Dahua Dual Optical Port 4-Port PoE Switch

Quick Start Guide

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.3

Important Safeguards and Warnings

Please read the following safeguards and warnings carefully before using the product in order to avoid damages and losses.

Attentions:

- Do not expose the device to lampblack, steam or dust. Otherwise it may cause fire or electric shock.
- Do not install the device at position exposed to sunlight or in high temperature. Temperature rise in device may cause fire.
- Do not expose the device to humid environment. Otherwise it may cause fire.
- The device must be installed on solid and flat surface in order to guarantee safety under load and earthquake. Otherwise, it may cause device to fall off or turnover.
- Do not place the device on carpet or quilt.
- Do not block air vent of the device or ventilation around the device. Otherwise, temperature in device will rise and may cause fire.
- Do not place any object on the device.
- Do not disassemble the device without professional instruction.

Warning:

- Please use battery properly to avoid fire, explosion and other dangers.
- Please replace used battery with battery of the same type.
- Do not use power line other than the one specified. Please use it properly. Otherwise, it may cause fire or electric shock.

Special Announcement:

- This manual is for reference only.
- All the designs and software here are subject to change without prior written notice.
- All trademarks and registered trademarks are the properties of their respective owners.
- If there is any uncertainty or controversy, please refer to the final explanation of us.
- Please visit our website for more information.

Table of Contents

1 Product Overview

1.1 Features

Common features:

- Two-layer industrial PoE switch.
- Conform to IEEE802.3, IEEE802.3u, IEEE802.3ab/z and IEEE802.3X standards.
- MAC auto study and aging, MAC address list capacity is 8K.
- All ports self-adapt MDI/MDIX mode.
- Three 10/100 Mbps self-adaptive RJ45 ports; support IEEE802.3af, IEEE802.3at standard power supply.
- One 10/100/1000 Mbps self-adaptive RJ45 port, support Hi-PoE 60W power supply.
- Support two 1000 Mbps SFP optical ports, used for cascading or forming looped network.
- Support PoE power consumption management function, make sure it won't cause power failure to the device when it is overloaded.
- The indicator light displays PoE power supply, power failure and other functions.
- Industrial wide temperature design.
- Adopt metal structure.
- Support 48-57 VDC power supply.

Individual features:

- DH-PFS3206-4P-96 and DH-PFS4206-4P-96 support PoE total output power 96 W;
  DH-PFS3206-4P-120 and DH-PFS4206-4P-120 support PoE total output power 120 W.
- DH-PFS3206-4P-96 and DH-PFS3206-4P-120 support dual optical port as cascading;
  DH-PFS4206-4P-96 and DH-PFS4206-4P-120 support dual port to form looped network with convergence switch DH-PFS5424-24T.
- Ring network PoE switch supports loop protection and RSTP.
- Cascading PoE switch is not equipped with network management function while ring network PoE switch is so, including system info check and setup, port mirroring, 802.1Q VLAN, ring network, SNMP, PoE page management and etc.

1.2 Typical Application

1.2.1 Cascading Mode

See Figure 1-1 for the cascading mode.

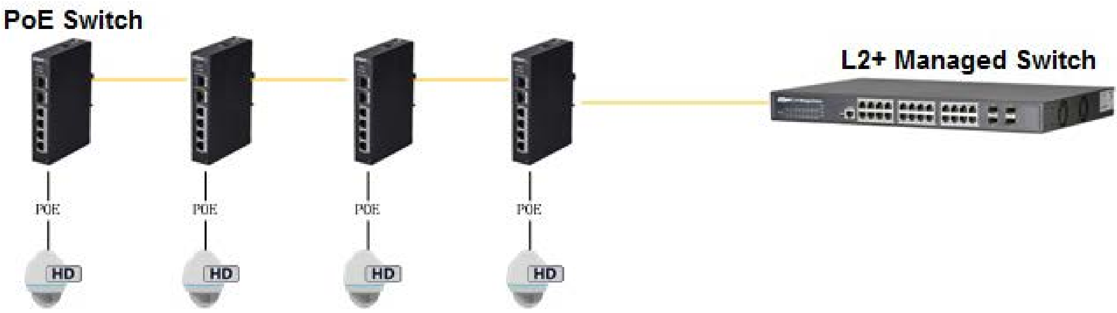


Figure 1-1

1.2.2 Ring Network Mode

See Figure 1-2 for the typical networking scene.

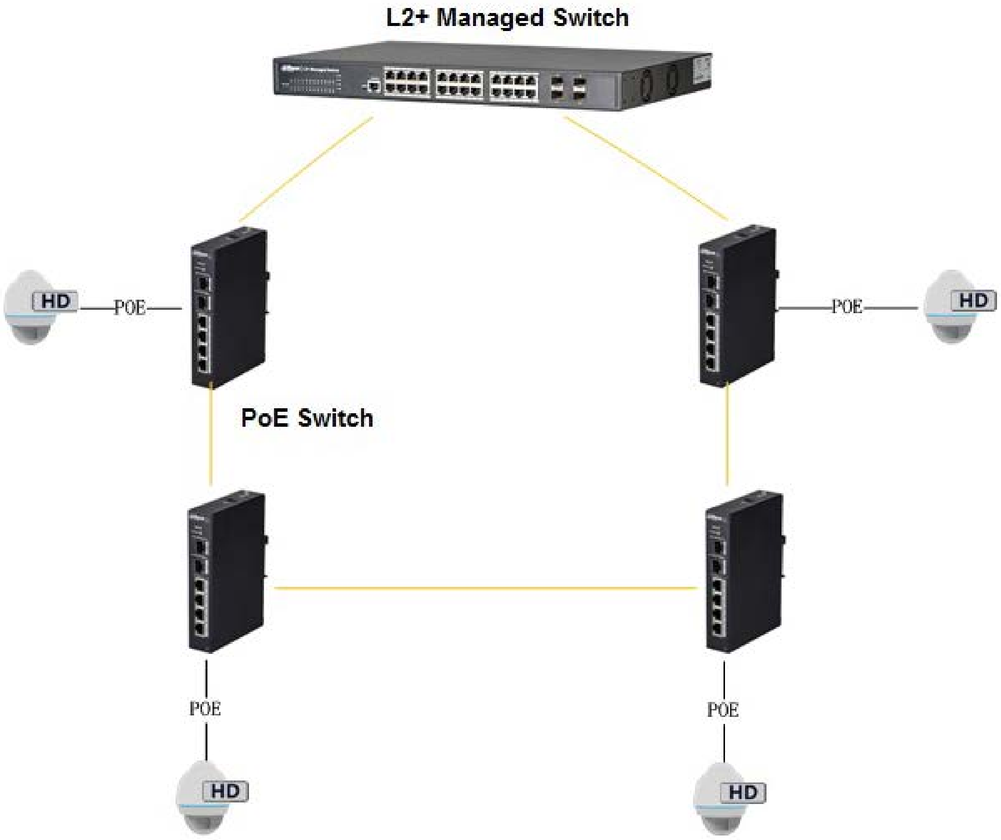


Figure 1-2

2 Device Structure

2.1 4-Port PoE Switch

2.1.1 Front Panel

The front panel is shown in Figure 2-1.

