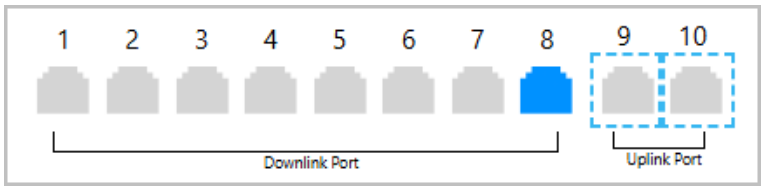


Port Information

Hover over a port to view its connection information, including port status, link status, and power consumption.

- The blue port indicates a successful connection. The gray port indicates no connection.
- Click any port to go to the **Port** page.

Figure 1-3 Port information



Home Page

Home page supports the following functions.

- **Device Info** : Configure the device name and management VLAN.

  After enabling management VLAN, you can only access the webpage of the device through an IP address belong to the management VLAN.

- **Port Info** : Displays the link status, flow control status, and VLAN mode of each port.

Table 1-1 Description of port information

Parameter	Description	
Port	Displays all ports of the device.	
Port description	Displays the port description. You can go to **Port Management** > **Port** to configure this parameter.	
Link Status	◇ DOWN: The port is not connected or the connection fails. ◇ Displays the port rate and the duplex mode: The port is connected. ○ **FULL** : The port can simultaneously receive and transmit data, achieving maximum throughput at double the rate. ○ **HALF** : The port can only either receive or transmit data at the same time.	
Flow Control Status	View the status of the flow control function, including **On** and **Off**. You can go to **Switch Config** > **Port** to configure this parameter.	
VLAN Mode	Includes **Access** and **Trunk**.	
PVID	Displays the VLAN of the port.	You can go to **Switch Config** > **VLAN** to configure this parameter.
Tagged VLAN	Displays the VLAN ID for the port that is allowed to be tagged when transmitting packets.	
Untagged VLAN	Displays the VLAN ID for the port that is allowed to be untagged when transmitting packets.	
TX/RX Rate	Displays the current reception rate or sending rate divided by the actual negotiated rate for a period of time.	
Media Type	Includes 2 types: **COPPER** and **FIBER**. ◇ **COPPER** : RJ-45 port. ◇ **FIBER** : Optical port.	

2 Switch Configuration

2.1 Configuring Port Information

You can configure the port parameters, including speed/duplexing, flow control, and other parameters.

Procedure

Step 1 Select **Port Management** > **Port**.

Step 2 In the **Port** list, select the port number, configure the parameters, and then click **Save**.

- **Speed/Duplexing** : In the **Speed/Duplexing** list, select the speed and the duplex mode. The speed/duplexing is set as **Auto** for combo port.
- **Flow Control** : In the **Flow Control** list, select **on** to enable this function, effectively relieving network congestion, reduce data loss, and improve network stability and data reliability.
- **EEE Config** : In the **EEE Config** list, select **on** to enable this function, reducing power consumption when the network is idle and achieve energy saving.

Figure 2-1 Port configuration (1)

Step 3 In the **Port Description** box, enter the description of the port, and then press Enter key or click any other area on the page to save the configuration.

The port description supports numbers, letters, special character (_), with a maximum length of 16 characters. The default value is empty.

Figure 2-2 Port configuration (2)

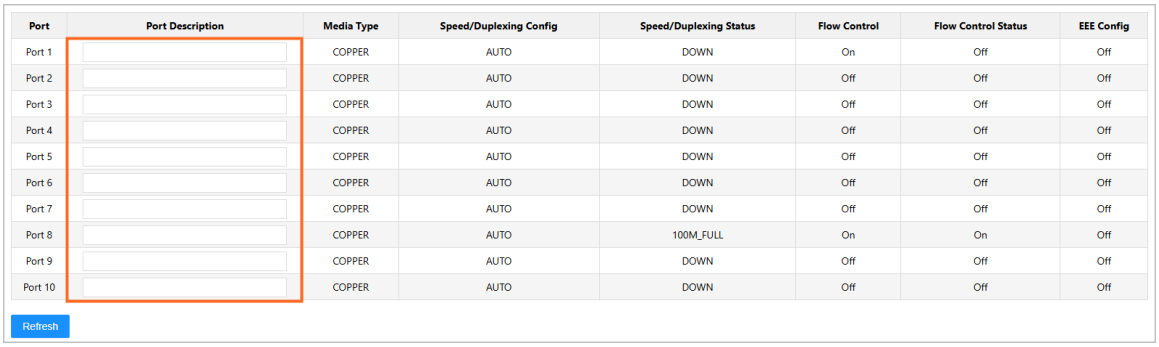


Table 2-1 Description of the port parameters

Parameter	Description
Media type	Includes 2 types: **COPPER** and **FIBER**. • **COPPER**: RJ-45 port. • **FIBER**: Optical port.