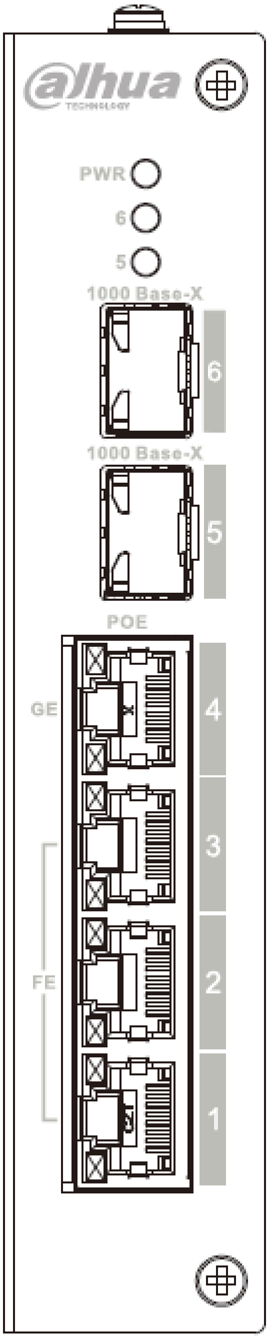


Figure 2-1

Refer to Sheet 2-1 for more details about the front panel.

SN	Name	Function
1	FE	10/100 Mbps self-adaptive RJ45 port, used for PoE power supply
2	GE	10/100/1000 Mbps self-adaptive RJ45 port, used for PoE power supply.
3	1000 Base-X	1000 Mbps SFP optical port.
4	Link / Act	Optical port status indicator light.
5	PWR	Power indicator light, used for PoE power supply indication as well, refer to the following sheet for more details.

Sheet 2-1

The PoE operation status indication shares the POWER light, which includes three statuses: single port device power on, single port device power off and unit device consumption overload. Please refer to the sheet 2-2 for more details.

SN	**Operation Status**	**Display Mode**
1	Single port device power on	Slow flash twice
2	Single port device power off	Quick flash once, slow flash once
3	Unit device consumption overload	Quick flash twice

2.1.2 Upper Cover

The device power port is shown in Figure 2-2; it supports 48-57 VDC power supply.

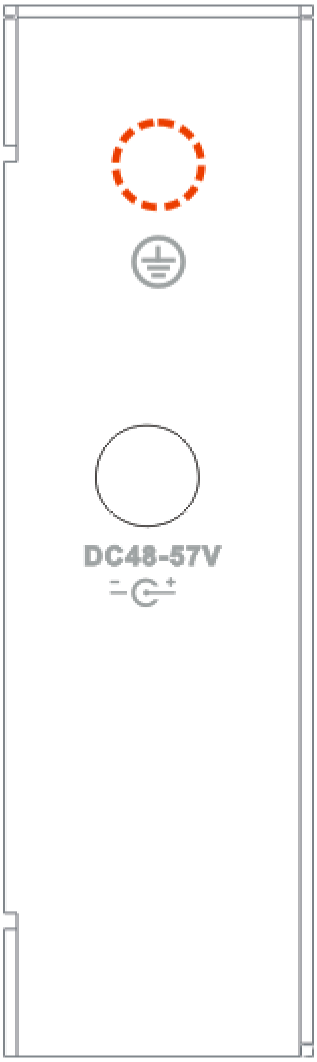


Figure 2-2

2.1.3 PoE Power Supply

- 3 FE RJ45 ports support IEEE802.3af, IEEE802.3at standard power supply.
- 1 GE RJ45 port supports IEEE802.3af, IEEE802.3at standard and Hi-PoE 60 W power supply.
- The total power of PoE power supply is no more than 96 W or 120 W according to different product models.

Users can connect the device to PC and implement system setup, device management and port management upon the device.

3 WEB Client Operation

3.1 Login

Make sure the device is connected to PC before logging in Web, and make the PC and device in the same network segment. The steps of logging in WEB client are as follows:

Step 1

Enter device IP address in the IE address bar (default IP address is: 192.168.1.110), press "Enter",

and the system displays the interface as shown in Figure 3-1.

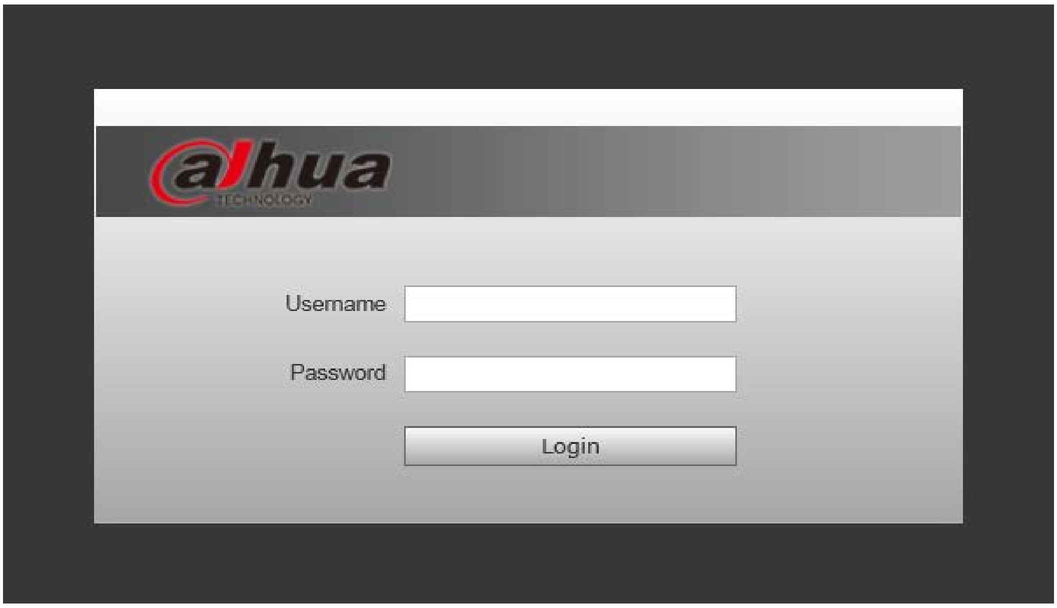


Figure 3-1

Step 2

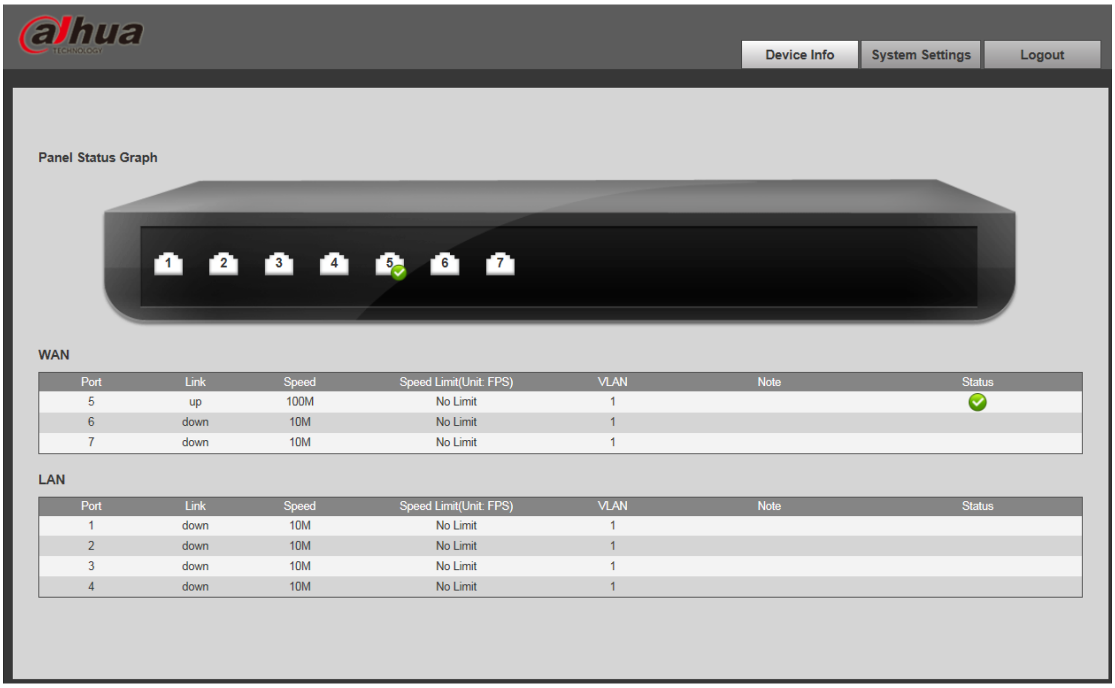
Enter "User name" and "password"; single click "Login", the system will enter the main interface of Web client.

Note:

Device factory default password is empty; users only need to enter user name "admin", and log in without entering password.

3.2 Device Info

✓： Greens means link is normal; ⚠： Yellow means abnormality, general; ⚠： Red means abnormality, serious. See Figure 3-2 for more details.



Panel Status Graph

WAN

Port	Link	Speed	Speed Limit(Unit: FPS)	VLAN	Note	Status
5	up	100M	No Limit	1		✓
6	down	10M	No Limit	1		
7	down	10M	No Limit	1		

LAN

Port	Link	Speed	Speed Limit(Unit: FPS)	VLAN	Note	Status
1	down	10M	No Limit	1		
2	down	10M	No Limit	1		
3	down	10M	No Limit	1		
4	down	10M	No Limit	1		

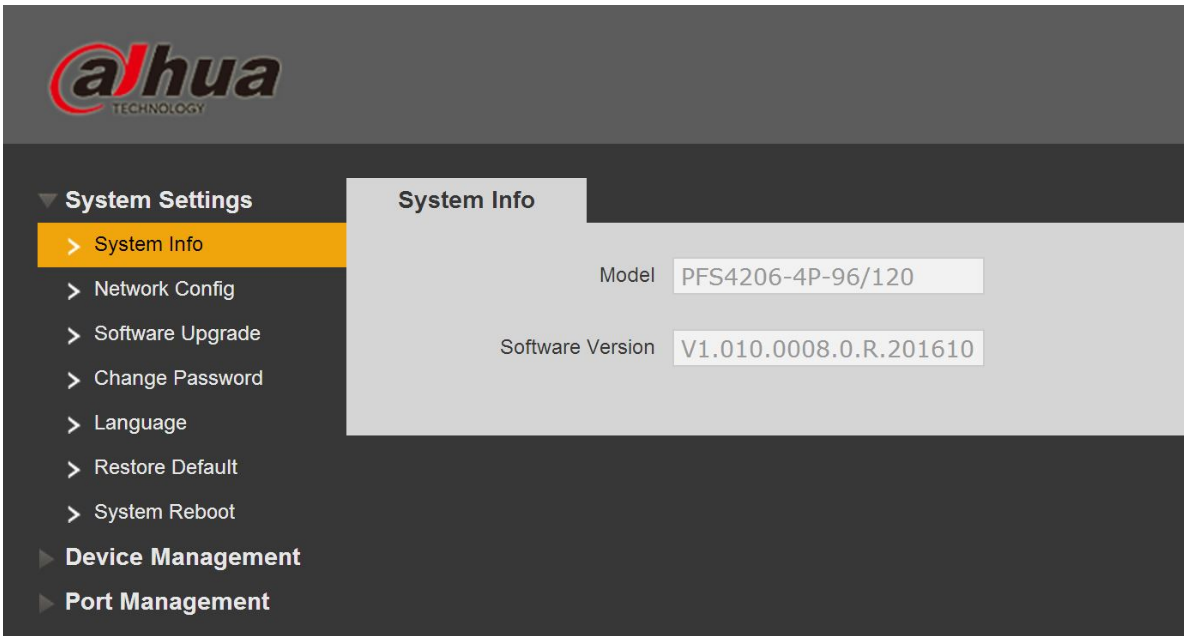
Figure 3-2

3.3 System Settings

Users can check system information in "system settings", and implement the operations of network config, software upgrade, password modification, restore default config and system reboot.