Parameter	Description
Speed/Duplexing configuration	Displays the configured parameters of this port.
Speed/Duplexing status	• **DOWN** : Displays the port is not connected or the connection fails. • Displays the port rate and the duplex mode: Displays the port is connected. ◇ **FULL** : The port can simultaneously receive and transmit data, achieving maximum throughput at double the rate. ◇ **HALF** : The port can only either receive or transmit data at the same time.
Flow control	Displays whether the flow control function is enabled and the current flow control status.
Flow control status	
EEE configuration	Displays whether the EEE function is enabled.

2.2 PoE Management

PoE refers to that the device uses network cables to externally connect PD (Powered Device) for remote power supply through Ethernet electrical ports. PoE function enables centralized power supply and convenient backup. Network terminals do not need external power supply, but only one network cable.

Non-PoE devices do not support this function.

2.2.1 Global Configuration

You can configure the perpetual PoE and available power.

Procedure

Step 1 Select **Port Management** > **PoE** > **Global Config**.

Step 2 Select **Perpetual PoE** checkbox, and then click **Save**.

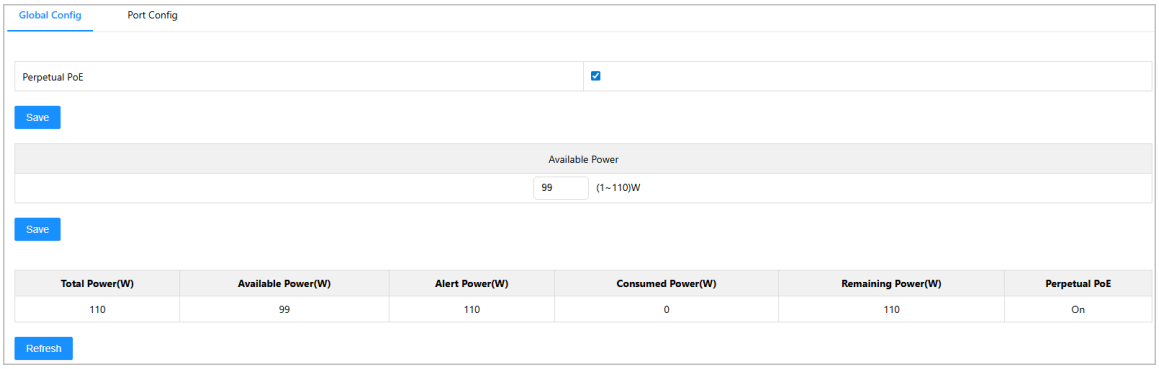
Enable perpetual PoE, which continues to supply power to powered devices when the device is soft-rebooted. If the device is power off and restart, it will not continue to supply to powered devices after the reboot.

Step 3 Configure the available power.

Displays information such as total power, available power, alert power, consumed power, remaining power and perpetual PoE at the bottom of the page.

- Available power refers to the maximum power that can be provided to powered devices. When the consumed power is less than available power, new PD is allowed to be powered on.
- During operation, the actual power consumption might fluctuate. When the consumed power exceeds the alert power, the ports will be powered down from low to high according to the priority (the higher the port number, the lower the priority), until the consumed power is less than the alert power.

Figure 2-3 Global configuration



Step 4 Click **Save**.

2.2.2 Port Configuration

Configure the PoE function of the port.

Procedure

Step 1 Select **Port Management** > **PoE** > **Port Config**.

Step 2 Configure the port parameters.

- Set the port configuration. In the **Port** list, select the port number, enable the PoE, long distance PoE, PoE watchdog, enhanced PoE, and force PoE as needed.

Figure 2-4 Port configuration (1)

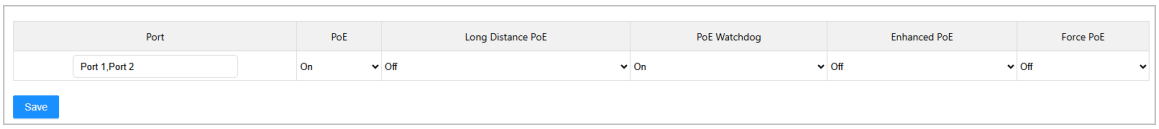


Table 2-2 Description of PoE parameters

Parameter	Description
PoE	The device uses network cables to externally connect PD for remote power supply through Ethernet electrical ports.
Long distance PoE	After you enable long distance PoE, the maximum transmission distance will change from 100 m to 250 m, and the transmission speed will be reduced to 10 Mbps. The actual transmission distance might vary due to power consumption of connected devices or the cable type and status.
PoE watchdog	With PoE watchdog enabled, the device periodically checks the status of the PD. If no data transmission is detected, it automatically powers off and restarts the PoE port, ensuring port monitoring and maintaining PD connectivity.
	Force PoE and **PoE watchdog** cannot be enabled at the same time.

Parameter	Description
Force PoE	When the powered device connected to the port is a non-standard device, use this function to force PoE power supply. After force PoE is enabled, connecting a non-PoE device to a forced PoE port might result in PD damage.
Enhanced PoE	When disabled, this function only supports PD compliant with standard PoE protocols, delivering power based on the device's defined power class. When enabled, it extends compatibility to both standard PoE devices and some non-standard PoE devices, delivering power based on the device's defined power class. The port types and the corresponding output power are as follows. ◇ AF/AT: 30 W ◇ Hi-PoE: 60 W ◇ BT: 90 W This configuration option is available only for standard PoE devices.