3.3.1 System Info

Select "system settings > System info", you can check the device model and software version; see Figure 3-3 for more details.



System Info

Model PFS4206-4P-96/120

Software Version V1.010.0008.0.R.201610

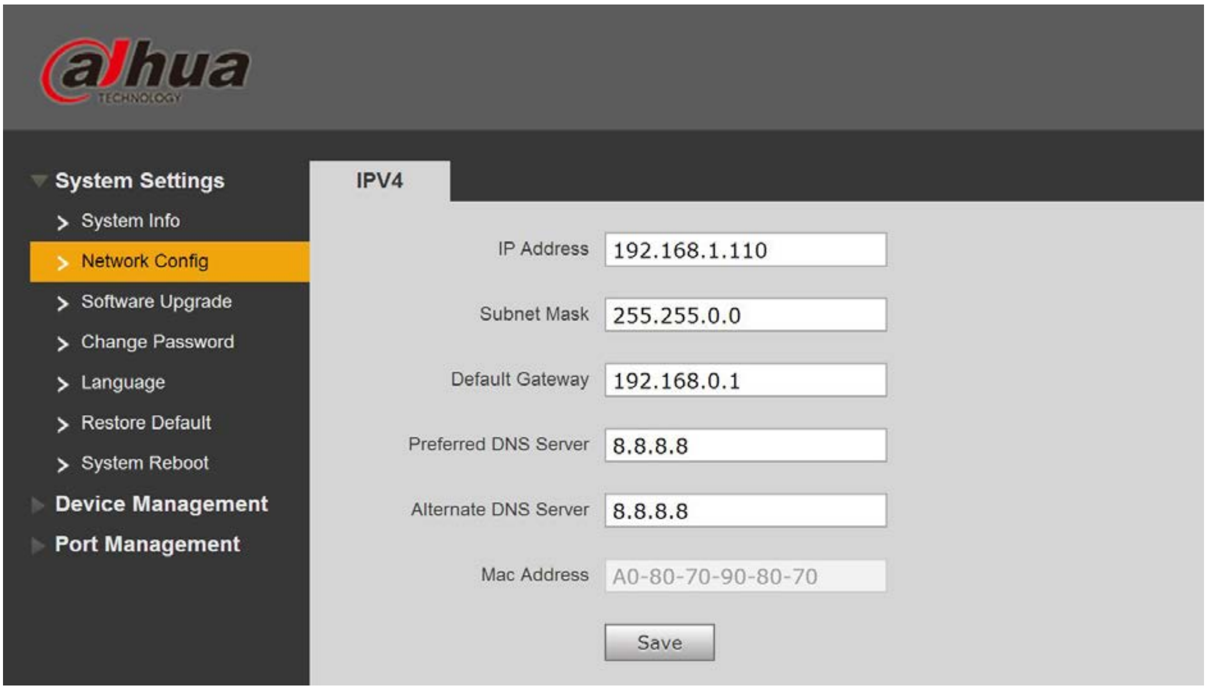
Figure 3-3

3.3.2 Network Config

You can configure device IP address, subnet mask and default gateway via network config.

Step 1

Select "System Settings > Network Config", the system will display the interface which is shown in Figure 3-4 below.



IP Address 192.168.1.110
Subnet Mask 255.255.0.0
Default Gateway 192.168.0.1
Preferred DNS Server 8.8.8.8
Alternate DNS Server 8.8.8.8
Mac Address A0-80-70-90-80-70

Figure 3-4

Step 2
Configure "IP address", "Subnet mask", "Default gateway" and "DNS server".

Step 3
Click "Save" and complete configuration.

3.3.3 Software Upgrade

You can upgrade software to the latest version by software upgrade.
Step 1
Select "System Settings > Software Upgrade", the system will display the interface which is shown in Figure 3-5 below.

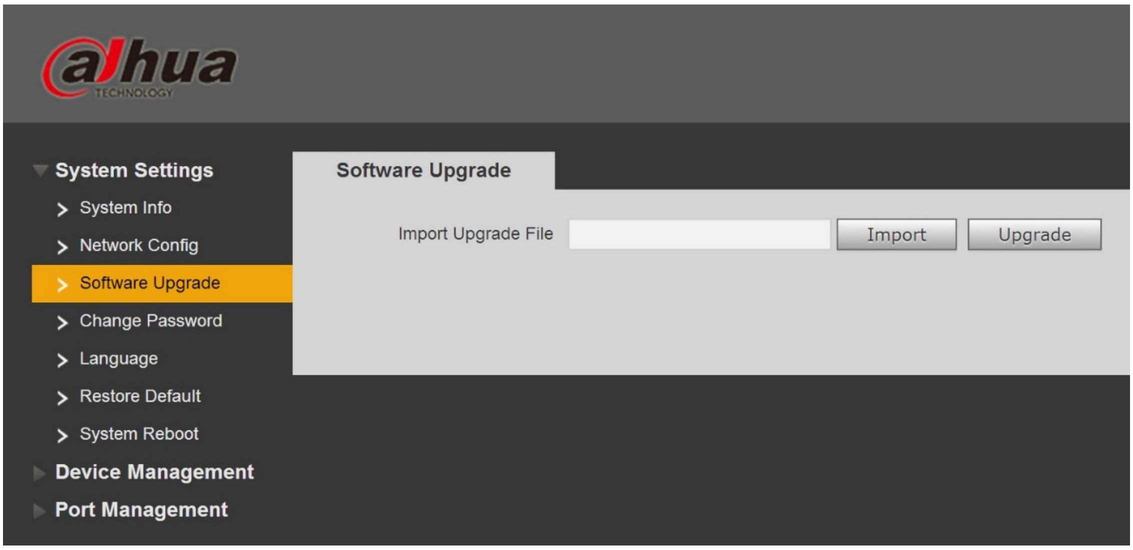


Figure 3-5

Step 2

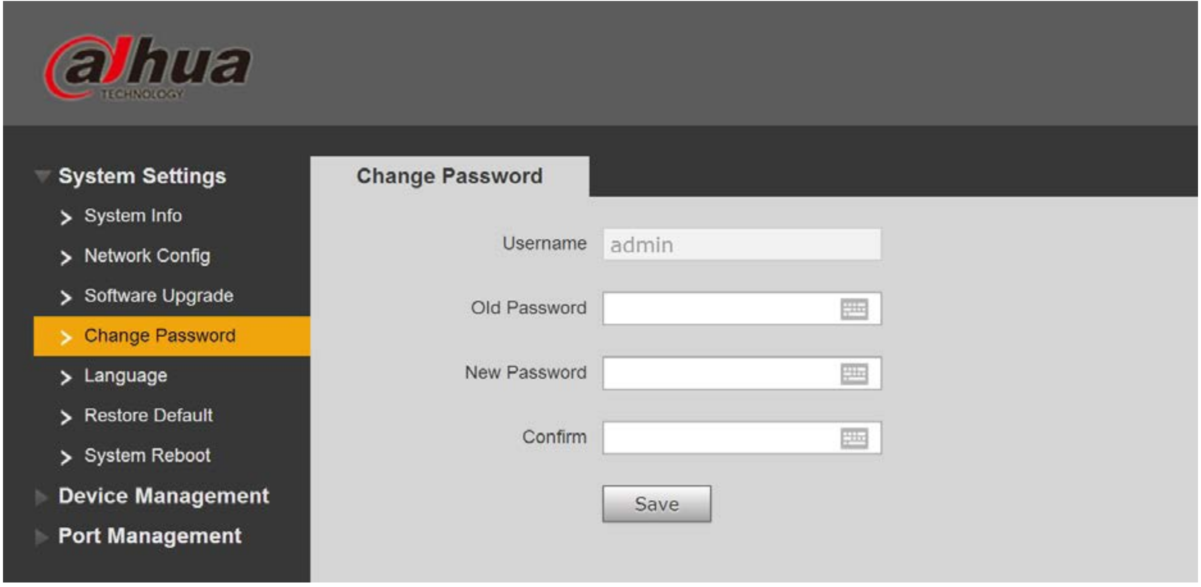
Click "Import" and select the upgrade file.

Step 3

Click "Upgrade".

3.3.4 Change Password

There is no password by default when the device is delivered out of factory. Therefore, you don't need to enter original password when changing password. See Figure 3-6 for more details.



Username admin

Figure 3-6

3.3.5 Restore Default

After you click "Restore Default Config", the system will restore factory default configuration, please operate carefully.

Note:

After clicking "Restore Default Config", IP address won't restore default configuration. See Figure 3-7 for more details.

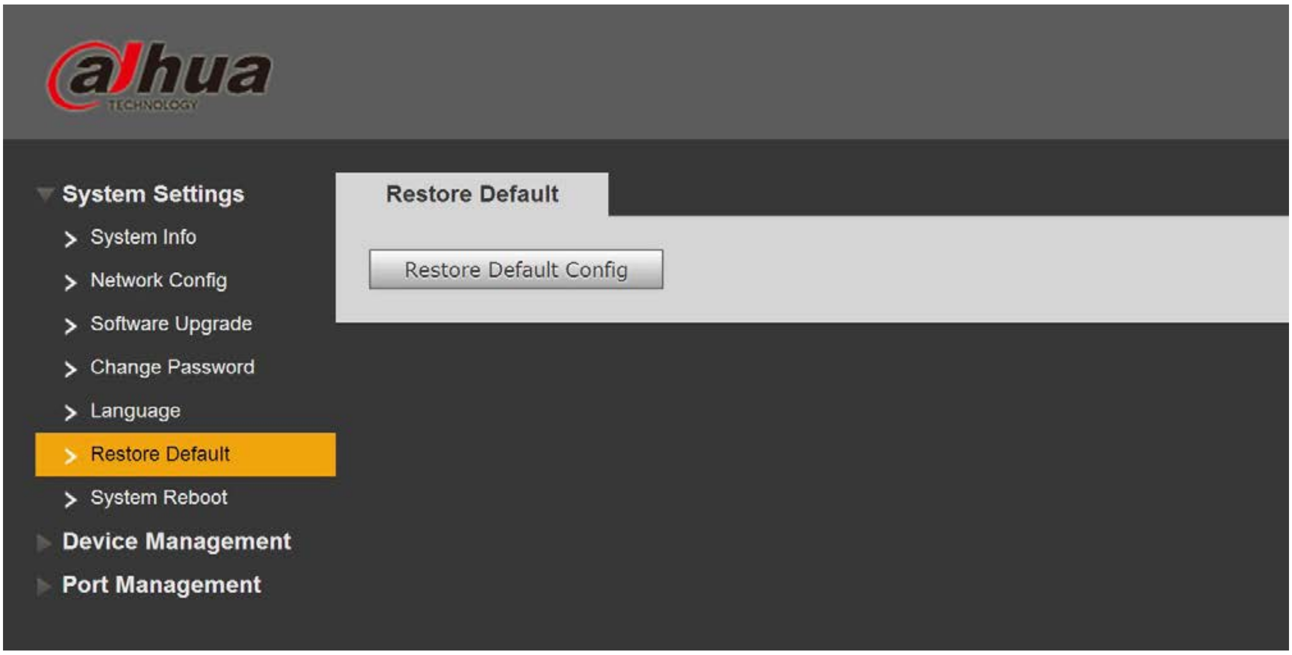


Figure 3-7

3.3.6 System Reboot

You can implement remote reboot operation upon the device via "System Reboot". See Figure 3-8 for more details.