- View the PoE parameter configuration of each port.

Figure 2-5 Port configuration (2)

Port	Level	Consumed Power(W)	PoE Enable	Long Distance PoE	PoE Watchdog	Enhanced PoE	Force PoE
Port1	-	0	On	Off	Off	Off	Off
Port2	-	0	On	Off	Off	Off	Off
Port3	-	0	On	Off	Off	Off	Off
Port4	-	0	On	Off	Off	Off	Off
Port5	-	0	On	Off	Off	Off	Off
Port6	-	0	On	Off	Off	Off	Off
Port7	-	0	On	Off	Off	Off	Off
Port8	-	0	On	Off	Off	Off	Off

Table 2-3 Description of PoE parameters

Parameter	Description
Level	Displays the power supply level of the terminal devices. The power supply level ranges from 0 through 8, and the Hi-PoE power supply standard level is displayed as 5+.
Consumed power (W)	Displays the current PoE power consumed by the corresponding single port.
PoE enable	Displays whether these 5 types of PoE features are enabled on the ports.
Long distance PoE	
PoE watchdog	
Enhanced PoE	
Force PoE	

Step 3 Click **Save**.

2.3 Port Statistics

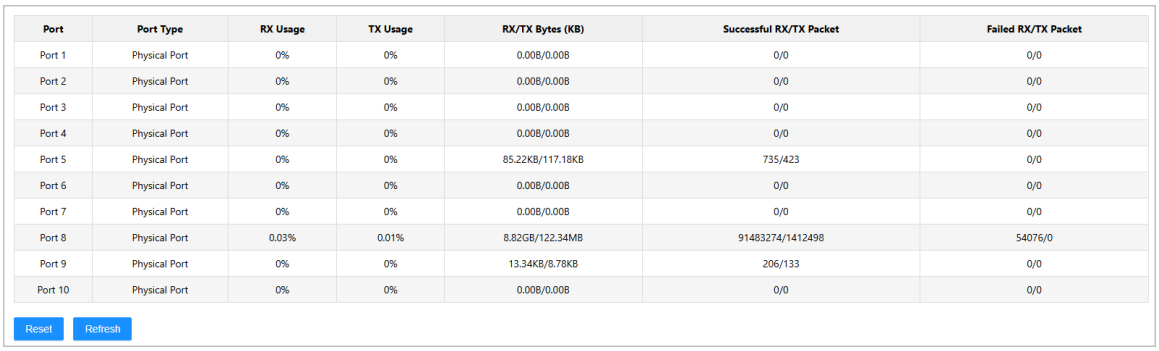
Procedure

Step 1 Select **Port Management** > **Port Statistics**.

Step 2 View the information of port such as port type, receive usage, transmit usage, and more.

Step 3 (Optional) Click **Reset** to clear port statistics.

Figure 2-6 Port statistics



Port	Port Type	RX Usage	TX Usage	RX/TX Bytes (KB)	Successful RX/TX Packet	Failed RX/TX Packet
Port 1	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 2	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 3	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 4	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 5	Physical Port	0%	0%	85.22KB/117.18KB	735/423	0/0
Port 6	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 7	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 8	Physical Port	0.03%	0.01%	8.82GB/122.34MB	91483274/1412498	54076/0
Port 9	Physical Port	0%	0%	13.34KB/8.78KB	206/133	0/0
Port 10	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0

Reset Refresh

Table 2-4 Description of PoE parameters

Parameter	Description
Port	Displays the port number.
Port type	Displays the port type, indicating the type of port, such as **Physical Port**.
RX usage	Displays the receive usage, indicating the percentage of bandwidth utilization for incoming traffic.
TX usage	Displays the transmit usage, indicating the percentage of bandwidth utilization for outgoing traffic.
RX/TX Bytes (KB)	Displays the received/transmitted Bytes (KB), showing the total data volume.
Successful RX/TX packet	Displays the successful received/transmitted packets, indicating the number of successfully received and sent data packets.
Failed RX/TX Packet	Displays the failed received/transmitted packets, indicating the number of failed received and sent data packets.

2.4 Cable Test

Background Information

Detect the status of network cables connected to ports to quickly locate faulty cables and their corresponding positions.

- The maximum detectable length is 100 meters for network cables.
- Only copper ports support cable testing; optical ports do not.
- The test results are based on signal attenuation and are for reference only. When the cable is connected and shorter than 3 meters, signal attenuation primarily comes from connectors rather than the cable itself, leading to relatively higher measurement errors.