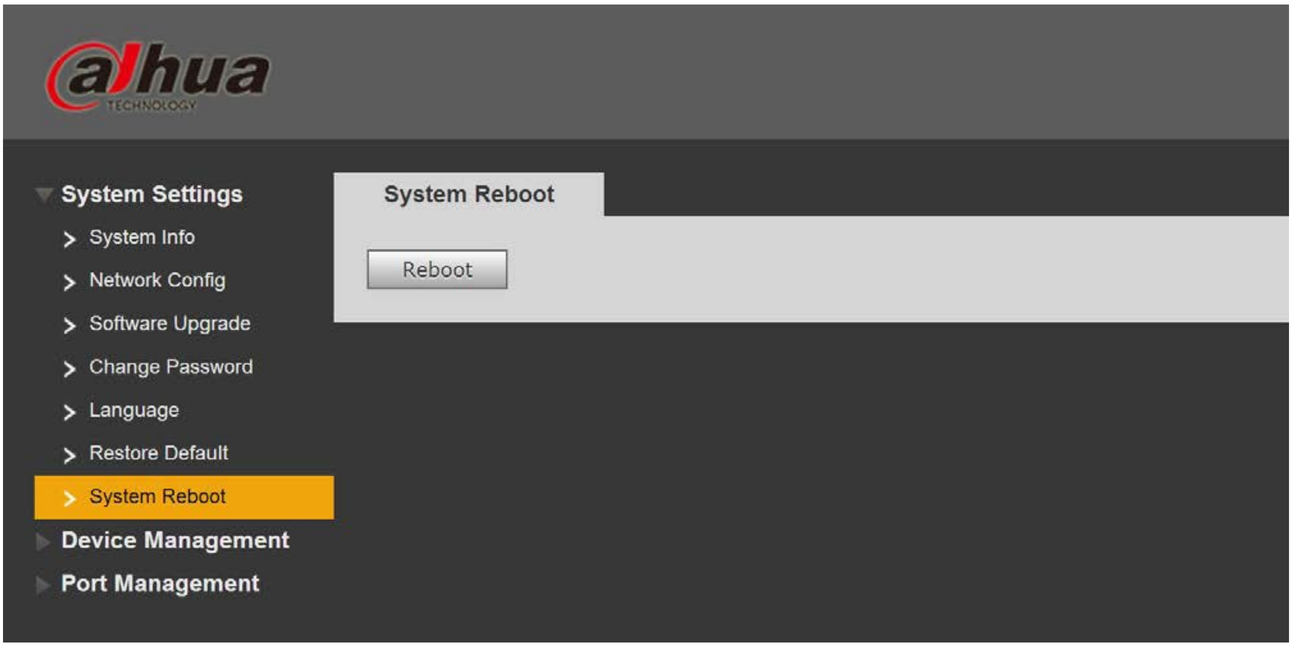


Figure 3-8

3.4 Device Management

You can implement looped network config, serial port config, 802.1Q VLAN config and PORT VLAN config via device management.

3.4.1 Ring Config

RSTP

Step 1

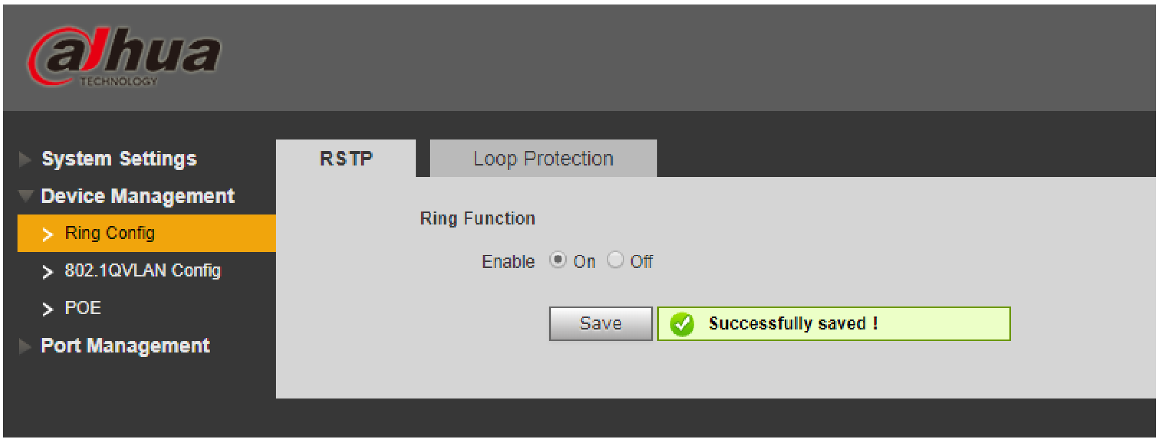
Connect cable according to the ring network mode shown in Figure 3-9.

Step 2

Log in WEB interface, select “System Settings > Device Management > Ring Config > RSTP”, click “Enable”.

Step 3

Click “Save”.



Enable ● On ○ Off

Successfully saved !

Figure 3-12

Loop Protection

Redundancy ring function can be realized via ring network config. Please be noted that the function has to be applied with convergence switch DH-PFS5424-24T or DH-PFS5924-24X. The fastest convergence time is 5s.

Step 1

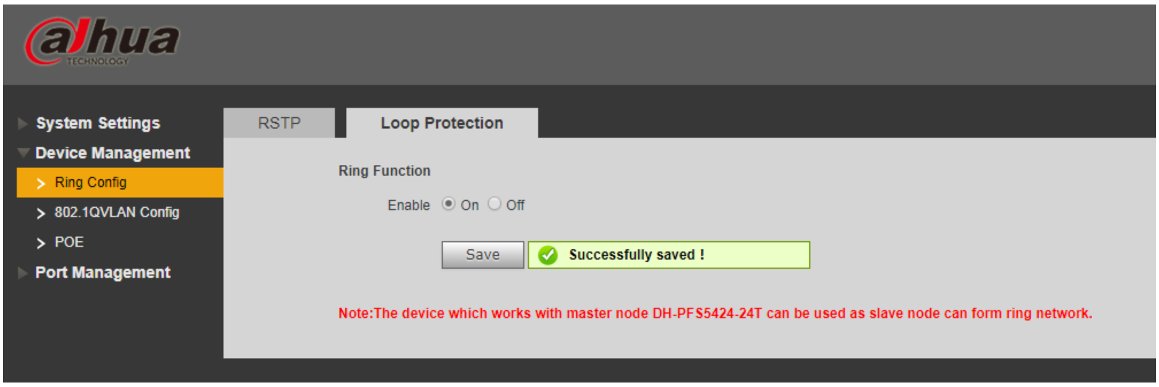
Connect cable according to the ring network mode which is shown in Figure 3-9.

Step 2

Log in WEB interface, select “System settings > Device Management > Ring Config >Loop Protection”, click “Enable”.

Step 3

Click “Save”.



Enable ● On ○ Off

Successfully saved !

Note:The device which works with master node DH-PFS5424-24T can be used as slave node can form ring network.

Figure 3-13

3.4.2 802.1Q VLAN Config

IEEE802.1Q is a protocol with VLAN identifying information for data frame which is authenticated by IEEE, which is also called “Tagging VLAN”. It can recognize max 4096 VLAN, the current configurable range is 1～4094.

- Default VLAN ID number

When the port receives a packet without VLAN Tag, the system will add default VLAN ID of the port, and forward the packet to a port with default VLAN ID.

- VLAN ID number which is allowed to pass

It means the VLAN which is allowed to pass by this port, and the range is 1～4094. When the port sends packet, and if the VLAN ID of this packet is the same as the default VLAN ID, then the system will remove the VLAN Tag of the packet, and send this packet.

Step 1

Select "Device Management > 802.1Q VLAN Config", which is shown in Figure 3-14.

Step 2

Check "Enable 802.1QVLAN Config", which means it is enabled.

Step 3

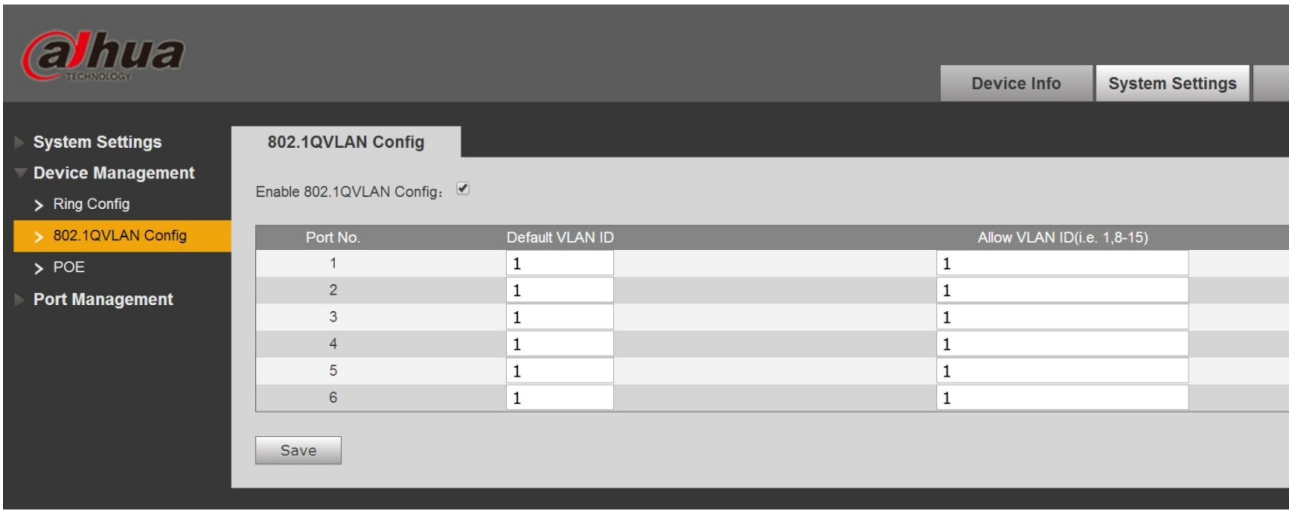
Set "default VLAN ID"; under the situation of default, the default VLAN ID of port is 1.

Step 4

Set VLAN ID which is allowed to pass.

Step 5

Click "Save", and complete the config.



Enable 802.1QVLAN Config: ☑

Port No.	Default VLAN ID	Allow VLAN ID(i.e. 1,8-15)
1	1	1
2	1	1
3	1	1
4	1	1
5	1	1
6	1	1

Figure 3-14

3.4.3 PoE

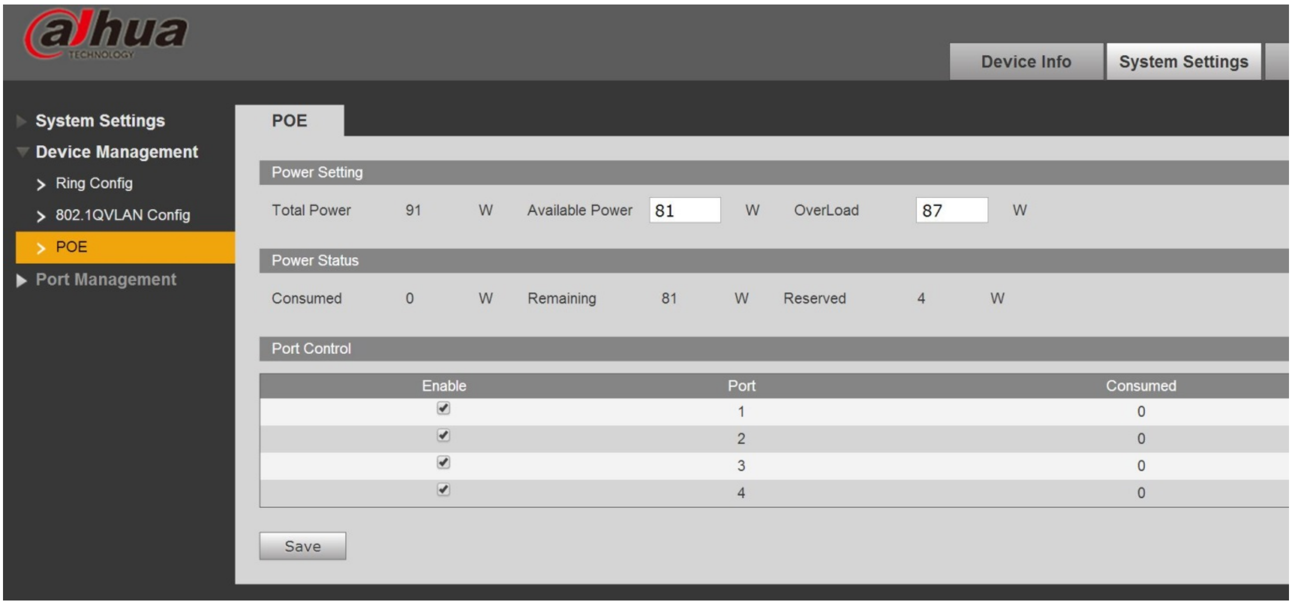
The PoE management page can provide a switch which can control PoE power supply function to the port, set reserved power and overload power and display the current overload situation.

Step 1

Log in WEB interface, select "System Settings > Device Management > PoE", and set remain power and overload, the remain power is 81W by default and the overload is 87W by default.

Step 2

Click "Save".