Procedure

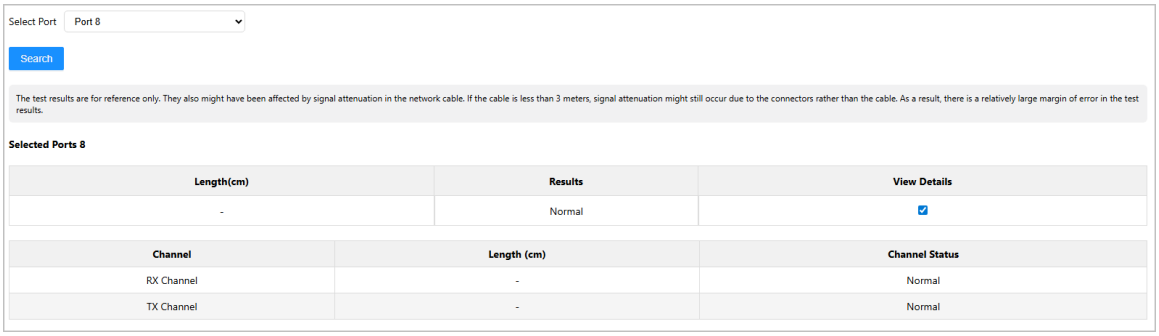
Step 1 Select **Port Management** > **Cable Test**.

Step 2 In the **Select Port** list, select the port number as needed, and then click **Search**.

Step 3 Confirm the cable status based on the test results.

- Normal: The cable is functioning properly.
- Open circuit: No cable is connected, or the cable is broken.
- Short circuit: The cable is faulty.

Figure 2-7 Cable test



Step 4 (Optional) Click under the **View Details** to view the distance from the normal or fault point to the port.

2.5 Port Mirroring

Port mirroring, also known as port monitoring, is a packet technique. By configuring the device, you can copy data packets from one or more source ports (mirrored ports) to a specific destination port (monitoring port). A host running packet analysis software is connected to the destination port to analyze the collected packets, enabling network monitoring and troubleshooting.

Procedure

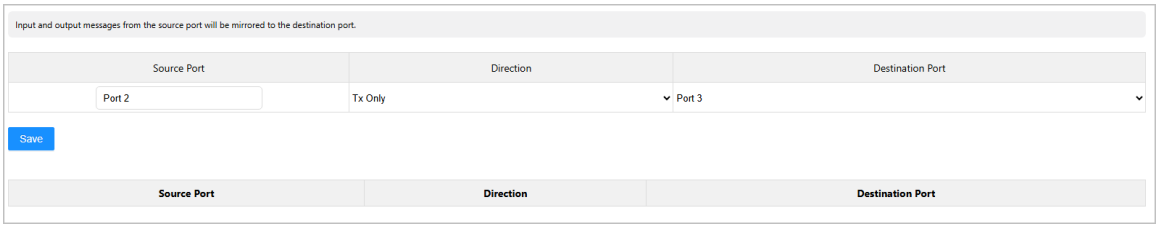
Step 1 Select **Port Management** > **Port Mirroring**.

Step 2 In the **Select Port** list, select the port number, direction and destination port as needed.

Direction supports Tx only, Rx only and bidirectional modes.

- Tx only: Only copies transmitted packets.
- Rx only: Only copies received packets.
- Bidirectional: Copies both transmitted and received packets.

Figure 2-8 Port mirroring



Step 3 Click **Save**, and then the added mirroring information is displayed at the bottom of the page.

3 Network Settings

3.1 Configuring VLAN

You can add the port to the VLAN, and then you can configure the VLAN parameters.

Procedure

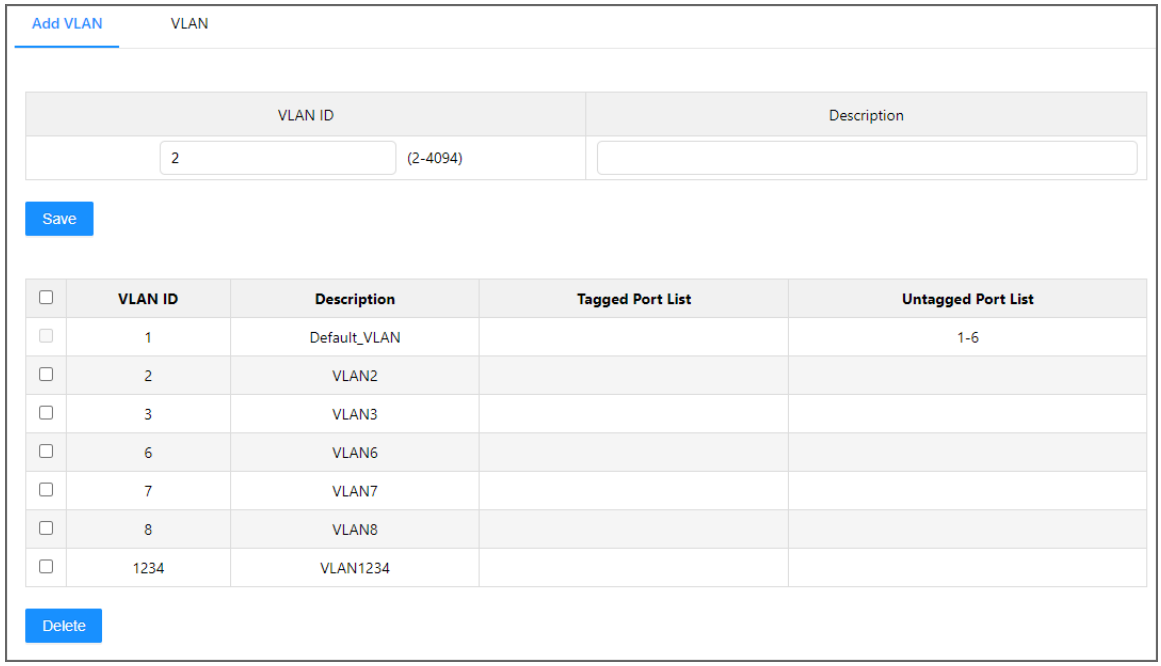
Step 1 Select **Network Settings** > **VLAN** > **Add VLAN**.

Step 2 Enter the VLAN ID and description, and then click **Save**.

- The added VLAN information is displayed at the bottom of the page.
- You can select the VLAN and then click **Delete** to delete the VLAN.

VLAN1 cannot be deleted.

Figure 3-1 Add VLAN



Step 3 Select **Network Settings** > **VLAN** > **VLAN**.

1. In the **Port** box, select one or more ports.
2. In the **Mode** list, select the VLAN mode, including **Access** and **Trunk**.
3. Configure PVID, tagged VLAN, and untagged VLAN.
   - When the **Mode** is **Access**, you must configure the **untagged VLAN**. Untagged VLAN indicates the VLAN ID for the port that is allowed to be untagged when sending packets.
   - When the **Mode** is **Trunk**, you must configure **PVID** and **tagged VLAN**.
     - PVID indicates that the port is added to a VLAN. By default, the port belongs to VLAN 1.
     - The VLAN ID for the port that is allowed to be tagged when sending packets.

Figure 3-2 VLAN

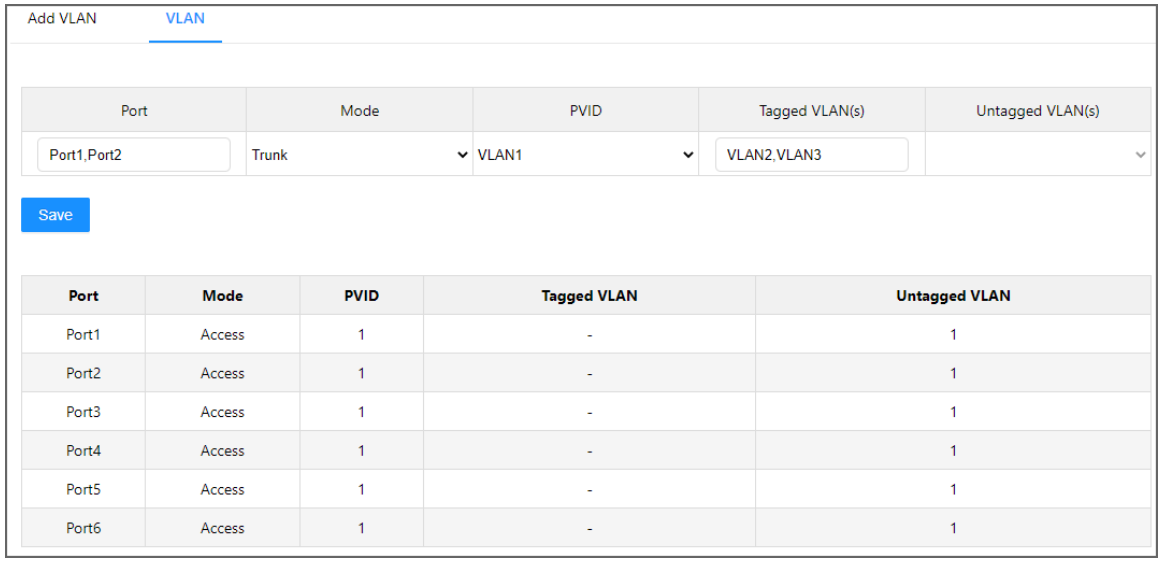


Table 3-1 Frame processing comparison

Port Type	Untagged Frame Processing	Tagged Frame Processing	Frame Transmission
Access	Adds the port PVID tag to the frame.	• Accepts the tagged frame if the frame's VLAN ID matches the default VLAN ID. • Discards the tagged frame if the frame's VLAN ID differs from the default VLAN ID.	After the PVID tag is removed, the frame is transmitted.
Trunk		• Accepts a tagged frame if the VLAN ID carried in the frame is permitted by the port. • Discards a tagged frame if the VLAN ID carried in the frame is denied by the port.	• If the frame's VLAN ID matches the default VLAN ID and the VLAN ID is permitted by the port, the device removes the tag and transmits the frame. • If the frame's VLAN ID differs from the default VLAN ID, but the VLAN ID is still permitted by the port, the device will directly transmit the frame.