Power Setting

Total Power 91 W Available Power 81 W OverLoad 87 W

Power Status

Consumed 0 W Remaining 81 W Reserved 4 W

Port Control

Enable	Port	Consumed
☑	1	0
☑	2	0
☑	3	0
☑	4	0

Figure 3-15

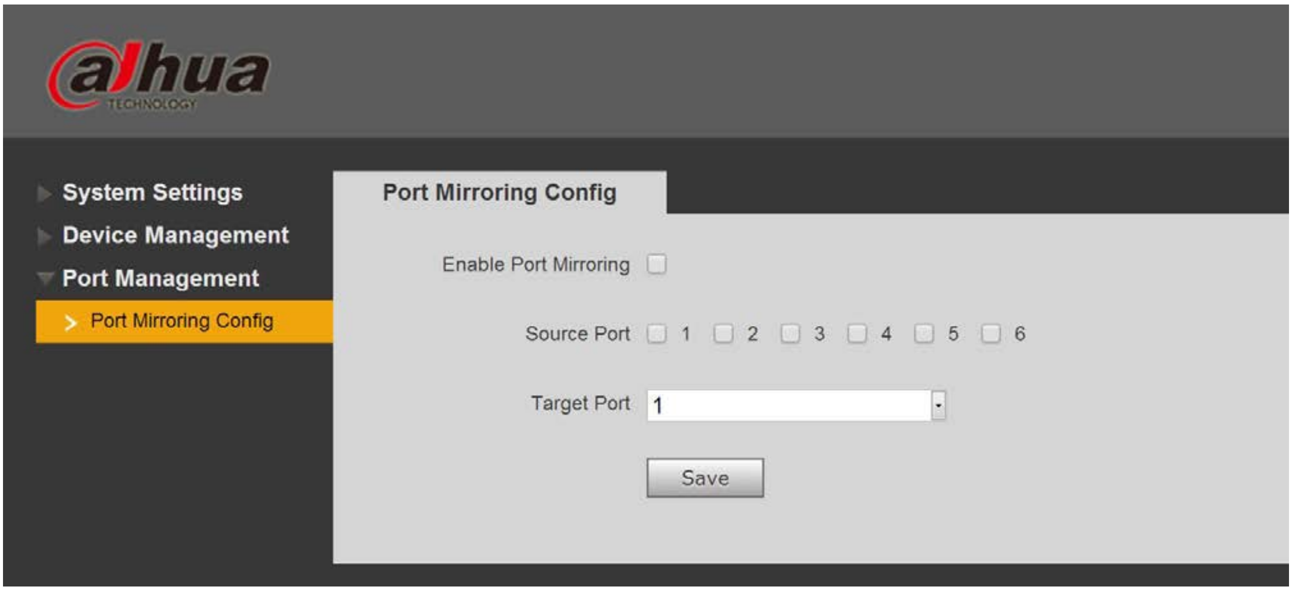
- Available power: the total power of access devices, the new access device will fail to power on if the total power of access devices exceeds the value of remain power.
- Overload power: when the total power of access devices exceeds the value of overload power, power failure will happen in sequence to the device with low priority, the port priority will decrease in sequence.

3.5 Port management

You can implement port mirroring config via port management.

3.5.1 Port Mirroring Config

You can mirror the data of one port to another port by port mirroring, which can help the maintenance staff to locate problems. See Figure 3-16 for more details.



Enable Port Mirroring ☐

Source Port ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6

Target Port 1

Figure 3-16

Step 1

Log in WEB interface, select "System Settings > Port Management > Port Mirroring Config".

Step 2

Enable port mirroring.

Step 3

Select “Source Port” and “Target Port”.

Step 4

Click “Save”.

3.6 SNMP Function

SNMP (Simple Network Management Protocol) is a type of industrial standard which is widely accepted and applied; the purpose of SNMP is to guarantee the transmission of management info between any two spots and makes it convenient for network administrator to search info at any network node and realize modification, capacity planning and report generation. It adopts polling mechanism and provides the most basic functionality set. The device supports SNMP V1 and V2C and provides basic information inquiry of the device status.

4 Installation Guide

PoE switch supports DIN rail mounting. Lay the switch hook on the rail, press the PoE switch to make the buckle get into the slide, see Figure 4-1.

Note:

4-port PoE switch supports the slide width of 28mm.

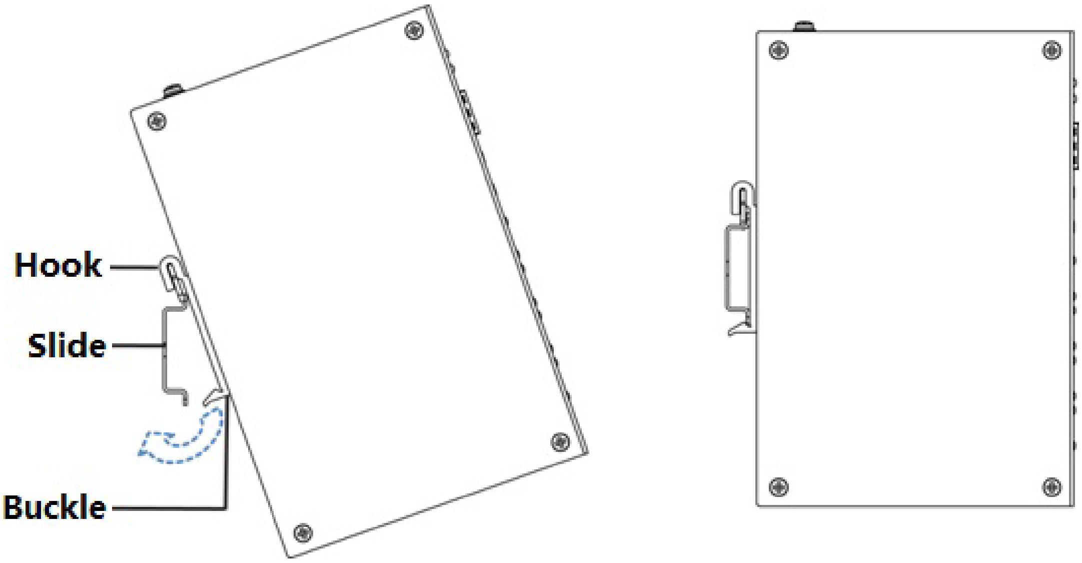


Figure 4-1

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it’s something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the “auto-check for updates” function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

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

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER 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