4. Click **Save**, and then the added VLAN information is displayed at the bottom of the page.

3.2 Viewing LLDP List

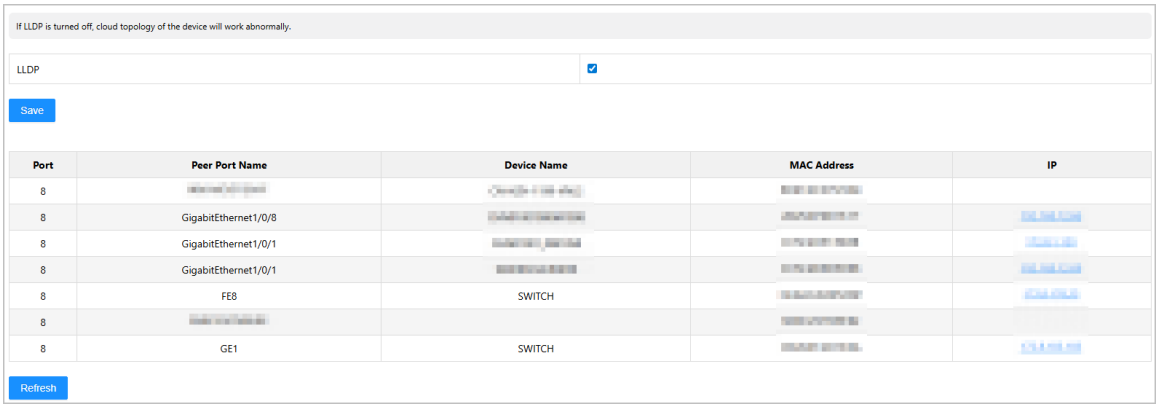
LLDP (Link Layer Discovery Protocol) is a standard link-layer discovery method. It organizes the local device's main capabilities, management address, device identifier, port identifier, and other information into different TLVs (Type Length Value) and encapsulates them in LLDPDU (Link Layer Discovery Protocol Data Unit). These are then sent to directly connected neighbors. Upon receiving this information, the neighbors store it in a standard MIB (Management Information Base) format, allowing network management systems to query and assess the communication status of the link.

Procedure

Step 1 Select **Network Settings** > **LLDP Neighbor List**.

Step 2 Select **LLDP** checkbox, and then click **Save**.

Figure 3-3 LLDP neighbor list



3.3 Configure MAC Tables

MAC (Media Access Control) table records the relationship between the MAC address and the port, and the information including the VLAN that the port belongs to. When the device is forwarding the packet, it queries in the MAC address table for the destination MAC address of the packet. If the destination MAC address of the packet is contained in the MAC address table, the packet is forwarded through the port in the table directly. And if the destination MAC address of the packet is not contained in the MAC address table, the device adopts broadcasting to forward the packet to all the ports except the receiving port in VLAN.

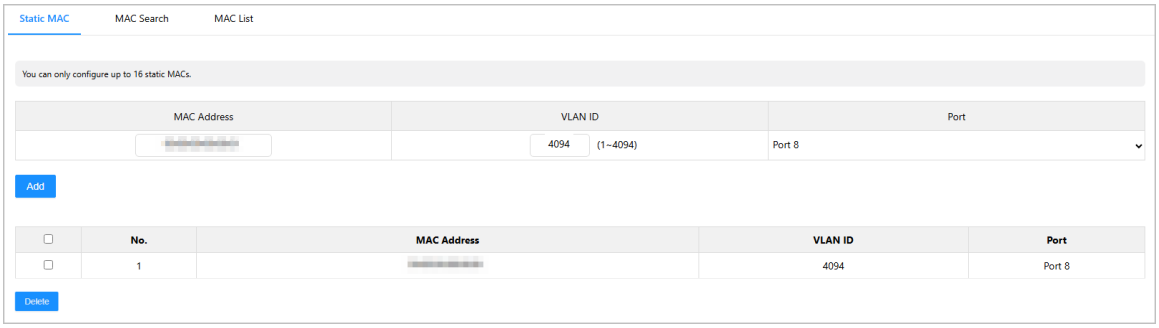
Procedure

Step 1 Add the Static MAC.

- The maximum number of static MAC entries that can be configured depends on the specific device.
- Select a MAC and then click **Delete**, you can delete the static MAC.

1. Select **Network Settings** > **MAC Management** > **Static MAC**.
2. Configure the MAC address, VLAN ID and port, and then click **Add**.

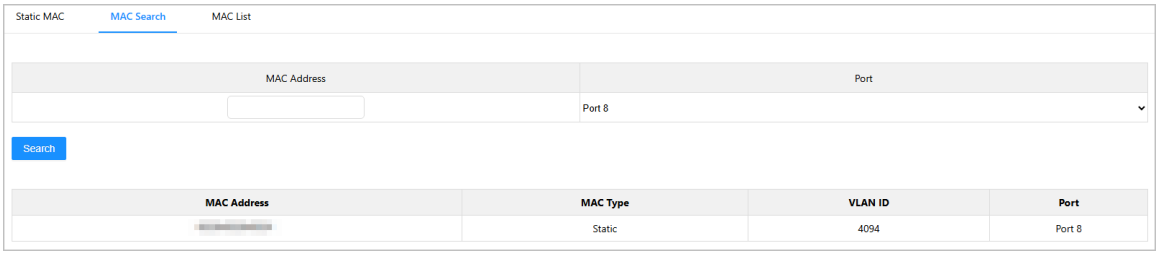
Figure 3-4 Static MAC



Step 2 Search the MAC address.

1. Select **Network Settings** > **MAC Management** > **MAC Search**.
2. Enter the MAC address or select the port, and then click **Search**.

Figure 3-5 MAC search



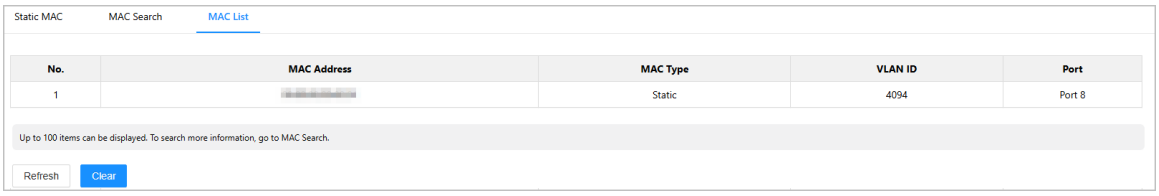
Step 3 View MAC address.

Select **Network Settings** > **MAC Management** > **MAC List** to view the added MAC address information.

Up to 100 items can be displayed. For details, go to **MAC Search**.

Click **Clear** , and then click **OK** to clear the information.

Figure 3-6 MAC list



3.4 Configuring Loop Protection

Select **Network Settings** > **Loop Protection**, enable loop protection, and then click **Save**. After loop protection is enabled, if a loop is detected, the port which caused the loop will be disabled and then automatically restored after the loop is eliminated.

Loop Protection is used to detect and block the abnormal loop. It is not designed for backuping the redundant links.

4 Security

4.1 Configuring Port Isolation

By using the port isolation feature, isolation between ports within the same VLAN can be achieved. The port isolation function provides users a more safer and flexible networking solution.

Procedure

Step 1 Select **Security** > **Port Isolation**.

Step 2 Enable port separation.

After port isolation is enabled, Ethernet ports will be isolated and uplink ports will not be isolated (data can only be transferred between uplink and Ethernet ports).

Step 3 Click **Save**.

4.2 Configuring Port Speed Limit

Configure port rate limiting policies to restrict the rate of data packet exchange in and out of the port.

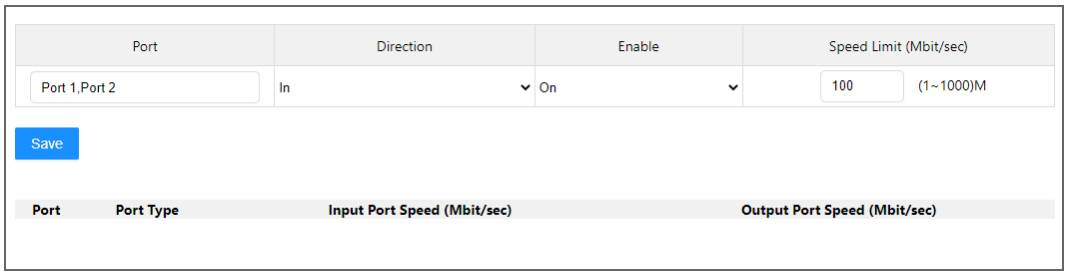
Procedure

Step 1 Select **Security** > **Port Speed Limit**.

Step 2 Select port and direction, enable port speed limit, and then enter the speed.

The direction includes in and out.

Figure 4-1 Port speed limit



Step 3 Click **Save**, and then the information that has been set is displayed at the bottom of the page.

4.3 Configuring Storm Control

The broadcast frames on the network are forwarded continuously, which affects the proper communications, and greatly reduces the network performance. The storm control can limit the broadcast flows of the port and discard the broadcast frames once the flow exceeds the specified threshold, which can reduce the risk of the broadcast storm and ensure the network proper operation.

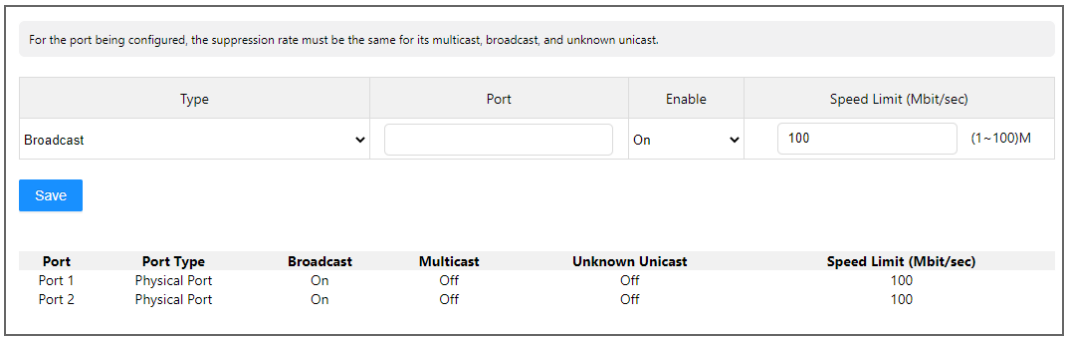
Procedure

Step 1 Select **Security** > **Storm Control**.

Step 2 Configure suppression for the rates of broadcast, multicast, and unknown unicast.

Select the packet type and port number, enable storm control, and then enter the speed limit.

Figure 4-2 Storm control



Step 3 Click **Save**, and then the information that has been set is displayed at the bottom of the page.

5 System

5.1 Restore Factory Default

Procedure

Step 1 Select **System** > **System**.

Step 2 Click **Default** , enter the password, and then click **OK**.

- All parameters restore to default settings except the IP address, subnet mask, gateway, and DNS.
- Yon can restore all configurations through the reset button.

5.2 Update Software

Procedure

Step 1 Select **System** > **System**.

Step 2 Click **Browse** to import the update file, and then click **Update**.

Step 3 Click **OK** in the pop-up prompt box.

It might take 3 minutes to update the software. After the update, the system will automatically restart.

5.3 Restarting Device

Procedure

Step 1 Select **System** > **System**.

Step 2 Click **Restart**.

Step 3 Click **OK** in the pop-up prompt box to restart the device.

You can also restart the device by clicking  in the upper-right corner of the page.

5.4 Changing Password

Changing the login password for the device web page.

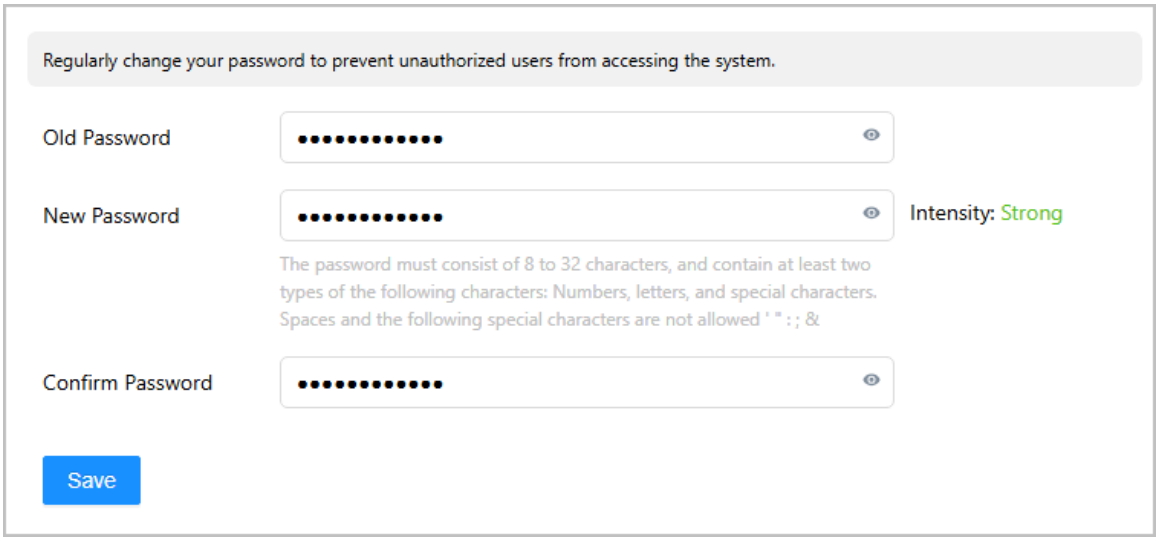
Procedure

Step 1 Select **System** > **Login Management**.

Step 2 Enter the old password, new password, and then confirm the new password.

The password must consist of 8 to 32 characters, and contain at least 2 types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

Figure 5-1 Change password



Step 3 Click **Save**.

5.5 Viewing Device Information

Select **System** > **Device Info**, you can view the information such as the device name, software version, MAC address, and running time. Support enabling cloud management functionality.

5.6 Viewing Log Information

Select **System** > **Log Info**, view the user login log information.

5.7 Configuring Network

Configure the IP address, DNS server, and more.

Procedure

Step 1 Select **System** > **IP Management**.

Step 2 Configure the parameters.

- **Enable DHCP** : After enabling DHCP, the device will be automatically acquire and assign an IP address, provided that a DHCP server is available in the network.
- **Disable DHCP** : Enter the IP address, subnet mask, and gateway to configure a static IP address.
- **Enable Auto Obtain DNS** : The device automatically obtains the IP address of the DNS server in the network, provided that a DNS server is available in the network.
- **Disable Auto Obtain DNS** : Enter the IP addresses of the DNS1 and DNS2.

Figure 5-2 Network information

Step 3 Click **Save**.

5.8 Viewing Legal Information

Select **System** > **Legal Statement**, click the corresponding tab to view the software license agreement and privacy policy.

Appendix 1 Security Commitment and Recommendation

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;
   - Stablish 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